Московский Государственный Университет
имени М. В. Ломоносова

Механико-математический факультет
Московское математическое общество

И. Р. ШАФАРЕВИЧ

ДЗЕТА-ФУНКЦИЯ

Москва 1969

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им.М.В.ЛОМОНОСОВА

Механико-математический факультет,
Московское математическое общество

ШАФАРЕВИЧ И.Р.

Д З Е Т А - Ф У Н К Ц И Я

1966-67 г.г.

Москва, 1969 г.

Подписано к печати 24/11-69 г.
Бумага 60x84/16 Объем 9,25 печ. листа
Л-24297. Заказ 46. Тираж 230. Цена 20 копеек

Ротапринт ВЦ МГУ

Основной целью этого курса является изложение последних результатов Ивасавы (K.Iwasawa) о группах классов дивизоров и ζ -функциях полей алгебраических чисел. Наиболее сенсационные из этих результатов до сих пор нигде не опубликованы. Повидимому, в этих работах сделаны первые шаги в совершенно новом разделе арифметики, дальнейшее развитие которого должно привести к более глубокому пониманию арифметики полей алгебраических чисел и свойств ζ -функций.

Чтобы сделать более ясным место результатов Ивасавы, я начал курс с изложения основных фактов, известных о ζ -функциях полей алгебраических чисел и алгебраических кривых.

Курс распадается на три части. Первая содержит доказательство функционального уравнения и конструкцию аналитического продолжения ζ -функций полей алгебраических чисел и алгебраических кривых над конечным полем. Изложение основано на методе Ивасавы и Тэйта, интегрирования по группе иделей. Эти вопросы изложены сейчас в нескольких местах (Лэнг "алгебраические числа", Algebraic Number theory", Academic Press I967), однако функциональный случай явно не рассмотрен, а это нам нужно для дальнейшего *).

Вторая часть посвящена алгебраическим кривым над конечным полем. Здесь доказываются два основных факта - формула Лефшетца для числа неподвижных точек соответствия и гипотеза Римана для ζ -функций кривой над конечным полем. В этой части изложение по необходимости более сжатое - эту часть курса следует рассматривать как конспект (или путеводитель) книги Лэнга "Abelian varietis, Intersüence, I959, к которой читатель отсылается за подробным проведением доказательств. С построением якобиева многообразия, которое в курсе только намечено, можно познакомиться по книге Мамфорда "Lectures on curves on an algebraic surface", Annals of Math. Studies, № 59. Наконец, стоит заметить, что наиболее естественное доказательство формулы Лефшетца можно, по-видимому, получить, пользуясь когомологиями Гротендика, но полные доказательства всех

*) Рассмотрение функционального случая содержится также в только что вышедшей книге А.Вейля "Basic number theorie", Springer , I967.

необходимых для этого результатов еще не опубликованы.

В третьей части излагается собственно теория Ивасавы. Часть содержащихся здесь результатов опубликована. Изложение можно найти в работах Ивасавы (ряд работ в Annals of Math. и обзор в Bull.Amer. Math.Soc.) и докладе Серра "Classes des corps cyclotomiques", Seminaire Bourbaki , 1958/59 № 174. Другая часть еще не опубликована и стала мне известной благодаря любезности К.Ивасавы, приславшего мне изложение своих результатов.

Курс записан Ю.И.Маниным. Без большого труда, вложенного им в эти записи, они никогда бы не появились.

И.Р.Шафаревич

В В Е Д Е Н И Е

Риман обнаружил связь между нулями ζ -функции и вопросом о поведении $\pi(x)=\sum_{p<x} 1$, где p пробегает простые числа.

Положим

$$F(x)=\sum_{i=1}^{\infty}\frac{1}{i}\pi(x^{\frac{1}{i}})$$

Если эту функцию несколько сгладить, положив

$$F_0(x)=\frac{F(x+0)+F(x-0)}{2},$$

то имеет место формула

$$F_0(x)=\mathrm{li}\,x-\sum_{\rho}\mathrm{li}(x^{\rho})+\int_x^{\infty}\frac{du}{(u^2-1)u\log u}-\log 2$$

где ρ пробегает нули ζ -функции, и $\mathrm{li}\,x=\int_2^x\frac{du}{\log u}$
Отсюда, в частности, видно, что

(I) $$\pi(x)-\mathrm{li}\,x=O(x^{\theta}\log x)$$

где $\theta=\sup \mathrm{Re}\,\rho$. Если бы мы могли доказать, что $\theta<1$, это дало бы нетривиальную оценку (I). К сожалению, мы знаем лишь, что на прямой $\mathrm{Re}\,s=1$ нет корней.

Другой аналогичный вопрос был рассмотрен независимо Га-

уссом и Дирихле.

Рассмотрим квадратичное поле $K = Q(\sqrt{d})$; положим

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}$$

где $\mathfrak{a}$ - пробегает целые дивизоры поля K.

(Определение Дедекинда, годное для всякого поля алгебраических чисел K ; Гаусс говорил о квадратичных формах).

Легко обнаружить, что

$$\zeta_K(s) = \zeta(s) L(s, \chi)$$

где $\zeta = \zeta_Q$ и

$$L(s, \chi) = \sum_{(n,d)=1} \frac{\chi(n)}{n^s}, \quad \chi(n) = \left(\frac{d}{n}\right)$$

Пользуясь функцией ζ_K , Гаусс и Дирихле установили бесконечность числа простых чисел p , для которых $\left(\frac{d}{p}\right) = 1$ или $\left(\frac{d}{p}\right) = -1$. Конечно, это - лишь первые нетривиальные случаи теоремы Дирихле о простых в арифметической прогрессии.

Движущие пружины доказательства состоят в том, что ввиду периодичности χ ряд $L(s,\chi)$ из-за интерференции членов сходится до n включая $s = 1$, так что $L(1,\chi) \neq 0, \infty$. Формально логарифмируя, при $s > 1$ находим

$$\log \zeta_K(s) = \log \zeta(s) + \log L(s,\chi) = \sum_p \frac{1}{p^s} + A(s) - B(s) + O(1).$$

где

$$A(s) = \sum_{\left(\frac{d}{p}\right)=1} \frac{1}{p^s}$$

$$B(s) = \sum_{\left(\frac{d}{p}\right)=-1} \frac{1}{p^s}$$

Теперь учтем, что

$$\log \zeta(s) = A(s) + B(s) + O(1),$$

$$\log L(s,\chi) = A(s) - B(s) + O(1),$$

а также

$$\zeta_K(s) = \frac{\varkappa \cdot h}{s-1} + O(1) \quad \text{при } s \to 1,$$

где h - число классов поля K , а $\varkappa$ - некоторая ненулевая константа.

Следовательно,

$$A(s) + B(s) \to \infty$$

$$A(s) - B(s) \to O(1) \quad \text{при } s \to 1$$

и, значит, $A(s)$ и $B(s)$ имеют полюс в $s = 1$.

Самое существенное во всем этом - что $L(1,\chi) \neq 0$.

Отметим аналогию с результатом $\zeta(s) \neq 0$ при $\mathrm{Re}\, s = 1$, который является основой асимптотического закона.

Формальная аналогия состоит в том, что функция $n \to n^{it}$ при фиксированном t есть характер группы $\mathbb{Z}$; условие $t \neq 0$ означает что он нетривиален.

Видна и разница: неравенство $L(1,\chi) \neq 0$ получается из содержательной интерпретации $L(1,\chi)$ через число классов; для $\zeta(s)$, однако, доказательство имеет иной характер.

Возникает естественный вопрос об исследовании функции Дедекинда $\zeta_K(s)$ и соответствующих L -рядов типа $\sum \frac{\chi(\alpha)}{(N\alpha)^s}$ для некоторых характеров χ группы дивизоров. Гекке установил для них существование функциональных уравнений, выяснил поведение при $s \to 1$, и вывел асимптотические формулы для числа простых идеалов.

Следующее обобщение ζ -функции, точнее, ее вариант, был введен Э.Артином. Кольца $\mathbb{Z}$ и $F_p[t]$ имеют весьма близкую арифметику (F_q , где q - степень простого числа p обозначает поле из q элементов; Артин систематически изучил квадратичные расширения кольца $F_p[t]$). Он обнаружил поразительное обстоятельство: что ζ - функции таких колец являются рациональными функциями от некоторого вспомогательного параметра; эти функции легко вычисляются в ряде конкретных случаев; и для этих случаев оказалась верной гипотеза Римана.

С более современной точки зрения, следует рассмотреть проективную геометрически неприводимую неособую кривую C, скажем, над F_p . Для любого целого дивизора α на C положим $N(\alpha) = p^{\deg \alpha}$ и

$$\zeta_C(s) = \sum_{\alpha} \frac{1}{(N\alpha)^s} .$$

Делая замену $u = p^{-s}$, положим $\zeta_C(s) = Z(u)$. Оказывается, что

$$Z(u) = \frac{F(u)}{(1-u)(1-pu)} \qquad (2)$$

где $F(u) = \prod (1 - \alpha_i u)$ - многочлен, и что всегда $|\alpha_i| = p^{\frac{1}{2}}$. Следовательно, корни $\zeta_C(s)$ имеют вид

$$s = \frac{1}{2} + \frac{2\pi n}{\log p} i .$$

Доказательство этой "гипотезы Римана" было получено впервые Хассе в первом нетривиальном случае, когда род кривой C равен I (для рода 0 все тривиально). На произвольный случай (кривая любого рода) теорема была перенесена А.Вейлем.

Следующие факты играют ключевую роль в доказательстве Вейля. Пусть $k = F_q$ - основное конечное поле; $D_K \supset D_K^0 \supset P_K$ группы всех дивизоров, дивизоров нулевой степени и главных дивизоров кривой соответственно над полем $K \supset k$. Группа классов дивизоров $D_k^0 / P_k = Cl_k^0$ есть группа k -точек на якобиевом многообразии кривой C . Для всевозможных конечных расширений $k_n \supset k$ рассмотрим объединение

$$Cl^0 = \bigcup_{k \subset k_n} Cl_{k_n}^0 .$$

Изучение группы Cl^0 содержит два аспекта. Эта группа периодична, ибо $Cl_{k_n}^0$ конечны. Пусть l - простое число $\neq \mathrm{Char}\, k$, $(Cl^0)_l$ - l - компонента группы Cl^0. Тогда

первый результат утверждает, что

$$(Cl^\circ)_\ell \simeq \left(\mathbb{Z}\left[\tfrac{1}{\ell}\right]/\mathbb{Z}\right)^{2g},$$

где g - род кривой C.

Удобно сформулировать этот факт в двойственном виде:

$$(Cl^\circ_\ell)^\wedge = Char\,(Cl^\circ)_\ell = T = \mathbb{Z}_\ell^{2g},$$

где $\mathbb{Z}_\ell$ - целые ℓ -адические числа.

Второй аспект теории состоит в том, что Cl° - операторная группа: на нее действует группа Галуа G алгебраического замыкания основного поля. Из теории конечных полей известно, что $G = \hat{\mathbb{Z}}$ - свободная топологическая циклическая группа. Существенно, что у G есть выделенная образующая

$$\varphi: x \longrightarrow x^q \quad , \; q \text{ - число элементов } k .$$

Это - знаменитый автоморфизм Фробениуса.

Следовательно, действие G на Cl° описывается действием φ на Cl°, или на $(Cl^\circ)_\ell$ для всех ℓ, или на $(Cl^\circ_\ell)^\wedge = \mathbb{Z}_\ell^{2g}$. Это значит, что φ представляется некоторой $(2g, 2g)$ матрицей Φ с элементами из $\mathbb{Z}_\ell$.

А.Вейль показывает, что, во-первых,

$$\det(E - u\Phi) = F(u),$$

где $F(u)$ - многочлен в формуле (2), и что, во-вторых, существует некое скалярное произведение, относительно которого φ удовлетворяет соотношению $\varphi\varphi^* = qE$. Отсюда следует утверждение о корнях, составляющее гипотезу Римана.

Этим в модельной ситуации была реализована идея, восходящая к Гильберту, о том, что нули обычной $\zeta(s)$ или, точнее, функции Римана $\Xi(t)$ должны быть нулями некоего самосопряженного оператора.

В самое последнее время были получены новые результаты в этом круге идей.

Классический подсчет $\zeta(2m)$, объединенный с функциональным уравнением, дает

$$\zeta(1-2m) = (-1)^m \frac{B_{2m}}{2m}$$

Сравнения Куммера для чисел Бернулли показывают, что функция $\zeta(1-2m)$ p- адически непрерывна на любой арифметической прогрессии $m \equiv a\,(p-1)$. Леопольдт установил, что продолжение $\zeta(s)$ по непрерывности на целые p -адические числа является аналитической функцией всюду, кроме $s=1$, где у нее есть полюс порядка I с вычетом $1-\frac{1}{p}$.

Обнаружено, что нули этой p -адической ζ -функции Леопольдта тоже могут быть реализованы как собственные значения линейного оператора заданного на некотором пространстве.

Для конструкции этого пространства в функциональном случае мы рассматривали группу Cl°_k. Расширению поля констант в числовом случае соответствует присоединению корней из единицы. Рассмотрим поле

$$K_n = Q(s_n), \quad s_n^{p^{n+1}} = 1 .$$

Группы $(Cl\,K_n)_p$ связаны гомоморфизмами норм, и мы можем положить

$$T_p = \varprojlim (Cl K_n)_p$$

Эта группа является аналогом группы $Char(Cl_k^0)$ в функциональном случае; она имеет естественную структуру $\mathbb{Z}_p$-модуля.

На T_p действует также группа Галуа G поля $\bigcup_{n=1}^{\infty} K_n / K_0$ которая также изоморфна $\mathbb{Z}_p$ (не канонически! Любая образующая φ этой группы описывает действие T_p на всей $\mathbb{Z}_p$).

Ивасава получил важные, хотя и не окончательные результаты о строении T_p.

Он установил, что с точностью до групп конечного индекса (или "до изогении") всякий модуль над кольцом $\mathbb{Z}_p[G]$ с конечным числом образующих является прямой суммой модулей двух сортов U и V, таких что

$$U \approx \mathbb{Z}_p^{\gamma}, \quad V \approx (\mathbb{Z}/p^n\mathbb{Z})^{\infty}$$

(как $\mathbb{Z}_p$-модули, без учета действия G!). Неизвестно, могут ли модули типа V входить реально в T_p.

Из этого результата вытекает, что $|(Cl_{K_n})_p| = p^{\nu_n}$, где $\nu_n = A + Bn^K + Cp^n$ для некоторого K и всех $n \geqslant n_0$.

Ивасава нашел некоторые условия для того, чтобы $C \neq 0$ (они необходимы и достаточны, но их бесконечно много). Равенство $C = 0$ равносильно отсутствию в разложении T_p модулей типа V.

Допустим, что p таково, то есть $T_p \approx \mathbb{Z}_p^{\gamma}$. Тогда действие группы G на T_p равносильно представлению G матрицами порядка γ.

Ивасава доказал, что тогда характеристические корни образа некоторой образующей φ группы G в этом представлении совпадают с корнями ζ-функции Леопольдта.

Доказательство теоремы Ивасава и будет главной целью курса. Предварительно будут изучены алгебраические свойства разных типов дзета-функций.

ГЛАВА I

ζ-ФУНКЦИИ ОДНОМЕРНЫХ СХЕМ

§ I. ζ-функции схем

Мы будем рассматривать $\mathbb{Z}$-схемы X конечного типа. (При желании читатель может понимать под X аффинное или проективное алгебраическое многообразие над полем F_p (p - простое), или над кольцом целых чисел. В последнем случае нам придется рассматривать точки на "$\mathbb{Z}$-многообразии" с координатами в полях конечной характеристики - *horribili dictu*...).

Пусть $x \in X$ - замкнутая точка. Поле классов вычетов $\mathfrak{k}(x)$, следовательно, конечно. Положим

$$\zeta(s, X) = \prod_{x \in X} \frac{1}{1 - N(x)^{-s}}, \qquad N(x) = \#(\mathfrak{k}(x)),$$

где $\#A$ - число элементов множества A. Начнем с примеров.

Пример I. $X = \operatorname{Spec} F_p[t_1, \ldots, t_n]$. Пусть a_m - число замкнутых точек $x \in X$ с $N(x) = p^m$; тогда

$$\zeta(s, X) = \prod_{m=1}^{\infty} \frac{1}{(1 - p^{-ms})^{a_m}}$$

Число геометрических точек X со значениями в F_{p^m} равно p^{mn} ; отсюда без труда находим

$$p^{mn} = \sum_{k \mid m} k\, a_k$$

Положим $t = p^{-s}$ и

$$F(t) = \prod_{m=1}^{\infty} (1 - t^m)^{-a_m}$$

произведение, очевидно, существует как формальный ряд, и

$$\log F(t) = -\sum_{m=1}^{\infty} a_m \log (1 - t^m)$$
$$= \sum_{m,k} \frac{a_m t^{mk}}{k} = \sum_{e} \frac{t^e}{e} \sum_{m \mid e} a_m \cdot m$$
$$= \sum_{e} \frac{t^e}{e} p^{en} = -\log (1 - p^n t),$$

так что

$$F(t) = \frac{1}{1 - p^n t} .$$

Отсюда сразу же получаем

$$\zeta (s, \mathbb{A}^n(F_p)) = \frac{1}{1 - p^{n-s}}$$

Пример 2. Перемножая по всем p , получаем:

$$\zeta (s, \mathbb{A}^n(\mathbb{Z})) = \zeta (s - n) .$$

Пример 3. Представляя $\mathbb{P}^n$ в виде $\mathbb{A}^n \cup \mathbb{P}^{n-1}$, получаем

$$\zeta (s, \mathbb{P}^n) = \zeta (s, \mathbb{A}^n)\, \zeta (s, \mathbb{P}^{n-1}),$$

откуда

$$\zeta (s, \mathbb{P}^n(F_p)) = \prod_{k=0}^{n} \frac{1}{1 - p^{k-s}} ,$$

$$\zeta (s, \mathbb{P}^n(\mathbb{Z})) = \prod_{k=0}^{n} \zeta (s - n) .$$

Мы докажем сейчас один результат о сходимости формального ряда Дирихле

$$\zeta (s, X) = \prod_{x \in X} \frac{1}{1 - N(x)^{-s}} = \sum \frac{a_n}{n^s} .$$

(Существование этого формального ряда вытекает из того, что число точек x с фиксированной $N(x)$ конечно).

Граница сходимости будет оценена в терминах размерности схемы X . Напомним, что размерность X - это наибольшая длина цепочки замкнутых неприводимых подсхем $Y_0 \subset Y_1 \subset \dots \subset Y_n$.

Размерность $\mathbb{Z}$ -схем конечного типа конечна. Вычислять ее часто удобно с помощью следующих двух свойств:

I) Если $X = \bigcup_{i=1}^{a} X_i$, где X_i - замкнутые подсхемы X, то $\dim X = \max_i \dim X_i$.

2) Если X неприводима, обозначим через $R(X)$ поле рациональных функций на X и пусть $\operatorname{tr} R(X)$ - его степень трансцендентности над простым подполем. Тогда

$$\dim X = \begin{cases} \operatorname{tr} R(X) & \text{, если } \operatorname{char} R(X) \neq 0 \\ \operatorname{tr} R(X) + 1 & \text{, если } \operatorname{char} R(X) = 0. \end{cases}$$

Например, $\dim \operatorname{Spec} \mathbb{Z} = \operatorname{tr} Q + 1 = 1$.

Теперь мы можем сформулировать следующее утверждение:

Теорема I. Ряд Дирихле $\zeta(s, X)$ абсолютно сходится при $\operatorname{Re} s > \dim X$.

Доказательство. Поскольку $\zeta(s, X \cup Y) \leq \zeta(s, X)\zeta(s, Y)$, достаточно ограничиться рассмотрением неприводимых X. Далее, можно рассматривать лишь аффинные схемы.

Пусть $X = \operatorname{Spec} A$, где A - F_p - алгебра конечного типа. Согласно нормализационной теореме Нетер, существует конечный эпиморфизм $f: X \to X_0$, где $X_0^{(p)}$ - аффинное пространство над F_p, причем $\dim X = \dim X_0$. Пусть $x_0 = f(x)$, где $x \in X$ - любая замкнутая точка. Тогда $N(x_0) \leq N(x)$; кроме того, число прообразов точки x не превосходит $m = \deg f$. Отсюда следует, что

$$\zeta(s, X) \leq \zeta(s, X_0)^m$$

(в смысле почленного сравнения коэффициентов рядов Дирихле). Но для аффинных пространств X_0 утверждение теоремы верно: это следует из явного вычисления $\zeta(s, X_0)$ в примере 2.

Для случая алгебр конечного типа над $\mathbb{Z}$ то же рассуждение показывает, что $\zeta(s, X) \leq \prod \zeta(s, X_0^{(p)})^m$, откуда теорема легко следует.

А.Вейль в I947 году вычислил в явном виде ζ - функции гиперповерхностей вида $\sum_{i=1}^{n} a_i X_i^{r} = 0$. В той же заметке, основываясь на аналогии с топологической задачей о числе неподвижных точек непрерывного отображения, он высказал несколько гипотез о структуре ζ -функций проективных многообразий над полем F_q. Положим, как выше, $t = q^{-s}$, $Z(t) = \zeta(s, X)$. Гипотезы Вейля следующим образом формулируются в терминах функции $Z(t)$.

а) Функция $Z(t)$ рациональна. Если многообразие X неособое, проективное размерности n, то она удовлетворяет функциональному уравнению

$$Z\left(\frac{1}{q^n t}\right) = \pm q^{n\chi/2} t^{\chi} Z(t),$$

где χ - характеристика Эйлера многообразия X, которую можно определить, например, как $[\Delta_X \cdot \Delta_X]$, $\Delta_X \subset X \times X$ - диагональ.

б) Более точно, $Z(t)$ имеет вид:

$$Z(t) = \frac{F_1(t) \cdots F_{2n-1}(t)}{F_0(t) \cdots F_{2n}(t)},$$

где $F_i(t) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} t)$ - многочлен с целыми коэффициентами, степень которого b_i равна i -мерному числу Бетти многообразия X.

в) $|\alpha_{ij}| = q^{i/2}$ ("гипотеза Римана").

Все эти утверждения были доказаны самим Вейлем в случае $\dim X = 1$ и для абелевых многообразий. Рациональность $Z(t)$, в общем случае доказал Дворк (даже не предполагая проективности и отсутствия особых точек). Условное доказательство рациональности и функционального уравнения предложили Сэмпсон и Уошнитцер: они опираются на недоказанную гипотезу о том, что группа циклов с точностью до численной эквивалентности имеет конечное число образующих. Гротендик и М.Артин построили чисто алгебраическую теорию когомологий алгебраических многообразий, что позволило придать смысл утверждению относительно степеней B_i и доказать гипотезу б) (за исключением той части, где утверждается, что многочлены $F_i(t)$ имеют целые коэффициенты). Гипотеза Римана в общем случае не доказана.

Относительно ζ -функций общих схем X с полем $R(X)$ нулевой характеристики известно очень мало. Предполагается, что по крайней мере эти функции мероморфно продолжаются на всю s -плоскость и удовлетворяют на ней обычному функциональному уравнению. Это доказано лишь в очень немногих случаях (абелевы многообразия с большим кольцом комплексных умножений, некоторые специальные классы кривых).

§ 2. Одномерные схемы

I. Пусть X - неприводимая одномерная схема. Нетрудно описать все такие схемы X. Если $\mathrm{Char}\, R(x) = 0$, их типичным представителем является $\mathrm{Spec}\, O$, где O - кольцо $\mathbb{Z}$ - целых элементов поля $R(x) = K$, представляющего собой, разумеется, конечное расширение поля $\mathbb{Q}$, ζ - функция $\mathrm{Spec}\, O$ есть ζ - функция поля K в классическом смысле.

Аналогично, в случае $\mathrm{Char}\, R(x) \neq 0$, существует каноническая "наибольшая" схема с таким полем функций - геометрически неприводимая регулярная проективная кривая.

ζ -функции, стало быть, определяются в одномерном случае в терминах полей, если ограничиться максимальными схе-

мами. ζ -функция любой такой схемы отличается от максимальной конечным числом элементарных множителей вида $\frac{1}{1-q^{-s}}$

2. Мы изложим сейчас принадлежащую Ивасаве и Тэйту интерпретацию ζ - и L -функций одномерных полей в виде некоторых интегралов.

Пусть K - одномерное поле, p - его простые дивизоры. (В том числе и бесконечные). Обсудим вопрос о характерах, которые мы должны ввести. Отметим, что в арифметике нас интересуют лишь периодические характеры: $\chi(n_1) = \chi(n_2)$ при $n_1 \equiv n_2 \pmod m$. Распространяя χ на рациональные числа, мы получаем $\chi(u) = 1$ при $u \equiv 1 \pmod m$. Мы истолковываем это равенство как некоторое условие непрерывности, оправдывая последующее введение характеров на группе иделей.

Пусть K_p - p -адическое пополнение поля, K, χ - некоторый характер K. Для всякого элемента $\alpha \in K_p^*$, положим $C(\alpha) = \chi(\alpha)\|\alpha\|_p^s$, где $s \in \mathbb{C}$; это квазихарактер то есть гомоморфизм $K_p^* \to \mathbb{C}$. Он равен I на единицах $\mathcal{U}_p$ поля K_p^*; $\chi(\alpha)$ определяется как $\chi(p)^{\nu_p(\alpha)}$.

Квазихарактер C называется неразветвленным, если он равен I на единицах; $\chi(\alpha)\|\alpha\|_p^s$ неразветвлен.

По квазихарактеру C можно построить гомоморфизм $|C|: K_p^* \to \mathbb{R}_+^*$; он заведомо неразветвлен, ибо $\mathcal{U}_p$ компактна, а в $\mathbb{R}_+^*$ компактных подгрупп нет. Полагая $|C(\alpha)| = \varphi(\alpha)$, получаем отсюда

$$\varphi(\alpha) = \|\alpha\|_p^{\sigma}, \quad \sigma \in \mathbb{R}$$

Число $\sigma = \mathrm{Re}\, C$ называется вещественной частью квазихарактера C. В дальнейшем мы будем считать, что $\mathrm{Re}\, C > 0$, и интерпретируем элементарный множитель $\frac{1}{1-C(P)}$ L -функции как некоторый интеграл по локально компактной группе K_p^*.

Имеем $K_p^* = \bigcup_{n\in\mathbb{Z}} \pi^n \mathcal{U}$, где $v_p(\pi) = 1$.

Вычислим сначала $\int_{\pi^n\mathcal{U}} c(\alpha)d\mu$. Положив $\alpha = \pi^n\varepsilon$, получим

$$\int_{\pi^n\mathcal{U}} c(\alpha)d\mu = \Big(\int_{\mathcal{U}} c(\varepsilon)d\mu\Big)\cdot c(\pi)^n = \mu(\mathcal{U})\cdot c(\pi)^n,$$

если c неразветвлен. Нормируем μ так, чтобы $\mu(\mathcal{U})=1$. Если $\operatorname{Re} c>0$, отсюда следует, что $c(\alpha)$ интегрируема на $\mathcal{O}_p - \{0\} = \bigcup_{n\geq 0} \pi^n\mathcal{U}$, и

$$\int_{\mathcal{O}_p-\{0\}} c\,d\mu = \sum_{n\geq 0}\int_{\pi^n\mathcal{U}} c\,d\mu = \sum_{n\geq 0} c(\pi)^n = \frac{1}{1-c(\pi)}.$$

Более существенно, что все произведение локальных множителей L-функции тоже можно интерпретировать как инвариантный интеграл по некоторой группе.

Естественно, нужно начать с произведения $\prod K_p^*$; однако, оно слишком велико, и следует ограничиться подгруппой иделей $\mathcal{J}_k$, элементы $(\dots \alpha_p \dots)$ которой характеризуются тем, что для почти всех p $\alpha_p \in \mathcal{U}_p$. Группа $\mathcal{J}_k$ топологизируется окрестностями единицы

$$\prod_{p\in S} V_p \times \prod_{p\notin S} \mathcal{U}_p$$

где S - конечные множества, V_p - окрестности 1 в K_p^*.

В этой топологии $\mathcal{J}_k$ локально компактна.

Мы будем интегрировать на $\mathcal{J}_k$ лишь очень простые функции вида

$$f(a) = \prod_p f_p(a_p)$$

Мера на $\mathcal{J}_k$ задается так. Для любого конечного множества простых S положим

$$\mathcal{U}_S = V_S \times \mathcal{U}_S^\circ,$$

где

$$V_S = \{(\underbrace{\dots \alpha_p \dots}_{S} \mid 1\dots 1\dots),\ \alpha_p\in K_p^*,\ V_S \approx \prod_{p\in S} K_p^*$$

$$\mathcal{U}_S^\circ = \{(\underbrace{1\dots 1}_{S} \mid \dots \alpha_p \dots)\},\ \alpha_p \in \mathcal{U}_p.$$

$\mathcal{U}_S$ - открытая подгруппа, V_S локально компактна, $\mathcal{U}_S^\circ$ компактна. Достаточно задать меру на $\mathcal{U}_S$, чтобы она однозначно продолжалась на всю $\mathcal{J}_k$. Поступим так: пусть μ_p - локальные меры, $\mu_p(\mathcal{U}_p)=1$; положим тогда

$$\int_{\mathcal{U}_S} \prod f_p(a_p)\,d\mu = \prod_p \int f_p\,d\mu_p$$

(Важна редукция задачи к введению меры на произведении компактной и конечного числа локально компактных групп, которая и позволяет провести доказательство корректности; детали см. в книге А.Вейля "Интегрирование на топологических группах").

§ 3. Характеры Гекке

Мы сейчас систематически исследуем обобщения классических характеров, встречающиеся в излагаемой теории. Начнем с частных случаев, расположив их в порядке возрастающей общности.

Пусть k - одномерное поле, Cl_k - группа его классов дивизоров (степени нуль в функциональном случае). В теории чисел естественно появляются ее характеры χ (и связанные с ними L -функции $\sum_{\alpha} \frac{\chi(\alpha)}{N(\alpha)^s}$). Их можно рассматривать как характеры группы иделей из-за существования стандартного гомоморфизма $J_k \to D$ (D - группа дивизоров):

$$(\dots \alpha_p \dots) \longrightarrow \prod_{P \setminus P_\infty} p^{\nu_p(\alpha_p)}$$

Так получаются характеры группы J_k, тривиальные на группе главных иделей P_k.

Второй важный класс теоретико-числовых характеров - это "периодические" характеры группы дивизоров, - точнее, подгруппы D_m, состоящей из элементов, взаимно простых с некоторым "ведущим модулем" m. "Периодичность" означает, что характер тривиален на дивизорах вида (α), $\alpha \equiv 1 \mod m, \alpha \in k$.

Для того, чтобы перенести эти характеры на группу иделей, нужно сначала ограничиться рассмотрением подгруппы вида

$$J_m = \{\alpha \mid \forall\, P/m \ , \ \alpha_p \equiv 1 \mod m_p\}.$$

Тогда определен естественный гомоморфизм $J_m \to D_m$, который переносит характеры с D_m на J_m. Продолжение его на J_k неоднозначно, если не вводить дополнительных ограничений. Заметим теперь, что $J_k = J_m P_k$, так что во всяком случае своими ограничениями на J_m и P_k любой характер определяется. Наоборот, данные два характера групп J_m и P_k продолжаются до одного и того же характера J_k, если они совпадают на $J_m \cap P_k$; теоретикочисловые характеры на этом пересечении тривиальны.

Распространим теперь эти характеры с J_m на J_k, так, чтобы они были тривиальными на P_k. Мы получаем таким образом "характеры Дирихле". Они тривиальны на связной компоненте группы J_k (которой, впрочем, нет в функциональном случае), потому что бесконечные точки в их определении не учитываются.

Гекке ввел новый класс характеров, который не обладает этим последним свойством.

Собственное определение Гекке относилось к группе D_m. Рассмотрим группы

$$P_m = \{\alpha \in k^* \mid \alpha \equiv 1 \mod m\}, \quad k_{P_\infty}^* = \prod_{P/P_\infty} k_p^* = (k \otimes_{\mathbb{Z}} \mathbb{R})^*$$

Имеем

$$P_m \subset k^* \subset k_{P_\infty}^*$$

Гекке рассматривает те характеры χ группы D_m, которые на подгруппе $(P_m) \subset D_m$ индуцированы некоторым характером

Ψ группы Ли $k^*_{p_\infty}$.

Теперь мы перенесем определение Гекке на группу иделей. Положим $\mathcal{J}^\circ_m = \{\alpha \in \mathcal{J}_m \mid \alpha_p = 1 \text{ при } P/P_\infty\}$. Перенесем характер Гекке χ с $\mathcal{D}_m$ на $\mathcal{J}^\circ_m$ с помощью естественного гомоморфизма $\mathcal{J}^\circ_m \to \mathcal{D}_m$. Группа $V_\infty \subset \mathcal{J}_k$ отождествляется с $k^*_{p_\infty}$; кроме того,

$$\mathcal{J}_m = \mathcal{J}^\circ_m \times V_\infty ;$$

теперь мы можем рассмотреть характер группы $\mathcal{J}_m$

$$\widetilde{\chi} = (\chi, \Psi^{-1})$$

Остается еще продолжить $\widetilde{\chi}$ на $\mathcal{J}_k$. На главных иделях $\alpha \in \mathcal{J}_m \cap P_k$ снова получаем

$$\widetilde{\chi}(\alpha) = \chi(\alpha)\Psi^{-1}(\alpha) = 1,$$

так что естественно продолжить $\widetilde{\chi}$ на $\mathcal{J}_k$ так, чтобы он был тривиален на P_k и, значит, определен на $C_k = \mathcal{J}_k / P_k$.

Покажем, что таким способом получаются все непрерывные характеры группы C_k. Пусть дан такой характер на C_k. Рассмотрим его на $\mathcal{J}_k$; в некоторой окрестности единицы на $\mathcal{J}_k$ он тривиален, поэтому он тривиален на некоторой группе $\mathcal{J}^\circ_m$.

Пусть $S = \{P \mid P/m\}$, $\mathcal{J}_S = \{(\dots \alpha_p \dots) \mid \alpha_p = 1,\ p \in S\}$, $U_S = \mathcal{J}_S \cap U$. Тогда $\mathcal{D}_m = \mathcal{J}_S / U_S$. Теперь каждый главный идель α представим в виде

$$(\alpha) = (\alpha)_0 (\alpha)_\infty ,$$

где $(\alpha)_0$ имеет компоненты 1 в P/P_∞, а $(\alpha)_\infty$ компоненты 1 в $P \setminus P_\infty$. Имеем

$$\chi((\alpha)_0) = \chi^{-1}((\alpha)_\infty).$$

В свою очередь, при $\alpha \equiv 1 \bmod m$ получаем, что $\chi((\alpha)_0) = 1$. Это показывает, что по χ восстанавливается соответствующий характер Гекке.

С каждым таким χ связывается L-ряд $\sum_{\alpha \in \mathcal{D}_m} \frac{\chi(\alpha)}{N(\alpha)^s}$.

Попытаемся теперь описать группу характеров Гекке.

Пусть H - связная компонента группы классов иделей C_k; рассмотрим последовательность

$$1 \to H^\circ \to C^\circ_k \to \mathcal{D}^\circ \to 1,$$

где C°_k - группа классов иделей поля k с нормой единица и двойственную последовательность

$$1 \to \hat{\mathcal{D}}^\circ \to \hat{C}^\circ_k \to \hat{H}^\circ \to 1$$

($\hat{C}^\circ_k = \mathrm{Char}\, C^\circ_k$ и т.п.). Из сказанного ясно, что характер Гекке χ принадлежит $\hat{\mathcal{D}}$, если соответствующий характер Ψ тривиален; верно и обратное. Выясним, какие характеры Ψ определяют характеры Гекке.

Для всех $\alpha \equiv 1\ (m)$ мы должны иметь

$$\chi((\alpha)) = \Psi^{-1}(\alpha) ;$$

таким образом, характер ψ должен зависеть лишь от дивизора (α), и потому быть равным I на группе единиц поля, содержащихся в $k^*_{p_\infty}$

Имеем

$$k^*_{p_\infty} = \prod_{p/p_\infty} k^*_p = K \times \mathbb{R}_+^{s+t},$$

где K - максимальная компактная подгруппа; в самом деле, локальные множители устроены так:

$$k_p = \begin{cases} \mathbb{C} & \text{, тогда } k^*_p = \mathcal{U}(1) \times \mathbb{R}_+ \\ \mathbb{R} & \text{, тогда } k^*_p = \mathcal{O}(1) \times \mathbb{R}_+ \end{cases}$$

Пусть s - число вещественных, t - число комплексных точек. Тогда

$$(k^*_{p_\infty})^\wedge = \mathbb{Z}^t \times (\mathbb{Z}/2\mathbb{Z})^s \times \mathbb{R}_+^{s+t}$$

В явном виде: любой характер группы $k^*_{p_\infty}$ на погруженной в нее группе k^* задается формулой

$$\psi(\alpha) = \prod_\nu (\alpha_\nu/|\alpha_\nu|)^{f_\nu} |\alpha_\nu|^{i\varphi_\nu}$$

где α_ν - все сопряженные к α, $f_\nu \in \mathbb{Z}$, $\varphi_\nu \in \mathbb{R}$.

Пусть теперь $E(m)$ - группа единиц $\equiv 1 \bmod m$. Мы докажем позже следующий результат:

Лемма (Шевалле). В группе единиц E любая подгруппа конечного индекса содержит подгруппу вида $E(m)$ для некоторого m.

Поэтому достаточно требовать, чтобы ψ был тривиален на подгруппе $E(n)$ для некоторого целого n.

Пусть ψ', ψ'' - компоненты ψ на K и $\mathbb{R}^{s+t}$ соответственно. Тогда наше условие, как следует из теоремы Дирихле, равносильно тому, что в разложении

$$\mathbb{R}^{s+t} = \mathbb{R}^{s+t-1} \times \mathbb{R},$$

где E с помощью логарифмирования вкладывается в первый множитель, ψ'' тривиализируется на некоторой решетке $\log(E(n)) \subset \mathbb{R}^{s+t-1}$. Следовательно, группа характеров ψ изоморфна

$$\mathbb{Z}^t \times Q^{s+t-1} \times \mathbb{R}$$

Последнему множителю соответствует характер

$$\alpha \to (N\alpha)^{ia}, \quad a \in \mathbb{R}.$$

Он малоинтересен, ибо L-функции, связанные с ним, выражаются через простейшую ζ-функцию сдвигом аргумента.

Первые два множителя могут быть нетривиальны лишь для полей, отличных от Q.

Рассмотрим простые примеры.

Пример I. k - квадратичное мнимое расширение Q. Значит, $k^*_p = \mathcal{U}(1) \times \mathbb{R}_+$; для всякого $z \in k$

$$\psi(z) = \left(\frac{z}{|z|}\right)^f |z|^{i\varphi}, \quad f \in \mathbb{Z}, \ \varphi \in \mathbb{R}$$

Часть $|z|^{i\varphi}$ неинтересна по соображениям, указанным выше; характеры $\left(\frac{z}{|z|}\right)^f$ уже очень интересны. Связанные с ними L-ряды $\sum \frac{(\alpha/|\alpha|)^f}{N(\alpha)^s}$, как и все L-ряды с характерми Гекке, продолжаются мероморфно на всю s-плоскость с помощью функционального уравнения и доставляет сведения о распределении простых чисел поля k в секторах.

Пример 2. k - квадратичное вещественное поле. Здесь $k^*_{p\infty} = R^* \times R^*$ и

$$\psi(\alpha) = \alpha^{i\varphi} N(\alpha)^{ia},$$

где $\frac{\log \varepsilon}{2\pi i} \cdot \varphi \in \mathbb{Q}$, $a \in \mathbb{R}$, ε - основная единица поля.

(Последнее можно усмотреть непосредственно: для некоторого $n \in \mathbb{Z}$ и для основной единицы ε мы должны иметь $(\varepsilon_1^{i\varphi_1} \varepsilon_2^{i\varphi_2})^n = 1$, что дает, ввиду $\varepsilon_1 \varepsilon_2 = 1$:

$$\varphi_1 = \varphi_2 + \left(2\pi / \log \varepsilon\right) \cdot \rho, \quad \rho \in \mathbb{Q}$$

и

$$\psi(\alpha) = N(\alpha)^{i\varphi_1} \cdot \alpha^{2\pi i \rho / \log \varepsilon}).$$

Приведем теперь доказательство леммы Шевалле.

Пусть E группа единиц поля k, $E(m) = \{\varepsilon \in E \mid \varepsilon \equiv 1 \,(m)\}$, где m - некоторый целый дивизор. Мы хотим доказать, что в

любой подгруппе $E_0 \subset E$ конечного индекса $n = (E : E_0)$ содержится группа вида $E(m)$.

Пусть сначала $\zeta_n \in k$, где ζ_n - первообразный корень из I степени n. Пусть $E = U \varepsilon_i \cdot E^n$, $K_i = k(\sqrt[n]{\varepsilon_i})$. Воспользуемся тем, что для каждого абелева расширения K поля k есть бесконечно много простых дивизоров k, которые в K остаются простыми.

Выберем простые дивизоры p_i поля k такие, что $(p_i, n) = 1$ и p_i остается простым в K_i, и положим $m = \prod p_i$. Я утверждаю, что $\varepsilon \equiv 1 \bmod m \Rightarrow \varepsilon = \varepsilon_0^n$, $\varepsilon_0 \in E$. Иначе $\varepsilon = \varepsilon_i \cdot \varepsilon_0^n$ и $k(\sqrt[n]{\varepsilon}) = k(\sqrt[n]{\varepsilon_i})$ и, значит, p_i не вполне распадается в $k(\sqrt[n]{\varepsilon})$, что невозможно, ибо $x^n - \varepsilon \equiv x^n - 1 \bmod p_i$. Если же $\zeta_n \notin k$, то следует рассмотреть сначала поле $k' = k(\zeta_n)$. Проведем дальше прежнее рассуждение по отношению к k'; мы получим, что для некоторого m' в k' $\varepsilon \equiv 1 \bmod m' \Rightarrow \varepsilon = \varepsilon_0^n$ в поле k'. Поэтому $k \subset k(\sqrt[n]{\varepsilon}) \subset k'$, значит, теперь $k(\sqrt[n]{\varepsilon})/k$ - абелево поле, и применяя то же рассуждение второй раз, можно увеличить модуль m' так, чтобы заставить ε стать n-й степенью уже в k.

На этом мы закончили описание характеров Гекке. Нужно еще сказать несколько слов о квазихарактерах: $c : C_k \to \mathbb{C}^*$. Напомним определение гомоморфизма

$$\| \| : C_k \to \mathbb{R}_+^*$$

Полагая для $\alpha_p \in k_p$: $\|\alpha_p\|_p = N(p)^{-\nu_p(\alpha_p)}$ при $p \nmid p_\infty$, $\|\alpha_p\|_p = |\alpha_p|$ при $k_p = \mathbb{R}$ и $\|\alpha_p\|_p = |\alpha_p|^2$ при $k_p = \mathbb{C}$, имеем:

$$\|(\ldots \alpha_p \ldots)\| = \prod_p \|\alpha_p\|_p .$$

Основное свойство этого гомоморфизма состоит в том, что он тривиален на подгруппе главных иделей P_k

Определим теперь для любого $s \in \mathbb{C}^*$ квазихарактер

$$\omega(s) : C_k \to \mathbb{C}^*$$

формулой

$$\omega(s)(a) = \|a\|^s$$

Пусть $C_k^\circ = \{a \in C_k \mid \|a\| = 1\}$; гомоморфизм $C_k \to R_+^*$ допускает сечение $R_+^* \to C_k$, так что $C_k \approx C_k^\circ \times R_+^*$ (явный вид сечения: $x \to (\dots 1 \dots 1; \underbrace{x^{\pm}, \dots, x^{\pm}}_{P/P_0})$, $n = (k:\mathbb{Q})$). Из теоремы Дирихле легко вывести, что группа C_k° компактна, поэтому значения любого квазихарактера c на C_k° принадлежат $U(1)$; что до квазихарактеров R_+^*, они все имеют вид $c(x) = x^s$, $s \in \mathbb{C}$

Поэтому для любого c имеем

$$c(a) = \chi(a)\|a\|^s,$$

где χ – некоторый характер J_k. Это разложение не определяет χ однозначно, ибо $\|a\|^{it}$, $t \in R$ можно отнести к $\chi(a)$. Во всяком случае, $Re\, s$ определяется канонически; мы будем писать $Re\, c$ вместо $Re\, s$

§ 4. Возвращение к L -функциям: план действий

Положим $f_p = \delta_{\mathcal{O}_p - \{0\}}$ (характеристическая функция множества $\mathcal{O}_p - \{0\} \in k_p^*$). Напомним, что, как мы доказали, для любого квазихарактера c

$$\frac{1}{1-c(p)} = \int_{\mathcal{O}_p - \{0\}} c(p)\, d\mu_p^* = \int_{k_p^*} f_p\, c(p)\, d\mu_p^* ,$$

так, что, полагая для всякого иделя a

$$f(a) = \prod_a f_p(a_p)$$

имеем:

$$L(s,\chi) = \int_{J_k} f c\, d\mu^*$$

Здесь существенно появление множеств $\mathcal{O}_p - \{0\}$, которые характерны для аддитивной, а не мультипликативной теоремы. Это весьма важно; последующая теория использует мультипликативную и аддитивную структуры вместе.

Для систематического использования этого обстоятельства следует ввести кольцо аделей $A_k \subset \prod_p k_p$, $(\dots a_p \dots) \in A_k \Leftrightarrow a_p \in \mathcal{O}_p$ для почти всех p .

Имеем $J_k \subset A_k$; на самом деле, J_k – группа единиц в A_k .

Естественный заменой L -функций в этом контексте служат интегралы вида $\int_{\mathcal{Y}_k} f c\, d\mu^*$, где f - ограничение на $\mathcal{Y}_k$ некоторой функции, заданной на A_k. Классические L -функции получаются, когда f - характеристическая функция множества $\prod_p \mathcal{O}_p$

Положим

$$\zeta(f,c) = \int_{\mathcal{Y}_k} f c\, d\mu^* \qquad (4.I)$$

Рассмотрим сначала простейшую модель этой ситуации, заменив $\mathcal{Y}_k$ на конечное поле F_q ; тогда

$$f \in L'(F_q^+) = Map(F_q^+, \mathbb{C}), \quad c = \chi : F_q^{+*} \to U(1)$$

Тогда

$$\zeta(f,\chi) = \sum_{a \in F_q^{+*}} f(a)\chi(a)$$

$\zeta(f,\chi)$ есть функционал от f , так что

$$\zeta(f,\chi) \in (L(F_q^+))^\wedge = L(\hat{F}_q^+)$$

Для вычисления этого функционала на всех f достаточно знать его значения на характерах $\psi : F_q^+ \to U(1)$,т.е.

суммы Гзусса

$$\zeta(\psi,\chi) = \sum_{a \in F_q^+} \psi(a)\chi(a)$$

Это объясняет появление таких сумм в функциональных уравнениях для L -рядов.

Вернемся теперь к общему случаю (4.I).

Пусть G - любая локально компактная абелева группа; для любой функции $f \in L'(G)$ и $\chi \in \hat{G}$ положим

$$\hat{f}(\chi) = \int_G f(g)\chi(g)\, d\mu_G$$

Тогда имеем

$$\hat{\hat{f}}(g) = const \cdot f(-g)$$

Меры на G и $\hat{G}$ можно нормировать так, чтобы $const = 1$: мы назовем такие меры согласованными.

Пример I. $G = \mathbb{Z}$, $\hat{G} = U(1)$;

$f = (\dots a_n \dots)_{n \in \mathbb{Z}}$; $\hat{f}(x) = \sum_n a_n e^{2\pi i n x}$;

переход от $\hat{f}$ к f есть восстановление по функции ее коэффициентов Фурье.

Пример 2. $G = \mathbb{R}$, $\hat{G} = \mathbb{R}$;

$$\hat{f}(x) = \frac{1}{\sqrt{2\pi}} \int f(t)\, e^{itx}\, dt$$

– преобразование Фурье.

Пример 3. Обобщение примера I: G – дискретная группа; полагая

$$\int_G f = \sum f(g),$$

получим, что согласованная с этой мера на $\hat{G}$ определяется формулой $\mu(\hat{G}) = 1$. (Для проверки достаточно вычислить константу для какой-нибудь функции $f(\chi)$ на $\hat{G}$; пусть $f(\chi) \equiv 1$; тогда

$$\hat{f}(g) = \int_{\hat{G}} f(\chi)\, g(\chi)\, d\mu_{\hat{G}} = \begin{cases} 0, \text{ если } g \neq e \\ \mu(\hat{G}), \text{ если } g = e \end{cases}$$

откуда легко следует требуемое).

Мы применим преобразование Фурье к группе $A_k = A_k^+$. Мы установим, что $\hat{A}_k = A_k$ (канонический изоморфизм групп и конструкция меры, согласованной с самой собой) и докажем, что

$$\zeta(\hat{f}, \hat{c}) = \zeta(f, c)$$

где $\hat{c}$ определяется формулой

$$\hat{c}(\alpha) = \|\alpha\|\, c(\alpha)^{-1} = \omega(\alpha)\, c^{-1},$$

что и дает функциональное уравнение.

§ 5. Анализ Фурье

Предложение. Группа k_p^+ двойственна себе.

Доказательство. Мы построим некоторый конкретный характер $\lambda_p : k_p^+ \to \mathcal{U}(1)$ и затем установим изоморфизм $k_p^+ \to (k_p^+)^\wedge$ формулой

$$\gamma_x(y) = \lambda_p(xy), \quad x, y \in k_p^+$$

Характеры λ_p мы должны ввести на всевозможных локально компактных топологических полях. Они являются расширениями соответствующих простых полей, с которых мы и начнем.

а. $k_p = R$, $\lambda_\infty(x) = e^{-2\pi i x}$

б. $k_p = Q_p$. Для любого $\alpha \in Q_p$ существует элемент $a \in \mathbb{Z}[\frac{1}{p}]$ такой, что $\alpha - a \in \mathbb{Z}_p$; положим

$$\lambda_p(\alpha) = e^{2\pi i a}$$

(определение не зависит от выбора a, которое определено с точностью до слагаемого из $\mathbb{Z}$).

в. $k_p = F_q((t))$, q – простое. Выберем стандартный изоморфизм $\varphi : F_q^+ \to \mathcal{U}(1)$ и положим

$$\lambda(\alpha) = \varphi(\mathrm{Res}(\alpha\, dt))$$

где Res означает вычет дифференциала при $t = 0$

Теперь для всякого конечного расширения $K_p \supset k_p$, сепа-

рабельного над простым простым подполем k_p, положим

$$\lambda_p(\alpha) = \lambda(S_{K_p/k_p}(\alpha))$$

где S_{K_p/k_p} – след.

Следует проверить, что отображение

$$x \to \chi_x(y) = \lambda_p(xy)$$

действительно дает изоморфизм $k_p^+ \to (k_p^+)^\wedge$. Очевидно, что это вложение. Формальная проверка, которую мы опускаем, показывает, что это гомеоморфизм группы k_p^+ на ее образ. Поэтому достаточно доказать, что образ k_p^+ всюду плотен. Иначе говоря, нужно проверить, что $\chi_x(y_0) = 0$ для всех $x \Rightarrow y_0 = 0$, что тривиально.

Предложение доказано.

Пусть теперь k – глобальное поле, A_k – его группа аделей. Положим для $\xi \in A_k$

$$\Lambda(\xi) = \prod_p \lambda_p(\xi_p)$$

Определение корректно, ибо для почти всех p $\lambda_p = 1$ на $\mathcal{O}_p$ (см. определения).

Предложение. Отображение $A_k \to \hat{A}_k^+$, заданное формулой

$$\xi \to \chi_\xi, \quad \chi_\xi(\eta) = \Lambda(\xi\eta)$$

является изоморфизмом. (Доказательство совершенно аналогично предыдущему).

Рассмотрим теперь подгруппу главных аделей $k^+ \subset A_k$. Легко проверить, что она дискретна.

Предложение. а) Группа A_k^+/k^+ компактна.

б) $(k^+)^\perp = k^+$

Доказательство. а) Допустим сначала, что k – числовое поле. Пусть $\Omega \subset A_k$ – множество аделей $(\dots \xi_p \dots)$ таких, что $\xi_p \in \mathcal{O}_p$ при $p \nmid p_\infty$. Обозначая через $\Omega_0 \subset \Omega$ подмножество аделей с $\xi_p = 0$ при $p \mid p_\infty$, имеем

$$\Omega = \Omega_0 \times k_{p_\infty}^+$$

$k_{p_\infty}^+$ есть $\mathbb{R}$-алгебра размерности $[k:\mathbb{Q}] = n$. Теорема об остатках показывает, что

$$k^+ + \Omega = A_k$$

Достаточно проверить, что $\Omega/\Omega \cap k^+$ компактна, потому что A_k/k^+ и $\Omega/\Omega \cap k^+$ изоморфны как топологические группы.

Но $k^+ \cap \Omega = \mathcal{O}_k$ (кольцо целых чисел поля k). Рассмотрим проекцию

$$(\Omega_0 \times k_{p_\infty}^+)/\mathcal{O}_k \to k_{p_\infty}^+/\mathcal{O}_k$$

Ее ядро есть $(\Omega_0 + \mathcal{O}_k)/\mathcal{O}_k \approx \Omega_0$, а образ $k_{p_\infty}^+/\mathcal{O}_k$; (отсюда легко усмотреть, что $\mathcal{O}_k$ дискретна в Ω: уже ее проекция в $k_{p_\infty}^+$ дискретна). Более того, $k_{p_\infty}^+/\mathcal{O}_k$ есть

n -мерный тор. Группа A_k/k^+, следовательно, компактна, и изоморфна расширению тора с помощью вполне несвязной группы Ω_0. Сама она, как мы убедимся, связна.

В случае, когда k - функциональное поле, следует представить k в виде сепарабельного конечного расширения своего подполя $\mathbb{F}_q(t)$. Выделим в качестве P_∞ дивизор полюсов t; пусть $\mathcal{O}_k$ - целое замыкание $\mathbb{F}_q[t]$ в поле k Все доказательство проходит без особых изменений. Следует лишь объяснить, почему $\mathcal{O}_k$ дискретна в $k^+_{P_\infty}$. Имеем $k^+_{P_\infty} \approx \mathbb{F}_q((\tau))^n$, $\tau = t^{-1}$, а $\mathcal{O}_k \subset k^+_{P_\infty}$ - свободный модуль над $\mathbb{F}_q[t] \subset \mathbb{F}_q((\tau))$ ранга n, базис которого одновременно является $\mathbb{F}_q((\tau))$ -базисом $k^+_{P_\infty}$. Отсюда вытекает, что $\mathcal{O}_k$ дискретна в $k^+_{P_\infty}$ и

$$\mathcal{O}_k/k^+_{P_\infty} \approx (\tau\, \mathbb{F}_q[[\tau]])^n \approx (\mathbb{F}_q[[\tau]])^n$$

В качестве приложения этого результата мы можем определить важный инвариант поля k - его род.

Именно, в функциональном случае можно действовать более естественно, не вводя P_∞ и положив

$$\overline{\Omega} = \{(\ldots \xi_P \ldots) \mid \xi_P \in \mathcal{O}_P \text{ для всех } P\}$$

Тогда группа $A_k/(k^+ + \overline{\Omega})$, будучи компактной (как образ A_k/k^+) и дискретной (как образ $A_k/\overline{\Omega}$), конечна. Следовательно, $\dim_{\mathbb{F}_q} A_k/(k^+ + \overline{\Omega}) < \infty$. Эта размерность называется родом поля k. Приведенное определение рода показывает, что это - размерность пространства линейных условий, которые следует наложить на главные части так, чтобы для них была разрешима аддитивная проблема Кузена.

б) Покажем теперь, что $(k^+)^\perp = k^+$. Включение $(k^+)^\perp \subset k^+$ следует из того, что $\Lambda(\xi) = 1$ для главных аделей ξ. (Действительно, в числовом случае $\Lambda_k(\alpha) = \Lambda_{\mathbb{Q}}(\zeta_{k/\mathbb{Q}}(\alpha))$, а для рациональных чисел α определение показывает, что $\Lambda_{\mathbb{Q}}(\alpha) = 1$ В функциональном случае вместо $\mathbb{Q}$ следует, как обычно рассмотреть $\mathbb{F}_q(t)$).

Теперь $(k^+)^\perp/k^+ \subset A_k/k^+$, так что $(k^+)^\perp/k^+$ компактна. С другой стороны, она двойственна A_k/k^+ и потому дискретна. Значит, она конечна. Но $(k^+)^\perp$ является векторным пространством над k^+, потому оно одномерно.

Теорема доказана.

Из нее следует, что $\hat{k}^+ = A_k/k^+$; так как в $\hat{k}^+$ нет элементов конечного порядка (в числовом случае), группа A_k/k^+ связна, как и утверждалось.

Вычисление самосогласованной меры.

Начнем с локального числового случая.

Пусть $p \nmid p_\infty$; положим $\varphi(g) = \delta_{\mathcal{O}_p}$. Воспользуемся следующим простым результатом:

Лемма. Пусть $H \subset G$ - открытая компактная подгруппа, $H^\perp \subset \hat{G}$ - ее аннулятор. Тогда

$$\hat{\delta}_H = \mu(H)\, \delta_{H^\perp}$$

Доказательство.

$$\hat{\delta}_H(\chi) = \int_G \delta_H(g)\, \chi(g)\, d\mu = \int \chi(g)\, d\mu = \begin{cases} 0, & \chi \notin H^\perp \\ \mu(H), & \chi \in H^\perp \end{cases}$$

Применим эту лемму к случаю $G = k_p^+$, $H = \mathcal{O}_p$. Вспоминая явное определение изоморфизма $\hat{k}_p^+ \to k_p^+$, получаем:

$$\mathcal{O}_p^\perp = \{ y \in k_p \mid \forall x \in \mathcal{O}_p, e^{2\pi i \lambda_p(S(xy))} = 1 \}$$

Иначе говоря,

$$\mathcal{O}_p^\perp = \{ y \in k_p \mid S(y\mathcal{O}_p) \subset \mathcal{O}_p \},$$

то есть $\mathcal{O}_p^\perp = \mathcal{D}_p^{-1} \supset \mathcal{O}_p$, где $\mathcal{D}_p$ – дифферента k_p. Следовательно,

$$\hat{\delta}_{\mathcal{O}_p} = \delta_{\mathcal{D}_p^{-1}} \cdot \mu(\mathcal{O}_p)$$

Аналогично, для любого целого идеала $a \subset \mathcal{O}$

$$\hat{\delta}_a = \delta_{a^{-1}\mathcal{D}^{-1}} \mu(a) = \delta_{\mathcal{D}^{-1}a^{-1}} \mu(\mathcal{O}) N(a)^{-1}$$

Применяя эту формулу дважды, получим:

$$\hat{\hat{\delta}}_{\mathcal{O}_p} = \delta_{\mathcal{O}_p} \mu(\mathcal{O})^2 \cdot N(\mathcal{D})$$

Следовательно, мера μ будет самосогласована, если

$$\mu(\mathcal{O}) = N(\mathcal{D})^{-\frac{1}{2}}$$

В случае $k_p = \mathbb{R}$ мера dx самосогласована: если $f(x) = e^{-\pi x^2}$, то полагая $\hat{f}(y) = \int_{\mathbb{R}} f(x) e^{2\pi i xy} dx$, имеем

$$\hat{f}(x) = f(x) = f(-x)$$

что доказывает требуемое.

Аналогично, при $k_p = \mathbb{C}$ самосогласована мера $2\,dx \wedge dy$ $(z = x + iy)$. Действительно, здесь

$$\chi_\omega(z) = e^{-4\pi i \operatorname{Re} z\omega};$$

полагая здесь $f(z) = e^{-2\pi|z|^2}$, как выше, получим

$$\hat{f}(z) = f(z)$$

Пусть теперь k – функциональное поле; $k \supset \mathbb{F}_q(t)$ – сепарабельное расширение. Пусть p – простой дивизор k

$$\mathcal{O}_p^\perp = \{ y \in k_p \mid \forall x \in \mathcal{O}_p, \operatorname{Res}_p(xy\,dt) = 0 \},$$

то есть

$$\mathcal{O}_p^\perp = \mathcal{O}_p \left(\frac{dt}{dz_p}\right)^{-1},$$

где τ_p - локальный параметр в кольце $\mathcal{O}_p$. Легкое вычисление тогда показывает, что самосогласованная мера определяется формулой

$$\mu(\mathcal{O}_p) = (N((dt)_p))^{-\frac{1}{2}}$$

где

$$N((dt)_p) = q^{\nu_p(dt)}$$

Вот приложение этого вычисления в функциональном случае: определяя меру на A_k как произведение локальных мер, имеем для кольца $\overline{\Omega}$ целых аделей:

$$\mu(\overline{\Omega}) = \prod_p N((dt)_p)^{-\frac{1}{2}} = q^{1-g} ,$$

где g - род k .

§ 6. Функциональное уравнение.

Формула Пуассона. Пусть f - непрерывная функция на A_k такая, что $|f|$ суммируема на $k \subset A_k$, $|\hat{f}|$ - суммируема и $\sum_\alpha |f(\xi+\alpha)|$ равномерно сходится на всяком компакте. Тогда

$$\sum_{\alpha \in k} f(\alpha) = \sum_{\alpha \in k} \hat{f}(\alpha)$$

Доказательство. Пусть $a = \xi + k^+ \subset A_k/k^+$, $\xi \in A_k$. Положим

$$\varphi(x) = \sum_{\alpha \in k} f(\xi+\alpha)$$

Для любых двух мер μ на A_k , $\tilde{\mu}$ на A_k/k^+ имеем

$$\int_{A_k/k^+} \left(\sum_\alpha f(\xi+\alpha)\right) d\tilde{\mu} = \text{const} \int_{A_k} f \, d\mu$$

(слева стоит инвариантный интеграл от f , так что можно воспользоваться единственностью). Пусть $\tilde{\mu}$ индуцирована мерой μ . Рассмотрим теперь $\hat{\varphi}(\beta)$, пользуясь тем, что $(k^+)^\perp = k^+$

$$\hat{\varphi}(\beta) = \int_{A_k/k^+} \varphi(x)(\beta,x)\, d\tilde{\mu} = \int_{A_k/k^+} \left(\sum_\alpha f(\xi+\alpha)(\beta,\xi+\alpha)\right) d\tilde{\mu} =$$

$$= \text{const} \int_{A_k} f(\xi)(\beta,\xi)\, d\mu = \text{const}\, \hat{f}(\beta)$$

Теперь пусть μ самосогласована. Тогда $\hat{\hat{\varphi}}(x) = \varphi(-x)$; но с другой стороны

$$\varphi(-x) = \sum_\alpha f(\xi+\alpha)$$

$$\hat{\hat{\varphi}}(x) = \text{const} \sum_\beta \hat{f}(\beta)(\beta,x)$$

Полагая здесь $\xi = 0$, получим

$$\sum_{\alpha \in k} f(\alpha) = const \sum_{\alpha \in k} \hat{f}(\alpha),$$

а применяя эту формулу дважды, находим $const = 1$

То, что $const = 1$, то есть самосогласованность μ, в числовом случае можно интерпретировать следующим образом.

Обозначим через D_0 – фундаментальный параллелепипед подгруппы $\mathcal{O}_k$ в k^+. Тогда $\Omega \times D_0$ есть фундаментальная область для k^+ в A_k. Мера $\Omega \times D_0$ равна I: это и есть условие самосогласованности меры. Но

$$\mu(\Omega_0 \times D_0) = \left(\prod_p \mu(\mathfrak{d}_p^{-1})\right) V,$$

где

$$V^2 = \det\left(\zeta(\omega_i \omega_j)\right),$$

$\omega_i - \mathbb{Z}$ – базис кольца $\mathcal{O}$. Следовательно, дискриминант поля есть произведение локальных дискриминантов.

Укажем теперь некоторые приложения формулы Пуассона. Пусть $k \supset \mathbb{F}_q(t)$ – функциональное поле. Для всякого дивизора $a = \prod p^{n_p}$ положим

$$a\bar{\Omega} = \{\xi \in A_k \mid \forall p,\ \xi_p \in p^{n_p}\mathcal{O}_p\}$$

и обозначим через δ_a характеристическую функцию множества $a\bar{\Omega}$, к которой и применим формулу

$$\sum_{\alpha \in k^+} \delta_a(\alpha) = \sum_{\alpha \in k^+} \hat{\delta}_a(\alpha)$$

Левая сумма есть число элементов конечного множества $a\bar{\Omega} \cap k^+$ Оно представляет собой линейное пространство – $\mathcal{L}(a^{-1})$ в классическом обозначении – размерности $l(a^{-1})$ над $\mathbb{F}_q$, так что левая сумма равна $q^{l(a^{-1})}$. С другой стороны,

$$\hat{\delta}_a = \delta_{a^\perp}\, \mu(a\bar{\Omega})$$

(где $a^\perp = (a\Omega)^\perp$), то есть учитывая, что $\mu(\Omega) = (N(dt))^{-\frac{1}{2}}$

$$\hat{\delta}_a = \delta_{a^{-1}(dt)^{-1}}\, N(a)^{-1} N((dt))^{-\frac{1}{2}}$$

Поэтому правая сумма равна $q^{l(a(dt))} N(a)^{-1} N((dt))^{-\frac{1}{2}}$

Сравнивая показатели степеней и учитывая, что $N(a) = q^{\sum n_p} = q^{n(a)}$, получаем

$$l(a^{-1}) = n(a^{-1}) - \tfrac{1}{2} n((dt)) + l(a(dt)),$$

то есть, меняя a на a^{-1} и обозначая $\kappa = (dt)$, находим,

$$l(a) = n(a) - \tfrac{1}{2} n((dt)) + l(a^{-1}(dt)).$$

Это – обычная теорема Римана–Роха.

Посмотрим теперь, что получается в числовых полях. Рассмотрим функцию f вида

$$f = \prod_{p \neq p_\infty} f_p \cdot f_\infty$$

"Конечную" часть выберем так, чтобы

$$\prod f_p = \delta_a$$

для некоторого дивизора a, а для "бесконечной" положим

$$f_\infty = \prod_{p/p_\infty} f_p ,$$

$$f_p = e^{-n_p \pi \| x \|_p^{2/n_p}} t_p ,$$

(где $n_p = 1$ при $k_p = \mathbb{R}$ и $n_p = 2$ при $k_p = \mathbb{C}$).

Преобразование Фурье этих функций вычислено и "почти совпадает" с ними - см. выше; t_p - переменные. Левая сумма в формуле Пуассона превращается в

$$\sum_{\alpha \in a} e^{F(\alpha)} = \theta_a (t_{p_1}, \dots, t_{p_r}) ,$$

где

$$F(\alpha) = \pi \sum_{p/p_\infty} -n_p \| \alpha \|_p^{2/n_p} t_p$$

квадратичная форма от α. Для вычисления правой части формулы Пуассона вспомним, что

$$\hat{\delta}_a = \delta_{\partial^{-1} a^{-1}} \mu(a) = \delta_{\partial^{-1} a^{-1}} N(a^{-1}) D^{-\frac{1}{2}}$$

где D - дискриминант; отсюда

$$\theta_a (t_1, \dots, t_r) = D^{-\frac{1}{2}} N(a^{-1}) \Big(\prod_{p/p_\infty} t_p^{n_p} \Big)^{-\frac{1}{2}} \theta_{a^*} (t_{p_1}^{-1}, \dots, t_{p_r}^{-1}),$$

где $a^* = \partial^{-1} a^{-1}$. Это - функциональное уравнение для θ - функций.

Теперь перейдем к основному приложению - выводу функционального уравнения ζ -функций. Для этого сначала сделаем в формуле Пуассона замену аргумента, рассмотрев вместо $f(\alpha)$ функцию $g(\alpha) = f(a\alpha)$ для некоторого иделя a. Имеем:

$$\hat{g}(\xi) = \int_{A_k} f(a\eta) \Lambda(\xi\eta) d^* \mu = \| a \|^{-1} \int_{A_k} f(\zeta) \Lambda(\zeta a^{-1} \xi) d^* \mu ,$$

откуда

$$\sum_{\alpha \in k^+} f(a\alpha) = \| a \|^{-1} \sum_{\alpha \in k^+} \hat{f}(a^{-1}\alpha)$$

Потребуем дополнительно, чтобы функция $|f(\xi)| \, \|\xi\|^\sigma$ при любом $\sigma > 1$ была интегрируема на группе иделей. Напомним, что

тогда можно определить

$$\zeta(f,c) = \int_{\mathcal{J}_k} f(a)\,c(a)\,d\mu^*$$

Теорема. $\zeta(f,c)$ продолжаема на всю s -плоскость, и

$$\zeta(f,c) = \zeta(\hat{f},\omega,c^{-1})$$

где $\omega_s = \|a\|^s$

Доказательство. Прежде всего

$$\zeta(f,c) = \int_{\|a\|\geq 1} f c\,d\mu^* + \int_{\|a\|\leq 1} f c\,d\mu^*$$

В силу условия на f , первый интеграл сходится для всех c
Второй интеграл преобразуем с помощью формулы Пуассона. Имеем

$$\int_{\|a\|\leq 1} f c\,d\mu^* = \int_{t\in\mathcal{J}/\mathcal{J}^\circ} \left(\int_{\mathcal{J}^\circ} f(ta)\,c(ta)\,d\mu^\circ\right) d\nu$$

где $d\mu^\circ$ - мера на $\mathcal{J}^\circ$, $d\nu$ - мера на $\mathcal{J}/\mathcal{J}^\circ$ ($= \mathbb{R}_+^*$ в числовом случае); затем

$$\int_{\mathcal{J}^\circ} f(ta)\,c(ta)\,d\mu^\circ = \int_{C^\circ} \left(\sum_{\alpha\in k^*} f(ta\alpha)\,c(ta\alpha)\right) d\tilde{\mu}\ ,$$

где $\tilde{\mu}$ - мера на $C^\circ = \mathcal{J}_k^\circ / k^*$. Внутренняя сумма равна

$$c(ta)\sum_{\alpha\in k^*} f(ta\alpha) = c(ta)\left(\sum_{\alpha\in k^*} f(ta\alpha) - f(0)\right) +$$

$$= c(ta)\left(\|ta\|^{-1}\sum_{\alpha\in k^*} \hat{f}(t^{-1}a^{-1}\alpha) - f(0)\right) =$$

$$= c(ta)\left(\|ta\|^{-1}\sum_{\alpha\in k^*} \hat{f}(t^{-1}a^{-1}\alpha) + \|ta\|^{-1}\hat{f}(0) - f(0)\right)$$

Положим теперь $u = t^{-1}$, $b = a^{-1}$; мера в $\mathcal{J}^\circ$, очевидно, не меняется. Подставляя результат под знак интеграла, получаем $(c_1 = \omega_s c^{-1})$:

$$\int_{\|a\|\leq 1} f c\,d\mu^* = \int_{\|a\|\geq 1} \hat{f}\,c_1\,d\mu^* + \int_{\|t\|\leq 1} \int_{\mathcal{J}^\circ} c(ta)\left(\|ta\|^{-1}\hat{f}(0) - f(0)\right) \times$$
$$\times\, d\tilde{\mu}\,d\nu$$

Для вычисления второго интеграла справа на $\mathcal{J}^\circ$ достаточно рассмотреть случай $c = \|\ \|^s$; тогда второй интеграл в числовом случае есть сумма членов вида

$$f(0)\,\mu(C^\circ)\int_0^1 t^s\,\frac{dt}{t} = -\frac{f(0)}{s}\,\varkappa\ ,$$

$$\varkappa = \mu^\circ(C^\circ)$$

и, аналогично, $\frac{\hat{f}(0)}{s-1}\mathcal{H}$

Итак, в числовом случае

$$\zeta(f,c) = \int\limits_{\|a\|\geq 1} f c\, d\mu^* + \int\limits_{\|a\|\geq 1} \hat{f} c_1\, d\mu^* + \left[\frac{\hat{f}(0)}{s-1} - \frac{f(0)}{s}\right]\mathcal{H}$$

Сумма двух интегралов – целая функция от s.

Теперь рассмотрим функциональный случай. В этом случае множество иделе $c\,\|a\| = 1$ имеет положительную меру. Мы учтем это, записав ζ-функцию так:

$$\zeta(f,c) = \int\limits_{J} f(a)\, c(a)\, d\mu^* =$$

$$= \int\limits_{\|a\|\geq 1} f(a)c(a)\,d\mu^* + \int\limits_{\|a\|\leq 1} f(a)c(a)\,d\mu^* - \int\limits_{\|a\|=1} f(a)c(a)\,d\mu^*$$

Преобразуя второе слагаемое, получаем:

$$(*)\quad \zeta(f,c) = \int\limits_{\|a\|\geq 1} f(a)c(a)\,d\mu^* + \int\limits_{\|a\|\geq 1} \hat{f}(a)\hat{c}(a)\,d\mu^* +$$
$$+ \delta_\chi \mathcal{H}\cdot\left(\frac{\hat{f}(0)}{1-q^{1-s}} - \frac{f(0)}{1-q^{-s}}\right) - \int\limits_{\|a\|=1} f(a)c(a)\,d\mu^* \quad .$$

Аналогично получим уравнение для последнего слагаемого:

$$\int\limits_{\|a\|=1} f(a)c(a)\,d\mu^* = \int\limits_{\|a\|=1} \hat{f}(a)\hat{c}(a)\,d\mu^* + \delta_\chi \mathcal{H}\cdot(\hat{f}(0) - f(0))$$

Заменяя в (*) f и c на $\hat{f}$ и $\hat{c}$ и учитывая выведенное только что соотношение, легко получить, что

$$\zeta(f,c) - \zeta(\hat{f},\hat{c}) = \delta_\chi \mathcal{H}\left[\hat{f}(0)\left(\frac{1}{1-q^{1-s}} + \frac{1}{1-q^{s-1}} - 1\right) - f(0)\left(\frac{1}{1-q^{-s}} + \frac{1}{1-q^{s}} - 1\right)\right] = 0$$

Теорема доказана.

В качестве примера получим классический вид функционального уравнения для обычной ζ-функции поля k. Имеем в функциональном случае

$$\zeta_k(s) = \zeta(\delta_\Omega, \omega_s)$$

(ср. выше вычисление локальных множителей). Далее, $\hat{\delta}_\Omega = \delta_{(dt)^{-1}} q^{-\frac{1}{2}n((dt))}$. Теперь $\zeta = \prod \zeta_p$,

$$\zeta_p = \int\limits_{p^{d_p}O_p} N(a)^{s-1} d^*\mu = \sum_{i=d_p}^{\infty} \int\limits_{p^i - p^{i+1}} N(a)^{s-1} d^*\mu =$$

Отсюда находим:

$$\zeta(\hat{\delta}_{\Omega}, \omega_{1-s}) = q^{-\frac{1}{2}n((dt))} N((dt))^{1-s} \zeta_k(1-s),$$

так что

$$\zeta_K(s) = q^{-\frac{1}{2}n((dt))} q^{-n((dt))(1-s)} \zeta_k(1-s)$$

Кроме того, из интегрального представления можно усмотреть, что $\zeta_k(s)$ есть рациональная функция от q^{-s}. В первом интеграле $\int_{\|a\|\geq 1} f c \, d\mu^*$ подинтегральная функция $\neq 0$ лишь при $\|a\| = 1$, и он есть константа, не зависящая от f. Для рассмотрения второго интеграла учтем, что $\hat{f} = q^{-\frac{1}{2}n((dt))} \delta_{(dt)^{-1}}$.

Далее, второй интеграл распространен на пересечение $\{\|a\| \geq 1\} \cap (dt^{-1})\bar{\Omega}$. Нормы иделей из этого множества принимают лишь конечное число значений q^m, $0 \leq m \leq n(dt)$: так как $c_1(a) = \|a\|^{1-s}$, отсюда следует рациональность:

$$\zeta_k(s) = P(q^{-s}) + \frac{\alpha}{1-q^{-s}} + \frac{\beta}{1-q^{1-s}} = \frac{L(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

где P, L - многочлены.

В числовом случае следует в качестве f взять

$$f = \prod f_p \qquad f_p = \begin{cases} \delta_{o_p}, & p \nmid p_\infty \\ e^{-\pi x^2}, & k_p = \mathbb{R} \\ e^{-2\pi|z|^2}, & k_p = \mathbb{C} \end{cases}$$

Тогда

$$\zeta(f, \omega_s) = \prod_{p \nmid p_\infty} \zeta_p \prod_{p \mid p_\infty} \zeta_p = \zeta_k(s) \prod_{p \mid p_\infty} \Gamma\left(\frac{s n_p}{2}\right) \pi^{-\frac{n_p s}{2}} = \varphi(s)$$

Аналогично

$$\zeta(\hat{f}, \omega_{1-s}) = \varphi(1-s) |D_k|^{\frac{1}{2}-s}$$

Функциональное уравнение поэтому имеет вид

$$\varphi(s) = \varphi(1-s) |D|^{\frac{1}{2}-s}$$

Г Л А В А II

ДЗЕТА-ФУНКЦИИ КРИВЫХ НАД КОНЕЧНЫМ ПОЛЕМ

§ I. Эндоморфизм Фробениуса и формула Лефшеца

Напомним общие тождества, относящиеся к дзета-функции схемы. Пусть X - алгебраическое многообразие над $\mathbb{F}_q$, ν_e число его геометрических точек со значениями в $\mathbb{F}_{q^e}$, $a(k)$ -число точек $x \in X$ таких, что $[k(x):\mathbb{F}_q] = q^{n(x)} = q^k$. Тогда, полагая $Z(q^{-s}) = \zeta_X(s)$, имеем:

$$Z(u) = \prod_{x \in X} \frac{1}{1-u^{n(x)}} = \prod_k (1-u^k)^{-a_k}$$

$$\log Z(u) = \sum \frac{\nu_e}{e} u^e$$

$$u \frac{Z'(u)}{Z(u)} = \sum_{e \geq 1} \nu_e u^e$$

Пусть $X \subset \mathbb{P}^N$, $(x_0, \ldots, x_N)$ - проективные координаты, $\varphi: (x_0, \ldots, x_N) \to (x_0^q, \ldots, x_N^q)$ - эндоморфизм Фробениуса. Он переводит X в себя и действует на множестве геометрических точек X со значениями в поле $\overline{\mathbb{F}_q}$. Очевидно, ν_e есть число неподвижных точек φ^e на множестве $X(\overline{\mathbb{F}_q})$

Рассмотрим модельную задачу: X - топологическое многообразие, $H^i(X)$ - i - мерное пространство когомологий. Для всякого эндоморфизма $\psi: X \to X$ обозначим через $S^i(\psi)$ след $H^i(\psi)$ на $H^i(X)$ и введем число Лефшеца

$$L(\psi) = \sum (-1)^i S^i(\psi)$$

Если неподвижные точки ψ на X изолированы, то им можно приписать некоторые кратности $\tau(x)$, и теорема Лефшеца утверждает, что

$$L(\psi) = \sum_{\psi(x)=x} \tau(x)$$

В этой ситуации можно ввести аналог (логарифмической производной) дзета-функции, и его нетрудно вычислить:

$$\sum_{e \geq 1} L_e(\psi^e) u^e$$

Пусть $(\alpha_{ij})_{j=1,\ldots,\beta_i}$ - характеристические корни $H^i(\psi)$ на H^i. Тогда

$$S^i(\psi^e) = \sum_{j=1}^{\beta_i} \alpha_{ij}^e, \quad L(\psi^e) = \sum_i (-1)^i \sum_{j=1}^{\beta_i} \alpha_{ij}^e$$

так что

$$\sum_{e \geq 1} L(\psi^e) u^e = \sum_i (-1)^i \sum_{j=1}^{\beta_i} \Big(\sum_{e \geq 1} \alpha_{ij}^e u^e \Big) =$$

$$= \sum_i (-1)^i \sum_{j=1}^{\beta_i} \frac{\alpha_{ij} u}{1-\alpha_{ij} u} = \sum_i (-1)^i \sum_j u \frac{d \log (1-\alpha_{ij} u)^{-1}}{du}$$

Считая этот ряд равным $u\frac{Z'(u)}{Z(u)}$ получаем:

$$Z(u)=\prod_i\Big(\prod_{j=1}^{b_i}(1-\alpha_{ij}u)^{-1}\Big)^{(-1)^{i-1}}$$

Тем самым, в модельной задаче Z -функция оказывается рациональной и вычисляется до конца.

В случае, когда X - алгебраическая кривая над $\mathbb{F}_q$, мы знаем, что

$$(*)\qquad Z(u)=\frac{L(u)}{(1-u)(1-qu)}$$

Пользуясь функциональным уравнением, без труда находим: $\deg L(u) = \deg n(k)+2 = 2g$, где $g=e(K)$. В топологическом случае $2g$ совпадает с $b_1(X)$, так что общий вид (*) согласуется с тем, который получается в модельной ситуации: в знаменателе определенно стоит $\det(E-uH^0(\varphi))(E-uH^1(\varphi))$, а в числителе по крайней мере многочлен должной степени.

Основываясь на этом, А.Вейль высказал свои гипотезы о рациональности и виде ζ -функции, доказанные впоследствии Гротендиком. Для кривых сам Вейль ввел понятие, представляющее собой абстрактный аналог группы H^1, и доказал формулу Лефшеца того же вида, что и в топологическом случае. В следующем параграфе будет описана его конструкция.

§ 2. Классы дивизоров и группа Тэйта

Пусть X - кривая над полем k; Cl^0 - ее группа классов дивизоров нулевой степени над k. Мы реализуем Cl^0 как множество геометрических точек некоторого группового k -

многообразия $\mathcal{J}$ со значениями в $\bar{k}$. Это соответствие будет таким, что $Cl^0(K)=\mathcal{J}(K)$ для любых полей K, между k и $\bar{k}$.

В случае $k=\mathbb{C}$ структура Cl^0 описывается теоремой Абеля. Пусть $\alpha=\sum n_i P_i$, $\sum n_i=0$. Это означает, что $\alpha=\partial C$, где C - некоторая одномерная цепь. Пусть (ω_i) - базис пространства регулярных дифференциалов на X. Рассмотрим точку

$$\Big(\dots\int_C\omega_i\dots\Big)\in\mathbb{C}^g$$

Она определена с точностью до вектора из "решетки периодов" $H_1(X)$ дифференциалов ω_i. Теорема Абеля утверждает, что Cl^0 при этом отображении отождествляется с тором $\mathbb{C}^g/H_1(X)$

Решетка $H_1(X)$ удовлетворяет "соотношениям Римана": в пространстве $\mathbb{C}^g$ существует такая эрмитова метрика, относительно которой $H_1(X)$ двойственна себе. Следовательно, $H_1(X)\approx\mathbb{C}^g/H_1(X)=Cl^0$. Это показывает, что группа Cl^0 в некотором смысле "заменяет" группу одномерных когомологий кривой X. С другой стороны, вложение Cl^0 с помощью тэта-функций в $\mathbb{P}^r(\mathbb{C})$ определяет на Cl^0 структуру алгебраической группы.

Оказывается возможным дать чисто алгебраическую конструкцию Cl^0, годную для любого основного поля k. Опишем кратко эту конструкцию.

Рассмотрим сначала множество классов дивизоров Cl^r степени r. Оно является смежным классом Cl по Cl^0, и достаточно ввести алгебраическую структуру на Cl^r. При $n(\alpha)>2g-2$ имеем:

$$e(\alpha)=n(\alpha)+1-g$$

Будем считать, что $r > 2g-2$. Тогда $l(\alpha)-1 = r-g$, и это число есть размерность проективного пространства положительных дивизоров, принадлежащих тому же классу, что и α.

Все множество эффективных дивизоров порядка r на кривой есть симметрическое произведение $S^r(X)$ кривой X на себя r раз. Теперь нужно построить фактор-пространство по отношению линейной эквивалентности: это делается с помощью явной конструкции сечения.

Заменой группы когомологий H^1 будет служить группа, двойственная к H_1; модельная задача подсказывает определение:

$$H^1(X, \mathbb{Z}_l) = \mathrm{Hom}(H_1, \mathbb{Z}_l) =$$
$$= \mathrm{Hom}(\hat{\mathbb{Z}}_l, \hat{H}_1) = \mathrm{Hom}(C_l, J),$$

где $C_l = \mathbb{Z}[\frac{1}{l}]/\mathbb{Z}$. Для произвольного поля k, мы будем поэтому рассматривать в качестве аналога группы $H^1(X, \mathbb{Z}_l)$ группу $\mathrm{Hom}(C_l, J)$, где l - некоторое простое число, отличное от характеристики k. Эта группа называется "модулем Тэйта" кривой X. Она представляет собой группу, состоящую из бесконечных векторов вида

$$(a_1, a_2, \dots), \quad a_i \in J_{l^i}, \quad l a_{i+1} = a_i$$

(J_{l^i} - ядро умножения на l^i в J) или

$$T_l(A) = \varprojlim_i (J_{l^i})$$

Нам понадобятся еще следующие свойства якобиевых многообразий J:

а. J является алгебраической группой, и структура группы на множестве геометрических точек $J(\bar{k})$ та же, что на $\mathbb{Z}^g$.

б. Для двух кривых X, Y, их якобиевых многообразий J_X, J_Y и каждого отображения конечной степени $f: X \to Y$ определен гомоморфизм алгебраических групп

$$f^*: J_Y \to J_X$$

(который индуцирован гомоморфизмом групп дивизоров).

В частности, для эндоморфизма Фробениуса $\varphi_X: X \to X$ имеем $J(\varphi_X) = \varphi_X^* = \varphi_J$

Модуль Тэйта $T_l(J)$ также является (контравариантным) функтором J.

Предложение. Для любого абелева многообразия A модуль Тэйта $T_l(A)$ изоморфен $\mathbb{Z}_l^r$, где r - некоторое целое число.

Доказательство. Нам понадобятся два факта:

а. $\kappa\delta: A \to A$ есть эпиморфизм, $\kappa \in \mathbb{Z} - \{0\}$

б. $\#(\mathrm{Ker}\,\kappa\delta) < \infty$. (Они верны для любого κ, но приводимое ниже доказательство годится лишь в случае $\mathrm{char}\, k \nmid \kappa$. Они, в свою очередь, вытекают из того, что для всякого морфизма проективных многообразий $f: U \to V$ образ $f(U)$ замкнут в V, для каждой замкнутой точки $u \in f(U)$ имеет место неравенство

$$\dim f^{-1}(u) \geq \dim U - \dim f(U),$$

и на открытом всюду плотном подмножестве $f(U)$ здесь имеет место знак равенства.

Поэтому достаточно проверить лишь первое утверждение. Рассмотрим касательные пространства $\Theta(A)$ и $\Theta(B)$ в единице

и касательное отображение

$$df: \Theta(A) \longrightarrow \Theta(B)$$

Его эпиморфизм доказывает а), так как A и B неособы; но $\Theta(f)$ - умножение на κ. Отсюда следует требуемое.

Теперь из а), б) без труда получается, что

$$Ker\, \kappa^a \delta \simeq \mathbb{Z}^r / \kappa^a \mathbb{Z}^r$$

и $T_e(A) \simeq \mathbb{Z}_e^r$. Доказательство закончено.

§ 3. Вывод формулы Лефшеца из свойств степени изогении

Мы будем рассматривать $T_e(A)$ как замену $H^1(A)$ и докажем для него формулу Лефшеца.

Пусть $\alpha: A \to A$ - любая изогения (т.е. эндоморфизм с конечным ядром), $\nu(\alpha)$ - его степень. Имеем $\nu(\alpha) = \#(Ker\, \alpha) \cdot p^f$ где p - характеристика поля k. При этом $f = 0$ в том и только том случае, когда $d\alpha$ не имеет ядра.

Доказательство формулы Лефшеца основано на следующей лемме:

Лемма. $\| \det T_e(\alpha) \|_e = \| \nu(\alpha) \|_e$, $e \neq p$

Доказательство. Так как $e \neq p$, $\| \nu(\alpha) \|_e = \| \#(Ker\, \alpha) \|_e$ Можно считать, что в базисе $T_e(J)$ матрица $T_e(\alpha)$ приведена к диагональному виду, после чего утверждение становится очевидным.

Теорема. $\det T_e(\alpha) = \nu(\alpha)$

Доказательство. Положим $f_e(u) = \det(T_e(\alpha) + uE)$. Применяя лемму к $\alpha + \kappa\delta$, получим

$$\| F_e(\kappa) \|_e = \| \nu(\alpha + \kappa\delta) \|_e$$

Покажем, что $\nu(\alpha + \kappa\delta)$ тоже является многочленом от κ

Более общо, продолжим $\nu(\alpha)$ на $End\, A$, считая $\nu(\alpha) = 0$ для тех α, которые не являются изогениями. Мы покажем, что $\nu(\alpha)$ как функция на аддитивной группе $End\, A$ является однородной полиномиальной функцией. Это - самое содержательное место доказательства.

Сначала выведем теорему из этого обстоятельства. Функция $\nu(\alpha + \kappa\delta)$ является многочленом G_α конечной степени от κ. Кроме того

$$\| F_e(\kappa) \|_e = \| G_\alpha(\kappa) \|_e$$

для всех $\kappa \in \mathbb{Z}$. Этого, однако, еще мало. Установим, что для любого $\kappa \in \overline{\mathbb{Q}}_e$ верно то же равенство. С этой целью рассмотрим вместо $\alpha + \kappa\delta$ любые многочлены от α. Если $P(x) = \prod_i (x + \kappa_i \delta)$, $\kappa_i \in \mathbb{Z}$, то

$$\nu(P(\alpha)) = \prod_i \nu(\alpha + \kappa_i \delta) =$$

$$= \prod_i G_\alpha(\kappa_i) = R^*(G_\alpha, P)$$

где R^* - это универсальный многочлен от коэффициентов G_α, P. Если теперь $P(x) \in \mathbb{Z}[x]$ - любой многочлен со старшим коэффициентом 1, то снова

$$\nu(P(\alpha)) = R^*(G_\alpha, P)$$

в силу универсальности R и совпадения левой и правой части на многочленах с целыми корнями.

То же по непрерывности верно для многочленов P с e - адическими коэффициентами. Вспомним теперь, что

$$\| N G_\alpha(\xi)\|_e = \| G_\alpha(\xi)\|_e^{\deg \xi}$$

для любых $\xi \in \bar{Q}_e$, так что

$$\| \vartheta(P(\alpha))\|_e = \| G_\alpha(\xi)\|_e ,$$

то есть

$$\| F_e(\xi)\|_e = \| G_\alpha(\xi)\|_e$$

для всех $\xi \in \bar{Q}_e$. Пусть $G = \prod P_i^{e_i}$, $F = \prod P_i^{f_i}$, где P_i неприводимы. Если $e_i > f_i$, то $\frac{G}{F}(\xi_i) = 0$, где ξ_i корень P_i, а это противоречит тому, что

$$\| \frac{G}{F}(\xi)\|_e = 1$$

при почти всех ξ.

Для доказательства "полиномиальности" $\vartheta(\alpha)$ нам понадобятся элементы теории пересечений.

§ 4. Численная и линейная эквивалентности. Критерий Вейля

Пусть X - n -мерное проективное многообразие. Тогда для любых n дивизоров $\mathfrak{D}_1, \dots, \mathfrak{D}_n$ можно определить индекс пересечения $(\mathfrak{D}_1, \dots, \mathfrak{D}_n)$.

Этот индекс пересечения обладает некоторыми свойствами, которые мы явно выпишем.

Пусть $X \xrightarrow{f} Y$ - морфизм многообразий. Для некоторых дивизоров $D \subset Y$ можно определить дивизор $f^*(D)$; если D главный, $f^*(D)$ тоже главный; в любом классе дивизоров имеется элемент, на котором f^* определено. Поэтому f^* превращает группы классов дивизоров Cl в контравариантный функтор (рассматриваются классы относительно линейной эквивалентности $D \sim D'$).

Нам важно иметь также некоторые сведения о ковариантном поведении дивизоров. Если $D \subset X$, и есть морфизм $f: X \to Y$, мы полагаем $f_*(D) = 0$, когда $\dim f(D) < \dim D$. В случае, когда $\dim f(D) = \dim D$ и D неприводим, положим $f_*(D) = k f(D)$, где $k = \deg f|_D$. Важно, что f_* также сохраняет линейную эквивалентность; в аффинном случае это ясно, потому что f_* соответствует взятию нормы элемента.

Имеет место следующая формула:

$$f_* f^*(D) = dD , \quad d = \deg f .$$

Теперь мы можем сформулировать нужные нам свойства индекса пересечения $(D_1, \dots D_n)$ на X.

1) Симметричность

2) Полилинейность

3) $(D_1 \dots D_n)_Y = \deg f \, (f^*(D_1) \dots f^*(D_n))_X$, где

$f: X \to Y$, $D_i \subset Y$.

4) $(D_1 \dots D_n)$ не меняется, если заменить D_i на алгебраически эквивалентный дивизор D_i' $(D_i \approx D_i')$.

5) Если $D_1, \dots, D_n$ находятся в "общем положении", то, полагая $S = Supp(\cap D_i)$ (конечное множество точек), имеем

$$(D_1 \dots D_n) = \sum_{s \in S} (D_1 \dots D_n)_s$$

где

$$(D_1 \dots D_n)_s = \dim_k \mathcal{O}_s / (f_{D_1}, \dots, f_{D_n})$$

где f_{D_i} - локальное уравнение D_i в окрестности s

Пример 1. Если $\dim X = 1$, то $(D) = \deg D = n(D)$

Пример 2. $X^n \subset \mathbb{P}^N$, $L \subset X$ - гиперплоское сечение. Тогда

$$(L^n) = (\underbrace{L \dots L}_{n \text{ раз}}) = \deg X$$

Определение. Дивизор D численно эквивалентен D' $(D \equiv D')$ если замена D на D' не меняет индексы пересечения.

Пусть $\mathcal{Y}(X)$ - группа классов дивизоров относительно численной эквивалентности. Мы исследуем $\mathcal{Y}(X)$ как функтор на категории абелевых многообразий и покажем, что при фиксированном $D \in \mathcal{Y}(A)$ элемент $\alpha^* D \in \mathcal{Y}(A)$ является квадратичной функцией от изогении α со значениями в $\mathcal{Y}(A)$ Так как

$$(L^n)^{-1}((\alpha^* L)^n) = \nu(\alpha)$$

отсюда будет следовать, что $\nu(\alpha)$ как функция от α имеет степень $2n$. Отсюда, в частности, получается также, что

$$\dim_{\mathbb{Z}_\ell} T_\ell(A) = 2 \dim A.$$

Квадратичность $\alpha^* D$ легко устанавливается над $\mathbb{C}$. Действительно, $\mathcal{Y}(A) \otimes \mathbb{Q} \subset H^2(A, \mathbb{Q})$; представление α на H^1 линейно, а на $H^2 = H^1 \wedge H^1$ квадратично.

В абстрактном случае рассуждение совершенно иное. Имеет место следующий

Критерий Вейля. Если $t_a(D) \sim D$, то $D \equiv 0$ (t_a - сдвиг на точку $a \in A$).

Пусть теперь X - кривая, $X \xrightarrow{\varphi} \mathcal{J}(X)$ - отображение $x \to cl(x - o)$, где o - фиксированная точка. Продолжим φ на группу дивизоров X по линейности. Ядро φ на дивизорах степени 0 состоит из главных дивизоров.

Пусть $g = p_g X = \dim \mathcal{J}$ и рассмотрим отображения

$$X^g \xrightarrow{\varphi^g} \mathcal{J}^g(X) \xrightarrow{\mu} \mathcal{J}(X)$$

(μ - сложение). Пусть ψ - сквозное отображение. Образ ψ совпадает с $\mathcal{J}(X)$: это легко следует из теоремы Римана-Роха. Кроме того, над открытым всюду плотным подмножеством $\mathcal{J}(X)$ отображение ψ имеет степень $g!$ (его можно пропустить через симметрическое произведение).

Если мы рассмотрим сквозное отображение

$$X^{g-1} \longrightarrow \mathcal{J}(X)$$

образом его будет некоторый дивизор Θ - дивизор Пуанкаре. Основой доказательства является следующая "теорема о квадрате".

Лемма. Для всякого $D \subset A$

$$t_{a+e}(D) - t_a(D) - t_e(D) + D \sim 0$$

Набросок доказательства. Лемма равносильна утверждению о том, что

$$\psi: a \to \mathcal{C}(D - t_a(D))$$

есть гомоморфизм $A \to \mathcal{C}A$

Пусть $X \xrightarrow{f} A$ - отображение в A некоторой кривой X Имеем $\varphi f^*(t_a(D)) \in J(X)$. Отображение

$$A \to J: \quad a \to \varphi f^*(t_a(D))$$

по общему свойству абелевых многообразий есть комбинация сдвига и гомоморфизма:

$$\varphi f^*(t_a(D)) = \alpha(a) + C$$

Отсюда легко получается, что

$$f^* t_{a+e}(D) - f^* t_a(D) - f^* t_e(D) + f^*(D) \sim 0$$

на кривой X : степень его равна нулю и он лежит в ядре φ Теперь можно установить линейную эквивалентность на A чисто техническими соображениями, которые опускаются.

С другой стороны, если предположить для любого многообразия X известным существование многообразия Пикара $Pic(X)$, играющего ту же роль, что и JX для кривой X, то предшествующее доказательство полностью доказывает лемму.

Рассмотрим теперь общую категорную ситуацию: пусть F - контравариантный функтор из аддитивной категории C в категорию коммутативных групп. Для всякого объекта $B \in C$ положим:

$$F_a(B) = \{\xi \in F(B) \mid \forall A \in C, \forall \alpha, \beta \in Hom(A,B) \quad F(\alpha+\beta)\xi = F(\alpha)\xi + F(\beta)\xi\}$$

Это максимальный аддитивный подфунктор функтора F (то, что это функтор, легко проверить).

Для конструкции $F_a(B)$ достаточно рассмотреть те $\xi \in F(B)$, для которых

$$F(\mu)\xi = F(p_1)\xi + F(p_2)\xi,$$

где $B \times B \xrightarrow{\mu} B$ - сложение, а $p_1, p_2: B \times B \to B$ - проекции. (Проверка опускается: она легко следует из универсальности $B \times B$). Классы $\xi \in F(B)$ с таким свойством называются примитивными.

Теперь мы утверждаем, что если $t_a(D) \sim D$, то

$$\mu^*(D) = p_1^*(D) + p_2^*(D)$$

(Верно и обратное, доказательство чего мы пропустим). Ограничим этот дивизор на $A \times a_0$; теоретико-множественное вычисление дает правильный ответ:

$$(\mu^*(D) - p_1^*(D) - p_2^*(D))\big|_{A\times a_0} =$$

$$= (t_{a_0}(D) - D)\times a_0 = (f_{a_0})$$

Этсюда можно вывести существование такой функции f на $A\times A$ что

$$\mu^*(D) - p_1^*(D) - p_2^*(D) - (f)$$

состоит из слоев. Но аналогичное рассуждение для второго множителя покажет, что этот дивизор ~ 0, что доказывает требуемое.

Следовательно, на инвариантных дивизорах любые гомоморфизмы образуют аддитивный функтор.

Доказательство критерия Вейля: ($D\subset A$, A - абелево; $\{t_a(D)\sim D, \forall a\in A\}\Rightarrow D\approx 0$)

Частный случай. Пусть $D\geqslant 0$; покажем, что тогда $D=0$

Пусть $t_a(D) - D = (f_a)$. Тогда $(f_a)+D\geqslant 0$, то есть $f_a\in L(D)$. Воспользуемся тем, что $\dim_k L(D) < \infty$; тогда сдвиги t_a дают автоморфизмы проективного пространства, связанного с $L(D)$, то есть определяют гомоморфизм $A\to PGL(L(D))$; он регулярен и потому имеет своим образом точку. Это означает, что $t_a(D)=D\Rightarrow D=0$. (Отсюда следует, что $\operatorname{Ker} n_a$ конечен даже для $\operatorname{char} k \mid n$. Иначе в ядре n_a есть абелево многообразие B, на нем дивизор $D>0$ такой, что класс линейной эквивалентности nD инвариантен: $t_a(nD)\sim t_{na}D = D$ (теорема о квадрате)$\Rightarrow D=0$, что противоречит предположению $\dim B>0$).

Общий случай. Пусть X - кривая, J - якобиево многообразие, $\psi: X^g \xrightarrow{\varphi_g} J^g \xrightarrow{\mu_g} J$. Имеем

$$\mu_g = p_1 + \dots + p_g$$

где p_i - проекция J^g на i-й множитель. Отсюда

$$\psi^*(D) = (\varphi^g)^*\mu_g^* D$$

$$\mu_g^*(D) = p_1^* D + \dots + p_g^* D$$

Но $(\varphi^g)^* p_i^* = (p_i\varphi^g)^* = (\varphi\pi_i)^*$ (где π_i справа от φ есть проекция $X^g\to X$!). Далее, $(\varphi\pi_i)^* = \pi_i^*\varphi^*$. Пусть $\varphi^*(D) = \sum k_j x_j$; учитывая, что $\pi_i^* x = X\times\dots\times x_i\times\dots\times X$ имеем:

$$\varphi^*(D) = \sum_{i,j} k_{i,j}(X\times\dots\times x\times\dots\times X)$$

Легко вычислить $\varphi_*(X\times\dots\times x\times\dots\times X)$: этот дивизор равен $e\,t_{\varphi(x)}(\Theta)$, где e - некоторое натуральное число. Следовательно,

$$\varphi_*\varphi^*(D)\sim \sum e_j\, t_{\varphi(x_j)}(\Theta)$$

Для вычисления $\varphi_*\varphi^*(D)$ заметим, что отображение $X^g\to J$ имеет степень $g!$, ибо пропускается через $S^g(X)$.

Отсюда:

$$g!\,D \sim \sum e_j\, t_{a_j}(\Theta)$$

По теореме о квадрате

$$g!\,D \sim (\Sigma e_j)\,\Theta + t_a(\Theta) - \Theta$$

Дивизор D определяет инвариантный класс, $t_a(\Theta)-\Theta$ – тоже (снова теорема о квадрате). Следовательно, $(\Sigma e_j)\,\Theta$ тоже должен давать инвариантный класс, так что $\Sigma e_j = 0$. Тем самым, $g!\,D \sim t_a(\Theta)-\Theta \approx 0$, поэтому $D \approx 0$. Критерий доказан.

Теперь вернемся к квадратичности. Покажем, что $(1-t_a)\alpha^* D$ квадратична по α. Имеем:

$$(1-t_a)\,\alpha^* D = \alpha^*(1-t_{\alpha(a)})D$$

Положим

$$F(\alpha,\beta) = \alpha^*(1-t_{\beta(a)})D$$

F линейна по β в силу теоремы о квадрате, а по α – в силу доказанного критерия. Это дает требуемое.

§ 5. Формула для следа эндоморфизма

Из теоремы о квадратичности следует:

$$(\alpha+n\delta)^* D \approx \alpha^* D + n\,L(\alpha,D) + n^2 D,$$

где

$$L(\alpha,D) = (\alpha+\delta)^* D - \alpha^* D - D$$

С другой стороны,

$$(\alpha+n\delta)^* D = \nu(\alpha+n\delta)(D^g)$$

Отсюда

$$\nu(\alpha+n\delta)(D^g) = n^{2g}(D^g) + g\,n^{2g-1}(D^{g-1}, L(\alpha,D)) + \ldots$$

Если $(D^g)\neq 0$, отсюда следует, что $\nu(\alpha+n\delta)$ есть многочлен степени $2g$. Мы уже вывели из этого, что $\nu(\alpha+n\delta)$ есть характеристический многочлен представления α в модуле Тэйта; его степень поэтому равна размерности модуля Тэйта, которая в свою очередь равна $\log_n \#(\mathrm{Ker}\, n\delta)$: значит,

$$\#(\mathrm{Ker}\, n\delta) = n^{2g}$$

Кроме того, мы доказали, что

$$(*) \qquad \mathrm{Sp}\,\alpha = g\,(D^g)^{-1}(D^{g-1}, L(\alpha,D))$$

Напомним, что в формуле Лефшеца фигурирует именно след; имея это в виду, мы провели это вычисление.

Формула (*) не зависит от выбора D. Мы применим ее на якобиевом многообразии к $D = \Theta$. Прежде всего, $\Theta^g \neq 0$. Покажем, что $t_a(\Theta) \sim \Theta \Rightarrow a = 0$. Пусть $\Theta' = (-\delta)\Theta$; достаточно проверить, что $t_a\Theta' \sim \Theta' \Rightarrow a = 0$. Покажем, что

$$\mu\varphi^*((1-t_a)\Theta') = a,$$

где μ - суммирование.

(Отсюда следует даже, что $(1-t_a)\Theta \sim (1-t_\beta)\Theta \Rightarrow a=\beta$). Действительно,

$$\varphi^*((1-t_a)\Theta') = \varphi^*(\Theta') - \varphi^* t_a(\Theta').$$

Вычислим $\varphi^* t_a(\Theta')$ теоретико-множественно:

$$x \in \varphi^* t_a(\Theta') \Leftrightarrow \varphi(x) = -(\varphi(x_1)+\ldots+\varphi(x_{g-1}))+a$$

Точки a, лежащие на открытом плотном подмножестве, имеют единственное представление в таком виде, так что для таких a

$$\varphi^*(t_a(\Theta)) = x_1+\ldots+x_{g-1}$$

а сумма $\sum_{i=1}^{g-1} x_i = a$. Это нам и нужно; условие того, что a не принадлежит исключительному замкнутому множеству, можно обойти, ибо $\varphi^*(t_a(\Theta)) = \varphi^*(t_{a+x}(\Theta)) - \varphi^*(t_x(\Theta))$ для

любой x, так что a всегда можно сдвинуть с и ключительного множества.

Значит, $(\Theta^g) = (\Theta, t_{a_1}(\Theta), \ldots, t_{a_{g-1}}(\Theta)) \neq 0$ для "хорошего" выбора точек a_i.

Теперь

$$S_P(d) = g(\Theta^g)^{-1}(\Theta^{g-1}, L(d,\Theta)).$$

Но можно показать, что

(**) $$\Theta^g = g!, (\Theta^{g-1}) \approx (g-1)!\,\varphi(X);$$
$$\varphi(X, D) = n(\varphi^*(D)).$$

Отсюда

(***) $$S_P(d) = n(\varphi^*(L(d,\Theta)))$$

Эту формулу можно вывести несколько иначе, следуя Ленгу, заменив (**) использованием Понтрягинских произведений.

Вернемся к выводу (***) с помощью Понтрягинского произведения. Пусть $U, V \subset A - \kappa$ и ℓ - мерные неприводимые многообразия. Положим

$$U * V = \mu_*(U \times V)$$

где

$$U \times V \subset A \times A \xrightarrow{\mu} A$$

Распространим затем * на циклы по линейности.

Теперь в смысле этого произведения

$$\varphi(x)^{(g)} = g!\,y, \quad \varphi(x)^{(g-1)} = (g-1)!\,\Theta$$

что немедленно следует из определения. Этим можно заменить формулы пересечения, что мы сейчас и сделаем.

Нам придется тогда пользоваться теорией пересечений для подмногообразий любой размерности, из которой нам понадобятся два свойства:

I) ассоциативность

2) $f_*(u, f^*(v)) = (f_*(u).v)$ в ситуации $f: X \to Y$, u - цикл на X, v - цикл на Y.

Имеется в виду, что рассматриваются классы циклов с точностью до численной эквивалентности. Понтрягинское произведение совместимо с этой эквивалентностью, и всякий гомоморфизм $\alpha: A \to B$ определяет гомоморфизм понтрягинских колец. (Второе утверждение очевидно; первое означает, что если $u \approx 0$, то $u * v \approx 0$). Для доказательства заметим, что

$$(u * v, w) = 0 \iff ((u \times v).\mu^* w) = 0 \iff$$

$$\iff ((u \times A).(A \times v).\mu^* w) = 0,$$

но, полагая $(A \times v).\mu^* w = T$, имеем

$$((u \times A).T) = p^*(u).T = (u.p_*(T)) \approx 0$$

Теперь мы сможем доказать формулу для следа. Во-первых,

$$(u.\alpha^* v) = (\alpha_* u.v).$$

Далее

$$(\alpha + n\delta)^* D \approx \alpha^* D + n L(\alpha, D) + n^2 D$$

"По двойственности", получаем, что аналогичное соотношение верно для кривых

$$(\alpha + n\delta)_* Y \approx \alpha_* Y + n M(\alpha, Y) + n^2 Y$$

где

$$M(\alpha, Y) = (\alpha + \delta)_* Y - \alpha_* Y - Y$$

Рассматривая n -ю понтрягинскую степень этого равенства, получаем формулу для $\nu(\alpha + n\delta)$ и, в частности, для $S_p(\alpha)$:

$$S_p(\alpha) = g(Y^{(g)})^{-1}(Y^{(g-1)} * M(\alpha, Y))$$

где $Y^{(g)}$ - число - кратность A в $Y * \dots * Y$; аналогично истолковывается выражение в скобках. Теперь мы хотим из этой формулы вывести первоначальную с пересечением. Для этого нужно воспользоваться тем, что

$$(D * Y) = (D'.Y), \quad D' = (-\delta)D$$

и снова применить двойственность.

§ 6. Приложения к соответствиям кривых

Установим сначала несколько полезных фактов.

Рассмотрим в группе дивизоров D абелева многообразия A подгруппу D°, порожденную дивизорами вида $(1-t_a)D$, $a \in A$ (в действительности D° совпадает с группой дивизоров ≈ 0) и пусть $\mathcal{C}^\circ$ - группа классов дивизоров из D°.

Если $A = J$ и если класс D инвариантен, то $g!D \sim (1-t_a)\theta$; если $D \sim (1-t_\beta)D'$, то

$$D \sim g!(1-t_a)D' \sim (1-t_{a_1})\theta,$$

где $b = g!c$. Следовательно, $\mathcal{C}^\circ$ состоит из классов дивизоров вида $(1-t_a)\theta$. Уже было проверено, что точка a таким классом определяется однозначно:

$$\mu(\varphi^*(1-t_a)\theta) = -a$$

Следовательно, снова пользуясь теоремой о квадрате, находим:

$$\mathcal{C}^\circ(J) \simeq J$$

(J здесь означает группу геометрических точек якобиева многообразия). На самом деле построено даже семейство дивизоров на J, содержащее все классы из $\mathcal{C}^\circ$ по одному разу. Базой этого семейства является J, поэтому его график лежит в $J \times J$. Мы утверждаем, что этот график совпадает с $\mu^*\theta = \tilde{\theta}$ (где $\mu: J \times J \to J$ - как обычно, умножение),

точнее, когда a пробегает J, дивизоры

$$\tilde{\theta}(a) - \tilde{\theta}(0)$$

пробегают по одному разу представители всех классов из $\mathcal{C}^\circ$.

Всякому эндоморфизму $\alpha: J \to J$ мы можем поставить в соответствие семейство $\tilde{\theta}_\alpha \subset J \times J$:

$$\tilde{\theta}_\alpha(a) = \tilde{\theta}(\alpha(a))$$

Вот его описание: рассмотрим гомоморфизм

$$\mu \circ (\alpha \times \delta): J \times J \to J$$

тогда

$$\tilde{\theta}_\alpha = (\alpha \times \delta)^* \mu^* \theta$$

В частности:

$$\tilde{\theta}_\alpha \big|_{a \times J} = t_{-\alpha(a)}(\theta)$$

Приложения.

Пусть X - алгебраическая кривая. "Соответствие" есть обобщение понятия "график алгебраического отображения X в себя": любой дивизор на $X \times X$ есть соответствие кривой с ней самой.

Пример: пусть дано отображение $f: X \to \mathbb{P}^1$, рассмотрим расслоенное произведение

$$X \underset{\mathbb{P}^1}{\times} X = \overline{D} \subset X \times X$$

Очевидно, $\Delta_X \subset \overline{D}$; $D = \overline{D} - \Delta$ - является соответствием, связанным с отображением f: "соответствуют друг другу" точки, имеющие один и тот же f-образ.

Соответствие вида $\alpha \times X + X \times \beta$, где α, β -дивизоры на X, называется тривиальным. Мы ограничимся рассмотрением группы соответствий, не содержащих тривиальных компонент.

Имеем:

$$(D \cdot (x \times X)) = n(D(x)), \quad D(x) = D|_{x \times X}$$

Рассмотрим на X фиксированную точку 0; тогда соответствие D определяет отображение

$$x \to cl(D(0) - D(x))$$

которое можно по линейности продолжить на группу дивизоров. Если $n(\sum k_i x_i) = 0$, т.е. $\sum k_i = 0$, то отображение, нужное нам, имеет вид

$$\sum k_i x_i = -cl(\sum k_i D(x_i))$$

При этом главные дивизоры, очевидно, переходят в нуль: по линейности достаточно проверить это для неприводимых D, а

тогда $\sum k_i D(x_i)$ является прямым образом главного дивизора $\sum k_i (x_i \times X)|_D$ на D.

Следовательно, соответствие D определяет эндоморфизм $J \to J$. Если $D \sim 0$ на $X \times X$, то этот эндоморфизм заведомо является нулевым. Поэтому естественно рассматривать группу классов соответствий относительно линейной эквивалентности. Оказывается, что построенный гомоморфизм

$$C(X) \to End\, J$$

является изоморфизмом ($C(X)$ - группа классов соответствий).

Для доказательства построим обратное отображение: рассматривая для $\alpha \in End\, J$ семейство $\Theta_\alpha \subset J \times J$ и его прообраз

$$(\varphi \times \varphi)^* \Theta_\alpha \subset X \times X$$

где $X \times X \xrightarrow{\varphi \times \varphi} J \times J$, без труда получим, что образ $(\varphi \times \varphi)^* \Theta_\alpha$ в группе $End\, J$ совпадает с α.

Для проверки рассмотрим диаграмму

$$(*) \qquad \begin{array}{ccccccc} X \times X & \xrightarrow{\varphi \times \varphi} & J \times J & \xrightarrow{\alpha \times \delta} & J \times J & \xrightarrow{\mu} & J \\ \uparrow \xi_x & & \uparrow \eta_x & & & & \\ X & \longrightarrow & J & & & & \end{array}$$

(Определяя ξ_x, η_x для $x \in X$ как $\xi_x(a) = x \times a$.

$\eta_x(a) = \varphi(x) \times \varphi(a)$). Прообраз Θ на $X \times X$ будет дивизором D_α; мы должны установить, что

$$Cl(D_\alpha(0) - D_\alpha(x)) = \alpha\, Cl(0-x)$$

По коммутативности получаем:

$$\varphi^* \eta_x^* (\alpha \times \delta)^* \mu^* =$$

$$= \varphi^* (\mu \circ (\alpha \times \delta) \cdot \eta_x)^* = \varphi^* (t_{\alpha\varphi(x)})$$

Значит,

$$D_\alpha(x) = \varphi^* t_{\alpha\varphi(x)}\, \Theta$$

$$D_\alpha(0) - D_\alpha(x) = \varphi^* ((1 - t_{\alpha\varphi(x)})\, \Theta)$$

Но

$$\mu \varphi^* ((1 - t_a)\, \Theta) = -a,$$

так что

$$\mu (D_\alpha(0) - D_\alpha(x)) = -\alpha\varphi(x) = \alpha\, Cl(0-x)$$

Это доказывает требуемое.

Лемма. Пусть $\alpha \in End\, J$. Обозначим через D_α – дивизор на $X \times X$, построенный выше, через D'_α – его образ при перестановке сомножителей $X \times X$. Тогда

$$n(D_\alpha(x)) = n(\varphi^*(\Theta))$$

$$n(D'_\alpha(x)) = n(\varphi^* \alpha^* (\Theta))$$

$$(D_\alpha, \Delta_x) = n(D'_{\alpha+\delta}(x)) = n(\varphi^* \alpha^* (\Theta))$$

Доказательство. Первое равенство следует из того, что, как мы уже проверили, $D_\alpha(x) = \varphi^* t_{\alpha\varphi(x)} \Theta$. При подсчете степени сдвиг Θ на $\alpha\varphi(x)$ не играет роли.

Для доказательства второго равенства заменим в диаграмме (*) отображения ξ_x, h_x на ξ'_x, h'_x, которые получаются из прежних перестановкой сомножителей; результат будет очевиден.

Наконец, для доказательства третьего равенства следует заменить ξ_x и h_x на диагональные вложения.

Пусть теперь $D \subset X \times X$ – дивизор; положим

$$d(D) = (D \cdot (x \times X))$$

$$d'(D) = (D \cdot (X \times x))$$

$$\tilde{d}(D) = (D \cdot \Delta_x)$$

Тогда $d + d' - \tilde{d}$ является инвариантом класса соответствия.

Предложение. $(d + d' - \tilde{d})(\alpha) = Tr(\alpha)$, где $Tr(\alpha)$ - след представления α в модуле Тэйта. Иначе говоря, учитывая, что $\tilde{d}$ есть число неподвижных точек α, получаем

$$\tilde{d}(\alpha) = d(\alpha) + d'(\alpha) - Tr(\alpha)$$

Доказательство. Выберем в качестве D дивизор D_α, канонически соответствующий α; по приведенным выше подсчетам

$$d(\alpha) = n(\varphi^*(\Theta))$$

$$d'(\alpha) = n(\varphi^*\alpha^*(\Theta))$$

$$\tilde{d}(\alpha) = n(\varphi^*(\alpha+\delta)^*(\Theta))$$

и нужно лишь сравнить результат с формулой (ххх) на стр.71.

Приложение: если $\alpha = \delta$, то доказанная формула дает индекс самопересечения диагонали: $(\Delta^2) = 2 - 2g$

В случае примера, приведенного в начале этого параграфа, мы приходим к формуле Гурвица, выражающей род кривой через степень накрытия $\varphi: X \to \mathbb{P}'$ и число точек ветвления.

§ 7. Гипотеза Римана

Мы теперь можем доказать следующий коренной результат:

Теорема ("Гипотеза Римана"). Характеристические корни эндоморфизма Фробениуса φ по модулю равны $q^{1/2}$

(Как всегда, q - число элементов основного поля; что касается характеристических корней φ, то они определены его представлением в модуле Тэйта $T_\ell(J)$; в этом случае соответствующий характеристический многочлен имеет целые, а не просто ℓ-адические коэффициенты).

Доказательство.

Сначала мы введем некоторую инволюцию $\varphi \to \varphi'$ в кольце эндоморфизмов, пользуясь установленным выше изоморфизмом $J \simeq Cl^\circ(J)$

Отображение $\alpha: J \to J$ определяет $\alpha^*: Cl^\circ(J) \to Cl^\circ(J)$ а α^* вместе с изоморфизмом $J \simeq Cl^\circ(J)$ определяют упомянутое α'.

Уточним сказанное. Для всех $a \in J$ и $\alpha \in End\, J$ имеем

$$\alpha^*(\tilde{\Theta}(0) - \tilde{\Theta}(a)) \sim \tilde{\Theta}(0) - \tilde{\Theta}(\alpha'(a)).$$

Иначе говоря, $\alpha^*(1 - t_a)\Theta \sim (1 - t_{\alpha'(a)})\Theta$. Из последней формулы следует полезное тождество:

$$(1 - t_a)\alpha^*\Theta = \alpha^*(1 - t_{\alpha(a)})\Theta \sim (1 - t_{\alpha'\alpha(a)})\Theta$$

Чтобы оправдать термин "инволюция", укажем основные свойства отображения $\alpha \to \alpha'$:

1. $(\alpha\beta)' = \beta'\alpha'$. (Для доказательства надо рассмотреть действие α^* на $Cl^\circ(J)$).

2. $(\alpha+\beta)' = \alpha' + \beta'$. (Чтобы проверить это равенство, надо вспомнить теорему о квадрате).

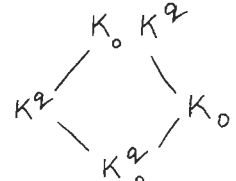
3. $(\alpha')' = \alpha$. (Это есть следствие симметрии $\tilde{\Theta}$ относительно перестановки множителей в $J \times J$).

4. Нашей инволюции $\alpha \to \alpha'$ соответствует перестановка множителей $X \times X$ при изоморфизме $End\, J \simeq C(X)$

Для доказательства сформулированной теоремы нам понадобятся

Лемма. Имеет место следующее равенство: $\varphi\varphi' = q$

Доказательство леммы. Во-первых, для любого n -мерного многообразия X над нашим основным полем k и эндоморфизма Фробениуса $\varphi: X \to X$ имеем: $deg\, \varphi = q^n$. В самом деле, если K - поле рациональных функций на X , то $deg\, \varphi = [K : K^q]$. Представим K в виде $K = K_0(\xi)$, где $K_0 = k(t_1, \dots, t_n)$ и K/K_0 конечно и сепарабельно. Тогда, очевидно, имеет место равенство $[K_0 : K_0^q] = q^n$. Равенство же $[K : K^q] = q^n$ следует из диаграммы:



в которой $K_0 K^q = K$, т.к. K над $K_0 K^q$ одновременно чисто несепарабельно и сепарабельно.

Поскольку Θ определен над k , $\varphi^*\Theta = r\Theta$ для некоторого целого r . Вычислим это r , применяя φ_* к обеим частям указанного равенства:

$$deg\, \varphi \cdot \Theta = \varphi_* \cdot \varphi^* \Theta = r \varphi_* \Theta = r q^{g-1} \Theta \text{ , где } g = \dim J$$

Откуда $\varphi^*\Theta = q\Theta$. Это же верно для любого дивизора D на J. Поэтому, с одной стороны

$$(1 - t_a)\varphi^*\Theta \sim (1 - t_{\varphi'\varphi(a)})\Theta$$

а с другой (напоминаем о теореме о квадрате и о тождестве)

$$\varphi^*\Theta = q\Theta$$

$$(1 - t_{qa})\Theta \sim (1 - t_{\varphi'\varphi(a)})\Theta$$

Откуда и вытекает, что $\varphi \cdot \varphi' = \varphi'\varphi = q$

Теперь приступим непосредственно к доказательству теоремы.

Введем в $End\, J$ скалярное произведение $(\alpha, \beta) = Tr(\alpha\beta')$ и покажем, что оно "эрмитово", т.е. что $(\alpha, \alpha) > 0$ при $\alpha \neq 0$.

Для этого воспользуемся формулой следа, доказанной выше:

$$Tr(\alpha) = n(D^n)^{-1}(D^{n-1}, L(\alpha, D))$$

при любом дивизоре D таком, что $(D^n) \neq 0$, например, при $D = \Theta$. Класс $L(\alpha, \Theta)$ нас интересует с точностью до численной эквивалентности. Он восстанавливается по классу линейной эквивалентности $(1 - t_a)L(\alpha, \Theta)$:

$$(1 - t_a)L(\alpha, \Theta) = (1 - t_{(\alpha+\delta)'(\alpha+\delta)a})\Theta -$$

$$(1 - t_{(\alpha'\alpha)a})\Theta - \Theta \sim (1 - t_\beta)\Theta = (1 - t_{(\alpha'+\alpha)(a)})\Theta$$

так как $\beta = [(\alpha+\delta)'(\alpha+\delta) - \alpha'\alpha - \delta]a = (\alpha'+\alpha)(a)$. В силу того, что $(\alpha\alpha')' = \alpha\alpha'$, получаем

$$(1 - t_a)L(\alpha\alpha', \Theta) \sim (1 - t_{2\alpha\alpha'(a)})\Theta = (1 - t_a)2\alpha^*\Theta$$

Следовательно, $L(\alpha\alpha', \Theta) \approx 2\alpha^*\Theta$ и $Tr(\alpha\alpha') = 2g(\Theta^g)^{-1} \times (\Theta^{g-1}, \alpha^*\Theta)$. Выше уже проверялось, что при $D > 0$ всегда $(D_0, \Theta^{g-1}) > 0$, чем и доказывается положительность скалярного произведения.

Применяя аналогичное рассуждение к $(\alpha+\beta)^*\theta - \alpha^*\theta - \beta^*\theta$ получаем равенство $T_\ell(\alpha') = T_\ell(\alpha)$ для всех α ; подробности мы опускаем.

Теперь остается применить неравенство Коши–Буняковского

$$|(\varphi^n, \delta)| \le (\varphi^n, \varphi^n)^{1/2} (\delta, \delta)^{1/2}$$

Имеем: $(\varphi^n, \varphi^n) = T_\ell(\varphi^n, \varphi'^n) = 2gq^n$

$$(\delta, \delta) = T_\ell \delta = 2g$$

Так что $|T_\ell(\varphi^n)| \le 2g q^{n/2}$ для всех n . С другой стороны

$$T_\ell(\varphi^n) = \sum_{i=1}^{2g} \lambda_i^n$$

Теперь легкое аналитическое рассуждение показывает, что $|\lambda_i| \le q^{1/2}$: ведь ряд

$$\sum_{i=1}^{2g} \frac{1}{1-\lambda_i T} = \sum_{n=0}^{\infty} T_\ell \varphi^n T^n$$

сходится в круге $|T| < q^{-1/2}$, а это и дает требуемое.

Наконец, так как $\prod \lambda_i = q^g$, то на самом деле $|\lambda_i| = q^{1/2}$, что и требовалось доказать.

Замечание. В этих рассуждениях мы пользовались инволюцией в $End\, J$ тогда как более естественным казалось бы использование некоторой инволюции в каком-нибудь $\mathbb{Z}$ -модуле представления M для $End\, J$ таком, что $T_\ell(J) = M \otimes Q_\ell$. Ж.П.Серр отмечает, что это невозможно: для суперсингулярной эллиптической кривой ранг $End_{\mathbb{Z}} M$ равен 4 и она проста; поэтому $rg_{\mathbb{Z}} M \ge 4$, тогда как $rg\, T_\ell(J) = 2$

§ 8. Приложение к оценке тригонометрической суммы

Пусть $f(x) \in \mathbb{F}_p[X]$, $0 < \deg f = m < p$ и $\zeta^p = 1$ Тогда

$$\left| \sum_{x=0}^{p-1} \zeta^{f(x)} \right| \le m p^{1/2}$$

Для доказательства строится вспомогательная кривая $y^p - y = f(x)$. Обозначим нормализацию ее пополнения через X . Пусть $X \xrightarrow{\pi} \mathbb{P}^1$ проекция $(x, y) \to (x)$. Тогда имеем:

$$\prod_{\xi \in X} \frac{1}{1-N(\xi)^{-s}} = \prod_{x \in \mathbb{P}} \prod_{\pi(\xi)=x} \frac{1}{1-N(x)^{-s}}$$

Если $x_\xi = \infty$, то $\pi(\xi) = x$ для единственной точки ξ и внутреннее произведение равно $\frac{1}{1-p^{-s}}$

Пусть $x_\xi \ne \infty$. Тогда уравнение $y^p - y = f(x)$ разрешимо в $\mathbb{F}_p(x_0)$ и при этом там p решений $y_0, y_0+1, \ldots, y_0+p-1$ с нормой $N(x_0)$. В этом случае внутреннее произведение равно $\left(\frac{1}{1-N(x)^{-s}}\right)^p$.

Уравнение $y^p - y = a$ разрешимо в $\mathbb{F}_p(a)$ тогда и только тогда, когда $T_{\mathbb{F}_p(a)/\mathbb{F}_p} a = 0$, т.е. когда

$$\sum_{i=0}^{\deg a - 1} a^{p^i} = 0$$

Нас интересует сумма

$$\sum f(x)\rho^i = \sum f(x^{p^i}) = \sum_{P(x)=0} f(x)$$

где в последней сумме x пробегает все корни неприводимого многочлена, отвечающего $\pi(\xi)$. Уже упоминавшееся внутреннее произведение всегда равно

$$\prod_{i=0}^{p-1} \frac{1}{1-\chi(\rho)N(\rho)^{-s}},$$

если положить $\chi(\rho)=\xi^{\lambda(\rho)}$, $\lambda(\rho)=\sum_{P(x)=0} f(x)$, $N(\rho)=p^{\deg P}$

В обычных обозначениях, положив $u=p^{-s}$, находим

$$Z_X(u) = \frac{1}{1-u}\prod_{\rho}\prod_{i=0}^{p-1}\frac{1}{1-\chi(\rho)^i u^{\deg \rho}}$$

где ρ пробегает все неприводимые многочлены из $\mathbb{F}_p[t]$

Выделяя множители с $i=0$ и меняя порядок умножения получаем:

$$Z_X(u) = \frac{1}{(1-u)(1-pu)}\prod_{i=1}^{p-1}\prod_{\rho}\frac{1}{1-\chi(\rho)^i u^{\deg \rho}}$$

Полагая для любого многочлена G со старшим коэффициентом 1:

$$\lambda(G)=\sum_{G(x)=0} f(x),\quad \chi(G)=\xi^{\lambda(G)}$$

получаем, что χ - мультипликативная, так что

$$L_i(u) = \prod_{\rho}\frac{1}{1-\chi(\rho)^i u^{\deg \rho}} = \sum_{G}\chi^i(G)u^{\deg G}.$$

Ниже будет показано, что $L_i(u)$ - многочлены и что $\deg L_i(u) \le \deg f$. А пока, поверив в это, вычислим коэффициент при первой степени u: он равен

$$\sum_{a\in\mathbb{F}_p}\chi^i(T-a) = \sum \xi^{i\lambda(T-a)} = \sum_{a=0}^{p-1}\xi^{i f(a)}$$

Но каждая из этих сумм равна поэтому сумме некоторых корней ξ-функции кривой X и число этих корней равно

$$\deg L_i(u) \le \deg f$$

Остается проверить, что $L_i(u)$ - многочлены.

В самом деле,

$$\lambda(G) = \sum_{G(x)=0} f(x) = \sum_i a_i \sum_{G(x)=0} x^i$$

если $f(x)=\sum a_i x^i$. Пользуясь формулами Ньютона, находим:

$$\sum_{\deg G = n}\chi(G) = \sum_{u_1,\dots,u_m}\xi^{(-1)^m m a_m + \varphi(u_1,\dots,u_{m-1})} =$$

$$= \left(\sum_{u_m}\xi^{(-1)^m a_m u_m}\right)\left(\sum_{u_1,\dots,u_{m-1}}\xi^{\varphi(u_1,\dots,u_{m-1})}\right)$$

и первая сумма равна нулю при $n > \deg f$.

Часть II

ЧИСЛОВЫЕ ПОЛЯ

§ 1. Модуль Тэйта числового поля

Модуль Тэйта якобиева многообразия кривой является функтором из категории кривых над полем k в категорию $\mathbb{Z}_\ell$-модулей. Мы хотим описать принадлежащую Ивасава конструкцию аналогичного функтора для категории одномерных числовых схем.

Напомним, что $T_\ell = \varprojlim J_{\ell^n}$, где

$$J_{\ell^n} = \mathrm{Ker}\, \ell^n \delta$$

и гомоморфизмы: $J_{\ell^n} \xrightarrow{\ell\delta} J_{\ell^{n-1}}$

Группу J_{ℓ^n} можно истолковать как группу Галуа неразветвленного накрытия $C_n \to C$ кривой C: C_n есть прообраз C (вложенной в J) относительно $\ell^n\delta$

Можно показать, что поле $\bigcup_n k(C_n)$ есть максимальное абелево неразветвленное ℓ-расширение поля $k(C)$. Группа Галуа его в точности совпадает с T_ℓ; это дает полезную содержательную интерпретацию модуля Тэйта. Здесь мы считаем, k алгебраически замкнутым.

Если априори поле k незамкнуто, то k может быть незамкнуто и внутри $k(J_{\ell^n})$; например, $k(J_{\ell^n})$ содержит корни степени ℓ^n из единицы (это следует из существования скалярного произведения Вейля).

В случае конечного поля k этого почти достаточно: для некоторого конечного расширения $k' \supset k$ имеем:

$$\bigcup_n k(J_{\ell^n}) = \bigcup_n k'(\zeta_{\ell^n})$$

В самом деле (топологические) степени эндоморфизма Фробениуса составляют одномерную подгруппу E группы $GL(2g, \mathbb{Z}_\ell) = \mathrm{Aut}(T_\ell(C))$. Группа $S = \{A \in GL(2g, \mathbb{Z}_\ell),\ A \equiv 1 \bmod 2\}$ является ℓ-силовским нормальным делителем; ее пересечение с E является ℓ-подгруппой конечного индекса в E. Поэтому, заменив k на конечное расширение k', мы получим, что $\bigcup_n k'(J_{\ell^n})$ является ζ-расширением и потому получается присоединением ζ_{ℓ^n}

Итак, $T_\ell C$, есть (в случае конечного поля k) группа Галуа сложного расширения $k(C) \subset \bar{k}(C) \subset A^{(\ell)}$, где $\bar{k} = \bigcup_n k'(\zeta_{\ell^n})$, $A(\ell)$ - максимальное неразветвленное абелево расширение поля $\bar{k}(C)$.

Теперь это определение можно перенести на числовой случай.

Пусть K - числовое поле; $K_n = K(\zeta_n)$, $\zeta_n^{\ell^n} = 1$; $\bar{K} = \bigcup K(\zeta_n)$, $A^{(\ell)} \supset \bar{K}$ - максимальное абелево неразветвленное расширение. Пусть $T_\ell(K)$ - группа Галуа $A^{(\ell)}/\bar{K}$. $T_\ell(K)$ является про-ℓ-группой, в частности, $\mathbb{Z}_\ell$-модулем. Неизвестно, имеет ли он конечное число образующих; Ивасава, однако, доказал, что пространство $V_\ell(K) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(K)$ конечномерно над $\mathbb{Q}_\ell$. На самом деле результат Ивасавы несколько точнее (см. ниже). $\dim V_\ell(K)$ может зависеть от ℓ, например, $V_\ell(\mathbb{Q}) = 0$, если и только если ℓ регулярно в смысле Куммера.

Для описания $T_\ell(K)$ нужно воспользоваться результатами теории полей классов.

§ 2. Применение теории полей классов

Пусть L/K - нормальное абелево расширение с группой G, D'_K - группа дивизоров K, неразветвленных в L. Закон взаимности Артина определяет эпиморфизм

$$D'_K \to G(L/K)$$

$$\mathfrak{a} \to (L/K, \mathfrak{a})$$

где для простых дивизоров $\mathfrak{p}$ поля K $(L/K, \mathfrak{p})$ определяется как соответствующий автоморфизм Фробениуса.

Нам еще нужно следующее функториальное свойство символа Артина:

$$(*)\quad (LK'/K', \mathfrak{a})\Big|_L = (L/K, N_{K'/K}\mathfrak{a})$$

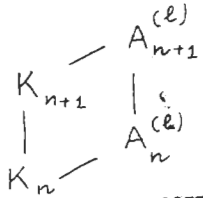
Нетривиальный результат теории полей классов, нужный нам, состоит в утверждении, что если A_K/K - максимальное неразветвленное абелево расширение, то ядро эпиморфизма $D_K \to G(A_K/K)$ состоит в точности из главных дивизоров. Отсюда и из (*) следует, что для всякого неразветвленного абелева расширения имеет место точная последовательность

$$Cl_L \xrightarrow{N} Cl_K \xrightarrow{(L/K,\,\mathfrak{a})} G(L/K) \to 1$$

где Cl - группа классов идеалов.

В частности, для расширений $K_n = K(\zeta_n)$ поля $A_n^{(\ell)}$ -

их максимальные абелевы неразветвленные расширения - имеют в качестве групп Галуа $Cl^{(\ell)}_{K_n}$. Рассматривая диаграмму



и (*), находим, что соответствующий гомоморфизм

$$Cl^{(\ell)}_{K_{n+1}} \to Cl^{(\ell)}_{K_n}$$

является норменным. Это показывает, что

$$T_\ell(K) = \varprojlim Cl^{(\ell)}_{K_n}$$

Мы установим сейчас, что сведения о модуле $T_\ell(K)$ позволяют получить информацию о числе классов полей K_n.

Группа Галуа расширения $\overline{K}/K$ является подгруппой конечного индекса группы $\mathbb{Z}_\ell \oplus \mathbb{Z}/(\ell-1)\mathbb{Z}$, т.е. изоморфна $\mathbb{Z}\oplus\mathbb{Z}/d\mathbb{Z}$, где $d \mid \ell-1$. С другой стороны, эта группа Галуа действует на $T_\ell(K)$; Ивасава сумел сделать из этого далеко идущие выводы. Расширение $\overline{K}/K_1$ имеет в качестве группы Галуа $\mathbb{Z}_\ell$ (и потому является Γ - расширением в смысле Ивасава). Башня полей $K_1 \subset \overline{K} \subset A$ определяет расширение $T_\ell(K)$ с помощью $\mathbb{Z}_\ell$, которое описывается структурой $T_\ell(K)$ как $\mathbb{Z}_\ell$-модуля. Ситуация аналогична той, которая изучена в функциональном случае.

Действие группы Галуа на $T_\ell(K)$ на конечных уровнях согласовано с интерпретацией с помощью символа Артина:

$$(L/K, w^g) = (L/K, w)^g$$

Расширение $\bar{K}/K_1$ разветвлено и притом только в делителях ℓ (легкое следствие из локальной теории).

Пусть $\ell_1, \dots, \ell_r$ - эти дителители ℓ в K_1; пусть $\mathcal{L}_1, \dots, \mathcal{L}_r$ - их продолжения на $\bar{K}$. Обозначим через $\bar{\mathcal{J}}_K$ группу инерции $\mathcal{L}_K$ в $A^{(\ell)}$; $\bar{\mathcal{J}}_K$. Образ $\bar{\mathcal{J}}$ в Γ тоже является группой инерции: $\bar{\mathcal{J}}_K \xrightarrow{\sim} \ell^{m_K}\Gamma$. Взяв $m = \max m_K$ и заменив K_1 на K_{m_ℓ} мы можем считать, что $\bar{\mathcal{J}}_K \xrightarrow{\sim} \Gamma$. Это проясняет структуру G :

$$T = \Gamma_{\left\{ \begin{matrix} A^{(\ell)} \\ \frac{1}{K} \end{matrix} \right.}$$

$$\mathbb{Z}_\ell = \Gamma_{\left\{ \begin{matrix} 1 \\ K_1 \end{matrix} \right.}$$

$$G = T\bar{\mathcal{J}}_K, \quad T \cap \bar{\mathcal{J}}_K = \{1\},$$

и $\bar{\mathcal{J}}_K$ вкладывается в G как группа инерции любого простого дивизора $\mathcal{L}_K$

Выберем в $\bar{\mathcal{J}}_K$ образующие согласованно с фиксированной образующей $\gamma \in \Gamma$: $\bar{\mathcal{J}}_K = \{s_K\}$. Элементы

$$a_K = s_K s_1^{-1} \in T$$

являются инвариантами нашего расширения; впрочем, $r = 1$ при $K = \mathbb{Q}$, так что здесь их не будет.

Расширение поля K_1 неразветвлено и абелево, если оно соответствует такой подгруппе $H \subset G$, что $H \supset \bar{\mathcal{J}}_K$ и $H \supset (G, G)$.

Для вычисления (G, G) заметим, что $s_1^{-1} a s = a^\gamma$;

имеем: $(G, G)\bar{\mathcal{J}}_K$ порождена S_K и элементами вида $a^{1-\gamma}$, $a \in T$. Поэтому группа Галуа поля $A_1^{(\ell)}/K_1$ изоморфна:

$$G/\{T^{1-\gamma}, s_1, \dots, s_r\} = G/\{T^{1-\gamma}, s_1, a_2, \dots, a_r\} =$$

$$= \{s_1, T\}/T_1$$

где $T_1 = \{T^{1-\gamma}, a_2, \dots, a_r\}$, т.е. $T/T_1 = G(A_1^{(\ell)}/K_1)$.

Следовательно,

$$Cl_{K_1}^{(\ell)} = T/\{T^{1-\gamma}, a_2, \dots, a_r\}$$

Замена K_1 на K_n изменит γ на $\gamma^{\ell^{n-1}}$

Далее, S_K заменится на $S_K^{\ell^{n-1}}$, а a_K перейдут в

$$S_K^{\ell^{n-1}} S_1^{-\ell^{n-1}} = (a_K S_1)^{\ell^{n-1}} S_1^{-\ell^{n-1}} =$$

$$= a_K^{1+\gamma+\dots+\gamma^{\ell^{n-1}-1}} =$$

$$= a_K^{\nu_{n-1}} .$$

где $\nu_n = 1 + \gamma + \dots + \gamma^{\ell^n - 1}$. Следовательно, полагая

$$G_n = Cl^{(\ell)}(A^{(\ell)}/K_n),$$

$$u_1 = (a_1, \dots, a_2, T^{1-\gamma}),$$

получим

$$G_n = T/u_n$$

где

$$u_n = u_1^{\nu_{n-1}}$$

Выведем теперь следствия из следующего предположения:

Гипотеза. $T_\ell(K_n)$ имеет конечное число образующих.

Пусть $\ell^{e(G)}$ - максимальный ℓ -делитель порядка группы G . Мы оценим $e(G_n)$.

В силу гипотезы $T_n \simeq \mathbb{Z}_\ell^\lambda \oplus H$, где $|H| < \infty$. Отбросив H , мы изменим $e(G_n)$ на константу, не зависящую от n при $n \geq n_0$. Действие γ определяет элемент $\gamma \in GL(\lambda, \mathbb{Z}_\ell)$ и $\gamma^{\ell^n} \to E$ при $n \to \infty$.

Пусть $\gamma^{\ell^k} \equiv E \bmod \ell^2$

Имеем

$$\nu_{n+1} = \nu_n (1 + \gamma^{\ell^n} + \gamma^{2\ell^n} + \dots + \gamma^{\ell^n(\ell-1)})$$

при $n \geq k$ выражение в скобках $= \ell(E + \ell C)$, где $C \in M(\lambda, \mathbb{Z}_\ell)$, откуда индукцией по n , имеем:

$$\nu_n = \ell^{n-k} \nu_k F_n$$

где F_n обратимы. Далее,

$$e(T/\nu_{n-1}u_1) = e(T/u_{k+1}) + e(u_{k+1}/\nu_{n-1}u_1)$$

$$e(u_{k+1}/\nu_{n-1}u_1) = e(u_{k+1}/\ell^{n-k-1}u_{k+1}) =$$

$$= \lambda(n-k-1) = \lambda_n - \lambda(k-1)$$

Здесь λ , k и $e(T/u_{k+1})$ не зависят от n , так что

(*) $e(G_n) = e_n = \lambda n + \text{Const}$ при $n \geq n_0$

Для некоторых полей гипотезу удается доказать, и тогда будет доказана и (*).

§ 3. Групповая алгебра группы $G(\bar{K}/K_1)$

Теперь мы будем исследовать T как Γ -модуль. Мы хотим построить некоторое "групповое кольцо" для группы Γ с коэффициентами $\mathbb{Z}_\ell$

Сделаем это для произвольной про- ℓ -группы $\mathcal{G} = \varprojlim G_n$.

Кольцо конечной группы $\mathbb{Z}_\ell[G]$ можно определить очевидным универсальным свойством для отображений групп в $\mathbb{Z}_\ell$ - алгебры.

Аналогичное универсальное свойство для отображений про- ℓ -группы $\mathcal{G}$ в компактные топологические $\mathbb{Z}_\ell$ - алгебры определяет топологическое групповое кольцо

$$\mathbb{Z}_\ell[\mathcal{G}] \overset{def}{=\!=} \varprojlim \mathbb{Z}_\ell[G_i]$$

Мы опустим формальную проверку универсальности.

В кольце $\mathbb{Z}_\ell[\Gamma]$ положим $X = \gamma - 1$; легко видеть, что $X^{\ell^n} \to 0$ при $n \to \infty$, так что определен гомоморфизм кольца формальных рядов

$$\mathbb{Z}[[T]] \to \mathbb{Z}_\ell[\Gamma] \ : \ T \to X$$

На самом деле это изоморфизм (в $\mathbb{Z}_\ell[[T]]$ топология покоэффициентной сходимости): действительно, $(1+T)^{\ell^n} \to 1$ при $n \to \infty$ и отображение $\gamma \to 1+T$ определено и обратно к рассмотренному на элементах группы Γ , потому что $(1+T)^\alpha$ имеет смысл для $\alpha \in \mathbb{Z}_\ell$; по универсальности оно продолжается до отображения $\mathbb{Z}_\ell[\Gamma]$.

Дальше мы будем отождествлять $\mathbb{Z}_\ell[\Gamma]$ с $\mathbb{Z}_\ell[[X]]$. Это регулярное двумерное локальное кольцо с максимальным идеалом (ℓ, X) ; T - компактный модуль над ним. Дальше мы будем записывать T -аддитивно.

Вот простое

Следствие. Пусть $r = 1$ (например, $K = \mathbb{Q}$) и пусть $\ell \chi | Cl\, K_1|$, например, ℓ регулярно при $K = \mathbb{Q}$. Тогда $G_1 = T/XT$, т.е. $T = XT = mT$. Из топологического варианта леммы Накаяма следует, что $\ell \chi |G_n|$ при всех n .

(Это рассуждение буквально верно для $\ell > 2$; при $\ell = 2$ следует предполагать, что $2\chi | Cl(K(\sqrt{-1}))$; отсюда будет следовать, что $2\chi | Cl\, K(\zeta_n)|$. Для $K = \mathbb{Q}$

это было доказано Вебером с помощью явных формул).

Топологическая лемма Накаямы. Если T - компактный модуль над локальным кольцом с м.и. m , $T = mT$, то $T = 0$.

Доказательство. При достаточно большом n имеем $m^n T \subset V$, где V - сколь угодно малая окрестность нуля у T - противоречие.

§ 4. Модуль Тэйта как операторный модуль

Мы докажем теперь для модулей Тэйта следующие два свойства:

а. T имеет конечное число образующих.

б. T является модулем кручения (над $\mathbb{Z}_\ell[\Gamma]$).

Для доказательства а. заметим, что

$$|G_1| = |T/(a_2, \dots, a_r, XT)| < \infty$$

откуда легко следует, что

$$|T/(\ell, X)T| < \infty$$

и с использованием леммы Накаяма получаем, что образующие $T/(\ell, X)T$ поднимаются до образующих T над $\mathbb{Z}_\ell[[X]]$

Перейдем к доказательству б. Пусть K - поле частных $\mathbb{Z}_\ell[[X]]$. Тогда последовательность

$$Tors\, T \to T \xrightarrow{\varphi} T \otimes_{\mathbb{Z}_\ell[[X]]} K$$

точна. Для доказательства периодичности T достаточно проверить, что $U_1 \otimes K = 0$. Если $U_1 \otimes K \neq 0$, т.е. есть такая линейная функция $\varphi: U_1 \otimes K \to K$, что $\varphi\varphi(U_1) \neq 0$. Пусть $\varphi\varphi(U_1)$ порожден элементами $\frac{a_i}{x_i}$; $x_i \in \mathbb{Z}_\ell[[X]]$, $i = 1, \dots, r$; тогда $(x_1 \dots x_r)\varphi\varphi(U_1) \subset \mathbb{Z}_\ell[[X]]$ есть некоторый идеал $w \neq 0$ гомоморфный образ U_1.

Имеем

$$|U_1 / \nu_n U_1| < \infty$$

$$\nu_n = \frac{(X+1)^{\ell^n} - 1}{X} = F_n(X)$$

Поэтому также

$$|w / F_n(X) w| < \infty$$

для всех n.

Заметим, что $\mathbb{Z}_\ell[X]/(F_n(X))$ есть свободный $\mathbb{Z}_\ell$-модуль ранга $\ell^n - 1$; из подготовительной леммы Вейерштрасса

следует, что $\mathbb{Z}_\ell[[X]]/(F_n(X))$ устроен так же.

Но у такого фактора нет конечных подгрупп, поэтому неизбежно $\alpha < (F_n(X))$, так что все образующие α делятся на $F_n(X)$. Пусть $\alpha = F_n(X)^\kappa \alpha_1$, где κ – максимальное целое число; $\alpha \simeq \alpha_1$, как $\mathbb{Z}_\ell[[X]]$-модули, а для α_1, то же рассуждение ведет к противоречию.

§ 5. Периодические $\mathcal{O}$-модули

Для дальнейшего исследования $\mathbb{Z}_\ell[[X]]$-модулей нам понадобятся сведения о структуре идеалов кольца $\mathbb{Z}_\ell[[X]]$. Оно двумерно; все цепочки его простых идеалов имеют вид $(0) \subset P \subset m = (\ell, X)$. Все не максимальные простые идеалы главные; в силу подготовительной леммы Вейерштрасса, в качестве образующей такого идеала всегда можно выбрать многочлен вида

$$\ell^\kappa (X^m + a_1 X^{m-1} + \dots + a_m), \quad a_i \in \ell\mathbb{Z}_\ell$$

Пользуясь этими сведениями, можно получить классификацию периодических модулей "с точностью до конечных модулей".

Определение. Модули M, M' называются квазиизоморфными, если существует такой гомоморфизм $f: M \to M'$, что $\operatorname{Ker} f$ и $\operatorname{Coker} f$ конечны.

Лемма. M квазиизоморфен нулю (то есть конечен), если и только если $M_P = 0$ для всех простых элементов P.

(Здесь $M_P = M \otimes \mathbb{Z}_\ell[[X]]_P$; $\mathcal{O}_P$ – кольцо частных относительно $\mathcal{O} \setminus (P)$).

Доказательство. $\operatorname{Ann} M$ не содержит ни одного простого P; поэтому его радикал совпадает с $m = (\ell, X)$; но тогда $m^\kappa \subset \operatorname{Ann} M$, так что M есть фактормодуль конечного модуля $\mathbb{Z}_\ell[[X]]^r / m^\kappa \mathbb{Z}_\ell[[X]]^r$

Следствие. $f: M \to M'$ является квазиизоморфизмом, если и только если все его локализации по минимальным простым идеалам $f: M_p \to M'_p$ являются изоморфизмами.

Впредь будем обозначать $\mathcal{O} = \mathbb{Z}_\ell[[X]]$ и будем рассматривать полулокальные кольца $\bar{\mathcal{O}}$, являющиеся локализациями относительно конечного числа идеалов P.

Всякому периодическому модулю M с конечным числом образующих можно поставить в соответствие полулокальное кольцо $\bar{\mathcal{O}}$, соответствующее тем P, которые аннулируют элементы из M, и $\bar{\mathcal{O}}$-модуль $\bar{M} = \bar{\mathcal{O}} \otimes M$

Легко видеть, что $f: M \to M'$ есть квазиизоморфизм, если и только если $f: \bar{M} \to \bar{M}'$ является изоморфизмом. С другой стороны, $\bar{\mathcal{O}}$ есть кольцо главных идеалов, так что структуру $\bar{\mathcal{O}}$-модуля $\bar{M}$ легко описать:

$$\bar{M} \simeq \oplus\, \bar{\mathcal{O}}/p_i^{k_i}$$

В категории $\mathcal{O}$-модулей прямые суммы $\oplus\, \mathcal{O}/p_i^{k_i}\mathcal{O}$ составляют такой набор модулей, что их локализации дают все периодические $\bar{\mathcal{O}}$-модули с точностью до изоморфизма.

Поэтому если задан периодический $\mathcal{O}$-модуль M, такой, что $\bar{\mathcal{O}}$-модуль $\bar{M}$ имеет вид $\oplus\, \bar{\mathcal{O}}/p_i^{k_i}\bar{\mathcal{O}}$, мы можем построить $\mathcal{O}$-модуль $N = \oplus\, \mathcal{O}/p_i^{k_i}\mathcal{O}$ с той же локализацией. Для доказательства квазиизоморфизма нам нужно еще построить гомоморфизм с конечным ядром и коядром.

Рассмотрим диаграмму

$$\begin{array}{ccccc} M & \to & \bar{M} & \simeq & \bar{N} \\ & & & & \uparrow \\ & & & & N \end{array}$$

(стрелки $M \to \bar{M}$ и $N \to \bar{N}$ - естественные, а $\bar{M} \to \bar{N}$ - любой $\bar{\mathcal{O}}$-изоморфизм). Существует такой элемент $c \in \mathcal{O}$ $c \notin \cup p_i$, что образ cM в $\bar{N}$ содержится в образе N. Это определяет гомоморфизм $M \to N$, который, как нетрудно проверить, является квазиизоморфизмом.

Итак, имеет место

Теорема. Всякий периодический $\mathcal{O}$-модуль с конечным числом образующих квазиизоморфен модулю вида

$$\oplus\, \mathcal{O}/p_i^{k_i}\mathcal{O}$$

Положим

$$e(M/\gamma_n M) = e_M(n)$$

Нетрудно проверить, что замена M на квазиизоморфный ему модуль M' приводит к тому, что

$$e_M(n) - e_{M'}(n) = const \quad \text{при } n \geq n_0$$

Вычислим функции e_M для $\oplus\, \mathcal{O}/p_i^{k_i}\mathcal{O}$

Лемма. Пусть $M = \mathcal{O}/p^k\mathcal{O}$. Тогда

$$e_M(n) = \begin{cases} (k \deg P)n, & \text{если } P = X^m + a_1 X^{m-1} + \dots \\ k\ell^n - k, & \text{если } P = \ell \end{cases}$$

Доказательство. На многочлены с единичным старшим коэффициентом можно делить с остатком в кольце $\mathbb{Z}_\ell[[X]]$; поэтому многочлены над $\mathbb{Z}_\ell$ степени $m-1$ образуют систему представителей $\bmod F$, $F = X^m + \dots + a_0$. В частности, M имеет конечный тип над $\mathbb{Z}_\ell$, и первая часть леммы следует из

подсчета, сделанного ранее.

Для доказательства второй части напомним, что

$$V_n = \frac{(1+X)^{\ell^n} - 1}{X} = X^{\ell^n - 1} + \dots$$

Далее, как выше, кольцо классов $\mathrm{mod}\,(V_n, \ell^K)$ имеет в качестве системы представителей многочлены из $\mathbb{Z}_\ell/\ell^K\mathbb{Z}_\ell[X]$ степени $\le \ell^n - 1$, что дает требуемое.

Следствие. Для всякого периодического $\mathcal{O}$-модуля M с конечным числом образующих

$$e_M(n) = \lambda n + \mu \ell^n + \nu, \quad n \ge n_0$$

λ, μ, ν - константы.

Экспоненциальное слагаемое получается из бесконечной ℓ-группы конечного периода, а линейное - из свободной ℓ-группы с конечным числом образующих. Неизвестны случаи, когда $\mu \neq 0$, но и вообще примеров вычисления μ мало.

Пространство $V_\ell(K) = T_\ell(K) \otimes \mathbb{Q}_\ell$ конечномерно; если $T_\ell(K) \sim \oplus \mathcal{O}/p_i^{\kappa_i}\mathcal{O}$, то

$$\dim V_\ell(K) = \sum \kappa_i \deg p_i$$

Эта размерность совпадает со степенью характеристического многочлена X при действии в $V_\ell(K)$; рассмотрение этого многочлена дальше будет играть большую роль.

Замечание. В последней части теории мы пользовались лишь тем, что группа Галуа K/K_1, изоморфна Γ. Вопрос об обозрении Γ-расширений очень интересен.

Γ-расширения абелевы; в них ветвятся лишь делители ℓ. Пусть S -множество этих делителей.

Теория полей классов позволяет описать максимальное абелево расширение, разветвленное лишь в S, поля k.

Пусть $\mathcal{J}$ - группа иделей k, C - группа классов иделей. Пусть $K \supset k$ - абелево расширение; $H \subset \mathcal{J}$ -соответствующая группа. Простой идеал $\mathfrak{p}$ поля k не ветвится в K, если H содержит все идели с $\mathfrak{p}$-компонентами в $\mathcal{U}_\mathfrak{p}$.

Пусть

$$\mathcal{U}_S = \prod_{\mathfrak{p} \notin S} \mathcal{U}_\mathfrak{p}, \quad \mathcal{U} = \mathcal{U}_\varnothing$$

Максимальное расширение, разветвленное в S, соответствует подгруппе $\overline{k^* \mathcal{U}_S}$ (черта - замыкание). Группа Галуа этого расширения изоморфна $\mathcal{J}/\overline{k^* \mathcal{U}_S}$; нас интересуют ее факторгруппы, изоморфные Γ.

Группа $\overline{k^* \mathcal{U}}$ имеет в $\mathcal{J}$ конечный индекс; поэтому достаточно рассмотреть $\overline{k^* \mathcal{U}}/\overline{k^* \mathcal{U}_S}$. Но $\mathcal{U}/\mathcal{U}_S$ компактна и применима теорема о гомоморфизмах:

$$\overline{k^* \mathcal{U}}/\overline{k^* \mathcal{U}_S} \simeq (\mathcal{U}/\mathcal{U}_S)/(\overline{k^* \cap \mathcal{U}})$$

Пусть $E = k^* \cap \mathcal{U}$ - группа единиц; $\mathcal{U}/\mathcal{U}_S = \prod_{\mathfrak{p} \in S} \mathcal{U}_\mathfrak{p}$ - группа ℓ - адических единиц.

У группы $\mathcal{U}_{\ell_i}$ есть подгруппа конечного индекса, изоморфная $\mathbb{Z}_\ell^{f_i}$ где $f_i = [k_{\ell_i} : \mathbb{Q}_\ell]$, а у $\mathcal{U}/\mathcal{U}_S$ - аналогичная подгруппа $\mathbb{Z}_\ell^{[k:\mathbb{Q}]}$. В эту группу вкладывается подгруппа единиц E_0 конечного индекса. Замыкание образа E_0 там име-

ет ранг $\leq rk\, E_s = r_1 + r_2 - 1$, (теорема Дирихле); здесь $[k:\mathbb{Q}] = r_1 + 2r_2$, $k\otimes\mathbb{R} = \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$. Поэтому во всяком случае

$$rk\,(U/U_S)/\overline{E} \geq r_2 + 1$$

Вопрос о ранге $\overline{E}_0$ не решен; "ℓ-адическая теорема Дирихле" доказана лишь в нескольких примерах (циклические кубические расширения $\mathbb{Q}$)*)

Во всяком случае, r_2+1 "независимых" Γ-расширений у всякого поля есть. Если $r_2 = 0$, то есть поле вполне вещественно, то, конечно, получается $\bigcup_n k(\zeta^n)$, $\zeta_n^{\ell^n} = 1$ (с точностью до расширений конечной степени).

Еще одна гипотеза: модуль $T_\ell(K)$ должен быть модулем одномерных когомологий в некоторой топологии, аналогичной топологии Гротендика.

Если это так, должно существовать скалярное произведение $T_\ell(K)\times T_\ell(K)\to\mathbb{Q}$. Конструкция А.Вейля с функционального случая переносится и на числовой, но получающееся произведение заведомо может быть вырожденным. Возможно, что его ядро совпадает с периодической частью!

§ 6. Формула для числа классов кругового поля

Мы переходим к исследованию модуля Тэйта поля рациональных чисел.

Исследование $T_\ell(\mathbb{Q})$ основано на том, что для числа классов круговых полей $\mathbb{Q}(\zeta_n)$, $\zeta^{\ell^n} = 1$ имеются точные

*) В последнее время Брюмер доказал эту гипотезу для любых абелевых расширений поля $\mathbb{Q}$, основываясь на теоремах Бейкера о приближениях.

формулы. Более тонкое исследование позволяет извлечь из этих формул сведения о структуре ℓ-компоненты группы классов. Переход к пределу дает информацию о $T_\ell(\mathbb{Q})$

Мы дадим набросок аналитической теории, приводящей к вычислению числа классов.

Пусть $[K:\mathbb{Q}] < \infty$; имеем

$$(*)\qquad \operatorname*{res}_{s=1} \zeta_K(s) = h\,2^{r_1+r_2}\,\pi^{r_2}\,\frac{R}{w\sqrt{|D|}}$$

Здесь $K\otimes\mathbb{R} = \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$; D - дискриминант поля; R - регулятор, w - порядок максимальной конечной подгруппы K^*; наконец, h - число классов.

В случае $K = \mathbb{Q}(\zeta_n)$ имеем :

$$\zeta_K(s) = \prod L(s,\chi)$$

где χ пробегает $Char\,(\mathbb{Z}/\ell^n\mathbb{Z})^*$, и

$$(**)\qquad L(s,\chi) = \sum \frac{\chi(m)}{m^s}$$

где суммирование происходит по всем m, взаимно простым с ведущим идеалом $f(\chi)$ характера χ. При $\chi\neq\varepsilon$ величина $L(1,\chi)$ конечна. Пользуясь тем, что $L(s,\chi) = \zeta_{\mathbb{Q}}(s)$ и $\operatorname*{res}_{s=1} \zeta_{\mathbb{Q}}(s) = 1$, находим из (*) и (**):

$$h\,2^{r_1+r_2}\,\pi^{r_2}\,\frac{R}{w\sqrt{|D|}} = \prod_{\chi\neq\varepsilon} L(1,\chi)$$

Правая часть вычисляется в конечном виде по следующей причине.

Пусть $\psi \in Char\ \mathbb{Z}/m\mathbb{Z}$ (аддитивный характер). Тогда

$$\sum \frac{\psi(n)}{n} = \sum \frac{\psi(1)^n}{n} = -\ln(1-\psi(1))$$

(суммирование по Абелю). Но любую комплексно-значную функцию на $\mathbb{Z}/m\mathbb{Z}$ можно разложить по характерам ψ:

$$f = \sum_{\psi} (f, \psi)\psi,$$

где

$$(f_1, f_2) = \frac{1}{m}\sum_{a} f_1(a)\overline{f_2(a)}$$

Отсюда немедленно находим:

$$L(1,\chi) = -\sum_{\psi} (\chi, \psi)\log(1-\psi(1)).$$

Рассмотрим суммы Гаусса:

$$\tau(\chi,\psi) = m(\chi, \overline{\psi}) = \sum \chi(a)\psi(a)$$

Пусть ψ_0 – образующая группы характеров. Для всякого $c \in \mathbb{Z}/m\mathbb{Z}$ положим

$$\psi_c(a) = \psi_0(ca)$$

Если $c \in (\mathbb{Z}/m\mathbb{Z})^*$, то $\sum \chi(a)\psi(a) = \sum \chi(c^{-1}a)\psi(a)$, так что

$$\tau(\chi, \psi_c) = \overline{\chi(c)}\,\tau(\chi, \psi_0)$$

Если же c необратим, то эта же формула верна потому, что $\tau(\chi, \psi_c) = 0$ и $\chi(c) = 0$ по определению.

Отсюда:

$$L(1,\chi) = -\frac{\tau(\chi,\psi_0)}{m}\sum \overline{\chi(c)}\log(1-\psi_0(c))$$

Пусть $\psi_0(1) = \varepsilon^{\frac{2\pi i}{m}} = \zeta$, $\tau(\chi, \psi_0) = \tau(\chi)$. Хорошо известно, что $|\tau(\chi)|^2 = m$

Выражение

$$L(1,\chi) = \frac{-\tau(\chi)}{m}\sum_{(c,m)=1} \chi(c)\log(1-\zeta^{-c})$$

преобразуем, воспользовавшись формулой:

$$\log(1-\zeta^{-c}) = \log|1-\zeta^{-c}| + i\pi\left(\frac{1}{2} - \frac{c}{m}\right)$$

Если $\chi(-1) = -1$, т.е. $\chi(-c) = -\chi(c)$, то

$$\sum \chi(c)\log|1-\zeta^{-c}| = 0,$$

так что

$$L(1,\chi) = \frac{i\pi\cdot\tau(\chi)}{m^2}\sum_{(c,m)=1} c\,\chi(c), \qquad \boxed{\chi(-1) = -1}$$

Если же $\chi(-1)=1$, т.е. $\chi(-c)=\chi(c)$, то

$$\sum_{(c,m)=1}\chi(c)\left(i\pi\left(\frac{1}{2}-\frac{c}{m}\right)\right) = 0,$$

так что

$$L(1,\chi) = -\frac{\tau(\chi)}{m}\sum_{(c,m)=1}\chi(c)\log|1-\zeta^{-c}|, \quad \chi(-1)=1$$

В результате для числа классов h получается разложение на два множителя, соответствующие четным и нечетным характерам χ (константы $2^{r_1+r_2}$, ω и регулятор перегруппировываются некоторым естественным способом): $h = h_+ h_-$

§ 7. Четные характеры

Множитель h_+ имеет вид $h_+ = R^{-1}H$, где

$$(*)\qquad H = \prod_{\substack{\chi(-1)=1\\ \chi\neq 1}}\sum_{c \bmod f(\chi)}\chi(c)\log|1-\zeta^{-c}|$$

Можно считать, что χ - характер $(\mathbb{Z}/m\mathbb{Z})^*/(\pm 1)$.

Произведение $\prod_{\chi\in Char G}\sum_{g\in G}\chi(g)\,x_g$, $x_g\in\mathbb{C}$ можно интерпретировать, введя элемент

$$x = \sum x_g\, g \in \mathbb{C}[G] = A$$

Имеем $A = \sum \mathbb{C}\,\varepsilon_\chi$; $x = \sum \chi(x)\,\varepsilon_\chi$. Произведение координат элемента x в этом разложении есть норма x в групповой алгебре:

$$\det A_x = \prod\chi(x)$$

Отсюда следует, что если $\Omega = \sum g\,\mathbb{Z}$, то

$$\prod_\chi \chi(x) = V(x\Omega)/V(\Omega)$$

где V - объем соответствующей решетки.

Произведение (*) можно считать распространенным на все неединичные характеры группы $(\mathbb{Z}/m\mathbb{Z})^*/(\pm 1)$

Если мы хотим обобщить данную выше интерпретацию произведения $\prod\chi(x)$ на произведения по $\chi=\varepsilon$, нам надо ограничить A_x на идеал, порожденный элементами $1-g$, $g\in G$:

$$\prod_{\chi\neq\varepsilon}\chi(x) = V(x\sigma)/V(\sigma),$$

$\sigma = \sum(1-g)\mathbb{Z}$. Так как $V(\sigma) = \sqrt{n}$, $n = |G|$, то достаточно вычислить

Мы хотим вычислить.

$$x = \sum x_{3i}\,\delta^i$$

$$(1-\delta)x = \sum(x_{3i} - x_{3i+1})\,\delta^i$$

У элемента (ж)

$$x_{s^i} = \log|1 - \zeta^{-s^i}| = \log|\lambda^{s^i}|$$

$$\lambda = 1 - \zeta^{-1}$$

Дальше:

$$\log|\lambda^{s^i}| - \log|\lambda^{s^{i+1}}| = \log\left|\frac{\lambda^{s^i}}{\lambda^{s^{i+1}}}\right|$$

Полагая

$$\varepsilon = \frac{\lambda}{\lambda^s} = \frac{1-\zeta}{1-\zeta^s}$$

находим наконец:

$$(1-s)x = \sum \log|\varepsilon^{s^i}|s^i$$

Здесь ε^{s^i} - так называемые круговые единицы. Координаты $(1-s)x$ - вектор, соответствующий ε в логарифмическом пространстве; меняя c, мы получим решетку, натянутую на образы всех круговых единиц. Круговые единицы корнями из 1 отличаются от вещественных; в логарифмическом пространстве их образы совпадают с образами вещественных единиц. Вспомнив определение регулятора, получим, что $h_+ = V(E_0)/V(E)$, где - объем решетки соответствующих единиц. Индекс решетки равен отношению объемов, и мы получаем

$$h_+ = (E : E_0)$$

где E_0 - подгруппа круговых единиц в вещественном подполе. Проверяется, что h_+ совпадает с числом классов вещественного подполя.

Пример. $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$, если $p \equiv 1 \bmod 4$. Единица

$$\varepsilon_0 = \frac{\prod(1-\zeta^a)}{\prod(1-\zeta^b)}, \quad \left(\frac{a}{p}\right) = 1, \quad \left(\frac{b}{p}\right) = -1$$

вещественная, и $\varepsilon_0 = \varepsilon_1^h$, где ε_1 - основная единица, а h число классов. Тем не менее, группы E/E_0 и $Cl\,K_0$ могут не быть изоморфны, ибо первая из них циклична, а вторая не всегда. Было бы очень интересно дать групповую интерпретацию этих формул.

Нас интересует l-компонента $Cl\,K_n$, $K_n = \mathbb{Q}(\zeta_{l^n})$. Пусть $K_n^+ \subset K_n$ - вещественное подполе. Для всех l, когда h^+ вычислено ($l \le 4001$), имеем $h^+ \not\equiv 0 \bmod l$ для K_1. Поэтому $h^+ \not\equiv \bmod l$ для всех n, ибо $\bigcup K_n$ есть Γ-расширение.

Результаты Ивасавы относятся только к тем l, для которых $h^+ \not\equiv 0 \bmod l$; этот факт используется в таком виде:

$$(E : E_0) \not\equiv 0 \bmod l$$

в полях K_n^+, т.е. $\bmod l^n$ - x степеней E_0 порождает группу E. Структура $E \otimes \mathbb{Z}_l$, как Γ-модуля совпадает со структурой $E_0 \otimes \mathbb{Z}_l$, и это обстоятельство будет основой дальнейшего изложения.

Последнее замечание. Так как $(K : K^+) = 2$ $l \neq 2$, вложения и норма устанавливают изоморфизм между $Cl^{(l)}(K^+)$ и $Cl^{(l)}(K)^{\mathbb{Z}_2}$, где $\mathbb{Z}_2 = Gal\,(K/K^+)$.

§ 8. Нечетные характеры. Интерпретация h^- как порядка группы

Теперь мы займемся ℓ-компонентой группы $Cl\,K$, порядок которой является делителем первого множителя числа классов и которая, предположительно, составляет всю ℓ-компоненту.

Пусть $S = Cl^{(\ell)}(K_n)$, $K_n = \mathbb{Q}(\zeta_n)$; положим $S = S^+ \oplus S^-$ где $x \in S^+ \Leftrightarrow \tau x = x$, $y \in S^- \Leftrightarrow \tau y = -y$; τ - оператор сопряжения $\zeta \to \zeta^{-1}$; нас интересует группа S^-. Ее порядок есть ℓ- делитель числа

$$h^- = 2m \prod_{\chi(-1)=-1} \sum_{\substack{0<a<m \\ (a,m)=1}} -\chi(a)^{-1} \frac{a}{2m}, \quad m = \ell^n,$$

то есть также числа

$$(\text{ж}) \qquad -2^{\alpha} h^- = 2m \prod_{\chi(-1)=-1} \sum_{\substack{0<a<m \\ (a,m)=1}} \chi(a)^{-1} \frac{a}{2m}$$

для некоторого α.

Сначала мы интерпретируем правую часть как некоторый индекс. Пусть $A = \mathbb{Z}_\ell[G]$; представление $\mathbb{Z}_2 = (1, \tau)$ на A разлагается в сумму

$$A = A\frac{1+\tau}{2} \oplus A\frac{1-\tau}{2} = A^+ \oplus A^-$$

Как обычно, характеры по линейности распространяются на A. Пусть для $\alpha \in A$ $\mathcal{L}_\alpha$ - умножение по α; тогда $\mathcal{L}_\alpha = \mathcal{L}_\alpha|_{A^+} \oplus \mathcal{L}_\alpha|_{A^-}$.

$$\prod_{\chi(-1)=-1} \chi(\alpha) = \mathrm{Det}\, \mathcal{L}_\alpha|_A = \mathrm{Det}\, \mathcal{L}_\alpha^-$$

Положим теперь

$$\omega = \sum_{\substack{0<a<m \\ (a,m)=1}} a\, \sigma(a)^{-1}, \qquad \zeta^{\sigma(a)} = \zeta^a$$

Тогда $\chi(a) = \chi(\sigma(a))$ (по определению), и в формуле (ж) под знаком $\prod$ стоит $\chi(\frac{\omega}{m})$. Если бы ω делилось на m мы могли бы интерпретировать формулу для h^- как желаемый индекс.

Стало быть, нам нужно исследовать делимость на m. Рассмотрим идеал

$$\mathcal{J} = A\frac{\omega}{m} \cap A$$

Теорема. $\mathcal{J}$ - главный идеал; кроме того, имеем:

$$\mathrm{Det}\, \mathcal{L}_\alpha^- = m \prod_{\chi(-1)=-1} \sum \frac{a\chi(a)^{-1}}{m} = |A^-/\mathcal{J}^-|$$

Доказательство будет дано ниже, после этого мы обнаружим, что больше того, ℓ-компонента S^-, как G-модуль, изоморфна $A^-/\mathcal{J}^-$.

Прежде всего проверим, что ω, $\frac{\sigma(a)-a}{m}\omega$ порождают

J, когда $a \in \mathbb{Z}$. Достаточно рассмотреть значения $(a,m)=1$ $0<a<m$. На самом деле даже

(жжк) $$J = \mathbb{Z}_\ell \omega \oplus \mathbb{Z}_\ell \frac{\sigma(a)-a}{m}\omega$$
$$1<a<m,\quad (a,m)=1$$

Начнем с ситуации $\bmod m$: докажем, что $\forall \eta \in A$

$$\eta\omega \equiv 0\,(m) \iff \eta \equiv \sum c_a(\sigma(a)-a) \bmod m$$
$$c_a \in \mathbb{Z}_\ell$$

Действительно, отображение

$$\sigma(a) \to a \bmod m$$

есть изоморфизм $G \to (\mathbb{Z}/m\mathbb{Z})^*$, так что элементы $a^{-1}\sigma(a)=\bar\sigma(a)$ образуют группу в кольце $\mathbb{Z}/m\mathbb{Z}[G]$, и

$$\omega \equiv \sum \bar\sigma(a) \bmod m$$

Но аннулятор суммы элементов этой группы в кольце $\mathbb{Z}/m\mathbb{Z}[G]$ порожден разностями $\bar\sigma(a)-1$; это доказывает требуемое по модулю m.

Пусть теперь $\xi \in J$; тогда $\xi = \eta\frac{\omega}{m}$, т.е. $\omega\eta$ делится на m. Поэтому

$$\eta = \sum c_a(\sigma(a)-a) + m\eta'$$

Но

$$\eta' = \sum d_a(\sigma(a)-a) + \sum d_a a$$

для некоторых $d_a \in \mathbb{Z}_\ell$

Тогда $\eta'\omega$ делится на m, а коэффициент $\sum d_a a$ даст в выражении для ξ_n кратность ω. Отсюда легко следует (жжк).

Теперь рассмотрим стандартное разложение

$$G = H \times G_0,\quad |H| = \ell-1,\quad |G_0| = \ell^{n-1}$$

Тогда

$$A = \mathbb{Z}_\ell[H] \times \mathbb{Z}_\ell[G_0].$$

Пусть φ - характеры H,

$$\varepsilon_\varphi = \frac{1}{\ell-1}\sum \varphi(h)h^{-1} \in \mathbb{Z}_\ell[H],$$
$$h\varepsilon_\varphi = \varphi(h)\varepsilon_\varphi,$$
$$\mathbb{Z}_\ell[H] = \oplus \mathbb{Z}_\ell \varepsilon_\varphi,$$

наконец,

$$A = \oplus \varepsilon_\varphi \mathbb{Z}_\ell[G_0]$$

Очевидно, $\tau \in H$, так что разделение χ на четные и нечетные отражается уже в $\mathrm{Char}\, H$: $\chi = \varphi \cdot \chi_0$, $\chi_0 \in \mathrm{Char}\, G_0$, $\varphi \in \mathrm{Char}\, H$ и $\varphi(\tau) = \chi(\tau)$

В частности,

$$\omega = \sum \omega \varepsilon_\varphi, \quad \omega \varepsilon_\varphi \in \mathcal{J}\varepsilon_\varphi$$

Распространим $\sigma: \mathbb{Z} \to G$ на $\sigma: \mathbb{Z}_\ell \to G$ и ограничим σ на корни из единицы степени $\ell-1$, содержащиеся в $\mathbb{Z}_\ell$. Это даст нам характер $\varphi_0 \in \mathrm{Char}\, H$. Структура $\varepsilon_\varphi \in \mathcal{J}$ разная при $\varphi \neq \varphi_0$ и $\varphi = \varphi_0$ соответственно.

Случай $\varphi = \varphi_0$.

Утверждение.

$$\mathcal{J}\varepsilon_\varphi = A\varepsilon_\varphi \frac{\omega}{m}$$

Действительно, пусть $c^{\ell-1} = 1$; тогда

$$\frac{(\sigma(c) - c)\omega}{m} \in A$$

Имеем, ввиду того, что $\sigma(c)\varepsilon_\varphi = \varphi(\sigma(c))\,\varepsilon_\varphi$ при $c \in H$:

$$\frac{(\sigma(c) - c)\omega\varepsilon_\varphi}{m} = \frac{(\varphi(\sigma(c)) - c)\omega\varepsilon_\varphi}{m};$$

но $c = \varphi_0(c)$, так что если $\varphi \neq \varphi_0$, то элемент $\varphi(\sigma(c)) - \varphi_0(\sigma(c))$ обратим, и мы получаем требуемое.

Случай $\varphi = \varphi_0$.

Утверждение.

$$\mathcal{J}\varepsilon_{\varphi_0} = A\frac{(\sigma(1+\ell) - 1 - \ell)\omega}{m}\varepsilon_{\varphi_0}$$

Пусть $c = uv$, $u^{\ell-1} = 1$, $v \equiv 1 \bmod \ell$. Тогда $\sigma(c) = \sigma(u)\sigma(v)$; $\sigma(c)\varepsilon_\varphi = \sigma(u)\sigma(v)\varepsilon_{\varphi_0} = u\,\sigma(v)\varepsilon_{\varphi_0}$, так что

$$\frac{(\sigma(c) - c)\omega}{m}\varepsilon_{\varphi_0} = \frac{u(\sigma(v) - v)\omega}{m}\varepsilon_{\varphi_0}$$

u обратим, поэтому достаточно ограничиться рассмотрением $v \equiv 1 \bmod \ell$. Такие v образуют циклическую группу, порожденную $1+\ell$. Элемент

$$\frac{(\sigma(1+\ell) - 1 - \ell)\omega}{m}\varepsilon_{\varphi_0}$$

принадлежит $\mathcal{J}\varepsilon_{\varphi_0}$. Для доказательства, что он его и порождает, нужно представить всякое v в виде $(1+\ell)^x$ и проделать простые преобразования.

Из доказанного уже следует, что $\mathcal{J}$ - главный идеал:

$$\mathcal{J} = A\left(\sum_{\varphi \neq \varphi_0} \frac{\omega}{m}\varepsilon_{\varphi_0} + \frac{(\sigma(1+\ell) - 1 - \ell)\omega}{m}\varepsilon_{\varphi_0}\right) \overset{\text{def}}{=} A \cdot \alpha$$

Установим теперь, что $Det\ \mathcal{L}_\chi^-$ и есть ℓ-компонента h^-. Прежде всего

$$A^-:\mathcal{J}^- = \prod_{\varphi(\tau)=-1} (A\varepsilon_\varphi : \mathcal{J}\varepsilon_\varphi)$$

При $\varphi=\varphi_0$ имеем:

$$(A\varepsilon_\varphi : \mathcal{J}\varepsilon_\varphi) = (A\varepsilon_\varphi : A\tfrac{\omega}{m}\varepsilon_\varphi) = Det\ \tfrac{\omega}{m}\Big|_{A\varepsilon_\varphi}$$

Но $A\varepsilon_\varphi = \sum \mathbb{Z}\xi_\chi$, где $\chi \in Char\ G$ пробегает характеры с H-компонентой φ. В этом базисе умножение на $\frac{\omega}{m}$ диагонально, т.е.

$$(A\varepsilon_\varphi : \mathcal{J}\varepsilon_\varphi) = \prod_{\chi\to\varphi} \chi(\tfrac{\omega}{m}), \quad \varphi\neq\varphi_0 .$$

Вычислим теперь $(A\varepsilon_{\varphi_0} : \mathcal{J}\varepsilon_{\varphi_0})$. Умножение на $\frac{(6(1+\ell)-1-\ell)\omega}{m}$ в $A\varepsilon_{\varphi_0}$ разобьем на умножение на $6(1+\ell)-1-\ell$ и $\frac{\omega}{m}$ в отдельности. Определитель умножения на $\frac{\omega}{m}$ снова равен $\prod_{\chi\to\varphi_0}\chi(\frac{\omega}{m})$. Вычислим последний оставшийся множитель Так как $A\varepsilon_{\varphi_0} = \mathbb{Z}_\ell[G_0]\varepsilon_{\varphi_0}$, считать можно внутри кольца $\mathbb{Z}_\ell[G_0]$. В старых обозначениях $6(1+\ell)=\gamma$, $\gamma^{\ell^{n-1}}=1$; полагая $\gamma-1=X$, имеем:

$$\mathbb{Z}_\ell[G_0] = \mathbb{Z}_\ell[X]\Big/\left((X+1)^{\ell^{n-1}}-1\right)$$

В последнем кольце нужно вычислить индекс главного идеала, порожденного $X-\ell$, т.е. подсчитать порядок конечного кольца

$$\mathbb{Z}_\ell[X]\Big/\left((X+1)^{\ell^{n-1}}-1,\ X-\ell\right)$$

Он, очевидно, равен ℓ-делителю числа

$$(\ell+1)^{\ell^{n-1}}-1$$

Индукция по n показывает, что это есть ℓ^n, т.е. m. Тем самым, теорема доказана:

$$|S^-| = |A^-/\mathcal{J}^-|,$$

где

$$\mathcal{J}^- = A^- \cap A^- \tfrac{\omega}{m}$$
$$A^- = \{x \mid \tau x = -x\}$$

§ 9. Теорема Куммера.

Первые результаты об операторной структуре группы классов дивизоров кругового поля были получены очень давно.

Теорема (Куммер)

$$\mathbb{Z}[G] \cap \mathbb{Z}[G]\tfrac{\omega}{m} \subset Ann\ Cl\ K$$

Следствие. $\mathcal{J}^- \subset Ann\ S^-$

(После этого нам останется доказать лишь, что S^- имеет одну образующую как A^--модуль, и мы получим фундаментальный изоморфизм

$$S^- \approx A^-/\gamma - \quad !\ )$$

Доказательство теоремы Куммера. Согласно двойственности Куммера,

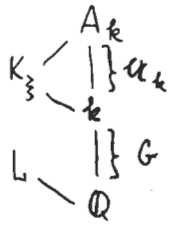
$$k^*/(k^*)^m \approx \mathrm{Hom}\,(\mathcal{U}_k, \mu_m)$$

где μ_m - корни степени m из I - принадлежат k, $\mathcal{U}_k$ - группа Галуа максимального абелева расширения k:

$$(\alpha k^*, s) \longrightarrow (\sqrt[m]{\alpha})^{1-s}$$

Если G действует на k, то изоморфизм Куммера является операторным. (Действие на $k^*/(k^*)^m$ очевидно, на μ_m тоже, а действие на $\mathcal{U}_k$ описывается через рассмотрение обычного расширения $1 \to \mathcal{U}_k \to \mathcal{U} \to G \to 1$, где $\mathcal{U} = \mathrm{Gal}(A_k/k^G)$

Каждый элемент $\xi \in \mathrm{Hom}\,(\mathcal{U}_k, \mu_m)$ определяет абелево расширение K_ξ, соответственно подгруппе $\ker \xi$. Выясним, для каких ξ имеем $K_\xi = Lk$, где L - абелево расширение $\mathbb{Q}$.



Пусть $\alpha \to \xi$, $\alpha \in k^*/(k^*)^m$
Тогда $\alpha^g \to \xi^g$. Имеем для $s \in \mathcal{U}_k$

$$\xi^g(s) = \xi(sg)^g$$

Если $K_\xi = kL$, то, очевидно, G действует тривиально

но

$$\xi(s^g) = \xi(s)$$

Значит, в этом случае

$$\xi^g(s) = \xi(s)^g$$

Но $\xi(s) \in \mu_m$; пусть g действует как возведение в степень $a(g)$, так что

$$\xi^g(s) = \xi(s)^{a(g)}$$

Значит

$$\alpha^g \to \xi^{a(g)}$$

и

$$\alpha^{a(g)} \to \xi^{a(g)}$$

поэтому

$$\boxed{\alpha^g = \alpha^{a(g)}\, \beta_g^{\,m}}$$

Резюмируем результат: $k(\sqrt[m]{\alpha})$ над k является композитом kL, L абелево над $\mathbb{Q}$, в случае, когда α под действием $g \in G = \mathrm{Gal}(k/\mathbb{Q})$ возводится в ту же степень, что и корни из единицы, $\mathrm{mod}\,(k^*)^m$

Применим это к случаю $k = \mathbb{Q}(\zeta)$, $\zeta^m = 1$. Мы получаем возможность описать абелевы расширения k как подрас-

ширения расширений $k(\sqrt[m]{\alpha})$

Вот идея дальнейшего. Пусть $p \equiv 1 \bmod m$, p - простое, $\varepsilon^p = 1$. Пусть $L_p \subset \mathbb{Q}(\varepsilon)$ - циклическое поле степени m. Его дискриминант делится лишь на p. Согласно вышесказанному $kL_p = k(\sqrt[m]{\alpha_p})$. Мы можем отыскать разложение α_p на простые дивизоры: будет доказано, что $(\alpha_p) = \mathfrak{y}^{x_a}$, где

$$x_a = \frac{(\sigma(a)-a)\omega}{m}$$

Это и даст тождественные соотношения в группе классов, порожденной делителями $\mathfrak{y}/p$ для таких p, что $p \equiv 1 \ (m)$. Отсюда уже можно будет извлечь доказательство.

Проведем эти рассуждения подробно.

В дальнейшем мы явно предполагаем, что $S^+ = 0$; проверять это достаточно для $n = 1$, и это верно для всех $l \le 4001$. Описание S^- тогда равносильно описанию S (как G-модулей). Кроме того, мы полагаем $A = \mathbb{Z}[G]$, A^-, J^- и т.д. определяются, как выше, но с кольцом коэффициентов $\mathbb{Z}$ вместо $\mathbb{Z}_l$.

Образующие идеала $\mathfrak{J}$ остаются прежними: ω, $\frac{\sigma(a)-a}{m}\omega$. Достаточно проверить поэтому, что все эти элементы переводят любой дивизор в главный, или даже любой простой дивизор в главный. Больше того, можно ограничиться простыми дивизорами порядка I, ибо они порождают группу классов дивизоров. (Набросок доказательства: $\sum_{\mathfrak{y}} \frac{1}{N\mathfrak{y}}$ расходится, где суммирование распространено на все простые идеалы данного класса; но дивизоры порядка > 2 дают сходящийся вклад. Существует еще элементарное доказательство Гильберта).

Это снимает необходимость рассматривать $p \not\equiv 1 \bmod m$.

Вернемся теперь к введенным выше числам α_p $(k = K)$. Было доказано, что

$$\alpha_p^{\sigma(a)} = \alpha_p^a \beta_p^m$$

Так как $p \equiv 1 \bmod m$, имеем $p = \mathfrak{y}^{\sum \sigma(a)}$, $\mathfrak{y}/p$. Мы утверждаем, прежде всего, что для удачного выбора α_p $(\alpha_p) = \mathfrak{y}^{\sum c_a \sigma(a)}$, $c_a \in \mathbb{Z}$. Дискриминант KL_p/K делится лишь на $\mathfrak{y}/p$, поэтому во всяком случае

$$(\alpha_p) = \mathfrak{y}^{\sum c_a \sigma(a)} \mathfrak{a}^m$$

Учитывая, что

$$\alpha_p^{\sigma(a)-a} = \beta_p^m$$

и сравнивая разложения слева и справа, найдем

$$x(\sigma(a)-a) \equiv 0 \quad (m)$$

где

$$x = \sum c_a \sigma(a)$$

Отсюда следует, что, по доказанному выше, $x \equiv k\omega \bmod m, k \in \mathbb{Z}$. Покажем, что $(k, l) = 1$. Иначе (α_p) был бы l-й степенью, и $K(\sqrt[l]{\alpha_p})/K$ было бы неразветвлено в p. Но тогда порядок ветвления p в L_p не мог бы быть равен m: противоречие.

Значит, мы доказали, что

$$\mathfrak{y}^{\omega} \mathfrak{a}^m \sim 1$$

Дальше будет установлено, что даже $\mathfrak{y}^{\omega} \sim 1$. Сейчас мы этим воспользуемся. Соотношения, относящиеся к элементам

$\frac{\sigma(a)-a}{m}\omega$ получатся при рассмотрении разложения β_p. Имеем

$$\alpha_p^{\sigma(a)-a} = \beta_p^m$$

откуда

$$\varepsilon^{\omega(\sigma(a)-a)} = (\beta_p^m) \Rightarrow$$

$$\Rightarrow \left(\varepsilon^{\frac{\omega(\sigma(a)-a)}{m}}\right)^m = (\beta_p)^m \Rightarrow$$

$$\Rightarrow \varepsilon^{\frac{\omega(\sigma(a)-a)}{m}} = \beta_p$$

Теперь покажем возможность выбора α_p с условием $(\alpha_p) = \mathfrak{p}^\omega$. Положим

$$\tau(\xi) = \sum_{0<c<p} \xi(c)\varepsilon^c, \quad \xi \in Char(\mathbb{Z}/p\mathbb{Z})^*$$

Очевидно, $\tau(\xi) \in K L_p$

Пусть ξ тождествен на подгруппе $Gal(\mathbb{Q}(\varepsilon)/L_p)$ Это равносильно тому, что $\xi^m = 1$. Действуя на $\tau(\xi)$ автоморфизмами из $Gal(\mathbb{Q}(\varepsilon)/L_p)$, без труда получим:

(*) $\tau^s = \xi(\kappa)^{-1}\tau$, где $\varepsilon^s = \varepsilon^\kappa$

Поэтому

$$\tau(\xi)^m \in K$$

Положим $\alpha_p = \tau(\xi)^m$ (то, что $KL_p = K(\tau(\xi))$, очевидно из рассмотрения (*)).

Поскольку $|\tau(\xi)| = \sqrt{p}$ и τ - целое, в разложение $\alpha_p = \tau(\xi)^m$ входят лишь делители $\mathfrak{p}$:

$$(\alpha_p) = \mathfrak{p}^x, \quad x \equiv \omega \mod m$$

Но $\omega = \sum a\sigma(a)^{-1}$, так что если $x = \sum c_a \sigma(a)^{-1}$, $c_a \geqslant 0$ то $c_a = a + m\cdot b_a$, где $b_a \geqslant 0$. Сравнивая нормы α_p и $\mathfrak{p}^x$ убедимся, что $b_a = 0$

Действительно, с одной стороны, $|\alpha_p| = p^{\frac{m}{2}}$, так что

$$N(\alpha_p) = p^{\frac{m}{2}\varphi(m)}$$

С другой стороны,

$$N\left(\mathfrak{p}^{\sum c_a \sigma(a)}\right) = p^{\sum c_a} = p^{\sum a + m\sum b_a}$$

Но

$$\sum_{\substack{0<a<m \\ (a,l)=1}} a = \sum_{0<b<l^n} b - l\sum_{0<b<l^{n-1}} b = \frac{m}{2}\varphi(m)$$

Теорема Куммера доказана.

§ I0. Структура группы S^- как операторной группы

Мы возвращаемся к обозначениям $A=\mathbb{Z}_\ell[G]$ и т.п. (ℓ-адические коэффициенты). Для доказательства G-изоморфизма $S^-\approx A^-/\gamma^-$, как уже было сказано, достаточно проверить.

Предложение. A-модуль S^- имеет одну образующую. (Отметим, что при $S^+=0$ имеем $A^+\gamma^-=0$, так что цикличность S^- как A-модуля или A^--модуля равносильны).

Доказательство. Вместо S достаточно рассматривать $S/\ell S$ - простой вариант леммы Накаяма.

Группа $S/\ell S$ является группой Галуа максимального абелева неразветвленного расширения $M_\ell \supset K$ периода ℓ. Для всякого характера $\chi \in Char(S/\ell S)$ рассмотрим $\alpha_\chi \in K^*$, соответствующий χ по Куммеру. Прежде всего,

$$(\alpha_\chi) = \mathfrak{a}^\ell$$

Отметим, что $\chi: S/\ell S \to \mu_\ell \subset K^*$; благодаря этому обе группы являются G-модулями.

Равенство $S=S^-$ означает тогда, что $s^{1+\tau}=0$ для всех s. Но $s^\tau = s \Rightarrow \chi^\tau(s)=(\chi(s^{-1}))^\tau = \chi(s)^{-\tau} = \chi(s)$. Поэтому

$$Char\, S/\ell S = (Char\, S/\ell S)^+$$

так что

$$\alpha_\chi^\tau = \alpha_\chi \beta_\chi^\ell \Rightarrow \alpha_\chi^{\tau-1} = \beta_\chi^\ell$$

Отсюда

$$\beta_\chi^\ell = (\mathfrak{a}^{(\tau-1)})^\ell \Rightarrow \beta_\chi = \mathfrak{a}^{\tau-1} \Rightarrow \mathfrak{a} \in S^+ = 0$$

Значит, $(\mathfrak{a})=\gamma$, так что

$$(\alpha_\chi) = (\gamma^\ell)$$

а так как α_χ определен с точностью до ℓ-степеней, можно считать, что α_χ - единицы:

$$Char\, S/\ell S = \{\alpha_\chi\}(K^*)^\ell/(K^*)^\ell \subset E(K^*)^\ell/(K^*)^\ell = E/E^\ell$$

Но $|E/E_0|$, где E_0 - подгруппа круговых единиц, имеет тривиальный ℓ-порядок, ибо он совпадает с порядком S^+. Поэтому

$$E/E^\ell \approx E_0/E_0^\ell$$

(как G-группы). Группа E_0 порождена $\frac{1-\zeta}{1-\zeta^a}$, так что E_0 является подмодулем свободного A-модуля F ранга I: $F=\mathbb{Z}/\ell\mathbb{Z}[G]$; следовательно, $S/\ell S$ является гомоморфным образом группы $Char\, \mathbb{Z}/\ell\mathbb{Z}[G]$, которая канонически изоморфна $\mathbb{Z}/\ell\mathbb{Z}[G]$ в силу существования стандартного скалярного произведения.

Предложение доказано.

§ II. Структура модуля Тэйта

Теперь мы можем приступить к вычислению структуры модуля Тэйта

$$T_\ell(\mathbb{Q}) = \lim S_n, \quad S_n = Cl(K_n)^{(\ell)}$$

Хотя группа S_n и вычислена, осуществление предельного перехода оказывается нетривиальной задачей.

Напомним результаты предыдущей лекции: полагая

$$G_n = Gal(K_n/\mathbb{Q}), \quad A_n = \mathbb{Z}_\ell[G_n]$$

(A) $$\omega_n = \sum a\,\sigma_n(a)^{-1}, \quad \mathfrak{J}_n = A_n \cap A_n\frac{\omega}{\ell^n}$$

мы установили, что

$$S^- = \mathbb{Z}_\ell[G]^-/\mathfrak{J}^-$$

Нас интересует структура $\varprojlim S_n$ над $\mathbb{Z}_\ell[\Gamma]$, где $\Gamma = Gal(K/K_1)$, $K = \bigcup K_n$. Имеем $\mathbb{Z}_\ell[\Gamma] \simeq \mathbb{Z}_\ell[[x]] = \mathcal{O}$ и с точностью до введенного отношения эквивалентности $T_\ell(\mathbb{Q}) \sim \oplus \mathcal{O}/(t)$, где $t \in \mathcal{O}$ - некоторые элементы. Их мы и хотим вычислить.

Выше было получено разложение

$$A_n = \oplus A_n\varepsilon_\varphi$$

$$A_n\varepsilon_\varphi = \mathbb{Z}_\ell[\Gamma]\varepsilon_\varphi$$

где ε_φ - идемпотенты, связанные с характерами φ группы H в разложении $G_n = H \times \Gamma_{n-1}$. Аналогично

$$S_n = \bigoplus_{\varphi(-1)=-1} S_{n,\varphi}$$

$$S_{n,\varphi} = A_n\varepsilon_\varphi/\mathfrak{J}_n\varepsilon_\varphi$$

Поэтому достаточно проводить предельный переход при фиксированном φ. Пусть

$$A_n\varepsilon_\varphi/\mathfrak{J}_n\varepsilon_\varphi = \mathbb{Z}_\ell[\Gamma_{n-1}]/\mathfrak{a}_{n,\varphi}$$

вычислим идеал $\mathfrak{a}_{n,\varphi}$. Идеал $\mathfrak{J}_n\varepsilon_\varphi$ главный: он порожден $\frac{\omega_n}{\ell^n}\varepsilon_\varphi$ при $\varphi \neq \varphi_0$ и $\frac{(\sigma_n(1+\ell) - (1+\ell))\omega_n}{\ell^n}\varepsilon_{\varphi_0}$ при $\varphi = \varphi_0$.

Гомоморфизм ограничения $\mathbb{Z}_\ell[G_{n+1}] \to \mathbb{Z}_\ell[G_n]$ переводит элемент ω_{n+1} в элемент следующего вида:

$$\omega_{n+1} = \sum_{\substack{1<a<\ell^{n+1}\\ \ell\nmid a}} a\,\sigma_{n+1}(a)^{-1} \longrightarrow \sum_{\substack{1<a'<\ell^n\\ 0<b<\ell}} (a' + \ell^n b)\,\sigma_n(a' + \ell^n b) =$$

$$= \sum_{a'}\sum_{b} (a' + \ell^n b)\,\sigma_n(a')^{-1} =$$

$$= \ell\omega_n + \ell^n \sum_b b \sum_{a'} \sigma_n(a')^{-1} = \ell\omega_n + \frac{\ell^{n+1}(\ell-1)}{2}\sum_{a'}\sigma_n(a') =$$

$$= \ell\omega_n + \ell^{n+1}\frac{\ell-1}{2}s_n$$

где $S_n = \sum \sigma_n(a')$, Поэтому

$$\frac{\omega_{n+1}}{\ell^{n+1}} \longrightarrow \frac{\omega_n}{\ell^n} + \frac{\ell-1}{2} S_n$$

Но $S_n \varepsilon_\varphi = 0$, если $\varphi \neq 1$, ибо $S_n = \left(\sum_{h \in H}\right)\left(\sum_{\gamma \in \Gamma_{n-1}} \gamma\right)$ и

$$S_n \varepsilon_\varphi = (\Sigma\gamma)(\Sigma h \varepsilon_\varphi) = (\Sigma\gamma)(\Sigma \varphi(h)\varepsilon_\varphi) = 0$$

Учитывая, что интересующие нас характеры φ все нечетные, получаем

$$\frac{\omega_{n+1}}{\ell^{n+1}} \varepsilon_\varphi \longrightarrow \frac{\omega_n}{\ell^n} \varepsilon_\varphi$$

Положим

$$(B) \qquad g_{n,\varphi} = \begin{cases} \dfrac{\omega_n}{\ell^n} \varepsilon_\varphi & \text{при } \varphi \neq \varphi_0 \\ \dfrac{\omega_n}{\ell^n} (\sigma_n(1+\ell) - (1+\ell)) \varepsilon_\varphi & \text{при } \varphi = \varphi_0 \end{cases}$$

Мы знаем, что

$$S_n = \bigoplus_{\varphi(-1)=-1} A_n / g_{n,\varphi}$$

и что при гомоморфизмах ограничения $g_{n+1,\varphi} \to g_{n,\varphi}$. Поэто-

му

$$(C) \qquad T_\ell(\mathbb{Q}) = \varprojlim S_n = \bigoplus_{\varphi(-1)=-1} \mathcal{O} / g_\varphi$$

где $g_\varphi = \varprojlim_n g_{n,\varphi} \in \varprojlim A_n = \mathcal{O}$

Формулы (C), (B) и (A) дают одну из возможных форм описания модуля Тэйта $T_\ell(\mathbb{Q})$. Это описание, однако, зависит от элементов $g_\varphi \in \mathcal{O}$, которые мы дальше представим в более явном виде.

§ I2. Вычисление функций g_φ .

Так как $\mathcal{O} \simeq \mathbb{Z}_\ell[[\Gamma]]$, то g_φ с уть степенные ряды с коэффициентами в $\mathbb{Z}_\ell$. Поэтому они сходятся при всех $x \in \ell\mathbb{Z}_\ell$ и мы сейчас опишем их явные формулы как функции на этом множестве.

Для этого заметим, что при $s \in \mathbb{Z}$ выражение $(1+\ell)^s$ имеет смысл и дает все числа $\equiv 1 \bmod \ell$ в $\mathbb{Z}_\ell$. "Придать x значение $\equiv 0 \bmod \ell^n$ - значит рассмотреть гомоморфизм колец

$$\mathcal{O} = \mathbb{Z}_\ell[\Gamma] \simeq \mathbb{Z}_\ell[[x]] \to \mathbb{Z}_\ell$$

при котором $\gamma = 1+x \xrightarrow{\Psi} (1+\ell)^s$: этот гомоморфизм, следовательно, индуцирован ℓ -адическим характером группы Γ . К сожалению, этот гомоморфизм нельзя непосредственно ограничить на факторкольцо $\mathbb{Z}_\ell[\Gamma_{n-1}]$; однако, это можно сделать „ $\bmod \ell^{n-1}$ “ , потому что

$$(1+\ell)^{s\ell^{n-1}} \equiv \ell \bmod \ell^{n-1}$$

Это приводит к рассмотрению коммутативной диаграммы

$$\begin{array}{ccc} \mathcal{O} = \mathbb{Z}_\ell[\Gamma] & \xrightarrow{\Psi} & \mathbb{Z}_\ell \\ \downarrow & & \downarrow \\ \mathbb{Z}_\ell[\Gamma_{n-1}] & \xrightarrow{\Psi_n} & \mathbb{Z}_\ell/\ell^{n-1}\mathbb{Z}_\ell \end{array}$$

из которого следует, что

$$g_\varphi\left((1+\ell)^s - 1\right) = \lim_n \Psi_n(g_{n,\varphi})$$

Как всегда, рассмотрим отдельно два случая.

$$\underline{\varphi \neq \varphi_0}$$

Здесь

$$\frac{\omega_n}{\ell^n}\varepsilon_\varphi = \frac{\sum a\sigma(a)^{-1}}{\ell^n}\varepsilon_\varphi$$

Пусть $a = \varphi_0(a)\langle a\rangle$, где $\varphi_0(a)^{\ell-1} = 1$, $\langle a\rangle \equiv 1 \bmod \ell$ (Здесь $\varphi_0(a) = \lim_{n\to\infty} a^{\ell^n}$: это дает явное разложение $G = H \times \Gamma$). Тогда

$$\frac{\omega_n}{\ell^n}\varepsilon_\varphi = \frac{\sum \varphi_0(a)\langle a\rangle\sigma(\varphi_0(a))^{-1}\sigma(\langle a\rangle)^{-1}}{\ell^n}\varepsilon_\varphi =$$

$$= \frac{\sum \varphi_0(a)\varphi^{-1}(a)\langle a\rangle\sigma(\langle a\rangle)^{-1}}{\ell^n}\varepsilon_\varphi$$

Положим $\varphi^{-1}\varphi_0 = \varphi' \neq 1$ и заметим, что $\sigma(\langle a\rangle) \in \Gamma_{n-1}$ поэтому

$$g_{n,\varphi} = \frac{1}{\ell^n}\sum \varphi'(a)\langle a\rangle\sigma(\langle a\rangle)^{-1}$$

Кроме того, $\gamma_{n-1} = \sigma(1+\ell)$, $\psi(\gamma_{n-1}) = (1+\ell)^s$; поэтому, представляя $\langle a\rangle$ в виде $\langle a\rangle = (1+\ell)^n = \gamma_{n-1}^n$, находим

$$\Psi_n(\sigma\langle a\rangle) = \langle a\rangle^s \bmod \ell^{n-1}$$

Однако, делать подстановку непосредственно в сумму нельзя из-за знаменателя ℓ^n.

Обходной путь: положим $\langle a\rangle = (1+\ell)^{K(a)} + \ell^n a'$, где $0 \leq K(a) < \ell^{n-1}$; тогда

$$g_{n,\varphi} = \frac{1}{\ell^n}\sum \varphi'(a)\left((1+\ell)^{K(a)} + \ell^n a'\right)\sigma(\langle a\rangle)^{-1} =$$

$$= \frac{1}{\ell^n}\sum_{\substack{1\leq a<\ell^n \\ \ell\nmid a}} \varphi'(a)(1+\ell)^{K(a)}\sigma(\langle a\rangle)^{-1} + \sum \varphi'(a)a'\sigma(\langle a\rangle)^{-1}$$

Первая сумма в последней строчке нулевая: так как $\varphi'(a)$ за-

висит лишь от $a \bmod \ell$, в этой сумме $\varphi'(a)$ и $K(a)$ независимо пробегают значения $\varphi'(a \bmod \ell)$ и $K(b)$, и $\sum \varphi'(a \bmod \ell) = 0$. Следовательно,

$$g_{n,\varphi} = \sum \varphi'(a)\, a^{1} \sigma(\langle a \rangle)^{-1}$$

Поэтому,

$$\Psi_n(g_{n,\varphi}) \equiv \sum_{\substack{1 \le a < \ell^n \\ \ell \nmid a}} \varphi'(a)\, a^{1} \langle a \rangle^{-s} \pmod{\ell^n}$$

Дальше:

$$\langle a \rangle^{1-s} \equiv (1+\ell)^{K(a)(1-s)} + (1-s)(1+\ell)^{-K(a)\cdot s} \ell^n a \equiv$$

$$\equiv (1+\ell)^{K(a)(1-s)} + (1-s)\langle a \rangle^{-s} a^{1} \ell^n \pmod{\ell^{2n}}$$

так что отсюда можно выделить $a^{1}\langle a \rangle^{-s}$. Технически это удобно делать так:

$$\sum \varphi'(a)\langle a \rangle^{1-s} \equiv \sum \varphi'(a)\,(1+\ell)^{K(a)(1-s)} +$$

$$+ (1-s)\,\ell^n \sum \varphi'(a)\langle a \rangle^{-s} a^{1} \pmod{\ell^{2n}}$$

Первая сумма справа равна нулю, как и выше.
Отсюда

$$\Psi_n(g_{n,\varphi}) \equiv \frac{1}{(1-s)\,\ell^n} \sum \varphi'(a)\langle a \rangle^{1-s} \pmod{\frac{\ell^n}{1-s}}$$

Переходя к пределу по n, находим

$$\Psi(g_\varphi) = g_\varphi\left((1+\ell)^s - 1\right) =$$

$$(*) \qquad = \frac{1}{s-1} \lim_{n\to\infty} \frac{\sum_{1 \le a < \ell^n} \varphi'(a)\langle a \rangle^{1-s}}{\ell^n}$$

(считая, что $\varphi'(a) = 0$ при $a \equiv 0 \bmod \ell$).

$\varphi = \varphi_0$

Совершенно аналогичные вычисления, подробности которых мы опускаем, приводят к ответу:

$$\Psi(g_{\varphi_0}) = g_{\varphi_0}\left((1+\ell)^s - 1\right) =$$

$$(**) \qquad = \left((1+\ell)^s - (1+\ell)\right) \frac{1}{s-1} \lim_{n\to\infty} \frac{\sum \langle a \rangle^{1-s}}{\ell^n}$$

§ I3. Значения рядов g_φ в целых точках

Формулы (*) и (**) § I2 описывают функции g_φ как функции аргумента $s \in \mathbb{Z}_\ell$. Однако, как аналитические функции, они определяются ввиду теоремы единственности, своими значениями на любом бесконечном подмножестве этого множества, имеющем предельную точку.

Мы получим новую информацию об этих функциях, вычислив их значения при $s = 1-m$, $m > 0$, $m \in \mathbb{Z}$

$$a = \varphi_0(a)\langle a\rangle \quad \Rightarrow \quad a^m = \langle a\rangle^m$$

так что суммы, входящие в выражения $\psi(g_\varphi)$ приобретают вид $\sum_{1\le a<\ell} \varphi_1(a)\, a^m$, где $\varphi_1 = \varphi_0^{1-m}\varphi^{-1}$. Если $\varphi_1 \equiv 1$, такие суммы, как известно вычисляются через числа Бернулли. Леопольдт ввел обобщенные числа Бернулли, приспособленные для вычисления как род таких сумм, которые получаются при $\varphi_1 \neq 1$

Числа Бернулли определяются формулой

$$e^{Bt} = \frac{t\,e^t}{e^t-1} = 1 + \sum_{n=1}^{\infty} \frac{B^n}{n!}\, t^n$$

формально

Числа Бернулли-Леопольдта определяются аналогичным разложением

$$e^{B_\varphi t} = \frac{t \sum_{a=1}^{\ell-1} \varphi(a)\, e^{at}}{e^{\ell t}-1}$$

где φ - характер $\bmod \ell$

Для вычисления чисел Бернулли удобны рекуррентные соотно-

шения (символические)

$$(B+1)^n - B^n = n \quad , \quad n \geqslant 2$$

(доказательство:

$$e^{(B+1)t} - e^{Bt} = \sum \left(\frac{(B+1)^n t^n}{n!} - \frac{B^n t^n}{n!} \right) =$$

$$= e^{Bt}(e^t - 1) = t\,e^t = \sum \frac{t^n}{(n-1)!}$$

Соответствующий результат для чисел Бернулли-Леопольдта

$$(B_\varphi + \ell)^n - B_\varphi^n = n \sum_{a=1}^{\ell-1} \varphi(a)\, a^{n-1}$$

Нужная нам формула суммирования для чисел Бернулли есть обобщение рекуррентного соотношения:

$$(B+K)^n - B^n = n \sum_{a=1}^{K} a^{n-1}$$

(Доказательство:

$$e^{(B+K)t} - e^{Bt} = e^{Bt}(e^{Kt} - 1) =$$

$$= t\,e^t \sum_{a=0}^{K-1} e^{at} = t \sum_{a=1}^{K} e^{at}$$

Сравнивая коэффициенты при t^n слева и справа, находим требуемое).

Наконец, формула суммирования с характерами:

$$(B_\varphi + k\ell)^n - B_\varphi^n = n \sum_{a=1}^{k\ell} \varphi(a)\, a^{n-1}$$

(Доказательство:

$$e^{(B_\varphi + k\ell)t} - e^{B_\varphi t} = e^{B_\varphi t}(e^{k\ell t} - 1) =$$

$$= t \sum_{a=1}^{\ell-1} \varphi(a) e^{at} \sum_{b=0}^{k-1} e^{b\ell t} = t \sum_{b=0}^{k\ell} \varphi(b) e^{bt}$$

и снова сравнение коэффициентов).

Пользуясь этими формулами суммирования, представим интересующие нас суммы в виде

$$\frac{1}{m+1} \frac{(B_{\varphi_1} + \ell^h)^{m+1} - B_{\varphi_1}^{m+1}}{\ell^h}$$

В числителе стоит многочлен от ℓ^h с нулевым свободным членом, и в пределе при $h \to \infty$ останется лишь коэффициент при

первой степени ℓ^h, который равен $(m+1) B_{\varphi_1}^m$. Следовательно,

$$(*) \quad g_\varphi\left((1+\ell)^{1-m} - 1\right) = \begin{cases} -\dfrac{B_{\varphi_1}^m}{m} & \text{при } \varphi \neq \varphi_0 \\ -\left((1+\ell)^{1-m} - (1+\ell)\right) \dfrac{B_{\varphi_0}^m}{m}, & \varphi = \varphi_0 \end{cases}$$

Еще до работ Ивасавы эти числа появлялись в совсем другой задаче. Именно, для поля $K_1 = \mathbb{Q}(\zeta)$ значения $L(1-m, \varphi)$ были вычислены Леопольдтом; они оказались такими же, что и значения g_φ. Следовательно, функция g_φ осуществляет ℓ-адическое аналитическое продолжение L-функции!

§ 14. Некоторые следствия

Прежде, чем перейти к доказательству основного (и последнего) результата этого курса – совпадению функций g_φ с ℓ-адическим продолжением L-рядов, покажем, что полученные нами представления для g_φ уже приводят к некоторым интересным выводам.

Вспомнив, что g_φ является образующей группы характеров группы H, положим $\varphi = \varphi_0^k$, $0 \leq k \leq \ell-1$. Последняя формула предшествующего параграфа дает:

$$g_{\varphi_0^k}\left((1+\ell)^{1-m} - 1\right) = \frac{B_{\varphi_0}^m}{m}$$

$$\left(\varphi \neq \varphi_0 \iff k \not\equiv 1 \mod (\ell-1)\right)$$

$$g_{\varphi_0}\left((1+\ell)^{1-m}-1\right)=-\left((1+\ell)^{1-m}-(1+\ell)\right)\frac{B_{\varphi_0^{-m}}^{m}}{m}$$

Рассмотрим только значения $m\equiv 1-\kappa \mod(\ell-1)$. Тогда $\varphi_0^{1-\kappa-m}=1$ и мы получаем обычные Бернуллиевы числа. Наши формулы дают при $s=1-m\equiv\kappa \mod(\ell-1)$

$$g_{\varphi_0^{\kappa}}\left((1+\ell)^{s}-1\right)=\frac{B^m}{m}$$

$$\kappa\not\equiv 1 \mod(\ell-1)$$

(ж)

$$g_{\varphi_0}\left((1+\ell)^{s}-1\right)=-\left((1+\ell)^{s}-(1+\ell)\right)\frac{B^m}{m}$$

Таким образом мы имеем $\ell-1$ степенной ряд $g_\kappa\in\mathbb{Z}_\ell[[x]]$ $g_\kappa=g_{\varphi_0^{\kappa}}$, причем нам известны значения $g_\kappa(u_m^{(\kappa)})$, $u_m^{(\kappa)}=(1+\ell)^{s}-1$ $m\equiv 1-\kappa \mod\ell$. Они задаются формулами (**).

Уже наличие степенных рядов с коэффициентами в $\mathbb{Z}_\ell$ приводит к некоторым арифметическим следствиям. Например, мы покажем, что при $\ell-1\nmid m$ имеет место сравнения Куммера:

$$\frac{B^m}{m}\equiv\frac{B^{m+\ell-1}}{m+\ell-1}\pmod{\ell-1}$$

Для доказательства достаточно представить g_κ в виде $g_\kappa=a_0+G_\kappa$, где $G_\kappa\in(\ell,x)$ - максимальному идеалу кольца формальных степенных рядов.

Поскольку $G_\kappa(u_m)\equiv 0(\ell)$, то $g_\kappa(u_m)$ зависит по

$\mod(\ell-1)$ лишь от a_0. А так как m изменяется по $\mod(\ell-1)$ по тривиальной арифметической прогрессии, то утверждение легко следует.

На стр. 131 мы получили разложение

$$S_n=\bigoplus_{\varphi(-1)=-1}A_n/(g_{n,\varphi}),\quad A_n=\mathbb{Z}_\ell[\Gamma_{n-1}]$$

благодаря которому столь просто полученный сейчас результат обнаружит глубокий смысл.

Нетрудно понять, что g_κ является единицей в кольце тогда и только тогда, когда $\frac{B^m}{m}\not\equiv 0(\ell)$. (Поскольку это эквивалентно тому, что $a_0\not\equiv 0(\ell)$).

Если, однако, $g_\kappa\in\mathcal{O}^*$ ($\mathcal{O}^*$ - мультипликативная группа кольца $\mathcal{O}$), то и проекция $g_{n,\varphi}$ этого ряда в $\mathbb{Z}_\ell[\Gamma_{n-1}]$ также обратима и, следовательно, при условии $\ell\nmid\frac{B^m}{m}$ соответствующая компонента в представлении $S_n=\bigoplus A_n/(g_{n,\varphi})$ пропадает.

(Кстати, $\frac{B^m}{m}$ делится или не делится на ℓ одновременно с B^m, что будем учитывать в дальнейшем). В частности, $S_n=0$ (это равенство верно для всех n, если верно хоть для одного) тогда и только тогда, когда $g_\kappa\in\mathcal{O}^*$ для всех $0\le\kappa<\ell-1$. Это в свою очередь, означает, что $B^\kappa\not\equiv 0(\ell)$ для $0\le\kappa<\ell-1$. Мы получим критерий Куммера регулярности простого числа

Совершенно аналогичное рассуждение показывает, что ℓ-компонента группы классов дивизоров поля $K_1=\mathbb{Q}(\zeta)$, $\zeta^\ell=1$ имеет столько образующих, каково число значений κ, $0\le\kappa<\ell-1$ для которых $B^\kappa\equiv 0 \mod(\ell)$

§ I5. ℓ-адическое продолжение L-рядов

Теорема. Рассмотрим в K_1 L-ряды $L(s,\varphi)$, где φ характеры $\mod\ell$. Тогда для четных φ, т.е. φ типа $\varphi(-1)=1$ имеет место равенство (при $\ell-1\nmid m$)

$$L(1-m,\varphi) = -\frac{B_\varphi^m}{m}$$

Доказательство. Нам предстоит вычислить значения L-ряда

$$\sum \frac{\varphi(n)}{n^s}$$

для чего удобно привлечь некоторые аналитические соображения.

Как известно, Γ-функция $\Gamma(s)$ определяется по формуле

$$\Gamma(s) = n^s \int_0^\infty e^{-nt}\, t^s\, \frac{dt}{t}$$

где на s накладывается условие: $\operatorname{Re} s > 1$

Отсюда следует, что

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty e^{-nt}\, t^s\, \frac{dt}{t}$$

После этого легко получается, что

$$\sum \frac{\varphi(n)}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty \sum e^{-nt}\, \varphi(n)\, t^s\, \frac{dt}{t}$$

Представим n в виде $n = a + b\ell$, где $0 \le a < \ell$ и b пробегает все значения. Тогда сумма $\sum \varphi(n) e^{-nt}$ преобразуется следующим образом:

$$\sum_n \varphi(n) e^{-nt} = \sum_{a,b} \varphi(a)\, e^{-at} e^{-b\ell t} =$$

$$= \Big(\sum_{1\le a<\ell} \varphi(a) e^{-at}\Big)\Big(\sum_b e^{-b\ell t}\Big) =$$

$$= \frac{\sum_{1\le a<\ell} \varphi(a) e^{-at}}{1 - e^{-\ell t}} = G_\varphi(t)$$

Отсюда получается следующее представление рассматриваемого L-ряда:

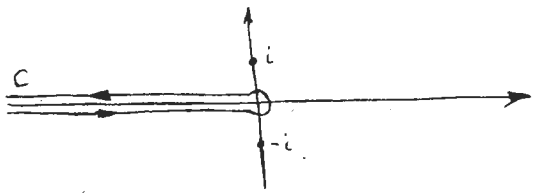
$$L(s,\varphi) = \frac{1}{\Gamma(s)} \int_0^\infty G_\varphi(t)\, t^s\, \frac{dt}{t}$$

К этому интегралу можно применить обычный метод вычисления интегралов при помощи вычетов.

Рассмотрим следующий интеграл:

$$J(s) = \frac{1}{2\pi i} \int_C \frac{\sum \varphi(a) e^{-az}}{1 - e^{\ell z}}\, z^s\, \frac{dz}{z}$$

где z^s - та ветвь степенной комплекснозначной функции, которая имеет вид $e^{s \log z}$, а у $\log z$ берется, в свою очередь та ветвь, которая на вещественной оси принимает вещественные значения обычного натурального логарифма, и где C - следующий контур



Мы опускаем проверку того, что на самом деле имеет место равенство

$$L(s,\varphi) = \Gamma(1-s)\frac{1}{2\pi i}\int_C \frac{\sum \varphi(a) e^{az} z^s}{e^{\ell z}-1}\cdot\frac{dz}{z}$$

При целых отрицательных s $\mathcal{J}(s)$ вычисляется как вычет в начале координат. Для нас наиболее важным во всем этом является тот факт, что с точностью до замены переменной подинтегральная функция в $\mathcal{J}(s)$ есть

$$e^{B_\varphi t}\cdot t^{1-m}\,\frac{dt}{t}$$

Простой подсчет дает теперь требуемый результат:

$$L(1-m,\varphi) = -\frac{B_\varphi^m}{m}$$

Теорема доказана.

Соединяя доказанную теорему с формулами (ж) § I3 (при $m\equiv 0 \mod(\ell-1)$) мы получаем, что

$$L(1-m,\varphi) = -g_{\varphi'}\left((1+\ell)^s-1\right)$$

$$\varphi\neq\varphi_0,\ s=1-m,\ m>0,\ m\in\mathbb{Z},\ m\equiv 0 \mod(\ell-1)$$

Читатель легко выведет аналогичное соотношение для $\varphi=\varphi_0$.

Так как нам уже известно, что $g_{\varphi'}$ является степенным рядом с коэффициентами из $\mathbb{Z}_\ell$, то мы можем утверждать, что функция $f(1-m) = L(1-m,\varphi)$, определенная для целых $m\equiv 0 \mod(\ell-1)$, $m>0$ ℓ-адически непрерывна. Тогда она может быть продолжена по непрерывности на все $\mathbb{Z}_\ell$. Получающуюся функцию мы будем называть ℓ-адическим продолжением функции целого аргумента f. Если ℓ-адическое продолжение функции f является аналитической ℓ-адической функцией, то мы будем говорить, что f обладает аналитическим ℓ-адическим продолжением.

Мы можем сказать теперь, что функция $L(1-m,\varphi)$ при указанных выше условиях обладает аналитическим ℓ-адическим продолжением. Обозначим его через $\mathcal{L}(s,\varphi)$. В качестве основного результата этого курса мы получаем связь между степенными рядами g_φ, определяющими модуль Тэйта поля рациональных чисел и ℓ-адическим продолжением $\mathcal{L}(s,\varphi)$ для L-рядов:

$$g_\varphi(x) = -\mathcal{L}(s,\varphi)$$

если $1+x = (1+\ell)^s$

(Напомним, однако, что это соотношение доказано только при предположении $\ell\nmid h_+$).

Заметим в заключение, что несмотря на такую явную форму для рядов g_φ из нее не удалось получить даже в случае $K=\mathbb{Q}$ ответ на вопрос об обращении в 0 констант μ, поставленный в § 5. Речь идет "всего лишь" о том, чтобы узнать, делятся ли коэффициенты степенных рядов g_φ на ℓ!

О Г Л А В Л Е Н И Е