MATHEMATICAL SURVEYS
NUMBER VI

INTRODUCTION TO THE THEORY OF ALGEBRAIC FUNCTIONS OF ONE VARIABLE

BY

CLAUDE CHEVALLEY

AMERICAN MATHEMATICAL SOCIETY
NEW YORK
1951

КЛОД ШЕВАЛЛЕ

ВВЕДЕНИЕ В ТЕОРИЮ АЛГЕБРАИЧЕСКИХ ФУНКЦИЙ ОТ ОДНОЙ ПЕРЕМЕННОЙ

Перевод с английского
З. И. БОРЕВИЧА

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1959

Настоящая книга посвящена систематическому изложению теории алгебраических функций от одной переменной над произвольным полем констант. Достоинством книги является довольно удачное сочетание стройности изложения, проведенного с учетом последних достижений в абстрактной алгебре, с обилием фактического материала. В последней главе книги дается модернизированное изложение классической теории алгебраических функций от одной переменной над полем комплексных чисел.

Книга представляет интерес для научных работников-математиков, аспирантов и студентов старших курсов математических факультетов, работающих в области алгебры, алгебраической геометрии и теории чисел. Для ее чтения необходимы предварительные сведения из общей теории полей, а в последней главе — некоторые сведения из топологии и теории функций.

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

Алгебраической функцией y от комплексной переменной x называется функция, удовлетворяющая уравнению $F(x, y)=0$, где F — многочлен с комплексными коэффициентами. Таким образом, алгебраическая функция y есть корень уравнения, коэффициентами которого являются рациональные функции от x. Уже в самом определении обнаруживается большое сходство между понятиями алгебраической функции и алгебраического числа; рациональные функции от x при этом играют ту же роль, что и рациональные числа. С другой стороны, уравнение $F(x, y)=0$ можно рассматривать как уравнение кривой на плоскости с координатами x и y, что указывает на тесную связь теории алгебраических функций от одной переменной с алгебраической геометрией.

Естественно ожидать, что при изложении теории алгебраических функций от одной переменной в той или иной мере будет подчеркиваться либо арифметико-алгебраическая сторона этой ветви математики, либо ее геометрическая сторона. И действительно, оба способа изложения одинаково приемлемы и фактически проводились различными математиками. Алгебраический аспект был впервые отчетливо выражен в статье Дедекинда и Вебера (R. Dedekind, H. Weber) „Theorie der algebraischen Funktionen einer Veränderlichen“ (Journ. für Math., 92, 1882, 181—290) и получил дальнейшее развитие в книге Хензеля и Ландсберга (K. Hensel, G. Landsberg) „Theorie der algebraischen Funktionen einer Variablen“ (Leipzig, 1902). Геометрическому подходу следовали Макс Нётер, Клебш, Гордан и вслед за ними геометры итальянской школы [см., в частности, книгу Севери (F. Severi) „Lezioni di Geometria algebrica“, Padova, 1908]. Ясно, что при любом подходе к теории алгебраи-

ческих функций изложению подлежат в основном одни и те же главные результаты. Однако этот общий фактический материал в руках математиков, придерживающихся алгебраического или геометрического направления, будет освещать различные стороны изучаемого предмета. Так как пара „наблюдаемое явление — наблюдатель" является, по-видимому, более реальной сущностью, чем инертное явление, взятое само по себе, то мы должны учитывать разнообразие позиций, с которых та или иная теория может быть сфотографирована. В частности, это относится и к теории алгебраических функций, где, как нам кажется, тот или другой подход возбуждает в математических умах сильные эмоциональные реакции — от искреннего восхищения до открытого пренебрежения. Отсюда, однако, не следует, что при написании книги мы достигнем идеала, если смешаем или синтезируем оба направления: от попытки получить две интересные фотографии предмета на одной и той же пластинке единственным результатом будет неразборчивое изображение. Никоим образом не подвергая сомнению законность геометрического подхода, мы не пытаемся в то же время скрыть свое пристрастие к алгебраическому направлению, которого и придерживались в процессе работы над настоящей книгой.

Главное отличие нашего изложения теории от изложений Дедекинда — Вебера или Хензеля — Ландсберга состоит в том, что у нас полем констант рассматриваемого поля алгебраических функций может быть совершенно произвольное поле, а не только поле комплексных чисел. Необходимость такого обобщения вызвана несколькими причинами. Во-первых, аналогия между алгебраическими функциями и алгебраическими числами становится более глубокой, если рассматривать алгебраические функции над конечным полем констант. В этом случае на поля алгебраических функций можно перенести теорию полей классов, а также трансцендентную теорию дзета-функции и L-рядов (см. F. K. Schmidt, „Analytische Zahlentheorie in Körpern der Charakteristik p", Math. Zeits., 33, 1931, 1—32). Заметим, что доказательство А. Вейля гипотезы Римана для полей алгебраических функций над конечным полем совершенно по-новому осветило, классический случай поля алгебраических чисел (см. A. Weil, „Sur les courbes algébriques et les variétés qui s'en dédui-

sent", Paris, Hermann, 1948; эта книга содержит изложение теории с геометрической точки зрения, которое, однако, несколько отличается от изложения, принятого итальянскими геометрами). Во-вторых, если S — алгебраическая поверхность, а R — поле рациональных функций на S, то R можно рассматривать как поле алгебраических функций от одной переменной над $K\langle x\rangle$, где K — основное поле, а x — отличный от константы элемент из R. Пикар и ряд других математиков для исследования поверхности S весьма успешно применяли метод, состоящий в изучении связей между R и различными полями вида $K\langle x\rangle$ (см. E. Picard и G. Simart, „Théorie des fonctions algébriques de deux variables independantes", Paris, Gauthier — Villars, 1897). Даже в случае, когда K есть поле комплексных чисел, поле $K\langle x\rangle$ не является алгебраически замкнутым. Таким образом возникает необходимость в теории алгебраических функций от одной переменной над полями, которые не являются алгебраически замкнутыми.

Начало теории алгебраических функций от одной переменной над произвольным полем (любой характеристики) было положено работами Хассе, который ввел для этих полей понятие дифференциала (H. Hasse, „Theorie der Differentiale in algebraischen Funktionenkörpern mit vollkommenen Konstantenkörper", Journ. für Math., 172, 1934, 55—64), и Шмидта, доказавшего теорему Римана — Роха (F. K. Schmidt, „Zur arithmetischen Theorie der algebraischen Funktionen. I", Math. Zeits., 41, 1936, 415—438). В настоящей книге определение дифференциалов и доказательство теоремы Римана — Роха приведены в форме, указанной Вейлем (A. Weil, „Zur algebraischen Theorie der algebraischen Funktionen", Journ. für Math., 179, 1938, 129—133).

Что касается содержания книги, то в нее мы включили только элементарную часть теории, оставив в стороне такие ее разделы, как теория полей классов или теория соответствий. Мы руководствовались главным образом желанием изложить надлежащие основы знаний для изучения этих более специальных глав. Именно поэтому с особой обстоятельностью изложена теория расширений полей алгебраических функций от одной переменной, в частности, тех расширений, которые получаются присоединением новых констант, может быть даже трансцендентных над полем

констант первоначального поля функций. То, что рассмотрение таких расширений целесообразно, было убедительно показано работой Дёйринга (M. Deuring) „Arithmetische Theorie der Korrespondenzen algebraischen Funktionenkörper (Journ. für Math., 177, 1937, 161—191). Теория дифференциалов второго рода изложена у нас лишь для случая, когда характеристика рассматриваемого поля равна нулю. Это ограничение вызвано тем, что пока еще не ясно, каково должно быть „хорошее" определение понятия дифференциала второго рода в общем случае: можно ли обойтись лишь условием равенства нулю всех вычетов или же необходимо потребовать, чтобы дифференциал можно было в любой точке аппроксимировать сколь угодно близко точными дифференциалами (или надлежащими их обобщениями)? Здесь возникает ряд проблем, требующих, как нам кажется, специального исследования. [1]) Последняя глава книги посвящена теории полей алгебраических функций от одной переменной над полем комплексных чисел, а также их римановым поверхностям. Определение понятия римановой поверхности с помощью разрезаний и склеиваний мы заменили более абстрактным определением, подсказанным книгой Г. Вейля о римановых поверхностях, которое не требует довольно искусственного выбора специальных образующих поля в виде независимой переменной и функции от этой переменной. Мы обошли также метод триангуляции римановой поверхности, использовав вместо него сингулярную теорию гомологий, развитую С. Эйленбергом.

Большую помощь в написании этой книги мне оказали советы Э. Артина и О. Голдмана, полученные во время наших частых бесед. Выражаю им обоим свою искреннюю благодарность.

---

[1]) Дифференциалы второго рода для полей характеристики $p \neq 0$ рассматриваются в работе Розенлихта (M. Rosenlicht) „Differentials of the second kind for algebraic function fields of one variable" (Ann, of Math., 57, 1953, 517—523). (*Прим. перев.*)

НЕКОТОРЫЕ ОБОЗНАЧЕНИЯ

$\mathrm{Con}_{R/S}$ — конорма из поля R в надполе S (§ 7 гл. IV).

$\mathrm{Cosp}_{R/S}$ — кослед из поля R в надполе S (для распределений: § 7 гл. IV; для дифференциалов: §§ 2 и 6 гл. VI).

$d(\mathfrak{a})$ — степень девизора $\mathfrak{a}$ (§ 7 гл. I).

$\mathfrak{d}(x)$ — дивизор элемента x (§ 8 гл. I).

$\mathfrak{d}(\omega)$ — дивизор дифференциала ω (§ 6 гл. II).

$\delta(\mathfrak{a})$ — размерность пространства дифференциалов, делящихся на дивизор $\mathfrak{a}$ (§ 5 гл. II).

$\partial\gamma$ — граница цепи γ (§ 3 гл. VII).

$H_n(X, Y)$ — n-мерная группа гомологий пространства X по модулю подмножества Y (§ 3 гл. VII).

$\iota(\gamma, \gamma')$ — индекс пересечения 1-цепей γ и γ' (§ 6 гл. VII).

$j(\omega, \omega')$ — см. § 5 гл. VII.

$K\langle\ldots\rangle$ — поле, которое получается из поля K присоединением элемента или множества элементов, указанных между знаками $\langle$ и $\rangle$; специальное значение этого обозначения для полей алгебраических функций от одной переменной определено в § 4 гл. V.

$l(\mathfrak{a})$ — размерность пространства тех элементов, которые делятся на дивизор $\mathfrak{a}$ (§ 1 гл. II).

$\nu_{\mathfrak{p}}$ — функция порядка в точке $\mathfrak{p}$ (для элементов: § 5 гл. I и § 1 гл. III; для распределений: § 4 гл. II; для дифференциалов: § 6 гл. II).

$N_{S/R}$ — норма из поля S в подполе R (§ 7 гл. IV).

$N^{\mathfrak{P}}_{S/R}$ — см. § 5 гл. IV.

$\omega^{\mathfrak{p}}$ — $\mathfrak{p}$-компонента дифференциала ω (§ 7 гл. II).

$\mathrm{res}_{\mathfrak{p}}\,\omega$ — вычет дифференциала ω в точке $\mathfrak{p}$ (§ 5 гл. III).

$\mathrm{Sp}_{S/R}$ — след из поля S в подполе R (для распределений: § 7 гл. IV; для дифференциалов: § 2 гл. VI).

$\mathrm{Sp}^{\mathfrak{P}}_{S/R}$ — см. § 5 гл. IV.

$|\gamma|$ — множество точек цепи γ (§ 3 гл. VII).

ГЛАВА I

ТОЧКИ И ДИВИЗОРЫ

§ 1. Поля алгебраических функций от одной переменной

Пусть K — поле. *Полем алгебраических функций от одной переменной над полем* K называется поле R, содержащее K в качестве подполя и являющееся алгебраическим расширением конечной степени поля $K\langle x\rangle$[1]) при некотором трансцендентном над K элементе $x \in R$.

Элемент x определен, конечно, не однозначно. Если x' — любой другой элемент поля R, трансцендентный над K, то R является также алгебраическим расширением конечной степени поля $K\langle x'\rangle$. Действительно, так как степень трансцендентности поля R над K равна единице, то R алгебраично на $K\langle x'\rangle$. В частности, элемент x алгебраичен над $K\langle x'\rangle$, и поле $K\langle x, x'\rangle$ имеет конечную степень над $K\langle x'\rangle$. Так как степень поля R над $K\langle x\rangle$ конечна, то степень R над $K\langle x, x'\rangle$ также будет конечной. Этим доказано, что R имеет конечную степень над $K\langle x'\rangle$.

Элементы поля R, алгебраические над K, называются *константами*. Все константы образуют подполе K' поля R, называемое *полем констант*. Поле R является также полем алгебраических функций от одной переменной над K'. Действительно, всякий элемент x из R, трансцендентный над K, будет также трансцендентным над K', и поле R, являющееся алгебраическим расширением конечной степени поля $K\langle x\rangle$, будет также алгебраическим расширением конечной степени над $K'\langle x\rangle$.

---

[1]) Если K — подполе и A — подмножество поля R, то через $K\langle A\rangle$ в книге обозначается наименьшее подполе поля R, содержащее K и A. Подкольцо поля R, порожденное полем K и подмножеством A, обозначается, как обычно, через $K[A]$. (*Прим. перев.*)

Важно иметь в виду, что при изучении поля R алгебраических функций от одной переменной мы фактически рассматриваем свойства не одного поля R, а свойства пары полей K и R. Пусть, например, Z есть некоторое поле и пусть $R = Z\langle x, y, z\rangle$, где x и y алгебраически независимы над Z, а элемент z алгебраичен над $Z\langle x, y\rangle$. Положим $K_1 = Z\langle x\rangle$, $K_2 = Z\langle y\rangle$. Тогда поле R будет полем алгебраических функций от одной переменной над каждым из полей K_1 или K_2; однако его свойства как поля алгебраических функций от одной переменной над K_1 могут существенно отличаться от его свойств как поля алгебраических функций от одной переменной над K_2.

Заметим, однако, что при изучении поля R алгебраических функций от одной переменной над полем K все чаще вместо поля K в качестве более существенного объекта будет выступать поле констант поля R, а само поле K постепенно будет отходить на задний план.

§ 2. Точки

Пусть R — поле и K — его подполе. Под *V-кольцом* в R (над K) будем понимать подкольцо $\mathfrak{o}$ поля R, удовлетворяющее следующим условиям:

1) $\mathfrak{o}$ содержит поле K;

2) $\mathfrak{o}$ не совпадает с R;

3) если элемент x из R не содержится в $\mathfrak{o}$, то x^{-1} содержится в $\mathfrak{o}$.

Пусть $\mathfrak{o}$ есть V-кольцо. Элементы кольца $\mathfrak{o}$, не являющиеся делителями единицы в $\mathfrak{o}$ (будем их называть необратимыми элементами), образуют идеал $\mathfrak{p}$ в кольце $\mathfrak{o}$. Действительно, если x необратим и $z \in \mathfrak{o}$, то xz также необратим, так как, если бы элемент xz обладал в кольце $\mathfrak{o}$ обратным элементом u, то элемент zu принадлежал бы кольцу $\mathfrak{o}$ и был бы обратным для x. Далее, пусть x и y — необратимые элементы из $\mathfrak{o}$. Если хоть один из элементов x или y равен 0, то $x - y$, очевидно, необратим. Если x и y отличны от 0, то по крайней мере один из пары взаимно обратных элементов $\frac{x}{y}$ и $\frac{y}{x}$ находится в кольце $\mathfrak{o}$. Если $\frac{x}{y} \in \mathfrak{o}$, то $x - y = y\left(\frac{x}{y} - 1\right)$ необратим; если $\frac{y}{x} \in \mathfrak{o}$, то $x - y = x\left(1 - \frac{y}{x}\right)$

также необратим. Таким образом, элементы, не являющиеся делителями единицы в кольце $\mathfrak{o}$, образуют идеал $\mathfrak{p}$. Всякий идеал кольца $\mathfrak{o}$, содержащий $\mathfrak{p}$ и отличный от $\mathfrak{p}$, содержит делителя единицы, а потому совпадает с $\mathfrak{o}$.

Пусть теперь R — поле алгебраических функций от одной переменной над полем K. Под *точкой* в R будем понимать подмножество $\mathfrak{p}$ поля R, которое является идеалом, состоящим из всех необратимых элементов некоторого V-кольца $\mathfrak{o}$ поля R (над K). Это V-кольцо однозначно определено заданием $\mathfrak{p}$. В самом деле, $\mathfrak{o}$ есть множество всех тех $x \in R$, для которых $x\mathfrak{p} \subset \mathfrak{p}$ (под $x\mathfrak{p}$ мы понимаем множество произведений элемента x на элементы из $\mathfrak{p}$). Чтобы показать это, заметим прежде всего, что каждый элемент $x \in \mathfrak{o}$ обладает требуемым свойством; с другой стороны, если $x \notin \mathfrak{o}$, то x^{-1} находится в кольце $\mathfrak{o}$ и не является делителем единицы, а значит $x^{-1} \in \mathfrak{p}$, $1 \in x\mathfrak{p}$ и $x\mathfrak{p} \not\subset \mathfrak{p}$. Кольцо $\mathfrak{o}$ называется *кольцом точки* $\mathfrak{p}$. Элементы из $\mathfrak{o}$ называются *целыми* в точке $\mathfrak{p}$.

Так как каждый элемент кольца $\mathfrak{o}$, не принадлежащий $\mathfrak{p}$, является делителем единицы в $\mathfrak{o}$, то фактор-кольцо $\mathfrak{o}/\mathfrak{p}$ есть поле. Это поле называется *полем вычетов* в точке $\mathfrak{p}$.

Кольцо $\mathfrak{o}$ цело-замкнуто в R, т. е. каждый элемент x из R, удовлетворяющий уравнению вида

$$x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0,$$

где $a_1, \ldots, a_n$ принадлежат $\mathfrak{o}$, сам принадлежит кольцу $\mathfrak{o}$. Действительно, если бы это было не так, то x^{-1} принадлежал бы $\mathfrak{p}$ и мы имели бы

$$1 = -\sum_{i=1}^{n} a_i (x^{-1})^i \in \mathfrak{p},$$

что невозможно. Отсюда, в частности, следует, что кольцо любой точки содержит поле констант K' поля R. Это показывает, что понятие точки в поле R не зависит от того, рассматриваем ли мы R как поле алгебраических функций над K или над K'. С другой стороны, мы имеем $K' \cap \mathfrak{p} = \{0\}$; следовательно, естественный гомоморфизм кольца $\mathfrak{o}$ на поле вычетов $\Sigma = \mathfrak{o}/\mathfrak{p}$ точки $\mathfrak{p}$ отображает K' изоморфно на подполе поля Σ. В дальнейшем удобно будет считать, что Σ

является расширением поля K'; это равносильно отождествлению элементов поля K' с их классами вычетов по модулю $\mathfrak{p}$.

§ 3. Точки поля $K\langle x\rangle$

Рассмотрим частный случай, когда $R=K\langle x\rangle$, где элемент x, разумеется, трансцендентен над K. Пусть $f=f(x)$ — неприводимый многочлен от x с коэффициентами из K. Каждый элемент u из R может быть записан в виде $u=\frac{g}{h}$, где g и h принадлежат кольцу $K[x]$. Пусть $\mathfrak{o}_f$ есть множество элементов u вида $\frac{g}{h}$, где h не делится на f. Так как f неприводим, то произведение многочленов делится на f только в случае, если хоть один из сомножителей делится на f. Формулы

$$\frac{g_1}{h_1}-\frac{g_2}{h_2}=\frac{g_1h_2-g_2h_1}{h_1h_2},\quad \frac{g_1}{h_1}\cdot\frac{g_2}{h_2}=\frac{g_1g_2}{h_1h_2}$$

показывают, что $\mathfrak{o}_f$ есть подкольцо поля R. Ясно, что это подкольцо содержит K. Кроме того, $\frac{1}{f}$ не содержится в $\mathfrak{o}_f$, так как, если мы запишем $\frac{1}{f}=\frac{g}{h}$, где g и h — многочлены от x, то $h=gf$ делится на f; этим показано, что $\mathfrak{o}_f\neq R$. Далее, пусть u — любой элемент из R, не содержащийся в $\mathfrak{o}_f$. Запишем u в виде $\frac{g}{h}$, где g и h — многочлены от x без общих множителей. Так как $u\notin\mathfrak{o}_f$, то h делится на f, а значит, g не делится на f, откуда $u^{-1}=\frac{g}{h}\in\mathfrak{o}_f$. Таким образом, $\mathfrak{o}_f$ есть V-кольцо; обозначим через $\mathfrak{p}_f$ соответствующую точку. Ясно, что $\mathfrak{p}_f$ состоит из всех элементов вида $\frac{fg}{h}$, где g и h — многочлены от x, причем h не делится на f.

Итак, каждому неприводимому многочлену f от x с коэффициентами из K мы сопоставили точку $\mathfrak{p}_f$ поля $K\langle x\rangle$. Если f и f' существенно различные неприводимые многочлены $\left(\text{т. е. } \frac{f'}{f} \text{ не принадлежит } K\right)$, то точки $\mathfrak{p}_f$ и $\mathfrak{p}_{f'}$ раз-

личны, ибо f^{-1} принадлежит кольцу $\mathfrak{o}_{f'}$, но не принадлежит кольцу $\mathfrak{o}_f$.

Заметим теперь, что при $x'=x^{-1}$ имеем $K\langle x'\rangle=K\langle x\rangle$. Отсюда следует, что каждому неприводимому многочлену от x' с коэффициентами из K также соответствует точка поля $K\langle x\rangle$. Это относится, в частности, и к неприводимому многочлену x'; точку, определяемую посредством x', будем обозначать через $\mathfrak{p}_{\frac{1}{x}}$, а кольцо этой точки — через $\mathfrak{o}_{\frac{1}{x}}$. Точка $\mathfrak{p}_{\frac{1}{x}}$ отлична от всех точек $\mathfrak{p}_f$, определенных выше, так как, если f есть произвольный неприводимый многочлен от x, то $x\in\mathfrak{o}_f$, в то время как x, очевидно, не принадлежит кольцу $\mathfrak{o}_{\frac{1}{x}}$.

Утверждаем теперь, что точки $\mathfrak{p}_f$ (для всех неприводимых многочленов f от x с коэффициентами из K) и $\mathfrak{p}_{\frac{1}{x}}$ исчерпывают собой все точки поля R. Пусть $\mathfrak{p}$ — произвольная точка поля R, а $\mathfrak{o}$ — ее кольцо. Предположим сначала, что $x\in\mathfrak{o}$. Так как $\mathfrak{o}$ является кольцом и содержит K, то $\mathfrak{o}$ содержит все кольцо $K[x]$. Так как $\mathfrak{p}$ является, очевидно, простым идеалом в $\mathfrak{o}$, то $\mathfrak{p}\cap K[x]$ есть простой идеал в $K[x]$. Значит, идеал $\mathfrak{p}\cap K[x]$ либо является нулевым идеалом, либо состоит из всех многочленов, делящихся на некоторый неприводимый многочлен f. Если бы имел место первый случай, то каждый элемент $\neq 0$ из $K[x]$ являлся бы делителем единицы в $\mathfrak{o}$, откуда немедленно следовало бы, что каждый элемент из R принадлежит $\mathfrak{o}$, а это невозможно. Значит, $\mathfrak{p}\cap K[x]$ состоит из многочленов, делящихся на некоторый неприводимый многочлен f. Если g и h принадлежат $K[x]$, и h не делится на f, то h не принадлежит $\mathfrak{p}$ и, значит, является делителем единицы в $\mathfrak{o}$, откуда $gh^{-1}\in\mathfrak{o}$; этим доказано, что кольцо $\mathfrak{o}$ содержит $\mathfrak{o}_f$. Пусть u есть элемент из R, не принадлежащий кольцу $\mathfrak{o}_f$; тогда можно записать $u=\frac{g}{h}$, где g и h — многочлены из $K[x]$, не имеющие общих множителей, причем h делится на f. Если бы элемент u принадлежал $\mathfrak{o}$, то $h^{-1}=g^{-1}u$ также принадлежал бы $\mathfrak{o}$; но это невозможно, ибо элемент h, находясь в $\mathfrak{p}$, не является делителем единицы в $\mathfrak{o}$. Таким образом, доказано, что при $x\in\mathfrak{o}$ точка $\mathfrak{p}$ есть одна из точек $\mathfrak{p}_f$. Если x не

принадлежит $\mathfrak{o}$, то $x' = x^{-1}$ принадлежит кольцу $\mathfrak{o}$, а тогда $\mathfrak{p} \cap K[x']$ состоит из всех элементов кольца $K[x']$, делящихся (в кольце $K[x']$) на некоторый неприводимый многочлен $f'(x')$ от x' с коэффициентами из K. Так как элемент x' не является делителем единицы в $\mathfrak{o}$, то он содержится в $\mathfrak{p} \cap K[x']$ и, значит, делится на $f'(x')$ в $K[x']$. Можно предположить, следовательно, что $f' = x'$. Таким образом, точка $\mathfrak{p}$ в этом случае совпадает с точкой $\mathfrak{p}_{\frac{1}{x}}$.

Очевидно, что для неприводимого многочлена f от x с коэффициентами из K точка $\mathfrak{p}_f$ является главным идеалом в кольце $\mathfrak{o}_f$, порожденным многочленом f: $\mathfrak{p}_f = f\mathfrak{o}_f$. Аналогично, $\mathfrak{p}_{\frac{1}{x}} = \frac{1}{x}\mathfrak{o}_{\frac{1}{x}}$.

Пусть $\mathfrak{p}$—произвольная точка поля $R = K\langle x\rangle$. Обозначим через $\mathfrak{o}$ кольцо точки $\mathfrak{p}$ и через t образующий элемент идеала $\mathfrak{p}$ (т. е. $\mathfrak{p} = t\mathfrak{o}$). Тогда ни один из отличных от нуля элементов кольца $\mathfrak{o}$ не может принадлежать всем идеалам $t^n\mathfrak{o}$ при всех $n > 0$. Действительно, предположим сначала, что $\mathfrak{o} = \mathfrak{o}_f$ для некоторого неприводимого многочлена f от x. Пусть элемент $u = \frac{g}{h}$ из $\mathfrak{o}$ принадлежит всем $t^n\mathfrak{o}$ для всех n (g и h принадлежат $K[x]$, причем h не делится на f). Так как $\mathfrak{p} = t\mathfrak{o} = f\mathfrak{o}$, то, как легко видеть, $t^n\mathfrak{o} = f^n\mathfrak{o}$. По предположению для каждого n мы имеем равенство $\frac{g}{h} = \frac{f^n g_n}{h_n}$, где g_n и h_n принадлежат $K[x]$, причем h_n не делится на f. Так как многочлен f неприводим и не делит h_n, то из $gh_n = f^n g_n h$ легко следует, что f^n делит g. Так как это верно для каждого n, то $g = 0$, откуда $u = 0$. Аналогичное рассуждение применимо и для случая $\mathfrak{o} = \mathfrak{o}_{\frac{1}{x}}$.

Отбросим теперь на некоторое время предположение о том, что поле R имеет вид $K\langle x\rangle$. Пусть R есть поле алгебраических функций от одной переменной над K и пусть $\mathfrak{p}$ есть точка поля R, удовлетворяющая условию:

Кольцо $\mathfrak{o}$ точки $\mathfrak{p}$ содержит такой элемент t, что $\mathfrak{p} = t\mathfrak{o}$ и $\bigcap_{n=1}^{\infty} t^n\mathfrak{o} = \{0\}$. (Ниже мы увидим, что каждая точка поля R удовлетворяет этому условию). Если $x \in R$, то существует по крайней мере одно такое целое n (которое может

быть отрицательным), что $x \in t^n\mathfrak{o}$. В самом деле, если $x \in \mathfrak{o}$, то мы можем взять $n = 0$. Если же это не так, то x^{-1} принадлежит $\mathfrak{o}$ и $\neq 0$; поэтому существует такое целое $m > 0$, что $x^{-1} \in t^m\mathfrak{o}$, $x^{-1} \notin t^{m+1}\mathfrak{o}$; значит, $t^{-m}x^{-1}$ принадлежит $\mathfrak{o}$, но не принадлежит $t\mathfrak{o} = \mathfrak{p}$, т. е. $t^{-m}x^{-1}$ является делителем единицы в $\mathfrak{o}$, и, следовательно, $x = t^{-m}(t^{-m}x^{-1})^{-1}$ принадлежит $t^{-m}\mathfrak{o}$. Если $x \neq 0$, то по предположению существует наибольшее целое n такое, что $x \in t^n\mathfrak{o}$; обозначим это целое число через $\nu_{\mathfrak{p}}(x)$. Для элементов x и y из R, не равных 0, имеем

$$\nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(y) = \nu_{\mathfrak{p}}(xy), \tag{1}$$

а, если $x + y \neq 0$, то

$$\nu_{\mathfrak{p}}(x+y) \geqslant \min\{\nu_{\mathfrak{p}}(x),\ \nu_{\mathfrak{p}}(y)\}. \tag{2}$$

В самом деле, xy, очевидно, принадлежит $t^{\nu_{\mathfrak{p}}(x)+\nu_{\mathfrak{p}}(y)}\mathfrak{o}$; значит, $\nu_{\mathfrak{p}}(xy) \geqslant \nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(y)$. В частности, $0 = \nu_{\mathfrak{p}}(1) \geqslant \nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(x^{-1})$, т. е. $\nu_{\mathfrak{p}}(x^{-1}) \leqslant -\nu_{\mathfrak{p}}(x)$. Далее, $x = t^{\nu_{\mathfrak{p}}(x)}u$, где u принадлежит $\mathfrak{o}$, но не принадлежит $t\mathfrak{o} = \mathfrak{p}$; так как u является делителем единицы в $\mathfrak{o}$, то из равенства $x^{-1} = t^{-\nu_{\mathfrak{p}}(x)}u^{-1}$ вытекает $\nu_{\mathfrak{p}}(x^{-1}) \geqslant -\nu_{\mathfrak{p}}(x)$, откуда $\nu_{\mathfrak{p}}(x^{-1}) = -\nu_{\mathfrak{p}}(x)$. Получаем теперь $\nu_{\mathfrak{p}}(y) = \nu_{\mathfrak{p}}(xyx^{-1}) \geqslant \nu_{\mathfrak{p}}(xy) - \nu_{\mathfrak{p}}(x)$, что вместе с вышеполученным неравенством дает $\nu_{\mathfrak{p}}(xy) = \nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(y)$. Для доказательства неравенства (2) положим $\mu = \min\{\nu_{\mathfrak{p}}(x),\ \nu_{\mathfrak{p}}(y)\}$, тогда $x \in t^{\mu}\mathfrak{o}$, $y \in t^{\mu}\mathfrak{o}$, откуда $x + y \in t^{\mu}\mathfrak{o}$ и $\nu_{\mathfrak{p}}(x+y) \geqslant \mu$.

Чтобы завершить определение функции $\nu_{\mathfrak{p}}$ (которая еще не определена для 0), условимся писать $\nu_{\mathfrak{p}}(0) = \infty$, считая, что для символа ∞ справедливы следующие положения: $\infty > n$ для каждого целого n; $\infty \geqslant \infty$; $\infty + n = \infty$ для каждого целого n; $\infty + \infty = \infty$. Приняв во внимание эти соглашения, убеждаемся, что формулы (1) и (2) справедливы всегда.

Можно заметить, что при $\nu_{\mathfrak{p}}(x) \neq \nu_{\mathfrak{p}}(y)$ имеет место равенство $\nu_{\mathfrak{p}}(x+y) = \min\{\nu_{\mathfrak{p}}(x),\ \nu_{\mathfrak{p}}(y)\}$. Действительно, пусть $\nu_{\mathfrak{p}}(x) < \nu_{\mathfrak{p}}(y)$, тогда

$$\nu_{\mathfrak{p}}(x) = \nu_{\mathfrak{p}}(x+y-y) \geqslant \min\{\nu_{\mathfrak{p}}(x+y),\ \nu_{\mathfrak{p}}(-y)\},$$

но, как легко видеть, $\nu_{\mathfrak{p}}(-y) = \nu_{\mathfrak{p}}(-1) + \nu_{\mathfrak{p}}(y) = \nu_{\mathfrak{p}}(y)$; таким образом, неравенство $\nu_{\mathfrak{p}}(x+y) > \nu_{\mathfrak{p}}(x)$ невозможно.

В более общем случае индукцией по m легко доказы-

вается, что для любых элементов $x_1, \ldots, x_m$ поля R имеем

$$\nu_{\mathfrak{p}}(x_1 + \ldots + x_m) \geqslant \min\{\nu_{\mathfrak{p}}(x_1), \ldots, \nu_{\mathfrak{p}}(x_m)\},$$

причем, если имеется только один индекс i, такой, что $\nu_{\mathfrak{p}}(x_i) = \min\{\nu_{\mathfrak{p}}(x_1), \ldots, \nu_{\mathfrak{p}}(x_m)\}$, то в этом неравенстве фактически будет иметь место знак равенства.

Определение функции $\nu_{\mathfrak{p}}$ зависело от выбора элемента t, такого, что $\mathfrak{p} = t\mathfrak{o}$; в действительности функция $\nu_{\mathfrak{p}}$ зависит только от точки $\mathfrak{p}$. В самом деле, пусть t' — произвольный элемент из $\mathfrak{p}$ такой, что $\mathfrak{p} = t'\mathfrak{o}$. Тогда $t = t'u$, где $u \in \mathfrak{o}$, а так как $t' \in t\mathfrak{o}$, то $u^{-1} \in \mathfrak{o}$. Отсюда следует, что $t^n\mathfrak{o} \subset t'^n\mathfrak{o}$ и $t'^n\mathfrak{o} \subset t^n\mathfrak{o}$ для всех n, и наше утверждение доказано. Функция $\nu_{\mathfrak{p}}$ называется *функцией порядка* в точке $\mathfrak{p}$; если $x \in R$, то $\nu_{\mathfrak{p}}(x)$ называется *порядком* элемента x в точке $\mathfrak{p}$. Так как кольцо $\mathfrak{o}$ точки $\mathfrak{p}$ состоит из всех тех элементов x, для которых $\nu_{\mathfrak{p}}(x) \geqslant 0$, то функция порядка в точке $\mathfrak{p}$ вполне определяет эту точку. Элементами точки $\mathfrak{p}$ являются те элементы, порядок которых > 0; делители единицы кольца $\mathfrak{o}$ — это элементы порядка 0. Элементы t, для которых $\mathfrak{p} = t\mathfrak{o}$, имеют порядок 1; они называются *униформизирующими переменными в точке* $\mathfrak{p}$.

Вернемся теперь к случаю, когда поле R имеет вид $K\langle x\rangle$, предположив дополнительно, что K есть поле комплексных чисел. Если $a \in K$, то $x - a$ является неприводимым многочленом, и каждый неприводимый многочлен от x с коэффициентами из K имеет вид $\lambda(x - a)$, $\lambda \in K$, $\lambda \neq 0$. Обозначим через $\mathfrak{p}_a$ точку, соответствующую неприводимому многочлену $x - a$. Многочлены h от x, делящиеся на $x - a$, характеризуются условием $h(a) = 0$. Поэтому кольцо $\mathfrak{o}_a$ точки $\mathfrak{p}_a$ состоит из рациональных дробей, для которых число a не является полюсом, а сама точка $\mathfrak{p}_a$ состоит из рациональных дробей, для которых a является нулем. Далее, пусть ν_a есть функция порядка в точке $\mathfrak{p}_a$, тогда всякая рациональная дробь $u \neq 0$ может быть представлена в виде $(x - a)^{\nu_a(u)} v$, где для v число a не является ни нулем, ни полюсом. Таким образом, если $\nu_a(u) > 0$, то для u число a является нулем порядка $\nu_a(u)$, а если $\nu_a(u) < 0$, то — полюсом порядка $-\nu_a(u)$.

Обобщая эту терминологию, введем следующие определения (для поля R алгебраических функций от одной переменной над полем K):

Пусть $\mathfrak{p}$ — точка поля R. Если элемент $x \in R$ принадлежит $\mathfrak{p}$, то будем говорить, что $\mathfrak{p}$ является *нулем* элемента x; если же $x^{-1} \in \mathfrak{p}$, то говорим, что $\mathfrak{p}$ является *полюсом* x. Более того, если в точке $\mathfrak{p}$ существует функция порядка $\nu_{\mathfrak{p}}$, то при $\nu_{\mathfrak{p}}(x) > 0$ говорим, что $\mathfrak{p}$ является *нулем порядка* $\nu_{\mathfrak{p}}(x)$ для элемента x, а при $\nu_{\mathfrak{p}}(x) < 0$ — *полюсом порядка* — $\nu_{\mathfrak{p}}(x)$.

Рассмотрим, в частности, случай $R = K\langle x\rangle$ и $\mathfrak{p} = \mathfrak{p}_{\frac{1}{x}}$. Пусть $g = a_0x^n + a_1x^{n-1} + \ldots + a_n$ есть многочлен степени n от x с коэффициентами из K. Полагая $x' = x^{-1}$, имеем

$$g = x'^{-n}(a_0 + a_1x' + \ldots + a_nx'^n).$$

Выражение $a_0 + a_1x' + \ldots + a_nx'^n$ принадлежит кольцу $\mathfrak{o}$ точки $\mathfrak{p}$ и не принадлежит $\mathfrak{p}$ (так как $a_0 \neq 0$). Поэтому для многочлена от x степени n точка $\mathfrak{p}_{\frac{1}{x}}$ является полюсом порядка n. Если $u = \frac{g}{h} \in R$, где g и h — многочлены от x, то порядок элемента u в точке $\mathfrak{p}$ равен, очевидно, разности между степенями многочленов h и g.

Все еще предполагая, что $R = K\langle x\rangle$, для неприводимого многочлена f от x с коэффициентами из K исследуем поле вычетов Σ точки $\mathfrak{p}_f$, т. е. кольцо $\mathfrak{o}_f/\mathfrak{p}_f$. Положим $\mathfrak{q} = \mathfrak{p}_f \cap K[x]$; тогда классы вычетов по модулю $\mathfrak{p}_f$, имеющие представителей из кольца $K[x]$, образуют подкольцо Σ_1 кольца Σ, изоморфное фактор-кольцу $K[x]/\mathfrak{q}$. Но $\mathfrak{q}$ состоит из многочленов, делящихся на f в $K[x]$, поэтому $K[x]/\mathfrak{q}$ есть поле, которое может быть получено из K присоединением элемента ζ, удовлетворяющего уравнению $f(\zeta) = 0$. Далее, каждый элемент u из $\mathfrak{o}_f$ может быть записан в виде $\frac{g}{h}$, где g и h принадлежат $K[x]$, причем h не содержится в $\mathfrak{q}$. Обозначим через $\bar{g}$, $\bar{h}$ и $\bar{u}$ классы вычетов элементов g, h и u соответственно; тогда $\bar{g} = \bar{u}\bar{h}$, $\bar{h} \neq 0$, откуда $\bar{u} = \bar{g}\bar{h}^{-1}$. Так как $\bar{g}$ и $\bar{h}$ принадлежат полю Σ_1, то $\bar{u} \in \Sigma_1$ и $\Sigma = \Sigma_1$. Таким образом, поле вычетов Σ точки $\mathfrak{p}_f$ может быть получено из K присоединением элемента ζ такого, что $f(\zeta) = 0$. Другими словами, *поле Σ является алгебраическим расширением поля K конечной степени, равной степени*

многочлена f. В случае $f=x$, имеем $\Sigma=K$; это показывает, что поле констант поля $K\langle x\rangle$ (которое содержит K и содержится в Σ) совпадает с K. Рассматривая вместо x элемент $\frac{1}{x}$, получаем, что поле вычетов точки $\mathfrak{p}_{\frac{1}{x}}$ также равно K.

Если поле K алгебраически замкнуто, то каждый неприводимый многочлен от x с коэффициентами из K имеет степень 1, поэтому поле вычетов в любой точке совпадает с K. Пусть в этом случае $\mathfrak{p}_a$ обозначает точку, соответствующую многочлену $x-a$, и пусть a не является полюсом элемента u из поля $K\langle x\rangle$. Если $u=\frac{g}{h}$, где g и h принадлежат $K[x]$ и $h(a)\neq 0$, то

$$u-u(a)=\frac{g(x)\,h(a)-h(x)\,g(a)}{h(a)\,h(x)},$$

причем $g(x)\,h(a)-h(x)\,g(a)$ делится на $x-a$. Таким образом, значение $u(a)$, принимаемое элементом u в a, совпадает с классом вычетов элемента u по модулю $\mathfrak{p}_a$ [1]).

Перейдем к общему случаю поля алгебраических функций R от одной переменной над произвольным полем K. Пусть $\mathfrak{p}$ — точка поля R, а x — элемент поля R, для которого $\mathfrak{p}$ не является полюсом. Тогда класс вычетов элемента x по модулю $\mathfrak{p}$ (являющийся элементом поля вычетов точки $\mathfrak{p}$) называется *значением элемента x в точке $\mathfrak{p}$*. Заметим, что если поле K не является алгебраически замкнутым, то значение x в точке $\mathfrak{p}$, вообще говоря, не является элементом поля K. Значение элемента x в точке $\mathfrak{p}$ обозначается через $x(\mathfrak{p})$; если точка $\mathfrak{p}$ не является полюсом элементов x и y, то, очевидно,

$$(x+y)(\mathfrak{p})=x(\mathfrak{p})+y(\mathfrak{p}),\quad (xy)(\mathfrak{p})=x(\mathfrak{p})\,y(\mathfrak{p}).$$

Элементы, для которых точка $\mathfrak{p}$ является нулем, характеризуются тем, что их значение в точке $\mathfrak{p}$ равно 0.

Часто удобно считать, что элемент поля R, для которого точка $\mathfrak{p}$ является полюсом, принимает в точке $\mathfrak{p}$ зна-

---

[1]) Совпадение понимается в смысле естественного отождествления, см. конец § 2. (*Прим. перев.*)

чение ∞; здесь символ ∞ не имеет никакой связи с символом ∞, который был использован при доопределении функции порядка в точке.

§ 4. Существование точек

В этом параграфе мы докажем теорему о том, что любое поле алгебраических функций от одной переменной имеет бесконечно много точек.

Теорема 1. *Пусть R — поле алгебраических функций от одной переменной над полем K. Предположим, что нам заданы подкольцо $\mathfrak{o}$ поля R, содержащее поле K, и некоторый идеал $\mathfrak{p}$ в кольце $\mathfrak{o}$, не содержащий 1 и отличный от $\{0\}$. Тогда существует точка $\mathfrak{P}$ поля R, кольцо которой $\mathfrak{O}$ содержит $\mathfrak{o}$ и для которой $\mathfrak{p} \subset \mathfrak{P} \cap \mathfrak{o}$.*

Для любого подкольца $\mathfrak{o}'$ поля R, содержащего $\mathfrak{o}$, через $\mathfrak{p}\mathfrak{o}'$ будем обозначать идеал в $\mathfrak{o}'$, порожденный элементами из $\mathfrak{p}$. Обозначим через $\mathcal{F}$ семейство всех подколец $\mathfrak{o}'$ поля R, содержащих $\mathfrak{o}$, для которых $\mathfrak{p}\mathfrak{o}' \neq \mathfrak{o}'$; кольцо $\mathfrak{o}$, очевидно, принадлежит семейству $\mathcal{F}$. Покажем, что семейство $\mathcal{F}$ содержит по крайней мере один максимальный элемент (т. е. что в $\mathcal{F}$ имеется кольцо, не являющееся собственным подкольцом другого кольца из семейства $\mathcal{F}$) и, далее, что любой такой максимальный элемент является V-кольцом.

Для доказательства первого утверждения, достаточно показать, в силу леммы Цорна, что семейство $\mathcal{F}$ индуктивно, [1]) т. е. если $\mathcal{F}'$ есть непустое подсемейство семейства $\mathcal{F}$ такое, что из двух любых колец, принадлежащих $\mathcal{F}'$, одно содержится в другом, то в $\mathcal{F}$ найдется кольцо, содержащее все кольца семейства $\mathcal{F}'$. Для этого обозначим через $\mathfrak{o}_1$ теоретико-множественное объединение всех колец, принадлежащих $\mathcal{F}'$. Если x и y принадлежат $\mathfrak{o}_1$, то $x \in \mathfrak{o}'$, $y \in \mathfrak{o}''$, где $\mathfrak{o}'$ и $\mathfrak{o}''$ содержатся в $\mathcal{F}'$.

---

[1]) Частично упорядоченное множество A называется индуктивным, если каждое линейно упорядоченное подмножество B множества A имеет в A верхнюю границу, т. е. существует элемент $a \in A$ такой, что $b \leqslant a$ при всех $b \in B$. Эквивалентная аксиоме выбора лемма Цорна утверждает, что каждое индуктивное частично упорядоченное множество содержит максимальный элемент (за которым не следуют другие элементы из A). Рассматриваемое в тексте семейство $\mathcal{F}$ частично упорядочено по включению. (*Прим. перев.*)

Одно из колец $\mathfrak{o}'$ и $\mathfrak{o}''$ содержится в другом. Пусть, например, $\mathfrak{o}''$ содержится в $\mathfrak{o}'$, тогда оба элемента x и y принадлежат $\mathfrak{o}'$, откуда $x-y\in\mathfrak{o}'$, $xy\in\mathfrak{o}'$, значит, $x-y$ и xy содержатся в $\mathfrak{o}_1$. То же получим, если $\mathfrak{o}'\subset\mathfrak{o}''$; таким образом, $\mathfrak{o}_1$ есть кольцо. Так как каждое кольцо, принадлежащее $\mathcal{F}$, содержит $\mathfrak{o}$, то $\mathfrak{o}_1$ также содержит $\mathfrak{o}$. Утверждаем, что $\mathfrak{p}\mathfrak{o}_1\neq\mathfrak{o}_1$. Действительно, если бы это было не так, то для 1 мы имели бы представление вида $1=x_1y_1+\ldots+x_hy_h$, где $x_i\in\mathfrak{p}$, $y_i\in\mathfrak{o}_1$ $(1\leqslant i\leqslant h)$. Каждый элемент y_i принадлежит некоторому кольцу $\mathfrak{o}^{(i)}\in\mathcal{F}'$. Для каждой пары (i, j), одно из колец $\mathfrak{o}^{(i)}$ и $\mathfrak{o}^{(j)}$ содержится в другом; так как имеется только конечное число колец $\mathfrak{o}^{(i)}$, то, как легко видеть, все эти кольца содержатся в одном из них, скажем в $\mathfrak{o}^{(k)}$. Но тогда мы имеем

$$1=\sum_{i=1}^{h}x_iy_i\in\mathfrak{p}\mathfrak{o}^{(k)},$$

откуда $\mathfrak{p}\mathfrak{o}^{(k)}=\mathfrak{o}^{(k)}$, что невозможно, ибо $\mathfrak{o}^{(k)}\in\mathcal{F}'$. Таким образом, $\mathfrak{p}\mathfrak{o}_1\neq\mathfrak{o}_1$ и, значит, $\mathfrak{o}_1\in\mathcal{F}$; этим доказано, что семейство $\mathcal{F}$ индуктивно.

Пусть $\mathfrak{O}$ — максимальное кольцо из $\mathcal{F}$; докажем, что $\mathfrak{O}$ является V-кольцом. Прежде всего покажем, что всякий элемент из $\mathfrak{O}$, который $\equiv 1 \pmod{\mathfrak{p}\mathfrak{O}}$, обладает в $\mathfrak{O}$ обратным элементом. Пусть Q обозначает множество этих элементов; ясно, что произведение элементов из Q также принадлежит Q. Пусть $\mathfrak{O}'$ обозначает множество элементов вида $\frac{x}{q}$, где $x\in\mathfrak{O}$, $q\in Q$; формулы

$$\frac{x'}{q'}-\frac{x}{q}=\frac{qx'-q'x}{qq'},\qquad \frac{x}{q}\cdot\frac{x'}{q'}=\frac{xx'}{qq'}$$

показывают, что $\mathfrak{O}'$ является кольцом. Так как $1\in Q$, то $\mathfrak{O}$ содержится в $\mathfrak{O}'$. Утверждаем, что $1\notin\mathfrak{p}\mathfrak{O}'$. Допустим противное, т. е. допустим, что

$$1=\sum_{i=1}^{h}x_i\frac{y_i}{q_i},\quad x_i\in\mathfrak{p},\ y_i\in\mathfrak{O},\ q_i\in Q\qquad(1\leqslant i\leqslant h).$$

Положим $q = q_1 \ldots q_h$; тогда $q \in Q$, т. е, $q = 1 + \sum_{i=1}^{h'} x_i' y_i'$, где $x_i' \in \mathfrak{p}$, $y_i' \in \mathfrak{O}$, и мы получаем

$$1 = \sum_{i=1}^{h} x_i \left(\prod_{j \neq i} q_j \right) y_i - \sum_{i=1}^{h'} x_i' y_i' \in \mathfrak{p}\mathfrak{O},$$

что невозможно. Таким образом, $\mathfrak{O}'$ принадлежит семейству $\mathcal{F}$; так как кольцо $\mathfrak{O}$ максимально, то $\mathfrak{O}' = \mathfrak{O}$, и, следовательно, для $q \in Q$ имеем $q^{-1} \in \mathfrak{O}$. Пусть теперь u есть произвольный элемент из R, не принадлежащий $\mathfrak{O}$; тогда $\mathfrak{O}[u] \neq \mathfrak{O}$, а значит $\mathfrak{O}[u] \notin \mathcal{F}$ и $\mathfrak{p}\mathfrak{O}[u] = \mathfrak{O}[u]$. Отсюда следует, что для единицы имеет место представление вида $1 = \sum_{i=0}^{n} x_i u^i$, где $x_i \in \mathfrak{p}\mathfrak{O}$ $(0 \leqslant i \leqslant n)$. Так как $1 - x_0 \in Q$, то получаем $1 = \sum_{i=1}^{n} x_i' u^i$, где $x_i' = x_i (1 - x_0)^{-1} \in \mathfrak{p}\mathfrak{O}$. Предположим, что среди всех представлений единицы в таком виде выбрано представление с наименьшим n, и, значит, не существует представления вида $1 = \sum_{i=1}^{n'} x_i'' u^i$, где $n' < n$, $x_i'' \in \mathfrak{p}\mathfrak{O}$ $(1 \leqslant i \leqslant n')$. Предположим, что $u^{-1} \notin \mathfrak{O}$. Тогда аналогичным образом мы представим единицу в виде $\sum_{i=1}^{m} y_i' u^{-i}$, где $y_i' \in \mathfrak{p}\mathfrak{O}$ $(1 \leqslant i \leqslant m)$; при этом мы можем считать, что среди всех представлений единицы в этом втором виде выбрано представление с наименьшим возможным значением m. Если $n \geqslant m$, то $u^n = \sum_{i=1}^{m} y_i' u^{n-i}$, откуда

$$1 = \sum_{i=1}^{n-1} x_i' u^i + x_n' \left(\sum_{i=1}^{m} y_i' u^{n-i} \right),$$

что невозможно в силу нашего выбора n. Поменяв ролями u и u^{-1}, мы таким же образом покажем, что предположение $n \leqslant m$ также невозможно. Таким образом, из предположения $u^{-1} \notin \mathfrak{O}$ получаем противоречие, значит $u^{-1} \in \mathfrak{O}$.

Так как $\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$, то $\mathfrak{O} \neq R$, и, следовательно, $\mathfrak{O}$ является V-кольцом.

Идеал $\mathfrak{P}$, состоящий из необратимых элементов кольца $\mathfrak{O}$, является точкой поля R; так как $\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$, то элементы из $\mathfrak{p}$ не могут быть делителями единицы в $\mathfrak{O}$, значит $\mathfrak{p} \subset \mathfrak{P} \cap \mathfrak{o}$. Теорема 1 доказана.

Замечание 1. При определении V-кольца в поле R, а также при доказательстве теоремы 1 мы нигде не пользовались тем, что R является полем алгебраических функций от одной переменной. Следовательно, наше доказательство теоремы 1 дает нам результат, справедливый для любой пары полей (K, R) где K — подполе поля R.

Замечание 2. Если R — поле алгебраических функций от одной переменной над полем K и если $\mathfrak{p}$ является простым идеалом в $\mathfrak{o}$, то можно доказать, что пересечение $\mathfrak{P} \cap \mathfrak{o}$ необходимо равно $\mathfrak{p}$; однако нам не придется пользоваться этим уточнением нашей теоремы.

Следствие 1. *Пусть R — поле алгебраических функций от одной переменной над полем K и пусть $x_1, \ldots, x_r$ — элементы поля R, причем не все они принадлежат K. Обозначим через $\mathfrak{a}$ множество многочленов $F(X_1, \ldots, X_r)$ от r переменных с коэффициентами из K, для которых $F(x_1, \ldots, x_r) = 0$. Пусть элементы $\xi_1, \ldots, \xi_r$ из поля K таковы, что $F(\xi_1, \ldots, \xi_r) = 0$ для всех $F \in \mathfrak{a}$. Тогда существует точка поля R, являющаяся общим нулем для $x_1 - \xi_1, \ldots, x_r - \xi_r$.*

Положим $\mathfrak{o} = K[x_1, \ldots, x_r]$; элемент y из $\mathfrak{o}$ может быть представлен в виде $P(x_1, \ldots, x_r)$, где P — многочлен с коэффициентами из K; если $P(x_1, \ldots, x_r) = P'(x_1, \ldots, x_r)$, то $P' - P$ принадлежит $\mathfrak{a}$. Отсюда следует, что $P(\xi_1, \ldots, \xi_r)$ имеет одно и то же значение для всех многочленов P таких, что $y = P(x_1, \ldots, x_r)$. Пусть $\mathfrak{p}$ обозначает множество тех элементов y из $\mathfrak{o}$, для которых это значение равно нулю. Очевидно, $\mathfrak{p}$ является идеалом в $\mathfrak{o}$, причем этот идеал $\neq \mathfrak{o}$, так как пересечение его с полем K состоит только из нуля. Если $\mathfrak{P}$ является точкой поля R, для которой $\mathfrak{p} \subset \mathfrak{P}$, то эта точка $\mathfrak{P}$ и будет общим нулем для $x_1 - \xi_1, \ldots, x_r - \xi_r$.

Следствие 2. *Пусть R — поле алгебраических функций от одной переменной над полем K и пусть x, y — элементы поля R, не являющиеся одновременно константами. Пусть F — неприводимый многочлен с коэффициен-*

тами из K такой, что $F(x, y)=0$. Если элементы ξ и η из поля K таковы, что $F(\xi, \eta)=0$, то в поле R существует точка, являющаяся общим нулем для $x-\xi$ и $y-\eta$.

Предположим, например, что x не является константой, тогда y алгебраичен над $K\langle x\rangle$. Пусть $Y^n+\rho_1(x)Y^{n-1}+\ldots$ $\ldots+\rho_n(x)$ есть многочлен от Y с коэффициентами из $K\langle x\rangle$, неприводимый в $K\langle x\rangle[Y]$, для которого y является корнем. Имеем $\rho_i(x)=\frac{P_i(x)}{Q_i(x)}$, где P_i и Q_i — взаимно простые многочлены с коэффициентами из K. Обозначим через Q общее наименьшее кратное многочленов $Q_1, \ldots, Q_n$; тогда, как известно, многочлен

$$F_1(X, Y)=Q(X)Y^n+\sum_{i=1}^{n}\frac{Q(X)}{Q_i(X)}P_i(X)Y^{n-i}$$

неприводим в $K[X, Y]$. Пусть F' — произвольный многочлен из $K[X, Y]$, для которого $F'(x, y)=0$; тогда $F'(x, Y)$ делится на $F_1(x, Y)$ в $K\langle x\rangle[Y]$; отсюда, в силу неприводимости многочлена F_1, следует, что F' делится на F_1. В частности, имеем $F=\alpha F_1$, $\alpha\in K$, откуда $F_1(\xi, \eta)=0$ и $F'(\xi, \eta)=0$. Следствие 2 вытекает теперь из следствия 1.

Следствие 3. *Если R есть поле алгебраических функций от одной переменной над полем K, то для любого элемента $x\in R$, не являющегося константой, в поле R существует по крайней мере один нуль и по крайней мере один полюс.*

Существование нуля следует легко из следствия 2 (надо взять $F=Y$, $y=0$). Так как элемент x^{-1} не является константой, то он имеет по крайней мере один нуль, а тогда x имеет по крайней мере один полюс.

Следствие 4. *Поле алгебраических функций от одной переменной имеет бесконечно много точек.*

Пусть R — рассматриваемое поле, K — его поле констант и x — элемент поля R, не являющийся константой. Кольцо многочленов $K[x]$ от x с коэффициентами из K содержит бесконечно много существенно различных неприводимых многочленов. Действительно, если поле K бесконечно, то мы можем взять многочлены $x-a$, $a\in K$; если же K конечно, то, как известно, для каждого целого $n>0$ существует

неприводимый многочлен степени n. Для каждого неприводимого многочлена f из $K[x]$ идеал, порожденный этим многочленом f в кольце $K[x]$, не является единичным. Из теоремы 1 следует, что тогда в поле R существует точка $\mathfrak{p}_f$, являющаяся нулем элемента f и кольцо которой содержит $K[x]$. Если неприводимые многочлены f и g от x существенно различны, то они взаимно просты, а тогда в $K[x]$ существуют элементы u и v такие, что $uf+vg=1$; отсюда легко следует, что $\mathfrak{p}_f \neq \mathfrak{p}_g$.

§ 5. Функция порядка. Степень точки

Пусть $\mathfrak{p}$ — точка поля R алгебраических функций от одной переменной над полем K. Нашей целью является доказательство того, что точка $\mathfrak{p}$ удовлетворяет сформулированным в § 3 условиям, которые гарантировали существование функции порядка. Мы докажем также, что поле вычетов Σ точки $\mathfrak{p}$ является алгебраическим расширением конечной степени поля K.

Пусть x — элемент $\neq 0$ из $\mathfrak{p}$. Предположим, что имеется конечная последовательность $(t_1, \ldots, t_{e+1})$ элементов кольца $\mathfrak{o}$ точки $\mathfrak{p}$, удовлетворяющая следующим условиям: $t_1=x$; $\frac{t_i}{t_{i+1}}$ принадлежит $\mathfrak{p}$, $1 \leqslant i \leqslant e$; $t_{e+1}=1$. Пусть, далее, $(u_1, \ldots, u_d)$ есть конечная последовательность элементов кольца $\mathfrak{o}$, классы вычетов которых $\bar{u}_1, \ldots, \bar{u}_d$ по модулю $\mathfrak{p}$ линейно независимы над K. Докажем, что система ed элементов $t_i u_j$ $(2 \leqslant i \leqslant e+1,\ 1 \leqslant j \leqslant d)$ из поля R линейно независима над полем $K\langle x\rangle$. Допуская противное, предположим, что существует линейное соотношение вида

$$\sum_{i=2}^{e+1} \sum_{j=1}^{d} \rho_{ij}(x)\, t_i u_j = 0,$$

где $\rho_{ij}(x) \in K\langle x\rangle$, причем не все ρ_{ij} равны нулю. Умножая это соотношение на общий знаменатель всех рациональных дробей $\rho_{ij}(x)$, мы получим соотношение того же вида, в котором ρ_{ij} будут многочленами. Поделив полученное соотношение в случае надобности на некоторую степень x, мы придем к соотношению

$$\sum_{i=2}^{e+1} \sum_{j=1}^{d} f_{ij}(x)\, t_i u_j = 0, \tag{1}$$

где $f_{ij}(x)$ — многочлены, причем не все они делятся на x. Положим $f_{ij}(0)=a_{ij}$, тогда

$$f_{ij}(x)-a_{ij}=xg_{ij}(x)\in x\mathfrak{o}$$

(здесь g_{ij} — многочлены). Пусть k обозначает наибольший индекс $\geqslant 2$, для которого существует l с условием $a_{kl}\neq 0$ (значит, при $k<i\leqslant e+1$, $1\leqslant j\leqslant d$ имеем $a_{ij}=0$). Из равенства (1) получаем

$$\sum_{i=2}^{k}\sum_{j=1}^{d}a_{ij}t_iu_j=xw,$$

где $w=-\sum_{i=2}^{e+1}\sum_{j=1}^{d}g_{ij}(x)t_iu_j\in\mathfrak{o}$. Запишем полученное равенство в виде

$$\sum_{j=1}^{d}a_{kj}u_j=w\frac{x}{t_k}-\sum_{i=2}^{k-1}\sum_{j=1}^{d}a_{ij}\frac{t_i}{t_k}u_j.$$

При $k\geqslant 2$ и $i<k$ элементы $\frac{x}{t_k}$ и $\frac{t_i}{t_k}$ принадлежат $\mathfrak{p}$, значит, правая часть в последней формуле является элементом из $\mathfrak{p}$. Отсюда следует, что

$$\sum_{j=1}^{d}a_{kj}\bar{u}_j=0,$$

однако это невозможно, ибо $a_{kl}\neq 0$ и классы вычетов $\bar{u}_1,\ldots,\bar{u}_d$ линейно независимы над K. Этим доказано, что элементы

$$t_iu_j\,(2\leqslant i\leqslant e+1,\ 1\leqslant j\leqslant d)$$

линейно независимы над полем $K\langle x\rangle$.

Так как $x\in\mathfrak{p}$, то x не является константой (см. § 2), поэтому поле R является конечным алгебраическим расширением поля $K\langle x\rangle$. Полагая $n=[R:K\langle x\rangle]$, заключаем, что $de\leqslant n$.

Возьмем теперь $e=1$, $t_1=x$, $t_2=1$; тогда получим $d\leqslant n$. Значит, поле Σ не может содержать более чем n элементов, линейно независимых над полем K. Таким образом, поле Σ является алгебраическим расширением конечной степени поля K.

Далее, полагая $d=1$, $u_1=1$, видим, что число членов в последовательности $(t_1, \ldots, t_{e+1})$, удовлетворяющей вышеуказанным условиям, не превосходит $n+1$. Среди всех последовательностей, удовлетворяющих этим условиям, выберем такую последовательность $(t_1, \ldots, t_{e+1})$, у которой число членов наибольшее, и положим $t=t_e$. Утверждаем, что для любого элемента z из $\mathfrak{p}$ имеем: $z \in t\mathfrak{o}$. Действительно, если бы это было не так, то элемент $\frac{z}{t}$ не принадлежал бы $\mathfrak{o}$; значит, $\frac{t}{z}$ был бы необратимым элементом кольца $\mathfrak{o}$, т. е. $\frac{t}{z}$ принадлежал бы $\mathfrak{p}$. Но тогда последовательность $\left(t_1, \ldots, t_e, \frac{t_e}{z}, t_{e+1}\right)$, число членов которой равно $e+2$, удовлетворяла бы всем нашим требованиям, что невозможно. Этим доказано, что $\mathfrak{p}=t\mathfrak{o}$ является главным идеалом. Возьмем элемент $y \neq 0$ из $\mathfrak{p}$; если $y \in t^m\mathfrak{o}$, то положим $u_1=y$, $u_{i+1}=\frac{y}{t^i}$ $(1 \leqslant i \leqslant m-1)$, $u_{m+1}=1$. Так как $\frac{u_i}{u_{i+1}} \in \mathfrak{p}$ $(1 \leqslant i \leqslant m)$, то согласно вышедоказанному будем иметь $m \leqslant [R:K\langle y\rangle]$. Значит, элемент $\neq 0$ не может принадлежать идеалам $t^m\mathfrak{o}$ при всех m. Таким образом, нами доказана следующая теорема.

Теорема 2. *Для любой точки $\mathfrak{p}$ поля алгебраических функций от одной переменной над полем K существует функция порядка, и поле вычетов точки $\mathfrak{p}$ является алгебраическим расширением конечной степени поля K.*

Следствие. *Если R — поле алгебраических функций от одной переменной над полем K, то поле констант поля R имеет конечную степень над K.*

Это непосредственно следует из того, что поле констант содержится в поле вычетов любой точки поля R.

Очевидно также, что поле вычетов точки $\mathfrak{p}$ имеет конечную степень над полем констант. Эта степень называется *степенью точки* $\mathfrak{p}$.

Замечание. На протяжении всей этой книги через ν будет обозначаться (без дополнительных пояснений) функция порядка в точке $\mathfrak{p}$.

§ 6. Теорема о независимости

Рассмотрим поле R рациональных функций от комплексной переменной с комплексными коэффициентами. Для каждого комплексного числа a существует одна и только одна точка $\mathfrak{p}_a$, в которой x принимает значение a. Произвольную функцию $u \in R$ мы можем в окрестности a разложить в ряд Лорана

$$u = \sum_{k=r}^{\infty} c_k (x-a)^k,$$

где c_k — комплексные числа. Если $c_r \neq 0$, то для функции $(x-a)^{-r} u$ точка $\mathfrak{p}_a$ не является ни нулем, ни полюсом; значит, порядок функции u в точке $\mathfrak{p}_a$ равен r. Если нам известно некоторое число первых коэффициентов нашего ряда, скажем для $r \leqslant k < m$ (m — целое, $m > r$), то это дает нам некоторые сведения о поведении функции u в окрестности a. Если положить $v = \sum_{k=r}^{m-1} c_k (x-a)^k$, то тот факт, что функция u имеет заданные коэффициенты $c_r, \ldots, c_{m-1}$, может быть выражен условием $\nu_{\mathfrak{p}_a}(u-v) \geqslant m$. В этом случае мы будем говорить, что в точке $\mathfrak{p}_a$ функция u ведет себя так же, как и функция v с точностью до порядка $m-1$. Рассмотрим теперь следующий вопрос. Пусть нам задано конечное число различных комплексных чисел $a_1, \ldots, a_h$ и пусть для каждого a_i заданы некоторая рациональная функция v_i и целое число m_i; существует ли рациональная функция u, удовлетворяющая одновременно h условиям $\nu_i(u-v_i) \geqslant m_i$ (ν_i — функция порядка в точке $\mathfrak{p}_{a_i}$)? Другими словами, имеется ли какая-нибудь необходимая зависимость между поведением рациональной функции в нескольких различных точках (поведение понимается, конечно, с точностью до некоторого порядка)? В общем случае произвольного поля алгебраических функций от одной переменной мы докажем, что никакой такой необходимой зависимости нет. Точнее, имеет место следующая теорема.

Теорема 3. *Пусть R — поле алгебраических функций от одной переменной, в котором задано h различных точек $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$. Каждой точке $\mathfrak{p}_i$ сопоставим некоторый элемент v_i из R и некоторое целое число m_i. Тогда*

в поле R существует элемент u, удовлетворяющий h условиям: $\nu_i(u-v_i)\geqslant m_i$ $(1\leqslant i\leqslant h)$ (здесь ν_i обозначает функцию порядка в точке $\mathfrak{p}_i$).

Доказательство проведем индукцией по h. При $h=1$ утверждение тривиально. Предположим, что $h>1$ и что теорема 3 справедлива для системы $h-1$ точек. Тогда для заданных целых чисел $e_1, \ldots, e_{h-1}$ в поле R существует элемент u такой, что $\nu_i(u)=e_i$ $(1\leqslant i\leqslant h-1)$. Действительно, для элементов v_i таких, что $\nu_i(v_i)=e_i$ $(1\leqslant i\leqslant h-1)$, существует элемент u с условиями $\nu_i(u-v_i)\geqslant e_i+1$. Так как $u=(u-v_i)+v_i$, то $\nu_i(u)=\nu_i(v_i)=e_i$ (см. § 3).

Докажем, что не существует рациональных чисел $\rho_1, \ldots, \rho_{n-1}$ таких, что $\nu_h(z)=\sum_{i=1}^{h-1}\rho_i\nu_i(z)$ при всех $z\neq 0$. Допустим, что такие числа существуют и рассмотрим сначала случай, когда хоть одно из этих чисел отрицательно. В поле R существуют элементы z и z' такие, что

$$\nu_i(z)=1,\ \nu_i(z')=0,\quad \text{если}\quad \rho_i\geqslant 0;$$
$$\nu_i(z)=0,\ \nu_i(z')=1,\quad \text{если}\quad \rho_i<0.$$

Ясно, что тогда $\nu_h(z)\geqslant 0$, $\nu_h(z')<0$. С другой стороны, так как $\nu_i(z)\neq\nu_i(z')$, то $\nu_i(z+z')=\min\{\nu_i(z), \nu_i(z')\}=0$ $(1\leqslant i\leqslant h-1)$, откуда $\nu_h(z+z')=0$; это однако, невозможно, ибо $\nu_h(z')<\nu_h(z)$ и значит, $\nu_h(z+z')=\nu_h(z')<0$. Предположим теперь, что все $\rho_i\geqslant 0$. Очевидно, числа ρ_i не могут равняться нулю одновременно; будем считать, что $\rho_1>0$. Если все числа $\rho_2, \ldots, \rho_{h-1}$ равны нулю, то условия $\nu_h(z)>0$ и $\nu_1(z)>0$ эквивалентны друг другу, откуда $\mathfrak{p}_h=\mathfrak{p}_1$, что противоречит предположению. Если хоть одно из чисел $\rho_2, \ldots, \rho_{h-1}$ не равно нулю, то, переписывая наше равенство в виде

$$\nu_1(z)=\frac{1}{\rho_1}\nu_h(z)-\sum_{i=2}^{h-1}\frac{\rho_i}{\rho_1}\nu_i(z),$$

мы приходим к случаю, рассмотренному выше. Этим наше утверждение доказано.

Таким образом, для рациональных чисел $\rho_1, \ldots, \rho_h$ равенство $\sum_{i=1}^{h}\rho_i\nu_i(z)=0$ для всех $z\neq 0$ имеет место только

при условии, что все ρ_i равны нулю. Пользуясь этим, покажем, что в поле R существуют отличные от нуля такие элементы $z_1, \ldots, z_h$, что $\det(\nu_i(z_j))_{i,j} \neq 0$. Для доказательства определяем эти элементы шаг за шагом. В качестве z_1 возьмем произвольный элемент $\neq 0$, для которого $\nu_1(z_1) \neq 0$. Рассмотрим множество рациональных линейных комбинаций функций $\nu_1, \ldots, \nu_h$; множество тех линейных комбинаций, которые в z_1 принимают значение 0, имеет размерность $h-1$ над полем рациональных чисел. Предположим, что нами уже определены элементы $z_1, \ldots, z_k$ $(k < h)$ так, что имеется ровно $h-k$ линейно независимых рациональных линейных комбинаций функций $\nu_1, \ldots, \nu_h$, которые в $z_1, \ldots, z_k$ принимают значение 0. Пусть $\sum_{i=1}^{h} \rho_i \nu_i$ — одна из таких линейных комбинаций, отличная от нуля; выбираем $z_{k+1} \neq 0$ так, чтобы $\sum_{i=1}^{h} \rho_i \nu_i(z_{k+1}) \neq 0$. Тогда имеем ровно $h-(k+1)$ линейно независимых рациональных линейных комбинаций функций $\nu_1, \ldots, \nu_h$, которые в $z_1, \ldots, z_{k+1}$ принимают значение 0. В конце концов мы будем иметь h элементов $z_1, \ldots, z_h$ поля R, не равных нулю, таких, что только тривиальная линейная комбинация функций $\nu_1, \ldots, \nu_h$ в $z_1, \ldots, z_h$ принимает значение 0. Так как числа $\nu_i(z_j)$ рациональны, то отсюда следует, что $\det(\nu_i(z_j))_{i,j} \neq 0$.

Уравнения $\sum_{j=1}^{h} \sigma_{j,k} \nu_i(z_j) = -1$ при $i = k$, $\sum_{j=1}^{h} \sigma_{j,k} \nu_i(z_j) = +1$ при $i \neq k$ (где k — любой индекс от 1 до h) имеют решение $(\sigma_{1,k}, \ldots, \sigma_{h,k})$ в рациональных числах. Обозначим через d такое положительное целое число, что все числа $d\sigma_{i,k}$ — целые $(1 \leqslant i \leqslant h,\ 1 \leqslant k \leqslant h)$. Если положить

$$\zeta_k = \prod_{j=1}^{h} z_j^{d\sigma_{j,k}},$$

то $\nu_k(\zeta_k) = -d$, $\nu_i(\zeta_k) = +d$ при $i \neq k$. Положим $t_k = \dfrac{1}{1+\zeta_k^{-1}}$. Так как при $i \neq k$ имеем $\nu_i(\zeta_k^{-1}) < 0 = \nu_i(1)$, то $\nu_i(1+\zeta_k^{-1}) = \nu_i(\zeta_k^{-1}) = -d$, значит, $\nu_i(t_k) = d$. С другой

стороны $t_k - 1 = -\frac{1}{\zeta_k(1+\zeta_k^{-1})}$ и $\nu_k(\zeta_k^{-1}) = d$, поэтому $\nu_k(t_k - 1) = d$. Заметим теперь, что число d можно взять сколь угодно большим. Выберем d так чтобы $d + \nu_i(v_j) \geqslant \max\{m_1, \ldots, m_h\}$ $(1 \leqslant i,\ j \leqslant h)$. Положим $u = \sum_{i=1}^{h} t_i v_i$, тогда

$$u - v_i = (t_i - 1)\, v_i + \sum_{k \neq i} t_k v_k.$$

Так как $\nu_i((t_i - 1)\, v_i) = d + \nu_i(v_i) \geqslant m_i$ и $\nu_i(t_k v_k) = d + \nu_i(v_k) \geqslant m_i$ при $k \neq i$, то $\nu_i(u - v_i) \geqslant m_i$ $(1 \leqslant i \leqslant h)$. Теорема 3, таким образом, доказана.

В процессе доказательства последней теоремы нами доказано также следующее утверждение.

Следствие. *Пусть в поле R алгебраических функций от одной переменной задано h различных точек $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ и пусть каждой точке $\mathfrak{p}_i$ сопоставлено некоторое целое число m_i. Тогда в поле R существует элемент u, удовлетворяющий условиям $\nu_i(u) = m_i$ $(1 \leqslant i \leqslant h)$ (где ν_i — функция порядка в точке $\mathfrak{p}_i$).*

§ 7. Дивизоры

Пусть R — поле алгебраических функций от одной переменной над полем K. Каждой точке $\mathfrak{p}$ поля R сопоставим целое число $e(\mathfrak{p})$ так, чтобы $e(\mathfrak{p}) \neq 0$ только для конечного числа точек $\mathfrak{p}$; полученная функция называется *дивизором* поля R и обозначается символически через $\prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$. Целое число $e(\mathfrak{p})$ называется *показателем*, с которым $\mathfrak{p}$ входит в дивизор; если этот показатель равен нулю, то говорят также, что $\mathfrak{p}$ не входит в дивизор.

Дивизоры будем перемножать согласно следующему формальному правилу:

$$\left(\prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}\right)\left(\prod_{\mathfrak{p}} \mathfrak{p}^{e'(\mathfrak{p})}\right) = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p}) + e'(\mathfrak{p})}.$$

Ясно, что дивизоры образуют абелеву группу. Единичным элементом этой группы является дивизор $\prod_{\mathfrak{p}} \mathfrak{p}^0$, называемый *единичным дивизором*.

Точку $\mathfrak{p}$ мы будем отождествлять с дивизором, который сопоставляет этой точке $\mathfrak{p}$ единицу, а всем другим точкам — нуль. Таким образом, если $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ — точки, а $e_1, \ldots, e_n$ — целые числа, то $\mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_n^{e_n}$ является дивизором; если точки $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ различны то $\mathfrak{p}_i$ входит в этот дивизор с показателем e_i.

Дивизор $\prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ называется *целым*, если все показатели $e(\mathfrak{p}) \geqslant 0$. Произведение целых дивизоров является, очевидно, целым дивизором. Если $\mathfrak{a}$ и $\mathfrak{b}$ — дивизоры, то говорят, что $\mathfrak{b}$ *делится* на $\mathfrak{a}$ (или $\mathfrak{a}$ делит $\mathfrak{b}$, $\mathfrak{a}$ делитель $\mathfrak{b}$), если $\mathfrak{b}\mathfrak{a}^{-1}$ является целым дивизором. Ясно, что если $\mathfrak{a}$ делит $\mathfrak{b}$, а $\mathfrak{b}$ делит $\mathfrak{c}$, то $\mathfrak{a}$ делит $\mathfrak{c}$.

Для дивизоров $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ и $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{f(\mathfrak{p})}$ всегда существуют дивизоры, являющиеся общими делителями $\mathfrak{a}$ и $\mathfrak{b}$; причем совокупность всех общих делителей $\mathfrak{a}$ и $\mathfrak{b}$ совпадает с совокупностью всех делителей дивизора $\mathfrak{c} = \prod_{\mathfrak{p}} \mathfrak{p}^{g(\mathfrak{p})}$, где $g(\mathfrak{p}) = \min\{e(\mathfrak{p}), f(\mathfrak{p})\}$. В силу этого дивизор $\mathfrak{c}$ называется *общим наибольшим делителем* дивизоров $\mathfrak{a}$ и $\mathfrak{b}$. Общий наибольший делитель двух целых дивизоров есть целый дивизор. Подобным же образом дивизоры, делящиеся одновременно на $\mathfrak{a}$ и $\mathfrak{b}$, совпадают с дивизорами, делящимися на $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{h(\mathfrak{p})}$, где $h(\mathfrak{p}) = \max\{e(\mathfrak{p}), f(\mathfrak{p})\}$. Дивизор $\mathfrak{m}$ называется *общим наименьшим кратным* дивизоров $\mathfrak{a}$ и $\mathfrak{b}$. Легко видеть, что общее наименьшее кратное дивизоров $\mathfrak{a}^{-1}$ и $\mathfrak{b}^{-1}$ равно обратному дивизору для общего наибольшего делителя дивизоров $\mathfrak{a}$ и $\mathfrak{b}$.

Обозначим через $d(\mathfrak{p})$ степень точки $\mathfrak{p}$. Для произвольного дивизора $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ число $\sum_{\mathfrak{p}} e(\mathfrak{p}) d(\mathfrak{p})$ (эта сумма имеет смысл, так как только конечное число показателей $e(\mathfrak{p})$ отлично от нуля) называется *степенью* дивизора $\mathfrak{a}$ и обозначается через $d(\mathfrak{a})$ (очевидно, что для точки $\mathfrak{a} = \mathfrak{p}$ степень $\mathfrak{a}$ как дивизора равна степени точки $\mathfrak{p}$). Если $\mathfrak{a}$ и $\mathfrak{b}$ дивизоры, то

$$d(\mathfrak{a}\mathfrak{b}) = d(\mathfrak{a}) + d(\mathfrak{b}), \quad d(\mathfrak{a}^{-1}) = -d(\mathfrak{a}).$$

Степень целого дивизора всегда $\geqslant 0$, поэтому, если дивизор $\mathfrak{a}$ делит дивизор $\mathfrak{b}$, то $d(\mathfrak{a}) \leqslant d(\mathfrak{b})$,

Пусть $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ — дивизор и пусть x и y — элементы поля R. Говорят, что x *сравним с* y *по модулю* $\mathfrak{a}$ и пишут

$$x \equiv y \pmod{\mathfrak{a}},$$

если для каждой точки $\mathfrak{p}$ выполнено условие $\nu_{\mathfrak{p}}(x-y) \geqslant e(\mathfrak{p})$. Пусть x, y, x', y' — элементы поля R и пусть λ, λ' — элементы поля констант K' поля R; тогда, очевидно, из сравнений $x \equiv y \pmod{\mathfrak{a}}$ и $x' \equiv y' \pmod{\mathfrak{a}}$ следует $\lambda x + \lambda' x' \equiv \lambda y + \lambda' y' \pmod{\mathfrak{a}}$. В частности, элементы поля R, сравнимые с нулем по модулю $\mathfrak{a}$, образуют векторное пространство $\mathfrak{D}$ над K'. Элементы x и y сравнимы между собой по модулю $\mathfrak{a}$ тогда и только тогда, если они принадлежат одному и тому же смежному классу по модулю $\mathfrak{D}$.

Пусть $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_m^{e_m} \mathfrak{q}_1^{f_1} \ldots \mathfrak{q}_n^{f_n}$ — дивизор, где $\mathfrak{p}_1, \ldots, \mathfrak{p}_m, \mathfrak{q}_1, \ldots, \mathfrak{q}_n$ — различные точки, причем $e_1 > 0, \ldots, e_m > 0$, $f_1 < 0, \ldots, f_n < 0$, и пусть x — элемент из поля R. Тогда условие $x \equiv 0 \pmod{\mathfrak{a}}$ может быть описано следующим образом: точка $\mathfrak{p}_i$ является нулем элемента x порядка $\geqslant e_i$ $(1 \leqslant i \leqslant m)$; элемент x не имеет полюсов вне множества точек $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$; если для x точка $\mathfrak{q}_j$ является полюсом, то порядок этого полюса $\leqslant -f_j$. Таким образом, сравнение $x \equiv 0 \pmod{\mathfrak{a}}$ состоит из бесконечного числа условий для элемента x (по одному для каждой точки).

Нам удобно будет ввести новый вид сравнений, которые будут учитывать поведение рассматриваемых элементов только в конечном числе точек. Пусть S — произвольное конечное множество точек. Для элементов x и y из поля R и дивизора $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ будем писать

$$x \equiv_S y \pmod{\mathfrak{a}},$$

если для всех точек $\mathfrak{p} \in S$ выполнены условия $\nu_{\mathfrak{p}}(x-y) \geqslant e(\mathfrak{p})$. Очевидно, что элементы x, удовлетворяющие условию $x \equiv_S 0 \pmod{\mathfrak{a}}$, образуют векторное пространство над K'; обозначим это пространство через $\mathfrak{K}(\mathfrak{a}, S)$. Сравнение $x \equiv_S y \pmod{\mathfrak{a}}$ эквивалентно условию $x - y \in \mathfrak{K}(\mathfrak{a}, S)$.

Лемма 1. *Пусть* $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e(\mathfrak{p})}$ *и* $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{f(\mathfrak{p})}$ — *дивизоры, причем* $\mathfrak{b}$ *делится на* $\mathfrak{a}$, *и пусть* S — *конечное множество точек. Тогда пространство* $\mathfrak{K}(\mathfrak{b}, S)$ *содержится в* $\mathfrak{K}(\mathfrak{a}, S)$,

и размерность векторного пространства $\mathfrak{K}(\mathfrak{a}, S)/\mathfrak{K}(\mathfrak{b}, S)$ *(над полем констант) конечна и равна* $\sum_{\mathfrak{p}\in S}(f(\mathfrak{p})-e(\mathfrak{p}))\,d(\mathfrak{p})$.

Включение $\mathfrak{K}(\mathfrak{b}, S)\subset\mathfrak{K}(\mathfrak{a}, S)$ очевидно. Положим $\mathfrak{a}_S=\prod_{\mathfrak{p}}\mathfrak{p}^{e'(\mathfrak{p})}$, где $e'(\mathfrak{p})$ равно $e(\mathfrak{p})$, если $\mathfrak{p}\in S$, и равно нулю в противном случае; аналогично определяем $\mathfrak{b}_S$. Тогда $\mathfrak{K}(\mathfrak{b}, S)=\mathfrak{K}(\mathfrak{b}_S, S)$, $\mathfrak{K}(\mathfrak{a}, S)=\mathfrak{K}(\mathfrak{a}_S, S)$ и $\mathfrak{b}_S$ делится на $\mathfrak{a}_S$. С другой стороны, имеем $\sum_{\mathfrak{p}\in S}(f(\mathfrak{p})-e(\mathfrak{p}))\,d(\mathfrak{p})=d(\mathfrak{b}_S)-d(\mathfrak{a}_S)$. Найдем теперь конечную последовательность $(\mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_h)$ дивизоров, удовлетворяющую следующим условиям: $\mathfrak{a}_0=\mathfrak{a}_S$; для $1\leqslant i\leqslant h$ дивизор $\mathfrak{a}_i$ имеет вид $\mathfrak{a}_{i-1}\mathfrak{p}$, где $\mathfrak{p}$ — точка из множества S; $\mathfrak{a}_h=\mathfrak{b}_S$. Имеем $\mathfrak{K}(\mathfrak{a}_S, S)=\mathfrak{K}(\mathfrak{a}_0, S)\supset\mathfrak{K}(\mathfrak{a}_1, S)\supset\ldots\supset\mathfrak{K}(\mathfrak{a}_h, S)=\mathfrak{K}(\mathfrak{b}_S, S)$. Если мы докажем, что каждое пространство $\mathfrak{K}(\mathfrak{a}_{i-1}, S)/\mathfrak{K}(\mathfrak{a}_i, S)$ имеет конечную размерность, равную $d(\mathfrak{a}_i)-d(\mathfrak{a}_{i-1})$, то отсюда будет следовать, что пространство $\mathfrak{K}(\mathfrak{a}_S, S)/\mathfrak{K}(b_S, S)$ имеет конечную размерность, равную $\sum_{i=1}^{h}(d(\mathfrak{a}_i)-d(\mathfrak{a}_{i-1}))=d(\mathfrak{b}_S)-d(\mathfrak{a}_S)$. Лемму 1 достаточно, следовательно, доказать для случая, когда $\mathfrak{b}=\mathfrak{b}_S=\mathfrak{a}_S\mathfrak{p}=\mathfrak{a}\mathfrak{p}$, где $\mathfrak{p}\in S$. Пусть $\mathfrak{p}=\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ — все различные точки множества S. Согласно следствию к теореме 3 § 6 в поле R можно найти такой элемент u, что $\nu_{\mathfrak{p}_i}'(u)=e(\mathfrak{p}_i)$ $(1\leqslant i\leqslant n)$. Нам надо доказать, что размерность $\mathfrak{K}(\mathfrak{a}, S)/\mathfrak{K}(\mathfrak{b}, S)$ над полем констант K' поля R равна d, где d — степень точки $\mathfrak{p}_1$. Поле вычетов точки $\mathfrak{p}$ относительно K' имеет базис $\{\bar{\omega}_1, \ldots, \bar{\omega}_d\}$, состоящий из d элементов. Пусть ω_k' есть элемент кольца точки $\mathfrak{p}$, принадлежащий классу вычетов $\bar{\omega}_k$ по модулю $\mathfrak{p}$ $(1\leqslant k\leqslant d)$. По теореме 3 § 6 в поле R можно найти такие элементы $\omega_1, \ldots, \omega_d$, что $\nu_{\mathfrak{p}}(\omega_k-\omega_k')\geqslant 1$, $\nu_{\mathfrak{p}_i}(\omega_k)\geqslant 0$ $(2\leqslant i\leqslant n)$. Ясно, что элемент ω_k также принадлежит классу вычетов $\bar{\omega}_k$. Каждый элемент поля вычетов точки $\mathfrak{p}$ может быть представлен в виде $\sum_{k=1}^{d}\lambda_k\bar{\omega}_k$ $(\lambda_k\in K',\ 1\leqslant k\leqslant d)$; поэтому каждый

элемент z из кольца точки $\mathfrak{p}$ можно представить в виде $z=\sum_{k=1}^{d}\lambda_k\omega_k+z'$, где $\lambda_k\in K'$, $(1\leqslant k\leqslant d)$ и $z'\in\mathfrak{p}$.

Элементы $u\omega_k$ $(1\leqslant k\leqslant d)$ принадлежат $\mathfrak{K}(\mathfrak{a}, S)$. Для произвольного элемента w из $\mathfrak{K}(\mathfrak{a}, S)$ имеем $\nu_{\mathfrak{p}}\left(\frac{w}{u}\right)\geqslant 0$; следовательно, элемент $\frac{w}{u}$ можно представить в виде $\sum_{k=1}^{d}\lambda_k\omega_k+z'$, где $z'\in\mathfrak{p}$, $\lambda_k\in K'$. Если $i>1$, то $\nu_{\mathfrak{p}_i}\left(\frac{w}{u}\right)\geqslant 0$, $\nu_{\mathfrak{p}_i}(\omega_k)\geqslant 0$, значит, $\nu_{\mathfrak{p}_i}(z')\geqslant 0$; если $i=1$, то $\nu_{\mathfrak{p}_1}(z'u)\geqslant$ $\geqslant e(\mathfrak{p}_1)+1$, ибо $z'\in\mathfrak{p}$. Отсюда следует, что $z'u$ принадлежит $\mathfrak{K}(\mathfrak{b}, S)$; таким образом, каждый элемент из $\mathfrak{K}(\mathfrak{a}, S)$ сравним по модулю $\mathfrak{K}(\mathfrak{b}, S)$ с некоторой линейной комбинацией элементов $u\omega_1, \ldots, u\omega_d$ с коэффициентами из K'. Этим уже доказано, что размерность $\mathfrak{K}(\mathfrak{a}, S)/\mathfrak{K}(\mathfrak{b}, S)$ конечна и $\leqslant d$. Чтобы доказать, что эта размерность равна d, достаточно показать, что элемент $w=\sum_{k=1}^{d}\lambda_k\omega_k u$ не принадлежит $\mathfrak{K}(\mathfrak{b}, S)$, если только коэффициенты $\lambda_1, \ldots, \lambda_d$ из поля K' не равны нулю одновременно. Класс вычетов элемента $\frac{w}{u}$ по модулю $\mathfrak{p}$ равен $\sum_{k=1}^{d}\lambda_k\bar{\omega}_k\neq 0$, поэтому $\nu_{\mathfrak{p}}\left(\frac{w}{u}\right)=0$ и $\nu_{\mathfrak{p}}(w)=\nu_{\mathfrak{p}}(u)=e(\mathfrak{p})$, что и доказывает наше утверждение (ибо $f(\mathfrak{p})=e(\mathfrak{p})+1$). Лемма 1, таким образом, доказана.

§ 8. Дивизор функции

Пусть K — поле комплексных чисел и пусть $u=\frac{f(x)}{g(x)}$ — рациональная функция, не равная 0, от комплексной переменной x, где f и g — многочлены с коэффициентами из K без общих множителей. Положим $R=K\langle x\rangle$; для $a\in K$ через $\mathfrak{p}_a$ обозначим точку поля R, в которой x принимает значения a, а через $\mathfrak{p}_\infty$ обозначим единственный полюс элемента x (точка $\mathfrak{p}_\infty$ в § 3 обозначалась через $\mathfrak{p}_{\frac{1}{x}}$). Числа a, для которых точка $\mathfrak{p}_a$ является нулем функции u, совпадают с корнями уравнения $f(x)=0$. Пусть $a_1, \ldots, a_h$ — все различные корни этого уравнения; если корень a_i имеет крат-

ность e_i $(1 \leqslant i \leqslant h)$, то точка $\mathfrak{p}_{a_i}$ является нулем функции u порядка e_i. С другой стороны,

$$f(x) = \alpha \prod_{i=1}^{h} (x - a_i)^{e_i}, \quad \alpha \in K,$$

значит, сумма $\sum_{i=1}^{h} e_i$ равна степени δ многочлена $f(x)$. Аналогично, числа a', для которых $\mathfrak{p}_{a'}$ является полюсом функции u, совпадают с корнями уравнения $g(x) = 0$; если $a'_1, \ldots, a'_{h'}$ — корни этого уравнения, а $e'_1, \ldots, e'_{h'}$ — их кратности, то сумма $\sum_{i=1}^{h'} e'_i$ равна степени δ' многочлена $g(x)$. Что касается точки $\mathfrak{p}_\infty$, то как мы видели, порядок функции u в этой точке равен $\delta' - \delta$. Имеем теперь

$$\delta' - \delta + \sum_{i=1}^{h} e_i - \sum_{i=1}^{h'} e'_i = 0,$$

что можно записать также в виде

$$\sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(u) = 0,$$

где суммирование ведется по всем точкам $\mathfrak{p}$ поля $K\langle x\rangle$. Таким образом, для любой рациональной функции $u \neq 0$ с комплексными коэффициентами сумма порядков функции u во всех точках поля $K\langle x\rangle$ равна 0.

Желая найти обобщение последнего утверждения, рассмотрим случай поля рациональных функций $R = K\langle x\rangle$ над полем вещественных чисел K и в этом поле рассмотрим многочлен $u = x^2 + px + q$ (p и q — вещественные числа). Многочлен u имеет единственный полюс $\mathfrak{p}_{\frac{1}{x}}$, и порядок этого полюса равен 2. Что касается нулей многочлена u, то здесь надо рассмотреть несколько случаев.

1) Если $p^2 - 4q > 0$, то $u = (x - x_1)(x - x_2)$, где x_1 и x_2 — различные вещественные числа. Следовательно, многочлен u имеет два нуля, каждый из которых имеет порядок 1; это будут точки $\mathfrak{p}_1$ и $\mathfrak{p}_2$, соответствующие неприводимым многочленам $x - x_1$ и $x - x_2$ (см. § 3).

2) Если $p^2-4q=0$, то $u=(x-x_3)^2$, где $x_3=-\frac{p}{2}$. В этом случае многочлен u имеет единственный нуль порядка 2; этим нулем является точка $\mathfrak{p}_3$, соответствующая неприводимому многочлену $x-x_3$.

3) Если $p^2-4q<0$, то многочлен u неприводим и, следовательно, имеет единственный нуль порядка 1, которым является точка $\mathfrak{p}_4$, соответствующая неприводимому многочлену u.

Таким образом, в случаях 1) и 2) сумма порядков элемента u во всех точках также равна 0; однако это утверждение в случае 3) уже неверно. В связи с этим можно заметить следующее. В случае, когда поле K было полем комплексных чисел, степень каждой точки была равна 1. В рассматриваемом поле степени точек $\mathfrak{p}_1$ и $\mathfrak{p}_2$ в случае 1) и точки $\mathfrak{p}_3$ в случае 2) также равны 1, но в случае 3) степень точки $\mathfrak{p}_4$ равна 2 (так как степень многочлена u равна 2; см. § 3). Таким образом, мы видим, что во всех рассмотренных нами случаях имеет место равенство

$$\sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(u)\, d(\mathfrak{p})=0;$$

другими словами, степень дивизора $\mathfrak{a}=\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(u)}$ равна 0. Именно это последнее утверждение мы и докажем в самом общем случае.

Итак, пусть теперь R — поле алгебраических функций от одной переменной над произвольным полем, x — отличный от 0 элемент поля R. Сумма $\sum_{\mathfrak{p}} d(\mathfrak{p})\nu_{\mathfrak{p}}(x)$ имеет смысл лишь при условии, что только конечное число чисел $\nu_{\mathfrak{p}}(x)$ отлично от 0, т. е. что элемент x имеет только конечное число нулей и полюсов. Докажем, что это действительно так.

Лемма 1. *Каждый отличный от константы элемент x поля R алгебраических функций от одной переменной имеет только конечное число нулей; далее, если $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ — все различные нули элемента x, то*

$$\sum_{i=1}^{h} d(\mathfrak{p}_i)\,\nu_{\mathfrak{p}_i}(x) \leqslant [R:K(x)],$$

где K — поле констант поля R.

Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ — различные нули элемента x (не обязательно все). Положим $\mathfrak{b} = \prod_{i=1}^{k} \mathfrak{p}_i^{b_i}$, где $b_i = \nu_{\mathfrak{p}_i}(x)$, и обозначим через $\mathfrak{e}$ единичный дивизор. Пусть S обозначает множество точек $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$. Согласно лемме 1 § 7 размерность δ пространства $\mathfrak{K}(\mathfrak{e}, S)/\mathfrak{K}(\mathfrak{b}, S)$ конечна и равна $\sum_{i=1}^{k} d(\mathfrak{p}_i)\nu_{\mathfrak{p}_i}(x)$. Пусть $z_1, \ldots, z_\delta$ — элементы пространства $\mathfrak{K}(\mathfrak{e}, S)$, смежные классы которых по модулю $\mathfrak{K}(\mathfrak{b}, S)$ линейно независимы над K. Докажем, что элементы $z_1, \ldots, z_\delta$ сами линейно независимы над $K\langle x\rangle$. Допустим, что это не так, т. е. что существует зависимость

$$\sum_{j=1}^{\delta} u_j z_j = 0, \tag{1}$$

где $u_1, \ldots, u_\delta$ — элементы поля $K\langle x\rangle$, причем не все они равны 0. Каждый элемент u_j может быть представлен в виде отношения двух многочленов от x с коэффициентами из K. Умножая на общий знаменатель, получим зависимость вида (1), в которой элементы u_j являются уже многочленами от x (хоть один из которых $\neq 0$). Кроме того, можно считать, что $u_1, \ldots, u_\delta$ не делятся на x одновременно (это достигается делением на некоторую степень x). Если записать $u_j = u_j(0) + xv_j$, где $v_j \in K[x]$, то (1) принимает вид

$$\sum_{j=1}^{\delta} u_j(0) z_j = -x \sum_{j=1}^{\delta} v_j z_j.$$

Так как $\nu_{\mathfrak{p}_i}(x) > 0$ и $v_j \in K[x]$, то $\nu_{\mathfrak{p}_i}(v_j) \geqslant 0$ $(1 \leqslant i \leqslant k)$; далее, $\nu_{\mathfrak{p}_i}(z_j) \geqslant 0$, ибо $z_j \in \mathfrak{K}(\mathfrak{e}, S)$ и $\mathfrak{p}_i \in S$. Следовательно, $\nu_{\mathfrak{p}_i}\left(-x \sum_{j=1}^{\delta} v_j z_j\right) \geqslant \nu_{\mathfrak{p}_i}(x)$, т. е. $-x \sum_{j=1}^{\delta} v_j z_j \in \mathfrak{K}(\mathfrak{b}, S)$, откуда $\sum_{j=1}^{\delta} u_j(0) z_j \in \mathfrak{K}(\mathfrak{b}, S)$. Последнее, однако, невозможно, так как смежные классы элементов $z_1, \ldots, z_\delta$ по модулю $\mathfrak{K}(\mathfrak{b}, S)$ линейно независимы над K, а элементы $u_j(0)$ поля K не все равны нулю. Этим доказано, что элементы $z_1, \ldots, z_\delta$

линейно независимы над $K\langle x\rangle$. Отсюда следует, что

$$\delta = \sum_{i=1}^{k} d(\mathfrak{p}_i)\, \nu_{\mathfrak{p}_i}(x) \leqslant [R : K\langle x\rangle]. \tag{2}$$

Так как $\nu_{\mathfrak{p}_i}(x) \geqslant 1$, то $k \leqslant [R : K\langle x\rangle]$. Таким образом, элемент x не может иметь более чем $[R : K\langle x\rangle]$ нулей. При $k = h$ неравенство (2) превращается в неравенство леммы 1.

Докажем теперь, что число $\sum_{i=1}^{k} d(\mathfrak{p}_i)\, \nu_{\mathfrak{p}_i}(x)$, указанное в лемме 1, в действительности равно $[R : K\langle x\rangle]$.

Для этого рассмотрим подкольцо $K[x^{-1}]$ поля $K\langle x\rangle$. Напомним, что элемент w поля R называется целым над $K[x^{-1}]$, если он удовлетворяет уравнению вида $w^m + f_1 w^{m-1} + \ldots + f_m = 0$, где $f_1, \ldots, f_m$ принадлежат кольцу $K[x^{-1}]$. В этом случае элемент w не может иметь полюсов вне множества $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}$. Действительно, если точка $\mathfrak{p}$ не является нулем элемента x, то кольцо $\mathfrak{o}$ точки $\mathfrak{p}$ целозамкнуто (см. § 2) и содержит кольцо $K[x^{-1}]$, значит $w \in \mathfrak{o}$.

Пусть $n = [R : K\langle x\rangle]$. Покажем, что в поле R можно найти базис $\{w_1, \ldots, w_n\}$ относительно $K\langle x\rangle$, элементы которого являются целыми над $K[x^{-1}]$. Пусть $\{w'_1, \ldots, w'_n\}$ — произвольный базис поля R относительно $K\langle x\rangle$. Каждый элемент w'_ν удовлетворяет уравнению вида

$$w'^n_\nu + \sum_{\lambda=1}^{n} \varphi_{\nu,\lambda} w'^{n-\lambda}_\nu = 0,$$

где $\varphi_{\nu,\lambda} \in K\langle x\rangle$. Каждый элемент $\varphi_{\nu,\lambda}$ можно представить в виде $\frac{f_{\nu,\lambda}}{g_\nu}$, где $f_{\nu,\lambda}$ и g_ν принадлежат $K[x^{-1}]$. Полагая $w_\nu = g_\nu w'_\nu$, будем иметь

$$w^n_\nu + \sum_{\lambda=1}^{n} g^\lambda_\nu \varphi_{\nu,\lambda} w^{n-\lambda}_\nu = 0,$$

где $g^\lambda_\nu \varphi_{\nu,\lambda} = g^{\lambda-1}_\nu f_{\nu,\lambda} \in K[x^{-1}]$; это означает, что элементы w_ν являются целыми над $K[x^{-1}]$. С другой стороны, очевидно, что $w_1, \ldots, w_n$ образуют базис поля R относительно $K\langle x\rangle$ (так как w_ν является произведением w'_ν на элемент $\neq 0$ из $K\langle x\rangle$).

Пусть целое $\sigma \geqslant 0$ таково, что $\nu_{\mathfrak{p}_i}(w_\nu) \geqslant -\sigma$ $(1 \leqslant i \leqslant h,$ $1 \leqslant \nu \leqslant n)$, и пусть μ — достаточно большое целое число (в частности, будем считать, что $\mu > \sigma$). Рассмотрим произведения $x^{-\rho}w_\nu$, где $0 \leqslant \rho \leqslant \mu - \sigma$, $1 \leqslant \nu \leqslant n$. Так как $\nu_{\mathfrak{p}_i}(x) \geqslant 1$, то

$$\nu_{\mathfrak{p}_i}(x^{-\rho}w_\nu) \geqslant -\rho\nu_{\mathfrak{p}_i}(x) - \sigma \geqslant -\mu\nu_{\mathfrak{p}_i}(x).$$

С другой стороны, для точки $\mathfrak{p}$, отличной от $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$, имеем $\nu_{\mathfrak{p}}(x^{-1}) \geqslant 0$, $\nu_{\mathfrak{p}}(w_\nu) \geqslant 0$ $(1 \leqslant \nu \leqslant n)$; значит, $\nu_{\mathfrak{p}}(x^{-\rho}w_\nu) \geqslant 0$. Таким образом,

$$x^{-\rho}w_\nu \equiv 0 \pmod{\mathfrak{b}^{-\mu}},$$

где $\mathfrak{b}$ есть дивизор $\prod_{i=1}^{h} \mathfrak{p}_i^{b_i}$, $b_i = \nu_{\mathfrak{p}_i}(x)$.

Обозначим через $\mathfrak{L}_\mu$ векторное пространство над полем K, состоящее из тех элементов поля R, которые $\equiv 0 \pmod{\mathfrak{b}^{-\mu}}$, а через $\mathfrak{L}'_\mu$ — подпространство пространства $\mathfrak{L}_\mu$, натянутое на элементы $x^{-\rho}w_\nu$ $(0 \leqslant \rho \leqslant \mu - \sigma,$ $1 \leqslant \nu \leqslant n)$. Так как элементы w_ν линейно независимы над $K\langle x\rangle$, а элементы $x^{-\rho}$ поля $K\langle x\rangle$ линейно независимы над K, то элементы $x^{-\rho}w_\nu$ (число которых равно $n(\mu - \sigma + 1)$) линейно независимы над K; значит, размерность пространства $\mathfrak{L}'_\mu$ равна $n(\mu - \sigma + 1)$. С другой стороны, мы имеем $\mathfrak{L}_\mu \subset \mathfrak{K}(\mathfrak{b}^{-\mu}, S)$, где $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}$. Если $\mathfrak{e}$ обозначает единичный дивизор, то, как нам уже известно, пространство $\mathfrak{K}(\mathfrak{b}^{-\mu}, S)/\mathfrak{K}(\mathfrak{e}, S)$ имеет размерность $\mu d(\mathfrak{b})$ (лемма 1 § 7); отсюда следует, что пространство $\mathfrak{L}_\mu/(\mathfrak{L}_\mu \cap \mathfrak{K}(\mathfrak{e}, S))$ имеет размерность $\leqslant \mu d(\mathfrak{b})$. Далее, каждый элемент из $\mathfrak{L}_\mu \cap \mathfrak{K}(\mathfrak{e}, S)$ не имеет полюсов вне S (так как он принадлежит $\mathfrak{L}_\mu$) и не имеет полюсов в S (так как он принадлежит $\mathfrak{K}(\mathfrak{e}, S)$); следовательно, всякий такой элемент является константой (следствие 3 к теореме 1 § 4), откуда следует, что пространство $\mathfrak{L}_\mu \cap \mathfrak{K}(\mathfrak{e}, S)$ имеет размерность $\leqslant 1$. Таким образом, пространство $\mathfrak{L}_\mu$ имеет размерность $\leqslant \mu d(\mathfrak{b}) + 1$. Так как $\mathfrak{L}'_\mu \subset \mathfrak{L}_\mu$, то $n(\mu - \sigma + 1) \leqslant$ $\leqslant \mu d(\mathfrak{b}) + 1$, откуда

$$d(\mathfrak{b}) \geqslant n - \frac{(\sigma - 1)n + 1}{\mu}.$$

Так как полученное неравенство имеет место для всех достаточно больших чисел μ, то $d(\mathfrak{b}) \geqslant n$. С другой стороны,

нами уже доказано, что $d(\mathfrak{b}) \leqslant n$ (лемма 1); таким образом, имеем $d(\mathfrak{b}) = n$. Кроме того, замечаем, что при возрастании μ до бесконечности взаимные разности между размерностью $\mathfrak{L}_\mu$, размерностью $\mathfrak{L}'_\mu$ и числом $\mu d(\mathfrak{b}) = n\mu$ остаются ограниченными.

Если $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ — все различные нули элемента $x \neq 0$ из поля R, и $b_i = \nu_{\mathfrak{p}_i}(x)$, то дивизор $\mathfrak{b} = \prod_{i=1}^{h} \mathfrak{p}_i^{b_i}$ называется *дивизором нулей* элемента x. Нами доказана

Теорема 4. *Пусть R — поле алгебраических функций от одной переменной, и пусть K — его поле констант. Если элемент x из R не принадлежит K, то степень дивизора нулей этого элемента равна* $[R : K\langle x\rangle]$.

Если наши результаты применить теперь к элементу x^{-1} (вместо x), то получим, что элемент x имеет только конечное число полюсов. Если $\mathfrak{q}_1, \ldots, \mathfrak{q}_l$ — все различные полюса элемента x и $c_i = -\nu_{\mathfrak{q}_i}(x)$, то целый дивизор $\mathfrak{c} = \prod_{i=1}^{l} \mathfrak{q}_i^{c_i}$ называется *дивизором полюсов* элемента x. Так как $K\langle x\rangle = K\langle x^{-1}\rangle$, то нами доказан следующий результат.

Следствие. *В обозначениях теоремы 4 имеем: степень дивизора полюсов элемента x равна* $[R : K\langle x\rangle]$.

Дивизор $\mathfrak{b}\mathfrak{c}^{-1}$ можно представить в виде $\mathfrak{b}\mathfrak{c}^{-1} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(x)}$. Этот дивизор называется *дивизором элемента x* и обозначается через $\mathfrak{d}(x)$. Он определен, разумеется, только для $x \neq 0$; если x является константой, то $\mathfrak{d}(x)$ — единичный дивизор. Если x и y являются элементами $\neq 0$ поля R, то, очевидно,

$$\mathfrak{d}(xy) = \mathfrak{d}(x)\,\mathfrak{d}(y), \quad \mathfrak{d}(x^{-1}) = (\mathfrak{d}(x))^{-1}.$$

Из предыдущего вытекает также

Теорема 5. *Степень дивизора любого отличного от нуля элемента поля алгебраических функций от одной переменной равна* 0.

Пусть $\mathfrak{D}$ — группа всех дивизоров поля R алгебраических функций от одной переменной, и пусть $\mathfrak{D}_0$ — группа дивизоров элементов поля R. Смежные классы элементов из $\mathfrak{D}$ по модулю $\mathfrak{D}_0$ называются *классами дивизоров*; два дивизора, принадлежащие одному и тому же классу, называются *эквивалентными* друг другу. Все дивизоры из одного

класса, как это следует из теоремы 5, имеют равные степени; эта степень называется *степенью класса*.

Заканчивая настоящий параграф, сформулируем в виде лемм два утверждения, установленные в процессе доказательства теоремы 4, которые понадобятся нам в дальнейшем.

Лемма 2. *Сохраняя условия теоремы* 4, *обозначим через* $\mathfrak{b}$ *дивизор нулей элемента* x. *Тогда пространство элементов поля* R, *которые* $\equiv 0 \pmod{\mathfrak{b}^{-\mu}}$ (μ — *целое положительное число*), *имеет над полем* K *размерность* $\geqslant \mu d(\mathfrak{b}) - \tau$, *где* τ — *целое число, не зависящее от* μ.

Лемма 3. *Пусть сохраняются условия теоремы* 4 *и пусть* $\mathfrak{R}$ *есть кольцо элементов поля* R, *не имеющих полюсов вне множества нулей элемента* x. *Утверждается, что в кольце* $\mathfrak{R}$ *существует конечное подмножество* $\{w_1, \ldots, w_N\}$, *содержащее базис* R *относительно* $K\langle x\rangle$, *такое, что каждый элемент из* $\mathfrak{R}$ *является линейной комбинацией элементов* $w_1, \ldots, w_N$ *с коэффициентами из* $K[x^{-1}]$.

Воспользуемся обозначениями доказательства теоремы 4. Очевидно, что кольцо $\mathfrak{R}$ является объединением пространств $\mathfrak{L}_\mu$ $(1 \leqslant \mu < \infty)$. Как было отмечено, разность между размерностями пространств $\mathfrak{L}_\mu$ и $\mathfrak{L}'_\mu$ ограничена; обозначим через m — наибольшее значение этой разности. Пусть $z_1, \ldots, z_r$ — элементы кольца $\mathfrak{R}$, классы вычетов которых по модулю пространства $\sum_{\nu=1}^{n} K[x^{-1}]\, w_\nu$ линейно независимы над K. Тогда существует такое число $\mu > 0$, что все элементы $z_1, \ldots, z_r$ принадлежат $\mathfrak{L}_\mu$; так как нетривиальная линейная комбинация элементов $z_1, \ldots, z_r$ с коэффициентами из K не может принадлежать $\mathfrak{L}'_\mu$, то $r \leqslant m$. Отсюда следует, что в кольце $\mathfrak{R}$ существует конечное число элементов $w_{n+1}, \ldots, w_N$ таких, что каждый элемент из $\mathfrak{R}$ представляется в виде суммы элемента из пространства $\sum_{\nu=1}^{n} K[x^{-1}]\, w_\nu$ и линейной комбинации элементов $w_{n+1}, \ldots, w_N$ с коэффициентами из K. Лемма 3, следовательно, доказана.

ГЛАВА II

ТЕОРЕМА РИМАНА — РОХА

§ 1. Род

Пусть R — поле алгебраических функций от одной переменной, а K — его поле констант. Мы уже видели, что для заданного конечного числа точек поля R не существует никакой необходимой зависимости между поведением произвольного элемента из R в этих точках (см. теорема 3 § 6 гл. I). Положение в корне меняется, если вместо конечного числа мы рассматриваем бесконечно много точек. В этом случае между поведением элемента поля R в этих точках уже существуют зависимости; например, для элемента поля R нулями могут являться либо все точки (если элемент равен 0), либо только конечное число точек. Изучение этих зависимостей и является главной целью настоящей главы. Проблема может быть сформулирована следующим образом: если для каждой точки $\mathfrak{p}$ задан элемент $x_{\mathfrak{p}} \in R$ и задано целое число $m_{\mathfrak{p}}$, то существует ли элемент $x \in R$, удовлетворяющий условиям

$$\nu_{\mathfrak{p}}(x - x_{\mathfrak{p}}) \geqslant m_{\mathfrak{p}}, \tag{1}$$

а если существует, то какова структура множества элементов x, удовлетворяющих этим условиям?

Если все элементы $x_{\mathfrak{p}}$ равны 0, то элементы, удовлетворяющие условиям (1), очевидно, образуют векторное пространство над K. Этот случай будем называть „однородным". В общем случае, если x является решением неравенств (1), то все другие решения этой же задачи могут быть представлены в виде суммы решения x с решениями y однородной задачи, определяемой условиями $\nu_{\mathfrak{p}}(y) \geqslant m_{\mathfrak{p}}$. Таким образом, как это обычно имеет место в линейных задачах, вопрос о решениях системы (1) распадается на

две части: 1) существует ли хоть одно решение? 2) каковы решения соответствующей однородной задачи?

Рассмотрим сначала однородную задачу, определяемую условиями

$$\nu_{\mathfrak{p}}(x) \geqslant m_{\mathfrak{p}}. \tag{2}$$

Если $m_{\mathfrak{p}} > 0$ для бесконечного числа точек $\mathfrak{p}$, то единственным решением этой задачи является константа 0 (лемма 1 § 8 гл. I). Нас будет интересовать главным образом случай, когда все целые числа $m_{\mathfrak{p}}$ за исключением конечного числа равны 0; в этом случае условия (2) эквивалентны условию $x \equiv 0 \pmod{\mathfrak{a}}$, где $\mathfrak{a}$ есть дивизор $\prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}$. Особый интерес этого случая состоит в том, что здесь, как мы увидим, решения образуют векторное пространство конечной размерности над полем K.

Для произвольного дивизора $\mathfrak{a}$ через $\mathfrak{L}(\mathfrak{a})$ будем обозначать пространство тех элементов $x \in R$, которые $\equiv 0 \pmod{\mathfrak{a}}$.

Если дивизор $\mathfrak{b}$ делится на $\mathfrak{a}$, то $\mathfrak{L}(\mathfrak{b})$, очевидно, содержится в $\mathfrak{L}(\mathfrak{a})$. Прежде всего мы докажем, что векторное пространство $\mathfrak{L}(\mathfrak{a})/\mathfrak{L}(\mathfrak{b})$ имеет конечную размерность, и найдем верхнюю границу для этой размерности.

Пусть S обозначает множество тех точек, которые входят в дивизоры $\mathfrak{a}$ или $\mathfrak{b}$ с показателями $\neq 0$; ясно, что S является конечным множеством точек. Пусть $\mathfrak{K}(\mathfrak{a}, S)$ и $\mathfrak{K}(\mathfrak{b}, S)$ — пространства, рассматривавшиеся в § 7 гл. I. Ясно $\mathfrak{L}(\mathfrak{a}) \subset \mathfrak{K}(\mathfrak{a}, S)$ и $\mathfrak{L}(\mathfrak{b}) \subset \mathfrak{K}(\mathfrak{b}, S)$. Более того, имеет место равенство

$$\mathfrak{L}(\mathfrak{b}) = \mathfrak{L}(\mathfrak{a}) \cap \mathfrak{K}(\mathfrak{b}, S). \tag{3}$$

Действительно, включение $\mathfrak{L}(\mathfrak{b}) \subset \mathfrak{L}(\mathfrak{a}) \cap \mathfrak{K}(\mathfrak{b}, S)$ очевидно. Обратно, если $x \in \mathfrak{L}(\mathfrak{a}) \cap \mathfrak{K}(\mathfrak{b}, S)$, то $\nu_{\mathfrak{p}}(x) \geqslant 0$ для всех точек $\mathfrak{p}$, не принадлежащих S (так как эти точки входят в $\mathfrak{a}$ с показателем 0), а так как $x \in \mathfrak{K}(\mathfrak{b}, S)$, то $x \in \mathfrak{L}(\mathfrak{b})$, и равенство (3) доказано.

Таким образом, пространство $\mathfrak{L}(\mathfrak{a})/\mathfrak{L}(\mathfrak{b})$ равно $\mathfrak{L}(\mathfrak{a})/(\mathfrak{L}(\mathfrak{a}) \cap \mathfrak{K}(\mathfrak{b}, S))$. Согласно теореме об изоморфизме, последнее пространство изоморфно подпространству $(\mathfrak{L}(\mathfrak{a}) + \mathfrak{K}(\mathfrak{b}, S))/\mathfrak{K}(\mathfrak{b}, S)$ пространства $\mathfrak{K}(\mathfrak{a}, S)/\mathfrak{K}(\mathfrak{b}, S)$, имеющего конечную размерность (лемма 1 § 7 гл I); следовательно, $\mathfrak{L}(\mathfrak{a})/\mathfrak{L}(\mathfrak{b})$ также имеет конечную размерность. Так как S содержит все точки, входящие в дивизоры $\mathfrak{a}$ и $\mathfrak{b}$ с показателями $\neq 0$, то

размерность пространства $\mathfrak{K}(\mathfrak{a}, S)/\mathfrak{K}(\mathfrak{b}, S)$ равна $d(\mathfrak{b}) - d(\mathfrak{a})$ (лемма 1 § 7 гл. I). Таким образом, размерность пространства $\mathfrak{L}(\mathfrak{a})/\mathfrak{L}(\mathfrak{b})$ не превосходит $d(\mathfrak{b}) - d(\mathfrak{a})$.

Докажем теперь, что $\mathfrak{L}(\mathfrak{a})$ имеет конечную размерность. В силу только что изложенного, для этого достаточно показать, что для некоторого дивизора $\mathfrak{b}$, делящегося на $\mathfrak{a}$, пространство $\mathfrak{L}(\mathfrak{b})$ имеет конечную размерность. В качестве $\mathfrak{b}$ мы возьмем целый дивизор, делящийся на $\mathfrak{a}$ и отличный от единичного дивизора (ясно, что такой дивизор существует). Если $x \in \mathfrak{L}(\mathfrak{b})$, то элемент x имеет по крайней мере один нуль (ибо $\mathfrak{b}$ — не единичный дивизор), но не имеет полюсов (ибо $\mathfrak{b}$ — целый). Согласно следствию 3 к теореме 1 § 4 гл. I элемент x является константой. Но отличная от 0 константа не имеет нулей, поэтому $x = 0$. Таким образом, $\mathfrak{L}(\mathfrak{b})$ состоит только из 0.

Для любого дивизора $\mathfrak{a}$ через $l(\mathfrak{a})$ будем обозначать размерность пространства $\mathfrak{L}(\mathfrak{a})$. Если $\mathfrak{b}$ делится на $\mathfrak{a}$, то размерность пространства $\mathfrak{L}(\mathfrak{a})/\mathfrak{L}(\mathfrak{b})$ равна $l(\mathfrak{a}) - l(\mathfrak{b})$; следовательно, мы имеем неравенство $l(\mathfrak{a}) - l(\mathfrak{b}) \leqslant d(\mathfrak{b}) - d(\mathfrak{a})$, или

$$l(\mathfrak{a}) + d(\mathfrak{a}) \leqslant l(\mathfrak{b}) + d(\mathfrak{b}). \tag{4}$$

С другой стороны, некоторые сведения о числе $l(\mathfrak{a})$ для дивизоров $\mathfrak{a}$ определенного вида дает нам лемма 2 § 8 гл. I. Пусть x — произвольный не равный константе элемент поля R и пусть $\mathfrak{x}$ — его дивизор нулей. Для всех достаточно больших целых чисел μ имеем $l(\mathfrak{x}^{-\mu}) \geqslant \mu d(\mathfrak{x}) - \tau$, где целое число τ зависит только от x. Это неравенство можно записать в виде $l(\mathfrak{x}^{-\mu}) + d(\mathfrak{x}^{-\mu}) \geqslant -\tau$. Принимая во внимание (4), получаем

$$l(\mathfrak{b}) + d(\mathfrak{b}) \geqslant -\tau \tag{5}$$

для всех дивизоров $\mathfrak{b}$, делящихся на $\mathfrak{x}^{-\mu}$ при некотором μ. Пользуясь этим, можно теперь доказать, что числа $l(\mathfrak{a}) + d(\mathfrak{a})$ ограничены снизу для всех дивизоров $\mathfrak{a}$.

Лемма 1. *Если дивизоры $\mathfrak{b}$ и $\mathfrak{b}'$ — эквивалентны, то $d(\mathfrak{b}) = d(\mathfrak{b}')$ и $l(\mathfrak{b}) = l(\mathfrak{b}')$.*

Первое утверждение непосредственно вытекает из теоремы 5 § 8 гл. I. Для доказательства второго утверждения обозначим через z такой элемент поля R, что $\mathfrak{b}' = \mathfrak{d}(z)\mathfrak{b}$. Условия $u \equiv 0 \pmod{\mathfrak{b}}$ и $zu \equiv 0 \pmod{\mathfrak{b}'}$, очевидно, эквивалентны друг другу. Таким образом, если $u \in \mathfrak{L}(\mathfrak{b})$, то $zu \in \mathfrak{L}(\mathfrak{b}')$;

обратно, если $u' \in \mathfrak{L}(\mathfrak{b}')$, то $z^{-1}u' \in \mathfrak{L}(\mathfrak{b})$. Отображение $u \to zu$ является взаимно однозначным линейным отображением $\mathfrak{L}(\mathfrak{b})$ на $\mathfrak{L}(\mathfrak{b}')$, а значит, $l(\mathfrak{b}) = l(\mathfrak{b}')$.

Из доказанной леммы 1 следует, что неравенство (5) справедливо также для всякого дивизора $\mathfrak{b}$, который эквивалентен дивизору, делящемуся на $\mathfrak{x}^{-\mu}$ (при каком-нибудь μ). Докажем сейчас, что последнее имеет место для каждого дивизора $\mathfrak{b}$ поля $\mathfrak{R}$.

Пусть $\mathfrak{p}$ — произвольная точка, не являющаяся нулем элемента x, а значит, не являющаяся полюсом элемента x^{-1}. Значение ξ, принимаемое элементом x^{-1} в точке $\mathfrak{p}$, является элементом поля вычетов точки $\mathfrak{p}$, которое алгебраично над K (теорема 2 § 5 гл. I). Следовательно, существует такой многочлен $f_{\mathfrak{p}}$ с коэффициентами из K, что $f_{\mathfrak{p}}(\xi) = 0$, т. е. $\nu_{\mathfrak{p}}(f_{\mathfrak{p}}(x^{-1})) \geqslant 1$. Пусть $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{b(\mathfrak{p})}$ — произвольный дивизор. Ясно, что имеется лишь конечное число точек $\mathfrak{p}$, для которых $b(\mathfrak{p}) < 0$. Положим

$$z = \prod{}' f_{\mathfrak{p}}^{-b(\mathfrak{p})}(x^{-1}),$$

где произведение $\prod'$ распространено на все точки $\mathfrak{p}$, не являющиеся нулями элемента x и для которых $b(\mathfrak{p}) < 0$ (если таких точек нет, то полагаем $z = 1$). Для этих точек, очевидно, имеем $\nu_{\mathfrak{p}}(z) \geqslant -b(\mathfrak{p})$, и, следовательно, все они входят в дивизор $\mathfrak{b}' = \mathfrak{d}(z)\mathfrak{b}$ с показателем $\geqslant 0$. С другой стороны, все полюса элемента $f_{\mathfrak{p}}(x^{-1})$ находятся среди нулей элемента x. Следовательно, элемент z не имеет полюсов вне множества нулей элемента x, поэтому каждая точка, не являющаяся нулем элемента x, входит в $\mathfrak{b}'$ с показателем $\geqslant 0$. Пусть теперь $\mathfrak{q}_1, \ldots, \mathfrak{q}_h$ — все различные нули элемента x, а μ — такое целое число, что $-\mu$ меньше всех показателей, с которыми точки $\mathfrak{q}_1, \ldots, \mathfrak{q}_h$ входят в $\mathfrak{b}'$. Так как каждая точка $\mathfrak{q}_i$ входит в $\mathfrak{x}$ с показателем $\geqslant 1$, то, очевидно, $\mathfrak{b}'$ делится на $\mathfrak{x}^{-\mu}$. Этим доказано, что каждый дивизор эквивалентен дивизору, делящемуся на $\mathfrak{x}^{-\mu}$ при некотором μ. Следовательно, неравенство $l(\mathfrak{b}) + d(\mathfrak{b}) \geqslant -\tau$ справедливо для всех дивизоров поля R.

Введем теперь в рассмотрение целое число g, определяемое формулой

$$-g + 1 = \min\{l(\mathfrak{b}) + d(\mathfrak{b})\},$$

где $\mathfrak{b}$ пробегает все дивизоры поля. Это число g, играющее весьма важную роль в изучении структуры поля R, называется *родом* поля R.

Род поля R всегда $\geqslant 0$. Действительно, для единичного дивизора $\mathfrak{e}$ имеем $d(\mathfrak{e})=0$; далее, пространство $\mathfrak{L}(\mathfrak{e})$ состоит только из констант (следствие 3 к теореме 1 § 4 гл. I), поэтому $l(\mathfrak{e})=1$ и $l(\mathfrak{e})+d(\mathfrak{e})=1$.

Так как $d(\mathfrak{a}^{-1})=-d(\mathfrak{a})$, то нами получена следующая теорема.

Теорема 1 (теорема Римана). *Пусть R — поле алгебраических функций от одной переменной и g — его род. Для любого дивизора $\mathfrak{a}$ поля R через $l(\mathfrak{a})$ обозначим размерность пространства тех элементов поля R, которые $\equiv 0 \pmod{\mathfrak{a}}$. Тогда имеем $l(\mathfrak{a}) \geqslant d(\mathfrak{a}^{-1})-g+1$; далее, по крайней мере для одного дивизора $\mathfrak{a}_0$ имеет место равенство $l(\mathfrak{a})=d(\mathfrak{a}^{-1})-g+1$, причем, если это равенство имеет место для $\mathfrak{a}_0$, то оно имеет место также для всякого дивизора $\mathfrak{a}$, являющегося делителем $\mathfrak{a}_0$.*

Последнее утверждение непосредственно следует из (4).

§ 2. Поля рода 0

Пусть $R=K\langle x\rangle$, где K — некоторое поле, а x — трансцендентный элемент над K. Как мы знаем, R является полем алгебраических функций от одной переменной, поле констант которого совпадает с K (§ 3 гл. I). Покажем, что род поля R равен нулю. Так как элемент x имеет единственный нуль $\mathfrak{x}$ (степень которого равна 1), то его дивизор нулей равен $\mathfrak{x}$. В процессе доказательства теоремы 1 § 1 мы видели, что произвольный дивизор $\mathfrak{b}$ поля R эквивалентен дивизору $\mathfrak{b}'$, делящемуся на $\mathfrak{x}^{-\mu}$ (при некотором μ); следовательно,

$$l(\mathfrak{b})+d(\mathfrak{b})=l(\mathfrak{b}')+d(\mathfrak{b}')\geqslant l(\mathfrak{x}^{-\mu})+d(\mathfrak{x}^{-\mu}).$$

Так как $d(\mathfrak{x}^{-\mu})=-\mu$, то род g поля R может быть определен формулой

$$-g+1=\min_{0<\mu<\infty}\{l(\mathfrak{x}^{-\mu})-\mu\}.$$

Вычислим $l(\mathfrak{x}^{-\mu})$. Всякий элемент u поля R можно представить в виде $\dfrac{f(x^{-1})}{h(x^{-1})}$, где f и h — многочлены с коэффи-

циентами из K без общих множителей. Выясним, при каком условии $u \equiv 0 \pmod{\mathfrak{x}^{-\mu}}$. Для любого неприводимого многочлена φ с коэффициентами из K элемент $\varphi(x^{-1})$ не является константой, поэтому существует точка $\mathfrak{p}_\varphi$ поля R, содержащая $\varphi(x^{-1})$ (теорема 1 § 4 гл. I); далее, пересечение $\mathfrak{p}_\varphi \cap K[x^{-1}]$ состоит из тех элементов кольца $K[x^{-1}]$, которые делятся в этом кольце на $\varphi(x^{-1})$. Так как $\mathfrak{p}_\varphi$ не является полюсом элемента u, то $h(x^{-1})$ не делится на $\varphi(x^{-1})$. В силу произвольности неприводимого многочлена φ отсюда следует, что h является константой; можно считать, что $h=1$. Если степень многочлена f равна m, то для $f(x^{-1})$ дивизор $\mathfrak{x}$ является полюсом порядка m (§ 3 гл. I), поэтому $m \leqslant \mu$. Таким образом, элементы поля R, которые $\equiv 0 \pmod{\mathfrak{x}^{-\mu}}$, являются линейными комбинациями элементов $1, x^{-1}, \ldots, x^{-\mu}$ с коэффициентами из K, откуда $l(\mathfrak{x}^{-\mu}) = \mu + 1$ и, значит, $g=0$. Итак, *род любого поля алгебраических функций от одной переменной, являющегося чисто трансцендентным расширением поля констант, равен* 0.

Обратно, пусть род поля R алгебраических функций от одной переменной равен 0. Покажем, что если в R существует хоть одна точка $\mathfrak{p}$ степени 1, то R является чисто трансцендентным расширением своего поля констант. По теореме Римана имеем $l(\mathfrak{p}^{-1}) \geqslant d(\mathfrak{p}) + 1 = 2$; следовательно в поле R существует по крайней мере один элемент x, не принадлежащий полю констант K, который $\not\equiv 0 \pmod{\mathfrak{p}^{-1}}$. Дивизор нулей элемента x^{-1} равен $\mathfrak{p}$, степень дивизора $\mathfrak{p}$ равна 1, поэтому согласно теореме 4 § 8 гл. I имеем $[R : K\langle x^{-1}\rangle] = 1$, откуда $R = K\langle x^{-1}\rangle$.

Если поле K алгебраически замкнуто, то в R всегда существует точка степени 1 (в этом случае степень каждой точки равна 1). Однако, если K не является алгебраически замкнутым, то это условие не всегда выполняется. Например, пусть K — поле вещественных чисел; положим $R = K\langle x, y\rangle$, где элемент x трансцендентен над K и $x^2 + y^2 + 1 = 0$. Легко доказываются следующие факты: поле констант поля R равно K; степень каждой точки поля R равна 2; род поля R равен 0. Так как поле R не имеет точек степени 1, то оно не является чисто трансцендентным расширением K.

Впоследствии будет доказано, что поле рода 0 всегда имеет точку, степень которой равна либо 1, либо 2 (см. конец § 6 этой главы)[1]).

§ 3. Поля рода 1

Пусть R — поле алгебраических функций от одной переменной рода 1. Обозначим через K его поле констант и предположим, что в поле R существует по крайней мере одна точка $\mathfrak{p}$ степени 1 (это условие, разумеется, выполнено, если K алгебраически замкнуто). По теореме Римана имеем $l(\mathfrak{p}^{-2}) \geqslant d(\mathfrak{p}^2) = 2$, откуда следует, что существует элемент $x \in R$, не содержащийся в K, который $\equiv 0 \pmod{\mathfrak{p}^{-2}}$. Дивизор нулей элемента x^{-1} равен либо $\mathfrak{p}$, либо $\mathfrak{p}^2$, значит, его степень равна 1 или 2. Если бы степень дивизора нулей элемента x^{-1} была равна 1, то согласно теореме 4 § 8 гл. 1 мы имели бы $R = K\langle x^{-1}\rangle$, т. е. род поля R был бы равен 0, а не 1. Следовательно, дивизор нулей элемента x^{-1} равен $\mathfrak{p}^2$, откуда вытекает, что степень поля R относительно $K\langle x\rangle = K\langle x^{-1}\rangle$ равна 2.

Так как $l(\mathfrak{p}^{-3}) \geqslant d(\mathfrak{p}^3) = 3$, то существует элемент $y \in R$ такой, что $y \equiv 0 \pmod{\mathfrak{p}^{-3}}$ и элементы 1, x, y линейно независимы над K. Покажем, что дивизор полюсов элемента y равен $\mathfrak{p}^3$. Пусть t — униформизирующая переменная в точке $\mathfrak{p}$. Тогда $\nu_{\mathfrak{p}}(xt^2) = 0$ и элемент xt^2 в точке $\mathfrak{p}$ принимает значение $\alpha \neq 0$; так как степень точки $\mathfrak{p}$ равна 1, то $\alpha \in K$. Допустим, что дивизор полюсов элемента y равен $\mathfrak{p}$ или $\mathfrak{p}^2$; тогда $\nu_{\mathfrak{p}}(yt^2) \geqslant 0$ и элемент yt^2 в точке $\mathfrak{p}$ принимает некоторое конечное значение β. Элемент $(y - \alpha^{-1}\beta x)t^2$ в точке $\mathfrak{p}$ принимает значение 0, а значит $\nu_{\mathfrak{p}}(y - \alpha^{-1}\beta x) \geqslant -1$. Если $z = y - \alpha^{-1}\beta x$, то $z \equiv 0 \pmod{\mathfrak{p}^{-1}}$ и z не принадлежит K (ибо 1, x, y линейно независимы над K), поэтому дивизор полюсов элемента z равен $\mathfrak{p}$, откуда $[R : K\langle z\rangle] = 1$, и мы получили противоречие.

---

[1]) Каждое поле R алгебраических функций от одной переменной рода 0, не являющееся чисто трансцендентным расширением поля констант K (а значит, не имеющее точек степени 1), имеет вид $R = K\langle x, y\rangle$, где x трансцендентен над K, а y удовлетворяет соотношению $F(x, y) = 0$, где $F(X, Y)$ — многочлен второй степени из кольца $K[X, Y]$. Обратно, всякое поле алгебраических функций от одной переменной такого вида имеет род 0. (*Прим. перев.*)

Итак, дивизор полюсов элемента y равен $\mathfrak{p}^3$. Так как степень $\mathfrak{p}^3$ равна 3, то $[R:K\langle y\rangle]=3$. Отсюда следует, что y не принадлежит $K\langle x\rangle$, ибо в противном случае степень $[R:K\langle y\rangle]$ должна была бы делиться на $[R:K\langle x\rangle]$. Далее, поле R квадратично над $K\langle x\rangle$, поэтому $R=K\langle x, y\rangle$. Элемент y удовлетворяет уравнению вида

$$C(x)y^2+A(x)y+B(x)=0,$$

где A, B, C — многочлены с коэффициентами из K, причем можно предполагать, что они не имеют общих множителей. Так как y не принадлежит $K\langle x\rangle$, то B и C отличны от 0; более того, многочлен $C(x)Y^2+A(x)Y+B(x)$ от Y с коэффициентами из $K\langle x\rangle$ неприводим. Так как многочлены A, B, C не имеют общих множителей, то многочлен $C(X)Y^2+A(X)Y+B(X)$ от X и Y с коэффициентами из K неприводим в $K[X, Y]$. Отсюда следует, что многочлен $C(X)y^2+A(X)y+B(X)$ от X с коэффициентами из $K\langle y\rangle$ также неприводим. Но поле $K\langle x, y\rangle$ имеет степень 3 над $K\langle y\rangle$; следовательно, степени многочленов A, B, C не превосходят 3, причем хоть одна из этих степеней равна 3.

Если $M(X)=a_0X^m+a_1X^{m-1}+\ldots+a_m$ — произвольный многочлен степени m с коэффициентами из K, то элемент $M(x)$ мы можем записать в виде $M(x)=x^m(a_0+a_1x^{-1}+\ldots+a_mx^{-m})$, откуда следует, что $\nu_{\mathfrak{p}}(M(x))=-2m$ (ибо $\nu_{\mathfrak{p}}(x^{-1})=2$). Если $A\neq 0$, то число $\nu_{\mathfrak{p}}(A(x)y)=-3+\nu_{\mathfrak{p}}(A(x))$ нечетно, а значит, отлично от четного числа $\nu_{\mathfrak{p}}(B(x))$. Следовательно, мы имеем

$$\nu_{\mathfrak{p}}(-A(x)y-B(x))=\min\{\nu_{\mathfrak{p}}(A(x)y),\ \nu_{\mathfrak{p}}(B(x))\}$$

(см. § 3 гл. I). Так как $\nu_{\mathfrak{p}}(C(x)y^2)$ четно, то $\nu_{\mathfrak{p}}(C(x)y^2)=\nu_{\mathfrak{p}}(B(x))<\nu_{\mathfrak{p}}(A(x)y)$. Пусть β и γ — степени многочленов B и C соответственно; тогда $-2\gamma-6=-2\beta$, откуда $\beta=\gamma+3$. Но $\beta\leqslant 3$ и $\gamma\leqslant 3$, поэтому $\gamma=0$, $\beta=3$. Так как $\gamma=0$, то можно считать, что $C=1$. Если $A\neq 0$, то, обозначая через α степень многочлена A, имеем $-6<-2\alpha-3$, откуда $\alpha\leqslant 1$.

Предположим теперь, что характеристика поля R не равна 2. Полагая $y_1=y+\frac{A}{2}$, получим $y_1^2=B_1(x)$, где

степень многочлена $B_1 = \frac{A^2}{4} - B$ равна 3. Утверждаем, что уравнение $B_1(X) = 0$ не имеет кратных корней. Действительно, допуская, что $B_1 = B_2^2 B_3$, где B_2 и B_3 — многочлены степени 1 с коэффициентами из K, будем иметь $\left(\frac{y_1}{B_2(x)}\right)^2 = B_3(x)$. Так как степень B_3 равна 1, то элемент x будет содержаться в $K\left\langle\frac{y_1}{B_2(x)}\right\rangle$, а тогда элементы $y_1 = B_2(x) \cdot \frac{y_1}{B_2(x)}$ и $y = y_1 - \frac{A(x)}{2}$ также будут принадлежать последнему полю, т. е. получим, что $R = K\left\langle\frac{y_1}{B_2(x)}\right\rangle$, а это невозможно.

Обратно, пусть K — поле характеристики $\neq 2$ и пусть $R = K\langle x, y\rangle$, где x — трансцендентный элемент над K и $y^2 = B(x)$, при этом B — многочлен степени 3 с коэффициентами из K без кратных множителей. Можно доказать, что тогда род поля R равен 1. Доказательство этого факта мы опускаем.

§ 4. Распределения

Пусть R — поле алгебраических функций от одной переменной и K — его поле констант. В § 1 была сформулирована следующая проблема. Если для каждой точки $\mathfrak{p}$ поля R задан элемент $x_{\mathfrak{p}} \in R$ и задано целое число $m_{\mathfrak{p}}$, то при каком условии существует элемент $x \in R$ такой, что

$$\nu_{\mathfrak{p}}(x - x_{\mathfrak{p}}) \geqslant m_{\mathfrak{p}} \tag{1}$$

для всех точек $\mathfrak{p}$?

Для исследования этой проблемы представляется целесообразным ввести следующее понятие. Отображение $\mathfrak{x}$, которое каждой точке $\mathfrak{p}$ поля R сопоставляет элемент $\mathfrak{x}(\mathfrak{p})$ из R, будем называть *распределением* [1]), если неравенство $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p})) < 0$ имеет место только для конечного числа точек $\mathfrak{p}$.

Множество $\mathfrak{X}$ всех распределений является подмножеством множества $\mathfrak{X}_0$ всех отображений $\mathfrak{p} \to \mathfrak{x}_0(\mathfrak{p})$ множества всех

---

[1]) В подлиннике — repartition. В русской литературе иногда употребляется термин „мероморфная функция". (*Прим. перев.*)

точек S в поле R. Так как R — кольцо, то $\mathfrak{X}_0$ также является кольцом, в котором действия определены формулами

$$(\mathfrak{x}_0+\mathfrak{x}_0')(\mathfrak{p})=\mathfrak{x}_0(\mathfrak{p})+\mathfrak{x}_0'(\mathfrak{p}),$$
$$(\mathfrak{x}_0\mathfrak{x}_0')(\mathfrak{p})=\mathfrak{x}_0(\mathfrak{p})\mathfrak{x}_0'(\mathfrak{p})$$

(для всех точек $\mathfrak{p}$). Если $\mathfrak{x}$ и $\mathfrak{x}'$ — два распределения, то имеется только конечное число точек $\mathfrak{p}$, для которых хоть одно из чисел $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p}))$ и $\nu_{\mathfrak{p}}(\mathfrak{x}'(\mathfrak{p}))$ отрицательно. Отсюда сразу же следует, что $\mathfrak{x}-\mathfrak{x}'$ и $\mathfrak{x}\mathfrak{x}'$ также являются распределениями. Таким образом, множество распределений $\mathfrak{X}$ является подкольцом кольца $\mathfrak{X}_0$.

Каждому элементу $x\in R$ мы можем сопоставить распределение $\mathfrak{x}_x$, которое каждую точку $\mathfrak{p}$ отображает на элемент x. Ясно, что соответствие $x\to\mathfrak{x}_x$ является изоморфизмом поля R на подкольцо кольца распределений. В дальнейшем распределение $\mathfrak{x}_x$, соответствующее элементу x поля R, мы будем обозначать также через x[1]). Следует, однако, быть осторожным, чтобы не спутать значение элемента x в точке $\mathfrak{p}$ (которое является элементом поля вычетов точки $\mathfrak{p}$) со значением в точке $\mathfrak{p}$ распределения $\mathfrak{x}_x$ (которое равно элементу x). Чтобы устранить возможность недоразумений, мы условимся значение распределения $\mathfrak{x}$ в точке $\mathfrak{p}$ называть *$\mathfrak{p}$-компонентой* распределения $\mathfrak{x}$.

Единица поля R является также и единицей кольца $\mathfrak{X}$. Так как мы имеем изоморфное отображение R в $\mathfrak{X}$, то кольцо $\mathfrak{X}$ можно рассматривать как векторное пространство над полем R, а значит, и подавно, как векторное пространство над полем K (которое является подполем поля R). *В дальнейшем, говоря о векторном пространстве $\mathfrak{X}$, мы всегда будем подразумевать, что оно рассматривается как векторное пространство над полем K (а не над полем R!).*

Для распределения $\mathfrak{x}$ и точки $\mathfrak{p}$ поля R положим

$$\nu_{\mathfrak{p}}(\mathfrak{x})=\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p})).$$

Число $\nu_{\mathfrak{p}}(\mathfrak{x})$ называется *порядком распределения $\mathfrak{x}$ в точке $\mathfrak{p}$*. (Заметим, что в случае $\mathfrak{x}=x\in R$ символ $\nu_{\mathfrak{p}}(x)$ имеет здесь

---

[1]) В дальнейшем распределения такого вида будут называться главными распределениями. (*Прим перев.*)

то же значение, что и ранее.) Очевидно, что для распределений $\mathfrak{x}$ и $\mathfrak{y}$ имеем

$$\nu_{\mathfrak{p}}(\mathfrak{x} \pm \mathfrak{y}) \geqslant \min\{\nu_{\mathfrak{p}}(\mathfrak{x}),\ \nu_{\mathfrak{p}}(\mathfrak{y})\}; \quad \nu_{\mathfrak{p}}(\mathfrak{x}\mathfrak{y}) = \nu_{\mathfrak{p}}(\mathfrak{x}) + \nu_{\mathfrak{p}}(\mathfrak{y}).$$

Кроме того, если $\nu_{\mathfrak{p}}(\mathfrak{x}) < \nu_{\mathfrak{p}}(\mathfrak{y})$, то $\nu_{\mathfrak{p}}(\mathfrak{x} \pm \mathfrak{y}) = \nu_{\mathfrak{p}}(\mathfrak{x})$.

Пусть $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}$ — дивизор. Будем говорить, что распределения $\mathfrak{x}$ и $\mathfrak{y}$ сравнимы между собой по модулю $\mathfrak{a}$ и писать $\mathfrak{x} \equiv \mathfrak{y} \pmod{\mathfrak{a}}$, если для всех точек $\mathfrak{p}$ выполнены условия $\nu_{\mathfrak{p}}(\mathfrak{x} - \mathfrak{y}) \geqslant m_{\mathfrak{p}}$. Очевидно, что это определение находится в согласии с определением сравнений для элементов поля R (в случае, если $\mathfrak{x}$ и $\mathfrak{y}$ — главные распределения).

Вернемся теперь к проблеме о существовании элемента x, удовлетворяющего вышеуказанным условиям (1). При этом введем дополнительно два ограничения. Именно будем предполагать: 1) $\nu_{\mathfrak{p}}(x_{\mathfrak{p}}) \geqslant 0$ почти для всех [1]) $\mathfrak{p}$, т. е. отображение $\mathfrak{p} \to x_{\mathfrak{p}}$ является распределением $\mathfrak{x}$; 2) целые числа $m_{\mathfrak{p}}$ почти все равны нулю, т. е. символ $\prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}$ является дивизором $\mathfrak{a}$. При этих предположениях наша проблема может быть сформулирована следующим образом: существует ли элемент $x \in R$, который $\equiv \mathfrak{x} \pmod{\mathfrak{a}}$?

Обозначим через $\mathfrak{X}(\mathfrak{a})$ совокупность тех распределений, которые $\equiv 0 \pmod{\mathfrak{a}}$; очевидно, что $\mathfrak{X}(\mathfrak{a})$ является векторным подпространством пространства $\mathfrak{X}$. Тогда наша проблема сводится к следующему вопросу: существует ли элемент $x \in R$, который можно представить в виде $\mathfrak{x} + \mathfrak{y}$, где $\mathfrak{y} \in \mathfrak{X}(\mathfrak{a})$? Но если $x = \mathfrak{x} + \mathfrak{y}$, то $\mathfrak{x} = x - \mathfrak{y}$ принадлежит пространству $\mathfrak{X}(\mathfrak{a}) + R$, состоящему из сумм элементов из $\mathfrak{X}(\mathfrak{a})$ и R; обратно, если $\mathfrak{x}$ принадлежит пространству $\mathfrak{X}(\mathfrak{a}) + R$, то наша задача имеет решение. Докажем теперь, что *векторное пространство* $\mathfrak{X}/(\mathfrak{X}(\mathfrak{a}) + R)$ *имеет конечную размерность.*

Если $\mathfrak{a}'$ является делителем дивизора $\mathfrak{a}$, то $\mathfrak{X}(\mathfrak{a})$ содержится в $\mathfrak{X}(\mathfrak{a}')$. Далее, для любого распределения $\mathfrak{x} \in \mathfrak{X}$ всегда можно найти делитель $\mathfrak{a}'$ дивизора $\mathfrak{a}$ такой, что $\mathfrak{x} \in \mathfrak{X}(\mathfrak{a}')$. В самом деле, положим $\mu(\mathfrak{p}) = \min\{0,\ \nu_{\mathfrak{p}}(\mathfrak{x})\}$; тогда $\mu(\mathfrak{p}) = 0$ почти для всех $\mathfrak{p}$ (ибо $\nu_{\mathfrak{p}}(\mathfrak{x}) \geqslant 0$ почти для

---

[1]) Выражение „почти все“ означает: все, за исключением конечного числа. (*Прим. перев.*)

всех $\mathfrak{p}$). Обозначая через $\mathfrak{a}_1'$ дивизор $\prod_{\mathfrak{p}} \mathfrak{p}^{\mu(\mathfrak{p})}$, имеем $\mathfrak{x} \equiv 0 \pmod{\mathfrak{a}_1'}$. Пусть теперь $\mathfrak{a}'$ — общий наибольший делитель дивизоров $\mathfrak{a}$ и $\mathfrak{a}_1'$, тогда $\mathfrak{a}'$ является делителем дивизора $\mathfrak{a}$, и $\mathfrak{x}$ принадлежит $\mathfrak{X}(\mathfrak{a}')$. Таким образом, каждый элемент пространства $\mathfrak{X}/(\mathfrak{X}(\mathfrak{a})+R)$ содержится в пространстве $(\mathfrak{X}(\mathfrak{a}')+R)/(\mathfrak{X}(\mathfrak{a})+R)$ при некотором $\mathfrak{a}'$. Мы сейчас докажем, что пространство $(\mathfrak{X}(\mathfrak{a}')+R)/(\mathfrak{X}(\mathfrak{a})+R)$ имеет конечную размерность и что эта размерность не превосходит некоторого числа, зависящего только от дивизора $\mathfrak{a}$.

Лемма 1. Если $\mathfrak{a}'$ является делителем дивизора $\mathfrak{a}$, то размерность пространства $\mathfrak{X}(\mathfrak{a}')/\mathfrak{X}(\mathfrak{a})$ конечна и равна $d(\mathfrak{a})-d(\mathfrak{a}')$.

Пусть S_0 обозначает конечное множество точек, содержащее все точки, которые входят в $\mathfrak{a}$ или в $\mathfrak{a}'$ с показателями $\neq 0$. Каждому элементу u из пространства $\mathfrak{K}(\mathfrak{a}', S_0)$ (см. § 7 гл. I) поставим в соответствие распределение $\mathfrak{z}_u$, для которого $\mathfrak{z}_u(\mathfrak{p})=u$, если $\mathfrak{p}\in S_0$, и $\mathfrak{z}_u(\mathfrak{p})=0$, если $\mathfrak{p}\notin S_0$. Очевидно, что $\mathfrak{z}_u$ принадлежит пространству $\mathfrak{X}(\mathfrak{a}')$ и что отображение $u\to\mathfrak{z}_u$ пространства $\mathfrak{K}(\mathfrak{a}', S_0)$ в $\mathfrak{X}(\mathfrak{a}')$ линейно. Если u принадлежит $\mathfrak{K}(\mathfrak{a}, S_0)$, то $\mathfrak{z}_u$ принадлежит $\mathfrak{X}(\mathfrak{a})$, и обратно. Следовательно, отображение $u\to\mathfrak{z}_u$ определяет изоморфное линейное отображение $\mathfrak{K}(\mathfrak{a}', S_0)/\mathfrak{K}(\mathfrak{a}, S_0)$ в $\mathfrak{X}(\mathfrak{a}')/\mathfrak{X}(\mathfrak{a})$. Утверждаем, что последнее отображение является отображением „на". Действительно, пусть $\mathfrak{z}$ — произвольный элемент из $\mathfrak{X}(\mathfrak{a}')$. Для $\mathfrak{p}\in S_0$ через $m_{\mathfrak{p}}$ обозначим показатель, с которым точка $\mathfrak{p}$ входит в $\mathfrak{a}$. Согласно теореме 3 § 6 гл. I в поле R существует такой элемент u, что $\nu_{\mathfrak{p}}(u-\mathfrak{z}(\mathfrak{p}))\geqslant m_{\mathfrak{p}}$ для всех точек $\mathfrak{p}\in S_0$. Пусть $m_{\mathfrak{p}}'$ обозначает показатель, с которым $\mathfrak{p}$ входит в $\mathfrak{a}'$; тогда $\nu_{\mathfrak{p}}(\mathfrak{z}(\mathfrak{p}))\geqslant m_{\mathfrak{p}}'$ (ибо $\mathfrak{z}$ принадлежит $\mathfrak{X}(\mathfrak{a}')$) и $m_{\mathfrak{p}}\geqslant m_{\mathfrak{p}}'$ (ибо $\mathfrak{a}$ делится на $\mathfrak{a}'$). Так как $u=(u-\mathfrak{z}(\mathfrak{p}))+\mathfrak{z}(\mathfrak{p})$, то $\nu_{\mathfrak{p}}(u)\geqslant m_{\mathfrak{p}}'$ при $\mathfrak{p}\in S_0$, т. е. u принадлежит $\mathfrak{K}(\mathfrak{a}', S_0)$. Если $\mathfrak{p}\in S_0$, то $\mathfrak{z}_u(\mathfrak{p})=u$, поэтому $\nu_{\mathfrak{p}}(\mathfrak{z}_u(\mathfrak{p})-\mathfrak{z}(\mathfrak{p}))\geqslant m_{\mathfrak{p}}$. Если точка $\mathfrak{q}$ не принадлежит S_0, то $\mathfrak{z}_u(\mathfrak{q})=0$, а значит $\nu_{\mathfrak{q}}(\mathfrak{z}_u(\mathfrak{q})-\mathfrak{z}(\mathfrak{q}))=\nu_{\mathfrak{q}}(\mathfrak{z}(\mathfrak{q}))\geqslant 0$ (в силу того, что $\mathfrak{z}\in\mathfrak{X}(\mathfrak{a}')$). Но все точки $\mathfrak{q}$, не принадлежащие S_0, входят в $\mathfrak{a}$ с показателем 0, поэтому $\mathfrak{z}_u\equiv\mathfrak{z}\pmod{\mathfrak{a}}$. Этим и доказано, что наше отобра-

жение пространства $\mathfrak{K}(\mathfrak{a}', S_0)/\mathfrak{K}(\mathfrak{a}, S_0)$ в $\mathfrak{X}(\mathfrak{a}')/\mathfrak{X}(\mathfrak{a})$ является отображением „на". Лемма 1 следует теперь из леммы 1 § 7 гл. I.

Займемся оценкой размерности пространства $(\mathfrak{X}(\mathfrak{a}')+R)/(\mathfrak{X}(\mathfrak{a})+R)$. Согласно теореме об изоморфизме, рассматриваемое векторное пространство изоморфно пространству $\mathfrak{X}(\mathfrak{a}')/(\mathfrak{X}(\mathfrak{a}')\cap(\mathfrak{X}(\mathfrak{a})+R))$. Если для элемента u из R мы имеем $u+\mathfrak{X}(\mathfrak{a})\subset\mathfrak{X}(\mathfrak{a}')$, то, очевидно, u принадлежит $\mathfrak{X}(\mathfrak{a}')$, т. е. $u\equiv 0 \pmod{\mathfrak{a}'}$. Множество таких элементов в § 1 было обозначено через $\mathfrak{L}(\mathfrak{a}')$; таким образом, $\mathfrak{X}(\mathfrak{a}')\cap(\mathfrak{X}(\mathfrak{a})+R)=\mathfrak{X}(\mathfrak{a})+\mathfrak{L}(\mathfrak{a}')$. Используя опять теорему об изоморфизме, получаем, что пространство $(\mathfrak{X}(\mathfrak{a})+\mathfrak{L}(\mathfrak{a}'))/\mathfrak{X}(\mathfrak{a})$ изоморфно пространству $\mathfrak{L}(\mathfrak{a}')/(\mathfrak{L}(\mathfrak{a}')\cap\mathfrak{X}(\mathfrak{a}))$. Пересечение $\mathfrak{L}(\mathfrak{a}')\cap\mathfrak{X}(\mathfrak{a})$ совпадает, очевидно, с $\mathfrak{L}(\mathfrak{a})$. Как мы уже доказали (см. § 1), пространство $\mathfrak{L}(\mathfrak{a})$ имеет конечную размерность $l(\mathfrak{a})$; поэтому $\mathfrak{L}(\mathfrak{a}')/\mathfrak{L}(\mathfrak{a})$ имеет размерность $l(\mathfrak{a}')-l(\mathfrak{a})$. Применяя теперь лемму 1, получаем, что размерность пространства $(\mathfrak{X}(\mathfrak{a}')+R)/(\mathfrak{X}(\mathfrak{a})+R)$ равна

$$(d(\mathfrak{a})-d(\mathfrak{a}'))-(l(\mathfrak{a}')-l(\mathfrak{a}))=$$
$$=(d(\mathfrak{a})+l(\mathfrak{a}))-(d(\mathfrak{a}')+l(\mathfrak{a}')).$$

Сумма $d(\mathfrak{a})+l(\mathfrak{a})$ зависит только от $\mathfrak{a}$; сумма $d(\mathfrak{a}')+l(\mathfrak{a}')$ всегда $\geqslant -g+1$, где g — род поля R (теорема 1 § 1). Отсюда следует, что пространство $(\mathfrak{X}(\mathfrak{a}')+R)/(\mathfrak{X}(\mathfrak{a})+R)$ имеет размерность $\leqslant d(\mathfrak{a})+l(\mathfrak{a})+g-1$, причем эта граница зависит только от $\mathfrak{a}$. Положим

$$\lambda(\mathfrak{a})=d(\mathfrak{a})+l(\mathfrak{a})+g-1.$$

Теперь уже легко доказывается, что размерность пространства $\mathfrak{X}/(\mathfrak{X}(\mathfrak{a})+R)$ конечна и не превосходит $\lambda(\mathfrak{a})$. Допустим противное, т. е. допустим, что в $\mathfrak{X}$ существуют элементы $\xi_1, \ldots, \xi_k$, линейно независимые по модулю $\mathfrak{X}(\mathfrak{a})+R$, причем число этих элементов k больше $\lambda(\mathfrak{a})$. Для каждого i $(1\leqslant i\leqslant k)$ мы можем найти такой дивизор $\mathfrak{a}_i'$, что $\mathfrak{a}$ делится на $\mathfrak{a}_i'$ и $\xi_i\in\mathfrak{X}(\mathfrak{a}_i')$. Если дивизор $\mathfrak{a}'$ является делителем всех дивизоров $\mathfrak{a}_1', \ldots, \mathfrak{a}_k'$, то все элементы ξ_i будут принадлежать $\mathfrak{X}(\mathfrak{a}')$, а это невозможно.

Оказывается, что в действительности размерность пространства $\mathfrak{X}/(\mathfrak{X}(\mathfrak{a})+R)$ равна $\lambda(\mathfrak{a})$. В самом деле, как нам

уже известно, существует дивизор $\mathfrak{a}_0$, для которого $l(\mathfrak{a}_0)+$ $+d(\mathfrak{a}_0)=-g+1$, при этом для любого дивизора $\mathfrak{a}'$, являющегося делителем $\mathfrak{a}_0$, имеем также $l(\mathfrak{a}')+d(\mathfrak{a}')=$ $=-g+1$ (теорема 1 § 1). Следовательно, для общего наибольшего делителя $\mathfrak{a}'$ дивизоров $\mathfrak{a}_0$ и $\mathfrak{a}$ размерность пространства $(\mathfrak{X}(\mathfrak{a}')+R)/(\mathfrak{X}(\mathfrak{a})+R)$ равна $\lambda(\mathfrak{a})$, и наше утверждение доказано. Таким образом, имеет место

Лемма 2. *Пусть для дивизора $\mathfrak{a}$ через $\mathfrak{X}(\mathfrak{a})$ обозначено пространство тех распределений, которые $\equiv 0 \pmod{\mathfrak{a}}$. Если $\mathfrak{X}$ есть пространство всех распределений, то размерность пространства $\mathfrak{X}/(\mathfrak{X}(\mathfrak{a})+R)$ равна $\lambda(\mathfrak{a})=l(\mathfrak{a})+$ $+d(\mathfrak{a})+g-1$, где g — род поля R, а $l(\mathfrak{a})$ — размерность пространства $\mathfrak{L}(\mathfrak{a})$, состоящего из тех элементов поля R, которые $\equiv 0 \pmod{\mathfrak{a}}$.*

Вернемся теперь к проблеме, сформулированной в начале этой главы. Как было установлено выше, эта проблема эквивалентна следующему вопросу: при каком условии данное распределение $\mathfrak{x}$ принадлежит пространству $\mathfrak{X}(\mathfrak{a})+R$? Пусть $\bar{\mathfrak{x}}$ обозначает класс смежности распределения $\mathfrak{x}$ по модулю $\mathfrak{X}(\mathfrak{a})+R$. Так как $\mathfrak{X}/(\mathfrak{X}(\mathfrak{a})+R)$ является векторным пространством, то равенство $\bar{\mathfrak{x}}=0$ имеет место тогда и только тогда, если $\bar{\omega}(\bar{\mathfrak{x}})=0$ для всякой линейной функции $\bar{\omega}$ на пространстве $\mathfrak{X}/(\mathfrak{X}(\mathfrak{a})+R)$, т. е. если $\omega(\mathfrak{x})=0$ для всякой линейной функции ω на $\mathfrak{X}$, аннулирующей подпространство $\mathfrak{X}(\mathfrak{a})+R$. Таким образом, условие $\mathfrak{x}\in(\mathfrak{X}(\mathfrak{a})+R)$ может быть выражено в виде системы $\lambda(\mathfrak{a})$ линейно независимых линейных соотношений.

Чтобы полученному результату придать более совершенную форму, нам необходимо подробнее изучить введенные выше линейные функции ω. В следующем параграфе будет выяснена природа этих функций в случае когда $R=K\langle x\rangle$, где K — поле комплексных чисел.

§ 5. Дифференциалы

Рассмотрим поле рациональных функций $R=K\langle x\rangle$ от x с коэффициентами из поля комплексных чисел K.

Для произвольного элемента u из R символ $u\,dx$ можно рассматривать как составную часть интеграла: если γ — некоторый путь, не проходящий через полюса функции u, то

выражение $\int\limits_{\gamma} u dx$ имеет вполне определенный смысл. Будем говорить, что $u dx$ является дифференциалом поля R.

Для произвольного комплексного числа a через $\mathfrak{p}(a)$ обозначим точку, в которой x принимает значение a. Число $\nu_{\mathfrak{p}(a)}(u)$ будем называть порядком дифференциала $u dx$ в точке $\mathfrak{p}(a)$. Обозначим через $\mathfrak{p}(\infty)$ единственный полюс элемента x. Если функцию u рассматривать как рациональную функцию от $x' = \frac{1}{x}$, то выражение $u dx$ (рассматриваемое как составная часть интеграла) принимает вид $-\frac{u}{x'^2} dx'$. Поэтому естественно число $\nu_{\mathfrak{p}(\infty)}(u) - 2$ назвать порядком дифференциала $u dx$ в точке $\mathfrak{p}(\infty)$.

Пусть a — некоторое комплексное число. Если γ есть простая замкнутая кривая, которая содержит внутри себя a, но не содержит никаких полюсов функции u кроме, быть может, самого числа a, то число

$$\frac{1}{2\pi i} \int\limits_{\gamma} u dx$$

называется вычетом дифференциала $u dx$ в точке $\mathfrak{p}(a)$. Ясно, что этот вычет равен 0, если $\mathfrak{p}(a)$ не является полюсом функции u. Вычет дифференциала $u dx$ в точке $\mathfrak{p}(\infty)$ по определению равен

$$\frac{1}{2\pi i} \int\limits_{\Gamma} u dx,$$

где Γ — простая замкнутая кривая [1]), которая содержит внутри себя все полюса функции u, расположенные на конечном расстоянии. Пусть $a_1, \ldots, a_h$ — все эти полюса. Для каждого k выберем простую замкнутую кривую γ_k, расположенную во внутренности кривой Γ и содержащую внутри себя a_k,

---

[1]) Здесь предполагается, что кривая Γ проходится в отрицательном направлении (внешность Γ остается слева). В предыдущем интеграле кривая γ приходилась в положительном направлении (внутренность γ оставалась слева). (*Прим. перев.*)

но не содержащую a_j при $j \neq k$. Согласно интегральной теореме Коши имеем

$$\int_{\Gamma} u dx + \sum_{k=1}^{h} \int_{\gamma_k} u dx = 0,$$

откуда следует, что *сумма всех вычетов дифференциала равна* 0.

Пусть $\mathfrak{x}$ — любое распределение поля R. Для произвольной точки $\mathfrak{p}$ поля R положим

$$\omega^{\mathfrak{p}}(\mathfrak{x}) = \text{Выч. } \mathfrak{x}(\mathfrak{p})\, u dx \text{ в точке } \mathfrak{p}. \tag{1}$$

Ясно, что почти для всех $\mathfrak{p}$ имеем $\omega^{\mathfrak{p}}(\mathfrak{x}) = 0$. Положим

$$\omega(\mathfrak{x}) = \sum \omega^{\mathfrak{p}}(\mathfrak{x}),$$

где суммирование ведется по всем точкам $\mathfrak{p}$. Функция ω, определенная последней формулой, является линейной функцией на пространстве $\mathfrak{X}$ всех распределений. Если $\mathfrak{x} = x_1 \in R$, то $\omega(\mathfrak{x})$ равно сумме вычетов дифференциала $x_1 u dx$, поэтому $\omega(\mathfrak{x}) = 0$, т. е. ω аннулирует подпространство R пространства $\mathfrak{X}$.

Пусть $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$ — дивизор. Будем говорить, что $u dx \equiv 0 \pmod{\mathfrak{a}}$, если в каждой точке $\mathfrak{p}$ дифференциал $u dx$ имеет порядок $\geqslant m(\mathfrak{p})$. Пусть $\mathfrak{X}(\mathfrak{a}^{-1})$ есть пространство, состоящее из тех распределений, которые $\equiv 0 \pmod{\mathfrak{a}^{-1}}$. Если $\mathfrak{x} \in \mathfrak{X}(\mathfrak{a}^{-1})$, то для любой точки $\mathfrak{p}$ имеем $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p})) \geqslant -m(\mathfrak{p})$. Если $u dx \equiv 0 \pmod{\mathfrak{a}}$, то дифференциал $\mathfrak{x}(\mathfrak{p})\, u dx$ в точке $\mathfrak{p}$ имеет порядок $\geqslant 0$ (ибо $u dx$ в точке $\mathfrak{p}$ имеет порядок $\geqslant m(\mathfrak{p})$), откуда следует, что $\omega^{\mathfrak{p}}(\mathfrak{x}) = 0$. Таким образом, функция ω аннулирует пространство $\mathfrak{X}(\mathfrak{a}^{-1}) + R$.

Заменяя $\mathfrak{a}$ на $\mathfrak{a}^{-1}$, получаем, что каждый дифференциал $u dx$, который $\equiv 0 \pmod{\mathfrak{a}^{-1}}$, порождает на пространстве распределений линейную функцию ω, аннулирующую подпространство $\mathfrak{X}(\mathfrak{a}) + R$. К рассмотрению точно таких же функций мы подошли в конце предыдущего параграфа.

Подсчитаем теперь сколько имеется линейно независимых (над полем K) дифференциалов $u dx$, которые $\equiv 0 \pmod{\mathfrak{a}^{-1}}$. Для того чтобы $u dx \equiv 0 \pmod{\mathfrak{a}^{-1}}$, где $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$, прежде всего необходимо, чтобы $\nu_{\mathfrak{p}(a)}(u) \geqslant -m(\mathfrak{p}(a))$ для каждого

комплексного числа a. Положим $h=\prod_a (x-a)^{m(\mathfrak{p}(a))}$, тогда $\nu_{\mathfrak{p}(a)}(hu)\geqslant 0$ для каждого $a\in K$, т. е. функция $hu=f$ должна быть многочленом от x. С другой стороны, мы должны иметь $\nu_{\mathfrak{p}(\infty)}(u)-2\geqslant -m(\mathfrak{p}(\infty))$, т. е. $\nu_{\mathfrak{p}(\infty)}(f)\geqslant 2-m(\mathfrak{p}(\infty))+\nu_{\mathfrak{p}(\infty)}(h)$. Число $\nu_{\mathfrak{p}(\infty)}(h)$ равно $-\sum_a m(\mathfrak{p}(\mathfrak{a}))$, а $-m(\mathfrak{p}(\infty))-\sum_a m(\mathfrak{p}(\mathfrak{a}))$ равно $-d(\mathfrak{a})$. Таким образом, мы получили условие $\nu_{\mathfrak{p}(\infty)}(f)\geqslant 2-d(\mathfrak{a})$. Если $d(\mathfrak{a})<2$, то необходимо $f=0$. Если же $d(\mathfrak{a})\geqslant 2$, то f может быть произвольным многочленом степени $\leqslant d(\mathfrak{a})-2$; в этом случае, очевидно, имеем точно $d(\mathfrak{a})-1$ линейно независимых дифференциалов, которые $\equiv 0 \pmod{\mathfrak{a}^{-1}}$.

Утверждаем теперь, что при $u\neq 0$ функция ω, соответствующая дифференциалу $u\,dx$, отлична от 0. В самом деле, пусть число a не является ни нулем, ни полюсом функции u, и пусть $\mathfrak{x}$ есть распределение, определенное равенствами: $\mathfrak{x}(\mathfrak{p}(a))=(x-a)^{-1}$, $\mathfrak{x}(\mathfrak{p})=0$ при $\mathfrak{p}\neq\mathfrak{p}(a)$. Тогда $\omega^{\mathfrak{p}(a)}(\mathfrak{x})=u(a)\neq 0$ и $\omega^{\mathfrak{p}}(\mathfrak{x})=0$ при $\mathfrak{p}\neq\mathfrak{p}(a)$, поэтому $\omega(\mathfrak{x})=u(a)\neq 0$. Таким образом, получаем, что дифференциалы $u\,dx$, которые $\equiv 0 \pmod{\mathfrak{a}^{-1}}$, порождают ровно $\max\{0, d(\mathfrak{a})-1\}$ линейно независимых линейных функций на пространстве распределений $\mathfrak{X}$, аннулирующих подпространство $\mathfrak{X}(\mathfrak{a})+R$. С другой стороны, так как род поля R равен 0, то максимальное число таких линейных функций равно $\lambda(\mathfrak{a})=d(\mathfrak{a})+l(\mathfrak{a})-1$ (см. § 4). Займемся вычислением $l(\mathfrak{a})$. В проведенных выше рассуждениях функции u были подчинены условию $u\equiv 0 \pmod{\mathfrak{a}^{-1}(\mathfrak{p}(\infty))^2}$, поэтому имеем $l(\mathfrak{a}^{-1}(\mathfrak{p}(\infty))^2)=\max\{0, d(\mathfrak{a})-1\}$. Так как последнее равенство справедливо при любом дивизоре $\mathfrak{a}$, то $l(\mathfrak{a})=\max\{0, d(\mathfrak{a}^{-1})+1\}$, откуда $d(\mathfrak{a})+l(\mathfrak{a})-1=\max\{d(\mathfrak{a})-1, 0\}$. Этим доказано, что *каждая линейная функция на пространстве распределений, аннулирующая подпространство $\mathfrak{X}(\mathfrak{a})+R$, порождается некоторым дифференциалом $u\,dx$, сравнимым с 0 по модулю $\mathfrak{a}^{-1}$.*

Принимая во внимание последний результат, естественно сделать следующее определение. Пусть R — произвольное поле алгебраических функций от одной переменной, K — его поле констант и $\mathfrak{X}$ — пространство распределений. Под *дифференциалом* поля R будем понимать линейную

функцию ω на пространстве $\mathfrak{X}$, для которой существует дивизор $\mathfrak{a}$ такой, что на подпространстве $\mathfrak{X}(\mathfrak{a}^{-1})+R$ функция ω равна тождественно нулю ($\mathfrak{X}(\mathfrak{a}^{-1})$ обозначает пространство распределений, сравнимых с 0 по модулю $\mathfrak{a}^{-1}$). Для любого дивизора $\mathfrak{a}$, обладающего указанным свойством, будем говорить, что ω *делится на* $\mathfrak{a}$, и писать $\omega \equiv 0 \pmod{\mathfrak{a}}$.

Если дивизор $\mathfrak{a}'$ является делителем $\mathfrak{a}$, то всякий дифференциал, делящийся на $\mathfrak{a}$, будет делиться также и на $\mathfrak{a}'$. Если ω и ω' — дифференциалы, а λ и λ' — элементы из K, то $\lambda\omega+\lambda'\omega'$ также является дифференциалом; если ω делится на $\mathfrak{a}$, а ω' делится на $\mathfrak{a}'$, то $\lambda\omega+\lambda'\omega'$ делится на общий наибольший делитель дивизоров $\mathfrak{a}$ и $\mathfrak{a}'$. Дифференциалы поля R образуют, очевидно, векторное пространство над K; дифференциалы, делящиеся на заданный дивизор $\mathfrak{a}$, образуют подпространство в пространстве всех дифференциалов.

Результат, полученный нами в § 4, можно теперь сформулировать следующим образом.

Теорема 2. *Пусть R — поле алгебраических функций от одной переменной, $\mathfrak{a}$ — дивизор поля R и $\mathfrak{x}$ — распределение в R. Для того чтобы в поле R существовал элемент x такой, что $x \equiv \mathfrak{x} \pmod{\mathfrak{a}}$, необходимо и достаточно, чтобы $\omega(\mathfrak{x})=0$ для каждого дифференциала ω, делящегося на $\mathfrak{a}^{-1}$.*

В дальнейшем через $\delta(\mathfrak{a})$ мы будем обозначать размерность пространства тех дифференциалов, которые $\equiv 0 \pmod{\mathfrak{a}}$. Из результатов § 4 следует, что $\delta(\mathfrak{a})=l(\mathfrak{a}^{-1})+d(\mathfrak{a}^{-1})+g-1$, где g — род поля. Таким образом, нами доказана

Теорема 3 (теорема Римана — Роха). *Пусть R есть поле алгебраических функций от одной переменной рода g и пусть $\mathfrak{a}$ — дивизор поля R. Обозначим через $l(\mathfrak{a})$ размерность пространства тех элементов поля R, которые $\equiv 0 \pmod{\mathfrak{a}}$, а через $\delta(\mathfrak{a}^{-1})$ — размерность пространства дифференциалов, делящихся на $\mathfrak{a}^{-1}$. Тогда имеет место равенство*

$$l(\mathfrak{a})=d(\mathfrak{a}^{-1})-g+1+\delta(\mathfrak{a}^{-1}).$$

Дифференциал ω, делящийся на единичный дивизор $\mathfrak{e}$, называется *дифференциалом первого рода*[1]. Так как $l(\mathfrak{e})=1$, $d(\mathfrak{e})=0$, то имеет место

---

[1]) Часто дифференциалы первого рода называют также целыми дифференциалами. (*Прим. перев.*)

Теорема 4. *Размерность пространства дифференциалов первого рода поля алгебраических функций от одной переменной равна роду этого поля.*

§ 6. Канонический класс

Пусть R — поле алгебраических функций от одной переменной с полем констант K. Обозначим через ω некоторый дифференциал поля R, а через $\mathfrak{X}$ — пространство распределений. Для каждого элемента $x \neq 0$ из поля R отображение $\mathfrak{x} \to \omega(x\mathfrak{x})$ является линейным отображением $\mathfrak{X}$ в K, при котором все элементы из R отображаются в 0. Если $\mathfrak{a}$ есть дивизор, для которого $\omega \equiv 0 \pmod{\mathfrak{a}}$, то $\omega(x\mathfrak{x}) = 0$, если только $x\mathfrak{x} \equiv 0 \pmod{\mathfrak{a}^{-1}}$, что равносильно условию $\mathfrak{x} \equiv 0 \pmod{\mathfrak{a}^{-1}(\mathfrak{d}(x))^{-1}}$. Отсюда следует, что наше отображение является дифференциалом, делящимся на $\mathfrak{a}\mathfrak{d}(x)$. Этот дифференциал мы будем обозначать через $x\omega$. Если $x = 0$, то $0 \cdot \omega$ будет обозначать, конечно, нулевой дифференциал. Очевидно, имеют место следующие равенства:

$$(x + x')\omega = x\omega + x'\omega; \quad x(\omega + \omega') = x\omega + x\omega';$$
$$(xx')\omega = x(x'\omega); \quad 1 \cdot \omega = \omega,$$

где x, x' — элементы из R, а ω, ω' — дифференциалы поля R.

Теорема 5. *Если ω есть отличный от 0 дифференциал поля R алгебраических функций от одной переменной, то всякий другой дифференциал поля R имеет вид $x\omega$, где $x \in R$.*

Пусть ω' — произвольный дифференциал поля R; $\mathfrak{a}$ и $\mathfrak{a}'$ — дивизоры, удовлетворяющие условиям $\omega \equiv 0 \pmod{\mathfrak{a}}$ и $\omega' \equiv 0 \pmod{\mathfrak{a}'}$. Обозначим через g род поля R и выберем целый дивизор $\mathfrak{b}$, степень которого удовлетворяет неравенствам: $d(\mathfrak{b}) > g - 1 - d(\mathfrak{a})$, $d(\mathfrak{b}) > g - 1 - d(\mathfrak{a}')$, $d(\mathfrak{b}) > 3g - 2 - d(\mathfrak{a}') - d(\mathfrak{a}')$ (можно взять $\mathfrak{b} = \mathfrak{p}^m$, где $\mathfrak{p}$ — точка, а m достаточно велико). Если мы положим $a = l(\mathfrak{a}^{-1}\mathfrak{b}^{-1})$ и $a' = l(\mathfrak{a}'^{-1}\mathfrak{b}^{-1})$, то по теореме Римана будем иметь $a \geqslant d(\mathfrak{a}\mathfrak{b}) - g + 1 > 0$ и аналогично $a' > 0$. Пусть $x_1, \ldots, x_a$ — линейно независимые элементы из R, которые $\equiv 0 \pmod{\mathfrak{a}^{-1}\mathfrak{b}^{-1}}$, а $x'_1, \ldots, x'_{a'}$ — линейно независимые элементы из R, которые $\equiv 0 \pmod{\mathfrak{a}'^{-1}\mathfrak{b}^{-1}}$. Тогда дифференциалы $x_i\omega$, $x'_j\omega'$ $(1 \leqslant i \leqslant a,\ 1 \leqslant j \leqslant a')$ все $\equiv 0 \pmod{\mathfrak{b}^{-1}}$. Так

как по теореме Римана — Роха $\delta(\mathfrak{b}^{-1}) = l(\mathfrak{b}) + d(\mathfrak{b}) + g - 1$, и $l(\mathfrak{b}) \leqslant 1$ (ибо $\mathfrak{b}$ — целый), то $\delta(\mathfrak{b}^{-1}) \leqslant d(\mathfrak{b}) + g$. С другой стороны, мы имеем $a + a' \geqslant d(\mathfrak{a}) + d(\mathfrak{a}') + 2d(\mathfrak{b}) - 2g + 2$. Но по предположению $d(\mathfrak{b}) > 3g - 2 - d(\mathfrak{a}) - d(\mathfrak{a}')$, поэтому $a + a' > \delta(\mathfrak{b}^{-1})$. Отсюда следует, что дифференциалы $x_i\omega$ и $x'_j\omega'$ линейно зависимы. Значит, существует зависимость вида

$$\left(\sum_{i=1}^{a} \lambda_i x_i\right)\omega + \left(\sum_{j=1}^{a'} \lambda'_j x'_j\right)\omega' = 0,$$

где $\lambda_1, \ldots, \lambda_a, \lambda'_1, \ldots, \lambda'_{a'}$ — элементы из поля констант K, причем не все они равны нулю. Положим $y = \sum_{i=1}^{a} \lambda_i x_i$ и $y' = \sum_{j=1}^{a'} \lambda'_j x'_j$; тогда $y\omega + y'\omega' = 0$, причем элементы y и y' не равны нулю одновременно. Если бы $y' = 0$, то мы имели бы $y \neq 0$ и $y\omega = 0$, что невозможно, так как $\omega = y^{-1}y\omega \neq 0$. Так как $y' \neq 0$, то $\omega' = \frac{y}{y'}\omega$, и теорема 5 доказана.

Пусть ω — произвольный отличный от нуля дифференциал поля R. Докажем, что если $\omega \equiv 0 \pmod{\mathfrak{a}}$, то степень дивизора $\mathfrak{a}$ не превосходит $2g - 2$, где g — род поля R. Если $x_1, \ldots, x_h$ — линейно независимые элементы из R, которые $\equiv 0 \pmod{\mathfrak{a}^{-1}}$, то $x_1\omega, \ldots, x_h\omega$ являются линейно независимыми дифференциалами первого рода, а значит, по теореме 4, $h \leqslant g$. Таким образом, имеем $l(\mathfrak{a}^{-1}) \leqslant g$. С другой стороны, $l(\mathfrak{a}^{-1}) = d(\mathfrak{a}) - g + 1 + \delta(\mathfrak{a})$ и $\delta(\mathfrak{a}) \geqslant 1$, ибо $\omega \equiv 0 \pmod{\mathfrak{a}}$. Следовательно, $d(\mathfrak{a}) \leqslant l(\mathfrak{a}^{-1}) + g - 2 \leqslant 2g - 2$, и наше утверждение доказано.

Пусть теперь дифференциал ω делится на два дивизора $\mathfrak{a}$ и $\mathfrak{a}'$. Оказывается, что тогда ω будет делиться и на общее наименьшее кратное $\mathfrak{b}$ дивизоров $\mathfrak{a}$ и $\mathfrak{a}'$. Для доказательства этого, достаточно показать, что $\mathfrak{X}(\mathfrak{b}^{-1}) \subset \mathfrak{X}(\mathfrak{a}^{-1}) + \mathfrak{X}(\mathfrak{a}'^{-1})$. Пусть $m_{\mathfrak{p}}$ и $m'_{\mathfrak{p}}$ — показатели, с которыми произвольная точка $\mathfrak{p}$ входит в $\mathfrak{a}$ и $\mathfrak{a}'$ соответственно; тогда в дивизор $\mathfrak{b}$ точка $\mathfrak{p}$ входит с показателем $n_{\mathfrak{p}} = \max\{m_{\mathfrak{p}}, m'_{\mathfrak{p}}\}$. Для любого распределения $\mathfrak{x}$ из $\mathfrak{X}(\mathfrak{b}^{-1})$ положим $\mathfrak{y}(\mathfrak{p}) = \mathfrak{x}(\mathfrak{p})$, если $n_{\mathfrak{p}} = m_{\mathfrak{p}}$, и $\mathfrak{y}(\mathfrak{p}) = 0$, если $n_{\mathfrak{p}} = m'_{\mathfrak{p}} > m_{\mathfrak{p}}$; пусть, далее, $\mathfrak{y}'(\mathfrak{p}) =$

$=\mathfrak{x}(\mathfrak{p})-\mathfrak{y}(\mathfrak{p})$. Легко видеть, что отображения $\mathfrak{p}\to\mathfrak{y}(\mathfrak{p})$ и $\mathfrak{p}\to\mathfrak{y}'(\mathfrak{p})$ являются распределениями $\mathfrak{y}$ и $\mathfrak{y}'$, причем $\mathfrak{x}=\mathfrak{y}+\mathfrak{y}'$, $\mathfrak{y}$ принадлежит $\mathfrak{X}(\mathfrak{a}^{-1})$ и $\mathfrak{y}'$ принадлежит $\mathfrak{X}(\mathfrak{a}'^{-1})$.

В силу ранее доказанного среди всех дивизоров $\mathfrak{a}$, для которых $\omega\equiv 0 \pmod{\mathfrak{a}}$, мы можем выбрать дивизор, скажем $\mathfrak{a}_0$, с наибольшей возможной степенью. Если $\mathfrak{a}$ есть произвольный дивизор, для которого $\omega\equiv 0 \pmod{\mathfrak{a}}$, то ω делится также на общее наименьшее кратное дивизоров $\mathfrak{a}$ и $\mathfrak{a}_0$. Так как степень этого общего наименьшего кратного не может быть больше степени $\mathfrak{a}_0$, то оно должно совпадать с $\mathfrak{a}_0$. Таким образом, каждому дифференциалу $\omega\neq 0$ мы можем сопоставить дивизор $\mathfrak{d}(\omega)$ такой, что ω делится на $\mathfrak{d}(\omega)$ и если ω делится на дивизор $\mathfrak{a}$, то $\mathfrak{d}(\omega)$ делится на $\mathfrak{a}$. Очевидно, дивизор $\mathfrak{d}(\omega)$ этими свойствами определен однозначно. Он называется *дивизором дифференциала* ω. Пусть $\mathfrak{p}$ — произвольная точка; показатель, с которым $\mathfrak{p}$ входит в $\mathfrak{d}(\omega)$, называется *порядком дифференциала* ω в точке $\mathfrak{p}$ и обозначается через $\nu_{\mathfrak{p}}(\omega)$. Если $\nu_{\mathfrak{p}}(\omega)>0$, то $\mathfrak{p}$ называется *нулем* (порядка $\nu_{\mathfrak{p}}(\omega)$) дифференциала ω; если же $\nu_{\mathfrak{p}}(\omega)<0$, то $\mathfrak{p}$ называется *полюсом* (порядка $-\nu_{\mathfrak{p}}(\omega)$) дифференциала ω. Если x есть отличный от 0 элемент поля R, то, очевидно, дивизор дифференциала $x\omega$ равен $\mathfrak{d}(x)\mathfrak{d}(\omega)$.

Из теоремы 5 следует, что дивизоры всех отличных от 0 дифференциалов поля R принадлежат одному и тому же классу дивизоров; этот класс называется *каноническим классом дивизоров*[1]) поля R. (Заметим, что всегда существует по крайней мере один дифференциал поля R, не равный 0. В самом деле, пусть $\mathfrak{a}$ — любой целый дивизор степени >1; тогда по теореме Римана — Роха имеем

$$\delta(\mathfrak{a}^{-1})=l(\mathfrak{a})+d(\mathfrak{a})+g-1>0).$$

Теорема 6. *Если поле R алгебраических функций от одной переменной имеет род g, то степень канонического класса дивизоров поля R равна $2g-2$.*

Пусть ω есть произвольный отличный от 0 дифференциал поля R. Ясно, что тогда $\delta(\mathfrak{d}(\omega))\geqslant 1$. Докажем, что $\delta(\mathfrak{d}(\omega))=1$. Пусть ω' — произвольный отличный от 0 дифференциал, делящийся на $\mathfrak{d}(\omega)$; тогда $\mathfrak{d}(\omega')$ делится на $\mathfrak{d}(\omega)$.

---

[1]) Употребляют также термин „класс дифференциалов". (*Прим. перев.*).

Но степени дивизоров $\mathfrak{d}(\omega')$ и $\mathfrak{d}(\omega)$ одинаковы, поэтому $\mathfrak{d}(\omega')=\mathfrak{d}(\omega)$. Представим теперь дифференциал ω' в виде $\omega'=x\omega$, где $x\in R$. Так как $\mathfrak{d}(x)$ есть единичный дивизор, то $x\in K$, а значит, $\delta(\mathfrak{d}(\omega))=1$. Далее, дифференциалы первого рода совпадают с дифференциалами вида $x\omega$, где $x\equiv 0\,(\mathrm{mod}\,(\mathfrak{d}(\omega))^{-1})$, поэтому, в силу теоремы 4 § 5, $l((\mathfrak{d}(\omega))^{-1})=g$. Так как по теореме Римана — Роха $l((\mathfrak{d}(\omega))^{-1})=d(\mathfrak{d}(\omega))-g+1+\delta(\mathfrak{d}(\omega))$, то $d(\mathfrak{d}(\omega))=2g-2$, и теорема доказана.

Следствие. *Пусть R — поле алгебраических функций от одной переменной рода g. Если дивизор $\mathfrak{a}$ поля R имеет степень $>2g-2$, то $l(\mathfrak{a}^{-1})=d(\mathfrak{a})-g+1$.*

Действительно, никакой дивизор из канонического класса не может делиться на $\mathfrak{a}$, следовательно, никакой отличный от 0 дифференциал поля R также не может делиться на $\mathfrak{a}$. Следствие непосредственно вытекает теперь из теоремы Римана — Роха.

Теореме Римана — Роха можно придать другую эквивалентную форму (именно эта новая формулировка исторически была первоначальной).

Теорема 7. *Пусть $\mathfrak{a}$ — дивизор поля R алгебраических функций от одной переменной. Если $\mathfrak{a}'$ есть такой дивизор, что $\mathfrak{a}\mathfrak{a}'$ принадлежит каноническому классу, то*

$$l(\mathfrak{a}^{-1})=d(\mathfrak{a})-g+1+l(\mathfrak{a}'^{-1}).$$

В самом деле, пусть ω — произвольный отличный от 0 дифференциал. Дифференциалы, делящиеся на $\mathfrak{a}$, имеют вид $x\omega$, где $x\equiv 0\,(\mathrm{mod}\,\mathfrak{a}(\mathfrak{d}(\omega))^{-1})$; следовательно, $\delta(\mathfrak{a})=l(\mathfrak{a}(\mathfrak{d}(\omega))^{-1})$. Но дивизор $(\mathfrak{a}(\mathfrak{d}(\omega))^{-1})^{-1}\mathfrak{a}=\mathfrak{d}(\omega)$ принадлежит каноническому классу, поэтому дивизор $\mathfrak{a}(\mathfrak{d}(\omega))^{-1}$ эквивалентен $\mathfrak{a}'^{-1}$, откуда $l(\mathfrak{a}(\mathfrak{d}(\omega))^{-1})=l(\mathfrak{a}'^{-1})$. Теорема 7 теперь следует непосредственно из теоремы Римана — Роха.

В качестве применения теоремы 6, докажем, что поле алгебраических функций от одной переменной рода 0 всегда имеет точку, степень которой равна либо 1, либо 2. Пусть K — поле констант, а d — наименьшая из степеней точек поля R. Утверждаем, что степень $n=d(\mathfrak{a})$ любого дивизора $\mathfrak{a}$ поля R делится на d. Действительно, допустим, что $n\not\equiv 0\,(\mathrm{mod}\,d)$; тогда $n=kd-n'$, где $0<n'<d$.

Пусть $\mathfrak{p}$ — точка, степень которой равна d. Согласно теореме Римана $l(\mathfrak{p}^{-k}\mathfrak{a}) > kd - n = n' > 0$; следовательно, в R существует элемент $y \neq 0$, делящийся на $\mathfrak{p}^{-k}\mathfrak{a}$. Если мы положим $\mathfrak{d}(y) = \mathfrak{a}\mathfrak{p}^{-k}\mathfrak{b}$, то целый дивизор $\mathfrak{b}$ будет иметь степень n'. Так как $n' > 0$, то существует точка $\mathfrak{q}$, входящая в $\mathfrak{b}$ с показателем $\neq 0$. Получили противоречие, ибо $d(\mathfrak{q}) \leqslant n' < d$. Таким образом, степени всех дивизоров поля R делятся на d. Но степень каждого дивизора из канонического класса поля R равна -2 (ибо род поля R равен 0), поэтому d равно либо 1, либо 2.

Если поле R имеет точку степени 1, то оно является чисто трансцендентным расширением поля K (см. § 2). В противном случае, существует точка $\mathfrak{p}$ степени 2, а тогда по теореме Римана $l(\mathfrak{p}^{-1}) \geqslant 3$, и поле R содержит отличный от константы элемент x, который $\equiv 0 \pmod{\mathfrak{p}^{-1}}$. Очевидно, что дивизор полюсов элемента x равен $\mathfrak{p}$. В силу следствия к теореме 4 § 8 гл. I получаем, что R является квадратичным расширением поля $K\langle x\rangle$.

§ 7. Локальные компоненты дифференциала

В начале § 5 были введены дифференциалы ω для поля вида $K\langle x\rangle$, где K — поле комплексных чисел, а x — трансцендентный элемент над K. Именно, каждому элементу $u \in K\langle x\rangle$ мы сопоставили дифференциал $\omega = u\,dx$; определив его формулой

$$\omega(\mathfrak{x}) = \sum_{\mathfrak{p}} \omega^{\mathfrak{p}}(\mathfrak{x}) \tag{1}$$

(где суммирование распространено по всем точкам $\mathfrak{p}$); при этом функция $\omega^{\mathfrak{p}}(\mathfrak{x})$ зависела только от $\mathfrak{p}$-компоненты $\mathfrak{x}(\mathfrak{p})$ распределения $\mathfrak{x}$.

Пусть теперь R — произвольное поле алгебраических функций от одной переменной, а ω — дифференциал поля R. В дальнейшем нам понадобится представление дифференциала ω в виде формулы, подобной формуле (1). Найдем такое представление.

Пусть $\mathfrak{p}$ — произвольная точка поля R; $\mathfrak{p}$-компонента дифференциала ω определяется равенством:

$$\omega^{\mathfrak{p}}(\mathfrak{x}) = \omega(\mathfrak{x}^{\mathfrak{p}}),$$

где для любого распределения $\mathfrak{x}$ через $\mathfrak{x}^{\mathfrak{p}}$ обозначено распределение, которое точке $\mathfrak{p}$ сопоставляет $\mathfrak{x}(\mathfrak{p})$, а всем другим точкам — нуль. Очевидно, что $\omega^{\mathfrak{p}}$ является линейной функцией на пространстве распределений и что $\omega^{\mathfrak{p}}(\mathfrak{x})$ зависит только от $\mathfrak{p}$-компоненты распределения $\mathfrak{x}$; поэтому мы можем $\omega^{\mathfrak{p}}$ рассматривать как линейную функцию на R. Эта функция называется *$\mathfrak{p}$-компонентой дифференциала* ω.

Лемма 1. *Пусть для каждой точки $\mathfrak{p}$ через $\omega^{\mathfrak{p}}$ обозначена $\mathfrak{p}$-компонента дифференциала ω поля R. Тогда для любого распределения $\mathfrak{x}$ существует только конечное число точек $\mathfrak{p}$, для которых $\omega^{\mathfrak{p}}(\mathfrak{x}) \neq 0$, и имеет место равенство:*

$$\omega(\mathfrak{x}) = \sum_{\mathfrak{p}} \omega^{\mathfrak{p}}(\mathfrak{x}).$$

Пусть ω делится на дивизор $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$. Существует только конечное число точек $\mathfrak{q}$, для которых $a(\mathfrak{q}) \neq 0$ или $\nu_{\mathfrak{q}}(\mathfrak{x}) < 0$; пусть $\mathfrak{q}_1, \ldots, \mathfrak{q}_h$ — эти точки. Если точка $\mathfrak{p}$ отлична от точек $\mathfrak{q}_1, \ldots, \mathfrak{q}_h$, то распределение, сопоставляющее точке $\mathfrak{p}$ значение $\mathfrak{x}(\mathfrak{p})$, а всем другим точкам — нуль, делится на $\mathfrak{a}^{-1}$; поэтому для таких точек $\mathfrak{p}$ будем иметь $\omega^{\mathfrak{p}}(\mathfrak{x}) = 0$. Пусть $\mathfrak{x}_i$ есть распределение, сопоставляющее точке $\mathfrak{q}_i$ значение $\mathfrak{x}(\mathfrak{q}_i)$, а всем другим точкам — нуль. Положим $\mathfrak{x}' = \sum_{i=1}^{h} \mathfrak{x}_i$; тогда $\mathfrak{x} - \mathfrak{x}'$ делится на $\mathfrak{a}^{-1}$, а значит, $\omega(\mathfrak{x}) = \omega(\mathfrak{x}') = \sum_{i=1}^{h} \omega(\mathfrak{x}_i) = \sum_{\mathfrak{p}} \omega^{\mathfrak{p}}(\mathfrak{x})$. Лемма 1 доказана.

Лемма 2. *Показатель, с которым точка $\mathfrak{p}$ входит в дивизор $\mathfrak{d}(\omega)$ дифференциала $\omega \neq 0$ поля R, равен наибольшему целому числу m, для которого равенство $\omega^{\mathfrak{p}}(x) = 0$ имеет место при всех $x \in R$, удовлетворяющих условию $\nu_{\mathfrak{p}}(x) \geqslant -m$.*

Положим $\mathfrak{d}(\omega) = \prod_{\mathfrak{q}} \mathfrak{q}^{a(\mathfrak{q})}$. Пусть элемент x из R удовлетворяет условию $\nu_{\mathfrak{p}}(x) \geqslant -a(\mathfrak{p})$ и пусть $x^{\mathfrak{p}}$ есть распределение, которое точке $\mathfrak{p}$ сопоставляет значение x, а всякой другой точке — нуль. Очевидно, что $x^{\mathfrak{p}}$ делится на $(\mathfrak{d}(\omega))^{-1}$, а следовательно, $\omega(x^{\mathfrak{p}}) = \omega^{\mathfrak{p}}(x) = 0$. С другой стороны, существует распределение $\mathfrak{x}$, делящееся на $\mathfrak{p}^{-1}(\mathfrak{d}(\omega))^{-1}$, для

которого $\omega(\mathfrak{x}) \neq 0$. Если точка $\mathfrak{q}$ отлична от $\mathfrak{p}$, то $\nu_{\mathfrak{q}}(\mathfrak{x}(\mathfrak{q})) \geqslant -a(\mathfrak{q})$, откуда $\omega^{\mathfrak{q}}(\mathfrak{x}) = \omega^{\mathfrak{q}}(\mathfrak{x}(\mathfrak{q})) = 0$. Таким образом, $\omega(\mathfrak{x}) = \omega^{\mathfrak{p}}(\mathfrak{x}) = \omega^{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p})) \neq 0$, причем $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p})) \geqslant -a(\mathfrak{p}) - 1$. Этим доказано, что $a(\mathfrak{p}) = m$.

Следствие. *Если дифференциал ω отличен от 0, то $\omega^{\mathfrak{p}} \neq 0$ для любой точки $\mathfrak{p}$.*

§ 8. Поля эллиптических функций

Пусть ζ и ζ' — два отличных от 0 комплексных числа, отношение которых $\frac{\zeta'}{\zeta}$ невещественно. Мы сейчас рассмотрим *эллиптические функции* $f(z)$ с периодами ζ и ζ', т. е. мероморфные на всей z-плоскости функции $f(z)$, для которых числа ζ и ζ' являются периодами. Если f и g — эллиптические функции, то функции $f+g$, $f-g$, fg и $\frac{f}{g}$ (если $g \neq 0$) также эллиптические. Отсюда следует, что эллиптические функции образуют поле R. Каждая постоянная функция является эллиптической; отождествляя постоянную функцию с ее постоянным значением, можно считать, что поле R содержит поле комплексных чисел K.

Покажем что существует по крайней мере одна непостоянная эллиптическая функция. Для целых чисел m и n положим $\zeta_{m,n} = m\zeta + n\zeta'$. Знаком $\sum\limits_{m,n}'$ будем обозначать суммирование, распространенное по всем парам целых значений m и n, кроме пары $m=0$ и $n=0$. Докажем прежде всего, что ряд

$$\sum_{m,n}' \frac{1}{|\zeta_{m,n}|^3} \tag{1}$$

сходится. Обозначим через P параллелограмм с вершинами в точках 0, ζ, ζ' и $\zeta+\zeta'$; P является, стало быть, множеством комплексных чисел вида $t\zeta + t'\zeta'$, где t и t' пробегают вещественные значения из замкнутого интервала [0, 1]. Пусть $P_{m,n}$ — параллелограмм, получающийся из P параллельным переносом комплексной плоскости, при котором 0 переходит в $\zeta_{m,n}$. Ясно, что никакие два различных множества $P_{m,n}$ не имеют общей внутренней точки. Обозначим через d диаметр, а через A — площадь параллелограмма P.

Пусть далее $\Gamma(R)$ обозначает замкнутый круг радиуса R с центром в 0, а $\nu(R)$ — число точек $\zeta_{m,n}$, лежащих в $\Gamma(R)$. Очевидно, что из $\zeta_{m,n} \in \Gamma(R)$ следует $P_{m,n} \subset \Gamma(R+d)$; поэтому $A\nu(R) \leqslant \pi(R+d)^2$, откуда $\nu(R) \leqslant \frac{4\pi}{A} R^2$ при $R \geqslant d$. Пусть $(R_1, \ldots, R_k, \ldots)$ есть такая возрастающая последовательность чисел $\geqslant d$, что ряд $\sum_{k=1}^{\infty} \frac{R_{k+1}^2}{R_k^3}$ сходится (можно взять, например, $R_k = dk^2$). Число пар (m, n), для которых $R_k < |\zeta_{m,n}| \leqslant R_{k+1}$, не превосходит $\nu(R_{k+1})$; следовательно,

$$\sum_{m,n}{}' \frac{1}{|\zeta_{m,n}|^3} < \alpha + \sum_{k=1}^{\infty} \frac{4\pi}{A} \frac{R_{k+1}^2}{R_k^3} < \infty,$$

где α равно сумме конечного числа членов ряда, которые $\geqslant \frac{1}{R_1^3}$.

Рассмотрим теперь ряд

$$\sum_{m,n}{}' \left\{ \frac{1}{(z-\zeta_{m,n})^2} - \frac{1}{\zeta_{m,n}^2} \right\}. \tag{2}$$

Пусть $0 < \varepsilon < \frac{d}{2}$; для каждой точки $\zeta_{m,n} \neq 0$ построим открытый круг радиуса ε с центром в $\zeta_{m,n}$ и обозначим через D множество, полученное после удаления из плоскости всех этих кругов. Мы покажем сейчас, что наш ряд сходится равномерно на любом ограниченном подмножестве E множества D. Имеем

$$\frac{1}{(z-\zeta_{m,n})^2} - \frac{1}{\zeta_{m,n}^2} = -\frac{z^2 - 2z\zeta_{m,n}}{\zeta_{m,n}^2 (z-\zeta_{m,n})^2}.$$

Обозначим через ρ верхнюю границу модулей всех точек из E. Если $|\zeta_{m,n}| \geqslant 2\rho$ и $z \in E$, то $|z-\zeta_{m,n}| \geqslant \frac{1}{2}|\zeta_{m,n}|$, откуда

$$\left| \frac{1}{(z-\zeta_{m,n})^2} - \frac{1}{\zeta_{m,n}^2} \right| \leqslant \frac{4\rho^2}{|\zeta_{m,n}|^4} + \frac{8\rho}{|\zeta_{m,n}|^3}.$$

Существует только конечное число пар (m, n), для которых $|\zeta_{m,n}| < 2\rho$. С другой стороны, так как ряд (1) сходится,

то ряд $\sum_{m,n}' \frac{1}{|\zeta_{m,n}|^4}$ также сходится. Этим и доказана равномерная сходимость ряда (2) на E.

Из доказанного следует, что функция

$$f(z)=\frac{1}{z^2}+\sum_{m,n}'\left\{\frac{1}{(z-\zeta_{m,n})^2}-\frac{1}{\zeta_{m,n}^2}\right\}$$

мероморфна на всей плоскости за исключением, быть может, точек $\zeta_{m,n}$, при этом в точке 0 эта функция имеет полюс порядка 2. Далее, согласно общим теоремам теории аналитических функций производная $f'(z)$ от $f(z)$ равна

$$f'(z)=-\frac{2}{z^3}-2\sum_{m,n}'\frac{1}{(z-\zeta_{m,n})^3}.$$

Если мы заменим z на $z+\zeta$ или на $z+\zeta'$, то члены ряда, стоящего в правой части последнего равенства, подвергнуться лишь некоторой перестановке. Следовательно, для $f'(z)$ числа ζ и ζ' являются периодами, а значит, функции $f(z+\zeta)-f(z)$ и $f(z+\zeta')-f(z)$ суть константы. С другой стороны, из представления $f(z)$ в виде ряда следует, что функция $f(z)$ четная, т. е. $f(-z)=f(z)$. Так как $f(z+\zeta)-f(z)=$ $=f\left(\frac{\zeta}{2}\right)-f\left(-\frac{\zeta}{2}\right)$, то $f(z+\zeta)=f(z)$; аналогично получим $f(z+\zeta')=f(z)$. Таким образом, $f(z+\zeta_{m,n})=f(z)$ при всех (m, n), и $\zeta_{m,n}$ является полюсом функции $f(z)$ порядка 2. Этим доказано, что $f(z)$ есть непостоянная (ибо она имеет полюса) эллиптическая функция.

Докажем теперь, что R есть поле алгебраических функций над K. Так как поле K алгебраически замкнуто, то элемент $f(z)$ трансцендентен над K; поэтому достаточно будет показать, что R является алгебраическим расширением поля $K\langle f(z)\rangle$ конечной степени; в действительности, как мы сейчас увидим, степень поля R над $K\langle f(z)\rangle$ равна 2.

Лемма 1. *Если эллиптическая функция $h(z)$ не имеет полюсов, то она есть константа.*

В самом деле, $h(z)$ является, очевидно, целой функцией. Она ограничена на параллелограмме P. С другой стороны, для любого комплексного числа z мы можем найти такие целые числа m и n, что $z+\zeta_{m,n}\in P$. Так как функция $h(z)$

эллиптическая, то $h(z+\zeta_{m,n})=h(z)$. Отсюда следует, что $h(z)$ ограничена на всей плоскости и, значит, является постоянной функцией.

Покажем, что всякая четная эллиптическая функция $g(z)$ принадлежит полю $K\langle f(z)\rangle$. Так как $g(z)$ мероморфна на всей плоскости, то на P она имеет только конечное число полюсов. Из них выберем такую максимальную подсистему отличных от 0, ζ, ζ' и $\zeta+\zeta'$ полюсов $\{a_1, \ldots, a_h\}$, что разность любой пары чисел из этой системы не равна ни ζ, ни ζ'. Пусть e_i есть порядок полюса a_i. Так как на P полюсами функции $f(z)$ являются только числа 0, ζ, ζ' и $\zeta+\zeta'$, то все числа a_i не будут полюсами $f(z)$. Рассмотрим функцию $g_1(z)=g(z)\prod_{i=1}^{h}(f(z)-f(a_i))^{e_i}$. Очевидно, числа $a_1, \ldots, a_h$ не являются полюсами $g_1(z)$. Если a' есть полюс функции $g(z)$ на P, отличный от 0, ζ, ζ' и $\zeta+\zeta'$ и отличный от чисел $a_1, \ldots, a_h$, то a' имеет вид $a_i\pm\zeta$ или $a_i\pm\zeta'$, а так как $g_1(z)$ — эллиптическая функция, то a' не является полюсом $g_1(z)$. Таким образом, функция $g_1(z)$ на параллелограмме P может иметь полюса лишь в точках 0, ζ, ζ' и $\zeta+\zeta'$. С другой стороны, $g_1(z)$ — четная функция. Значит, ее разложение в ряд Лорана в окрестности 0 имеет вид

$$g_1(z)=\sum_{k=1}^{r}\frac{c_k}{z^{2k}}+\sum_{k=0}^{\infty}d_kz^{2k}.$$

Покажем, что функция $g_1(z)$ может быть представлена в виде $\gamma_0f^r(z)+\gamma_1f^{r-1}(z)+\ldots+\gamma_r$, где $\gamma_0, \gamma_1, \ldots, \gamma_r$ — константы. Положим $\gamma_0=c_r$; тогда для функции $g_1(z)-\gamma_0f^r(z)$ число 0 является полюсом порядка $<2r$. Допустим, что для некоторого $h<r-1$ уже определены такие константы $\gamma_0, \ldots, \gamma_h$, что для функции $g_1(z)-\sum_{i=0}^{h}\gamma_if^{r-i}(z)$ число 0 является полюсом порядка $<2(r-h)$. Так как эта функция четная, то ее разложение в ряд Лорана в окрестности 0 имеет вид

$$\sum_{k=1}^{r-h-1}\frac{c_{k,h}}{z^{2k}}+\sum_{k=0}^{\infty}d_{k,h}z^{2k}.$$

Если мы положим $\gamma_{h+1}=c_{r-h-1,h}$, то для функции $g_1(z)-\sum_{i=0}^{h+1}\gamma_i f^{r-i}(z)$ число 0 будет полюсом порядка $<2(r-h-1)$. Продолжая этот процесс, мы в конце концов получим функцию вида $g_1(z)-\sum_{i=0}^{r-1}\gamma_i f^{r-i}(z)$, для которой 0 является полюсом порядка <2. Будучи четной, эта функция вовсе не имеет полюса в точке 0. Являясь эллиптической функцией, она не имеет полюсов и в точках $\zeta_{m,n}$. С другой стороны, эта функция не имеет полюсов на P вне точек 0, ζ, ζ' и $\zeta+\zeta'$. Таким образом, она вообще не имеет полюсов, а значит, является константой γ_r. Этим доказано, что наша первоначальная функция $g(z)$ может быть представлена в виде рациональной функции от $f(z)$.

Если теперь $\varphi(z)$ есть произвольная функция из поля R, то $\varphi(-z)$ также принадлежит R. Отображение σ: $\varphi(z)\to\varphi(-z)$ является, очевидно, автоморфизмом второго порядка поля R. Из вышеизложенного следует, что подполе элементов, инвариантных относительно σ, равно $K\langle f(z)\rangle$. Отсюда заключаем, что R является алгебраическим расширением поля $K\langle f(z)\rangle$ степени 2.

Пусть a — некоторое комплексное число. Множество $\mathfrak{o}_a$ эллиптических функций, для которых a не является полюсом, образует, как легко видеть, подкольцо поля R. Это кольцо отлично от R. В самом деле, если α не совпадает с $\zeta_{m,n}$, то $(f(z)-f(a))^{-1}$ не принадлежит $\mathfrak{o}_a$; если же $a=\zeta_{m,n}$, то $f(z)\notin\mathfrak{o}_a$. С другой стороны, если эллиптическая функция $g(z)$ не принадлежит $\mathfrak{o}_a$, то $\frac{1}{g(z)}\in\mathfrak{o}_a$. Таким образом, $\mathfrak{o}_a$ есть V-кольцо в поле R (над K). Обозначим через $\mathfrak{p}_a$ соответствующую точку поля R. Точки, соответствующие указанным образом числам a и $a+\zeta_{m,n}$, очевидно, совпадают; если же комплексные числа a и a' таковы, что их разность не равна ни одному из чисел $\zeta_{m,n}$, то точки $\mathfrak{p}_a$ и $\mathfrak{p}_{a'}$ различны (ибо $f(z-a)$ принадлежит $\mathfrak{o}_{a'}$ и не принадлежит $\mathfrak{o}_a$).

Покажем теперь, что каждая точка $\mathfrak{p}$ поля R имеет вид $\mathfrak{p}_a$ при некотором a. Выберем целое число m, большее, чем род поля R. Так как $d(\mathfrak{p}^m)=m$, то по теореме Римана

имеем $l(\mathfrak{p}^{-m}) \geqslant 2$. Следовательно, существует функция $u(z) \in R$, отличная от константы, порядок которой в каждой точке $\neq \mathfrak{p}$ неотрицателен. Если бы точка $\mathfrak{p}$ была отлична от всех точек $\mathfrak{p}_a$, то эллиптическая функция $u(z)$ не имела бы полюсов, что противоречит лемме 1. Для любого комплексного числа a существует эллиптическая функция $p_a(z)$, для которой a является простым нулем; такой функцией является, например, $\frac{f(z-a)}{f'(z-a)}$. Если $h(z)$ есть произвольная эллиптическая функция, а ν — порядок в a мероморфной функции $h(z)$, то $h(z) = (p_a(z))^\nu h_1(z)$, где для эллиптической функции $h_1(z)$ число a не является ни нулем, ни полюсом, т. е. $h_1(z)$ является делителем единицы в кольце точки $\mathfrak{p}_a$. Отсюда непосредственно следует, что $\nu_{\mathfrak{p}_a}(h(z))$ равно порядку функции $h(z)$ в точке a.

Найдем теперь род g поля R. Если $\mathfrak{p}_0$ есть точка, соответствующая числу 0, то функция $f(z)$ (рассматриваемая как элемент поля R) делится, очевидно, на дивизор $\mathfrak{p}_0^{-2}$, а $f'(z)$ делится на $\mathfrak{p}_0^{-3}$. Следовательно, если a и b — целые неотрицательные числа, то $(f(z))^a f'(z)$ делится на $\mathfrak{p}_0^{-2a-3}$, а $(f(z))^b$ делится на $\mathfrak{p}_0^{-2b}$. Выберем целое число m так, чтобы оно было больше наибольшего из чисел 2, $2g-2$. Обозначим через m_1 целую часть числа $\frac{m-3}{2}$, а через m_2 — целую часть $\frac{m}{2}$. Если числа a и b таковы, что $0 \leqslant a \leqslant m_1$, $0 \leqslant b \leqslant m_2$, то функции $(f(z))^a f'(z)$ и $(f(z))^b$ делятся на $\mathfrak{p}_0^{-m}$. Эти функции, число которых равно $m_1 + m_2 + 2 = m$, линейно независимы над K. В самом деле, пусть P и Q — такие многочлены с комплексными коэффициентами, что $P(f(z))f'(z) + Q(f(z)) = 0$. Заменяя в этом тождестве z на $-z$ и замечая, что $f'(z)$ — нечетная функция, мы получим $-P(f(z))f'(z) + Q(f(z)) = 0$. Так как $f'(z) \neq 0$ и элемент $f(z)$ трансцендентен над K, то $P = Q = 0$, и наше утверждение доказано. Таким образом, $l(\mathfrak{p}_0^{-m}) \geqslant m$. С другой стороны, в силу следствия к теореме 6 § 6, мы имеем $l(\mathfrak{p}_0^{-m}) = d(\mathfrak{p}_0^m) - g + 1 = m - g + 1$, откуда следует, что $g \leqslant 1$. Остается доказать, что g не может быть нулем. Для этого, достаточно показать, что эллиптическая функция $h(z)$,

делящаяся на $\mathfrak{p}_0^{-1}$, является константой. Ряд Лорана для $h(z)$ в окрестности 0 имеет вид $h(z)=\frac{a}{z}+\sum_{k=0}^{\infty} a_k z^k$. Для эллиптической функции $h(z)+h(-z)$ число 0 не является полюсом; следовательно, эта функция вообще не имеет полюсов, а значит, она есть константа C. Функция $h_1(z)=h(z)-\frac{1}{2}C$ является нечетной эллиптической функцией, делящейся на $\mathfrak{p}_0^{-1}$. Имеем $h_1\left(-\frac{\zeta}{2}\right)=-h_1\left(\frac{\zeta}{2}\right)$; с другой стороны, так как $-\frac{\zeta}{2}=\frac{\zeta}{2}-\zeta$, то $h_1\left(-\frac{\zeta}{2}\right)=h_1\left(\frac{\zeta}{2}\right)$, откуда $h_1\left(\frac{\zeta}{2}\right)=0$. Аналогично $h_1\left(\frac{\zeta'}{2}\right)=0$. Так как $\mathfrak{p}_{\frac{\zeta}{2}}\neq\mathfrak{p}_{\frac{\zeta'}{2}}$, то получаем, что $h_1(z)$ делится на дивизор $\mathfrak{p}_0^{-1}\mathfrak{p}_{\frac{\zeta}{2}}\mathfrak{p}_{\frac{\zeta'}{2}}$, степень которого равна 1. Отсюда непосредственно следует, что $h_1(z)=0$, т. е. $h(z)=\frac{1}{2}C$. Таким образом, мы доказали, что *род поля эллиптических функций равен* 1.

Так как функция $f'(z)$ нечетная, то она не принадлежит полю $K\langle f(z)\rangle$. Но R есть квадратичное расширение поля $K\langle f(z)\rangle$, поэтому $R=K\langle f(z), f'(z)\rangle$. С другой стороны, функция $(f'(z))^2$ четная, и для нее 0 является полюсом порядка 6. Отсюда легко следует, что $(f'(z))^2$ имеет вид $P(f(z))$, где P — многочлен степени 3. Последний результат был нами уже получен в § 3, где рассматривались более общие поля рода 1. В нашем случае можно было бы без труда доказать, что многочлен $P(Z)$ имеет вид $4Z^3+aZ+b$.

ГЛАВА III

ПОЛНЫЕ $\mathfrak{p}$-АДИЧЕСКИЕ РАСШИРЕНИЯ

§ 1. Определение $\mathfrak{p}$-адического пополнения

Пусть K — поле комплексных чисел, а x — трансцендентный элемент над K. Каждая рациональная функция $u(x)$ от x в окрестности $a \in K$ может быть разложена в ряд Лорана

$$u(x) = \sum_{k=r}^{\infty} c_k (x-a)^k. \tag{1}$$

Однако не всякая функция, представимая в окрестности a таким рядом, является рациональной. В некоторых случаях все же бывает целесообразно рассматривать множество всех функций от x, мероморфных в a (т. е. представимых рядом Лорана в окрестности a). Существование этого множества функций зависит, конечно, всецело от топологических свойств поля K, ибо ряд

$$\sum_{k=r}^{\infty} c_k (x-a)^k \tag{2}$$

только тогда представляет некоторую функцию, если он сходится в некоторой окрестности a. Однако для всех алгебраических целей имеет значение только последовательность коэффициентов таких рядов, а не тот факт, что они сходятся в некоторой области. Это приводит нас к мысли (вместо множества функций, мероморфных в a) рассматривать совокупность всех рядов вида (2) независимо от того, сходятся они или нет. Аналогом этого множества формальных степенных рядов (для рассмотренного сейчас поля $K\langle x\rangle$) в случае произвольного поля R алгебраических

функций от одной переменной будет так называемое пополнение поля R.

Пусть $\mathfrak{p}$ — точка поля R. Будем говорить, что последовательность (x_n) элементов поля R *сходится в точке* $\mathfrak{p}$ к элементу x из R, если выполнено следующее условие:

$$\lim_{n\to\infty} \nu_{\mathfrak{p}}(x - x_n) = \infty. \tag{3}$$

Если (3) имеет место, то, очевидно, имеем также

$$\lim_{n\to\infty} \nu_{\mathfrak{p}}(x_{n+1} - x_n) = \infty. \tag{4}$$

Однако может случиться, что последовательность (x_n) удовлетворяет условию (4) и не удовлетворяет условию (3). Всякая последовательность, удовлетворяющая условию (4), будет называться *последовательностью Коши в точке* $\mathfrak{p}$.

Пусть X есть множество всех последовательностей $(x_n)_{1\leqslant n<\infty}$ элементов поля R. В множестве X определяем сложение и умножение:

$$(x_n) + (y_n) = (x_n + y_n),$$
$$(x_n)(y_n) = (x_n y_n).$$

Очевидно, что относительно этих действий X является кольцом. Покажем, что последовательности Коши в точке $\mathfrak{p}$ образуют подкольцо кольца X. Так как

$$\nu_{\mathfrak{p}}((x_{n+1} - y_{n+1}) - (x_n - y_n)) \geqslant$$
$$\geqslant \min\{\nu_{\mathfrak{p}}(x_{n+1} - x_n),\ \nu_{\mathfrak{p}}(y_{n+1} - y_n)\},$$

то разность двух последовательностей Коши является также последовательностью Коши. Чтобы доказать аналогичное утверждение для произведения, установим сначала следующую лемму.

Лемма 1. *Если (x_n) есть последовательность Коши в точке $\mathfrak{p}$, то последовательность чисел $\nu_{\mathfrak{p}}(x_n)$ либо неограниченно возрастает вместе с n (в этом случае (x_n) сходится к 0 в точке $\mathfrak{p}$), либо стабилизируется (т. е. все числа $\nu_{\mathfrak{p}}(x_n)$, начиная с некоторого значения n, равны друг другу).*

Действительно, допустим, что $\nu_{\mathfrak{p}}(x_n)$ не является неограниченно возрастающей последовательностью чисел. Тогда существует такое целое число N, что $\nu_{\mathfrak{p}}(x_n) < N$ для

бесконечного числа значений n. С другой стороны, существует такое натуральное число n_0, что $\nu_{\mathfrak{p}}(x_{n+1}-x_n)\geqslant N$ при всех $n\geqslant n_0$. Можно считать, что n_0 есть один из тех индексов n, для которых $\nu_{\mathfrak{p}}(x_n)<N$. Утверждаем, что $\nu_{\mathfrak{p}}(x_n)=\nu_{\mathfrak{p}}(x_{n_0})$ для всех $n\geqslant n_0$. При $n=n_0$ последнее равенство справедливо. Допустим, что оно справедливо для некоторого $n\geqslant n_0$. Так как $x_{n+1}=x_n+(x_{n+1}-x_n)$ и

$$\nu_{\mathfrak{p}}(x_{n+1}-x_n)\geqslant N>\nu_{\mathfrak{p}}(x_{n_0})=\nu_{\mathfrak{p}}(x_n),$$

то $\nu_{\mathfrak{p}}(x_{n+1})=\nu_{\mathfrak{p}}(x_n)=\nu_{\mathfrak{p}}(x_{n_0})$ (см. § 3 гл. I).

Пусть теперь (x_n) и (y_n) — две последовательности Коши. Имеем

$$x_{n+1}y_{n+1}-x_ny_n=y_n(x_{n+1}-x_n)+x_{n+1}(y_{n+1}-y_n).$$

В силу леммы 1 существуют такие целые числа A и B, что

$$\nu_{\mathfrak{p}}(x_n)\geqslant A,\quad \nu_{\mathfrak{p}}(y_n)\geqslant B$$

для всех n. Поэтому получаем

$$\nu_{\mathfrak{p}}(x_{n+1}y_{n+1}-x_ny_n)\geqslant$$
$$\geqslant\min\{B+\nu_{\mathfrak{p}}(x_{n+1}-x_n),\ A+\nu_{\mathfrak{p}}(y_{n+1}-y_n)\},$$

откуда следует, что $\nu_{\mathfrak{p}}(x_{n+1}y_{n+1}-x_ny_n)$ неограниченно возрастает вместе с n, т. е. (x_ny_n) является последовательностью Коши.

Обозначим через X_0 кольцо всех последовательностей Коши в точке $\mathfrak{p}$, а через $\mathfrak{X}$ — множество всех последовательностей, сходящихся к 0 в точке $\mathfrak{p}$. Очевидно, что $\mathfrak{X}$ есть подмножество кольца X_0. Докажем что $\mathfrak{X}$ является идеалом в X_0. Если $(x_n)\in\mathfrak{X}$ и $(y_n)\in\mathfrak{X}$, то, очевидно, $(x_n-y_n)\in\mathfrak{X}$. Пусть $(x_n)\in\mathfrak{X}$ и $(z_n)\in X_0$. В силу леммы 1 существует такое целое число C, что $\nu_{\mathfrak{p}}(z_n)\geqslant C$ при всех n, откуда $\nu_{\mathfrak{p}}(x_nz_n)\geqslant C+\nu_{\mathfrak{p}}(x_n)$. Следовательно, $\nu_{\mathfrak{p}}(x_nz_n)$ неограниченно возрастает вместе с n, т. е. $(x_nz_n)\in\mathfrak{X}$. Займемся изучением фактор-кольца $X_0/\mathfrak{X}$. Это фактор-кольцо мы обозначим через $\bar{R}_{\mathfrak{p}}$.

Каждому элементу $x\in R$ поставим в соответствие последовательность (x_n), для которой $x_n=x$ при всех n. Этим мы определили изоморфное отображение поля R в кольцо последовательностей элементов из R. Последовательность (x_n), соответствующая элементу $x\in R$, является,

очевидно, последовательностью Коши; при этом она сходится к 0 только в случае, если $x=0$. Следовательно, множество последовательностей, соответствующих элементам из R, содержится в X_0 и отображается изоморфно в $\bar{R}_{\mathfrak{p}}$ при естественном гомоморфизме X_0 на $X_0/\mathfrak{X}=\bar{R}_{\mathfrak{p}}$. Таким образом, мы имеем изоморфное отображение R на подполе кольца $\bar{R}_{\mathfrak{p}}$. В дальнейшем мы будем отождествлять элементы из R с соответствующими им элементами из $\bar{R}_{\mathfrak{p}}$, т. е. будем считать, что поле R является подполем кольца $\bar{R}_{\mathfrak{p}}$. Кроме того, если $\bar{x}\in R_{\mathfrak{p}}$ есть класс вычетов по модулю $\mathfrak{X}$, содержащий последовательность Коши (x_n), то будем писать

$$\bar{x}=\lim_{n\to\infty} x_n.$$

Если $x_n=x$ при всех n, то, очевидно, $x=\lim\limits_{n\to\infty} x_n$.

Докажем теперь, что кольцо $\bar{R}_{\mathfrak{p}}$ является полем. Пусть $\bar{x}$ есть отличный от 0 элемент из $\bar{R}_{\mathfrak{p}}$; положим $\bar{x}=\lim\limits_{n\to\infty} x_n$, $x_n\in R$. Так как (x_n), являясь последовательностью Коши, не сходится к 0, то $x_n\neq 0$ для всех достаточно больших n (лемма 1). Положим $x_n'=x_n^{-1}$, если $x_n\neq 0$, и $x_n'=0$, если $x_n=0$. Тогда для достаточно больших n будем иметь $x_{n+1}'-x_n'=x_{n+1}^{-1}x_n^{-1}(x_n-x_{n+1})$. В силу леммы 1 число $\nu_{\mathfrak{p}}(x_n x_{n+1})$ постоянно для достаточно больших n. Так как $\nu_{\mathfrak{p}}(x_{n+1}-x_n)$ неограниченно возрастает, то $\nu_{\mathfrak{p}}(x_{n+1}'-x_n')$, следовательно, также неограниченно возрастает (при $n\to\infty$), т. е. (x_n') есть последовательность Коши. Положим $\bar{x}'=\lim\limits_{n\to\infty} x_n'$ и докажем, что $\bar{x}'$ является обратным для элемента $\bar{x}$ в кольце $\bar{R}_{\mathfrak{p}}$. Пусть $u_n=1$ при всех n; тогда $x_n x_n'=u_n$ для всех достаточно больших n, откуда $\bar{x}\bar{x}'=\lim\limits_{n\to\infty} x_n x_n'=\lim\limits_{n\to\infty} u_n=1$. Так как 1 является, очевидно, единичным элементом в $\bar{R}_{\mathfrak{p}}$, то $\bar{x}'$ есть обратный элемент для $\bar{x}$. Этим доказано, что $\bar{R}_{\mathfrak{p}}$ — поле.

Продолжим теперь функцию порядка $\nu_{\mathfrak{p}}$, определенную на поле R, до функции на поле $\bar{R}_{\mathfrak{p}}$. Пусть $\bar{x}$ — отличный

от 0 элемент поля $\bar{R}_{\mathfrak{p}}$ и пусть $\bar{x} = \lim\limits_{n\to\infty} x_n$, $x_n \in R$. Последовательность (x_n) не сходится к 0, поэтому, в силу леммы 1, $\nu_{\mathfrak{p}}(x_n)$ постоянно для всех достаточно больших n, и это постоянное значение отлично от ∞. Если (x'_n) — любая другая последовательность Коши, для которой $\lim\limits_{n\to\infty} x'_n = \bar{x}$, то $\lim\limits_{n\to\infty} \nu_{\mathfrak{p}}(x'_n - x_n) = \infty$, следовательно, начиная с некоторого значения n, будем иметь $\nu_{\mathfrak{p}}(x'_n - x_n) > \nu_{\mathfrak{p}}(x_n)$, а значит $\nu_{\mathfrak{p}}(x'_n) = \nu_{\mathfrak{p}}(x'_n - x_n + x_n) = \nu_{\mathfrak{p}}(x_n)$. Обозначим через $\nu_{\mathfrak{p}}(\bar{x})$ постоянное для всех достаточно больших n значение $\nu_{\mathfrak{p}}(x_n)$, где (x_n) есть последовательность Коши, для которой $\lim\limits_{n\to\infty} x_n = \bar{x}$. Если $\bar{x} = 0$, то полагаем $\nu_{\mathfrak{p}}(\bar{x}) = \infty$. Так определяемая функция $\nu_{\mathfrak{p}}$ является продолжением функции порядка $\nu_{\mathfrak{p}}$ поля R на поле $\bar{R}_{\mathfrak{p}}$. Действительно, если $\bar{x} = x \in R$, то мы можем взять $x_n = x$ для всех n.

Из определения непосредственно следует, что

$$\nu_{\mathfrak{p}}(\bar{x} + \bar{y}) \geqslant \min\{\nu_{\mathfrak{p}}(\bar{x}),\ \nu_{\mathfrak{p}}(\bar{y})\},$$
$$\nu_{\mathfrak{p}}(\bar{x}\bar{y}) = \nu_{\mathfrak{p}}(\bar{x}) + \nu_{\mathfrak{p}}(\bar{y}),$$

где $\bar{x}$ и $\bar{y}$ принадлежат $\bar{R}_{\mathfrak{p}}$. Более того, если $\nu_{\mathfrak{p}}(\bar{x}) \neq \nu_{\mathfrak{p}}(\bar{y})$, то в неравенстве фактически имеет место знак равенства (см. § 3 гл. I).

Обозначим через $\bar{\mathfrak{o}}$ множество тех элементов $\bar{x} \in \bar{R}_{\mathfrak{p}}$, для которых $\nu_{\mathfrak{p}}(\bar{x}) \geqslant 0$. Очевидно, что $\bar{\mathfrak{o}}$ — кольцо, причем пересечение $\bar{\mathfrak{o}} \cap R$ равно кольцу $\mathfrak{o}$ точки $\mathfrak{p}$. Имеем $\bar{\mathfrak{o}} \neq \bar{R}_{\mathfrak{p}}$, кроме того, если элемент $\bar{x}$ из $\bar{R}_{\mathfrak{p}}$ не принадлежит $\bar{\mathfrak{o}}$, то $\bar{x}^{-1}$ принадлежит $\bar{\mathfrak{o}}$, ибо $\nu_{\mathfrak{p}}(\bar{x}^{-1}) = -\nu_{\mathfrak{p}}(\bar{x})$. Это означает, что $\bar{\mathfrak{o}}$ является V-кольцом в $\bar{R}_{\mathfrak{p}}$. Элементы из $\bar{\mathfrak{o}}$ называются *целыми элементами* поля $\bar{R}_{\mathfrak{p}}$. Идеал $\bar{\mathfrak{p}}$ всех необратимых элементов из $\bar{\mathfrak{o}}$ состоит из тех элементов $\bar{x} \in \bar{R}_{\mathfrak{p}}$, для которых $\nu_{\mathfrak{p}}(\bar{x}) > 0$; очевидно, что $\bar{\mathfrak{p}} \cap R = \mathfrak{p}$.

Пусть $\bar{x} = \lim\limits_{n\to\infty} x_n$ — элемент из $\bar{R}_{\mathfrak{p}}$, где (x_n) есть последовательность Коши элементов поля R. Рассматривая

элементы поля R как элементы поля $\bar{R}_{\mathfrak{p}}$, докажем, что $\lim\limits_{n\to\infty} \nu_{\mathfrak{p}}(\bar{x}-x_n)=\infty$. Имеем $\bar{x}-x_m=\lim\limits_{n\to\infty}(x_{m+n}-x_m)$ и

$$x_{m+n}-x_m=\sum_{k=1}^{n}(x_{m+k}-x_{m+k-1}),$$

откуда $\nu_{\mathfrak{p}}(x_{m+n}-x_m)\geqslant \min\limits_{1\leqslant k\leqslant n}\nu_{\mathfrak{p}}(x_{m+k}-x_{m+k-1})$. Так как (x_n) есть последовательность Коши, то $\nu_{\mathfrak{p}}(x_{q+1}-x_q)$ неограниченно возрастает при $q\to\infty$. Следовательно, для любого целого числа M существует такое m_0, что $\nu_{\mathfrak{p}}(x_{q+1}-x_q)>M$ при всех $q\geqslant m_0$. Таким образом, при $m\geqslant m_0$ имеет место неравенство $\nu_{\mathfrak{p}}(x_{m+n}-x_m)>M$ для всех $n>0$. Отсюда следует, что $\nu_{\mathfrak{p}}(\bar{x}-x_m)>M$ для всех $m\geqslant m_0$, и наше утверждение доказано.

Из доказанного прежде всего вытекает, что если последовательность Коши (x_n) сходится к элементу x из R (т. е. если $\nu_{\mathfrak{p}}(x-x_n)$ неограниченно возрастает при $n\to\infty$), то $x=\lim\limits_{n\to\infty}x_n$. Действительно, положим $\bar{x}=\lim\limits_{n\to\infty}x_n$, тогда $\nu_{\mathfrak{p}}(\bar{x}-x)\geqslant\min\{\nu_{\mathfrak{p}}(\bar{x}-x_n),\ \nu_{\mathfrak{p}}(x-x_n)\}$. Так как $\nu_{\mathfrak{p}}(\bar{x}-x_n)$ и $\nu_{\mathfrak{p}}(x-x_n)$ одновременно неограниченно возрастают при $n\to\infty$, то $\nu_{\mathfrak{p}}(\bar{x}-x)=\infty$, откуда $\bar{x}=x$.

Далее, для любого элемента $\bar{x}$ из $\bar{R}_{\mathfrak{p}}$ и любого целого числа a всегда можно найти такой элемент $x\in R$, что $\nu_{\mathfrak{p}}(\bar{x}-x)\geqslant a$. Если мы возьмем $\bar{x}$ из $\bar{\mathfrak{o}}$ и $a>0$, то $\nu_{\mathfrak{p}}(x)\geqslant\min\{a,\ \nu_{\mathfrak{p}}(\bar{x})\}\geqslant 0$. Отсюда следует, что элементы из $\bar{\mathfrak{o}}$ характеризуются тем, что они могут быть представлены как пределы последовательностей Коши с элементами из $\mathfrak{o}$. Полагая, в частности, $a=1$, получаем, что каждый элемент из $\bar{\mathfrak{o}}$ по модулю $\bar{\mathfrak{p}}$ сравним с некоторым элементом из $\mathfrak{o}$. Это означает, что *поле вычетов* $\bar{\mathfrak{o}}/\bar{\mathfrak{p}}$ *можно отождествить с полем вычетов* $\mathfrak{o}/\mathfrak{p}$ *точки* $\mathfrak{p}$. Если $\bar{x}\in\bar{\mathfrak{o}}$, то класс вычетов элемента $\bar{x}$ по модулю $\bar{\mathfrak{p}}$ в дальнейшем иногда будем называть также классом вычетов элемента $\bar{x}$ по модулю $\mathfrak{p}$.

Естественно говорить, что последовательность $(\bar{x}_n)$ элементов из $\bar{R}_{\mathfrak{p}}$ является последовательностью Коши, если

$\nu_{\mathfrak{p}}(\bar{x}_{n+1}-\bar{x}_n)$ неограниченно возрастает при $n\to\infty$, а также что $(\bar{x}_n)$ сходится к элементу $\bar{x}\in\bar{R}_{\mathfrak{p}}$, если $\nu_{\mathfrak{p}}(\bar{x}-\bar{x}_n)$ неограниченно возрастает при $n\to\infty$. Утверждаем, что *каждая последовательность Коши с элементами из $\bar{R}_{\mathfrak{p}}$ сходится к некоторому элементу поля $\bar{R}_{\mathfrak{p}}$*. В самом деле, пусть $(\bar{x}_n)$ — последовательность Коши. Для каждого n в поле R можно найти такой элемент x_n, что $\nu_{\mathfrak{p}}(\bar{x}_n-x_n)\geqslant n$. Имеем: $x_{n+1}-x_n=(x_{n+1}-\bar{x}_{n+1})+(\bar{x}_{n+1}-\bar{x}_n)+(\bar{x}_n-x_n)$, откуда

$$\nu_{\mathfrak{p}}(x_{n+1}-x_n)\geqslant\min\{n,\ \nu_{\mathfrak{p}}(\bar{x}_{n+1}-\bar{x}_n)\}.$$

Следовательно, $\nu_{\mathfrak{p}}(x_{n+1}-x_n)$ неограниченно возрастает при $n\to\infty$, т. е. (x_n) есть последовательность Коши с элементами из R. Положим $\bar{x}=\lim\limits_{n\to\infty}x_n$, тогда $\bar{x}-\bar{x}_n=(\bar{x}-x_n)+(x_n-\bar{x}_n)$ и $\nu_{\mathfrak{p}}(\bar{x}-\bar{x}_n)\geqslant\min\{\nu_{\mathfrak{p}}(\bar{x}-x_n),\ n\}$. Так как $\nu_{\mathfrak{p}}(\bar{x}-x_n)$ неограниченно возрастает при $n\to\infty$, то это же справедливо и для $\nu_{\mathfrak{p}}(\bar{x}-\bar{x}_n)$. Этим доказано, что последовательность $(\bar{x}_n)$ сходится к $\bar{x}$.

Имея в виду только что доказанное свойство, говорят, что $\bar{R}_{\mathfrak{p}}$ есть *полное поле*. Поле $\bar{R}_{\mathfrak{p}}$ называется *$\mathfrak{p}$-адическим пополнением* поля R.

Если последовательность $(\bar{x}_n)$ элементов поля $\bar{R}_{\mathfrak{p}}$ сходится к элементу $\bar{x}$, то будем писать $\bar{x}=\lim\limits_{n\to\infty}\bar{x}_n$. Легко видеть, что если $\bar{x}=\lim\limits_{n\to\infty}\bar{x}_n$, $\bar{y}=\lim\limits_{n\to\infty}\bar{y}_n$, то $\bar{x}\pm\bar{y}=\lim\limits_{n\to\infty}(\bar{x}_n\pm\bar{y}_n)$, $\bar{x}\bar{y}=\lim\limits_{n\to\infty}(\bar{x}_n\bar{y}_n)$, а при $\bar{y}\neq0$ и $\bar{y}_n\neq0$ для всех n имеем также $\bar{y}^{-1}=\lim\limits_{n\to\infty}\bar{y}_n^{-1}$.

§ 2. Лемма Хензеля

Пусть $\mathfrak{p}$ — точка поля R алгебраических функций от одной переменной и пусть $\bar{R}_{\mathfrak{p}}$ — его $\mathfrak{p}$-адическое пополнение. Обозначим через $\bar{\mathfrak{o}}$ кольцо целых элементов поля $\bar{R}_{\mathfrak{p}}$, через $\bar{\mathfrak{p}}$ — идеал необратимых элементов кольца $\bar{\mathfrak{o}}$ и через Σ — поле вычетов $\bar{\mathfrak{o}}/\bar{\mathfrak{p}}$. Если $\bar{x}\in\bar{\mathfrak{o}}$, то через $\bar{x}^*$ будем

обозначать класс вычетов элемента $\bar{x}$ по модулю $\bar{\mathfrak{p}}$. Для многочлена $f(X)$ от X с коэффициентами из $\bar{R}_{\mathfrak{p}}$ через $\nu_{\mathfrak{p}}(f)$ обозначим наименьшее значение, принимаемое функцией порядка $\nu_{\mathfrak{p}}$ (продолженной на поле $\bar{R}_{\mathfrak{p}}$) на множестве коэффициентов многочлена f. Легко видеть, что для двух многочленов f и g от X с коэффициентами из $\bar{R}_{\mathfrak{p}}$ имеют место неравенства

$$\nu_{\mathfrak{p}}(f \pm g) \geqslant \min\{\nu_{\mathfrak{p}}(f),\ \nu_{\mathfrak{p}}(g)\};\quad \nu_{\mathfrak{p}}(fg) \geqslant \nu_{\mathfrak{p}}(f) + \nu_{\mathfrak{p}}(g).$$

Для многочлена f с коэффициентами из $\bar{\mathfrak{o}}$ через f^* обозначим многочлен с коэффициентами из Σ, получающийся из f заменой всех его коэффициентов соответствующими классами вычетов по модулю $\bar{\mathfrak{p}}$. Отображение $f \to f^*$ является гомоморфизмом кольца $\bar{\mathfrak{o}}[X]$ на $\Sigma[X]$.

Лемма 1 (лемма Хензеля). *Пусть f — многочлен с коэффициентами из $\bar{\mathfrak{o}}$. Предположим, что $f^* = \varphi\psi \neq 0$, где φ и ψ — взаимно простые многочлены с коэффициентами из Σ. Тогда существуют многочлены g и h с коэффициентами из $\bar{\mathfrak{o}}$ такие, что*

$$f = gh,$$

причем $g^* = \varphi$, $h^* = \psi$ и степень многочлена g равна степени многочлена φ.

Через $\partial^\circ\theta$ будем обозначать степень многочлена $\theta \neq 0$. Легко видеть, что существуют многочлены g_1 и h_1 с коэффициентами из $\bar{\mathfrak{o}}$, удовлетворяющие следующим условиям: $g_1^* = \varphi$, $h_1^* = \psi$, $\partial^\circ g_1 = \partial^\circ\varphi$, $\partial^\circ h_1 = \partial^\circ\psi$, $\nu_{\mathfrak{p}}(f - g_1h_1) \geqslant 1$; в самом деле, многочлены g_1 и h_1, удовлетворяющие первым четырем условиям, необходимо будут удовлетворять и последнему условию, ибо $f^* = \varphi\psi$. Предположим, что для некоторого целого $n > 0$ уже определены многочлены $g_1, \ldots, g_n, h_1, \ldots, h_n$ с коэффициентами из $\bar{\mathfrak{o}}$, удовлетворяющие условиям:

1) $g_n^* = \varphi$; $h_n^* = \psi$;

2) $\partial^\circ g_n = \partial^\circ\varphi$, $\partial^\circ h_n \leqslant \partial^\circ f - \partial^\circ g_n$;

3) $\nu_{\mathfrak{p}}(f - g_nh_n) \geqslant n$;

4) $\nu_{\mathfrak{p}}(g_{k+1} - g_k) \geqslant k$, $\nu_{\mathfrak{p}}(h_{k+1} - h_k) \geqslant k$ $(1 \leqslant k \leqslant n-1)$.

Выберем в $\bar{\mathfrak{o}}$ элемент t, для которого $\nu_{\mathfrak{p}}(t)=1$. Тогда коэффициенты многочлена $\zeta=t^{-n}(f-g_nh_n)$ принадлежат $\bar{\mathfrak{o}}$. Так как φ и ψ взаимно просты, то, как известно, существуют такие многочлены $\lambda(X)$ и $\mu(X)$ с коэффициентами из Σ, что $\zeta^*=\lambda\varphi+\mu\psi$. Многочлены λ и μ этим равенством определены неоднозначно: они могут быть заменены на $\lambda-\chi\psi$ и $\mu+\chi\varphi$ соответственно, где χ — произвольный многочлен с коэффициентами из Σ. Выбирая надлежащим образом многочлен χ, можно добиться, чтобы степень многочлена μ была меньше степени многочлена φ (или, возможно, $\mu=0$). Выбрав таким образом многочлены λ и μ, найдем многочлены $l(X)$ и $m(X)$ с коэффициентами из $\bar{\mathfrak{o}}$ так, чтобы $l^*=\lambda$, $m^*=\mu$, при этом мы можем предполагать, что $\partial^\circ m<\partial^\circ\varphi$ (или $m=0$) и $\partial^\circ l=\partial^\circ\lambda$ (или $l=0$). Положим $g_{n+1}=g_n+t^nm$, $h_{n+1}=h_n+t^nl$. Очевидно, что

$$g^*_{n+1}=\varphi,\ h^*_{n+1}=\psi,\ \partial^\circ g_{n+1}=\partial^\circ\varphi,$$

$$\nu_{\mathfrak{p}}(g_{n+1}-g_n)\geqslant n,\ \nu_{\mathfrak{p}}(h_{n+1}-h_n)\geqslant n.$$

Имеем теперь $f-g_{n+1}h_{n+1}=t^n(\zeta-(lg_n+mh_n)-t^nlm)$. Так как $\zeta^*=\lambda\varphi+\mu\psi$, то $\nu_{\mathfrak{p}}(\zeta-(lg_n+mh_n))\geqslant 1$, поэтому

$$\nu_{\mathfrak{p}}(f-g_{n+1}h_{n+1})\geqslant n+1.$$

Остается проверить, что $\partial^\circ h_{n+1}\leqslant\partial^\circ f-\partial^\circ g_{n+1}$. Так как $\partial^\circ h_n\leqslant\partial^\circ f-\partial^\circ g_n$, то $\partial^\circ\zeta\leqslant\partial^\circ f$. С другой стороны, из равенства $\varphi\psi=f^*$ следует, что $\partial^\circ\psi=\partial^\circ f^*-\partial^\circ\varphi\leqslant\partial^\circ f-\partial^\circ\varphi$, откуда $\partial^\circ\mu\psi<\partial^\circ f$ (если $\mu\neq 0$) и, далее, $\partial^\circ\lambda\varphi\leqslant\partial^\circ f$ (если $\lambda\neq 0$), а значит $\partial^\circ\lambda\leqslant\partial^\circ f-\partial^\circ\varphi$ и $\partial^\circ l\leqslant\partial^\circ f-\partial^\circ\varphi=\partial^\circ f-\partial^\circ g_n$. Но $h_{n+1}=h_n+t^nl$, причем степени многочленов h_n и l не превосходят $\partial^\circ f-\partial^\circ g_n$, поэтому $\partial^\circ h_{n+1}\leqslant\partial^\circ f-\partial^\circ g_n=$ $=\partial^\circ f-\partial^\circ g_{n+1}$.

Продолжая наш процесс до бесконечности, мы получим две последовательности многочленов (g_n) и (h_n), для которых будут выполнены условия 1) — 4) при всех n.

Обозначим через a и b степени многочленов f и φ соответственно. Тогда мы можем записать

$$g_n=\sum_{i=0}^{b}\gamma_{i,n}X^i,\quad h_n=\sum_{j=0}^{a-b}\delta_{j,n}X^j,$$

где элементы $\gamma_{i,n}$ и $\delta_{j,n}$ принадлежат $\bar{\mathfrak{o}}$. Так как $\nu_{\mathfrak{p}}(\gamma_{i,n+1}-\gamma_{i,n})\geqslant n$ и $\nu_{\mathfrak{p}}(\delta_{j,n+1}-\delta_{j,n})\geqslant n$, то после-

довательности $(\gamma_{i,n})$ и $(\delta_{j,n})$ (при $0 \leqslant i \leqslant b$, $0 \leqslant j \leqslant a-b$) являются последовательностями Коши. В силу полноты поля $\bar{R}_{\mathfrak{p}}$ эти последовательности сходятся к некоторым элементам γ_i и δ_j, которые, очевидно, также принадлежат $\bar{\mathfrak{o}}$. Положим

$$g = \sum_{i=0}^{b} \gamma_i X^i, \qquad h = \sum_{j=0}^{a-b} \delta_j X^j.$$

Так как $\nu_{\mathfrak{p}}(\gamma_i - \gamma_{i,1}) \geqslant 1$ и $\nu_{\mathfrak{p}}(\delta_j - \delta_{j,1}) \geqslant 1$, то $g^* = \varphi$ и $h^* = \psi$. Так как $\partial^\circ \varphi = b$ и $\partial^\circ g \leqslant b$, то из равенства $g^* = \varphi$ следует, что $\partial^\circ g = \partial^\circ \varphi$. Имеем $f - gh = (f - g_n h_n) - (gh - g_n h_n)$. Легко видеть, что $\nu_{\mathfrak{p}}(gh - g_n h_n)$ неограниченно возрастает при $n \to \infty$; с другой стороны, $\nu_{\mathfrak{p}}(f - g_n h_n) \geqslant n$. Отсюда следует, что $\nu_{\mathfrak{p}}(f - gh) = \infty$, т. е. $f = gh$. Лемма Хензеля, таким образом, доказана.

§ 3. Структура $\mathfrak{p}$-адических пополнений

Пусть $\mathfrak{p}$ — точка поля R алгебраических функций от одной переменной, K — его поле констант и Σ — поле вычетов в точке $\mathfrak{p}$. Пусть, далее, $\bar{R}$ — $\mathfrak{p}$-адическое пополнение поля R, $\bar{\mathfrak{o}}$ — кольцо целых элементов поля $\bar{R}$ и $\bar{\mathfrak{p}}$ — идеал, состоящий из необратимых элементов кольца $\bar{\mathfrak{o}}$. Как нам уже известно, поле $\bar{\mathfrak{o}}/\bar{\mathfrak{p}}$ может быть отождествлено с полем Σ. Пусть Σ' есть произвольное подмножество поля Σ. Будем говорить, что подмножество $\bar{\Sigma}'$ поля $\bar{R}$ является *системой представителей для* Σ', если оно содержится в $\bar{\mathfrak{o}}$ и при естественном гомоморфизме $\bar{\mathfrak{o}}$ на $\Sigma = \bar{\mathfrak{o}}/\bar{\mathfrak{p}}$ отображается взаимно однозначно на Σ'.

Теорема 1. *Сохраняя вышеизложенные обозначения, положим дополнительно, что Σ_s есть подполе сепарабельных над K элементов поля Σ. Тогда в $\bar{R}$ существует подполе $\bar{\Sigma}_s$, содержащее поле K и являющееся системой представителей для элементов поля Σ_s. Этими двумя условиями поле $\bar{\Sigma}_s$ определено однозначно.*

Так как Σ_s есть сепарабельное расширение поля K конечной степени, то $\Sigma_s = K\langle\alpha^*\rangle$, где α^* — некоторый эле-

мент из Σ_s. Этот элемент является корнем неприводимого многочлена $f(X)$ с коэффициентами из K. В поле Σ_s имеет место разложение: $f(X)=(X-\alpha^*)g(X)$. Так как Σ_s сепарабельно над K, то $g(\alpha^*)\neq 0$, т. е. многочлены $X-\alpha^*$ и $g(X)$ взаимно просты.

Многочлен f мы можем рассматривать как многочлен с коэффициентами из $\bar{\mathfrak{o}}$. Применяя лемму Хензеля, получаем, что f обладает множителем первой степени, скажем $aX+b$, с коэффициентами из $\bar{\mathfrak{o}}$ таким, что классы вычетов элементов a и b по модулю $\mathfrak{p}$ равны 1 и $-\alpha^*$ соответственно. Отсюда следует, что элемент $\alpha=-\dfrac{b}{a}$ является целым и принадлежит классу вычетов α^*. Так как $f(\alpha)=0$, то элемент α алгебраичен над K, и каждый элемент из $K\langle\alpha\rangle$ есть линейная комбинация элементов $1, \alpha, \ldots, \alpha^{d-1}$ с коэффициентами из K (где d — степень многочлена f). Так как элементы $1, \alpha^*, \ldots, (\alpha^*)^{d-1}$ линейно независимы над K, то поле $K\langle\alpha\rangle$ является системой представителей для Σ_s. Пусть теперь $\bar{\Sigma}_s'$ — произвольное подполе поля $\bar{R}$, содержащее K и являющееся системой представителей для элементов поля Σ_s. Пусть α' есть элемент из $\bar{\Sigma}_s'$, принадлежащий классу вычетов α^*. Так как $\Sigma_s=K[\alpha^*]$, то, очевидно, $\bar{\Sigma}_s'=K[\alpha']=K\langle\alpha'\rangle$. Элемент $f(\alpha')$ принадлежит классу вычетов $f(\alpha^*)=0$, поэтому $f(\alpha')=0$. Далее, мы имеем $f(X)=(aX+b)\bar{g}(X)$, где $\bar{g}$ — многочлен с коэффициентами из $\bar{\mathfrak{o}}$, откуда следует, что $(a\alpha'+b)\bar{g}(\alpha')=0$. Но $\bar{g}(\alpha')$ принадлежит классу вычетов $g(\alpha^*)$, который отличен от 0, поэтому $\bar{g}(\alpha')\neq 0$, а значит, $a\alpha'+b=0$, $\alpha=\alpha'$ и $\bar{\Sigma}_s'=K\langle\alpha\rangle$. Теорема 1, следовательно, доказана.

Пусть теперь x — произвольный элемент $\neq 0$ из поля R, для которого $\nu_{\mathfrak{p}}(x)>0$. Пусть нам задана последовательность $(c_k)_{r\leqslant k<\infty}$ элементов из $\bar{\Sigma}_s$, начинающаяся с члена c_r, где индекс r может быть отрицательным, равным нулю или положительным. Если мы положим $u_n=\sum_{k=r}^{n} c_k x^k$, то последовательность (u_n) будет, очевидно, последовательностью Коши в $\bar{R}$. Предел этой последовательности обозначается

через $\sum_{k=r}^{\infty} c_k x^k$. Из равенства

$$\sum_{k=r}^{\infty} c_k x^k = \sum_{k=r}^{\infty} c'_k x^k$$

следует, что $c_k = c'_k$ при всех $k \geqslant r$. В самом деле, допустим, что это не так. Тогда найдется наименьший индекс m, для которого $c_m \neq c'_m$, и мы будем иметь

$$\lim_{n \to \infty} \left((c'_m - c_m) x^m + \sum_{k=1}^{n} (c'_{m+k} - c_{m+k}) x^{m+k} \right) = 0.$$

Но $\nu_{\mathfrak{p}}((c'_m - c_m) x^m) = m\nu_{\mathfrak{p}}(x)$ и в то же время

$$\nu_{\mathfrak{p}}\left(\sum_{k=1}^{n} (c'_{m+k} - c_{m+k}) x^{m+k} \right) \geqslant (m+1)\nu_{\mathfrak{p}}(x);$$

следовательно, вышенаписанное равенство невозможно.

Каждый элемент вида $\sum_{k=r}^{\infty} c_k x^k$ можно записать также в виде $\sum_{k=s}^{\infty} c_k x^k$, где $s < r$ и $c_k = 0$ при $s \leqslant k < r$. Легко видеть, что

$$\sum_{k=r}^{\infty} c_k x^k - \sum_{k=r}^{\infty} c'_k x^k = \sum_{k=r}^{\infty} (c_k - c'_k) x^k,$$

$$\left(\sum_{k=r}^{\infty} c_k x^k \right) \left(\sum_{k=r'}^{\infty} c'_k x^k \right) = \sum_{l=r+r'}^{\infty} \left(\sum_{k+k'=l} c_k c'_{k'} \right) x^l.$$

Эти равенства показывают, что элементы вида $\sum_{k=r}^{\infty} c_k x^k$ образуют подполе поля $\overline{R}$, изоморфное полю формальных степенных рядов от x с коэффициентами из $\overline{\Sigma}_s$.

Рассмотрим теперь случай, когда поле вычетов Σ точки $\mathfrak{p}$ сепарабельно над K (т. е. $\Sigma = \Sigma_s$). Пусть тогда $\overline{\Sigma}$ есть подполе поля $\overline{R}$, содержащее K и являющееся системой представителей для элементов поля Σ. Выберем униформизирующую переменную x в точке $\mathfrak{p}$. Утверждается, что *тогда*

каждый элемент y из $\bar{R}$ *может быть представлен в виде* $\sum_{k=r}^{\infty} c_k x^k$. Мы можем, конечно, предполагать, что $y \neq 0$. Положим $r = \nu_{\mathfrak{p}}(y)$ и найдем надлежащую последовательность $(c_k)_{r \leqslant k < \infty}$ элементов поля $\bar{\Sigma}$. Очевидно, что $yx^{-r} \in \bar{\mathfrak{o}}$; в качестве c_r возьмем тот элемент из $\bar{\Sigma}$, который является представителем для класса вычетов элемента yx^{-r} по модулю $\bar{\mathfrak{p}}$. Ясно, что тогда $\nu_{\mathfrak{p}}(y - c_r x^r) > r$. Допустим, что элементы $c_r, \ldots, c_n$ уже определены так, что

$$\nu_{\mathfrak{p}}\left(y - \sum_{k=r}^{n} c_k x^k\right) > n.$$

Элемент $x^{-n-1}\left(y - \sum_{k=r}^{n} c_k x^k\right)$ — целый; в качестве c_{n+1} возьмем элемент из $\bar{\Sigma}$, сравнимый с элементом $x^{-n-1}\left(y - \sum_{k=r}^{n} c_k x^k\right)$ по модулю $\bar{\mathfrak{p}}$. Тогда будем иметь

$$\nu_{\mathfrak{p}}\left(y - \sum_{k=r}^{n+1} c_k x^k\right) > n + 1.$$

Этим определена последовательность (c_k), причем, очевидно, имеем $y = \sum_{k=r}^{\infty} c_k x^k$. Формула $y = \sum_{k=r}^{\infty} c_k x^k$ $\left(\text{или } y = \sum_{k=s}^{\infty} c_k x^k,\right.$ где $s < r$ и $c_k = 0$ при $\left.s \leqslant k < r\right)$ носит название *разложения элемента* y *по степеням* x *в* $\mathfrak{p}$*-адическом пополнении поля* R.

Замечание. В случае, когда поле Σ несепарабельно над K, в поле $\bar{R}$ также всегда существует подполе $\bar{\Sigma}$, являющееся системой представителей для элементов поля Σ. Мы не будем здесь доказывать это утверждение. Помимо того, что доказательство его довольно сложно, полезность результата незначительна в силу следующих обстоятельств: 1) поле $\bar{\Sigma}$, вообще говоря, не единственно; 2) не всегда поле $\bar{\Sigma}$ можно выбрать так, чтобы оно содержало поле констант K поля R, что мы покажем на примере.

Пусть K — несовершенное поле характеристики $p > 0$, и пусть a — элемент поля K, не являющийся p-ой степенью в K. Положим $R = K\langle x\rangle$, где элемент x трансцендентен над K. Многочлен $x^p - a$ неприводим в $K[x]$; значит, он определяет точку $\mathfrak{p}$ поля $K\langle x\rangle$. Поле вычетов Σ точки $\mathfrak{p}$ имеет вид $K\langle\xi\rangle$, где элемент ξ удовлетворяет условию $\xi^p = a$. Покажем, что элемент a не является p-ой степенью и в $\mathfrak{p}$-адическом пополнении $\overline{R}$ поля R. В самом деле, допустим, что $a = y^p$, $y \in \overline{R}$. Тогда мы имели бы $(y - x)^p = a - x^p$, откуда $p\nu_{\mathfrak{p}}(y - x) = 1$, что, однако, невозможно. Отсюда непосредственно следует, что никакое подполе поля $\overline{R}$, содержащее K, не может быть системой представителей для элементов поля Σ.

§ 4. Обобщение понятия распределения

Пусть R — поле алгебраических функций от одной переменной и K — его поле констант. Каждой точке $\mathfrak{p}$ поля R соответствует $\mathfrak{p}$-адическое пополнение $\overline{R}_{\mathfrak{p}}$ поля R. Распределение поля R было определено нами как отображение $\mathfrak{x}$, сопоставляющее каждой точке $\mathfrak{p}$ поля R элемент $\mathfrak{x}(\mathfrak{p})$ из R так, что $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p})) \geqslant 0$ почти для всех $\mathfrak{p}$. Для удобства изложения представляется целесообразным ввести обобщение этого понятия, допуская к рассмотрению значения $\mathfrak{x}(\mathfrak{p})$ из $\mathfrak{p}$-адического пополнения $\overline{R}_{\mathfrak{p}}$ поля R. Таким образом, в дальнейшем под *распределением* мы будем понимать отображение $\mathfrak{x}$, сопоставляющее каждой точке $\mathfrak{p}$ поля R элемент $\mathfrak{x}(\mathfrak{p})$ из $\overline{R}_{\mathfrak{p}}$ так, что выполнено условие $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p})) \geqslant 0$ почти для всех $\mathfrak{p}$ (здесь $\nu_{\mathfrak{p}}$ обозначает продолжение функции порядка в точке $\mathfrak{p}$ на поле $\overline{R}_{\mathfrak{p}}$). Элемент $\mathfrak{x}(\mathfrak{p})$ называется $\mathfrak{p}$-*компонентой* распределения $\mathfrak{x}$. По определению полагаем $\nu_{\mathfrak{p}}(\mathfrak{x}) = \nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p}))$.

Распределения в новом смысле также образуют кольцо, в котором операции определены формулами $(\mathfrak{x} + \mathfrak{y})(\mathfrak{p}) = \mathfrak{x}(\mathfrak{p}) + \mathfrak{y}(\mathfrak{p})$, $(\mathfrak{x}\mathfrak{y})(\mathfrak{p}) = \mathfrak{x}(\mathfrak{p})\mathfrak{y}(\mathfrak{p})$. Это кольцо содержит все распределения в старом смысле в качестве подкольца. В частности, оно содержит в качестве подкольца поле R, поэтому его также можно рассматривать, как векторное пространство над полем K.

Пусть $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$ — дивизор. Перенесем понятие сравнения по модулю $\mathfrak{a}$ на наши новые распределения. Будем говорить, что распределения $\mathfrak{x}$ и $\mathfrak{y}$ сравнимы между собой по модулю $\mathfrak{a}$, если $\nu_{\mathfrak{p}}(\mathfrak{x} - \mathfrak{y}) \geqslant m(\mathfrak{p})$ для каждой точки $\mathfrak{p}$.

Для любого распределения $\mathfrak{x}$ в нашем новом смысле и для любого дивизора $\mathfrak{a}$ всегда существует такое распределение $\mathfrak{x}'$ в старом смысле, что $\mathfrak{x} \equiv \mathfrak{x}' \pmod{\mathfrak{a}}$. Действительно, пусть $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$. Для каждой точки $\mathfrak{p}$ мы можем найти такой элемент $x(\mathfrak{p})$ из R, что $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p}) - x(\mathfrak{p})) \geqslant m(\mathfrak{p})$. Так как $\nu_{\mathfrak{p}}(x(\mathfrak{p})) \geqslant \min\{\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p})), m(\mathfrak{p})\}$, то $\nu_{\mathfrak{p}}(x(\mathfrak{p})) \geqslant 0$ почти для всех $\mathfrak{p}$. Следовательно, отображение $\mathfrak{p} \to x(\mathfrak{p})$ является распределением $\mathfrak{x}'$ в старом смысле, при этом, очевидно, имеем $\mathfrak{x} \equiv \mathfrak{x}' \pmod{\mathfrak{a}}$.

Пусть $\mathfrak{a}$ и $\mathfrak{a}'$ — два дивизора, причем $\mathfrak{a}$ делится на $\mathfrak{a}'$. Обозначим через $\mathfrak{X}(\mathfrak{a})$ и $\mathfrak{X}(\mathfrak{a}')$ пространства распределений в старом смысле, сравнимых с 0 по модулю $\mathfrak{a}$ и по модулю $\mathfrak{a}'$ соответственно, а через $\mathfrak{X}^*(\mathfrak{a})$ и $\mathfrak{X}^*(\mathfrak{a}')$ — пространства распределений в новом смысле, удовлетворяющих соответственно тем же условиям. Если $\mathfrak{x}^* \in \mathfrak{X}^*(\mathfrak{a}')$, то мы можем найти такое распределение $\mathfrak{x}$ в старом смысле, что $\mathfrak{x} \equiv \mathfrak{x}^* \pmod{\mathfrak{a}}$. Так как $\mathfrak{a}'$ является делителем дивизора $\mathfrak{a}$, то $\mathfrak{x} \in \mathfrak{X}(\mathfrak{a}')$; следовательно, мы имеем $\mathfrak{X}^*(\mathfrak{a}') = \mathfrak{X}(\mathfrak{a}') + \mathfrak{X}^*(\mathfrak{a})$. Согласно теореме об изоморфизме пространство $\mathfrak{X}^*(\mathfrak{a}')/\mathfrak{X}^*(\mathfrak{a})$ изоморфно $\mathfrak{X}(\mathfrak{a}')/(\mathfrak{X}(\mathfrak{a}') \cap \mathfrak{X}^*(\mathfrak{a})) = \mathfrak{X}(\mathfrak{a}')/\mathfrak{X}(\mathfrak{a})$. В силу леммы 1 § 4 гл. II получаем, что *размерность пространства $\mathfrak{X}^*(\mathfrak{a}')/\mathfrak{X}^*(\mathfrak{a})$ над полем K конечна и равна $d(\mathfrak{a}) - d(\mathfrak{a}')$*. Таким образом, мы видим, что полученный нами ранее результат остается справедливым и для распределений в новом смысле.

Пусть теперь ω — дифференциал поля R. Покажем, что дифференциал ω может быть естественным образом продолжен до линейной функции на пространстве распределений в новом смысле. Если $\omega = 0$, то продолжением будет, конечно, нулевая функция. Пусть $\omega \neq 0$ и пусть $\mathfrak{x}$ есть произвольное распределение в новом смысле. Найдем распределение $\mathfrak{x}'$ в старом смысле такое, что $\mathfrak{x} \equiv \mathfrak{x}' \left(\mathrm{mod}\, (\mathfrak{d}(\omega))^{-1}\right)$. Если $\mathfrak{x}'$ и $\mathfrak{x}''$ — два распределения в старом смысле, удовлетворяющие последнему условию, то $\mathfrak{x}' \equiv \mathfrak{x}'' \left(\mathrm{mod}\, (\mathfrak{d}(\omega))^{-1}\right)$ и, следовательно, $\omega(\mathfrak{x}') = \omega(\mathfrak{x}'')$. Поэтому можно положить $\omega(\mathfrak{x}) = \omega(\mathfrak{x}')$. Функция ω, продолженная нами на пространство

распределений в новом смысле, является, очевидно, линейной. Легко видеть, что теорема 2 § 5 гл. II остается справедливой, если в ней под $\mathfrak{x}$ понимать распределение в новом смысле.

Пусть $\mathfrak{p}$ — точка поля R. Так же как и в § 7 гл. II под $\mathfrak{p}$-компонентой дифференциала ω понимаем функцию $\omega^{\mathfrak{p}}$, определенную формулой

$$\omega^{\mathfrak{p}}(\mathfrak{x}) = \omega(\mathfrak{x}^{\mathfrak{p}}),$$

где $\mathfrak{x}^{\mathfrak{p}}$ есть распределение, сопоставляющее точке $\mathfrak{p}$ значение $\mathfrak{x}(\mathfrak{p})$, а всем другим точкам — значение 0. Функция $\omega^{\mathfrak{p}}$ является продолжением на пространство распределений в новом смысле $\mathfrak{p}$-компоненты дифференциала ω, введенной нами в § 7 гл. II. Очевидно, что функцию $\omega^{\mathfrak{p}}$ можно рассматривать как линейную функцию на $\overline{R}_{\mathfrak{p}}$. Легко видеть также, что леммы 1 и 2 § 7 гл. II справедливы и при новом понимании распределения и дифференциала. Заметим, что в утверждении леммы 2 § 7 гл. II слова „при всех $x \in R$" можно заменить словами „при всех $x \in \overline{R}_{\mathfrak{p}}$".

§ 5. Вычеты дифференциала

Пусть R — поле алгебраических функций от одной переменной и пусть K — его поле констант. Пусть далее ω — дифференциал поля R; $\mathfrak{p}$ — точка поля R; Σ — поле вычетов точки $\mathfrak{p}$; Σ_s — поле, состоящее из тех элементов поля Σ, которые сепарабельны над K; $\overline{R}$ — $\mathfrak{p}$-адическое пополнение поля R; $\overline{\Sigma}_s$ — подполе поля $\overline{R}$, содержащее K и являющееся системой представителей для элементов поля Σ_s (теорема 1 § 3).

$\mathfrak{p}$-компоненту $\omega^{\mathfrak{p}}$ дифференциала ω можно рассматривать как функцию на $\overline{R}$ со значениями в K. Эта функция индуцирует некоторую функцию на $\overline{\Sigma}_s$. Через $\overline{\xi}$ будет обозначаться представитель из класса вычетов $\xi \in \Sigma$, принадлежащий $\overline{\Sigma}_s$, а через $\omega^{\mathfrak{p}}(\xi)$ — элемент $\omega^{\mathfrak{p}}(\overline{\xi})$. Таким образом, $\mathfrak{p}$-компоненте $\omega^{\mathfrak{p}}$ дифференциала ω мы сопоставили функцию на Σ_s со значениями в K. Очевидно, что эта функция линейна, если поле Σ_s рассматривать как векторное пространство над K.

Лемма 1. *Пусть K — поле, а L — конечное сепарабельное расширение поля K. Если L рассматривать как векторное пространство над полем K, то всякая линей-*

ная функция на L имеет вид $\xi \to \mathrm{Sp}_{L/K}\xi\rho$, где ρ — однозначно определенный элемент из L.

Если $\rho \in L$, то через λ_ρ обозначим линейную функцию, определенную равенством $\lambda_\rho(\xi) = \mathrm{Sp}_{L/K}\xi\rho$. Отображение $\rho \to \lambda_\rho$ есть линейное отображение пространства L в пространство L^* линейных функций на L. Так как L сепарабельно над K, то существует такой элемент $\gamma \in L$, что $\mathrm{Sp}_{L/K}\gamma \neq 0$; если $\rho \neq 0$, то $\lambda_\rho(\gamma\rho^{-1}) \neq 0$, откуда $\lambda_\rho \neq 0$. Это означает, что отображение $\rho \to \lambda_\rho$ взаимно однозначно. Так как размерности пространств L и L^* равны, то каждый элемент из L^* может быть записан одним и только одним способом в виде λ_ρ, что и доказывает лемму 1.

Возвращаясь к указанным выше обозначениям, мы видим, что в поле Σ_s существует однозначно определенный элемент ρ такой, что $\omega^{\mathfrak{p}}(\xi) = \mathrm{Sp}_{\Sigma_s/K}\xi\rho$ при всех $\xi \in \Sigma_s$. Этот элемент называется *вычетом* дифференциала ω в точке $\mathfrak{p}$ и обозначается через $\mathrm{res}_{\mathfrak{p}}\,\omega$.

Очевидно, что отображение $\omega \to \mathrm{res}_{\mathfrak{p}}\,\omega$ есть линейное отображение пространства дифференциалов (рассматриваемого как векторное пространство над полем K) в поле Σ_s. Из определения непосредственно следует, что

$$\omega^{\mathfrak{p}}(1) = \mathrm{Sp}_{\Sigma_s/K}(\mathrm{res}_{\mathfrak{p}}\omega). \tag{1}$$

В частности, если поле вычетов точки $\mathfrak{p}$ чисто несепарабельно над K, то $\mathrm{res}_{\mathfrak{p}}\,\omega = \omega^{\mathfrak{p}}(1)$.

Теорема 2. *Пусть ω есть дифференциал поля R алгебраических функций от одной переменной. Если точка $\mathfrak{p}$ поля R не является полюсом дифференциала ω, то $\mathrm{res}_{\mathfrak{p}}\,\omega = 0$. Если точка $\mathfrak{p}$ такова, что, во-первых, ее поле вычетов сепарабельно над полем констант поля R, во-вторых, $\mathrm{res}_{\mathfrak{p}}\,\omega = 0$, и, в третьих, $\nu_{\mathfrak{p}}(\omega) \geqslant -1$, то эта точка $\mathfrak{p}$ не является полюсом дифференциала ω.*

Если $\mathfrak{p}$ не является полюсом дифференциала ω, то $\omega^{\mathfrak{p}}(x) = 0$ для любого целого элемента x из $\bar{R}$, в частности, для любого элемента из $\bar{\Sigma}_s$, откуда и следует, что $\mathrm{res}_{\mathfrak{p}}\,\omega = 0$. Если $\mathrm{res}_{\mathfrak{p}}\,\omega = 0$, то $\omega^{\mathfrak{p}}(\bar{\xi}) = 0$ для любого элемента $\bar{\xi} \in \bar{\Sigma}_s$. Если теперь Σ сепарабельно над K, то каждый целый элемент из $\bar{R}$ сравним по модулю $\bar{\mathfrak{p}}$ с некоторым элементом из $\bar{\Sigma}_s$. Если $\nu_{\mathfrak{p}}(\omega) \geqslant -1$, то $\omega^{\mathfrak{p}}(y) = 0$ для всех элементов $y \in \bar{R}$,

удовлетворяющих условию $\nu_{\mathfrak{p}}(y) > 0$; отсюда следует, что $\omega^{\mathfrak{p}}(x) = \omega^{\mathfrak{p}}(x')$, если только целые элементы x и x' из $\overline{R}$ сравнимы между собой по модулю $\overline{\mathfrak{p}}$. Таким образом, если выполнены условия второй части теоремы 2, то $\omega^{\mathfrak{p}}(x) = 0$ для любого целого элемента из $\overline{R}$, откуда $\nu_{\mathfrak{p}}(\omega) \geqslant 0$.

Из теоремы 2, в частности, следует, что каждый дифференциал имеет только конечное число вычетов, отличных от 0.

Теорема 3. *Пусть ω есть дифференциал поля R алгебраических функций от одной переменной, и пусть K — его поле констант. Для каждой точки $\mathfrak{p}$ поля R через $\Sigma_s(\mathfrak{p})$ обозначим поле, состоящее из тех элементов поля вычетов точки $\mathfrak{p}$, которые сепарабельны над K. Тогда имеет место равенство*

$$\sum_{\mathfrak{p}} \mathrm{Sp}_{\Sigma_s(\mathfrak{p})/K} \operatorname{res}_{\mathfrak{p}} \omega = 0.$$

В силу равенства $0 = \omega(1) = \sum_{\mathfrak{p}} \omega^{\mathfrak{p}}(1)$, теорема 3 непосредственно вытекает из вышеприведенной формулы (1).

Следствие. *Если R есть поле алгебраических функций от одной переменной над алгебраически замкнутым полем констант, то сумма вычетов любого дифференциала поля R равна* 0.

Это вытекает непосредственно из теоремы 3.

Лемма 2. *Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ — конечное множество различных точек поля R алгебраических функций от одной переменной. Пусть для каждого i $(1 \leqslant i \leqslant h)$ задано линейное отображение μ_i поля вычетов Σ_i точки $\mathfrak{p}_i$ в поле констант K поля R. Если $\sum_{i=1}^{h} \mu_i(1) = 0$, то существует дифференциал ω поля R, удовлетворяющий следующим условиям:* 1) *ω делится на $(\mathfrak{p}_1 \ldots \mathfrak{p}_h)^{-1}$ и* 2) *для любого целого в точке $\mathfrak{p}_i$ элемента x_i поля R имеет место равенство $\omega^{\mathfrak{p}_i}(x_i) = \mu_i(\xi_i)$, где ξ_i есть значение, принимаемое элементом x_i в точке $\mathfrak{p}_i$.*

Пусть $\mathfrak{D}$ — пространство дифференциалов, делящихся на $(\mathfrak{p}_1 \ldots \mathfrak{p}_h)^{-1}$. Если $h \geqslant 1$ (что мы предполагаем), то размерность пространства элементов поля R, делящихся на $\mathfrak{p}_1 \ldots \mathfrak{p}_h$, равна 0; в силу теоремы Римана — Роха от-

сюда следует, что размерность пространства $\mathfrak{D}$ равна $\sum_{i=1}^{h} d(\mathfrak{p}_i)+g-1$, где g—род поля R. Если $\omega \in \mathfrak{D}$ и $\nu_{\mathfrak{p}_i}(x_i) \geqslant 0$, то $\omega^{\mathfrak{p}_i}(x_i)$ зависит только от значения ξ_i, принимаемого элементом x_i в точке $\mathfrak{p}_i$ (ибо, если $\nu_{\mathfrak{p}_i}(x_i'-x_i)>0$, то $\omega^{\mathfrak{p}_i}(x_i'-x_i)=0$). Положим $\omega^{\mathfrak{p}_i}(x_i)=\lambda_{i,\omega}(\xi_i)$. Ясно, что $\lambda_{i,\omega}$ является линейной функцией на Σ_i (если Σ_i рассматривать как векторное пространство над K). Обозначим через Σ_i^* пространство линейных функций на Σ_i и рассмотрим векторное пространство $\prod_{i=1}^{h} \Sigma_i^*$ (произведение векторных пространств Σ_i^* $(1 \leqslant i \leqslant h)$). Если каждому дифференциалу $\omega \in \mathfrak{D}$ мы сопоставим элемент $\Lambda(\omega)=(\lambda_{1,\omega}, \ldots, \lambda_{h,\omega})$ из этого прямого произведения, то получим линейное отображение Λ пространства $\mathfrak{D}$ в $\prod_{i=1}^{h} \Sigma_i^*$. Так как при $\omega \in \mathfrak{D}$ имеем

$$0=\omega(1)=\sum_{i=1}^{h} \omega^{\mathfrak{p}_i}(1)=\sum_{i=1}^{h} \lambda_{i,\omega}(1),$$

то Λ отображает $\mathfrak{D}$ в подпространство P пространства $\prod \Sigma_i^*$, состоящее из тех элементов $(\lambda_1, \ldots, \lambda_h)$, для которых $\sum_{i=1}^{h} \lambda_i(1)=0$. Если $\lambda_{i,\omega}=0$, то $\omega^{\mathfrak{p}_i}(x_i)=0$ при всех целых в точке $\mathfrak{p}_i$ элементах $x_i \in R$, т. е. точка $\mathfrak{p}_i$ не является полюсом дифференциала ω. Отсюда следует, что ядро отображения Λ состоит из дифференциалов первого рода поля R. Так как это ядро имеет размерность g, то размерность пространства $\Lambda(\mathfrak{D})$ равна

$$\left(\sum_{i=1}^{h} d(\mathfrak{p}_i)+g-1\right)-g=\sum_{i=1}^{h} d(\mathfrak{p}_i)-1.$$

С другой стороны, размерность пространства $\prod_{i=1}^{h} \Sigma_i^*$ равна $\sum_{i=1}^{h} d(\mathfrak{p}_i)$, поэтому размерность P также равна $\sum_{i=1}^{h} d(\mathfrak{p}_i)-1$. Таким образом, $\Lambda(\mathfrak{D})=P$, и лемма 2 доказана.

Теорема 4. *Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ — конечное множество различных точек поля R алгебраических функций от одной переменной. Обозначим через $\Sigma_{i,s}$ поле тех элементов из поля вычетов точки $\mathfrak{p}_i$, которые сепарабельны над полем констант K поля R. Пусть для каждого i $(1 \leqslant i \leqslant h)$ в поле $\Sigma_{i,s}$ задан элемент ρ_i. Если*

$$\sum_{i=1}^{h} \mathrm{Sp}_{\Sigma_{i,s}/K}\, \rho_i = 0,$$

то существует дифференциал ω поля R, делящийся на $(\mathfrak{p}_1 \ldots \mathfrak{p}_h)^{-1}$ и такой, что $\mathrm{res}_{\mathfrak{p}_i}\omega = \rho_i$ $(1 \leqslant i \leqslant h)$.

Для каждого i построим линейное отображение μ_i поля вычетов Σ_i точки $\mathfrak{p}_i$ в K, продолжающее отображение $\xi_i \to \mathrm{Sp}_{\Sigma_{i,s}/K}\, \xi_i\rho_i$ поля $\Sigma_{i,s}$ в K. Очевидно, будем иметь $\sum_{i=1}^{h} \mu_i(1) = 0$. Пусть дифференциал ω удовлетворяет условиям леммы 1 относительно этих линейных функций μ_i. Через x_i обозначим элемент поля R, принимающий в точке $\mathfrak{p}_i$ значение $\xi_i \in \Sigma_{i,s}$, а через $\overline{\xi}_i$ — алгебраический над K элемент из $\mathfrak{p}_i$-адического пополнения поля R, принадлежащий классу вычетов ξ_i по модулю $\mathfrak{p}_i$. Так как $\nu_{\mathfrak{p}_i}(\overline{\xi}_i - x_i) > 0$ и $\nu_{\mathfrak{p}_i}(\omega) \geqslant -1$, то $\omega^{\mathfrak{p}_i}(\overline{\xi}_i - x_i) = 0$, откуда

$$\mathrm{Sp}_{\Sigma_{i,s}/K}\, \xi_i(\mathrm{res}_{\mathfrak{p}_i}\omega) = \omega^{\mathfrak{p}_i}(\overline{\xi}_i) = \omega^{\mathfrak{p}_i}(x_i) = \mu_i(\xi_i) = \mathrm{Sp}_{\Sigma_{i,s}/K}\, \xi_i\rho_i.$$

Так как это равенство справедливо при любом $\xi_i \in \Sigma_{i,s}$ то в силу леммы 1 имеем $\mathrm{res}_{\mathfrak{p}_i}\omega = \rho_i$.

Дифференциал ω поля алгебраических функций от одной переменной характеристики 0 называется *дифференциалом второго рода*, если все его вычеты равны 0. Ясно, что любой дифференциал первого рода является также дифференциалом второго рода.

Лемма 3. *Пусть R — поле алгебраических функций от одной переменной характеристики 0, и пусть $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ — целый дивизор поля R. Положим $a^*(\mathfrak{p}) = \max\{0, a(\mathfrak{p}) - 1\}$. Тогда дифференциалы второго рода поля R, делящиеся на $\mathfrak{a}^{-1}$, образуют векторное прост-*

ранство над полем констант K поля R, и размерность этого пространства равна $\sum_{\mathfrak{p}} a^*(\mathfrak{p})\, d(\mathfrak{p}) + g$, где g — род поля R.

Лемма очевидна, если $\mathfrak{a}$ — единичный дивизор. Будем считать поэтому, что $\mathfrak{a}$ не является единичным дивизором. Так как размерность пространства элементов поля R, делящихся на $\mathfrak{a}$, равна 0, то в силу теоремы Римана — Роха размерность пространства $\mathfrak{D}$ дифференциалов, делящихся на $\mathfrak{a}^{-1}$, равна $d(\mathfrak{a}) + g - 1$. Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ — все различные точки, для которых $a(\mathfrak{p}) \neq 0$, и пусть Σ_i — поле вычетов точки $\mathfrak{p}_i$. Если каждому дифференциалу $\omega \in \mathfrak{D}$ мы поставим в соответствие элемент $(\operatorname{res}_{\mathfrak{p}_1} \omega, \ldots, \operatorname{res}_{\mathfrak{p}_h} \omega)$ из произведения $\prod_{i=1}^{h} \Sigma_i$, то получим линейное отображение P пространства $\mathfrak{D}$ в $\prod_{i=1}^{h} \Sigma_i$. Из теоремы 4 вытекает, что $\mathrm{P}(\mathfrak{D})$ состоит из тех элементов $(\rho_1, \ldots, \rho_h)$ пространства $\prod_{i=1}^{h} \Sigma_i$, для которых $\sum_{i=1}^{h} \mathrm{Sp}_{\Sigma_i/K}\, \rho_i = 0$; следовательно, размерность $\mathrm{P}(\mathfrak{D})$ равна $\sum_{i=1}^{h} d(\mathfrak{p}_i) - 1$. Пространство дифференциалов второго рода, делящихся на $\mathfrak{a}^{-1}$, является ядром отображения P; поэтому размерность этого пространства равна

$$d(\mathfrak{a}) + g - 1 - \left(\sum_{i=1}^{h} d(\mathfrak{p}_i) - 1\right) = \sum_{\mathfrak{p}} a^*(\mathfrak{p})\, d(\mathfrak{p}) + g.$$

ГЛАВА IV

РАСШИРЕНИЯ ПОЛЕЙ АЛГЕБРАИЧЕСКИХ ФУНКЦИЙ ОТ ОДНОЙ ПЕРЕМЕННОЙ

§ 1. Относительная степень и индекс разветвления

В этой главе будет рассматриваться пара (R, S) полей алгебраических функций от одной переменной, причем одно из полей R будет подполем другого поля S. *Без специальных оговорок мы всегда будем предполагать, что поле констант K поля R содержится в поле констант L поля S и что каждый элемент из R, трансцендентный над K, является также трансцендентным и над L.* Это равносильно тому, что $K = L \cap R$.

Пусть $\mathfrak{P}$ — точка поля S и пусть $\mathfrak{O}$ — кольцо точки $\mathfrak{P}$. Если кольцо $\mathfrak{O}$ содержит R, то будем говорить, что $\mathfrak{P}$ есть *переменная точка* (по отношению к R); в противном случае точку $\mathfrak{P}$ будем называть *постоянной точкой* (по отношению к R). В последнем случае пересечение $\mathfrak{O} \cap R = \mathfrak{o}$ является, очевидно, V-кольцом поля R, содержащим поле K. Кольцо $\mathfrak{o}$ определяет точку $\mathfrak{p}$ поля R. Будем говорить, что точка $\mathfrak{p}$ *лежит под* $\mathfrak{P}$ или что $\mathfrak{P}$ *лежит над* $\mathfrak{p}$. Если поле S является алгебраическим расширением поля R, то каждая точка поля S постоянна по отношению к R. Действительно, в этом случае каждый элемент из S алгебраичен над R и, значит, является целым над R (ибо R — поле); если бы R содержалось в $\mathfrak{O}$, то все элементы из S были бы целыми относительно $\mathfrak{O}$, вопреки цело-замкнутости кольца $\mathfrak{O}$ в S (см. § 2 гл. I). С другой стороны, если поле S трансцендентно над R (это имеет место только в случае, если L трансцендентно над K), то в поле S, как легко показать, всегда существуют переменные точки по отношению к R.

Предположим, что точка $\mathfrak{P}$ поля S лежит над точкой $\mathfrak{p}$ поля R. Значения, принимаемые функцией порядка $\nu_{\mathfrak{P}}$ в точке $\mathfrak{P}$ на мультипликативной группе отличных от 0 элементов поля R, образуют подгруппу в аддитивной группе целых чисел, и эта подгруппа содержит числа, не равные нулю. Следовательно, рассматриваемая подгруппа состоит из всех целых чисел, делящихся на некоторое вполне определенное положительное целое число e. Это число e называется *индексом разветвления* точки $\mathfrak{P}$ относительно $\mathfrak{p}$ (или относительно поля R). Если $e > 1$, то точка $\mathfrak{P}$ называется *разветвленной* относительно R, в противном случае она называется *неразветвленной*. Если все точки поля S, лежащие над $\mathfrak{p}$, неразветвлены относительно R, то говорят, что точка $\mathfrak{p}$ *неразветвлена* в S.

В общем случае, очевидно, имеем

$$\nu_{\mathfrak{P}}(x) = e\nu_{\mathfrak{p}}(x) \qquad \text{для всех } x \neq 0 \text{ из } R.$$

Далее, пересечение $\mathfrak{P}$ с кольцом $\mathfrak{o}$ точки $\mathfrak{p}$ равно $\mathfrak{p}$, поэтому поле вычетов $\Sigma_{\mathfrak{p}} = \mathfrak{o}/\mathfrak{p}$ точки $\mathfrak{p}$ мы можем отождествить с подполем поля вычетов $\Sigma_{\mathfrak{P}} = \mathfrak{O}/\mathfrak{P}$ точки $\mathfrak{P}$. Если $\Sigma_{\mathfrak{P}}$ является алгебраическим расширением конечной степени поля $\Sigma_{\mathfrak{p}}$, то $[\Sigma_{\mathfrak{P}} : \Sigma_{\mathfrak{p}}]$ называется *относительной степенью* точки $\mathfrak{P}$ по отношению к точке $\mathfrak{p}$ (или по отношению к полю R); в противном случае говорят, что точка $\mathfrak{P}$ имеет бесконечную относительную степень по отношению к R.

Теорема 1. *Пусть R и S — два поля алгебраических функций от одной переменной, причем R является подполем поля S. Тогда для любой точки $\mathfrak{p}$ поля R существует по крайней мере одна точка поля S, лежащая над $\mathfrak{p}$, и число таких точек конечно. Пусть $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все точки поля S, лежащие над $\mathfrak{p}$. Если поле S имеет конечную степень над R, то относительные степени $f_1, \ldots, f_h$ точек $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ также конечны, и имеет место равенство*

$$[S : R] = \sum_{i=1}^{h} f_i e_i,$$

где e_i — индекс разветвления точки $\mathfrak{P}_i$ относительно R.

Докажем предварительно несколько лемм.

Лемма 1. *Для любой точки $\mathfrak{p}$ поля R существует элемент $x \in R$, имеющий точку $\mathfrak{p}$ своим единственным нулем.*

Пусть g — род поля R, а d — степень точки $\mathfrak{p}$. По теореме Римана имеем $l(\mathfrak{p}^{-g-1}) \geqslant d(g+1) - g + 1 \geqslant 2$; следовательно, в поле R существует такой элемент y, отличный от константы, что $y \equiv 0 \pmod{\mathfrak{p}^{-g-1}}$. Для элемента $x = y^{-1}$ точка $\mathfrak{p}$ является единственным нулем.

Лемма 2. *Пусть K, L и T — три подполя некоторого поля, причем $K \subset L$, $K \subset T$ и поле L имеет конечную степень над K. Пусть $\{\lambda_1, \ldots, \lambda_m\}$ базис поля L над K; тогда каждый элемент из $T\langle L\rangle$ может быть представлен в виде линейной комбинации элементов $\lambda_1, \ldots, \lambda_m$ с коэффициентами из T, а значит, $[T\langle L\rangle : T] \leqslant [L : K]$.*

Обозначим через U множество всех линейных комбинаций элементов $\lambda_1, \ldots, \lambda_m$ с коэффициентами из T. Так как произведения $\lambda_i\lambda_j$ $(1 \leqslant i, j \leqslant m)$ принадлежат U, то U есть кольцо. Из включения $L \subset U$ следует, что $1 \in U$, а значит, и $T \subset U$. Пусть $u_1 \neq 0$, $u_1 \in U$; тогда отображение $u \to u_1 u$ кольца U в себя является линейным отображением (если кольцо U рассматривать как векторное пространство над T), при котором на 0 не отображается никакой элемент $u \neq 0$. Но пространство U имеет конечную размерность над T, поэтому наше отображение отображает U на себя. Так как $1 \in U$, то $u_1^{-1} \in U$, откуда следует, что U есть поле. Так как T и L содержатся в U, то получаем, что $U = T\langle L\rangle$.

Лемма 3. *Пусть L — надполе поля K и пусть x — элемент из некоторого надполя поля L, трансцендентный над L. Для того чтобы поле $L\langle x\rangle$ имело конечную степень над $K\langle x\rangle$, необходимо и достаточно, чтобы поле L имело конечную степень над K. Если последнее условие выполнено, то имеем $[L\langle x\rangle : K\langle x\rangle] = [L : K]$.*

Если поле L имеет конечную степень над K, то в силу леммы 2 поле $L\langle x\rangle$ имеет конечную степень над $K\langle x\rangle$ и $[L\langle x\rangle : K\langle x\rangle] \leqslant [L : K]$. Предположим теперь, что $L\langle x\rangle$ имеет конечную степень над $K\langle x\rangle$. Пусть $\lambda_1, \ldots, \lambda_m$ — элементы из L, линейно независимые над K; докажем, что они линейно независимы и над $K\langle x\rangle$. Допустим, что $\lambda_1 r_1 + \ldots + \lambda_m r_m = 0$, где $r_i \in K\langle x\rangle$. Найдем многочлен $q \neq 0$ из $K[x]$ такой, чтобы элементы $p_i = qr_i$ $(1 \leqslant i \leqslant m)$ при-

надлежали $K[x]$. Так как коэффициенты многочлена $\sum_{i=1}^{m}\lambda_i p_i$ равны нулю, а элементы $\lambda_1, \ldots, \lambda_m$ линейно независимы над K, то, как легко видеть, $p_i = 0$ $(1 \leqslant i \leqslant m)$, и наше утверждение доказано. Таким образом, степень $[L:K]$ конечна и не превосходит $[L\langle x\rangle : K\langle x\rangle]$. Лемма 3 доказана.

Вернемся к доказательству теоремы 1. Обозначим через K и L поля констант полей R и S соответственно. Выберем элемент $x \in R$, для которого точка $\mathfrak{p}$ является единственным нулем. Тогда x, являясь трансцендентным над K элементом поля R, не принадлежит L; следовательно, элемент x обладает по крайней мере одним нулем $\mathfrak{P}$ в поле S. Кольцо $\mathfrak{O}$ точки $\mathfrak{P}$ не содержит элемента x^{-1}, поэтому пересечение $\mathfrak{O} \cap R$ является кольцом некоторой точки поля R, содержащей элемент x. Этой точкой может быть только точка $\mathfrak{p}$; значит, $\mathfrak{P}$ лежит над $\mathfrak{p}$. Обратно, всякая точка поля S, лежащая над $\mathfrak{p}$, является нулем элемента x; таким образом, имеется только конечное число точек поля S, лежащих над $\mathfrak{p}$. Предположим теперь, что S имеет конечную степень над R. Так как R имеет конечную степень над $K\langle x\rangle$, то, как легко видеть, $L\langle x\rangle$ имеет конечную степень над $K\langle x\rangle$. Отсюда следует, что степень L над K также конечна и $[L\langle x\rangle : K\langle x\rangle] = [L:K]$. Пусть $a = \nu_{\mathfrak{p}}(x)$, тогда дивизор нулей элемента x в поле S равен $\mathfrak{P}_1^{ae_1} \ldots \mathfrak{P}_h^{ae_h}$. Используя теорему 4 § 8 гл. I, получаем

$$[S : L\langle x\rangle] = \sum_{i=1}^{h} ae_i [\mathfrak{O}_i/\mathfrak{P}_i : L],$$

где $\mathfrak{O}_i$ — кольцо точки $\mathfrak{P}_i$. Так как $[L\langle x\rangle : K\langle x\rangle] = [L:K]$, то $[S : K\langle x\rangle] = a\sum_{i=1}^{h} e_i [\mathfrak{O}_i/\mathfrak{P}_i : K]$. Поле $\mathfrak{O}_i/\mathfrak{P}_i$, имея конечную степень над K, будет иметь конечную степень f_i и над полем вычетов $\mathfrak{o}/\mathfrak{p}$ точки $\mathfrak{p}$. Таким образом, мы имеем

$$[S:R]\,[R : K\langle x\rangle] = a\,[\mathfrak{o}/\mathfrak{p} : K] \sum_{i=1}^{h} e_i f_i .$$

Применяя теорему 4 § 8 гл. I вместо поля S к полю R, получим $[R : K\langle x\rangle] = a\,[\mathfrak{o}/\mathfrak{p} : K]$. Теорема 1, следовательно, доказана.

Лемма 4. *Пусть R, S и T — поля алгебраических функций от одной переменной, причем R содержится в S, а S — в T. Пусть точка $\mathfrak{P}$ поля T постоянна по отношению к R. Тогда $\mathfrak{P}$ является постоянной точкой и по отношению к полю S, а точка $\mathfrak{p}$ поля S, лежащая под $\mathfrak{P}$, является постоянной точкой по отношению к R. Далее, индекс разветвления точки $\mathfrak{P}$ относительно R равен произведению индекса разветвления $\mathfrak{P}$ относительно S на индекс разветвления $\mathfrak{p}$ относительно R. Если поле T имеет конечную степень над R, то относительная степень точки $\mathfrak{P}$ по отношению к R равна произведению ее относительной степени по отношению к S на относительную степень точки $\mathfrak{p}$ по отношению к R.*

Утверждения о том, что $\mathfrak{P}$ есть постоянная точка по отношению к S, а $\mathfrak{p}$ — постоянная точка по отношению к R, очевидны. Пусть $\mathfrak{q}$ есть точка поля R, лежащая под $\mathfrak{P}$, а x — униформизирующая переменная поля R в точке $\mathfrak{q}$. Тогда индекс разветвления точки $\mathfrak{p}$ относительно R равен $e_0 = \nu_{\mathfrak{p}}(x)$, а индекс разветвления точки $\mathfrak{P}$ относительно R равен $\nu_{\mathfrak{P}}(x) = e\nu_{\mathfrak{p}}(x)$, где e — индекс разветвления $\mathfrak{P}$ относительно S. Пусть $\Sigma(\mathfrak{q})$, $\Sigma(\mathfrak{p})$ и $\Sigma(\mathfrak{P})$ — поля вычетов точек $\mathfrak{q}$, $\mathfrak{p}$ и $\mathfrak{P}$ соответственно. Тогда имеем $\Sigma(\mathfrak{q}) \subset \Sigma(\mathfrak{p}) \subset \Sigma(\mathfrak{P})$, а если T имеет конечную степень над R, то $[\Sigma(\mathfrak{P}) : \Sigma(\mathfrak{q})] = [\Sigma(\mathfrak{P}) : \Sigma(\mathfrak{p})]\,[\Sigma(\mathfrak{p}) : \Sigma(\mathfrak{q})]$. Лемма 4, таким образом, доказана.

§ 2. Случай нормальных алгебраических расширений

Пусть R и S — два поля алгебраических функций от одной переменной, причем R является подполем поля S. Пусть σ есть изоморфное отображение S на поле S', отображающее каждый элемент из R на себя. Поле S' можно рассматривать как поле алгебраических функций от одной переменной, поле констант которого равно образу поля констант поля S при изоморфизме σ. Если $\mathfrak{P}$ есть точка поля S, то, очевидно, $\sigma\mathfrak{P}$ является точкой поля S'. Легко видеть, что σ индуцирует изоморфизм поля вычетов точки $\mathfrak{P}$ на поле вычетов точки $\sigma\mathfrak{P}$, а также изоморфизм $\mathfrak{P}$-адического пополнения поля S на $\sigma\mathfrak{P}$-адическое пополнение поля S'. Для любого элемента x поля S имеем $\nu_{\sigma\mathfrak{P}}(\sigma x) = \nu_{\mathfrak{P}}(x)$. Если точка $\mathfrak{P}$ постоянна по отношению к R, то точка $\sigma\mathfrak{P}$ также постоянна, при этом $\mathfrak{P}$ и $\sigma\mathfrak{P}$ лежат над одной и той же точкой поля R; индексы разветвления точек $\mathfrak{P}$ и $\sigma\mathfrak{P}$ отно-

сительно R равны между собой. Если S имеет конечную степень над R, то относительные степени точек $\mathfrak{P}$ и $\sigma\mathfrak{P}$ по отношению к R также равны друг другу.

Если точки $\mathfrak{P}$ и $\sigma\mathfrak{P}$ находятся между собой в описанном выше отношении, то говорят, что точка $\sigma\mathfrak{P}$ *сопряжена* с точкой $\mathfrak{P}$ относительно поля R. В частности, точки самого поля S, сопряженные с точкой $\mathfrak{P}$, получаются из $\mathfrak{P}$ применением автоморфизмов поля S, не меняющих элементов из R.

Теорема 2. *Пусть R и S — два поля алгебраических функций от одной переменной, причем поле S является алгебраическим нормальным расширением поля R. Тогда все точки поля S, лежащие над данной точкой $\mathfrak{p}$ поля R, сопряжены между собой.*

Пусть $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все точки поля S, лежащие над $\mathfrak{p}$. В силу следствия к теореме 3 § 6 гл. I в поле S существует такой элемент z, что $\nu_{\mathfrak{P}_1}(z) > 0$, $\nu_{\mathfrak{P}_i}(z) = 0$ при $i > 1$. Обозначим через S' поле, полученное присоединением к полю R элемента z и всех элементов с ним сопряженных относительно R; поле S' является алгебраическим нормальным расширением поля R конечной степени. Пусть $\sigma'_1, \ldots, \sigma'_m$ — все различные автоморфизмы поля S' над R. Как известно, каждый автоморфизм σ'_k можно продолжить до автоморфизма σ_k поля S. Относительная норма $N_{S'/R}z$ элемента z из S' в R может быть записана в виде $x = \prod_{k=1}^{m} (\sigma_k z)^q$, где q — некоторый положительный показатель. Имеем $\nu_{\sigma_k\mathfrak{P}_1}(\sigma_k z) > 0$, но $\nu_{\mathfrak{P}_i}(\sigma_k z) = 0$ при $\mathfrak{P}_i \neq \sigma_k\mathfrak{P}_1$. Таким образом, $\nu_{\mathfrak{P}_1}(\sigma_k z) \geqslant 0$ при всех k. Так как z встречается среди элементов $\sigma_k z$, то $\nu_{\mathfrak{P}_1}(x) > 0$, откуда $\nu_{\mathfrak{p}}(x) > 0$ и $\nu_{\mathfrak{P}_i}(x) > 0$ при $1 \leqslant i \leqslant h$. В силу изложенного выше отсюда непосредственно следует, что каждая точка $\mathfrak{P}_i$ должна встречаться среди точек $\sigma_k\mathfrak{P}_1$. Теорема 2, следовательно, доказана.

§ 3. Целые базисы

Пусть R и S — поля алгебраических функций от одной переменной, причем S является расширением поля R конечной степени. Пусть, далее, $\mathfrak{p}$ — точка поля R, а $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ —

все точки поля S, лежащие над $\mathfrak{p}$. Введем в рассмотрение следующие кольца: 1) $\mathfrak{o}$ — кольцо точки $\mathfrak{p}$; 2) $\mathfrak{r}$ — кольцо тех элементов поля R, которые не имеют полюсов вне $\{\mathfrak{p}\}$; 3) $\mathfrak{D}$ — пересечение колец точек $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$; кольцо $\mathfrak{D}$ состоит, таким образом, из тех элементов поля S, для которых каждая из точек $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ не является полюсом; 4) $\mathfrak{R}$ — кольцо элементов поля S, не имеющих полюсов вне множества $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_h\}$. Очевидно, что пересечение $\mathfrak{o} \cap \mathfrak{r}$ совпадает с полем констант поля R, а пересечение $\mathfrak{D} \cap \mathfrak{R}$ — с полем констант поля S. Кроме того, имеем $\mathfrak{D} \cap R = \mathfrak{o}$ и $\mathfrak{R} \cap R = \mathfrak{r}$.

Пусть $\{y_1, \ldots, y_n\}$ — некоторый базис поля S относительно R. Тогда каждый элемент $y \in S$ можно представить в виде $\sum_{i=1}^{n} x_i y_i$, $x_i \in R$. Займемся исследованием свойств коэффициентов $x_1, \ldots, x_n$, предполагая, что y принадлежит $\mathfrak{R}$ или $\mathfrak{D}$.

Лемма 1. *В поле R существует элемент $u \neq 0$, зависящий только от точки $\mathfrak{p}$ и от базиса $\{y_1, \ldots, y_n\}$ и обладающий следующим свойством: если элемент $y = \sum_{i=1}^{n} x_i y_i$ (где $x_i \in R$, $1 \leqslant i \leqslant n$) принадлежит кольцу $\mathfrak{R}$, то $ux_i \in \mathfrak{r}$ $(1 \leqslant i \leqslant n)$.*

Обозначим через K и L поля констант полей R и S соответственно. В поле R выберем элемент x, для которого точка $\mathfrak{p}$ является единственным нулем (лемма 1 § 1). В силу леммы 3 § 8 гл. I в кольце $\mathfrak{R}$ существует такое конечное подмножество $\{w_1, \ldots, w_N\}$, что $\mathfrak{R} = \sum_{\nu=1}^{N} L[x^{-1}]\, w_\nu$. Так как поле S имеет конечную степень над R, то $L\langle x\rangle$ имеет конечную степень над $K\langle x\rangle$, а L — конечную степень над K (лемма 3 § 1). Если $\{\lambda_1, \ldots, \lambda_t\}$ — базис поля L относительно K, то каждый элемент из $L[x^{-1}]$ можно представить в виде линейной комбинации элементов $\lambda_1, \ldots, \lambda_t$ с коэффициентами из $K[x^{-1}]$, откуда

$$\mathfrak{R} = \sum_{\tau=1}^{t} \sum_{\nu=1}^{N} K[x^{-1}]\, \lambda_\tau w_\nu.$$

Положим $\lambda_\tau w_\nu = \sum_{i=1}^{n} a_{\tau\nu i} y_i$, $a_{\tau\nu i} \in R$, и выпишем все точки $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ поля R, которые являются полюсами хоть одного из коэффициентов $a_{\tau\nu i}$. Положим $m_k = \min_{\tau, \nu, i} \nu_{\mathfrak{q}_k}(a_{\tau\nu i})$; степень дивизора $\mathfrak{p}^m \prod_{k=1}^{r} \mathfrak{q}_k^{m_k}$ неограниченно возрастает при возрастании m, следовательно, в силу теоремы Римана при достаточно большом m в поле R существует элемент $u \neq 0$, который

$$\equiv 0 \left(\operatorname{mod} \mathfrak{p}^{-m} \prod_{k=1}^{r} \mathfrak{q}_k^{-m_k} \right).$$

Имеем теперь $ua_{\tau\nu i} \in \mathfrak{r}$ $(1 \leqslant \tau \leqslant t,\ 1 \leqslant \nu \leqslant N,\ 1 \leqslant i \leqslant n)$; так как $K[x^{-1}] \subset \mathfrak{r}$, то элемент u обладает требуемым свойством, и лемма 1 доказана.

Лемма 2. *В поле R существует элемент $v \neq 0$, зависящий только от точки $\mathfrak{p}$ и от базиса $\{y_1, \ldots, y_n\}$ и обладающий следующим свойством: если элемент $y = \sum_{i=1}^{n} x_i y_i$ $(x_i \in R,\ 1 \leqslant i \leqslant n)$ принадлежит кольцу $\mathfrak{O}$, то $vx_i \in \mathfrak{o}$ $(1 \leqslant i \leqslant n)$.*

Пусть $\mathfrak{p}^*$ — произвольная точка поля R, отличная от точки $\mathfrak{p}$, и пусть $\mathfrak{r}^*$ и $\mathfrak{R}^*$ — кольца, построенные для точки $\mathfrak{p}^*$ таким же образом, как $\mathfrak{r}$ и $\mathfrak{R}$ были построены для точки $\mathfrak{p}$. Докажем, что для любого элемента $y \in \mathfrak{O}$ в кольце $\mathfrak{o}$ существует такой делитель единицы ξ, что $\xi y \in \mathfrak{R}^*$. Пусть $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$ — все те полюса элемента y, которые лежат над точками поля R, отличными от $\mathfrak{p}^*$ (если таковые существуют). Обозначим через $\mathfrak{q}_\rho$ точку поля R, лежащую под $\mathfrak{Q}_\rho$. Для каждого ρ мы можем найти такое целое число m_ρ, что из условия $\nu_{\mathfrak{q}_\rho}(\xi) \geqslant m_\rho$, $\xi \in R$, будет следовать $\nu_{\mathfrak{Q}_\rho}(\xi y) \geqslant 0$. Пусть μ — целое положительное число; если $\xi \in R$ и $\xi \equiv 0 \left(\operatorname{mod} \mathfrak{p}^{*-\mu} \prod_{\rho=1}^{r} \mathfrak{q}_\rho^{m_\rho} \right)$, то, как легко видеть, $\xi y \in \mathfrak{R}^*$. Выберем теперь μ настолько большим, чтобы $d\left(\mathfrak{p}^{*\mu} \prod_{\rho=1}^{r} \mathfrak{q}_\rho^{-m_\rho} \right) > 2g - 2 + d(\mathfrak{p})$, где g — род поля R. Тогда размерность l_μ пространства $\mathfrak{Z}$ тех элементов поля R, которые

$\equiv 0\left(\operatorname{mod} \mathfrak{p}^{*-\mu}\prod_{\rho=1}^{r}\mathfrak{q}_\rho^{m_\rho}\right)$, будет равна $d\left(\mathfrak{p}^{*\mu}\prod_{\rho=1}^{r}\mathfrak{q}_\rho^{-m_\rho}\right)-g+1$, в то время как размерность l'_μ пространства Ξ' тех элементов поля R, которые $\equiv 0\left(\operatorname{mod} \mathfrak{p}\mathfrak{p}^{*-\mu}\prod_{\rho=1}^{r}\mathfrak{q}_\rho^{m_\rho}\right)$, равна $l_\mu-d(\mathfrak{p})$ (следствие к теореме 6 § 6 гл. II). Отсюда следует, что пространство Ξ содержит элемент ξ, не содержащийся в Ξ'. Мы имеем $\xi y\in\mathfrak{R}^*$; с другой стороны, так как $y\in\mathfrak{O}$, то точки $\mathfrak{q}_\rho$ отличны от $\mathfrak{p}$, поэтому $\nu_\mathfrak{p}(\xi)=0$ (ибо $\xi\notin\Xi'$), т. е. ξ является делителем единицы в кольце $\mathfrak{o}$.

Найдем теперь в поле R элемент $u^*\neq 0$, удовлетворяющий по отношению к точке $\mathfrak{p}^*$ (и к базису $\{y_1, \ldots, y_n\}$) такому же условию, какому элемент u из леммы 1 удовлетворял по отношению к точке $\mathfrak{p}$. Если $y=\sum_{i=1}^{n}x_iy_i\in\mathfrak{O}$ (где $x_i\in R$, $1\leqslant i\leqslant n$), то $\xi u^*x_i\in\mathfrak{r}^*$ $(1\leqslant i\leqslant n)$, а тогда, и подавно, $\xi u^*x_i\in\mathfrak{o}$. Так как ξ является делителем единицы в кольце $\mathfrak{o}$, то элемент $v=u^*$ удовлетворяет условию леммы 2.

Более того, мы видим, что при фиксированном базисе $\{y_1, \ldots, y_n\}$ и фиксированной точке $\mathfrak{p}^*$ элемент v может быть взят один и тот же для всех точек $\mathfrak{p}\neq\mathfrak{p}^*$. Заметим теперь, что в поле R существует только конечное число точек $\mathfrak{p}$, которые не удовлетворяют хоть одному из следующих трех условий: 1) $\mathfrak{p}\neq\mathfrak{p}^*$; 2) $\nu_\mathfrak{P}(y_i)\geqslant 0$ $(1\leqslant i\leqslant n)$ для всех точек $\mathfrak{P}$ поля S, лежащих над $\mathfrak{p}$; 3) $\nu_\mathfrak{p}(u^*)=0$. Будем говорить, что базис $\{y_1, \ldots, y_n\}$ является *целым базисом в точке* $\mathfrak{p}$, если выполняются следующие условия: 1) каждый элемент y_i принадлежит пересечению $\mathfrak{O}$ колец всех точек поля S, лежащих над $\mathfrak{p}$; 2) если элемент $y=\sum_{i=1}^{n}x_iy_i$ $(x_i\in R,\ 1\leqslant i\leqslant n)$ принадлежит $\mathfrak{O}$, то $x_1, \ldots, x_n$ принадлежат кольцу точки $\mathfrak{p}$. Из предыдущего вытекает следующая лемма.

Лемма 3. *Произвольный базис поля S относительно R является целым базисом почти во всех точках поля R.*

Докажем теперь следующую теорему.

Теорема 3. *Пусть R и S — поля алгебраических функций от одной переменной, причем S является рас-*

ширением конечной степени поля R. Тогда для любой точки $\mathfrak{p}$ поля R в S существует базис относительно R, являющийся целым в точке $\mathfrak{p}$.

Обозначим через $\mathfrak{o}$ кольцо точки $\mathfrak{p}$, через $\mathfrak{O}$ — пересечение колец тех точек поля S, которые лежат над $\mathfrak{p}$, и через $\{y'_1, \ldots, y'_n\}$ — произвольный базис S относительно R. Пусть $\mathfrak{M}_m$, где $1 \leqslant m \leqslant n$, обозначает множество всех элементов из $\mathfrak{O}$, являющихся линейными комбинациями элементов $y'_1, \ldots, y'_m$ с коэффициентами из R. Пусть $y \in \mathfrak{M}_m$, тогда $y = \sum_{i=1}^{m} u'_i y'_i$, где $u'_i \in R$ $(1 \leqslant i \leqslant m)$; из леммы 2 следует, что числа $\nu_{\mathfrak{p}}(u'_m)$ при всех $y \in \mathfrak{M}_m$ ограничены снизу. Если t есть некоторый элемент поля R, для которого $\nu_{\mathfrak{p}}(t) > 0$, то $t^{\mu} y'_m \in \mathfrak{M}_m$ при достаточно большом μ; таким образом, существуют элементы $y \in \mathfrak{M}_m$, для которых $u'_m \neq 0$. Пусть $-q_m$ есть наименьшее из чисел $\nu_{\mathfrak{p}}(u'_m)$ при всех $y \in \mathfrak{M}_m$, и пусть $y_m = \sum_{i=1}^{m} u'_{im} y'_i$ — элемент из $\mathfrak{M}_m$, для которого $\nu_{\mathfrak{p}}(u'_{mm}) = -q_m$. Так как $u'_{mm} \neq 0$, то элементы $y_1, \ldots, y_n$ образуют, очевидно, базис поля S относительно R. Так как $y_m \in \mathfrak{M}_m$, то элементы $y_1, \ldots, y_n$ и все их линейные комбинации с коэффициентами из $\mathfrak{o}$ принадлежат $\mathfrak{O}$. Обратно, пусть $y = \sum_{i=1}^{n} u_i y_i$ $(u_i \in R,\ 1 \leqslant i \leqslant n)$ есть произвольный элемент из $\mathfrak{O}$. Утверждаем, что $u_i \in \mathfrak{o}$ $(1 \leqslant i \leqslant n)$. Действительно, допустим, что $u_i \in \mathfrak{o}$ при $i > m$, но $u_m \notin \mathfrak{o}$. Положим $y' = y - \sum_{i > m} u_i y_i$; тогда y' принадлежит $\mathfrak{O}$; следовательно, y' принадлежит $\mathfrak{M}_m$, ибо элементы $y_1, \ldots, y_m$ являются линейными комбинациями элементов $y'_1, \ldots, y'_m$ с коэффициентами из R. Если мы положим $y' = \sum_{i=1}^{m} u'_i y'_i$, то будем иметь $u'_m = u_m u'_{mm}$, откуда $\nu_{\mathfrak{p}}(u'_m) = -q_m + \nu_{\mathfrak{p}}(u_m) < -q_m$, что противоречит выбору y_m. Таким образом, теорема 3 доказана.

Пусть $\{y_1, \ldots, y_n\}$ — базис поля S относительно R, целый в точке $\mathfrak{p}$ поля R. Пусть $\mathfrak{O}$ — пересечение колец

точек поля S, лежащих над $\mathfrak{p}$, и пусть y — произвольный элемент из $\mathfrak{O}$. Так как $yy_i \in \mathfrak{O}$, то $yy_i = \sum_{j=1}^{n} a_{ij} y_j$, где элементы a_{ij} принадлежат кольцу $\mathfrak{o}$ точки $\mathfrak{p}$. Характеристический многочлен $F(X)$ элемента y относительно поля R равен определителю матрицы $XE - (a_{ij})$, где E — единичная матрица n-го порядка, поэтому коэффициенты многочлена $F(X)$ принадлежат кольцу $\mathfrak{o}$. В частности, мы видим, что след и норма элемента y (взятые относительно поля R) принадлежат $\mathfrak{o}$ и, далее, что y является целым элементом относительно кольца $\mathfrak{o}$. Обратно, всякий элемент поля S, являющийся целым относительно $\mathfrak{o}$, принадлежит кольцу $\mathfrak{O}$; это следует из того, что кольцо любой точки целозамкнуто (§ 2 гл. I). Таким образом, нами доказана

Лемма 4. *Пусть $\mathfrak{o}$ — кольцо точки $\mathfrak{p}$ поля R алгебраических функций от одной переменной и пусть S — расширение поля R конечной степени. Тогда пересечение $\mathfrak{O}$ колец всех точек поля S, лежащих над $\mathfrak{p}$, совпадает с кольцом целых относительно $\mathfrak{o}$ элементов поля S. Если $y \in \mathfrak{O}$, то коэффициенты характеристического многочлена элемента y относительно R принадлежат $\mathfrak{o}$.*

Теперь будет доказана

Лемма 5. *Пусть сохраняются обозначения леммы 4 и пусть $\{y_1, \ldots, y_n\}$ — базис поля S относительно R, целый в точке $\mathfrak{p}$. Пусть, далее, $\mathfrak{P}$ — некоторая точка поля S, лежащая над $\mathfrak{p}$, и y_i^* — класс вычетов элемента y_i по модулю $\mathfrak{P}$ $(1 \leqslant i \leqslant n)$. Тогда каждый элемент из поля вычетов точки $\mathfrak{P}$ может быть представлен в виде линейной комбинации элементов $y_1^*, \ldots, y_n^*$ с коэффициентами из поля вычетов точки $\mathfrak{p}$.*

Пусть η^* — элемент из поля вычетов точки $\mathfrak{P}$ и η_0 — элемент из S, принадлежащий классу η^*. Обозначим через $\mathfrak{P}_1 = \mathfrak{P}, \mathfrak{P}_2, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$. В силу теоремы 3 § 6 гл. I в поле S существует такой элемент η, что $\nu_{\mathfrak{P}}(\eta - \eta_0) > 0$, $\nu_{\mathfrak{P}_i}(\eta) \geqslant 0$ $(2 \leqslant i \leqslant h)$. Так как η принадлежит кольцу $\mathfrak{O}$, то $\eta = \sum_{i=1}^{n} x_i y_i$,

где $x_i \in \mathfrak{o}$ $(1 \leqslant i \leqslant n)$. Обозначая через x_i^* значение, принимаемое элементом x_i в точке $\mathfrak{p}$, получаем $\eta^* = \sum_{i=1}^{n} x_i^* y_i^*$.

§ 4. Кронекеровские произведения коммутативных алгебр

Пусть $\mathfrak{L}$ и $\mathfrak{M}$ — коммутативные алгебры над полем K (конечной или бесконечной размерности). Алгебрам $\mathfrak{L}$ и $\mathfrak{M}$ мы сопоставим коммутативную алгебру $\mathfrak{L} \otimes \mathfrak{M}$ над K, обладающую следующими свойствами:

1) Существует соответствие, сопоставляющее каждой паре (x, y) элементов $x \in \mathfrak{L}$ и $y \in \mathfrak{M}$ некоторый элемент $xy \in \mathfrak{L} \otimes \mathfrak{M}$ так, что

$$(x + x')y = xy + x'y, \quad x(y + y') = xy + xy',$$
$$(xx')(yy') = (xy)(x'y'), \qquad (\alpha x)y = x(\alpha y) = \alpha(xy)$$

для любых $x, x' \in \mathfrak{L}$; $y, y' \in \mathfrak{M}$; $\alpha \in K$.

2) Каждый элемент из $\mathfrak{L} \otimes \mathfrak{M}$ может быть представлен в виде конечной суммы элементов вида xy, $x \in \mathfrak{L}$, $y \in \mathfrak{M}$.

3) Если $x_1, \ldots, x_m$ — линейно независимые над K элементы из $\mathfrak{L}$, а $y_1, \ldots, y_n$ — линейно независимые над K элементы из $\mathfrak{M}$, то элементы $x_i y_j \in \mathfrak{L} \otimes \mathfrak{M}$ $(1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n)$ также линейно независимы над K.

Чтобы доказать существование алгебры с этими свойствами, выберем в алгебрах $\mathfrak{L}$ и $\mathfrak{M}$ базисы $(\xi_\alpha)_{\alpha \in A}$ и $(\eta_\beta)_{\beta \in B}$ соответственно (здесь A и B — множества индексов, конечные или бесконечные). Введем в рассмотрение множество символов $\zeta_{\alpha, \beta}$, для которых индексами являются пары $(\alpha, \beta) \in A \times B$, и построим векторное пространство, состоящее из всех формальных линейных комбинаций $\sum_{\alpha, \beta} a_{\alpha\beta} \zeta_{\alpha\beta}$ этих символов с коэффициентами $a_{\alpha\beta} \in K$ (имеется в виду, что в каждой такой линейной комбинации имеется только конечное число пар (α, β), для которых $a_{\alpha\beta} \neq 0$). Если $x = \sum_{\alpha \in A} c_\alpha \xi_\alpha \in \mathfrak{L}$ и $y = \sum_{\beta \in B} d_\beta \eta_\beta \in \mathfrak{M}$, то положим $xy = \sum_{\alpha, \beta} c_\alpha d_\beta \zeta_{\alpha\beta}$; тогда все условия, содержащиеся в 1) и 2), будут выполнены, кроме условия $(xx')(yy') = (xy)(x'y')$, относящегося к умножению в $\mathfrak{L} \otimes \mathfrak{M}$, которое еще не определено. Сначала проверим, что условие 3) будет также выполнено.

Выразим элементы $x_1, \ldots, x_m$ в виде линейных комбинаций конечного числа элементов ξ_α, скажем $\xi_{\alpha_1}, \ldots, \xi_{\alpha_p}$. Так как $x_1, \ldots, x_m$ линейно независимы над K, то $p \geqslant m$; если к элементам $x_1, \ldots, x_m$ мы присоединим $p-m$ подходящим образом выбранных элементов ξ_{α_i}, то получим p элементов $x_1, \ldots, x_p$, порождающих то же самое подпространство пространства $\mathfrak{L}$, которое порождают и элементы $\xi_{\alpha_1}, \ldots, \xi_{\alpha_p}$. Аналогичным образом, присоединяя к $y_1, \ldots, y_n$ некоторое число элементов $y_{n+1}, \ldots, y_q$ из базиса $(\eta_\beta)_{\beta \in B}$, мы получим систему линейно независимых элементов $y_1, \ldots, y_q$, порождающих подпространство, в котором имеется базис из q элементов $\eta_{\beta_1}, \ldots, \eta_{\beta_q}$ базиса $(\eta_\beta)_{\beta \in B}$. Элементы $x_i y_j$ $(1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q)$ являются линейными комбинациями элементов $\zeta_{\alpha_i \beta_j}$ $(1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q)$ и обратно, следовательно, эти элементы $x_i y_j$ линейно независимы над K.

Чтобы определить билинейное умножение в нашем векторном пространстве, достаточно определить произведение базисных элементов $\zeta_{\alpha\beta}$. Положим $\zeta_{\alpha\beta}\zeta_{\alpha'\beta'} = (\xi_\alpha \xi_{\alpha'})(\eta_\beta \eta_{\beta'})$; легко видеть, что определенное таким образом умножение ассоциативно и коммутативно и что наше векторное пространство становится алгеброй. Очевидно, что формула $(xx')(yy') = (xy)(x'y')$ справедлива, если x и x' равны элементам ξ_α, а y и y' — элементам η_β; используя свойство линейности, легко проверить, что эта формула справедлива также и в общем случае.

Таким образом, мы доказали существование алгебры $\mathfrak{L} \otimes \mathfrak{M}$ с требуемыми свойствами. Покажем теперь, что условиями 1), 2) и 3) алгебра $\mathfrak{L} \otimes \mathfrak{M}$ определена однозначно с точностью до изоморфизма. Действительно, в силу 1) и 2) каждый элемент из $\mathfrak{L} \otimes \mathfrak{M}$ является линейной комбинацией произведений $\xi_\alpha \eta_\beta$ элементов базисов $(\xi_\alpha)_{\alpha \in A}$ и $(\eta_\beta)_{\beta \in B}$. В силу 3) эти произведения образуют базис пространства $\mathfrak{L} \otimes \mathfrak{M}$. Наконец, в силу 1) имеем $(\xi_\alpha \eta_\beta)(\xi_{\alpha'} \eta_{\beta'}) = (\xi_\alpha \xi_{\alpha'})(\eta_\beta \eta_{\beta'})$, откуда следует, что умножение в $\mathfrak{L} \otimes \mathfrak{M}$ определено однозначно.

Алгебра $\mathfrak{L} \otimes \mathfrak{M}$ называется *кронекеровским произведением* алгебр $\mathfrak{L}$ и $\mathfrak{M}$. Очевидно, что если $\mathfrak{L}'$ и $\mathfrak{M}'$ — подалгебры алгебр $\mathfrak{L}$ и $\mathfrak{M}$ соответственно, то $\mathfrak{L}' \otimes \mathfrak{M}'$ является подалгеброй алгебры $\mathfrak{L} \otimes \mathfrak{M}$.

Предположим теперь, что алгебры $\mathfrak{L}$ и $\mathfrak{M}$ имеют единицы $1(\mathfrak{L})$ и $1(\mathfrak{M})$ соответственно. Очевидно, что тогда $1(\mathfrak{L})\,1(\mathfrak{M})$ является единицей алгебры $\mathfrak{L}\otimes\mathfrak{M}$. Далее, элементы $x1(\mathfrak{M})\,(x\in\mathfrak{L})$ образуют подалгебру алгебры $\mathfrak{L}\otimes\mathfrak{M}$, изоморфную алгебре $\mathfrak{L}$; эту подалгебру мы будем отождествлять с $\mathfrak{L}$. Аналогично, алгебру $\mathfrak{M}$ будем также рассматривать как подалгебру в $\mathfrak{L}\otimes\mathfrak{M}$.

Пусть $\mathfrak{L}=L$ есть поле. Так как L является подалгеброй алгебры $L\otimes\mathfrak{M}$ (и единица поля L совпадает с единицей алгебры $L\otimes\mathfrak{M}$), то $L\otimes\mathfrak{M}$ можно рассматривать как алгебру над полем L. Эта алгебра обозначается через $\mathfrak{M}_L$. Будем говорить, что алгебра $\mathfrak{M}_L$ получена из $\mathfrak{M}$ расширением основного поля K до поля L. Покажем, что каждый базис $(\eta_\beta)_{\beta\in B}$ алгебры $\mathfrak{M}$ относительно K является также базисом алгебры $\mathfrak{M}_L$ относительно L. Прежде всего очевидно, что каждый элемент из $\mathfrak{M}_L$ может быть представлен в виде линейной комбинации элементов η_β с коэффициентами из L. Далее, предположим, что $\sum\limits_{\beta\in B} x_\beta\eta_\beta=0$, где среди элементов $x_\beta\in L$ имеется только конечное число отличных от 0. Если $(\xi_\alpha)_{\alpha\in A}$ есть базис L относительно K, то каждый элемент x_β можно записать в виде $\sum\limits_{\alpha\in A} c_{\alpha\beta}\xi_\alpha$, $c_{\alpha\beta}\in K$, и мы получаем $\sum\limits_{\alpha,\beta} c_{\alpha\beta}\xi_\alpha\eta_\beta=0$, откуда $c_{\alpha\beta}=0$ при всех α и β, а значит, $x_\beta=0$ при всех β.

Если L' есть подполе поля L, содержащее K, то $\mathfrak{M}_{L'}$ является алгеброй над L'; из предыдущего непосредственно следует, что алгебру $\mathfrak{M}_L$ можно рассматривать как алгебру, полученную из $\mathfrak{M}_{L'}$ расширением основного поля L' до поля L, т. е. $\mathfrak{M}_L=(\mathfrak{M}_{L'})_L$.

Нас будет интересовать главным образом случай, когда обе алгебры $\mathfrak{L}=L$ и $\mathfrak{M}=M$ являются полями. Может случиться, что поля L и M являются подполями некоторого поля Ω. В этом случае возникает трудность в обозначениях, ибо такие выражения как $x+y$ или xy (где $x\in L$, $y\in M$) имеют разные значения, смотря по тому, где рассматриваются операции сложения и умножения, в алгебре $L\otimes M$ или в поле Ω. В случае возможных недоразумений для выяснения ситуации мы будем давать дополнительные указания в контексте.

Лемма 1. Пусть L и M — два расширения поля K. Предположим, что нам заданы изоморфизмы λ и μ полей L и M соответственно в некоторое надполе Ω поля K, причем оба изоморфизма λ и μ отображают каждый элемент поля K на себя. Тогда существует гомоморфизм φ алгебры $L \otimes M$ в поле Ω, который совпадает с λ на L и с μ на M; при этом образ $\varphi(L \otimes M)$ будет равен подкольцу поля Ω, порожденному полями $\lambda(L)$ и $\mu(M)$.

Пусть $(\xi_\alpha)_{\alpha \in A}$ и $(\eta_\beta)_{\beta \in B}$ — базисы относительно K полей L и M соответственно. Тогда произведения $\xi_\alpha \eta_\beta$ образуют базис алгебры $L \otimes M$. Мы можем определить линейное отображение φ алгебры $L \otimes M$ в поле Ω, при котором произведению $\xi_\alpha \eta_\beta$ соответствует элемент $\lambda(\xi_\alpha)\mu(\eta_\beta)$ поля Ω. Можно считать, что единица поля L является одним из элементов ξ_α, скажем ξ_{α_0}, а единица поля M является одним из элементов η_β, скажем η_{β_0}. Так как $\xi_\alpha = \xi_\alpha \eta_{\beta_0}$ и $\eta_\beta = \xi_{\alpha_0} \eta_\beta$, то φ совпадает с λ на L и с μ на M. Из нашего определения умножения в алгебре $L \otimes M$ непосредственно следует, что φ есть гомоморфизм алгебры $L \otimes M$ в поле Ω (рассматриваемое также как алгебра над K). Образ $\varphi(L \otimes M)$ является, следовательно, подкольцом поля Ω; очевидно, что оно совпадает с кольцом, порожденным полями $\lambda(L)$ и $\mu(M)$.

§ 5. Расширение $\mathfrak{p}$-адического пополнения

Пусть R и S — поля алгебраических функций от одной переменной, причем S является надполем поля R (с обычными предположениями о полях констант, см. § 1). Обозначим через $\mathfrak{p}$ точку поля R, а через $\mathfrak{P}$ — точку поля S, лежащую над $\mathfrak{p}$. Пусть $\bar{R}$ — $\mathfrak{p}$-адическое пополнение поля R, а $\bar{S}$ — $\mathfrak{P}$-адическое пополнение поля S. Если элемент $\bar{u} \in \bar{R}$ является пределом последовательности (u_n) элементов из R, то последовательность (u_n), рассматриваемая как последовательность элементов поля S, также сходится к некоторому пределу из $\bar{S}$. Действительно, число $\nu_{\mathfrak{P}}(u_{n+1} - u_n) = e\nu_{\mathfrak{p}}(u_{n+1} - u_n)$ неограниченно растет при возрастании n (здесь через e обозначен индекс разветвления точки $\mathfrak{P}$ относительно R). Более того, если $\bar{u}$ является в то же время пределом другой последовательности (u'_n) элементов из R, то $\nu_{\mathfrak{P}}(u'_n - u_n) = e\nu_{\mathfrak{p}}(u'_n - u_n)$ неограниченно возрастает при

$n \to \infty$, а это говорит о том, что последовательности (u_n) и (u'_n) имеют один и тот же предел в поле $\bar{S}$. Если мы этот предел сопоставим элементу $\bar{u}$, то получим отображение поля $\bar{R}$ в $\bar{S}$, при котором каждый элемент поля R отображается на себя. Легко видеть, что это отображение является кольцевым гомоморфизмом. Так как $\bar{R}$ — поле, то оно является изоморфизмом. Часто поле $\bar{R}$ мы будем отождествлять с его образом при только что построенном изоморфизме, т. е. поле $\bar{R}$ будем рассматривать как подполе поля $\bar{S}$.

Предположим теперь, что S имеет конечную степень над R. Обозначим через $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$, а через $\bar{S}_\lambda$ — $\mathfrak{P}_\lambda$-адическое пополнение поля S $(1 \leqslant \lambda \leqslant h)$. Произведение $\prod_{\lambda=1}^{h} \bar{S}_\lambda$ есть алгебра над полем $\bar{R}$, элементами которой являются последовательности $(y_1, \ldots, y_n)$, где $y_\lambda \in \bar{S}_\lambda$ $(1 \leqslant \lambda \leqslant h)$. В этой алгебре действия определены формулами:

$$(y_1, \ldots, y_h) + (z_1, \ldots, z_h) = (y_1 + z_1, \ldots, y_h + z_h),$$
$$(y_1, \ldots, y_h)(z_1, \ldots, z_h) = (y_1 z_1, \ldots, y_h z_h),$$
$$x(y_1, \ldots, y_h) = (xy_1, \ldots, xy_h)$$

(где $y_\lambda, z_\lambda \in \bar{S}_\lambda$, $1 \leqslant \lambda \leqslant h$; $x \in \bar{R}$).

Теорема 4. *Пусть R и S — два поля алгебраических функций от одной переменной, причем S является расширением поля R конечной степени. Пусть $\mathfrak{p}$ — точка поля R, $\bar{R}$ — $\mathfrak{p}$-адическое пополнение поля R и $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$. Тогда произведение $\mathfrak{P}_\lambda$-адических пополнений поля S $(1 \leqslant \lambda \leqslant h)$ является алгеброй над полем $\bar{R}$, изоморфной алгебре $S_{\bar{R}}$, которая получена из S (рассматриваемого как алгебра над R) расширением основного поля R до поля $\bar{R}$.*

Для доказательства построим гомоморфизм Φ алгебры $S_{\bar{R}}$ в $\prod_{\lambda=1}^{h} \bar{S}_\lambda$ и отображение Ψ произведения $\prod_{\lambda=1}^{h} \bar{S}_\lambda$ в $S_{\bar{R}}$, а затем

докажем, что $\Phi\Psi$ есть тождественное отображение $\prod_{\lambda=1}^{h}\bar{S}_\lambda$ на себя, а $\Psi\Phi$ — тождественное отображение $S_{\bar{R}}$ на себя.

Каждое поле $\bar{S}_\lambda$ содержит в качестве подполей S и $\bar{R}$; поэтому, в силу леммы 1 § 4, существует гомоморфизм Φ_λ алгебры $S_{\bar{R}}$ в поле $\bar{S}_\lambda$, при котором каждый элемент из полей S и $\bar{R}$ отображается на себя. Если мы положим $\Phi(u)=(\Phi_1(u), \ldots, \Phi_h(u))$ (для $u\in S_{\bar{R}}$), то, очевидно, получим гомоморфизм Φ алгебры $S_{\bar{R}}$ в $\prod_{\lambda=1}^{h}\bar{S}_\lambda$.

Пусть $(y_1, \ldots, y_n)$ — произвольный элемент из $\prod_{\lambda=1}^{h}\bar{S}_\lambda$. Для каждого целого числа $m>0$ и для каждого λ $(1\leqslant\lambda\leqslant h)$ мы можем найти такой элемент $y'_{m,\lambda}\in S$, что

$$\nu_{\mathfrak{P}_\lambda}(y_\lambda-y'_{m,\lambda})\geqslant me_\lambda$$

(где e_λ — индекс разветвления точки $\mathfrak{P}_\lambda$ относительно R). В силу теоремы 3 § 6 гл. I в поле S существует элемент y'_m такой, что $\nu_{\mathfrak{P}_\lambda}(y'_m-y'_{m,\lambda})\geqslant me_\lambda$ $(1\leqslant\lambda\leqslant h)$. Очевидно, что

$$\nu_{\mathfrak{P}_\lambda}(y_\lambda-y'_m)\geqslant me_\lambda \quad (1\leqslant\lambda\leqslant h), \tag{1}$$

откуда

$$\nu_{\mathfrak{P}_\lambda}(y'_{m+1}-y'_m)\geqslant me_\lambda \quad (1\leqslant\lambda\leqslant h). \tag{2}$$

Введем теперь в рассмотрение базис $\{z_1, \ldots, z_n\}$ поля S относительно R, который будем предполагать целым в точке $\mathfrak{p}$. Пусть t — униформизирующая переменная в точке $\mathfrak{p}$ поля R. Запишем

$$y'_m=\sum_{i=1}^{n}x_{im}z_i, \quad x_{im}\in R;$$

в силу (2) имеем $\nu_{\mathfrak{P}_\lambda}(t^{-m}(y'_{m+1}-y'_m))\geqslant 0$; так как базис $\{z_1, \ldots, z_n\}$ целый в точке $\mathfrak{p}$, то $\nu_{\mathfrak{p}}(t^{-m}(x_{i,m+1}-x_{i,m}))\geqslant 0$, т. е. $\nu_{\mathfrak{p}}(x_{i,m+1}-x_{i,m})\geqslant m$. Таким образом, каждая последовательность $(x_{i,m})_{1\leqslant m<\infty}$ сходится к некоторому элементу x_i поля $\bar{R}$. Покажем, что элементы x_i не зависят

от выбора аппроксимирующих элементов y'_m, удовлетворяющих условиям (1). Действительно, если (y^*_m) есть другая последовательность элементов поля S такая, что $\nu_{\mathfrak{P}_\lambda}(y_\lambda - y^*_m) \geqslant me_\lambda$ $(1 \leqslant \lambda \leqslant h)$, то $\nu_{\mathfrak{P}_\lambda}(y^*_m - y'_m) \geqslant me_\lambda$; пусть $y^*_m = \sum_{i=1}^{n} x^*_{i,m} z_i$, тогда аналогично вышеизложенному получим, что $\nu_{\mathfrak{p}}(x^*_{i,m} - x_{i,m}) \geqslant m$, откуда $\lim\limits_{m \to \infty} x^*_{i,m} = x_i$. Теперь мы можем определить отображение Ψ произведения $\prod_{\lambda=1}^{h} \overline{S}_\lambda$ в $S_{\overline{R}}$, полагая $\Psi(y_1, \ldots, y_h) = \sum_{i=1}^{n} x_i z_i$.

Образ элемента $\sum_{i=1}^{n} x_i z_i$ из $S_{\overline{R}}$ $(x_i \in \overline{R},\ 1 \leqslant i \leqslant n)$ при гомоморфизме Φ_λ алгебры $S_{\overline{R}}$ в поле $\overline{S}_\lambda$ есть элемент поля $\overline{S}_\lambda$, который представляется тем же выражением $\sum_{i=1}^{n} x_i z_i$, но теперь в этом выражении операции сложения и умножения предполагаются выполненными в поле $\overline{S}_\lambda$.

Так как $\nu_{\mathfrak{P}_\lambda}(x_i - x_{i,m}) \geqslant me_\lambda$ и $\nu_{\mathfrak{P}_\lambda}(z_i) \geqslant 0$, то $\nu_{\mathfrak{P}_\lambda}(\Phi_\lambda \Psi(y_1, \ldots, y_h) - y'_m) \geqslant me_\lambda$. Сравнивая последнее неравенство с неравенством (1), получаем, что $\Phi_\lambda \Psi(y_1, \ldots, y_h) = y_\lambda$ $(1 \leqslant \lambda \leqslant h)$. Этим доказано, что отображение $\Phi\Psi$ является тождественным отображением произведения $\prod_{\lambda=1}^{h} \overline{S}_\lambda$ на себя.

Пусть $x_1, \ldots, x_n$ — произвольные элементы поля $\overline{R}$. Для каждого целого числа $m > 0$ выберем в поле R элементы $x_{1m}, \ldots, x_{nm}$ так, чтобы $\nu_{\mathfrak{p}}(x_i - x_{im}) \geqslant m$ $(1 \leqslant i \leqslant n)$, и положим

$$y'_m = \sum_{i=1}^{n} x_{im} z_i.$$

Тогда для каждого λ будем иметь $\nu_{\mathfrak{P}_\lambda}(y'_{m+1} - y'_m) \geqslant me_\lambda$, откуда следует, что последовательность (y'_m) сходится в поле $\overline{S}_\lambda$ к некоторому пределу y_λ, кроме того, $y_\lambda =$

$=\sum_{i=1}^{n} x_i z_i$, считая при этом, что операции выполнены в поле $\bar{S}_\lambda$. Если $u=\sum_{i=1}^{n} x_i z_i$ (где операции выполнены в $S_{\bar{R}}$), то $\Phi(u)=(y_1, \ldots, y_h)$ и $\Psi\Phi(u)=u$. Этим доказано, что $\Psi\Phi$ есть тождественное отображение алгебры $S_{\bar{R}}$ на себя.

Таким образом, Φ есть взаимно однозначное отображение алгебры $S_{\bar{R}}$ на $\prod_{\lambda=1}^{h} \bar{S}_\lambda$. Так как нам уже известно, что Φ является гомоморфизмом, то на самом деле Φ есть изоморфизм. Теорема 4, таким образом, доказана.

Замечание. Элемент $(y_1, \ldots, y_h)$ из $\prod_{\lambda=1}^{h} \bar{S}_\lambda$ назовем *целым*, если для каждого λ элемент y_λ является целым в поле $\bar{S}_\lambda$. Пользуясь обозначениями доказательства теоремы 4, замечаем тогда, что элементы y'_m из S являются целыми в каждой точке $\mathfrak{P}_\lambda$; поэтому коэффициенты x_{im}, а также их пределы x_i, являются целыми в точке $\mathfrak{p}$. Таким образом, *построенный изоморфизм между* $S_{\bar{R}}$ *и* $\prod_{\lambda=1}^{h} \bar{S}_\lambda$ *обладает следующим свойством: элемент из* $\prod_{\lambda=1}^{h} \bar{S}_\lambda$ *является целым тогда и только тогда, если он соответствует линейной комбинации элементов целого в точке* $\mathfrak{p}$ *базиса поля* S *относительно* R *с целыми коэффициентами из* $\bar{R}$.

Из теоремы 4 вытекает также, что каждое поле $\bar{S}_\lambda$ имеет конечную степень n_λ над $\bar{R}$ и что $\sum_{\lambda=1}^{h} n_\lambda = n = [S:R]$. Пусть e_λ и f_λ — индекс разветвления и относительная степень точки $\mathfrak{P}_\lambda$ по отношению к полю R. Нам уже известно (теорема 1 § 1), что $\sum_{\lambda=1}^{h} e_\lambda f_\lambda = n$. Мы сейчас докажем, что n_λ всегда равно $e_\lambda f_\lambda$.

Теорема 5. *Пусть* R *и* S — *два поля алгебраических функций от одной переменной, причем* S *является расширением поля* R *конечной степени. Введем следующие*

обозначения: $\mathfrak{p}$ — точка поля R; $\mathfrak{P}$ — точка поля S, лежащая над $\mathfrak{p}$; $\bar{R}$ — $\mathfrak{p}$-адическое пополнение поля R; $\bar{S}$ — $\mathfrak{P}$-адическое пополнение поля S; e и f — индекс разветвления и относительная степень соответственно точки $\mathfrak{P}$ по отношению к полю R; $\Sigma(\mathfrak{p})$ и $\Sigma(\mathfrak{P})$ — поля вычетов точек $\mathfrak{p}$ и $\mathfrak{P}$ соответственно. Пусть $v_1, \ldots, v_f$ — целые элементы поля $\bar{S}$, классы вычетов которых по модулю $\mathfrak{P}$ образуют базис поля $\Sigma(\mathfrak{P})$ относительно $\Sigma(\mathfrak{p})$, и пусть u — элемент из $\bar{S}$, для которого $\nu_{\mathfrak{P}}(u)=1$. Тогда ef элементов $u^i v_j$ $(0 \leqslant i \leqslant e-1,\ 1 \leqslant j \leqslant f)$ образуют базис поля $\bar{S}$ относительно $\bar{R}$, и каждый целый элемент из $\bar{S}$ может быть записан в виде

$$\sum_{i=0}^{e-1} \sum_{j=1}^{f} x_{ij} u^i v_j,$$

где коэффициенты x_{ij} — целые элементы поля $\bar{R}$.

Пусть x_{ij} — элементы поля $\bar{R}$, а m — целое неотрицательное число. Докажем, что если

$$\nu_{\mathfrak{P}}\left(\sum_{i=0}^{e-1} \sum_{j=1}^{f} x_{ij} u^i v_j\right) \geqslant em,$$

то $\nu_{\mathfrak{p}}(x_{ij}) \geqslant m$ при всех i и j. Пусть m_0 — наименьшее из чисел $\nu_{\mathfrak{p}}(x_{ij})$; будем считать, что $m_0 = \nu_{\mathfrak{p}}(x_{i_0 j_0})$ и что $\nu_{\mathfrak{p}}(x_{ij}) > m_0$ при $i < i_0$, $1 \leqslant j \leqslant f$. Пусть t — униформизирующая переменная в точке $\mathfrak{p}$ поля R. Тогда элементы $t^{-m_0} x_{i_0 j}$ $(1 \leqslant j \leqslant f)$ являются целыми в поле $\bar{R}$. Пусть ξ_j есть класс вычетов элемента $t^{-m_0} x_{i_0 j}$ по модулю $\mathfrak{p}$; так как классы вычетов $v_1^*, \ldots, v_f^*$ элементов $v_1, \ldots, v_f$ образуют базис поля $\Sigma(\mathfrak{P})$ относительно $\Sigma(\mathfrak{p})$ и $\xi_{j_0} \neq 0$, то

$$\sum_{j=1}^{f} \xi_j v_j^* \neq 0, \text{ откуда } \nu_{\mathfrak{P}}\left(\sum_{j=1}^{f} t^{-m_0} x_{i_0 j} v_j\right) = 0 \text{ и}$$

$$\nu_{\mathfrak{P}}\left(\sum_{j=1}^{f} x_{i_0 j} u^{i_0} v_j\right) = i_0 + m_0 e. \tag{3}$$

Если $i < i_0$, то

$$\nu_{\mathfrak{P}}(x_{ij} u^i v_j) = i + e\nu\ (x_{ij}) \geqslant i + e(m_0 + 1) > i_0 + m_0 e, \tag{4}$$

ибо $i+e \geqslant e > i_0$. Если $i > i_0$, то

$$\nu_{\mathfrak{P}}(x_{ij}u^iv_j) \geqslant i + m_0e > i_0 + m_0e. \tag{5}$$

В силу (3), (4) и (5) получаем $\nu_{\mathfrak{P}}\left(\sum_{i=0}^{e-1}\sum_{j=1}^{f} x_{ij}u^iv_j\right) = i_0 + m_0e \geqslant me$, откуда следует, что $m_0 \geqslant m$ (ибо $i_0 < e$).

В частности, если $\sum_{i=0}^{e-1}\sum_{j=1}^{f} x_{ij}u^iv_j = 0$, то необходимо $x_{ij} = 0$ $(0 \leqslant i \leqslant e-1,\ 1 \leqslant j \leqslant f)$. Таким образом, элементы u^iv_j линейно независимы над $\bar{R}$, откуда следует, что $[\bar{S} : \bar{R}] \geqslant ef$. Пусть теперь $\mathfrak{P}_1 = \mathfrak{P}, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$, и пусть e_λ и f_λ — индекс разветвления и относительная степень соответственно точки $\mathfrak{P}_\lambda$ по отношению к полю R. Если $\bar{S}_\lambda$ есть $\mathfrak{P}_\lambda$-адическое пополнение поля S, то по доказанному $[\bar{S}_\lambda : \bar{R}] \geqslant e_\lambda f_\lambda$. С другой стороны, $\sum_{\lambda=1}^{h}[\bar{S}_\lambda : \bar{R}] = [S : R] = \sum_{\lambda=1}^{h} e_\lambda f_\lambda$ (теорема 4 и теорема 1 § 1). Следовательно, для всех λ мы имеем $[\bar{S}_\lambda : \bar{R}] = e_\lambda f_\lambda$, в частности, $[\bar{S} : \bar{R}] = ef$. Таким образом, система линейно независимых над $\bar{R}$ элементов u^iv_j является базисом поля $\bar{S}$ относительно $\bar{R}$. Применяя установленный в начале доказательства результат для случая $m = 0$, заключаем, что наш базис обладает свойством, указанным в конце теоремы 5.

Следствие 1. *Пусть сохраняются обозначения теоремы 5. Тогда коэффициенты характеристического многочлена относительно $\bar{R}$ любого целого элемента y поля $\bar{S}$ принадлежат кольцу целых элементов поля $\bar{R}$.*

Пусть $z_1, \ldots, z_{\bar{n}}$ — элементы u^iv_j, выписанные в некотором порядке $(\bar{n} = ef)$. Тогда $yz_i = \sum_{i=1}^{\bar{n}} \eta_{ij}z_j$, где η_{ij} — целые элементы из $\bar{R}$. Так как характеристический многочлен $F(X)$ элемента y относительно $\bar{R}$ равен определителю матрицы $XE - (\eta_{ij})$, где E — единичная матрица порядка $\bar{n}$, то следствие 1 доказано.

Следствие 2. *Если $y \in \bar{S}$ и $y \neq 0$, то $\nu_{\mathfrak{p}}(N_{\bar{S}/\bar{R}} y) = f\nu_{\mathfrak{P}}(y)$.*

Из следствия 1 вытекает, что норма (относительно поля $\bar{R}$) целого элемента поля $\bar{S}$ является целым элементом поля $\bar{R}$; следовательно, норма любого делителя единицы из кольца целых элементов поля $\bar{S}$ является делителем единицы в кольце целых элементов поля $\bar{R}$. Элемент y мы можем представить в виде $y = wu^m$, где w — делитель единицы в кольце целых элементов поля $\bar{S}$ и $m = \nu_{\mathfrak{P}}(y)$. Тогда, очевидно, будем иметь $\nu_{\mathfrak{p}}(N_{\bar{S}/\bar{R}} y) = a\nu_{\mathfrak{P}}(y)$, где число $a = \nu_{\mathfrak{p}}(N_{\bar{S}/\bar{R}} u)$ не зависит от y. Возьем теперь в качестве y элемент $t \in \bar{R}$, для которого $\nu_{\mathfrak{p}}(t) = 1$; тогда $N_{\bar{S}/\bar{R}} t = t^{ef}$, откуда $ef = a\nu_{\mathfrak{P}}(t) = ae$ и $a = f$.

Следствие 3. *Сохраняя обозначения теоремы 5, имеем $\bar{S} = \bar{R}\langle S\rangle$.*

Это следствие вытекает из того, что элементы $u, v_1, \ldots, v_f$ поля $\bar{S}$ могут быть взяты из поля S.

Вернемся опять к обозначениям теоремы 4. Пусть y — произвольный элемент из $S_{\bar{R}}$; отображение $z \to yz$ является эндоморфизмом векторного пространства $S_{\bar{R}}$ над полем $\bar{R}$. Алгебру $S_{\bar{R}}$ отождествим на время с алгеброй $\prod_{\lambda=1}^{h} \bar{S}_\lambda$, используя изоморфизм, построенный при доказательстве теоремы 4. Пусть $\{z_{1\lambda}, \ldots, z_{n_\lambda\lambda}\}$ есть базис поля $\bar{S}_\lambda$ относительно $\bar{R}$ $(1 \leqslant \lambda \leqslant h)$; обозначим через $z'_{i\lambda}$ элемент алгебры $S_{\bar{R}}$, у которого $\left(\text{если его рассматривать как элемент произведения } \prod_{\lambda=1}^{h} \bar{S}_\lambda\right)$ λ-координата равна $z_{i\lambda}$, а все остальные координаты равны 0. Все элементы $z'_{i\lambda}$ $(1 \leqslant i \leqslant n_\lambda,\ 1 \leqslant \lambda \leqslant h)$, вместе взятые, образуют базис алгебры $S_{\bar{R}}$ относительно $\bar{R}$. Если мы через y_λ обозначим λ-координату элемента y $\left(\text{рассматриваемого как элемент из } \prod_{\lambda=1}^{h} \bar{S}_\lambda\right)$, то будем иметь

$y_\lambda z_{i\lambda} = \sum_{j=1}^{n_\lambda} x_{ij\lambda} z_{j\lambda}$, где $x_{ij\lambda} \in \overline{R}$, откуда

$$yz'_{i\lambda} = \sum_{j=1}^{n_\lambda} x_{ij\lambda} z'_{j\lambda}.$$

Обозначим через Ξ_λ матрицу $(x_{ij\lambda})_{1 \leqslant i,\, j \leqslant n_\lambda}$; тогда как легко видеть, характеристический многочлен эндоморфизма $z \to yz$ будет равен произведению характеристических многочленов матриц Ξ_λ, а характеристический многочлен матрицы Ξ_λ в свою очередь равен характеристическому многочлену элемента y_λ относительно $\overline{R}$. С другой стороны, если $y \in S$, то все элементы y_λ будут равны y, а характеристический, многочлен эндоморфизма $z \to yz$ алгебры $S_{\overline{R}}$ будет, очевидно, равен характеристическому многочлену элемента y относительно R. Таким образом, нами доказана

Теорема 6. *Пусть R и S — поля алгебраических функций от одной переменной, причем S есть расширение поля R конечной степени. Пусть, далее, $\mathfrak{p}$ — точка поля R; $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$; $\overline{R}$ — $\mathfrak{p}$-адическое пополнение поля R; $\overline{S}_\lambda$ — $\mathfrak{P}_\lambda$-адическое пополнение поля S $(1 \leqslant \lambda \leqslant h)$. Тогда характеристический многочлен элемента $y \in S$ относительно R равен произведению характеристических многочленов этого элемента, рассматриваемого последовательно как элемент полей $\overline{S}_1, \ldots, \overline{S}_h$ относительно поля $\overline{R}$.*

Пусть $\mathfrak{P}$ — одна из точек $\mathfrak{P}_\lambda$, а $\overline{S}$ — соответствующее пополнение поля S. Если $y \in \overline{S}$, то через $\mathrm{Sp}^{\mathfrak{P}} y$ и $\mathrm{N}^{\mathfrak{P}} y$ мы будем обозначать, соответственно, след и норму элемента y относительно поля $\overline{R}$. Из теоремы 6 непосредственно вытекает следующее следствие:

Следствие 1. *В обозначениях теоремы 6 имеем*

$$\mathrm{N}_{S/R} y = \prod_{\lambda=1}^{h} \mathrm{N}^{\mathfrak{P}_\lambda} y, \quad \mathrm{Sp}_{S/R} y = \sum_{\lambda=1}^{h} \mathrm{Sp}^{\mathfrak{P}_\lambda} y.$$

Следствие 2. *В обозначениях теоремы 6 имеем*

$$\nu_{\mathfrak{p}}(\mathrm{N}_{S/R} y) = \sum_{\lambda=1}^{h} f_\lambda \nu_{\mathfrak{P}_\lambda}(y),$$

где f_λ — относительная степень точки $\mathfrak{P}_\lambda$ по отношению к полю R.

Это следствие непосредственно вытекает из следствия 1 и следствия 2 к теореме 5.

§ 6. Разложения Пюизё

Пусть R — поле алгебраических функций от одной переменной над алгебраически замкнутым полем констант K, и пусть S — расширение поля R конечной степени. Обозначим через $\mathfrak{p}$ точку поля R, а через $\mathfrak{P}$ — точку поля S, лежащую над $\mathfrak{p}$. Так как поле K алгебраически замкнуто, то степени точек $\mathfrak{p}$ и $\mathfrak{P}$ равны 1. Пусть t — униформизирующая переменная в точке $\mathfrak{p}$; тогда $\mathfrak{p}$-адическое пополнение $\bar{R}$ поля R можно отождествить с полем формальных степенных рядов от t с коэффициентами из K (§ 3 гл. III).

Пусть e — индекс разветвления точки $\mathfrak{P}$ относительно R. *Предположим, что e не делится на характеристику p поля K.* Докажем, что в этом случае элемент t является e-ой степенью некоторого элемента из $\mathfrak{P}$-адического пополнения $\bar{S}$ поля S. Пусть u — униформизирующая переменная в точке $\mathfrak{P}$ поля S. Мы знаем, что $\nu_{\mathfrak{P}}(t) = e$; следовательно, $t = u^e v$, где $\nu_{\mathfrak{P}}(v) = 0$. Так как поле K алгебраически замкнуто, то существует элемент $a \in K$ такой, что $\nu_{\mathfrak{P}}(v - a) > 0$, кроме того, элемент a можно представить в виде b^e, $b \in K$. Рассмотрим многочлен $W^e - v = f(W)$ от W. Его коэффициенты принадлежат кольцу целых элементов поля $\bar{S}$; если мы заменим эти коэффициенты их классами вычетов по модулю $\mathfrak{P}$, то получим многочлен $f^*(W) = W^e - b^e$, обладающий линейным множителем $W - b$: $f^*(W) = (W - b)h^*(W)$. Элемент b является простым корнем многочлена $f^*(W)$; в самом деле, $\left.\frac{df^*(W)}{dW}\right|_{W=b} = eb^{e-1} \neq 0$, ибо $b \neq 0$ и e не делится на p. Используя лемму Хензеля (§ 2 гл. III), получаем, что многочлен $f(W)$ обладает линейным множителем с коэффициентами из $\bar{S}$; а это означает, что $v = w^e$, $w \in \bar{S}$, откуда $t = (uw)^e$.

Обозначим через $t^{\frac{1}{e}}$ какой-нибудь один из корней e-ой степени из элемента t в поле $\bar{S}$; тогда очевидно, что

$$\nu_{\mathfrak{P}}\left(t^{\frac{1}{e}}\right) = 1,$$

Отсюда следует, что поле $\bar{S}$ можно рассматривать как поле формальных степенных рядов от $t^{\frac{1}{e}}$ с коэффициентами из K. Разложения элементов поля S в степенные ряды от $t^{\frac{1}{e}}$ называются *разложениями Пюизё*.

В случае, если индекс разветвления e точки $\mathfrak{P}$ поля S делится на характеристику p поля K, то, вообще говоря, элемент t не является e-ой степенью в поле $\bar{S}$. Рассмотрим, например, случай, когда $R=K\langle x\rangle$ (x — трансцендентный элемент над K) и $S=K\langle x, y\rangle$, где y удовлетворяет уравнению $y^p-y-\frac{1}{x}=0$. Пусть точка $\mathfrak{p}$ является нулем элемента x в поле R и пусть $\mathfrak{P}$ есть точка поля S, лежащая над $\mathfrak{p}$. Мы имеем $\nu_{\mathfrak{P}}\left(\frac{1}{x}\right)=-e$, где e — индекс разветвления точки $\mathfrak{P}$ относительно R. Отсюда следует, что $\nu_{\mathfrak{P}}(y)<0$; значит $\nu_{\mathfrak{P}}(y^p)<\nu_{\mathfrak{P}}(y)$ и $\nu_{\mathfrak{P}}(y^p)=\nu_{\mathfrak{P}}(y^p-y)=-e$, и мы получили, что e делится на p. С другой стороны, $e\leqslant[S:R]\leqslant p$; следовательно, $e=[S:R]=p$ и уравнение $Y^p-Y-\frac{1}{x}=0$ неприводимо в поле R. Так как $[\bar{S}:\bar{R}]=e=p$, то многочлен $Y^p-Y-\frac{1}{x}$ неприводим и в поле $\bar{R}$. Легко видеть, что $y+1$ также является корнем уравнения $Y^p-Y-\frac{1}{x}=0$. Следовательно, поле $\bar{S}$ обладает автоморфизмом порядка p, который не меняет элементов из $\bar{R}$. Таким образом, поле $\bar{S}$ сепарабельно над $\bar{R}$. Так как элемент t не является, очевидно, p-ой степенью в поле $\bar{R}$, то он не является p-ой степенью также и в поле $\bar{S}$.

§ 7. Норма и конорма; след и коследа

Пусть R и S — два поля алгебраических функций от одной переменной, причем поле R содержится в S. Как всегда, мы считаем, что выполняются наши обычные предположения о полях констант (см. § 1). В этом параграфе мы установим некоторые соответствия между дивизорами и распределениями полей R и S.

Если x есть отличный от 0 элемент поля R, то через $\mathfrak{d}_R(x)$ и $\mathfrak{d}_S(x)$ мы будем обозначать дивизоры элемента x в полях R и S соответственно. Пусть $\mathfrak{p}$ — произвольная точка поля R, а $\mathfrak{P}$ — точка поля S, лежащая над $\mathfrak{p}$; показатель $a(\mathfrak{p})$, с которым точка $\mathfrak{p}$ входит в дивизор $\mathfrak{d}_R(x)$, равен $\nu_{\mathfrak{p}}(x)$, в то время как показатель точки $\mathfrak{P}$ в дивизоре $\mathfrak{d}_S(x)$ равен $\nu_{\mathfrak{P}}(x) = e(\mathfrak{P})\nu_{\mathfrak{p}}(x) = e(\mathfrak{P})a(\mathfrak{p})$, где $e(\mathfrak{P})$ — индекс разветвления точки $\mathfrak{P}$ относительно R. С другой стороны, если $\mathfrak{P}$ — переменная точка поля S по отношению к R, то $\nu_{\mathfrak{P}}(x) = 0$. Это подводит нас к следующему определению. Пусть $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ — произвольный дивизор поля R. Если $\mathfrak{P}$ есть точка поля S, лежащая над точкой $\mathfrak{p}$ поля R, то положим $A(\mathfrak{P}) = e(\mathfrak{P})a(\mathfrak{p})$, где $e(\mathfrak{P})$ — индекс разветвления точки $\mathfrak{P}$ относительно R; если же $\mathfrak{P}$ — переменная точка поля S, то полагаем $A(\mathfrak{P}) = 0$. Так как над каждой точкой поля R лежит лишь конечное число точек поля S, то $A(\mathfrak{P}) \neq 0$ только для конечного числа точек $\mathfrak{P}$ поля S. Следовательно, символ $\prod_{\mathfrak{P}} \mathfrak{P}^{A(\mathfrak{P})}$ является дивизором поля S. Этот дивизор мы будем называть *конормой* дивизора $\mathfrak{a}$ (из R в S) и обозначать через $\mathrm{Con}_{R/S}\mathfrak{a}$. Если $\mathfrak{a}$ и $\mathfrak{b}$ — дивизоры поля R, то, очевидно, имеем

$$\mathrm{Con}_{R/S}\mathfrak{a}\mathfrak{b} = (\mathrm{Con}_{R/S}\mathfrak{a})(\mathrm{Con}_{R/S}\mathfrak{b}),$$

а если x — элемент поля R, отличный от 0, то

$$\mathrm{Con}_{R/S}\,\mathfrak{d}_R(x) = \mathfrak{d}_S(x).$$

Лемма 1. *Предположим, что поле S имеет конечную степень над R, и обозначим через K и L поля констант полей R и S соответственно. Тогда для любого дивизора $\mathfrak{a}$ поля R имеем:*

$$d(\mathrm{Con}_{R/S}\mathfrak{a}) = \frac{[S:R]}{[L:K]}\, d(\mathfrak{a}).$$

Достаточно рассмотреть случай, когда $\mathfrak{a}$ есть точка $\mathfrak{p}$ поля R. Пусть $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все точки поля S, лежащие над $\mathfrak{p}$; тогда $\mathrm{Con}_{R/S}\mathfrak{p} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_h^{e_h}$, где e_i — индекс разветвления $\mathfrak{P}_i$ относительно R. Пусть Σ есть поле вычетов

точки $\mathfrak{p}$, а Σ_i — поле вычетов точки $\mathfrak{P}_i$; тогда $d(\mathrm{Con}_{R/S}\mathfrak{p}) = \sum_{i=1}^{h} e_i [\Sigma_i : L]$. Далее,

$$[\Sigma_i : L] = \frac{[\Sigma_i : K]}{[L : K]} = \frac{[\Sigma_i : \Sigma][\Sigma : K]}{[L : K]}.$$

Число $[\Sigma : K]$ равно $d(\mathfrak{p})$, а $[\Sigma_i : \Sigma]$ равно относительной степени f_i точки $\mathfrak{P}_i$ по отношению к R. Для завершения доказательства леммы 1 остается только заметить, что $\sum_{i=1}^{h} e_i f_i = [S : R]$ (теорема 1 § 1).

Предполагая, что S имеет конечную степень над R, перенесем на дивизоры понятие нормы элемента из S относительно R. Пусть y — произвольный элемент из S, отличный от 0. Пустя $\mathfrak{p}$ — точка поля R, а $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — точки поля S, лежащие над $\mathfrak{p}$. Тогда $\mathrm{N}_{S/R} y = \prod_{i=1}^{h} \mathrm{N}^{\mathfrak{P}_i} y$ (следствие 1 к теореме 6 § 5). С другой стороны, мы имеем $\nu_{\mathfrak{p}}(\mathrm{N}^{\mathfrak{P}_i} y) = f_i \nu_{\mathfrak{P}_i}(y)$ (следствие 2 к теореме 5 § 5); следовательно, $\nu_{\mathfrak{p}}(\mathrm{N}_{S/R} y) = \sum_{i=1}^{h} f_i \nu_{\mathfrak{P}_i}(y)$. Возьмем теперь произвольный дивизор $\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{A(\mathfrak{P})}$ поля S. Для каждой точки $\mathfrak{p}$ поля R положим $a(\mathfrak{p}) = \sum_{i=1}^{h} f_i A(\mathfrak{P}_i)$, где $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$, а f_i — степень точки $\mathfrak{P}_i$ относительно R. Очевидно, что имеется только конечное число точек $\mathfrak{p}$, для которых $a(\mathfrak{p}) \neq 0$, поэтому символ $\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ является дивизором поля R. Этот дивизор будем называть *нормой* дивизора $\mathfrak{A}$ (относительно поля R) и обозначать через $\mathrm{N}_{S/R}\mathfrak{A}$. Легко видеть, что для дивизоров $\mathfrak{A}$ и $\mathfrak{B}$ из S имеем

$$\mathrm{N}_{S/R}\mathfrak{A}\mathfrak{B} = (\mathrm{N}_{S/R}\mathfrak{A})(\mathrm{N}_{S/R}\mathfrak{B}),$$

а если y есть элемент поля S, отличный от 0, то

$$\mathrm{N}_{S/R}(\mathfrak{d}_S(y)) = \mathfrak{d}_R(\mathrm{N}_{S/R} y).$$

Норма и конорма связаны между собой формулой

$$\mathrm{N}_{S/R}(\mathrm{Con}_{R/S}\mathfrak{a}) = \mathfrak{a}^{[R:S]},$$

в которой под $\mathfrak{a}$ понимается дивизор поля R. Для доказательства этой формулы достаточно, очевидно, рассмотреть лишь случай, когда $\mathfrak{a}$ есть точка $\mathfrak{p}$ поля R. Пусть $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$; обозначим через e_i и f_i соответственно индекс разветвления и относительную степень точки $\mathfrak{P}_i$ относительно R. Тогда

$$\mathrm{N}_{S/R}(\mathrm{Con}_{R/S}\mathfrak{p}) = \mathrm{N}_{S/R}\prod_{i=1}^{h}\mathfrak{P}_i^{e_i} = \prod_{i=1}^{h}\mathfrak{p}^{e_i f_i} = \mathfrak{p}^{\sum_{i=1}^{h} e_i f_i},$$

и наша формула следует теперь из теоремы 1 § 1.

Лемма 2. *Пусть S имеет конечную степень над R и пусть K и L — поля констант полей R и S соответственно. Тогда для любого дивизора $\mathfrak{A}$ поля S имеем* $d(\mathrm{N}_{S/R}\mathfrak{A}) = [L:K]\,d(\mathfrak{A})$.

Достаточно эту формулу доказать для случая, когда $\mathfrak{A}$ есть точка $\mathfrak{P}$. Пусть $\mathfrak{p}$ — точка поля R, лежащая под $\mathfrak{P}$, и пусть $\Sigma(\mathfrak{P})$ и $\Sigma(\mathfrak{p})$ — поля вычетов точек $\mathfrak{P}$ и $\mathfrak{p}$ соответственно. Если f есть относительная степень $\mathfrak{P}$ по отношению к R, то

$$d(\mathrm{N}_{S/R}\mathfrak{P}) = d(\mathfrak{p}^f) = f\,[\Sigma(\mathfrak{p}):K] = [\Sigma(\mathfrak{P}):\Sigma(\mathfrak{p})]\,[\Sigma(\mathfrak{p}):K] = \\ = [\Sigma(\mathfrak{P}):K] = [\Sigma(\mathfrak{P}):L]\,[L:K] = [L:K]\,d(\mathfrak{P}),$$

и лемма 2 доказана.

Предположим теперь, что поле S алгебраично над R. Каждому распределению в поле R мы сопоставим сейчас некоторое распределение в поле S так, что главному распределению, связанному с элементом $x \in R$, будет соответствовать главное распределение в поле S, связанное с тем же элементом x.

Пусть $\mathfrak{P}$ — точка поля S. Так как S алгебраично над R, то $\mathfrak{P}$ лежит над некоторой точкой $\mathfrak{p}$ поля R. Как обычно, мы можем считать, что $\mathfrak{P}$-адическое пополнение $\overline{S}$ поля S содержит в качестве подполя $\mathfrak{p}$-адическое пополнение $\overline{R}$ поля R. Пусть $\mathfrak{x}$ есть распределение в поле R; если мы каждой точке $\mathfrak{P}$ поля S поставим в соответствие элемент $\mathfrak{x}(\mathfrak{p}) \in \overline{R} \subset \overline{S}$, то получим распределение поля S. Действительно, так как над каждой точкой поля R лежит только конечное число точек поля S, то, очевидно, существует лишь

конечное число точек $\mathfrak{P}$ из S, для которых $\nu_{\mathfrak{P}}(\mathfrak{x}(\mathfrak{p}))<0$. Так определенное распределение поля S называется *коследом распределения* $\mathfrak{x}$ *из поля* R *в* S и обозначается через $\mathrm{Cosp}_{R/S}\mathfrak{x}$. Если $\mathfrak{x}$ и $\mathfrak{x}'$ — распределения в R, а λ и λ' — константы поля R (а значит, и поля S), то

$$\mathrm{Cosp}_{R/S}(\lambda\mathfrak{x}+\lambda'\mathfrak{x}')=\lambda\,\mathrm{Cosp}_{R/S}\mathfrak{x}+\lambda'\,\mathrm{Cosp}_{R/S}\mathfrak{x}'.$$

Если $x\in R$, то элементу x соответствуют главное распределение в поле R и главное распределение в поле S. До сих пор элемент поля и главное распределение, соответствующее этому элементу, мы обозначали одинаковым образом; однако теперь, когда мы рассматриваем одновременно два поля, это соглашение может вызвать недоразумения. Поэтому главное распределение поля R, соответствующее элементу $x\in R$, мы будем обозначать через x_R; если же $y\in S$, то главное распределение поля S, соответствующее элементу y, будет обозначаться через y_S. Приняв эти обозначения, мы, очевидно, будем иметь

$$\mathrm{Cosp}_{R/S}x_R=x_S.$$

Предположим теперь, что S имеет конечную степень над R. В этом случае мы перенесем на распределения понятие следа элемента из S относительно R. Пусть y — элемент из S, $\mathfrak{p}$ — точка поля R и $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$. Тогда, как нам известно, $\mathrm{Sp}_{S/R}y=\sum_{i=1}^{h}\mathrm{Sp}^{\mathfrak{P}_i}y$ (следствие 1 к теореме 6 § 5). Пусть теперь $\mathfrak{y}$ — произвольное распределение поля S; для каждой точки $\mathfrak{p}$ поля R положим $\mathfrak{x}(\mathfrak{p})=\sum_{i=1}^{h}\mathrm{Sp}^{\mathfrak{P}_i}\mathfrak{y}(\mathfrak{P}_i)$. Утверждаем, что отображение $\mathfrak{p}\to\mathfrak{x}(\mathfrak{p})$ есть распределение поля R. Действительно, в поле S существует только конечное число точек, для которых $\nu_{\mathfrak{P}}(\mathfrak{y}(\mathfrak{P}))<0$, поэтому, если $\mathfrak{p}$ есть любая точка поля R, не лежащая под такими точками, то $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p}))\geqslant 0$ (следствие 1 к теореме 5 § 5). Так определенное распределение $\mathfrak{x}$ называется *следом распределения* $\mathfrak{y}$ *относительно* R и обозначается через $\mathrm{Sp}_{S/R}\mathfrak{y}$. Если $\mathfrak{y}$ и $\mathfrak{y}'$ —

распределения поля S, а λ и λ' — константы поля R, то, очевидно, имеем

$$\mathrm{Sp}_{S/R}(\lambda\mathfrak{y}+\lambda'\mathfrak{y}')=\lambda\,\mathrm{Sp}_{S/R}\mathfrak{y}+\lambda'\,\mathrm{Sp}_{S/R}\mathfrak{y}'.$$

Далее, если $y\in S$, то

$$\mathrm{Sp}_{S/R}y_S=(\mathrm{Sp}_{S/R}y)_R.$$

Замечание. Пусть распределение $\mathfrak{y}$ поля S таково, что $\mathfrak{y}(\mathfrak{P})\in S$ для всех точек $\mathfrak{P}$ поля S. Тогда может все-таки оказаться, что элемент $(\mathrm{Sp}_{S/R}\mathfrak{y})(\mathfrak{p})$ не принадлежит полю R. Это показывает нам, что определение следа не может быть дано в терминах нашего старого определения распределений; введенное в § 4 гл. III обобщение является здесь необходимым.

Если поле S несепарабельно над R, то $\mathrm{Sp}_{S/R}\mathfrak{y}=0$ для каждого распределения $\mathfrak{y}$ поля S. Пусть $\mathfrak{P}$ — точка поля S, $\mathfrak{p}$ — точка поля R, лежащая под $\mathfrak{P}$, $\bar{R}$ — $\mathfrak{p}$-адическое пополнение поля R и $\bar{S}$ — $\mathfrak{P}$-адическое пополнение поля S. Для доказательства нашего утверждения достаточно показать, что поле $\bar{S}$ несепарабельно над $\bar{R}$. Обозначим через R' подполе сепарабельных над R элементов поля S. Пусть $\mathfrak{p}'$ — точка поля R', лежащая под $\mathfrak{P}$, и пусть $\bar{R}'$ — $\mathfrak{p}'$-адическое пополнение поля R'. Если p — характеристика поля S, то при некотором показателе m будем иметь $y^{p^m}\in R'$ для любого $y\in S$. Очевидно, что условия $\nu_{\mathfrak{P}}(y)>0$ и $\nu_{\mathfrak{p}'}(y^{p^m})>0$ эквивалентны друг другу; следовательно, $\mathfrak{P}$ есть единственная точка поля S, лежащая над $\mathfrak{p}'$. Таким образом, $[\bar{S}:\bar{R}']=[S:R']>1$ (теорема 4 § 5). Но $\bar{S}=\bar{R}'\langle S\rangle$ (следствие 3 к теореме 5 § 5), поэтому $\bar{S}$ — чисто несепарабельно над $\bar{R}'$, и наше утверждение доказано.

Пусть $\mathfrak{x}$ — распределение поля R, а z — элемент поля S. Докажем следующую формулу:

$$\mathrm{Sp}_{S/R}(z\,\mathrm{Cosp}_{R/S}\mathfrak{x})=(\mathrm{Sp}_{S/R}z)\,\mathfrak{x}. \tag{1}$$

Обозначим через $\mathfrak{p}$ точку поля R и через $\mathfrak{P}_1,\ldots,\mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$. Тогда

$$\left(\mathrm{Sp}_{S/R}(z\,\mathrm{Cosp}_{R/S}\mathfrak{x})\right)(\mathfrak{p})=\sum_{i=1}^{h}\mathrm{Sp}^{\mathfrak{P}_i}(z\,\mathrm{Cosp}_{R/S}\mathfrak{x})(\mathfrak{P}_i).$$

Так как $(\mathrm{Cosp}_{R/S}\mathfrak{x})(\mathfrak{P}_i) = \mathfrak{x}(\mathfrak{p})$ принадлежит $\mathfrak{p}$-адическому пополнению поля R, то это равно

$$\left(\sum_{i=1}^{h} \mathrm{Sp}^{\mathfrak{P}_i} z\right)\mathfrak{x}(\mathfrak{p}) = (\mathrm{Sp}_{S/R} z)\,\mathfrak{x}(\mathfrak{p}),$$

что и доказывает нашу формулу.

Лемма 3. *Пусть R, S и T — поля алгебраических функций от одной переменной, причем R является подполем поля S, а S — подполем поля T. Для любого дивизора $\mathfrak{a}$ поля R имеем $\mathrm{Con}_{R/T}\mathfrak{a} = \mathrm{Con}_{S/T}(\mathrm{Con}_{R/S}\mathfrak{a})$. Если поле T алгебраично над R, то для любого распределения $\mathfrak{x}$ поля R имеем $\mathrm{Cosp}_{R/T}\mathfrak{x} = \mathrm{Cosp}_{S/T}(\mathrm{Cosp}_{R/S}\mathfrak{x})$. Если поле T имеет конечную степень над R, то $\mathrm{N}_{T/R}\mathfrak{A} = \mathrm{N}_{S/R}(\mathrm{N}_{T/S}\mathfrak{A})$ для любого дивизора $\mathfrak{A}$ поля T и $\mathrm{Sp}_{T/R}\mathfrak{y} = \mathrm{Sp}_{S/R}(\mathrm{Sp}_{T/S}\mathfrak{y})$ для любого распределения $\mathfrak{y}$ поля T.*

1. Первую формулу достаточно доказать для случая, когда $\mathfrak{a}$ есть точка $\mathfrak{p}_0$. В этом случае в дивизоры $\mathrm{Con}_{R/T}\mathfrak{a}$ и $\mathrm{Con}_{S/T}(\mathrm{Con}_{R/S}\mathfrak{a})$ входят только те точки поля T, которые лежат над $\mathfrak{p}_0$. Пусть $\mathfrak{P}$ — одна из этих точек; тогда в силу леммы 4 § 1 точка $\mathfrak{P}$ входит в оба наши дивизора с одинаковым показателем.

2. Формула $\mathrm{Cosp}_{R/T}\mathfrak{x} = \mathrm{Cosp}_{S/T}(\mathrm{Cosp}_{R/S}\mathfrak{x})$ (если T алгебраично над R) очевидна.

3. Предположим теперь, что T имеет конечную степень над R. Формулу $\mathrm{N}_{T/R}\mathfrak{A} = \mathrm{N}_{S/R}(\mathrm{N}_{T/S}\mathfrak{A})$ достаточно доказать для случая, когда $\mathfrak{A}$ есть точка поля T. В этом случае формула вытекает непосредственно из последнего утверждения леммы 4 § 1.

4. Докажем теперь формулу $\mathrm{Sp}_{T/R}\mathfrak{y} = \mathrm{Sp}_{S/R}(\mathrm{Sp}_{T/S}\mathfrak{y})$. Пусть $\mathfrak{p}_0$ — произвольная точка поля R. Тогда $(\mathrm{Sp}_{T/R}\mathfrak{y})(\mathfrak{p}_0) = \sum_{i=1}^{h} \mathrm{Sp}^{\mathfrak{P}_i}_{T/R}\mathfrak{y}(\mathfrak{P}_i)$, где $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля T, лежащие над $\mathfrak{p}_0$, а $\mathrm{Sp}^{\mathfrak{P}_i}_{T/R}$ обозначает след из $\mathfrak{P}_i$-адического пополнения поля T в $\mathfrak{p}_0$-адическое пополнение поля R. Если $\mathfrak{p}_i$ есть точка поля S, лежащая под $\mathfrak{P}_i$, то $\mathrm{Sp}^{\mathfrak{P}_i}_{T/R}\mathfrak{y}(\mathfrak{P}_i) = \mathrm{Sp}^{\mathfrak{p}_i}_{S/R}(\mathrm{Sp}^{\mathfrak{P}_i}_{T/S}\mathfrak{y}(\mathfrak{P}_i))$, где через $Sp^{\mathfrak{p}_i}_{S/R}$ обозначен след из

$\mathfrak{p}_i$-адического пополнения поля S в $\mathfrak{p}_0$-адическое пополнение поля R, а через $\mathrm{Sp}_{T/S}^{\mathfrak{P}_i}$ — след из $\mathfrak{P}_i$-адического пополнения поля T в $\mathfrak{p}_i$-адическое пополнение поля S. Пусть $\mathfrak{p}$ — одна из точек поля S, лежащих над $\mathfrak{p}_0$. Обозначим через $U_{\mathfrak{p}}$ сумму выражений $\mathrm{Sp}_{T/S}^{\mathfrak{P}_i}\mathfrak{y}(\mathfrak{P}_i)$, соответствующих тем индексам i, для которых $\mathfrak{p}_i = \mathfrak{p}$. Тогда $U_{\mathfrak{p}} = (\mathrm{Sp}_{T/S}\mathfrak{y})(\mathfrak{p})$, а $(\mathrm{Sp}_{T/R}\mathfrak{y})(\mathfrak{p}_0)$ равно сумме выражений $\mathrm{Sp}_{S/R}^{\mathfrak{p}}U_{\mathfrak{p}}$, соответствующих всем различным точкам $\mathfrak{p}$ поля S, лежащим над $\mathfrak{p}_0$ ($\mathrm{Sp}_{S/R}^{\mathfrak{p}}$ обозначает след из $\mathfrak{p}$-адического пополнения поля S в $\mathfrak{p}_0$-адическое пополнение поля R). Таким образом, наша формула доказана.

§ 8. Дифферента

В этом параграфе мы будем предполагать, что R и S — поля алгебраических функций от одной переменной, причем S является сепарабельным расширением поля R конечной степени. Пусть $\mathfrak{P}$ — произвольная точка поля S, а $\mathfrak{p}$ — точка поля R, лежащая под $\mathfrak{P}$. Из следствия 3 к теореме 5 § 5 вытекает, что $\mathfrak{P}$-адическое пополнение $\bar{S}$ поля S сепарабельно над $\mathfrak{p}$-адическим пополнением $\bar{R}$ поля R. Если $y \in \bar{S}$, то, как нам известно, из условия $\nu_{\mathfrak{P}}(y) \geqslant 0$ следует, что $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}}y) \geqslant 0$ (следствие 1 к теореме 5 § 5). Обратное, вообще говоря, неверно: в поле $\bar{S}$ можно найти такой элемент y, что $\nu_{\mathfrak{P}}(y) < 0$, но $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}}y) \geqslant 0$. Однако неравенство $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}}y) \geqslant 0$ при всех $y \in \bar{S}$ не может иметь места. Действительно, так как $\bar{S}$ сепарабельно над $\bar{R}$, то в поле $\bar{S}$ существует такой элемент y_1, что $\mathrm{Sp}^{\mathfrak{P}}y_1 \neq 0$. Если x есть элемент поля $\bar{R}$, для которого $\nu_{\mathfrak{p}}(x) < -\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}}y_1)$, то $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}}xy_1) < 0$. Таким образом, существует наибольшее целое число $m = m(\mathfrak{P})$, для которого $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}}y) \geqslant 0$ для всех элементов $y \in S$, удовлетворяющих условию $\nu_{\mathfrak{P}}(y) \geqslant -m(\mathfrak{P})$. Очевидно, что $m(\mathfrak{P}) \geqslant 0$. Число $m(\mathfrak{P})$ называется *$\mathfrak{P}$-показателем дифференты* поля S относительно R.

Теорема 7. *Пусть R и S — поля алгебраических функций от одной переменной, причем S является сепарабельным расширением поля R конечной степени. Если $\mathfrak{P}$ — точка поля S, то $\mathfrak{P}$-показатель дифференты $m(\mathfrak{P})$ поля S относительно R не меньше $e-1$, где e — индекс*

разветвления точки $\mathfrak{P}$ относительно R. Равенство $m(\mathfrak{P}) = e - 1$ имеет место тогда и только тогда, если, во-первых, поле вычетов точки $\mathfrak{P}$ сепарабельно над полем вычетов точки $\mathfrak{p}$ поля R, лежащей под $\mathfrak{P}$, и, во-вторых, число e не делится на характеристику поля R.

Пусть $\Sigma(\mathfrak{P})$ и $\Sigma(\mathfrak{p})$ — поля вычетов точек $\mathfrak{P}$ и $\mathfrak{p}$ соответственно. Если z есть целый элемент из $\mathfrak{P}$-адического пополнения $\bar{S}$ поля S, то через z^* мы будем обозначать его класс вычетов по модулю $\mathfrak{P}$. Докажем следующую формулу:

$$(\mathrm{Sp}^{\mathfrak{P}} z)^* = e\, \mathrm{Sp}_{\Sigma(\mathfrak{P})/\Sigma(\mathfrak{p})} z^*. \tag{1}$$

Пусть u — униформизирующая переменная в точке $\mathfrak{P}$ поля S и пусть $\theta_1, \ldots, \theta_f$ — элементы кольца точки $\mathfrak{P}$, классы вычетов которых $\theta_1^*, \ldots, \theta_f^*$ образуют базис поля $\Sigma(\mathfrak{P})$ над $\Sigma(\mathfrak{p})$. Тогда, как нам известно, элементы $u^i\theta_j$ $(0 \leqslant i \leqslant e-1,$ $1 \leqslant j \leqslant f)$ образуют базис поля $\bar{S}$ относительно $\mathfrak{p}$-адического пополнения $\bar{R}$ поля R, при этом, если мы положим

$$zu^i\theta_j = \sum_{k=0}^{e-1} \sum_{l=1}^{f} a_{ijkl} u^k \theta_l, \quad a_{ijkl} \in \bar{R}, \tag{2}$$

то элементы a_{ijkl} будут целыми в $\bar{R}$ (теорема 5 § 5). Имеем $\mathrm{Sp}^{\mathfrak{P}} z = \sum_{i=0}^{e-1} \sum_{j=1}^{f} a_{ijij}$. Если мы в равенстве (2) положим $i = 0$, а затем умножим на u^i, то получим

$$zu^i\theta_j = \sum_{k=0}^{e-1} \sum_{l=1}^{f} a_{0jkl} u^{k+i} \theta_l. \tag{3}$$

Пусть t — униформизирующая переменная в точке $\mathfrak{p}$ поля R; тогда $\nu_{\mathfrak{P}}(t) = e$. Если $k + i \geqslant e$, то $u^{k+i}\theta_l = tv_{ikl}$, где v_{ikl} — целый элемент из $\bar{S}$. Каждый элемент v_{ikl} мы можем представить в виде линейной комбинации произведений $u^{k'}\theta_{l'}$ $(0 \leqslant k' \leqslant e-1,\ 1 \leqslant l' \leqslant f)$ с целыми коэффициентами из $\bar{R}$. Подставив эти выражения в (3), мы должны получить равенства (2) (после приведения подобных членов). Отсюда легко следует, что $\nu_{\mathfrak{p}}(a_{ijkl}) > 0$ при $k < i$ и $\nu_{\mathfrak{p}}(a_{ijkl} - a_{0j,\, k-i,\, l}) > 0$ при $i \leqslant k \leqslant e-1$. Таким образом, $a_{ijij}^* = b_j^*$ не зависит от i, а значит, $(\mathrm{Sp}_{\mathfrak{P}} z)^* = e \sum_{j=1}^{f} b_j^*$. С другой стороны, из равенств (2)

при $i=0$ получаем $z^*\theta_j^* = \sum_{l=1}^{f} \overset{*}{a}_{0j0l}\theta_l^*$; но $b_j^* = \overset{*}{a}_{0j0j}$, поэтому $\mathrm{Sp}_{\Sigma(\mathfrak{P})/\Sigma(\mathfrak{p})} z^* = \sum_{j=1}^{f} b_j^*$, и формула (1) доказана.

Пусть теперь y есть элемент поля $\bar{S}$ такой, что $\nu_{\mathfrak{P}}(y) \geqslant -(e-1)$. Так как $\nu_{\mathfrak{P}}(t) = e$, то $\nu_{\mathfrak{P}}(ty) > 0$, откуда, в силу формулы (1), $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}} ty) = 1 + \nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}} y) \geqslant 1$ и $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}} y) \geqslant 0$. Таким образом, $m(\mathfrak{P}) \geqslant e-1$. Далее, из формулы (1) следует, что если хоть одно из условий, указанных в теореме 7, не выполнено, то $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}} z) > 0$ для всех целых элементов z из $\bar{S}$ (если поле $\Sigma(\mathfrak{P})$ несепарабельно над $\Sigma(\mathfrak{p})$, то, как известно, след любого элемента из $\Sigma(\mathfrak{P})$ относительно $\Sigma(\mathfrak{p})$ равен 0). Пусть y есть элемент поля $\bar{S}$ такой, что $\nu_{\mathfrak{P}}(y) \geqslant -e$; тогда аналогично вышеизложенному докажем, что $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}} y) \geqslant 0$, т. е. что $m(\mathfrak{P}) \geqslant e$. Пусть теперь оба условия теоремы 7 выполняются. Тогда в поле $\Sigma(\mathfrak{P})$ существует такой элемент z^*, что $\mathrm{Sp}_{\Sigma(\mathfrak{P})/\Sigma(\mathfrak{p})} z^* \neq 0$. Если z есть целый элемент поля $\bar{S}$, принадлежащий классу z^*, то $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}} z) = 0$, откуда $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}} t^{-1} z) = -1$. Следовательно, в этом случае имеем $m(\mathfrak{P}) < e$, т. е. $m(\mathfrak{P}) = e-1$.

Установим теперь связь между $\mathfrak{P}$-показателем дифференты и дискриминантом базиса. Пусть U — поле, а V — сепарабельное расширение поля U конечной степени. Если $\{v_1, \ldots, v_n\}$ есть произвольный базис поля V относительно U, то определитель матрицы $(\mathrm{Sp}_{V/U} v_i v_j)_{1 \leqslant i, j \leqslant n}$ называется *дискриминантом* базиса $\{v_1, \ldots, v_n\}$; мы будем его обозначать через $D(v_1, \ldots, v_n)$. Утверждаем, что $D(v_1, \ldots, v_n) \neq 0$. Действительно, матрица $(\mathrm{Sp}_{V/U}\, v_i v_j)$ является матрицей билинейной функции B, определенной равенством $B(v, v') = \mathrm{Sp}_{V/U}\, vv'$, в базисе $\{v_1, \ldots, v_n\}$. Так как поле V сепарабельно над U, то существует такой элемент $v_0 \in V$, что $\mathrm{Sp}_{V/U} v_0 \neq 0$; если $v \in V$, $v \neq 0$, то $\mathrm{Sp}_{V/U} v(v^{-1}v_0) \neq 0$, откуда следует, что билинейная функция B невырождена.

Лемма 1. *Пусть сохраняются обозначения теоремы 7 и пусть $\bar{S}$ есть $\mathfrak{P}$-адическое пополнение поля S, а $\bar{R}$ — $\mathfrak{p}$-адическое пополнение поля R. Пусть, далее, $\{y_1, \ldots, y_n\}$ есть базис поля $\bar{S}$ относительно $\bar{R}$, состоящий*

из целых элементов поля $\bar{S}$. Тогда $\nu_{\mathfrak{P}}(D(y_1, \ldots, y_n)) \geqslant fm(\mathfrak{P})$, где f — относительная степень точки $\mathfrak{P}$ по отношению к R. Для того чтобы имело место равенство $\nu_{\mathfrak{P}}(D(y_1, \ldots, y_n)) = fm(\mathfrak{P})$, необходимо и достаточно, чтобы наш базис был целым базисом (т. е. чтобы каждый целый элемент из $\bar{S}$ можно было представить в виде линейной комбинации элементов $y_1, \ldots, y_n$ с целыми коэффициентами из поля $\bar{R}$).

Как нам известно, в поле $\bar{S}$ существует целый базис $\{z_1, \ldots, z_n\}$ относительно $\bar{R}$. Имеем

$$z_i = \sum_{j=1}^{n} b_{ij} y_j \quad \text{и} \quad y_i = \sum_{j=1}^{n} c_{ij} z_j,$$

где коэффициенты b_{ij} и c_{ij} принадлежат полю $\bar{R}$, причем c_{ij} — целые. Матрицы (b_{ij}) и (c_{ij}) являются взаимно обратными матрицами. Легко видеть, что $D(y_1, \ldots, y_n) = \gamma^2 D(z_1, \ldots, z_n)$, где $\gamma = \det(c_{ij})$. Так как элементы c_{ij} целые, то $\nu_{\mathfrak{P}}(\gamma) \geqslant 0$, откуда $\nu_{\mathfrak{P}}(D(y_1, \ldots, y_n)) \geqslant \nu_{\mathfrak{P}}(D(z_1, \ldots, z_n))$. Если $\nu_{\mathfrak{P}}(\gamma) = 0$, то γ^{-1} есть целый элемент, а тогда, как легко видеть, элементы b_{ij} также целые (как элементы обратной матрицы для матрицы (c_{ij})). В этом случае каждый целый элемент из $\bar{S}$ (который является линейной комбинацией элементов $z_1, \ldots, z_n$ с целыми коэффициентами из $\bar{R}$) можно представить также в виде линейной комбинации элементов $y_1, \ldots, y_n$ с целыми коэффициентами. Это означает, что $\{y_1, \ldots, y_n\}$ есть также целый базис. Обратно, если базис $\{y_1, \ldots, y_n\}$ — целый, то коэффициенты b_{ij} являются целыми элементами, а тогда элемент γ^{-1}, равный $\det(b_{ij})$, также целый, откуда $\nu_{\mathfrak{P}}(\gamma) = 0$. Таким образом, базис $\{y_1, \ldots, y_n\}$ является целым тогда и только тогда, если $\nu_{\mathfrak{P}}(D(y_1, \ldots, y_n)) = \nu_{\mathfrak{P}}(D(z_1, \ldots, z_n))$. Займемся теперь вычислением числа $\nu_{\mathfrak{P}}(D(z_1, \ldots, z_n))$. Пусть $\mathfrak{A}$ есть множество тех $\zeta \in \bar{S}$, для которых $\mathrm{Sp}^{\mathfrak{P}} \zeta y$ является целым элементом при любом целом y. Если u есть униформизирующая переменная в точке $\mathfrak{P}$ поля S, то, очевидно, $\mathfrak{A} = u^{-m(\mathfrak{P})}\mathfrak{O}$, где $\mathfrak{O}$ — кольцо целых элементов поля $\bar{S}$. Опишем множество $\mathfrak{A}$ другим способом. Так как $D(z_1, \ldots, z_n) \neq 0$, то в поле $\bar{S}$ можно найти такие элементы $z'_1, \ldots, z'_n$, что

$\mathrm{Sp}^{\mathfrak{P}} z_i z'_i = 1$ и $\mathrm{Sp}^{\mathfrak{P}} z_i z'_j = 0$ при $i \neq j$. Если элементы $x'_1, \ldots, x'_n$ принадлежат $\bar{R}$, то $\mathrm{Sp}^{\mathfrak{P}}\left(\sum_{i=1}^{n} x'_i z'_i\right) z_j = x'_j$, откуда $\mathrm{Sp}^{\mathfrak{P}}\left(\sum_{i=1}^{n} x'_i z'_i\right) z = \sum_{j=1}^{n} x_j x'_j$, где $z = \sum_{j=1}^{n} x_j z_j$, $x_j \in \bar{R}$. Отсюда следует, что элемент $\sum_{i=1}^{n} x'_i z'_i$ принадлежит $\mathfrak{A}$ тогда и только тогда, если элементы $x'_1, \ldots, x'_n$ целые. В частности, получаем, что $\{z'_1, \ldots, z'_n\}$ есть базис, а значит, $\{u^{m(\mathfrak{P})} z'_1, \ldots, u^{m(\mathfrak{P})} z'_n\}$ есть целый базис. Если мы запишем $u^{m(\mathfrak{P})} z'_i = \sum_{j=1}^{n} \alpha_{ij} z'_j$, где $\alpha_{ij} \in \bar{R}$, то будем иметь $\det(\alpha_{ij}) = N^{\mathfrak{P}} u^{m(\mathfrak{P})}$, откуда $\nu_{\mathfrak{p}}(\det(\alpha_{ij})) = fm(\mathfrak{P})$ (следствие 2 к теореме 5 § 5). С другой стороны, полагая $z_i = \sum_{j=1}^{n} \beta_{ij} u^{m(\mathfrak{P})} z'_j$, будем иметь $\nu_{\mathfrak{p}}(\det(\beta_{ij})) = 0$. Если (γ_{ij}) есть произведение матриц (β_{ij}) и (α_{ij}), то $z_i = \sum_{j=1}^{n} \gamma_{ij} z'_j$, откуда $\gamma_{ij} = \mathrm{Sp}^{\mathfrak{P}} z_i z_j$. Таким образом, $\nu_{\mathfrak{p}}(D(z_1, \ldots, z_n)) = \nu_{\mathfrak{p}}(\det(\beta_{ij})) + \nu_{\mathfrak{p}}(\det(\alpha_{ij})) = fm(\mathfrak{P})$, и лемма 1 доказана.

Лемма 2. *Пусть R и S — поля алгебраических функций от одной переменной, причем S является сепарабельным расширением поля R конечной степени. Пусть $\mathfrak{p}$ — точка поля R, а $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$. Через m_λ обозначим $\mathfrak{P}_\lambda$-показатель дифференты, а через f_λ — относительную степень точки $\mathfrak{P}_\lambda$ (относительно поля R). Пусть $\{y_1, \ldots, y_n\}$ — базис поля S над R, элементы которого являются целыми относительно кольца точки $\mathfrak{p}$. Тогда $\nu_{\mathfrak{p}}(D(y_1, \ldots, y_n)) \geqslant \sum_{\lambda=1}^{h} m_\lambda f_\lambda$, при этом знак равенства имеет место тогда и только тогда, если базис $\{y_1, \ldots, y_n\}$ целый в точке $\mathfrak{p}$.*

Пусть $\bar{R}$ — $\mathfrak{p}$-адическое пополнение поля R. Рассмотрим алгебру $S_{\bar{R}}$, полученную из S расширением основного поля R до поля $\bar{R}$. Используя изоморфизм, построенный в дока-

зательстве теоремы 4 § 5, мы можем алгебру $S_{\overline{R}}$ отождествить с произведением $\prod_{\lambda=1}^{h} \overline{S}_\lambda$, где $\overline{S}_\lambda$ есть $\mathfrak{P}_\lambda$-адическое пополнение поля S $(1 \leqslant \lambda \leqslant h)$. Для каждого λ найдем целый базис $\{z'_{1\lambda}, \ldots, z'_{n_\lambda \lambda}\}$ поля $\overline{S}_\lambda$ относительно $\overline{R}$. Обозначим через $z_{i\lambda}$ тот элемент алгебры $S_{\overline{R}}$, у которого λ-координата равна $z'_{i\lambda}$, а все остальные координаты равны 0. Тогда элементы $z_{i\lambda}$ $(1 \leqslant i \leqslant n_\lambda,\ 1 \leqslant \lambda \leqslant h)$ образуют базис алгебры $S_{\overline{R}}$, при этом целые элементы из $S_{\overline{R}}$ представляются в виде линейных комбинаций элементов $z_{i\lambda}$ с целыми коэффициентами из $\overline{R}$. Пусть $\zeta_1, \ldots, \zeta_n$ — элементы $z_{i\lambda}$, выписанные в некотором порядке, и пусть $\{z_1, \ldots, z_n\}$ — произвольный целый в точке $\mathfrak{p}$ базис S относительно R. Так же как в доказательстве леммы 1, легко показать, что если $z_i = \sum_{j=1}^{n} \alpha_{ij}\zeta_j$, то $\nu_{\mathfrak{p}}(\det(\alpha_{ij})) = 0$ (см. замечание в конце доказательства теоремы 4 § 5). Если теперь $u \in S$, то $\mathrm{Sp}_{S/R} u = \sum_{\lambda=1}^{h} \mathrm{Sp}^{\mathfrak{P}_\lambda} u$ (следствие 1 к теореме 6 § 5). Естественно поэтому для каждого $u = (u_1, \ldots, u_h) \in S_{\overline{R}}$ $(u_\lambda \in \overline{S}_\lambda,$ $1 \leqslant \lambda \leqslant h)$ положить $\mathrm{Sp}_{S_{\overline{R}}/\overline{R}} u = \sum_{\lambda=1}^{h} \mathrm{Sp}^{\mathfrak{P}_\lambda} u_\lambda$. Тогда

$$D(z_1, \ldots, z_n) = (\det(\alpha_{ij}))^2 \left(\det\left(\mathrm{Sp}_{S_{\overline{R}}/\overline{R}} \zeta_i\zeta_j\right)\right).$$

Далее, $z_{i\lambda}z_{i'\lambda'} = 0$ при $\lambda \neq \lambda'$, а элемент $z_{i\lambda}z_{i'\lambda}$ из $\prod_{\lambda=1}^{h} \overline{S}_\lambda$ имеет λ-координату, равную $z'_{i\lambda}z'_{i'\lambda}$, в то время как все другие его координаты равны 0. Следовательно, получаем

$$\det\left(\mathrm{Sp}_{S_{\overline{R}}/\overline{R}} \zeta_i\zeta_j\right) = \prod_{\lambda=1}^{h} D(z'_{1\lambda}, \ldots, z'_{n_\lambda \lambda}),$$

откуда, в силу леммы 1, следует, что $\nu_{\mathfrak{p}}(D(z_1, \ldots, z_n)) = \sum_{\lambda=1}^{h} f_\lambda m_\lambda$. Запишем теперь $y_i = \sum_{j=1}^{n} b_{ij}z_j$, $b_{ij} \in R$; так как

элементы b_{ij} принадлежат кольцу точки $\mathfrak{p}$, то

$$\nu_{\mathfrak{p}}(D(y_1, \ldots, y_n)) \geqslant \nu_{\mathfrak{p}}(D(z_1, \ldots, z_n)).$$

Кроме того, так же как в доказательстве леммы 1, получаем, что базис $\{y_1, \ldots, y_n\}$ является целым в точке $\mathfrak{p}$ тогда и только тогда, если $\nu_{\mathfrak{p}}(\det(b_{ij})) = 0$, т. е. если $\nu_{\mathfrak{p}}(D(y_1, \ldots, y_n)) = \nu_{\mathfrak{p}}(D(z_1, \ldots, z_n))$.

Лемма 3. *Пусть R и S — поля алгебраических функций от одной переменной, причем S является сепарабельным расширением поля R конечной степени. Тогда почти для всех точек $\mathfrak{P}$ поля S имеем: 1) точка $\mathfrak{P}$ неразветвлена относительно R и 2) поле вычетов точки $\mathfrak{P}$ сепарабельно над полем вычетов точки $\mathfrak{p}$ поля R, лежащей под $\mathfrak{P}$.*

Пусть $\{y_1, \ldots, y_n\}$ — произвольный базис поля S относительно R. Этот базис является целым почти во всех точках поля R (лемма 3 § 3). Так как $D(y_1, \ldots, y_n) \neq 0$, то $\nu_{\mathfrak{p}}(D(y_1, \ldots, y_n)) = 0$ почти для всех точек $\mathfrak{p}$ поля R. Если базис $\{y_1, \ldots, y_n\}$ в точке $\mathfrak{p}$ поля R является целым и если $\nu_{\mathfrak{p}}(D(y_1, \ldots, y_n)) = 0$, то, как это следует из леммы 2, $\mathfrak{P}$-показатель дифференты равен 0 для каждой точки $\mathfrak{P}$ поля S, лежащей над $\mathfrak{p}$. В силу теоремы 7 получаем, что каждая такая точка не разветвлена относительно R и что ее поле вычетов сепарабельно над полем вычетов точки $\mathfrak{p}$. Лемма 3 доказана.

Сохраняя условия леммы 3, для каждой точки $\mathfrak{P}$ поля S через $m(\mathfrak{P})$ обозначим $\mathfrak{P}$-показатель дифференты относительно R. Тогда $m(\mathfrak{P}) = 0$ почти для всех точек $\mathfrak{P}$ поля S, следовательно, символ $\prod_{\mathfrak{P}} \mathfrak{P}^{m(\mathfrak{P})}$ является дивизором поля S. Этот дивизор называется *дифферентой* поля S относительно R.

Лемма 4. *Пусть R и S — поля алгебраических функций от одной переменной, причем S является сепарабельным расширением поля R конечной степени. Пусть F — конечное множество точек поля R, а F^* — множество всех точек поля S, лежащих над точками из F. Пусть для каждой точки $\mathfrak{p} \in F$ задано некоторое целое число $a(\mathfrak{p})$. Обозначим через $e(\mathfrak{P})$ и $m(\mathfrak{P})$ соответственно индекс разветвления и $\mathfrak{P}$-показатель дифференты точки $\mathfrak{P}$ поля S относительно R. Тогда следующие два условия*

для элемента $y \in S$ *эквивалентны между собой*: 1) $\nu_{\mathfrak{P}}(y) \geqslant -m(\mathfrak{P}) + a(\mathfrak{p})e(\mathfrak{P})$ *для всех* $\mathfrak{P} \in F^*$, *где* $\mathfrak{p}$ — *точка поля* R, *лежащая под* $\mathfrak{P}$; 2) $\nu_{\mathfrak{p}}(\mathrm{Sp}_{S/R}\, yz) \geqslant a(\mathfrak{p})$ *для всех* $\mathfrak{p} \in F$ *и для всех элементов* $z \in S$, *удовлетворяющих условию* $\nu_{\mathfrak{P}}(z) \geqslant 0$ *при любой точке* $\mathfrak{P} \in F^*$.

Выберем в поле R элемент t, для которого $\nu_{\mathfrak{p}}(t) = -a(\mathfrak{p})$ при всех $\mathfrak{p} \in F$ (следствие к теореме 3 § 6 гл. I). Тогда $\nu_{\mathfrak{P}}(ty) = \nu_{\mathfrak{P}}(y) - a(\mathfrak{p})e(\mathfrak{P})$, где $\mathfrak{P} \in F^*$, а $\mathfrak{p}$ — точка поля R, лежащая под $\mathfrak{P}$. С другой стороны, $\mathrm{Sp}_{S/R}\, txy = t\,\mathrm{Sp}_{S/R}\, xy$, поэтому $\nu_{\mathfrak{p}}(\mathrm{Sp}_{S/R}\, tyz) = \nu_{\mathfrak{p}}(\mathrm{Sp}_{S/R}\, yz) - a(\mathfrak{p})$ для любой точки $\mathfrak{p} \in F$. Таким образом, лемму 4 достаточно доказать для случая, когда $a(\mathfrak{p}) = 0$. Будем считать, поэтому, что $a(\mathfrak{p}) = 0$.

Пусть выполнено условие 1). Обозначим через $\mathfrak{p}$ точку из F, а через $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$. Если $z \in S$, то $\mathrm{Sp}_{S/R}\, yz = \sum_{i=1}^{h} \mathrm{Sp}^{\mathfrak{P}_i} yz$ (следствие 1 к теореме 6 § 5). Если $\nu_{\mathfrak{P}}(z) \geqslant 0$ при всех $\mathfrak{P} \in F^*$, то $\nu_{\mathfrak{P}_i}(yz) \geqslant -m(\mathfrak{P}_i)$ $(1 \leqslant i \leqslant h)$, откуда $\nu_{\mathfrak{p}}(\mathrm{Sp}^{\mathfrak{P}_i} yz) \geqslant 0$ и $\nu_{\mathfrak{p}}(\mathrm{Sp}_{S/R}\, yz) \geqslant 0$.

Пусть теперь выполнено условие 2). Будем считать, что $y \neq 0$. Пусть $\mathfrak{P}_0$ — любая точка из F^* и пусть $\bar{z}$ — произвольный целый элемент из $\mathfrak{P}_0$-адического пополнения $\bar{S}$ поля S. В поле S найдем элемент z такой, что $\nu_{\mathfrak{P}}(z - \bar{z}) \geqslant \max\{0, -\nu_{\mathfrak{P}}(y)\}$ и $\nu_{\mathfrak{P}}(z) \geqslant \max\{0, -\nu_{\mathfrak{P}}(y)\}$ при всех $\mathfrak{P} \in F^*$, $\mathfrak{P} \neq \mathfrak{P}_0$ (теорема 3 § 6 гл. I). Очевидно, что z является целым элементом в каждой точке из F^*, а значит $\nu_{\mathfrak{p}}(\mathrm{Sp}_{S/R}\, yz) \geqslant 0$ при всех $\mathfrak{p} \in F$. Пусть $\mathfrak{p}_0$ — точка поля R, лежащая под $\mathfrak{P}_0$, и пусть $\mathfrak{P}_1 = \mathfrak{P}_0, \mathfrak{P}_2, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}_0$. Тогда $\mathrm{Sp}_{S/R}\, yz = \sum_{i=1}^{h} \mathrm{Sp}^{\mathfrak{P}_i} yz$. Если $i > 1$, то $\nu_{\mathfrak{P}_i}(yz) \geqslant 0$, а значит, $\nu_{\mathfrak{p}_0}(\mathrm{Sp}^{\mathfrak{P}_i} yz) \geqslant 0$; отсюда следует, что $\nu_{\mathfrak{p}_0}(\mathrm{Sp}^{\mathfrak{P}_0} yz) \geqslant 0$. Так как $\nu_{\mathfrak{P}_0}(yz - y\bar{z}) \geqslant 0$, то $\nu_{\mathfrak{p}_0}(\mathrm{Sp}^{\mathfrak{P}} y\bar{z}) \geqslant 0$. Каждый элемент $\bar{y}$ из $\bar{S}$, для которого $\nu_{\mathfrak{P}_0}(\bar{y}) \geqslant \nu_{\mathfrak{P}_0}(y)$, может быть представлен в виде $y\bar{z}$, где $\bar{z}$ — целый элемент из $\bar{S}$; следовательно, для каждого такого $\bar{y}$ имеем $\nu_{\mathfrak{p}_0}(\mathrm{Sp}^{\mathfrak{P}_0} \bar{y}) \geqslant 0$. Отсюда следует, что $\nu_{\mathfrak{P}_0}(y) \geqslant -m(\mathfrak{P}_0)$, и лемма 4 доказана.

Теорема 8. *Пусть R, S и T — поля алгебраических функций от одной переменной, причем поле T является сепарабельным расширением поля R конечной степени, а S — промежуточное поле между R и T. Обозначим через $\mathfrak{D}_{T/R}$, $\mathfrak{D}_{T/S}$ и $\mathfrak{D}_{S/R}$ — дифференты полей T относительно R, T относительно S и S относительно R соответственно. Тогда имеет место равенство $\mathfrak{D}_{T/R} = \mathfrak{D}_{T/S} \cdot \mathrm{Con}_{S/T}\, \mathfrak{D}_{S/R}$.*

Пусть $\mathfrak{p}$ — точка поля R, F — множество точек поля S, лежащих над $\mathfrak{p}$, и F^* — множество точек поля T, лежащих над $\mathfrak{p}$. Если $\mathfrak{Q} \in F^*$, то через $m(\mathfrak{Q})$, $\mu(\mathfrak{Q})$ и $e(\mathfrak{Q})$ мы обозначим соответственно $\mathfrak{Q}$-показатель дифференты относительно R, $\mathfrak{Q}$-показатель дифференты относительно S и индекс разветвления точки $\mathfrak{Q}$ относительно S. Если $\mathfrak{q} \in F$, то через $m(\mathfrak{q})$ мы обозначим $\mathfrak{q}$-показатель дифференты (поля S) относительно R. Мы должны доказать, что $m(\mathfrak{Q}) = \mu(\mathfrak{Q}) + e(\mathfrak{Q})\, m(\mathfrak{q})$, где $\mathfrak{q}$ — точка поля S, лежащая под $\mathfrak{Q}$. Обозначим через $m'(\mathfrak{Q})$ правую часть этой формулы. Пусть y есть такой элемент поля T, что $\nu_{\mathfrak{Q}}(y) = -m(\mathfrak{Q})$ для всех $\mathfrak{Q} \in F^*$ (см. следствие к теореме 3 § 6 гл. I). В силу леммы 4 $\nu_{\mathfrak{p}}(\mathrm{Sp}_{T/R}\, yz) \geqslant 0$ для всех $z \in T$, удовлетворяющих условию $\nu_{\mathfrak{Q}}(z) \geqslant 0$ при всех $\mathfrak{Q} \in F^*$. Пусть z_1 есть такой элемент поля S, что $\nu_{\mathfrak{q}}(z_1) \geqslant 0$ для всех $\mathfrak{q} \in F$. Так как $\mathrm{Sp}_{T/R}\, yz = \mathrm{Sp}_{S/R}(\mathrm{Sp}_{T/S}\, yz)$, то $\nu_{\mathfrak{p}}(\mathrm{Sp}_{S/R}\, z_1 \mathrm{Sp}_{T/S}\, yz) = \nu_{\mathfrak{p}}(\mathrm{Sp}_{T/R}\, yzz_1) \geqslant 0$, ибо $\nu_{\mathfrak{Q}}(zz_1) \geqslant 0$ для всех $\mathfrak{Q} \in F^*$. В силу леммы 4 получаем, прежде всего, что $\nu_{\mathfrak{q}}(\mathrm{Sp}_{T/S}\, yz) \geqslant -m(\mathfrak{q})$, и далее, что $\nu_{\mathfrak{Q}}(y) \geqslant -m'(\mathfrak{Q})$ для всех $\mathfrak{Q} \in F^*$. Следовательно, $m(\mathfrak{Q}) \leqslant m'(\mathfrak{Q})$. Пусть теперь y' есть элемент поля T такой, что $\nu_{\mathfrak{Q}}(y') = -m'(\mathfrak{Q})$ при всех $\mathfrak{Q} \in F^*$ (см. следствие к теореме 3 § 6 гл. I). Используя лемму 4, получаем, что $\nu_{\mathfrak{q}}(\mathrm{Sp}_{T/S}\, y'z) \geqslant -m(\mathfrak{q})$ для всех $z \in T$, удовлетворяющих условию $\nu_{\mathfrak{Q}}(z) \geqslant 0$ при всех $\mathfrak{Q} \in F^*$, и далее, что $\nu_{\mathfrak{p}}(\mathrm{Sp}_{T/R}\, y'z) \geqslant 0$, откуда $\nu_{\mathfrak{Q}}(y') \geqslant -m(\mathfrak{Q})$ при всех $\mathfrak{Q} \in F^*$. Таким образом, $m'(\mathfrak{Q}) \leqslant m(\mathfrak{Q})$, и теорема 8 доказана.

§ 9. Структура гиперэллиптических полей

Пусть R — поле алгебраических функций от одной переменной, а ω — дифференциал поля R, отличный от 0. Любой

дифференциал ω' поля R может быть представлен в виде $u\omega$, где u — однозначно определенный (при заданных ω и ω') элемент поля R. Элемент u называется *отношением дифференциалов* ω' *и* ω и часто обозначается через $\frac{\omega'}{\omega}$.

Предположим, что поле R имеет род $g > 0$. Тогда очевидно, что каждая константа может быть представлена в виде отношения дифференциалов первого рода. Если $g = 1$, то, и обратно, отношение любых дифференциалов первого рода является константой. Однако если $g > 1$, то существуют элементы, отличные от констант и представляющиеся в виде отношения дифференциалов первого рода. Поле R называется *гиперэллиптическим*, если подполе, порожденное всеми отношениями дифференциалов первого рода, отлично от самого поля R. Докажем следующий результат.

Теорема 9. *Пусть R — поле алгебраических функций от одной переменной, род которого больше 1. Для того чтобы поле R было гиперэллиптическим, необходимо и достаточно, чтобы в R существовало подполе S рода 0, содержащее поле констант поля R, и над которым R имеет степень 2. Если это условие выполнено, то подполе S определено однозначно, именно оно является подполем, порожденным отношениями дифференциалов первого рода поля R.*

Сначала мы докажем, что условие необходимо.

Лемма 1. *Для любой точки $\mathfrak{p}$ поля R алгебраических функций от одной переменной рода $g > 0$ существует дифференциал поля R первого рода, для которого эта точка не является нулем.*

Допустим противное. Для любого дивизора $\mathfrak{a}$ через $\delta(\mathfrak{a})$, как обычно, мы обозначим размерность пространства дифференциалов, делящихся на $\mathfrak{a}$. Тогда $\delta(\mathfrak{p}) = g$, откуда, в силу теоремы Римана—Роха, получаем $l(\mathfrak{p}^{-1}) = d(\mathfrak{p}) - g + 1 + g = d(\mathfrak{p}) + 1$; следовательно, существует элемент $x \in R$, отличный от константы и делящийся на $\mathfrak{p}^{-1}$. Пусть ω есть произвольный дифференциал первого рода, отличный от 0. Так как $\nu_{\mathfrak{p}}(x) = -1$, то $x^{\nu_{\mathfrak{p}}(\omega)}\omega$ является дифференциалом первого рода и для него точка $\mathfrak{p}$ не является нулем.

Следствие. *Если в поле R алгебраических функций от одной переменной существует целый дивизор $\mathfrak{a}$, удовле-*

творяющий условиям $l(\mathfrak{a}^{-1}) = d(\mathfrak{a}) + 1$ *и* $d(\mathfrak{a}) > 0$, *то род поля* R *равен* 0.

Действительно, из равенства $l(\mathfrak{a}^{-1}) = d(\mathfrak{a}) + 1$ следует (в силу теоремы Римана — Роха), что $\delta(\mathfrak{a}) = g$, где g — род поля R, а это означает, что каждый дифференциал первого рода делится на $\mathfrak{a}$.

Предположим теперь, что поле R имеет род $g > 1$ и является гиперэллиптическим; через S обозначим подполе, порожденное отношениями дифференциалов первого рода поля R. Так как $2g - 2 > 0$, то существует точка $\mathfrak{p}$ поля R, которая является нулем некоторого дифференциала первого рода поля R (и значит, $\delta(\mathfrak{p}) > 0$). Обозначим через $\mathfrak{p}_0$ точку поля S, лежащую под $\mathfrak{p}$, а через $\mathfrak{s}$ дивизор $\mathrm{Con}_{S/R}\,\mathfrak{p}_0$. Пусть ω_0 есть дифференциал первого рода поля R, для которого $\mathfrak{p}$ не является нулем. Если ω — дифференциал, делящийся на $\mathfrak{p}$, то $\omega = u\omega_0$, где $u \in S$, ибо ω и ω_0 — дифференциалы первого рода. Очевидно, что $\mathfrak{p}$ является нулем элемента u в поле R; следовательно, $\mathfrak{p}_0$ является нулем элемента u в поле S, а значит, дивизор нулей элемента u в поле R делится на $\mathfrak{s}$. Таким образом, каждый дифференциал, делящийся на $\mathfrak{p}$, делится также и на $\mathfrak{s}$.

Лемма 2. *Пусть* $\mathfrak{p}$ — *точка поля* R *алгебраических функций от одной переменной, а* $\mathfrak{s}$ — *целый дивизор, делящийся на* $\mathfrak{p}$. *Предположим, что каждый дифференциал поля* R, *делящийся на* $\mathfrak{p}$, *делится также и на* $\mathfrak{s}$, *причем хоть один такой дифференциал, отличный от* 0, *существует. Тогда* $l(\mathfrak{s}^{-1}) = l(\mathfrak{p}^{-1}) + d(\mathfrak{s}\mathfrak{p}^{-1})$ *и* $d(\mathfrak{s}\mathfrak{p}^{-1}) \leqslant d(\mathfrak{p})$.

По предположению имеем $\delta(\mathfrak{s}) = \delta(\mathfrak{p})$. С другой стороны, $l(\mathfrak{p}^{-1}) = d(\mathfrak{p}) - g + 1 + \delta(\mathfrak{p})$, где g — род поля R, и $l(\mathfrak{s}^{-1}) = d(\mathfrak{s}) - g + 1 + \delta(\mathfrak{s})$. Из этих формул непосредственно вытекает первое утверждение леммы 2. Пусть u — произвольный элемент поля R, делящийся на $\mathfrak{s}^{-1}\mathfrak{p}$. Тогда, если ω есть дифференциал, делящийся на $\mathfrak{p}$ (а значит, делящийся и на $\mathfrak{s}$), то $u\omega$ также делится на $\mathfrak{p}$. Покажем, что u необходимо является константой. Допустим противное; тогда элемент u имеет полюс $\mathfrak{q}$. Пусть m есть наименьшее значение, принимаемое выражением $\nu_{\mathfrak{q}}(\omega)$, когда ω пробегает все дифференциалы, делящиеся на $\mathfrak{p}$ ($m \neq \infty$, так как наше множество содержит хоть один дифференциал, отличный от 0). Выберем дифференциал ω_1, делящийся на $\mathfrak{p}$, для которого $\nu_{\mathfrak{q}}(\omega_1) = m$. Получаем теперь $\nu_{\mathfrak{q}}(u\omega_1) < m$, что противоречит

выбору ω_1. Таким образом, $l(\mathfrak{s}^{-1}\mathfrak{p}) = 1$. В силу формулы (4) § 1 гл. II имеем $l(\mathfrak{s}^{-1}) - l(\mathfrak{s}^{-1}\mathfrak{p}) \leqslant d(\mathfrak{p})$, откуда, применяя вышедоказанную формулу, получаем $l(\mathfrak{s}^{-1}\mathfrak{p}) \geqslant l(\mathfrak{p}^{-1}) + d(\mathfrak{s}\mathfrak{p}^{-1}) - d(\mathfrak{p}) \geqslant 1 + d(\mathfrak{s}\mathfrak{p}^{-1}) - d(\mathfrak{p})$, и неравенство $d(\mathfrak{s}\mathfrak{p}^{-1}) \leqslant d(\mathfrak{p})$ доказано.

Сохраняя введенные выше обозначения, вернемся теперь к доказательству теоремы 9. Среди всех точек поля R, лежащих над $\mathfrak{p}_0$, выберем точку $\mathfrak{p}'$ с наименьшей относительной степенью по отношению к полю S. Тогда $\delta(\mathfrak{p}') > 0$ и каждый дифференциал, делящийся на $\mathfrak{p}'$, делится и на $\mathfrak{s}$. Таким образом, мы имеем $d(\mathfrak{s}\mathfrak{p}'^{-1}) \leqslant d(\mathfrak{p}')$; отсюда следует, что либо $\mathfrak{s} = \mathfrak{p} = \mathfrak{p}'$, либо $\mathfrak{s}$ есть произведение двух точек (различных или равных), имеющих одну и ту же относительную степень f по отношению к S. Допустим, что имеет место второй случай. Каждый элемент поля R, делящийся на $\mathfrak{s}^{-1}$, принадлежит S (если y — любой из таких элементов, а ω — отличный от 0 дифференциал, делящийся на $\mathfrak{s}$, то $y\omega$ есть дифференциал первого рода). Следовательно, $l(\mathfrak{s}^{-1}) = l(\mathfrak{p}_0^{-1})$, откуда, применяя лемму 2, получаем, что $l(\mathfrak{p}_0^{-1}) \geqslant 1 + d(\mathfrak{p}) = 1 + f\,d(\mathfrak{p}_0)$. С другой стороны, мы имеем $l(\mathfrak{p}_0^{-1}) \leqslant 1 + d(\mathfrak{p}_0)$ (ибо $\delta(\mathfrak{p}_0)$ не превосходит рода поля S). Таким образом, $f = 1$ и $l(\mathfrak{p}_0^{-1}) = 1 + d(\mathfrak{p}_0)$. Применяя теорему 1 § 1, получаем, что $[R:S] = 2$ (так как $f = 1$). В силу следствия к лемме 1 род поля S равен 0.

Теперь мы должны рассмотреть случай, когда $\mathfrak{s} = \mathfrak{p}$. Пусть $f = [R:S]$ есть относительная степень точки $\mathfrak{p}$ по отношению к полю S. Обозначим через $\mathfrak{d}$ дивизор какого-нибудь дифференциала $\omega_0 \neq 0$ первого рода, не делящегося на $\mathfrak{p}$, а через $\Sigma(\mathfrak{p})$ и $\Sigma(\mathfrak{p}_0)$ — поля вычетов точек $\mathfrak{p}$ и $\mathfrak{p}_0$ соответственно. Пусть ξ — произвольный элемент из $\Sigma(\mathfrak{p})$, а η — дифференциал поля R, делящийся на $\mathfrak{p}^{-1}\mathfrak{d}$. Рассмотрим распределение $\mathfrak{x}$ поля R, сопоставляющее точке $\mathfrak{p}$ какой-нибудь элемент поля R, значение которого в $\mathfrak{p}$ равно ξ, а всем другим точкам — значение 0. Тогда $\eta(\mathfrak{x})$ зависит только от ξ и η, так как, если $\mathfrak{x}$ и $\mathfrak{x}'$ — два распределения, удовлетворяющие нашим условиям, то $\mathfrak{x}' - \mathfrak{x} \equiv 0 \pmod{\mathfrak{p}}$, а значит, и подавно, $\mathfrak{x}' - \mathfrak{x} \equiv 0 \pmod{\mathfrak{d}^{-1}\mathfrak{p}}$. Если мы положим $L_\eta(\xi) = \eta(\mathfrak{x})$, то отображение $\eta \to L_\eta$ будет линейным отображением пространства $\mathfrak{D}$ дифференциалов, делящихся на

$\mathfrak{p}^{-1}\mathfrak{d}$, в пространство линейных функций на поле $\Sigma(\mathfrak{p})$ (если его рассматривать как векторное пространство над полем констант K поля R). Дифференциал ω_0 является дифференциалом первого рода и содержится в $\mathfrak{D}$. Так как $L_{\omega_0}=0$, то размерность пространства, образованного функциями L_η, не превосходит $\dim\mathfrak{D}-1$. Отсюда следует, что подпространство X поля $\Sigma(\mathfrak{p})$, состоящее из тех элементов ξ, для которых $L_\eta(\xi)=0$ при всех $\eta\in\mathfrak{D}$, имеет размерность $\geqslant d(\mathfrak{p})-\dim\mathfrak{D}+1$. Дифференциалы $\eta\in\mathfrak{D}$ совпадают с дифференциалами вида $y\omega_0$, где $y\in R$, $y\equiv 0 \pmod{\mathfrak{p}^{-1}}$; следовательно, $\dim\mathfrak{D}=l(\mathfrak{p}^{-1})$, а это равно $l(\mathfrak{p}_0^{-1})$ (см. проведенное выше рассуждение). Далее, пусть ξ — элемент из X, а $\mathfrak{x}$ — указанное выше распределение. В силу теоремы 2 § 5 гл. II в поле R существует такой элемент u, что $u-\mathfrak{x}\equiv 0 \pmod{\mathfrak{p}\mathfrak{d}^{-1}}$. Элемент u делится на $\mathfrak{d}^{-1}$ и принимает в точке $\mathfrak{p}$ значение ξ. Так как дифференциал $u\omega_0$ первого рода, то $u\in S$, а значит, $\xi\in\Sigma(\mathfrak{p}_0)$. Следовательно, $\dim X\leqslant d(\mathfrak{p}_0)$, откуда $d(\mathfrak{p}_0)\geqslant d(\mathfrak{p})-l(\mathfrak{p}^{-1})+1=f\,d(\mathfrak{p}_0)-l(\mathfrak{p}_0^{-1})+1$ и $l(\mathfrak{p}_0^{-1})\geqslant(f-1)\,d(\mathfrak{p}_0)+1$. С другой стороны, $l(\mathfrak{p}_0^{-1})\leqslant d(\mathfrak{p}_0)+1$. Таким образом, мы имеем $[R:S]=f=2$ и $l(\mathfrak{p}_0^{-1})=d(\mathfrak{p}_0)+1$. В силу следствия к лемме 1 род поля S равен 0. Этим завершено доказательство того, что всякое гиперэллиптическое поле рода $g>1$ является квадратичным расширением над полем рода 0 (именно над полем, порожденным отношениями дифференциалов первого рода).

Обратно, пусть R есть поле алгебраических функций от одной переменной рода $g>1$, в котором имеется подполе S, содержащее поле констант K поля R и обладающее свойствами: степень $[R:S]$ равна 2 и род поля S равен 0. Пусть $\mathfrak{q}_0$ — точка поля S наименьшей возможной степени, тогда, как мы знаем, $d(\mathfrak{q}_0)$ равно либо 1, либо 2 (§ 6 гл. II). Рассмотрим сначала случай, когда $d(\mathfrak{q}_0)=1$, или $d(\mathfrak{q}_0)=2$, но $g\equiv 1 \pmod 2$. В этом случае положим $\mathfrak{a}_0=\mathfrak{q}_0^{g-1}$, если $d(\mathfrak{q}_0)=1$, и $\mathfrak{a}_0=\mathfrak{q}_0^{\frac{g-1}{2}}$, если $d(\mathfrak{q}_0)=2$; очевидно, что $d(\mathfrak{a}_0)=g-1$. Пусть $\mathfrak{a}=\mathrm{Con}_{S/R}\mathfrak{a}_0$, тогда $d(\mathfrak{a})=2g-2$ (лемма 1 § 7). Обозначим через $\mathfrak{L}$ пространство тех элементов $z\in S$, которые делятся на $\mathfrak{a}_0^{-1}$. Так как род поля S равен 0, то $l(\mathfrak{a}_0^{-1})=d(\mathfrak{a}_0)+1=g$, т. е.

$\dim \mathfrak{L} = g$. Далее, $g = l(\mathfrak{a}_0^{-1}) \leqslant l(\mathfrak{a}^{-1}) = d(\mathfrak{a}) - g + 1 + \delta(\mathfrak{a}) = g - 1 + \delta(\mathfrak{a})$, поэтому $\delta(\mathfrak{a}) > 0$. Таким образом, существует дифференциал $\omega \neq 0$ поля R, делящийся на $\mathfrak{a}$. Если $z \in \mathfrak{L}$, то $z\omega$ является дифференциалом первого рода. Так как $\dim \mathfrak{L} = g$, то получаем, что каждый дифференциал поля R первого рода имеет вид $z\omega$, где $z \in S$. Таким образом, поле R является гиперэллиптическим, и поле S', порожденное отношениями дифференциалов первого рода поля R, содержится в S. Так как в первой части доказательства было установлено, что $[R : S'] = 2$, то $S' = S$.

Рассмотрим теперь случай, когда $d(\mathfrak{q}_0) = 2$ и $g \equiv 0 \pmod 2$. Положим $\mathfrak{a}_0 = \mathfrak{q}_0^{\frac{g-2}{2}}$ и $\mathfrak{a} = \mathrm{Con}_{S/R}\, \mathfrak{a}_0$. Так же как и в предыдущем случае, легко доказывается, что $l(\mathfrak{a}_0^{-1}) = g - 1$ и $\delta(\mathfrak{a}) > 0$. Пусть ω — отличный от 0 дифференциал, делящийся на $\mathfrak{a}$; дивизор $\mathfrak{d}(\omega)$ дифференциала ω имеет вид $\mathfrak{a}\mathfrak{b}$, где $\mathfrak{b}$ — целый дивизор степени 2. Так как $d(\mathfrak{q}_0) = 2$, то каждая точка поля S имеет степень $\geqslant 2$; это же справедливо, тем более, для каждой точки поля R. Таким образом, $\mathfrak{b}$ есть точка $\mathfrak{p}$. Если элемент z из поля S делится на $\mathfrak{a}_0^{-1}$, то $z\omega$ делится на $\mathfrak{p}$, откуда $\delta(\mathfrak{p}) \geqslant g - 1$. Следовательно, $l(\mathfrak{p}^{-1}) = d(\mathfrak{p}) - g + 1 + \delta(\mathfrak{p}) \geqslant 2$. Если w есть отличный от константы элемент поля R, делящийся на $\mathfrak{p}^{-1}$, то $[R : K\langle w\rangle] = 2$, ибо дивизор полюсов элемента w равен $\mathfrak{p}$ (следствие к теореме 4 § 8 гл. I). Если мы вместо S рассмотрим поле $W = K\langle w\rangle$, в котором имеется точка степени 1, то будем иметь уже рассмотренный случай; следовательно, поле W порождено отношениями дифференциалов первого рода поля R. Мы имеем $l(\mathfrak{q}_0^{-1}) = d(\mathfrak{q}_0) + 1 = 3$; Пусть $\{1, u, v\}$ есть базис пространства тех элементов поля S, которые делятся на $\mathfrak{q}_0^{-1}$. Дивизор полюсов элемента u в поле S равен $\mathfrak{q}_0$, поэтому $[S : K\langle u\rangle] = 2$. Если $\mathfrak{q}_0'$ есть точка поля $K\langle u\rangle$, лежащая под $\mathfrak{q}_0$, то $l(\mathfrak{q}_0'^{-1}) = 2$, откуда следует, что $v \notin K\langle u\rangle$, а значит, $S = K\langle u, v\rangle$. Если $g > 2$, то элементы u и v делятся на $\mathfrak{a}_0^{-1}$, а значит $u\omega$ и $v\omega$ являются дифференциалами первого рода, но тогда u и v принадлежат W, т. е. $S \subset W$, а это невозможно, так как поле S не имеет точек степени 1, в то время как W имеет такие точки. Пусть $g = 2$; обозначим через $\mathfrak{p}_0$ точку поля S, лежащую под $\mathfrak{p}$, а через $\mathfrak{c}$

дивизор $\mathrm{Con}_{S/R}\,\mathfrak{p}_0$. Так как $d(\mathfrak{p})=2$ и $d(\mathfrak{p}_0)\geqslant 2$, то $d(\mathfrak{p}_0)=2$ и $d(\mathfrak{c})=4$ (лемма 1 § 7). В силу того, что $2g-2=2$, имеем $\delta(\mathfrak{c})=0$, откуда $l(\mathfrak{c}^{-1})=d(\mathfrak{s})-2+1=3$. С другой стороны $l(\mathfrak{p}_0^{-1})=d(\mathfrak{p}_0)+1=3$, и каждый элемент поля S, делящийся на $\mathfrak{p}_0^{-1}$, делится и на $\mathfrak{c}^{-1}$ в поле R. Так как $l(\mathfrak{c}^{-1})=l(\mathfrak{p}_0^{-1})$, то, стало быть, каждый элемент поля R, делящийся на $\mathfrak{c}^{-1}$, принадлежит S. Это относится, в частности, и к элементу w, ибо $\mathfrak{c}$ делится на $\mathfrak{p}$. Следовательно, поле $K\langle w\rangle$ содержится в S. Так как $[R:S]=[R:K\langle w\rangle]=2$, то $S=K\langle w\rangle$. Но это опять невозможно по тем же причинам, что и выше. Таким образом, второй случай вообще не может иметь места. Теорема 9 теперь доказана полностью.

Так как род поля S теоремы 9 равен 0, то это поле имеет точки степени $\leqslant 2$; отсюда следует, что *гиперэллиптическое поле рода $g>1$ имеет точку степени $\leqslant 4$*. Более того, последняя часть доказательства показывает, что *при четном g поле R имеет точку степени $\leqslant 2$*. Если поле R сепарабельно над S (что всегда имеет место, если характеристика поля R не равна 2), то, как легко доказать, поле R имеет по крайней мере одну точку, разветвленную относительно S (см. следствие 2 к теореме 2 § 2 гл. VI); следовательно, в этом случае поле R имеет точку степени $\leqslant 2$, а если g четно, то имеет точку степени 1.

Теорема 10. *Пусть R — поле алгебраических функций от одной переменной рода $g>1$. Предположим, что R имеет точку $\mathfrak{p}$ степени 1 и не является гиперэллиптическим. Тогда для любой точки $\mathfrak{q}\neq\mathfrak{p}$ поля R существует дифференциал ω первого рода поля R такой, что $\nu_{\mathfrak{p}}(\omega)=1$ и $\nu_{\mathfrak{q}}(\omega)=0$.*

Так как $1\leqslant l(\mathfrak{p}^{-1})=d(\mathfrak{p})-g+1+\delta(\mathfrak{p})=2-g+\delta(\mathfrak{p})$ и $g\geqslant 2$, то $\delta(\mathfrak{p})>0$, т. е. существует по крайней мере один дифференциал, отличный от 0 и делящийся на $\mathfrak{p}$. Пусть $\mathfrak{s}$ есть целый дивизор наибольшей степени, на который делится каждый дифференциал, делящийся на $\mathfrak{p}$. В силу леммы 2 имеем $d(\mathfrak{s}\mathfrak{p}^{-1})\leqslant d(\mathfrak{p})=1$, откуда $d(\mathfrak{s})\leqslant 2$. Предположим, что $d(\mathfrak{s})=2$; тогда $l(\mathfrak{s}^{-1})=l(\mathfrak{p}^{-1})+1\geqslant 2$; следовательно, в поле R существует отличный от константы элемент x, который делится на $\mathfrak{s}^{-1}$. Так как дивизор полюсов элемента x равен либо $\mathfrak{p}$, либо $\mathfrak{s}$, то по следствию к теореме 4 § 8 гл. I степень $[R:K\langle x\rangle]$ равна либо 1, либо 2. Но тогда поле R

либо имеет род 0 или 1, либо является гиперэллиптическим, что противоречит предположению. Таким образом, мы имеем $\mathfrak{d} = \mathfrak{p}$. Отсюда следует, что существуют дифференциалы ω_1 и ω_2 поля R, делящиеся на $\mathfrak{p}$, такие, что $\nu_{\mathfrak{p}}(\omega_1) = 1$ и $\nu_{\mathfrak{q}}(\omega_2) = 0$. Если $\nu_{\mathfrak{q}}(\omega_1) = 0$ или $\nu_{\mathfrak{p}}(\omega_2) = 1$, то $\omega = \omega_1$ или $\omega = \omega_2$ удовлетворяет нашим условиям; если же $\nu_{\mathfrak{q}}(\omega_1) > 0$ и $\nu_{\mathfrak{p}}(\omega_2) > 1$, то мы можем взять $\omega = \omega_1 + \omega_2$. Теорема 10, таким образом, доказана.

В применении к алгебраической геометрии теорема 10 дает возможность построить „нормальную модель“ поля R — кривую в g-мерном проективном пространстве, которая не имеет особенностей и поле рациональных функций которой равно R.

ГЛАВА V

РАСШИРЕНИЯ ПОЛЯ КОНСТАНТ

§ 1. Трансцендентные сепарабельные расширения

Обычно понятие сепарабельности определяется только для алгебраических расширений. Сейчас мы распространим это понятие на произвольные расширения, используя для этой цели кронекеровское произведение коммутативных алгебр (см. § 4 гл. IV).

Лемма 1. *Пусть K — произвольное поле, а M — его алгебраическое расширение. Если поле M сепарабельно над K, то для любого расширения L поля K алгебра $L \otimes M$ не имеет нильпотентных элементов, отличных от 0. Если же M несепарабельно над K, то существует такое расширение L поля K, что алгебра $L \otimes M$ содержит нильпотентные элементы, отличные от 0; при этом поле L можно выбрать так, чтобы степень $[L:K]$ была конечной и чтобы $L^p \subset K$, где p — характеристика поля K.*

Пусть поле M сепарабельно над K и пусть $x = \sum_{k=1}^{h} u_k v_k$ есть нильпотентный элемент из $L \otimes M$ ($u_k \in L$, $v_k \in M$, $1 \leqslant k \leqslant h$). Поле $M_1 = K\langle v_1, \ldots, v_n\rangle$ сепарабельно и имеет конечную степень над K, причем $x \in L \otimes M_1$. Мы имеем $M_1 = K\langle v\rangle$, где $v \in M_1$; пусть $F(X)$ — неприводимый многочлен с коэффициентами из K, для которого $F(v) = 0$. Если n есть степень F, то элементы $1, v, \ldots, v^{n-1}$ образуют базис поля M_1 относительно K, а значит, и базис алгебры $L \otimes M_1$ относительно L. Отсюда следует, что кольцо $L \otimes M_1$ изоморфно фактор-кольцу $L[X]/\mathfrak{r}$, где $\mathfrak{r}$ — идеал, порожденный многочленом $F(X)$ в кольце $L[X]$. Элемент x мы можем представить в виде $G(v)$, где G — многочлен с коэффициентами из L. Если $x^\alpha = 0$, то многочлен G^α должен делиться на F.

Так как элемент v сепарабелен над K, то многочлен F и над полем L не содержит кратных множителей; следовательно, не только G^{α}, но и сам многочлен G делится на F, откуда $x=0$.

Пусть теперь поле M несепарабельно над K, а v элемент из M, несепарабельный над K. Пусть $F(X)$ есть неприводимый многочлен с коэффициентами из K, для которого $F(v)=0$. Тогда, как известно, имеем $F=F_1(X^p)$, где F_1 — многочлен с коэффициентами из K. Пусть L есть расширение поля K, в котором все коэффициенты многочлена F являются p-ыми степенями; очевидно, что поле L можно выбрать так, чтобы степень $[L:K]$ была конечной и $L^p \subset K$. Имеем тогда $F(X)=(G(X))^p$, где G — многочлен с коэффициентами из L. Так как степень многочлена G меньше степени F, то $G(v) \neq 0$ в алгебре $L \otimes M$; однако $(G(v))^p=0$. Лемма 1, таким образом, доказана.

Пусть K есть поле характеристики $p>0$; расширение L поля K будем называть *радикальным расширением*, если $L^p \subset K$. Если характеристика поля K равна 0, то будем считать, что только $L=K$ является радикальным расширением поля K. Радикальное расширение назовем *конечным*, если оно имеет конечную степень. Расширение M поля K будем называть *сепарабельным над* K, если для любого конечного радикального расширения L поля K алгебра $L \otimes M$ не имеет нильпотентных элементов, отличных от 0. Согласно этому определению всякое расширение поля характеристики 0 является сепарабельным. Для алгебраических расширений наше новое понятие сепарабельности совпадает с классическим (лемма 1).

Лемма 2. *Пусть L и M — расширения поля K. Если поле L чисто несепарабельно над K, то в алгебре $L \otimes M$ каждый делитель нуля нильпотентен.*

Пусть элемент $x=\sum_{k=1}^{h} u_k v_k \, (u_k \in L, \ v_k \in M)$ из $L \otimes M$ является делителем нуля. Так как поле L чисто несепарабельно над K, то существует такой показатель $a>0$, что $u_k^{p^a} \in K \, (1 \leqslant k \leqslant h)$, а тогда $x^{p^a}=\sum_{k=1}^{h} u_k^{p^a} v_k^{p^a} \in M$. Если бы $x^{p^a} \neq 0$, то для x^{p^a} существовал бы в M обратный

элемент, что, однако, невозможно, ибо x является делителем нуля. Лемма 2, таким образом, доказана.

Следствие. *Если M — сепарабельное, а L — конечное радикальное расширения поля K, то алгебра $L \otimes M$ есть поле, и это поле является конечным радикальным расширением поля M, причем $[L \otimes M : M] = [L : K]$.*

Из определения и леммы 2 следует, что $L \otimes M$ не имеет делителей нуля, отличных от 0. Если $L = K[u_1, \ldots, u_r]$, то $L \otimes M = M[u_1, \ldots, u_r]$, причем $u_k^p \in K \subset M$ $(1 \leqslant k \leqslant r)$; значит, $L \otimes M$ есть поле и является конечным радикальным расширением поля M. Последнее утверждение следствия вытекает из определения кронекеровских произведений.

Лемма 3. *Пусть M есть расширение поля K, а M_1 — промежуточное поле между K и M. Если M сепарабельно над K, то и M_1 сепарабельно над K. Если M_1 сепарабельно над K, а M сепарабельно над M_1, то M сепарабельно над K.*

Пусть L есть конечное радикальное расширение поля K. Первое утверждение леммы непосредственно вытекает из включения $L \otimes M_1 \subset L \otimes M$. Пусть M_1 сепарабельно над K, а M — над M_1. Мы имеем $L_M = (L_{M_1})_M$. По следствию к лемме 2 L_{M_1} есть конечное радикальное расширение поля M_1. Так как M сепарабельно над M_1, то L_M не имеет нильпотентных элементов, отличных от 0.

Лемма 4. *Пусть L и M — расширения поля K. Если поле M чисто трансцендентно над K, то алгебра $L \otimes M$ не имеет делителей нуля, отличных от 0; при этом поле отношений U этого кольца чисто трансцендентно над L. Если $M = K\langle x_i \rangle_{i \in I}$, где элементы x_i алгебраически независимы над K, то $U = L\langle x_i \rangle_{i \in I}$ и элементы x_i алгебраически независимы также и над L.*

Элементы $x_{i_1}^{e_1} \ldots x_{i_n}^{e_n} \in M$ (где $i_1, \ldots, i_n$ — любые различные элементы из I, а $e_1, \ldots, e_n$ — неотрицательные показатели) линейно независимы над K, поэтому в кольце $L \otimes M$ они будут линейно независимы и над L. Следовательно, кольцо $L[x_i]_{i \in I}$ не имеет делителей нуля, отличных от 0. Пусть u и u' — элементы из $L \otimes M$ такие, что $uu' = 0$. Мы имеем $u = \sum_{k=1}^{h} y_k z_k$, $u' = \sum_{k=1}^{h'} y'_k z'_k$, где $y_k, y'_k \in L$ и $z_k, z'_k \in M$.

В кольце $K[x_i]_{i\in I}$ найдем такой элемент $v\neq 0$, чтобы все элементы vz_k $(1\leqslant k\leqslant h)$, vz'_k $(1\leqslant k\leqslant h')$ принадлежали кольцу $K[x_i]_{i\in I}$. Тогда $vu\in L[x_i]_{i\in I}$ и $vu'\in L[x_i]_{i\in I}$, причем $(vu)(vu')=0$. Следовательно, хоть один из элементов vu и vu' равен 0. Так как для v существует обратный элемент в M, а значит, и в $L\otimes M$, то хоть один из элементов u и u' равен 0. Поле отношений кольца $L[x_i]_{i\in I}$, содержащее L и M, необходимо содержит и U. Лемма 4 доказана.

Будем говорить, что расширение M поля K *сепарабельно порождаемо над* K, если между K и M существует промежуточное поле T, являющееся чисто трансцендентным расширением поля K, над которым поле M алгебраично и сепарабельно. Поле R алгебраических функций от одной переменной называется *сепарабельно порождаемым*, если оно сепарабельно порождаемо над своим полем констант K; в этом случае всякий элемент x из R, для которого поле R алгебраично и сепарабельно над $K\langle x\rangle$ называется *сепарабельно порождающей переменной* поля R. Из лемм 3 и 4 следует, что всякое сепарабельно порождаемое расширение M поля K является также сепарабельным расширением. Обратное утверждение, вообще говоря, не имеет места. Однако справедливо следующее частичное обращение.

Лемма 5. *Если сепарабельное расширение M поля K может быть получено из K присоединением конечного числа элементов, то оно является сепарабельно порождаемым расширением поля K.*

Пусть $M=K\langle y_1, \ldots, y_r\rangle$, где элементы $y_1, \ldots, y_r$ принадлежат M. Обозначим через p характеристику поля K (можно считать, что $p>0$), а через P — поле $K\langle M^p\rangle$, полученное из K присоединением p-ых степеней элементов из M; тогда $M=P\langle y_1, \ldots, y_r\rangle$. Пусть s есть наименьшее целое число такое, что M может быть получено из P присоединением s элементов y_i; будем считать, что $M=P\langle y_1, \ldots, y_s\rangle$. Докажем, что элементы $y_1, \ldots, y_s$ алгебраически независимы над K. Допустим противное; тогда существует такой неприводимый многочлен $F(Y_1, \ldots, Y_s)$ с коэффициентами из K, что

$$F(y_1, \ldots, y_s)=0.$$

Можно считать, что F имеет наименьшую степень d среди многочленов с этими свойствами. Для любого i; $1 \leqslant i \leqslant s$, мы можем записать

$$F = \sum_{k=0}^{p-1} G_k(X_1, \ldots, X_s) X_i^k,$$

где $G_k(X_1, \ldots, X_s)$ — многочлен с коэффициентами из K, в который переменная X_i входит только с показателями, делящимися на p. Элемент $G_k(y_1, \ldots, y_s)$ принадлежит полю P_i, полученному из P присоединением элементов y_j при $j \neq i$ (ибо $y_i^p \in P$). Так как $y_i^p \in P_i$, а $y_i \notin P_i$, то элемент y_i не может удовлетворять никакому уравнению степени $< p$ с коэффициентами из P_i; отсюда следует, что $G_k(y_1, \ldots, y_s) = 0$ $(0 \leqslant k \leqslant p-1)$. Но многочлен F мы выбрали с наименьшей возможной степенью, поэтому $F = G_0$ и $G_k = 0$ при $k > 0$. Так как это верно для каждого i $(1 \leqslant i \leqslant s)$, то $F(y_1, \ldots, y_s) = H(Y_1^p, \ldots, Y_s^p)$, где H — многочлен с коэффициентами из K. Пусть L есть поле, полученное из K присоединением p-ых корней коэффициентов многочлена H; тогда

$$F(Y_1, \ldots, Y_s) = (J(Y_1, \ldots, Y_s))^p,$$

где J — многочлен степени $\frac{d}{p}$ с коэффициентами из L. Так как многочлен F по выбору имеет наименьшую возможную степень, то одночлены вида $y_1^{\alpha_1} \ldots y_s^{\alpha_s} \in M$ степени $< d$ линейно независимы над K, поэтому они линейно независимы также и над полем L в алгебре $L \otimes M$. Следовательно, $J(y_1, \ldots, y_s) \neq 0$, в то время как $(J(y_1, \ldots, y_s))^p = 0$; мы получили противоречие, ибо по предположению поле M сепарабельно над K. Таким образом, элементы $y_1, \ldots, y_s$ действительно алгебраически независимы над K. Обозначим через T_0 поле, полученное из K присоединением элементов $y_1, \ldots, y_s$, тогда поле $T_0\langle M^p \rangle$ содержит $P\langle y_1, \ldots, y_s \rangle = M$, а значит, $T_0\langle M^p \rangle = M$. Если поле M алгебраично над T_0 (именно это на самом деле всегда и имеет место, однако этот факт мы здесь не доказываем), то оно также и сепарабельно над T_0. Действительно, пусть N есть подполе элементов поля M, сепарабельных над T_0. Тогда, как известно, $N \supset M^{p^a}$ при некотором $a > 0$; с другой стороны,

так как $M = T_0\langle M^p\rangle$, то $M = T_0\langle M^p\rangle = T_0\langle M^{p^2}\rangle = \ldots$ $\ldots = T_0\langle M^{p^a}\rangle$, откуда $M = N$. Если же M не алгебраично над T_0, то из множества $\{y_{s+1}, \ldots, y_r\}$ мы можем выделить трансцендентный базис поля M относительно T_0. Присоединяя элементы этого трансцендентного базиса к полю T_0, мы получим поле T, чисто трансцендентное над K, над которым поле M алгебраично. Так как $T_0 \subset T$, то $M = T\langle M^p\rangle$; теперь так же, как и выше, легко получаем, что M сепарабельно над T.

Следствие 1. *Для того чтобы поле алгебраических функций от одной переменной было сепарабельным над своим полем констант, необходимо и достаточно, чтобы оно было сепарабельно порождаемым.*

Следствие 2. *Пусть L и M — два расширения поля K. Если поле M сепарабельно над K, то алгебра $L \otimes M$ не имеет нильпотентных элементов, отличных от* 0.

Действительно пусть $x = \sum_{k=1}^{h} u_k v_k$ $(u_k \in L, v_k \in M, 1 \leqslant k \leqslant h)$ есть нильпотентный элемент алгебры $L \otimes M$. Элемент x, очевидно, принадлежит алгебре $L \otimes M'$, где $M' = K\langle v_1, \ldots, v_h\rangle$. Так как поле M' сепарабельно над K (лемма 3), то оно алгебраично и сепарабельно над некоторым чисто трансцендентным расширением T поля K (лемма 5). Мы имеем $L_{M'} = (L_T)_{M'}$, и L_T содержится в поле U (лемма 4), откуда $L_{M'} \subset U_{M'}$ (где U рассматривается как алгебра над T). Так как поле M' алгебраично и сепарабельно над T, то $U_{M'}$ не имеет нильпотентных элементов, отличных от 0 (лемма 1); значит, $x = 0$.

§ 2. Относительно алгебраически замкнутые подполя

Подполе K поля L называется *относительно алгебраически замкнутым* в L, если каждый элемент из L, алгебраический над K, содержится в поле K.

Лемма 1. *Пусть K — относительно алгебраически замкнутое подполе поля L. Если многочлен $F(X_1, \ldots, X_n)$ от n переменных с коэффициентами из K неприводим в кольце*

$$K[X_1, \ldots, X_n],$$

то он неприводим также и в кольце $L[X_1, \ldots, X_n]$.

1) Рассмотрим сначала случай $n=1$. Пусть в кольце $L[X_1]$ многочлен $F(X_1)$ имеет множитель $G(X_1)$, степень которого >0; будем считать, что старший коэффициент многочлена $G(X_1)$ равен 1. В некотором расширении L' поля L многочлен G раскладывается на линейные множители:

$$G(X_1)=\prod_{i=1}^{r}(X_1-x_i).$$

Так как $F(x_i)=0$ $(1\leqslant i\leqslant r)$, то элементы x_i алгебраичны над K. Отсюда следует, что коэффициенты многочлена G также алгебраичны над K. Но эти коэффициенты принадлежат L, поэтому они на самом деле принадлежат полю K. Так как многочлен F неприводим в $K[X_1]$, то G отличается от F только постоянным множителем. Таким образом, для случая $n=1$ лемма 1 доказана.

2) В общем случае мы используем один остроумный прием, предложенный Кронекером. Пусть D — степень многочлена F; положим $a_i=(D+1)^i\cdot i!$ $(1\leqslant i\leqslant n)$. Если $H(X_1,\ldots,X_n)$ есть многочлен от $X_1,\ldots,X_n$, то через H^* мы обозначим многочлен, получаемый из H с помощью подстановки $X_i\to T^{a_i}$ $(1\leqslant i\leqslant n)$, где T — новая переменная. Пусть $M_1=X_1^{e_1}\ldots X_n^{e_n}$ и $M_2=X_1^{f_1}\ldots X_n^{f_n}$ — одночлены, степени которых не превосходят D; тогда из равенства $M_1^*=M_2^*$ следует, что $M_1=M_2$. В самом деле, предположим, что $\sum_{i=1}^{n}e_ia_i=\sum_{i=1}^{n}f_ia_i$ и что $e_i=f_i$ при $i>r$ (где $1\leqslant r\leqslant n$); тогда будем иметь

$$a_r(f_r-e_r)=-\sum_{i<r}a_i(f_i-e_i).$$

Так как $|f_i-e_i|\leqslant D$ при всех i, то

$$\left|\sum_{i<r}a_i(f_i-e_i)\right|\leqslant rD(D+1)^{r-1}(r-1)!<(D+1)^r r!=a_r,$$

откуда $e_r=f_r$. Из доказанного следует, что для любого многочлена H степени $\leqslant D$ все коэффициенты H^* являются коэффициентами H, и обратно. Под старшим коэффициентом многочлена H (степени $\leqslant D$) будем понимать старший

коэффициент многочлена H^*. Допустим, что

$$F = aG_1 \ldots G_h,$$

где $G_1, \ldots, G_h$ — неприводимые многочлены с коэффициентами из L, старшие коэффициенты которых равны 1 (здесь a является, очевидно, старшим коэффициентом F). Так как $F^* = a\overset{*}{G}_1 \ldots \overset{*}{G}_h$, то каждый многочлен $\overset{*}{G}_i$ является произведением неприводимых множителей многочлена F^* в кольце $L[T]$, старшие коэффициенты которых равны 1. Но из первой части доказательства следует, что каждый неприводимый множитель многочлена F^* в кольце $L[T]$ со старшим коэффициентом 1 является на самом деле неприводимым множителем многочлена F^* в кольце $K[T]$. Таким образом, коэффициенты каждого многочлена $\overset{*}{G}_i$ принадлежат полю K. Так как степень многочлена G_i не превосходит D, то коэффициенты каждого G_i также принадлежат K. Этим доказано, что многочлен F неприводим в кольце $L[X_1, \ldots, X_n]$.

Следствие. *Пусть L есть расширение поля K, и пусть $F(X_1, \ldots, X_n)$ — многочлен от n переменных с коэффициентами из K. Тогда многочлен F может быть разложен на неприводимые в кольце $L[X_1, \ldots, X_n]$ множители, коэффициенты которых алгебраичны над K.*

Элементы поля L, алгебраичные над K, образуют подполе K'; мы можем взять разложение многочлена F на неприводимые множители в кольце $K'[X_1, \ldots, X_n]$.

Лемма 2. *Пусть K — относительно алгебраически замкнутое подполе поля L. Пусть $M = L\langle x_i\rangle_{i\in I}$ есть расширение поля L, полученное присоединением элементов x_i, алгебраически независимых над L. Тогда поле $K\langle x_i\rangle_{i\in I}$ относительно алгебраически замкнуто в M.*

Пусть элемент y из M алгебраичен над $K\langle x_i\rangle_{i\in I}$. Очевидно, что в множестве I можно найти такое конечное число индексов $i_1, \ldots, i_m$, что элемент y принадлежит полю $L\langle x_{i_1}, \ldots, x_{i_m}\rangle$ и алгебраичен над $K\langle x_{i_1}, \ldots, x_{i_m}\rangle$. Пусть $F(X_1, \ldots, X_m, Y)$ — неприводимый многочлен от $m+1$ переменных с коэффициентами из K такой, что $F(x_{i_1}, \ldots, x_{i_m}, y) = 0$. Из леммы 1 вытекает, что F неприводим также и в кольце $L[X_1, \ldots, X_m, Y]$; следовательно, многочлен

$$F(x_{i_1}, \ldots, x_{i_m}, Y)$$

неприводим в кольце $L\langle x_{i_1}, \ldots, x_{i_m}\rangle[Y]$. Так как $y \in L\langle x_{i_1}, \ldots, x_{i_m}\rangle$, то степень F относительно Y равна 1, а значит, $y \in K\langle x_{i_1}, \ldots, x_{i_m}\rangle$.

Лемма 3. *Пусть L и R — расширения поля K. Если каждый элемент поля R, алгебраический над K, чисто несепарабелен над K, то в алгебре $L \otimes R$ всякий делитель нуля нильпотентен.*

Всякий делитель нуля в $L \otimes R$ является также делителем нуля и в некоторой алгебре $L' \otimes R'$, где L' и R' — подполя полей L и R соответственно, которые могут быть получены из K присоединением конечного числа элементов. Поэтому, не ограничивая общности, мы можем считать, что поля L и R сами могут быть получены из K присоединением конечного числа элементов. Пусть R_1 есть поле, состоящее из тех элементов поля R, которые алгебраичны над K. Если поле K имеет характеристику $p > 0$, то при некотором показателе e будем иметь $R_1^{p^e} \subset K$. Действительно, поле R является алгебраическим расширением конечной степени поля R_0, которое чисто трансцендентно над K; следовательно, существует такое целое число $e > 0$, что $R_0\langle R^{p^e}\rangle$ сепарабельно над R_0. Из лемм 3 и 4 § 1 вытекает, что $R_0\langle R^{p^e}\rangle$ сепарабельно над K. В частности, поле $K\langle R_1^{p^e}\rangle$ сепарабельно над K; с другой стороны, это поле чисто несепарабельно над K; значит, оно совпадает с K. Обозначим через B трансцендентный базис поля L относительно K и положим $T = K\langle B\rangle$. Тогда, как нам известно (лемма 4 § 1), алгебра $T \otimes R$ не имеет делителей нуля, отличных от 0; кроме того, если S есть поле отношений этого кольца, то $S = R\langle B\rangle$, при этом элементы из B алгебраически независимы над полем R. Обозначим через S_1 подполе $T\langle R_1\rangle$ поля S, тогда в силу леммы 2 поле S_1 относительно алгебраически замкнуто в S. Так как $S_1^{p^e} \subset T$, то, очевидно, каждый элемент из S, алгебраический над T, чисто несепарабелен над T. Алгебра R_L равна $(R_T)_L$, поэтому можно считать, что она содержится в S_L (S и L рассматриваются как алгебры над T). Так как поле L имеет конечную степень над T, то, следовательно, лемму 3 достаточно доказать для случая, когда L имеет конечную степень над K.

Итак, пусть L имеет конечную степень над K. Обозначим через L_0 подполе, состоящее из тех элементов поля L, которые сепарабельны над K; тогда $L_0 = K\langle y\rangle$, где $y \in L_0$. Пусть $F(Y)$ — неприводимый многочлен с коэффициентами из K, для которого элемент y является корнем. Если n есть степень многочлена F, то элементы $1, y, \ldots, y^{n-1}$ образуют базис L_0 относительно K, а значит, и базис алгебры $(L_0)_R$ относительно R. Отсюда следует, что алгебра $(L_0)_R$ изоморфна фактор-кольцу $R[Y]/\mathfrak{r}$, где $\mathfrak{r}$ есть идеал, порожденный многочленом $F(Y)$ в кольце $R[Y]$. Пусть $F_1(Y)$ — неприводимый множитель многочлена $F(Y)$ в кольце $R_1[Y]$. Если поле K имеет характеристику $p > 0$, то $F_1^{p^e}(Y) \in K[Y]$; следовательно, $F_1^{p^e}(Y)$ делится на $F(Y)$, и, значит, многочлен F является (с точностью до постоянного множителя) степенью многочлена F_1. Если характеристика поля K равна 0, то $R_1 = K$ и $F_1 = F$ (с точностью до постоянного множителя). Далее, в силу леммы 1 многочлен $F_1(Y)$ неприводим и в кольце $R[Y]$. Пусть $x = G(y)$ — произвольный элемент из $(L_0)_R$ (где G — многочлен с коэффициентами из R). Если G делится на F_1, то элемент x нильпотентен. В противном случае многочлен G взаимно прост с F_1, а значит, взаимно прост также и с F; следовательно, в этом случае существуют такие многочлены U и V с коэффициентами из R, что $GU + FV = 1$, откуда $xU(y) = 1$. Таким образом, каждый элемент из $(L_0)_R$ либо нильпотентен, либо имеет обратный элемент. Если характеристика поля K равна 0, то этим лемма 3 уже доказана. Предположим, что поле K имеет характеристику $p > 0$. Каждый элемент x' из R_L может быть представлен в виде $x' = \sum_{k=1}^{h} u_k v_k$, где $u_k \in L$, $v_k \in R$ $(1 \leqslant k \leqslant h)$. Так как поле L чисто несепарабельно над L_0, то существует такой показатель $c > 0$, что $u_k^{p^c} \in L_0 (1 \leqslant k \leqslant h)$, откуда $x'^{p^c} = \sum_{k=1}^{h} u_k^{p^c} v_k^{p^c} \in (L_0)_R$. Если x' есть делитель нуля, то элемент x'^{p^c} не может иметь обратного элемента; значит, он нильпотентен. Лемма 3, таким образом, доказана.

Лемма 4. Пусть расширение R поля K содержит алгебраический над K элемент y, который не является чисто несепарабельным элементом над K. Тогда существует такое сепарабельное расширение L поля K конечной степени, что алгебра $L \otimes R$ содержит ненильпотентный делитель нуля.

Как известно, некоторая степень z элемента y является сепарабельным элементом над K, но не содержится в K; положим $L = K\langle z\rangle$. Так как $L \subset R$, то отождествление поля L с подполем алгебры $L \otimes R$ в данном случае вызовет путаницу в обозначениях. Поэтому элемент $z \otimes 1$ из $L \otimes R$ мы обозначим через z'. Элемент z является корнем неприводимого многочлена $F(Z)$ с коэффициентами из K. Если n есть степень F, то элементы $1, z', \ldots, z'^{n-1}$ образуют базис алгебры L_R относительно R. Мы имеем

$$0 = F(z) - F(z') = (z - z')\, G(z, z'),$$

где $G(Z, Z')$ — многочлен с коэффициентами из K. Так как степень G относительно Z' равна $n-1$, то $G(z, z') \neq 0$, и, значит, элемент $z - z'$ является делителем нуля. С другой стороны, элемент z является простым корнем многочлена $F(Z)$, степень которого > 1. Поэтому никакая степень двучлена $Z - z$ не делится в кольце $R[Z]$ на $F(Z)$, а это означает, что элемент $z' - z$ не нильпотентен.

§ 3. Коммутативные алгебры

Пусть $\mathfrak{A}$ — коммутативная алгебра над полем K. Обозначим через $\mathfrak{n}$ множество всех нильпотентных элементов алгебры $\mathfrak{A}$. Утверждаем, что $\mathfrak{n}$ *есть идеал алгебры* $\mathfrak{A}$. Действительно, если $x \in \mathfrak{n}$, $a \in K$, $z \in \mathfrak{A}$, то, очевидно, имеем $ax \in \mathfrak{n}$, $zx \in \mathfrak{n}$. Далее, пусть x и y — элементы из $\mathfrak{n}$; тогда $x^a = 0$ и $y^b = 0$ при некоторых показателях a и b. Применяя к степени $(x-y)^{a+b}$ биномиальную формулу (которая справедлива для элементов любого коммутативного кольца), мы видим, что каждый член разложения содержит либо x с показателем $\geqslant a$, либо y с показателем $\geqslant b$; следовательно, $(x-y)^{a+b} = 0$, т. е. $x - y \in \mathfrak{n}$. Этим доказано, что $\mathfrak{n}$ есть идеал. Идеал $\mathfrak{n}$ называется *радикалом* алгебры $\mathfrak{A}$.

Так как радикал $\mathfrak{n}$ алгебры $\mathfrak{A}$ является идеалом в $\mathfrak{A}$, то мы можем построить фактор-алгебру $\mathfrak{A}/\mathfrak{n}$.

Лемма 1. *Радикал фактор-алгебры* $\mathfrak{A}/\mathfrak{n}$ *алгебры* $\mathfrak{A}$ *по ее радикалу* $\mathfrak{n}$ *равен* $\{0\}$. *Если каждый делитель нуля алгебры* $\mathfrak{A}$ *нильпотентен, то алгебра* $\mathfrak{A}/\mathfrak{n}$ *не имеет делителей нуля, отличных от* 0.

Пусть x^* и y^* — элементы из $\mathfrak{A}/\mathfrak{n}$, а x и y — элементы из $\mathfrak{A}$, принадлежащие соответственно классам вычетов x^* и y^* по модулю $\mathfrak{n}$. Пусть элемент x^* нильпотентен, т. е. $(x^*)^a = 0$ при некотором показателе a. Так как $x^a \in \mathfrak{n}$, то существует такой показатель a', что $(x^a)^{a'} = 0$, откуда $x \in \mathfrak{n}$ и $x^* = 0$. Предположим теперь, что каждый делитель нуля алгебры $\mathfrak{A}$ нильпотентен. Пусть $x^*y^* = 0$; тогда при некотором показателе m имеем $x^m y^m = 0$. Если $y^m = 0$, то y нильпотентен, т. е. $y^* = 0$. Если $y^m \neq 0$, то элемент x^m является делителем нуля. В силу предположения получаем, что x^m нильпотентен; следовательно, элемент x также нильпотентен, и, значит, $x^* = 0$.

Лемма 2. *Если алгебра* $\mathfrak{A}$ *раскладывается в прямую сумму некоторого числа ее идеалов, скажем* $\mathfrak{A}_1, \ldots, \mathfrak{A}_h$, *то всякое произведение элемента из* $\mathfrak{A}_i$ *на элемент из* $\mathfrak{A}_j$ *при* $i \neq j$ *равно* 0, *и радикал алгебры* $\mathfrak{A}$ *является прямой суммой радикалов подалгебр* $\mathfrak{A}_1, \ldots, \mathfrak{A}_h$.

Произведение элемента из $\mathfrak{A}_i$ на элемент из $\mathfrak{A}_j$ принадлежит обоим идеалам $\mathfrak{A}_i$ и $\mathfrak{A}_j$, поэтому при $i \neq j$ это произведение равно 0. Отсюда следует, что если x_i и y_i — элементы из $\mathfrak{A}_i$ $(1 \leqslant i \leqslant h)$, то $\left(\sum_{i=1}^{h} x_i\right)\left(\sum_{i=1}^{h} y_i\right) = \sum_{i=1}^{h} x_i y_i$. В частности, для любого показателя $a > 0$ имеем $\left(\sum_{i=1}^{h} x_i\right)^a = \sum_{i=1}^{h} x_i^a$. Таким образом, элемент $\sum_{i=1}^{h} x_i$ нильпотентен тогда и только тогда, если все элементы x_i нильпотентны.

Замечание. Формула $\left(\sum_{i=1}^{h} x_i\right)\left(\sum_{i=1}^{h} y_i\right) = \sum_{i=1}^{h} x_i y_i$ означает, что при предположениях леммы 2 алгебра $\mathfrak{A}$ изоморфна прямой сумме алгебр $\mathfrak{A}_1, \ldots, \mathfrak{A}_h$.

Обратимся теперь к рассмотрению тех коммутативных алгебр, которые имеют конечную размерность над основным полем.

Конечномерная алгебра называется *полупростой*, если ее радикал равен $\{0\}$. Для любой конечномерной алгебры $\mathfrak{A}$ фактор-алгебра $\mathfrak{A}/\mathfrak{n}$, очевидно, полупроста.

Идеал $\mathfrak{a}$ алгебры $\mathfrak{A}$ называется *минимальным*, если он отличен от $\{0\}$ и не содержит никаких идеалов алгебры $\mathfrak{A}$, кроме самого себя и нулевого идеала $\{0\}$.

Лемма 3. *Каждая коммутативная конечномерная полупростая алгебра есть прямая сумма своих минимальных идеалов, а сами эти минимальные идеалы являются полями.*

Пусть алгебра $\mathfrak{A}$ имеет конечную размерность над полем K. Среди всех идеалов алгебры $\mathfrak{A}$, отличных от $\{0\}$, выберем идеал наименьшей размерности (над K). Этот идеал, очевидно, будет минимальным. Таким образом, если $\mathfrak{A} \neq \{0\}$, то в $\mathfrak{A}$ имеется по крайней мере один минимальный идеал. Предположим теперь, что алгебра $\mathfrak{A}$ полупроста, и пусть $\mathfrak{a}$ — ее минимальный идеал. Если элемент $x \neq 0$ принадлежит $\mathfrak{a}$, то множество $\mathfrak{a}x$ всех произведений yx, $y \in \mathfrak{a}$ является, очевидно, идеалом, содержащимся в $\mathfrak{a}$; так как $x^2 \neq 0$ (иначе элемент x был бы нильпотентным), то этот идеал отличен от $\{0\}$, а следовательно, $\mathfrak{a}x = \mathfrak{a}$. Так как последнее равенство справедливо для каждого $x \neq 0$ из $\mathfrak{a}$, то $\mathfrak{a}$ есть поле. Пусть $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ — различные минимальные идеалы алгебры $\mathfrak{A}$. Утверждаем, что сумма $\mathfrak{a}_1 + \ldots + \mathfrak{a}_h$ прямая. Действительно, еcле $i \neq j$, то идеал $\mathfrak{a}_i \cap \mathfrak{a}_j$, содержащийся в $\mathfrak{a}_i$, равен либо $\{0\}$ либо $\mathfrak{a}_i$; равенство $\mathfrak{a}_i \cap \mathfrak{a}_j = \mathfrak{a}_i$ невозможно, так как включение $\mathfrak{a}_i \subset \mathfrak{a}_j$, $\mathfrak{a}_i \neq \mathfrak{a}_j$, противоречит минимальности $\mathfrak{a}_j$; таким образом, $\mathfrak{a}_i \cap \mathfrak{a}_j = \{0\}$. Отсюда следует, что если $x_i \in \mathfrak{a}_i$ и $x_j \in \mathfrak{a}_j$, то $x_i x_j = 0$. Предположим теперь, что $\sum_{i=1}^{h} x_i = 0$, где $x_i \in \mathfrak{a}_i$ $(1 \leqslant i \leqslant h)$; умножая это равенство на x_i, получим $x_i^2 = 0$, откуда $x_i = 0$. Этим и доказано, что сумма $\mathfrak{a}_1 + \ldots + \mathfrak{a}_h$ прямая. Так как каждый идеал $\mathfrak{a}_i$ имеет размерность $\geqslant 1$, то h не может быть больше размерности алгебры $\mathfrak{A}$. Таким образом, алгебра $\mathfrak{A}$ имеет лишь конечное число минимальных идеалов. Пусть $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ — все минимальные идеалы алгебры $\mathfrak{A}$. Каждый идеал $\mathfrak{a}_i$, являясь полем, содержит единичный элемент e_i; положим $e = \sum_{i=1}^{h} e_i$. Пусть $\mathfrak{a}'$ есть множество тех элементов $x \in \mathfrak{A}$,

для которых $xe=0$. Очевидно, что $\mathfrak{a}'$ идеал алгебры $\mathfrak{A}$. Если бы $\mathfrak{a}'\neq\{0\}$, то среди всех идеалов алгебры $\mathfrak{A}$, содержащихся в $\mathfrak{a}'$ мы могли бы выбрать идеал наименьшей размерности. Этот идеал, будучи минимальным, совпадал бы с одним из идеалов $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$. Но это невозможно, ибо из равенства $e_ie_j=0$ при $i\neq j$ следует, что $e_ie=e_i^2=e_i\neq 0$. Таким образом, $\mathfrak{a}'=\{0\}$. Для произвольного элемента x из $\mathfrak{A}$ мы имеем $x=xe+$ $+(x-xe)$. Из равенства $e^2=\left(\sum_{i=1}^{h} e_i\right)e=e$ следует, что $(x-xe)e=0$, а значит, $x-xe=0$. Так как $x=xe=$ $=\sum_{i=1}^{h} xe_i\in\mathfrak{a}_1+\ldots+\mathfrak{a}_h$, то $\mathfrak{A}=\mathfrak{a}_1+\ldots+\mathfrak{a}_h$, и лемма 3 доказана.

Лемма 4. *Пусть* $\mathfrak{n}$ — *радикал коммутативной алгебры* $\mathfrak{A}$ *конечной размерности над полем* K. *Представим фактор-алгебру* $\mathfrak{A}/\mathfrak{n}$ *в виде прямой суммы полей* $Z_1, \ldots, Z_h$, *являющихся минимальными идеалами в* $\mathfrak{A}/\mathfrak{n}$. *Тогда для каждого* $i(1\leqslant i\leqslant h)$ *существует гомоморфизм* φ_i *алгебры* $\mathfrak{A}$ *на* Z_i. *Обратно, если* φ *есть произвольный гомоморфизм алгебры* $\mathfrak{A}$ *в некоторое поле* Z (*содержащее поле* K *в качестве подполя*) *и если* $\varphi(\mathfrak{A})\neq\{0\}$, *то существует и притом только один такой индекс* i, *что гомоморфизм* φ *может быть представлен в виде* $\psi\varphi_i$, *где* ψ — *изоморфизм поля* Z_i *в поле* Z.

Замечание. Рассматриваемые здесь гомоморфизмы являются гомоморфизмами алгебр (а не только колец), т. е. если θ — любой из этих гомоморфизмов, то $\theta(ax)=a\theta(x)$ при $a\in K$.

Пусть x — произвольный элемент алгебры $\mathfrak{A}$. Обозначим через x^* класс вычетов элемента x по модулю $\mathfrak{n}$; тогда $x^*=\sum_{i=1}^{h} z_i$, где $z_i\in Z_i(1\leqslant i\leqslant h)$. Если мы каждому $x\in\mathfrak{A}$ сопоставим элемент z_i, то получим, очевидно, гомоморфизм φ_i алгебры $\mathfrak{A}$ на Z_i. Обратно, пусть φ — произвольный гомоморфизм алгебры $\mathfrak{A}$ в поле Z, содержащее K. Если $u\in\mathfrak{n}$, то $(\varphi(u))^m=0$ при некотором показателе $m>0$, а значит и $\varphi(u)=0$, ибо Z есть поле. Так как гомоморфизм φ отображает $\mathfrak{n}$ на $\{0\}$, то он естественным образом порождает

гомоморфизм φ^* алгебры $\mathfrak{A}/\mathfrak{n}$ в Z. Если $\varphi(\mathfrak{A}) \neq \{0\}$, то существует индекс i и такой элемент $z_i \in Z_i$, что $\varphi^*(z_i) \neq 0$. Пусть $z_j \in Z_j$, $j \neq i$, тогда $z_i z_j = 0$, откуда $\varphi^*(z_j) = 0$ (так как Z—поле). С другой стороны, ограничение гомоморфизма φ^* на Z_i является гомоморфизмом Z_i в Z, а значит, изоморфизмом Z_i в Z (ибо Z_i — поле). Лемма 4, таким образом, доказана.

Лемма 5. *Пусть L и M — два расширения поля K, причем M имеет конечную степень над K. Рассматривая M как алгебру над полем K, построим алгебру M_L над L, получающуюся из M расширением основного поля K до поля L. Предположим, что фактор-алгебра алгебры M_L по ее радикалу $\mathfrak{n}$ представляется в виде суммы h минимальных идеалов. Тогда существует подполе L' поля L, имеющее конечную степень и сепарабельное над K, такое, что уже алгебра $M_{L'}$ является суммой h минимальных идеалов.*

Обозначим через L_0 множество тех элементов поля L, которые алгебраичны и сепарабельны над K. В силу леммы 1 § 1 алгебра M_{L_0} полупроста. Пусть $T_1, \ldots, T_{h_0}$ — различные минимальные идеалы алгебры M_{L_0}. Так как M_{L_0} есть прямая сумма идеалов $T_1, \ldots, T_{h_0}$, то алгебра $M_L = (M_{L_0})_L$ является прямой суммой содержащихся в ней алгебр $(T_1)_L, \ldots, (T_{h_0})_L$. Каждый алгебраический над L_0 элемент из L чисто несепарабелен над L_0; поэтому алгебра $(T_i)_L$ имеет только нильпотентные делители нуля (лемма 3 § 2). Следовательно, фактор-алгебра алгебры $(T_i)_L$ по ее радикалу $\mathfrak{n}_i$ не имеет делителей нуля (лемма 1). В силу леммы 3 эта фактор-алгебра есть поле Z_i. Применяя лемму 2, получаем, что $\mathfrak{n} = \mathfrak{n}_1 + \ldots + \mathfrak{n}_{h_0}$, а следовательно, $M_L/\mathfrak{n}$ есть прямая сумма полей $Z_1, \ldots, Z_{h_0}$, которые будут, очевидно, идеалами в этой фактор-алгебре. Отсюда следует, что $h = h_0$. Пусть e_i — единица поля T_i. Очевидно, что тогда существует подполе L' поля L_0, получающееся из K присоединением конечного числа элементов и такое, что элементы e_i $(1 \leqslant i \leqslant h)$ принадлежат уже алгебре $M \otimes L'$. Главный идеал, порожденный элементом e_i в $M_{L'}$, содержится в T_i, а поэтому не имеет делителей нуля, отличных от 0. Из леммы 3 вытекает, что этот идеал есть поле T_i'. Так как $e_i e_j = 0$ при $i \neq j$, то поля $T_1', \ldots, T_h'$ различны. Элемент $\sum_{i=1}^{h} e_i$ является единицей

в $M_{L'}$, поэтому для каждого $x \in M_{L'}$ имеем $x = \sum_{i=1}^{h} xe_i \in \in T'_1 + \ldots + T'_h$, т. е. $M_{L'}$ является суммой h минимальных идеалов.

§ 4. Расширение поля констант

Пусть R — поле алгебраических функций от одной переменной, K — его поле констант и L — произвольное расширение поля K. Паре (R, L) мы сейчас сопоставим некоторое поле S алгебраических функций от одной переменной над полем L. Для этого мы сначала построим алгебру R_L, получающуюся из поля R (рассматриваемого как алгебра над K) расширением основного поля K до L. Обозначим через $\mathfrak{S}$ фактор-кольцо алгебры R_L по ее радикалу $\mathfrak{n}$. Так как K относительно алгебраически замкнуто в R, то $\mathfrak{S}$ не имеет делителей нуля, отличных от 0 (лемма 3 § 2 и лемма 1 § 3). Пусть S есть поле отношений кольца $\mathfrak{S}$. Поле R можно рассматривать как подалгебру алгебры $R \otimes L$. При естественном гомоморфизме алгебры R_L на $\mathfrak{S} = R_L/\mathfrak{n}$ поле R отображается изоморфно на подполе R^* кольца $\mathfrak{S}$. Ясно, что каждый элемент из $\mathfrak{S}$ может быть записан в виде линейной комбинации элементов поля R^* с коэффициентами из L; следовательно, $S = R^*\langle L\rangle$. Пусть x — элемент из R, не принадлежащий K, и пусть x^* — его класс вычетов по модулю $\mathfrak{n}$. Тогда R^* имеет конечную степень над $K\langle x^*\rangle$, откуда следует, что S имеет конечную степень над $L\langle x^*\rangle$. Утверждаем, что элемент x^* трансцендентен над L. Действительно, если бы это было не так, то существовал бы такой многочлен $F \neq 0$ с коэффициентами из L, что $F(x^*) = 0$. Но тогда при некотором показателе $m > 0$ мы имели бы $(F(x))^m = F^m(x) = 0$. Это, однако, невозможно, ибо элементы $1, x, \ldots, x^k, \ldots$ линейно независимы над K в поле R, а значит, линейно независимы также и над L в алгебре R_L. Таким образом, мы доказали, что S есть поле алгебраических функций над полем L.

В дальнейшем поле R мы будем отождествлять с подполем R^* поля S. В силу этого отождествления можно будет писать $S = L\langle R\rangle = R\langle L\rangle$. Будем говорить, что *поле S получено из R расширением поля констант K до поля L.*

Следует заметить, что в случае, когда поля R и L являются подполями некоторого общего поля Ω, обозначение $R\langle L\rangle$ имеет двоякий смысл, ибо в этом случае $R\langle L\rangle$ обозначает также подполе S_1 поля Ω, порожденное полями R и L. Однако мы докажем, что если S_1 не алгебраично над L, то существует изоморфное отображение S на S_1, при котором каждый элемент из R и каждый элемент из L отображаются на себя. Точнее, мы докажем следующий результат.

Лемма 1. *Пусть R — поле алгебраических функций от одной переменной, K — его поле констант и L — произвольное расширение поля K. Предположим, что нам задано некоторое поле Ω, содержащее K в качестве подполя, и заданы изоморфизмы ρ поля R в Ω и λ поля L в Ω, при которых каждый элемент из K отображается на себя. Обозначим через S_1 подполе поля Ω, порожденное полями $\rho(R)$ и $\lambda(L)$. Тогда если поле S_1 не алгебраично* над $\lambda(L)$, *то существует изоморфное отображение σ поля $R\langle L\rangle$ на S_1, которое совпадает с ρ на R и с λ на L.*

В силу леммы 1 § 4 гл. IV, существует гомоморфизм φ алгебры $R\otimes L$ в S_1, совпадающий с ρ на R и с λ на L. Так как поле S_1 не имеет делителей нуля, отличных от 0, то гомоморфизм φ отображает радикал $\mathfrak{n}$ алгебры $R\otimes L$ на $\{0\}$, поэтому φ естественным образом порождает гомоморфизм φ^* кольца $\mathfrak{S}=(R\otimes L)/\mathfrak{n}$ в S_1; в силу нашего отождествления поля R с подкольцом кольца $R_L/\mathfrak{n}$ можно считать, что φ^* совпадает с ρ на R и с λ на L. Покажем, что φ^* на самом деле есть изоморфизм. Положим $R_1=\rho(R)$ и $L_1=\lambda(L)$. Пусть x — элемент из R, не принадлежащий K; тогда поле R_1 алгебраично над $K\langle x_1\rangle$, где $x_1=\rho(x)$, а поле S_1 алгебраично над $L_1\langle x_1\rangle$. Так как по условию поле S_1 не алгебраично над L_1, то элемент x_1 трансцендентен над L_1. Пусть y — элемент из $\mathfrak{S}$, отличный от 0; тогда y удовлетворяет уравнению вида $\sum_{i=0}^{n} F_i(x)\,y^{n-i}=0$, где $F_i\,(0\leqslant i\leqslant n)$ — многочлены с коэффициентами из L, причем $F_n\neq 0$. Обозначим через G_i многочлен, который получается из многочлена F_i применением ко всем его коэффициентам отображения λ. Если $y_1=\varphi^*(y)$, то $\sum_{i=0}^{n} G_i(x_1)\,y_1^{n-1}=0$. Так как $G_n\neq 0$ и элемент x_1 трансцендентен над L_1, то

$G_n(x_1) \neq 0$, а значит, $y_1 \neq 0$. Этим доказано, что φ^* — изоморфизм. Изоморфизм φ^*, как известно, можно продолжить до изоморфизма σ поля отношений $R\langle L\rangle$ кольца $\mathfrak{S}$ в S_1. Образ поля $R\langle L\rangle$ при изоморфизме σ является полем и содержит поля R_1 и L_1, поэтому этот образ совпадает с S_1. Лемма 1, таким образом, доказана.

Следствие 1. *Пусть R — поле алгебраических функций от одной переменной и L — расширение поля констант K поля R. Тогда каждый автоморфизм поля L над K может быть продолжен, и притом единственным образом, до автоморфизма поля $R\langle L\rangle$ над R.*

Это вытекает непосредственно из леммы 1.

Следствие 2. *Пусть R — поле алгебраических функций от одной переменной, K — его поле констант и $L = K\langle B\rangle$ — чисто трансцендентное расширение поля K, причем элементы из B алгебраически независимы над K. Тогда $R\langle L\rangle = R\langle B\rangle$, и элементы из B алгебраически независимы над R.*

Мы можем построить расширение Ω поля R вида $R\langle B_1\rangle$, где элементы из B_1 алгебраически независимы над R и находятся во взаимно однозначном соответствии с элементами из B. Так как поле Ω не алгебраично над $K\langle B_1\rangle$, то по лемме 1 существует изоморфное отображение поля $R\langle L\rangle$ на Ω, при котором B отображается на B_1.

Лемма 2. *Если R — сепарабельно порождаемое поле алгебраических функций от одной переменной, а L — произвольное расширение его поля констант K, то поле $R\langle L\rangle$ также сепарабельно порождаемо.*

В поле R существует такой элемент x, что R алгебраично и сепарабельно над $K\langle x\rangle$, т. е. $R = K\langle x, y\rangle$, где y — сепарабельный элемент над $K\langle x\rangle$. Имеем теперь $R\langle L\rangle = L\langle x, y\rangle$, причем элемент y, очевидно, алгебраичен и сепарабелен над $L\langle x\rangle$.

Теорема 1. *Пусть R — поле алгебраических функций от одной переменной, а L — расширение поля констант K поля R. Предположим, что по крайней мере одно из полей L или R сепарабельно над K. Тогда всякие элементы поля R, линейно независимые над K, линейно независимы также и над полем L (в поле $R\langle L\rangle$), и всякие элементы поля L, линейно независимые над K, линейно независимы в поле $R\langle L\rangle$ и над R.*

Из нашего предположения вытекает, что алгебра $R \otimes L$ не имеет нильпотентных элементов, отличных от 0 (следствие 2 к лемме 5 § 1). Поэтому $R\langle L\rangle$ есть поле отношений кольца $R \otimes L$; теорема 1 следует теперь непосредственно из определения кронекеровского произведения.

Следствие 1. *Сохраняя условия теоремы 1, предположим, что поле L алгебраично над K. Тогда всякий базис поля L над K является также базисом поля $R\langle L\rangle$ над R. Далее, если L имеет конечную степень над K, то $[R\langle L\rangle : R] = [L : K]$ и для любого элемента $a \in L$ имеем* $\mathrm{Sp}_{R\langle L\rangle/R}\, a = \mathrm{Sp}_{L/K} a$, $\mathrm{N}_{R\langle L\rangle/R} a = \mathrm{N}_{L/K} a$.

В силу теоремы 1 элементы любого базиса поля L относительно K линейно независимы также и над полем R. Далее, каждый элемент y из $R\langle L\rangle$ принадлежит полю вида $R\langle L'\rangle$, где L' получено из K присоединением конечного числа элементов поля L. Так как L алгебраично над K, то L' имеет конечную степень над K. Из леммы 2 § 1 гл. IV следует, что элемент y может быть представлен в виде линейной комбинации элементов поля L' (а значит, и поля L) с коэффициентами из R. Отсюда следует, что всякий базис поля L над K является также базисом поля $R\langle L\rangle$ над R. Остальные утвержения следствия 1 очевидны.

Следствие 2. *Сохраняя условия теоремы 1, обозначим через S подполе поля R, которое содержит K и над которым поле R алгебраично. Тогда всякий базис поля R над S является также базисом поля $R\langle L\rangle$ над $S\langle L\rangle$, в частности $[R\langle L\rangle : S\langle L\rangle] = [R : S]$. Если x — произвольный элемент из R, то*

$$\mathrm{Sp}_{R\langle L\rangle/S\langle L\rangle}\, x = \mathrm{Sp}_{R/S} x, \quad \mathrm{N}_{R\langle L\rangle/S\langle L\rangle}\, x = \mathrm{N}_{R/S} x.$$

Если элемент u из поля S не принадлежит K, то поле R имеет конечную степень над $K\langle u\rangle$, значит, тем более, оно имеет конечную степень над S. Пусть $\{y_1, \ldots, y_n\}$ — базис поля R над S. Так как, очевидно, $R\langle L\rangle = (S\langle L\rangle)\langle R\rangle$ и R имеет конечную степень над S, то, в силу леммы 2 § 1 гл. IV, каждый элемент из $R\langle L\rangle$ может быть представлен в виде линейной комбинации элементов $y_1, \ldots, y_n$ с коэффициентами из $S\langle L\rangle$. Докажем, что элементы $y_1, \ldots, y_n$ линейно независимы над $S\langle L\rangle$. Допустим, что $\sum_{i=1}^{n} u_i y_i = 0$, где $u_i \in S\langle L\rangle$ $(1 \leqslant i \leqslant n)$.

Так как S есть подполе поля R, то по крайней мере одно из полей S или L сепарабельно над K (лемма 3 § 1), поэтому поле $S\langle L\rangle$ является полем отношений кольца $S\otimes L$ (см. доказательство теоремы 1). Отсюда следует, что в поле $S\langle L\rangle$ существует такой элемент $v\neq 0$, что $vu_i\in S\otimes L$ $(1\leqslant i\leqslant n)$. Пусть $\{s_j\}_{j\in J}$ есть базис поля S относительно K (J — некоторое бесконечное множество индексов). Элементы y_is_j $(1\leqslant i\leqslant n,\ j\in J)$ из поля R линейно независимы над K; действительно, если $\sum\limits_{i=1}^{n}\sum\limits_{j\in J}a_{ij}y_is_j=0$, $a_{ij}\in K$, то $\sum\limits_{i=1}^{n}\left(\sum\limits_{j\in J}a_{ij}s_j\right)y_i=0$, откуда $\sum\limits_{j\in J}a_{ij}s_j=0$ при всех i (ибо $y_1,\ldots,y_n$ линейно независимы над S) и, далее, $a_{ij}=0$ при всех i и j. Элементы y_is_j линейно независимы, следовательно, и над L в алгебре $R\otimes L$. С другой стороны, мы имеем $u_iv=\sum\limits_{j\in J}b_{ij}s_j$, где $b_{ij}\in L$ $(1\leqslant i\leqslant n,\ j\in J)$, откуда $\sum\limits_{i=1}^{n}\sum\limits_{j\in J}b_{ij}y_is_j=0$; следовательно, $b_{ij}=0$ при всех i и j, т. е. $vu_i=0$ и $u_i=0$ $(1\leqslant i\leqslant n)$. Этим и доказано, что всякий базис поля R над S является также базисом поля $R\langle L\rangle$ над $S\langle L\rangle$. Остальные утверждения следствия 2 очевидны.

Пусть R — поле алгебраических функций от одной переменной, а L — произвольное расширение его поля констант K. Тогда поле $S=R\langle L\rangle$ есть поле алгебраических функций над L; однако поле констант поля S не всегда равно L. Возьмем, например, поле $K=P\langle a, b\rangle$, где P — произвольное поле характеристики $p>0$, а элементы a и b алгебраически независимы над P. Пусть $R=K\langle x, y\rangle$, где x — трансцендентный элемент над K, а y удовлетворяет уравнению $y^p=ax^p+b$. Нетрудно показать, что K является полем констант поля R. Положим теперь $L=K\left\langle a^{\frac{1}{p}}\right\rangle$. В поле $R\langle L\rangle$ элемент b является p-ой степенью $\left(\text{ибо } b=\left(y-a^{\frac{1}{p}}x\right)^p\right)$, в то же время он не является p-ой степенью в поле $L=P\left\langle a^{\frac{1}{p}}, b\right\rangle$. Таким образом, поле констант поля $R\langle L\rangle$ не совпадает с L. Однако имеет место следующий результат.

Теорема 2. *Пусть R — поле алгебраических функций от одной переменной и пусть L — произвольное расширение поля констант K поля R. Тогда поле констант поля $R\langle L\rangle$ чисто несепарабельно над L. Если же хоть одно из полей R или L сепарабельно над K, то поле констант поля $R\langle L\rangle$ равно L.*

Пусть c — константа поля $R\langle L\rangle$. Ясно, что существует подполе L' поля L, получающееся из K присоединением конечного числа элементов и такое, что элемент c принадлежит $R\langle L'\rangle$ и алгебраичен над L'. Заметим, что если поле L сепарабельно над K, то поле L' также сепарабельно над K (лемма 3 § 1). Таким образом, теорему 2 достаточно доказать для случая когда L может быть получено из K присоединением конечного числа элементов. Пусть B есть трансцендентный базис поля L над K, при этом будем предполагать, что если L сепарабельно над K, то L сепарабельно также и над $K\langle B\rangle$ (лемма 5 § 1). Построим поле $R_1 = R\langle K\langle B\rangle\rangle$, полученное из R расширением поля констант K до поля $K\langle B\rangle$. Применяя следствие 2 к лемме 1 и лемму 2 § 2, мы видим, что поле констант поля R_1 равно $K\langle B\rangle$. Далее, если R сепарабельно над K, то R_1 сепарабельно над $K\langle B\rangle$ (лемма 2). Ясно, что поле $R\langle L\rangle$ равно полю $R_1\langle L\rangle$, которое получено из поля R_1 расширением его поля констант $K\langle B\rangle$ до поля L. Таким образом, достаточно рассмотреть случай, когда поле L алгебраично и имеет конечную степень над K. В этом случае L является чисто несепарабельным расширением поля $L_0 = K\langle a\rangle$, где a — некоторый сепарабельный элемент над K. Если n есть степень элемента a относительно K, то элементы $1, a, \ldots, a^{n-1}$ образуют базис поля L_0 над K, а в силу следствия 1 к теореме 1 они образуют также и базис поля $R\langle L_0\rangle$ над R. Пусть $c = \sum_{i=0}^{n-1} r_i a^i$ есть константа поля $R\langle L_0\rangle$. Обозначим через $a_1 = a, \ldots, a_n$ элементы, сопряженные с a относительно K (в некотором нормальном расширении L' поля K, содержащем L_0). Для каждого j $(1 \leqslant j \leqslant n)$ существует автоморфизм σ_j поля L' над K, отображающий a на a_j. В силу следствия 1 к лемме 1 автоморфизм σ_j может быть продолжен до автоморфизма (обозначаемого также через σ_j)

поля $R\langle L'\rangle$ над R. Положим $c_j = \sigma_j(c)$; тогда

$$c_j = \sum_{i=0}^{n-1} r_i a_j^i. \tag{1}$$

Так как элемент c алгебраичен над L_0 (а значит, и над K), то все элементы c_j алгебраичны над K. С другой стороны, так как элемент a сепарабелен над K, то определитель системы (1) (которую мы рассматриваем как систему линейных уравнений относительно $r_0, \ldots, r_{n-1}$) отличен от нуля. Но коэффициенты системы (1) и свободные члены алгебраичны над K, поэтому элементы $r_0, \ldots, r_{n-1}$ также алгебраичны над K; следовательно, все они принадлежат K, откуда $c \in L_0$. Таким образом, L_0 является полем констант поля $R\langle L_0\rangle$. Так как L чисто несепарабельно над L_0, то и $R\langle L\rangle$ чисто несепарабельно над $R\langle L_0\rangle$. Если c' есть константа поля $R\langle L\rangle$, то существует такой показатель $e > 0$, что $c'^{p^e} \in R\langle L_0\rangle$, где p — характеристика поля K (мы считаем, что $p > 0$). Так как элемент c'^{p^e} алгебраичен над L_0, то он принадлежит L_0. Отсюда следует, что элемент c' чисто несепарабелен над L. Если поле R сепарабельно над K, то $R\langle L\rangle$ сепарабельно над L (лемма 2). В силу леммы 3 § 1 поле констант поля $R\langle L\rangle$ также сепарабельно над L. Следовательно, это поле констант, будучи одновременно сепарабельным и чисто несепарабельным над L, совпадает с L. Теорема 2, таким образом, доказана.

Следствие. *Пусть R — поле алгебраических функций от одной переменной и L — некоторое расширение поля констант K поля R. Если по крайней мере одно из полей R или L сепарабельно над K, то для любого дивизора $\mathfrak{a}$ поля R имеем*

$$d(\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{a}) = d(\mathfrak{a}).$$

Достаточно указанное равенство доказать для случая, когда $\mathfrak{a}$ есть точка $\mathfrak{p}$. В поле R выберем элемент x, для которого точка $\mathfrak{p}$ является единственным нулем (лемма 1 § 1 гл. IV). Если $\mathfrak{p}^h$ есть дивизор нулей элемента x в поле R, то $hd(\mathfrak{p}) = [R : K\langle x\rangle]$ (теорема 4 § 8 гл. 1). Дивизор нулей элемента x в поле $R\langle L\rangle$ равен $(\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{p})^h$, откуда $hd(\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{p}) = [R\langle L\rangle : L\langle x\rangle]$ (ибо L есть поле

констант поля $R\langle L\rangle$). В силу следствия 2 к теореме 1 последнее число равно $[R:K\langle x\rangle]$, и наше утверждение доказано.

§ 5. Поведение точек при расширении поля констант

Пусть R — поле алгебраических функций от одной переменной и пусть L — произвольное расширение его поля констант. В этом параграфе мы займемся изучением точек поля $R\langle L\rangle$, лежащих над заданной точкой поля R.

Теорема 3. *Пусть $\mathfrak{p}$ есть точка поля R алгебраических функций от одной переменной, а L — расширение поля констант K поля R. Обозначим через Σ поле вычетов точки $\mathfrak{p}$ и рассмотрим алгебру Σ_L, полученную из поля Σ (которое мы рассматриваем как алгебру над K) расширением основного поля до поля L. Пусть $\mathfrak{n}$ — радикал алгебры Σ_L, а $Z_1, \ldots, Z_h$ — все различные минимальные идеалы фактор-алгебры $\Sigma_L/\mathfrak{n}$. Точки $\mathfrak{P}_i$ поля $R\langle L\rangle$, лежащие над $\mathfrak{p}$, находятся во взаимно однозначном соответствии с полями Z_i. Если поле Z_i соответствует точке $\mathfrak{P}_i$, то существует изоморфизм φ_i поля Z_i на подполе поля вычетов Σ_i точки $\mathfrak{P}_i$, при этом поле Σ_i чисто несепарабельно над $\varphi_i(Z_i)$. Для элемента $\xi\in\Sigma$ через ξ^* обозначим класс вычетов элемента ξ по модулю $\mathfrak{n}$; положим $\xi^*=\sum_{i=1}^{h}\zeta_i$, где $\zeta_i\in Z_i$ $(1\leqslant i\leqslant h)$. Тогда $\varphi_i(\zeta_i)$ является образом элемента ξ при естественном изоморфизме поля Σ в Σ_i. Если алгебра Σ_L полупроста, то $\varphi_i(Z_i)=\Sigma_i$ и каждая точка $\mathfrak{P}_i$ неразветвлена относительно R; кроме того, в этом случае алгебра $R\otimes L$ не имеет делителей нуля, отличных от* 0.

Обозначим через $\mathfrak{o}$ кольцо точки $\mathfrak{p}$, а через $\mathfrak{O}$ — подкольцо $\mathfrak{o}\otimes L$ алгебры $R\otimes L$. Каждому элементу $\sum_{i=1}^{r}x_ia_i$ $(x_i\in\mathfrak{o},\ a_i\in L)$ из $\mathfrak{O}$ поставим в соответствие элемент $\sum_{i=1}^{r}\xi_ia_i$ из Σ_L, где ξ_i — класс вычетов элемента x_i по модулю $\mathfrak{p}$. Этим определен, очевидно, гомоморфизм ψ кольца $\mathfrak{O}$ на Σ_L. Для каждого i $(1\leqslant i\leqslant h)$ существует гомоморфизм θ_i алгебры Σ_L на Z_i (лемма 4 § 3); гомоморфизм $\theta_i\psi$ отображает

кольцо $\mathfrak{O}$ на Z_i. Пусть $\mathfrak{N}$ есть радикал алгебры $R \otimes L$; тогда, как известно, поле $R\langle L\rangle$ есть поле отношений фактор-кольца $(R \otimes L)/\mathfrak{N}$. Образом кольца $\mathfrak{O}$ при естественном гомоморфизме алгебры $R \otimes L$ на $(R \otimes L)/\mathfrak{N}$ является подкольцо $\mathfrak{O}'$ поля $R\langle L\rangle$, порожденное кольцом $\mathfrak{o}$ и полем L; с другой стороны, ясно, что $\mathfrak{O}' = \mathfrak{O}/(\mathfrak{O} \cap \mathfrak{N})$. Каждый элемент из $\mathfrak{O} \cap \mathfrak{N}$, являясь нильпотентным, гомоморфизмом $\theta_i\psi$ отображается на 0 (ибо Z_i — поле). Отсюда следует, что $\theta_i\psi$ естественным образом определяет гомоморфизм χ_i кольца $\mathfrak{O}'$ на Z_i. Обозначим через $\mathfrak{Q}_i$ ядро этого гомоморфизма; так как Z_i — поле, то $\mathfrak{Q}_i$ — простой идеал. В силу теоремы 1 § 4 гл. 1 в поле $R\langle L\rangle$ существует точка $\mathfrak{P}_i$, такая, что $\mathfrak{P}_i \cap \mathfrak{O}' \supset \mathfrak{Q}_i$. Очевидно, что каждая линейная комбинация элементов из $\mathfrak{p}$ с коэффициентами из L гомоморфизмом χ_i отображается на 0; следовательно, $\mathfrak{p} \subset \mathfrak{Q}_i \subset \mathfrak{P}_i$, т. е. точка $\mathfrak{P}_i$ лежит над $\mathfrak{p}$. Так как Z_i есть поле, то $\mathfrak{Q}_i$ — максимальный идеал в кольце $\mathfrak{O}'$, откуда $\mathfrak{Q}_i = \mathfrak{O}' \cap \mathfrak{P}_i$. Отсюда следует, что фактор-кольцо $\mathfrak{O}'/\mathfrak{Q}_i$ естественным образом изоморфно некоторому подкольцу поля вычетов Σ_i точки $\mathfrak{P}_i$; но $\mathfrak{O}'/\mathfrak{Q}_i$ изоморфно полю Z_i, поэтому мы получаем изоморфизм φ_i поля Z_i на некоторое подполе поля Σ_i. Пользуясь обозначениями теоремы 3, в поле R выберем элемент u, который в точке $\mathfrak{p}$ принимает значение ξ. Тогда элемент $u \cdot 1$ из $\mathfrak{o} \otimes L$ гомоморфизмом $\theta_i\psi$ отображается на ζ_i; следовательно, $\varphi_i(\zeta_i)$ является классом вычетов элемента u по модулю $\mathfrak{P}_i$, т. е. является образом элемента ξ при естественном изоморфизме поля Σ в Σ_i. Теперь мы должны доказать, что полем Z_i точка $\mathfrak{P}_i$ определена однозначно и что Σ_i чисто несепарабельно над $\varphi_i(Z_i)$. Однако сначала мы рассмотрим случай, когда алгебра Σ_L полупроста.

Пусть x есть элемент поля R, для которого точка $\mathfrak{p}$ является его единственным нулем (лемма 1 § 1 гл. IV). Тогда $[R : K\langle x\rangle] = \nu_{\mathfrak{p}}(x)[\Sigma : K]$ (теорема 4 § 8 гл. I). Так как алгебра Σ_L полупроста, то

$$[\Sigma : K] = [\Sigma_L : L] = \sum_{i=1}^{h} [Z_i : L]$$

(лемма 3 § 3). С другой стороны, так как R имеет конечную степень над $K\langle x\rangle$, то, в силу леммы 2 § 1 гл. IV, имеем $[R : K\langle x\rangle] \geqslant [R\langle L\rangle : L\langle x\rangle]$. Степень $[R\langle L\rangle : L\langle x\rangle]$ мы можем представить в виде $[R\langle L\rangle : M\langle x\rangle][M\langle x\rangle : L\langle x\rangle]$, где M —

поле констант поля $R\langle L\rangle$. В силу леммы 3 § 1 гл. IV, $[M\langle x\rangle : L\langle x\rangle] = [M : L]$. Пусть, далее, $\mathfrak{P}_1, \ldots, \mathfrak{P}_{h'}$ — все точки поля $R\langle L\rangle$, лежащие над $\mathfrak{p}$ (где $h' \geqslant h$), и пусть e_j — индекс разветвления точки $\mathfrak{P}_j$ относительно R. Тогда по теореме 4 § 8 гл. I будем иметь $[R\langle L\rangle : M\langle x\rangle] = \nu_{\mathfrak{p}}(x)\sum_{j=1}^{h'} e_j[\Sigma_j : M]$, откуда $\sum_{i=1}^{h}[Z_i : L] \geqslant \sum_{j=1}^{h'} e_j[\Sigma_j : L]$. Если $j \leqslant h$, то $[\Sigma_j : L] = [Z_j : \varphi_j(Z_j)][Z_j : L]$. Из только что полученного неравенства следует теперь, что $h' = h$, $e_j = 1$ $(1 \leqslant j \leqslant h)$ и $\Sigma_j = \varphi_j(Z_j)$ $(1 \leqslant j \leqslant h)$. Пусть $\sum_{k=1}^{r} v_k a_k$ есть нильпотентный элемент из $R \otimes L$ $(v_k \in R,\ a_k \in L)$, при этом будем считать, что элементы a_k линейно независимы над K. Если не все элементы v_k равны 0, то в поле R мы можем найти такой элемент w, что все элементы wv_k принадлежат $\mathfrak{o}$, но хоть один из них не принадлежит $\mathfrak{p}$. При гомоморфизме $\theta_i\psi$ элемент $\sum_{k=1}^{r} wv_k a_k$, принадлежащий кольцу $\mathfrak{O}$, отобразится на нильпотентный элемент алгебры Σ_L, т. е. на 0. С другой стороны, очевидно, что ядро гомоморфизма $\theta_i\psi$ состоит из всех линейных комбинаций элементов из $\mathfrak{p}$ с коэффициентами из L. Дополним элементы a_k до некоторого базиса поля L над K. Тогда элемент $\sum_{k=1}^{r} wv_k a_k$ можно будет записать в виде $\sum_{k=1}^{r'} z_k a_k$, где $z_k \in \mathfrak{p}$, $a_k \in L$ $(1 \leqslant k \leqslant r')$ и $a_1, \ldots, a_{r'}$ линейно независимы над K. Но отсюда будет следовать, что $wv_k = z_k$ $(1 \leqslant k \leqslant r)$, а это невозможно, ибо хоть один из элементов wv_k не принадлежит $\mathfrak{p}$. Этим доказано, что если алгебра Σ_L полупроста, то алгебра $R \otimes L$ не имеет нильпотентных элементов, отличных от 0. Используя лемму 3 § 2, заключаем, что алгебра $R \otimes L$ не имеет делителей нуля, отличных от 0.

Вернемся теперь к общему случаю. Пусть T есть чисто трансцендентное расширение поля K (содержащееся в L), над которым поле L алгебраично. Обозначим через L' подполе сепарабельных над T элементов из L. Так как L' сепарабельно над T, а T сепарабельно над K (лемма 4 § 1), то L' сепарабельно также и над K (лемма 3 § 1). С другой стороны, так как L чисто несепарабельно над L', то $R\langle L\rangle$

чисто несепарабельно над $R\langle L'\rangle$. Докажем теперь следующую лемму.

Лемма 1. *Пусть R и S — два поля алгебраических функций от одной переменной, причем R является подполем поля S. Если S чисто несепарабельно над R, то над каждой точкой $\mathfrak{p}$ поля R лежит только одна точка $\mathfrak{P}$ поля S, и поле вычетов точки $\mathfrak{P}$ чисто несепарабельно над полем вычетов точки $\mathfrak{p}$.*

Для любого элемента u из S существует такой показатель a, что $u^{p^a}\in R$, где p — характеристика поля R (мы предполагаем, что $p>0$). Для того чтобы элемент u принадлежал некоторой точке поля S, лежащей над $\mathfrak{p}$, необходимо и достаточно, чтобы $u^{p^a}\in\mathfrak{p}$. Отсюда и следует, что имеется только одна точка $\mathfrak{P}$ поля S, лежащая над $\mathfrak{p}$. Далее, если элемент u принадлежит кольцу точки $\mathfrak{P}$, то p^a-ая степень значения, принимаемого элементом u в точке $\mathfrak{P}$ принадлежит полю вычетов точки $\mathfrak{p}$, а значит, поле вычетов точки $\mathfrak{P}$ чисто несепарабельно над полем вычетов точки $\mathfrak{p}$.

Принимая во внимание доказанную лемму 1, мы видим, что число точек поля $R\langle L\rangle$, лежащих над $\mathfrak{p}$, равно числу точек поля $R\langle L'\rangle$, также лежащих над $\mathfrak{p}$. Так как поле L' сепарабельно над K, то алгебра $\Sigma_{L'}$ полупроста (следствие 2 к лемме 5 § 1). Поэтому наше число точек равно числу минимальных идеалов алгебры $\Sigma_{L'}$. В силу леммы 5 § 3 в поле L существует подполе L'', которое алгебраично и сепарабельно над K и для которого алгебра $\Sigma_{L''}$ также является суммой h минимальных идеалов. Так как L чисто несепарабельно над L', то $L'\langle L''\rangle=L'$ и $L''\subset L'$. Таким образом, число минимальных идеалов во всех трех алгебрах $\Sigma_{L'}$, $\Sigma_{L''}$ и $\Sigma_L/\mathfrak{n}$ равно h. Этим доказано, что в поле $R\langle L\rangle$ имеется ровно h точек, лежащих над $\mathfrak{p}$. Следовательно, соответствие $Z_i\to\mathfrak{P}_i$ является взаимно однозначным соответствием между полями Z_i и всеми точками поля $R\langle L\rangle$, лежащими над $\mathfrak{p}$. Далее, пусть $\mathfrak{P}_i'$ есть точка поля $R\langle L'\rangle$, лежащая под $\mathfrak{P}_i$. Так как алгебра $\Sigma_{L'}$ полупроста, то поле вычетов Σ_i' точки $\mathfrak{P}_i'$ порождается элементами поля L и образом поля Σ при естественном изоморфизме Σ в Σ_i'. Так как поле вычетов точки $\mathfrak{P}_i$ чисто несепарабельно над Σ_i' (лемма 1), то оно чисто несепарабельно также и над $\varphi_i(Z_i)$. Теорема 3 доказана теперь полностью.

Следствие 1. *Сохраняя обозначения теоремы 3, предположим, что каждый элемент поля L, алгебраический над K, чисто несепарабелен над K. Тогда над любой точкой поля R лежит только одна точка поля $R\langle L\rangle$.*

Действительно, в этом случае каждый делитель нуля алгебры Σ_L нильпотентен (лемма 3 § 2), поэтому фактор-алгебра $\Sigma_L/\mathfrak{n}$ не имеет делителей нуля, отличных от 0 (лемма 1 § 3), а значит, $\Sigma_L/\mathfrak{n}$ есть поле.

Следствие 2. *Сохраняя обозначения теоремы 3, предположим, что поле L чисто трансцендентно над K. Тогда в поле $R\langle L\rangle$ существует только одна точка $\mathfrak{P}$, лежащая над $\mathfrak{p}$. Точка $\mathfrak{P}$ неразветвлена относительно R, и ее поле вычетов может быть получено из поля вычетов точки $\mathfrak{p}$ присоединением элементов из L, кроме того $d(\mathfrak{P})=d(\mathfrak{p})$.*

Так как поле L сепарабельно над K (лемма 4 § 1), то утверждения следствия 2 вытекают непосредственно из теоремы 3, следствия 1 и следствия к теореме 2 § 4.

Следствие 3. *Пусть сохраняются обозначения теоремы 3, и пусть Σ_s есть подполе сепарабельных над K элементов из Σ. Тогда подалгебра $(\Sigma_s)_L$ алгебры Σ_L является прямой суммой h полей Z_i' $(1\leqslant i\leqslant n)$, и для каждого i поле $Z_i''=(Z_i'+\mathfrak{n})/\mathfrak{n}$ является подполем сепарабельных над L элементов поля Z_i. Далее, $\varphi_i(Z_i'')$ совпадает с подполем сепарабельных над L элементов поля Σ_i.*

Можно считать, что поле K имеет характеристику $p>0$. Так как Σ_s сепарабельно над K, то алгебра $(\Sigma_s)_L$ полупроста (лемма 1 § 1), поэтому ее пересечение с $\mathfrak{n}$ состоит только из 0. Отсюда следует, что естественный гомоморфизм Σ_L на $\Sigma_L/\mathfrak{n}$ отображает $(\Sigma_s)_L$ изоморфно на некоторую подалгебру $\mathfrak{A}$ алгебры $\Sigma_L/\mathfrak{n}$. Выберем целое число $m>0$ так, чтобы p^m-ая степень любого элемента из Σ принадлежала Σ_s. Если $\eta=\sum_{j=1}^{r}a_j\xi_j\in\Sigma_L$ $(a_j\in L,\ \xi_j\in\Sigma,\ 1\leqslant j\leqslant r)$, то $\eta^{p^m}=\sum_{j=1}^{r}a_j^{p^m}\xi_j^{p^m}\in(\Sigma_s)_L$. Следовательно, p^m-ая степень каждого элемента из $\Sigma_L/\mathfrak{n}$ принадлежит $\mathfrak{A}$. Пусть ε_i — единица поля Z_i $(1\leqslant i\leqslant h)$; так как $\varepsilon_i^{p^m}=\varepsilon_i$, то $\varepsilon_i\in\mathfrak{A}$. Если

элемент $\zeta = \sum_{i=1}^{h} \zeta_i$ (где $\zeta_i \in Z_i$, $1 \leqslant i \leqslant h$) принадлежит $\mathfrak{A}$, то $\zeta_i = \zeta\varepsilon_i \in \mathfrak{A}$, откуда следует, что $\mathfrak{A}$ есть прямая сумма подалгебр $\mathfrak{A}\varepsilon_i$ $(1 \leqslant i \leqslant h)$. Так как поле Z_i имеет конечную степень над L, а подалгебра $\mathfrak{A}\varepsilon_i$ содержится в Z_i, то она сама является полем Z_i''. Очевидно, что p^m-ая степень любого элемента из Z_i принадлежит Z_i'', т. е. Z_i чисто несепарабельно над Z_i''. Каждый элемент из Z_i'' может быть представлен в виде линейной комбинации с коэффициентами из L элементов поля $(\Sigma_s + \mathfrak{n})/\mathfrak{n}$ (умноженных на ε_i), которые сепарабельны над подполем K поля L. Отсюда следует, что поле Z_i'' сепарабельно над L, а значит, оно является подполем сепарабельных над L элементов из Z_i. Последнее утверждение следствия 3 вытекает непосредственно из предыдущих утверждений и теоремы 3.

Следствие 4. *Сохраняя обозначения теоремы 3, предположим, что поле L алгебраически замкнуто. Тогда естественные изоморфизмы поля Σ в поля вычетов точек поля $R\langle L\rangle$, лежащих над $\mathfrak{p}$, — это все различные изоморфизмы поля Σ в L, тождественные на K. Число точек поля $R\langle L\rangle$, лежащих над $\mathfrak{p}$, равно $[\Sigma_s : K]$, где Σ_s — подполе сепарабельных над K элементов из Σ.*

Так как поле L алгебраически замкнуто, то поля Z_i и Σ_i (которые всегда имеют конечную степень над L) совпадают с L. Первое утверждение следствия 4 вытекает теперь из леммы 4 § 3. Второе утверждение следует из общеизвестной теоремы теории Галуа.

Замечание. Если алгебра Σ_L не полупроста, то может случиться, что некоторые точки поля $R\langle L\rangle$, лежащие над $\mathfrak{p}$, разветвлены относительно R, а также, что $\Sigma_i \neq \varphi_i(Z_i)$ для некоторых точек $\mathfrak{P}_i$. Покажем на примере, что обе эти возможности действительно могут иметь место даже в случае, когда R сепарабельно над K. Пусть K — поле характеристики $p > 0$, в котором имеются такие элементы a и b, что $\left[K\left\langle a^{\frac{1}{p}}, b^{\frac{1}{p}}\right\rangle : K\right] = p^2$. Пусть $R_1 = K\langle x\rangle$, где x трансцендентен над K, и пусть $\mathfrak{p}$ — единственный нуль элемента $x^p - a$ в поле R_1. Так как многочлен $x^p - a$ неприводим в $K[x]$, то $\nu_{\mathfrak{p}}(x^p - a) = 1$. Положим $L = K\left\langle a^{\frac{1}{p}}\right\rangle$, тогда

в поле $R_1\langle L\rangle$ элемент $x^p - a$ является p-ой степенью элемента $x - a^{\frac{1}{p}}$. Если $\mathfrak{P}$ есть точка поля $R_1\langle L\rangle$, лежащая над $\mathfrak{p}$, то $\nu_{\mathfrak{P}}(x^p - a)$ делится на p, т. е. точка $\mathfrak{P}$ разветвлена относительно $K\langle x\rangle$. Положим, далее, $R_2 = R_1\langle y\rangle$, где элемент y удовлетворяет уравнению $y^p = (b + y)(x^p - a)$. Очевидно, что y сепарабелен над R_1, а значит, поле R_2 сепарабельно над K. Пусть $\mathfrak{q}$ — точка поля R_2, лежащая над $\mathfrak{p}$; тогда, как легко видеть, $\mathfrak{q}$ является нулем элемента y, откуда $\nu_{\mathfrak{p}}(x^p - a) \equiv 0 \pmod{p}$. Это означает, что индекс разветвления точки $\mathfrak{q}$ относительно R_1 больше или равен p; но степень поля R_2 над R_1 не превосходит p, поэтому этот индекс равен p, откуда $\nu_{\mathfrak{q}}(y) = 1$, и поле вычетов точки $\mathfrak{q}$ совпадает с полем вычетов точки $\mathfrak{p}$, т. е. оно изоморфно полю $L = K\langle a^{\frac{1}{p}}\rangle$. Пусть $\mathfrak{Q}$ есть точка поля $R_2\langle L\rangle$, лежащая над $\mathfrak{q}$; равенство $\left(y\left(x - a^{\frac{1}{p}}\right)^{-1}\right)^p = b + y$ показывает, что в поле вычетов точки $\mathfrak{Q}$ элемент b является p-ой степенью. Таким образом, поле вычетов точки $\mathfrak{Q}$ не может быть получено из поля вычетов точки $\mathfrak{q}$ присоединением элементов поля L. Мы видим также, что если к полю $R_2\langle L\rangle$ мы присоединим корень p-ой степени из b, то в полученном поле точка, лежащая над $\mathfrak{Q}$, будет разветвлена относительно $R_2\langle L\rangle$. В дальнейшем мы увидим, что это является общей закономерностью: если (в обозначениях теоремы 3) какое-нибудь поле Σ_i отлично от $\varphi_i(Z_i)$, то для поля L существует такое расширение M, что некоторая точка поля $R\langle M\rangle$, лежащая над $\mathfrak{P}_i$, разветвлена относительно $R\langle L\rangle$.

§ 6. Расширение поля констант и род поля

Теорема 4. *Пусть R — поле алгебраических функций от одной переменной, K — его поле констант, L — сепарабельное расширение поля K и $\mathfrak{a}$ — произвольный дивизор поля R. Если элемент y из поля $R\langle L\rangle$ делится на $\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{a}$, то он может быть представлен в виде линейной комбинации элементов поля R, делящихся на $\mathfrak{a}$, с коэффициентами из L.*

Элемент y принадлежит некоторому полю вида $R\langle L_1\rangle$, где L_1 — подполе поля L, получающееся из K присоединением

конечного числа элементов. Поле L_1 сепарабельно над K (лемма 3 § 1). По лемме 3 § 7 гл. IV мы имеем

$$\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{a}=\mathrm{Con}_{R\langle L_1\rangle/R\langle L\rangle}\left(\mathrm{Con}_{R/R\langle L_1\rangle}\mathfrak{a}\right).$$

Положим $\mathfrak{a}_1=\mathrm{Con}_{R/R\langle L_1\rangle}\mathfrak{a}$; так как элемент y принадлежит $R\langle L_1\rangle$ и делится на $\mathrm{Con}_{R\langle L_1\rangle/R\langle L\rangle}\mathfrak{a}_1$ (если его рассматривать как элемент поля $R\langle L\rangle$), то он делится и на дивизор $\mathfrak{a}_1$ в поле $R\langle L_1\rangle$. Таким образом, теорему 4 достаточно доказать для случая, когда L может быть получено из K присоединением конечного числа элементов. Будем считать поэтому, что именно этот случай и имеет место.

Между полями K и L существует промежуточное поле M, чисто трансцендентное над K, над которым поле L имеет конечную степень и сепарабельно (лемма 5 § 1). Пусть $\{b_1, \ldots, b_r\}$ — базис поля L относительно M. По следствию 1 к теореме 1 § 4 элементы $b_1, \ldots, b_r$ линейно независимы над $R\langle M\rangle$ и образуют базис поля $R\langle L\rangle$ относительно $R\langle M\rangle$. Докажем, что если $y=\sum_{i=1}^{r} b_i z_i$, где $z_i\in R\langle M\rangle$ $(1\leqslant i\leqslant r)$, то $z_i\equiv 0 \pmod{\mathfrak{b}}$, где $\mathfrak{b}=\mathrm{Con}_{R/R\langle M\rangle}\mathfrak{a}$. Пусть $\mathfrak{q}$ — произвольная точка поля $R\langle M\rangle$. Обозначим через q показатель, с которым $\mathfrak{q}$ входит в $\mathfrak{b}$. Пусть u есть униформизирующая переменная в точке $\mathfrak{q}$. Так как $y\equiv 0\left(\mathrm{mod}\,\mathrm{Con}_{R\langle M\rangle/R\langle L\rangle}\mathfrak{b}\right)$, то элемент $u^{-q}y$ является целым в каждой точке поля $R\langle L\rangle$, лежащей над $\mathfrak{q}$. С другой стороны, дискриминант базиса $\{b_1, \ldots, b_r\}$ есть отличный от 0 элемент поля M, откуда следует, что этот базис является целым в точке $\mathfrak{q}$ (лемма 2 § 8 гл. IV), а значит, $\nu_{\mathfrak{q}}(u^{-q}z_i)\geqslant 0$ $(1\leqslant i\leqslant r)$. Так как это верно для любой точки $\mathfrak{q}$ поля $R\langle M\rangle$, то $z_i\equiv 0 \pmod{\mathfrak{b}}$. Для доказательства теоремы 4 теперь достаточно показать, что каждый элемент z_i есть линейная комбинация элементов поля R, делящихся на $\mathfrak{a}$, с коэффициентами из M. Другими словами, теорему 4 достаточно доказать для случая, когда $L=K\langle t_1, \ldots, t_n\rangle$, где элементы $t_1, \ldots, t_n$ алгебраически независимы над K. В этом случае доказательство проведем индукцией по n. Если $n=0$, то доказывать нечего. Пусть $n>0$ и предположим, что теорема справедлива для полей, степень трансцендентности которых равна $n-1$. Положим $N=K\langle t_1, \ldots, t_{n-1}\rangle$ и $S=R\langle N\rangle$. Элемент y можно пред-

ставить в виде $y=\frac{P(t_n)}{Q(t_n)}$, где P и Q — взаимно простые многочлены с коэффициентами из S, причем старший коэффициент многочлена Q равен 1. Докажем, что при таком представлении все коэффициенты многочлена Q принадлежат N. Допустим противное. Тогда, если мы многочлен Q в подходящем алгебраическом расширении поля $R\langle L\rangle$ разложим на линейные множители, то хоть один из его корней, скажем s, в этом расширении будет трансцендентным над N (иначе все коэффициенты многочлена Q были бы алгебраичны над N и, по лемме 2 § 2, принадлежали бы N). Положим $U=(R\langle L\rangle)\langle s\rangle$. Элемент s алгебраичен над S, но не алгебраичен над N; так как степень трансцендентности поля S над N равна 1, то поле $S\langle s\rangle$ алгебраично над $N\langle s\rangle$, а поле U алгебраично над $L\langle s\rangle$. Рассматривая поле U как поле алгебраических функций от одной переменной над L, мы видим, что элемент $s-t_n$ имеет по крайней мере один нуль $\mathfrak{Q}$ в поле U. Значение t_n, принимаемое элементом s в точке $\mathfrak{Q}$, трансцендентно над полем констант N поля S. Отсюда следует, что поле вычетов точки $\mathfrak{Q}$ трансцендентно над N, и, следовательно, $\mathfrak{Q}$ является переменной точкой относительно подполя $S\langle s\rangle$ поля U. В частности, для любого элемента из S точка $\mathfrak{Q}$ не является полюсом. Так как коэффициенты многочленов P и Q принадлежат S и $\nu_{\mathfrak{Q}}(t_n-s)>0$, то $\nu_{\mathfrak{Q}}(Q(t_n))>0$ и $\nu_{\mathfrak{Q}}(P(t_n)-P(s))>0$. Многочлены P и Q взаимно просты, поэтому $P(s)\neq 0$. Но элемент $P(s)$ принадлежит полю $S\langle s\rangle$, относительно которого точка $\mathfrak{Q}$ переменная; следовательно, $\nu_{\mathfrak{Q}}(P(s))=0$, откуда $\nu_{\mathfrak{Q}}(P(t_n))=0$. Этим показано, что $\mathfrak{Q}$ является полюсом элемента y. Пусть $\mathfrak{q}$ есть точка поля $R\langle L\rangle$, лежащая под $\mathfrak{Q}$; тогда $\mathfrak{q}$ является полюсом элемента y в поле $R\langle L\rangle$ и является, очевидно, переменной точкой относительно поля $R\langle N\rangle=S$, а, следовательно, и относительно поля R. Отсюда следует, что точка $\mathfrak{q}$ не входит в дивизор $\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{a}$, и мы получили противоречие, ибо по предположению y делится на этот дивизор. Таким образом, мы доказали, что $Q(t_n)\in L$. Положим $P(t_n)=\sum_{k=0}^{d} t_n^k y_k$, где $y_k\in R\langle N\rangle$, тогда $y=\sum_{k=0}^{d}\frac{t_n^k}{Q(t_n)}y_k$. Докажем, что $y_k\equiv 0\left(\mathrm{mod}\,\mathrm{Con}_{R/R\langle N\rangle}\mathfrak{a}\right)$ $(0\leqslant k\leqslant d)$. Пусть $\mathfrak{p}$ — произвольная точка поля R, а v — униформизирующая

переменная в этой точке. В силу следствия 2 к теореме 3 § 5 в поле $R\langle L\rangle$ существует только одна точка $\mathfrak{P}$, лежащая над $\mathfrak{p}$, при этом $\nu_{\mathfrak{P}}(v)=1$. Выберем целое число a так, чтобы $\nu_{\mathfrak{P}}(v^{-a}y_k)\geqslant 0$ при всех k и $\nu_{\mathfrak{P}}(v^{-a}y_k)=0$ хотя бы для одного значения k. Если мы через η_k обозначим значение, принимаемое элементом $v^{-a}y_k$ в точке $\mathfrak{P}$, то значение элемента $v^{-a}y$ в точке $\mathfrak{P}$ будет равно $\sum_{k=0}^{d}\frac{t_n^k}{Q(t_n)}\eta_k$. Все элементы η_k принадлежат полю вычетов точки поля $R\langle N\rangle$, лежащей над $\mathfrak{p}$, и элемент t_n, очевидно, трансцендентен над этим полем вычетов. Поэтому $\nu_{\mathfrak{P}}(v^{-a}y)=0$, откуда $\nu_{\mathfrak{P}}(y)=a$. Пусть a' есть показатель, с которым точка $\mathfrak{p}$ входит в $\mathfrak{a}$, тогда $\nu_{\mathfrak{P}}(y)\geqslant a'$, т. е. $a\geqslant a'$. Этим доказано, что $y_k\equiv 0$ $\left(\operatorname{mod}\operatorname{Con}_{R/R\langle N\rangle}\mathfrak{a}\right)$ при всех k. В силу нашего индуктивного предположения каждый элемент y_k может быть представлен в виде линейной комбинации элементов поля R, делящихся на $\mathfrak{a}$, с коэффициентами из N. Так как $\frac{t_n^k}{Q(t_n)}\in L$, то, как мы видим, элемент y представим в виде линейной комбинации элементов поля R, делящихся на $\mathfrak{a}$, с коэффициентами из L. Теорема 4, таким образом, доказана.

Следствие 1. *В предположениях теоремы 4 имеем*

$$l\left(\operatorname{Con}_{R/R\langle L\rangle}\mathfrak{a}\right)=l(\mathfrak{a}).$$

Пусть $l(\mathfrak{a})=l$ и пусть $x_1,\ldots,x_l$ — элементы поля R, линейно независимые над K и делящиеся на $\mathfrak{a}$. Эти элементы $x_1,\ldots,x_l$, если их рассматривать в поле $R\langle L\rangle$, делятся на $\operatorname{Con}_{R/R\langle L\rangle}\mathfrak{a}$ и линейно независимы над L (теорема 1 § 4). В силу теоремы 4 каждый элемент поля $R\langle L\rangle$, делящийся на $\operatorname{Con}_{R/R\langle L\rangle}\mathfrak{a}$, является линейной комбинацией элементов $x_1,\ldots,x_l$ с коэффициентами из L. Для завершения доказательства следствия 1 теперь остается только заметить, что L есть поле констант поля $R\langle L\rangle$ (теорема 2 § 4).

Следствие 2. *Пусть соблюдаются предположения теоремы 4. Тогда для того чтобы элемент $y\in R\langle L\rangle$ можно было представить в виде линейной комбинации элементов поля R с коэффициентами из L, необходимо и достаточно, чтобы среди полюсов элемента y не было переменных точек поля $R\langle L\rangle$ относительно R.*

Что условие необходимо — очевидно. Обратно, допустим, что оно выполнено. Пусть $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все полюса элемента y. По предположению каждая точка $\mathfrak{P}_i$ лежит над некоторой точкой $\mathfrak{p}_i$ поля R. При достаточно большом n, очевидно будем иметь $y \equiv 0 \left(\operatorname{mod} \operatorname{Con}_{R/R\langle L\rangle}(\mathfrak{p}_1 \ldots \mathfrak{p}_h)^{-n}\right)$. В силу теоремы 4 отсюда следует, что y можно представить в виде линейной комбинации элементов поля R с коэффициентами из L.

Замечание. *Утверждение следствия 2 справедливо также для случая, когда поле L произвольно, но R сепарабельно порождаемо.*

Для доказательства поступим следующим образом. Пусть x — сепарабельно порождающая переменная поля R и пусть $\{a_i\}_{i \in I}$ — базис поля L относительно K (I — некоторое множество индексов). Для любого элемента z из поля R положим $u_z = \operatorname{Sp}_{R\langle L\rangle/L\langle x\rangle} yz \in L\langle x\rangle$. Если $\mathfrak{P}_0$ есть точка поля $L\langle x\rangle$, переменная относительно $K\langle x\rangle$, то всякая точка $\mathfrak{P}$ поля $R\langle L\rangle$, лежащая над $\mathfrak{P}_0$, будет переменной точкой относительно R. Действительно, если бы это было не так, то пересечение $\mathfrak{P} \cap R$ являлось бы точкой поля R, а следовательно, пересечение $\mathfrak{P} \cap K\langle x\rangle = \mathfrak{P}_0 \cap K\langle x\rangle$ являлось бы точкой поля $K\langle x\rangle$, что противоречит предположению. Таким образом, мы видим, что все точки поля $R\langle L\rangle$, лежащие над $\mathfrak{P}_0$, не являются полюсами элемента yz (если y не имеет в $R\langle L\rangle$ переменных полюсов относительно R), откуда следует, что $\mathfrak{P}_0$ не является полюсом элемента u_z. Так как элемент $u_z \in L\langle x\rangle$ не имеет переменных полюсов относительно $K\langle x\rangle$, то его дивизор полюсов является делителем дивизора вида $\operatorname{Con}_{K\langle x\rangle/L\langle x\rangle} \mathfrak{u}_z$, где $\mathfrak{u}_z$ — целый дивизор поля $K\langle x\rangle$. Выберем многочлен $V_z \neq 0$ с коэффициентами из K, дивизор которого имеет вид $\mathfrak{u}_z \mathfrak{q}_0^{-m_z}$, где $\mathfrak{q}_0$ — полюс элемента x в поле $K\langle x\rangle$, а m_z — некоторое целое неотрицательное число. Тогда полюсом элемента $V_z(x) u_z$ в поле $L\langle x\rangle$ может являться только полюс элемента x, поэтому $V_z(x) u_z = U_z(x)$, где U_z — многочлен с коэффициентами из L. Так как коэффициенты V_z принадлежат K, то $u_z = \sum_{i \in I} a_i \varphi_i(z)$, где $\varphi_i(z) \in K\langle x\rangle$. Очевидно, что если $v \in K\langle x\rangle$, то $\varphi_i(vz) = v\varphi_i(z)$ при всех $i \in I$. Пусть $\{z_1, \ldots, z_n\}$ — базис поля R относительно $K\langle x\rangle$, тогда каждый элемент $z \in R$ можно представить

в виде $\sum_{j=1}^{n} v_j z_j$, откуда $\varphi_i(z) = \sum_{j=1}^{n} v_j \varphi_i(z_j)$. Для каждого j имеется только конечное число индексов i, для которых $\varphi_i(z_j) \neq 0$; отсюда следует, что только для конечного числа индексов i функция φ_i не равна тождественно нулю. В силу леммы 1 § 5 гл. III для каждого $i \in I$ существует такой элемент $y_i \in R$, что при всех $z \in R$ имеем $\varphi_i(z) = \mathrm{Sp}_{R/K\langle x\rangle} y_i z = \mathrm{Sp}_{R\langle L\rangle/L\langle x\rangle} y_i z$ (следствие 2 к теореме 1 § 4). Так как существует только конечное число индексов i, для которых $y_i \neq 0$, то можно положить $y' = \sum_{i \in I} a_i y_i$. Имеем теперь $\mathrm{Sp}_{R\langle L\rangle/L\langle x\rangle}(y - y') z = 0$ при всех $z \in R$. Последнее равенство справедливо, в частности, для элементов $z_1, \ldots, z_n$, образующих базис поля $R\langle L\rangle$ относительно $L\langle x\rangle$ (следствие 2 к теореме 1 § 4), а следовательно, оно справедливо также для всех $z \in R\langle L\rangle$. Но поле $R\langle L\rangle$ сепарабельно над $L\langle x\rangle$, поэтому $y = y'$ (лемма 1 § 5 гл. III), и наше утверждение доказано.

Теорема 5. *Пусть R — поле алгебраических функций от одной переменной и пусть L — произвольное расширение поля констант K поля R. Тогда род g' поля $R\langle L\rangle$ не превосходит рода g поля R, а если поле L сепарабельно над K, то имеет место равенство $g' = g$.*

Рассмотрим сначала случай, когда поле L сепарабельно над K. Пусть $\mathfrak{a}$ — дивизор поля R, для которого $d(\mathfrak{a}^{-1}) > 2g - 2$ и $d(\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{a}^{-1}) > 2g' - 2$. По теореме Римана—Роха мы имеем $l(\mathfrak{a}) = -d(\mathfrak{a}) - g + 1$ и $l(\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{a}) = -d(\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{a}) - g' + 1$. Согласно следствию 1 к теореме 4 левые части этих равенств равны между собой. С другой стороны, $d(\mathfrak{a}) = d(\mathrm{Con}_{R/R\langle L\rangle}\mathfrak{a})$ (следствие к теореме 2 § 4). Следовательно, $g = g'$.

Вернемся к общему случаю. Поле L является алгебраическим расширением некоторого поля M_0, которое чисто трансцендентно над K. Пусть M есть поле тех элементов из L, которые сепарабельны над M_0. Так как M сепарабельно над M_0, а M_0 сепарабельно над K (лемма 4 § 1), то поле M сепарабельно над K (лемма 3 § 1). С другой стороны, поле L чисто несепарабельно над M. Как уже доказано, род поля $R\langle M\rangle$ равен g. Таким образом, теорему 5

достаточно доказать для случая, когда L алгебраично и чисто несепарабельно над K. Пусть тогда L' есть поле констант поля $R\langle L\rangle$ и пусть $\{a_i\}_{i\in I}$ — базис поля L' над K (I — множество индексов, которое может быть конечным или бесконечным). Пусть $\Omega_1, \ldots, \Omega_{g'}$ — линейно независимые дифференциалы первого рода поля $R\langle L\rangle$. Если $\mathfrak{x}$ — распределение в поле R, то $\mathrm{Cosp}_{R/R\langle L\rangle}\mathfrak{x}$ есть распределение в поле $R\langle L\rangle$, и мы можем записать $\Omega_k(\mathrm{Cosp}_{R/R\langle L\rangle}\mathfrak{x}) = \sum_{i\in I}\omega_{ik}(\mathfrak{x})\,a_i$, где $\omega_{ik}(\mathfrak{x})\in K$. Ясно, что все ω_{ik} являются линейными функциями на векторном пространстве распределений поля R. Пусть $\mathfrak{e}$ — единичный дивизор поля R; если $\mathfrak{x}\equiv 0 \pmod{\mathfrak{e}}$, то $\mathrm{Cosp}_{R/R\langle L\rangle}\mathfrak{x}$ делится на единичный дивизор поля $R\langle L\rangle$, а значит, $\omega_{ik}(\mathfrak{x}) = 0$ при всех i и k. С другой стороны, если $\mathfrak{x}$ есть главное распределение x_R, соответствующее элементу $x\in R$, то $\mathrm{Cosp}_{R/R\langle L\rangle}\mathfrak{x}$ есть главное распределение $x_{R\langle L\rangle}$, соответствующее элементу x в поле $R\langle L\rangle$; поэтому имеем также $\omega_{ik}(\mathfrak{x}) = 0$ при всех i и k. Этим доказано, что все функции ω_{ik} являются дифференциалами первого рода поля R. Покажем, что только конечное число этих дифференциалов отлично от 0. Пусть $\mathfrak{b}$ — целый дивизор поля R степени $d > 2g-2$; тогда согласно теореме 2 § 5 гл. II для каждого распределения $\mathfrak{x}$ в поле R найдется главное распределение x_R, где $x\in R$, такое, что $\mathfrak{x}\equiv x_R \pmod{\mathfrak{b}^{-1}}$. В силу леммы 1 § 4 гл. II мы можем найти d распределений $\mathfrak{x}_1, \ldots, \mathfrak{x}_d$, делящихся на $\mathfrak{b}^{-1}$ и таких, что всякое распределение $\mathfrak{x}'$, делящееся на $\mathfrak{b}^{-1}$ можно представить в виде $\sum_{j=1}^{d} c_j\mathfrak{x}_j + \mathfrak{x}''$, где $\mathfrak{x}''\equiv 0 \pmod{\mathfrak{e}}$ и $c_j\in K$. Таким образом, каждое распределение $\mathfrak{x}$ поля R может быть представлено в виде $x_R + \sum_{j=1}^{d} c_j\mathfrak{x}_j + \mathfrak{x}''$, где $\mathfrak{x}''\equiv 0 \pmod{\mathfrak{e}}$, откуда $\Omega_k(\mathrm{Cosp}_{R/R\langle L\rangle}\mathfrak{x}) = \sum_{j=1}^{d} c_j\Omega_k(\mathrm{Cosp}_{R/R\langle L\rangle}\mathfrak{x}_j)$. Мы можем найти теперь такое конечное подмножество I_0 множества I, что все элементы $\Omega_k(\mathrm{Cosp}_{R/R\langle L\rangle}\mathfrak{x}_j)$ могут быть представлены в виде линейных комбинаций элементов $\{a_i\}_{i\in I_0}$

с коэффициентами из K. Ясно, что тогда $\omega_{ik}=0$, если только $i \notin I_0$. Если бы теперь имело место неравенство $g' > g$, то мы могли бы найти такой дифференциал $\Omega \neq 0$ поля $R\langle L\rangle$ первого рода, что $\Omega\left(\mathrm{Cosp}_{R/R\langle L\rangle}\mathfrak{x}\right)=0$ для любого распределения $\mathfrak{x}$ поля R. Покажем, что существование такого дифференциала ведет к противоречию. Так как $\Omega \neq 0$, то существует такое распределение $\mathfrak{y}$ поля $R\langle L\rangle$, что $\Omega(\mathfrak{y}) \neq 0$, при этом мы можем даже предполагать, что $\mathfrak{y}(\mathfrak{P}) \in R\langle L\rangle$ для всех точек $\mathfrak{P}$ поля $R\langle L\rangle$ (т. е. что $\mathfrak{y}$ есть распределение в смысле первого определения этого понятия, данного в § 4 гл. II). Для каждой точки $\mathfrak{P}$ поля $R\langle L\rangle$ через $\mathfrak{y}_{\mathfrak{P}}$ обозначим распределение, сопоставляющее точке $\mathfrak{P}$ значение $\mathfrak{y}(\mathfrak{P})$, а всем другим точкам — значение 0. Тогда среди элементов $\Omega(\mathfrak{y}_{\mathfrak{P}})$ имеется только конечное число отличных от 0, и имеет место равенство $\Omega(\mathfrak{y})=\sum\limits_{\mathfrak{P}}\Omega(\mathfrak{y}_{\mathfrak{P}})$. Пусть $\mathfrak{P}$ — одна из тех точек, для которых $\Omega(\mathfrak{y}_{\mathfrak{P}}) \neq 0$. Так как поле L алгебраично над K, то значение $\mathfrak{y}(\mathfrak{P})$ может быть записано в виде $\sum\limits_{i\in I} a_i x_i$, где $x_i \in R$ (это легко следует из леммы 2 § 1 гл. IV). Пусть $\mathfrak{p}$ есть точка поля R, лежащая под $\mathfrak{P}$, и пусть $\mathfrak{x}_i$ — распределение поля R, сопоставляющее точке $\mathfrak{p}$ значение x_i, а всем другим точкам — значение 0. Так как $\mathfrak{P}$ является единственной точкой поля $R\langle L\rangle$, лежащей над $\mathfrak{p}$ (следствие 1 к теореме 3 § 5), то $\mathfrak{y}_{\mathfrak{P}}=\sum\limits_{i\in I} a_i\,\mathrm{Cosp}_{R/R\langle L\rangle}\mathfrak{x}_i$. Но тогда $\Omega(\mathfrak{y}_{\mathfrak{P}})=0$, и желаемое противоречие получено. Теорема 5, таким образом, доказана.

Заметим, что строгое неравенство $g' < g$ может иметь место даже в том случае, когда поле R сепарабельно порождаемо над K [1]).

---

[1]) Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной характеристики $p \neq 0$, K — его поле констант и x — сепарабельно порождающая переменная поля R. Для того чтобы при любом расширении L/K поля констант род поля $R\langle L\rangle$ был равен роду поля R, необходимо и достаточно, чтобы каждая точка поля $K\langle x\rangle$, соответствующая неприводимому многочлену вида $f(x^p)$, была неразветвлена в поле R. (*Прим. перев.*)

ГЛАВА VI

ТОЧНЫЕ ДИФФЕРЕНЦИАЛЫ

§ 1. Дифференциал dx в поле $K\langle x\rangle$

Пусть R — поле алгебраических функций от одной переменной. В этой главе каждому элементу x из R мы сопоставим дифференциал dx поля R и покажем, что полученные таким образом дифференциалы обладают такими же формальными свойствами, какими обладают дифференциалы, рассматриваемые в математическом анализе.

Прежде всего мы рассмотрим случай, когда поле R имеет вид $K\langle x\rangle$, где K — произвольное поле, а x — трансцендентный элемент над K. Для этого случая в настоящем параграфе дадим определение дифференциала dx только для элемента x. К общему случаю перейдем позднее, применив понятие коследа дифференциала.

В § 5 второй главы было дано определение дифференциалов поля $K\langle x\rangle$ для случая, когда K есть поле комплексных чисел. Это были выражения вида udx, где u — произвольный элемент из $K\langle x\rangle$. Полагая $u=1$, получим дифференциал, который будем называть дифференциалом элемента x. Для произвольного u дифференциал udx является, очевидно, произведением элемента u на дифференциал dx. Мы видели, что порядок дифференциала udx в точке $\mathfrak{p}$, не являющейся полюсом элемента x, равен $\nu_{\mathfrak{p}}(u)$, а его порядок в полюсе $\mathfrak{p}(\infty)$ элемента x равен $\nu_{\mathfrak{p}(\infty)}(u)-2$. Далее, если $\mathfrak{x}$ есть распределение, сопоставляющее точке $\mathfrak{p}(\infty)$ значение x^{-1}, а всем другим точкам — значение 0, то, как легко видеть, $(dx)(\mathfrak{x})=-1$. Отсюда следует, что дивизор дифференциала dx равен $(\mathfrak{p}(\infty))^{-2}$.

Пусть теперь K — произвольное поле; положим $R=K\langle x\rangle$, где элемент x трансцендентен над K. В поле R элемент x

имеет единственный полюс $\mathfrak{p}(\infty)$, и степень $\mathfrak{p}(\infty)$ равна 1. Так как род поля $K\langle x\rangle$ равен 0, то согласно теореме Римана — Роха $l((\mathfrak{p}(\infty))^2) = d\left((\mathfrak{p}(\infty))^{-2}\right) + 1 + \delta\left((\mathfrak{p}(\infty))^{-2}\right) = \delta\left((\mathfrak{p}(\infty))^{-2}\right) - 1$, где $\delta\left((\mathfrak{p}(\infty))^{-2}\right)$ есть размерность пространства дифференциалов, делящихся на $(\mathfrak{p}(\infty))^{-2}$. Таким образом, мы видим, что существует дифференциал $\omega_1 \neq 0$ поля R, делящийся на $(\mathfrak{p}(\infty))^{-2}$. Так как степень дивизора $\mathfrak{d}(\omega_1)$ равна $-2 = d\left((\mathfrak{p}(\infty))^{-2}\right)$, то $\mathfrak{d}(\omega_1) = (\mathfrak{p}(\infty))^{-2}$. Пусть $\mathfrak{x}$ есть распределение, сопоставляющее точке $\mathfrak{p}(\infty)$ значение x^{-1}, а всем другим точкам — значение 0. Для любого дивизора $\mathfrak{a}$ через $\mathfrak{X}(\mathfrak{a})$ обозначим пространство тех распределений, которые делятся на $\mathfrak{a}$. Из леммы 1 § 4 гл. II следует, что размерность пространства $\mathfrak{X}(\mathfrak{p}(\infty))/\mathfrak{X}\left((\mathfrak{p}(\infty))^2\right)$ над полем K равна 1. Распределение $\mathfrak{x}$ принадлежит $\mathfrak{X}(\mathfrak{p}(\infty))$, но не принадлежит $\mathfrak{X}\left((\mathfrak{p}(\infty))^2\right)$; отсюда следует, что всякое распределение $\mathfrak{y}$ из $\mathfrak{X}(\mathfrak{p}(\infty))$ может быть представлено, и притом только единственным способом, в виде $a\mathfrak{x} + \mathfrak{y}'$, где $a \in K$ и $\mathfrak{y}' \in \mathfrak{X}((\mathfrak{p}(\infty))^2)$. Ясно, что $\omega_1(\mathfrak{y}') = 0$; если бы $\omega_1(\mathfrak{x}) = 0$, то $\omega_1(\mathfrak{y})$ было бы равно 0 для всех распределений $\mathfrak{y}$, делящихся на $\mathfrak{p}(\infty)$, т. е. дифференциал ω_1 делился бы на $(\mathfrak{p}(\infty))^{-1}$, что невозможно. Положим $\omega = -h^{-1}\omega_1$, где $h = \omega_1(\mathfrak{x})$. Очевидно, что дифференциал ω поля R делится на $(\mathfrak{p}(\infty))^{-2}$ и $\omega(\mathfrak{x}) = -1$. Утверждаем, что дифференциал ω последними двумя условиями определен однозначно. Действительно, пусть дифференциал ω' удовлетворяет тем же условиям, тогда $\omega' - \omega$ делится на $(\mathfrak{p}(\infty))^{-2}$ и $(\omega' - \omega)(\mathfrak{x}) = 0$. Отсюда следует, что $(\omega' - \omega)(\mathfrak{y}) = 0$ для всех распределений $\mathfrak{y} \in \mathfrak{X}(\mathfrak{p}(\infty))$, т. е. дивизор $\mathfrak{d}(\omega' - \omega)$ делится на $(\mathfrak{p}(\infty))^{-1}$. Но степень дивизора любого дифференциала поля R, отличного от 0, равна -2, что меньше, чем $d\left((\mathfrak{p}(\infty))^{-1}\right)$; следовательно, $\omega' - \omega = 0$.

Дифференциал ω, существование и единственность которого мы только что доказали, будем обозначать через dx. Сейчас мы найдем явные выражения для $\mathfrak{p}$-компонент $(dx)^{\mathfrak{p}}$ дифференциала dx для различных точек $\mathfrak{p}$ поля R (см. § 7 гл. II). Для этой цели достаточно вычислить $(dx)^{\mathfrak{p}}(u)$ для каждого $u \in R$.

Предположим сначала, что точка $\mathfrak{p}$ отлична от $\mathfrak{p}(\infty)$. Тогда существует неприводимый многочлен $f \in K[x]$, для которого $\mathfrak{p}$ является нулем порядка 1. Если мы предположим, что старший коэффициент многочлена f равен 1, то этим f будет определен однозначно. Как известно, каждый элемент $u \in R$ можно представить в виде

$$u = \frac{g_r}{f^r} + \ldots + \frac{g_1}{f} + v, \tag{1}$$

где v есть рациональная дробь, знаменатель которой не делится на f, т. е. $\nu_{\mathfrak{p}}(v) \geqslant 0$, а $g_1, \ldots, g_r$ — многочлены из $K[x]$, которые либо равны 0, либо имеют степень, меньшую степени d многочлена f. Так как $\mathfrak{p}$ не входит в $\mathfrak{d}(dx)$, то $(dx)^{\mathfrak{p}}(v) = 0$ (лемма 2 § 7 гл. II). Аналогично, если точка $\mathfrak{q}$ отлична от $\mathfrak{p}$ и $\mathfrak{p}(\infty)$, то $\nu_{\mathfrak{q}}(g_i f^{-i}) \geqslant 0$, откуда $(dx)^{\mathfrak{q}}(g_i f^{-i}) = 0$. В силу леммы 1 § 7 гл. II мы имеем $0 = (dx)(g_i f^{-i}) = \sum_{\mathfrak{r}} (dx)^{\mathfrak{r}}(g_i f^{-i})$, где суммирование распространено по всем точкам $\mathfrak{r}$. Отсюда следует, что $(dx)^{\mathfrak{p}}(g_i f^{-i}) = -(dx)^{\mathfrak{p}(\infty)}(g_i f^{-i})$. Пусть γ_i — степень многочлена g_i (если $g_i \neq 0$); тогда $\nu_{\mathfrak{p}(\infty)}(g_i f^{-i}) = id - \gamma_i$. Если $i > 1$, то последнее число $\geqslant 2$ и, следовательно, $(dx)^{\mathfrak{p}}(g_i f^{-i}) = 0$. Положим, далее, $g_1 = \sum_{k=0}^{d-1} a_k x^k$; тогда разность $xg_1 - a_{d-1} f$ либо равна 0, либо имеет степень $\leqslant d-1$, а значит, $\nu_{\mathfrak{p}(\infty)}(g_1 f^{-1} - a_{d-1} x^{-1}) \geqslant 2$. Отсюда следует, что $(dx)^{\mathfrak{p}}(g_1 f^{-1}) = -(dx)^{\mathfrak{p}(\infty)}(a_{d-1} x^{-1}) = a_{d-1}$. Таким образом, мы получили следующий результат.

Лемма 1. *Пусть f — неприводимый многочлен из кольца $K[x]$ степени d, старший коэффициент которого равен 1, и пусть $\mathfrak{p}$ — соответствующая этому многочлену точка поля $K\langle x\rangle$. Допустим, что элемент $u \in K\langle x\rangle$ представлен в указанном выше виде* (1), *где $\nu_{\mathfrak{p}}(v) \geqslant 0$, а $g_1, \ldots, g_r$ — многочлены из $K[x]$ степени $< d$. Тогда $(dx)^{\mathfrak{p}}(u)$ равно коэффициенту при x^{d-1} многочлена g_1.*

Рассмотрим простейший случай, когда $d = 1$, т. е. $f = x - a$, $a \in K$. В этом случае $\mathfrak{p}$-адическое пополнение поля $K\langle x\rangle$ можно отождествить с полем формальных степенных рядов от $x - a$ с коэффициентами из K (§ 3 гл. III).

Наш результат для этого случая может быть сформулирован следующим образом.

Лемма 2. *Пусть $\mathfrak{p}$ — нуль элемента $x-a$ в поле $K\langle x\rangle$, где $a\in K$. Если $y=\sum_{k=r}^{\infty} c_k(x-a)^k$ $(c_k\in K,\ r\leqslant k<\infty)$ есть произвольный элемент из $\mathfrak{p}$-адического пополнения поля $K\langle x\rangle$, то $(dx)^{\mathfrak{p}}(y)=c_{-1}$.*

Рассмотрим детальнее случай, когда точка $\mathfrak{p}$ такова, что ее поле вычетов Σ сепарабельно над K (а степень $\mathfrak{p}$ не обязательно равна 1). Для этого случая мы рассмотрим распределение $\mathfrak{x}$, для которого $\nu_{\mathfrak{p}}(\mathfrak{x})\geqslant -1$, и дадим другую формулу для $(dx)^{\mathfrak{p}}(\mathfrak{x})$. Если ξ есть значение, принимаемое элементом x в точке $\mathfrak{p}$, то $\Sigma=K\langle\xi\rangle$ и ξ является корнем уравнения $f(X)=0$. Так как элемент ξ сепарабелен над K, то $f'(\xi)\neq 0$ (f' обозначает производную от многочлена f). С другой стороны, так как $\nu_{\mathfrak{p}}(\mathfrak{x})\geqslant -1$, то $\nu_{\mathfrak{p}}(f\mathfrak{x}(\mathfrak{p}))\geqslant 0$. Обозначим через φ класс вычетов элемента $f\mathfrak{x}(\mathfrak{p})$ по модулю $\mathfrak{p}$. Принимая эти обозначения, мы докажем сейчас, что

$$(dx)^{\mathfrak{p}}(\mathfrak{x})=\mathrm{Sp}_{\Sigma/K}\frac{\varphi}{f'(\xi)}. \tag{2}$$

Положим $\mathfrak{x}(\mathfrak{p})=\frac{g(x)}{f(x)}+v$, где g — многочлен степени $<d$ и $\nu_{\mathfrak{p}}(v)\geqslant 0$; тогда φ будет равно $g(\xi)$. С другой стороны, по лемме 1, $(dx)^{\mathfrak{p}}(\mathfrak{x})$ равно коэффициенту при x^{d-1} в многочлене $g(x)$. Формула (2) непосредственно вытекает теперь из следующей леммы.

Лемма 3. *Пусть поле Σ получено из поля K присоединением элемента $\xi\neq 0$, который алгебраичен и сепарабелен над K. Обозначим через $f(X)$ характеристический многочлен элемента ξ относительно K, а через d — его степень. Тогда имеем*

$$\mathrm{Sp}_{\Sigma/K}\frac{\xi^k}{f'(\xi)}=0 \quad \text{при } 0\leqslant k<d-1; \quad \mathrm{Sp}_{\Sigma/K}\frac{\xi^{d-1}}{f'(\xi)}=1.$$

В подходящем расширении поля Σ уравнение $f(X)=0$ имеет d различных корней $\xi_1=\xi, \ldots, \xi_d$. Положим

$$g_i(X)=\frac{f(X)}{(X-\xi_i)f'(\xi_i)} \qquad (1\leqslant i\leqslant d).$$

Тогда степень многочлена g_i равна $d-1$, кроме того $g_i(\xi_i)=1$, $g_i(\xi_j)=0$ при $j\neq i$. Пусть $0\leqslant k\leqslant d-1$; многочлен $h_k(X)=\sum_{i=1}^{d}\xi_i^k g_i(X)$ имеет степень $\leqslant d-1$ и $h_k(\xi_i)=\xi_i^k$ при $1\leqslant i\leqslant d$, откуда следует, что $h_k(X)=X^k$. Полагая $X=0$, получим

$$f(0)\,\mathrm{Sp}_{\Sigma/K}\frac{\xi^{k-1}}{f'(\xi)}=\begin{cases}-1, & \text{если } k=0;\\ 0, & \text{если } 1\leqslant k\leqslant d-1.\end{cases}$$

Если $f(X)=X^d+\sum_{k=1}^{d}a_kX^{d-k}$, то $f(0)=a_d$ и $\xi^{d-1}=-\sum_{k=1}^{d}a_k\xi^{d-k-1}$, откуда $\mathrm{Sp}_{\Sigma/K}\frac{\xi^{d-1}}{f'(\xi)}=1$. Лемма 1 и, следовательно, формула (2) доказаны.

Чтобы завершить изучение дифференциала dx, мы должны рассмотреть еще его $\mathfrak{p}(\infty)$-компоненту $(dx)^{\mathfrak{p}(\infty)}$. Каждый элемент u из $K\langle x\rangle$ можно представить в виде

$$u=\sum_{k=0}^{r}a_kx^k+a_{-1}x^{-1}+v, \tag{3}$$

где $a_{-1}, a_0, \ldots, a_r$ принадлежат K, а v удовлетворяет условию $\nu_{\mathfrak{p}(\infty)}(v)\geqslant 2$. Утверждаем, что если $k\geqslant 0$, то $(dx)^{\mathfrak{p}(\infty)}(x^k)=0$. Действительно, мы имеем $(dx)^{\mathfrak{p}(\infty)}(x^k)=-\sum_{\mathfrak{p}}(dx)^{\mathfrak{p}}(x^k)$, где суммирование ведется по всем точкам $\mathfrak{p}\neq\mathfrak{p}(\infty)$. Каждая из этих точек не является полюсом ни элемента x, ни дифференциала dx, поэтому для любой из них мы имеем $(dx)^{\mathfrak{p}}(x^k)=0$, и наше утверждение доказано. Вспоминая, что $(dx)^{\mathfrak{p}(\infty)}(x^{-1})=-1$ и $\mathfrak{d}(dx)=(\mathfrak{p}(\infty))^{-2}$, мы получаем:

Лемма 4. *Если элемент u из поля $K\langle x\rangle$ представлен в виде* (3), *где $\nu_{\mathfrak{p}(\infty)}(v)\geqslant 2$, то $(dx)^{\mathfrak{p}(\infty)}(u)=-a_{-1}$.*

§ 2. След и коснед дифференциалов

Пусть R — поле алгебраических функций от одной переменной и S — расширение поля R конечной степени. Поле S мы также можем рассматривать как поле алгебраических функций от одной переменной. Каждому дифференциалу Ω

поля S мы сейчас сопоставим некоторый дифференциал ω поля R. Обозначим через K и L поля констант полей R и S соответственно. Для любого распределения $\mathfrak{x}$ в поле R положим $\omega(\mathfrak{x}) = \mathrm{Sp}_{L/K}\Omega(\mathrm{Cosp}_{R/S}\mathfrak{x})$. Ясно, что определенная таким образом функция ω линейна. Если $\mathfrak{x} = x_R$, где $x \in R$, то $\mathrm{Cosp}_{R/S}\mathfrak{x} = x_S$, откуда $\omega(\mathfrak{x}) = 0$ (см. § 7 гл. IV; напомним, что x_R и x_S являются главными распределениями, соответствующими элементу x в полях R и S соответственно). Если $\Omega = 0$, то $\omega = 0$, и, значит, ω в этом случае есть дифференциал. Пусть $\Omega \neq 0$ и пусть $\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{a(\mathfrak{P})}$ есть дивизор дифференциала Ω. Пусть $\mathfrak{p}$ — точка поля R, $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$, и e_i — индекс разветвления точки $\mathfrak{P}_i$ относительно R $(1 \leqslant i \leqslant h)$. Обозначим через $a'(\mathfrak{p})$ наибольшее целое число такое, что $e_i a'(\mathfrak{p}) \leqslant a(\mathfrak{P}_i)$ $(1 \leqslant i \leqslant h)$. Ясно, что $a'(\mathfrak{p}) = 0$ почти для всех точек $\mathfrak{p}$ и, следовательно, $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a'(\mathfrak{p})}$ есть дивизор поля R. Пусть $\mathfrak{x}$ есть произвольное распределение поля R, которое $\equiv 0 \pmod{\mathfrak{a}^{-1}}$. Тогда для каждой точки $\mathfrak{p}$ поля R мы имеем $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p})) \geqslant -a'(\mathfrak{p})$, откуда $\nu_{\mathfrak{P}}((\mathrm{Cosp}_{R/S}\mathfrak{x})(\mathfrak{P})) \geqslant -ea'(\mathfrak{p}) \geqslant$ $\geqslant -a(\mathfrak{P})$, где $\mathfrak{P}$ — любая точка поля S, лежащая над $\mathfrak{p}$, а e — ее индекс разветвления относительно R. Отсюда следует, что $\Omega(\mathrm{Cosp}_{R/S}\mathfrak{x}) = 0$, а значит, и $\omega(\mathfrak{x}) = 0$. Этим доказано, что ω есть дифференциал поля R. Этот дифференциал ω мы будем называть *следом дифференциала* Ω (из S в R) и обозначать через $\mathrm{Sp}_{S/R}\Omega$.

Очевидно, что если Ω и Ω' — дифференциалы поля S, то

$$\mathrm{Sp}_{S/R}(\Omega + \Omega') = \mathrm{Sp}_{S/R}\Omega + \mathrm{Sp}_{S/R}\Omega'. \tag{1}$$

Далее, если $x \in R$, то

$$\mathrm{Sp}_{S/R}\, x\Omega = x\, \mathrm{Sp}_{S/R}\Omega. \tag{2}$$

Действительно, пусть $\mathfrak{x}$ — произвольное распределение в поле R. Тогда $(\mathrm{Sp}_{S/R}\, x\Omega)(\mathfrak{x}) = \mathrm{Sp}_{L/K}((x\Omega)(\mathrm{Cosp}_{R/S}\mathfrak{x})) =$ $= \mathrm{Sp}_{L/K}(\Omega(\mathrm{Cosp}_{R/S}\, x\mathfrak{x})) = (\mathrm{Sp}_{S/R}\Omega)(x\mathfrak{x})$, и формула (2) доказана.

Если T есть промежуточное поле между R и S, то

$$\mathrm{Sp}_{S/R}\Omega = \mathrm{Sp}_{T/R}(\mathrm{Sp}_{S/T}\Omega). \tag{3}$$

В самом деле, пусть M — поле констант поля T, а $\mathfrak{x}$ — произвольное распределение в R. В силу леммы 3 § 7 гл. IV имеем

$$\begin{aligned}(\mathrm{Sp}_{T/R}(\mathrm{Sp}_{S/T}\Omega))(\mathfrak{x}) &= \mathrm{Sp}_{M/K}((\mathrm{Sp}_{S/T}\Omega)(\mathrm{Cosp}_{R/T}\mathfrak{x})) = \\ &= \mathrm{Sp}_{M/K}(\mathrm{Sp}_{L/M}(\Omega(\mathrm{Cosp}_{T/S}(\mathrm{Cosp}_{R/T}\mathfrak{x})))) = \\ &= \mathrm{Sp}_{L/K}(\Omega(\mathrm{Cosp}_{R/S}\mathfrak{x})) = (\mathrm{Sp}_{S/R}\Omega)(\mathfrak{x}),\end{aligned}$$

и наша формула доказана.

Теорема 1. *Пусть R и S — поля алгебраических функций от одной переменной, причем S является расширением поля R конечной степени. Пусть Ω есть дифференциал поля S, а $\mathfrak{p}$ — точка поля R. Обозначим через $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ все различные точки поля S, лежащие над $\mathfrak{p}$, через K и L — поля констант полей R и S соответственно через $\Sigma_s(\mathfrak{p})$ — поле сепарабельных над K элементов поля вычетов точки $\mathfrak{p}$ и через $\Sigma_s(\mathfrak{P}_i)$ — поле сепарабельных над L элементов поля вычетов точки $\mathfrak{P}_i$ $(1 \leqslant i \leqslant h)$. Тогда имеет место формула*

$$\mathrm{res}_{\mathfrak{p}}\,\mathrm{Sp}_{S/R}\,\Omega = \sum_{i=1}^{h} \mathrm{Sp}_{\Sigma_s(\mathfrak{P}_i)/\Sigma_s(\mathfrak{p})}\,\mathrm{res}_{\mathfrak{P}_i}\,\Omega.$$

Замечание. В этой теореме, как обычно (см. § 1 гл. IV), мы предполагаем, что K содержится в L, поэтому поле $\Sigma_s(\mathfrak{p})$ содержится в $\Sigma_s(\mathfrak{P}_i)$.

Пусть γ — произвольный элемент из $\Sigma_s(\mathfrak{p})$, а $\bar{\gamma}$ — элемент из $\mathfrak{p}$-адического пополнения поля R, который алгебраичен над K и принадлежит классу вычетов γ по модулю $\mathfrak{p}$ (см. теорему 1 § 3 гл. III). Обозначим через α и β соответственно левую и правую части формулы, которую мы должны доказать. Тогда $\mathrm{Sp}_{\Sigma_s(\mathfrak{p})/K}\alpha\gamma = (\mathrm{Sp}_{S/R}\Omega)(\mathfrak{c})$, где $\mathfrak{c}$ — распределение поля R, принимающее значение $\bar{\gamma}$ в точке $\mathfrak{p}$ и 0 — во всех других точках. По определению следа, это равно $\mathrm{Sp}_{L/K}(\Omega(\mathrm{Cosp}_{R/S}\mathfrak{c})) = \sum_{i=1}^{h} \mathrm{Sp}_{L/K}(\Omega^{\mathfrak{P}_i}(\bar{\gamma}))$. Так как элемент $\bar{\gamma}$ алгебраичен над L и принадлежит классу вычетов γ по модулю $\mathfrak{P}_i$, то $\Omega^{\mathfrak{P}_i}(\bar{\gamma}) = \mathrm{Sp}_{\Sigma_s(\mathfrak{P}_i)/L}\,\gamma\,\mathrm{res}_{\mathfrak{P}_i}\Omega$, откуда

$$\begin{aligned}\mathrm{Sp}_{L/K}\Omega^{\mathfrak{P}_i}(\bar{\gamma}) &= \mathrm{Sp}_{\Sigma_s(\mathfrak{P}_i)/K}\gamma\,\mathrm{res}_{\mathfrak{P}_i}\Omega = \\ &= \mathrm{Sp}_{\Sigma_s(\mathfrak{p})/K}(\gamma\,\mathrm{Sp}_{\Sigma_s(\mathfrak{P}_i)/\Sigma_s(\mathfrak{p})}\,\mathrm{res}_{\mathfrak{P}_i}\Omega).\end{aligned}$$

Таким образом, мы видим, что $\mathrm{Sp}_{\Sigma_s(\mathfrak{p})/K}\alpha\gamma = \mathrm{Sp}_{\Sigma_s(\mathfrak{p})/K}\beta\gamma$. Так как это верно при любом $\gamma \in \Sigma_s(\mathfrak{p})$, то по лемме 1 § 5 гл. III получаем, что $\alpha = \beta$. Теорема 1, таким образом, доказана.

Пользуясь понятием коследа для распределений, мы ввели только что понятие следа дифференциала. Обратно, используя понятие следа для распределений, мы дадим определение коследа дифференциала. Однако сейчас пока мы ограничимся случаем пары полей алгебраических функций от одной переменной, имеющих одно и то же поле констант. В случае, когда поля констант различны, понятие коследа мы сможем ввести только после определения точных дифференциалов в произвольном поле алгебраических функций от одной переменной.

Итак, пусть R и S — поля алгебраических функций от одной переменной, удовлетворяющие условиям: R является подполем поля S и оба поля имеют одно и то же поле констант K. Ясно, что тогда S имеет конечную степень над R. Для любого дифференциала ω поля R положим

$$\Omega(\mathfrak{y}) = \omega\left(\mathrm{Sp}_{S/R}\,\mathfrak{y}\right).$$

Очевидно, что Ω является линейной функцией на пространстве распределений $\mathfrak{y}$ поля S. Докажем, что Ω — дифференциал. Если $\mathfrak{y}$ есть главное распределение y_S, соответствующее элементу y поля S, то $\mathrm{Sp}_{S/R}\,\mathfrak{y} = (\mathrm{Sp}_{S/R}\,y)_R$, откуда $\Omega(y_S) = 0$. Если S несепарабельно над R, то, как мы видели в § 7 гл. IV, $\mathrm{Sp}_{S/R}\,\mathfrak{y} = 0$ для любого распределения $\mathfrak{y}$ в S, а значит, $\Omega = 0$. Предположим теперь, что S сепарабельно над R и что $\omega \neq 0$; через $\mathfrak{d}(\omega)$, как обычно, мы обозначаем дивизор дифференциала ω. Пусть $\mathfrak{P}$ — произвольная точка поля S, а $\mathfrak{p}$ — точка поля R, лежащая под $\mathfrak{P}$. Обозначим через $a(\mathfrak{p})$ показатель, с которым $\mathfrak{p}$ входит в $\mathfrak{d}(\omega)$, через $e(\mathfrak{P})$ — индекс разветвления точки $\mathfrak{P}$ относительно R и через $m(\mathfrak{P})$ — $\mathfrak{P}$-показатель дифференты поля S относительно R. Для произвольного элемента u из $\mathfrak{P}$-адического пополнения $\bar{S}$ поля S мы имеем[1]) $\Omega^{\mathfrak{P}}(u) = \omega^{\mathfrak{p}}\left(\mathrm{Sp}_{\bar{S}/\bar{R}}\,u\right)$, где $\bar{R}$ обо-

---

[1]) Под $\Omega^{\mathfrak{P}}(u)$ следует понимать $\Omega(u^{\mathfrak{P}})$, где $u^{\mathfrak{P}}$ есть распределение поля S, принимающее в точке $\mathfrak{P}$ значение u, а во всех других точках — 0. (*Прим. перев.*)

значает $\mathfrak{p}$-адическое пополнение поля R. Пусть t — униформизирующая переменная в точке $\mathfrak{p}$ поля R. Если $\nu_{\mathfrak{P}}(u) \geqslant -e(\mathfrak{P})\,a(\mathfrak{p}) - m(\mathfrak{P})$, то $\nu_{\mathfrak{P}}(t^{a(\mathfrak{p})}u) \geqslant -m(\mathfrak{P})$, откуда $\nu_{\mathfrak{p}}(\mathrm{Sp}_{\bar{S}/\bar{R}}\, t^{a(\mathfrak{p})}u) \geqslant 0$; таким образом, $\nu_{\mathfrak{p}}(\mathrm{Sp}_{\bar{S}/\bar{R}}\, u) \geqslant -a(\mathfrak{p})$ и, следовательно, $\Omega^{\mathfrak{P}}(u) = 0$. С другой стороны, в поле $\bar{S}$ существует такой элемент z, что $\nu_{\mathfrak{P}}(z) = -m(\mathfrak{P}) - 1$ и $\nu_{\mathfrak{p}}(\mathrm{Sp}_{\bar{S}/\bar{R}}\, z) < 0$. Так как $\nu_{\mathfrak{P}}(tz) \geqslant -m(\mathfrak{P})$, то $\nu_{\mathfrak{p}}(t\,\mathrm{Sp}_{\bar{S}/\bar{R}}\, z) \geqslant 0$, откуда $\nu_{\mathfrak{p}}(\mathrm{Sp}_{\bar{S}/\bar{R}}\, z) = -1$. Точка $\mathfrak{p}$ входит в $\mathfrak{d}(\omega)$ с показателем $a(\mathfrak{p})$, поэтому в поле R можно найти такой элемент w, что $\nu_{\mathfrak{p}}(w) = -a(\mathfrak{p}) - 1$ и $\omega^{\mathfrak{p}}(w) \neq 0$. Легко видеть, что тогда $\nu_{\mathfrak{P}}\left(wz\left(\mathrm{Sp}_{\bar{S}/\bar{R}}\, z\right)^{-1}\right) = -e(\mathfrak{P})\,a(\mathfrak{p}) - m(\mathfrak{P}) - 1$ и $\Omega^{\mathfrak{P}}\left(wz\left(\mathrm{Sp}_{\bar{S}/\bar{R}}\, z\right)^{-1}\right) = \omega^{\mathfrak{p}}(w) \neq 0$. Пусть $\mathfrak{D}$ есть дифферента поля S относительно R, тогда число $e(\mathfrak{P})\,a(\mathfrak{p}) + m(\mathfrak{P})$ является показателем, с которым $\mathfrak{P}$ входит в дивизор $\mathfrak{D}\,\mathrm{Con}_{R/S}\,\mathfrak{d}(\omega)$. Таким образом, является поле S сепарабельным над R или нет, в обоих случаях функция Ω есть дифференциал поля S, при этом, если S сепарабельно над R, то дивизор дифференциала Ω равен $\mathfrak{D}\,\mathrm{Con}_{R/S}\,\mathfrak{d}(\omega)$.

Дифференциал Ω называется *коследом дифференциала* ω *из* R *в* S и обозначается через $\mathrm{Cosp}_{R/S}\,\omega$. Сформулируем полученный результат.

Теорема 2. *Пусть R и S — поля алгебраических функций от одной переменной, причем S является расширением поля R и оба поля имеют одно и то же поле констант. Пусть ω — дифференциал поля R, отличный от 0. Если S несепарабельно над R, то $\mathrm{Cosp}_{R/S}\,\omega = 0$. Если S сепарабельно над R, то $\mathrm{Cosp}_{R/S}\,\omega$ есть дифференциал поля S, отличный от 0, дивизор которого равен $\mathfrak{D}\,\mathrm{Con}_{R/S}\,\mathfrak{d}(\omega)$, где $\mathfrak{D}$ — дифферента поля S относительно R.*

Следствие 1. *Пусть сохраняются обозначения теоремы 2. Тогда коследа из R в S любого дифференциала первого рода поля R есть дифференциал первого рода поля S.*

Следствие 2. *Сохраняя обозначения теоремы 2, предположим, что S сепарабельно над R. Если g есть род поля R, а G — род поля S, то $G - 1 = [S : R]\,(g - 1) + \frac{1}{2}\,d(\mathfrak{D})$.*

Действительно, по теореме 6 § 6 гл. II мы имеем

$$2G-2=d\left(\mathfrak{d}\left(\mathrm{Cosp}_{R/S}\,\omega\right)\right)=d\left(\mathrm{Con}_{R/S}\,\mathfrak{d}(\omega)\right)+d(\mathfrak{D}),$$

а в силу леммы 1 § 7 гл. IV это равно $[S:R](2g-2)+d(\mathfrak{D})$.

Следствие 3 (теорема Люрота). *Пусть поле R имеет вид $K\langle x\rangle$, где K — поле, а элемент x трансцендентен над K. Если T есть промежуточное поле между K и R, отличное от K, то в T существует такой элемент t, что $T=K\langle t\rangle$.*

Ясно, что R алгебраично над T. Пусть U есть поле тех элементов из R, которые сепарабельны над T. Если $U\neq R$, то поле R имеет характеристику $p\neq 0$, и степень элемента x над U равна p^n при некотором n. Так как x чисто несепарабелен над U, то $x^{p^n}\in U$. С другой стороны, дивизор полюсов элемента x^{p^n} имеет степень p^n; следовательно, $[R:K\langle x^{p^n}\rangle]=p^n$ (следствие к теореме 4 § 8 гл. I). Но $[R:U]\geqslant p^n$ и $K\langle x^{p^n}\rangle\subset U$, поэтому $U=K\langle x^{p^n}\rangle$, и род поля U равен 0. Применяя следствие 2 к полям T и U (вместо R и S) и замечая, что дифферента поля U относительно T есть целый дивизор, мы получаем $-1\geqslant[U:T](g-1)$, где g — род поля T. Отсюда следует, что $g=0$. Так как поле R имеет точку степени 1, то поле T, очевидно, также имеет точку степени 1, а значит, T есть чисто трансцендентное расширение поля K (см. § 2 гл. II).

Пусть R и S — поля алгебраических функций от одной переменной, причем поле S является расширением поля R и оба поля имеют одно и то же поле констант. Очевидно, что для любых дифференциалов ω и ω' поля R имеем

$$\mathrm{Cosp}_{R/S}(\omega+\omega')=\mathrm{Cosp}_{R/S}\,\omega+\mathrm{Cosp}_{R/S}\,\omega'. \tag{4}$$

Далее, если x — элемент из R, то

$$\mathrm{Cosp}_{R/S}\,x\omega=x\,\mathrm{Cosp}_{R/S}\,\omega. \tag{5}$$

В самом деле, пусть $\mathfrak{y}$ — произвольное распределение в S. Тогда

$$\left(\mathrm{Cosp}_{R/S}\,x\omega\right)(\mathfrak{y})=(x\omega)\left(\mathrm{Sp}_{S/R}\,\mathfrak{y}\right)=\omega\left(x\,\mathrm{Sp}_{S/R}\,\mathfrak{y}\right)=$$
$$=\omega\left(\mathrm{Sp}_{S/R}\,x\mathfrak{y}\right)=\left(\mathrm{Cosp}_{R/S}\,\omega\right)(x\mathfrak{y})=\left(x\,\mathrm{Cosp}_{R/S}\,\omega\right)(\mathfrak{y}),$$

что и доказывает наше утверждение. Если теперь T — промежуточное поле между R и S, то

$$\mathrm{Cosp}_{R/S}\,\omega = \mathrm{Cosp}_{T/S}(\mathrm{Cosp}_{R/T}\,\omega). \tag{6}$$

Действительно, если $\mathfrak{y}$ — распределение в S, то

$$(\mathrm{Cosp}_{R/S}\,\omega)(\mathfrak{y}) = \omega(\mathrm{Sp}_{S/R}\,\mathfrak{y}) = \omega(\mathrm{Sp}_{T/R}(\mathrm{Sp}_{S/T}\,\mathfrak{y})) =$$
$$= (\mathrm{Cosp}_{R/T}\,\omega)(\mathrm{Sp}_{S/T}\,\mathfrak{y}) = (\mathrm{Cosp}_{T/S}(\mathrm{Cosp}_{R/T}\,\omega))(\mathfrak{y}),$$

и формула (6) доказана.

Если ω — дифференциал поля R и $z \in S$, то

$$\mathrm{Sp}_{S/R}(z\,\mathrm{Cosp}_{R/S}\omega) = (\mathrm{Sp}_{S/R}z)\,\omega. \tag{7}$$

В самом деле, пусть $\mathfrak{x}$ — распределение в R. Тогда

$$(\mathrm{Sp}_{S/R}(z\,\mathrm{Cosp}_{R/S}\omega))(\mathfrak{x}) = (z\,\mathrm{Cosp}_{R/S}\omega)(\mathrm{Cosp}_{R/S}\mathfrak{x}) =$$
$$= (\mathrm{Cosp}_{R/S}\omega)(z\,\mathrm{Cosp}_{R/S}\mathfrak{x}) = \omega(\mathrm{Sp}_{S/R}(z\,\mathrm{Cosp}_{R/S}\mathfrak{x})),$$

а это по формуле (1) § 7 гл. IV равно

$$\omega((\mathrm{Sp}_{S/R}z)\,\mathfrak{x}) = ((\mathrm{Sp}_{S/R}z)\,\omega)(\mathfrak{x}),$$

и равенство (7) доказано.

Теорема 3. *Пусть R и S — поля алгебраических функций от одной переменной, причем R является подполем поля S и оба поля имеют одно и то же поле констант. Обозначим через ω дифференциал поля R, через $\mathfrak{p}$ — точку поля R и через $\mathfrak{P}$ — точку поля S, лежащую над $\mathfrak{p}$. Пусть e — индекс разветвления точки $\mathfrak{P}$ относительно R. Если поле вычетов точки $\mathfrak{P}$ несепарабельно над полем вычетов точки $\mathfrak{p}$, то $\mathrm{res}_{\mathfrak{P}}\mathrm{Cosp}_{R/S}\omega = 0$. Если же поле вычетов точки $\mathfrak{P}$ сепарабельно над полем вычетов точки $\mathfrak{p}$, то $\mathrm{res}_{\mathfrak{P}}\mathrm{Cosp}_{R/S}\omega = e\,\mathrm{res}_{\mathfrak{p}}\omega$.*

Обозначим через $\Sigma(\mathfrak{p})$ и $\Sigma(\mathfrak{P})$ поля вычетов точек $\mathfrak{p}$ и $\mathfrak{P}$ соответственно, а через $\Sigma_s(\mathfrak{p})$ и $\Sigma_s(\mathfrak{P})$ — наибольшие подполя полей $\Sigma(\mathfrak{p})$ и $\Sigma(\mathfrak{P})$ соответственно, которые сепарабельны над общим полем констант K полей R и S. По-

строим $\mathfrak{p}$-адическое пополнение $\bar{R}$ поля R и $\mathfrak{P}$-адическое пополнение $\bar{S}$ поля S; мы можем считать, что $\bar{R}$ является подполем поля $\bar{S}$. Пусть $\bar{\Sigma}_s(\mathfrak{p})$ и $\bar{\Sigma}_s(\mathfrak{P})$ — подполя полей $\bar{R}$ и $\bar{S}$ соответственно, которые содержат K и которые являются системами представителей для $\Sigma_s(\mathfrak{p})$ и $\Sigma_s(\mathfrak{P})$ (см. теорему 1 § 3 гл. III). Дифференциал $\mathrm{Cosp}_{R/S}\omega$ обозначим через Ω. Пусть u — произвольный элемент из $\Sigma_s(\mathfrak{P})$. Если $\bar{u} \in \bar{\Sigma}_s(\mathfrak{P})$ — представитель класса u, то $\Omega^{\mathfrak{P}}(\bar{u}) = \mathrm{Sp}_{\Sigma_s(\mathfrak{P})/K} u \operatorname{res}_{\mathfrak{P}} \Omega$. По определению коследа дифференциала это также равно $\omega^{\mathfrak{p}}\left(\mathrm{Sp}_{\bar{S}/\bar{R}} \bar{u}\right)$. Теперь, элемент $\bar{u}$ алгебраичен над K, а значит, и над $\bar{R}$. Элементы, сопряженные с $\bar{u}$ относительно $\bar{R}$ (в надлежащем нормальном расширении поля $\bar{R}$), сопряжены с $\bar{u}$ и относительно K, а потому они алгебраичны и сепарабельны над K. Отсюда следует, что элемент $\mathrm{Sp}_{\bar{S}/\bar{R}} \bar{u}$ алгебраичен и сепарабелен над K, а значит, он содержится в $\bar{\Sigma}_s(\mathfrak{p})$. Как мы знаем, класс вычетов элемента $\mathrm{Sp}_{\bar{S}/\bar{R}} \bar{u}$ равен $e\mathrm{Sp}_{\Sigma(\mathfrak{P})/\Sigma(\mathfrak{p})} u$ [см. формулу (1) § 8 гл. IV]. Если $\Sigma(\mathfrak{P})$ несепарабельно над $\Sigma(\mathfrak{p})$, то этот класс вычетов равен 0; значит, в этом случае $\mathrm{Sp}_{\bar{S}/\bar{R}} \bar{u} = 0$ и $\Omega^{\mathfrak{P}}(\bar{u}) = 0$ при любом $u \in \Sigma_s(\mathfrak{P})$, откуда $\operatorname{res}_{\mathfrak{P}} \Omega = 0$. Предположим теперь, что поле $\Sigma(\mathfrak{P})$ сепарабельно над $\Sigma(\mathfrak{p})$. Пусть f — степень поля $\Sigma(\mathfrak{P})$ над $\Sigma(\mathfrak{p})$, и пусть $\bar{K}$ — алгебраически замкнутое расширение поля K, содержащее $\Sigma(\mathfrak{P})$. Как известно, существует f различных изоморфизмов поля $\Sigma(\mathfrak{P})$ в $\bar{K}$, тождественных на $\Sigma(\mathfrak{p})$. Так как $\Sigma(\mathfrak{P})$ чисто несепарабельно над $\Sigma_s(\mathfrak{P})$, то эти изоморфизмы индуцируют f различных изоморфизмов поля $\Sigma_s(\mathfrak{P})$ в $\bar{K}$, тождественных на $\Sigma_s(\mathfrak{p})$. Обратно, всякий изоморфизм поля $\Sigma_s(\mathfrak{P})$ в $\bar{K}$, тождественный на $\Sigma_s(\mathfrak{p})$, может быть продолжен до изоморфизма поля $\Sigma(\mathfrak{P})$, а так как $\Sigma(\mathfrak{p})$ чисто несепарабельно над $\Sigma_s(\mathfrak{p})$, то продолженный изоморфизм на $\Sigma(\mathfrak{p})$ совпадает с тождественным. Таким образом, в рассматриваемом случае мы имеем $[\Sigma(\mathfrak{P}) : \Sigma(\mathfrak{p})] = [\Sigma_s(\mathfrak{P}) : \Sigma_s(\mathfrak{p})]$ и

$$\mathrm{Sp}_{\Sigma(\mathfrak{P})/\Sigma(\mathfrak{p})} u = \mathrm{Sp}_{\Sigma_s(\mathfrak{P})/\Sigma_s(\mathfrak{p})} u.$$

Отсюда следует, что $\mathrm{Sp}_{\Sigma_s(\mathfrak{P})/K}\, u \operatorname{res}_{\mathfrak{P}}\Omega = e\omega^{\mathfrak{p}}(\bar{v})$, где $\bar{v}$ — представитель класса $\mathrm{Sp}_{\Sigma_s(\mathfrak{P})/\Sigma_s(\mathfrak{p})}\, u$ из $\bar{\Sigma}_s(\mathfrak{p})$. Но

$$\omega^{\mathfrak{p}}(\bar{v}) = \mathrm{Sp}_{\Sigma_s(\mathfrak{p})/K}\left(\left(\mathrm{Sp}_{\Sigma_s(\mathfrak{P})/\Sigma_s(\mathfrak{p})} u\right) \operatorname{res}_{\mathfrak{p}}\omega\right) = \mathrm{Sp}_{\Sigma_s(\mathfrak{P})/K}\, u \operatorname{res}_{\mathfrak{p}}\omega,$$

поэтому $\Omega^{\mathfrak{P}}(\bar{u}) = \mathrm{Sp}_{\Sigma_s(\mathfrak{P})/K} u\,(e \operatorname{res}_{\mathfrak{p}}\omega)$, откуда $\operatorname{res}_{\mathfrak{P}}\Omega = e \operatorname{res}_{\mathfrak{p}}\omega$. Теорема 3, таким образом, доказана.

§ 3. Дифференциал dx в произвольном поле

Теперь мы уже можем каждому элементу x поля R алгебраических функций от одной переменной поставить в соответствие некоторый дифференциал поля R. Этот дифференциал будем обозначать через $(dx)_R$ или, если рассматривается только одно поле R, — через dx.

Пусть K — поле констант поля R. Если элемент x не принадлежит K, то он трансцендентен над K; согласно § 1 в поле $K\langle x\rangle$ определен дифференциал $(dx)_{K\langle x\rangle}$. Полагаем в этом случае

$$(dx)_R = \mathrm{Cosp}_{K\langle x\rangle/R}\,(dx)_{K\langle x\rangle}.$$

Ясно, что в случае, когда $R = K\langle x\rangle$, это определение не противоречит предыдущему. Если x — элемент из K, то положим $(dx)_R$ равным нулевому дифференциалу. Всякий дифференциал поля R, имеющий вид $(dx)_R$ (при некотором $x \in R$), будем называть *точным дифференциалом*.

Теорема 4. *Пусть R — поле алгебраических функций от одной переменной и K — его поле констант. Если R не является сепарабельно порождаемым, то каждый точный дифференциал поля R равен 0. Если R сепарабельно порождаемо и $x \in R$, то дифференциал $(dx)_R$ отличен от 0 тогда и только тогда, если x есть сепарабельно порождающая переменная поля R.*

Пусть x — произвольный элемент из R. Если поле R не алгебраично над $K\langle x\rangle$, то x принадлежит K и, значит, $(dx)_R = 0$. Если R алгебраично над $K\langle x\rangle$, то, по теореме 2, дифференциал $(dx)_R$ отличен от 0 тогда и только тогда, если поле R сепарабельно над $K\langle x\rangle$.

Теорема 5. *Все вычеты точного дифференциала поля R алгебраических функций от одной переменной равны 0. Если поле R имеет характеристику $p>0$ и $x\in R$, то для любого целого $m>0$ все вычеты дифференциала $x^{pm-1}(dx)_R$ равны 0. Пусть K — поле констант поля R и $\mathfrak{p}$ — точка поля R. Тогда для элемента $x\neq 0$ из R вычет $\operatorname{res}_{\mathfrak{p}} x^{-1}(dx)_R$ равен 0, если поле вычетов точки $\mathfrak{p}$ несепарабельно над K, и равен $\nu_{\mathfrak{p}}(x)$, если поле вычетов точки $\mathfrak{p}$ сепарабельно над K.*

Можно считать, что x не принадлежит K. В силу формулы (5) § 2 мы имеем $x^h(dx)_R=\operatorname{Cosp}_{K\langle x\rangle/R}x^h(dx)_{K\langle x\rangle}$. Пусть $\mathfrak{p}(0)$ и $\mathfrak{p}(\infty)$ — соответственно нуль и полюс элемента x в $K\langle x\rangle$; тогда дифференциал $x^h(dx)_{K\langle x\rangle}$ не имеет полюсов вне точек $\mathfrak{p}(0)$ и $\mathfrak{p}(\infty)$. С другой стороны, степени точек $\mathfrak{p}(0)$ и $\mathfrak{p}(\infty)$ равны 1. Если $c\in K$, то

$$\left(x^h(dx)_{K\langle x\rangle}\right)^{\mathfrak{p}(\infty)}(c)=\left((dx)_{K\langle x\rangle}\right)^{\mathfrak{p}(\infty)}(cx^h).$$

а это, в силу леммы 4 § 1, равно 0, если $h\neq -1$, и равно $-c$, если $h=-1$. Отсюда следует, что вычет $\operatorname{res}_{\mathfrak{p}(\infty)}x^h(dx)_{K\langle x\rangle}$ равен 0, если $h\neq -1$, и равен -1, если $h=-1$. Применяя теорему 3 § 5 гл III, получаем, что вычет $\operatorname{res}_{\mathfrak{p}(0)}x^h(dx)_{K\langle x\rangle}$ равен 0, если $h\neq -1$, и равен 1, если $h=-1$. Теорема 5 непосредственно следует теперь из теоремы 3 § 2.

Лемма 1. *Пусть R — поле алгебраических функций от одной переменной, K — его поле констант и x — элемент из R, не принадлежащий K. Если R сепарабельно над $K\langle x\rangle$, то существует бесконечно много точек поля R, поля вычетов которых сепарабельны над K и которые неразветвлены относительно $K\langle x\rangle$.*

Прежде всего заметим, что существует бесконечно много существенно различных неприводимых многочленов $f(X)$ с коэффициентами из K, для которых $f'(X)\neq 0$. Действительно, если поле K бесконечно, то мы можем взять многочлены $f(X)=X-a$, $a\in K$; если же K конечно, то, как известно, для всякого целого $n>0$ существует неприводимый многочлен степени n с коэффициентами из K; так как поле K совершенно, то производная от этого многочлена отлична от 0. Этим доказано, что существует бесконечно

много точек поля $K\langle x\rangle$, поля вычетов которых сепарабельны над K. Только для конечного числа этих точек $\mathfrak{p}_0$ может существовать точка $\mathfrak{p}$ поля R, лежащая над $\mathfrak{p}_0$, которая либо разветвлена относительно $K\langle x\rangle$, либо имеет поле вычетов, несепарабельное над полем вычетов точки $\mathfrak{p}_0$ (лемма 3 § 8 гл. IV). Лемма 1, таким образом, доказана.

Пусть теперь $\mathfrak{p}$ — точка поля R, которая неразветвлена относительно $K\langle x\rangle$, имеет сепарабельное над K поле вычетов и не является полюсом элемента x. Пусть $f(x)$ есть неприводимый многочлен из $K[x]$, старший коэффициент которого равен 1 и для которого $\mathfrak{p}$ является нулем. Так как точка $\mathfrak{p}$ неразветвлена относительно $K\langle x\rangle$, то $\nu_{\mathfrak{p}}(f)=1$. Пусть $\mathfrak{x}$ — распределение поля R такое, что $\nu_{\mathfrak{p}}(\mathfrak{x}(\mathfrak{p}))\geqslant -1$. Тогда $\nu_{\mathfrak{p}}(f\mathfrak{x}(\mathfrak{p}))\geqslant 0$. Обозначим через φ класс вычетов элемента $f\mathfrak{x}(\mathfrak{p})$ по модулю $\mathfrak{p}$ и докажем следующую формулу:

$$(dx)_R^{\mathfrak{p}}(\mathfrak{x})=\mathrm{Sp}_{\Sigma/K}\frac{\varphi}{f'(\xi)}, \tag{1}$$

где Σ — поле вычетов точки $\mathfrak{p}$, а ξ — класс вычетов элемена x по модулю $\mathfrak{p}$.

Пусть $\mathfrak{x}^{\mathfrak{p}}$ — распределение, принимающее в точке $\mathfrak{p}$ значение $\mathfrak{x}(\mathfrak{p})$, а во всех других точках — значение 0. Тогда $(dx)_R^{\mathfrak{p}}(\mathfrak{x})=(dx)_R(\mathfrak{x}^{\mathfrak{p}})=(dx)_{K\langle x\rangle}\left(\mathrm{Sp}_{R/K\langle x\rangle}\mathfrak{x}^{\mathfrak{p}}\right)$. Пусть $\mathfrak{p}_0$ — точка поля $K\langle x\rangle$, лежащая под $\mathfrak{p}$; ясно, что $\mathfrak{p}_0$-компонента распределения $\mathrm{Sp}_{R/K\langle x\rangle}\mathfrak{x}^{\mathfrak{p}}$ равна $\mathrm{Sp}^{\mathfrak{p}}\mathfrak{x}(\mathfrak{p})$, где $\mathrm{Sp}^{\mathfrak{p}}$ обозначает след из $\mathfrak{p}$-адического пополнения поля R в $\mathfrak{p}_0$-адическое пополнение поля $K\langle x\rangle$. Пусть Σ_0 — поле вычетов точки $\mathfrak{p}_0$, а φ_0 — класс вычетов элемента $f\mathrm{Sp}^{\mathfrak{p}}\mathfrak{x}(\mathfrak{p})$ по модулю $\mathfrak{p}_0$. Применяя формулу (2) § 1, мы получаем

$$(dx)_{K\langle x\rangle}\left(\mathrm{Sp}_{R/K\langle x\rangle}\mathfrak{x}^{\mathfrak{p}}\right)=\mathrm{Sp}_{\Sigma_0/K}\frac{\varphi_0}{f'(\xi)}.$$

С другой стороны, так как точка $\mathfrak{p}$ неразветвлена относительно $K\langle x\rangle$ и $f\,\mathrm{Sp}^{\mathfrak{p}}\mathfrak{x}(\mathfrak{p})=\mathrm{Sp}^{\mathfrak{p}}f\mathfrak{x}(\mathfrak{p})$, то, в силу формулы 1 § 8 гл. IV, $\varphi_0=\mathrm{Sp}_{\Sigma/\Sigma_0}\varphi$. Замечая, что $f'(\xi)\in\Sigma_0$, получаем теперь

$$(dx)_R^{\mathfrak{p}}(\mathfrak{x})=\mathrm{Sp}_{\Sigma_0/K}\left(\mathrm{Sp}_{\Sigma/\Sigma_0}\frac{\varphi}{f'(\xi)}\right)=\mathrm{Sp}_{\Sigma/K}\frac{\varphi}{f'(\xi)},$$

и формула (1) доказана

Рассмотрим несколько подробнее случай, когда степень точки $\mathfrak{p}$ равна 1. В этом случае $f=x-a$, где $a\in K$,

и $\mathfrak{p}$-адическое пополнение $\bar{R}$ поля R может быть отождествлено с полем формальных степенных рядов от $x-a$ с коэффициентами из K; кроме того, поле $\bar{R}$ совпадает с $\mathfrak{p}_0$-адическим пополнением поля $K\langle x\rangle$, а значит, $\mathrm{Sp}^{\mathfrak{p}} y = y$ при всех $y \in \bar{R}$. Из леммы 2 § 1 вытекает теперь следующая теорема.

Теорема 6. *Пусть R — поле алгебраических функций от одной переменной и K — его поле констант. Предположим, что поле R алгебраично и сепарабельно над $K\langle x\rangle$, где x — некоторый элемент из R. Пусть $\mathfrak{p}$ — точка поля R степени 1, которая неразветвлена относительно $K\langle x\rangle$ и не является полюсом элемента x. Обозначим через a значение, принимаемое элементом x в точке $\mathfrak{p}$. Тогда для элемента $u = \sum_{k=r}^{\infty} c_k (x-a)^k$ $(c_k \in K,\ r \leqslant k < \infty,\ r < 0)$ из $\mathfrak{p}$-адического пополнения поля R имеем $(dx)^{\mathfrak{p}}(u) = c_{-1}$.*

Следствие. *Пусть сохраняются обозначения теоремы 6. Если для элемента y из R в $\mathfrak{p}$-адическом пополнении поля R имеем разложение*

$$y = \sum_{k=s}^{\infty} b_k (x-a)^k \quad (b_k \in K,\ s \leqslant k < \infty,\ s < 0),$$

то $\mathrm{res}_{\mathfrak{p}}\, y\, dx = b_{-1}$.

Если c — произвольный элемент из K, то $(y\,dx)^{\mathfrak{p}}(c) = (dx)^{\mathfrak{p}}(cy) = cb_{-1}$, что и доказывает наше утверждение.

Предполагая опять-таки, что R сепарабельно над $K\langle x\rangle$, мы легко можем определить дивизор дифференциала $(dx)_R$. Пусть $\mathfrak{r}$ — полюс элемента x в $K\langle x\rangle$; тогда дивизор дифференциала $(dx)_{K\langle x\rangle}$ равен $\mathfrak{r}^{-2}$, Применяя теорему 2 § 2, мы видим, что $\mathfrak{d}\big((dx)_R\big) = \mathfrak{d}_x \mathfrak{n}^{-2}$, где $\mathfrak{d}_x$ — дифферента поля R относительно $K\langle x\rangle$ и $\mathfrak{n} = \mathrm{Con}_{K\langle x\rangle/R}\mathfrak{r}$. Ясно, что $\mathfrak{n}$ есть дивизор полюсов элемента x. Таким образом, доказана

Теорема 7. *Пусть R — поле алгебраических функций от одной переменной и пусть K — его поле констант. Если поле R алгебраично и сепарабельно над $K\langle x\rangle$, где x — некоторый элемент из R, то дивизор дифференциала dx в поле R равен $\mathfrak{d}_x \mathfrak{n}^{-2}$, где $\mathfrak{d}_x$ — дифферента*

поля R относительно $K\langle x\rangle$, а $\mathfrak{n}$ — дивизор полюсов элемента x.

Следствие. *При выполнении условий теоремы 7 все полюса дифференциала dx находятся среди полюсов элемента x.*

Если поле R алгебраично и сепарабельно над $K\langle x\rangle$, то $dx \neq 0$ и, следовательно, каждый дифференциал ω поля R может быть представлен в виде $u\,dx$, где $u \in R$. С другой стороны, так как R сепарабельно и имеет конечную степень над $K\langle x\rangle$, то $R = K\langle x, y_1\rangle$ при некотором $y_1 \in R$. Характеристический многочлен элемента y_1 относительно $K\langle x\rangle$ имеет вид $Y^n + \sum_{i=1}^{n} \frac{a_i(x)}{a_0(x)} Y^{n-i}$, где $a_0, \ldots, a_n$ — многочлены с коэффициентами из K. Отсюда легко следует, что коэффициенты характеристического многочлена $F(Y)$ элемента $y = a_0(x)\,y_1$ принадлежат $K[x]$, т. е. что y — целый элемент над $K[x]$. Предположим теперь, что полюса дифференциала ω (если таковые имеются) находятся среди полюсов элемента x в поле R. Мы докажем, что в этом случае элемент u имеет вид $u = \frac{G(x, y)}{F'(y)}$, где G — многочлен от двух переменных с коэффициентами из K, а F' — производная $\frac{dF}{dY}$ от многочлена F. Очевидно, что элемент y является целым над кольцом любой точки $\mathfrak{p}_0$ поля $K\langle x\rangle$, не являющейся полюсом элемента x; отсюда следует, что полюса элемента y в R находятся среди полюсов элемента x. Возьмем произвольно целое число $k \geqslant 0$. Так как полюса дифференциала $y^k\omega$ также находятся среди полюсов элемента x, то дифференциал $\mathrm{Sp}_{R/K\langle x\rangle} y^k\omega$ имеет, самое бо́льшее, только один полюс, именно полюс $\mathfrak{p}_\infty$ элемента x в $K\langle x\rangle$. Теперь

$$(dx)_R = \mathrm{Sp}_{K\langle x\rangle/R}\,(dx)_{K\langle x\rangle}$$

и

$$\mathrm{Sp}_{R/K\langle x\rangle} y^k\omega = \left(\mathrm{Sp}_{R/K\langle x\rangle} y^k u\right)(dx)_{K\langle x\rangle}$$

(формула (7) § 2). Так как дифференциал $(dx)_{K\langle x\rangle}$ не имеет нулей, то отсюда заключаем, что элемент $\mathrm{Sp}_{R/K\langle x\rangle} y^k u$ не имеет полюсов вне точки $\mathfrak{p}_\infty$, а потому принадлежит кольцу $K[x]$.

Наше утверждение будет следовать теперь из следующей леммы.

Лемма 2. *Пусть S — поле, $\mathfrak{o}$ — подкольцо поля S, содержащее 1, и R — расширение поля S, полученное из S присоединением элемента y, который алгебраичен и сепарабелен над S. Предположим, что коэффициенты характеристического многочлена $F(Y)$ элемента y (относительно S) принадлежат кольцу $\mathfrak{o}$. Пусть $u \in R$; тогда для того чтобы все элементы $\mathrm{Sp}_{R/S} y^k u \ (0 \leqslant k < \infty)$ принадлежали $\mathfrak{o}$, необходимо и достаточно, чтобы элемент u имел вид $\frac{v}{F'(y)}$, где $v \in \mathfrak{o}[y]$.*

Если n есть степень многочлена F, то элементы $1, y, \ldots, y^{n-1}$ образуют базис поля R относительно S, поэтому $uF'(y) = \sum_{i=0}^{n-1} a_i y^i$, где $a_i \in S \ (0 \leqslant i \leqslant n-1)$. Если $0 \leqslant k \leqslant n-1$, то, по лемме 3 § 1, имеем

$$a_k = \mathrm{Sp}_{R/S} y^{n-1-k} u - \sum_{k < i \leqslant n-1} a_i \, \mathrm{Sp}_{R/S} \frac{y^{i+n-1-k}}{F'(y)}. \qquad (2)$$

Индукцией по l докажем теперь, что $\mathrm{Sp}_{R/S} \frac{y^l}{F'(y)} \in \mathfrak{o}$ при всех $l \geqslant 0$. Для $l \leqslant n-1$ это верно в силу упомянутой выше леммы. Предположим, что это верно для некоторого $l \geqslant n-1$. Если $F(Y) = Y^n + \sum_{j=1}^{n} b_j Y^{n-j}$, то $y^{l+1} = -\sum_{j=1}^{n} b_j y^{l+1-j}$, откуда непосредственно и вытекает наше утверждение для $l+1$ (ибо $b_j \in \mathfrak{o}$). Из доказанного следует, что если $a_i \in \mathfrak{o} \ (0 \leqslant i \leqslant n-1)$, то $\mathrm{Sp}_{R/S} y^k u \in \mathfrak{o}$ $(0 \leqslant k < \infty)$, Обратно, допустим, что последние условия выполнены. Тогда $a_{n-1} = \mathrm{Sp}_{R/S} u \in \mathfrak{o}$, а формула (2) показывает, что если $a_k \in \mathfrak{o}$ при $i < k \leqslant n-1$, то и $a_i \in \mathfrak{o}$. Таким образом, все коэффициенты $a_0, \ldots, a_{n-1}$ принадлежат $\mathfrak{o}$, и лемма 2 доказана.

Нами доказана следующая

Теорема 8. *Пусть R — поле алгебраических функций от одной переменной вида $K\langle x, y\rangle$, где K — поле кон-*

станет R, x — трансцендентен над K, а y — алгебраичен и сепарабелен над $K\langle x\rangle$. Предположим, далее, что коэффициенты характеристического многочлена $F(Y)$ элемента y относительно $K\langle x\rangle$ принадлежат $K[x]$. Пусть ω — дифференциал поля R, полюса которого (если они имеются) находятся среди полюсов элемента x. Тогда ω можно представить в виде

$$\omega = \frac{G(x, y)}{F'(y)}\,dx,$$

где G — многочлен с коэффициентами из K.

§ 4. Дифференцирования полей

Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной и x — сепарабельно порождающая переменная поля R. Так как $dx \neq 0$, то каждый дифференциал поля R может быть представлен в виде $u\,dx$, где $u \in R$. Это относится, в частности, и к дифференциалу dy элемента $y \in R$. Наша ближайшая цель состоит в том, чтобы выяснить, каким образом можно вычислить элемент u при заданных x и y. Для этого мы должны будем сначала изучить понятие дифференцирования поля.

Пусть R — поле, а S — расширение поля R. Под *дифференцированием поля R в S* понимают отображение D поля R в S, удовлетворяющее следующим условиям:

$$D(y_1 + y_2) = Dy_1 + Dy_2, \tag{1}$$

$$D(y_1 y_2) = (Dy_1)\,y_2 + y_1\,(Dy_2) \tag{2}$$

для любых y_1 и y_2 из R.

Первое условие означает, что D есть гомоморфизм аддитивной группы поля R в аддитивную группу поля S. Отсюда непосредственно следует, что

$$D(y_1 - y_2) = Dy_1 - Dy_2 \quad (y_1,\ y_2 \in R); \quad D(0) = 0. \tag{3}$$

Далее, $D(1) = D(1 \cdot 1) = 2D(1)$, отсюда $D(1) = 0$. Индукцией по k, используя (2), легко докажем, что $D(y^k) = ky^{k-1}D(y)$ при всех $k \geqslant 0$. Если y_1 и y_2 принадлежат R и $y_2 \neq 0$, то

$$D\left(\frac{y_1}{y_2}\right) = \frac{(Dy_1)\,y_2 - y_1\,(Dy_2)}{y_2^2}. \tag{4}$$

Действительно, пусть $z=\frac{y_1}{y_2}$, тогда $y_1=zy_2$ и $D(y_1)=$ $=(Dz)y_2+z(Dy_2)$, откуда, заменив z его значением, мы легко выведем требуемую формулу (4).

Если D — дифференцирование R в S и $u\in S$, то, как легко видеть, отображение uD поля R в S, определенное равенством $(uD)(y)=u(Dy)$, также является дифференцированием. Таким образом, дифференцирования поля R в S образуют векторное пространство над S.

Дифференцирование поля R в себя называется просто *дифференцированием поля* R. Пусть D_1 и D_2 — два дифференцирования поля R; отображение $D=[D_1, D_2]$, определенное равенством $Dy=D_2(D_1y)-D_1(D_2y)$, также является дифференцированием поля R. Действительно, условие (1), очевидно, выполняется. Далее,

$$\begin{aligned}D(y_1y_2)&=\\&=D_2((D_1y_1)y_2+y_1(D_1y_2))-D_1((D_2y_1)y_2+y_1(D_2y_2))=\\&=(D_2(D_1y_1))y_2+y_1(D_2(D_1y_2))-(D_1(D_2y_1))y_2-y_1(D_1(D_2y_2))=\\&=(Dy_1)y_2+y_1(Dy_2),\end{aligned}$$

что и доказывает наше утверждение.

Лемма 1. *Пусть D и D' — два дифференцирования поля R в надполе S. Предположим, что D и D' совпадают на некотором подмножестве E поля R. Тогда эти дифференцирования совпадают и на подполе F поля R, порожденном элементами из E.*

Действительно, из формул (1), (2), (3) и (4) непосредственно следует, что множество элементов $y\in R$, для которых $Dy=D'y$, является полем.

Лемма 2. *Пусть D — дифференцирование поля R в надполе S, и пусть z — элемент из S, алгебраический и сепарабельный над R. Тогда D может быть продолжено, и притом единственным способом, до дифференцирования поля $R\langle z\rangle$ в S.*

Пусть $G(Z)=\sum_{k=0}^{m}c_kZ^k$ — произвольный многочлен от переменной Z с коэффициентами из R. Положим $(DG)(Z)=$ $=\sum_{k=0}^{m}(Dc_k)Z^k$. Тогда, как легко видеть, для многочленов G

и G' с коэффициентами из R будут справедливы равенства:

$$D(G+G') = DG + DG' \quad \text{и} \quad D(GG') = (DG)\,G' + G\,(DG').$$

Допустим, что дифференцирование D продолжимо до дифференцирования D' поля $R\langle z\rangle$ в S. Тогда для произвольного $c \in R$ имеем $D'(cz^k) = (Dc)\,z^k + kcz^{k-1}D'z$, откуда $D'(G(z)) = (DG)(z) + G'(z)\,D'z$, где G' обозначает производную от G. Применим это к характеристическому многочлену $F(Z)$ элемента z относительно R; так как $F(z) = 0$, то $0 = (DF)(z) + F'(z)\,D'z$. Элемент z сепарабелен над R, поэтому $F'(z) \neq 0$, а значит, полученная формула вполне определяет $D'z$. Таким образом, мы видим (применяя лемму 1), что если дифференцирование D' существует, то оно единственно.

Чтобы доказать существование D', заметим, что всякий элемент $u \in R\langle z\rangle$ может быть представлен, и притом единственным образом, в виде $u = G(z)$, где G — многочлен с коэффициентами из R, степень которого меньше степени n многочлена F. Определим тогда $D'u$ формулой

$$D'u = (DG)(z) - \frac{(DF)(z)}{F'(z)}\,G'(z)$$

и докажем, что D' есть дифференцирование, продолжающее D. Если $u \in R$, то $G = u$ есть многочлен нулевой степени, значит $D'u = Du$, т. е. отображение D' совпадает на R с D. Пусть $u_1 = G_1(z)$ и $u_2 = G_2(z)$ — элементы из $R\langle z\rangle$ (где G_1 и G_2 — многочлены степени $< n$ с коэффициентами из R). Тогда $u_1 + u_2 = (G_1 + G_2)(z)$ и $G_1 + G_2$ имеет степень $< n$. Так как

$$D(G_1 + G_2) = DG_1 + DG_2, \quad (G_1 + G_2)' = G_1' + G_2',$$

то получаем $D'(u_1 + u_2) = D'u_1 + D'u_2$. Далее, произведение u_1u_2 равно $(G_1G_2)(z)$, однако многочлен G_1G_2 может иметь степень $\geqslant n$. Чтобы найти правильное представление элемента u_1u_2, мы разделим G_1G_2 на F с остатком: $G_1G_2 = FQ + G_3$, где G_3 имеет степень $< n$; тогда будем иметь $u_1u_2 = G_3(z)$. Так как $F(z) = 0$, то

$$(DG_3)(z) = (DG_1)(z)\,u_2 + u_1\,(DG_2)(z) - ((DF)(z))\,Q(z),$$

$$G_3'(z) = G_1'(z)\,u_2 + u_1G_2'(z) - F'(z)\,Q(z).$$

Легко теперь видеть, что

$$D'(u_1u_2)=(DG_3)(z)-\frac{(DF)(z)}{F'(z)}G_3'(z)$$

равно $(D'u_1)u_2+u_1(D'u_2)$. Лемма 2 доказана.

Лемма 3. *Пусть R — поле, а S — расширение поля R конечной степени. Если дифференцирование D поля S отображает подполе R в себя, то для любого $y\in S$ имеем*

$$\mathrm{Sp}_{S/R}\,Dy=D(\mathrm{Sp}_{S/R}\,y).$$

Мы можем предполагать, что S сепарабельно над R, ибо в противном случае наша формула тривиальна. Найдем расширение S^* поля S, которое нормально, сепарабельно и имеет конечную степень над R. Пусть j_k $(1\leqslant k\leqslant n)$ — все различные изоморфизмы поля S в S^*, тождественные на R. Тогда $\mathrm{Sp}_{S/R}\,y=\sum_{k=1}^{n}j_ky$ и $\mathrm{Sp}_{S/R}\,Dy=\sum_{k=1}^{n}j_k(Dy)$. Дифференцирование D мы можем продолжить до дифференцирования поля S^* (будем его обозначать также через D). Так как j_k — изоморфизм, то, как легко видеть, отображение $j_k^{-1}Dj_k$ есть также дифференцирование поля S в S^*. Это дифференцирование совпадает на поле R с D (ибо j_k каждый элемент из R отображает на себя); следовательно, оно совпадает с D и на S. Отсюда следует, что отображения j_kD и Dj_k на поле S совпадают друг с другом, и мы получаем

$$\mathrm{Sp}_{S/R}\,Dy=\sum_{k=1}^{n}D(j_ky)=D(\mathrm{Sp}_{S/R}\,y).$$

Лемма 4. *Пусть R — поле алгебраических функций от одной переменной и $\mathfrak{p}$ — точка поля R. Пусть D — дифференцирование поля R, которое поле констант K поля R отображает в себя. Тогда существует такое целое число s, что $\nu_{\mathfrak{p}}(Dy)\geqslant\nu_{\mathfrak{p}}(y)-s$ при всех $y\in R$.*

Пусть x — униформизирующая переменная в точке $\mathfrak{p}$. Положим $s_0=\max\{0,\ -\nu_{\mathfrak{p}}(Dx)\}$ (если $Dx=0$, то считаем $s_0=0$). Если $f(x)=\sum_{k=0}^{m}a_kx^k$ — элемент из $K[x]$, то

$$D(f(x)) = \sum_{k=0}^{m} (Da_k)\, x^k + \left(\sum_{k=1}^{m} k a_k x^{k-1}\right) Dx,$$

откуда

$$\nu_{\mathfrak{p}}(D(f(x))) \geqslant -s_0.$$

Каждый элемент $y \neq 0$ из $K\langle x\rangle$ можно записать в виде $y = x^{\nu_{\mathfrak{p}}(y)} \dfrac{f(x)}{g(x)}$, где f и g — многочлены с коэффициентами из K, причем $g(0) \neq 0$. Замечая, что формула $Dx^{\nu} = \nu x^{\nu-1} Dx$ справедлива и для $\nu < 0$, получаем

$$Dy = \nu_{\mathfrak{p}}(y)\, x^{\nu_{\mathfrak{p}}(y)-1} \frac{f(x)}{g(x)} Dx + \\ + x^{\nu_{\mathfrak{p}}(y)} \frac{D(f(x))\, g(x) - f(x)\, D(g(x))}{g^2(x)},$$

откуда $\nu_{\mathfrak{p}}(Dy) \geqslant \nu_{\mathfrak{p}}(y) - s_0 - 1$ (при $y \in K\langle x\rangle$). Пусть теперь $\mathfrak{p}_0$ есть нуль элемента x в поле $K\langle x\rangle$ и пусть $\{z_1, \ldots, z_n\}$ — базис поля R относительно $K\langle x\rangle$, целый в точке $\mathfrak{p}_0$. Обозначим через $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ точки поля R, отличные от $\mathfrak{p}$ и лежащие над $\mathfrak{p}_0$. В силу следствия к теореме 3 § 6 гл. 1, в поле R можно найти такой элемент u, что $\nu_{\mathfrak{p}}(u) = 0$, $\nu_{\mathfrak{p}_i}(u) > 0$ $(1 \leqslant i \leqslant h)$. Каждый элемент $y \neq 0$ из R можно представить в виде $y = x^{\nu_{\mathfrak{p}}(y)} u^r y'$, где r — некоторое целое число и

$$\nu_{\mathfrak{p}}(y') = 0, \quad \nu_{\mathfrak{p}_i}(y') \geqslant 0 \quad (1 \leqslant i \leqslant h).$$

Имеем теперь

$$\frac{Dy}{y} = \nu_{\mathfrak{p}}(y) \frac{Dx}{x} + r \frac{Du}{u} + \frac{Dy'}{y'},$$

откуда $\nu_{\mathfrak{p}}(Dy) \geqslant \nu_{\mathfrak{p}}(y) + \min\left\{\nu_{\mathfrak{p}}\left(\dfrac{Dx}{x}\right), \nu_{\mathfrak{p}}\left(\dfrac{Du}{u}\right), \nu_{\mathfrak{p}}(Dy')\right\}$.

Если элемент y' записать в виде $y' = \sum_{i=1}^{n} y_i z_i$, где $y_1, \ldots, y_n$ принадлежат $K\langle x\rangle$, то

$$\nu_{\mathfrak{p}_0}(y_i) \geqslant 0 \quad (1 \leqslant i \leqslant n).$$

Так как $Dy' = \sum_{i=1}^{n} (Dy_i) z_i + \sum_{i=1}^{n} y_i (Dz_i)$ и $\nu_{\mathfrak{p}}(Dy_i) \geqslant -s_0 - 1$, то

$$\nu_{\mathfrak{p}}(Dy') \geqslant \min_{1 \leqslant i \leqslant n} \{-s_0 - 1 + \nu_{\mathfrak{p}}(z_i), \nu_{\mathfrak{p}}(Dz_i)\}.$$

Лемма 4, таким образом, доказана.

Лемма 5. *Пусть сохраняются предположения леммы 4. Обозначим через $\bar{R}$ $\mathfrak{p}$-адическое пополнение поля R. Утверждается, что D может быть продолжено, и притом единственным способом, до непрерывного дифференцирования $\bar{D}$ поля $\bar{R}$ (непрерывность $\bar{D}$ здесь означает, что если элемент $z \in \bar{R}$ является пределом последовательности (z_n) элементов из $\bar{R}$, то $\bar{D}z = \lim\limits_{n\to\infty} \bar{D}z_n$).*

Если последовательность (x_n) элементов поля R сходится, скажем к элементу $z \in \bar{R}$, то последовательность (Dx_n) также сходится. Действительно, так как $\nu_{\mathfrak{p}}(x_{n+1} - x_n)$ неограниченно возрастает вместе с n, то, в силу леммы 4, это же верно и для $\nu_{\mathfrak{p}}(Dx_{n+1} - Dx_n)$. Более того, предел $\lim\limits_{n\to\infty} Dx_n$ зависит только от z, а не от последовательности (x_n); в самом деле, если $z = \lim\limits_{n\to\infty} x_n = \lim\limits_{n\to\infty} x'_n$, то $\nu_{\mathfrak{p}}(x'_n - x_n)$ неограниченно возрастает вместе с n, а значит, по лемме 4, это же справедливо также и для $\nu_{\mathfrak{p}}(Dx'_n - Dx_n)$, откуда $\lim\limits_{n\to\infty} Dx'_n = \lim\limits_{n\to\infty} Dx_n$. Если мы положим теперь $\bar{D}z = \lim\limits_{n\to\infty} Dx_n$, то получим отображение $\bar{D}$ поля $\bar{R}$ в себя. Если (x_n) и (y_n) — две сходящиеся последовательности элементов поля R, то имеет место формула

$$\lim_{n\to\infty} (x_n + y_n) = \lim_{n\to\infty} x_n + \lim_{n\to\infty} y_n,$$

а также аналогичная формула для произведения. Отсюда непосредственно следует, что $\bar{D}$ есть дифференцирование. Применяя вышеприведенные обозначения, мы имеем (лемма 4)

$$\nu_{\mathfrak{p}}(\bar{D}z) = \lim_{n\to\infty} \nu_{\mathfrak{p}}(Dx_n) \geqslant \lim_{n\to\infty} \nu_{\mathfrak{p}}(x_n) - s = \nu_{\mathfrak{p}}(z) - s,$$

где s — целое число, не зависящее от z. Если z являетс пределом последовательности (z_n) элементов из $\bar{R}$, то $\lim\limits_{n\to\infty} \nu_{\mathfrak{p}}(z - z_n) = \infty$, откуда $\lim\limits_{n\to\infty} \nu_{\mathfrak{p}}(\bar{D}z - \bar{D}z_n) = \infty$ и $\bar{D}(z) = \lim\limits_{n\to\infty} \bar{D}z_n$. Ясно, что $\bar{D}$ есть единственное непрерывное отображение поля $\bar{R}$ в себя, продолжающее D.

Рассмотрим подробнее случай, когда поле вычетов Σ точки $\mathfrak{p}$ сепарабельно над K. Пусть x — униформизирующая переменная в точке $\mathfrak{p}$. Тогда, как мы знаем (§ 3 гл. III), поле $\bar{R}$ содержит подполе Σ_1, изоморфное полю Σ (при этом имеется естественный изоморфизм, отображающий элементы из K на себя). Далее, поле $\bar{R}$ может быть отождествлено с полем формальных степенных рядов от x с коэффициентами из Σ_1. Так как Σ сепарабельно над K, то ограничение дифференцирования D на поле K может быть продолжено до дифференцирования D_1 поля Σ_1, которое, в силу единственности такого продолжения (лемма 2), должно совпадать с ограничением дифференцирования $\bar{D}$ на Σ_1. Этим доказано, что $\bar{D}$ отображает Σ_1 в себя. В силу непрерывности $\bar{D}$, отсюда непосредственно следует формула

$$\bar{D}\left(\sum_{k=r}^{\infty} c_k x^k\right) = \sum_{k=r}^{\infty} (D_1 c_k)\, x^k + \left(\sum_{k=r}^{\infty} k c_k x^{k-1}\right) Dx. \qquad (5)$$

Обратно, пусть нам задано произвольное поле Σ_1 и дифференцирование D_1 этого поля. Построим поле $\bar{R}$ формальных степенных рядов от символа x с коэффициентами из Σ_1. Пусть u — произвольно заданный элемент из $\bar{R}$. Тогда формула

$$\bar{D}\left(\sum_{k=r}^{\infty} c_k x^k\right) = \sum_{k=r}^{\infty} (D_1 c_k)\, x^k + \left(\sum_{k=r}^{\infty} k c_k x^{k-1}\right) u$$

(где c_k — элементы из Σ_1) определяет дифференцирование $\bar{D}$ поля $\bar{R}$. Действительно, пусть $y = \sum_{k=r}^{\infty} c_k x^k$ и $y' = \sum_{k=r'}^{\infty} c'_k x^k$ — два элемента из $\bar{R}$. Прежде всего очевидно, что

$$\bar{D}(y + y') = \bar{D}y + \bar{D}y'.$$

Далее, мы имеем $yy' = \sum_{l=r+r'} e_l x^l$, где

$$e_l = \sum_{k+k'=l} c_k c'_{k'}.$$

Так как

$$D_1 e_l = \sum_{k+k'=l} (D_1 c_k)\, c'_{k'} + \sum_{k+k'=l} c_k (D_1 c'_{k'})$$

и

$$le_l = \sum_{k+k'=l} (kc_k)\, c'_{k'} + \sum_{k+k'=l} c_k (k' c'_{k'}),$$

то получаем $\bar{D}(yy') = (\bar{D}y)\, y' + y(\bar{D}y')$. Ясно, что дифференцирование $\bar{D}$ является продолжением D_1 и отображает x на u.

Лемма 6. *Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной. Если x есть сепарабельно порождающая переменная поля R, то в R существует единственное дифференцирование, которое каждую константу отображает на* 0, *а элемент x — на* 1.

Пусть K — поле констант поля R. Мы можем рассматривать поле $K\langle x\rangle$ как подполе поля $\bar{S}$ формальных степенных рядов от x с коэффициентами из K. Как мы только что доказали, существует дифференцирование $\bar{D}$ поля $\bar{S}$, отображающее каждый элемент из K на 0, а элемент x — на 1. Применяя вышеприведенную формулу (4), мы видим, что $\bar{D}$ отображает $K\langle x\rangle$ в себя. Так как R сепарабельно над $K\langle x\rangle$, то ограничение дифференцирования $\bar{D}$ на $K\langle x\rangle$ может быть продолжено до дифференцирования D поля R с требуемыми свойствами. Единственность D непосредственно следует из лемм 1 и 2.

Дифференцирование, существование и единственность которого только что доказаны (лемма 6), называется *дифференцированием поля R по x.*

Лемма 7. *Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной и пусть D — дифференцирование поля констант K поля R. Если x есть сепарабельно порождающая переменная поля R, то D может быть продолжено, притом единственным образом, до дифференцирования поля R, при котором элемент x отображается на* 0.

Используем обозначения из доказательства леммы 6. Из предыдущего следует, что D может быть продолжено до дифференцирования $\bar{D}$ поля $\bar{S}$, отображающего элемент x на 0. Как и в доказательстве леммы 6 мы видим, что дифференцирование $\bar{D}$ отображает $K\langle x\rangle$ в себя и что его огра-

ничение на $K\langle x\rangle$ может быть продолжено до дифференцирования поля R. Единственность здесь вытекает также из лемм 1 и 2.

§ 5. Дифференцирования и дифференциалы

Теперь мы уже можем дать решение проблемы, поставленной в начале § 4. Именно имеет место следующая теорема.

Теорема 9. *Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной и пусть x — сепарабельно порождающая переменная в R. Тогда для любого элемента $y \in R$ имеем $dy = (D_x y)\,dx$, где D_x — дифференцирование поля R по x.*

Если y не является сепарабельно порождающей переменной поля R, то, как мы знаем, $dy = 0$. Пусть в этом случае $F(X, Y)$ — неприводимый многочлен с коэффициентами из K, для которого $F(x, y) = 0$. Тогда $F(x, Y)$ есть неприводимый многочлен с коэффициентами из $K\langle x\rangle$. Так как элемент y сепарабелен над $K\langle x\rangle$, то $\frac{\partial F}{\partial Y}(x, y) \neq 0$. С другой стороны, элемент x несепарабелен над $K\langle y\rangle$, ибо в противном случае поле R (которое сепарабельно над $K\langle x\rangle$, а значит и над $K\langle x, y\rangle$) было бы сепарабельным над $K\langle y\rangle$; отсюда следует, что $\frac{\partial F}{\partial X}(x, y) = 0$. Теперь, как легко видеть, имеем $0 = D_x F(x, y) = \frac{\partial F}{\partial X}(x, y) D_x x + \frac{\partial F}{\partial Y}(x, y) D_x y$, откуда $D_x y = 0$ и, следовательно, $dy = (D_x y)\,dx$.

Предположим теперь, что x и y — сепарабельно порождающие переменные. Применяя лемму 3 § 8 гл. IV и лемму 1 § 3, мы видим, что в поле R существует бесконечно много точек $\mathfrak{p}$, удовлетворяющих следующим условиям:

1) поле вычетов точки $\mathfrak{p}$ сепарабельно над K;

2) точка $\mathfrak{p}$ неразветвлена как относительно $K\langle x\rangle$, так и относительно $K\langle y\rangle$;

3) $\mathfrak{p}$ не является полюсом каждого из элементов x и y.

Мы докажем, что если $\mathfrak{p}$ есть любая из этих точек, а $\mathfrak{x}$ — распределение, для которого $\nu_{\mathfrak{p}}(\mathfrak{x}) \geqslant -1$, то

$$(dy - (D_x y)\,dx)^{\mathfrak{p}}(\mathfrak{x}) = 0.$$

Отсюда непосредственно и будет следовать теорема 9. Действительно, если бы дифференциал $dy-(D_x y)\,dx$ был отличен от 0, то, согласно лемме 2 § 7 гл. II, каждая точка $\mathfrak{p}$, удовлетворяющая условиям 1), 2) и 3), входила бы в дивизор этого дифференциала с показателем >0, что, очевидно, невозможно.

Итак, пусть $\mathfrak{p}$ — точка, удовлетворяющая условиям 1), 2) и 3). Обозначим через Σ поле вычетов точки $\mathfrak{p}$, а через ξ и η — классы вычетов по модулю $\mathfrak{p}$ элементов x и y соответственно. Пусть f и g — неприводимые многочлены с коэффициентами из поля констант K поля R со старшим коэффициентом 1, для которых $f(\xi)=0$ и $g(\eta)=0$. Так как точка $\mathfrak{p}$ неразветвлена относительно полей $K\langle x\rangle$ и $K\langle y\rangle$, то

$$\nu_{\mathfrak{p}}(f(x))=\nu_{\mathfrak{p}}(g(y))=1.$$

Пусть $\overline{R}$ — $\mathfrak{p}$-адическое пополнение поля R. Так как Σ сепарабельно над K, то в $\overline{R}$ имеется подполе Σ_1, содержащее K и изоморфное полю Σ. Поле $\overline{R}$ может быть отождествлено с полем формальных степенных рядов от $f(x)$ с коэффициентами из Σ_1 (§ 3 гл. III). Дифференцирование D_x может быть продолжено до дифференцирования $\overline{D}$ поля $\overline{R}$, которое определяется формулой

$$\overline{D}\left(\sum_{k=r}^{\infty} s_k(f(x))^k\right)=(D_x f(x))\left(\sum_{k=r}^{\infty} k s_k(f(x))^{k-1}\right),$$

где $s_k\in\Sigma_1$ $(r\leqslant k<\infty)$. Далее, очевидно, что $D_x f(x)=f'(x)$, где f' — производная от многочлена f. Для элемента $g(y)$ в поле $\overline{R}$ имеем следующее разложение:

$$g(y)=z_1 f(x)+\sum_{k=2}^{\infty} s_k(f(x))^k \qquad (z_1,\ s_k\in\Sigma_1),$$

где $z_1\neq 0$. Отсюда следует, что точка $\mathfrak{p}$ не является полюсом элемента $D_x g(y)$ и что его класс вычетов по модулю $\mathfrak{p}$ равен $\zeta f'(\xi)$, где ζ — класс вычетов элемента z_1 по модулю $\mathfrak{p}$. С другой стороны, $D_x g(y)=g'(y)D_x y$ и $g'(\eta)\neq 0$ (ибо элемент η сепарабелен над K), поэтому $\nu_{\mathfrak{p}}(g'(y))=0$ и $\nu_{\mathfrak{p}}(D_x y)\geqslant 0$. Отсюда следует, что класс вычетов элемента $D_x y$ по модулю $\mathfrak{p}$ равен $\dfrac{\zeta f'(\xi)}{g'(\eta)}$. Пусть теперь $\mathfrak{z}$ — распре-

деление, для которого $\nu_{\mathfrak{p}}(\mathfrak{x}) \geqslant -1$, тогда $\nu_{\mathfrak{p}}(f(x)\mathfrak{x}(\mathfrak{p})) \geqslant 0$ и $\nu_{\mathfrak{p}}(g(y)\mathfrak{x}(\mathfrak{p})) \geqslant 0$. Обозначим через φ и ψ классы вычетов по модулю $\mathfrak{p}$ элементов $f(x)\mathfrak{x}(\mathfrak{p})$ и $g(y)\mathfrak{x}(\mathfrak{p})$ соответственно. В силу формулы (1) § 3 мы имеем

$$(dx)^{\mathfrak{p}}(\mathfrak{x}) = \mathrm{Sp}_{\Sigma/K}\frac{\varphi}{f'(\xi)}, \quad (dy)^{\mathfrak{p}}(\mathfrak{x}) = \mathrm{Sp}_{\Sigma/K}\frac{\psi}{g'(\eta)}.$$

Но $((D_x y)\,dx)^{\mathfrak{p}}(\mathfrak{x}) = (dx)^{\mathfrak{p}}((D_x y)\mathfrak{x})$, и класс вычетов элемента $f(x)(D_x y)\mathfrak{x}(\mathfrak{p})$ равен $\zeta\varphi\dfrac{f'(\xi)}{g'(\eta)}$, поэтому

$$((D_x y)\,dx)^{\mathfrak{p}}(\mathfrak{x}) = \mathrm{Sp}_{\Sigma/K}\frac{\zeta\varphi}{g'(\eta)}.$$

С другой стороны, так как $g(y)\mathfrak{x}(\mathfrak{p}) = \dfrac{g(y)}{f(x)}f(x)\mathfrak{x}(\mathfrak{p})$ и класс вычетов элемента $\dfrac{g(y)}{f(x)}$ по модулю $\mathfrak{p}$ равен ζ, то $\psi = \zeta\varphi$, откуда

$$((D_x y)\,dx)^{\mathfrak{p}}(\mathfrak{x}) = (dy)^{\mathfrak{p}}(\mathfrak{x}).$$

Теорема 9, таким образом, доказана.

Следствие. *Пусть в поле R, удовлетворяющем условиям теоремы 9, заданы элементы $y_1, \ldots, y_m$. Если F есть многочлен от m переменных $Y_1, \ldots, Y_m$ с коэффициентами из поля констант K поля R, то*

$$dF(y_1, \ldots, y_m) = \sum_{i=1}^{m}\frac{\partial F}{\partial Y_i}(y_1, \ldots, y_m)\,dy_i.$$

Непосредственными вычислениями легко проверяется, что

$$D_x F(y_1, \ldots, y_m) = \sum_{i=1}^{m}\frac{\partial F}{\partial Y_i}(y_1, \ldots, y_m)\,D_x y_i,$$

откуда и вытекает наше следствие.

В частности, имеют место формулы:

$$d(y_1 + y_2) = dy_1 + dy_2,$$
$$d(y_1 y_2) = (dy_1)\,y_2 + y_1(dy_2).$$

§ 6. Обобщение понятия коследа

Пусть R и S — поля алгебраических функций от одной переменной, причем R является подполем поля S. Обозначим через K и L поля констант полей R и S соответственно. Мы предполагаем, как обычно, что $K = L \cap R$. Для случая, когда $K = L$, в § 2 была определена операция коследа, которая каждому дифференциалу ω поля R ставит в соответствие дифференциал $\mathrm{Cosp}_{R/S}\,\omega$ поля S. Сейчас мы хотим такую же операцию определить и для случая $K \neq L$; однако в этом случае мы должны будем предположить, что поле R сепарабельно порождаемо. Итак, пусть u сепарабельно порождающая переменная поля R. Каждый дифференциал ω поля R может быть представлен тогда в виде $x\,(du)_R$ при некотором $x \in R$. Положим $\Omega(\omega) = x\,(du)_S$. Очевидно, что при любом $y \in R$ будем иметь $\Omega(y\omega) = y\Omega(\omega)$. Утверждаем, что если $K = L$, то $\Omega(\omega) = \mathrm{Cosp}_{R/S}\,\omega$, а также что, в общем случае, дифференциал $\Omega(\omega)$ не зависит от выбора сепарабельно порождающей переменной u.

Предположим, что $K = L$. В силу формулы (6) § 2, мы имеем

$$\mathrm{Cosp}_{R/S}(du)_R = \mathrm{Cosp}_{R/S}\left(\mathrm{Cosp}_{K\langle u\rangle/R}(du)_{K\langle u\rangle}\right) = \\ = \mathrm{Cosp}_{K\langle u\rangle/S}(du)_{K\langle u\rangle} = (du)_S.$$

Отсюда, в силу формулы (5) § 2, следует, что если $K = L$, то $\Omega(\omega) = \mathrm{Cosp}_{R/S}\,\omega$.

Докажем теперь, что и в общем случае $\Omega\left((dv)_R\right) = (dv)_S$ для каждого элемента $v \in R$. Пусть $F(U, V)$ — неприводимый многочлен с коэффициентами из K, для которого $F(u, v) = 0$. По следствию к теореме 9 § 5 мы имеем

$$\frac{\partial F}{\partial U}(u, v)(du)_R + \frac{\partial F}{\partial V}(u, v)(dv)_R = 0$$

и $\frac{\partial F}{\partial U}(u, v)(du)_S + \frac{\partial F}{\partial V}(u, v)(dv)_S = 0$. С другой стороны, так как элемент v сепарабелен над $K\langle u\rangle$, то $\frac{\partial F}{\partial V}(u, v) \neq 0$.

Таким образом,

$$\Omega\left((dv)_R\right) = -\frac{\frac{\partial F}{\partial U}(u, v)}{\frac{\partial F}{\partial V}(u, v)}(du)_S = (dv)_S.$$

Считая, в частности, что элемент v является сепарабельно порождающей переменной поля R, мы видим, что отображение $\omega \to \Omega(\omega)$ не зависит от выбора сепарабельно порождающей переменной u.

Дифференциал $\Omega(\omega)$ будем называть *косследом дифференциала* ω *из* R *в* S и обозначать через $\mathrm{Cosp}_{R/S}\,\omega$.

Пусть T есть промежуточное поле между R и S, являющееся сепарабельно порождаемым полем алгебраических функций от одной переменной (поле констант которого равно $L \cap T$); тогда для каждого дифференциала ω поля R имеем $\mathrm{Cosp}_{R/S}\,\omega = \mathrm{Cosp}_{T/S}\left(\mathrm{Cosp}_{R/T}\,\omega\right)$. Справедливость этой формулы достаточно проверить, очевидно, для дифференциала $\omega = (du)_R$, где u — сепарабельно порождающая переменная поля R. В этом случае правая часть нашего равенства равна

$$\mathrm{Cosp}_{T/S}(du)_T = (du)_S = \mathrm{Cosp}_{R/S}(du)_R.$$

Из доказанной формулы, в частности, следует, что если u является сепарабельно порождающей переменной в S, то u является также сепарабельно порождающей переменной и в поле T.

Таким образом, доказана

Теорема 10. *Пусть R и S — поля алгебраических функций от одной переменной, причем R является подполем поля S и поле констант поля R равно пересечению поля R с полем констант L поля S. Если поле R сепарабельно порождаемо, то существует отображение $\omega \to \mathrm{Cosp}_{R/S}\,\omega$ множества дифференциалов поля R в множество дифференциалов поля S, такое, что если $v \in R$, то $\mathrm{Cosp}_{R/S}(dv)_R = (dv)_S$, и, кроме того, имеют место формулы (4), (5) и (6), приведенные в § 2 (в случае формулы (6) промежуточное поле T между R и S должно быть сепарабельно порождаемым полем алгебраических функций от одной переменной, поле констант которого равно $L \cap T$).*

Теперь будет доказана

Теорема 11. *Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной, и пусть L — произвольное расширение поля констант K поля R. Положим $S = R\langle L\rangle$. Пусть ω есть дифференциал поля R, а Ω — дифференциал $\mathrm{Cosp}_{R/S}\,\omega$ поля S. Тогда для любого распределения $\mathfrak{x}$ поля R будем иметь $\omega(\mathfrak{x}) = \Omega(\mathrm{Cosp}_{R/S}\mathfrak{x})$.*[1] *Далее, если $\mathfrak{p}$ — точка поля R, а $\mathfrak{P}$ — точка поля S, лежащая над $\mathfrak{p}$, то $\mathrm{res}_{\mathfrak{P}}\,\Omega = \mathrm{res}_{\mathfrak{p}}\,\omega$ (считая, что поле вычетов точки $\mathfrak{p}$ отождествлено с подполем поля вычетов точки $\mathfrak{P}$). Наконец, если $\omega \neq 0$, то дивизор $\mathfrak{d}(\Omega)$ является делителем дивизора $\mathrm{Con}_{R/S}\,\mathfrak{d}(\omega)$, а если поля R и S имеют один и тот же род, то $\mathfrak{d}(\Omega) = \mathrm{Con}_{R/S}\,\mathfrak{d}(\omega)$.*

Как нам известно, $\omega(\mathfrak{x}) = \sum_{\mathfrak{q}} \omega^{\mathfrak{q}}(\mathfrak{x})$ ($\mathfrak{q}$ пробегает все точки поля R) и $\Omega(\mathrm{Cosp}_{R/S}\mathfrak{x}) = \sum_{\mathfrak{Q}} \Omega^{\mathfrak{Q}}(\mathrm{Cosp}_{R/S}\mathfrak{x})$ ($\mathfrak{Q}$ пробегает все точки поля S). Для доказательства первого утверждения теоремы 11 достаточно проверить, что $\omega^{\mathfrak{q}}(\mathfrak{x}) = \sum_{k=1}^{h} \Omega^{\mathfrak{Q}_k}(\mathrm{Cosp}_{R/S}\mathfrak{x})$, где $\mathfrak{q}$ — произвольная точка поля R, а $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_h$ — все различные точки поля S, лежащие над $\mathfrak{q}$. Пусть (z_n) есть последовательность элементов поля R, которая в $\mathfrak{q}$-адическом пополнении поля R сходится к элементу $\mathfrak{x}(\mathfrak{q})$. Эта же последовательность в $\mathfrak{Q}_k$-адическом пополнении поля S $(1 \leqslant k \leqslant h)$ сходится к элементу $(\mathrm{Cosp}_{R/S}\mathfrak{x})(\mathfrak{Q}_k)$. Начиная с некоторого n, имеют место равенства $\omega^{\mathfrak{q}}(\mathfrak{x}) = \omega^{\mathfrak{q}}(z_n)$ и $\Omega^{\mathfrak{Q}_k}(\mathrm{Cosp}_{R/S}\mathfrak{x}) = \Omega^{\mathfrak{Q}_k}(z_n)$ $(1 \leqslant k \leqslant h)$, поэтому нам достаточно будет доказать, что для каждого

---

[1]) Здесь следует обратить внимание на следующее обстоятельство. Коспед $\mathrm{Cosp}_{R/S}\mathfrak{x}$ распределения $\mathfrak{x}$ был определен (см. § 7 гл. IV, стр. 126) только для случая, когда S алгебраично над R. Однако в данной теореме S может и не быть алгебраическим расширением поля R. В этом случае, как это явствует из последующего изложения, под $\mathrm{Cosp}_{R/S}\mathfrak{x}$ понимается распределение $\mathfrak{y}$ поля S, которое для каждой переменной точки $\mathfrak{Q}$ поля S относительно R принимает значение $\mathfrak{y}(\mathfrak{Q}) = 0$ (а для постоянной точки $\mathfrak{P}$, лежащей над $\mathfrak{p}$, как обычно, $\mathfrak{y}(\mathfrak{P}) = \mathfrak{x}(\mathfrak{p})$). (*Прим. перев.*)

$z \in R$ справедливо равенство $\omega^{\mathfrak{q}}(z) = \sum_{k=1}^{h} \Omega^{\mathfrak{Q}_k}(z)$. Предварительно мы докажем следующую лемму.

Лемма 1. *Если $\mathfrak{q}$ есть точка сепарабельно порождаемого поля R алгебраических функций от одной переменной, то в этом поле существует сепарабельно порождающая переменная, для которой точка $\mathfrak{q}$ является ее единственным полюсом.*

Пусть t — произвольная сепарабельно порождающая переменная поля R. Обозначим дивизор полюсов элемента t через $\mathfrak{n}$. Выберем целое число $m > 0$ так, чтобы разность $md(\mathfrak{q}) - d(\mathfrak{n})$ была больше, чем $2g - 2$ и $g - 1$, где g—род поля R. В поле R нет отличных от 0 дифференциалов, делящихся на $\mathfrak{q}^m\mathfrak{n}^{-1}$, поэтому, по теореме Римана — Роха, $l(\mathfrak{q}^{-m}\mathfrak{n}) = md(\mathfrak{q}) - d(\mathfrak{n}) - g + 1 > 0$. Это означает, что в поле R существует элемент $x_1 \neq 0$, делящийся на $\mathfrak{q}^{-m}\mathfrak{n}$. Все точки поля R, отличные от $\mathfrak{q}$, не являются полюсами элементов x_1 и tx_1. Так как

$$d(tx_1) = t\,dx_1 + x_1\,dt$$

и $dt \neq 0$, то хоть один из элементов tx_1 и x_1 имеет дифференциал, отличный от 0, а потому этот элемент является сепарабельно порождающей переменной (теорема 4 § 3).

Вернемся теперь к доказательству формулы

$$\omega^{\mathfrak{q}}(z) = \sum_{k=1}^{h} \Omega^{\mathfrak{Q}_k}(z).$$

Пусть x есть сепарабельно порождающая переменная поля R, имеющая точку $\mathfrak{q}$ своим единственным полюсом. Если дифференциал ω мы представим в виде $\omega = y(dx)_R$, $y \in R$, то $\Omega = y(dx)_S$. Нам надо доказать, что

$$\left((dx)_R\right)^{\mathfrak{q}}(yz) = \sum_{k=1}^{h} \left((dx)_S\right)^{\mathfrak{Q}_k}(yz).$$

Пусть $\mathfrak{q}_0$ — полюс элемента x в поле $K\langle x\rangle$. Так как $\mathfrak{q}$ является единственной точкой поля R, лежащей над $\mathfrak{q}_0$, то левая часть последнего равенства равна $\left((dx)_{K\langle x\rangle}\right)^{\mathfrak{q}_0}\left(\mathrm{Sp}_{R/K\langle x\rangle}\, yz\right)$. Пусть $\mathfrak{Q}_0$ — полюс элемента x в поле $L\langle x\rangle$. Ясно, что $\mathfrak{Q}_0$ есть точка поля $L\langle x\rangle$, лежащая над $\mathfrak{q}_0$, а точки

$\mathfrak{Q}_1, \ldots, \mathfrak{Q}_h$ — это точки поля S, лежащие над $\mathfrak{Q}_0$. Пусть $\mathfrak{s}$ обозначает распределение поля S, которое в каждой из точек $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_h$ принимает значение yz, а во всех остальных точках — значение 0. Тогда правая часть доказываемого равенства равна $(dx)_S(\mathfrak{s}) = (dx)_{L\langle x\rangle}(\mathrm{Sp}_{S/L\langle x\rangle}\mathfrak{s}) = ((dx)_{L\langle x\rangle})^{\mathfrak{Q}_0}(\mathrm{Sp}_{S/L\langle x\rangle} yz)$ (следствие 1 к теореме 6 § 5 гл. IV). По следствию 2 к теореме 1 § 4 гл. V мы имеем $\mathrm{Sp}_{S/L\langle x\rangle} yz = \mathrm{Sp}_{R/K\langle x\rangle} yz$. Таким образом, для доказательства нашего равенства достаточно показать, что $((dx)_{K\langle x\rangle})^{\mathfrak{q}_0}(u) = ((dx)_{L\langle x\rangle})^{\mathfrak{Q}_0}(u)$ при всех $u \in K\langle x\rangle$. В $\mathfrak{q}_0$-адическом пополнении поля $K\langle x\rangle$ мы можем элемент u разложить в степенной ряд по x^{-1}: $u = \sum_{i=-t}^{\infty} c_i x^{-i}$. В силу леммы 4 § 1 обе части доказываемой формулы равны $-c_1$. Этим завершено доказательство первого утверждения теоремы 11.

Обозначим через $\Sigma_s(\mathfrak{p})$ поле тех элементов из поля вычетов точки $\mathfrak{p}$, которые сепарабельны над K, через $\mathfrak{P}_1 = \mathfrak{P}, \ldots, \mathfrak{P}_h$ — все различные точки поля S, лежащие над $\mathfrak{p}$, и через $\Sigma_s(\mathfrak{P}_i)$ — поле тех элементов из поля вычетов точки $\mathfrak{P}_i$, которые сепарабельны над L $(1 \leqslant i \leqslant h)$. Как нам известно (следствие 3 к теореме 3 § 5 гл. V), алгебра $(\Sigma_s(\mathfrak{p}))_L$ является прямой суммой h полей $Z_1', \ldots, Z_h'$, которые изоморфны полям $\Sigma_s(\mathfrak{P}_1), \ldots, \Sigma_s(\mathfrak{P}_h)$ соответственно; более того, существует изоморфизм φ_i' поля Z_i' на $\Sigma_s(\mathfrak{P}_i)$, который на $\Sigma_s(\mathfrak{P})$ индуцирует естественный изоморфизм этого поля в $\Sigma_s(\mathfrak{P}_i)$. Пусть γ — произвольный элемент из $\Sigma_s(\mathfrak{P}_1)$ и пусть ζ — тот элемент из Z_1', который при изоморфизме φ_1' отображается на γ. Элемент ζ мы можем представить в виде

$$\sum_{k=1}^{r} a_k \otimes \xi_k,$$

где $a_k \in L$, $\xi_k \in \Sigma_s(\mathfrak{p})$ $(1 \leqslant k \leqslant r$; знак $\otimes$ обозначает умножение в $(\Sigma_s(\mathfrak{p}))_L$. Обозначим через $\overline{\Sigma_s(\mathfrak{p})}$ подполе $\mathfrak{p}$-адического пополнения $\overline{R}$ поля R, содержащее K и являющееся системой представителей для $\Sigma_s(\mathfrak{p})$ (теорема 1 § 3 гл. III), а через $\overline{\Sigma_s(\mathfrak{P}_i)}$ — подполе $\mathfrak{P}_i$-адического пополнения $\overline{S}_i$ поля S,

содержащее L и являющееся системой представителей для $\Sigma_s(\mathfrak{P}_i)$. Так как поле $\overline{R}$ мы рассматриваем как подполе поля $\overline{S_i}$, то $\overline{\Sigma_s(\mathfrak{p})}$ является, в силу естественного отождествления, подполем поля $\overline{\Sigma_s(\mathfrak{P}_i)}$. Пусть $\overline{\xi_k}$ есть представитель из $\overline{\Sigma_s(\mathfrak{p})}$ для класса ξ_k. Обозначим через $\overline{\gamma_i}$ элемент $\sum_{k=1}^{r} a_k\overline{\xi_k}$, где действия считаются выполненными в поле $\overline{S_i}$; ясно, что $\overline{\gamma_i}$ принадлежит $\overline{\Sigma_s(\mathfrak{P}_i)}$ и что $\overline{\gamma_1}$ является представителем из $\overline{\Sigma_s(\mathfrak{P}_1)}$ для класса γ. С другой стороны, так как $\zeta \in Z_1'$, то элемент $\sum_{k=1}^{r} a_k\varphi_i'(\xi_k)$ из $\Sigma_s(\mathfrak{P}_i)$ равен 0, если только $i > 1$. Отсюда следует, что $\overline{\gamma_i} = 0$ при $i > 1$. Обозначим через $\mathfrak{z}_k$ распределение поля R, которое в точке $\mathfrak{p}$ принимает значение $\overline{\xi_k}$, а во всех других точках — значение 0, и через $\mathfrak{z}$ — распределение поля S, которое в точке $\mathfrak{P}$ принимает значение $\overline{\gamma_1}$, а во всех других точках — значение 0. Из сказанного выше следует, что $\mathfrak{z} = \sum_{k=1}^{r} a_k \operatorname{Cosp}_{R/S} \mathfrak{z}_k$. Таким образом в силу первого утверждения теоремы 11, мы имеем

$$\Omega^{\mathfrak{P}}(\overline{\gamma_1}) = \Omega(\mathfrak{z}) = \sum_{k=1}^{r} a_k\omega(\mathfrak{z}_k) = \sum_{k=1}^{r} a_k \operatorname{Sp}_{\Sigma_s(\mathfrak{p})/K} \xi_k \operatorname{res}_{\mathfrak{p}} \omega.$$

Элемент $\operatorname{Sp}_{\Sigma_s(\mathfrak{p})/K} \xi_k \operatorname{res}_{\mathfrak{p}} \omega$ является следом эндоморфизма поля $\Sigma_s(\mathfrak{p})$ (рассматриваемого как векторное пространство над K), который индуцирован умножением на $\xi_k \operatorname{res}_{\mathfrak{p}} \omega$; ясно, что он является также следом эндоморфизма алгебры $(\Sigma_s(\mathfrak{p}))_L$ (рассматриваемой как векторное пространство над L), индуцированного умножением на $\xi_k \operatorname{res}_{\mathfrak{p}} \omega$. Отсюда следует, что элемент $\Omega^{\mathfrak{P}}(\overline{\gamma_1})$ равен следу θ эндоморфизма алгебры $(\Sigma_s(\mathfrak{p}))_L$, индуцированного умножением на $\zeta \operatorname{res}_{\mathfrak{p}} \omega$. Пространство $(\Sigma_s(\mathfrak{p}))_L$ является прямой суммой полей

$$Z_1', \ldots, Z_h',$$

и умножение на ζ отображает Z_i' на 0 при $i > 1$. Следовательно, $\theta = \operatorname{Sp}_{Z_1'/L} \zeta \operatorname{res}_{\mathfrak{p}} \omega = \operatorname{Sp}_{\Sigma_s(\mathfrak{P}_1)/L} \gamma \operatorname{res}_{\mathfrak{p}} \omega$. Так как

$\Omega^{\mathfrak{P}}(\bar{\gamma}_1) = \mathrm{Sp}_{\Sigma_s(\mathfrak{P}_1)/L}\, \gamma \operatorname{res}_{\mathfrak{p}} \omega$ при любом $\gamma \in \Sigma_s(\mathfrak{P}_1)$, то $\operatorname{res}_{\mathfrak{P}} \Omega = \operatorname{res}_{\mathfrak{p}} \omega$. Таким образом, нами доказано второе утверждение теоремы 11.

Докажем теперь, что $\mathfrak{d}(\Omega)$ является делителем дивизора $\mathrm{Con}_{R/S}\, \mathfrak{d}(\omega)$. Представим дифференциал ω в виде $y(dx)_R$, где x — сепарабельно порождающая переменная поля R и $y \in R$; тогда

$$\mathfrak{d}(\omega) = \mathfrak{d}_R(y)\, \mathfrak{d}\big((dx)_R\big), \quad \mathfrak{d}(\Omega) = \mathfrak{d}_S(y)\, \mathfrak{d}\big((dx)_S\big),$$

где $\mathfrak{d}_R(y)$ и $\mathfrak{d}_S(y)$ обозначают дивизоры элемента y в полях R и S соответственно. Как нам известно $\mathfrak{d}_S(y) = \mathrm{Con}_{R/S}\, \mathfrak{d}_R(y)$ (см. § 7 гл. IV), поэтому, не нарушая общности, мы можем считать, что $\omega = (dx)_R$. Обозначим через $\mathfrak{D}$ дифференту поля R относительно $K\langle x\rangle$, а через $\mathfrak{E}$ — дифференту поля S относительно $L\langle x\rangle$. Тогда по теореме 7 § 3 будем иметь $\mathfrak{d}(\omega) = \mathfrak{D}\mathfrak{n}_R^{-2}$ и $\mathfrak{d}(\Omega) = \mathfrak{E}\mathfrak{n}_S^{-2}$, где $\mathfrak{n}_R$ и $\mathfrak{n}_S$ — дивизоры полюсов элемента x в полях R и S соответственно. Из определений непосредственно следует, что $\mathfrak{n}_S = \mathrm{Con}_{R/S}\mathfrak{n}_R$. Таким образом, мы должны доказать, что $\mathfrak{E}$ является делителем $\mathrm{Con}_{R/S}\, \mathfrak{D}$.

Пусть $\mathfrak{q}_0$ — произвольная точка поля $K\langle x\rangle$; обозначим через E множество всех точек поля R, лежащих над $\mathfrak{q}_0$, и через F — множество всех точек поля S, лежащих над $\mathfrak{q}_0$. Если $\mathfrak{Q} \in F$, то через $m(\mathfrak{Q})$ мы обозначим $\mathfrak{Q}$-показатель дифференты поля S относительно $L\langle x\rangle$. В поле S выберем такой элемент y, что

$$\nu_{\mathfrak{Q}}(y) = -m(\mathfrak{Q})$$

при всех $\mathfrak{Q} \in F$ (см. следствие к теореме 3 § 6 гл. I). Пусть z — произвольный элемент поля R, удовлетворяющий условиям $\nu_{\mathfrak{q}}(z) \geqslant 0$ при всех $\mathfrak{q} \in E$. Тогда мы имеем также $\nu_{\mathfrak{Q}}(z) \geqslant 0$ при всех $\mathfrak{Q} \in F$; применяя лемму 4 § 8 гл. IV, мы видим, что элемент $\mathrm{Sp}_{S/L\langle x\rangle}\, yz$ является целым во всех точках поля $L\langle x\rangle$, лежащих над $\mathfrak{q}_0$. Отметим еще, что если y' есть элемент из R, то $\mathrm{Sp}_{S/L\langle x\rangle}\, y'z = \mathrm{Sp}_{R/K\langle x\rangle}\, y'z$ (следствие 2 к теореме 1 § 4 гл. V). После сделанных замечаний, рассмотрим сначала случай, когда поле L чисто трансцендентно над K. В этом случае над каждой точкой

$\mathfrak{q} \in E$ лежит только одна точка $\mathfrak{Q} \in F$, при этом точка $\mathfrak{Q}$ неразветвлена относительно R (следствие 2 к теореме 3 § 5 гл. V); поэтому элемент y мы можем выбрать в поле R. Применяя опять лемму 4 § 8 гл. IV, получаем, что

$$\nu_{\mathfrak{Q}}(y) \geqslant -m(\mathfrak{q})$$

при всех $\mathfrak{q} \in E$, где через $m(\mathfrak{q})$ обозначен $\mathfrak{q}$-показатель дифференты поля R относительно $K\langle x\rangle$. Отсюда следует, что $m(\mathfrak{Q}) \leqslant m(\mathfrak{q})$, т. е. $\mathfrak{E}$ является делителем дивизора $\mathrm{Con}_{R/S}\,\mathfrak{D}$. Таким образом, для доказательства нашего утверждения в общем случае достаточно рассмотреть случай, когда L алгебраично над K. Будем считать, что имеет место именно этот случай. Элемент y принадлежит полю, полученному из R присоединением конечного числа элементов поля L, поэтому он может быть представлен в виде

$$y = \sum_{i=1}^{n} a_i y_i,$$

где $y_i \in R$ и $a_i \in L$ $(1 \leqslant i \leqslant n)$, при этом можно считать, что элементы $a_1, \ldots, a_n$ линейно независимы над K (лемма 2 § 1 гл. IV). Имеем $\mathrm{Sp}_{S/L\langle x\rangle}\, yz = \sum_{i=1}^{n} a_i \mathrm{Sp}_{R/K\langle x\rangle}\, y_i z$. Последний элемент является целым в каждой точке $\mathfrak{r}$ поля $L\langle x\rangle$, лежащей над $\mathfrak{q}_0$. Мы докажем сейчас, что все элементы $u_i = \mathrm{Sp}_{R/K\langle x\rangle}\, y_i z$ являются целыми в точке $\mathfrak{q}_0$. Можно считать, что $\nu_{\mathfrak{q}_0}(x) \geqslant 0$ (в противном случае мы элемент x заменим на x^{-1}). Пусть G есть неприводимый многочлен с коэффициентами из K, для которого $\nu_{\mathfrak{q}_0}(G(x)) > 0$. Элементы u_i представим в виде $\dfrac{P_i(x)}{Q(x)}$, где $P_1, \ldots, P_n$, Q — многочлены с коэффициентами из K, взаимно простые в совокупности. Утверждаем, что многочлен Q не делится на G. Допустим, что $G = cG_1^{e_1} \ldots G_h^{e_h}$, где $c \in L$, а $G_1, \ldots, G_h$ — различные неприводимые многочлены с коэффициентами из L, старший коэффициент которых равен 1. Каждому G_k соответствует точка $\mathfrak{r}_k$ поля $L\langle x\rangle$, лежащая над $\mathfrak{q}_0$, для которой $\nu_{\mathfrak{r}_k}(G_k(x)) = 1$; ясно, что для этой точки $\nu_{\mathfrak{r}_k}(G(x)) = e_k$. Если бы многочлен Q делился на G,

то мы имели бы $\nu_{\tau_k}\left(\sum_{i=1}^{n} a_i P_i\right) \geqslant e_k$, т. е. многочлен $\sum_{i=1}^{n} a_i P_i$ делился бы на $G_k^{e_k}$ $(1 \leqslant k \leqslant h)$, а значит, и на G. Но элементы $a_1, \ldots, a_n$ линейно независимы над K, поэтому, как легко видеть, отсюда вытекало бы, что все многочлены $P_1, \ldots, P_n$ делятся на G, что невозможно. Таким образом, мы видим, что для любого элемента $z \in R$, целого во всех точках $\mathfrak{q} \in E$, элементы $\mathrm{Sp}_{R/K\langle x\rangle}\, y_i z$ являются целыми в точке $\mathfrak{q}_0$. Это означает, что

$$\nu_{\mathfrak{q}}(y_i) \geqslant -m(\mathfrak{q}) \quad (1 \leqslant i \leqslant n)$$

для всех точек $\mathfrak{q} \in E$. Обозначим через $e(\mathfrak{Q})$ индекс разветвления точки $\mathfrak{Q} \in F$ относительно R; тогда

$\nu_{\mathfrak{Q}}(y_i) \geqslant -e(\mathfrak{Q})\, m(\mathfrak{q})$, откуда $-m(\mathfrak{Q}) = \nu_{\mathfrak{Q}}(y) \geqslant -e(\mathfrak{Q})\, m(\mathfrak{q})$, и дивизор $\mathrm{Con}_{R/S}\, \mathfrak{D}$ делится на $\mathfrak{E}$.

Если R и S имеют один и тот же род g, то дивизоры $\mathfrak{d}(\Omega)$ и $\mathfrak{d}(\omega)$ имеют одну и ту же степень $2g-2$. Применяя следствие к теореме 2 § 4 гл. V, получаем, что степень дивизора $\mathrm{Con}_{R/S}\, \mathfrak{d}(\omega)$ также равна $2g-2$, т. е. равна степени дивизора $\mathfrak{d}(\Omega)$. Отсюда непосредственно следует, что $\mathfrak{d}(\Omega) = \mathrm{Con}_{R/S}\, \mathfrak{d}(\omega)$. Теорема 11 теперь доказана полностью.

Следствие 1. *При обозначениях теоремы* 11 *род поля S не превосходит рода поля R.*

Обозначим через g род поля R, а через G — род поля S. Если ω есть дифференциал поля R, отличный от 0, то, как мы видели в конце доказательства теоремы 11, дивизоры $\mathrm{Con}_{R/S}\, \mathfrak{d}(\omega)$ и $\mathfrak{d}(\Omega)$ имеют степени $2g-2$ и $2G-2$ соответственно. Следствие 1 вытекает теперь непосредственно из третьего утверждения теоремы 11. Таким образом, теорема 11 дает нам новое доказательство первой части теоремы 5 § 6 гл. V.

Следствие 2. *Пусть сохраняются обозначения теоремы* 11. *Тогда каждый дифференциал первого рода поля S есть линейная комбинация с коэффициентами из L коследов (из R в S) дифференциалов первого рода поля R.*

Пусть Ω — дифференциал первого рода поля S. Если x есть сепарабельно порождающая переменная поля R, то дифференциал Ω мы можем представить в виде $\Omega = y(dx)_S$,

где $y \in S$. Так как $\mathfrak{d}((dx)_S)$ является делителем дивизора $\mathrm{Con}_{R/S}\mathfrak{d}((dx)_R)$, то дифференциал $(dx)_S$ не имеет переменных точек относительно R в качестве своих нулей, откуда следует, что элемент y не имеет переменных точек относительно R в качестве своих полюсов. Если $(a_i)_{i \in I}$ есть базис поля L относительно K (I — некоторое множество индексов), то элемент y можно представить в виде $\sum_{i \in I} a_i y_i$, где $y_i \in R$ (см. замечание после следствия 2 к теореме 4 § 6 гл. V). Полагая $\omega_i = y_i (dx)_R$, мы получим, что $\Omega = \sum_{i \in I} a_i \mathrm{Cosp}_{R/S}\omega_i$. Если $\mathfrak{x}$ — произвольное распределение поля R, не имеющее полюсов, то $\mathrm{Cosp}_{R/S}\mathfrak{x}$ также не имеет полюсов (в поле S) и, следовательно, $0 = \Omega(\mathrm{Cosp}_{R/S}\mathfrak{x}) = \sum_{i \in I} a_i \omega_i(\mathfrak{x})$. Так как $\omega_i(\mathfrak{x}) \in K$ при всех $i \in I$, то $\omega_i(\mathfrak{x}) = 0$ при всех $i \in I$. Это означает, что все дифференциалы ω_i — первого рода.

Следствие 3. *Сохраняя обозначения теоремы* 11, *предположим, что поле L совершенно. Если точка $\mathfrak{P}$ поля S неразветвлена относительно R, то поле вычетов точки $\mathfrak{p}$ поля R, лежащей под $\mathfrak{P}$, сепарабельно над K.*

Пусть x — униформизирующая переменная в точке $\mathfrak{p}$ поля R, а значит, и в точке $\mathfrak{P}$ поля S. Так как поле L совершенно, то поле вычетов точки $\mathfrak{P}$ сепарабельно над L. Применяя теорему 5 § 3 и теорему 11, получаем, что $\mathrm{res}_{\mathfrak{p}} x^{-1}(dx)_R = \mathrm{res}_{\mathfrak{P}} x^{-1}(dx)_S = 1 \neq 0$, и наше утверждение следует из теоремы 5 § 3.

Следствие 4. *Для любой точки $\mathfrak{p}$ сепарабельно порождаемого поля R алгебраических функций от одной переменной с полем констант K существует алгебраическое чисто несепарабельное расширение L поля K конечной степени, для которого поле вычетов точки $\mathfrak{P}$ поля $R\langle L\rangle$, лежащей над $\mathfrak{p}$, сепарабельно над L.*

Пусть $\bar{K}$ — алгебраически замкнутое расширение поля K и пусть L_1 — наименьшее совершенное подполе поля $\bar{K}$, содержащее K; тогда L_1 чисто несепарабельно над K. Обозначим через $\mathfrak{P}_1$ точку поля $R\langle L_1\rangle$, лежащую над $\mathfrak{p}$, а через x — униформизирующую переменную в точке $\mathfrak{P}_1$ поля $R\langle L_1\rangle$. Элемент x принадлежит полю, которое может быть

получено из R присоединением конечного числа элементов $a_1, \ldots, a_m$ из L_1. Из следствия 3 теперь легко вытекает, что поле $L = K\langle a_1, \ldots, a_m\rangle$ обладает требуемыми свойствами.

Замечание. Используя обозначение из доказательства третьего утверждения теоремы 11, мы видим, что

$$\mathfrak{d}(\Omega)\left(\mathrm{Con}_{R/S}\mathfrak{d}(\omega)\right)^{-1} = \mathfrak{d}\left((dx)_S\right)\left(\mathrm{Con}_{R/S}\mathfrak{d}\left((dx)_R\right)\right)^{-1}.$$

Пусть поля R и S фиксированы, тогда левая часть последнего равенства зависит только от ω, в то время как правая часть зависит только от x. Отсюда следует, что дивизор $\mathfrak{M} = \mathfrak{d}(\Omega)\left(\mathrm{Con}_{R/S}\mathfrak{d}(\omega)\right)^{-1}$ зависит только от полей R и S. Формула $\mathfrak{d}(\Omega) = \mathfrak{M}\,\mathrm{Con}_{R/S}\mathfrak{d}(\omega)$ показывает нам, что $\mathfrak{M}$ является аналогом дифференты сепарабельного расширения конечной степени (см. теорема 2 § 2); однако в отличие от дифференты (которая является целым дивизором) дивизор $\mathfrak{M}$ является обратным для целого.

Теорема 12. *Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной и пусть S — расширение поля R конечной степени. Если ω есть дифференциал поля R, а z — элемент поля S, то имеет место формула:* $\mathrm{Sp}_{S/R}\left(z\,\mathrm{Cosp}_{R/S}\omega\right) = \left(\mathrm{Sp}_{S/R}z\right)\omega$.

Пусть x — сепарабельно порождающая переменная поля R. Тогда $\omega = y(dx)_R$, где $y \in R$, и, значит, $\mathrm{Cosp}_{R/S}\omega = y(dx)_S$. Так как $\mathrm{Sp}_{S/R}yz = y\mathrm{Sp}_{S/R}z$, то теорему 12 достаточно доказать для случая, когда $\omega = (dx)_R$.

Пусть $\mathfrak{x}$ — произвольное распределение поля R. Тогда $\left(\mathrm{Sp}_{S/R}\left(z(dx)_S\right)\right)(\mathfrak{x}) = \mathrm{Sp}_{L/K}\left((dx)_S\left(z\,\mathrm{Cosp}_{R/S}\mathfrak{x}\right)\right)$, где K и L — поля констант полей R и S соответственно. Так как $(dx)_S = \mathrm{Cosp}_{L\langle x\rangle/S}(dx)_{L\langle x\rangle}$, то

$$\mathrm{Sp}_{L/K}\left((dx)_S\left(z\,\mathrm{Cosp}_{R/S}\mathfrak{x}\right)\right) = \\ = \mathrm{Sp}_{L/K}\left((dx)_{L\langle x\rangle}\left(\mathrm{Sp}_{S/L\langle x\rangle}z\,\mathrm{Cosp}_{R/S}\mathfrak{x}\right)\right) \quad (1)$$

(здесь мы использовали первое определение коследа; см. § 2). Если мы положим $\mathfrak{y} = \mathrm{Sp}_{S/L\langle x\rangle}\left(z\,\mathrm{Cosp}_{R/S}\mathfrak{x}\right)$, то будем иметь $\left(\mathrm{Sp}_{S/R}\left(z(dx)_S\right)\right)(\mathfrak{x}) = \mathrm{Sp}_{L/K}\left((dx)_{L\langle x\rangle}(\mathfrak{y})\right)$. Утверждаем теперь, что правая часть последнего равенства

равна $(dx)_{K\langle x\rangle}(\mathrm{Sp}_{L\langle x\rangle/K\langle x\rangle}\mathfrak{y})$. Обозначим через $\mathfrak{p}$ полюс элемента x в поле $K\langle x\rangle$, а через $\mathfrak{P}$ — его полюс в $L\langle x\rangle$. Из теоремы 2 § 5 гл. II легко следует, что в поле $L\langle x\rangle$ существует такой элемент u, что $\nu_{\mathfrak{Q}}(\mathfrak{y}-u)\geqslant 0$ для всех точек $\mathfrak{Q}\neq\mathfrak{P}$ поля $L\langle x\rangle$ (здесь мы обозначили одной и той же буквой u элемент поля $L\langle x\rangle$ и главное распределение поля $L\langle x\rangle$, соответствующее этому элементу. Если $\mathfrak{y}'=\mathfrak{y}-u$, то $(dx)_{L\langle x\rangle}(\mathfrak{y})=(dx)_{L\langle x\rangle}(\mathfrak{y}')$. Положим

$$\mathfrak{y}'(\mathfrak{P})=\sum_{k=-m}^{1}c_kx^{-k}+x^{-2}w,$$

где w—целый элемент из $\mathfrak{P}$-адического пополнения поля $L\langle x\rangle$. Тогда $(dx)_{L\langle x\rangle}(\mathfrak{y}')=-c_1$ (лемма 4 § 1), откуда

$$\mathrm{Sp}_{L/K}((dx)_{L\langle x\rangle}(\mathfrak{y}))=-\mathrm{Sp}_{L/K}c_1.$$

Далее, $\mathrm{Sp}_{L\langle x\rangle/K\langle x\rangle}\mathfrak{y}=\mathrm{Sp}_{L\langle x\rangle/K\langle x\rangle}\mathfrak{y}'+\mathrm{Sp}_{L\langle x\rangle/K\langle x\rangle}u$, а, следовательно, $(dx)_{K\langle x\rangle}(\mathrm{Sp}_{L\langle x\rangle/K\langle x\rangle}\mathfrak{y})=(dx)_{K\langle x\rangle}(\mathrm{Sp}_{L\langle x\rangle/K\langle x\rangle}\mathfrak{y}')$. Если $\mathfrak{q}$ есть точка поля $K\langle x\rangle$, отличная от $\mathfrak{p}$, то $\nu_{\mathfrak{Q}}(\mathfrak{y}')\geqslant 0$ для каждой точки $\mathfrak{Q}$ поля $L\langle x\rangle$, лежащей над $\mathfrak{q}$, откуда $\nu_{\mathfrak{q}}(\mathrm{Sp}_{L\langle x\rangle/K\langle x\rangle}\mathfrak{y}')\geqslant 0$ (см. следствие 1 к теореме 5 § 5 гл. IV). Поэтому $(dx)_{K\langle x\rangle}(\mathrm{Sp}_{L\langle x\rangle/K\langle x\rangle}\mathfrak{y}')=((dx)_{K\langle x\rangle})^{\mathfrak{p}}(v)$, где v — $\mathfrak{p}$-компонента распределения $\mathrm{Sp}_{L\langle x\rangle/K\langle x\rangle}\mathfrak{y}'$. Обозначим через $\overline{K\langle x\rangle}$ $\mathfrak{p}$-адическое пополнение поля $K\langle x\rangle$, а через $\overline{L\langle x\rangle}$ — $\mathfrak{P}$-адическое пополнение поля $L\langle x\rangle$. Так как $\mathfrak{P}$ есть единственная точка поля $L\langle x\rangle$, лежащая над $\mathfrak{p}$, то

$$v=\sum_{k=-m}^{1}(\mathrm{Sp}_{\overline{L\langle x\rangle}/\overline{K\langle x\rangle}}c_k)x^{-k}+x^{-2}\mathrm{Sp}_{\overline{L\langle x\rangle}/\overline{K\langle x\rangle}}w.$$

Как мы знаем, $\mathrm{Sp}_{\overline{L\langle x\rangle}/\overline{K\langle x\rangle}}w$ есть целый элемент поля $\overline{K\langle x\rangle}$. С другой стороны, всякий базис поля L относительно K является также базисом поля $L\langle x\rangle$ относительно $K\langle x\rangle$ (леммы 2 и 3 § 1 гл. IV), а значит, и базисом поля $\overline{L\langle x\rangle}$ относительно $\overline{K\langle x\rangle}$ (теорема 4 § 5 гл. IV). Отсюда непосредственно следует, что $\mathrm{Sp}_{\overline{L\langle x\rangle}/\overline{K\langle x\rangle}}c_k=\mathrm{Sp}_{L/K}c_k$. Применяя

опять лемму 4 § 1, получаем, что $\left((dx)_{K\langle x\rangle}\right)^{\mathfrak{p}}(v) = -\operatorname{Sp}_{L/K} c_1$. Таким образом, формула $\operatorname{Sp}_{L/K}\left((dx)_{L\langle x\rangle}(\mathfrak{y})\right) = (dx)_{K\langle x\rangle}\left(\operatorname{Sp}_{L\langle x\rangle/K\langle x\rangle}\mathfrak{y}\right)$ доказана. Вернемся теперь к равенству (1). Применяя лемму 3 § 7 гл. IV, получаем

$$\operatorname{Sp}_{L/K}(dx)_S\left(z\operatorname{Cosp}_{R/S}\mathfrak{x}\right) = \left((dx)_{K\langle x\rangle}\right)\left(\operatorname{Sp}_{S/K\langle x\rangle} z\operatorname{Cosp}_{R/S}\mathfrak{x}\right) = (dx)_{K\langle x\rangle}\left(\operatorname{Sp}_{R/K\langle x\rangle}\left(\operatorname{Sp}_{S/R} z\operatorname{Cosp}_{R/S}\mathfrak{x}\right)\right).$$

Так как $(dx)_R = \operatorname{Cosp}_{K\langle x\rangle/R}(dx)_{K\langle x\rangle}$, то это равно

$$(dx)_R\left(\operatorname{Sp}_{S/R} z\left(\operatorname{Cosp}_{R/S}\mathfrak{x}\right)\right) = (dx)_R\left(\left(\operatorname{Sp}_{S/R} z\right)(\mathfrak{x})\right) = \left(\left(\operatorname{Sp}_{S/R} z\right)(dx)_R\right)(\mathfrak{x}).$$

Так как левая часть равенства (1) равна $\left(\operatorname{Sp}_{S/R}\left(z\,(dx)_S\right)\right)(\mathfrak{x})$, то теорема 12, следовательно, доказана.

§ 7. Дифференцирования поля констант

Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной и пусть D — дифференцирование его поля констант K. Дифференцирование D можно продолжить (бесконечным числом способов) до дифференцирования поля R. Если x — произвольная сепарабельно порождающая переменная, то существует единственное дифференцирование поля R, совпадающее на K с D и отображающее x на 0 (лемма 7 § 4). Это дифференцирование будем обозначать через D^x. Каждый дифференциал ω поля R мы можем представить в виде $y\,dx$, где $y \in R$. Определим дифференциал $D^x\omega$ равенством:

$$D^x\omega = \left(D^x y\right)dx.$$

Этим задано некоторое отображение D^x (нелинейное) пространства дифференциалов поля R в себя. Для любого элемента $z \in R$ имеем

$$D^x(z\omega) = \left(D^x z\right)\omega + z\left(D^x\omega\right).$$

В самом деле, левая часть этого равенства равна

$$\left(D^x(zy)\right)dx = \left(\left(D^x z\right)y + z\left(D^x y\right)\right)dx,$$

что равно также и правой части.

Лемма 1. *Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной и D — дифференцирование поля констант K поля R. Если x есть сепарабельно порождающая переменная поля R, то через D^x обозначим дифференцирование поля R, которое является продолжением D и отображает x на 0. Утверждается, что D^x коммутирует с дифференцированием поля R по x (т. е. с дифференцированием D_x, которое все элементы из K отображает на 0, а x — на 1).*

Оператор $\Delta = D^x D_x - D_x D^x$ является дифференцированием поля R (см. § 4). Легко видеть, что Δ отображает на 0 все элементы поля K и x, а значит, и все элементы из $K\langle x\rangle$ (лемма 1 § 4). Применяя лемму 2 § 4, заключаем, что $\Delta = 0$.

Лемма 2. *При обозначениях леммы 1 имеем $D^x(dz) = d(D^x z)$, где z — произвольный элемент из R.*

Действительно, $dz = (D_x z)\,dx$ (теорема 9 § 5), откуда, по лемме 1, $D^x(dz) = (D^x D_x z)\,dx = (D_x D^x z)\,dx = d(D^x z)$.

Лемма 3. *Пусть сохраняются обозначения леммы 1 и пусть x' — любая другая сепарабельно порождающая переменная поля R. Тогда для всякого дифференциала ω поля R разность $D^x\omega - D^{x'}\omega$ является точным дифференциалом.*

Пусть $\omega = y\,dx = y'dx'$, где y и y' — элементы из R. Дифференцирование $D^{x'} - D^x - (D^{x'}x)D_x$ отображает x и все элементы из K на 0, а потому оно является нулевым дифференцированием (см. доказательство леммы 1); таким образом, $D^{x'}y' = D^x y' + (D^{x'}x)D_x y'$ и $0 = D^{x'}x' = D^x x' + (D^{x'}x)D_x x'$. Так как $D^{x'}\omega = (D^{x'}y')\,dx'$ и $dx' = (D_x x')\,dx$ (теорема 9 § 5), то

$$D^{x'}\omega = (D^x y')(D_x x')\,dx - (D^x x')(D_x y')\,dx.$$

С другой стороны, так как $y = y'(D_x x')$, то, применяя лемму 1, получаем

$$D^x\omega = (D^x y)\,dx = (D^x y')(D_x x')\,dx + y'(D^x D_x x')\,dx = \\ = (D^x y')(D_x x')\,dx + y'(D_x D^x x')\,dx.$$

Отсюда следует, что $D^x\omega - D^{x'}\omega = y'(D_x D^x x')\,dx + (D^x x')(D_x y')\,dx = (D_x(y' D^x x'))\,dx$, и лемма 3 доказана.

Лемма 4. Сохраняя обозначения леммы 1, *обозначим через* ω *дифференциал поля* R, *через* $\mathfrak{p}$ — *точку поля* R *и через* u — *элемент из* $\mathfrak{p}$-*адического пополнения* $\bar{R}$ *поля* R. *Тогда* $D(\omega^{\mathfrak{p}}(u)) = (D^x\omega)^{\mathfrak{p}}(u) + \omega^{\mathfrak{p}}(D^x u)$.

Здесь $D^x u$ обозначает результат применения к элементу u непрерывного дифференцирования поля $\bar{R}$, продолжающего дифференцирование D^x (см. лемма 5 § 4).

Положим $\omega = y\,dx$, где $y \in R$. Формула, подлежащая доказательству, принимает тогда вид $D((dx)^{\mathfrak{p}}(yu)) = (dx)^{\mathfrak{p}}((D^x y)u + y(D^x u))$ или $D((dx)^{\mathfrak{p}}(v)) = (dx)^{\mathfrak{p}}(D^x v)$, где $v = yu$. Пусть $\mathfrak{p}_0$ есть точка поля $K\langle x\rangle$, лежащая под $\mathfrak{p}$, а w — след элемента v из $\bar{R}$ в $\mathfrak{p}_0$-адическое пополнение поля $K\langle x\rangle$. Тогда, в силу леммы 3 § 4, наша формула принимает вид $D(((dx)_{K\langle x\rangle})^{\mathfrak{p}_0}(w)) = ((dx)_{K\langle x\rangle})^{\mathfrak{p}_0}(D^x w)$.

Предположим сначала, что $\mathfrak{p}_0$ есть полюс $\mathfrak{q}_0$ элемента x в поле $K\langle x\rangle$. Элемент w мы можем представить в виде $w = \sum_{k=-m}^{\infty} c_k x^{-k}$, где $c_k \in K$. Применяя формулу (5) § 4, получаем, что $D^x w = \sum_{k=-m}^{\infty} (Dc_k)\,x^{-k}$. Таким образом, обе части доказываемой формулы равны $-Dc_1$. Предположим теперь, что $\mathfrak{p}_0 \neq \mathfrak{q}_0$. В поле $K\langle x\rangle$ мы можем найти элемент z, не имеющий кроме, быть может, $\mathfrak{p}_0$ и $\mathfrak{q}_0$ других полюсов и такой, что $\nu_{\mathfrak{p}_0}(w - z) \geqslant 0$. Тогда будем иметь

$$((dx)_{K\langle x\rangle})^{\mathfrak{p}_0}(w) = ((dx)_{K\langle x\rangle})^{\mathfrak{p}_0}(z) = -((dx)_{K\langle x\rangle})^{\mathfrak{q}_0}(z).$$

С другой стороны, для любой точки $\mathfrak{r}_0$ поля $K\langle x\rangle$, отличной от $\mathfrak{q}_0$, дифференцирование D^x отображает кольцо $\mathfrak{o}$ этой точки в себя. Действительно, каждый элемент из $\mathfrak{o}$ представим в виде дроби $\frac{P(x)}{Q(x)}$, где P и Q — многочлены с коэффициентами из K, причем $\nu_{\mathfrak{r}_0}(Q(x)) = 0$. Так как $D^x\left(\frac{P(x)}{Q(x)}\right)$ равно отношению многочлена от x на $Q^2(x)$, то

$D^x(\mathfrak{o})\subset\mathfrak{o}$. Отсюда следует, что $D^x z$ не имеет других полюсов кроме, быть может, $\mathfrak{p}_0$ и $\mathfrak{q}_0$, а также, что $D^x w - D^x z$ есть целый элемент $\mathfrak{p}_0$-адического пополнения поля $K\langle x\rangle$. Получаем теперь $((dx)_{K\langle x\rangle})^{\mathfrak{p}_0}(D^x w) = -((dx)_{K\langle x\rangle})^{\mathfrak{q}_0}(D^x z)$. Так как нами уже установлено, что $D(((dx)_{K\langle x\rangle})^{\mathfrak{q}_0}(z)) = ((dx)_{K\langle x\rangle})^{\mathfrak{q}_0}(D^x z)$ то наша формула, следовательно, доказана полностью.

Теорема 13. *Пусть R — сепарабельно порождаемое поле алгебраических функций от одной переменной и D — дифференцирование поля констант K поля R. Обозначим через x какую-нибудь сепарабельно порождающую переменную поля R и через D^x — дифференцирование поля R, которое на K совпадает с D и отображает x на 0. Пусть $\mathfrak{p}$ — точка поля R; через Σ_s обозначим подполе тех элементов из поля вычетов точки $\mathfrak{p}$, которые сепарабельны над K. Дифференцирование поля Σ_s, являющееся продолжением дифференцирования D поля K, обозначим также через D. Тогда для любого дифференциала ω поля R имеем:* $\operatorname{res}_{\mathfrak{p}} D^x\omega = D(\operatorname{res}_{\mathfrak{p}}\omega)$.

Построим $\mathfrak{p}$-адическое пополнение $\bar{R}$ поля R и обозначим через $\bar{\Sigma}_s$ подполе поля $\bar{R}$, содержащее K и являющееся системой представителей для Σ_s (теорема 1 § 3 гл. III). Диффернецирование D^x можно продолжить до непрерывного дифференцирования поля $\bar{R}$, которое мы обозначим также через D^x (лемма 5 § 4). Дифференцирование D поля K может быть продолжено до дифференцирования поля $\bar{\Sigma}_s$, которое, в силу леммы 2 § 4, должно совпадать с ограничением D^x на поле $\bar{\Sigma}_s$. Ясно, что если $\bar{\xi}$ — представитель из $\bar{\Sigma}_s$ для класса $\xi\in\Sigma_s$, то $D^x\bar{\xi}$ является представителем для $D\xi$. Пусть теперь γ — произвольный элемент из Σ_s, а $\bar{\gamma}$ — его представитель из $\bar{\Sigma}_s$. Если ρ есть вычет дифференциала ω в точке $\mathfrak{p}$, то $D(\omega^{\mathfrak{p}}(\bar{\gamma})) = D(\operatorname{Sp}_{\Sigma_s/K}\gamma\rho)$. Правая часть этого равенства, в силу леммы 3 § 4, равна

$$\operatorname{Sp}_{\Sigma_s/K} D(\gamma\rho) = \operatorname{Sp}_{\Sigma_s/K}(D\gamma)\rho + \operatorname{Sp}_{\Sigma_s/K}\gamma(D\rho) = \\ = \omega^{\mathfrak{p}}(D^x\bar{\gamma}) + \operatorname{Sp}_{\Sigma_s/K}\gamma(D\rho).$$

С другой стороны, по лемме 4,

$$D(\omega^{\mathfrak{p}}(\bar{\gamma})) = (D^x\omega)^{\mathfrak{p}}(\bar{\gamma}) + \omega^{\mathfrak{p}}(D^x\bar{\gamma});$$

следовательно, $(D^x\omega)^{\mathfrak{p}}(\bar{\gamma}) = \mathrm{Sp}_{\Sigma_s/K}\gamma(D\rho)$. Так как последнее равенство справедливо при любом γ из Σ_s, то отсюда следует, что $\mathrm{res}_{\mathfrak{p}} D^x\omega = D\rho$.

§ 8. Дифференциалы второго рода

В этом параграфе мы ограничимся рассмотрением полей только нулевой характеристики. [1])

Дифференциал второго рода поля алгебраических функций от одной переменной был определен нами как дифференциал, все вычеты которого равны 0; в частности, каждый дифференциал первого рода является дифференциалом второго рода. Из теоремы 5 § 3 следует, что все точные дифференциалы являются дифференциалами второго рода. Очевидно, что все дифференциалы второго рода образуют векторное пространство над полем констант рассматриваемого поля. Главной целью настоящего параграфа является вычисление размерности фактор-пространства пространства дифференциалов второго рода по подпространству точных дифференциалов.

Пусть R и S — поля алгебраических функций от одной переменной характеристики 0, причем R является подполем поля S и поле констант K поля R равно пересечению поля R с полем констант L поля S. Тогда, если ω — дифференциал второго рода поля R, то $\mathrm{Cosp}_{R/S}\omega$ есть дифференциал второго рода поля S. Действительно, пусть $T = R\langle L\rangle$, тогда $\theta = \mathrm{Cosp}_{R/T}\omega$ — второго рода по теореме 11 § 6, и $\mathrm{Cosp}_{R/S}\omega = \mathrm{Cosp}_{T/S}\theta$ — второго рода по теореме 3 § 2. С другой стороны, если S имеет конечную степень над R и если Ω — дифференциал второго рода поля S, то, как это следует из теоремы 1 § 2, $\mathrm{Sp}_{S/R}\Omega$ есть дифференциал второго рода поля R.

Теорема 14. *Пусть R — поле алгебраических функций от одной переменной характеристики 0 и пусть ω — диф-*

---

[1]) См. примечание на стр. 10. (*Прим. перев.*)

ференциал поля R. Тогда для произвольной точки $\mathfrak{p}$ поля R существует такой элемент $x \in R$, что $\nu_{\mathfrak{p}}(\omega - dx) \geqslant -1$. Для того чтобы в R существовал элемент x, удовлетворяющий условию $\nu(\omega - dx) \geqslant 0$, необходимо и достаточно, чтобы $\operatorname{res}_{\mathfrak{p}}\omega = 0$. Если последнее условие выполнено, то для каждого целого числа n существует такой элемент $x_n \in R$, что

$$\nu_{\mathfrak{p}}(\omega - dx_n) \geqslant n.$$

Выбрав униформизирующую переменную t в точке $\mathfrak{p}$ поля R, представим дифференциал ω в виде $\omega = y\,dt$, где $y \in R$. Обозначим через Σ поле вычетов точки $\mathfrak{p}$, через $\bar{R}$ — $\mathfrak{p}$-адическое пополнение поля R и через $\bar{\Sigma}$ — подполе поля $\bar{R}$, содержащее K и являющееся системой представителей для Σ (теорема 1 § 3 гл. III). Как мы знаем, поле $\bar{R}$ может быть отождествлено с полем формальных степенных рядов от t с коэффициентами из $\bar{\Sigma}$ (§ 3 гл. III), и элемент y можно представить в виде $\sum_{k=-m}^{\infty} c_k t^k$, где m — некоторое положительное целое число. Для каждого целого $n \geqslant -m$ мы можем найти элемент $x_n \in R$, имеющий разложение вида $\sum_{k=1-m}^{\infty} c'_k t^k$, где $c'_k \in \bar{\Sigma}$ и $kc'_k = c_{k-1}$ при $1-m \leqslant k \leqslant n$, $k \neq 0$. Если D_t есть дифференцирование по t поля R, то, в силу формулы (5) § 4, $D_t x_n = \sum_{k=1-m}^{\infty} kc'_k t^{k-1}$, откуда $\nu_{\mathfrak{p}}(y - D_t x_n - c_{-1}t^{-1}) \geqslant n$. Но $\nu_{\mathfrak{p}}(dt) \geqslant 0$, поэтому получаем $\nu_{\mathfrak{p}}(\omega - dx_n - c_{-1}t^{-1}\,dt) \geqslant n$. В частности, $\nu_{\mathfrak{p}}(\omega - dx_{-1}) \geqslant -1$. Будем считать теперь, что $n \geqslant 0$. Тогда $\operatorname{res}_{\mathfrak{p}}(\omega - dx_n - c_{-1}t^{-1}\,dt) = 0$, а так как $\operatorname{res}_{\mathfrak{p}} dx_n = 0$, то $\operatorname{res}_{\mathfrak{p}}\omega = c_{-1}\operatorname{res}_{\mathfrak{p}} t^{-1}\,dt = c_{-1}$ (теорема 5 § 3). Таким образом, если $\operatorname{res}_{\mathfrak{p}}\omega = 0$, то $\nu_{\mathfrak{p}}(\omega - dx_n) \geqslant n$. Обратно, если в поле R существует элемент x такой, что $\nu_{\mathfrak{p}}(\omega - dx) \geqslant 0$, то $\operatorname{res}_{\mathfrak{p}}\omega = \operatorname{res}_{\mathfrak{p}} dx = 0$. Теорема 14, следовательно, доказана.

Лемма 1. *Пусть $\mathfrak{p}$ — точка поля R алгебраических функций от одной переменной характеристики 0 и пусть x — элемент из R. Если $\nu_{\mathfrak{p}}(x) \geqslant 0$, то $\nu_{\mathfrak{p}}(dx) \geqslant 0$. Если $\nu_{\mathfrak{p}}(x) \neq 0$, то $\nu_{\mathfrak{p}}(dx) = \nu_{\mathfrak{p}}(x) - 1$.*

Первое утверждение, справедливое без каких-либо предположений о характеристике поля R, нами уже доказано (следствие к теореме 7 § 3). Если $\nu_{\mathfrak{p}}(x) \neq 0$, то индекс разветвления точки $\mathfrak{p}$ относительно $K(x)$ равен $|\nu_{\mathfrak{p}}(x)|$. В силу теоремы 7 § 8 гл. IV, отсюда следует, что $\mathfrak{p}$-показатель дифференты поля R относительно $K(x)$ равен $|\nu_{\mathfrak{p}}(x)|-1$. В дивизор полюсов элемента x точка $\mathfrak{p}$ входит с показателем 0, если $\nu_{\mathfrak{p}}(x) > 0$, и с показателем $-\nu_{\mathfrak{p}}(x)$, если $\nu_{\mathfrak{p}}(x) < 0$; в обоих случаях этот показатель равен $\frac{|\nu_{\mathfrak{p}}(x)|-\nu_{\mathfrak{p}}(x)}{2}$. Второе утверждение леммы 1 следует теперь непосредственно из теоремы 7 § 3.

Лемма. 2. *Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ — различные точки поля R алгебраических функций от одной переменной характеристики 0 и пусть $\mathfrak{M}$ — некоторое векторное пространство дифференциалов поля R (над полем констант K поля R), содержащее все дифференциалы, которые делятся на $(\mathfrak{p}_1 \ldots \mathfrak{p}_m)^{-1}$, и состоящее из дифференциалов, вычеты которых в точках $\mathfrak{p} \neq \mathfrak{p}_i (i=1, \ldots, m)$ равны 0. Если $\mathfrak{N}$ есть подпространство тех дифференциалов пространства $\mathfrak{M}$, вычеты которых в точках $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ равны 0, то размерность фактор-пространства $\mathfrak{M}/\mathfrak{N}$ конечна и равна* $\max\left\{0, \left(\sum_{i=1}^{m} d(\mathfrak{p}_i)\right)-1\right\}$.

Обозначим через Σ_i поле вычетов точки $\mathfrak{p}_i (1 \leqslant i \leqslant m)$ и рассмотрим векторное пространство $\prod_{i=1}^{m} \Sigma_i$ над K. Каждому $\omega \in \mathfrak{M}$ поставим в соответствие элемент $\Phi(\omega)$ из $\prod_{i=1}^{m} \Sigma_i$, у которого Σ_i-координата равна $\operatorname{res}_{\mathfrak{p}_i}\omega$ для всех i. Этим определено линейное отображение Φ пространства $\mathfrak{M}$ в $\prod_{i=1}^{m} \Sigma_i$, ядром которого является $\mathfrak{N}$. Из теоремы 4 § 5 гл. III непосредственно следует, что $\Phi(\mathfrak{M})$ есть подпространство пространства $\prod_{i=1}^{m} \Sigma_i$, состоящее из тех элементов $(\rho_1, \ldots, \rho_m)$, которые удовлетворяют условию $\sum_{i=1}^{m} \operatorname{Sp}_{\Sigma_i/K} \rho_i = 0$. Отображение

$(\rho_1, \ldots, \rho_m) \to \sum_{i=1}^{m} \mathrm{Sp}_{\Sigma_i/K} \rho_i$ есть линейная функция на пространстве $\prod_{i=1}^{m} \Sigma_i$, которая при $m \neq 0$ не равна тождественно нулю. Отсюда легко следует, что $\dim(\mathfrak{M}/\mathfrak{N}) = \dim \Phi(\mathfrak{M}) = \max\left\{0, \left(\sum_{i=1}^{m} d(\mathfrak{p}_i)\right) - 1\right\}$.

Теорема 15. *Пусть R — поле алгебраических функций от одной переменной характеристики 0, и пусть P и Q — два непересекающихся конечных множества точек поля R. Обозначим через $\mathfrak{D}$ пространство тех дифференциалов поля R, которые не имеют полюсов среди точек множества P и вычеты которых во всех точках, не принадлежащих Q, равны 0. Обозначим, далее, через $\mathfrak{E}$ пространство точных дифференциалов, соответствующих тем элементам поля R, для которых все точки из P являются нулями. Тогда размерность фактор-пространства $\mathfrak{D}/\mathfrak{E}$ конечна и равна $2g+p+q$, где g — род поля R, $p = \max\left\{0, \left(\sum_{\mathfrak{p} \in P} d(\mathfrak{p})\right) - 1\right\}$ и $q = \max\left\{0, \left(\sum_{\mathfrak{q} \in Q} d(\mathfrak{q})\right) - 1\right\}$.*

Обозначим через $\mathfrak{D}'$ пространство тех дифференциалов из $\mathfrak{D}$, вычеты которых во всех точках $\mathfrak{q} \in Q$ равны 0 (значит, $\mathfrak{D}'$ есть пространство дифференциалов второго рода, принадлежащих $\mathfrak{D}$), а через $\mathfrak{E}'$ — пространство точных дифференциалов, не имеющих полюсов в множестве P. В силу леммы 2 размерность пространства $\mathfrak{D}/\mathfrak{D}'$ конечна и равна q.

Для вычисления размерности пространства $\mathfrak{D}'/\mathfrak{E}'$ введем следующее понятие. Целый дивизор $\mathfrak{a}$ поля R алгебраических функций от одной переменной называется *специальным* или *неспециальным* в зависимости от того, существует или не существует дифференциал поля R, отличный от 0 и делящийся на $\mathfrak{a}$. Если g есть род поля R, то, очевидно, всякий целый дивизор степени $> 2g-2$ является неспециальным.

Лемма 3. *Если $\mathfrak{a}$ — произвольный неспециальный дивизор поля R алгебраических функций от одной переменной характеристики 0, то для любого дифференциала ω второго рода в поле R существует такой точный дифференциал dx, что $\omega - dx \equiv 0 \pmod{\mathfrak{a}^{-2}}$.*

Пусть $\mathfrak{r}_1, \ldots, \mathfrak{r}_s$ — все различные полюса дифференциала ω. Так как дифференциал ω — второго рода, то, в силу теоремы 14, для каждого $i\,(1 \leqslant i \leqslant s)$ можно найти такой элемент $x_i \in R$, что $\nu_{\mathfrak{r}_i}(\omega - dx_i) \geqslant 0$. Обозначим через $\mathfrak{x}$ распределение поля R, которое в точке $\mathfrak{r}_i$ принимает значение $x_i\,(1 \leqslant i \leqslant s)$, а во всех других точках — значение 0. Применяя теорему 2 § 5 гл. II, получаем, что в поле R существует такой элемент x, что $x - \mathfrak{x} \equiv 0 \pmod{\mathfrak{a}^{-1}}$. Пусть $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$, тогда $\nu_{\mathfrak{r}_i}(x - x_i) \geqslant -a(\mathfrak{r}_i)$, откуда $\nu_{\mathfrak{r}_i}(dx - dx_i) \geqslant -2a(\mathfrak{r}_i)$ (действительно, если $a(\mathfrak{r}_i) > 0$, то $\nu_{\mathfrak{r}_i}(dx - dx_i) \geqslant -a(\mathfrak{r}_i) - 1 \geqslant -2a(\mathfrak{r}_i)$ по лемме 1; если же $a(\mathfrak{r}_i) = 0$, то $\nu_{\mathfrak{r}_i}(dx - dx_i) \geqslant 0$). Если точка $\mathfrak{p}$ отлична от $\mathfrak{r}_1, \ldots, \mathfrak{r}_s$, то $\nu_{\mathfrak{p}}(x) \geqslant -a(\mathfrak{p})$, откуда, как и выше, $\nu_{\mathfrak{p}}(dx) \geqslant -2a(\mathfrak{p})$. Отсюда непосредственно следует, что во всех случаях $\nu_{\mathfrak{p}}(\omega - dx) \geqslant -2a(\mathfrak{p})$, и лемма 4 доказана.

Вернемся теперь к доказательству теоремы 15. Так как поле R имеет бесконечно много точек, то мы можем найти конечное число различных точек $\mathfrak{s}_1, \ldots, \mathfrak{s}_t$ поля R, не принадлежащих множеству P и таких, что дивизор $\mathfrak{a} = \mathfrak{s}_1 \ldots, \mathfrak{s}_t$ неспециален. Пусть $\mathfrak{D}''$ есть пространство дифференциалов, принадлежащих $\mathfrak{D}'$ и делящихся на $\mathfrak{a}^{-2}$. Если $\omega \in \mathfrak{D}'$, то в R мы можем найти такой элемент x, что $\omega - dx \equiv 0 \pmod{\mathfrak{a}^{-2}}$. Точка $\mathfrak{p} \in P$ (которая не входит в $\mathfrak{a}$ и не является полюсом дифференциала ω) не может быть полюсом дифференциала dx; значит, $dx \in \mathfrak{E}'$ и $\omega - dx \in \mathfrak{D}''$. Отсюда вытекает, что $\mathfrak{D}' = \mathfrak{E}' + \mathfrak{D}''$, а следовательно, пространство $\mathfrak{D}'/\mathfrak{E}'$ изоморфно $\mathfrak{D}''/\mathfrak{E}''$, где $\mathfrak{E}'' = \mathfrak{E}' \cap \mathfrak{D}''$. Пусть теперь $\mathfrak{M}$ есть пространство всех дифференциалов, делящихся на $\mathfrak{a}^{-2}$. Тогда $\mathfrak{D}''$ может быть охарактеризовано как пространство дифференциалов второго рода, принадлежащих $\mathfrak{M}$; при этом для того чтобы дифференциал из $\mathfrak{M}$ принадлежал $\mathfrak{D}''$, необходимо и достаточно, чтобы его вычеты в точках $\mathfrak{s}_1, \ldots, \mathfrak{s}_t$ были равны 0. Мы можем предполагать, что $t > 0$. Применяя лемму 2, получаем, что пространство $\mathfrak{M}/\mathfrak{D}''$ имеет размерность $\left(\sum_{j=1}^{t} d(\mathfrak{s}_j)\right) - 1 = d(\mathfrak{a}) - 1$. С другой стороны, по теореме Римана — Роха $0 = l(\mathfrak{a}^2) = -2d(\mathfrak{a}) - g + 1 + \dim \mathfrak{M}$, откуда $\dim \mathfrak{M} = 2d(\mathfrak{a}) + g - 1$. Таким образом, размерность векторного

пространства $\mathfrak{D}''$ конечна и равна $2d(\mathfrak{a})+g-1-(d(\mathfrak{a})-1)=$ $=d(\mathfrak{a})+g$. Теперь мы должны вычислить размерность пространства $\mathfrak{E}''$. Из леммы 1 непосредственно следует, что элемент $y\in R$ удовлетворяет условию $dy\equiv 0 \pmod{\mathfrak{a}^{-2}}$ тогда и только тогда, если $y\equiv 0 \pmod{\mathfrak{a}^{-1}}$. Так как дивизор $\mathfrak{a}$ неспециален, то по теореме Римана — Роха размерность пространства $\mathfrak{F}$ элементов поля R, делящихся на $\mathfrak{a}^{-1}$, равна $d(\mathfrak{a})-g+1$. Отображение $y\to dy$ отображает $\mathfrak{F}$ линейно на $\mathfrak{E}''$, и ядром этого отображения является пространство констант, имеющее размерность 1. Следовательно, $\dim\mathfrak{E}''=\dim\mathfrak{F}-1=d(\mathfrak{a})-g$. Таким образом, мы доказали, что размерность векторного пространства $\mathfrak{D}'/\mathfrak{E}'$ конечна и равна $(d(\mathfrak{a})+g)-(d(\mathfrak{a})-g)=2g$.

Наконец, нам осталось вычислить размерность пространства $\mathfrak{E}'/\mathfrak{E}$. Обозначим через $\mathfrak{G}'$ пространство всех элементов поля R, не имеющих полюсов среди точек из P, а через $\mathfrak{G}$ — пространство элементов, для которых все точки из P являются нулями. Отображение $z\to dz$ отображает $\mathfrak{G}'$ линейно на $\mathfrak{E}'$, а $\mathfrak{G}$ — на $\mathfrak{E}$. Ядром нашего отображения является пространство констант $\mathfrak{C}$; отсюда легко следует, что пространство $\mathfrak{E}'/\mathfrak{E}$ изоморфно $\mathfrak{G}'/(\mathfrak{G}+\mathfrak{C})$. Обозначим через $\Sigma_1, \ldots, \Sigma_n$ соответственно поля вычетов точек $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, принадлежащих P, и образуем векторное пространство $\prod_{i=1}^{n}\Sigma_i$ над K. Каждому $z\in\mathfrak{G}'$ сопоставим элемент $\Theta(z)\in$ $\in\prod_{i=1}^{n}\Sigma_i$, у которого Σ_i-координата (при каждом i) равна значению, принимаемому элементом z в точке $\mathfrak{p}_i$. Из теоремы 3 § 6 гл. 1 следует, что Θ отображает $\mathfrak{G}'$ на $\prod_{i=1}^{n}\Sigma_i$. Так как ядро Θ равно $\mathfrak{G}$, то векторное пространство $\mathfrak{G}'/\mathfrak{G}$ имеет конечную размерность и эта размерность равна $\dim\prod_{i=1}^{n}\Sigma_i=\sum_{\mathfrak{p}\in P}d(\mathfrak{p})$. Если P не пусто, то пересечение $\mathfrak{C}\cap\mathfrak{G}$ состоит только из 0, откуда $\dim\mathfrak{E}'/\mathfrak{E}=\left(\sum_{\mathfrak{p}\in P}d(\mathfrak{p})\right)-1=p$ (ибо $\dim\mathfrak{C}=1$); если же P пусто, то $\mathfrak{E}'=\mathfrak{E}$ и $\dim\mathfrak{E}'/\mathfrak{E}=0=p$. Теорема 15 доказана теперь полностью.

Следствие 1. *Если поле R алгебраических функций от одной переменной характеристики 0 имеет род g, то фактор-пространство пространства дифференциалов второго рода поля R по подпространству точных дифференциалов имеет конечную размерность, равную $2g$.*

Это непосредственно следует из теоремы 15 при пустых множествах P и Q.

Следствие 2. *Если R — поле алгебраических функций от одной переменной характеристики 0 и L — произвольное расширение его поля констант K, то каждый дифференциал второго рода поля $R\langle L\rangle$ может быть представлен в виде суммы точного дифференциала и линейной комбинации с коэффициентами из L коследов дифференциалов второго рода поля R.*

Пусть g — род поля R. Согласно следствию 1 в поле R мы можем найти $2g$ дифференциалов $\omega_1, \ldots, \omega_{2g}$ второго рода, которые линейно независимы (над K) по модулю подпространства точных дифференциалов. Положим $\Omega_i = \mathrm{Cosp}_{R/R\langle L\rangle}\,\omega_i$ $(1 \leqslant i \leqslant 2g)$. Как мы знаем, Ω_i являются дифференциалами второго рода поля $R\langle L\rangle$. Покажем, что они линейно независимы (над L) по модулю подпространства точных дифференциалов поля $R\langle L\rangle$. Допустим, что при некоторых элементах $a_1, \ldots, a_{2g}$ поля L имеем $\sum_{i=1}^{2g} a_i\Omega_i = dx$, где $x \in R\langle L\rangle$ Так как поля $R\langle L\rangle$ и R имеют один и тот же род (теорема 5 § 6 гл. V), то дифференциал, стоящий в левой части последнего равенства не имеет переменных полюсов относительно поля R (теорема 11 § 6). Применяя лемму 1, заключаем, что элемент x не имеет переменных полюсов относительно R, а потому может быть представлен в виде линейной комбинации элементов поля R с коэффициентами из L (следствие 2 к теореме 4 § 6 гл. V). Пусть $\{b_j\}_{j\in J}$ — базис поля L относительно K; тогда $x = \sum_{j\in J} b_j x_j$, $x_j \in R$. Запишем $a_i = \sum_{j\in J} c_{ij} b_j$ и положим $\eta_j = \sum_{i=1}^{2g} c_{ij}\omega_i$. Тогда будем иметь $\sum_{j\in J} b_j((dx_j)_{R\langle L\rangle} - \mathrm{Cosp}_{R/R\langle L\rangle}\,\eta_j) = 0$. Выбрав элемент $t \in R$, отличный от константы, положим $(dx_j)_R - \eta_j = u_j(dt)_R$, где $u_j \in R$.

Тогда $\sum_{j\in J} u_j b_j = 0$, откуда, в силу теоремы 1 § 4 гл. V, $u_j = 0$ при всех j. Так как $\sum_{i=1}^{2g} c_{ij}\omega_i = (dx_j)_R$, то $c_{ij} = 0$ при всех i и j, а значит $a_i = 0$ $(1 \leqslant i \leqslant 2g)$, и наше утверждение доказано. Так как поля $R\langle L\rangle$ и R имеют одинаковый род g, то по следствию 1 каждый дифференциал второго рода поля $R\langle L\rangle$ сравним по модулю подпространства точных дифференциалов с линейной комбинацией дифференциалов $\Omega_1, \ldots, \Omega_{2g}$, что и доказывает следствие 2.

Замечание. Из следствия 2, а также из следствия 2 к теореме 4 § 6 гл. V вытекает, что каждый дифференциал второго рода поля $R\langle L\rangle$, не имеющий переменных полюсов относительно R, является линейной комбинацией с коэффициентами из L коследов дифференциалов второго рода поля R.

Перейдем теперь к рассмотрению полей алгебраических функций от одной переменной над алгебраически замкнутым полем характеристики 0.

Лемма 4. *Пусть R — поле алгебраических функций от одной переменной над алгебраически замкнутым полем K и пусть E — произвольное бесконечное множество точек поля R. Если g есть род поля R, то в множестве E можно найти g точек $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$, таких, что дивизор $\mathfrak{p}_1 \ldots \mathfrak{p}_g$ неспециален.*

Мы можем считать, что $g > 0$. Пусть ω_1 — произвольный дифференциал первого рода поля R, отличный от 0; тогда мы можем найти точку $\mathfrak{p}_1 \in E$, не являющуюся нулем дифференциала ω_1. Ясно, что пространство дифференциалов, делящихся на $\mathfrak{p}_1$, имеет размерность $\leqslant g-1$. Пусть h — любое целое число, удовлетворяющее условию $1 \leqslant h \leqslant g$. Предположим, что мы уже нашли $h-1$ точек $\mathfrak{p}_1, \ldots, \mathfrak{p}_{h-1}$ из множества E, таких, что, пространство дифференциалов, делящихся на $\mathfrak{p}_1 \ldots \mathfrak{p}_{h-1}$, имеет размерность $\leqslant g-h+1$. Если это пространство $\neq \{0\}$, то выберем в нем дифференциал $\omega \neq 0$, а затем в множестве E выберем точку $\mathfrak{p}_h$, не являющуюся нулем дифференциала ω; если же наше пространство равно $\{0\}$, то в качестве $\mathfrak{p}_h$ возьмем произвольную точку из множества E, отличную от $\mathfrak{p}_1, \ldots, \mathfrak{p}_{h-1}$. В первом случае размерность пространства дифференциалов поля R, делящихся на $\mathfrak{p}_1 \ldots \mathfrak{p}_h$, меньше размерности пространства дифференциалов, делящихся на $\mathfrak{p}_1 \ldots \mathfrak{p}_{h-1}$,

а, следовательно, она не превосходит $g-h$. Это же заключение, разумеется, справедливо и для второго случая. Продолжая этот процесс, мы в конце концов в множестве E найдем g точек с требуемым свойством.

Сохраняя обозначения леммы 4, положим $\mathfrak{a}=\mathfrak{p}_1\ldots\mathfrak{p}_g$. В силу леммы 3 каждый дифференциал второго рода сравним по модулю подпространства точных дифференциалов с дифференциалом, делящимся на $\mathfrak{a}^{-2}$. Для каждого i $(1\leqslant i\leqslant g)$ выберем униформизирующую переменную x_i в точке $\mathfrak{p}_i$. Пусть ω есть дифференциал второго рода, делящийся на $\mathfrak{a}^{-2}$. Представим его в виде $\omega=u_i\,dx_i$, где $u_i\in R$. Применяя следствие к теореме 6 § 3, мы видим, что коэффициент при x_i^{-1} в разложении элемента u_i в степенной ряд по x_i в $\mathfrak{p}_i$-адическом пополнении поля R равен 0. Поэтому мы имеем

$$\omega=\left(a_i(\omega)\,x_i^{-2}+b_i(\omega)+x_iv_i\right)dx_i,$$

где v_i — целый элемент в точке $\mathfrak{p}_i$. Пусть через $\mathfrak{D}$ обозначено пространство дифференциалов второго рода, делящихся на $\mathfrak{a}^{-2}$. На пространстве $\mathfrak{D}$ мы имеем $2g$ линейных функций $a_1,\ldots,a_g,b_1,\ldots,b_g$. Если $a_i(\omega)=b_i(\omega)=0$ $(1\leqslant i\leqslant g)$ при некотором $\omega\in\mathfrak{D}$, то для ω точки $\mathfrak{p}_1,\ldots,\mathfrak{p}_g$ будут нулями, т. е. $\omega\equiv 0\pmod{\mathfrak{a}}$, откуда $\omega=0$. С другой стороны, $\mathfrak{D}$ не может содержать никакого точного дифференциала, отличного от 0. В самом деле, если $x\in R$ и $dx\in\mathfrak{D}$, то, в силу леммы 1, $x\equiv 0\pmod{\mathfrak{a}^{-1}}$, но по теореме Римана — Роха $l(\mathfrak{a}^{-1})=d(\mathfrak{a})-g+1=1$, т. е. среди элементов поля R только константы делятся на $\mathfrak{a}^{-1}$. Из следствия 1 к теореме 15 теперь непосредственно следует, что размерность пространства $\mathfrak{D}$ равна $2g$, а значит, функции $a_i(\omega)$, $b_i(\omega)$ линейно независимы. Таким образом, нами доказана

Теорема 16. *Пусть R — поле алгебраических функций от одной переменной над алгебраически замкнутым полем K характеристики 0 и пусть g — его род. Допустим, что g различных точек $\mathfrak{p}_1,\ldots,\mathfrak{p}_g$ поля R выбраны так, что дивизор $\mathfrak{a}=\mathfrak{p}_1\ldots\mathfrak{p}_g$ неспециален. Пусть x_i есть униформизирующая переменная в точке $\mathfrak{p}_i$ $(1\leqslant i\leqslant g)$. Тогда для любых $2g$ элементов a_i, b_i поля K $(1\leqslant i\leqslant g)$ существует однозначно определенный дифференциал ω второго рода поля R, удовлетворяющий условиям $\nu_{\mathfrak{p}_i}\left(\omega-\left(a_ix_i^{-2}+b_i\right)dx_i\right)>0$ $(1\leqslant i\leqslant g)$.*

ГЛАВА VII

РИМАНОВА ПОВЕРХНОСТЬ

На протяжении всей этой главы через C будет обозначаться поле комплексных чисел, а через R — поле алгебраических функций от одной переменной над C. Присоединяя известным образом к полю C точку ∞, мы получаем компактное топологическое пространство, гомеоморфное двумерной сфере в трехмерном евклидовом пространстве. Это пространство, называемое сферой Римана, мы будем обозначать через Σ.

§ 1. Определение римановой поверхности

Обозначим через S множество всех точек поля R. Если точка $\mathfrak{p}$ поля R является полюсом элемента $x \in R$, то будем говорить, что x в точке $\mathfrak{p}$ принимает значение ∞. В противном случае (так как C алгебраически замкнуто) значение $x(\mathfrak{p})$, принимаемое элементом x в точке $\mathfrak{p}$, есть некоторое комплексное число. Таким образом, каждому $x \in R$ мы можем сопоставить отображение $\mathfrak{p} \to x(\mathfrak{p})$ множества S в Σ. Пусть x и x' — два различных элемента из R. Среди точек поля R существует точка $\mathfrak{p}$, отличная от нулей и полюсов элемента $x' - x$ и от полюсов элемента x. Следовательно, отображения $\mathfrak{p} \to x(\mathfrak{p})$ и $\mathfrak{p} \to x'(\mathfrak{p})$ множества S в Σ различны. Отображение S в Σ, соответствующее элементу $x \in R$, мы будем обозначать в дальнейшем также через x.

В множество S мы введем сейчас топологию, относительно которой все отображения x $(x \in R)$ будут непрерывны. Как известно, для заданной совокупности отображений множества X в топологическое пространство E на множестве X существует слабейшая из топологий, при которой данные отображения непрерывны. В дальнейшем множество S

мы будем рассматривать как топологическое пространство с наиболее слабой топологией, при которой все отображения x ($x \in R$) непрерывны. Открытыми множествами пространства S являются объединения множеств вида

$$x_1^{-1}(U_1) \cap x_2^{-1}(U_2) \cap \ldots \cap x_k^{-1}(U_k), \tag{1}$$

где $x_1, \ldots, x_k$ — элементы из R, а $U_1, \ldots, U_k$ — открытые множества пространства Σ (здесь $x^{-1}(U)$ обозначает множество точек $\mathfrak{p}$, для которых $x(\mathfrak{p}) \in U$).

Введенная топология может быть определена и другим способом. Для каждого $x \in R$ построим экземпляр Σ_x пространства Σ и рассмотрим топологическое произведение P пространств Σ_x для всех $x \in R$. Если мы каждой точке $\mathfrak{p} \in S$ поставим в соответствие точку $\Phi(\mathfrak{p}) \in P$, у которой Σ_x-координата равна $x(\mathfrak{p})$ (при любом x), то получим отображение Φ множества S на подмножество S' пространства P. Это отображение взаимно однозначно. В самом деле, если $\mathfrak{p}$ и $\mathfrak{q}$ — различные точки поля R, то существует элемент $x \in R$, который в точках $\mathfrak{p}$ и $\mathfrak{q}$ принимает различные значения (теорема 3 § 6 гл. I), а значит, $\Phi(\mathfrak{p}) \neq \Phi(\mathfrak{q})$. Множество (1) является прообразом при отображении Φ множества $V(x_1, U_1; \ldots; x_k, U_k)$, состоящего из тех точек произведения P, у которых Σ_{x_i}-координата принадлежит U_i ($1 \leqslant i \leqslant k$). Множество $V(x_1, U_1; \ldots; x_k, U_k)$ открыто в P, и всякое множество, открытое в P, есть объединение множеств этого вида. Отсюда непосредственно следует, что Φ есть гомеоморфизм пространства S на подпространство S' произведения P. Так как в P, а значит, и в S' имеет место аксиома отделимости Хаусдорфа, то она имеет место и в S, т. е. S является хаусдорфовым пространством.

Докажем теперь, что *пространство S компактно*. Пространство P, как произведение компактных пространств, само компактно. Поэтому нам достаточно показать, что S' замкнуто в P. Пусть $\mathfrak{u} = (u_x)_{x \in R}$ есть точка из P, принадлежащая замыканию подпространства S'. Обозначим через $\mathfrak{o}$ множество тех элементов $x \in R$, для которых $u_x \neq \infty$. Утверждаем, что $\mathfrak{o}$ есть V-кольцо в поле R и что $\mathfrak{u} = \Phi(\mathfrak{p})$, где $\mathfrak{p}$ — точка, соответствующая кольцу $\mathfrak{o}$.

Если c — константа, то $c(\mathfrak{p}) = c$ для каждой точки $\mathfrak{p}$. Это означает, что все точки из S' имеют одну и ту же

Σ_c-координату, а именно c. Так как $\mathfrak{u}$ принадлежит замыканию S', то, очевидно, $u_c = c$, откуда следует, что $C \subset \mathfrak{o}$. Пусть a — точка из Σ и пусть ε — вещественное положительное число. Если $a \neq \infty$, то через $\delta(a, \varepsilon)$ обозначим множество точек $a' \neq \infty$ из Σ для которых $|a' - a| < \varepsilon$; если же $a = \infty$, то $\delta(\infty, \varepsilon)$ будет обозначать множество, состоящее из точки ∞ и из точек $a' \neq \infty$ из Σ, для которых $|a'| > \varepsilon^{-1}$. В обоих случаях $\delta(a, \varepsilon)$ есть открытое подмножество пространства Σ. Пусть x и y — два элемента из R. Обозначим через V_ε множество точек $\mathfrak{v} = (v_z)_{z \in R}$ из P, для которых $v_z \in \delta(u_z, \varepsilon)$ как только z равен одному из элементов x, y, $x - y$ или xy. Ясно, что V_ε открыто в P и содержит $\mathfrak{u}$; следовательно V_ε содержит точку $\mathfrak{u}_\varepsilon = (v_{z,\varepsilon})_{z \in R}$ из S'. Положим $\mathfrak{u}_\varepsilon = \Phi(\mathfrak{p}_\varepsilon)$, где $\mathfrak{p}_\varepsilon \in S$. Если x и y принадлежат $\mathfrak{o}$, то u_x и u_y отличны от ∞, а значит $v_{x,\varepsilon}$ и $v_{y,\varepsilon}$ также отличны от ∞. Так как $\mathfrak{u}_\varepsilon = \Phi(\mathfrak{p}_\varepsilon)$, то $v_{x,\varepsilon} = x(\mathfrak{p}_\varepsilon)$, $v_{y,\varepsilon} = y(\mathfrak{p}_\varepsilon)$, $v_{x-y,\varepsilon} = (x - y)(\mathfrak{p}_\varepsilon) = v_{x,\varepsilon} - v_{y,\varepsilon}$ и аналогично $v_{xy,\varepsilon} = v_{x,\varepsilon} v_{y,\varepsilon}$. С другой стороны, ясно, что $u_z = \lim\limits_{\varepsilon \to 0} v_{z,\varepsilon}$, если только z равен одному из элементов x, y, $x - y$ или xy. Отсюда заключаем, что u_{x-y} и u_{xy} соответственно равны $u_x - u_y$ и $u_x u_y$. Этим доказано, что $\mathfrak{o}$ есть кольцо и что отображение $x \to u_x$ $(x \in \mathfrak{o})$ является гомоморфизмом кольца $\mathfrak{o}$ на C, при котором элементы из C отображаются на себя. Предположим теперь, что $x \notin \mathfrak{o}$. Положим $y = x^{-1}$. Если $v_{x,\varepsilon} = \infty$, то $\mathfrak{p}_\varepsilon$ является полюсом элемента x, а значит, нулем элемента y, откуда $v_{y,\varepsilon} = 0$; если же $v_{x,\varepsilon} \neq \infty$, то $v_{y,\varepsilon} = v_{x,\varepsilon}^{-1}$ и $|v_{x,\varepsilon}| > \varepsilon^{-1}$, откуда $|v_{y,\varepsilon}| < \varepsilon$. В обоих случаях $|v_{y,\varepsilon}| < \varepsilon$. Так как это верно для любого $\varepsilon > 0$, то $u_y = 0$, и, следовательно, $x^{-1} \in \mathfrak{o}$. Наконец, мы имеем $\mathfrak{o} \neq R$. Действительно, если элемент x из $\mathfrak{o}$ не принадлежит C и $x' = x - u_x$, то $u_{x'} = 0$, но $x' \neq 0$; элемент x'^{-1} из R не может принадлежать кольцу $\mathfrak{o}$, ибо в противном случае мы имели бы $u_{x'^{-1}} u_{x'} = 1$. Таким образом, мы доказали, что $\mathfrak{o}$ есть V-кольцо. Пусть $\mathfrak{p}$ — соответствующая ему точка. Элемент x из $\mathfrak{o}$ принадлежит $\mathfrak{p}$, очевидно, тогда и только тогда, когда $u_x = 0$. Если x — произвольный элемент из $\mathfrak{o}$, то $x - u_x \in \mathfrak{p}$, откуда $u_x = x(\mathfrak{p})$. Отсюда следует, что $\mathfrak{u} = \Phi(\mathfrak{p})$. Этим и доказано, что подпространство S' замкнуто в P.

Докажем теперь, что любая униформизирующая переменная x произвольной точки $\mathfrak{p} \in S$ отображает некоторую окрестность этой точки $\mathfrak{p}$ (в пространстве S) топологически на окрестность нуля в Σ. Обозначим через $\mathfrak{p}_1 = \mathfrak{p}, \ldots, \mathfrak{p}_h$ все различные нули элемента x и положим $e_i = \nu_{\mathfrak{p}_i}(x)$ $(1 \leqslant i \leqslant h)$. Тогда $e_1 = 1$ и $\sum_{i=1}^{h} e_i = [R : C\langle x\rangle] = n$ (теорема 4 § 8 гл. 1). Пусть $a_1, \ldots, a_h$ — h различных комплексных чисел; как мы знаем (теорема 3 § 6 гл. I), в поле R существует такой элемент y, что $\nu_{\mathfrak{p}_i}(y - a_i) = 1$ $(1 \leqslant i \leqslant h)$. Пусть $F(X, Y)$ — неприводимый многочлен с комплексными коэффициентами, для которого $F(x, y) = 0$. Многочлен $F(x, Y)$ неприводим в кольце $C\langle x\rangle[Y]$, поэтому степень F относительно Y не превосходит n. Так как $y(\mathfrak{p}_i) = a_i$ $(1 \leqslant i \leqslant h)$, то $F(0, a_i) = 0$. Утверждаем, что кратность корня a_i уравнения $F(0, Y) = 0$ равна e_i. Действительно, пусть $F(0, Y) = (Y - a_i)^{m_i} G_i(Y)$, где G_i — многочлен, не делящийся на $Y - a_i$; тогда $\nu_{\mathfrak{p}_i}(F(0, y)) = m_i$. Далее, $F(X, Y) - F(0, Y) = XH(X, Y)$, где H — многочлен, поэтому $F(0, y) = -xH(x, y)$ и, значит, $m_i \geqslant \nu_{\mathfrak{p}_i}(x) = e_i$. С другой стороны, сумма $\sum_{i=1}^{h} m_i$ не может быть больше степени многочлена $F(0, Y)$, которая, в свою очередь, не превосходит $n = \sum_{i=1}^{h} e_i$. Отсюда следует, что $m_i = e_i$ $(1 \leqslant i \leqslant h)$; кроме того, мы видим, что степень F относительно Y равна n и, следовательно, $R = C\langle x, y\rangle$. Используем теперь свойство непрерывности корней алгебраического уравнения. Выберем вещественное положительное число s, меньшее всех чисел $\frac{1}{2}|a_i - a_j|$ $(1 \leqslant i < j \leqslant h)$. Тогда можно найти такое число $r > 0$, что для любого комплексного числа $\xi \neq 0$, такого что $|\xi| \leqslant r$, и для любого i $(1 \leqslant i \leqslant h)$ уравнение $F(\xi, Y) = 0$ будет иметь ровно e_i различных корней η_{ik} $(1 \leqslant k \leqslant e_i)$, удовлетворяющих условию $|\eta_{ik} - a_i| \leqslant s$. Так как $|a_i - a_j| > 2s$ при $i \neq j$, то, очевидно, числа η_{ik} все различны (заметим, что число этих чисел равно n). В силу следствия 2 к теореме 1 § 4 гл. I для каждого η_{ik}

существует точка $\mathfrak{q}_{ik}$ поля R, являющаяся общим нулем элементов $x-\xi$ и $y-\eta_{ik}$. Все n точек $\mathfrak{q}_{ik}$ различны между собой; но $[R:C\langle x-\xi\rangle]=[R:C\langle x\rangle]=n$, поэтому, в силу теоремы 4 § 8 гл. I точки $\mathfrak{q}_{ik}$ исчерпывают собой все нули элемента $x-\xi$ в поле R и эти нули имеют порядок 1. Пусть N есть множество всех точек $\mathfrak{q}$, для которых $|x(\mathfrak{q})|\leqslant r$ и $|y(\mathfrak{q})-a_1|\leqslant s$. Ясно, что N является замкнутой окрестностью точки $\mathfrak{p}$ в пространстве S. Так как $e_1=1$, то в силу вышеизложенного, для каждого $\xi\neq 0$, удовлетворяющего условию $|\xi|\leqslant r$, N содержит ровно один нуль элемента $x-\xi$ (этим нулем является точка $\mathfrak{q}_{11}$). Таким образом, x отображает множество N взаимно однозначно и непрерывно на замкнутый круг пространства Σ, состоящий из тех $\xi\in\Sigma$, для которых $|\xi|\leqslant r$. Так как N компактно (как замкнутое подмножество в S), то это отображение является гомеоморфизмом.

Таким образом, мы видим, что каждая точка из S имеет окрестность, гомеоморфную окрестности точки на плоскости. Пространство S естественно поэтому назвать поверхностью. Мы будем называть его *римановой поверхностью поля* R. Сформулируем полученный нами результат.

Теорема 1. *Пусть S есть риманова поверхность поля R. Каждый элемент $x\in R$ индуцирует непрерывное отображение $\mathfrak{p}\to x(\mathfrak{p})$ поверхности S в риманову сферу, при этом топология на S — самая слабая, относительно которой все эти отображения непрерывны. Если x — униформизирующая переменная в точке $\mathfrak{p}\in S$, то существует окрестность точки $\mathfrak{p}$ в S, которая элементом x отображается топологически на окрестность нуля римановой сферы.*

Пусть Δ есть подмножество поверхности S, обладающее следующим свойством: в S существует открытое подмножество U, содержащее Δ, которое некоторым элементом $x\in R$ отображается топологически на окрестность нуля в Σ, а само множество Δ отображается при этом на замкнутый круг в Σ с центром в точке 0 (радиуса $r>0$). Будем говорить тогда, что Δ есть *замкнутый круг* в S или, более точно, *замкнутый x-круг*. Открытое подмножество V в S называется *открытым кругом* (или *открытым x-кругом*), если его замыкание в S является замкнутым кругом. Точка x-круга открытого или замкнутого), которая элементом x отобра-

жается на 0, называется *x-центром* этого круга, а радиус образа x-круга при отображении x называется его *x-радиусом*. Граница x-круга (открытого или замкнутого) отображается элементом x на окружность в Σ; эта граница называется *окружностью* круга. Из теоремы 1 легко следует, что если x есть униформизирующая переменная в точке $\mathfrak{p} \in S$, то замкнутые x-круги с x-центром в $\mathfrak{p}$ образуют фундаментальную систему окрестностей точки $\mathfrak{p}$; то же самое, разумеется, справедливо и для открытых x-кругов с x-центром в $\mathfrak{p}$. Далее, каждый замкнутый x-круг с x-центром в $\mathfrak{p}$ содержится в открытом x-круге с x-центром в $\mathfrak{p}$, и каждый открытый x-круг с x-центром в $\mathfrak{p}$ — в замкнутом x-круге с x-центром в $\mathfrak{p}$.

Примеры римановых поверхностей.

1) Предположим, что $R = C\langle x\rangle$, где x — трансцендентный элемент над C. Для каждого $a \in C$ элемент $x - a$ имеет единственный нуль $\mathfrak{p}_a$; с другой стороны, элемент x имеет единственный полюс $\mathfrak{p}_\infty$. Как мы знаем, точками $\mathfrak{p}_\infty$ и $\mathfrak{p}_a$ $(a \in C)$ исчерпываются все точки поля R. Отсюда следует, что (в рассматриваемом случае) элемент x отображает S взаимно однозначно на Σ. Так как это отображение непрерывно, а пространство S компактно, то получаем, что поверхность S гомеоморфна Σ.

2) Предположим, что R есть поле эллиптических функций от одной переменной с периодами ζ и ζ' (см. § 8 гл. II). Как мы уже видели, каждому комплексному числу a соответствует точка $\mathfrak{p}_a$ поля R, являющаяся множеством всех тех эллиптических функций из R, для которых a является нулем; далее, все точки поля R имеют вид $\mathfrak{p}_a$, и две точки $\mathfrak{p}_a$ и $\mathfrak{p}_{a'}$ совпадают тогда и только тогда, если a и a' принадлежат одному и тому же смежному классу аддитивной группы G комплексных чисел по подгруппе H, порожденной числами ζ и ζ'. Таким образом, мы видим, что в этом случае точки из S находятся во взаимно однозначном соответствии с элементами факторгруппы G/H. Если $\mathfrak{p}(\mathfrak{z})$ есть точка, соответствующая элементу $\mathfrak{z} \in G/H$, то для каждого $x \in R$ имеем $x(\mathfrak{p}(\mathfrak{z})) = x(z)$, где z — комплексное число, принадлежащее смежному классу $\mathfrak{z}$. Так как функция $x(z)$ мероморфна, то она и непрерывна (как отображение C в Σ). Отсюда легко следует, что отображение $\mathfrak{z} \to x(\mathfrak{p}(\mathfrak{z}))$ группы G/H в Σ также непрерывно. Так как это верно для ка-

ждого $x \in R$, а топология на S — самая слабая, при которой отображения $\mathfrak{p} \to x(\mathfrak{p})$ непрерывны, то взаимно однозначное отображение $\mathfrak{z} \to \mathfrak{p}(\mathfrak{z})$ группы G/H на S также непрерывно. Но группа G/H компактна, поэтому наше отображение является гомеоморфизмом. Таким образом, в этом случае поверхность S гомеоморфна 2-мерному тору.

В приведенном выше первом примере род поля R был равен нулю, и риманова поверхность этого поля была гомеоморфна сфере, т. е. поверхности, топологический род которой равен нулю. Во втором примере, поле R имело род 1, и его риманова поверхность была гомеоморфна тору, т. е. поверхности, топологический род которой равен 1. В дальнейшем мы докажем, что топологический род римановой поверхности поля R всегда равен роду поля R.

§ 2. Мероморфные функции на римановой поверхности

Пусть $\mathfrak{p}$ — точка на римановой поверхности S поля R, x — униформизирующая переменная в точке $\mathfrak{p}$ и N — открытый x-круг с x-центром в $\mathfrak{p}$. Положим $D = x(N)$. Если $\xi \in D$, то через $\mathfrak{p}_\xi$ мы обозначим точку из N, которая элементом x отображается на ξ. Пусть y — произвольный элемент из R. Если мы положим $f(\xi) = y(\mathfrak{p}_\xi)$, то получим отображение f круга D в Σ. Утверждаем, что это отображение является мероморфной функцией (в круге D).

Пусть $F(X, Y)$ — неприводимый многочлен с комплексными коэффициентами, для которого $F(x, y) = 0$. Тогда $\frac{\partial F}{\partial Y}(x, y) \neq 0$, и элемент $\frac{\partial F}{\partial Y}(x, y)$ имеет только конечное число нулей. Далее, так как число полюсов элемента y конечно, то в D существует лишь конечное число точек ξ, для которых $f(\xi) = \infty$. Таким образом, удалив из круга D конечное число точек, мы получим подмножество D_1, обладающее свойством: если $\xi \in D_1$, то $f(\xi) \neq \infty$, $F(\xi, f(\xi)) = 0$ и $\frac{\partial F}{\partial Y}(\xi, f(\xi)) \neq 0$. Применяя теорему о неявных функциях, получаем, что функция f голоморфна в каждой точке из D_1. С другой стороны, функция f, очевидно, непрерывна на D. Но D_1 отличается от D лишь конечным числом точек (которые являются поэтому изолированными точками в D). В силу общеизвестной теоремы из теории функций комплексного

переменного, отсюда следует, что функция f мероморфна в круге D.

Выберем теперь в круге D открытый круг D' с центром в 0 радиуса $r > 0$, в котором f не имеет полюсов за исключением, быть может, точки 0. В круге D' функцию f мы можем разложить в ряд Лорана

$$f(\xi) = \sum_{k=m}^{\infty} a_k \xi^k,$$

сходящийся во всех точках D' за исключением, быть может, точки 0. С другой стороны, $\mathfrak{p}$-адическое пополнение $\overline{R}$ поля R может быть отождествлено с полем формальных степенных рядов от x с комплексными коэффициентами (§ 3 гл. III); следовательно, элемент y в поле $\overline{R}$ может быть представлен в виде $\sum_{k=m'}^{\infty} a'_k x^k$. Предполагая, что $y \neq 0$ и что $a_m \neq 0$, $a'_{m'} \neq 0$, мы докажем сейчас, что $m = m'$ и $a_k = a'_k$ при всех $k \geqslant m$.

Если элемент $y \in R$ и мероморфная функция f находятся между собой в описанном выше отношении, то будем говорить, что f является представляющей функцией для элемента y в круге D'. Если f и g являются представляющими функциями в D' для элементов y и z поля R, то, как легко видеть, $f - g$ и fg будут представляющими функциями в D' для элементов $y - z$ и yz соответственно (здесь под $f - g$ понимается та единственная мероморфная в D' функция, которая в любой точке $\xi \in D'$, отличной от полюсов функций f и g, принимает значение $f(\xi) - g(\xi)$; аналогично определяется fg). С другой стороны, для любого целого числа h представляющей функцией в D' для элемента $x^h \in R$ будет, очевидно, ξ^h. Заметим теперь, что целое число m однозначно определено условием: функция $\xi^{-m} f(\xi)$ принимает в точке 0 конечное значение, отличное от 0, а именно, a_m. Отсюда следует, что для элемента $x^{-m} y - a_m$ точка $\mathfrak{p}$ является нулем, и, значит, $m' = m$, $a'_{m'} = a_m$. Допустим, что $a_k = a'_k$ при $m \leqslant k < n$, где n — целое число, большее m. Представляющей функцией для элемента $x^{-n}\left(y - \sum_{m \leqslant k < n} a_k x^k\right)$

является функция $\xi^{-n}\left(f(\xi)-\sum_{m\leqslant k<n} a_k\xi^k\right)$. Но элемент $x^{-n}\left(y-\sum_{m\leqslant k<n} a_k x^k\right)$ в точке $\mathfrak{p}$ принимает значение a'_n, в то время как функция $\xi^{-n}\left(f(\xi)-\sum_{m\leqslant k<n} a_k\xi^k\right)$ в точке 0 принимает значение a_n; отсюда следует, что $a_n=a'_n$, и наше утверждение доказано.

Таким образом, нами доказана

Теорема 2. *Пусть $\mathfrak{p}$ — точка поля R и x — униформизирующая переменная в точке $\mathfrak{p}$. Пусть, далее, y — элемент из R и $y=\sum_{k=m}^{\infty} a_k x^k$ — его представление в виде формального степенного ряда от x в $\mathfrak{p}$-адическом пополнении поля R. Тогда для точки $\mathfrak{p}\in S$ существует окрестность N, не содержащая полюсов элемента x и такая, что для любой точки $\mathfrak{q}\in N$ за исключением, быть может, самой точки $\mathfrak{p}$, ряд $\sum_{k=m}^{\infty} a_k(x(\mathfrak{q}))^k$ сходится к $y(\mathfrak{q})$.*

Теорему 2 можно использовать для изучения локальной природы отображения поверхности S в Σ, индуцированного произвольным элементом поля R.

Теорема 3. *Пусть x — отличный от константы элемент поля R и $\mathfrak{p}$ — точка поля R. Обозначим через e индекс разветвления точки $\mathfrak{p}$ относительно $C\langle x\rangle$. Тогда каждая окрестность точки $\mathfrak{p}$ на римановой поверхности поля R содержит открытую окрестность N точки $\mathfrak{p}$, обладающую следующими свойствами: 1) элемент x отображает N на открытое подмножество $x(N)$ сферы Σ; 2) $\mathfrak{p}$ является единственной точкой из N, которая элементом x отображается на $x(\mathfrak{p})$; 3) если ξ — произвольная точка из $x(N)$, отличная от $x(\mathfrak{p})$, то в N существует ровно e точек, которые элементом x отображаются на ξ.*

Если $x(\mathfrak{p})\neq\infty$, то полагаем $y=x-x(\mathfrak{p})$; если же $x(\mathfrak{p})=\infty$, то положим $y=x^{-1}$. В обоих случаях мы имеем $\nu_{\mathfrak{p}}(y)=e$. Пусть t — униформизирующая переменная в $\mathfrak{p}$ и пусть N_0 — заданная окрестность точки $\mathfrak{p}$. Из теоремы 2 следует, что для точки $\mathfrak{p}$ существует окрестность N_1, обладающая следующими свойствами: N_1 содержится в N_0;

элемент t отображает N_1 топологически на круг Δ_1 комплексной плоскости с центром в точке 0; если $\mathfrak{q} \in N_1$, то $y(\mathfrak{q}) = f(t(\mathfrak{q}))$, где f—голоморфная на Δ_1 функция, для которой число 0 является нулем порядка e. В силу теорем элементарной теории функций комплексного переменного в комплексной плоскости существуют открытые окрестности U и Δ_2 точки 0, обладающие свойствами: Δ_2 содержится в Δ_1; число 0 является единственным нулем функции f в Δ_2; если ξ есть произвольная точка из U, отличная от 0, то в Δ_2 существует ровно e точек, которые функцией f отображаются на ξ. Пусть N есть множество тех точек $\mathfrak{q} \in N_1$, для которых $y(\mathfrak{q}) \in U$. Легко видеть, что N является открытой окрестностью точки $\mathfrak{p}$, содержащейся в N_0 и обладающей указанными в теореме 3 свойствами.

Введем теперь понятие *мероморфной функции* в точке $\mathfrak{p}$ римановой поверхности S поля R. Пусть f — отображение некоторой окрестности точки $\mathfrak{p} \in S$ в риманову сферу Σ и пусть x — униформизирующая переменная в точке $\mathfrak{p}$. В силу теоремы 1 § 1 мы можем найти окрестность N точки $\mathfrak{p}$, на которой отображение f определено и которая элементом x отображается топологически на окрестность числа 0 в комплексной плоскости. Если мы для каждой точки $\mathfrak{q} \in N$ положим $f(\mathfrak{q}) = f_x(x(\mathfrak{q}))$, то получим отображение f_x окрестности $x(N)$ в Σ. Будем говорить, что f принадлежит классу $\mathcal{M}(\mathfrak{p}, x)$, если при подходящем выборе окрестности N функция f_x мероморфна в $x(N)$. Функция f_x, очевидно, зависит от выбора униформизирующей переменной x; однако, как мы сейчас увидим, класс $\mathcal{M}(\mathfrak{p}, x)$ не зависит от x. Пусть x' — любая другая униформизирующая переменная в точке $\mathfrak{p}$, и пусть окрестность N' и функция $f_{x'}$ по отношению к x' имеют тот же смысл, какой N и f_x имели по отношению к x. Если мы вместо f рассмотрим функцию x, то получим функцию $x_{x'}$, определенную в некоторой окрестности нуля комплексной плоскости. Легко видеть, что если модуль $|\xi'|$ достаточно мал, то имеет место равенство $f_{x'}(\xi') = f_x(x_{x'}(\xi'))$. Но $x \in R$, поэтому функция $x_{x'}$ мероморфна в некоторой окрестности нуля, а так как $x(\mathfrak{p}) = 0$, то $x_{x'}(0) = 0$. Таким образом, мы видим, что если функция f_x мероморфна в некоторой окрестности нуля, то это же справедливо и для функции $f_{x'}$; другими словами, $\mathcal{M}(\mathfrak{p}, x) \subset \mathcal{M}(\mathfrak{p}, x')$. Аналогично мы могли бы доказать, что

$\mathcal{M}(\mathfrak{p}, x') \subset \mathcal{M}(\mathfrak{p}, x)$. Этим и доказано наше утверждение о том, что класс $\mathcal{M}(\mathfrak{p}, x)$ не зависит от выбора униформизирующей переменной x. Положим $\mathcal{M}(\mathfrak{p}) = \mathcal{M}(\mathfrak{p}, x)$; всякое отображение, принадлежащее классу $\mathcal{M}(\mathfrak{p})$, будем называть *мероморфной функцией в точке* $\mathfrak{p}$. Если отображение f открытого подмножества U поверхности S в Σ мероморфно в каждой точке из U, то f будет называться *мероморфной функцией на* U. Если, кроме того, $f(U)$ не содержит точку ∞, то f называется *голоморфной функцией на* U. Ясно, что всякое мероморфное отображение подмножества U непрерывно. Каждый элемент $x \in R$ индуцирует мероморфное отображение всей римановой поверхности S в Σ; как мы сейчас увидим, этими отображениями и исчерпываются все мероморфные отображения всей поверхности S.

Теорема 4. *Риманова поверхность S поля R есть связное топологическое пространство, и каждое мероморфное отображение S в Σ индуцируется некоторым элементом поля R.*

Пусть f — мероморфное отображение некоторого открытого подмножества U поверхности S. Точка $\mathfrak{p}$ называется нулем функции f, если $f(\mathfrak{p}) = 0$, и полюсом, если $f(\mathfrak{p}) = \infty$. Утверждаем, что полюса функции f изолированы, а если U связно и $f(U) \neq \{0\}$, то и нули функции f изолированы. Действительно, пусть $\mathfrak{p}$ — точка из U и пусть x — униформизирующая переменная в этой точке. Тогда для точки $\mathfrak{p}$ существует окрестность N, содержащаяся в U, которая элементом x отображается топологически на круг Δ в Σ с центром в точке 0. Если мы для любой точки $\mathfrak{q} \in N$ положим $f(\mathfrak{q}) = f^*(x(\mathfrak{q}))$, то получим функцию f^*, определенную на Δ и мероморфную в некоторой окрестности точки 0. Если $\mathfrak{p}$ является полюсом функции f, то 0 является полюсом функции f^*; но тогда, как известно, для точки 0 существует окрестность, содержащаяся в Δ, в которой f^* не имеет других полюсов, кроме 0. Этим доказано, что $\mathfrak{p}$ является изолированным полюсом функции f. Далее, если каждая окрестность точки $\mathfrak{p}$ содержит нуль функции f, отличный от $\mathfrak{p}$, то каждая окрестность точки 0 в Δ содержит нуль функции f^*, отличный от 0; отсюда следует, что f^* есть константа, равная 0, на некоторой окрестности точки 0, т. е. f отображает некоторую окрестность точки $\mathfrak{p}$ в U на $\{0\}$. Это показывает нам, что множество всех неизолированных нулей

функции f в U открыто. С другой стороны, множество всех нулей функции f в U замкнуто относительно U. Если U связно, то множество неизолированных нулей функции f в U, будучи одновременно замкнутым и открытым относительно U, совпадает с U, и наше утверждение доказано.

Пусть теперь f и g — два мероморфных отображения одного и того же связного открытого подмножества U поверхности S. Если $g(U)=\{0\}$, то полагаем $f-g=f$. Предположим, что $g(U)\neq\{0\}$; обозначим через U_1 множество тех точек из U, которые не являются полюсами функций f и g и нулями функции g; ясно, что U_1 открыто. Если $\mathfrak{p}\in U_1$, то положим $u(\mathfrak{p})=f(\mathfrak{p})-g(\mathfrak{p})$, $v(\mathfrak{p})=\dfrac{f(\mathfrak{p})}{g(\mathfrak{p})}$. Легко видеть, что u и v являются мероморфными отображениями подмножества U_1. Пусть теперь $\mathfrak{p}$ есть точка множества U, не принадлежащая U_1, а x — униформизирующая переменная в этой точке. Для точки $\mathfrak{p}$ выберем окрестность $N\subset U$, в которой кроме $\mathfrak{p}$ нет других точек из $U\setminus U_1$ и которая элементом x отображается топологически на открытый круг Δ в Σ с центром в точке 0. Для любой точки $\mathfrak{q}\in N$ положим $f(\mathfrak{q})=f^*(x(\mathfrak{q}))$ и $g(\mathfrak{q})=g^*(x(\mathfrak{q}))$. Введенные функции f^* и g^* мероморфны в некоторой окрестности точки 0, содержащейся в Δ. Поэтому для $\xi\in\Delta$, $\xi\neq 0$, мы имеем

$$f^*(\xi)=\xi^h f_1^*(\xi),\quad g^*(\xi)=\xi^k g_1^*(\xi),$$

где h и k — целые показатели, а f_1^* и g_1^* — функции, определенные на Δ, голоморфные в некоторой окрестности точки 0 и принимающие в точке 0 значения, отличные от 0. Пусть Δ' есть круг с центром в 0, во всех точках которого f_1^* и g_1^* голоморфны и отличны от 0. Для любой точки $\xi\neq 0$ из Δ' положим

$$u_1^*(\xi)=f^*(\xi)-g^*(\xi)=\xi^l\left(\xi^{h-l}f_1^*(\xi)-\xi^{\ \ l}g_1^*(\xi)\right),$$
$$v_1^*(\xi)=f^*(\xi)(g^*(\xi))^{-1}=\xi^{h-k}f_1^*(\xi)(g_1^*(\xi))^{-1},$$

где $l=\min\{h,k\}$. Легко видеть, что определенные таким образом функции u_1^* и v_1^* могут быть продолжены до функций u^* и v^*, заданных на Δ' и мероморфных в некоторой окрестности точки 0. Положим $\alpha=u^*(0)$, $\beta=v^*(0)$ (α и β

принадлежат Σ). Расширим теперь область определения функций u и v, заданных до сих пор лишь на U_1, полагая $u(\mathfrak{p})=\alpha$ и $v(\mathfrak{p})=\beta$. Ясно, что расширенные функции, определенные указанным образом, мероморфны в точке $\mathfrak{p}$. Проделав то же самое со всеми точками из $U\setminus U_1$, мы распространим u и v до мероморфных отображений всего подмножества U. Эти мероморфные продолжения функций u и v определены однозначно (это непосредственно следует из непрерывности мероморфного отображения, а также из того, что U_1 всюду плотно в U). Обозначим наши расширенные функции через $f-g$ и $\frac{f}{g}$ соответственно. Пусть 0_U и 1_U обозначают отображения, которые каждой точке из U ставят в соответствие 0 и 1 соответственно. Положим $0_U-g=-g$, а если $g\neq 0_U$, то $\frac{1_U}{g}=g^{-1}$. В множестве $\mathcal{M}(U)$ всех мероморфных на U функций определяем теперь действия сложения и умножения:

$$f+g=f-(-g),$$

$$fg=\begin{cases}\frac{f}{g^{-1}}, & \text{если } g\neq 0_U,\\ 0_U, & \text{если } g=0_U.\end{cases}$$

Легко видеть, что эти действия удовлетворяют всем аксиомам поля. Проверим, например, ассоциативность сложения. Пусть f_1, f_2 и f_3 — элементы из $\mathcal{M}(U)$. Из наших определений легко следует, что $(f_1+f_2)(\mathfrak{p})=f_1(\mathfrak{p})+f_2(\mathfrak{p})$ для любой точки $\mathfrak{p}\in U$, не являющейся полюсом ни одной из функций f_1 и f_2. Следовательно, функции $(f_1+f_2)+f_3$ и $f_1+(f_2+f_3)$ совпадают на множестве U_2 тех точек из U, которые не являются полюсами функций f_1, f_2 или f_3. Так как мероморфные отображения непрерывны, а множество U_2 всюду плотно в U, то $(f_1+f_2)+f_3=f_1+(f_2+f_3)$. Аналогичным образом проверяются и остальные аксиомы.

Таким образом, множество $\mathcal{M}(U)$ является полем. Если мы каждое $c\in C$ отождествим с постоянным отображением, сопоставляющим любой точке из U число c, то C можно будет рассматривать как подполе поля $\mathcal{M}(U)$. Далее, каждый элемент $x\in R$ определяет функцию $\mathfrak{p}\to x(\mathfrak{p})$, принадлежащую $\mathcal{M}(U)$. Это дает нам изоморфное отображение

поля R на некоторое подполе поля $\mathcal{M}(U)$, тождественное на C.

Предположим теперь, что U есть компонента пространства S. Так как S, очевидно, локально связно, то подмножество U открыто. С другой стороны, U замкнуто в S и, следовательно, компактно. Утверждаем, что *мероморфное отображение f подмножества U, не имеющее полюсов, необходимо является постоянным отображением*. Действительно, так как U компактно, то непрерывная вещественная функция $|f|$ в некоторой точке $\mathfrak{p}_0 \in U$ принимает свое наибольшее значение. Пусть x_0 — униформизирующая переменная в точке $\mathfrak{p}_0$, а N_0 — открытый x_0-круг с x_0-центром в $\mathfrak{p}_0$. Если для любой точки $\mathfrak{p} \in N_0$ мы положим $f(\mathfrak{p}) = f^*(x(\mathfrak{p}))$, то получим функцию f^*, определенную на $x_0(N_0)$ и голоморфную в некоторой окрестности точки 0. Функция $|f^*|$ в точке 0 имеет максимум; отсюда следует, что f^* в некоторой окрестности точки 0 принимает постоянное значение c. Точка $\mathfrak{p}_0$ является, следовательно, неизолированным нулем функции $f - c$, а значит, эта функция отображает все подмножество U на $\{0\}$.

Пусть x — элемент поля R, отличный от константы. Если множество $S \setminus U$ не пусто, то будем предполагать, что x имеет по крайней мере один полюс на этом множестве. Пусть f — произвольная функция, мероморфная на U. Обозначим через $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ все различные точки подмножества U, являющиеся полюсами либо x либо f. Для каждого i выберем униформизирующую переменную t_i в точке $\mathfrak{p}_i$ $(1 \leqslant i \leqslant h)$. Найдем целые показатели a_i и b_i так, чтобы оба значения $(t_i^{a_i} x)(\mathfrak{p}_i)$ и $(t_i^{b_i} f)(\mathfrak{p}_i)$ были отличны от 0 и ∞. Если k и l — произвольные неотрицательные целые числа, то $(t_i^{ka_i + lb_i} x^k f^l)(\mathfrak{p}_i) \neq \infty$. Пусть p и q — положительные целые числа и λ_{kl} $(0 \leqslant k \leqslant p,\ 0 \leqslant l \leqslant q)$ — произвольные комплексные числа; положим

$$z = \sum_{k=0}^{p} \sum_{l=0}^{q} \lambda_{kl} x^k f^l.$$

Для точек $\mathfrak{p}$ из подходящей окрестности точки $\mathfrak{p}_i$ мы можем положить $z(\mathfrak{p}) = z_i^*(t_i(\mathfrak{p}))$, где z_i^* — мероморфная функция

в окрестности точки 0. Легко видеть, что разложение функции z_i^* в ряд Лорана в окрестности нуля имеет вид

$$z_i^*(\xi) = \sum_{r=pa_i^*+qb_i^*}^{\infty} L_{ir}(\ldots, \lambda_{kl}, \ldots)\xi^r,$$

где $a_i^* = \min\{0, a_i\}$, $b_i^* = \min\{0, b_i\}$, а L_{ir} — линейная форма от $(p+1)(q+1)$ переменных. Будем считать теперь, что $q = -\sum_{i=1}^{h} a_i^*$ (это число положительно, ибо функция x не является постоянной на U и имеет, следовательно, хоть один полюс на U). В качестве p возьмем положительное целое число $\geqslant -q\left(\sum_{i=1}^{h} b_i^* + 1\right)$. При этих условиях будем иметь $(p+1)(q+1) > -p\sum_{i=1}^{h} a_i^* - q\sum_{i=1}^{h} b_i^*$, а тогда система линейных однородных уравнений

$$L_{ir}(\ldots, \lambda_{kl}, \ldots) = 0 \quad (1 \leqslant i \leqslant h,\ pa_i^* + qb_i^* \leqslant r < 0)$$

имеет нетривиальное решение. Предположим, что числа λ_k являются решением этой системы. Ясно, что тогда функция z не имеет полюсов на U, а значит она является константой. Этим доказано, что элемент f алгебраичен над $C\langle x\rangle$ и его степень над $C\langle x\rangle$ не превосходит q. Таким образом, каждый элемент из $\mathcal{M}(U)$ алгебраичен над $C\langle x\rangle$, причем степени всех элементов из $\mathcal{M}(U)$ над полем $C\langle x\rangle$ ограничены числом q, зависящим только от x. Пусть n есть степень поля R над $C\langle x\rangle$; как нам известно (следствие к теореме 4 § 8 гл. 1) число n равно степени дивизора полюсов $\mathfrak{n}$ элемента x. Ясно, что $\mathfrak{n} = \prod_{i=1}^{h} \mathfrak{p}_i^{-a_i^*}\mathfrak{n}'$, где $\mathfrak{n}'$ — целый дивизор, поэтому $q \leqslant n$; более того, если $U \neq S$, то x имеет по крайней мере один полюс вне U, и, следовательно, $q < n$. Так как характеристика поля R равна 0, то в R существует такой элемент u, что $R = C\langle x, u\rangle$, при этом степень элемента u над $C\langle x\rangle$ равна n. С другой стороны, степень элемента u (как элемента из $\mathcal{M}(U)$) над $C\langle x\rangle$ не превосходит q, т. е. $q \geqslant n$. Из полученных неравенств вытекает теперь, что

$q=n$ и $U=S$. Далее, если бы в $\mathcal{M}(U)$ существовал элемент f, не принадлежащий R, то поле $R\langle f\rangle$ было бы алгебраическим расширением поля $C\langle x\rangle$ степени $>n$ и, следовательно, оно содержало бы некоторый элемент степени $>n$ над $C\langle x\rangle$, что невозможно. Теорема 4, таким образом, доказана.

Замечание. Связность S можно было бы доказать короче следующим образом. Допустим, что S имеет компоненту $U\neq S$, и пусть $\mathfrak{q}$ — точка из S, не принадлежащая U. В силу леммы 1 § 1 гл. IV в поле R существует элемент x, для которого точка $\mathfrak{q}$ является его единственным полюсом. Элемент x индуцирует на U мероморфную функцию без полюсов; эта функция, следовательно, постоянна на U. Однако это невозможно, ибо для любого $c\in C$ элемент $x-c$ имеет только конечное число нулей (напомним, что x не является константой поля R).

§ 3. О сингулярной теории гомологий

В этом параграфе мы дадим краткое изложение основных результатов и определений сингулярной теории гомологий. Подробное изложение этой теории и доказательства приведенных ниже утверждений читатель может найти в книге С. Эйленберга и Н. Стинрода „Основания алгебраической топологии".

Обозначим через R^n n-мерное декартово пространство. Под T^n будем понимать наименьшее выпуклое подмножество пространства R^{n+1}, содержащее точки $e_{1,n}=(1, 0, \ldots, 0)$, $e_{2,n}=(0, 1, \ldots, 0)$, $\ldots$, $e_{n+1,n}=(0, 0, \ldots, 1)$; другими словами, T^n есть множество тех точек

$$(t_1, \ldots, t_{n+1})$$

из R^{n+1}, для которых $0\leqslant t_i\leqslant 1$ $(1\leqslant i\leqslant n+1)$ и $t_1+t_2+\ldots+t_{n+1}=1$.

Пусть X — топологическое пространство. Непрерывное отображение множества T^n в X называется *n-симплексом в X*. Построим свободную абелеву группу, свободными образующими которой являются все n-симплексы в пространстве X. Элементы этой группы называются *n-цепями на X*. Каждая n-цепь γ может быть представлена в виде $\sum_{k=1}^{h} a_k\sigma_k$,

где $\sigma_1, \ldots, \sigma_h$ — различные n-симплексы, а $a_1, \ldots, a_h$ — целые числа, отличные от 0 (если γ есть нулевая n-цепь, то полагаем $h=0$). Будем говорить тогда, что симплексы $\sigma_1, \ldots, \sigma_h$ *входят в* γ, а также что σ_k входит в γ с коэффициентом a_k. Если симплекс σ не входит в γ, то говорят также, что σ входит в γ с коэффициентом 0. Объединение множеств $\sigma_k(T^n)$ $(1 \leqslant k \leqslant h)$ называется *множеством точек цепи* γ и обозначается через $|\gamma|$; если $\gamma=0$, то множество точек $|\gamma|$ пусто. Множество точек любой n-цепи, очевидно, компактно. Если $|\gamma|$ содержится в некотором подмножестве Y пространства X, то говорят, что γ *есть цепь на* Y.

Множество T^0 состоит из одной точки. Поэтому 0-симплекс σ однозначно определен заданием точки $\mathfrak{p}=\sigma(T^0)$ пространства X. В силу этого, 0-симплексы мы будем отождествлять с точками пространства X.

Если $n \geqslant 1$ и $1 \leqslant i \leqslant n+1$, то через f_i мы обозначим барицентрическое отображение T^{n-1} в T^n, при котором $e_{j,\,n-1}$ отображается на $e_{j,\,n}$, если $j<i$, и на $e_{j+1,\,n}$, если $j \geqslant i$. Таким образом,

$$f_i(t_1, \ldots, t_n)=\sum_{j<i} t_j e_{j,\,n}+\sum_{j \geqslant i} t_j e_{j+1,\,n}.$$

Если σ есть n-симплекс, то каждое из отображений σf_i $(1 \leqslant i \leqslant n+1)$ является $(n-1)$-симплексом. Положим

$$\partial\sigma=\sum_{i=1}^{n+1}(-1)^{i+1}(\sigma f_i)$$

и продолжим ∂ до гомоморфизма (обозначаемого также через ∂) группы n-цепей в группу $(n-1)$-цепей. Если γ есть n-цепь, то $\partial\gamma$ называется *границей цепи* γ. Если γ есть 0-цепь, то $\partial\gamma$ считаем равным числу 0.

Легко доказывается, что $\partial(\partial\gamma)=0$ для любой n-цепи γ (при $n \geqslant 1$). Всякая n-цепь, граница которой равна 0, называется *n-циклом*. Пусть Y есть подмножество пространства X; тогда n-цепь называется *n-циклом по модулю* Y, если ее граница является цепью на Y. Обычные n-циклы — это n-циклы по модулю пустого множества $\varnothing$.

Говорят, что n-цепь γ есть *n-граница на* X, если существует такая $(n+1)$-цепь φ, что $\partial\varphi=\gamma$. Пусть Y — подмножество пространства X; говорят, что цепь γ есть

n-граница по модулю Y, если γ имеет вид $d\varphi+\gamma_1$, где φ — некоторая $(n+1)$-цепь на X, а γ_1 — n-цепь на Y. Всякая n-граница по модулю Y, является также и n-циклом по модулю Y; однако обратное, вообще говоря, неверно. Ясно, что граница по модулю $\varnothing$ — это то же самое, что и просто граница.

Пусть Z — группа n-циклов по модулю Y, а B — группа n-границ по модулю Y. Фактор-группа Z/B называется *n-мерной группой гомологий пространства X по модулю Y* и обозначается через $H_n(X, Y)$. Группа $H_n(X, \varnothing)$ называется *n-мерной группой гомологий пространства X* и обозначается через $H_n(X)$. Элементы группы $H_n(X, Y)$ называются *классами гомологий пространства X по модулю Y* (или *классами гомологий пространства X*, если $Y=\varnothing$). Два цикла по модулю Y, принадлежащие одному и тому же классу гомологий по модулю Y, называются *гомологичными друг другу по модулю Y* (или просто *гомологичными друг другу*, если $Y=\varnothing$).

Пусть $\gamma=\sum_{k=1}^{h} a_k\mathfrak{p}_k$ есть 0-цикл на X (здесь $\mathfrak{p}_k$ — точки пространства X). Для того чтобы цепь γ была границей на X, необходимо, чтобы число $\sum_{k=1}^{h} a_k$ было равно 0. Если пространство X линейно связно, то это условие также и достаточно. Таким образом, если X не пусто и линейно связно, то $H_0(X)$ есть бесконечная циклическая группа. Из теоремы 1 § 1 следует, что всякое связное открытое подмножество римановой поверхности поля алгебраических функций от одной переменной над полем C линейно связно.

Пусть X и X' — два топологических пространства, а Y и Y' — подмножества пространств X и X' соответственно. Предположим, что нам задано непрерывное отображение f пространства X в X', при котором Y отображается в Y'; в таком случае будем говорить, что f есть непрерывное отображение пары (X, Y) в пару (X', Y'). Пусть σ есть n-симплекс в X; тогда $f\sigma$ есть n-симплекс в X'. Отображение $\sigma\to f\sigma$ может быть продолжено до гомоморфизма группы n-цепей пространства X в группу n-цепей пространства X'; этот гомоморфизм будем обозначать также через f. При

гомоморфизме f циклы и границы по модулю Y в X отображаются соответственно в циклы и границы по модулю Y' в X'. Отсюда следует, что f естественным образом определяет гомоморфизм (обозначаемый также через f) группы $H_n(X, Y)$ в $H_n(X', Y')$.

Пусть g — непрерывное отображение пространства X' в пространство X''; предположим, что g отображает Y' в подмножество Y'' пространства X''. Тогда гомоморфизм группы $H_n(X, Y)$ в $H_n(X'', Y'')$, соответствующий отображению gf, может быть получен применением сначала гомоморфизма группы $H_n(X, Y)$ в $H_n(X', Y')$, соответствующего отображению f, а затем гомоморфизма группы $H_n(X', Y')$ в $H_n(X'', Y'')$, соответствующего отображению g.

Два непрерывных отображения f и f' пары (X, Y) в пару (X', Y') называются *гомотопными друг другу*, если существует непрерывное отображение F пары $(X \times [0, 1], Y \times [0, 1])$ в пару (X', Y') такое, что $F(x, 0) = f(x)$, $F(x, 1) = f'(x)$ при всех $x \in X$. Если отображения f и f' гомотопны, то гомоморфизмы группы $H_n(X, Y)$ в $H_n(X', Y')$, соответствующие этим отображениям f и f', совпадают между собой.

Подмножество Y пространства X называется *деформационным ретрактом* пространства X, если существует непрерывное отображение пространства X в себя, которое гомотопно тождественному отображению (отображающему каждую точку на себя), отображает X в Y и на Y совпадает с тождественным отображениям. Если Y есть деформационный ретракт пространства X, то гомоморфизм группы $H_n(Y)$ в $H_n(X)$, соответствующий тождественному отображению Y в X, является изоморфизмом $H_n(Y)$ на $H_n(X)$. В частности, каждый n-цикл на X гомологичен n-циклу на Y.

Пусть Y — подмножество пространства X. Предположим, что Y содержит открытое подмножество U пространства X такое, что $\overline{U} \subset V \subset Y$, где V — также открытое множество ($\overline{U}$ обозначает замыкание множества U). Тогда гомоморфизм группы $H_n(X \setminus U, Y \setminus U)$ в $H_n(X, Y)$, соответствующий тождественному отображению, является изоморфизмом первой группы на вторую. Это утверждение носит название *теоремы вырезания*.

Пусть Y — подмножество пространства X и пусть c — элемент из группы $H_n(X, Y)$. Если $n > 0$ и γ — произвольная n-цепь из класса c, то $\partial\gamma$ есть $(n-1)$-цикл на Y, класс гомологий которого ∂c в группе $H_{n-1}(Y)$ зависит только от c. Отображение $c \to \partial c$ является гомоморфизмом группы $H_n(X, Y)$ в $H_{n-1}(Y)$. Этот гомоморфизм называется *граничным гомоморфизмом*. Если $n = 0$, то для любого $c \in H_0(X, Y)$ полагаем $\partial c = 0$.

Пусть Y и Z — два подмножества пространства X, причем $Z \subset Y$. Рассмотрим следующую последовательность групп:

$$\{0\},\ H_0(X, Y),\ \ldots,\ H_{n-1}(X, Y),\ H_{n-1}(X, Z),$$
$$H_{n-1}(Y, Z),\ H_n(X, Y),\ \ldots$$

Для каждой группы этой последовательности (кроме первой) мы имеем гомоморфизм в соседнюю слева группу. Эти гомоморфизмы определяются следующим образом: 1) граничный гомоморфизм ∂ группы $H_n(X, Y)$ в $H_{n-1}(Y, Z)$ получается как результат применения сначала граничного гомоморфизма группы $H_n(X, Y)$ в $H_{n-1}(Y)$, а затем гомоморфизма группы $H_{n-1}(Y)$ в $H_{n-1}(Y, Z)$, соответствующего тождественному отображению пары $(Y, \varnothing)$ в (Y, Z); 2) гомоморфизм группы $H_{n-1}(Y, Z)$ в $H_{n-1}(X, Z)$ — это гомоморфизм, соответствующий тождественному отображению пары (Y, Z) в (X, Z); 3) гомоморфизм группы $H_{n-1}(X, Z)$ в $H_{n-1}(X, Y)$ есть гомоморфизм, соответствующий тождественному отображению пары (X, Z) в (X, Y). Наша последовательность групп вместе с определенными выше гомоморфизмами носит название *гомологической последовательности* для тройки (X, Y, Z). *Теорема о точности* утверждает, что эта последовательность точная, т. е. если A, B и C — три последовательных члена последовательности, то ядро гомоморфизма B в A совпадает с образом группы C при гомоморфизме C в B.

Если $Z = \varnothing$, то наша последовательность носит название гомологической последовательности для пары (X, Y). В этом случае она имеет вид

$$\{0\},\ H_0(X, Y),\ \ldots,\ H_{n-1}(X, Y),\ H_{n-1}(X),\ H_{n-1}(Y),\ H_n(X, Y),\ \ldots$$

Предположим, что пространство X является объединением конечного числа попарно непересекающихся открытых множеств $X_1, \ldots, X_n$. Пусть Y есть подмножество X; положим

$Y_i = Y \cap X_i$ $(1 \leqslant i \leqslant m)$. Для каждого i $(1 \leqslant i \leqslant m)$ тождественное отображение пары (X_i, Y_i) в (X, Y) определяет гомоморфизм η_i группы $H_n(X_i, Y_i)$ в $H_n(X, Y)$. Можно доказать, что все гомоморфизмы η_i являются изоморфизмами и что $H_n(X, Y)$ есть прямая сумма групп $\eta_i(H_n(X_i, Y_i))$ $(1 \leqslant i \leqslant m)$. Таким образом, в этом случае группа $H_n(X, Y)$ может быть отождествлена с произведением $\prod_{i=1}^{m} H_n(X_i, Y_i)$.

Каждой n-цепи γ на пространстве X некоторым вполне определенным образом сопоставляется новая n-цепь, которая называется *барицентрическим подразделением* цепи γ и обозначается через $\operatorname{subd}\gamma$. Мы не будем давать здесь определения цепи $\operatorname{subd}\gamma$, а ограничимся лишь перечислением основных свойств отображения $\gamma \to \operatorname{subd}\gamma$.

1) Отображение $\gamma \to \operatorname{subd}\gamma$ является гомоморфизмом группы n-цепей в себя.

2) Если γ есть 0-цепь, то $\operatorname{subd}\gamma = \gamma$.

3) Если γ есть 1-симплекс и $\partial\gamma = \mathfrak{b} - \mathfrak{a}$ (где $\mathfrak{a}$ и $\mathfrak{b}$ — точки), то $\operatorname{subd}\gamma$ есть сумма двух 1-симплексов, границы которых соответственно равны $\mathfrak{b}_1 - \mathfrak{a}$ и $\mathfrak{b} - \mathfrak{b}_1$, где $\mathfrak{b}_1$ — точка из $|\gamma|$, называемая барицентром симплекса γ.

4) Для любой n-цепи γ имеем $\partial(\operatorname{subd}\gamma) = \operatorname{subd}\partial\gamma$.

5) Если цепь γ лежит на некотором подмножестве Y пространства X, то $\operatorname{subd}\gamma$ также лежит на Y и не зависит от того, где мы рассматриваем цепь γ, на X или на Y.

6) Если $\partial\gamma$ лежит на некотором подмножестве Y пространства X, то цепь $\operatorname{subd}\gamma$ гомологична γ по модулю Y, в частности, цепь $\operatorname{subd}\gamma$ гомологична γ на $|\gamma|$ по модулю $|\partial\gamma|$.

7) Для целого числа $p \geqslant 0$ цепь $\operatorname{subd}^p\gamma$ определяется индуктивно формулами:

$$\operatorname{subd}^0\gamma = \gamma, \quad \operatorname{subd}^{p+1}\gamma = \operatorname{subd}(\operatorname{subd}^p\gamma).$$

Если пространство X покрыто семейством $\mathscr{F}$ открытых множеств, то для любой цепи γ существует целое число $p \geqslant 0$ такое, что каждый симплекс, входящий в $\operatorname{subd}^p\gamma$, лежит на некотором множестве из семейства $\mathscr{F}$.

Если Δ есть замкнутый круг на комплексной плоскости с центром в точке a, то $\{a\}$ является, очевидно, деформационным ретрактом круга Δ, откуда легко следует, что

$H_n(\Delta)=\{0\}$ для всех $n>0$. Предполагая, что $\Delta\neq\{a\}$, обозначим через Γ окружность круга Δ. Можно доказать, что тогда $H_0(\Gamma)$ и $H_1(\Gamma)$ — бесконечные циклические группы, а если $n>1$, то $H_n(\Gamma)=\{0\}$. Группы $H_0(\Delta, \Gamma)$, $H_1(\Delta, \Gamma)$ и $H_n(\Delta, \Gamma)$ при $n>2$ — все нулевые, в то время как $H_2(\Delta, \Gamma)$ — бесконечная циклическая группа. Так как Γ является деформационным ретрактом множества $\Delta\setminus\{a\}$, то получаем, что $H_n(\Delta, \Delta\setminus\{a\})=\{0\}$ при $n\neq 2$, а $H_2(\Delta, \Delta\setminus\{a\})$ — бесконечная циклическая группа.

Если I есть интервал, открытый или замкнутый, то $H_n(I)=\{0\}$ при всех $n>0$.

§ 4. Периоды дифференциалов

Согласно гл. VI каждому элементу x из R мы можем сопоставить дифференциал dx поля R. Далее, если x не есть константа, то, как мы знаем, каждый дифференциал поля R может быть представлен в виде $y\,dx$, где $y\in R$. Если элементы x и x' из R не являются константами, то

$$y\,dx=(yD_{x'}x)\,dx', \tag{1}$$

где $D_{x'}$ — дифференцирование в R по x'.

Пусть U — открытое множество римановой поверхности S поля R. Каждой паре (f, x), состоящей из мероморфной на U функции f и отличного от константы элемента $x\in R$, мы поставим в соответствие новый объект, который будем называть *мероморфным дифференциалом на U*. По определению мероморфные дифференциалы, соответствующие парам (f, x) и (f', x'), считаются равными между собой тогда и только тогда, если $f=f'D_xx'$, где D_x — дифференцирование в R по x. Если $U=S$, то f является элементом поля R (теорема 4 § 2), поэтому мы можем в этом случае мероморфный дифференциал, соответствующий паре (f, x), отождествить с дифференциалом $f\,dx$ поля R, что допустимо в силу вышеприведенной формулы (1). В случае, когда U есть произвольное открытое множество, мероморфный дифференциал, соответствующий паре (f, x), мы будем обозначать также через $f\,dx$. Если $\omega=f\,dx$ и $\omega'=f'\,dx$ — мероморфные дифференциалы на U и если g — произвольная мероморфная на U функция, то полагаем $g\omega=(gf)\,dx$

и $\omega+\omega'=(f+f')dx$; легко проверить, что эти определения находятся в согласии с условием равенства мероморфных дифференциалов.

Пусть fdx есть мероморфный дифференциал на U, и пусть $\mathfrak{p}$ — точка из U. Выберем униформизирующую переменную t в точке $\mathfrak{p}$. Тогда мы можем записать $fdx=(fD_tx)\,dt$. Если для функции fD_tx точка $\mathfrak{p}$ не является полюсом, то будем говорить, что дифференциал fdx *голоморфен в точке* $\mathfrak{p}$. Вводя это определение мы должны показать, что факт отсутствия полюса в точке $\mathfrak{p}$ для функции fD_tx не зависит от выбора униформизирующей переменной t. Пусть t' — любая другая униформизирующая переменная в точке $\mathfrak{p}$; тогда $fdx=(fD_tx)\,dt=(fD_txD_{t'}t)\,dt'$. В $\mathfrak{p}$-адическом пополнении поля R разложение элемента t в степенной ряд по t' имеет вид $t=\sum_{k=1}^{\infty}a_kt'^k$, откуда $D_{t'}t=\sum_{k=1}^{\infty}ka_kt'^{k-1}$. Из последнего равенства следует, что функция $D_{t'}t$ в точке $\mathfrak{p}$ не имеет полюса. Таким образом, если точка $\mathfrak{p}$ не является полюсом для fD_tx, то она не является полюсом и для $fD_{t'}x=fD_txD_{t'}t$. Мероморфный дифференциал, голоморфный в каждой точке множества U, называется *голоморфным на* U.

Пусть g — мероморфная функция на открытом подмножестве U поверхности S, и пусть x — элемент поля R, отличный от константы. Пусть $\mathfrak{p}$ — произвольная точка из U; выберем в точке $\mathfrak{p}$ униформизирующую переменную t и обозначим через V открытый t-круг с t-центром в точке $\mathfrak{p}$ (содержащийся в U). Тогда для любой точки $\mathfrak{q}\in V$ мы имеем $g(\mathfrak{q})=G(t(\mathfrak{q}))$, где G — функция, мероморфная на круге $t(V)$. Производная G' от функции G также мероморфна на $t(V)$. Для каждой точки $\mathfrak{q}\in V$ положим $g'(\mathfrak{q})=G'(t(\mathfrak{q}))$. Ясно, что функция D_xtg' мероморфна на V; значение этой функции в точке $\mathfrak{p}$ обозначим через $f_{\mathfrak{p}}$. Точка $f_{\mathfrak{p}}\in\Sigma$ не зависит от выбора униформизирующей переменной t в точке $\mathfrak{p}$ и t-круга V. Действительно, пусть t_1 — любая другая униформизирующая переменная в точке $\mathfrak{p}$, и пусть V_1 — произвольный открытый t_1-круг с t_1-центром в точке $\mathfrak{p}$. Положим $g(\mathfrak{q})=G_1(t_1(\mathfrak{q}))$, где G_1 — мероморфная функция на $t_1(V_1)$. Если $\tau\in t(V\cap V_1)$, то $G(\tau)=G_1(\theta(\tau))$, где функция $\theta(\tau)$

определена равенством $\theta(t(\mathfrak{q})) = t_1(\mathfrak{q})$ для $\mathfrak{q} \in V \cap V_1$. Отсюда следует, что $G'(\tau) = G_1'(\theta(\tau))\theta'(\tau)$, где θ' — производная от голоморфной функции θ. Для $\mathfrak{q} \in V_1$ положим $g_1'(\mathfrak{q}) = G_1'(t_1(\mathfrak{q}))$. Так как $\theta'(t(\mathfrak{q})) = (D_t t_1)(\mathfrak{q})$ (что легко следует из теоремы 2 § 2), то для любой точки $\mathfrak{q} \in V \cap V_1$ мы имеем $g'(\mathfrak{q}) = (g_1' D_t t_1)(\mathfrak{q})$, откуда $(g' D_x t)(\mathfrak{q}) = (g_1' D_x t_1)(\mathfrak{q})$, что и доказывает наше утверждение. Легко теперь видеть, что отображение $\mathfrak{p} \to f_{\mathfrak{p}}$ является мероморфной функцией f на U; эту функцию будем обозначать через $\frac{dg}{dx}$ (если $g \in R$, то, как легко показать, определенная здесь функция $\frac{dg}{dx}$ совпадает с отношением дифференциалов dg и dx, т. е. равна $D_x g$). Далее, если x' — любой другой элемент поля R, отличный от константы, то $\frac{dg}{dx'} = \frac{dg}{dx} D_{x'} x$. Отсюда следует, что дифференциал $\frac{dg}{dx} dx$ не зависит от выбора x. Этот мероморфный дифференциал будем обозначать через dg. Легко видеть, что если функция g голоморфна на U, то дифференциал dg также голоморфен на U.

Пусть $f\,dx$ — мероморфный дифференциал на открытом множестве U и пусть U_1 — открытое подмножество множества U. Если на U_1 существует мероморфная функция g, такая, что $\frac{dg}{dx} = f$ на U_1, то эта функция g будет называться *первообразной функцией* дифференциала $f\,dx$ на U_1. *Если множество U_1 связно, то две первообразные функции g и g' дифференциала $f\,dx$ на U_1 могут отличаться друг от друга только постоянным слагаемым.* В самом деле, в U_1 мы можем найти точку $\mathfrak{p}_0$, в которой обе функции g и g' голоморфны и такую, что $x(\mathfrak{p}_0) \neq \infty$ и $x - x(\mathfrak{p}_0)$ является униформизирующей переменной в точке $\mathfrak{p}_0$. Если мы в вышеприведенном определении вместо t возьмем $x - x(\mathfrak{p}_0)$, то в силу равенства $d(g' - g) = 0$ легко получим, что $g' - g$ на некоторой окрестности точки $\mathfrak{p}_0$ совпадает с константой a. Функция $g' - g - a$ мероморфна на U_1 и имеет неизолированный нуль, поэтому на U_1 она равна тождественно нулю, и наше утверждение доказано.

Пусть теперь ω есть дифференциал, голоморфный на некотором открытом множестве U. Мы сейчас дадим опре-

деление *интеграла* $\int\limits_{\gamma} \omega$ от дифференциала ω по произвольной 1-цепи γ, лежащей в U.

Лемма 1. *Всякий дифференциал ω, голоморфный на открытом круге V, имеет на этом круге первообразную функцию.*

Предположим, что V есть x-круг, где $x \in R$. Из теоремы 3 § 2 непосредственно следует, что для каждой точки $\mathfrak{p} \in V$ элемент $x - x(\mathfrak{p})$ является униформизирующей переменной в точке $\mathfrak{p}$. Запишем $\omega = f\,dx$ и $f(\mathfrak{p}) = F(x(\mathfrak{p}))$ для $\mathfrak{p} \in V$, где F — функция, голоморфная на $x(V)$. Как известно, на $x(V)$ существует голоморфная функция G, производная от которой равна F. Если мы для $\mathfrak{p} \in V$ положим $g(\mathfrak{p}) = G(x(\mathfrak{p}))$, то g и будет первообразной функцией для дифференциала ω.

Дадим теперь определение интеграла $\int\limits_{\gamma} \omega$ для случая, когда γ есть 1-симплекс на некотором открытом круге V, содержащемся в U. Как известно, 0-цепь $\partial\gamma$ имеет вид $\mathfrak{b} - \mathfrak{a}$, где $\mathfrak{a}$ и $\mathfrak{b}$ — точки из V. Пусть g — первообразная функция дифференциала ω на V. Утверждаем, что число $g(\mathfrak{b}) - g(\mathfrak{a})$ не зависит от выбора V и g. Пусть V' — любой другой открытый круг, содержащийся в U и содержащий $|\gamma|$, и пусть g' — первообразная функция дифференциала ω на V'. Так как множество $|\gamma|$, очевидно, связно, то оно содержится в некоторой компоненте W пересечения $V \cap V'$. Но, как мы видели выше, разность $g' - g$ на W есть константа; следовательно, $g'(\mathfrak{b}) - g'(\mathfrak{a}) = g(\mathfrak{b}) - g(\mathfrak{a})$, и наше утверждение доказано. Для рассматриваемого случая положим теперь

$$\int\limits_{\gamma} \omega = g(\mathfrak{b}) - g(\mathfrak{a}).$$

Пусть $\mathfrak{b}_1$ есть барицентр 1-симплекса γ. Тогда цепь $\operatorname{subd}\gamma$ имеет вид $\gamma_1 + \gamma_2$, где γ_1 и γ_2 — 1-симплексы, для которых $\partial\gamma_1 = \mathfrak{b}_1 - \mathfrak{a}$ и $\partial\gamma_2 = \mathfrak{b} - \mathfrak{b}_1$. Отсюда вытекает равенство

$$\int\limits_{\gamma} \omega = \int\limits_{\gamma_1} \omega + \int\limits_{\gamma_2} \omega.$$

Далее, пусть γ есть 1-цепь, такая, что каждый 1-симплекс, входящий в γ, лежит на некотором открытом круге.

Если $\gamma = \sum_{k=1}^{h} a_k \sigma_k$, где $\sigma_1, \ldots, \sigma_h$ — симплексы, входящие в γ, то полагаем

$$\int_\gamma \omega = \sum_{k=1}^{h} a_k \int_{\sigma_k} \omega.$$

Из определения непосредственно следует, что

$$\int_\gamma \omega = \int_{\operatorname{subd}\gamma} \omega.$$

Пусть, наконец, γ — произвольная 1-цепь на U. Открытые круги, содержащиеся в U, образуют покрытие множества U открытыми множествами; следовательно, при достаточно большом p, каждый симплекс, входящий в $\operatorname{subd}^p \gamma$, лежит в некотором открытом круге, содержащемся в U. Так как для $p' > p$ мы имеем $\operatorname{subd}^{p'} \gamma = \operatorname{subd}^{p'-p}(\operatorname{subd}^p \gamma)$, то число $\int_{\operatorname{subd}^p \gamma} \omega$ не зависит от выбора целого p, удовлетворяющего вышеуказанному условию. Это и есть то число, которое называется *интегралом* от дифференциала ω по 1-цепи γ и обозначается через $\int_\gamma \omega$.

Ясно, что отображение $\gamma \to \int_\gamma \omega$ есть гомоморфизм группы 1-цепей на U в аддитивную группу комплексных чисел, а при фиксированном γ отображение $\omega \to \int_\gamma \omega$ есть линейная функция на векторном пространстве (над полем C) всех голоморфных на U дифференциалов. Кроме того, $\int_\gamma \omega = \int_{\operatorname{subd}^p \gamma} \omega$ для любой 1-цепи γ на U и для любого целого числа $p \geqslant 0$.

Лемма 2. *Пусть ω — голоморфный дифференциал на открытом множестве U римановой поверхности и пусть γ — 1-цепь на U. Положим $\partial\gamma = \sum_{k=1}^{h} a_k \mathfrak{p}_k$, где $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ —*

точки множества U. Если дифференциал ω обладает на U первообразной функцией g, то

$$\int_\gamma \omega = \sum_{k=1}^{h} a_k g(\mathfrak{p}_k).$$

Выберем целое число $p \geqslant 0$ так, чтобы каждый симплекс, входящий в $\operatorname{subd}^p \gamma$, лежал в некотором открытом круге, содержащемся в U. Положим $\operatorname{subd}^p \gamma = \sum_{l=1}^{m} b_l \sigma_l$, где $\sigma_1, \ldots, \sigma_m$ — симплексы, входящие в $\operatorname{subd}^p \gamma$. Если $\partial \sigma_l = \mathfrak{b}_l - \mathfrak{a}_l$, то $\int_\gamma \omega = \int_{\operatorname{subd}^p \gamma} \omega = \sum_{l=1}^{m} b_l (g(\mathfrak{b}_l) - g(\mathfrak{a}_l))$. С другой стороны, $\sum_{l=1}^{m} b_l (\mathfrak{b}_l - \mathfrak{a}_l) = \partial(\operatorname{subd}^p \gamma) = \partial\gamma = \sum_{k=1}^{h} a_k \mathfrak{p}_k$, откуда и следует лемма 2.

Теорема 5 (теорема Коши). *Пусть ω — голоморфный дифференциал на открытом множестве U римановой поверхности поля R. Если γ есть 1-цикл, являющийся на U границей, то $\int_\gamma \omega = 0$.*

Положим $\gamma = \partial\varphi$, где φ — 2-цепь на U. Выберем целое число $p \geqslant 0$ так, чтобы каждый 2-симплекс, входящий в $\operatorname{subd}^p \varphi$, лежал в некотором открытом круге, содержащемся в U. Так как $\int_\gamma \omega = \int_{\operatorname{subd}^p \gamma} \omega$ и $\operatorname{subd}^p \gamma = \partial(\operatorname{subd}^p \varphi)$, то теорему 5 достаточно доказать для случая, когда γ есть граница 2-симплекса φ, лежащего в некотором открытом круге V, содержащемся в U. Так как дифференциал ω обладает на V первообразной функцией (лемма 1) и $\partial\gamma = 0$, то для этого случая утверждение теоремы непосредственно следует из леммы 2.

Лемма 3. *Пусть U — открытое подмножество римановой поверхности поля R и пусть Q — конечное подмножество множества U. Если γ и γ' — 1-циклы на U по модулю Q, представляющие один и тот же элемент*

группы $H_1(U, Q)$, то разность $\gamma' - \gamma$ является гомологичным нулю циклом на U.

Рассмотрим следующие четыре члена гомологической последовательности для пары (U, Q):

$$H_1(Q) \to H_1(U) \to H_1(U, Q) \to H_0(Q).$$

Так как γ и γ' представляют один и тот же элемент группы $H_1(U, Q)$, то $\partial\gamma$ и $\partial\gamma'$ представляют один и тот же элемент группы $H_0(Q)$, а значит, $\partial\gamma = \partial\gamma'$, ибо множество Q конечно. Отсюда следует, что $\gamma' - \gamma$ есть цикл на U, класс гомологий которого принадлежит ядру гомоморфизма группы $H_1(U)$ в $H_1(U, Q)$. В силу теоремы о точности, это ядро равно образу группы $H_1(Q)$, а эта группа состоит только из нулевого элемента (ибо Q конечно). Лемма 3, таким образом, доказана.

Сохраняя обозначения леммы 3, рассмотрим голоморфный на U дифференциал ω и элемент c из группы $H_1(U, Q)$. Пусть γ — 1-цепь, принадлежащая c. Из теоремы Коши и леммы 3 следует, что $\int\limits_\gamma \omega$ зависит только от c и ω. Это число называется *интегралом от дифференциала ω по c* и обозначается через $\int\limits_c \omega$. Если множество Q пусто, т. е. если $c \in H_1(U)$, то $\int\limits_c \omega$ называется также *периодом дифференциала ω относительно c*. Если ω и Q фиксированы, то отображение $c \to \int\limits_c \omega$ является гомоморфизмом группы $H_1(U, Q)$ в аддитивную группу комплексных чисел. Если элемент c фиксирован, то отображение $\omega \to \int\limits_c \omega$ есть линейная функция на векторном пространстве (над полем C) дифференциалов, голоморфных на U. Пусть U_1 — открытое подмножество множества U и Q_1 — подмножество пересечения $Q \cap U_1$; обозначим через c_1 элемент группы $H_1(U_1, Q_1)$ и через c — элемент группы $H_1(U, Q)$, соответствующий элементу c_1 при тождественном отображении пары (U_1, Q_1) в (U, Q). Ясно, что тогда $\int\limits_{c_1} \omega = \int\limits_c \omega$.

Рассмотрим теперь случай, когда дифференциал ω мероморфен, но не голоморфен на U. Всякую точку $\mathfrak{p} \in U$, в которой ω не голоморфен, будем называть *полюсом* дифференциала ω. Простоты ради мы рассмотрим лишь случай, когда ω имеет только конечное число полюсов; это, разумеется, всегда имеет место, если ω есть дифференциал поля R. Пусть P есть множество всех полюсов дифференциала ω (или любое конечное множество, содержащее все полюса); положим $U_1 = U \setminus P$. Пусть Q — конечное подмножество множества U_1. Для каждого элемента $c \in H_1(U_1, Q)$ интеграл $\int\limits_c \omega$ уже определен. Тождественное отображение U_1 в U определяет некоторый гомоморфизм группы $H_1(U_1, Q)$ в $H_1(U, Q)$; займемся более детальным изучением этого гомоморфизма.

Пусть P обозначает произвольное конечное подмножество открытого множества U, а Q — произвольное подмножество множества $U \setminus P$. Рассмотрим следующие четыре члена гомологической последовательности для тройки $(U, U \setminus P, Q)$:

$$H_2(U, U \setminus P) \xrightarrow{\eta_1} H_1(U \setminus P, Q) \xrightarrow{\eta} \\ \xrightarrow{\eta} H_1(U, Q) \xrightarrow{\eta_2} H_1(U, U \setminus P)$$

(через η_1, η и η_2 обозначены гомоморфизмы гомологической последовательности). Как нам известно, ядра гомоморфизмов η и η_2 совпадают с $\eta_1(H_2(U, U \setminus P))$ и $\eta(H_1(U \setminus P, Q))$ соответственно.

Так как P конечно, то индукцией по числу элементов множества P легко доказывается, что для каждой точки $\mathfrak{p} \in P$ мы можем построить замкнутый круг $D_{\mathfrak{p}}$, содержащийся в U и содержащий $\mathfrak{p}$ внутри себя, так, чтобы $D_{\mathfrak{p}} \cap D_{\mathfrak{q}} = \varnothing$ при $\mathfrak{p} \neq \mathfrak{q}$. Обозначим через W объединение множеств $D_{\mathfrak{p}}$ для всех $\mathfrak{p} \in P$. Замыкание множества $U \setminus W$ в U содержится в открытом подмножестве множества $U \setminus P$; поэтому, в силу теоремы вырезания, группы $H_2(U, U \setminus P)$ и $H_1(U, U \setminus P)$ изоморфны группам $H_2(W, W \setminus P)$ и $H_1(W, W \setminus P)$ соответственно. Так как множества $D_{\mathfrak{p}}$ попарно не пересекаются, то группы $H_2(W, W \setminus P)$ и $H_1(W, W \setminus P)$ изоморфны произведениям $\prod\limits_{\mathfrak{p} \in P} H_2(D_{\mathfrak{p}}, D_{\mathfrak{p}} \setminus \{\mathfrak{p}\})$

и $\prod_{\mathfrak{p}\in P} H_1(D_{\mathfrak{p}}, D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$ соответственно. Рассмотрим теперь следующие семь членов гомологической последовательности для пары $(D_{\mathfrak{p}}, D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$:

$$H_2(D_{\mathfrak{p}}) \to H_2(D_{\mathfrak{p}}, D_{\mathfrak{p}}\setminus\{\mathfrak{p}\}) \xrightarrow{\zeta} H_1(D_{\mathfrak{p}}\setminus\{\mathfrak{p}\}) \to H_1(D_{\mathfrak{p}}) \xrightarrow{\zeta_1}$$
$$\xrightarrow{\zeta_1} H_1(D_{\mathfrak{p}}, D_{\mathfrak{p}}\setminus\{\mathfrak{p}\}) \xrightarrow{\zeta_2} H_0(D_{\mathfrak{p}}\setminus\{\mathfrak{p}\}) \to H_0(D_{\mathfrak{p}})$$

(греческие буквы обозначают гомоморфизмы гомологической последовательности). Мы знаем, что группы $H_2(D_{\mathfrak{p}})$ и $H_1(D_{\mathfrak{p}})$ тривиальны; следовательно, по теореме о точности, ζ есть изоморфизм группы $H_2(D_{\mathfrak{p}}, D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$ на $H_1(D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$. Обозначим через $C_{\mathfrak{p}}$ окружность круга $D_{\mathfrak{p}}$; как известно, $H_1(C_{\mathfrak{p}})$ есть бесконечная циклическая группа. Пусть $\gamma_{\mathfrak{p}}$ есть 1-цикл на $C_{\mathfrak{p}}$, класс гомологий которого порождает $H_1(C_{\mathfrak{p}})$. Ясно, что $C_{\mathfrak{p}}$ является деформационным ретрактом множества $D_{\mathfrak{p}}\setminus\{\mathfrak{p}\}$; следовательно, $H_1(D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$ есть бесконечная циклическая группа, порожденная классом гомологий цикла $\gamma_{\mathfrak{p}}$ в $H_1(D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$. Отсюда следует, что $H_2(D_{\mathfrak{p}}, D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$ — бесконечная циклическая группа; кроме того, так как ζ — граничный гомоморфизм, то $H_2(D_{\mathfrak{p}}, D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$ порождается классом гомологий 2-цепи $\delta_{\mathfrak{p}}$ на $D_{\mathfrak{p}}$, для которой $\partial\delta_{\mathfrak{p}} = \gamma_{\mathfrak{p}}$. Таким образом, группа $H_2(W, W\setminus P)$, а значит и группа $H_2(U, U\setminus P)$, порождается классами гомологий цепей $\delta_{\mathfrak{p}}$ для всех $\mathfrak{p}\in P$. Так как отображение η_1 есть граничный гомоморфизм, то получаем, что ядро гомоморфизма η группы $H_1(U\setminus P, Q)$ в $H_1(U, Q)$ порождается в группе $H_1(U\setminus P, Q)$ классами гомологий цепей $\gamma_{\mathfrak{p}}$.

Пусть теперь $\mathfrak{q}$ — произвольная точка из $D_{\mathfrak{p}}$, отличная от $\mathfrak{p}$. Так как $D_{\mathfrak{p}}$ и $D_{\mathfrak{p}}\setminus\{\mathfrak{p}\}$ линейно связны, то группы гомологий $H_0(D_{\mathfrak{p}})$ и $H_0(D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$ порождаются классами гомологий 0-цепи $\mathfrak{q}$ в этих группах. Отсюда следует, что образ группы $H_1(D_{\mathfrak{p}}, D_{\mathfrak{p}}\setminus\{\mathfrak{p}\})$ при гомоморфизме ζ_2 равен $\{0\}$ и, следовательно, что $H_1(D_{\mathfrak{p}}, D_{\mathfrak{p}}\setminus\{\mathfrak{p}\}) = \zeta_1(H_1(D_{\mathfrak{p}})) = \{0\}$. Этим доказано, что $H_1(U, U\setminus P) = \{0\}$, а значит, η отображает $H_1(U\setminus P, Q)$ на $H_1(U, Q)$. Таким образом, нами доказана

Лемма 4. *Пусть U — открытое подмножество римановой поверхности поля R, P — конечное подмножество множества U и Q — подмножество множества $U\setminus P$. Для каждой точки $\mathfrak{p}\in P$ построим замкнутый круг*

$D_{\mathfrak{p}} \subset U$, содержащий $\mathfrak{p}$ внутри себя, так, чтобы $D_{\mathfrak{p}} \cap D_{\mathfrak{q}} = \varnothing$ при $\mathfrak{p} \neq \mathfrak{q}$. Обозначим через $C_{\mathfrak{p}}$ окружность круга $D_{\mathfrak{p}}$ и через $\gamma_{\mathfrak{p}}$ — 1-цикл на $C_{\mathfrak{p}}$, класс гомологий которого порождает $H_1(C_{\mathfrak{p}})$. Тогда тождественное отображение пары $(U \setminus P, Q)$ в пару (U, Q) определяет гомоморфизм группы $H_1(U \setminus P, Q)$ на $H_1(U, Q)$, ядро которого порождается классами гомологий циклов $\gamma_{\mathfrak{p}}$ в $H_1(U \setminus P, Q)$. Пусть, далее, $\delta_{\mathfrak{p}}$ есть 2-цепь на $D_{\mathfrak{p}}$ такая, что $\partial\delta_{\mathfrak{p}} = \gamma_{\mathfrak{p}}$, и пусть $d_{\mathfrak{p}}$ — класс гомологий цепи $\delta_{\mathfrak{p}}$ в $H_2(U, U \setminus P)$. Тогда группа $H_2(U, U \setminus P)$ есть свободная абелева группа, для которой элементы $d_{\mathfrak{p}}$ являются свободными образующими.

Следствие. *Пусть сохраняются обозначения леммы 4 и пусть γ есть 1-цепь на U, для которой $|\partial\gamma| \cap P = \varnothing$; тогда на $U \setminus P$ существует 1-цепь γ' такая, что $\gamma' - \gamma$ есть гомологичный нулю цикл на U.*

Положим $Q = |\partial\gamma|$; в силу леммы 4, класс гомологий с цепи γ в $H_1(U, Q)$ может быть представлен 1-цепью γ' на $U \setminus P$. Так как Q конечно, то, применяя лемму 3, получаем, что $\gamma' - \gamma$ есть гомологичный нулю цикл на U.

Сохраняя введенные выше обозначения, вернемся теперь к изучению мероморфного дифференциала ω. Если элемент z_1 из $H_1(U \setminus P)$ принадлежит ядру гомоморфизма группы $H_1(U \setminus P)$ в $H_1(U)$, соответствующего тождественному отображению $U \setminus P$ в U, то $\int\limits_{z_1} \omega$ называется *логарифмическим периодом* дифференциала ω. Легко видеть, что каждый логарифмический период дифференциала ω есть линейная комбинация с целыми коэффициентами чисел $\int\limits_{\gamma_{\mathfrak{p}}} \omega$, где $\gamma_{\mathfrak{p}}$ — циклы, определение которых дано в лемме 4. Сейчас мы займемся вычислением этих чисел.

Пусть $\mathfrak{p}$ — произвольная точка из P и D — замкнутый круг, содержащий $\mathfrak{p}$ внутри себя и такой, что $D \cap P = \{\mathfrak{p}\}$. Мы можем выбрать униформизирующую переменную x в точке $\mathfrak{p}$ так, чтобы круг D был x-кругом с x-центром в точке $\mathfrak{p}$. Если мы запишем $\omega = f\,dx$, то можно будет найти открытый x-круг V с x-центром в $\mathfrak{p}$, на котором функция f мероморфна и не имеет полюсов кроме, быть

может, самой точки $\mathfrak{p}$. Для любой точки $\mathfrak{q} \in V$, $\mathfrak{q} \neq \mathfrak{p}$, $f(\mathfrak{q})$ можно представить в виде $f(\mathfrak{q}) = \sum_{i=-r}^{\infty} c_i (x(\mathfrak{q}))^i$ (где $r > 0$). Обозначим через f_1 мероморфную функцию, определенную на V равенством $f_1(\mathfrak{q}) = f(\mathfrak{q}) - c_{-1}(x(\mathfrak{q}))^{-1}$ ($\mathfrak{q} \in V$, $\mathfrak{q} \neq \mathfrak{p}$). Дифференциал $f_1 dx$ имеет на V первообразную функцию. Действительно, ряд

$$\sum_{\substack{-r \leq i < \infty \\ i \neq -1}} (i+1)^{-1} c_i (x(\mathfrak{q}))^{i+1}$$

сходится, как известно, для всех $\mathfrak{q} \neq \mathfrak{p}$ из V; обозначим его сумму через $g(\mathfrak{q})$. Ясно, что отображение $\mathfrak{q} \to g(\mathfrak{q})$ множества $V \setminus \{\mathfrak{p}\}$ в Σ может быть продолжено до мероморфной функции на V (обозначаемой также через g), и мы будем иметь $dg = f_1 dx$. Мы можем считать, что $D \subset V$. Обозначим через C — окружность круга D и через γ — 1-цикл на C, класс гомологий которого порождает $H_1(C)$. В силу леммы 2, имеем $\int_\gamma f_1 dx = 0$, откуда

$$\int_\gamma \omega = c_{-1} \int_\gamma x^{-1} dx.$$

Попутно мы получили, что если $c_{-1} = 0$, то существует открытый круг, содержащий $\mathfrak{p}$ внутри себя, на котором ω имеет первообразную функцию.

Пусть теперь $\mathfrak{a}_1$, $\mathfrak{a}_2$ и $\mathfrak{a}_3$ — три различные точки окружности C. Обозначим через V_k множество тех точек $\mathfrak{q} \in V$, для которых $x(\mathfrak{q})$ не равно числу вида $\rho x(\mathfrak{a}_k)$, где ρ — вещественное неотрицательное число. Тогда на каждом множестве V_k дифференциал $x^{-1} dx$ имеет первообразную функцию. В самом деле, для любой точки $\mathfrak{q} \in V$ число $x(\mathfrak{q})$ можно представить в виде $x(\mathfrak{a}_k) r(\mathfrak{q}) \exp(i\theta_k(\mathfrak{q}))$, где $r(\mathfrak{q})$ и $\theta_k(\mathfrak{q})$ — вещественные непрерывные функции на V_k, $r(\mathfrak{q}) > 0$, $0 < \theta_k(\mathfrak{q}) < 2\pi$. Функция Λ_k, определенная на V_k равенством $\Lambda_k(\mathfrak{q}) = \log r(\mathfrak{q}) + i\theta_k(\mathfrak{q})$, и будет первообразной функцией для дифференциала $x^{-1} dx$ на V_k. Пусть k, l и m — записанные в произвольном порядке индексы 1, 2 и 3. На окружности C мы можем найти такой 1-симплекс σ_{kl},

что $\partial\sigma_{kl} = \mathfrak{a}_l - \mathfrak{a}_k$ и $a_m \notin |\sigma_{kl}|$. Тогда цепь $\gamma_1 = \sigma_{12} + \sigma_{23} + \sigma_{31}$ есть цикл на C, и мы имеем

$$\frac{1}{l}\int\limits_{\gamma_1} x^{-1}\,dx = (\theta_3(\mathfrak{a}_2) - \theta_3(\mathfrak{a}_1)) + \\ + (\theta_1(\mathfrak{a}_3) - \theta_1(\mathfrak{a}_2)) + (\theta_2(\mathfrak{a}_1) - \theta_2(\mathfrak{a}_3)).$$

Если $k \neq l$, то $\dfrac{x(\mathfrak{a}_l)}{x(\mathfrak{a}_k)} = \exp(i\theta_k(\mathfrak{a}_l))$. Так как оба значения $\theta_k(\mathfrak{a}_l)$ и $\theta_l(\mathfrak{a}_k)$ заключены между 0 и 2π, то их сумма равна 2π, откуда

$$\frac{1}{l}\int\limits_{\gamma_1} x^{-1}\,dx = 6\pi - 2(\theta_1(\mathfrak{a}_2) + \theta_2(\mathfrak{a}_3) + \theta_3(\mathfrak{a}_1)).$$

Так как $\dfrac{x(\mathfrak{a}_2)}{x(\mathfrak{a}_1)}\dfrac{x(\mathfrak{a}_3)}{x(\mathfrak{a}_2)}\dfrac{x(\mathfrak{a}_1)}{x(\mathfrak{a}_3)} = 1$, то сумма $\theta_1(\mathfrak{a}_2) + \theta_2(\mathfrak{a}_3) + \theta_3(\mathfrak{a}_1)$ кратна 2π. Но $0 < \theta_k(\mathfrak{a}_l) < 2\pi$, поэтому эта сумма равна либо 2π, либо 4π. Этим доказано, что $\int\limits_{\gamma_1} x^{-1}\,dx = \pm 2\pi i$. Цепь $\sigma_{21} + \sigma_{32} + \sigma_{13} = \gamma_1'$ является также циклом, при этом, как легко видеть, $\int\limits_{\gamma_1'} x^{-1}\,dx = -\int\limits_{\gamma_1} x^{-1}\,dx$.

Выберем целое число $p \geqslant 0$ так, чтобы каждый симплекс, входящий в $\operatorname{subd}^p\gamma$, лежал на одном из множеств V_k. Обозначив через $\tau_1, \ldots, \tau_h$ эти симплексы, положим $\operatorname{subd}^p\gamma = \sum\limits_{l=1}^{h} a_l\tau_l$. Если $\partial\tau_l = \mathfrak{d}_l - \mathfrak{c}_l$, то, как легко видеть,

$$\exp\left(\int\limits_{\tau_l} x^{-1}\,dx\right) = \frac{x(\mathfrak{d}_l)}{x(\mathfrak{c}_l)}.$$

Так как γ — цикл, то

$$\sum_{l=1}^{h} a_l(\mathfrak{d}_l - \mathfrak{c}_l) = 0,$$

поэтому $\exp\left(\int\limits_\gamma x^{-1}dx\right)=1$. Этим доказано, что значение $\int\limits_\gamma x^{-1}dx$ кратно $2\pi i$. Класс гомологий цепи γ порождает всю группу $H_1(C)$; значит, цепь γ_1 гомологична на C цепи $r\gamma$, где r — целое число, и, следовательно, $2\pi i = r\int\limits_\gamma x^{-1}\,dx$. Отсюда непосредственно следует, что $r=\pm 1$. Заменив, если это необходимо, γ на $-\gamma$, мы в дальнейшем можем считать, что для цепи γ имеет место равенство $\int\limits_\gamma x^{-1}dx = 2\pi i$.

Этим условием, при заданных D и x, вполне определен класс гомологий z цепи γ в группе $H_1(C)$. Покажем сейчас, что в действительности z не зависит от выбора x (при соблюдении условия, что D является x-кругом). В самом деле, пусть x' — любой другой элемент поля R, такой, что D является x'-кругом. Тогда x' является униформизирующей переменной для некоторой внутренней точки $\mathfrak{p}'$ круга D. Положим $x(\mathfrak{p}')=a$. Если $a=0$, то по лемме Шварца $x'=bx$, где b — константа, откуда $\int\limits_\gamma x'^{-1}dx' = \int\limits_\gamma x^{-1}dx$. Если же $a\neq 0$, то обозначим через l множество точек $\mathfrak{q}\in D$, для которых $x(\mathfrak{q})$ имеет вид ta, где t вещественно и $0\leqslant t\leqslant 1$. Легко видеть, что дифференциал $x^{-1}dx-(x-a)^{-1}dx$ на $V\setminus l$ имеет первообразную функцию и, следовательно, $\int\limits_\gamma x^{-1}dx = \int\limits_\gamma (x-a)^{-1}dx$ (лемма 2).

С другой стороны, существует открытое множество, содержащее D, на котором функция $(x-a)^{-1}x'$ голоморфна и не имеет нулей. Если мы эту функцию обозначим через u, то будем иметь $0=\int\limits_\gamma u^{-1}du = \int\limits_\gamma x'^{-1}dx' - \int\limits_\gamma (x-a)^{-1}dx$, откуда $\int\limits_\gamma x'^{-1}dx' = \int\limits_\gamma x^{-1}dx$. Таким образом, любому замкнутому кругу D мы можем сопоставить определенную

образующую z группы $H_1(C)$, где C — окружность этого круга. Будем говорить, что z является *положительной образующей группы* $H_1(C)$. Эта образующая характеризуется условием $\int\limits_{\gamma} x^{-1}\,dx = 2\pi i$, где x — любой элемент поля R, для которого D является x-кругом.

В случае, когда ω есть дифференциал поля R, то число, обозначенное выше через c_{-1}, есть вычет дифференциала ω в точке $\mathfrak{p}$ (следствие к теореме 6 § 3 гл. VI); это число не зависит от выбора x. Покажем, что c_{-1} не зависит от выбора x и в общем случае любого мероморфного дифференциала. Пользуясь введенными выше обозначениями, заметим, что дифференциал $\omega - \left(\sum\limits_{i=-r}^{-1} c_i x^i\,dx\right)$ не имеет полюса в точке $\mathfrak{p}$. Пусть x' — любая другая униформизирующая переменная в точке $\mathfrak{p}$. Если мы положим $\omega = f'\,dx'$, то функция $f' - \left(\sum\limits_{i=-r}^{-1} c_i x^i\right) D_x x'$ также не будет иметь полюса в точке $\mathfrak{p}$. Наше утверждение непосредственно следует теперь из того, что $\left(\sum\limits_{i=-r}^{-1} c_i x^i\right) dx = \left(\sum\limits_{i=-r}^{-1} c_i x^i\right) D_x x'\,dx'$ есть дифференциал поля R. Число c_{-1} называется *вычетом дифференциала* ω *в точке* $\mathfrak{p}$. Итак, нами доказана

Теорема 6. *Пусть ω — мероморфный дифференциал на открытом множестве U римановой поверхности поля R. Пусть $\mathfrak{p}$ — точка из U и D — замкнутый круг, содержащий $\mathfrak{p}$ внутри себя, на котором ω не имеет полюсов, кроме, быть может, точки $\mathfrak{p}$. Обозначим через C окружность круга D и через z — положительную образующую группы $H_1(C)$. Тогда $\int\limits_{z} \omega = 2\pi i\rho$, где ρ — вычет дифференциала ω в точке $\mathfrak{p}$.*

Используя те же обозначения, что и выше, мы видим, что классы гомологий циклов γ_1 и γ_1' в $H_1(C)$ не зависят от выбора симплексов σ_{kl} и что один и только один из этих классов является положительной образующей группы $H_1(C)$. Если γ_1 принадлежит положительной образующей, то будем говорить, что точки $\mathfrak{a}_1$, $\mathfrak{a}_2$ и $\mathfrak{a}_3$ (взятые в указанном порядке)

определяют *положительную ориентацию* на C; в противном случае, будем говорить, что $\mathfrak{a}_1$, $\mathfrak{a}_2$ и $\mathfrak{a}_3$ определяют *отрицательную ориентацию* на C. В первом случае, мы положим $\varepsilon(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3) = 1$, во втором $\varepsilon(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3) = -1$. Легко устанавливаются следующие свойства введенного символа: при четной перестановке аргументов $\mathfrak{a}_1$, $\mathfrak{a}_2$ и $\mathfrak{a}_3$ значение символа $\varepsilon(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3)$ не меняется, а при нечетной перестановке — меняет знак на противоположный; если C' и C'' — компоненты множества $C \setminus \{\mathfrak{a}_1, \mathfrak{a}_2\}$, то значение символа $\varepsilon(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a})$ (при фиксированных $\mathfrak{a}_1$ и $\mathfrak{a}_2$) постоянно на каждом из множеств C' и C'', и эти два значения различны между собой.

Пусть ω — мероморфный дифференциал на открытом множестве U; предположим, что ω имеет только конечное число полюсов на U. Из леммы 4 и теоремы 6 непосредственно следует, что логарифмические периоды дифференциала ω являются линейными комбинациями с целыми коэффициентами чисел $2\pi i\rho$, где ρ пробегает все вычеты дифференциала ω. Если все вычеты дифференциала ω равны 0, то равны 0 и все его логарифмические периоды. Предполагая, что именно этот случай имеет место, обозначим через P множество полюсов дифференциала ω на U. Пусть Q — конечное подмножество множества $U \setminus P$. Согласно лемме 4 каждый элемент $c \in H_1(U, Q)$ является образом некоторого элемента $c_1 \in H_1(U \setminus P, Q)$ при гомоморфизме, соответствующем тождественному отображению пары $(U \setminus P, Q)$ в (U, Q). Так как логарифмические периоды дифференциала ω равны 0, то число $\int\limits_{c_1} \omega$ зависит только от c и не зависит от выбора c_1. Это число мы обозначим через $\int\limits_{c} \omega$.

Теорема 7. *Пусть ω — мероморфный дифференциал на открытом множестве U римановой поверхности поля R. Предположим, что дифференциал ω имеет на U только конечное число полюсов и что его вычеты во всех этих полюсах равны 0. Для того, чтобы для дифференциала ω существовала на U первообразная функция, необходимо и достаточно, чтобы $\int\limits_{z} \omega = 0$ для всех $z \in H_1(U)$.*

Не ограничивая общности, мы можем, очевидно, считать, что U связно. Необходимость условия вытекает непосредственно из леммы 2. Допустим, что условие выполнено. Пусть P — множество полюсов дифференциала ω на U. Тогда $U \setminus P$ открыто и, как легко видеть, связно, а значит, и линейно связно. Фиксируем произвольную точку $\mathfrak{p}_0$ из $U \setminus P$. Тогда для любой точки $\mathfrak{p} \in U \setminus P$ мы можем на $U \setminus P$ найти такую 1-цепь $\gamma_{\mathfrak{p}}$, что $\partial\gamma_{\mathfrak{p}} = \mathfrak{p} - \mathfrak{p}_0$. Положим $g(\mathfrak{p}) = \int\limits_{\gamma_{\mathfrak{p}}} \omega$.

Покажем, что функция g голоморфна на $U \setminus P$. Пусть $\mathfrak{p}$ — произвольная точка из $U \setminus P$, и пусть V — открытый круг, содержащийся в $U \setminus P$ и содержащий точку $\mathfrak{p}$. На V дифференциал ω обладает первообразной функцией g_1. Для любой точки $\mathfrak{q}$ из V мы можем на V найти 1-цепь $\gamma_{\mathfrak{pq}}$, для которой $\partial\gamma_{\mathfrak{pq}} = \mathfrak{q} - \mathfrak{p}$. Тогда $\gamma_{\mathfrak{p}} + \gamma_{\mathfrak{pq}} - \gamma_{\mathfrak{q}}$ есть 1-цикл на $U \setminus P$, и, в силу наших предположений, интеграл от дифференциала ω по этому циклу равен 0. Отсюда следует, что $g(\mathfrak{q}) = g(\mathfrak{p}) + \int\limits_{\gamma_{\mathfrak{pq}}} \omega = g(\mathfrak{p}) + g_1(\mathfrak{q}) - g_1(\mathfrak{p})$. Таким образом, функция $g - g_1$ постоянна на V, а значит, на V функция g является первообразной для ω. Пусть теперь $\mathfrak{a}$ — полюс дифференциала ω. Так как вычет ω в точке $\mathfrak{a}$ равен 0, то, как мы видели, существует открытый круг $W \subset U$, содержащий точку $\mathfrak{a}$, на котором ω имеет первообразную функцию g_2. Множество $W \setminus (W \cap P)$, очевидно, связно, поэтому на этом множестве функция $g_2 - g$ постоянна. Отсюда следует, что функция g может быть продолжена до функции, мероморфной на W. Так как изложенное применимо к любому полюсу дифференциала ω, то функция g, следовательно, может быть продолжена до функции, мероморфной на U. Эта функция и является, очевидно, первообразной для ω на U.

§ 5. Билинейная функция $j(\omega, \omega')$

Пусть ω и ω' — два дифференциала поля R и $\mathfrak{p}$ — точка поля R. Будем предполагать, что если $\mathfrak{p}$ является полюсом одного из дифференциалов ω или ω', то вычет другого дифференциала в этой точке равен 0. При этом условии паре (ω, ω') и точке $\mathfrak{p}$ мы сопоставим некоторое число $j_{\mathfrak{p}}(\omega, \omega')$.

Рассмотрим сначала случай, когда $\operatorname{res}_{\mathfrak{p}}\omega=0$. Тогда, как мы знаем, для любого целого m можно найти такой элемент $f\in R$, что $\nu_{\mathfrak{p}}(\omega-df)\geqslant m$ (теорема 14 § 8 гл. VI). Возьмем $f\in R$ так, чтобы $\nu_{\mathfrak{p}}(\omega-df)\geqslant-\nu_{\mathfrak{p}}(\omega')-1$, кроме того, если $\nu_{\mathfrak{p}}(\omega)\geqslant 0$, то потребуем дополнительно, чтобы $\nu_{\mathfrak{p}}(f)>0$ (ясно, что последнее условие всегда может быть удовлетворено). Утверждаем, что тогда число $\operatorname{res}_{\mathfrak{p}} f\omega'$ не зависит от выбора f. Действительно, пусть f' — любой другой элемент поля R, удовлетворяющий тем же условиям, что и f. Тогда $\nu_{\mathfrak{p}}(d(f'-f))\geqslant-\nu_{\mathfrak{p}}(\omega')-1$, а если $\nu_{\mathfrak{p}}(\omega)\geqslant 0$, то $\nu_{\mathfrak{p}}(f'-f)>0$. Положим $g=f'-f$; если $\nu_{\mathfrak{p}}(g)\neq 0$, то $\nu_{\mathfrak{p}}(dg)=\nu_{\mathfrak{p}}(g)-1$ (лемма 1 § 8 гл. VI), откуда $\nu_{\mathfrak{p}}(g\omega')\geqslant 0$ и значит, $\operatorname{res}_{\mathfrak{p}} g\omega'=0$. Если же $\nu_{\mathfrak{p}}(g)=0$, то $\nu_{\mathfrak{p}}(dg)=$ $=\nu_{\mathfrak{p}}(g-g(\mathfrak{p}))-1$ и $\operatorname{res}_{\mathfrak{p}}((g-g(\mathfrak{p}))\omega')=0$, откуда $\operatorname{res}_{\mathfrak{p}} g\omega'=g(\mathfrak{p})\operatorname{res}_{\mathfrak{p}}\omega'$; если $\operatorname{res}_{\mathfrak{p}}\omega'\neq 0$, то $\nu_{\mathfrak{p}}(\omega)\geqslant 0$ и $g(\mathfrak{p})=0$. Таким образом, в обоих случаях $\operatorname{res}_{\mathfrak{p}} g\omega'=0$, и наше утверждение доказано. Полагаем теперь (если $\operatorname{res}_{\mathfrak{p}}\omega=0$): $j_{\mathfrak{p}}(\omega,\omega')=\operatorname{res}_{\mathfrak{p}} f\omega'$. Заметим, что для случая $\nu_{\mathfrak{p}}(\omega)\geqslant 0$ и $\operatorname{res}_{\mathfrak{p}}\omega'=0$ условие $\nu_{\mathfrak{p}}(f)>0$ не является необходимым.

Докажем теперь, что если $\operatorname{res}_{\mathfrak{p}}\omega=\operatorname{res}_{\mathfrak{p}}\omega'=0$, то имеет место равенство

$$j_{\mathfrak{p}}(\omega',\omega)=-j_{\mathfrak{p}}(\omega,\omega').$$

Выберем элементы f и f' в поле R так, чтобы $\nu_{\mathfrak{p}}(\omega-df)\geqslant$ $\geqslant\max\{-\nu_{\mathfrak{p}}(\omega')-1,\ \nu_{\mathfrak{p}}(\omega)+1\}$ и $\nu_{\mathfrak{p}}(\omega'-df')\geqslant$ $\geqslant\max\{-\nu_{\mathfrak{p}}(\omega)-1,\ \nu_{\mathfrak{p}}(\omega')+1\}$. Тогда $j_{\mathfrak{p}}(\omega,\omega')=\operatorname{res}_{\mathfrak{p}} f\omega'=$ $=\operatorname{res}_{\mathfrak{p}} f\,df'+\operatorname{res}_{\mathfrak{p}} f(\omega'-df')$. Так как $\nu_{\mathfrak{p}}(\omega-df)\geqslant\nu_{\mathfrak{p}}(\omega)+1$, то $\nu_{\mathfrak{p}}(df)=\nu_{\mathfrak{p}}(\omega)$. Если $\nu_{\mathfrak{p}}(\omega)<0$, то $\nu_{\mathfrak{p}}(f)=\nu_{\mathfrak{p}}(\omega)+1$, откуда $\nu_{\mathfrak{p}}(f(\omega'-df'))\geqslant 0$ и $\operatorname{res}_{\mathfrak{p}} f(\omega'-df')=0$. Если же $\nu_{\mathfrak{p}}(\omega)\geqslant 0$, то $\nu_{\mathfrak{p}}(f)\geqslant 0$ и $\nu_{\mathfrak{p}}(\omega'-df')\geqslant-1$; но $\operatorname{res}_{\mathfrak{p}}(\omega'-$ $-df')=0$, поэтому, в силу теоремы 2 § 5 гл. III, $\nu_{\mathfrak{p}}(\omega'-df')\geqslant 0$, откуда $\operatorname{res}_{\mathfrak{p}} f(\omega'-df')=0$. Таким образом, в любом случае мы имеем $j_{\mathfrak{p}}(\omega,\omega')=\operatorname{res}_{\mathfrak{p}} f\,df'$. Аналогично $j_{\mathfrak{p}}(\omega',\omega)=\operatorname{res}_{\mathfrak{p}} f'df$. Сумма $j_{\mathfrak{p}}(\omega,\omega')+j_{\mathfrak{p}}(\omega',\omega)$ равна теперь

$$\operatorname{res}_{\mathfrak{p}}(f\,df'+f'\,df)=\operatorname{res}_{\mathfrak{p}} d(ff')=0,$$

и наша формула доказана.

В случае когда $\operatorname{res}_{\mathfrak{p}}\omega\neq 0$ (а значит, $\nu_{\mathfrak{p}}(\omega')\geqslant 0$), число $j_{\mathfrak{p}}(\omega,\omega')$ естественно теперь определить формулой $j_{\mathfrak{p}}(\omega,\omega')=$ $=-j_{\mathfrak{p}}(\omega',\omega)$.

Ясно, что $j_{\mathfrak{p}}(\omega, \omega') = 0$, если только $\mathfrak{p}$ не является полюсом ни ω ни ω'. Далее, если $f \in R$, то $j_{\mathfrak{p}}(df, \omega') = \operatorname{res}_{\mathfrak{p}} f\omega'$, если $\operatorname{res}_{\mathfrak{p}} \omega' = 0$, и $j_{\mathfrak{p}}(df, \omega') = \operatorname{res}_{\mathfrak{p}} f\omega' - f(\mathfrak{p}) \operatorname{res}_{\mathfrak{p}} \omega'$, если $\operatorname{res}_{\mathfrak{p}} \omega' \neq 0$ (и значит $\nu_{\mathfrak{p}}(f) \geqslant 0$).

Пусть теперь ω и ω' — дифференциалы поля R. Предположим, что вычеты каждого из этих дифференциалов в полюсах другого равны 0. Тогда для всех точек $\mathfrak{p}$ поля R определено число $j_{\mathfrak{p}}(\omega, \omega')$, и это число отлично от 0 только для конечного числа точек $\mathfrak{p}$. Поэтому мы можем определить число $j(\omega, \omega')$, полагая $j(\omega, \omega') = \sum_{\mathfrak{p}} j_{\mathfrak{p}}(\omega, \omega')$, где суммирование распространено по всем точкам поля R. Отметим следующие очевидные свойства функции $j(\omega, \omega')$.

1) Если число $j(\omega, \omega')$ определено, то $j(\omega', \omega)$ также определено и имеет место равенство $j(\omega', \omega) = -j(\omega, \omega')$.

2) Пусть ω' — фиксированный дифференциал поля R. Обозначим через P множество всех его полюсов, а через P' — множество тех полюсов дифференциала ω', в которых его вычеты отличны от 0. Дифференциалы ω, не имеющие полюсов в P' и вычеты которых во всех точках множества P равны 0, образуют векторное пространство над полем комплексных чисел. Отображение $\omega \to j(\omega, \omega')$ является линейной функцией на этом пространстве.

3) Если элемент $f \in R$ таков, что число $j(df, \omega')$ определено, то

$$j(df, \omega') = -\sum_{\mathfrak{p}} f(\mathfrak{p}) \operatorname{res}_{\mathfrak{p}} \omega',$$

где суммирование ведется по всем точкам $\mathfrak{p}$, отличным от полюсов элемента f (это непосредственно следует из того, что $\sum_{\mathfrak{p}} \operatorname{res}_{\mathfrak{p}} f\omega' = 0$; см. теорему 3 § 5 гл. III).

Введем следующие обозначения:

$\mathfrak{E}$ — пространство дифференциалов второго рода поля R;

$\mathfrak{J}$ — пространство точных дифференциалов поля R;

P и Q — два конечных непересекающихся множества точек поля R;

$\mathfrak{E}_{P,Q}$ — множество дифференциалов поля R, не имеющих полюсов в Q и вычеты которых во всех точках вне P равны 0;

$\mathfrak{F}_Q$ — множество точных дифференциалов, соответствующих тем элементам поля R, для которых все точки из Q являются нулями.

Ясно, что для любых $\omega \in \mathfrak{E}_{P,Q}$ и $\omega' \in \mathfrak{E}_{Q,P}$ функция $j(\omega, \omega')$ имеет смысл; нашей ближайшей целью является изучение свойств этой функции.

Рассмотрим сначала случай, когда P и Q — пустые множества; в этом случае $\mathfrak{E}_{P,Q} = \mathfrak{E}_{Q,P} = \mathfrak{E}$, $\mathfrak{F}_P = \mathfrak{F}_Q = \mathfrak{F}$. Если $\omega \in \mathfrak{E}$, то, очевидно, $j(\omega, \omega') = 0$ при любом $\omega' \in \mathfrak{F}$. Утверждаем, что и обратно, если дифференциал ω' из $\mathfrak{E}$ таков, что $j(\omega, \omega') = 0$ при всех $\omega \in \mathfrak{E}$, то $\omega' \in \mathfrak{F}$. Пусть g — род поля R. Тогда мы можем найти g различных точек $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ таких, что дивизор $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_g$ неспециален (лемма 4 § 8 гл. VI). В силу леммы 3 § 8 гл. VI дифференциал ω' сравним по модулю $\mathfrak{F}$ с дифференциалом, делящимся на $\mathfrak{a}^{-2}$; не нарушая общности, мы можем, следовательно, считать, что ω' сам делится на $\mathfrak{a}^{-2}$. Докажем, что тогда $\omega' = 0$. Пусть ω — произвольный дифференциал второго рода, делящийся на $\mathfrak{a}^{-2}$. Пользуясь обозначениями теоремы 16 § 8 гл. VI, положим, что $a_i(\omega)$ и $b_i(\omega)$ — числа, для которых $\nu_{\mathfrak{p}_i}(\omega - (a_i(\omega) x_i^{-2} + b_i(\omega))\, dx_i) > 0$ $(1 \leqslant i \leqslant g)$. Тогда будем иметь

$$\nu_{\mathfrak{p}_i}(\omega + d(a_i(\omega) x_i^{-1} - b_i(\omega) x_i)) \geqslant 1 \geqslant -\nu_{\mathfrak{p}_i}(\omega') - 1,$$

и, следовательно, $j_{\mathfrak{p}_i}(\omega, \omega')$ равно

$$\operatorname{res}_{\mathfrak{p}_i}(-a_i(\omega) x_i^{-1} + b_i(\omega) x_i)\, \omega' = b_i(\omega) a_i(\omega') - b_i(\omega') a_i(\omega).$$

Таким образом, для любого $\omega \in \mathfrak{E}$, делящегося на $\mathfrak{a}^{-2}$, имеем $0 = j(\omega, \omega') = \sum_{i=1}^{g} (b_i(\omega) a_i(\omega') - b_i(\omega') a_i(\omega))$. В силу теоремы 16 § 8 гл. VI, отсюда легко следует, что $a_i(\omega') = b_i(\omega') = 0$ и, значит, $\omega' = 0$.

Перейдем теперь к общему случаю. Если $\omega \in \mathfrak{E}_{P,Q}$ и если f — элемент поля R, не имеющий полюсов среди точек множества P, то $j(\omega, df) = \sum_{\mathfrak{p} \in P} f(\mathfrak{p}) \operatorname{res}_{\mathfrak{p}} \omega$; если $df \in \mathfrak{F}_P$, то последнее число равно 0. Обратно, пусть ω' — элемент из $\mathfrak{E}_{Q,P}$, такой, что $j(\omega, \omega') = 0$ при всех $\omega \in \mathfrak{E}_{P,Q}$. Возьмем сначала $\omega = dg$, где g — элемент поля R, не имеющий по-

люсов среди точек множества Q. Тогда $0 = j(dg, \omega') = -\sum_{\mathfrak{q} \in Q} g(\mathfrak{q}) \operatorname{res}_{\mathfrak{q}} \omega'$. Но, как мы знаем, в поле R существует элемент g, принимающий произвольные наперед заданные значения во всех точках множества Q; отсюда следует, что $\operatorname{res}_{\mathfrak{q}} \omega' = 0$ при всех $\mathfrak{q} \in Q$, то есть $\omega' \in \mathfrak{E}$. Для произвольного дифференциала ω второго рода в поле R существует такой элемент h, что дифференциал $\omega - dh$ не имеет полюсов в Q (это легко следует, например, из леммы 3 § 8 гл. VI и леммы 4 § 8 гл. VI). Значение $j(\omega, \omega')$ определено и равно $j(dh, \omega') + j(\omega - dh, \omega') = 0$ (первое слагаемое равно 0, так как $dh \in \mathfrak{F}$ и $\omega' \in \mathfrak{E}$, а второе — так как $\omega - dh \in \mathfrak{E}_{P,Q}$). В силу доказанного выше получаем, что $\omega' \in \mathfrak{F}$; таким образом, $\omega' = df$, где f — элемент поля R, не имеющий полюсов на P. Если теперь $\omega \in \mathfrak{E}_{P,Q}$, то $0 = j(\omega, \omega') = \sum_{\mathfrak{p} \in P} f(\mathfrak{p}) \operatorname{res}_{\mathfrak{p}} \omega$. Применяя теорему 4 § 5 гл. III, получаем, что

$$\sum_{\mathfrak{p} \in P} f(\mathfrak{p}) \rho(\mathfrak{p}) = 0$$

для любых чисел $\rho(\mathfrak{p})$ $(\mathfrak{p} \in P)$, удовлетворяющих условию $\sum_{\mathfrak{p} \in P} \rho(\mathfrak{p}) = 0$. Отсюда следует, что числа $f(\mathfrak{p})$ все равны друг другу; если f_0 — их общее значение, то $\omega' = d(f - f_0) \in \mathfrak{F}_P$.

Функция j естественным образом определяет билинейную функцию на произведении $(\mathfrak{E}_{P,Q}/\mathfrak{F}_Q) \times (\mathfrak{E}_{Q,P}/\mathfrak{F}_P)$; из только что доказанного следует, что эта билинейная функция невырождена. Используя свойства невырожденных билинейных функций, получаем следующий результат:

Теорема 8. *Пусть P и Q — два конечных непересекающихся подмножества римановой поверхности поля R. Пусть λ есть линейная функция на пространстве тех дифференциалов поля R, которые не имеют полюсов в множестве Q и вычеты которых во всех точках вне P равны 0. Предположим, что $\lambda(df) = 0$ при любом элементе $f \in R$, для которого все точки из Q являются нулями. Тогда существует дифференциал ω' поля R, не имеющий полюсов в множестве P и вычеты которого во всех точках вне Q равны 0, такой, что $\lambda(\omega) = j(\omega, \omega')$ для всех ω из области определения λ. Класс смежности*

дифференциала ω' по подпространству точных дифференциалов, соответствующих тем элементам поля R, для которых все точки из P являются нулями, определен однозначно.

§ 6. Определение индексов пересечения

Пусть P и Q — два конечных непересекающихся подмножества римановой поверхности S поля R, и пусть $\mathfrak{E}_{P,Q}$ — пространство дифференциалов, определенное в § 5. Для каждого элемента $c \in H_1(S \setminus P, Q)$ и для каждого дифференциала $\omega \in \mathfrak{E}_{P,Q}$ определен интеграл $\int\limits_c \omega$, и отображение $\omega \to \int\limits_c \omega$ является линейной функцией на $\mathfrak{E}_{P,Q}$. Положим $\partial c = \sum\limits_{\mathfrak{q} \in Q} a(\mathfrak{q})\,\mathfrak{q}$; если элемент $f \in R$ не имеет полюсов на Q, то $\int\limits_c df = \sum\limits_{\mathfrak{q} \in Q} a(\mathfrak{q}) f(\mathfrak{q})$ (лемма 2 § 4). Последнее число равно 0, если только все точки из Q являются нулями элемента f. В силу теоремы 8 § 5 в пространстве $\mathfrak{E}_{Q,P}$ существует такой дифференциал ω_c, что

$$\int\limits_c \omega = j(\omega_c, \omega)$$

при всех $\omega \in \mathfrak{E}_{P,Q}$. Кроме того, если пространство $\mathfrak{F}_P$ определено так же, как и в § 5, то класс смежности дифференциала ω_c по модулю $\mathfrak{F}_P$ определен однозначно; обозначим этот класс смежности через $\Omega(c)$.

Пусть теперь Ω — произвольный класс смежности пространства всех дифференциалов по модулю $\mathfrak{F}_P$. Очевидно, что тогда для любой точки $\mathfrak{p}$ все дифференциалы, принадлежащие классу Ω, имеют в $\mathfrak{p}$ один и тот же вычет. Это число будем называть *вычетом класса Ω в точке $\mathfrak{p}$* и обозначать через $\operatorname{res}_{\mathfrak{p}} \Omega$. Найдем вычеты класса $\Omega(c)$, введенного выше. Так как $\omega_c \in \mathfrak{E}_{Q,P}$, то вычеты класса $\Omega(c)$ во всех точках вне Q равны 0. Если элемент $f \in R$ не имеет полю-

сов на множестве Q, то

$$\sum_{\mathfrak{q}\in Q} a(\mathfrak{q}) f(\mathfrak{q}) = \int_c df = j(\omega_c, df) = \sum_{\mathfrak{q}\in Q} (\operatorname{res}_{\mathfrak{q}} \omega_c) f(\mathfrak{q}).$$

Так как в поле R существует элемент f, принимающий любые наперед заданные значения во всех точках множества Q, то получаем, что $\operatorname{res}_{\mathfrak{q}} \Omega(c) = a(\mathfrak{q})$. Таким образом, доказана

Теорема 9. *Пусть P и Q — два конечных непересекающихся множества точек поля R, и пусть c — элемент группы $H_1(S \setminus P, Q)$. Пусть, далее, пространства $\mathfrak{E}_{P,Q}$ и $\mathfrak{F}_P$ определены так же, как и в § 5. Тогда существует однозначно определенный класс смежности $\Omega(c)$ пространства $\mathfrak{E}_{Q,P}$ по подпространству $\mathfrak{F}_P$, такой, что для любого $\omega_c \in \Omega(c)$ и любого $\omega \in \mathfrak{E}_{P,Q}$ имеет место равенство $\int_c \omega = j(\omega_c, \omega)$. Если $\mathfrak{q} \in Q$, то вычет каждого дифференциала из класса $\Omega(c)$ в точке $\mathfrak{q}$ равен коэффициенту при $\mathfrak{q}$ в цепи dc.*

Отсюда непосредственно следует, что логарифмические периоды любого дифференциала из класса $\Omega(c)$ являются целыми кратными числа $2\pi i$.

Отображение $c \to \Omega(c)$ есть, очевидно, гомоморфизм группы $H_1(S \setminus P, Q)$ в аддитивную группу фактор-пространства $\mathfrak{E}_{Q,P}/\mathfrak{F}_P$. Далее, пусть P_1 и Q_1 — конечные непересекающиеся подмножества поверхности S, такие, что $Q \subset Q_1$ и $P \supset P_1$, и пусть c_1 — элемент группы $H_1(S \setminus P_1, Q_1)$, соответствующий элементу $c \in H_1(S \setminus P, Q)$ при тождественном отображении пары $(S \setminus P, Q)$ в $(S \setminus P_1, Q_1)$; тогда $\mathfrak{F}_P \subset \mathfrak{F}_{P_1}$ и, как легко видеть, $\Omega(c_1)$ является смежным классом по модулю $\mathfrak{F}_{P_1}$, содержащим $\Omega(c)$.

Для любого конечного подмножества P поверхности S и 1-цепи γ на $S \setminus P$ положим

$$\Omega(\gamma, P) = \Omega(c),$$

где c — элемент из $H_1(S \setminus P, |\partial\gamma|)$ с представителем γ. Тогда при фиксированном P отображение $\gamma \to \Omega(\gamma, P)$ является, как легко видеть, гомоморфизмом группы 1-цепей на $S \setminus P$

в $\mathfrak{D}/\mathfrak{F}_P$, где $\mathfrak{D}$ — пространство всех дифференциалов. Кроме того, $\mathfrak{Q}(\operatorname{subd}\gamma, P) = \mathfrak{Q}(\gamma, P)$.

Пусть $\mathfrak{Q}$ — произвольный класс смежности пространства дифференциалов по модулю $\mathfrak{F}_P$; если элементы из $\mathfrak{Q}$ принадлежат пространству $\mathfrak{E}_{Q,P}$ (где Q — конечное множество, не имеющее общих точек с P), то для каждого $c' \in H_1(S \setminus Q, P)$ и для каждого $\omega \in \mathfrak{Q}$ определен интеграл $\int\limits_{c'} \omega$, значение которого зависит только от c' и $\mathfrak{Q}$. Действительно, если f — элемент поля R, имеющий нули во всех точках множества P, то, по лемме 2 § 4, $\int\limits_{c'} df = 0$. Число $\int\limits_{c'} \omega$ называется *интегралом от класса смежности* $\mathfrak{Q}$ *по* c' и обозначается через $\int\limits_{c'} \mathfrak{Q}$.

Если теперь c и c' — произвольные элементы из групп $H_1(S \setminus P, Q)$ и $H_1(S \setminus Q, P)$ соответственно, то имеет смысл интеграл $\int\limits_{c} \mathfrak{Q}(c')$. Число

$$\iota(c, c') = \frac{1}{2\pi i} \int\limits_{c} \mathfrak{Q}(c')$$

называется *индексом пересечения классов гомологий* c *и* c'.

Теорема 10. *Пусть P и Q — конечные непересекающиеся подмножества римановой поверхности S поля R, а c и c' — элементы групп $H_1(S \setminus P, Q)$ и $H_1(S \setminus Q, P)$ соответственно. Тогда индекс пересечения $\iota(c, c')$ есть целое число, причем $\iota(c', c) = -\iota(c, c')$. Если классы гомологий c и c' могут быть представлены такими 1-цепями γ и γ' соответственно, что $|\gamma| \cap |\gamma'| = \varnothing$, то $\iota(c, c') = 0$.*

Пусть ω и ω' — дифференциалы, принадлежащие классам смежности $\mathfrak{Q}(c)$ и $\mathfrak{Q}(c')$ соответственно. Тогда $\int\limits_{c} \mathfrak{Q}(c') = j(\omega, \omega')$, откуда $\iota(c, c') = \frac{1}{2\pi i} j(\omega, \omega')$. Этим доказана формула $\iota(c, c') = -\iota(c', c)$.

Пусть γ и γ' — произвольные 1-цепи на S, удовлетворяющие условиям

$$|\gamma| \cap |\partial\gamma'| = \varnothing, \quad |\gamma'| \cap |\partial\gamma| = \varnothing. \tag{1}$$

Обозначим тогда через $\iota(\gamma, \gamma')$ число $\iota(c, c')$, где c — класс гомологий цепи γ в группе $H_1(S \setminus |\partial\gamma'|, |\partial\gamma|)$, а c' — класс гомологий цепи γ' в группе $H_1(S \setminus |\partial\gamma|, |\partial\gamma'|)$. Ясно, что тогда $\iota(\gamma', \gamma) = -\iota(\gamma, \gamma')$ и $\iota(\operatorname{subd}\gamma, \gamma') = \iota(\gamma, \gamma')$. Кроме того, при фиксированной цепи γ' отображение $\gamma \to \iota(\gamma, \gamma')$ является, как легко видеть, гомоморфизмом аддитивной группы 1-цепей, удовлетворяющих условиям (1), в аддитивную группу комплексных чисел.

Рассмотрим сначала случай, когда γ и γ' являются 1-симплексами, лежащими в непересекающихся открытых кругах V и V' соответственно. Докажем, что при этих условиях $\iota(\gamma, \gamma') = 0$. Мы можем, разумеется, считать, что $S \setminus (V \cup V')$ содержит бесконечно много точек. Положим $\partial\gamma = \mathfrak{b} - \mathfrak{a}$ и $\partial\gamma' = \mathfrak{b}' - \mathfrak{a}'$ (где $\mathfrak{a}, \mathfrak{b} \in V$ и $\mathfrak{a}', \mathfrak{b}' \in V'$). В поле R мы можем найти элементы x и x', такие, что V будет x-кругом, а V' — x'-кругом, и, кроме того, $x(\mathfrak{a}) = x'(\mathfrak{a}') = 0$. Если $\xi \in x(V)$, то через $\mathfrak{p}(\xi)$ мы обозначим ту точку из V, которая элементом x отображается на ξ; построим на V 1-симплекс γ_ξ, для которого $\partial\gamma_\xi = \mathfrak{p}(\xi) - \mathfrak{a}$. Так как $H_1(V) = 0$, а точки $\mathfrak{a}'$ и $\mathfrak{b}'$ не принадлежат V, то, очевидно, все симплексы γ_ξ, удовлетворяющие нашим условиям, представляют один и тот же элемент группы $H_1(S \setminus \{\mathfrak{a}', \mathfrak{b}'\}, \{\mathfrak{a}, \mathfrak{p}(\xi)\})$; следовательно, класс дифференциалов $\Omega(\gamma_\xi, \{\mathfrak{a}', \mathfrak{b}'\})$ зависит только от ξ. Обозначим этот класс через Ω_ξ. Ясно, что тогда число $\iota(\gamma_\xi, \gamma') = -\iota(\gamma', \gamma_\xi)$ равно произведению $-\frac{1}{2\pi i}$ на интеграл от любого дифференциала из класса Ω_ξ по γ'.

Пусть g — род поля R; на множестве $S \setminus (V \cup V')$ мы можем найти g различных точек $\mathfrak{r}_1, \ldots, \mathfrak{r}_g$, таких, что дивизор $\mathfrak{v}_0 = \mathfrak{r}_1 \ldots \mathfrak{r}_g$ неспециален (лемма 4 § 8 гл. VI). По теореме Римана — Роха $l(\mathfrak{v}_0^{-1}) = g - g + 1 + \delta(\mathfrak{v}_0) = 1$ (так как $\mathfrak{v}_0$ неспециален) и $l(\mathfrak{a}'\mathfrak{b}'\mathfrak{v}_0^{-1}) = g - 2 - g + 1 + \delta(\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}_0) = -1 + \delta(\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}_0)$. Из первой формулы следует, что среди элементов поля R только константы делятся на $\mathfrak{v}_0^{-1}$, а значит, $l(\mathfrak{a}'\mathfrak{b}'\mathfrak{v}_0^{-1}) = 0$; из второй формулы

следует тогда, что $\delta(\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}_0)=1$. Пусть ζ_0 — базисный элемент пространства дифференциалов, делящихся на $\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}_0$, и пусть $\mathfrak{r}_0$ — точка из $S\setminus(V\cup V')$, не являющаяся нулем дифференциала ζ_0. Положим $\mathfrak{v}=\mathfrak{r}_0\mathfrak{v}_0$. Утверждаем теперь, что в классе Ω_ξ существует дифференциал ω_ξ, делящийся на $\mathfrak{v}^{-2}\mathfrak{a}^{-1}(\mathfrak{p}(\xi))^{-1}$, и что этот дифференциал определен однозначно, если только $\xi\neq 0$. Пусть ω_ξ^* — произвольный дифференциал из класса Ω_ξ. Для каждой точки $\mathfrak{p}$ поля R мы можем найти такой элемент $f_\mathfrak{p}\in R$, что $\nu_\mathfrak{p}(\omega_\xi^*-df_\mathfrak{p})\geqslant -1$ (теорема 14 § 8 гл. VI). Покажем, что в поле R существует элемент f, удовлетворяющий следующим условиям: 1) если точка $\mathfrak{p}$ отлична от $\mathfrak{a}'$, $\mathfrak{b}'$, $\mathfrak{r}_0$, $\mathfrak{r}_1$, ..., $\mathfrak{r}_g$, то $\nu_\mathfrak{p}(f-f_\mathfrak{p})\geqslant 0$; 2) числа $\nu_{a'}(f)$ и $\nu_{b'}(f)$ положительны; 3) $\nu_{\mathfrak{r}_j}(f-f_{\mathfrak{r}_j})\geqslant -1$ $(0\leqslant j\leqslant g)$. Действительно, в силу теоремы 2 § 5 гл. II, нам достаточно убедиться в том, что в R нет отличного от 0 дифференциала, который делился бы на $\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}$. Если бы такой дифференциал существовал, то он имел бы точку $\mathfrak{r}_0$ в качестве нуля и делился бы на $\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}_0$, а значит, имел бы вид $\lambda\zeta_0$, где λ — константа; но это невозможно, ибо $\mathfrak{r}_0$ не является нулем дифференциала ζ_0. Этим и доказано существование элемента $f\in R$, удовлетворяющего нашим условиям. Так как точки $\mathfrak{a}'$ и $\mathfrak{b}'$ являются нулями элемента f, то дифференциал $\omega_\xi^*-df=\omega_\xi$ принадлежит классу Ω_ξ. Для любой точки $\mathfrak{p}$, отличной от $\mathfrak{r}_0$, $\mathfrak{r}_1$, ..., $\mathfrak{r}_g$, имеем $\nu_\mathfrak{p}(\omega_\xi)\geqslant -1$ (ибо $\mathfrak{a}'$ и $\mathfrak{b}'$ не являются полюсами дифференциала ω_ξ^*); с другой стороны, $\nu_{\mathfrak{r}_j}(\omega_\xi)\geqslant -2$. Если $\mathfrak{p}$ — точка, отличная от точек $\mathfrak{a}$, $\mathfrak{p}(\xi)$, $\mathfrak{r}_0$, ..., $\mathfrak{r}_g$, то вычет дифференциала ω_ξ в точке $\mathfrak{p}$ равен 0 (ибо $\omega_\xi\in\Omega_\xi$), поэтому из неравенства $\nu_\mathfrak{p}(\omega_\xi)\geqslant -1$ следует, что $\nu_\mathfrak{p}(\omega_\xi)\geqslant 0$. Этим доказано, что дифференциал ω_ξ делится на $\mathfrak{v}^{-2}\mathfrak{a}^{-1}(\mathfrak{p}(\xi))^{-1}$. Если ω_ξ' — любой другой дифференциал из класса Ω_ξ, делящийся на $\mathfrak{v}^{-2}\mathfrak{a}^{-1}(\mathfrak{p}(\xi))^{-1}$, то $\omega_\xi'-\omega_\xi$ имеет вид $d\varphi$, где φ — элемент поля R, имеющий точки $\mathfrak{a}'$ и $\mathfrak{b}'$ в качестве своих нулей. Если $\xi\neq 0$, т. е. $\mathfrak{p}(\xi)\neq\mathfrak{a}$, то точки $\mathfrak{a}$ и $\mathfrak{p}(\xi)$, являясь полюсами дифференциала $\omega_\xi'-\omega_\xi$ порядка $\leqslant 1$, не могут быть полюсами дифференциала $d\varphi$, откуда следует, что φ делится на $\mathfrak{a}'\mathfrak{b}'\mathfrak{v}^{-1}$ (в этом рассуждении предпола-

гается, что $\mathfrak{a}' \neq \mathfrak{b}'$; если $\mathfrak{a}' = \mathfrak{b}'$, то γ' есть цикл, гомологичный нулю на V', и равенство $\iota(\gamma, \gamma') = 0$ очевидно). Имеем теперь $l(\mathfrak{a}'\mathfrak{b}'\mathfrak{v}^{-1}) = g - 1 - g + 1 + \delta(\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}) = 0$, откуда $\varphi = 0$, и наше утверждение доказано. Класс Ω_0 содержит, очевидно, нулевой дифференциал; положим $\omega_0 = 0$.

Вычислим теперь значение элемента $\frac{\omega_\xi}{dx'}$ поля R в точке $\mathfrak{q}' \in V'$, отличной от $\mathfrak{a}'$ и $\mathfrak{b}'$. Ясно, что $l(\mathfrak{q}'\mathfrak{a}'\mathfrak{b}'\mathfrak{v}^{-1}) = l(\mathfrak{q}'^2\mathfrak{a}'\mathfrak{b}'\mathfrak{v}^{-1}) = 0$, откуда, по теореме Римана — Роха, $\delta(\mathfrak{q}'^{-1}\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}) = 1$ и $\delta(\mathfrak{q}'^{-2}\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}) = 2$.

Пусть $\zeta_{\mathfrak{q}'}$ — отличный от 0 дифференциал, делящийся на $\mathfrak{q}'^{-1}\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}$; так как

$$\delta(\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}) = 0,$$

то $\mathfrak{q}'$ является полюсом дифференциала $\zeta_{\mathfrak{q}'}$ порядка 1, а значит, $\operatorname{res}_{\mathfrak{q}'}\zeta_{\mathfrak{q}'} \neq 0$. Умножив $\zeta_{\mathfrak{q}'}$ на подходящую константу, мы можем считать, что $\operatorname{res}_{\mathfrak{q}'}\zeta_{\mathfrak{q}'} = 1$. Возьмем произвольно дифференциал, делящийся на $\mathfrak{q}'^{-2}\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{v}$ и линейно независимый с $\zeta_{\mathfrak{q}'}$; вычитая из него подходящее произведение $\zeta_{\mathfrak{q}'}$ на константу, мы получим дифференциал $\bar{\eta}_{\mathfrak{q}'}$, делящийся на $\mathfrak{q}'^{-2}\mathfrak{a}'^{-1}\mathfrak{b}'^{-1}\mathfrak{b}$, вычет которого в полюсе $\mathfrak{q}'$ (порядка 2) будет равен $\dot{0}$. Умножив дифференциал $\bar{\eta}_{\mathfrak{q}'}$ на подходящую константу, мы получим дифференциал $\eta_{\mathfrak{q}'}$, для которого $\nu_{\mathfrak{q}'}(\eta_{\mathfrak{q}'} - (x' - x'(\mathfrak{q}'))^{-2}dx') \geqslant 0$. По определению класса Ω_ξ мы имеем

$$j(\omega_\xi, \eta_{\mathfrak{q}'}) = \int_{\gamma_\xi} \eta_{\mathfrak{q}'}.$$

Докажем теперь следующую лемму:

Лемма 1. *Пусть* ω *и* ω' — *дифференциалы поля* R *и* $\mathfrak{r}$ — *точка поля* R. *Если* $\nu_{\mathfrak{r}}(\omega) + \nu_{\mathfrak{r}}(\omega') \geqslant -1$, *то число* $j_{\mathfrak{r}}(\omega, \omega')$ *имеет смысл и равно* 0.

Ясно, что $\mathfrak{r}$ не может быть полюсом обоих дифференциалов ω и ω'; следовательно, число $j_{\mathfrak{r}}(\omega, \omega')$ определено. Так как $j_{\mathfrak{r}}(\omega, \omega') = -j_{\mathfrak{r}}(\omega', \omega)$, то можно предполагать, что $\nu_{\mathfrak{r}}(\omega) \geqslant 0$. Пусть y есть такой элемент поля R, что $\nu_{\mathfrak{r}}(\omega - dy) \geqslant -\nu_{\mathfrak{r}}(\omega') - 1$ и $\nu_{\mathfrak{r}}(y) > 0$. Тогда $\nu_{\mathfrak{r}}(y) = \nu_{\mathfrak{r}}(dy) + 1$ (лемма 1 § 8 гл. VI) и $\nu_{\mathfrak{r}}(dy) \geqslant$

$\geqslant \min\{\nu_{\mathfrak{r}}(\omega), \nu_{\mathfrak{r}}(\omega - dy)\} \geqslant -\nu_{\mathfrak{r}}(\omega') - 1$, откуда $\nu_{\mathfrak{r}}(y\omega') \geqslant 0$, а значит, $j_{\mathfrak{r}}(\omega, \omega') = \operatorname{res}_{\mathfrak{r}} y\omega' = 0$.

Из леммы 1 следует, что $\mathfrak{q}'$ является единственной точкой $\mathfrak{p}$, для которой $j_{\mathfrak{p}}(\omega_\xi, \eta_{\mathfrak{q}'})$ может быть отлично от 0. Так как $\nu_{\mathfrak{q}'}(\eta_{\mathfrak{q}'} + d((x' - x'(\mathfrak{q}'))^{-1})) \geqslant 0$ и $j(\omega_\xi, \eta_{\mathfrak{q}'}) = -j(\eta_{\mathfrak{q}'}, \omega_\xi)$, то, в силу следствия к теореме 6 § 3 гл. VI, имеем

$$j(\omega_\xi, \eta_{\mathfrak{q}'}) = \operatorname{res}_{\mathfrak{q}'} \frac{\omega_\xi}{x' - x'(\mathfrak{q}')} = \frac{\omega_\xi}{dx'}(\mathfrak{q}').$$

Таким образом, получаем

$$\frac{\omega_\xi}{dx'}(\mathfrak{q}') = \int_{\gamma_\xi} \eta_{\mathfrak{q}'}.$$

Полученная формула показывает нам, что при фиксированной точке $\mathfrak{q}'$ значение $\frac{\omega_\xi}{dx'}(\mathfrak{q}')$, рассматриваемое как функция от $\mathfrak{p}(\xi)$, является первообразной функцией в круге V для дифференциала $\eta_{\mathfrak{q}'}$. Следовательно, $\frac{\omega_\xi}{dx'}(\mathfrak{q}')$ (для любой фиксированной точки $\mathfrak{q}'$) есть голоморфная функция от ξ в круге $x(V)$ и производная от нее равна

$$\frac{d}{d\xi}\left(\frac{\omega_\xi}{dx'}(\mathfrak{q}')\right) = \frac{\eta_{\mathfrak{q}'}}{dx}(\mathfrak{p}(\xi)).$$

Докажем теперь, что функцию $\frac{\omega_\xi}{dx'}(\mathfrak{q}')$ можно рассматривать как голоморфную функцию от пары $(\xi, x'(\mathfrak{q}')) \in x(V) \times x'(V')$. Для этого прежде всего заметим, что $v_\xi = \frac{\omega_\xi}{dx'}$ есть элемент поля R, дивизор полюсов которого имеет ограниченную степень; отсюда следует, что число точек $\mathfrak{q}' \in V'$, в которых v_ξ принимает любое заданное значение, ограничено независимо от ξ. Если $\mathfrak{q}'$ — произвольная точка из V', то функция $v_\xi(\mathfrak{q}')$, голоморфная в $x(V)$, ограничена, когда ξ принимает значения из любого замкнутого круга $D \subset x(V)$. Применяя теорему Монтеля (П. Монтель, „Нормальные семейства аналитических функций“, М. — Л., 1936, стр. 63

и 65), заключаем, что функции v_ξ, $\xi \in D$, образуют „нормальное семейство", т. е. относительно компактное множество голоморфных функций (по отношению к топологии равномерной сходимости) на каждом компактном подмножестве круга V'. Отсюда следует, что если последовательность $\xi_1, \ldots, \xi_n, \ldots$ точек из $x(V)$ сходится к точке $\xi \in x(V)$, то v_{ξ_n} сходится к v_ξ, равномерно на каждом компактном подмножестве круга V'. Этим доказано, что $v_\xi(\mathfrak{q}')$ есть непрерывная функция от пары

$$(\xi, x'(\mathfrak{q}')) \in x(V) \times x'(V').$$

Эта функция, будучи голоморфной функцией по каждому ее аргументу при фиксированном другом, является также и голоморфной функцией от пары $(\xi, x'(\mathfrak{q}'))$. Положим $v_\xi(\mathfrak{q}') = \theta(\xi, x'(\mathfrak{q}'))$. Пусть $\Theta(\xi, x')$ есть голоморфная функция от ξ и x', заданная условиями:

$$\frac{\partial\Theta}{\partial x'}(\xi, x') = \theta(\xi, x'), \qquad \Theta(\xi, 0) = 0.$$

Ясно, что тогда будем иметь

$$\int_{\gamma'} \omega_\xi = \Theta(\xi, x'(\mathfrak{b}')).$$

Нам надо доказать, что это число равно 0. Функция $\frac{\partial\Theta}{\partial\xi}$ при фиксированном ξ является первообразной функцией (относительно x') для $\frac{\partial\theta}{\partial\xi}(\xi, x')$, поэтому

$$\frac{\partial^2\Theta}{\partial\xi\,\partial x'}(\xi, x'(\mathfrak{q}')) = \frac{\eta_{\mathfrak{q}'}}{dx}(\mathfrak{p}(\xi)).$$

Вычислим последнее число другим способом. Степень дивизора $(\mathfrak{p}(\xi))^{-1}\mathfrak{a}'\mathfrak{b}'\mathfrak{v}^{-1}$ равна $-g$; в силу теоремы Римана — Роха в поле R существует элемент $u_\xi \neq 0$, делящийся на этот дивизор. Так как $l(\mathfrak{a}'\mathfrak{b}'\mathfrak{v}^{-1}) = 0$, то $\mathfrak{p}(\xi)$ является полюсом элемента u_ξ первого порядка; умножив u_ξ на подходящую константу, мы можем считать, что $(x - \xi)u_\xi$ в точке $\mathfrak{p}(\xi)$ принимает значение 1. Сумма вычетов дифференциала $u_\xi\eta_{\mathfrak{q}'}$ равна 0 (теорема 3 § 5 гл. III), при этом,

как легко видеть, только в точках $\mathfrak{p}(\xi)$ и $\mathfrak{q}'$ дифференциал $u_\xi \eta_{\mathfrak{q}'}$ может иметь вычеты, отличные от 0. Мы имеем

$$\operatorname{res}_{\mathfrak{p}(\xi)} u_\xi \eta_{\mathfrak{q}'} = \operatorname{res}_{\mathfrak{p}(\xi)} \frac{\eta_{\mathfrak{q}'}}{x-\xi} = \frac{\eta_{\mathfrak{q}'}}{dx}(\mathfrak{p}(\xi)).$$

Так как $\nu_{\mathfrak{q}'}\left(\eta_{\mathfrak{q}'} - (x' - x'(\mathfrak{q}'))^{-2} dx'\right) \geqslant 0$, то легко получаем, что

$$\operatorname{res}_{\mathfrak{q}'} u_\xi \eta_{\mathfrak{q}'} = \frac{du_\xi}{dx'}(\mathfrak{q}').$$

Таким образом, мы установили формулу

$$\frac{\partial^2 \Theta}{\partial \xi\, \partial x'}(\xi,\ x'(\mathfrak{q}')) = -\frac{du_\xi}{dx'}(\mathfrak{q}').$$

Эта формула доказана нами для случая, когда точка $\mathfrak{q}'$ отлична от $\mathfrak{a}'$ и $\mathfrak{b}'$; однако она справедлива также и для случая, когда $\mathfrak{q}'$ совпадает с $\mathfrak{a}'$ или $\mathfrak{b}'$, так как обе части равенства являются непрерывными функциями от $\mathfrak{q}'$. Имеем теперь $0 = u_\xi(\mathfrak{b}') - u_\xi(\mathfrak{a}') = \int\limits_{\gamma'} \left(\frac{du_\xi}{dx'}\right) dx'$, откуда

$$\frac{\partial}{\partial \xi}(\Theta(\xi,\ x'(\mathfrak{b}')) - \Theta(\xi,\ 0)) = \frac{\partial}{\partial \xi}(\Theta(\xi,\ x'(\mathfrak{b}'))) = 0.$$

Этим доказано, что $\int\limits_{\gamma'} \omega_\xi$ не зависит от ξ. Так как $\omega_0 = 0$, то $\int\limits_{\gamma'} \omega_\xi = 0$ при всех ξ, откуда вытекает, что $\iota(\gamma,\ \gamma') = 0$.

Предположим теперь, что γ и γ' — произвольные 1-цепи, удовлетворяющие условию $|\gamma| \cap |\gamma'| = \varnothing$. Так как множества $|\gamma|$ и $|\gamma'|$ замкнуты в компактном, а значит, и нормальном пространстве S, то существуют такие открытые множества U и U', что $|\gamma| \subset U$, $|\gamma'| \subset U'$ и $U \cap U' = \varnothing$. Множества U и U' могут быть покрыты содержащимися в них открытыми кругами; отсюда следует, что можно подобрать целое число $p \geqslant 0$ так, чтобы каждый симплекс, входящий в $\operatorname{subd}^p \gamma$, лежал в некотором открытом круге, содержащемся в U, и каждый симплекс, входящий в $\operatorname{subd}^p \gamma'$, лежал в некотором открытом круге, содержащемся в U'.

Пусть $\operatorname{subd}^p \gamma = \sum_{k=1}^{h} a_k \sigma_k$ и $\operatorname{subd}^p \gamma' = \sum_{l=1}^{h'} a'_l \sigma'_l$, где σ_k $(1 \leqslant k \leqslant h)$ и σ'_l $(1 \leqslant l \leqslant h')$ — симплексы, входящие в $\operatorname{subd}^p \gamma$ и $\operatorname{subd}^p \gamma'$ соответственно; тогда будем иметь

$$\iota(\gamma, \gamma') = \sum_{k=1}^{h} \sum_{l=1}^{h'} a_k a'_l \iota(\sigma_k, \sigma'_l) = 0.$$

Нам осталось доказать еще, что $\iota(\gamma, \gamma')$ есть целое число, если только это число определено. Каждая точка множества $|\gamma|$ является внутренней для некоторого замкнутого круга, не пересекающегося с $|\partial\gamma'|$; отсюда следует, что существует такое целое число $p \geqslant 0$, что каждый симплекс, входящий в $\operatorname{subd}^p \gamma$, лежит во внутренности некоторого замкнутого круга, не пересекающегося с $|\partial\gamma'|$. Положим $\operatorname{subd}^p \gamma = \sum_{k=1}^{h} a_k \sigma_k$, где $\sigma_1, \ldots, \sigma_h$ — симплексы, входящие в $\operatorname{subd}^p \gamma$. Множество $|\partial\sigma_1| \cup \ldots \cup |\partial\sigma_h|$ конечно и не пересекается с $|\partial\gamma'|$; следовательно, существует цепь γ'_1, которая гомологична цепи γ' на $S \setminus |\partial\gamma|$ по модулю $|\partial\gamma'|$ и которая лежит на $S \setminus \bigcup_{k=1}^{h} |\partial\sigma_k|$ (см. следствие к лемме 4 § 4). Имеем $\iota(\gamma, \gamma') = \iota(\gamma, \gamma'_1)$ и $\iota(\operatorname{subd}^p \gamma, \gamma'_1) = \sum_{k=1}^{h} a_k \iota(\sigma_k, \gamma'_1)$. Таким образом, нам достаточно доказать, что $\iota(\gamma, \gamma')$ есть целое число для случая, когда $|\gamma|$ содержится во внутренности замкнутого круга D, непересекающегося с $|\partial\gamma'|$. Пусть тогда ω — дифференциал из класса $\Omega(\gamma, |\partial\gamma'|)$. Мы имеем $\iota(\gamma, \gamma') = -\frac{1}{2\pi i} \int_{c'} \omega$, где c' — класс гомологий цепи γ' в $H_1(S \setminus |\partial\gamma|, |\partial\gamma'|)$. Пусть $\mathfrak{c}$ — внутренняя точка круга D; тогда c' содержит цепь γ'_2 на $S \setminus (|\partial\gamma| \cup \{\mathfrak{c}\})$ (следствие к лемме 4 § 4). С другой стороны, ясно, что если V есть внутренность круга D, то $S \setminus V$ является деформационным ретрактом множества $S \setminus \{\mathfrak{c}\}$. Отсюда следует, что класс гомологий c'^* цепи γ'_2 в $H_1(S, |\partial\gamma'|)$ содержит цепь γ'' на $S \setminus V$. Пусть

c'' — класс гомологий цепи γ'' в $H_1(S \setminus |\partial\gamma|, |\partial\gamma'|)$. Тогда, так как $|\gamma| \cap |\gamma''| = \varnothing$, то $\iota(\gamma, \gamma'') = 0$, т. е. $\int\limits_{c''} \omega = 0$. С другой стороны, класс гомологий $c' - c''$ может быть представлен циклом $\gamma_2' - \gamma''$, гомологичным нулю на S. Следовательно, интеграл $\int\limits_{c'-c''} \omega$ является логарифмическим периодом дифференциала ω. В силу теоремы 9 вычеты дифференциала ω — целые числа, поэтому интеграл $\int\limits_{c'} \omega = \int\limits_{c'-c''} \omega$ есть целочисленное кратное числа $2\pi i$. Теорема 10, таким образом, доказана полностью.

§ 7. Геометрические леммы

Лемма 1. *Пусть D — замкнутый круг на римановой поверхности S поля R и C — его окружность. Выберем 1-цикл ζ на C, класс гомологий которого является положительной образующей группы $H_1(C)$. Пусть P — конечное подмножество поверхности S, не имеющее точек на C, и пусть c — элемент группы $H_1(S, P)$. Обозначим через z класс гомологий цикла ζ в группе $H_1(S \setminus P)$. Утверждается, что если $\partial c = \sum\limits_{\mathfrak{p} \in P} a(\mathfrak{p})\mathfrak{p}$, то $\iota(z, c) = \sum\limits_{\mathfrak{p} \in D \cap P} a(\mathfrak{p})$.*

В классе c выберем 1-цепь γ и зафиксируем некоторую точку $\mathfrak{p}_0 \in D \setminus C$. Для каждой точки $\mathfrak{p} \in D \cap P$ построим на $D \setminus C$ такую 1-цепь $\sigma(\mathfrak{p})$, что $\partial\sigma(\mathfrak{p}) = \mathfrak{p}_0 - \mathfrak{p}$. Тогда для $\mathfrak{p} \in D \cap P$ будем иметь $\iota(\zeta, \sigma(\mathfrak{p})) = 0$, откуда $\iota(\zeta, \gamma) = \iota\left(\zeta, \gamma + \sum\limits_{\mathfrak{p} \in D \cap P} a(\mathfrak{p})\sigma(\mathfrak{p})\right)$. Единственной точкой круга D, входящей в $\partial\left(\gamma + \sum\limits_{\mathfrak{p} \in D \cap P} a(\mathfrak{p})\sigma(\mathfrak{p})\right)$, является $\mathfrak{p}_0$, и эта точка входит с коэффициентом $\sum\limits_{\mathfrak{p} \in D \cap P} a(\mathfrak{p})$. Пусть ω — дифференциал из класса $\Omega\left(\gamma + \sum\limits_{\mathfrak{p} \in D \cap P} a(\mathfrak{p})\sigma(\mathfrak{p})\right)$ (см. § 6); тогда по теореме 9 § 6 мы имеем $\operatorname{res}_{\mathfrak{p}_0}\omega = \sum\limits_{\mathfrak{p} \in D \cap P} a(\mathfrak{p})$ и $\operatorname{res}_{\mathfrak{q}}\omega = 0$ для всех $\mathfrak{q} \neq \mathfrak{p}_0$ из D. В силу теоремы 6 § 4 отсюда выте-

кает, что $\int\limits_z \omega = 2\pi i \sum\limits_{\mathfrak{p}\in D\cap P} a(\mathfrak{p})$, и лемма 1 непосредственно следует теперь из определения индекса пересечения.

Если $\mathfrak{a}$ и $\mathfrak{b}$ — две различные точки окружности C круга D, то одна и только одна компонента множества $C\setminus\{\mathfrak{a}, \mathfrak{b}\}$ обладает тем свойством, что $\varepsilon(\mathfrak{a}, \mathfrak{c}, \mathfrak{b}) = 1$ для всех точек $\mathfrak{c}$ из этой компоненты (см. конец § 4); замыкание этой компоненты называется *положительной дугой*, определяемой точками $\mathfrak{a}$ и $\mathfrak{b}$ на C.

Лемма 2. *Пусть на римановой поверхности S поля R задан замкнутый круг D с окружностью C и на нем задана 1-цепь γ, для которой $|\partial\gamma| \subset C$. Пусть, далее, Γ есть положительная дуга на C, определяемая двумя различными точками $\mathfrak{a}$ и $\mathfrak{b}$ окружности C, не принадлежащими $|\gamma|$. Если λ есть 1-цепь на D, такая, что $\partial\lambda = \mathfrak{b} - \mathfrak{a}$ и $|\lambda| \cap |\partial\gamma| = \varnothing$, и если $\partial\gamma = \sum\limits_{\mathfrak{p}\in C} a(\mathfrak{p})\mathfrak{p}$, то $\iota(\gamma, \lambda) = \sum\limits_{\mathfrak{p}\in\Gamma} a(\mathfrak{p})$.*

В поле R мы можем найти такой элемент x, что D является x-кругом. Мы можем предполагать, что $x(\mathfrak{a}) = -i$ и $x(\mathfrak{b}) = i$ (это всегда можно устроить посредством надлежащего дробно-линейного преобразования элемента x). Пусть V — открытый x-круг, содержащий D. Обозначим через U_1 множество, получающееся из V удалением тех точек $\mathfrak{p}$, для которых $x(\mathfrak{p})$ есть вещественное неотрицательное число, а через U_2 — множество, получающееся из V удалением тех точек $\mathfrak{p}$, для которых $x(\mathfrak{p})$ — вещественное неположительное число. Легко видеть, что тогда дифференциал $x^{-1}dx$ на U_1 и U_2 обладает такими первообразными функциями f_1 и f_2 соответственно, что $f_1(\mathfrak{a}) = \frac{3\pi i}{2}$, $f_1(\mathfrak{b}) = \frac{\pi i}{2}$, $f_2(\mathfrak{a}) = -\frac{\pi i}{2}$ и $f_2(\mathfrak{b}) = \frac{\pi i}{2}$. Докажем, что $\Gamma \subset U_2$. Пусть $\mathfrak{c}$ — точка окружности C, в которой x принимает значение 1. Если σ_1 и σ_2 — 1-симплексы на $C \cap U_2$, для которых $\partial\sigma_1 = \mathfrak{c} - \mathfrak{a}$ и $\partial\sigma_2 = \mathfrak{b} - \mathfrak{c}$, а σ_3 — 1-симплекс на $C \cap U_1$, для которого $\partial\sigma_3 = \mathfrak{a} - \mathfrak{b}$, то

$$\int\limits_{\sigma_1+\sigma_2+\sigma_3} x^{-1}dx = i\left(\frac{\pi}{2} + \frac{\pi}{2} + \pi\right) = 2\pi i,$$

откуда $\varepsilon(\mathfrak{a}, \mathfrak{c}, \mathfrak{b}) = 1$ и $\Gamma \subset U_2$.

Легко видеть, что существует такое вещественное число α, $0<\alpha<1$, что все точки $\mathfrak{q}\in V$, удовлетворяющие условию $|x(\mathfrak{q})-\alpha|\leqslant|i-\alpha|$, образуют круг D' и $D'\cap C=\Gamma$. Обозначим через C' окружность круга D'. Точки $\mathfrak{a}$ и $\mathfrak{b}$ лежат на C'. Пересечение $D\cap C'$ является одной из дуг, определяемых точками $\mathfrak{a}$ и $\mathfrak{b}$ на C', при этом $D\cap C'\subset U_1$. Пусть λ' есть 1-симплекс на $D\cap C'$, для которого $\partial\lambda'=\mathfrak{b}-\mathfrak{a}$. Утверждаем, что тогда $\iota(\gamma,\ \lambda)=\iota(\gamma,\ \lambda')$. Для каждой точки $\mathfrak{p}\in|\partial\gamma|$ можно найти 1-симплекс $\mu(\mathfrak{p})$, лежащий на V, такой, что $|\mu(\mathfrak{p})|\cap D=\{\mathfrak{p}\}$ и $\partial\mu(\mathfrak{p})=\mathfrak{p}_1-\mathfrak{p}$, где $\mathfrak{p}_1$ — точка из $V\setminus D$. Множества $|\lambda|$ и $|\lambda'|$ не имеют общих точек с любым из множеств $|\mu(\mathfrak{p})|$, поэтому

$$\iota(\gamma,\ \lambda)=\iota\Big(\gamma+\sum_{\mathfrak{p}\in|\partial\gamma|}a(\mathfrak{p})\mu(\mathfrak{p}),\ \lambda\Big)$$

и

$$\iota(\gamma,\ \lambda')=\iota\Big(\gamma+\sum_{\mathfrak{p}\in|\partial\gamma|}a(\mathfrak{p})\mu(\mathfrak{p}),\ \lambda'\Big).$$

Множество $\Big|\partial\Big(\gamma+\sum\limits_{\mathfrak{p}\in|\partial\gamma|}a(\mathfrak{p})\mu(\mathfrak{p})\Big)\Big|$ не имеет общих точек с D. Цепь $\lambda'-\lambda$ является циклом на D, а значит, она гомологична нулю на D, ибо $H_1(D)=0$. Отсюда следует, что $\iota\Big(\gamma+\sum\limits_{\mathfrak{p}\in|\partial\gamma|}a(\mathfrak{p})\mu(\mathfrak{p}),\ \lambda'-\lambda\Big)=0$, и наше утверждение доказано. На C' можно построить такой 1-симплекс λ'', что $\partial\lambda''=\mathfrak{a}-\mathfrak{b}$ и $|\lambda''|\cap D=\{\mathfrak{a},\ \mathfrak{b}\}$. Множества $|\lambda''|$ и $|\gamma|$ не имеют общих точек, поэтому $\iota(\gamma,\ \lambda')=\iota(-(\lambda'+\lambda''),\ \gamma)$. Цепь $-(\lambda'+\lambda'')$ является 1-циклом на C'; так как $|\lambda'|\subset U_1$, а $|\lambda''|\subset U_2$, то $\int\limits_{-\lambda'}x^{-1}dx=\pi i$ и $\int\limits_{-\lambda''}x^{-1}dx=\pi i$, откуда $\int\limits_{-(\lambda'+\lambda'')}x^{-1}dx=2\pi i$. Этим доказано, что цикл $-(\lambda'+\lambda'')$ принадлежит положительной образующей группы $H_1(C')$. Так как $|\partial\gamma|\cap D'=|\partial\gamma|\cap\Gamma$, то лемма 2 следует теперь из леммы 1.

Лемма 3. *Пусть D — замкнутый круг и E — замкнутое линейно-связное подмножество на римановой поверхности S поля R. Обозначим через V некоторое открытое подмножество поверхности S, содержащее D, и через n — целое число. Предположим, что 1-цикл ζ на $S\setminus E$ таков, что $\iota(\zeta,\ \lambda)\equiv 0\pmod n$ для всех 1-циклов λ*

на S. Тогда ζ может быть представлен в виде $n\zeta_1+\zeta_2+$ $+d\tau$, где ζ_1 — 1-цикл на S, ζ_2 — 1-цикл на $S\setminus(D\cup E)$ и τ — 2-цепь на $V\cup|\zeta|$. Если $D\cap E\neq\varnothing$, то всякий 2-цикл φ на $S\setminus E$ гомологичен на S некоторому 2-циклу на $S\setminus(D\cup E)$.

Выберем в поле R элемент x так, чтобы D был x-кругом, и обозначим через $\mathfrak{c}$ x-центр круга D. Пусть D' — замкнутый x-круг с x-центром в $\mathfrak{c}$, содержащий D внутри себя и содержащийся в V. Обозначим через C' окружность круга D'. Если $\mathfrak{q}_0\in C'$, то множество тех точек $\mathfrak{q}\in D'$, для которых $x(\mathfrak{q})=tx(\mathfrak{q}_0)$, где t — вещественно, $0\leqslant t\leqslant 1$, будем называть *радиальным множеством* точки $\mathfrak{q}_0$.

Прежде всего докажем, что существует замкнутый x-круг D'' с x-центром в точке $\mathfrak{c}$, обладающий следующими свойствами: 1) D'' содержится внутри D' и содержит внутри себя D и 2) если F есть объединение тех радиальных множеств круга D', которые содержат точки множества $\overline{D'\setminus D''}\cap E$ (черта сверху означает замыкание), то F не имеет общих точек с множеством $\overline{D'\setminus D''}\cap(|\zeta|\cup|\varphi|)$, где ζ и φ — фиксированные циклы, о которых говорится в лемме. Допустим, что такого круга D'' не существует. Обозначим через r' x-радиус круга D'. Тогда для каждого целого числа $m>0$ найдутся точки $\mathfrak{p}_m\in D'\cap E$ и $\mathfrak{q}_m\in D'\cap(|\zeta|\cup|\varphi|)$, лежащие на одном и том же радиальном множестве круга D' и такие, что $|x(\mathfrak{p}_m)|\geqslant r'-\frac{1}{m}$, $|x(\mathfrak{q}_m)|\geqslant r'-\frac{1}{m}$, а следовательно, $|x(\mathfrak{p}_m)-x(\mathfrak{q}_m)|\leqslant\frac{1}{m}$. Так как $D'\cap E$ компактно, то некоторая подпоследовательность последовательности $(\mathfrak{p}_m)$ сходится к точке $\mathfrak{p}_0\in D'\cap E$. Ясно, что $\mathfrak{p}_0$ является также пределом некоторой подпоследовательности последовательности $(\mathfrak{q}_m)$, откуда следует, что $\mathfrak{p}_0\in|\zeta|\cup|\varphi|$, ибо $|\zeta|\cup|\varphi|$ компактно. Это, однако, невозможно, так как $|\zeta|\cup|\varphi|\subset S\setminus E$. Будем считать, что круг D'' удовлетворяет указанным выше условиям. Найдем целое число $p\geqslant 0$, такое, что каждый симплекс, входящий в какую-нибудь из цепей $\zeta^*=\mathrm{subd}^p\zeta$ или $\varphi^*=\mathrm{subd}^p\varphi$, множество точек которого пересекается с D'', лежит на D'. В цепях ζ^* и φ^* выделим симплексы, лежащие на D'; снабдив эти симплексы теми же коэффициентами, с которыми они входят в ζ^* и φ^*, мы получим

цепи γ_1 и ψ_1 соответственно. Очевидно, что $\zeta^* - \gamma_1$ и $\varphi^* - \psi_1$ будут тогда цепями на $S \setminus (D \cup E)$.

Если мы произвольную точку $\mathfrak{p} \in \overline{D' \setminus D''} \setminus (\overline{D' \setminus D''} \cap F)$ отобразим на точку окружности C', лежащую на том же радиальном множестве что и $\mathfrak{p}$, то получим непрерывное отображение множества $\overline{D' \setminus D''} \setminus (\overline{D' \setminus D''} \cap F)$, гомотопное, очевидно, тождественному отображению и совпадающее с тождественным отображением на $C' \setminus (C' \cap F)$. Циклы $\partial\gamma_1$ и $\partial\psi_1$ лежат на $\overline{D' \setminus D''} \setminus (\overline{D' \setminus D''} \cap F)$; поэтому они гомологичны на этом множестве циклам на $C' \setminus (C' \cap F)$. Это означает, что на $\overline{D' \setminus D''} \setminus (\overline{D' \setminus D''} \cap F)$ существуют 1-цепь γ_2 и 2-цепь ψ_2, такие, что $|\partial(\gamma_1 + \gamma_2)| \subset C'$ и $|\partial(\psi_1 + \psi_2)| \subset C'$.

Положим $\partial(\gamma_1 + \gamma_2) = \sum_{k=1}^{h} a_k \mathfrak{r}_k$, где $\mathfrak{r}_1, \ldots, \mathfrak{r}_h$ — точки окружности C' и $a_k \neq 0$ $(1 \leqslant k \leqslant h)$. Точки $\mathfrak{r}_k$ лежат на $C' \setminus (C' \cap E)$. Утверждаем, что для любой связной компоненты A множества $C' \setminus (C' \cap E)$ имеет место сравнение $\sum_{\mathfrak{r}_k \in A} a_k \equiv 0 \pmod{n}$. Это справедливо очевидным образом, если $C' \cap E$ пусто или состоит из одной точки, ибо $\sum_{k=1}^{h} a_k = 0$. Если $C' \cap E$ состоит по крайней мере из двух точек, то относительная граница компоненты A на C' состоит из двух точек $\mathfrak{a}$ и $\mathfrak{b}$ множества E; можно считать, что эти точки обозначены так, что $\overline{A}$ является положительной дугой, определяемой $\mathfrak{a}$ и $\mathfrak{b}$. Найдем на F такую 1-цепь λ_1, что $\partial\lambda_1 = \mathfrak{b} - \mathfrak{a}$. Тогда $|\gamma_1 + \gamma_2| \cap |\partial\lambda_1| = \varnothing$ и $|\lambda_1| \cap |\partial(\gamma_1 + \gamma_2)| = \varnothing$. В силу леммы 2 получаем $\sum_{\mathfrak{r}_k \in A} a_k = \iota(\gamma_1 + \gamma_2, \lambda_1)$. Далее, множество $|\zeta^* - \gamma_1 - \gamma_2|$ не пересекается с F, поэтому $\iota(\gamma_1 + \gamma_2, \lambda_1) = \iota(\zeta^*, \lambda_1) = \iota(\zeta, \lambda_1)$. Так как E линейно связно, то на E существует такая 1-цепь λ_2, что $\partial\lambda_2 = \mathfrak{a} - \mathfrak{b}$. Цепь $\lambda_1 + \lambda_2$ является циклом, и $\iota(\zeta, \lambda_1) = \iota(\zeta, \lambda_1 + \lambda_2)$ (ибо $|\zeta| \subset S \setminus E$, а значит, $|\zeta| \cap |\lambda_2| = \varnothing$). По предположению последнее число $\equiv 0 \pmod{n}$.

Для каждой компоненты A множества $C' \setminus (C' \cap E)$, пересекающейся с $|\partial(\gamma_1 + \gamma_2)|$, выберем точку $\mathfrak{f}_A \in A$ и обозна-

чим через b_A число $\frac{1}{n}\sum_{\tau_k \in A} a_k$ (если $n \neq 0$; если же $n=0$, то полагаем $b_A=0$). Очевидно тогда, что $n\sum_A b_A \mathfrak{f}_A - \partial(\gamma_1+\gamma_2)$ является границей некоторой 1-цепи γ_3 на $C' \setminus (C' \cap E)$. Таким образом, $\partial(\gamma_1+\gamma_2+\gamma_3) = n\sum_A b_A \mathfrak{f}_A$. Отсюда следует, что $\sum_A b_A = 0$ и, следовательно, что $\sum_A b_A \mathfrak{f}_A$ является границей цепи $-\gamma_4$ на C'. Положим $\zeta^* = \gamma_1+\gamma_2+\gamma_3+n\gamma_4 + (\zeta^* - \gamma_1 - \gamma_2 - \gamma_3 - n\gamma_4)$. Цепь $\gamma_1+\gamma_2+\gamma_3+n\gamma_4$ является 1-циклом на D', а так как $H_1(D')=0$, то этот цикл есть граница 2-цепи τ_1 на D', откуда $\zeta^* = \partial\tau_1 + (\zeta^* - \gamma_1 - \gamma_2 - \gamma_3 - n\gamma_4)$. Так как ζ^* есть цикл, то цепь $\zeta^* - \gamma_1 - \gamma_2 - \gamma_3 - n\gamma_4$ также является циклом. Цепь $\zeta^* - \gamma_1 - \gamma_2 - \gamma_3$ лежит на $S \setminus (D \cup E)$, поэтому $n\partial\gamma_4 = \partial(\zeta^* - \gamma_1 - \gamma_2 - \gamma_3)$ есть граница 1-цепи на $S \setminus (D \cup E)$. Но, как легко видеть, для любого пространства X группа $H_0(X)$ никогда не содержит элементов конечного порядка, отличных от 0. Следовательно, $\partial\gamma_4$ есть граница 1-цепи γ_5 на $S \setminus (D \cup E)$. Положим $\zeta_1 = \gamma_5 - \gamma_4$ и $\zeta_2 = \zeta^* - \gamma_1 - \gamma_2 - \gamma_3 - n\gamma_5$. Тогда ζ_1 есть 1-цикл, ζ_2 — 1-цикл на $S \setminus (D \cup E)$, и мы имеем $\zeta = (\zeta - \zeta^*) + \partial\tau_1 + n\zeta_1 + \zeta_2$. Так как $\zeta^* = \mathrm{subd}^p \zeta$, то цепь ζ^* гомологична ζ на $|\zeta|$, т. е. $\zeta - \zeta^* = \partial\tau_2$, где τ_2 — 2-цепь на $|\zeta|$. Но $|\tau_1| \subset D' \subset V$, поэтому $|\tau_1+\tau_2| \subset |\zeta| \cup V$. Этим доказано первое утверждение леммы 3.

Будем теперь предполагать, что $D \cap E \neq \varnothing$. Имеем $|\partial(\psi_1+\psi_2)| \subset C' \setminus (C' \cap E)$. Если $C' \cap E$ не пусто, то $C' \setminus (C' \cap E)$ является объединением попарно непересекающихся множеств, каждое из которых относительно открыто в $C' \setminus (C' \cap E)$ и гомеоморфно открытому интервалу вещественной оси. Каждый 1-цикл на $C' \setminus (C' \cap E)$ лежит на объединении конечного числа этих множеств, откуда легко следует, что в этом случае $H_1(C' \setminus (C' \cap E)) = 0$, а потому $\partial(\psi_1+\psi_2)$ является границей 2-цепи $-\psi_3$ на $C' \setminus (C' \cap E)$. Последнее заключение справедливо также и в случае, когда $C' \cap E$ пусто. Действительно, пусть $\mathfrak{a}$ — точка из $D \cap E$, а значит, $\mathfrak{a} \notin |\psi_1+\psi_2|$. Так как $\mathfrak{a}$ является внутренней точкой круга D', то C' — деформационный ретракт множества $D' \setminus \{\mathfrak{a}\}$. Цепь $\partial(\psi_1+\psi_2)$, лежащая на C' и являющаяся границей на $D' \setminus \{\mathfrak{a}\}$, является границей также и на $C' = C' \setminus (C' \cap E)$.

Таким образом, в любом случае мы имеем $\partial(\psi_1+\psi_2)=-\partial\psi_3$, где ψ_3 — 2-цепь на $C'\setminus(C'\cap E)$. Положим $\varphi^*=\psi_1+\psi_2+\psi_3+(\varphi^*-\psi_1-\psi_2-\psi_3)$. Цепь $\psi_1+\psi_2+\psi_3$ есть 2-цикл на D', а значит, она гомологична нулю на D', ибо $H_2(D')=0$. С другой стороны, $|\varphi^*-\psi_1|\subset S\setminus(D\cup E)$, $|\psi_2|\subset S\setminus(D\cup E)$ и $|\psi_3|\subset S\setminus(D\cup E)$. Так как цикл φ^* на S гомологичен φ, то получаем, что цикл φ гомологичен 2-циклу на $S\setminus(D\cup E)$. Лемма 3 доказана.

Лемма 4. *Пусть $\mathfrak{p}$ — точка римановой поверхности S поля R и пусть ζ — такой 1-цикл на $S\setminus\{\mathfrak{p}\}$, что $\iota(\zeta,\lambda)\equiv 0\,(\mathrm{mod}\,n)$ для любого 1-цикла λ на S, где n — некоторое фиксированное целое число. Тогда цикл ζ гомологичен на $S\setminus\{\mathfrak{p}\}$ циклу вида $n\zeta_1$, где ζ_1 — некоторый цикл. Далее, всякий 2-цикл φ на $S\setminus\{\mathfrak{p}\}$ гомологичен нулю на S.*

Для каждой точки $\mathfrak{q}\in S$ выберем открытый круг $V_\mathfrak{q}$, содержащий эту точку, так, чтобы $V_\mathfrak{p}\cap(|\zeta|\cup|\varphi|)=\varnothing$ и $\mathfrak{p}\notin V_\mathfrak{q}$, если $\mathfrak{p}\neq\mathfrak{q}$. Пусть $D_\mathfrak{q}$ есть замкнутый круг, содержащийся в $V_\mathfrak{q}$, для которого $\mathfrak{q}$ является внутренней точкой, и пусть U — множество внутренних точек круга $D_\mathfrak{q}$. Множества $U_\mathfrak{q}$, $\mathfrak{q}\in S$, образуют покрытие пространства S. Так как S компактно, то оно может быть покрыто конечным числом множеств $U_\mathfrak{q}$. Пусть Q — некоторое конечное подмножество поверхности S, такое, что множества $U_\mathfrak{q}$, $\mathfrak{q}\in Q$, образуют покрытие S. Обозначим через a число точек в Q. Эти точки мы сейчас занумеруем надлежащим образом целыми числами от 1 до a. Так как $\mathfrak{p}\notin V_\mathfrak{q}$, если $\mathfrak{q}\neq\mathfrak{p}$, то $\mathfrak{p}\in Q$. Будем считать, что $\mathfrak{q}_1=\mathfrak{p}$. Предположим, что точки $\mathfrak{q}_1,\ldots,\mathfrak{q}_i$ из Q, где $i<a$, уже занумерованы. Если $D_{\mathfrak{q}_1}\cup\ldots\cup D_{\mathfrak{q}_i}=S$, то в качестве $\mathfrak{q}_{i+1}$ возьмем любую точку из Q, отличную от $\mathfrak{q}_1,\ldots,\mathfrak{q}_i$. В противном случае, в силу связности S, множество $D_{\mathfrak{q}_1}\cup\ldots\cup D_{\mathfrak{q}_i}$ имеет по крайней мере одну граничную точку $\mathfrak{r}_i\in S$, и в качестве $\mathfrak{q}_{i+1}$ мы возьмем такую точку из Q, для которой $\mathfrak{r}_i\in U_{\mathfrak{q}_{i+1}}$. Ясно, что точка $\mathfrak{q}_{i+1}$ отлична от $\mathfrak{q}_1,\ldots,\mathfrak{q}_i$.

Положим $E_i=D_{\mathfrak{q}_1}\cup\ldots\cup D_{\mathfrak{q}_i}$. Каждое множество E_i замкнуто и линейно связно. В самом деле, при $i=1$ это верно; если утверждение справедливо для некоторого $i<a$, то оно будет справедливым также и для $i+1$, так как $E_{i+1}=E_i\cup D_{\mathfrak{q}_{i+1}}$ и $D_{\mathfrak{q}_{i+1}}$ имеет общую точку с множе-

ством E_i (если $E_i \neq S$; если же $E_i = S$, то $E_{i+1} = S$). Очевидно, что $E_a = S$.

Циклы $\zeta_1 = \zeta$ и $\varphi_1 = \varphi$ лежат на $S \setminus E_1$. Допустим, что для некоторого $i < a$ мы уже доказали, что цикл ζ гомологичен на $S \setminus \{\mathfrak{p}\}$ циклу вида $n\theta_1 + \theta_2$, где θ_1 — цикл на S, а θ_2 — цикл на $S \setminus E_i$. Для любого цикла λ на S имеем $\iota(\theta_2, \lambda) = \iota(\zeta, \lambda) - n\iota(\theta_1, \lambda) \equiv 0 \pmod{n}$. Применяя лемму 3, заключаем, что цикл θ_2 гомологичен на $|\theta_2| \cup V_{q_{i+1}}$ циклу вида $n\theta_1' + \theta_2'$, где θ_1' — цикл на S, а θ_2' — цикл на $S \setminus (D_{q_{i+1}} \cup E_i) = S \setminus E_{i+1}$. Но $|\theta_2| \subset S \setminus \{\mathfrak{p}\}$ и $V_{q_{i+1}} \subset S \setminus \{\mathfrak{p}\}$, поэтому ζ гомологичен на $S \setminus \{\mathfrak{p}\}$ циклу $n(\theta_1 + \theta_1') + \theta_2'$, где θ_2' — цикл на $S \setminus E_{i+1}$. Так как $S \setminus E_a = \varnothing$, то первое утверждение леммы 4 непосредственно следует из нашего индуктивного процесса.

Аналогичным образом, предположим, что при некотором $i < a$ цикл φ гомологичен 2-циклу φ_i на $S \setminus E_i$. Так как пересечение $D_{q_{i+1}} \cap E_i$ не пусто, то, в силу леммы 3, цикл φ_i гомологичен 2-циклу φ_{i+1} на $S \setminus (D_{q_{i+1}} \cup E_i) = S \setminus E_{i+1}$. Таким образом, φ гомологичен 2-циклу на $S \setminus E_a$; но $S \setminus E_a$ пусто, поэтому φ гомологичен нулю. Лемма 4 теперь доказана полностью.

§ 8. Группы гомологий римановой поверхности

Теорема 11. *Пусть P и Q — два конечных непересекающихся подмножества римановой поверхности S поля R. Обозначим через g род поля R, а через p и q — количества элементов в множествах P и Q соответственно. Положим $p^* = \max\{p-1, 0\}$, $q^* = \max\{q-1, 0\}$. Утверждается, что тогда $H_1(S \setminus P, Q)$ есть свободная абелева группа с $2g + p^* + q^*$ образующими. Далее, для произвольного гомоморфизма $c \to \eta(c)$ этой группы в аддитивную группу целых чисел существует и притом единственный элемент $c' \in H_1(S \setminus Q, P)$, такой, что $\eta(c) = \iota(c, c')$ при всех $c \in H_1(S \setminus P, Q)$. Наконец, для произвольного гомоморфизма $c \to \pi(c)$ группы $H_1(S \setminus P, Q)$ в аддитивную группу комплексных чисел существует дифференциал ω, не имеющий полюсов в Q, вычеты которого во всех точках вне P равны 0 и такой, что $\pi(c) = \int_c \omega$*

для всех $c \in H_1(S \setminus P, Q)$; *дифференциал* ω *определен последним условием с точностью до слагаемого вида* df, *где* f — *элемент поля* R, *для которого все точки из* Q *являются нулями.*

Для каждой точки $\mathfrak{r} \in P \cup Q$ выберем замкнутый круг $D_{\mathfrak{r}}$, содержащий $\mathfrak{r}$ внутри себя и не имеющий других общих точек с $P \cup Q$. Обозначим через $C_{\mathfrak{r}}$ окружность круга $D_{\mathfrak{r}}$ и через $\zeta(\mathfrak{r})$ — цикл на $C_{\mathfrak{r}}$, принадлежащий положительной образующей группы $H_1(C_{\mathfrak{r}})$. Множество $S \setminus Q$, очевидно, связно, а значит, и линейно связно; если $\mathfrak{p}$ и $\mathfrak{p}'$ — различные точки из P, то через $\gamma(\mathfrak{p}, \mathfrak{p}')$ мы обозначим 1-цепь на $S \setminus Q$, для которой $\partial\gamma(\mathfrak{p}, \mathfrak{p}') = \mathfrak{p}' - \mathfrak{p}$. Докажем сначала, что цикл $\sum_{\mathfrak{p} \in P} \zeta(\mathfrak{p})$ гомологичен нулю на $S \setminus P$. Мы можем, конечно, предполагать, что P не пусто; пусть $\mathfrak{p}$ — произвольная точка из P. Для любого цикла λ на S мы имеем $\iota(\zeta(\mathfrak{p}), \lambda) = 0$, ибо $\zeta(\mathfrak{p})$ гомологичен нулю на $D_{\mathfrak{p}}$, а следовательно, и на S. Применяя лемму 4 § 7 (для случая $n = 0$), получаем, что цикл $\zeta(\mathfrak{p})$ гомологичен нулю на $S \setminus \{\mathfrak{p}\}$. Если $P \neq \{\mathfrak{p}\}$, то в силу леммы 4 § 4 (примененной к множествам $U = S \setminus \{\mathfrak{p}\}$ и $P \setminus \{\mathfrak{p}\}$) цикл $\zeta(\mathfrak{p})$ гомологичен на $S \setminus P$ циклу вида $\sum_{\mathfrak{p}' \in P,\, \mathfrak{p}' \neq \mathfrak{p}} a(\mathfrak{p}')\zeta(\mathfrak{p}')$. Так как $\gamma(\mathfrak{p}, \mathfrak{p}')$ есть цикл по модулю P, то

$$\iota\Big(\zeta(\mathfrak{p}) - \sum_{\mathfrak{p}' \in P,\, \mathfrak{p}' \neq \mathfrak{p}} a(\mathfrak{p}')\zeta(\mathfrak{p}'),\ \gamma(\mathfrak{p}, \mathfrak{p}')\Big) = 0$$

для всех $\mathfrak{p}' \in P \setminus \{\mathfrak{p}\}$. Из леммы 1 § 7 следует, что

$$\iota(\zeta(\mathfrak{p}), \gamma(\mathfrak{p}, \mathfrak{p}')) = -1;\ \iota(\zeta(\mathfrak{p}'), \gamma(\mathfrak{p}, \mathfrak{p}')) = 1;$$
$$\iota(\zeta(\mathfrak{p}''), \gamma(\mathfrak{p}, \mathfrak{p}')) = 0, \text{ если } \mathfrak{p}'' \in P,\ \mathfrak{p}'' \neq \mathfrak{p}, \mathfrak{p}'.$$

Таким образом, получаем $-1 - a(\mathfrak{p}') = 0$ при всех $\mathfrak{p}' \in P \setminus \{\mathfrak{p}\}$, а это и доказывает, что цикл $\sum_{\mathfrak{p} \in P} \zeta(\mathfrak{p})$ гомологичен нулю на $S \setminus P$.

Пусть n — некоторое целое число, и пусть c_0 — элемент из группы $H_1(S \setminus P, Q)$, такой, что $\iota(c_0, c') \equiv (\mathrm{mod}\, n)$ при всех $c' \in H_1(S \setminus Q, P)$. Покажем, что тогда c_0 имеет вид nc, где $c \in H_1(S \setminus P, Q)$. Положим $\partial c_0 = \sum_{\mathfrak{q} \in Q} a(\mathfrak{q})\mathfrak{q}$. Если через c' мы обозначим класс гомологий цикла $\zeta(\mathfrak{q})$ в $H_1(S \setminus Q, P)$,

то, в силу леммы 1 § 7, $\iota(c_0, c') = -a(\mathfrak{q})$. Таким образом, $a(\mathfrak{q}) = nb(\mathfrak{q})$, где $b(\mathfrak{q})$ — целое число, которое считаем равным 0, если $n = 0$. Так как $\sum_{\mathfrak{q} \in Q} a(\mathfrak{q}) = 0$, то $\sum_{\mathfrak{q} \in Q} b(\mathfrak{q}) = 0$. Пространство $S \setminus P$ линейно связно, поэтому любые две точки из Q гомологичны между собой на $S \setminus P$. В силу равенства $\sum_{\mathfrak{q} \in Q} b(\mathfrak{q}) = 0$ цепь $\sum_{\mathfrak{q} \in Q} b(\mathfrak{q})\mathfrak{q}$ может быть представлена в виде линейной комбинации с целыми коэффициентами цепей вида $\mathfrak{q}' - \mathfrak{q}''$, где $\mathfrak{q}'$ и $\mathfrak{q}''$ принадлежат Q. Отсюда следует, что $\partial c_0 = n\,\partial c_1$, где c_1 — некоторый элемент из $H_1(S \setminus P, Q)$. Заменив c_0 на $c_0 - nc_1$, мы можем предполагать, что $\partial c_0 = 0$.

Пусть теперь γ — цикл из класса c_0. Каждый 1-цикл λ на S гомологичен на S некоторому циклу на $S \setminus Q$ (следствие к лемме 4 § 4). Отсюда следует, что $\iota(\gamma, \lambda) \equiv 0 \pmod{n}$. Применяя лемму 4 § 7, получаем, что цикл γ гомологичен на S циклу вида $n\gamma_2$, где γ_2 — цикл на S, который можно даже считать циклом на $S \setminus P$ (следствие к лемме 4 § 4). Пусть c_2 — класс гомологий цикла γ_2 в $H_1(S \setminus P, Q)$. Тогда $c_0 - nc_2$ принадлежит ядру гомоморфизма группы $H_1(S \setminus P, Q)$ в $H_1(S, Q)$, соответствующего тождественному отображению пары $(S \setminus P, Q)$ в (S, Q). Применяя лемму 4 § 4, заключаем, что $c_0 - nc_2 = \sum_{\mathfrak{p} \in P} e(\mathfrak{p})\, z(\mathfrak{p})$, где $z(\mathfrak{p})$ — класс гомологий цикла $\zeta(\mathfrak{p})$ в $H_1(S \setminus P, Q)$. Для различных точек $\mathfrak{p}$ и $\mathfrak{p}'$ из P через $c'(\mathfrak{p}, \mathfrak{p}')$ обозначим класс гомологий цепи $\gamma(\mathfrak{p}, \mathfrak{p}')$ в $H_1(S \setminus Q, P)$. В силу вышеприведенной формулы, мы имеем $\iota(c_0 - nc_2, c'(\mathfrak{p}, \mathfrak{p}')) = e(\mathfrak{p}') - e(\mathfrak{p})$. По предположению это число $\equiv 0 \pmod{n}$. Таким образом, все числа $e(\mathfrak{p})$ сравнимы между собой по модулю n. С другой стороны, выше было доказано, что $\sum_{\mathfrak{p} \in P} z(\mathfrak{p}) = 0$. Следовательно, мы можем считать, что $e(\mathfrak{p}) \equiv 0 \pmod{n}$ при всех $\mathfrak{p} \in P$. Этим доказано, что c_0 имеет вид nc, где $c \in H_1(S \setminus P, Q)$. Взяв, в частности, $n = 0$, получаем, что если $\iota(c, c') = 0$ при всех $c' \in H_1(S \setminus Q, P)$, то $c = 0$. Отсюда вытекает, что группа $H_1(S \setminus P, Q)$ не имеет элементов конечного порядка, отличных от 0. Действительно, если для целого числа $u \neq 0$ имеем $uc = 0$, то $u\iota(c, c') = \iota(uc, c') = 0$ при всех $c' \in H_1(S \setminus Q, P)$, откуда $\iota(c, c') = 0$ и $c = 0$.

Пусть пространства $\mathfrak{E}_{P,Q}$ и $\mathfrak{F}_P$ определены так же, как и в § 5, и пусть $\Omega(c)$ — класс смежности из $\mathfrak{E}_{Q,P}/\mathfrak{F}_P$, соответствующий элементу $c \in H_1(S \setminus P, Q)$ согласно теореме 9 § 6. Если $c' \in H_1(S \setminus Q, P)$, то $\iota(c, c') = -\frac{1}{2\pi i}\int\limits_{c'} \Omega(c)$.

В силу вышедоказанного отсюда следует, что гомоморфизм $c \to \Omega(c)$ группы $H_1(S \setminus P, Q)$ в $\mathfrak{E}_{Q,P}/\mathfrak{F}_P$ является изоморфизмом. Обозначим через $\mathfrak{M}$ подпространство пространства $\mathfrak{E}_{Q,P}/\mathfrak{F}_P$, натянутое на элементы $\Omega(c)$, $c \in H_1(S \setminus P, Q)$. В § 5 было установлено, что функция $j(\omega, \omega')$ естественным образом определяет невырожденную билинейную функцию на произведении $(\mathfrak{E}_{Q,P}/\mathfrak{F}_P) \times (\mathfrak{E}_{P,Q}/\mathfrak{F}_Q)$; обозначим эту билинейную функцию также через j. Пусть Ω_0' — элемент из $\mathfrak{E}_{P,Q}/\mathfrak{F}_Q$, такой, что $j(\Omega, \Omega_0') = 0$ для всех $\Omega \in \mathfrak{M}$. Если ω_0' — дифференциал, принадлежащий классу смежности Ω_0', то $\int\limits_c \omega_0' = 0$ для каждого $c \in H_1(S \setminus P, Q)$. Так как $\int\limits_{\zeta(\mathfrak{p})} \omega_0' = 0$ для любой точки $\mathfrak{p} \in P$, то, по теореме 6 § 4, $\operatorname{res}_{\mathfrak{p}} \omega_0' = 0$. Но $\omega_0' \in \mathfrak{E}_{P,Q}$, поэтому ω_0' — дифференциал второго рода. Каждый класс гомологий на S может быть представлен циклом на $S \setminus P$, следовательно, интеграл от ω_0' по любому классу гомологий из $H_1(S)$ равен 0, откуда следует, что ω_0' обладает на S первообразной функцией f (теорема 7 § 4). Эта функция f, будучи всюду мероморфной, является элементом поля R (теорема 4 § 2). Так как $\omega_0' \in \mathfrak{E}_{P,Q}$, то f не имеет полюсов на множестве Q. Для различных точек $\mathfrak{q}$ и $\mathfrak{q}'$ множества Q через $\gamma(\mathfrak{q}, \mathfrak{q}')$ обозначим 1-цепь на $S \setminus P$, для которой $\partial\gamma(\mathfrak{q}, \mathfrak{q}') = \mathfrak{q}' - \mathfrak{q}$. Тогда, по лемме 2 § 4, $0 = \int\limits_{\gamma(\mathfrak{q}, \mathfrak{q}')} df = f(\mathfrak{q}') - f(\mathfrak{q})$. Таким образом, числа $f(\mathfrak{q})$, $\mathfrak{q} \in Q$, все равны между собой. Обозначим через f_0 их общее значение; тогда $\omega_0' = d(f - f_0) \in \mathfrak{F}_Q$, т. е. $\Omega_0' = 0$. Так как билинейная функция j невырождена, то отсюда следует, что $\mathfrak{M}$ совпадает со всем пространством $\mathfrak{E}_{Q,P}/\mathfrak{F}_P$. Положим $m = 2g + p^* + q^*$. Согласно теореме 15 § 8 гл. VI размерность пространства $\mathfrak{E}_{Q,P}/\mathfrak{F}_P$ равна m. Так как $\mathfrak{M}$ имеет размерность m, то в группе $H_1(S \setminus P, Q)$ мы можем найти m таких элементов $d_1, \ldots, d_m$, что $\Omega(d_1), \ldots, \Omega(d_m)$

линейно независимы в $\mathfrak{E}_{Q,P}/\mathfrak{F}_P$. Аналогичным образом в группе $H_1(S \setminus Q, P)$ мы можем найти m таких элементов $d_1', \ldots, d_m'$, что $\Omega(d_1'), \ldots, \Omega(d_m')$ линейно независимы в $\mathfrak{E}_{P,Q}/\mathfrak{F}_Q$. Так как функция j невырождена, то определитель матрицы $(j(\Omega(d_k), \Omega(d_l')))_{1 \leqslant k, l \leqslant m}$ отличен от 0, откуда следует, что определитель D матрицы $(\iota(d_k, d_l))_{1 \leqslant k, l \leqslant m}$, являющийся целым числом, также отличен от 0.

Пусть d — произвольный элемент из $H_1(S \setminus P, Q)$. Тогда $\Omega(d)$ является линейной комбинацией $\sum_{k=1}^{m} \alpha_k \Omega(d_k)$ элементов $\Omega(d_1), \ldots, \Omega(d_m)$ с комплексными коэффициентами $\alpha_1, \ldots, \alpha_m$. Далее,

$$\iota(d, d_l') = -\frac{1}{2\pi i} \int_{d_l'} \Omega(d) =$$

$$= -\frac{1}{2\pi i} \sum_{k=1}^{m} \alpha_k \int_{d_l'} \Omega(d_k) = \sum_{k=1}^{m} \alpha_k \iota(d_k, d_l').$$

Таким образом, числа $\alpha_1, \ldots, \alpha_m$ удовлетворяют системе m линейных уравнений с целыми коэффициентами и целыми свободными членами, при этом определитель D этой системы отличен от 0. Отсюда следует, что числа $\alpha_1, \ldots, \alpha_m$ рациональны, и целое число D является их общим знаменателем. Следовательно, для любого $d \in H_1(S \setminus P, Q)$ элемент Dd является линейной комбинацией элементов $d_1, \ldots, d_m$ с целыми коэффициентами. Так как группа $H_1(S \setminus P, Q)$ не имеет элементов конечного порядка, отличных от 0, то из доказанного следует (в силу известных теорем теории абелевых групп), что $H_1(S \setminus P, Q)$ есть свободная абелева группа с m образующими. Будем предполагать теперь, что элементы $d_1, \ldots, d_m$ образуют базис группы $H_1(S \setminus P, Q)$, а элементы $d_1', \ldots, d_m'$ — базис группы $H_1(S \setminus Q, P)$. Докажем, что тогда $D = \pm 1$. Действительно, если бы это было не так, то D делилось бы на некоторое простое число n, и система линейных однородных сравнений $\sum_{k=1}^{m} a_k \iota(d_k, d_l') \equiv 0 \pmod{n}$ $(1 \leqslant l \leqslant m)$ имела бы нетривиальное решение

$(a_1, \ldots, a_m)$. Для элемента $d = \sum_{k=1}^{m} a_k d_k$ мы имели бы тогда $\iota(d, c') \equiv 0 \pmod{n}$ для всех $c' \in H_1(S \setminus Q, P)$ (так как $d'_1, \ldots, d'_m$ образуют базис группы $H_1(S \setminus Q, P)$). Но отсюда следовало бы, что $d = nc$ при некотором $c \in H_1(S \setminus P, Q)$, а это невозможно, ибо числа $a_1, \ldots, a_m$ не все делятся на n, а $d_1, \ldots, d_m$ образуют базис группы $H_1(S \setminus P, Q)$.

Так как $D = \pm 1$, то, как известно, для заданного базиса $\{d_1, \ldots, d_m\}$ группы $H_1(S \setminus P, Q)$ базис $\{d'_1, \ldots, d'_m\}$ группы $H_1(S \setminus Q, P)$ может быть выбран так, что $\iota(d_k, d'_l)$ равно 1, если $k = l$, и равно 0, если $k \neq l$, Будем считать, что базис $\{d'_1, \ldots, d'_m\}$ выбран именно таким образом. Допустим, что нам задан гомоморфизм η группы $H_1(S \setminus P, Q)$ в аддитивную группу целых чисел. Если $c' = \sum_{k=1}^{m} \eta(d_k) d'_k$, то $\eta(d_k) = \iota(d_k, c')$ $(1 \leqslant k \leqslant m)$, откуда $\eta(c) = \iota(c, c')$ для всех $c \in H_1(S \setminus P, Q)$. Далее, пусть c'_1 — элемент из $H_1(S \setminus Q, P)$, такой, что $\eta(c) = \iota(c, c'_1)$ при всех $c \in H_1(S \setminus P, Q)$. Тогда c'_1 можно представить в виде $\sum_{k=1}^{m} a'_k d'_k$. Так как $a'_k = \iota(d_k, c'_1) = \eta(d_k)$, то $c'_1 = c'$.

Пусть π — гомоморфизм группы $H_1(S \setminus P, Q)$ в аддитивную группу комплексных чисел. Для любого дифференциала ω из класса смежности $\frac{1}{2\pi i} \sum_{k=1}^{m} \pi(d_k) \mathfrak{Q}(d'_k)$ мы имеем $\int_{d_k} \omega = \pi(d_k)$ $(1 \leqslant k \leqslant m)$, откуда $\int_c \omega = \pi(c)$ для всех $c \in H_1(S \setminus P, Q)$. Ясно, что последним условием дифференциал ω определен с точностью до слагаемого из $\mathfrak{F}_Q$. Теорема 11, таким образом, доказана.

Рассмотрим теперь частный случай, когда множества P и Q пустые. В этом случае обе группы $H_1(S \setminus P, Q)$ и $H_1(S \setminus Q, P)$ совпадают с $H_1(S)$, и мы получаем, что $H_1(S)$ есть свободная абелева группа с $2g$ образующими. Таким образом, *топологический род римановой поверхности S поля рода g также равен g*. Далее, для любого базиса

$\{z_1^*, \ldots, z_{2g}^*\}$ группы $H_1(S)$ определитель матрицы $(\iota(z_k^*, z_l^*))$ равен ± 1. Так как эта матрица кососимметрична, то существует целочисленная матрица L, определитель которой равен 1, такая, что

$$L(\iota(z_k^*, z_l^*))L' = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \tag{1}$$

(где L' означает транспонированную матрицу для L, а I_g — единичную матрицу порядка g). Если мы от базиса $\{z_1^*, \ldots, z_{2g}^*\}$ группы $H_1(S)$ перейдем к новому базису $\{z_1, \ldots, z_{2g}\}$ при помощи матрицы L, то в силу (1) будем иметь

$$\iota(z_k, z_l) = \begin{cases} 0, & \text{если } k \leqslant g,\ l \neq k+g; \\ 1, & \text{если } k \leqslant g,\ l = k+g; \\ 0, & \text{если } k > g,\ l \neq k-g; \\ -1, & \text{если } k > g,\ l = k-g. \end{cases} \tag{2}$$

Таким образом, нами доказана

Теорема 12. *Если поле R имеет род g, то первая группа гомологий $H_1(S)$ римановой поверхности S поля R есть свободная абелева группа с $2g$ образующими, и эта группа имеет базис, состоящий из таких элементов $z_1, \ldots, z_{2g}$, индексы пересечений между которыми определяются формулами* (2).

Всякий такой базис называется *каноническим базисом* группы $H_1(S)$.

Вернемся к рассмотрению групп $H_1(S \setminus P, Q)$ и $H_1(S \setminus Q, P)$. Пусть $\{z_1, \ldots, z_{2g}\}$ — канонический базис группы $H_1(S)$. В классе гомологий z_k $(1 \leqslant k \leqslant 2g)$ мы можем найти цикл ζ_k на $S \setminus (P \cup Q)$ (следствие к лемме 4 § 4). Обозначим через u_k и u_k' классы гомологий цикла ζ_k в группах $H_1(S \setminus P, Q)$ и $H_1(S \setminus Q, P)$ соответственно. Для каждой точки $\mathfrak{p} \in P$ определим цикл $\zeta(\mathfrak{p})$ так же, как и при доказательстве теоремы 11. Обозначим через $z(\mathfrak{p})$ класс гомологий цикла $\zeta(\mathfrak{p})$ в $H_1(S \setminus P, Q)$. Тогда, как мы знаем, имеет место равенство $\sum_{\mathfrak{p} \in P} z(\mathfrak{p}) = 0$. Если $Q \neq \varnothing$, то в Q фиксируем точку $\mathfrak{q}_0$; для любой точки $\mathfrak{q} \in Q$, отличной от $\mathfrak{q}_0$, выберем элемент $c^*(\mathfrak{q})$ группы $H_1(S \setminus P, Q)$, для которого

$\partial c^*(\mathfrak{q}) = \mathfrak{q} - \mathfrak{q}_0$. Положим

$$c(\mathfrak{q}) = c^*(\mathfrak{q}) - \sum_{k=1}^{g} \iota\left(c^*(\mathfrak{q}),\ u'_{k+g}\right) u_k + \sum_{k=1}^{g} \iota\left(c^*(\mathfrak{q}),\ u'_k\right) u_{k+g}.$$

Тогда $\partial c(\mathfrak{q}) = \mathfrak{q} - \mathfrak{q}_0$ и, кроме того, $\iota\left(c(\mathfrak{q}),\ u'_k\right) = 0$ при $\leqslant k \leqslant 2g$.

Если $P \neq \varnothing$, то в P фиксируем точку $\mathfrak{p}_0$. Утверждаем теперь, что $2g + p^* + q^* = m$ элементов

$$u_k\ (1 \leqslant k \leqslant 2g);\ z(\mathfrak{p})\ (\mathfrak{p} \in P,\ \mathfrak{p} \neq \mathfrak{p}_0);\ c(\mathfrak{q})\ (\mathfrak{q} \in Q,\ \mathfrak{q} \neq \mathfrak{q}_0) \quad (3)$$

образуют базис группы $H_1(S \setminus P,\ Q)$. Действительно, если мы поменяем ролями P и Q, то аналогичным образом найдем m элементов

$$u'_k\ (1 \leqslant k \leqslant 2g);\ z'(\mathfrak{q})\ (\mathfrak{q} \in Q,\ \mathfrak{q} \neq \mathfrak{q}_0);\ c'_1(\mathfrak{p})\ (\mathfrak{p} \in P,\ \mathfrak{p} \neq \mathfrak{p}_0)$$

группы $H_1(S \setminus Q,\ P)$, для которых $\iota\left(u_k,\ c'_1(\mathfrak{p})\right) = 0$ $(1 \leqslant k \leqslant 2g,\ \mathfrak{p} \in P,\ \mathfrak{p} \neq \mathfrak{p}_0)$ и $\partial c'_1 = \mathfrak{p} - \mathfrak{p}_0$. Для каждой точки $\mathfrak{p} \in P$, отличной от $\mathfrak{p}_0$, положим

$$c'(\mathfrak{p}) = c'_1(\mathfrak{p}) + \sum_{\mathfrak{q} \in Q,\ \mathfrak{q} \neq \mathfrak{q}_0} \iota\left(c(\mathfrak{q}),\ c'_1(\mathfrak{p})\right) z'(\mathfrak{q}).$$

Тогда опять-таки будем иметь $\iota(u_k,\ c'(\mathfrak{p})) = 0$ (так как $z'(\mathfrak{q})$ может быть представлен циклом, гомологичным нулю на S, то $\iota(u_k,\ z'(\mathfrak{q})) = 0$) и $\partial c'(\mathfrak{p}) = \mathfrak{p} - \mathfrak{p}_0$. Кроме того, в силу леммы 1 § 7 имеем $\iota(c(\mathfrak{q}),\ z'(\mathfrak{q})) = -1$ и $\iota(c(\mathfrak{q}),\ z'(\mathfrak{q}')) = 0$ (где $\mathfrak{q}$ и $\mathfrak{q}'$ — различные точки из Q, отличные от $\mathfrak{q}_0$). Отсюда следует, что $\iota(c(\mathfrak{q}),\ c'(\mathfrak{p})) = 0$ при $\mathfrak{p} \in P$, $\mathfrak{p} \neq \mathfrak{p}_0$ и $\mathfrak{q} \in Q$, $\mathfrak{q} \neq \mathfrak{q}_0$. Запишем элементы (3) группы $H_1(S \setminus P,\ Q)$ в виде последовательности $(d_1,\ \ldots,\ d_m)$, а элементы

$$u'_k\ (1 \leqslant k \leqslant g);\ z'(\mathfrak{q})\ (\mathfrak{q} \in Q,\ \mathfrak{q} \neq \mathfrak{q}_0);\ c'(\mathfrak{p})\ (\mathfrak{p} \in P,\ \mathfrak{p} \neq \mathfrak{p}_0) \quad (4)$$

группы $H_1(S \setminus Q,\ P)$ — в виде последовательности $\left(d'_1,\ \ldots,\ d'_m\right)$. Тогда, как легко видеть, для каждого индекса k $(1 \leqslant k \leqslant m)$ существует только один индекс l_k, для которого $\iota\left(d_k,\ d'_{l_k}\right) \neq 0$, при этом $\iota\left(d_k,\ d'_{l_k}\right) = \pm 1$. Таким образом, определитель матрицы $\left(\iota\left(d_k,\ d'_l\right)\right)_{1 \leqslant k,\ l \leqslant m}$ равен ± 1. Отсюда вытекает, что $\{d_1,\ \ldots,\ d_m\}$ и $\left\{d'_1,\ \ldots,\ d'_m\right\}$ являются базисами групп

$H_1(S \setminus P, Q)$ и $H_1(S \setminus Q, P)$ соответственно. Об этих базисах говорят, что они образуют пару *ассоциированных канонических базисов* для наших двух групп.

Обозначим через ω произвольный дифференциал из множества $\mathfrak{E}_{Q,P}$. Тогда класс смежности Ω дифференциала ω по модулю $\mathfrak{F}_P$ может быть записан в виде

$$\Omega = \sum_{k=1}^{2g} \alpha_k \Omega(u_k) + \sum_{\mathfrak{p} \in P, \mathfrak{p} \neq \mathfrak{p}_0} \beta_{\mathfrak{p}} \Omega(z(\mathfrak{p})) + \sum_{\mathfrak{q} \in Q, \mathfrak{q} \neq \mathfrak{q}_0} \gamma_{\mathfrak{q}} \Omega(c(\mathfrak{q})),$$

где α_k, $\beta_{\mathfrak{p}}$ и $\gamma_{\mathfrak{q}}$ — комплексные числа. Аналогично, если $\omega' \in \mathfrak{E}_{P,Q}$, то класс смежности Ω' дифференциала ω' по модулю $\mathfrak{F}_Q$ может быть записан в виде

$$\Omega' = \sum_{k=1}^{2g} \alpha'_k \Omega(u'_k) + \sum_{\mathfrak{q} \in Q, \mathfrak{q} \neq \mathfrak{q}_0} \beta'_{\mathfrak{q}} \Omega(z'(\mathfrak{q})) + \sum_{\mathfrak{p} \in P, \mathfrak{p} \neq \mathfrak{p}_0} \gamma'_{\mathfrak{p}} \Omega(c'(\mathfrak{p})),$$

где α'_k, $\beta'_{\mathfrak{q}}$, $\gamma'_{\mathfrak{p}}$ — комплексные числа. Отсюда следует, что

$$j(\omega, \omega') = j(\Omega, \Omega') = 2\pi i \left(\sum_{k=1}^{g} \alpha_k \alpha'_{k+g} - \sum_{k=g+1}^{2g} \alpha_k \alpha'_{k-g} \right) + \\ + 2\pi i \sum_{\mathfrak{p} \in P, \mathfrak{p} \neq \mathfrak{p}_0} \beta_{\mathfrak{p}} \gamma'_{\mathfrak{p}} - 2\pi i \sum_{\mathfrak{q} \in Q, \mathfrak{q} \neq \mathfrak{q}_0} \gamma_{\mathfrak{q}} \beta'_{\mathfrak{q}}.$$

С другой стороны,

$$2\pi i \alpha_k = j(\Omega, \Omega(u'_{k+g})) = -\int_{u'_{k+g}} \Omega \qquad (1 \leqslant k \leqslant g),$$

$$2\pi i \alpha_k = -j(\Omega, \Omega(u'_{k-g})) = \int_{u'_{k-g}} \Omega \qquad (g+1 \leqslant k \leqslant 2g),$$

и аналогично

$$2\pi i \alpha'_k = -\int_{u_{k+g}} \Omega' \qquad (1 \leqslant k \leqslant g),$$

$$2\pi i \alpha'_k = \int_{u_{k-g}} \Omega' \qquad (g+1 \leqslant k \leqslant 2g).$$

Далее,

$$2\pi i\beta_{\mathfrak{p}} = j(\Omega,\ \Omega(c'(\mathfrak{p}))) = -\int\limits_{c'(\mathfrak{p})} \Omega,$$

$$2\pi i\gamma_{\mathfrak{q}} = -j(\Omega,\ \Omega(z'(\mathfrak{q}))) = \int\limits_{z'(\mathfrak{q})} \Omega = 2\pi i \operatorname{res}_{\mathfrak{q}} \omega,$$

и аналогичные формулы имеют место также для $\beta'_{\mathfrak{q}}$ и $\gamma'_{\mathfrak{p}}$. Мы получили, следовательно, формулу

$$j(\omega,\ \omega') = -\frac{1}{2\pi i}\sum_{k=1}^{g}\left(\int\limits_{u'_{k+g}} \omega \int\limits_{u_k} \omega' - \int\limits_{u'_k} \omega \int\limits_{u_{k+g}} \omega'\right) -$$

$$- \sum_{\mathfrak{p}\in P,\ \mathfrak{p}\neq \mathfrak{p}_0}\left(\int\limits_{c'(\mathfrak{p})} \omega\right)\operatorname{res}_{\mathfrak{p}} \omega' + \sum_{\mathfrak{q}\in Q,\ \mathfrak{q}\neq \mathfrak{q}_0}\left(\int\limits_{c(\mathfrak{q})} \omega'\right)\operatorname{res}_{\mathfrak{q}} \omega. \qquad (5)$$

Применим эту формулу к тому частному случаю, когда ω и ω' — дифференциалы первого рода. Тогда, очевидно, $j(\omega,\ \omega') = \operatorname{res}_{\mathfrak{p}} \omega' = \operatorname{res}_{\mathfrak{q}} \omega = 0$, и мы получаем следующую теорему.

Теорема 13. *Если $\{z_1, \ldots, z_{2g}\}$ — канонический базис одномерной группы гомологий римановой поверхности поля R, а ω и ω' — дифференциалы первого рода поля R, то*

$$\sum_{k=1}^{g}\left(\int\limits_{z_{k+g}} \omega \int\limits_{z_k} \omega' - \int\limits_{z_k} \omega \int\limits_{z_{k+g}} \omega'\right) = 0.$$

Эти соотношения носят название *билинейных равенств Римана.*

В заключение этого параграфа докажем следующую теорему.

Теорема 14. *Двумерная группа гомологий римановой поверхности поля R есть бесконечная циклическая группа.*

Пусть $\mathfrak{p}$ — произвольная точка римановой поверхности S. Обозначим через D замкнутый круг, содержащий точку $\mathfrak{p}$ внутри себя, а через C — его окружность. Выберем 1-цикл γ на C, принадлежащий положительной образующей группы $H_1(C)$. Так как $H_1(D) = 0$, то γ ограничивает 2-цепь δ

на D. С другой стороны, из леммы 4 § 7 следует, что γ ограничивает 2-цепь δ' на $S \setminus \{\mathfrak{p}\}$ (так как, очевидно, $\iota(\gamma, \lambda) = 0$ для любого 1-цикла λ на S). Цепь $\varphi = \delta - \delta'$ является 2-циклом на S. Возьмем целое число $m \neq 0$. Цикл $m\varphi$ гомологичен $m\delta$ по модулю $S \setminus \{\mathfrak{p}\}$, но по лемме 4 § 4 цепь $m\delta$ не гомологична нулю по модулю $S \setminus \{\mathfrak{p}\}$. Отсюда следует, что класс гомологий цикла φ в группе $H_2(S)$ имеет бесконечный порядок. Пусть φ' — произвольный 2-цикл на S. В силу леммы 4 § 4 цикл φ' гомологичен по модулю $S \setminus \{\mathfrak{p}\}$ цепи вида $k\delta$, где k — целое число, а значит, и цепи вида $k\varphi$. Это означает, что цикл $\varphi' - k\varphi$ гомологичен на S 2-циклу на $S \setminus \{\mathfrak{p}\}$. Но из леммы 4 § 7 следует, что каждый 2-цикл на $S \setminus \{\mathfrak{p}\}$ является границей на S. Таким образом, цикл φ' гомологичен на S циклу $k\varphi$, и теорема 14 доказана.

§ 9. Теорема Абеля

Группа дивизоров поля R была определена нами как свободная абелева группа, порожденная точками поля R. Но точки поля R являются в то же время и точками римановой поверхности S. Следовательно, понятие дивизора поля R и понятие 0-цепи на S эквивалентны между собой. Единственная разница между дивизорами и 0-цепями состоит в обозначении: группа дивизоров записывается мультипликативно, а группа 0-цепей — аддитивно. Тем не менее, мы условимся в дальнейшем обозначать одной и той же буквой и 0-цепь и соответствующий ей дивизор.

Так как поверхность S линейно связана, то $H_0(S)$ есть бесконечная циклическая группа, и 0-цепь $\sum_{k=1}^{h} a_k \mathfrak{p}_k$ является границей на S тогда и только тогда, если $\sum_{k=1}^{h} a_k = 0$. Таким образом, 0-цепи, являющиеся границами, соответствуют дивизорам нулевой степени.

Теорема 15 (теорема Абеля). *Для того чтобы дивизор $\mathfrak{d}$ поля R являлся дивизором некоторого элемента из R, необходимо и достаточно, чтобы на римановой поверхности S поля R существовала 1-цепь γ, такая,*

что $\partial\gamma = \mathfrak{d}$ *и* $\int\limits_{\gamma} \eta = 0$ *для каждого дифференциала первого рода* η *поля* R.

Доказательство основывается на следующей лемме.

Лемма 1. *Для того чтобы дифференциал* ω *поля* R *имел вид* $x^{-1}dx$ *при некотором* $x \in R$, *необходимо и достаточно, чтобы* 1) ω *не имел полюсов порядка* > 1 *и* 2) *каждый его период был целым кратным* $2\pi i$.

Докажем сначала необходимость условий. Что касается условия 1), то его необходимость непосредственно следует из леммы 1 § 8 гл. VI. Пусть, далее, V есть открытый круг, не содержащий полюсов дифференциала $x^{-1}dx$; тогда этот дифференциал имеет на V первообразную функцию f. Так как функция x на V не имеет нулей, то функция $x^{-1}e^f$ голоморфна на V. Но $d(x^{-1}e^f) = -x^{-2}e^f dx + x^{-1}e^f df = 0$, поэтому $e^f = Cx$, где C — константа. Пусть σ — произвольный 1-симплекс на V. Если $\partial\sigma = \mathfrak{b} - \mathfrak{a}$, то $\exp\left(\int\limits_{\sigma} x^{-1}dx\right) = x(\mathfrak{b})(x(\mathfrak{a}))^{-1}$. Если 1-цепь γ такова, что каждый входящий в нее симплекс лежит в открытом круге, не содержащем полюсов дифференциала $x^{-1}dx$, и если $\partial\gamma = \sum\limits_{k=1}^{h} a_k \mathfrak{p}_k$, то получаем, что $\exp\left(\int\limits_{\gamma} x^{-1}dx\right) = \prod\limits_{k=1}^{h} (x(\mathfrak{p}_k))^{a_k}$. Пусть теперь ζ — цикл, множество точек которого $|\zeta|$ не содержит полюсов дифференциала $x^{-1}dx$. Тогда при достаточно большом целом $p \geqslant 0$ каждый симплекс, выходящий в $\operatorname{subd}^p \zeta$, лежит в некотором открытом круге, в котором $x^{-1}dx$ не имеет полюсов. Отсюда следует, что $\exp\left(\int\limits_{\zeta} x^{-1}dx\right) = 1$, и, следовательно, $\int\limits_{\zeta} x^{-1}dx$ есть целое кратное $2\pi i$. Этим и доказана необходимость условия 2).

Предположим теперь, что условия 1) и 2) выполнены. Обозначим через P множество полюсов дифференциала ω и зафиксируем некоторую точку $\mathfrak{p}_0$ из $S \setminus P$. Для каждой точки $\mathfrak{p} \in S \setminus P$ выберем 1-цепь $\gamma(\mathfrak{p})$ на $S \setminus P$, для которой

$\partial\gamma(\mathfrak{p}) = \mathfrak{p} - \mathfrak{p}_0$, и положим $g(\mathfrak{p}) = \exp\left(\int\limits_{\gamma(\mathfrak{p})} \omega\right)$. Покажем, что функция g голоморфна на $S \setminus P$. Пусть $\mathfrak{p}$ — точка из $S \setminus P$ и V — открытый круг, содержащийся в $S \setminus P$ и содержащий точку $\mathfrak{p}$. Как мы знаем, дифференциал ω на V имеет первообразную функцию f. Для каждой точки $\mathfrak{q} \in V$ выберем на V такой 1-симплекс $\sigma(\mathfrak{q})$, что $\partial\sigma(\mathfrak{q}) = \mathfrak{q} - \mathfrak{p}$. Так как цепь $\gamma(\mathfrak{q}) - (\gamma(\mathfrak{p}) + \sigma(\mathfrak{q}))$ является циклом на $S \setminus P$, то $\int\limits_{\gamma(\mathfrak{q})} \omega = \int\limits_{\gamma(\mathfrak{p})} \omega + (f(\mathfrak{q}) - f(\mathfrak{p})) + 2\pi i \cdot k$, где k — некоторое целое число, и, следовательно, $g(\mathfrak{q}) = g(\mathfrak{p}) \cdot \exp(f(\mathfrak{q}) - f(\mathfrak{p}))$. Этим и доказано, что функция g голоморфна на V.

Пусть теперь $\mathfrak{p}'$ — точка из P, а значит, $\nu_{\mathfrak{p}'}(\omega) = -1$. Так как логарифмический период дифференциала ω относительно $\mathfrak{p}'$ является целым кратным числа $2\pi i$, то вычет ω в точке $\mathfrak{p}'$ есть целое число m. Выберем в поле R элемент y так, чтобы $\nu_{\mathfrak{p}'}(y) = 1$ и $\nu_{\mathfrak{p}_0}(y) = 0$. Тогда $\nu_{\mathfrak{p}'}(y^{-m}\,dy^m) = -1$ и $\operatorname{res}_{\mathfrak{p}'}(y^{-m}\,dy^m) = m$, а значит, дифференциал $\omega - y^{-m}\,dy^m$ в точке $\mathfrak{p}'$ не имеет полюса. Мы можем считать, что цепь $\gamma(\mathfrak{p})$, с помощью которой определена функция g, выбрана так, что все точки множества $|\gamma(\mathfrak{p})|$, кроме, быть может, точки $\mathfrak{p}$, не являются ни нулями, ни полюсами элемента y. Для точки $\mathfrak{p}'$ существует окрестность, в которой элемент y не имеет нулей и полюсов, кроме самой точки $\mathfrak{p}'$. Для любой точки $\mathfrak{p} \neq \mathfrak{p}'$ из этой окрестности имеем $(y^{-m}g)(\mathfrak{p}) = C\exp\left(\int\limits_{\gamma(\mathfrak{p})} (\omega - y^{-m}\,dy^m)\right)$, где C — константа. Так как дифференциал $\omega - y^{-m}\,dy^m$ голоморфен в $\mathfrak{p}'$, то отсюда следует, что функция g может быть продолжена до функции, мероморфной в $\mathfrak{p}'$. Так как это справедливо для каждой точки $\mathfrak{p}' \in P$, то получаем, что функция g может быть продолжена до функции, мероморфной на всей римановой поверхности S. В силу теоремы 4 § 2 эта функция является элементом поля R, при этом, очевидно, $\omega = g^{-1}\,dg$.

Приступим теперь к доказательству теоремы Абеля. Допустим сначала, что $\mathfrak{d}$ есть дивизор элемента $x \in R$. Тогда отображение $u \to \frac{1}{2\pi i}\int\limits_u x^{-1}\,dx$ является гомоморфизмом группы $H_1(S \setminus |\mathfrak{d}|)$ в аддитивную группу целых чисел.

По теореме 11 § 8 в группе $H_1(S, |\mathfrak{d}|)$ существует такой элемент c, что $\iota(u, c) = \frac{1}{2\pi i}\int\limits_u x^{-1}dx$ для всех $u \in H_1(S \setminus |\mathfrak{d}|)$.

Согласно теореме 9 § 6 элементу c соответствует некоторый класс смежности $\Omega(c)$ пространства тех дифференциалов, вычеты которых во всех точках, не входящих в $\mathfrak{d}$, равны 0, по подпространству точных дифференциалов. Из определения $\Omega(c)$ легко следует, что $x^{-1}dx \in \Omega(c)$. Если $\mathfrak{p}$ — точка, входящая в $\mathfrak{d}$, то вычет дифференциала $x^{-1}dx$ в точке $\mathfrak{p}$ равен, очевидно, $\nu_{\mathfrak{p}}(x)$. С другой стороны, вычет класса смежности $\Omega(c)$ в точке $\mathfrak{p}$ равен коэффициенту, с которым $\mathfrak{p}$ входит в ∂c (теорема 9 § 6). Отсюда следует, что $\partial c = \mathfrak{d}$. Пусть η — произвольный дифференциал первого рода; тогда $\int\limits_c \eta = j(x^{-1}dx, \eta)$. Так как $x^{-1}dx$ не имеет полюсов порядка > 1, а η вообще не имеет полюсов, то, по лемме 1 § 6, $j(x^{-1}dx, \eta) = 0$.

Обратно, пусть для дивизора $\mathfrak{d}$ поля R существует такой элемент $c \in H_1(S, |\mathfrak{d}|)$, что $\partial c = \mathfrak{d}$ и $\int\limits_c \eta = 0$ для каждого дифференциала η первого рода. Пусть ω — дифференциал из класса $\Omega(c)$. Для каждого полюса $\mathfrak{p}$ дифференциала ω выберем элемент $f_{\mathfrak{p}} \in R$ так, чтобы $\nu_{\mathfrak{p}}(\omega - df_{\mathfrak{p}}) \geqslant -1$ (теорема 14 § 8 гл. VI). По определению функции $j_{\mathfrak{p}}$ для любого дифференциала η первого рода мы имеем $j_{\mathfrak{p}}(\omega, \eta) = \operatorname{res}_{\mathfrak{p}} f_{\mathfrak{p}}\eta$. Таким образом, $0 = \int\limits_c \eta = j(\omega, \eta) = \sum\limits_{\mathfrak{p}} \operatorname{res}_{\mathfrak{p}} f_{\mathfrak{p}}\eta$, где $\mathfrak{p}$ пробегает все полюса дифференциала ω. Обозначим через $\mathfrak{f}$ распределение поля R, которое в каждом полюсе $\mathfrak{p}$ дифференциала ω принимает значение $f_{\mathfrak{p}}$, а во всех других точках — значение 0. Тогда $\sum\limits_{\mathfrak{p}} \operatorname{res}_{\mathfrak{p}} f_{\mathfrak{p}}\eta = \sum\limits_{\mathfrak{p}} (f_{\mathfrak{p}}\eta)^{\mathfrak{p}}(1) = \eta(\mathfrak{f})$.

Из теоремы 2 § 5 гл. II следует теперь, что в поле R существует такой элемент f, что $\nu_{\mathfrak{p}}(f - f_{\mathfrak{p}}) \geqslant 0$ для любого полюса $\mathfrak{p}$ дифференциала ω и $\nu_{\mathfrak{q}}(f) \geqslant 0$ для всех других точек $\mathfrak{q}$. Дифференциал $\omega_1 = \omega - df$ является также представителем из класса $\Omega(c)$; кроме того, он не имеет полюсов порядка > 1. Для любого элемента $u \in H_1(S \setminus |\mathfrak{d}|)$

интеграл $\int\limits_u \omega_1 = 2\pi i\iota(u, c)$ есть целое кратное $2\pi i$. В силу леммы 1 отсюда следует, что ω_1 имеет вид $x^{-1}dx$ при некотором $x \in R$. Так как $\partial c = \mathfrak{d}$, то вычет дифференциала $x^{-1}dx$ в точке $\mathfrak{p}$ равен показателю, с которым $\mathfrak{p}$ входит в $\mathfrak{d}$; с другой стороны, этот вычет равен, очевидно, $\nu_{\mathfrak{p}}(x)$. Этим установлено, что $\mathfrak{d}$ является дивизором элемента x, и теорема Абеля доказана.

Пусть g — род поля R и пусть $\{\eta_1, \ldots, \eta_g\}$ — базис пространства дифференциалов первого рода поля R. Если для элемента $z \in H_1(S)$ мы положим $P_i(z) = \int\limits_z \eta_i$ $(1 \leqslant i \leqslant g)$, то отображение $z \to (P_1(z), \ldots, P_g(z))$ будет гомоморфизмом группы $H_1(S)$ в аддитивную группу g-мерного комплексного пространства C^g; обозначим через $\mathfrak{P}$ образ группы $H_1(S)$ при этом отображении.

Для произвольного дивизора $\mathfrak{a}$ поля R нулевой степени мы можем найти такую 1-цепь γ, что $\partial\gamma = \mathfrak{a}$. Положим $B_i(\gamma) = \int\limits_\gamma \eta_i$ $(1 \leqslant i \leqslant g)$ и обозначим через $A(\gamma)$ класс вычетов точки $B(\gamma) = (B_1(\gamma), \ldots, B_g(\gamma)) \in C^g$ по модулю $\mathfrak{P}$. Утверждаем, что $A(\gamma)$ зависит только от $\mathfrak{a}$. В самом деле, если γ' — любая другая 1-цепь, для которой $\partial\gamma' = \mathfrak{a}$, то $\gamma' - \gamma$ есть цикл, а так как $B_i(\gamma') - B_i(\gamma) = \int\limits_{\gamma'-\gamma} \eta_i$, то $B(\gamma') - B(\gamma) \in \mathfrak{P}$, что и доказывает наше утверждение. Вместо $A(\gamma)$ можно писать теперь $A(\mathfrak{a})$.

Если $\mathfrak{a}_1$ и $\mathfrak{a}_2$ — два дивизора степени 0, а γ_1 и γ_2 — цепи, для которых $\partial\gamma_1 = \mathfrak{a}_1$ и $\partial\gamma_2 = \mathfrak{a}_2$, то $\partial(\gamma_1 + \gamma_2) = \mathfrak{a}_1\mathfrak{a}_2$, откуда $A(\mathfrak{a}_1\mathfrak{a}_2) = A(\mathfrak{a}_1) + A(\mathfrak{a}_2)$, т. е. A есть гомоморфизм группы дивизоров нулевой степени в группу $C^g/\mathfrak{P}$. Пусть $\mathfrak{D}_0$ — группа главных дивизоров (т. е. дивизоров элементов поля R). Из теоремы Абеля непосредственно следует, что $A(\mathfrak{a}) = 0$ для всех $\mathfrak{a} \in \mathfrak{D}_0$. Обратно, пусть для дивизора $\mathfrak{a}$ нулевой степени имеем $A(\mathfrak{a}) = 0$. Выберем 1-цепь γ, для которой $\partial\gamma = \mathfrak{a}$. Тогда $B(\gamma) \in \mathfrak{P}$ и на S существует такой цикл ζ, что $B_i(\gamma) = \int\limits_\zeta \eta_i$ $(1 \leqslant i \leqslant g)$. Отсюда следует,

что $\int\limits_{\gamma-\zeta}\eta=0$ для всех дифференциалов η первого рода. Так как, кроме того, $\partial(\gamma-\zeta)=\mathfrak{a}$, то по теореме Абеля $\mathfrak{a}$ есть главный дивизор.

Мы видим, таким образом, что $A(\mathfrak{a})$ зависит только от класса вычетов $\bar{\mathfrak{a}}$ дивизора $\mathfrak{a}$ по модулю $\mathfrak{D}_0$; если мы положим $\bar{A}(\bar{\mathfrak{a}})=A(\mathfrak{a})$, то получим изоморфизм $\bar{A}$ группы $\mathfrak{D}/\mathfrak{D}_0$ (где $\mathfrak{D}$ — группа всех дивизоров нулевой степени) в фактор-группу $C^g/\mathfrak{P}$. Докажем сейчас, что $\bar{A}(\mathfrak{D}/\mathfrak{D}_0)=C^g/\mathfrak{P}$.

Обозначим через Γ подгруппу пространства C^g, содержащую $\mathfrak{P}$ и такую, что $\Gamma/\mathfrak{P}=\bar{A}(\mathfrak{D}/\mathfrak{D}_0)$. Очевидно, что для доказательства нашего утверждения достаточно показать, что Γ содержит некоторую окрестность начала в C^g (ибо отсюда будет следовать, что $\Gamma=C^g$).

Выберем g различных точек $\mathfrak{v}_1, \ldots, \mathfrak{v}_g$ поля R так, чтобы дивизор $\mathfrak{v}_1 \ldots \mathfrak{v}_g$ был неспециален (лемма 4 § 8 гл. VI). Пусть x_i — униформизирующая переменная в точке $\mathfrak{v}_i$ $(1\leqslant i\leqslant g)$. Каждому дифференциалу η первого рода поля R поставим в соответствие точку $\left(\left(\frac{\eta}{dx_1}\right)(\mathfrak{v}_1), \ldots \right.$ $\left.\ldots, \left(\frac{\eta}{dx_g}\right)(\mathfrak{v}_g)\right)\in C^g$; так как дивизор $\mathfrak{v}_1\ldots\mathfrak{v}_g$ неспециален, то на 0 отобразится только нулевой дифференциал, и мы получаем изоморфизм пространства дифференциалов первого рода поля R в C^g. Как нам известно, размерность пространства дифференциалов первого рода равна g, поэтому наш изоморфизм является изоморфизмом „на". Положим $\left(\frac{\eta_i}{dx_j}\right)(\mathfrak{v}_j)=h_{ij}$ $(1\leqslant i, j\leqslant g)$; ясно, что определитель матрицы (h_{ij}) отличен от 0.

Для каждого j $(1\leqslant j\leqslant g)$ через V_j обозначим некоторый открытый x_j-круг с x_j-центром в точке $\mathfrak{v}_j$ и через f_{ij} — первообразную функцию дифференциала η_i на V_j, для которой $f_{ij}(\mathfrak{v}_j)=0$. Если $\mathfrak{p}_j\in V_j$, то полагаем $\mathfrak{C}_i(\mathfrak{p}_1, \ldots, \mathfrak{p}_g)=\sum\limits_{j=1}^{g} f_{ij}(\mathfrak{p}_j)$ $(1\leqslant i\leqslant g)$; точку $(\mathfrak{C}_1(\mathfrak{p}_1, \ldots, \mathfrak{p}_g), \ldots$ $\ldots, \mathfrak{C}_g(\mathfrak{p}_1, \ldots, \mathfrak{p}_g))\in C^g$ обозначим через $\mathfrak{C}(\mathfrak{p}_1, \ldots, \mathfrak{p}_g)$. Пусть еще $\sigma_j(\mathfrak{p}_j)$ есть 1-симплекс на V_j, такой, что $\partial\sigma_j(\mathfrak{p}_j)=\mathfrak{p}_j-\mathfrak{v}_j$,

Положим $\gamma(\mathfrak{p}_1, \ldots, \mathfrak{p}_g) = \sum_{j=1}^{g} \sigma_j(\mathfrak{p}_j)$; тогда $\partial\gamma(\mathfrak{p}_1, \ldots, \mathfrak{p}_g) = (\mathfrak{p}_1 \ldots \mathfrak{p}_g)(\mathfrak{v}_1 \ldots \mathfrak{v}_g)^{-1}$ и $\mathfrak{C}(\mathfrak{p}_1, \ldots, \mathfrak{p}_g) = B(\gamma(\mathfrak{p}_1, \ldots, \mathfrak{p}_g))$, ибо $\mathfrak{C}_i(\mathfrak{p}_1, \ldots, \mathfrak{p}_g) = \int\limits_{\gamma(\mathfrak{p}_1, \ldots, \mathfrak{p}_g)} \eta_i$. Таким образом, наше утверждение о том, что Γ содержит окрестность начала в C^g, будет доказано, если мы покажем, что $\mathfrak{C}$ отображает $\prod_{j=1}^{g} V_j$ на окрестность начала в C^g. Функция $\mathfrak{C}_i(\mathfrak{p}_1, \ldots, \mathfrak{p}_g)$ может быть записана в виде $\mathfrak{C}_i^*(x_1(\mathfrak{p}_1), \ldots, x_g(\mathfrak{p}_g))$, где $\mathfrak{C}_i^*$ — функция от g переменных, голоморфная на полицилиндре $\prod_{j=1}^{g} x_j(V_j)$. В силу теоремы о неявных функциях для доказательства нашего утверждения достаточно теперь показать, что функциональный определитель для функций $\mathfrak{C}_1^*, \ldots, \mathfrak{C}_g^*$ отличен от нуля в начале. Так как f_{ij} есть первообразная функция для η_i, то $\frac{df_{ij}}{dx_j}(\mathfrak{v}_j) = \frac{\eta_i}{dx_j}(\mathfrak{v}_j) = h_{ij}$, откуда $\frac{\partial \mathfrak{C}_i^*}{\partial x_j}(0, \ldots, 0) = h_{ij}$, а нам известно, что определитель матрицы (h_{ij}) отличен от 0.

Таким образом, мы доказали, что группа классов дивизоров нулевой степени поля R изоморфна фактор-группе $C^g/\mathfrak{P}$. Займемся теперь более детальным изучением структуры группы $\mathfrak{P}$.

Сохраняя введенные выше обозначения, заметим, что определитель матрицы $\left(\frac{\eta_i}{dx_j}(\mathfrak{p}_j)\right)$ отличен от 0, если $(\mathfrak{p}_1, \ldots, \mathfrak{p}_g)$ меняется в некоторой окрестности N точки $(\mathfrak{v}_1, \ldots, \mathfrak{v}_g)$ из произведения $\prod_{j=1}^{g} V_j$. Это означает, что если $(\mathfrak{p}_1, \ldots, \mathfrak{p}_g) \in N$, то линейная комбинация дифференциалов $\eta_1, \ldots, \eta_g$ с постоянными коэффициентами, не равными 0 одновременно, не может иметь все точки $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ в качестве своих нулей, т. е. дивизор $\mathfrak{p}_1 \ldots \mathfrak{p}_g$ неспециален. Применяя теорему Римана — Роха, получаем, что $l((\mathfrak{p}_1 \ldots \mathfrak{p}_g)^{-1}) = 1$, т. е. только константы делятся на $(\mathfrak{p}_1 \ldots \mathfrak{p}_g)^{-1}$. Этим доказано,

что $(\mathfrak{v}_1 \ldots \mathfrak{v}_g)(\mathfrak{p}_1 \ldots \mathfrak{p}_g)^{-1}$ является главным дивизором только в том случае, если $\mathfrak{v}_1 \ldots \mathfrak{v}_g = \mathfrak{p}_1 \ldots \mathfrak{p}_g$. Так как $\mathfrak{C}$ отображает N на окрестность начала в C^g, то отсюда следует, что существует окрестность начала в C^g, не содержащая точек из $\mathfrak{P}$, кроме точки $(0, \ldots, 0)$. Таким образом, $\mathfrak{P}$ есть дискретная подгруппа пространства C^g, а следовательно, она является свободной абелевой группой с m образующими, где $m \leqslant 2g$. Покажем, что на самом деле m равно $2g$.

Пусть $\{z_1, \ldots, z_{2g}\}$ — базис группы $H_1(S)$. Точки $P(z_k) = (P_1(z_k), \ldots, P_g(z_k))$ $(1 \leqslant k \leqslant 2g)$ образуют систему образующих группы $\mathfrak{P}$, поэтому наше утверждение будет доказано, если мы покажем, что равенство $\sum_{k=1}^{2g} a_k P(z_k) = 0$, где $a_1, \ldots, a_{2g}$ — целые числа, возможно только при $a_k = 0$ $(1 \leqslant k \leqslant 2g)$. Если мы положим $z = \sum_{k=1}^{2g} a_k z_k$, то $\int_z \eta = 0$ для любого дифференциала η первого рода. Наше утверждение будет следовать теперь из следующей леммы.

Лемма 2. *Пусть z — одномерный класс гомологий на римановой поверхности S поля R. Если для любого дифференциала первого рода η имеем $\int_z \eta = 0$, то $z = 0$.*

Обозначим через $\mathfrak{D}$ пространство дифференциалов второго рода поля R, через $\mathfrak{D}_1$ — пространство дифференциалов первого рода и через $\mathfrak{F}$ — пространство точных дифференциалов. Пусть $\Omega(z)$ — элемент из $\mathfrak{D}/\mathfrak{F}$, соответствующий классу гомологий z согласно теореме 9 § 6, и пусть ω — дифференциал из класса смежности $\Omega(z)$. Тогда для любого дифференциала первого рода η будем иметь $j(\omega, \eta) = \int_z \eta = 0$. С другой стороны, $\mathfrak{D}_1 \cap \mathfrak{F} = \{0\}$, ибо каждый полюс элемента $x \in R$ является также полюсом дифференциала dx. Отсюда следует, что размерность пространства $(\mathfrak{D}_1 + \mathfrak{F})/\mathfrak{F}$ равна g. Как мы знаем, функция j определяет невырожденную билинейную функцию на $(\mathfrak{D}/\mathfrak{F}) \times (\mathfrak{D}/\mathfrak{F})$. Следовательно, дифференциалы $\theta \in \mathfrak{D}$, удовлетворяющие условию $j(\theta, \eta) = 0$ при всех $\eta \in \mathfrak{D}_1$, образуют подпростран-

ство $\mathfrak{D}_2$ пространства $\mathfrak{D}$, для которого $\dim(\mathfrak{D}_2/\mathfrak{F})=\dim(\mathfrak{D}/\mathfrak{F})-\dim\mathfrak{D}_1=2g-g=g$. Но $\mathfrak{D}_2$, очевидно, содержит $\mathfrak{D}_1$, поэтому $\mathfrak{D}_2=\mathfrak{D}_1+\mathfrak{F}$. Таким образом, можно считать, что выбранный выше дифференциал ω содержится в $\mathfrak{D}_1$. Так как $\omega\in\Omega(z)$, то все его периоды являются целыми кратными числа $2\pi i$, а так как к тому же он первого рода, то, в силу леммы 1, $\omega=x^{-1}dx$ при некотором $x\in R$. Но тогда x не может иметь ни нулей, ни полюсов, а потому является константой, откуда $\omega=0$ и $z=0$.

Таким образом, мы доказали, что $\mathfrak{P}$ есть дискретная подгруппа пространства C^g, имеющая $2g$ независимых образующих. Но тогда, как известно, группа $C^g/\mathfrak{P}$ изоморфна $2g$-мерной торовидной группе. Итак, нами доказана

Теорема 16. *Если род поля R равен g, то группа классов дивизоров нулевой степени поля R изоморфна $2g$-мерной торовидной группе.*

Следствие. *Если род поля R равен g, то число классов дивизоров нулевой степени, порядок которых конечен и является делителем целого числа $n>0$, равно n^{2g}.*

§ 10. Поля рода 1

В этом параграфе будем предполагать, что род нашего поля R равен 1.

Обозначим через $\mathfrak{D}$ группу дивизоров нулевой степени поля R и через $\mathfrak{D}_0$ — группу главных дивизоров. Покажем, что элементы факторов-группы $\mathfrak{D}/\mathfrak{D}_0$ находятся во взаимно однозначном соответствии с точками римановой поверхности S поля R. Пусть $\mathfrak{p}_0$ — произвольная фиксированная точка поверхности S; для точки $\mathfrak{p}\in S$ через $h(\mathfrak{p})$ обозначим класс смежности дивизора $\mathfrak{p}\mathfrak{p}_0^{-1}$ по модулю $\mathfrak{D}_0$. Утверждаем, что $h(\mathfrak{p})\neq h(\mathfrak{q})$, если только $\mathfrak{p}\neq\mathfrak{q}$. Действительно, дивизор любого, отличного от 0 дифференциала поля R имеет степень $2\cdot 1-2=0$, поэтому только нулевой дифференциал делится на $\mathfrak{p}$. Применяя теорему Римана — Роха, получаем, что $l(\mathfrak{p}^{-1})=1$, т. е. среди элементов поля R только константы делятся на $\mathfrak{p}^{-1}$. Таким образом, если $\mathfrak{q}\neq\mathfrak{p}$, то $\mathfrak{q}\mathfrak{p}^{-1}$ не является главным дивизором, откуда $h(\mathfrak{p})\neq h(\mathfrak{q})$. Далее, в каждом классе дивизоров нулевой степени содержится представитель вида $h(\mathfrak{p})$. В самом деле, пусть $\mathfrak{a}$ —

произвольный дивизор из рассматриваемого класса. Так как $d(\mathfrak{a})=0$, то $l(\mathfrak{a}^{-1}\mathfrak{p}_0^{-1})\geqslant 1$; выберем в поле R элемент $x\neq 0$, делящийся на $\mathfrak{a}^{-1}\mathfrak{p}_0^{-1}$. Степень дивизора $\mathfrak{d}(x)$ элемента x равна 0, поэтому $\mathfrak{d}(x)=\mathfrak{a}^{-1}\mathfrak{p}_0^{-1}\mathfrak{p}$, где $\mathfrak{p}$ — точка поля R. Отсюда следует что дивизоры $\mathfrak{a}$ и $\mathfrak{p}\mathfrak{p}_0^{-1}$ принадлежат одному и тому же классу.

Обозначим через η базисный элемент пространства дифференциалов первого рода поля R и через $\{z_1, z_2\}$ — базис группы $H_1(S)$. Положим $\int\limits_{z_1}\eta=\alpha_1$ и $\int\limits_{z_2}\eta=\alpha_2$. Тогда, как мы знаем, числа α_1 и α_2 порождают дискретную подгруппу $\mathfrak{P}$ аддитивной группы C комплексных чисел (см. § 9). Для каждой точки $\mathfrak{p}\in S$ выберем на S 1-цепь $\gamma(\mathfrak{p})$, для которой $\partial\gamma(\mathfrak{p})=\mathfrak{p}-\mathfrak{p}_0$. Через $A(\mathfrak{p})$ обозначим класс вычетов числа $\int\limits_{\gamma(\mathfrak{p})}\eta$ по модулю $\mathfrak{P}$ (в § 9 установлено, что этот класс вычетов зависит только от $\mathfrak{p}$). В силу результатов § 9 получаем, что отображение $\mathfrak{p}\to A(\mathfrak{p})$ отображает S взаимно однозначно на $C/\mathfrak{P}$. Группа $C/\mathfrak{P}$ имеет естественную топологию как фактор-группа группы C. Покажем, что отображение $\mathfrak{p}\to A(\mathfrak{p})$ непрерывно. Пусть $\mathfrak{p}$ — точка из S и V — открытый круг, содержащий $\mathfrak{p}$; обозначим через f первообразную функцию дифференциала η на V, для которой $f(\mathfrak{p})=0$. Для каждой точки $\mathfrak{q}\in V$ выберем 1-симплекс $\sigma(\mathfrak{q})$ на V так, чтобы $\partial\sigma(\mathfrak{q})=\mathfrak{q}-\mathfrak{p}$. Цепь $\gamma(\mathfrak{p})+\sigma(\mathfrak{q})$ отличается от $\gamma(\mathfrak{q})$ на цикл ξ, и $\int\limits_{\xi}\eta\in\mathfrak{P}$. Таким образом, $A(\mathfrak{q})$ является суммой $A(\mathfrak{p})$ и класса вычетов числа $\int\limits_{\sigma(\mathfrak{q})}\eta=f(\mathfrak{q})$ по модулю $\mathfrak{P}$, что и доказывает непрерывность отображения A на V. Так как поверхность S компактна, то отсюда следует, что она гомеоморфна фактор-группе $C/\mathfrak{P}$, т. е. 2-мерному тору.

Пусть теперь x — элемент поля R. Определим на C функцию x^*, полагая $x^*(u)=x(\mathfrak{p}(u))$ $(u\in C)$, где $\mathfrak{p}(u)$ — точка поверхности S, которая при отображении A соответствует классу вычетов числа u по модулю $\mathfrak{P}$. Утверждаем, что x^* — мероморфная функция. Возьмем произвольное комплексное число u и положим $\mathfrak{p}=\mathfrak{p}(u)$. Определим V

и f так же как и выше. Выберем униформизирующую переменную y в точке $\mathfrak{p}$ так, чтобы круг V являлся y-кругом. Для точек $\mathfrak{q} \in V$ положим $f(\mathfrak{q}) = f^*(y(\mathfrak{q}))$, где f^* — функция, голоморфная на $y(V)$. Так как η на S не имеет нулей и $df = \eta$, то производная от функции f^* нигде на $y(V)$ не обращается в 0. Отсюда следует, что функция $y(\mathfrak{q})$ может быть представлена в виде голоморфной функции от $f(\mathfrak{q})$ для всех $\mathfrak{q}$ из надлежащей окрестности точки $\mathfrak{p}$. Так как $f(\mathfrak{p}(v)) = v - u$, если только модуль $|v - u|$ достаточно мал, то $y(\mathfrak{p}(v))$ является голоморфной функцией от v на некоторой окрестности числа u. С другой стороны, $x(\mathfrak{q})$ можно представить (для $\mathfrak{q} \in V$) как мероморфную функцию от $y(\mathfrak{q})$, поэтому функция x^* мероморфна в точке u.

Далее, очевидно, что α_1 и α_2 являются периодами для функции x^*. Следовательно, x^* есть эллиптическая функция с периодами α_1 и α_2 (см. § 8 гл. II). Обратно, пусть g^* — произвольная эллиптическая функция с периодами α_1 и α_2. Тогда $g^*(u)$, где $u \in C$, зависит только от класса вычетов числа u по модулю $\mathfrak{P}$. Значит, существует функция g, определенная на S, такая, что $g(\mathfrak{p}(u)) = g^*(u)$ для всех $u \in C$. Рассуждая как и выше, легко устанавливаем, что функция g мероморфна всюду, а следовательно, она является элементом поля R (теорема 4 § 2). Итак, доказана следующая теорема.

Теорема 17. *Если род поля R равен 1, то существуют такие комплексные числа α_1 и α_2, для которых поле R изоморфно полю эллиптических функций с периодами α_1 и α_2.*

Обратно, пусть α_1 и α_2 — комплексные числа, отношение которых невещественно, и пусть R — поле эллиптических функций с периодами α_1 и α_2. Тогда, как мы знаем (§ 8 гл. II), $R = C\langle f, f'\rangle$, где f — эллиптическая функция, имеющая полюса только в точках группы $\mathfrak{P}$, порожденной α_1 и α_2, причем $u^2 f(u)$ принимает при $u = 0$ значение 1, а f' — производная от f. Легко видеть, что $\eta = f'^{-1} d_f$ будет дифференциалом первого рода поля R. Риманова поверхность S поля R может быть отождествлена с $C/\mathfrak{P}$. Для $u \in C$ выберем на C 1-цепь $\gamma^*(u)$, для которой $\partial\gamma^*(u) = \{u\} - \{0\}$, и обозначим через $\gamma(u)$ цепь на S, являющуюся образом цепи $\gamma^*(u)$ при естественном отображении C

в S. Так как $df = f'\,du$, то $\int\limits_{\gamma(u)} \eta = u$. Отсюда следует, что группа периодов дифференциала η порождена числами α_1 и α_2. Отличные от 0 дифференциалы первого рода поля R имеют вид $c\eta$, где $c \in C$, $c \neq 0$. С другой стороны, группа периодов дифференциала $c\eta$ есть группа, порожденная числами $c\alpha_1$ и $c\alpha_2$. Таким образом, поле эллиптических функций с периодами β_1 и β_2 изоморфно полю эллиптических функций с периодами α_1 и α_2 тогда и только тогда, когда существует такое комплексное число c, что группа, порожденная β_1 и β_2, совпадает с группой, порожденной $c\alpha_1$ и $c\alpha_2$. Последнее имеет место при условии, что $\beta_1 = c\,(k\alpha_1 + l\alpha_2)$ и $\beta_2 = c\,(m\alpha_1 + n\alpha_2)$, где k, l, m, n — целые числа такие, что $kn - lm = \pm 1$. Можно также сказать, что $\tau = \frac{\alpha_2}{\alpha_1}$ и $\tau' = \frac{\beta_2}{\beta_1}$ должны быть связаны соотношением вида

$$\tau' = \frac{m + n\tau}{k + l\tau},$$

где k, l, m, n — целые числа, удовлетворяющие условию $kn - lm = \pm 1$. Этим и объясняются связи, существующие между теорией эллиптических функций и теорией модулярных функций.

§ 11. Риманова поверхность как аналитическое многообразие

Относительно определения и элементарных свойств аналитических многообразий отсылаем читателя к книге автора „Теория групп Ли. I", гл. III и V.

В настоящем параграфе мы покажем, что риманову поверхность S поля R можно превратить в аналитическое многообразие. Пусть $\mathfrak{p}$ — произвольная точка поверхности S и пусть x — униформизирующая переменная в точке $\mathfrak{p}$. Если $\mathfrak{q}$ не является полюсом функции x, то через $x_1(\mathfrak{q})$ и $x_2(\mathfrak{q})$ мы обозначим вещественную и мнимую части значения $x(\mathfrak{q})$ [1]). Функции x_1 и x_2 имеют вещественные значения и определены

---

[1]) Под мнимой частью комплексного числа $a + bi$ понимается коэффициент b при i. (*Прим. перев.*)

на некоторой окрестности точки $\mathfrak{p}$. Обозначим через $\mathcal{A}_x(\mathfrak{p})$ класс вещественных функций, определенных на окрестностях точки $\mathfrak{p} \in S$ и аналитически зависящих от x_1 и x_2 вблизи $\mathfrak{p}$. Класс $\mathcal{A}_x(\mathfrak{p})$ не зависит от выбора x. Действительно, пусть y — любая другая униформизирующая переменная в точке $\mathfrak{p}$, а y_1 и y_2 — вещественная и мнимая части y. В некоторой окрестности точки $\mathfrak{p}$ переменная y может быть представлена в виде $F(x)$, где функция F определена и голоморфна в некоторой окрестности начала в комплексной плоскости. Отсюда легко следует, что y_1 и y_2 принадлежат классу $\mathcal{A}_x(\mathfrak{p})$, откуда $\mathcal{A}_y(\mathfrak{p}) \subset \mathcal{A}_x(\mathfrak{p})$. Аналогично имеем также $\mathcal{A}_x(\mathfrak{p}) \subset \mathcal{A}_y(\mathfrak{p})$, а значит, $\mathcal{A}_x(\mathfrak{p}) = \mathcal{A}_y(\mathfrak{p})$. В дальнейшем класс $\mathcal{A}_x(\mathfrak{p})$ будем обозначать через $\mathcal{A}(\mathfrak{p})$.

Пусть V — открытый x-круг с x-центром в точке $\mathfrak{p}$. Ясно, что V содержит множество V_1, которое при соответствии $\mathfrak{q} \to (x_1(\mathfrak{q}), x_2(\mathfrak{q}))$ отображается топологически на квадрат с центром в начале в 2-мерном вещественном декартовом пространстве. Если $\mathfrak{q} \in V_1$, то $x - x(\mathfrak{q})$ является униформизирующей переменной в точке $\mathfrak{q}$. Положим $a_i = x_i(\mathfrak{q})$ $(i = 1, 2)$. Тогда $\mathcal{A}(\mathfrak{q})$ является классом функций f, определенных на окрестностях точки $\mathfrak{q}$ и аналитически зависящих от $x_1 - a_1$ и $x_2 - a_2$ вблизи $\mathfrak{q}$. Последнее условие эквивалентно тому, что функции f аналитически зависят от x_1 и x_2 вблизи $\mathfrak{q}$. Отсюда следует, что сопоставление $\mathfrak{p} \to \mathcal{A}(\mathfrak{p})$ превращает поверхность S в аналитическое многообразие размерности 2.

Будем говорить, что комплексная функция f, определенная в окрестности точки $\mathfrak{p} \in S$, *аналитична вблизи* $\mathfrak{p}$, если ее вещественная и мнимая части аналитичны вблизи $\mathfrak{p}$. Далее, будем говорить, что функция f, определенная в открытом подмножестве U поверхности S, аналитична в U, если она аналитична в каждой точке из U. Последнее понятие не следует смешивать с определенным в § 2 понятием голоморфной в U функции: голоморфная в U функция всегда аналитична, однако обратное, вообще говоря, неверно.

Пусть $L(\mathfrak{p})$ — касательное векторное пространство к поверхности S в точке $\mathfrak{p}$. В „Теории групп Ли. I" дифференциал $\omega_{\mathfrak{p}}$ в точке $\mathfrak{p}$ был определен как вещественная линейная функция на пространстве $L(\mathfrak{p})$; далее, было доказано, что все дифференциалы в точке $\mathfrak{p}$ образуют векторное пространство размерности 2 над полем вещественных чисел. Если x есть униформизирующая переменная в точке $\mathfrak{p}$, то

дифференциалы в $\mathfrak{p}$ функций x_1 и x_2 (вещественной и мнимой частей функции x) образуют базис пространства дифференциалов в точке $\mathfrak{p}$. Сейчас мы слегка обобщим это понятие. Именно под дифференциалом в точке $\mathfrak{p}$ будем понимать *любую комплексную* линейную функцию на $L(\mathfrak{p})$. Таким образом, теперь дифференциалы в $\mathfrak{p}$ образуют векторное пространство размерности 2 над полем комплексных чисел, и в этом пространстве имеется базис, состоящий из дифференциалов в $\mathfrak{p}$ функций x_1 и x_2. Если f есть комплексная функция, аналитичная в точке $\mathfrak{p}$, то под ее дифференциалом в $\mathfrak{p}$ будем понимать дифференциал $(df_1)_{\mathfrak{p}}+i(df_2)_{\mathfrak{p}}$, где f_1 и f_2 — вещественная и мнимая части функции f.

Пусть U — открытое подмножество поверхности S. Под *дифференциальной формой* степени 1 на U мы понимаем отображение $\mathfrak{p}\to\omega_{\mathfrak{p}}$, которое каждой точке $\mathfrak{p}\in U$ сопоставляет элемент $\omega_{\mathfrak{p}}$ из пространства дифференциалов в $\mathfrak{p}$. Введенное понятие отличается (хотя и связано с ним) от понятия голоморфного дифференциала, определенного в § 4. Пусть ω — голоморфный дифференциал на U. Если x есть униформизирующая переменная в точке $\mathfrak{p}\in U$, то $\omega=f\,dx$, где функция f голоморфна в $\mathfrak{p}$. Обозначим через x_1 и x_2 вещественную и мнимую части функции x. Выражение $f(\mathfrak{p})((dx_1)_{\mathfrak{p}}+i(dx_2)_{\mathfrak{p}})$ представляет собой элемент $\omega_{\mathfrak{p}}$ пространства дифференциалов в точке $\mathfrak{p}$. Этот элемент не зависит от x. Действительно, пусть y — любая другая униформизирующая переменная в $\mathfrak{p}$. Тогда в некоторой окрестности точки $\mathfrak{p}$ функция y может быть представлена в виде $F(x)$, где F — функция, определенная и голоморфная в окрестности начала комплексной плоскости. Если через α мы обозначим значение производной от F в точке 0, то будем иметь $\left(\frac{dy}{dx}\right)(\mathfrak{p})=\alpha$. Если теперь y_1 и y_2 — вещественная и мнимая части функции y, то $(dy_1)_{\mathfrak{p}}+i(dy_2)_{\mathfrak{p}}=\alpha((dx_1)_{\mathfrak{p}}+i(dx_2)_{\mathfrak{p}})$. Полагая $\omega=g\,dy$, мы имеем $f=g\,\frac{dy}{dx}$, откуда $f(\mathfrak{p})((dx_1)_{\mathfrak{p}}+i(dx_2)_{\mathfrak{p}})=g(\mathfrak{p})\alpha((dx_1)_{\mathfrak{p}}+i(dx_2)_{\mathfrak{p}})=g(\mathfrak{p})((dy_1)_{\mathfrak{p}}+i(dy_2)_{\mathfrak{p}})$, что и доказывает наше утверждение. Отображение $\mathfrak{p}\to\omega_{\mathfrak{p}}$ есть дифференциальная форма на U, которая будет обозначаться нами тем же символом ω, что и заданный голоморфный дифференциал. В частности, для произвольной функции h, голоморфной на U, dh будет обозначать как

голоморфный дифференциал на U, так и дифференциальную форму степени 1 на U.

В „Теории групп Ли. I“ было определено внешнее произведение $\omega \square \omega'$ двух дифференциальных форм степени 1 на открытом множестве U; это понятие без труда переносится и на случай комплексных дифференциальных форм. Полезно заметить, что $\omega \square \omega' = 0$, если только ω и ω' голоморфны (ибо в этом случае для любой точки $\mathfrak{p} \in U$ имеем $\omega_{\mathfrak{p}} = \alpha (dx)_{\mathfrak{p}}$, $\omega'_{\mathfrak{p}} = \alpha' (dx)_{\mathfrak{p}}$, где α и α' — комплексные числа, а x — униформизирующая переменная в точке $\mathfrak{p}$, откуда следует, что $\omega_{\mathfrak{p}} \square \omega'_{\mathfrak{p}} = \alpha\alpha' (dx)_{\mathfrak{p}} \square (dx)_{\mathfrak{p}} = 0$).

Пусть ω — дифференциальная форма степени 1 на открытом множестве U, $\mathfrak{p}$ — точка из U, x — униформизирующая переменная в $\mathfrak{p}$, x_1 и x_2 — вещественная и мнимая части функции x. Тогда для точки $\mathfrak{p}$ существует такая окрестность N, что для $\mathfrak{q} \in N$ имеем $\omega_{\mathfrak{q}} = f_1(x_1(\mathfrak{q}), x_2(\mathfrak{q}))(dx_1)_{\mathfrak{q}} + f_2(x_1(\mathfrak{q}), x_2(\mathfrak{q}))(dx_2)_{\mathfrak{q}}$, где f_1 и f_2 — комплексные функции, определенные в окрестности начала комплексной плоскости. Если f_1 и f_2 принадлежат классу C_k в начале (т. е. имеют непрерывные частные производные порядка k в окрестности начала), то говорят, что ω принадлежит *классу C_k в точке* $\mathfrak{p}$; если f_1 и f_2 являются аналитическими функциями от вещественных переменных x_1 и x_2 в окрестности начала, то дифференциальная форма ω называется *аналитической в точке* $\mathfrak{p}$. Легко видеть, что эти определения не зависят от выбора униформизирующей переменной x (если вместо x взять другую униформизирующую переменную в точке $\mathfrak{p}$, то f_1 и f_2 заменятся функциями, которые будут линейными комбинациями f_1 и f_2, причем коэффициенты этих линейных комбинаций будут аналитическими функциями в окрестности начала). Если дифференциальная форма ω принадлежит классу C_k (или аналитична) во всех точках $\mathfrak{p} \in U$, то говорят, что ω принадлежит классу C_k (или аналитична) на U.

В „Теории групп Ли. I“ был определен дифференциал $d\omega$ вещественной аналитической дифференциальной формы ω. Определение без труда переносится на случай комплексных дифференциальных форм, принадлежащих классу C_1. Если функция f и дифференциальная форма ω принадлежат классу C_1, то $d(f\omega) = df \square \omega + f\,d\omega$. Если дифференциальная форма ω принадлежит классу C_2, то $d\omega$ принадлежит классу C_1 и $dd\omega = 0$. Если ω есть голоморфный дифференциал на открытом

множестве U, то $d\omega = 0$. Действительно, пусть p — произвольная точка из U и пусть V — открытый круг, содержащий p и содержащийся в U. На V дифференциал ω имеет первообразную функцию f, поэтому на V имеем $d\omega = ddf = 0$.

Одномерный симплекс σ на S называется *дифференцируемым*, если отображение $t \to \sigma(1-t, t)$ замкнутого интервала $[0, 1]$ в S может быть продолжено до отображения $t \to \sigma^*(t)$ некоторого открытого интервала $(-\alpha, 1+\beta)$ (где $\alpha > 0$, $\beta > 0$) в S, которое всюду принадлежит классу C_1 (т. е. для любой функции f, аналитичной в точке $\sigma^*(t_0)$, $-\alpha < t_0 < 1+\beta$, функция $f(\sigma^*(t))$ имеет непрерывную производную в некоторой окрестности t_0). В этом случае отображение $f \to \left(\frac{df(\sigma^*(t))}{dt}\right)_{t=t_0}$ класса аналитических функций в $\sigma^*(t_0)$ в поле вещественных чисел является касательным вектором L_{t_0} в $\sigma^*(t_0)$, и этот касательный вектор зависит только от σ и $t_0 \in [0, 1]$ (а не от продолжения σ^*); L_{t_0} называется *касательным вектором к σ при значении параметра t_0*. Если отрытое множество U содержит $|\sigma|$ и если голоморфный на U дифференциал ω имеет на U первообразную функцию f, то, как мы знаем,

$$\int_\sigma \omega = f(\sigma^*(1)) - f(\sigma^*(0))$$

(лемма 2 § 4), что равно

$$\int_0^1 \frac{df(\sigma^*(t))}{dt}\, dt = \int_0^1 \omega_{\sigma^*(t)}(L_t)\, dt.$$

Естественно поэтому ввести следующее определение: если дифференциальная форма ω принадлежит классу C_0 на некотором открытом множестве, содержащем $|\sigma|$, то число $\int_0^1 \omega_{\sigma^*(t)}(L_t)\, dt$ называется *интегралом от ω по σ*.

Одномерная цепь γ на S называется дифференцируемой, если каждый симплекс, входящий в γ, дифференцируем. Пусть $\gamma = \sum_{k=1}^{h} a_k \sigma_k$, где $\sigma_1, \ldots, \sigma_h$ — симплексы, входящие в γ, и пусть ω — дифференциальная форма, определенная на некотором открытом множестве, содержащем $|\gamma|$, и принадлежащая классу C_0 на этом множестве. Под интегралом от

дифференциальной формы ω по 1-цепи γ понимается число $\int\limits_{\gamma} \omega = \sum\limits_{k=1}^{h} a_k \int\limits_{\sigma_k} \omega$. Легко видеть, что вместе с γ цепь $\operatorname{subd} \gamma$ также дифференцируема и что $\int\limits_{\operatorname{subd}\gamma} \omega = \int\limits_{\gamma} \omega$.

Докажем теперь, что аналитическое многообразие S ориентируемо (см. „Теория групп Ли. I"), при этом мы выделим некоторую определенную ориентацию S. Обозначим через $\mathfrak{D}_{\mathfrak{p}}$ пространство комплексных дифференциалов в точке $\mathfrak{p} \in S$. Так же как и в случае вещественных дифференциалов, мы вводим грассмановскую алгебру $\mathfrak{G}_{\mathfrak{p}}$ над пространством $\mathfrak{D}_{\mathfrak{p}}$. В этой алгебре над полем комплексных чисел однородными элементами степени 2 являются косо-симметричные комплексные билинейные функции на касательном пространстве $L(\mathfrak{p})$. Они образуют векторное пространство $\mathfrak{D}_{\mathfrak{p}}^2$ размерности 1 над полем комплексных чисел. Каждой паре (ω, ω') элементов из $\mathfrak{D}_{\mathfrak{p}}$ соответствует элемент $\omega \square \omega'$ из $\mathfrak{D}_{\mathfrak{p}}^2$ (внешнее произведение этих элементов). Элементы из $\mathfrak{D}_{\mathfrak{p}}^2$, являющиеся вещественными билинейными функциями на $L(\mathfrak{p})$, называются вещественными; они являются однородными элементами степени 2 грассмановской алгебры над пространством вещественных дифференциалов. Пусть теперь x — униформизирующая переменная в точке $\mathfrak{p}$, а x_1 и x_2 — вещественная и мнимая части функции x. Тогда $(dx_1)_{\mathfrak{p}}$ и $(dx_2)_{\mathfrak{p}}$ образуют, как мы знаем, базис пространства $\mathfrak{D}_{\mathfrak{p}}$, а $(dx_1)_{\mathfrak{p}} \square (dx_2)_{\mathfrak{p}}$ является базисным элементом пространства вещественных элементов из $\mathfrak{D}_{\mathfrak{p}}^2$. Пусть $\bar{x}$-комплексно сопряженная функция с x. Так как $(dx)_{\mathfrak{p}} = (dx_1)_{\mathfrak{p}} + i\,(dx_2)_{\mathfrak{p}}$ и $(d\bar{x})_{\mathfrak{p}} = (dx_1)_{\mathfrak{p}} - i\,(dx_2)_{\mathfrak{p}}$, то $(dx)_{\mathfrak{p}}$ и $(d\bar{x})_{\mathfrak{p}}$ образуют базис $\mathfrak{D}_{\mathfrak{p}}$ и $(dx)_{\mathfrak{p}} \square (d\bar{x})_{\mathfrak{p}} = -2i\,(dx_1)_{\mathfrak{p}} \square (dx_2)_{\mathfrak{p}}$. Отсюда следует, что $i\,(dx)_{\mathfrak{p}} \square (d\bar{x})_{\mathfrak{p}}$ является вещественным базисным элементом пространства $\mathfrak{D}_{\mathfrak{p}}^2$. Если теперь y — любая другая униформизирующая переменная в точке $\mathfrak{p}$, то $(dy)_{\mathfrak{p}} = \alpha\,(dx)_{\mathfrak{p}}$, где α есть значение функции $\frac{dy}{dx}$ в точке $\mathfrak{p}$, откуда $i\,(dy)_{\mathfrak{p}} \square (d\bar{y})_{\mathfrak{p}} = \alpha\bar{\alpha}\,(i\,(dx)_{\mathfrak{p}} \square (d\bar{x})_{\mathfrak{p}})$, причем $\alpha\bar{\alpha} > 0$. Таким образом, вещественный элемент $\varphi \in \mathfrak{D}_{\mathfrak{p}}^2$ мы можем назвать *положительным*, если $\varphi = \beta i\,(dx)_{\mathfrak{p}} \square (d\bar{x})_{\mathfrak{p}}$,

где $\beta > 0$ (в силу вышеизложенного это определение не зависит от выбора униформизирующей переменной x).

Так как для каждой точки $\mathfrak{q}$ из некоторой окрестности $\mathfrak{p}$ элемент $x - x(\mathfrak{q})$ является униформизирующей переменной в $\mathfrak{q}$, то, как легко видеть, дифференциальная форма $i(dx)\square(\overline{dx})$ степени 2 положительна во всех точках некоторой окрестности точки $\mathfrak{p}$. Так как эта форма, очевидно, непрерывна, то наше определение положительности вещественных элементов из $\mathfrak{D}^2_{\mathfrak{p}}$ порождает ориентацию S.

Ориентировав многообразие S, мы можем на S интегрировать любую непрерывную вещественную дифференциальную форму степени 2, что легко обобщается и на случай непрерывных комплексных дифференциальных форм степени 2.

Пусть теперь φ — дифференциальная форма степени 2, которая определена и непрерывна только на некотором открытом подмножестве U многообразия S. Мы хотим дать определение интеграла от формы φ по U (если он существует). Для этого введем в рассмотрение класс F непрерывных функций f на S, обладающих следующими свойствами: 1) $|f(\mathfrak{p})| \leqslant 1$ для всех $\mathfrak{p} \in S$ и 2) для некоторого компактного подмножества K множества U (зависящего от f) $f(\mathfrak{p}) = 0$ при всех $\mathfrak{p} \notin K$. Если $f \in F$, то $f\varphi$ можно продолжить до непрерывной дифференциальной формы (обозначаемой также через $f\varphi$) на S, которая равна 0 вне U, и интеграл $\int\limits_S f\varphi$ будет иметь смысл. Для любого компактного подмножества K множества U через F_K обозначим совокупность функций $f \in F$, равных 1 на K. Множества F_K не пусты (см. „Теория групп Ли. I“, Лемма 1 § VII гл. V). Если K и K' — два компактных подмножества U, то объединение $K \cup K'$ также компактно и $F_{K \cup K'} = F_K \cap F_{K'}$. Применяя терминологию Н. Бурбаки (N. Bourbaki, Eléments de Mathématique, книга III, Topologie Générale, гл. I)[1]), получаем, что множества F_K образуют базис фильтра Φ на множестве F. Будем говорить что форма φ *интегрируема на* U, если отображение $f \to \int\limits_S f\varphi$ множества F в поле комплексных чисел имеет предел I от-

[1]) Имеется русский перевод: Н. Бурбаки, Общая топология (Основные структуры). М. 1958. (*Прим. перев.*)

носительно фильтра Φ. Этот предел I (если он существует) называется *интегралом от формы* φ *по* U и обозначается через $\int\limits_U \varphi$. Ясно, что если $U=S$, то любая непрерывная дифференциальная форма φ степени 2 на S интегрируема в смысле последнего определения и интеграл от нее совпадает с ранее определенным интегралом $\int\limits_S \varphi$.

Для того чтобы форма φ была интегрируема на U, достаточно, чтобы множество чисел $\int\limits_S f\varphi$, $f \in F$, было ограниченным. Действительно, пусть указанное условие выполнено. В силу полноты C для доказательства существования предела I достаточно показать, что для любого $\varepsilon > 0$ существует такое компактное подмножество K_ε множества U, что $\left|\int\limits_S f\varphi - \int\limits_S f'\varphi\right| \leqslant \varepsilon$ для любых f и f', принадлежащих F_{K_ε}. Допустим, что такого подмножества не существует. Тогда для каждого компактного подмножества K множества U мы можем найти функцию $g_K \in F$, равную 0 на K и такую, что $\left|\int\limits_S g_K\varphi\right| > \frac{\varepsilon}{2}$ (достаточно взять $g_K = \frac{1}{2}(f-f')$, где f и f' — функции из F_K такие, что $\left|\int\limits_S f\varphi - \int\limits_S f'\varphi\right| > \varepsilon$). Индуктивно построим теперь последовательность (K_n) компактных подмножеств множества U. В качестве K_1 возьмем пустое множество; если $K_1, \ldots, K_n$ уже определены, то в качестве K_{n+1} возьмем компактное подмножество множества U, вне которого все функции $g_{K_1}, \ldots, g_{K_n}$ равны 0. Пусть ζ_n — комплексное число, по модулю равное 1 и такое, что значение интеграла $\int\limits_S \zeta_n g_{K_n}\varphi$ вещественно и положительно, а значит $> \frac{\varepsilon}{2}$. Функция $h_n = \zeta_1 g_{K_1} + \ldots + \zeta_n g_{K_n}$, очевидно, принадлежит F, в то же время $\int\limits_S h_n\varphi > \frac{n\varepsilon}{2}$, что противоречит

предположению о том, что для всех $f \in F$ числа $\left|\int_S f\varphi\right|$ ограничены.

Если форма φ может быть продолжена до дифференциальной формы φ_1, которая определена и непрерывна на некотором открытом множестве U_1, содержащем замыкание $\overline{U}$ множества U, то φ интегрируема на U. Действительно, на S существует непрерывная функция h, равная 1 на $\overline{U}$ и 0 вне U_1; форма $h\varphi_1$ может быть продолжена до непрерывной дифференциальной формы φ_2 на S, и φ_2 совпадает с φ на U.

§ 12. Билинейные неравенства Римана

Пусть $P = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}$ — конечное подмножество точек римановой поверхности S поля R и ω — дифференциальная форма степени 1, заданная на $S \setminus P$ и принадлежащая классу C_1 на этом множестве; $d\omega$ является, следовательно, непрерывной дифференциальной формой степени 2 на $S \setminus P$.

Для каждого $i\,(1 \leqslant i \leqslant h)$ выберем униформизирующую переменную x_i в точке $\mathfrak{p}_i$ и замкнутый x_i-круг D_i с x_i-центром в $\mathfrak{p}_i$; при этом будем предполагать, что $D_i \cap D_j = \varnothing$ при $i \neq j$. Через r_i обозначим x_i-радиус круга D_i и через C_i — его окружность. Для вещественного числа θ через $\mathfrak{q}_i(\theta)$ мы обозначим точку окружности C_i, для которой $x_i(\mathfrak{q}_i(\theta)) = r_i e^{2\pi i\theta}$. Отображение $(1-\theta,\ \theta) \to \mathfrak{q}_i(\theta)$ (где θ меняется от 0 до 1) является дифференцируемым 1-симплексом γ_i на C_i. Легко видеть, что γ_i есть цикл и принадлежит положительной образующей группы $H_1(C_i)$. Обозначим через U открытое множество $S \setminus \bigcup_{i=1}^{h} D_i$. Нашей целью является доказательство следующей формулы:

$$\int_U d\omega + \sum_{i=1}^{h} \int_{\gamma_i} \omega = 0 \tag{1}$$

(являющейся частным случаем общей формулы Стокса).

Обозначим через $\overline{U}$ замыкание множества U. Для каждой точки $\mathfrak{q} \in U$ выберем униформизирующую переменную $y_{\mathfrak{q}}$ и замкнутую окрестность $N(\mathfrak{q})$ этой точки в U, которая при

помощи $y_{\mathfrak{q}}$ отображается топологически на замкнутый квадрат с центром в начале комплексной плоскости. Далее, если $\mathfrak{q} \in \overline{U} \setminus U$, то $\mathfrak{q}$ принадлежит одному и только одному множеству C_i. В этом случае для $\mathfrak{q}$ существует окрестность, в которой дифференциал $x_i^{-1}\, dx_i$ имеет первообразную $y_{\mathfrak{q}}$; эту первообразную мы нормализуем условием $y_{\mathfrak{q}}(\mathfrak{q}) = 0$. Легко видеть, что для каждой такой точки $\mathfrak{q} \in C_i$ существует замкнутая окрестность $N(\mathfrak{q})$, на которой функция $y_{\mathfrak{q}}$ определена и которая при помощи $y_{\mathfrak{q}}$ отображается топологически на замкнутый квадрат с центром в начале комплексной плоскости. Можно предполагать при этом, что $N(\mathfrak{q})$ не пересекает множеств D_j при $j \neq i$.

Пусть $N'(\mathfrak{q})$ — замкнутая окрестность точки $\mathfrak{q}$, содержащаяся во внутренности множества $N(\mathfrak{q})$. Окрестности $N'(\mathfrak{q})$ при всех $\mathfrak{q} \in \overline{U}$ образуют покрытие компактного множества $\overline{U}$; следовательно, существует конечное подмножество Q множества $\overline{U}$ такое, что окрестности $N'(\mathfrak{q})$ при всех $\mathfrak{q} \in Q$ также покрывают $\overline{U}$.

Как известно, каждой точке $\mathfrak{q} \in Q$ мы можем сопоставить функцию $f_{\mathfrak{q}}$ класса C_1 на S, равную 0 вне $N(\mathfrak{q})$, так, чтобы $\sum\limits_{\mathfrak{q} \in Q} f_{\mathfrak{q}}(\mathfrak{r}) = 1$ при всех $\mathfrak{r} \in U$. Так как форма ω на U совпадает с $\sum\limits_{\mathfrak{q} \in Q} f_{\mathfrak{q}}\omega$, то формулу (1) достаточно доказать в предположении, что форма ω равна 0 вне некоторого множества $N(\mathfrak{q})$.

Предположим сначала, что форма ω равна 0 вне множества $N(\mathfrak{q})$, соответствующего точке $\mathfrak{q} \in U$. Тогда $\int\limits_{\gamma_i} \omega = 0$ $(1 \leqslant i \leqslant h)$, и мы должны, следовательно, показать, что $\int\limits_U d\omega = 0$. Пусть y_1 и y_2 — вещественная и мнимая части функции $y_{\mathfrak{q}}$. Если $\mathfrak{r} \in N(\mathfrak{q})$, то

$$\omega_{\mathfrak{r}} = A_1(y_1(\mathfrak{r}), y_2(\mathfrak{r}))(dy_1)_{\mathfrak{r}} + A_2(y_1(\mathfrak{r}), y_2(\mathfrak{r}))(dy_2)_{\mathfrak{r}}, \quad (2)$$

где A_1 и A_2 — непрерывно дифференцируемые функции на множестве $y_{\mathfrak{q}}(N(\mathfrak{q}))$ комплексной плоскости. Имеем

$$d\omega_{\mathfrak{r}} = \left(\frac{\partial A_2}{\partial y_1}(y_1(\mathfrak{r}), y_2(\mathfrak{r})) - \frac{\partial A_1}{\partial y_2}(y_1(\mathfrak{r}), y_2(\mathfrak{r}))\right)(dy_1)_{\mathfrak{r}} \square (dy_2)_{\mathfrak{r}}. \tag{3}$$

Так как $d\omega_{\mathfrak{r}}$ вне $N(\mathfrak{q})$ равно 0, а $dy_1 \square dy_2$ есть положительная дифференциальная форма степени 2 на $N(\mathfrak{q})$, то

$$\int\limits_U d\omega = \int\limits_{y_{\mathfrak{q}}(N(\mathfrak{q}))} \left(\frac{\partial A_2}{\partial y_1} - \frac{\partial A_1}{\partial y_2}\right) dy_1\, dy_2.$$

Пусть сторона квадрата $y_{\mathfrak{q}}(N(\mathfrak{q}))$ равна $2a$. Тогда

$$\int\limits_{y_{\mathfrak{q}}(N(\mathfrak{q}))} \frac{\partial A_2}{\partial y_1} dy_1\, dy_2 = \int\limits_{-a}^{a} \left(\int\limits_{-a}^{a} \frac{\partial A_2}{\partial y_1} dy_1\right) dy_2 =$$

$$= \int\limits_{-a}^{a} (A_2(a, y_2) - A_2(-a, y_2))\, dy_2 = 0,$$

ибо A_1 и A_2 на границе квадрата $y_{\mathfrak{q}}(N(\mathfrak{q}))$ равны нулю, что вытекает из равенства нулю ω вне $N(\mathfrak{q})$. Аналогично докажем, что $\int\limits_{y_{\mathfrak{q}}(N(\mathfrak{q}))} \frac{\partial A_1}{\partial y_2} dy_1\, dy_2 = 0$, откуда $\int\limits_U d\omega = 0$.

Рассмотрим теперь случай, когда $\mathfrak{q} \in C_i$ при некотором i. Надо доказать, что $\int\limits_U d\omega + \int\limits_{\gamma_i} \omega = 0$. Пусть y_1 и y_2 — вещественная и мнимая части функции $y_{\mathfrak{q}}$. Так как $dy_{\mathfrak{q}} = x_i^{-1} dx_i$, то $(dy_1)_{\mathfrak{r}}$ и $(dy_2)_{\mathfrak{r}}$ образуют базис пространства дифференциалов в точке $\mathfrak{r} \in N(\mathfrak{q})$. Форма $dy_1 \square dy_2$, как легко видеть, положительна во всех точках из $N(\mathfrak{q})$. Для $\omega_{\mathfrak{r}}$ и $d\omega_{\mathfrak{r}}$ при $\mathfrak{r} \in N(\mathfrak{q})$ мы имеем, как и выше, формулы (2) и (3). С другой стороны, $x_i(\mathfrak{r}) = x_i(\mathfrak{q}) e^{y_{\mathfrak{q}}(\mathfrak{r})}$, откуда следует, что $U \cap N(\mathfrak{q})$ есть множество тех точек $\mathfrak{r} \in N(\mathfrak{q})$, в которых $y_1(\mathfrak{r}) > 0$. Утверждаем, что

$$\int\limits_U d\omega = \int\limits_{-a}^{a} \left(\int\limits_0^a \left(\frac{\partial A_2}{\partial y_1} - \frac{\partial A_1}{\partial y_2}\right) dy_1\right) dy_2, \tag{4}$$

где $2a$ есть длина стороны квадрата $y_{\mathfrak{q}}(N(\mathfrak{q}))$. Положим $B=\frac{\partial A_2}{\partial y_1}-\frac{\partial A_1}{\partial y_2}$. Пусть f — любая непрерывная функция на S, равная 0 вне компактного подмножества K множества U. Ясно, что тогда $\int\limits_U f\,d\omega=\int\limits_{y_{\mathfrak{q}}(N(\mathfrak{q}))} f^*(y_1,\ y_2)\,B\,dy_1\,dy_2$, где $f^*(y_1,\ y_2)$ есть значение, принимаемое функцией f в точке $\mathfrak{r}\in N(\mathfrak{q})$, для которой $y(\mathfrak{r})=y_1+iy_2$. Так как функция f вне U равна 0, то $f^*(y_1,\ y_2)=0$, если только $y_1\leqslant 0$, откуда

$$\int\limits_U f\,d\omega=\int\limits_{-a}^{a}\left(\int\limits_0^a f^*(y_1,\ y_2)\,B\,dy_1\right)dy_2.$$

Пусть ε — положительное число. Если $|f(\mathfrak{r})|\leqslant 1$ при всех $\mathfrak{r}\in S$ и $f(\mathfrak{r})=1$ для всех тех точек $\mathfrak{r}\in N(\mathfrak{q})$, для которых $y_1(\mathfrak{r})\geqslant\varepsilon$, то

$$\left|\int\limits_U f\,d\omega-\int\limits_{-a}^{a}\left(\int\limits_0^a B\,dy_1\right)dy_2\right|\leqslant\int\limits_{-a}^{a}\left(\int\limits_0^{\varepsilon}|B|\,dy_1\right)dy_2.$$

Отсюда и следует формула (4), ибо стоящее справа выражение вместе с ε стремится к 0. Так как дифференциальная форма ω вне $N(\mathfrak{q})$ равна 0, то $A_2(a,\ y_2)=0$, откуда

$$\int\limits_{-a}^{a}\left(\int\limits_0^a\frac{\partial A_2}{\partial y_1}dy_1\right)dy_2=-\int\limits_{-a}^{a}A_2(0,\ y_2)\,dy_2.$$

Покажем, что правая часть последнего равенства равна $-\int\limits_{\gamma_i}\omega$.

Для любого вещественного числа t через $\mathcal{A}(\mathfrak{q}_i(t))$ обозначим класс аналитических функций в точке $\mathfrak{q}_i(t)\in S$ (определение точки $\mathfrak{q}_i(\theta)$ дано выше). Отображение

$$g\to\left(\frac{dg(\mathfrak{q}_i(\theta))}{d\theta}\right)_{\theta=t},\quad g\in\mathcal{A}(\mathfrak{q}_i(t)),$$

есть касательный вектор L_t к S в точке $\mathfrak{q}_i(t)$. Если $0 \leqslant t \leqslant 1$, то L_t есть касательный вектор к γ_i при значении параметра t, откуда

$$\int_{\gamma_i} \omega = \int_0^1 \omega_{\mathfrak{q}_i(t)}(L_t)\,dt.$$

Так как $L_{t+1} = L_t$, то для любого вещественного числа b имеем также

$$\int_{\gamma_i} \omega = \int_b^{b+1} \omega_{\mathfrak{q}_i(t)}(L_t)\,dt.$$

Пусть t_0 — вещественное число, для которого $\mathfrak{q}_i(t_0) = \mathfrak{q}$. Так как при $\mathfrak{r} \in N(\mathfrak{q})$ мы имеем $x_i(\mathfrak{r}) = x_i(\mathfrak{q})\,e^{y_{\mathfrak{q}}(\mathfrak{r})}$, то при $\mathfrak{q}_i(t) \in N(\mathfrak{q})$ число $t - \frac{1}{2\pi} y_2(\mathfrak{q}_i(t)) - t_0$ будет целым. Легко видеть, что $a < \pi$ и что $\mathfrak{q}_i(t) \in N(\mathfrak{q})$, если только $|t - t_0| \leqslant \frac{a}{2\pi}$. Таким образом, получаем

$$\int_{\gamma_i} \omega = \int_{t_0 - \frac{1}{2}}^{t_0 + \frac{1}{2}} \omega_{\mathfrak{q}_i(t)}(L_t)\,dt = \int_{t_0 - \frac{a}{2\pi}}^{t_0 + \frac{a}{2\pi}} \omega_{\mathfrak{q}_i(t)}(L_t)\,dt,$$

ибо форма ω вне $N(\mathfrak{q})$ равна 0. Далее, если $|\theta - t_0| \leqslant \frac{a}{2\pi}$, то $y_{\mathfrak{q}}(\mathfrak{q}_i(\theta)) = 2\pi i(\theta - t_0)$, откуда

$$(dy_{\mathfrak{q}})_{\mathfrak{q}_i(t)}(L_t) = \left(\frac{dy_{\mathfrak{q}}(\mathfrak{q}_i(\theta))}{d\theta}\right)_{\theta = t} = 2\pi i.$$

Таким образом, $\omega_{\mathfrak{q}_i(t)}(L_t) = 2\pi A_2(0,\ y_2(\mathfrak{q}_i(t)))$, а значит

$$\int_{\gamma_i} \omega = \int_{-a}^{a} A_2(0,\ y_2)\,dy_2,$$

С другой стороны, мы имеем

$$\int_{-a}^{a}\left(\int_{0}^{a}\frac{\partial A_1}{\partial y_2}dy_1\right)dy_2=\int_{0}^{a}\left(\int_{-a}^{a}\frac{\partial A_1}{\partial y_2}dy_2\right)dy_1=$$

$$=\int_{0}^{a}(A_1(y_1, a)-A_1(y_1, -a))\,dy_1=0,$$

так как форма ω вне $N(\mathfrak{q})$ равна 0. Формула (1), таким образом, доказана. Этой формулой мы воспользуемся при доказательстве следующей теоремы.

Теорема 18 (билинейные неравенства Римана). *Пусть $\{z_1, \ldots, z_{2g}\}$ есть канонический базис одномерной группы гомологий римановой поверхности поля R. Если π_k есть период дифференциала $\omega\neq 0$ первого рода поля R относительно $z_k (1\leqslant k\leqslant 2g)$, то*

$$\frac{1}{2\pi i}\sum_{k=1}^{g}\left(\pi_{k+g}\bar{\pi}_k-\pi_k\bar{\pi}_{k+g}\right)>0.$$

Применяя теорему 11 § 8, заключаем, что существует такой дифференциал η поля R второго рода, что $\int\limits_{z_k}\eta=$ $=\bar{\pi}_k (1\leqslant k\leqslant 2g)$. Из формулы (5) § 8 следует, что

$$\frac{1}{2\pi i}\sum_{k=1}^{g}\left(\pi_{k+g}\bar{\pi}_k-\pi_k\bar{\pi}_{k+g}\right)=j(\eta, \omega).$$

Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ — все различные полюса дифференциала η. Для каждого $s (1\leqslant s\leqslant h)$ выберем униформизирующую переменную x_s в точке $\mathfrak{p}_s$. Обозначим через D_s замкнутый x_s-круг с x_s-центром в $\mathfrak{p}_s$ и x_s-радиуса r_s; при этом предполагаем, что $D_s\cap D_t=\varnothing$ при $s\neq t$. Пусть C_s — окружность круга D_s и c_s — положительная образующая группы $H_1(C_s)$. Для каждого s мы можем найти элемент $f_s\in R$ так, чтобы точка $\mathfrak{p}_s$ не являлась полюсом дифференциала $\eta-df_s$ (теорема 14 § 8 гл. VI). Будем еще предполагать, что радиус

r_s настолько мал, что $\mathfrak{p}_s$ является единственным полюсом элемента f_s в круге D_s. Тогда

$$j(\eta, \omega) = \sum_{s=1}^{h} \operatorname{res}_{\mathfrak{p}_s} f_s \omega = \sum_{s=1}^{h} \frac{1}{2\pi i} \int_{c_s} f_s \omega.$$

Введем теперь в рассмотрение комплексно сопряженную с ω форму $\bar{\omega}$, которая определяется формулой $\bar{\omega}_{\mathfrak{p}}(L) = \overline{\omega_{\mathfrak{p}}(L)}$, где $\mathfrak{p} \in S$, а L — касательный вектор к S в точке $\mathfrak{p}$. Пусть $\omega = u\,dx$, где x — отличный от константы элемент поля R и $u \in R$. Тогда, как легко видеть, $\bar{\omega}_{\mathfrak{p}} = \overline{u(\mathfrak{p})}\,(d\bar{x})_{\mathfrak{p}}$, если только $\mathfrak{p}$ не является ни нулем, ни полюсом дифференциала dx. Отсюда следует, что форма $\bar{\omega}$ везде аналитична на S. Если V — произвольный открытый круг на S, а λ — первообразная функция дифференциала ω на V, то для всех $\mathfrak{p} \in V$ имеем $(d\bar{\lambda})_{\mathfrak{p}} = \bar{\omega}_{\mathfrak{p}}$.

Докажем, что дифференциальная форма $\eta - \bar{\omega}$, которая аналитична на $U = S \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_h\}$, является дифференциалом от аналитической функции на U. Для произвольного 1-цикла ζ на U мы имеем $\int_\zeta (\eta - \bar{\omega}) = \int_\zeta \eta - \int_\zeta \bar{\omega}$; второй член справа, очевидно, есть число, сопряженное с $\int_\zeta \omega$. Если ζ принадлежит классу гомологий $\sum_{k=1}^{2g} a_k z_k$ на S, то

$$\int_\zeta \eta = \sum_{k=1}^{2g} a_k \int_{z_k} \eta \quad \text{и} \quad \int_\zeta \omega = \sum_{k=1}^{2g} a_k \int_{z_k} \omega, \text{ откуда } \int_\zeta (\eta - \bar{\omega}) = 0,$$

ибо $\int_{z_k} \eta = \bar{\pi}_k$. Фиксируем теперь некоторую точку $\mathfrak{p}_0 \in U$. Так как U связно, то, очевидно, для каждой точки $\mathfrak{p} \in U$ существует дифференцируемая цепь $\gamma(\mathfrak{p})$, для которой $\partial\gamma(\mathfrak{p}) = \mathfrak{p} - \mathfrak{p}_0$. В силу только что доказанного число $\varphi(\mathfrak{p}) = \int_{\gamma(\mathfrak{p})} (\eta - \bar{\omega})$ зависит лишь от $\mathfrak{p}$ и не зависит от выбора $\gamma(\mathfrak{p})$.

Как мы сейчас увидим, определенная таким образом функция φ аналитична на U и $d\varphi = \eta - \bar{\omega}$. Пусть V есть открытый круг, содержащийся в U. Так как η и $\bar{\omega}$ обладают на V первообразными функциями, то существует такая аналитическая на V функция φ_V, что $d\varphi_V = \eta - \bar{\omega}$ на V. Пусть $\mathfrak{p}$ и $\mathfrak{q}$ — точки из V и τ — дифференцируемый 1-симплекс на V, для которого $\partial\tau = \mathfrak{q} - \mathfrak{p}$. Так как $\int\limits_\tau \omega$ и $\int\limits_\tau \bar{\omega}$ комплексно сопряжены между собой, то

$$\int\limits_\tau (\eta - \bar{\omega}) = \varphi_V(\mathfrak{q}) - \varphi_V(\mathfrak{p}).$$

С другой стороны, $\tau + \gamma(\mathfrak{p}) - \gamma(\mathfrak{q})$ есть дифференцируемый цикл, поэтому

$$\int\limits_\tau (\eta - \bar{\omega}) = \int\limits_{\gamma(\mathfrak{q})} (\eta - \bar{\omega}) - \int\limits_{\gamma(\mathfrak{p})} (\eta - \bar{\omega}) = \varphi(\mathfrak{q}) - \varphi(\mathfrak{p}).$$

Таким образом, функция $\varphi - \varphi_V$ постоянна на V, а значит функция φ аналитична на V, кроме того $d\varphi = \eta - \bar{\omega}$.

Имеем теперь

$$j(\eta, \omega) = \frac{1}{2\pi i}\sum_{s=1}^{h} \int\limits_{\gamma_s} f_s\omega =$$

$$= \frac{1}{2\pi i}\sum_{s=1}^{h} \int\limits_{\gamma_s} (f_s - \varphi)\omega + \frac{1}{2\pi i}\sum_{s=1}^{h} \int\limits_{\gamma_s} \varphi\omega,$$

где 1-симплекс γ_s определен так же, как и при доказательстве формулы (1). Обозначим через U' дополнение к множеству $\bigcup\limits_{s=1}^{h} D_s$. В силу формулы (1) имеем $\sum\limits_{s=1}^{h} \int\limits_{\gamma_s} \varphi\omega = -\int\limits_{U'} d(\varphi\omega)$. Так как $d\omega = 0$ и $\omega \square \eta = 0$, то $d(\varphi\omega) =$

$= d\varphi \square \omega = (\eta - \bar{\omega}) \square \omega = -\bar{\omega} \square \omega$, откуда

$$\frac{1}{2\pi i} \sum_{s=1}^{h} \int_{\gamma_s} \varphi\omega = \frac{1}{2\pi i} \int_{U'} \bar{\omega} \square \omega.$$

Рассмотрим теперь выражение $\int_{\gamma_s} (f_s - \varphi)\omega$. Пусть V_s' — открытый x_s-круг с x_s-центром в точке $\mathfrak{p}_s$, который содержит D_s, но не содержит, кроме $\mathfrak{p}_s$, других полюсов элемента f_s, а также не содержит точек $\mathfrak{p}_t$ при $t \neq s$. Дифференциал $\eta - df_s$ голоморфен на V_s', поэтому на этом множестве он имеет первообразную функцию g_s. Обозначим через λ_s первообразную функцию дифференциала ω на V_s'. Так как $d\bar{\lambda}_s - dg_s = df_s - \eta + \eta - (\eta - \bar{\omega}) = df_s - d\varphi$, то на множестве $V_s' \setminus \{\mathfrak{p}_s\}$ функции $f_s - \varphi$ и $\bar{\lambda}_s - g_s$ отличаются друг от друга лишь на константу. Следовательно, модуль $|f_s - \varphi|$ ограничен на $V_s' \setminus \{\mathfrak{p}_s\}$. Пусть x_{s1} и x_{s2} — вещественная и мнимая части функции x_s. Если $\mathfrak{q} \in V_s'$, $\mathfrak{q} \neq \mathfrak{p}_s$, то

$$((f_s - \varphi)\omega)_{\mathfrak{q}} = A_{s1}(x_{s1}(\mathfrak{q}), x_{s2}(\mathfrak{q}))(dx_{s1})_{\mathfrak{q}} + \\ + A_{s2}(x_{s1}(\mathfrak{q}), x_{s2}(\mathfrak{q}))(dx_{s2})_{\mathfrak{q}},$$

где A_{s1} и A_{s2} — ограниченные аналитические функции на $x_s(V_s' \setminus \{\mathfrak{p}_s\})$. Таким образом,

$$\int_{\gamma_s} (f_s - \varphi)\omega = r_s \int_0^{2\pi} (-A_{s1}(r_s \cos\theta, r_s \sin\theta)\sin\theta + \\ + A_{s2}(r_s \cos\theta, r_s \sin\theta)\cos\theta)\, d\theta,$$

откуда следует, что интеграл $\int_{\gamma_s} (f_s - \varphi)\omega$ стремится к 0 при $r_s \to 0$.

Пусть $0 < \varepsilon < 1$. Обозначим через $D_{s,\varepsilon}$ замкнутый круг с x_s-центром $\mathfrak{p}_s$ и x_s-радиуса $r_s\varepsilon$, а через U_ε' — дополнение

к множеству $\bigcup_{s=1}^{h} D_{s,\varepsilon}$. Тогда

$$j(\eta, \omega) = \lim_{\varepsilon \to 0} \int_{U'_\varepsilon} \frac{1}{2\pi i} \bar{\omega} \square \omega.$$

Пусть теперь $\mathfrak{p}$ — произвольная точка из U и x — униформизирующая переменная в $\mathfrak{p}$. Если $\omega = u\,dx$, $u \in R$, то

$$\frac{1}{2\pi i} \bar{\omega}_{\mathfrak{p}} \square \omega_{\mathfrak{p}} = \frac{1}{2\pi i} |u(\mathfrak{p})|^2 (d\bar{x})_{\mathfrak{p}} \square (dx)_{\mathfrak{p}} =$$

$$= \frac{1}{2\pi} |u(\mathfrak{p})|^2 i (dx)_{\mathfrak{p}} \square (d\bar{x})_{\mathfrak{p}}.$$

Таким образом, форма $\frac{1}{2\pi i} \bar{\omega} \square \omega$ положительна в $\mathfrak{p}$, если только $u(\mathfrak{p}) \neq 0$, т. е. если $\mathfrak{p}$ не является нулем дифференциала ω. Так как ω имеет только конечное число нулей, то $\frac{1}{2\pi i} \int_{U'_\varepsilon} \bar{\omega} \square \omega$ является вещественным положительным числом и это число возрастает при уменьшении ε. Таким образом, $j(\eta, \omega)$ есть вещественное положительное число, и теорема 18 доказана.

Следствие 1. *Числа $\pi_1, \ldots, \pi_g$, определенные в теореме 18, не равны 0 одновременно.*

Следствие 2. *Пусть сохраняются обозначения теоремы 18 и пусть $a_1, \ldots, a_g$ — произвольные комплексные числа. Тогда существует и притом единственный дифференциал ω первого рода, такой, что*

$$\int_{z_k} \omega = a_k \quad (1 \leqslant k \leqslant g).$$

Обозначая через $\{\eta_1, \ldots, \eta_g\}$ базис пространства дифференциалов первого рода поля R, положим

$$\int_{z_k} \eta_l = \pi_{kl} \quad (1 \leqslant k, l \leqslant g),$$

В силу следствия 1 система однородных уравнений $\sum_{l=1}^{g} x_l \pi_{kl} = 0$ $(1 \leqslant k \leqslant g)$ не имеет нетривиальных решений. Поэтому система уравнений $\sum_{l=1}^{g} x_l \pi_{kl} = a_k$ $(1 \leqslant k \leqslant g)$ имеет единственное решение, что и доказывает следствие 2.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Клод Шевалле

ВВЕДЕНИЕ В ТЕОРИЮ АЛГЕБРАИЧЕСКИХ ФУНКЦИЙ ОТ ОДНОЙ ПЕРЕМЕННОЙ

Редактор *Ф. А. Иванов*
Техн. редактор *Р. Г. Польская*
Корректор *Е. А. Максимова*

Сдано в набор 20/XII 1958 г. Подписано к печати 30/X 1959 г. Формат 84×108¹/₃₂.
Печатных л. 18,44. Уч.-изд. л. 17,22.
Тираж 7000 экз. Цена книги 11 р. 20 к.
Т-11032. Зак. № 555.

Государственное издательство физико-математической литературы
Москва, В-71, Ленинский пр., 15.

Типография № 2 им. Евг. Соколовой УПП Ленсовнархоза.
Ленинград, Измайловский пр., 29.