

БИБЛИОТЕКА СБОРНИКА



МАТЕМАТИКА

Ж.-П. СЕРР

Абелевы
l-адические
представления
и эллиптические
кривые

**ABELIAN ℓ -ADIC
REPRESENTATIONS
AND ELLIPTIC CURVES**

Jean-Pierre Serre
Collège de France

McGill University Lecture Notes
written with the collaboration of
Willem Kuyk and John Labute

W. A. BENJAMIN
New York • Amsterdam
1968

Ж.-П. Серр

АБЕЛЕВЫ
 ℓ -АДИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ
И ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Перевод с английского
В. А. Исковских

Под редакцией
Ю. И. Манина

Работы выдающегося французского математика Ж.-П. Серра хорошо знакомы советскому читателю по русскому переводу его книг: «Алгебраические группы и поля классов», «Когомологии Галуа» («Мир», 1968), «Алгебры Ли и группы Ли» («Мир», 1969), «Линейные представления конечных групп» («Мир», 1970), «Курс арифметики» («Мир», 1972). Его новая книга, посвященная арифметике алгебраических (в особенности абелевых) многообразий в тех ее аспектах, которые связаны с дзета-функциями, автоморфными функциями и теорией Галуа, написана с присущим этому автору мастерством. Она, несомненно, представляет интерес для математиков, и в первую очередь для специалистов по теории чисел, алгебре и топологии.

Редакция литературы по математическим наукам

ПРЕДИСЛОВИЕ

Книга Серра, перевод которой предлагается русскому читателю, посвящена кругу идей на стыке алгебраической геометрии и теории чисел. Пусть V — проективное алгебраическое многообразие над полем алгебраических чисел K , l — простое число, $H^i(V)$ — пространство эtaльных l -адических когомологий Гrotендика многообразия V (над замыканием \bar{K} поля K). Тогда группа Галуа $\text{Gal}(\bar{K}/K)$ действует на $H^i(V)$, так что V определяет серию l -адических представлений этой группы (для разных i и l). Согласно А. Вейлю, дзета-функции многообразия V связаны с этими представлениями так же, как обычные L -ряды Артина связаны с комплексными представлениями группы Галуа. В свою очередь становится все яснее, что эти дзета-функции несут в себе самую фундаментальную информацию об арифметике и топологии многообразия V .

В книге Серра, удачно сочетающей в себе достоинства учебника (с упражнениями и примерами) и монографической работы, подведены первые итоги этой теории, которая, вероятно, будет в центре внимания специалистов по алгебраическим числам, автоморфным функциям и алгебраической геометрии в ближайшие десятилетия. К книге в русском издании приложен перевод доклада П. Делия в семинаре Бурбаки, который доставляет одно из самых эффектных приложений алгебраической геометрии к классической теории чисел. В этом докладе, в частности, доказано, что функция Рамануджана $\sum_{n=1}^{\infty} \tau(n) n^{-s}$, где $\sum_{n=1}^{\infty} \tau(n) x^n = x \prod (1 - x^n)^{24}$, связана с l -адическими представлениями типа рассмотр-

ренных в книге Серра. На этом основана, например, удивительно изящная интерпретация сравнений Рамануджана для коэффициентов $\tau(n)$, данная Серром: он установил, что простые модули l , по которым существуют сравнения, отвечают „уменьшению образа“ l -адического представления по сравнению с априори возможным. Это позволило также показать, что, кроме известных исключительных простых чисел, других не существует.

Сочетание сильной современной техники с конкретностью приложений к классическим задачам, фундаментальность и широкие перспективы излагаемой теории, находящейся в самом начале своего развития, — вот качества этой книги, которые обеспечат ей долгую жизнь.

Ю. И. Манин

ИЗ ПРЕДИСЛОВІЯ АВТОРА

Эта книга воспроизводит с небольшими дополнениями курс лекций, прочитанный в университете Макгила, Монреаль, с 5 по 18 сентября 1967 г. Он был записан в сотрудничестве с Джоном Лабютом (гл. I, IV) и Виллемом Куиком (гл II, III). Им обоим я выражаю глубокую благодарность.

Ж.-П. Серр

ВВЕДЕНИЕ

Понятие „ l -адического представления“, рассматриваемое в этой книге, является алгебраическим аналогом понятия локально постоянного пучка (или „локальных коэффициентов“) в топологии. Типичный пример такого представления строится с помощью точек порядка l^n абелевых многообразий (см. гл. I, п. 1.2); соответствующие l -адические пространства, впервые введенные Вейлем [5], являются одним из основных наших средств в изучении этих многообразий. Даже в одномерном случае возникают нетривиальные проблемы; некоторые из них будут изучены в гл. IV.

Общее понятие l -адического представления впервые было определено Таниямой [37] (см. также реферат этой статьи, выполненный Вейлем в Math. Rev., 20(1959), реферат 1667). Он показал, как можно связать между собой l -адические представления для различных простых чисел l с помощью свойств элементов Фробениуса (см. ниже). В той же статье Танияма изучает также некоторые абелевы представления, которые тесно связаны с комплексным умножением (см. Вейль [6], [7] и Шимура, Танияма [46]). Эти абелевы представления и некоторые их приложения к эллиптическим кривым являются предметом изучения в настоящей книге.

Книга состоит из четырёх глав; вот краткое содержание каждой из них.

Глава I начинается с определения и некоторых примеров l -адических представлений (§ 1). В § 2 основное поле предполагается *числовым*. Поэтому определены элементы Фробениуса и имеется понятие рационального l -адического представления — представления, в котором характеристические многочлены элементов Фробениуса

имеют *рациональные* коэффициенты (а не просто l -адицеские). Два представления, соответствующие различным простым числам, *согласованы*, если совпадают характеристические многочлены их элементов Фробениуса (по крайней мере почти всюду). Мало что известно обо всем этом в неабелевом случае (см. список открытых вопросов в конце п. 2.3). В последнем параграфе показывается, какое отношение имеют L -функции к рациональным l -адицеским представлениям; хорошо известная связь между понятием равномерного распределения и аналитическими свойствами L -функций обсуждается в добавлении.

В главе II строятся некоторые абелевы l -адицеские представления числового поля K . Как отмечалось выше, эта конструкция принадлежит Шимуре, Танияме и Вейлю. Однако я считал удобным представить их результаты в несколько иной форме, определив сначала некоторые алгебраические группы над \mathbf{Q} (группы S_m), представления которых — в обычном алгебраическом смысле — служат основой для l -адицеских представлений поля K . Эти группы были рассмотрены ранее Гротендиком в его пока еще гипотетической теории „мотивов“ (предполагается, что мотивы являются „ l -адицескими когомологиями без l “, так что связь не удивительна). Конструкция групп S_m и l -адицеских представлений, с ними связанных, приводится в § 2 (§ 1 содержит некоторые предварительные факты об алгебраических группах довольно элементарного характера). Я бегло указал также на связь этих групп с комплексным умножением (см. п. 2.8). В последнем параграфе изложены дальнейшие свойства групп S_m .

Глава III посвящена следующему вопросу: пусть ρ — произвольное абелево l -адицеское представление числового поля K , можно ли его получить методом главы II? Ответ положителен, если и только если ρ является *локально алгебраическим* в смысле определения § 1. В большинстве приложений локальная алгебраичность проверяется с помощью результата Тейта, согласно которому она эквивалентна существованию разложения „Ходжа — Тейта“, по крайней мере в том случае, когда представление полупросто. Доказательство этого результата Тейта довольно длинно и существенно использует

его теоремы о p -делимых группах [41]. Оно дано в добавлении. Можно поставить также вопрос: будет ли *ipso facto* любое рациональное полупростое l -адическое представление локально алгебраическим? Возможно, что это так, но я могу доказать это, только когда K является композитом квадратичных полей. Доказательство опирается на одну теорему о трансцендентности Зигеля и Ленга (см. § 3).

В главе IV изучается l -адическое представление ρ_l , определяемое некоторой эллиптической кривой E . Цель этой главы — определить как можно точнее образ группы Галуа или по крайней мере ее алгебры Ли при гомоморфизме ρ_l . Здесь опять основное поле предполагается числовым (случай функционального поля был рассмотрен Игузой [13]). Большая часть результатов этой главы была сформулирована в статьях [29], [35], но в лучшем случае только с набросками доказательств. Здесь я привожу полные доказательства, использующие только некоторые основные факты об эллиптических кривых, собранные в § 1. Принятые в этих доказательствах методы являются более „глобальными“, чем в [29]. Мы исходим из факта, замеченного Касселсом и другими, что число классов с точностью до изоморфизма эллиптических кривых, изогенных данной кривой E , конечно: это легкое следствие теоремы Шафаревича (см. п. 1.4) о конечности числа эллиптических кривых, имеющих хорошую редукцию вне заданного конечного множества точек. Отсюда выводится теорема неприводимости (см. п. 2.1). Определение алгебры Ли образа $\text{Im } \rho_l$ получается после этого, исходя из свойств абелевых представлений, изученных в гл. II и III. Здесь нужно знать, что представление ρ_l абелево и локально алгебраично, но это следует из теоремы Тейта, доказанной в гл. III. Изменение $\text{Im } \rho_l$ в зависимости от l изучается в § 3. Аналогичные результаты для локального случая изложены в добавлении.

ОБОЗНАЧЕНИЯ

Общие понятия

Положительность означает ≥ 0 .

Через \mathbf{Z} (соответственно \mathbf{Q} , \mathbf{R} , \mathbf{C}) обозначается кольцо (соответственно поле) целых (соответственно рациональных, вещественных, комплексных) чисел.

Для простого числа p через \mathbf{F}_p обозначается простое поле $\mathbf{Z}/p\mathbf{Z}$, а через \mathbf{Z}_p (соответственно \mathbf{Q}_p) — кольцо целых (соответственно поле рациональных) p -адических чисел. Имеют место соотношения:

$$\mathbf{Z}_p = \lim_{\leftarrow} \mathbf{Z}/p^n\mathbf{Z}, \quad \mathbf{Q}_p = \mathbf{Z}_p \left[\frac{1}{p} \right].$$

Простые числа

Их мы обозначаем буквами l , l' , p , Буква l преимущественно используется для „ l -адического представления“, а буква p — для обозначения характеристики поля вычетов некоторого нормирования.

Поля

Для произвольного поля K через \bar{K} обозначается его алгебраическое замыкание, а через K_s — его сепарабельное замыкание в \bar{K} . Большинство полей, которые мы рассматриваем, являются совершенными, для них $K_s = \bar{K}$.

Если L/K — расширение Галуа (возможно, бесконечное), то через $\text{Gal}(L/K)$ обозначается его группа Галуа — она является проективным пределом конечных групп.

Алгебраические группы

Пусть G — алгебраическая группа над полем K и K' — коммутативная K -алгебра, тогда через $G(K')$ мы будем обозначать группу K' -точек группы G („ K' -рациональные“ точки группы G). Если K' является полем, то $G_{/K'}$ будет обозначать алгебраическую K' -группу $G \otimes_K K'$, получающуюся из G расширением основного поля K до K' .

Пусть V — конечномерное векторное K -пространство. Через $\text{Aut}_K V$ или $\text{Aut} V$ мы будем обозначать группу его K -линейных автоморфизмов, а через GL_V — соответствующую алгебраическую K -группу (см. гл. I, II, IV). Для любой коммутативной K -алгебры K' группа $GL_V(K')$ K' -точек GL_V — это группа $\text{Aut}_{K'} V \otimes_K K'$; в частности, $GL_V(K) = \text{Aut} V$.

l*-АДИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ**§ 1. Понятие l-адического представления*****1.1. Определение**

Пусть K — некоторое поле и K_s — его сепарабельное алгебраическое замыкание. Будем обозначать через $G = \text{Gal}(K_s/K)$ группу Галуа расширения K_s/K . Снабженная топологией Крулля, она компактна и вполне несвязна. Пусть l — простое число и V — конечномерное векторное пространство над полем l -адических чисел \mathbf{Q}_l . Полная линейная группа $\text{Aut } V$ является l -адической группой Ли с топологией, индуцированной естественной топологией пространства $\text{End } V$. Если $\dim V = n$, то $\text{Aut } V \cong GL(n, \mathbf{Q}_l)$.

Определение. *l*-адическим представлением группы G (или поля K) называется непрерывный гомоморфизм $\rho: G \rightarrow \text{Aut } V$.

Замечания. 1) Решеткой пространства V называется любой свободный \mathbf{Z}_l -подмодуль T в V конечного ранга, который порождает пространство V над \mathbf{Q}_l , так что V может быть отождествлено с $T \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$. Отметим, что всегда существует решетка пространства V , инвариантная относительно действия группы G . Это вытекает из того факта, что группа G компактна. В самом деле, пусть L — произвольная решетка в V и H — множество таких элементов $g \in G$, что $\rho(g)L = L$. Тогда H является открытой подгруппой в G и фактор G/H конечен. Следовательно, решетка T , порожденная решетками $\rho(g)L$, $g \in G/H$, будет уже инвариантна относительно действия группы G .

Отметим, что T может быть отождествлена с проективным пределом свободных $\mathbf{Z}/l^m\mathbf{Z}$ -модулей T/l^mT , на которых действует группа G ; векторное пространство V восстанавливается по T по формуле $V = T \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$.

2) Если ρ — некоторое l -адическое представление группы G , то группа $G_\rho = \text{Im } \rho$ является замкнутой подгруппой группы $\text{Aut } V$ и, следовательно, по l -адическому аналогу теоремы Картана (см. [32], LG, стр. 5—42) G_ρ является l -адической группой Ли. Ее алгебра Ли $\mathfrak{g}_\rho = \text{Lie } G_\rho$ будет подалгеброй алгебры $\text{End } V = \text{Lie Aut } V$. Легко видеть, что эта алгебра Ли инвариантна относительно расширений конечного типа основного поля K (ср. [28], п. 1.2).

Упражнение. 1) Пусть V — двумерное векторное пространство над полем k и H — некоторая подгруппа группы $\text{Aut } V$. Предположим, что $\det(I - h) = 0$ для всех $h \in H$. Показать, что существует базис пространства V , в котором H содержит либо в подгруппе матриц $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$, либо в подгруппе матриц $\begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix}$ группы $\text{Aut } V$.

2) Пусть $\rho: G \rightarrow \text{Aut } V_l$ — некоторое l -адическое представление группы G , где V_l — векторное \mathbf{Q}_l -пространство размерности 2. Предположим, что $\det(1 - \rho(s)) \equiv 0 \pmod{l}$ для всех $s \in G$. Пусть T — инвариантная относительно G решетка в V_l . Показать, что существует решетка T' в V_l со следующими двумя свойствами:

а) T' инвариантна относительно G ;

б) либо T' является подрешеткой индекса l в T и G действует тривиально на T/T' , либо T является подрешеткой индекса l в T' и G действует тривиально на T'/T . (Применить упражнение 1 с $k = \mathbf{F}_l$ и $V = T/IT$.)

3) Пусть ρ — полупростое l -адическое представление группы G и U — некоторый нормальный делитель в G . Предположим, что для каждого $x \in U$ элемент $\rho(x)$ унипотентен (т. е. все его собственные значения равны 1). Показать, что $\rho(x) = 1$ для всех $x \in U$. (Показать, что ограничение ρ на U полупросто, и воспользоваться теоремой Колчина для того, чтобы привести его к треугольному виду.)

4) Пусть $\rho: G \rightarrow \text{Aut } V_l$ есть l -адическое представление группы G и T — решетка в V_l , инвариантная относительно G . Доказать эквивалентность следующих утверждений:

- а) представление группы G в векторном \mathbf{F}_l -пространстве T/lT неприводимо;
 б) только решетки вида l^nT с $n \in \mathbf{Z}$ в пространстве V_l инвариантны относительно группы G .

1.2. Примеры

1. Корни из единицы. Пусть $l \neq \text{char } K$. Тогда группа $G = \text{Gal}(K_s/K)$ действует на группе μ_m l^m -корней из единицы и, следовательно, также на группе $T_l(\mu) = \varprojlim \mu_m$. Векторное \mathbf{Q}_l -пространство $V_l(\mu) = T_l(\mu) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$ имеет размерность 1, и гомоморфизм $\chi_l: G \rightarrow \text{Aut } V_l = \mathbf{Q}_l^*$, определяемый действием группы G на V_l , является одномерным l -адическим представлением группы G . Характер χ_l принимает значения в группе единиц U_l кольца \mathbf{Z}_l ; по определению

$$g(z) = z^{\chi_l(g)}, \quad g \in G, \quad z^{l^m} = 1.$$

2. Эллиптические кривые. Пусть $l \neq \text{char } K$ и E — эллиптическая кривая, определенная над K , с фиксированной рациональной точкой 0. Известно, что существует единственная структура алгебраической группы на E с нулевым элементом 0. Обозначим через E_m ядро умножения на l^m в группе точек $E(K_s)$ и положим

$$T_l(E) = \varprojlim E_m, \quad V_l(E) = T_l(E) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l.$$

Модуль $T_l(E)$, называемый модулем Тейта, является свободным \mathbf{Z}_l -модулем, на котором действует группа $G = \text{Gal}(K_s/K)$ (см. [17], гл. VII). Соответствующий гомоморфизм $\pi_l: G \rightarrow \text{Aut } V_l(E)$ является l -адическим представлением группы G . Образ $\text{Im } \pi_l = G_l$ является замкнутой подгруппой группы $\text{Aut } T_l(E)$, 4-мерной группы Ли, изоморфной $GL(2, \mathbf{Z}_l)$. (В гл. IV мы вычислим алгебру Ли группы G_l в случае, когда поле K числовое.)

Так как кривую E мы можем отождествить с двойственной к ней (в смысле двойственности абелевых многообразий), то символ (x, y) (см. [17], loc. cit.) определяет канонические изоморфизмы

$$\Lambda^2 T_l(E) = T_l(\mu), \quad \Lambda^2 V_l(E) = V_l(\mu).$$

Следовательно, $\det \pi_l$ — это характер χ_l , определенный в примере 1.

3. Абелевы многообразия. Пусть A является d -мерным абелевым многообразием над K . Для $l \neq \text{char } K$ определим $T_l(A)$ и $V_l(A)$ так же, как и в примере 2. Тогда $T_l(A)$ является свободным \mathbf{Z}_l -модулем ранга $2d$ (см. [17], loc. cit.), и на нем действует группа $G = \text{Gal}(K_s/K)$.

4. Когомологические представления. Пусть X — алгебраическое многообразие, определенное над полем K , и $X_s = X \times_K K_s$ — соответствующее многообразие над K_s . Пусть $l \neq \text{char } K$ и i — целое число. Положим

$$H^i(X_s, \mathbf{Z}_l) = \varprojlim H^i(X_{s, et}, \mathbf{Z}/l^n\mathbf{Z}),$$

$$H_l^i(X_s) = H^i(X_s, \mathbf{Z}_l) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l,$$

где $H^i(X_{s, et}, \mathbf{Z}/l^n\mathbf{Z})$ — этальные когомологии Артина — Гrotендика [3]. Группа $H_l^i(X_s)$ является векторным пространством над \mathbf{Q}_l , на котором действует группа $G = \text{Gal}(K_s/K)$ (посредством действия G на X_s). Оно конечномерно, по крайней мере если $\text{char } K = 0$ или если X является собственным над K . Мы получаем, таким образом, l -адическое представление группы G на $H_l^i(X_s)$; по двойственности можно получить еще и гомологические l -адические представления. Примеры 1, 2, 3 являются частными случаями гомологических l -адических представлений с $i = 1$ и с X , равным соответственно мультипликативной группе \mathbf{G}_m , эллиптической кривой E и абелеву многообразию A .

Упражнение. (а) Показать, что существует эллиптическая кривая E , определенная над $K_0 = \mathbf{Q}(T)$, с j -инвариантом, равным T .

(б) Показать, что для каждой такой кривой над $K = \mathbf{C}(T)$ имеет место отождествление $G_l = SL(T_l(E))$ (см. алгебраическое доказательство Игузы [13]).

(в) Показать, используя (б), что над полем K_0 имеет место равенство $G_l = GL(T_l(E))$.

(г) Показать, что для любой замкнутой подгруппы H группы $GL(2, \mathbf{Z}_l)$ существует такая эллиптическая кривая (определенная над некоторым полем), что $G_l = H$.

§ 2. *l*-адические представления числовых полей

2.1. Предварительные результаты

(Основные понятия, касающиеся числовых полей, можно найти, например, в книгах [15], [18] или [9].) Пусть K — числовое поле (т. е. конечное расширение поля \mathbf{Q}). Обозначим через Σ_K множество всех конечных точек поля K , т. е. множество всех нормализованных дискретных нормирований поля K (или, что то же самое, множество всех простых идеалов кольца целых чисел $A_K \subset K$). Поле вычетов k_v точки v конечно, и число его элементов равно $Nv = p_v^{\deg v}$, где $p_v = \text{char } k_v$, а $\deg v$ — степень поля k_v над \mathbf{F}_{p_v} . Индексом ветвления e_v точки v называется $v(p_v)$.

Пусть L/K — конечное расширение Галуа с группой Галуа G , и пусть $w \in \Sigma_L$. Подгруппа $D_w \subset G$ таких элементов $g \in G$, что $gw = w$, называется *группой разложения* точки w . Ограничение w на K кратно (с целым коэффициентом) некоторому элементу $v \in \Sigma_K$; для кратности мы будем говорить также, что v является ограничением w на поле K , и писать $w|v$ („ w делит v “). Пусть L_w (соответственно K_v) — пополнение поля L (соответственно K) относительно w (соответственно v). Тогда $D_w = \text{Gal}(L_w/K_v)$. Группа D_w гомоморфно отображается на группу Галуа $\text{Gal}(l_w/k_v)$ соответствующего расширения поля вычетов l_w/k_v . Ядро I_w гомоморфизма $D_w \rightarrow \text{Gal}(l_w/k_v)$ называется *группой инерции* точки w . Факторгруппа D_w/I_w циклична и порождена элементом Фробениуса F_w , и мы имеем $F_w(\lambda) = \lambda^{Nv}$ для любого $\lambda \in l_w$. Нормирование w (соответственно v) называется *неразветвленным*, если $I_w = \{1\}$. Почти все нормирования поля K не разветвлены.

Для произвольного алгебраического расширения L поля \mathbf{Q} множество Σ_L определяется как проективный предел множеств Σ_{L_a} , где L_a пробегает конечные под-

расширения расширения L/\mathbf{Q} . В случае когда L/K — произвольное расширение Галуа числового поля K и $w \in \Sigma_L$ — некоторая точка, объекты D_w, I_w, F_w определяются так же, как и выше. Если точка v поля K не разветвлена в L и w — ее продолжение на L , то через F_v мы обозначаем класс элемента F_w в группе $G = \text{Gal}(L/K)$ с точностью до сопряженности.

Определение. Пусть $\rho: \text{Gal}(\bar{K}/K) \rightarrow \text{Aut } V$ — некоторое l -адическое представление поля K и $v \in \Sigma_K$ — произвольная точка. Мы будем говорить, что ρ не разветвлено в v , если $\rho(I_w) = \{1\}$ для каждого нормирования w поля \bar{K} , продолжающего v .

Если представление ρ не разветвлено в v , то ограничение его на D_w пропускается через D_w/I_w для любого $w|v$; следовательно, определен элемент $\rho(F_w) \in \text{Aut } V$, который мы будем называть элементом Фробениуса точки w в представлении ρ и обозначать через $F_{w, \rho}$. Класс сопряженности элемента $F_{w, \rho}$ в группе $\text{Aut } V$ зависит только от v , он обозначается через $F_{v, \rho}$. Пусть L/K — расширение поля K , соответствующее подгруппе $H = \text{Ker } \rho$; ρ не разветвлено в v тогда и только тогда, когда v не разветвлено в L/K .

2.2. Теорема плотности Чеботарёва

Пусть P — некоторое подмножество в Σ_K . Для каждого целого числа n обозначим через $a_n(P)$ число точек $v \in P$, таких, что $Nv \leq n$. Говорят, что P имеет плотность a , где a — некоторое действительное число, если

$$\lim_{n \rightarrow \infty} \frac{a_n(P)}{a_n(\Sigma_K)} = a \quad \text{при } n \rightarrow \infty.$$

Заметим, что $a_n(\Sigma_K) \sim n/\log n$ по теореме о распределении простых чисел (см. добавление или [18], гл. VIII), так что предыдущее равенство можно переписать в виде

$$a_n(P) = an/\log n + o(n/\log n).$$

Примеры. Конечное множество имеет плотность 0. Множество $U \subset \Sigma_K$ точек степени 1 (т. е. таких v , что Nv — простое число) имеет плотность 1. Множество обычных простых чисел, первая цифра которых (скажем, в десятичной системе) равна 1, не имеет плотности.

Теперь мы можем сформулировать теорему плотности Чеботарева.

Теорема. Пусть L — конечное расширение Галуа числового поля K с группой Галуа G . Пусть X — подмножество в G , инвариантное относительно сопряжения. Обозначим через P_X множество точек $v \in \Sigma_K$, неразветвленных в L , таких, что класс Фробениуса F_v содержится в X . Тогда плотность множества P_X равна $\text{Card } X / \text{Card } G$.

Доказательство см. в [42], [1] или в добавлении.

Следствие 1. Для каждого элемента $g \in G$ существует бесконечно много неразветвленных точек $w \in \Sigma_L$, таких, что $F_w = g$.

Для бесконечных расширений имеем

Следствие 2. Пусть L — расширение Галуа поля K , которое неразветвлено вне конечного множества точек S . Тогда

а) Элементы Фробениуса неразветвленных точек поля L составляют плотное подмножество в группе $\text{Gal}(L/K)$.

б) Пусть X — подмножество в $\text{Gal}(L/K)$, инвариантное относительно сопряжения. Предположим, что его граница имеет меру нуль относительно меры Хаара μ на G , нормализованной так, чтобы $\mu(G) = 1$. Тогда множество точек $v \notin S$, таких, что $F_v \in X$, имеет плотность, равную $\mu(X)$.

Утверждение б) получается из теоремы с помощью представления L в виде направленного объединения конечных расширений Галуа и перехода к пределу (можно воспользоваться также предложением 1 добавления). Утверждение а) вытекает из б), если взять в качестве X подходящую окрестность заданного класса.

Упражнение. Пусть G — некоторая *l*-адическая группа Ли и X — ее аналитическое подмножество (т. е.

множество, определяемое общими нулями семейства аналитических функций на G). Показать, что граница X имеет меру нуль относительно меры Хаара на G .

2.3. Рациональные l -адические представления

Пусть ρ — некоторое l -адическое представление числового поля K . Для каждой точки $v \in \Sigma_K$, неразветвленной в представлении ρ , обозначим через $P_{v,\rho}(T)$ многочлен $\det(1 - F_{v,\rho}T)$.

Определение. l -адическое представление ρ называется *рациональным* (соответственно *целым*), если существует такое конечное подмножество $S \subset \Sigma_K$, что

- (а) любой элемент из $\Sigma_K \setminus S$ неразветвлен в представлении ρ ,
- (б) если $v \notin S$, то коэффициенты многочлена $P_{v,\rho}(T)$ принадлежат полю \mathbf{Q} (соответственно кольцу \mathbf{Z}).

Замечание. Пусть K'/K — конечное расширение. Тогда l -адическое представление ρ поля K определяет (посредством ограничения) l -адическое представление $\rho_{/K'}$ поля K' . Если представление ρ рациональное (соответственно целое), то таким же будет и $\rho_{/K'}$: это следует из того, что элементы Фробениуса относительно K' являются степенями элементов Фробениуса относительно K .

Примеры. l -адические представления поля K , рассмотренные в примерах 1, 2 и 3 п. 1.2, являются рациональными (даже *целыми*). В примере 1 в качестве S надо взять множество S_l элементов $v \in \Sigma_K$, таких, что $p_v = l$; в качестве элемента Фробениуса надо взять Nv , рассматриваемый как элемент группы U_l . В примерах 2 и 3 множество S — это объединение множеств S_l и S_A , где S_A — множество точек, в которых A имеет „плохую редукцию“. Тот факт, что характеристический многочлен соответствующего элемента Фробениуса имеет целые коэффициенты (не зависящие от l), является следствием результатов Вейля об эндоморфизмах абелевых многообразий (см. [5] и [17], гл. VII). Рациональность когомологических представлений — хорошо известный открытый вопрос.

ОПРЕДЕЛЕНИЕ. Пусть l' — простое число, а ρ' есть l' -адическое представление поля K . Предположим, что представления ρ и ρ' рациональны. Тогда они называются *согласованными*, если существует конечное подмножество $S \subset \Sigma_K$, такое, что ρ и ρ' неразветвлены вне S и $P_{v, \rho}(T) = P_{v, \rho'}(T)$ для каждого $v \in \Sigma_K \setminus S$.

[Иными словами, характеристические многочлены элементов Фробениуса являются одними и теми же для представлений ρ и ρ' по крайней мере для почти всех v .]

Если $\rho: \text{Gal}(\bar{K}/K) \rightarrow \text{Aut } V$ — рациональное l -адическое представление поля K , то V имеет композиционный ряд

$$V = V_0 \supset V_1 \supset \dots \supset V_q = 0,$$

состоящий из ρ -инвариантных подпространств с *простыми* (т. е. *неприводимыми*) факторпространствами V_i/V_{i+1} , $(0 \leq i \leq q-1)$. При этом l -адическое представление ρ поля K в пространстве $V' = \sum_{i=0}^{q-1} V_i/V_{i+1}$ полуупросто, рационально и согласовано с ρ ; это *полупростая оболочка* представления V .

ТЕОРЕМА. Пусть ρ — рациональное l -адическое представление поля K и l' — простое число. Тогда существует самое большее одно (с точностью до изоморфизма) l' -адическое рациональное представление ρ' поля K , которое полуупросто и согласовано с ρ .

[Следовательно, существует и единственno с точностью до изоморфизма рациональное полуупростое l -адическое представление, согласованное с ρ .]

Доказательство. Пусть ρ'_1 и ρ'_2 — полуупростые l -адические представления поля K , рациональные и согласованные с ρ . Докажем прежде всего, что $\text{Tr } \rho'_1(g) = \text{Tr } \rho'_2(g)$ для всех $g \in G$. Пусть $H = G / (\text{Кер } \rho'_1 \cap \text{Кер } \rho'_2)$, тогда ρ'_1 и ρ'_2 можно рассматривать как представления группы H и достаточно показать, что $\text{Tr } \rho'_1(h) = \text{Tr } \rho'_2(h)$ для всех $h \in H$. Пусть $M \subset \bar{K}$ — поле неподвижных

элементов для группы H . Тогда в силу согласованности ρ'_1, ρ'_2 с ρ существует конечное подмножество $S \subset \Sigma_K$, такое, что для каждого $v \in \Sigma_K \setminus S$ и $w \in \Sigma_M$, $w \mid v$, имеет место равенство $\text{Tr } \rho'_1(F_w) = \text{Tr } \rho'_2(F_w)$. Но, согласно следствию 2 теоремы Чеботарева (см. п. 2.2), множество элементов F_w плотно в H . Следовательно, $\text{Tr } \rho'_1(h) = \text{Tr } \rho'_2(h)$ для всех $h \in H$, так как отображения $\text{Tr} \circ \rho'_1$ и $\text{Tr} \circ \rho'_2$ непрерывны. Доказательство теоремы выводится теперь из следующего результата, примененного к групповому кольцу $\Lambda = \mathbf{Q}_l[H]$:

Лемма. *Пусть k — поле характеристики нуль, Λ — некоторая k -алгебра и ρ_1, ρ_2 — конечномерные представления алгебры Λ . Если ρ_1 и ρ_2 полупросты и имеют одинаковые следы, $\text{Tr} \circ \rho_1 = \text{Tr} \circ \rho_2$, то они изоморфны.*

Доказательство. (См. Бурбаки Н., Алгебра, гл. VIII, § 12, п. 1, предложение 3.)

Определение. Пусть для каждого простого числа l задано l -адическое представление ρ_l поля K . Система (ρ_l) называется *согласованной*, если для любых двух простых чисел l и l' представления ρ_l и $\rho_{l'}$ согласованы. Система (ρ_l) называется *строго согласованной*, если существует конечное подмножество $S \subset \Sigma_K$, такое, что

(а) Если $S_l = \{v \mid p_v = l\}$, то для каждого $v \notin S \cup S_l$ представление ρ_l не разветвлено в точке v и многочлен $P_{v, \rho_l}(T)$ имеет рациональные коэффициенты.

(б) Если $v \notin S \cup S_l \cup S_{l'}$, то $P_{v, \rho_l}(T) = P_{v, \rho_{l'}}(T)$.

Наименьшее конечное подмножество $S \subset \Sigma_K$ со свойствами (а) и (б) для строго согласованной системы представлений (ρ_l) мы будем называть *исключительным множеством* этой системы.

Примеры. Системы l -адических представлений в примерах 1, 2 и 3 п. 1.2 являются строго согласованными. Исключительное множество первой из них пусто. Во втором (соответственно третьем) примере исключительное множество состоит из тех точек, где эллиптическая кривая (соответственно абелево многообразие) имеет „плохую редукцию“ (см. [36]).

Вопросы. 1. Пусть ρ — рациональное l -адическое представление. Верно ли, что $P_{v, \rho}$ имеет рациональные коэффициенты для каждой точки v , в которой ρ не разветвлено?

В некотором роде аналогичный вопрос: любая ли согласованная система строго согласована?

2. Всякое ли рациональное l -адическое представление может быть получено (с помощью тензорных произведений, прямых сумм и т. д.) из представлений, возникающих из l -адических когомологий?

3. Задано рациональное l -адическое представление ρ поля K и простое число l' . Существует ли l' -адическое представление ρ' , согласованное с $\rho^{?1)}$

4. Пусть ρ, ρ' — согласованные полупростые рациональные l - и l' -адические представления поля K . Тогда

(i) Если ρ абелово (т. е. если $\text{Im } \rho$ — абелева группа), то будет ли таким $\rho^{?}$ (В главе III мы увидим, что это верно, по крайней мере, если ρ „локально алгебраично“.)

(ii) Верно ли, что $\text{Im } \rho$ и $\text{Im } \rho'$ являются группами Ли одной и той же размерности? Более оптимистически, верно ли, что существует алгебра Ли g над \mathbf{Q} , такая, что $\text{Lie}(\text{Im } \rho) = g \otimes_{\mathbf{Q}} \mathbf{Q}_p$, $\text{Lie}(\text{Im } \rho') = g \otimes_{\mathbf{Q}} \mathbf{Q}_{l'}$?

5. Пусть X — неособое проективное многообразие, определенное над K , и i — некоторое целое число. Будет ли i -е когомологическое представление $H^i(X_s)$ полупросто? Содержит ли его алгебра Ли гомотетии, если $i \geq 1$? (В случае $i=1$ утвердительный ответ на этот вопрос означал бы положительное решение „проблемы конгруэнцподгрупп“ для абелевых многообразий (см. [28], § 3.)

Замечание. Понятие l -адического представления можно обобщить, заменив простое число l точкой λ

¹⁾ Как сообщил автор, ответ отрицательный. Надо взять такое неприводимое представление конечной группы, значения характера которого принадлежат \mathbf{Q} и индекс Шура > 1 . Тогда соответствующая простая алгебра распадается вне некоторого конечного непустого множества S простых чисел. Для построения контрпримера достаточно взять l вне S , а l' из S . Вопрос 3 должен быть переформулирован таким образом: верно ли, что для почти всех l' существуют l -адические представления, согласованные с $\rho^{?}$ — Прим. ред.

числового поля E . Тогда λ -адическое представление — это непрерывный гомоморфизм $\text{Gal}(K_s/K) \rightarrow \text{Aut } V$, где V — конечномерное векторное пространство над локальным полем E_λ . Понятия рационального λ -адического представления, согласованных представлений и т. д. определяются так же, как и в l -адическом случае.

Упражнения. 1) Пусть ρ и ρ' — рациональные полупростые согласованные представления. Показать, что если $\text{Im } \rho$ конечен, то это верно и для $\text{Im } \rho'$, и что $\text{Ker } \rho = \text{Ker } \rho'$. (Применить упр. 3 из п. 1.1 к ρ' и $U = \text{Ker } \rho$.) Обобщить это утверждение на λ -адические представления (для числового поля E).

2) Пусть ρ (соответственно ρ') — рациональное l -адическое (соответственно l' -адическое) представление поля K степени n . Предположим, что ρ и ρ' согласованы. Пусть $s \in G = \text{Gal}(\bar{K}/K)$ и $\sigma_i(s)$ (соответственно $\sigma'_i(s)$) есть i -й коэффициент характеристического многочлена $\rho(s)$ (соответственно $\rho'(s)$). Пусть $P(X_0, \dots, X_n)$ — некоторый многочлен с рациональными коэффициентами и X_P (соответственно $X'_{P'}$) — множество таких элементов $s \in G$, что $P(\sigma_0(s), \dots, \sigma_n(s)) = 0$ (соответственно $P(\sigma'_0(s), \dots, \sigma'_n(s)) = 0$).

а) Показать, что границы множеств X_P и $X'_{P'}$ имеют меру нуль в мере Хаара μ на группе G (использовать упр. п. 2.2).

б) Предположим, что мера μ нормализована, т. е. $\mu(G) = 1$. Пусть T_P — множество точек $v \in \Sigma_K$, в которых ρ неразветвлено и для которых коэффициенты характеристического многочлена автоморфизма $F_{v, \rho}$ удовлетворяют уравнению $P(\sigma_0, \dots, \sigma_n) = 0$. Показать, что множество T_P имеет плотность, равную $\mu(X_P)$.

в) Показать, что $\mu(X_P) = \mu(X'_{P'})$.

2.4. Представления со значениями в линейной алгебраической группе

Пусть H — линейная алгебраическая группа, определенная над полем k . Для любой коммутативной k -алгебры k' обозначим через $H(k')$ группу точек группы H со значениями в k' . Пусть A — координатное

кольцо (или „аффинное кольцо“) группы H . Элемент $f \in A$ называется *центральным*, если $f(xy) = f(yx)$ для всех $x, y \in H(k')$, где k' — любая коммутативная k -алгебра. Пусть $x \in H(k')$, мы говорим, что *класс сопряженности элемента x рационален над k* , если $f(x) \in k$ для каждого центрального элемента f кольца A .

ОПРЕДЕЛЕНИЕ. Пусть H — линейная алгебраическая группа над \mathbf{Q} и K — некоторое поле. Тогда непрерывный гомоморфизм $\rho: \text{Gal}(K_s/K) \rightarrow H(\mathbf{Q}_l)$ называется *l-адическим представлением поля K со значениями в H* .

[Заметим, что множество $H(\mathbf{Q}_l)$ естественным образом снабжено структурой топологической группы и даже *l*-адической группы Ли.]

Для числового поля K очевидным образом определяется понятие неразветвленности представления ρ в точке $v \in \Sigma_K$, элемент Фробениуса $F_{w, \rho} \in H(\mathbf{Q}_l)$ для $w|v$ и его класс сопряженности $F_{v, \rho}$. Будем говорить, как и выше, что представление ρ рационально, если

(а) существует конечное множество $S \subset \Sigma_K$, такое, что ρ неразветвлено вне S ,

(б) если $v \notin S$, то класс сопряженности $F_{v, \rho}$ рационален над \mathbf{Q} .

Два рациональных представления ρ и ρ' (для простых l и l') называются *согласованными*, если существует такое конечное подмножество $S \subset \Sigma_K$, что ρ и ρ' неразветвлены вне S и для каждого центрального элемента $f \in A$ и любого $v \in \Sigma_K \setminus S$ выполняется равенство $f(F_{v, \rho}) = f(F_{v, \rho'})$. Таким же образом определяются понятия *согласованности* и *строгой согласованности* систем рациональных представлений.

Замечания. 1) Если алгебраическая группа H абелева, то условие (б) означает, что $F_{v, \rho}$ (являющийся в этом случае элементом из $H(\mathbf{Q}_l)$) рационален над \mathbf{Q} , т. е. принадлежит $H(\mathbf{Q})$.

2) Пусть V_0 — конечномерное векторное пространство над \mathbf{Q} и GL_{V_0} — линейная алгебраическая группа над \mathbf{Q} , группа точек которой в любой коммутативной \mathbf{Q} -алгебре k есть $\text{Aut}(V_0 \otimes_{\mathbf{Q}} k)$; в частности, если $V_l = V_0 \otimes_{\mathbf{Q}} \mathbf{Q}_l$,

то $GL_{V_l}(\mathbf{Q}_l) = \text{Aut } V_l$. Для каждого гомоморфизма $\varphi: H \rightarrow GL_{V_0}$ линейных алгебраических групп над \mathbf{Q} определен индуцированный гомоморфизм $\varphi_l: H(\mathbf{Q}_l) \rightarrow GL_{V_0}(\mathbf{Q}_l) = \text{Aut } V_l$. Если ρ есть l -адическое представление группы $\text{Gal}(K_s/K)$ в $H(\mathbf{Q}_l)$, то в композиции с φ_l оно дает линейное l -адическое представление $\varphi_l \circ \rho: \text{Gal}(K_s/K) \rightarrow \text{Aut } V_l$. Учитывая, что коэффициенты характеристического многочлена являются центральными функциями, мы убеждаемся, что *представление $\varphi_l \circ \rho$ рационально, если рационально ρ* (для числового поля K). Согласованность представлений в H дает, конечно, согласованность и соответствующих линейных представлений. Мы используем этот метод для конструкции согласованных представлений в случае абелевой группы H (см. гл. II, п. 2.5).

2.5. L -функции, связанные с рациональными представлениями

Пусть K — числовое поле и $\rho = (\rho_l)$ — строго согласованная система рациональных l -адических представлений с исключительным множеством S . Если $v \notin S$, обозначим через $P_{v, \rho}(T)$ рациональный многочлен $\det(1 - F_{v, \rho_l} T)$ для каждого $l \neq p_v$; по предположению этот многочлен не зависит от выбора l . Пусть s — комплексное число. Имеем

$$P_{v, \rho}((Nv)^{-s}) = \det(1 - F_{v, \rho}/(Nv)^s) = \prod_i (1 - \lambda_{i, v}/(Nv)^s),$$

где $\lambda_{i, v}$ — собственные значения элементов $F_{v, \rho}$ (заметим, что $\lambda_{i, v}$ — алгебраические числа и, следовательно, могут быть отождествлены с комплексными числами). Положим

$$L_\rho(s) = \prod_{v \notin S} \frac{1}{P_{v, \rho}((Nv)^{-s})}.$$

Это *формальный ряд Дирихле* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ с коэффициентами в \mathbf{Q} . Во всех известных случаях существует такая константа k , что $|\lambda_{i, v}| \leq (Nv)^k$, что влечет за собой схо-

димость ряда $L_\rho(s)$ в некоторой полуплоскости $\operatorname{Re}(s) > C$. Предполагается, что $L_\rho(s)$ продолжается до мероморфной функции на всю плоскость. В случае когда ρ — представление в *l*-адических когомологиях, имеются дальнейшие гипотезы о нулях и полюсах функции L_ρ , см. Тейт [38]. Как указал Тейт, их можно использовать для вывода свойств равномерной распределенности элементов Фробениуса, см. добавление.

Замечания. 1) *L*-функции можно также построить, исходя из *E-рациональных* систем λ -адических представлений (замечание в п. 2.3), где *E* — числовое поле с фиксированным вложением в поле комплексных чисел **C**.

2) Мы определили локальные множители L_ρ только для точек $v \notin S$. Можно предложить более изощренное определение, пригодное для всех точек поля, даже (в подходящих предположениях) и для бесконечных (гамма-множители); это необходимо при изучении функциональных уравнений. Мы не будем приводить его здесь.

3) Пусть $\varphi(s) = \sum a_n/n^s$ — некоторый ряд Дирихле. Воспользовавшись теоремой п. 2.3, заметим, что может существовать самое большее одна (с точностью до изоморфизма) полупростая система $\rho = (\rho_l)$ над **Q**, такая, что $L_\rho = \varphi$. Вопрос о ее существовании (для заданного φ) часто бывает весьма интересен. Например, существует ли такая система для функции Рамануджана $\varphi(s) = \sum_{n=1}^{\infty} \tau(n)/n^s$, где $\tau(n)$ определяется из тождества

$$x \prod_{n=1}^{\infty} (1 - x^n)^{24} = \sum_{n=1}^{\infty} \tau(n) x^{n-1}?$$

В пользу этого предположения имеются численные свидетельства, основанные на свойствах сравнений для $\tau(n)$ (Синнертон — Дайер, не опубликовано). Разумеется, такая система ρ должна иметь размерность 2 и ее исключительное множество *S* должно быть пустым.

¹⁾ Положительный ответ на этот вопрос получен П. Делинем, см. приложение. — *Прим. ред.*

Более общо, существует, по-видимому, тесная связь между модулярными формами, такими, как $\sum \tau(n) x^n$, и рациональными (или алгебраическими) l -адическими представлениями, см., например, статьи Шимуры [45] и Вейля [10].

Примеры. 1. Если G действует как конечная группа, то L_ρ совпадает с точностью до конечного числа множителей с (неабелевым) L -рядом Артина (см. [1]). Таким способом получаются все L -ряды Артина, если, конечно, использовать E -рациональные представления [см. замечание 1], а не только рациональные.

2. Если ρ — система представлений, ассоциированная с эллиптической кривой E (см. п. 1.2), то соответствующая L -функция — это нетривиальная часть дзета-функции кривой E . Симметрические степени представления ρ дают дзета-функции произведений $E \times \dots \times E$ (см. Тейт [38]).

Добавление

Равнораспределенность и L -функции

Д.1. Равнораспределенность

Пусть X — компактное топологическое пространство и $C(X)$ — банахово пространство непрерывных комплекснозначных функций на X с обычной нормой $\|f\| = \sup_{x \in X} |f(x)|$. Для каждой точки $x \in X$ пусть δ_x обозначает меру Дирака, ассоциированную с x ; если $f \in C(X)$, то $\delta_x(f) = f(x)$. Пусть $(x_n)_{n \geq 1}$ — последовательность точек в X . Для $n \geq 1$ положим

$$\mu_n = (\delta_{x_1} + \dots + \delta_{x_n})/n$$

и обозначим через μ некоторую меру Радона на X (т. е. непрерывную линейную форму на $C(X)$, см. Бурбаки, Интегрирование, меры, интегрирование мер, М., 1967, гл. III, § 1). Последовательность (x_n) называется μ -равнораспределенной или μ -равномерно распределенной, если $\mu_n \rightarrow \mu$ в смысле слабой сходимости при $n \rightarrow \infty$, т. е.

если $\mu_n(f) \rightarrow \mu(f)$ при $n \rightarrow \infty$ для любой функции $f \in C(X)$. Отметим, что это влечет положительность меры μ и равенство $\mu(X) = 1$. Отметим еще, что сходимость $\mu_n(f) \rightarrow \mu(f)$ означает, что

$$\mu(f) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n f(x_i).$$

Лемма 1. Пусть (φ_a) — такое семейство непрерывных функций на X , что их линейные комбинации образуют плотное подмножество в $C(X)$. Предположим, что для каждого a последовательность $\mu_n(\varphi_a)_{n \geq 1}$ имеет предел. Тогда последовательность (x_n) равномерно распределена относительно некоторой меры μ . Это — единственная мера со свойством $\mu(\varphi_a) = \lim_{n \rightarrow \infty} \mu_n(\varphi_a)$ для каждого a .

Стандартное рассуждение с использованием равномерной непрерывности показывает, что для $f \in C(X)$ последовательность $(\mu_n(f))$ имеет предел $\mu(f)$, который непрерывен и линеен по f . Это доказывает лемму.

Предложение 1. Предположим, что последовательность (x_n) μ -равнораспределена. Пусть U — подмножество в X , граница которого имеет μ -меру нуль, и пусть n_U для каждого n означает число индексов $m \leq n$, таких, что $x_m \in U$. Тогда

$$\lim_{n \rightarrow \infty} (n_U/n) = \mu(U).$$

Пусть U^0 — внутренность U . Имеем $\mu(U^0) = \mu(U)$. Выберем $\varepsilon > 0$. По определению $\mu(U^0)$ существует такая непрерывная функция $\varphi \in C(X)$, $0 \leq \varphi \leq 1$, что $\varphi = 0$ на $X \setminus U^0$ и $\mu(\varphi) \geq \mu(U) - \varepsilon$. Так как $\mu_n(\varphi) \leq n_U/n$, то

$$\liminf_{n \rightarrow \infty} n_U/n \geq \lim_{n \rightarrow \infty} \mu_n(\varphi) = \mu(\varphi) \geq \mu(U) - \varepsilon,$$

отсюда получаем, что $\liminf_{n \rightarrow \infty} n_U/n \geq \mu(U)$. Те же рассуждения, примененные к $X \setminus U$, показывают, что

$$\liminf_{n \rightarrow \infty} (n - n_U)/n \geq \mu(X \setminus U).$$

Следовательно, $\limsup_{n \rightarrow \infty} n_U/n \leq \mu(U) \leq \liminf_{n \rightarrow \infty} n_U/n$, что доказывает предложение.

Примеры. 1. Пусть $X = [0, 1]$ — единичный интервал с мерой Лебега μ . Последовательность точек (x_n) из X μ -равнораспределена тогда и только тогда, когда для каждого интервала $[a, b]$ длины $d > 0$ в $[0, 1]$ число индексов $m \leq n$, таких, что $x_m \in [a, b]$, асимптотически эквивалентно dn при $n \rightarrow \infty$.

2. Пусть G — компактная группа и X — пространство ее классов сопряженности (т. е. факторпространство пространства G по отношению эквивалентности, индуцированному внутренними автоморфизмами группы G). Пусть μ — некоторая мера на G , она индуцирует меру на X , которую мы будем обозначать также через μ . Имеет место следующее

Предложение 2. *Последовательность (x_n) элементов из X μ -равнораспределена тогда и только тогда, когда для каждого неприводимого характера χ группы G выполнено соотношение*

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n \chi(x_i) = \mu(\chi).$$

Отображение $C(X) \rightarrow C(G)$ устанавливает изоморфизм $C(X)$ с пространством центральных функций на G . А в силу теоремы Петера — Вейля неприводимые характеры группы G порождают плотное подпространство в $C(X)$. Следовательно, можно применить лемму 1. Доказательство закончено.

Следствие 1. *Пусть μ — мера Хаара на G с $\mu(G) = 1$. Тогда последовательность (x_n) элементов из X μ -равнораспределена, если и только если для каждого неприводимого характера χ группы G , $\chi \neq 1$, имеет место равенство*

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n \chi(x_i) = 0.$$

Это вытекает из предложения 2 и следующих фактов:

$$\mu(\chi) = \begin{cases} 0, & \text{если } \chi \text{ неприводим и } \neq 1, \\ 1, & \text{если } \chi = 1. \end{cases}$$

Следствие 2 (Г. Вейль [11]). Пусть $G = \mathbf{R}/\mathbf{Z}$ и μ — нормализованная мера Хаара на G . Последовательность (x_n) тогда и только тогда μ -равнораспределена, когда для каждого целого $t \neq 0$ имеет место соотношение

$$\sum_{n \leq N} e^{2\pi i t x_n} = o(N), \quad N \rightarrow \infty.$$

Для доказательства достаточно заметить, что неприводимые характеры группы \mathbf{R}/\mathbf{Z} — это отображения вида $x \mapsto e^{2\pi i mx}$, $m \in \mathbf{Z}$.

Д.2. Связь с L-функциями

Пусть G и X такие же, как и в примере 2: G — компактная группа и X — пространство ее классов сопряженности. Пусть x_v , $v \in \Sigma$, — семейство элементов из X , перенумерованных счетным множеством Σ , и пусть $v \mapsto Nv$ — функция на Σ со значениями в целых числах ≥ 2 .

Сделаем следующие *предположения*:

(1) Бесконечное произведение $\prod_{v \in \Sigma} \frac{1}{1 - (Nv)^{-s}}$ сходится

для всех $s \in \mathbf{C}$ с $\operatorname{Re}(s) > 1$ и продолжается до мероморфной функции на полуплоскость $\operatorname{Re}(s) \geq 1$, не имеющей ни нулей, ни полюсов, кроме простого полюса в $s = 1$.

(2) Пусть ρ — неприводимое представление группы G с характером χ ; положим

$$L(s, \rho) = \prod_{v \in \Sigma} \frac{1}{\det(1 - \rho(x_v)(Nv)^{-s})}.$$

Это произведение сходится при $\operatorname{Re}(s) > 1$ и продолжается до мероморфной функции на полуплоскость $\operatorname{Re}(s) \geq 1$, нигде не имеющей ни нулей, ни полюсов, кроме, быть может, точки $s = 1$.

Порядок функции $L(s, \rho)$ в $s = 1$ будет обозначаться через $-c_\chi$, так что если $L(s, \rho)$ имеет полюс (соответственно нуль) порядка m в $s = 1$, то $c_\chi = m$ (соответ-

ственno $c_\chi = -m$). При этих предположениях имеет место следующая

Теорема 1. (а) Число точек $v \in \Sigma$ с $Nv \leq n$ асимптотически эквивалентно $n/\log n$ при $n \rightarrow \infty$.

(б) Для каждого неприводимого характера χ группы G выполняется соотношение

$$\sum_{\substack{Nv \leq n \\ Nv}} \chi(x_v) = c_\chi n / \log n + o(n/\log n), \quad n \rightarrow \infty.$$

Стандартными рассуждениями эта теорема выводится из теоремы Винера — Икеары, см. Д.3 ниже.

Предположим теперь, что функция $v \mapsto Nv$ обладает следующим свойством:

(3) Существует такая константа C , что для каждого $n \in \mathbf{Z}$ число точек $v \in \Sigma$ с $Nv = n$ не превосходит C .

Тогда можно упорядочить элементы из Σ в последовательность $(v_i)_{i \geq 1}$ так, что если $i \leq j$, то $Nv_i \leq Nv_j$. (Это можно сделать, вообще говоря, многими способами.) Имеет смысл говорить тогда о равнораспределенности последовательности x_{v_i} . Пользуясь условием (3), легко показать, что она не зависит от выбора порядка на Σ . Из теоремы 1 и предложения 2 получаем:

Теорема 2. Элементы x_v , $v \in \Sigma$, равнораспределены в X относительно меры μ , такой, что для каждого неприводимого характера χ группы G

$$\mu(\chi) = c_\chi.$$

Следствие. Элементы x_v , $v \in \Sigma$, равнораспределены относительно нормализованной меры Хаара на G тогда и только тогда, когда $c_\chi = 0$ для каждого неприводимого характера $\chi \neq 1$ группы G , т. е. тогда и только тогда, когда для всех нетривиальных неприводимых характеров соответствующие L -функции голоморфны и не обращаются в нуль при $s = 1$.

Примеры. 1. Пусть G — группа Галуа конечного расширения Галуа L/K числового поля K , Σ — множество всех неразветвленных точек поля K , x_v — класс сопряженности элемента Фробениуса в точке $v \in \Sigma$ и Nv —

норма точки v , ср. 2.1. Тогда условия (1), (2) и (3) выполнены с $c_\chi = 0$ для любого неприводимого характера $\chi \neq 1$. Тривиально проверяется условие (3). Для проверки условия (1) заметим, что функция $L(s, 1)$ совпадает (с точностью до конечного числа членов) с дзета-функцией поля K , следовательно, имеет простой полюс в точке $s = 1$ и голоморфна в остальных точках прямой $\operatorname{Re}(s) = 1$ (см., например, Ленг [18], гл. VII); для доказательства (2) см. Артин [1], стр. 121. Таким образом, из теоремы 2 следует равнораспределенность элементов Фробениуса, т. е. теорема Чеботарева о плотности, ср. п. 2.2.

2. Пусть C — группа классов идеалей числового поля K и ρ — непрерывный гомоморфизм из C в некоторую компактную абелеву группу Ли G . Простое рассуждение (см. гл. III, п. 2.2) показывает тогда, что ρ почти всюду неразветвлен (т. е. если U_v — группа единиц K_v , то $\rho(U_v) = 1$ для почти всех v). Выберем элемент $\pi_v \in K$ с $v(\pi_v) = 1$. Если ρ неразветвлен в точке v , то $\rho(\pi_v)$ зависит только от v и мы положим $x_v = \rho(\pi_v)$. Сделаем следующее *предположение*:

(*) Гомоморфизм ρ отображает группу C^0 идеалей единичного объема на всю группу G .

(Напомним, что *объем* идеяля $a = (a_v)$ определяется как произведение нормализованных абсолютных значений его компонент a_v , см. Ленг [18] или Вейль [9].)

В таком случае элементы x_v равномерно распределены в G относительно нормализованной меры Хаара. Это следует (теорема 1) из того, что L -функции, соответствующие неприводимым характерам χ группы G , — это L -функции Гекке с грэссенхарактерами; они голоморфны и не обращаются в нуль при $\operatorname{Re}(s) \geq 1$, если $\chi \neq 1$, см. [18], гл. VII.

Замечание. Этот пример (принадлежащий, в сущности, Гекке) приведен в книге Ленга (loc. cit., гл. VIII, § 5) с той разницей, что вместо условия (*) Ленг накладывает условие „ ρ сюръективно“, которого недостаточно. Это приводит его к утверждению, что последовательность $(\log p)$ (а также последовательность

$(\log n)$) равномерно распределена по модулю 1; однако, как известно, эта последовательность не является равномерно распределенной ни для какой меры на \mathbf{R}/\mathbf{Z} (см. Полиа и Сёге [27]).

З (гипотетический пример). Пусть E — эллиптическая кривая, определенная над K , и пусть Σ — множество конечных точек v поля K , таких, что E имеет хорошую редукцию в v (см. п. 1.2 и гл. IV). Пусть $v \in \Sigma$, $l \neq p_v$ и F_v — класс сопряженности элемента Фробениуса v в $\text{Aut } T_l(E)$. Тогда собственные значения F_v являются алгебраическими числами, которые при вложении в \mathbf{C} определяют пары комплексно сопряженных чисел π_v и $\bar{\pi}_v$ с $|\pi_v| = (Nv)^{1/2}$. Следовательно, их можно записать в виде

$$\pi_v = (Nv)^{\frac{1}{2}} e^{i\varphi_v}, \quad \bar{\pi}_v = (Nv)^{\frac{1}{2}} e^{-i\varphi_v}, \quad 0 \leq \varphi_v \leq \pi.$$

С другой стороны, пусть $G = SU(2)$ — группа Ли унитарных 2×2 -матриц с определителем 1. Тогда каждый элемент пространства X классов сопряженности группы G содержит единственную матрицу вида $\begin{pmatrix} e^{i\Phi} & 0 \\ 0 & e^{-i\Phi} \end{pmatrix}$, $0 \leq \Phi \leq \pi$. Известно, что образ на X меры Хаара на G имеет вид $\frac{2}{\pi} \sin^2 \Phi d\Phi$. Кроме того, все неприводимые представления группы G исчерпываются m -ми симметрическими степенями ρ_m естественного представления ρ_1 степени 2.

Возьмем теперь в качестве x_v элемент из X , соответствующий углу $\varphi = \varphi_v$. Тогда L -функция представления ρ_m будет иметь вид

$$L_{\rho_m}(s) = \prod_v \prod_{a=0}^m \frac{1}{1 - e^{i(m-2a)\varphi_v} (Nv)^{-s}}.$$

Положим

$$L_m^1(s) = \prod_v \prod_{a=0}^m \frac{1}{1 - \pi_v^{m-a} \bar{\pi}_v^a (Nv)^{-s}}.$$

Тогда

$$L_{\rho_m}(s) = L_m^1(s - m/2).$$

Функция L_m^1 была рассмотрена Тейтом [38]. Он предположил, что для $m \geq 1$ она голоморфна и не обращается в нуль при $\operatorname{Re}(s) \geq 1 + m/2$ при условии, что кризисная E не имеет комплексного умножения. Если принять эту гипотезу, то из следствия теоремы 2 будет вытекать равномерная распределенность элементов x_v или, что эквивалентно, равномерная распределенность углов φ_v элементов Фробениуса в интервале $[0, \pi]$ с мерой $\frac{2}{\pi} \sin^2 \varphi d\varphi$ („гипотеза Сато -- Тейта“).

Возможно, что аналогичные результаты имеют место и для других l -адических представлений.

Д.3. Доказательство теоремы 1

Логарифмическая производная функции L имеет вид

$$L'/L = - \sum_{v, m \geq 1} \frac{\chi(x_v^m) \log(Nv)}{(Nv)^{ms}},$$

где x_v^m — класс сопряженности m -х степеней элементов из класса x_v . Это непосредственно видно из представления L в виде произведения

$$\prod_{i, v} \frac{1}{1 - \lambda_v^{(i)} (Nv)^{-s}},$$

где $\lambda_v^{(i)}$ — собственные значения элементов x_v в заданном представлении. Ряд

$$\sum_{v, m \geq 2} \frac{\log(Nv)}{|(Nv)^{ms}|}$$

сходится при $\operatorname{Re}(s) > 1/2$. В самом деле, достаточно показать, что

$$\sum_v \frac{\log(Nv)}{(Nv)^\sigma} < \infty,$$

если $\sigma > 1$; но этот ряд мажорируется рядом

$$(\text{const}) \times \sum_v \frac{1}{(Nv)^{\sigma+\varepsilon}}, \quad \varepsilon > 0.$$

С другой стороны, сходимость произведения $\prod_v \frac{1}{1-(Nv)^{-\sigma}}$ при $\sigma > 1$ показывает, что $\sum_v \frac{1}{(Nv)^\sigma} < \infty$ при $\sigma > 1$, откуда следует наше утверждение. Поэтому мы можем написать

$$L'/L = - \sum_v \frac{\chi(x_v) \log(Nv)}{(Nv)^s} + \varphi(s),$$

где $\varphi(s)$ — голоморфная функция при $\operatorname{Re}(s) > 1/2$. Более того, по предположению, L'/L можно продолжить на полу平面 $\operatorname{Re}(s) \geq 1$ до мероморфной функции, которая будет голоморфной всюду, кроме, возможно, простого полюса в точке $s = 1$ с вычетом $-c_\chi$. Следовательно, можно применить теорему Винера — Икеары (см. [2], стр. 123):

ТЕОРЕМА. Пусть $F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ — ряд Дирихле с комплексными коэффициентами. Предположим, что существует такой ряд Дирихле $F^+(s) = \sum_{n=1}^{\infty} \frac{a_n^+}{n^s}$ с положительными коэффициентами, что

- (а) $|a_n| \leq a_n^+$ для каждого n ;
- (б) ряд F^+ сходится при $\operatorname{Re}(s) > 1$;
- (в) функцию F^+ (соответственно F) можно продолжить до мероморфной функции на полу平面 $\operatorname{Re}(s) \geq 1$, не имеющей нигде полюсов, кроме (соответственно кроме, возможно) простого полюса в $s = 1$ с вычетом $c_+ > 0$ (соответственно c).

Тогда

$$\sum_{m \leq n} a_m = cn + o(n), \quad n \rightarrow \infty$$

(здесь $c = 0$, если F голоморфна в $s = 1$).

Применим эту теорему к ряду

$$F(s) = - \sum_v \frac{\chi(x_v) \log(Nv)}{(Nv)^s},$$

взяв в качестве F^+ ряд

$$d \sum_v \frac{\log(Nv)}{(Nv)^s},$$

где d — степень данного представления ρ ; это возможно, так как $\chi(x_v)$ является суммой комплексных чисел с абсолютным значением 1, поэтому $|\chi(x_v)| \leq d$; кроме того, ряд $\sum_v \frac{\log(Nv)}{(Nv)^s}$ отличается от логарифмической производной произведения $\prod \frac{1}{1 - (Nv)^{-s}}$ на функцию, голоморфную при $\operatorname{Re}(s) > 1/2$, как было показано выше. Следовательно, по теореме Винера — Икеары

$$\sum_{Nv \leq n} \chi(x_v) \log(Nv) = c_\chi n + o(n), \quad n \rightarrow \infty.$$

Суммированием по Абелю (см. [18], стр. 174, предложение 1) получаем

$$\sum_{Nv \leq n} \chi(x_v) = c_\chi n / \log n + o(n/\log n), \quad n \rightarrow \infty$$

и, в частности,

$$\sum_{Nv \leq n} 1 = n / \log n + o(n/\log n), \quad n \rightarrow \infty.$$

Следовательно,

$$\left(\sum_{Nv \leq n} \chi(x_v) \right) / \left(\sum_{Nv \leq n} 1 \right) \rightarrow c_\chi, \quad n \rightarrow \infty.$$

Осталось применить предложение 2, чтобы закончить доказательство.

ГЛАВА II

ГРУППЫ S_m

Всюду в этой главе K обозначает некоторое поле алгебраических чисел. Полю K мы сопоставляем проективное семейство (S_m) коммутативных алгебраических групп над \mathbf{Q} и показываем, что каждая группа S_m порождает некоторую строго согласованную систему рациональных l -адических представлений поля K . В следующей главе мы покажем, что каждое „локально алгебраическое“ абелево рациональное представление имеет описанный здесь вид.

§ 1. Предварительные результаты

1.1. Тор T

Пусть $T = R_{K/\mathbf{Q}}(\mathbf{G}_{m/K})$ — алгебраическая группа над \mathbf{Q} , полученная из мультиликативной группы \mathbf{G}_m ограничением поля скаляров K до \mathbf{Q} , см. Вейль [8], § 1.3. Для каждой коммутативной \mathbf{Q} -алгебры A точки алгебраической группы T образуют по определению мультиликативную группу $(K \otimes_{\mathbf{Q}} A)^*$ обратимых элементов кольца $K \otimes_{\mathbf{Q}} A$. В частности, $T(\mathbf{Q}) = K^*$. Если $[K : \mathbf{Q}] = d$, то группа T является d -мерным тором; это означает, что группа $T_{/\bar{\mathbf{Q}}} = T \otimes_{\mathbf{Q}} \bar{\mathbf{Q}}$, полученная из T расширением поля скаляров \mathbf{Q} до $\bar{\mathbf{Q}}$, изоморфна $G_{m/\bar{\mathbf{Q}}} \times \dots \times G_{m/\bar{\mathbf{Q}}}$ (d множителей). Точнее, пусть Γ — множество вложений поля K в $\bar{\mathbf{Q}}$. Каждый элемент $\sigma \in \Gamma$ продолжается до гомоморфизма $K \otimes_{\mathbf{Q}} \bar{\mathbf{Q}} \rightarrow \bar{\mathbf{Q}}$ и определяет, следовательно, морфизм $[\sigma]: T_{/\bar{\mathbf{Q}}} \rightarrow G_{m/\bar{\mathbf{Q}}}$. Тогда совокупность всех морфизмов $[\sigma]$ дает изоморфизм $T_{/\bar{\mathbf{Q}}} \rightarrow G_{m/\bar{\mathbf{Q}}} \times \dots \times G_{m/\bar{\mathbf{Q}}}$. Более того, морфизмы $[\sigma]$ об-

разуют базис группы характеров $X(T) = \text{Hom}_{\bar{\mathbb{Q}}}(T_{/\bar{\mathbb{Q}}}, \mathbf{G}_{m/\bar{\mathbb{Q}}})$ для группы T . Заметим, что группа Галуа $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ естественным образом действует на $X(T)$, а именно перестановкой морфизмов $[\sigma]$. (О соответствии между торами и модулями Галуа см., например, Оно [26].)

1.2. Факторы тора T

Пусть E — некоторая подгруппа группы $K^* = T(\mathbb{Q})$ и \bar{E} — ее замыкание в топологии Зарисского T . Пользуясь формулой $\bar{E} \times \bar{E} = \bar{E} \overline{\times E}$, легко убедиться, что \bar{E} является алгебраической подгруппой в T . Обозначим через T_E факторгруппу T/\bar{E} — это тоже некоторый тор над \mathbb{Q} . Его группа характеров $X_E = X(T_E)$ является подгруппой группы $X = X(T)$, состоящей из характеров, принимающих значение 1 на E . Пусть $\lambda = \prod_{\sigma \in \Gamma} [\sigma]^{\nu_\sigma}$ — произвольный характер тора T , тогда подгруппа X_E в X состоит из таких $\lambda \in X$, что $\prod \sigma(x)^{\nu_\sigma} = 1$ для всех $x \in E$.

Упражнение. а) Пусть K — квадратичное расширение поля \mathbb{Q} , так что $\dim T = 2$. Обозначим через E группу единиц поля K . Показать, что тор T_E двумерен (соответственно одномерен), если поле K мнимое (соответственно действительное).

б) Возьмем в качестве K кубическое поле с одним действительным и парой комплексных вложений, и пусть опять E — группа единиц (ранга 1). Показать, что $\dim T = 3$ и $\dim T_E = 1$. (Другие примеры см. в п. 3.3.)

1.3. Расширения групп

Пусть k — некоторое поле и A — коммутативная алгебраическая группа над k . Пусть

$$0 \rightarrow Y_1 \rightarrow Y_2 \rightarrow Y_3 \rightarrow 0 \tag{*}$$

— точная последовательность (абстрактных) коммутативных групп, где группа Y_3 конечна, и пусть

$$\epsilon: Y_1 \rightarrow A(k)$$

— гомоморфизм группы Y_1 в группу k -рациональных точек алгебраической группы A . Мы хотим построить алгебраическую группу B вместе с морфизмом алгебраических групп $A \rightarrow B$ и гомоморфизмом Y_2 в $B(k)$ так, чтобы выполнялись два условия:

(а) *диаграмма*

$$\begin{array}{ccc} Y_1 & \rightarrow & A(k) \\ \downarrow & & \downarrow \\ Y_2 & \rightarrow & B(k) \end{array}$$

коммутативна,

(б) *группа B „универсальна“ относительно условия (а).* Универсальность группы B означает, что для любой алгебраической группы B' над k и любых морфизмов $A \rightarrow B'$, $Y_2 \rightarrow B'(k)$, удовлетворяющих условию (а) (с B' вместо B), существует единственный морфизм алгебраических групп $f: B \rightarrow B'$, такой, что заданные отображения $A \rightarrow B'$ и $Y_2 \rightarrow B'(k)$ являются композициями соответствующих отображений для B с морфизмом f . (Иными словами, B — это „расслоенное произведение“ над Y_1 алгебраической группы A и „постоянной“ групповой схемы, определяемой группой Y_2 .)

Единственность B является следствием ее универсальности. Докажем ее существование. Для каждого элемента $y \in Y_3$ выберем некоторый представитель \bar{y} его прообраза в Y_2 . Для произвольных $y, y' \in Y_3$ имеем

$$\bar{y} + \bar{y}' = \overline{\bar{y} + y'} + c(y, y'),$$

где $c(y, y') \in Y_1$; коцепь c является двумерным коциклом, определяющим расширение (*). Обозначим через B несвязное объединение множества экземпляров A_y группы A , пронумерованных элементами $y \in Y_3$. Определим групповой закон на B посредством отображений

$$\pi_{y, y'}: A_y \times A_{y'} \rightarrow A_{y+y'}, \quad y, y' \in Y_3,$$

задаваемых сложением в A с последующим сдвигом на $c(y, y')$. Легко проверить, что B обладает требуемым универсальным свойством, а отображения $A \rightarrow B$ и $Y_2 \rightarrow B(k)$ определяются следующим образом:

$A \rightarrow B$ — это естественное отображение $A \rightarrow A_0$ с последующим сдвигом на $-c(0, 0)$,

$Y_2 \rightarrow B(k)$ переводит элемент $\bar{y} + z$, $y \in Y_3$, $z \in Y_1$, в образ элемента z в A_y ,

Отметим, что для любого расширения k' поля k имеет место точная последовательность

$$0 \rightarrow A(k') \rightarrow B(k') \rightarrow Y_3 \rightarrow 0$$

и коммутативная диаграмма

$$\begin{array}{ccccccc} 0 & \rightarrow & Y_1 & \rightarrow & Y_2 & \rightarrow & Y_3 \rightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \rightarrow & A(k') & \rightarrow & B(k') & \rightarrow & Y_3 \rightarrow 0 \end{array}$$

Алгебраическая группа B является, таким образом, некоторым *расширением* „постоянной“ алгебраической группы Y_3 при помощи алгебраической группы A .

Замечания. 1) Пусть k' — некоторое расширение поля k и $A' = A \times_k k'$. Тогда предыдущая конструкция применима к алгебраической k' -группе A' , точной последовательности (*) и отображению $Y_1 \rightarrow A(k) \rightarrow A'(k')$. Полученная таким образом группа B' канонически изоморфна группе $B \times_k k'$. Это видно, например, из явного построения групп B и B' .

2) Мы будем пользоваться предыдущей конструкцией только в случае, когда $\text{char } k = 0$ и A — некоторый тор. Расширенная группа B является тогда „группой мультиплекативного типа“: это означает, что после подходящего конечного расширения основного поля B становится изоморфной произведению тора и конечной абелевой группы. Такая группа однозначно определяется своей группой характеров $X(B) = \text{Hom}_{\bar{k}}(\bar{B}_{/\bar{k}}, \mathbf{G}_{m/\bar{k}})$, являющейся модулем Галуа конечного типа над \mathbf{Z} . В нашем случае группа $X(B)$ может быть описана еще как множество пар (φ, χ) , где $\varphi: Y_2 \rightarrow \bar{k}^*$ — некоторый гомоморфизм, а $\chi \in X(A)$ — такой элемент, что $\varphi(y_1) = \chi(y_1)$ для всех $y_1 \in Y_1$. Отметим, что так мы получаем некоторую другую конструкцию группы B .

Упражнения. а) Пусть k' — коммутативная k -алгебра, отличная от 0 , и $\text{Spec } k'$ связан (т. е. k'

содержит только два идемпотента: 0 и 1). Показать, что тогда существует точная последовательность вида

$$0 \rightarrow A(k') \rightarrow B(k') \rightarrow Y_3 \rightarrow 0.$$

б) Что получится, если $\text{Spec } k'$ не будет связным?

§ 2. Построение групп T_m и S_m

2.1. Идели и классы идеалей

В главе I, п. 2.1, мы определили множество Σ_K конечных точек числового поля K . Пусть теперь Σ_K^∞ — это множество классов эквивалентности архimedовых абсолютных значений поля K и $\bar{\Sigma}_K$ — объединение Σ_K и Σ_K^∞ . Для каждого $v \in \bar{\Sigma}_K$ через K_v обозначается *пополнение* поля K относительно соответствующего нормирования. Если $v \in \Sigma_K^\infty$, то $K_v = \mathbf{R}$ или $K_v = \mathbf{C}$; если $v \in \Sigma_K$, то K_v снабжено ультраметрикой. Группу единиц поля K_v мы будем обозначать через U_v . Группа идеалей I поля K по определению является подгруппой произведения $\prod_{v \in \bar{\Sigma}_K} K_v^*$, состоящей из таких семейств (a_v) ,

что $a_v \in U_v$ для почти всех v : она снабжена тзкой топологией, в которой подгруппа (с топологией произведения)

$$\prod_{v \in \Sigma_K^\infty} K_v^* \times \prod_{v \in \Sigma_K} U_v$$

открыта. Вложим K^* в I , сопоставляя элементу $a \in K^*$ идеаль (a_v) , где $a_v = a$ для всех v . Тогда на K^* индуцируется дискретная топология. Факторгруппа $C = I/K^*$ называется *группой классов идеалей* поля K . (См. по этому поводу Касселс — Фрёлих [15], Ленг [18] или Вейль [9].)

Пусть S — конечное подмножество в Σ_K . Тогда *модулем носителя* S мы называем любое семейство $m = (m_v)_{v \in S}$, где m_v — целые числа ≥ 1 . Если $v \in \bar{\Sigma}_K$ и m — модуль носителя S , то через $U_{v,m}$ мы будем

обозначать связную компоненту K_v^* , если $v \in \Sigma_K^\infty$, подгруппу группы U_v , состоящую из таких элементов $u \in U_v$, что $v(1-u) \geq m_v$, если $v \in S$, и U_v , если $v \in \Sigma_K \setminus S$. Группа $U_m = \prod_v U_{v,m}$ открыта в группе I .

Пусть E — группа единиц поля K , положим $E_m = E \cap U_m$. Подгруппа E_m имеет конечный индекс в группе E . (Обратно, согласно теореме Шевалле ([44], см. также [28], п. 3.5) каждая подгруппа конечного индекса в E содержит E_m для подходящего модуля m .)

Пусть $I_m = I/U_m$ и $C_m = I/K^*U_m = C/(\text{Im } U_m)$. Тогда имеет место точная последовательность групп

$$1 \rightarrow K^*/E_m \rightarrow I_m \rightarrow C_m \rightarrow 1.$$

Здесь группа C_m конечна; в самом деле, образ U_m в C открыт, следовательно, содержит связную компоненту D группы C , а группа C/D , как известно (см. [18], [8]), компактна. Более того, любая открытая подгруппа в I содержит какую-нибудь подгруппу U_m , следовательно, C/D является *проективным пределом* групп C_m . Теория полей классов (см. например, Касселс — Фрёлих [15]) устанавливает изоморфизм группы $C/D = \varprojlim C_m$ с группой

Галуа G^{ab} максимального абелева расширения поля K .

Замечание. Более классическое определение групп C_m таково. Пусть Ids_S — группа дробных идеалов поля K , взаимно простых с S , и $P_{S,m}$ — подгруппа главных идеалов вида (γ) , где γ всюду положительно и $\gamma \equiv 1 \pmod{m}$ (т. е. γ принадлежит к $U_{v,m}$ для всех $v \in S$ и $v \in \Sigma_K^\infty$). Положим $\text{Cl}_m = \text{Ids}_S/P_{S,m}$. Мы имеем тогда точную последовательность

$$1 \rightarrow P_{S,m} \rightarrow \text{Ids}_S \rightarrow \text{Cl}_m \rightarrow 1;$$

для каждого $a = \prod_{v \notin S} v^{a_v} \in \text{Ids}_S$ выберем некоторый идеаль $a = (a_v)$ с $a_v \in U_{v,m}$, если $v \in S$ или $v \in \Sigma_K^\infty$, и $v(a_v) = a_v$, если $v \in \Sigma_K \setminus S$. Образ a в $I_m = I/U_m$ зависит только от a . Мы получаем, таким образом, гомоморфизм $g: \text{Ids}_S \rightarrow I_m$. Легко проверить, что g продолжается до

коммутативной диаграммы

$$\begin{array}{ccccccc} 1 & \rightarrow & P_{S_m} & \rightarrow & \text{Id}_S & \rightarrow & \text{Cl}_m \rightarrow 1 \\ & & \downarrow & & \downarrow g & & \downarrow f \\ 1 & \rightarrow & K^*/E_m & \rightarrow & I_m & \rightarrow & C_m \rightarrow 1 \end{array}$$

и что $f: \text{Cl}_m \rightarrow C_m$ является изоморфизмом. Следовательно, C_m можно отождествить с группой классов идеалов по $\text{mod } m$ (это еще раз показывает, что она конечна).

2.2. Группы T_m и S_m

Воспользуемся теперь конструкцией п. 1.3. Возьмем в качестве точной последовательности (*) последовательность

$$1 \rightarrow K^*/E_m \rightarrow I_m \rightarrow C_m \rightarrow 1,$$

а в качестве A — алгебраическую группу $T_m = T/\bar{E}_m$, где E_m — группа, определенная в предыдущем пункте, T — это тор $R_{K/\mathbb{Q}}(\mathbf{G}_{m/K})$, определенный в п. 1.1, и E_m — замыкание в топологии Зарисского группы E в T ; ср. п. 1.2.

Тогда в качестве B мы получаем алгебраическую \mathbb{Q} -группу S_m , заданную вместе с морфизмом алгебраических групп $T_m \rightarrow S_m$ и гомоморфизмом групп $e: I_m \rightarrow S_m(\mathbb{Q})$. Имеем точную последовательность

$$1 \rightarrow T_m \rightarrow S_m \rightarrow C_m \rightarrow 1$$

(C_m отождествлена с соответствующей постоянной алгебраической группой) и коммутативную диаграмму

$$\begin{array}{ccccccc} 1 & \rightarrow & K^*/E_m & \rightarrow & I_m & \rightarrow & C_m \rightarrow 1 \\ & & \downarrow & & \downarrow e & & \downarrow \text{id} \\ 1 & \rightarrow & T_m(\mathbb{Q}) & \rightarrow & S_m(\mathbb{Q}) & \rightarrow & C_m \rightarrow 1 \end{array} \quad (**)$$

Замечание. Пусть m' — некоторый другой модуль, предположим, что $m' \geq m$, т. е. $\text{Supp } m' \supset \text{Supp } m$ и $m'_v \geq m_v$, если $v \in \text{Supp } m$. Из включения $U_{m'} \subset U_m$ вытекает существование отображений $T_{m'} \rightarrow T_m$ и $I_{m'} \rightarrow I_m$.

и, следовательно, существование морфизма $S_{m'} \rightarrow S_m$. Поэтому группы S_m образуют проективную систему: их пределом является некоторая проалгебраическая группа над \mathbf{Q} — расширение проконечной группы $C/D = \varprojlim C_m$ при помощи тора.

Упражнения. 1) Пусть $\bar{E}_m(\mathbf{Q})$ — замыкание в топологии Зарисского группы E_m в $K^* = T(\mathbf{Q})$. Показать, что ядро гомоморфизма $\epsilon_m: I/U_m \rightarrow S_m(\mathbf{Q})$ совпадает с образом гомоморфизма $\bar{E}_m(\mathbf{Q}) \rightarrow I/U_m$.

2) Пусть $H_{m'/m}$ — ядро морфизма $S_{m'} \rightarrow S_m$, где $m' \geq m$:
а) показать, что $H_{m'/m}$ является конечной подгруппой группы $S_{m'}(\mathbf{Q})$ и что она содержится в образе гомоморфизма $\epsilon_{m'}$;

б) построить точную последовательность (ср. упр. 1)

$$1 \rightarrow (E_m \cap \bar{E}_{m'}(\mathbf{Q}))/E_{m'} \rightarrow U_m/U_{m'} \rightarrow H_{m'/m} \rightarrow 1.$$

2.3. Каноническое l -адическое представление со значениями в S_m

Пусть m — некоторый модуль, и пусть l — простое число. Рассмотрим гомоморфизм $\epsilon: I \rightarrow I_m \rightarrow S_m(\mathbf{Q})$, определенный в п. 2.2. Обозначим через $\pi: T \rightarrow S_m$ морфизм алгебраических групп $T \rightarrow T_m \rightarrow S_m$; на точках со значениями в \mathbf{Q}_l он определяет гомоморфизм

$$\pi_l: T(\mathbf{Q}_l) \rightarrow S_m(\mathbf{Q}_l),$$

так как $K \otimes \mathbf{Q}_l = \prod_{v|l} K_v$, то группа $T(\mathbf{Q}_l)$ может быть отождествлена с группой $K_l^* = \prod_{v|l} K_v^*$ и, следовательно, с некоторым прямым множителем группы иделий I . Пусть pr_l — проекция группы I на этот множитель. Тогда отображение

$$a_l = \pi_l \circ \text{pr}_l: I \rightarrow T(\mathbf{Q}_l) \rightarrow S_m(\mathbf{Q}_l)$$

является непрерывным гомоморфизмом.

Лемма. Гомоморфизмы a_l и ϵ совпадают на K^* .

Это тривиально следует из коммутативности диаграммы $(**)$ п. 2.2.

Определим теперь гомоморфизм $\varepsilon_l: I \rightarrow S_m(\mathbf{Q}_l)$ формулой

$$\varepsilon_l(a) = \varepsilon(a) a_l(a^{-1}), \quad (***)$$

т. е. $\varepsilon_l = \varepsilon \circ a_l^{-1}$. (Для $a \in I$ через a_l будем обозначать l -компоненту элемента a . Тогда $\varepsilon_l(a) = \varepsilon(a) \pi_l(a_l^{-1})$.) В силу леммы ε_l тривиален на K^* и, следовательно, определяет гомоморфизм $C \rightarrow S_m(\mathbf{Q}_l)$. Так как $S_m(\mathbf{Q}_l)$ вполне несвязна (это l -адическая группа Ли), последний гомоморфизм тривиален на связной компоненте D группы C . Мы уже упоминали, что C/D можно отождествить с группой Галуа G^{ab} максимального абелева расширения поля K . Таким образом, мы приходим, наконец, к гомоморфизму $\varepsilon_l: G^{ab} \rightarrow S_m(\mathbf{Q}_l)$, т. е. к некоторому l -адическому представлению поля K со значениями в S_m (см. гл. I, п. 2.3).

Это представление является *рациональным* в смысле гл. I, п. 2.3. Точнее, пусть $v \notin \text{Supp } \mathfrak{m}$, и пусть $f_v \in I$ — идеяль, v -компонента которого совпадает с униформизирующим элементом поля K_v , а все остальные его компоненты равны 1; пусть $F_v = \varepsilon(f_v)$ — образ идеяля f_v в $S_m(\mathbf{Q})$. В этих обозначениях имеет место

ПРЕДЛОЖЕНИЕ. а) Представление $\varepsilon_l: G^{ab} \rightarrow S_m(\mathbf{Q}_l)$ является рациональным представлением со значениями в S_m ;

б) ε_l неразветвлено всюду вне $\text{Supp } \mathfrak{m} \cup S_l$, где $S_l = \{v \mid p_v = l\}$;

в) если $v \notin \text{Supp } \mathfrak{m} \cup S_l$, то элемент Фробениуса F_{v, ε_l} (см. гл. I, п. 2.3) совпадает с $F_v \in S_m(\mathbf{Q})$.

Доказательство. Известно, что изоморфизм полей классов $C/D \xrightarrow{\sim} G^{ab}$ отображает K_v^* (соответственно U_v) в плотную подгруппу группы разложения точки v в группе G^{ab} (соответственно в группу инерции точки v в G^{ab}) и что униформизирующий элемент f_v поля K_v^* отображается в класс Фробениуса точки v .

Если $v \notin \text{Supp } \mathfrak{m}$ и $a \in U_v$, то $\varepsilon(a) = 1$; если, кроме того, $p_v \neq l$, то $a_l(a) = 1$. Следовательно, $\varepsilon_l(a) = 1$ и ε_l

неразветвлено в v , это доказывает утверждение б). Для каждой такой точки v имеем $\varepsilon_l(f_v) = \varepsilon(f_v) = F_v$, т. е. справедливо утверждение в), а из него следует а).

Следствие. Представления ε_l для всех l образуют систему строго согласованных l -адических представлений со значениями в S_m .

Мы видим, таким образом, что исключительное множество этой системы содержится в $\text{Supp } m$; упражнение 2 доставляет пример системы, для которой оно отлично от $\text{Supp } m$.

Замечание. По построению $\varepsilon_l: I \rightarrow S_m(\mathbf{Q}_l)$ на открытой подгруппе $U_{l,m} = \prod_{v \mid l} U_{v,m}$ группы K_l^* задается формулой $x \mapsto \pi_l(x^{-1})$. Следовательно, $\text{Im } \varepsilon_l$ содержит $U_{l,m} \subset T_m(\mathbf{Q}_l) \subset S_m(\mathbf{Q}_l)$ и является открытой подгруппой в $S_m(\mathbf{Q}_l)$. Эта открытая подгруппа, как отмечалось выше, отображается на все C_m . Отсюда следует, в частности, что $\text{Im } \varepsilon_l$ плотно в S_m относительно топологии Зарисского.

Упражнения. 1) Пусть $K = \mathbf{Q}$, $\text{Supp } m = \emptyset$.

(а) Показать, что $E_m = \{1\}$, $C_m = \{1\}$, следовательно, $T_m = S_m = \mathbf{G}_m$ и $S_m(\mathbf{Q}) = \mathbf{Q}^*$, $S_m(\mathbf{Q}_l) = \mathbf{Q}_l^*$.

(б) Показать, что группа I является прямым произведением своих подгрупп I_m и \mathbf{Q}^* ; следовательно, любой элемент $a \in I$ может быть записан в виде

$$a = u\gamma, \quad u \in U_m, \quad \gamma \in \mathbf{Q}^*.$$

Показать, что если $a = (a_p)$, то

$$\varepsilon(a) = \gamma = \text{sgn } a_\infty \prod_p p^{v_p(a_p)}.$$

(в) Показать, что $\varepsilon_l(a) = \gamma a_l^{-1}$ и $F_p = p$.

(г) Показать, что ε_l совпадает с характером χ_l гл. I, 1.2.

2) Пусть $K = \mathbf{Q}$, $\text{Supp } m = \{2\}$ и $m_2 = 1$. Показать, что группы E_m , C_m , T_m , S_m совпадают с соответствующими группами из упражнения 1, и, следовательно, исключительное множество соответствующей системы пусто.

2.4. Линейные представления групп S_m

Напомним прежде всего некоторые хорошо известные факты из теории представлений алгебраических групп.

а) Пусть k — поле характеристики 0, H — некоторая аффинная коммутативная алгебраическая группа над k . Пусть $X(H) = \text{Hom}_{\bar{k}}(H_{/\bar{k}}, \mathbf{G}_{m/\bar{k}})$ — группа характеров (степени 1) группы H . Здесь мы будем записывать характеры из $X(H)$ мультипликативно. Группа $G = \text{Gal}(\bar{k}/k)$ действует на $X(H)$.

Пусть Λ — аффинная алгебра группы H и $\bar{\Lambda} = \Lambda \otimes_k \bar{k}$ — соответствующая алгебра для $H_{/\bar{k}}$. Каждый элемент $\chi \in X(H)$ может быть отождествлен с некоторым обратимым элементом алгебры $\bar{\Lambda}$. Следовательно, по линейности, имеем гомоморфизм

$$\alpha: \bar{k}[X(H)] \rightarrow \bar{\Lambda},$$

где $\bar{k}[X(H)]$ — групповая алгебра группы $X(H)$ над \bar{k} . Он будет даже G -гомоморфизмом, если действие G определить формулой $s(\sum a_\chi \chi) = \sum s(a_\chi) s(\chi)$, где $a_\chi \in \bar{k}$ и $\chi \in X(H)$. Хорошо известно (линейная независимость характеров), что гомоморфизм α инъективен. Он биективен тогда и только тогда, когда группа H мультипликативного типа [см. п. 1.3, замечание 2)]. Следовательно, мы можем отождествить $\bar{k}[X(H)]$ с некоторой подалгеброй алгебры $\bar{\Lambda}$.

б) Пусть V — конечномерное векторное пространство над k , и пусть

$$\varphi: H \rightarrow GL_V$$

— некоторое линейное представление группы H в V . Предположим, что φ полупросто (это всегда так, если группа H имеет мультипликативный тип). Сопоставим φ его след

$$\theta_\varphi = \sum n_\chi(\varphi) \chi$$

в $\mathbf{Z}[X(H)]$, где $n_\chi(\varphi)$ — кратность характера χ в разложении φ над \bar{k} . Для любой точки $h \in H$ (со значением

в произвольной коммутативной k -алгебре) имеем $\theta_\varphi(h) = \text{Tr } \varphi(h)$. Пусть $\text{Rep}_k(H)$ — множество классов изоморфизмов линейных полупростых представлений группы H . Расширение поля скаляров k до k_1 определяет отображение $\text{Rep}_k(H) \rightarrow \text{Rep}_{k_1}(H_{/k_1})$, которое, как легко видеть, инъективно. Будем говорить, что элемент из $\text{Rep}_{k_1}(H_{/k_1})$ может быть определен над k , если он принадлежит образу этого отображения.

ПРЕДЛОЖЕНИЕ 1. Отображение $\varphi \mapsto \theta_\varphi$ определяет биективное соответствие между $\text{Rep}_k(H)$ и множеством элементов $\theta = \sum n_\chi \chi$ из $\mathbf{Z}[\text{X}(H)]$, обладающих свойствами:

- (а) θ инвариантен относительно G (т. е. $n_\chi = n_{s(\chi)}$ для всех $s \in G$, $\chi \in \text{X}(H)$),
- (б) $n_\chi \geq 0$ для каждого $\chi \in \text{X}(H)$.

Доказательство. Инъективность отображения $\varphi \mapsto \theta_\varphi$ хорошо известна (и даже не зависит от коммутативности H). Чтобы доказать сюръективность, рассмотрим сначала случай, когда θ имеет вид $\theta = \sum \chi^{(i)}$, где $\chi^{(i)}$ — полное множество различных сопряженных к χ характеров из $\text{X}(H)$. Пусть $G(\chi)$ — стационарная подгруппа в G для характера χ , тогда

$$\theta = \sum_{s \in G/G(\chi)} s(\chi). \quad (*)$$

Обозначим через k_χ подполе в \bar{k} , соответствующее подгруппе $G(\chi)$, тогда k_χ является наименьшим подполем, для которого $\chi \in \Lambda \otimes k_\chi$. Рассмотрим χ как представление степени 1 группы $H_{/k_\chi}$. Ограничиваая поле скаляров до k , получаем некоторое представление φ группы H степени $[k_\chi : k]$. Легко видеть, что след θ_φ представления φ равен θ . Сюръективность отображения $\varphi \mapsto \theta_\varphi$ следует теперь из того факта, что любой элемент θ , удовлетворяющий условиям (а) и (б), является суммой элементов вида (*).

Следствие. Для того чтобы $\varphi_1 \in \text{Rep}_{k_1}(H_{/k_1})$ можно было определить над k , необходимо и достаточно, чтобы элемент $\theta_{\varphi_1} \in \Lambda \otimes_k k_1$ принадлежал Λ .

(в) Возвратимся к группам S_m

Предложение 2. Пусть k_1 — некоторое расширение поля k , и пусть $\varphi \in \text{Rep}_{k_1}(S_{m/k_1})$. Тогда следующие свойства эквивалентны:

- (i) представление φ может быть определено над k ,
- (ii) для каждого $v \notin \text{Supp } \varphi$ коэффициенты характеристического многочлена $\varphi(F_v)$ принадлежат k ,
- (iii) существует такое множество Σ точек поля k плотности 1 (см. гл. I, п. 2.2), что $\text{Tr } \varphi(F_v) \in k$ для всех $v \in \Sigma$.

Доказательство. Импликации $(i) \Rightarrow (ii) \Rightarrow (iii)$ тривиальны. Чтобы доказать $(iii) \Rightarrow (i)$, нам понадобится следующая

Лемма Множество элементов Фробениуса F_v , $v \in \Sigma$, плотно в S_m относительно топологии Зарисского.

Доказательство. Пусть X — множество всех F_v , $v \in \Sigma$, и l — простое число. Пусть $\bar{X} \subset S_m$ (соответственно $\bar{X}_l \subset S_m(\mathbf{Q}_l)$) — замыкание множества X в топологии Зарисского (соответственно в l -адической топологии). Очевидно, что $\bar{X}_l \subset \bar{X}(\mathbf{Q}_l)$. С другой стороны, из теоремы Чеботарева (см. гл. I, п. 2.2) следует, что $\bar{X}_l = \text{Im } \varepsilon_l$ (см. п. 2.3). Но множество $\text{Im } \varepsilon_l$ плотно в топологии Зарисского на S_m (см. замечание в 2.3). Поэтому $\bar{X} = S_m$, что доказывает лемму.

Осталось доказать, что $(iii) \Rightarrow (i)$. Пусть θ_{φ} — след представления φ в $\Lambda \otimes_k k_1$, где Λ — аффинная алгебра группы $H = S_{m/k}$, и пусть $\{l_a\}$ — базис векторного k -пространства k_1 с $l_{a_0} = 1$ для некоторого индекса a_0 . Имеем $\theta_{\varphi} = \sum \lambda_a \otimes l_a$, $\lambda_a \in \Lambda$, следовательно, $\text{Tr } \varphi(h) = \theta_{\varphi}(h) = \sum \lambda_a(h) l_a$ для всех $h \in H(k_1)$. Положим $h = F_v$, где $v \in \Sigma$. Поскольку F_v принадлежит $H(k)$, то $\lambda_a(F_v) \in k$ для всех a , а так как $\text{Tr } \varphi(F_v) \in k$, то $\lambda_a(F_v) = 0$ для всех $a \neq a_0$. По лемме множество $\{F_v\}$, $v \in \Sigma$, плотно

по Зарискому в H , следовательно, $\lambda_a = 0$ при $a \neq a_0$ и $\theta_\Phi = \lambda_{a_0}$ принадлежит Λ . Утверждение (i) вытекает теперь из следствия предложения 1.

Упражнение. Показать, что характеристы группы S_m находятся во взаимно однозначном соответствии с гомоморфизмами $\chi: I \rightarrow \bar{\mathbf{Q}}^*$, обладающими следующими двумя свойствами:

(a) $\chi(x) = 1$, если $x \in U_m$;

(б) для каждого вложения $\sigma: K \rightarrow \bar{\mathbf{Q}}$ существует такое целое число $n(\sigma)$, что

$$\chi(x) = \prod_{\sigma \in \Gamma} \sigma(x)^{n(\sigma)}$$

для всех $x \in K^*$.

2.5. l -адические представления, ассоциированные с линейным представлением группы S_m

1) l -адический случай. Пусть V_l — конечно-мерное векторное \mathbf{Q}_l -пространство и

$$\varphi: S_{m/\mathbf{Q}_l} \rightarrow GL_{V_l}$$

— линейное представление группы S_{m/\mathbf{Q}_l} в V_l . Оно определяет гомоморфизм групп \mathbf{Q}_l -точек

$$\varphi: S_m(\mathbf{Q}_l) \rightarrow GL_{V_l}(\mathbf{Q}_l) = \text{Aut } V_l,$$

который непрерывен в l -адической топологии этих групп.

Композиция его с отображением $\varepsilon_l: G^{ab} \rightarrow S_m(\mathbf{Q}_l)$, определенным в п. 2.3, дает отображение

$$\varphi_l = \varphi \circ \varepsilon_l: G^{ab} \rightarrow \text{Aut } V_l,$$

т. е. некоторое абелево l -адическое представление поля K в V_l .

Предложение. а) Представление φ_l полупросто.

б) Пусть $v \in \Sigma_K$, $v \notin \text{Supp } m$ и $p_v \neq l$, тогда φ_l неразветвлено в v и соответствующий элемент Фробениуса $F_{v, \varphi_l} \in \text{Aut } V_l$ равен $\varphi(F_v)$, где F_v обозначает элемент группы $S_m(\mathbf{Q})$, определенный в п. 2.3.

в) Представление φ_l рационально (см. гл. I, п. 2, 3) тогда и только тогда, когда φ может быть определено над \mathbf{Q} (см. п. 2.4).

Так как S_m — группа мультиликативного типа, то все ее представления могут быть приведены к диагональной форме при подходящем расширении основного поля, откуда следует а). Утверждение б) следует из п. 2.3, а утверждение в) — из предложения 2 п. 2.4.

Замечание. Отождествим φ_l с соответствующим гомоморфизмом группы идеалей I в $\text{Aut } V_l$. Тогда

г) $\text{Ker } \varphi_l$ содержит $U_{v, m}$, если $v \notin \text{Supp } \mathfrak{m}$, $p_v \neq l$,

д) определим $\varphi_T: T_{/\mathbf{Q}_l} \rightarrow GL_{V_l}$ как композицию морфизма $T_{/\mathbf{Q}_l} \rightarrow S_{m/\mathbf{Q}_l}$ с φ . Тогда если x принадлежит открытой подгруппе $U_{l, m} = \prod_{v \mid l} U_{v, m}$ группы $T(\mathbf{Q}_l)$, то

$$\varphi_l(x) = \varphi_T(x^{-1}).$$

Эти свойства легко следуют из аналогичных свойств для ε_l .

2) Рациональный случай. Пусть теперь V_0 — конечномерное векторное пространство над \mathbf{Q} и $\varphi_0: S_m \rightarrow GL_{V_0}$ — линейное представление группы S_m . Для каждого простого числа l мы можем применить предыдущую конструкцию к представлению $\varphi_{0/l}: S_{m/\mathbf{Q}_l} \rightarrow GL_{V_l}$, где $V_l = V_0 \otimes \mathbf{Q}_l$. В результате получим l -адическое представление $\varphi_l: G^{\text{ab}} \rightarrow \text{Aut } V_l$.

ТЕОРЕМА. 1) Семейство (φ_l) образует строго согласованную систему рациональных абелевых полупростых представлений. Исключительное множество этой системы содержится в $\text{Supp } \mathfrak{m}$.

2) Для каждого $v \notin \text{Supp } \mathfrak{m}$ его элемент Фробениуса относительно системы (φ_l) совпадает с элементом $\varphi_0(F_v)$ в $\text{Aut } V_0$.

3) Существует бесконечно много простых чисел l , таких, что φ_l диагонализируемо над \mathbf{Q}_l .

Первые два утверждения непосредственно следуют из предыдущего предложения. Чтобы доказать третье,

заметим прежде всего, что существует конечное расширение E поля \mathbf{Q} , над которым ϕ_0 диагонализируемо. Если простое число l полностью распадается в E , то можно вложить E в \mathbf{Q}_l и ϕ_l также будет диагонализируемым. Утверждение 3) следует теперь из хорошо известного факта, что существует бесконечно много таких l (это является, например, следствием теоремы Чеботарева, см. гл. I, п. 2.2).

Замечание. Элементы Фробениуса $\phi_0(F_v) \in \text{Aut } V_0$ можно определять также с помощью гомоморфизма

$$\phi_0 \circ \varepsilon: I \rightarrow S_m(\mathbf{Q}) \rightarrow \text{Aut } V_0.$$

Отметим, что их собственные значения порождают некоторое *конечное расширение* поля \mathbf{Q} : в самом деле, все они содержатся в любом поле, над которым ϕ_0 может быть приведено к диагональному виду.

Упражнения. 1) Пусть $\phi_0: S_m \rightarrow GL_{V_0}$ — линейное представление группы S_m и l — простое число.

а) Показать, что замыкание в топологии Зарисского образа $\text{Im } \phi_l$ является алгебраической группой $\phi_0(S_m)$. (Использовать тот факт, что $\text{Im } \varepsilon_l$ плотен в S_m в топологии Зарисского, см. п. 2.3.)

б) Пусть s_m — алгебра Ли группы S_m и $\phi_0(s_m)$ — ее образ при гомоморфизме ϕ_0 , т. е. алгебра Ли группы $\phi_0(S_m)$. Показать, что алгебра Ли l -адической группы Ли $\text{Im } \phi_l$ совпадает с $\phi_0(s_m) \otimes \mathbf{Q}_l$. (Использовать тот факт, что $\text{Im } \varepsilon_l$ открыто в $S_m(\mathbf{Q}_l)$, см. п. 2.3.)

2) а) Показать, что существует единственное одномерное представление

$$N: S_m \rightarrow \mathbf{G}_m,$$

такое, что $N(F_v) = Nv \in \mathbf{Q}^*$ для всех $v \notin \text{Supp } m$.

б) Показать, что морфизм $T \rightarrow S_m \xrightarrow{N} \mathbf{G}_m$ индуцируется норменным отображением из K в \mathbf{Q} .

в) Показать, что l -адическое представление, определяемое представлением N , изоморфно представлению $V_l(\mu)$, определенному в гл. I, п. 1.2.

2.6. Другая конструкция

Пусть $\varphi_0: S_m \rightarrow GL_{V_0}$ означает то же, что и в 2.5. Если мы скомпанием φ_0 с отображением $\varepsilon: I \rightarrow S_m(\mathbf{Q})$, определенным в п. 2.4, то получим некоторый гомоморфизм

$$\varphi_0 \circ \varepsilon: I \rightarrow GL_{V_0}(\mathbf{Q}) = \text{Aut } V_0.$$

С другой стороны, имеет место следующее

ПРЕДЛОЖЕНИЕ. Пусть $f: I \rightarrow \text{Aut } V_0$ — некоторый гомоморфизм. Тогда для существования гомоморфизма $\varphi_0: S_m \rightarrow GL_{V_0}$ со свойством $\varphi_0 \circ \varepsilon = f$ необходимо и достаточно выполнение следующих условий:

- а) Ядро гомоморфизма f содержит U_m .
- б) Существует такой морфизм алгебраических групп $\psi: T \rightarrow GL_{V_0}$, что $\psi(x) = f(x)$ для каждого $x \in K^* = T(\mathbf{Q})$.

Более того, гомоморфизм φ_0 определен однозначно.

Доказательство. Необходимость условий (а) и (б) тривиальна. Докажем достаточность. Если f обладает свойствами (а) и (б), то он определяет гомоморфизм $I/U_m \rightarrow \text{Aut } V_0$. С другой стороны, так как f и ψ согласованы на K^* , морфизм ψ равен 1 на $E_m = K^* \cap U_m$, следовательно, и на замыкании в топологии Зарисского \bar{E}_m . Это означает, что ψ пропускается через

$$T \rightarrow T_m \rightarrow GL_{V_0}.$$

По свойству универсальности S_m (см. п. 1.3 и 2.2) отображения $I/U_m \rightarrow GL_{V_0}(\mathbf{Q})$ и $T_m \rightarrow GL_{V_0}$ определяют морфизм алгебраических групп $\varphi_0: S_m \rightarrow GL_{V_0}$, и легко проверить, что φ_0 обладает требуемыми свойствами и единственен.

Замечание. Поскольку подгруппа U_m открыта, из свойства (а) следует, что f непрерывен в дискретной топологии на $\text{Aut } V_0$. Обратно, любой непрерывный гомоморфизм $f: I \rightarrow \text{Aut } V_0$ тривиален на некотором U_m , более того, существует наименьший такой модуль m , он называется *кондуктором* гомоморфизма f .

Упражнение. Пусть m — некоторый модуль и V_0 — конечномерное векторное Q -пространство. Для каждого

$v \notin \text{Supp } m$ пусть F_v — некоторый элемент из $\text{Aut } V_0$. Предположим, что

- (а) F_v попарно коммутируют,
 - (б) существует такой морфизм алгебраических групп $\psi: T \rightarrow GL_{V_0}$, что $\psi(a) = \prod_v F_v^{v(a)}$ для каждого $a \in K^*$,
- $a \equiv 1 \pmod{m}$ и $a > 0$ во всех вещественных вложениях.

Показать, что существует морфизм алгебраических групп $\varphi_0: S_m \rightarrow GL_{V_0}$, для которого элементы Фробениуса равны F_v .

2.7. Вещественный случай

Предыдущие конструкции связывались с заданным простым числом l . Они имеют, однако, и некоторый архимедов аналог. Именно, пусть $\pi: T \rightarrow S_m$ — каноническое отображение, определенное в п. 2.3, и пусть

$$\pi_\infty: T(\mathbf{R}) \rightarrow S_m(\mathbf{R})$$

—соответствующий гомоморфизм вещественных групп Ли. Так как $T(\mathbf{R}) = (K \otimes K)^* = \prod_{v \in \Sigma_K^\infty} K_v^*$, мы можем отож-

дествить $T(\mathbf{R})$ с прямым множителем группы идеалей I . Пусть pr_∞ — проекция группы I на этот множитель. Тогда отображение

$$\alpha_\infty = \pi_\infty \circ \text{pr}_\infty: I \rightarrow T(\mathbf{R}) \rightarrow S_m(\mathbf{R})$$

непрерывно, и, как и в п. 2.3, проверяется, что α_∞ совпадает с e на K^* . Поэтому можно определить отображение

$$\varepsilon_\infty: I \rightarrow S_m(\mathbf{R}),$$

полагая

$$\varepsilon_\infty(a) = e(a) \alpha_\infty(a^{-1}).$$

Имеем $\varepsilon_\infty(a) = 1$, если $a \in K^*$, следовательно, ε_∞ можно рассматривать как гомоморфизм группы классов идеалей $C = I/K^*$ в вещественную группу Ли $S_m(\mathbf{R})$.

Основное отличие от «конечного» случая состоит в том, что ε_∞ нетривиально на связной компоненте

группы C , следовательно, не интерпретируется в терминах группы Галуа. Компьютер $\varepsilon_\infty: C \rightarrow S_m(\mathbf{R})$ с некоторым комплексным характером $S_{m/C} \rightarrow G_{m/C}$, получаем гомоморфизм $C \rightarrow \mathbf{C}^*$, т. е. характер Гекке поля K . Легко видеть, что получаемые таким образом характеры совпадают с „характерами типа A_0 “ Вейля (см. [37], [6]), кондукторы которых делят m .

Упражнение. Пусть

$$e: I \rightarrow S_m(\mathbf{R}) \times \prod_l S_m(\mathbf{Q}_l)$$

— произведение отображений ε_∞ и ε_l для всех l .

а) Показать, что образ e содержится в подгруппе $S_m(\mathbf{A})$ группы $S_m(\mathbf{R}) \times \prod_l S_m(\mathbf{Q}_l)$, где \mathbf{A} — кольцо аделей поля \mathbf{Q} , и что отображение $e: I \rightarrow S_m(\mathbf{A})$ непрерывно (в естественной топологии адельной группы $S_m(\mathbf{A})$).

б) Пусть $\pi_A: T(\mathbf{A}) \rightarrow S_m(\mathbf{A})$ — отображение, определенное посредством $\pi: T \rightarrow S_m$. Показать, что если отождествить $T(\mathbf{A})$ с I очевидным образом, то будем иметь

$$e(x) = \varepsilon(x) \pi_A(x^{-1}),$$

где $\varepsilon: I \rightarrow S_m(\mathbf{Q}) \subset S_m(A)$ — отображение, определенное в п. 2.3. (Отметим, что это дает другое определение отображений ε_l .)

в) Показать, что $\varepsilon(I)$ не является открытым в $S_m(A)$, если $C_m \neq \{1\}$.

2.8. Пример: комплексное умножение абелевых многообразий

(Мы дадим здесь только беглый набросок теории с краткими указаниями на доказательства. Подробности см. в работах Шимуры — Танимы [46], Танимы [37], Вейля [6], [7] и Серра — Тейта [36].) Пусть A — абелево многообразие размерности d , определенное над K , и $\text{End}_K(A)$ — кольцо его эндоморфизмов. Положим $\text{End}_K(A)_0 = \text{End}_K(A) \otimes \mathbf{Q}$. Пусть E — числовое поле степени $2d$ и

$$i: E \rightarrow \text{End}_K(A)_0$$

— некоторое вложение E в $\text{End}_K(A)_0$. В таком случае говорят, что многообразие A имеет „комплексное умножение“ E ; в терминологии Шимуры — Таниамы — это многообразие „СМ-типа“.

Пусть l — простое число, определим $T_l(A)$ и $V_l = T_l(A) \otimes \mathbf{Q}_l$, как в гл. I, п. 1.2. Это свободные модули ранга $2d$ над \mathbf{Z}_l и \mathbf{Q}_l соответственно. \mathbf{Q} -алгебра $\text{End}_K(A)_0$ действует на V_l , следовательно, на нем действует и E , а по линейности и $E_l = E \otimes_{\mathbf{Q}} \mathbf{Q}_l$. Легко доказывается следующая

Лемма. V_l — свободный E_l -модуль ранга 1.

Пусть $\rho_l: \text{Gal}(\bar{K}/K) \rightarrow \text{Aut } V_l$ есть l -адическое представление, определяемое многообразием A . Для любого $s \in \text{Gal}(\bar{K}/K)$ автоморфизм $\rho_l(s)$, очевидно, коммутирует с E и, следовательно, с E_l . Но из леммы следует, что централизатор алгебры E_l в $(\text{End})V_l$ совпадает с E_l . Следовательно, ρ_l можно отождествить с гомоморфизмом

$$\rho_l: \text{Gal}(\bar{K}/K) \rightarrow E_l^*.$$

Пусть теперь T_E является $2d$ -мерным тором, связанным с E (как T связан с K), тогда $T_E(\mathbf{Q}_l) = E_l^*$ и ρ_l принимает значения в $T_E(\mathbf{Q}_l)$.

Теорема 1. (а) Система (ρ_l) является строго согласованной системой рациональных l -адических представлений поля K со значениями в T_E (в смысле гл. I, п. 2.4).

(б) Существует модуль \mathfrak{m} и морфизм

$$\varphi: S_m \rightarrow T_E,$$

такие, что (ρ_l) является образом относительно φ канонической системы (ε_l) , связанной с S_m (см. п. 2.3).

Более того, ограничение φ на T_m можно указать явно.

Пусть \mathbf{t} — касательное пространство в нуле A . Оно является K -пространством, на котором действует E , т. е. (E, K) -бимодулем. Если рассматривать его как E -пространство, то действие K на нем будет задаваться гомоморфизмом $j: K \rightarrow \text{End}_E(\mathbf{t})$. В частности, если $x \in K^*$, то $\det_E j(x)$ — это элемент из E^* ; отображение

$\det_E j: K^* \rightarrow E^*$ является, очевидно, ограничением морфизма $\delta: T \rightarrow T_E$.

Теорема 2. Отображение $\delta: T \rightarrow T_E$ совпадает с композицией отображений $T \rightarrow T_m \rightarrow S_m \xrightarrow{\Psi} T_E$.

Примеры. Пусть A — эллиптическая кривая, E — мнимое квадратичное поле, и действие E на одномерное векторное K -пространство t определяется вложением $E \rightarrow K$. Тогда отображение $\det_E j: K^* \rightarrow E^*$ — это норменное отображение, связанное с этим вложением.

Указания к доказательствам теорем 1 и 2. Часть (а) теоремы 1 доказывается следующим образом. Пусть S — конечное множество точек $v \in \Sigma_K$, в которых A имеет „плохую редукцию“. Если $v \notin S$, $l \neq p_v$, то легко показать, что ρ_l неразветвлено в v (обратное тоже верно, см. [36]); более того, соответствующий элемент Фробениуса F_{v, ρ_l} может быть отождествлен с эндоморфизмом Фробениуса F_v редукции \tilde{A}_v . Но F_v коммутирует с E в $\text{End}(\tilde{A}_v)_0$ и коммутант E в $\text{End}(\tilde{A}_v)_0$ есть само E (см. [46], стр. 39). Следовательно, F_v принадлежит $E^* = T_E(\mathbf{Q})$, из этого следует утверждение (а).

Теорема 2 и часть (б) теоремы 1 доказываются труднее. Их доказательства в несколько иной форме имеются у Шимуры — Танимы [46] (см. также [36]). Отметим, что их (как и в § 2.6) можно было бы сформулировать в таком виде: существует гомоморфизм $f: I \rightarrow E^*$ (где I , как обычно, обозначает группу идеалей поля K), обладающий следующими свойствами:

(а) f тривиален на U_m для некоторого модуля m с носителем S ;

(б) если $v \notin S$, то образом униформизирующего параметра в точке v относительно f является элемент Фробениуса $F_v \in E^*$;

(в) если $x \in K^*$ — главный идеал, то $f(x) = \det_E j(x)$.

Это в сущности и доказано в [46] (стр. 148, формула (3)), если не считать того, что результат сформулирован в терминах идеалов, а не идеалей и $\det_E j(x)$ записан в иной форме, а именно как $\prod N_{K/K^*}(x)^{\psi_a}$.

Замечание. Другой способ доказательства теорем 1 и 2 заключается в следующем. Пусть l — простое число, отличное от каждого из $p_v, v \in S$. Тогда модуль Галуа V_l имеет тип Ходжа — Тейта в смысле гл. III, п. 1.2 (в самом деле, соответствующие локальные множители ассоциированы с l -делимыми группами и можно воспользоваться теоремой Тейта [41]). Следовательно, представление ρ_l „локально алгебраично“ (гл. III, loc. cit.), поэтому, согласно теореме гл. III, п. 2.3, оно определяет морфизм $\varphi: S_m \rightarrow T_E$. Имеем $\varphi \circ \varepsilon_l = \rho_l$ по построению, и это верно для любого простого числа l' , так как $\varphi \circ \varepsilon_{l'}$ и $\rho_{l'}$ имеют одинаковые элементы Фробениуса для почти всех v . Это доказывает часть (б) теоремы 1. Для доказательства теоремы 2 используется явный вид разложения Ходжа — Тейта модуля V_l , данный Тейтом в [41], в комбинации с результатами добавления к гл. III.

§ 3. Строение группы T_m и приложения

3.1. Строение группы $X(T_m)$

Пусть ω — комплексная точка поля $\overline{\mathbf{Q}}$, тогда пополнение поля $\overline{\mathbf{Q}}$ относительно ω изоморфно полю комплексных чисел \mathbf{C} . Группа разложения точки ω — циклическая группа порядка 2, нетривиальный элемент которой мы будем обозначать через c_ω (это „элемент Фробениуса бесконечной точки ω “). Элементы c_ω сопряжены в группе $G = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$; класс сопряженности их обозначим через C_∞ . (По теореме Артина [1], стр. 257, элементы из C_∞ и только они являются нетривиальными элементами конечного порядка в G .)

Пусть $X(T)$ — группа характеров тора T , см. п. 1.1. Будем записывать группу $X(T)$ аддитивно и положим $Y(T) = X(T) \otimes_{\mathbf{Z}} \mathbf{Q}$. Разложим Y в прямую сумму $Y = Y^0 \oplus Y^- \oplus Y^+$ G -инвариантных подпространств (см. добавление, Д. 2), где

$$Y^0 = Y^G = \{y \in Y \mid gy = y \quad \text{для всех } g \in G\},$$

$$Y^- = \{y \in Y \mid cy = -y \quad \text{для всех } c \in C_\infty\},$$

а Y^+ является G -инвариантным дополнением к $Y^0 \oplus Y^-$ в Y . Легко показать, что Y^+ определено однозначно (см. добавление, loc. cit.).

Более явно, если $\sigma \in \Gamma$ — произвольное вложение поля K в $\bar{\mathbf{Q}}$ и $[\sigma] \in X(T)$ — соответствующий характер тора T , то $\{[\sigma]\}, \sigma \in \Gamma$, образуют базис в $X(T)$ и $g[\sigma] = [g\sigma]$, $g \in G$. Пространство Y^0 порождается нормами $\sum_{\sigma \in \Gamma} [\sigma]$, а его G -инвариантное дополнение имеет вид $Y^- \oplus Y^+ = \left\{ \sum_{\sigma \in \Gamma} b_\sigma [\sigma] \mid b_\sigma \in \mathbf{Q}, \sum_{\sigma \in \Gamma} b_\sigma = 0 \right\}$. Следовательно, любой характер $\chi \in X(T)$ можно записать в виде

$$\chi = a \sum_{\sigma \in \Gamma} [\sigma] + \sum_{\sigma \in \Gamma} b_\sigma [\sigma], \quad a, b_\sigma \in \mathbf{Q}, \quad \sum_{\sigma \in \Gamma} b_\sigma = 0, \quad a + b_\sigma \in \mathbf{Z}. \quad (*)$$

В частности, отсюда видно, что $da \in \mathbf{Z}$, где $d = [K : \mathbf{Q}]$. Подпространство Y^- можно описать теперь так:

$$Y^- = \left\{ \sum b_\sigma [\sigma] \mid b_\sigma \in \mathbf{Q}, \quad \sum b_\sigma = 0, \quad b_{c\sigma} = -b_\sigma \quad \forall c \in C_\infty, \sigma \in \Gamma \right\}.$$

С другой стороны, проекция $T \rightarrow T_m$ определяет вложение $X(T_m)$ в $X(T)$. Отождествим $X(T_m)$ с его образом при этом вложении.

ПРЕДЛОЖЕНИЕ. $X(T_m) \otimes_{\mathbf{Z}} \mathbf{Q} = Y^0 \oplus Y^-$.

Это следует из добавления, Д.2.

СЛЕДСТВИЕ 1. Группа характеров $X(T_m)$ является подрешеткой конечного индекса в $X(T) \cap (Y^0 \oplus Y^-)$.

СЛЕДСТВИЕ 2. Если $\chi \in X(T_m)$ записано в виде (*), то $2a \in \mathbf{Z}$.

В самом деле, для данных $c \in C_\infty$ и $\sigma \in \Gamma$ имеем

$$2a = 2a + b_\sigma + b_{c\sigma} = (a + b_\sigma) + (a + b_{c\sigma}) \in \mathbf{Z}.$$

3.2. Морфизм $j^*: G_m \rightarrow T_m$

Мы убедились, что любой характер $\chi \in X(T_m)$ может быть записан в виде

$$\chi = a \sum_{\sigma \in \Gamma} [\sigma] + \sum_{\sigma \in \Gamma} b_\sigma [\sigma],$$

где $a, b_\sigma \in \mathbf{Q}$, $\sum b_\sigma = 0$, $2a \in \mathbf{Z}$. Следовательно, отображение $\chi \mapsto 2a$ определяет гомоморфизм $j: X(T_m) \rightarrow X(\mathbf{G}_m) = \mathbf{Z}$ и по двойственности морфизм алгебраических групп $j^*: \mathbf{G}_m \rightarrow T_m$. Пусть $\varphi_0: S_m \rightarrow GL_{V_0}$ — некоторое представление группы S_m , тогда композиция его с j^* дает морфизм алгебраических групп $\mathbf{G}_m \rightarrow GL_{V_0}$. Это представление группы \mathbf{G}_m определяет градуировку $V_0 = \sum_{i \in \mathbf{Z}} V_0^{(i)}$ на V_0 (и определяется ею): напомним, что

\mathbf{G}_m действует на $V_0^{(i)}$ посредством характера $i \in \mathbf{Z} = X(\mathbf{G}_m)$.

Будем говорить, что V_0 однородна степени n , если $V_0 = V_0^{(n)}$.

Замечание. Для представлений, получаемых из l -адических гомологий $H_*(\bar{X})$ гладких проективных многообразий X , определенная выше градуировка, предположительно, совпадает с естественной градуировкой: $H_*(\bar{X}) = \sum_i H_i(\bar{X})$.

Упражнения. 1) Пусть $N: S_m \rightarrow \mathbf{G}_m$ — морфизм, определенный в упражнении 2 п. 2.5. Показать, что отображение $N \circ j: \mathbf{G}_m \rightarrow S_m \rightarrow \mathbf{G}_m$ имеет вид $\lambda \mapsto \lambda^2$ и что любой морфизм $S_m \rightarrow \mathbf{G}_m$ совпадает с eN^n , $n \in \mathbf{Z}$, где e — характер группы \mathbf{G}_m со значениями в $\{\pm 1\}$.

2) Пусть $\varphi: S_m \rightarrow GL_{V_0}$ — некоторое линейное представление группы S_m . Предположим, что φ однороден степени d , и положим $h = \dim V_0$.

а) Показать, что dh четно (применить упр. 1 к морфизму $\det(\varphi): S_m \rightarrow \mathbf{G}_m$).

б) Доказать, что на V_0 существует положительно определенная квадратичная форма Q , такая, что

$$Q(\varphi(x)y) = N(x)^d Q(y)$$

для любых $y \in V_0$ и $x \in S_m(\mathbf{Q})$. (Пусть H — ядро морфизма $N: S_m \rightarrow \mathbf{G}_m$. Пользуясь тем фактом, что $H(\mathbf{R})$ компактно, доказать существование положительно определенной квадратичной формы Q на V_0 , инвариантной относительно H , и заметить, что S_m порождается подгруппой H и $j^*(\mathbf{G}_m)$.)

3.3. Строение группы T_m

Прежде всего введем некоторые обозначения.

Пусть H_c — обозначает замкнутую подгруппу группы $G = \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, порожденную C_∞ (см. п. 3.1). Существует единственный непрерывный гомоморфизм $\varepsilon: H_c \rightarrow \{\pm 1\}$, такой, что $\varepsilon(c) = -1$ для всех $c \in C_\infty$. В самом деле, его единственность очевидна, а существование устанавливается ограничением на H_c гомоморфизма $G \rightarrow \{\pm 1\}$, соответствующего некоторому мнимому квадратичному расширению поля \mathbf{Q} . Положим $H = \text{Кег } \varepsilon$. Группы H_c и H являются замкнутыми инвариантными подгруппами группы G и $(H: H_c) = 2$.

Пусть теперь K , как и выше, — некоторое конечное расширение поля \mathbf{Q} ; мы отождествляем его с подполем поля $\bar{\mathbf{Q}}$. Пусть $G_K = \text{Gal}(\bar{\mathbf{Q}}/K)$ — соответствующая подгруппа группы G . Поле K чисто вещественно тогда и только тогда, когда все элементы c из C_∞ действуют тривиально на K , т. е. тогда и только тогда, когда G_K содержит H_c . Следовательно, существует максимальное чисто вещественное подполе K_0 поля K , группа Галуа которого есть $G_{K_0} = G_K \cdot H_c$. Обозначим через K_1 поле, соответствующее подгруппе $G_K \cdot H$. Имеем

$$K_0 \subset K_1 \subset K \text{ и } [K_1 : K_0] = 1 \text{ или } 2.$$

Как показал Вейль (см. [6], стр. 4), поля K_0 и K_1 тесно связаны с группами T_m , построеными для K . В самом деле, если $\chi = \sum b_\sigma[\sigma]$ — элемент группы Y^- (см. п. 3.1), то $b_{c\sigma} = -b_\sigma$ для всех $c \in C_\infty$. Если $c_1 \dots c_n = h$, то

$$b_{h\sigma} = (-1)^n b_\sigma = \varepsilon(h) b_\sigma$$

и по непрерывности это верно и для всех $h \in H_c$. Отсюда следует

ПРЕДЛОЖЕНИЕ. *Норменное отображение определяет изоморфизм пространства $Y_{K_1}^-$, связанного с K_1 , с пространством Y_K^- , связанным с K .*

Точнее, если $\chi_1 = \sum b_{\sigma_1}[\sigma_1]$ принадлежит $Y_{K_1}^-$, где $\sigma_1 \in \Gamma_{K_1}$, то образ χ_1 при норменном отображении имеет вид

$$N_{K_1/K}^*(\chi_1) = \sum b_{\sigma[K_1]}[\sigma], \quad \sigma \in \Gamma_K,$$

где σ/K_1 — ограничение σ на K_1 . Очевидно, что это отображение инъективно. Обратно, если $\chi = \sum b_\sigma [\sigma]$ принадлежит Y_K^- , то, как было отмечено выше, $b_{h\sigma} = e(h)b_\sigma$ для всех $h \in H_c$, следовательно, $b_{h\sigma} = b_\sigma$ для $h \in H$ и, конечно, для $h \in H \cdot G_K$. Это показывает, что b_σ зависит только от ограничения σ на K_1 . Следовательно, χ принадлежит образу норменного отображения.

Следствие. Торы T_m , связанные с K и K_1 , изогенны.

Остается описать торы T_m , связанные с K_1 . Возможны два случая.

(1) $K_1 = K_0$. В этом случае $Y^- = 0$ и T_m одномерен и изоморчен \mathbf{G}_m .

Действительно, если $\chi = \sum b_\sigma [\sigma]$ принадлежит Y^- и $c \in C_\infty$, то $b_{c\sigma} = -b_\sigma$ (см. п. 3.1); в то же время $b_{c\sigma} = b_\sigma$, так как $c \in G_K \cdot H_c = G_K \cdot H$. Отсюда $b_\sigma = 0$ для всех σ , следовательно, $Y^- = 0$.

(2) $[K_1 : K_0] = 2$. Поле K_1 тогда есть *чисто мнимое квадратичное расширение* поля K_0 (единственное, содержащееся в K , как нетрудно проверить). В этом случае Y^- имеет размерность $d = [K_0 : \mathbf{Q}]$, а тор T_m $(d+1)$ -мерен.

Более точно, пространство Y , связанное с K_1 , $2d$ -мерно, а инволюция σ поля K_1 , соответствующая K_0 , раскладывает Y в два собственных подпространства размерности d каждое. Пространство Y^- отвечает собственному значению -1 . Это доказывается теми же рассуждениями, что и выше, поскольку было замечено, что каждый элемент $c \in C_\infty$ индуцирует σ на K_1 .

Замечание. В последнем (и наиболее интересном) случае тор T_m изогенен произведению группы \mathbf{G}_m на d -мерный тор — ядро норменного отображения из K_1 в K_0 .

3.4. Как вычислять элементы Фробениуса

Пусть ϕ — линейное представление степени n группы S_m . Ограничение ϕ на T_m можно привести к диагональному виду в некотором расширении основного поля; пусть χ_1, \dots, χ_n — полученные таким образом n характеров

группы T_m . Запишем (в аддитивной форме)

$$\chi_i = \sum_{\sigma \in \Gamma} n_\sigma(i) [\sigma], \quad n_\sigma(i) \in \mathbf{Z}.$$

Назовем χ_i *положительным*, если все $n_\sigma(i)$ неотрицательны. Пусть $v \notin \text{Supp } \mathfrak{m}$ и $F_v \in S_m(\mathbf{Q})$ — соответствующий элемент Фробениуса (см. п. 2.3). Так как факторгруппа $C_m = S_m/T_m$ конечна, то существует такое целое число $N \geq 1$, что $F_v^N \in T_m(\mathbf{Q})$. Пусть \mathbf{p}_v — простой идеал точки v , тогда это означает, что существует элемент $a \in K^*$ с $\mathbf{p}_v^N = (a)$, $a \equiv 1 \pmod{\mathfrak{m}}$ и $a > 0$ во всех вещественных точках поля K .

ПРЕДЛОЖЕНИЕ 1. Числа $\chi_i(a) = \prod_{\sigma} \sigma(a)^{n_{\sigma}(i)}$, $i=1, \dots, n$ являются собственными значениями преобразования $\varphi(F_v^N)$.

Это тривиально следует из построения, поскольку F_v^N является образом элемента a при отображении $T(\mathbf{Q}) \rightarrow T_m(\mathbf{Q})$.

Следствие 1. Собственные значения преобразования $\varphi(F_v)$ являются $\{\mathbf{p}_v\}$ -единицами (т. е. они являются единицами во всех точках поля $\overline{\mathbf{Q}}$, не делящих \mathbf{p}_v).

Следствие 2. Пусть z_1, \dots, z_n — собственные значения преобразования $\varphi(F_v)$, перенумерованные таким образом, чтобы $z_i^N = \chi_i(a)$, и пусть w — точка поля $\overline{\mathbf{Q}}$, делящая \mathbf{p}_v и нормализованная так, чтобы $w(\mathbf{p}_v) = v(\mathbf{p}_v) = e_v$. Тогда $w(z_i) = \sum_{\substack{\sigma \in \Gamma \\ w \circ \sigma = v}} n_\sigma(i)$.

В самом деле, имеем

$$w(z_i^N) = w\left(\prod_{\sigma \in \Gamma} \sigma(a)^{n_{\sigma}(i)}\right) = \sum_{\sigma \in \Gamma} n_\sigma(i) w \circ \sigma(a)$$

и

$$w \circ \sigma(a) = 0, \quad \text{если } w \circ \sigma \neq v,$$

$$w \circ \sigma(a) = N, \quad \text{если } w \circ \sigma = v,$$

поскольку $(a) = \mathbf{p}_v^N$. Отсюда все следует.

Следствие 3. Пусть l — простое число, и пусть φ_l : $\text{Gal}(\bar{K}/K) \rightarrow \text{Aut } V_l$ есть l -адическое представление поля K , ассоциированное с φ . Представление φ_l тогда и только тогда является целым (см. гл. I, п. 2.2), когда все характеристики χ_i , связанные с φ , положительны.

Доказательство следствия 3. Предположим сначала, что все χ_i положительны. Пусть $v \notin \text{Supp } \mathfrak{m}$ и z_1, \dots, z_n — соответствующие собственные значения эндовоморфизма F_v , как в следствии 2. Из следствий 1 и 2 вытекает тогда, что $w(z_i)$ положительны во всех нормированиях w поля $\bar{\mathbf{Q}}$, следовательно, z_i являются целыми над \mathbf{Z} , т. е. представление φ_l цело.

Обратно, пусть φ_l цело для некоторого l . Тогда существует конечное подмножество S' в Σ_K , содержащее $\text{Supp } \mathfrak{m}$, вне которого собственные значения преобразования $\varphi(F_v)$ являются целыми. Выберем простое число p , полностью распадающееся в K и такое, что если $p_v = p$, то $v \notin S'$. Пусть w — точка поля $\bar{\mathbf{Q}}$, делящая p . Тогда нормирования $w \circ \sigma$, $\sigma \in \Gamma$, попарно неэквивалентны. Пусть $\sigma \in \Gamma$ и v — нормализованное нормирование поля K , эквивалентное $w \circ \sigma$, так что $\lambda v = w \circ \sigma$ для некоторого $\lambda > 0$. Обозначим через z_1, \dots, z_n собственные значения преобразования $\varphi(F_v)$. Тогда, согласно следствию 2, $w(z_i) = \lambda n_\sigma(i)$, и так как z_i являются целыми, то это показывает, что все $n_\sigma(i)$ неотрицательны.

ПРЕДЛОЖЕНИЕ 2. Пусть $v \notin \text{Supp } \mathfrak{m}$ и χ — характер группы S_m . Обозначим через $\chi_T \in X(T_m)$ ограничение χ на T_m , и пусть $i = j(\chi_T)$ — целое число, определенное в п. 3.2. Тогда для каждого архimedова абсолютного значения w поля $\bar{\mathbf{Q}}$, продолжающего обычное абсолютное значение поля \mathbf{Q} , имеем

$$\omega(\chi(F_v)) = (Nv)^{i/2}.$$

Доказательство. Если $\chi = a \sum_{\sigma \in \Gamma} [\sigma] + \sum_{\sigma \in \Gamma} b_\sigma [\sigma]$, как в п. 3.1, то

$$\omega(\chi(F_v))^\vee = \omega(\chi(F_v^N)) = \prod_{\sigma} \omega \circ \sigma(a)^a \prod_{\sigma} \omega \circ \sigma(a)^{b_\sigma}$$

и

$$\prod_{\sigma} \omega \circ \sigma(\alpha)^a = \omega(N(\alpha))^a = Nv^{aN} = Nv^{iN/2},$$

где $i = 2a$. Осталось показать, что $\prod_{\sigma} \omega \circ \sigma(\alpha)^{b_{\sigma}} = x$ равно 1. Пусть $c = c_{\omega}$ — элемент Фробениуса, связанный с ω (см. п. 3.1). Поскольку $b_{\sigma} + b_{c\sigma} = 0$, то $xy = 1$, где $y = \prod_{\sigma} \omega \circ \sigma(\alpha)^{b_{c\sigma}}$. Но с другой стороны, $y = \prod_{\tau} \omega \circ c \circ \tau(\alpha)^{b_{\tau}}$, и так как $\omega \circ c = \omega$, то $y = x$. Следовательно, $x^2 = 1$, откуда $x = 1$, так как $x > 0$.

Упражнения. 1) Проверить формулу произведения для собственных значений элемента $\varphi(F_v)$. Воспользоваться следствиями 1 и 2 предложения 1 и предложением 2.

2) Показать, что предложение 2 и следствия 1 и 2 предложения 1 определяют собственные значения элементов $\varphi(F_v)$ с точностью до умножения на корни из 1.

3) (Обобщение следствия 1 предложения 1.) Пусть (ρ_l) — строго согласованная система рациональных l -адических представлений с исключительным множеством S (см. гл. I, п. 2.3). Показать, что для любого $v \in \Sigma_K \setminus S$ собственные значения эндоморфизмов F_{v, ρ_l} , $l \neq p_v$, являются p_v -единицами.

Добавление

Факторизация по арифметическим группам в торах

Д.1. Арифметические группы в торах

Пусть A — линейная алгебраическая группа над \mathbf{Q} и Γ — подгруппа группы $A(\mathbf{Q})$ рациональных точек этой группы. Подгруппа Γ называется *арифметической*, если для любого вложения алгебраических групп $A \subset GL_n$ (n произвольное) группы Γ и $A(\mathbf{Q}) \cap GL_n(\mathbf{Z})$ будут *соизмеримы* (подгруппы Γ_1, Γ_2 называются соизмеримыми, если $\Gamma_1 \cap \Gamma_2$ имеет конечный индекс в Γ_1 и Γ_2). Хорошо известно, что достаточно проверять соизмеримость

групп Γ и $A(\mathbf{Q}) \cap GL_n(\mathbf{Z})$ только для одного вложения $A \subset GL_n$.

Пример. Пусть K — числовое поле и E — группа единиц поля K . Тогда E является арифметической подгруппой группы $T = R_{K/\mathbf{Q}}(\mathbf{G}_m)$.

Пусть T — тор над \mathbf{Q} и T^0 — пересечение ядер гомоморфизмов тора T в \mathbf{G}_m . Тор T называется *анизотропным*, если $T = T^0$; в терминах группы характеров $X = X(T)$ это означает, что X не имеет нетривиальных элементов, левоинвариантных относительно группы $G = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Теорема. *Пусть T — тор над \mathbf{Q} и Γ — арифметическая подгруппа в T . Тогда $\Gamma \cap T^0$ имеет конечный индекс в Γ и факторгруппа $T^0(\mathbf{R})/\Gamma \cap T^0$ компактна.*

Этот результат принадлежит Оно; доказательство более общего утверждения („гипотезы Големана“) имеется у Мостова — Тамагавы [24].

Следствие. *Пусть T — тор над \mathbf{Q} и Γ — арифметическая подгруппа в T . Если T анизотропен, то факторгруппа $T(\mathbf{R})/\Gamma$ компактна.*

Упражнение. Пусть T — тор над \mathbf{Q} с группой характеров X .

а) Показать, что $T(\mathbf{Q}) = \text{Hom}_{\text{Gal}}(X, \overline{\mathbf{Q}}^*)$.

б) Пусть U — подгруппа группы $\overline{\mathbf{Q}}^*$, состоящая из алгебраических единиц поля \mathbf{Q} . Положим

$$\Gamma = \text{Hom}_{\text{Gal}}(X, U).$$

Показать, что Γ — арифметическая подгруппа группы $T(\mathbf{Q})$ и что любая арифметическая подгруппа $T(\mathbf{Q})$ содержится в Γ .

Д.2. Факторизация по арифметическим подгруппам.

Пусть T — тор над \mathbf{Q} и $X(T)$ — его группа характеров. Положим $Y(T) = X(T) \otimes_{\mathbf{Z}} \mathbf{Q}$.

Пусть Λ — множество классов \mathbf{Q} -неприводимых представлений группы $G = \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ посредством конечных факторгрупп. Для каждого $\lambda \in \Lambda$ обозначим через Y_λ

соответствующий изотипический G -подмодуль в Y , т. е. сумму всех G -подмодулей модуля Y , изоморфных λ . Имеет место следующее разложение в прямую сумму:

$$Y = \bigoplus_{\lambda \in \Lambda} Y_\lambda.$$

Пусть $Y^0 = Y_1$, где 1 означает единичное представление группы G , пусть Y^- — сумма таких Y_λ , что для всех бесконечных элементов Фробениуса $c \in C_\infty$ (см. п. 3. 1) $\lambda(c) = -1$, и пусть Y^+ — сумма оставшихся Y_λ . Тогда

$$\begin{aligned} Y^0 &= Y^G = \{y \in Y \mid gy = y \text{ для всех } g \in G\}, \\ Y^- &= \{y \in Y \mid cy = -y \quad \text{для всех } c \in C_\infty\}, \\ Y &= Y^0 \oplus Y^- \oplus Y^+. \end{aligned}$$

Отметим, что $Y = Y^0$ тогда и только тогда, когда тор T анизотропен. Пусть $c \in C_\infty$ и $H = \{1, c\}$; поскольку $T(\mathbf{R}) = \text{Hom}_H(X(T), \mathbf{C}^*)$, мы видим, что группа $T(\mathbf{R})$ компактна тогда и только тогда, когда $Y = Y^-$.

ПРЕДЛОЖЕНИЕ. *Пусть Γ — арифметическая подгруппа тора T и $\bar{\Gamma}$ — ее замыкание Зарисского (см. п. 1.2). Тогда*

$$Y(T/\bar{\Gamma}) = Y^0 \oplus Y^-. \quad (*)$$

[Поскольку тор $T/\bar{\Gamma}$ является фактором тора T , то мы отождествляем $Y(T/\bar{\Gamma})$ с подмодулем модуля $Y(T)$.]

Доказательство. Предположим сначала, что модуль Y неприводим, т. е. T не имеет собственных подторов и отличен от 0. Если $Y = Y^0$, то T изоморфен \mathbf{G}_m и, следовательно, группа Γ конечна. Это показывает, что $Y(T/\bar{\Gamma}) = Y(T)$, откуда следует разложение (*). Если $Y = Y^-$, то группа $T(\mathbf{R})$ компактна. Следовательно, Γ , являясь дискретной подгруппой в $T(\mathbf{R})$, конечна. Поэтому опять $Y(T/\bar{\Gamma}) = Y(T)$ и имеет место разложение (*).

Если $Y = Y^+$, то группа $T(\mathbf{R})$ не компактна. Следовательно, группа Γ бесконечна, так как факторгруппа $T(\mathbf{R})/\Gamma$ компактна по теореме Оно. Поэтому $\bar{\Gamma}$

является алгебраической подгруппой группы T размерности ≥ 1 . Ее связная компонента определяет нетривиальный подтор тора T . Это показывает, что $\bar{\Gamma} = T$, стало быть, $Y(T/\bar{\Gamma}) = 0$. Отсюда опять следует (*).

Общий случай легко выводится из случая неприводимого тора. В самом деле, рассмотрим тор T' , изогенный тору T , который распадается в прямое произведение неприводимых подторов, и заметим, что группа Γ соизмерима с образом при отображении $T' \rightarrow T$ некоторой арифметической подгруппы тора T' .

Упражнение. Пусть $y \in Y$. Определим Ny как среднее значение образов y при действии G .

а) Доказать, что N является G -линейной проекцией Y на Y^0 , следовательно, $\text{Кер } N = Y^- \oplus Y^+$.

б) Доказать, что Y^+ порождается элементами вида $cy + y$, где $y \in \text{Кер } N$, $c \in C_\infty$.

ГЛАВА III

ЛОКАЛЬНО АЛГЕБРАИЧЕСКИЕ АБЕЛЕВЫ ПРЕДСТАВЛЕНИЯ

В этой главе мы определим понятие *локальной алгебраичности* абелева l -адического представления и докажем (см. п. 2.3), что каждое такое представление, если оно рационально, возникает из линейного представления одной из групп S_m , рассмотренных в гл. II.

В случае когда основное поле является композитом квадратичных расширений поля \mathbf{Q} , любое рациональное полупростое l -адическое представление будет *ipso facto* локально алгебраическим; это доказано в § 3 в качестве следствия результатов о трансцендентных числах Зигеля и Ленга.

В локальном случае абелево полупростое представление тогда и только тогда является локально алгебраическим, когда оно обладает „разложением Ходжа — Тейта“. Этот факт, принадлежащий Тейту (Колледж де Франс, 1966), доказан вместе с некоторыми дополнениями в добавлении к этой главе.

§ 1. Локальный случай

1.1. Определения

Пусть p — простое число и K — конечное расширение поля \mathbf{Q}_p . Пусть $T = R_{K/\mathbf{Q}_p}(\mathbf{G}_{m/K})$ — соответствующий алгебраический тор над \mathbf{Q}_p (см. Вейль [8], гл. I).

Рассмотрим конечномерное векторное \mathbf{Q}_p -пространство V и обозначим, как обычно, через GL_V соответствующую линейную группу; это алгебраическая группа над \mathbf{Q}_p и $GL_V(\mathbf{Q}_p) = \text{Aut } V$.

Пусть $\rho: \text{Gal}(\bar{K}/K)^{\text{ab}} \rightarrow \text{Aut } V$ — абелево p -адическое представление поля K в V , где $\text{Gal}(\bar{K}/K)^{\text{ab}}$ обозначает группу Галуа максимального абелева расширения поля K . Обозначим через $i: K^* \rightarrow \text{Gal}(\bar{K}/K)^{\text{ab}}$ канонический гомоморфизм локальной теории полей классов (см., например, Касселс — Фрёлих [15], гл. VI, § 2). Мы получаем тогда непрерывный гомоморфизм $\rho \circ i$ группы $K^* = T(\mathbf{Q}_p)$ в $\text{Aut } V$.

ОПРЕДЕЛЕНИЕ. Представление ρ называется *локально алгебраическим*, если существует такой морфизм алгебраических групп $r: T \rightarrow GL_V$, что $\rho \circ i(x) = r(x^{-1})$ для всех $x \in K^*$, достаточно близких к 1.

Отметим, что если морфизм $r: T \rightarrow GL_V$ удовлетворяет этому условию, то он единствен: это следует из того, что любое непустое открытое множество группы $K^* = T(\mathbf{Q}_p)$ плотно в топологии Зарисского в T . Мы будем называть r *алгебраическим морфизмом, ассоциированным с ρ* .

Примеры. 1. Возьмем $K = \mathbf{Q}_p$ и $\dim V = 1$ так, что представление ρ имеет вид $\text{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)^{\text{ab}} \rightarrow U_p$, где U_p — группа единиц поля \mathbf{Q}_p . Легко видеть, что существует такой элемент $v \in \mathbf{Z}_p$, что $\rho \circ i(x) = x^v$, если x достаточно близок к 1. Представление ρ в таком случае локально алгебраично тогда и только тогда, когда v принадлежит \mathbf{Z} . Например, это имеет место, когда $V = V_p(\mu)$ (см. гл. I, п. 1.2), здесь $v = -1$, а r — каноническое одномерное представление тора $T = \mathbf{G}_{m/\mathbf{Q}_p}$.

2. Локально алгебраическим является представление, ассоциированное с формальной группой Любина — Тейта (см. [22] и [15], гл. VI, § 3) (оно также имеет вид $u \mapsto u^{-1}$ на группе инерций).

ПРЕДЛОЖЕНИЕ 1. Пусть $\rho: \text{Gal}(\bar{K}/K)^{\text{ab}} \rightarrow \text{Aut } V$ — локально алгебраическое абелево представление поля K . Тогда ограничение представления ρ на подгруппу инерции группы $\text{Gal}(\bar{K}/K)^{\text{ab}}$ полупросто.

Отождествим подгруппу инерции в $\text{Gal}(\bar{K}/K)^{\text{ab}}$ с группой U_K единиц поля K . По предположению существуют открытая подгруппа U' группы U_K и алгебраический морфизм $r: T \rightarrow GL_V$, такие, что $\rho(x) = r(x^{-1})$, если $x \in U'$. Пусть W — подпространство пространства V , инвариантное относительно $\rho(U_K)$; тогда оно инвариантно относительно $\rho(U')$, а значит, и относительно $r(T)$. Но каждое линейное представление тора полупросто. Следовательно, существует проектор $\pi: V \rightarrow W$, коммутирующий с действием T . Положив $\pi' = \frac{1}{(U_K: U')} \sum_{s \in U_K/U} \rho(s) \pi \rho(s^{-1})$, получим проектор $\pi': V \rightarrow W$, который будет коммутировать со всеми $\rho(s)$, $s \in U_K$, что и требовалось доказать.

Обратно, пусть задано представление ρ , ограничение которого на U_K полупросто. Возьмем достаточно большое расширение E поля \mathbf{Q}_p так, чтобы ограничение ρ на U_K можно было привести к диагональному виду, т. е. задать с помощью непрерывных характеров $\chi_i: U_K \rightarrow E^*$, $i = 1, \dots, n$. Предположим, кроме того, что E содержит все сопряженные с K поля, и обозначим через Γ_K множество всех \mathbf{Q} -вложений K в E . Напомним (см. гл. II, п. 1.1), что $[\sigma]$, $\sigma \in \Gamma_K$, образуют базис группы характеров $X(T)$ тора T . Имеет место следующее

Предложение 2. Представление ρ тогда и только тогда локально алгебраично, когда существуют такие целые числа $n_\sigma(i)$, что

$$\chi_i(u) = \prod_{\sigma \in \Gamma_K} \sigma(u)^{-n_\sigma(i)}$$

для каждого i и всех u , достаточно близких к 1.

Необходимость тривиальна. Обратно, если существуют такие целые $n_\sigma(i)$, то они определяют алгебраические характеры $r_i = \prod [\sigma]^{n_\sigma(i)}$ тора T_n , следовательно, линейное представление r тора $T_{/E}$. Ясно, что существует такая открытая подгруппа U' группы U_K , что $\rho(u) = r(u^{-1})$ для всех $u \in U'$. Осталось показать, следовательно, что r может быть определено над \mathbf{Q}_p (см. гл. II, п. 2.4). Но след (loc. cit.) $\theta_r = \sum_i r_i$ представле-

ния r обладает свойством $\theta_r(u) \in \mathbf{Q}_p$ для всех $u \in U'$. Поскольку U' плотно в топологии Зарисского в T , то отсюда следует, что след θ_r , „определен над \mathbf{Q}_p “, стало быть, и r можно определить над \mathbf{Q}_p (loc. cit.). Доказательство закончено.

Расширение основного поля. Пусть K' — конечное расширение поля K и ρ' — ограничение заданного представления ρ на $\text{Gal}(\bar{K}/K')$. Представление ρ' тогда и только тогда локально алгебраично, когда этим свойством обладает ρ . Более того, если оно локально алгебраично, то ассоциированные алгебраические морфизмы

$$r: T \rightarrow GL_V, \quad r': T' \rightarrow GL_V$$

связаны соотношением $r' = N_{K'/K} \circ r$, где T' — тор, связанный с K' , и $N_{K'/K}: T' \rightarrow T$ — морфизм алгебраических групп, определенный норменным отображением из K' в K .

Все это легко следует из коммутативности диаграммы

$$\begin{array}{ccc} K^* & \xrightarrow{\quad} & \text{Gal}(\bar{K}/K)^{\text{ab}} \\ \uparrow_N & & \uparrow \\ K'^* & \xrightarrow{\quad} & \text{Gal}(\bar{K}/K')^{\text{ab}} \end{array}$$

и из того факта, что ядро морфизма $N_{K'/K}: T' \rightarrow T$ связано в топологии Зарисского.

Упражнение. Привести пример локально алгебраического абелева p -адического представления размерности 2, не являющегося полупростым.

1.2. Другое определение „локальной алгебраичности“ с помощью модулей Ходжа — Тейта

Напомним прежде всего определение *модуля Ходжа — Тейта* (см. [31], § 2). Поле K предполагается полным относительно дискретного нормирования с совершенным полем вычетов k и $\text{char } K = 0$, $\text{char } k = p$. Обозначим через C пополнение $\hat{\bar{K}}$ алгебраического замыкания поля K .

Группа Галуа $G = \text{Gal}(\bar{K}/K)$ действует непрерывно на \bar{K} . Это действие непрерывно продолжается и на C . Пусть W — векторное C -пространство конечной размерности, на котором группа G действует непрерывно и полулинейно по формуле

$$s(cw) = s(c)s(w), \quad s \in G, \quad c \in C, \quad w \in W.$$

Пусть $\chi: G \rightarrow U_p$ — гомоморфизм группы G в группу $U_p = \mathbf{Z}_p^\times$ p -адических единиц, определенный действием G на p^v -корнях из 1 (см. гл. I, п. 1.2):

$$s(z) = z^{\chi(s)}, \quad s \in G, \quad z^{p^v} = 1.$$

Для каждого целого $i \in \mathbf{Z}$ определим подпространство

$$W^i = \{w \in W \mid sw = \chi(s)^i w \text{ для всех } s \in G\}$$

пространства W . Оно является векторным K -подпространством в W . Пусть $W(i) = W^i \otimes_K C$. На C -пространстве $W(i)$ естественным образом действует группа G (по формуле $s(y \otimes c) = s(y) \otimes s(c)$). Вложение $W^i \rightarrow W$ однозначно продолжается до C -линейного отображения $a_i: W(i) \rightarrow W$, коммутирующего с действием группы G .

ПРЕДЛОЖЕНИЕ (Тейт). *Пусть $\bigoplus_i W(i)$ — прямая сумма пространств $W(i)$, $i \in \mathbf{Z}$, и $\alpha: \bigoplus_i W(i) \rightarrow W$ — сумма отображений a_i , определенных выше. Тогда отображение α инъективно.*

Доказательство см. в [31], § 2, предложение 4.

Следствие. *Пространства W^i , $i \in \mathbf{Z}$, конечномерны над K и линейно независимы над C .*

ОПРЕДЕЛЕНИЕ 1. Если гомоморфизм $\alpha: \bigoplus_{i \in \mathbf{Z}} W(i) \rightarrow W$ является изоморфизмом, то W называется *модулем типа Ходжа — Тейта*.

Пусть теперь V — конечномерное пространство над \mathbf{Q}_p , как и в п. 1.1, $\rho: G \rightarrow \text{Aut } V$ — некоторое p -адическое

представление. Положим $W = V \otimes_{\mathbb{Q}_p} C$ и определим действие группы G на W по формуле

$$s(v \otimes c) = \rho(s)(v) \otimes s(c), \quad s \in G, \quad c \in C, \quad v \in V.$$

ОПРЕДЕЛЕНИЕ 2. Если C -пространство $W = V \otimes_{\mathbb{Q}_p} C$ имеет тип Ходжа — Тейта, то ρ называется *представлением типа Ходжа — Тейта*.

Пример. Пусть F — некоторая p -делимая группа конечной высоты (см. [39], [41]), T — ее модуль Тейта (*loc. cit.*) и $V = T \otimes \mathbb{Q}_p$. Группа G действует на V и, как доказал Тейт ([41], следствие 2 теоремы 3), V является модулем Галуа типа Ходжа — Тейта. Более точно, $W = W(0) \oplus W(1)$, где $W = V \otimes C$, как и выше.

Теорема (Тейт). *Предположим, что поле K является конечным расширением поля \mathbb{Q}_p (следовательно, его поле вычетов K конечно). Пусть $\rho: G \rightarrow \text{Aut } V$ — абелево p -адическое представление поля K . Тогда следующие условия эквивалентны:*

- (а) ρ локально алгебраично (см. п. 1.1),
- (б) ρ имеет тип Ходжа — Тейта и его ограничение на группу инерции полупросто.

Доказательство см. в добавлении.

§ 2. Глобальный случай

2.1. Определения

Возвратимся теперь к обозначениям гл. II: K снова будет обозначать числовое поле. Пусть l — простое число и

$$\rho: \text{Gal}(\bar{K}/K)^{\text{ab}} \rightarrow \text{Aut } V_l$$

— абелево l -адическое представление поля K . Пусть $v \in \Sigma_K$ — точка поля K с полем вычетов характеристики l и $D_v \subset \text{Gal}(\bar{K}/K)^{\text{ab}}$ — соответствующая группа разложения. Она является факторгруппой локальной группы Галуа $\text{Gal}(\bar{K}_v/K_v)^{\text{ab}}$ (на самом деле обе эти

группы изоморфны, хотя здесь нам это не важно). Мы получаем, следовательно, композицию l -адических представлений

$$\rho_v: \mathrm{Gal}(\bar{K}_v/K_v)^{\mathrm{ab}} \rightarrow D_v \xrightarrow{\rho} \mathrm{Aut} V_l.$$

Определение. Представление ρ называется *локально алгебраическим*, если все локальные представления ρ_v , для которых $p_v = l$, локально алгебраичны (в смысле определения п. 1.1 с $p = l$).

Удобно переформулировать это определение с привлечением тора $T = R_{K/\mathbb{Q}}(\mathbf{G}_{m/K})$ гл. II, п. 1.1. Пусть $T_{/\mathbf{Q}_l} = T \otimes_{\mathbb{Q}} \mathbf{Q}_l$ есть \mathbf{Q}_l -тор, полученный из T расширением основного поля \mathbb{Q} до \mathbf{Q}_l . Имеем

$$T_{/\mathbf{Q}_l}(\mathbf{Q}_l) = (K \otimes \mathbf{Q}_l)^* = K_l^*,$$

где $K_l = K \otimes \mathbf{Q}_l$.

Пусть I — группа идеалей поля K (см. гл. II, п. 2.1). Тогда вложение $K_l^* \rightarrow I$ и гомоморфизм полей классов $i: I \rightarrow \mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}}$ определяют некоторый гомоморфизм

$$i_l: K_l^* \rightarrow \mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}}.$$

Предложение. *Представление ρ локально алгебраично тогда и только тогда, когда существует такой алгебраический морфизм*

$$f: T_{/\mathbf{Q}_l} \rightarrow GL_{V_l},$$

что $\rho \circ i_l(x) = f(x^{-1})$ для всех достаточно близких к 1 элементов $x \in K_l^*$.

(Отметим, что, как и в локальном случае, это условие определяет f однозначно. Будем называть f алгебраическим морфизмом, *ассоциированным с представлением ρ* .)

Так как $K \otimes_{\mathbb{Q}} \mathbf{Q}_l = \prod_{v \nmid l} K_v$, то $T_{/\mathbb{Q}} = \prod_{v \nmid l} T_v$, где T_v есть \mathbf{Q}_l -тор, определенный полем K_v (см. п. 1.1). Исходя из этого разложения, немедленно получаем доказательство предложения.

Упражнение. Установить критерий локальной алгебраичности, аналогичный тому, который дан в предложении 2, п. 1.1.

2.2. Модуль локально алгебраического абелева представления

Пусть $\rho: \text{Gal}(\bar{K}/K)^{\text{ab}} \rightarrow \text{Aut } V_l$ — как и выше, абелево l -адическое представление. В композиции с гомоморфизмом полей классов $i: I \rightarrow \text{Gal}(\bar{K}/K)^{\text{ab}}$ представление ρ определяет гомоморфизм $\rho \circ i: I \rightarrow \text{Aut } V_l$. Предположим, что представление ρ алгебраично, и обозначим через f ассоциированный с ним алгебраический морфизм $T_{/\mathbf{Q}_l} \rightarrow GL_{V_l}$.

Определение. Пусть \mathfrak{m} — некоторый модуль (гл. II, п. 1.1). Говорят, что ρ определено по модулю \mathfrak{m} (или \mathfrak{m} является определяющим модулем для ρ), если

- (i) $\rho \circ i$ тривиально на $U_{v, \mathfrak{m}}$, где $p_v \neq l$,
- (ii) $\rho \circ i_l(x) = f(x^{-1})$ для $x \in \prod_{v \mid l} U_{v, \mathfrak{m}}$.

[Отметим, что $\prod_{v \mid l} U_{v, \mathfrak{m}}$ является открытой подгруппой группы $K_l^* = T_{/\mathbf{Q}_l}(\mathbf{Q}_l)$.]

Для того чтобы доказать существование определяющего модуля, нам понадобится следующий вспомогательный результат.

Предложение. Пусть H — группа Ли над \mathbf{Q}_l (соответственно над \mathbf{R}) и α — непрерывный гомоморфизм группы идеалей I в H . Тогда

(а) если $p_v \neq l$ (соответственно $p_v \neq \infty$), то ограничение гомоморфизма α на K_v^* равно 1 на некоторой открытой подгруппе группы K_v^* ;

(б) ограничение гомоморфизма α на группу единиц U_v поля K_v^* равно 1 для почти всех точек v .

Утверждение (а) следует из того факта, что K_v^* является p -адической группой Ли и что гомоморфизм p -адической группы Ли в l -адическую локально равен 1, если $l \neq p$.

Для доказательства утверждения (б) обозначим через N окрестность 1 в H , не содержащую никаких конечных подгрупп, кроме $\{1\}$. Существование такой окрестности является классическим фактом для вещественных групп Ли и очень легко доказывается для l -адических. По определению топологии на группе идеалей $\alpha(U_v)$ содержится в N для почти всех v . Но из утверждения (а) следует, что если $p_v \neq l$, то группа $\alpha(U_v)$ конечна, поэтому $\alpha(U_v) = \{1\}$ для почти всех v , что и требовалось доказать.

Следствие. *Любое абелево l -адическое представление поля K неразветвлено вне конечного множества точек.*

Это вытекает из утверждения (б) для гомоморфизма α группы идеалей I , индуцированного данным представлением, поскольку известно, что $\alpha(U_v)$ — группы инерции.

Замечание. Этот результат не распространяется на неабелевы представления (даже разрешимые), см. упражнение.

Предложение 2. *Каждое локально алгебраическое абелево l -адическое представление имеет определяющий модуль.*

Пусть $\rho: \text{Gal}(\bar{K}/K)^{\text{ab}} \rightarrow \text{Aut } V_l$ — заданное представление и f — ассоциированный с ним морфизм $T_{/\mathbb{Q}_l}$ в GL_{V_l} . Обозначим через X множество точек $v \in \Sigma_K$ с $p_v \neq l$, в которых представление ρ разветвлено. Согласно следствию предложения 1, множество X конечно. В силу утверждения (а) предложения 1 мы можем найти такой модуль \mathfrak{m} , что гомоморфизм $\rho \circ i: I \rightarrow \text{Aut } V_l$ тривиален на каждой группе $U_{v, \mathfrak{m}}$, если $v \in X$. Увеличивая, если нужно, модуль \mathfrak{m} , мы можем считать, что $\rho \circ i_l(x) = f(x^{-1})$ для всех $x \in \prod_{p_v=l} U_{v, \mathfrak{m}}$. Следовательно, \mathfrak{m} является определяющим модулем для представления ρ .

Замечание. Легко показать, что существует наименьший определяющий модуль для ρ , который называется *кондуктором* представления ρ .

Упражнение. Пусть $z_1, \dots, z_n, \dots \in K^*$ — последовательность элементов из K^* . Для каждого n обозначим через E_n подполе поля \bar{K} , порожденное всеми корнями степени l^n из элемента $z_1 z_2^{l} \dots z_n^{l^{n-1}}$.

а) Показать, что E_n — расширение Галуа поля K , содержащее корни l^n -й степени из единицы, и его группа Галуа изоморфна подгруппе аффинной группы $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$ в группе $GL(2, \mathbf{Z}/l^n\mathbf{Z})$.

б) Обозначим через E объединение полей E_n . Показать, что E — расширение Галуа поля K , группа Галуа которого является замкнутой подгруппой аффинной группы над \mathbf{Z}_l .

в) Построить пример, когда E (и, следовательно, соответствующее 2-мерное l -адическое представление) разветвлено в каждой точке поля K .

2.3. Возвращение к S_m

Пусть m — некоторый модуль поля K и

$$\varphi: S_{m/\mathbf{Q}_l} \rightarrow GL_{V_l}$$

— линейное представление группы S_{m/\mathbf{Q}_l} . Обозначим через

$$\varphi_l: \text{Gal}(\bar{K}/K)^{\text{ab}} \rightarrow \text{Aut } V_l$$

соответствующее l -адическое представление (см. гл. II, п. 2.5).

Теорема 1. Представление φ_l локально алгебраично и определено mod m . Ассоциированный с ним алгебраический морфизм $f: T_{/\mathbf{Q}_l} \rightarrow GL_{V_l}$ имеет вид $\varphi \circ \pi$, где π — канонический морфизм T в S_m (см. гл. II, п. 2.2).

Доказательство тривиально следует из построения представления φ_l как композиции $\varphi \circ \varepsilon_l$ (гл. II, п. 2.5) и соответствующих свойств морфизма ε_l (гл. II, п. 2.3).

Верна также и обратная теорема. Мы приведем ее здесь только для случая рациональных представлений.

Теорема 2. Пусть $\rho: \text{Gal}(\bar{K}/K)^{\text{ab}} \rightarrow \text{Aut } V_l$ — абелево l -адическое представление числового поля K . Предположим, что представление ρ рационально (гл. I, п. 2.3) и локально алгебраично с определяющим модулем m (см. п. 2.2). Тогда существует \mathbf{Q} -подпространство V_0 пространства V_l , для которого $V_l = V_0 \otimes_{\mathbf{Q}} \mathbf{Q}_l$, и морфизм $\varphi_0: S_m \rightarrow GL_{V_0}$ алгебраических групп над \mathbf{Q} , такой, что ρ совпадает с l -адическим представлением φ_l , ассоциированным с φ_0 (гл. II, п. 2.5).

[Условие $V_l = V_0 \otimes_{\mathbf{Q}} \mathbf{Q}_l$ означает, что V_0 является „ \mathbf{Q} -структурой“ на V_l , см. Бурбаки, Алгебра, гл. II, (3-е издание).]

Доказательство. Пусть $r: T_{/\mathbf{Q}_l} \rightarrow GL_{V_l}$ — алгебраический морфизм, ассоциированный с представлением ρ . Тогда имеет место равенство

$$\rho \circ i(x) = r(x^{-1}), \quad x \in K^* \cap U_m = \prod_{v \neq l} U_{v, m}.$$

Определим отображение $\psi: I \rightarrow \text{Aut } V_l$ формулой

$$\psi(x) = \rho \circ i(x) \cdot r(x_l),$$

где x_l есть l -я компонента идея x . Немедленно проверяется, что ψ тривиально на U_m и совпадает с r на K^* . Следовательно, r тривиально на $F_m = K \cap U_m$ и пропускается через морфизм алгебраических групп $r_m: T_{m/\mathbf{Q}_l} \rightarrow GL_{V_l}$. По свойству универсальности алгебраической группы S_{m/\mathbf{Q}_l} над \mathbf{Q}_l (гл. II, п. 1.3 и 2.2) существует морфизм алгебраических групп

$$\varphi: S_{m/\mathbf{Q}_l} \rightarrow GL_{V_l}$$

со следующими свойствами:

- (а) сквозной морфизм $T_{m/\mathbf{Q}_l} \rightarrow S_{m/\mathbf{Q}_l} \xrightarrow{\varphi} GL_{V_l}$ совпадает с r_m ,
- (б) отображение $I \xrightarrow{\varphi} S_m(\mathbf{Q}_l) \xrightarrow{\varphi} \text{Aut } V_l$ совпадает с ψ .

Тривиально проверяется, что l -адическое представление φ_l , связанное с φ , совпадает с ρ . В самом деле, пусть $a \in I$, тогда (в обозначениях гл. II)

$$\begin{aligned}\varphi_l \circ i(a) &= \varphi(\varepsilon_l(a)) = \varphi(\varepsilon(a)) \varphi(\pi_l(a_l^{-1})) = \\ &= \psi(a) \varphi(\pi_l(a_l^{-1})) = \rho \circ i(a) r(a_l) \varphi(\pi_l(a_l^{-1})) = \\ &= \rho \circ i(a),\end{aligned}$$

поскольку $\varphi \circ \pi_l = r$ в силу свойства (а).

Следовательно, $\varphi_l = \rho$, и так как ρ рационально, то φ может быть определено над \mathbf{Q} (гл. II, п. 2.4, предложение 1), что дает V_0 и φ_0 . Доказательство закончено.

Замечание. Подпространство V_0 в V_l определено не однозначно. Однако любое другое имеет вид σV_0 , где σ — некоторый автоморфизм пространства V_l , коммутирующий с ρ . По выбранному V_0 уже, конечно, однозначно строится φ .

Следствие 1. Для каждого простого числа l' существует и единственно (с точностью до изоморфизма) l' -адическое рациональное полупростое представление $\rho_{l'}$ поля K , согласованное с ρ . Оно является абелевым и локально алгебраическим. Эти представления образуют строго согласованную систему (см. гл. I, п. 2.3), исключительное множество которой содержится в $\text{Supp } \mathfrak{m}$. Для бесконечного множества простых чисел l' представление $\rho_{l'}$ можно привести к диагональному виду.

Доказательство. Единственность представления $\rho_{l'}$ следует из теоремы гл. I, п. 2.3. Для доказательства существования возьмем за $\rho_{l'}$ l' -адическое представление $\varphi_{l'}$, ассоциированное с φ , как в гл. II, п. 2.5. Остальное следует из предложения гл. II, п. 2.5.

Следствие 2. Собственные значения элементов Фробениуса $F_{v, \rho}$ ($v \notin \text{Supp } \mathfrak{m}$, $p_v \neq l$) порождают конечное расширение поля \mathbf{Q} .

Это вытекает из соответствующего свойства представления φ_l [см. гл. II, п. 2.5, замечание 1].

2.4. Некоторое обобщение

Большинство результатов этой и предыдущей глав можно распространить на случай, когда вместо основного поля \mathbf{Q} линейного представления V взято некоторое числовое поле E . Точнее, пусть λ — конечная точка поля E и E_λ есть λ -адическое дополнение поля E . Понятие E -рационального λ -адического представления поля K было определено в гл. I, п. 2.3, в замечании.

Пусть

$$\rho: \text{Gal}(\bar{K}/K) \rightarrow \text{Aut } V_\lambda$$

— такое представление, и предположим, что оно абелево. Если l — характеристика поля вычетов λ , то E_λ содержит поле \mathbf{Q}_l . Как и в п. 2.1, назовем представление ρ локально алгебраическим, если существует такой морфизм алгебраических групп $f: T_{|E_\lambda} \rightarrow GL_{V_\lambda}$, что $\rho \circ i_l(x) = f(x^{-1})$ для всех достаточно близких к 1 элементов $x \in K_l^*$ (отметим, что $K_l^* = T(\mathbf{Q}_l)$ является подгруппой группы $T(E_\lambda)$). Так же как и в п. 2.3, доказывается, что такое представление ρ возникает из E -линейного представления некоторой группы S_m (и обратно).

2.5. Случай функционального поля

Изложенные выше конструкции имеют (довольно элементарный) аналог для функциональных полей одной переменной с конечным полем констант. Пусть K — такое поле и p — его характеристика. Пусть m — некоторый модуль для K (т. е. некоторый положительный дивизор), определим подгруппу U_m группы иделей I , как и в гл. II, п. 2.1, и положим $\Gamma_m = I/U_m K^*$. Тогда отображение степени $\deg: I \rightarrow \mathbf{Z}$ тривиально на U_m , поэтому имеет место точная последовательность

$$1 \rightarrow J_m \rightarrow \Gamma_m \rightarrow \mathbf{Z} \rightarrow 1.$$

Легко видеть, что группа J_m конечна. Более того, ее можно интерпретировать как группу рациональных точек «обобщенного якобиевого многообразия, определенного модулем m ». Обозначим через $\hat{\Gamma}_m$ пополнение

группы Γ_m относительно топологии, порожденной подгруппами конечного индекса. Известно тогда (теория полей классов), что имеет место изоморфизм $\text{Gal}(\bar{K}/K)^{\text{ab}} \xrightarrow{\sim} \varprojlim \hat{\Gamma}_m = \hat{\Gamma}_m$.

Пусть теперь $\rho: \text{Gal}(\bar{K}/K)^{\text{ab}} \rightarrow \text{Aut } V_l$ — абелево l -адическое представление поля K , $l \neq p$. Как в п. 2.2, доказывается, что существует такой модуль m , что ρ триангульно на U_m , т. е. ρ можно отождествить с гомоморфизмом группы $\hat{\Gamma}_m$ в группу $\text{Aut } V_l$. Более того, имеет место

ПРЕДЛОЖЕНИЕ. Гомоморфизм $\phi: \Gamma_m \rightarrow \text{Aut } V_l$ можно продолжить до непрерывного гомоморфизма группы $\hat{\Gamma}_m$ тогда и только тогда, когда существует решетка в V_l , инвариантная относительно $\rho(\Gamma_m)$.

Необходимость следует из замечания 1) гл. I, п. 1.1. Достаточность очевидна.

Отметим, что в функциональном случае, как и в случае числового поля, определены элементы Фробениуса и можно определить понятие *рациональности* l -адического представления.

ТЕОРЕМА. Абелево l -адическое представление

$$\phi: \hat{\Gamma}_m \rightarrow \text{Aut } V_l$$

поля K тогда и только тогда рационально, когда для каждого $y \in \Gamma_m$ след $\text{Tg } \phi(y)$ принадлежит полю \mathbf{Q} .

Действительно, если $v \notin \text{Supp } m$ и f_v — униформизирующий параметр в точке v , то образ F_v элемента f_v в Γ_m является элементом Фробениуса группы Галуа $\hat{\Gamma}_m$. Следовательно, если $\text{Tg } \phi$ принимает рациональные значения на Γ_m , то характеристический многочлен автоморфизма $\phi(F_v)$ имеет рациональные коэффициенты для всех $v \notin \text{Supp } m$, и ϕ рационально.

Для доказательства обратного утверждения заметим прежде всего, что теорема Чеботарева (гл. I, п. 2.2) остается справедливой и для функционального поля K , если воспользоваться несколько более слабым определением

равнораспределенности. Поэтому элементы Фробениуса образуют плотное подмножество в Γ_m . В частности, они порождают группу Γ_m , откуда видно, что $\text{Tr } \rho(\gamma)$ принадлежит некоторому числовому полю E . Тогда можно построить E -линейное представление $\phi: \Gamma_m \rightarrow GL(n, E)$ с тем же следом, что и у представления ρ , и теорема будет вытекать из следующей леммы:

Лемма. *Пусть Γ — конечно порожденная абелева группа и $\phi: \Gamma \rightarrow GL(n, E)$ — линейное представление над числовым полем E . Пусть Σ — плотное подмножество в Γ относительно топологии, порожденной подгруппами конечного индекса. Предположим, что $\text{Tr } \phi(\gamma) \in \mathbf{Q}$ для каждого $\gamma \in \Sigma$, тогда $\text{Tr } \phi(\gamma) \in \mathbf{Q}$ для всех $\gamma \in \Gamma$.*

Доказательство леммы. Так как группа $\phi(\Gamma)$ также конечно порождена, существует конечное множество S точек поля E , таких, что все элементы из $\phi(\Gamma)$ являются S -целыми матрицами. Пусть l' — простое число, не делящееся ни на какой элемент из S , тогда образ $\phi(\Gamma)$ в $GL(n, E \otimes \mathbf{Q}_{l'})$ содержится в компактной подгруппе группы $GL(n, E \otimes \mathbf{Q}_{l'})$, следовательно, ϕ продолжается по непрерывности до гомоморфизма

$$\hat{\phi}: \hat{\Gamma} \rightarrow GL(n, E \otimes \mathbf{Q}_{l'}),$$

где $\hat{\Gamma}$ — пополнение группы Γ в топологии, порожденной подгруппами конечного индекса. Поскольку Σ плотно в $\hat{\Gamma}$, отсюда следует, что $\text{Tr}(\hat{\phi}(\hat{\gamma}))$ для каждого $\hat{\gamma} \in \hat{\Gamma}$ принадлежит множеству предельных точек $\mathbf{Q}_{l'}$ поля \mathbf{Q} в $E \otimes \mathbf{Q}_{l'}$. Следовательно, если $\gamma \in \Gamma$, то

$$\text{Tr } \phi(\Gamma) \subseteq E \cap \mathbf{Q}_{l'} = \mathbf{Q},$$

что и требовалось доказать.

Упражнения. 1) Пусть $\phi: \Gamma_m \rightarrow \text{Aut } V_l$ — полу-простое l -адическое представление группы Γ_m . Доказать эквивалентность следующих утверждений:

- (а) ϕ непрерывно продолжается на $\hat{\Gamma}_m$;
- (б) собственные значения автоморфизма $\phi(\gamma)$ для каждого $\gamma \in \Gamma_m$ являются единицами (в подходящем расширении поля \mathbf{Q}_l);

(в) существует такой элемент $\gamma \in \Gamma_m$ с $\deg \gamma \neq 0$, что собственные значения автоморфизма $\varphi(\gamma)$ являются единицами;

(г) для любого $\gamma \in \Gamma_m$ след $\mathrm{Tr} \varphi(\gamma)$ принадлежит \mathbf{Z}_l .

2) Пусть $\varphi: \widehat{\Gamma}_m \rightarrow \mathrm{Aut} V_l$ — рациональное l -адическое представление поля K . Показать, что почти для каждого простого числа l' существует l' -адическое представление поля K , согласованное с φ . Установить, что это справедливо для каждого $l' \neq p$ тогда и только тогда, когда выполнено следующее свойство: коэффициенты характеристического многочлена автоморфизма $\varphi(\gamma)$ являются p -целыми для всех $\gamma \in \Gamma_m$.

§ 3. Случай композита квадратичных полей

3.1. Формулировка основного результата

Цель этого параграфа — доказать следующую теорему.

Теорема. *Пусть ρ — рациональное полупростое l -адическое абелево представление поля K . Предположим, что*

() поле K является композитом квадратичных расширений поля \mathbf{Q} .*

Тогда представление ρ локально алгебраично (и, следовательно, оно получается из линейного представления некоторой группы S_m , см. п. 2.3).

В частности, это применимо к $K = \mathbf{Q}$ или квадратичному полю K над \mathbf{Q} .

Замечания. 1) Аналогичные результаты имеют место для E -рациональных полупростых абелевых λ -адических представлений (см. п. 2.4).

2) Вполне вероятно, что условие (*) не является необходимым. Но для доказательства этого требуются, по-видимому, более глубокие результаты о трансцендентных числах, чем те, которые сейчас известны.

3.2. Критерий локальной алгебраичности

Предложение. *Пусть $\rho: \mathrm{Gal}(\bar{K}/K)^{\text{ab}} \rightarrow \mathrm{Aut} V_l$ — рациональное полупростое l -адическое представление поля K . Предположим, что существует такое целое число*

$N \geq 1$, что представление ρ^N локально алгебраично, тогда ρ также локально алгебраично.

Доказательство. Так как ρ полупросто, оно приводится к диагональному виду над некоторым конечным расширением поля \mathbf{Q}_l и, следовательно, определяет n непрерывных характеров ψ_1, \dots, ψ_n , $\psi_i: C_K \rightarrow \bar{\mathbf{Q}}_l^*$, где C_K — группа классов идеалей поля K и $n = \dim V_l$. Пусть $\chi_1 = \psi_1^N, \dots, \chi_n = \psi_n^N$ — соответствующие характеристики для ρ^N . Поскольку представление ρ^N локально алгебраично, каждому χ_i отвечает некоторый алгебраический характер $\chi_i^{\text{alg}} \in X(T)$ тора T (мы отождествляем здесь $X(T)$ с $\text{Hom}(T_{/\bar{\mathbf{Q}}_l}, \mathbf{G}_{m/\bar{\mathbf{Q}}_l})$, так как поле $\bar{\mathbf{Q}}_l$ алгебраически замкнуто). Но каждый из χ_i^{alg} имеет вид $\prod_{\sigma \in \Gamma} [\sigma]^{n_\sigma(i)}$, где Γ — множество вложений поля K в поле $\bar{\mathbf{Q}}_l$ (см. гл. II, п. 1.1). Поэтому для всех $x \in K_l^*$, достаточно близких к 1, имеет место равенство

$$\chi_i(x) = \chi_i^{\text{alg}}(x^{-1}) = \prod_{\sigma \in \Gamma} \sigma(x)^{-n_\sigma(i)}.$$

Лемма. Каждое из целых чисел $n_\sigma(i)$, $1 \leq i \leq n$, $\sigma \in \Gamma$, делится на N .

Доказательство леммы. Пусть U — открытая подгруппа в $\bar{\mathbf{Q}}_l^*$, не содержащая никаких коней N -й степени из 1, кроме 1, и \mathfrak{m} — такой модуль поля K , что $\psi_i(x) \in U$ для всех $x \in U_m$, $i = 1, \dots, n$. Существование такого \mathfrak{m} следует из непрерывности характеров ψ_1, \dots, ψ_n . Выберем \mathfrak{m} настолько большим, чтобы выполнялись следующие условия:

- а) \mathfrak{m} — определяющий модуль для ρ^N ,
- б) представление ρ неразветвлено во всех точках $v \notin \text{Supp } \mathfrak{m}$ и соответствующие элементы Фробениуса $E_{v, \rho}$ имеют характеристические многочлены с рациональными коэффициентами.

Обозначим через K_m абелево расширение поля K , соответствующее открытой подгруппе K^*U_m группы идеалей I , и пусть L — конечное расширение Галуа поля \mathbf{Q} , содержащее K_m . Выберем простое число p , отличное

от l , не делящееся ни на какое $v \in \text{Supp } \mathfrak{m}$ и полностью распадающееся в L . Пусть v — точка поля K , делящая p , и f_v — идель, равный 1 всюду, кроме v , и униформизирующему параметру в точке v . Из того что v полностью распадается в $K_{\mathfrak{m}}$ (так как $K_{\mathfrak{m}} \subset L$), следует, что f_v является нормой некоторого идеяля из $K_{\mathfrak{m}}$, следовательно (по теории полей классов), он принадлежит $K^*U_{\mathfrak{m}}$. Это означает, что простой идеал \mathbf{p}_v является главным идеалом вида (а), где $a \equiv 1 \pmod{\mathfrak{m}}$, а положительно во всех вещественных точках поля K .

Пусть $x = \psi_i(f_v)$ и $y = \chi_i(f_v)$, так что $y = x^N$. Это элементы Фробениуса для ψ_i и χ_i в точке v . По определению характера χ_i^{alg} имеем

$$y = \chi_i^{\text{alg}}(a) = \prod_{\sigma \in \Gamma} \sigma(a)^{n_{\sigma}(i)},$$

где a — то же, что и выше.

Следовательно, y принадлежит подполю \tilde{L} поля \mathbf{Q}_l , соответствующему полю L (\tilde{L} определено однозначно, поскольку L является расширением Галуа поля \mathbf{Q}). Более того, если w_{σ} — такая точка поля L , что $w_{\sigma} \circ \sigma$ индуцирует v на K , то (как в гл. II, п. 3.4) имеем

$$w_{\sigma}(y) = n_{\sigma}(i).$$

Предположим теперь, что $n_{\sigma}(i)$ не делится на N . Тогда x , являясь корнем степени N из элемента y , не принадлежит полю \tilde{L} . Следовательно, существует такой нетривиальный корень N -й степени из единицы z , что x и zx сопряжены над \tilde{L} и тем более над \mathbf{Q} . Поскольку характеристический многочлен автоморфизма $F_{v, \rho}$ имеет рациональные коэффициенты, то любое число, сопряженное над \mathbf{Q} с собственным значением автоморфизма $F_{v, \rho}$, также будет его собственным значением. Поэтому существует такой индекс j , что

$$\psi_j(f_v) = zx = z\psi_i(f_v).$$

Но $f_v \in K^*U_{\mathfrak{m}}$, а ψ_j для любого j тривиально на K^* и отображает $U_{\mathfrak{m}}$ в открытую подгруппу U , с выбора

которой мы начинали. Следовательно, $z = \psi_j(f_v) \psi_i(f_v)^{-1}$ принадлежит U , что противоречит выбору последней.

Доказательство предложения. Так как $n_\sigma(i)$ делятся на N , то существует такой $\varphi_i \in X(T)$, что $\varphi_i^N = \chi_i^{\text{alg}}$. Поэтому для достаточно близкого к 1 элемента $x \in K_l^*$ имеет место равенство

$$\varphi_i(x^{-1})^N = \chi_i^{\text{alg}}(x^{-1}) = \chi_i(x) = \psi_i(x)^N.$$

Следовательно, для таких x элементы $\varphi_i(x) \psi_i(x)$ являются корнями из 1 степени N и в силу непрерывности отображение $\varphi_i(x) \psi_i(x)$ единично в некоторой окрестности 1. Стало быть, ограничение ρ на K_l^* локально совпадает с φ^{-1} , где φ — алгебраическое представление тора T , определенное характерами $(\varphi_1, \dots, \varphi_n)$. Представление φ , a priori определенное над $\bar{\mathbf{Q}}_l$, может быть определено над \mathbf{Q}_l (и даже над \mathbf{Q}): это следует, например, из того, что семейство $(\varphi_1, \dots, \varphi_n)$ инвариантно относительно действия группы Галуа $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, так же как и семейство $(\chi_1^{\text{alg}}, \dots, \chi_n^{\text{alg}})$.

Поэтому представление ρ локально алгебраично, что и требовалось доказать.

3.3. Один вспомогательный результат о торах

В книге [20] Ленг доказал, что две экспоненциальные функции $\exp(b_1 z)$ и $\exp(b_2 z)$, $b_1, b_2 \in \mathbf{C}$, принимающие алгебраические значения по крайней мере для трех \mathbf{Q} -линейно независимых значений z , мультипликативно зависимы, т. е. отношение b_1/b_2 — рациональное число. Это было замечено также Зигелем.

Ленг доказал следующий l -адический аналог этого утверждения:

ПРЕДЛОЖЕНИЕ 1. *Пусть E — поле, содержащее \mathbf{Q}_l и полное относительно вещественного нормирования, продолжающего нормирование поля \mathbf{Q}_l . Пусть $b_1, b_2 \in E$ и Γ — некоторая аддитивная подгруппа поля E . Предположим, что*

(1) *ранг группы Γ над \mathbf{Z} не меньше 3;*

(2) экспоненциальный ряд $\exp(z) = \sum \frac{z^n}{n!}$ сходится абсолютно на $b_1\Gamma$ и $b_2\Gamma$;

(3) для всех $z \in \Gamma$ элементы $\exp(b_1 z)$ и $\exp(b_2 z)$ алгебраичны над \mathbf{Q} .

Тогда b_1 и b_2 линейно зависимы над \mathbf{Q} (т. е. отношение b_1/b_2 принадлежит \mathbf{Q} , если $b_2 \neq 0$).

Доказательство см. в [20], дополнение, или в [30], § 1.

Мы применим этот результат к торам, взяв в качестве E пополнение поля $\bar{\mathbf{Q}}_l$. Нам понадобится прежде всего несколько определений.

а) Пусть T есть n -мерный тор над \mathbf{Q} с группой характеров $X(T)$. Как и раньше, отождествим группу $X(T)$ с группой морфизмов $T_{/E}$ в $\mathbf{G}_{m/E}$. Будем говорить, что тор T является *суммой одномерных торов*, если существуют такие одномерные подторы T_i , $1 \leq i \leq n$, что отображение сложения $T_1 \times \dots \times T_n \rightarrow T$ сюръективно (и, следовательно, может иметь только конечное ядро). Это эквивалентно тому, что $X(T) \otimes \mathbf{Q}$ является *прямой суммой одномерных подпространств, инвариантных относительно действия группы $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$* .

б) Пусть f — непрерывный гомоморфизм группы $T(\mathbf{Q}_l)$ в E^* . Будем говорить, что f локально алгебраичен, если существует такая окрестность единицы U в l -адической группе Ли $T(\mathbf{Q}_l)$ и такой элемент $\varphi \in X(T)$, что $f(x) = \varphi(x)$ для $x \in U$. Будем говорить, что f почти локально алгебраичен, если существует такое целое число $N \geq 1$, что f^N локально алгебраичен.

в) Пусть S — конечное множество простых чисел и для каждого $p \in S$ задана открытая подгруппа W_p группы $T(\mathbf{Q}_p)$. Семейство $(W_p)_{p \in S}$ обозначим через W .

Пусть $T(\mathbf{Q})_W$ — это множество элементов $x \in T(\mathbf{Q})$, образы которых в $T(\mathbf{Q}_p)$ принадлежат W_p для всех $p \in S$. Ясно, что $T(\mathbf{Q})_W$ — подгруппа в $T(\mathbf{Q})$. В этих обозначениях имеет место

ПРЕДЛОЖЕНИЕ 2. Пусть $f: T(\mathbf{Q}_p) \rightarrow E^*$ — непрерывный гомоморфизм. Предположим, что

- (а) существует такое семейство $W = (W_p)_{p \in S}$, что $f(x)$ алгебраично над \mathbf{Q} для каждого $x \in T(\mathbf{Q})_W$;
- (б) T является суммой одномерных торов; тогда f почти локально алгебраичен.

Доказательство. i) Пусть сначала тор T одномерен и χ — образующий элемент группы $X(T)$. Если χ инвариантен относительно $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, то T изоморфен \mathbf{G}_m и $T(\mathbf{Q}) \cong \mathbf{Q}^*$. Если нет, то $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ действует на $X(T)$ посредством группы порядка 2, соответствующей некоторому квадратичному расширению F поля \mathbf{Q} . Тогда характер χ определяет изоморфизм группы $T(\mathbf{Q})$ с группой F^\times элементов поля F с нормой 1. В обоих случаях $T(\mathbf{Q})$ — абелева группа бесконечного ранга (более точный результат сформулирован ниже в упражнении). С другой стороны, каждая факторгруппа $T(\mathbf{Q}_p)/W_p$ конечно порождена и имеет ранг, меньший либо равный 1. Поэтому факторгруппа $T(\mathbf{Q})/T(\mathbf{Q})_W$ также конечно порождена и, стало быть, $T(\mathbf{Q})_W$ имеет бесконечный ранг.

Далее, поскольку $T(\mathbf{Q}_l)$ является одномерной l -адической группой Ли, она локально изоморфна *аддитивной группе* \mathbf{Q}_l . Значит, существует гомоморфизм

$$e: \mathbf{Z}_l \rightarrow T(\mathbf{Q}_l),$$

изоморфно отображающий \mathbf{Z}_l на некоторую открытую подгруппу группы $T(\mathbf{Q}_l)$. С помощью композиции мы получаем два непрерывных гомоморфизма

$$f \circ e: \mathbf{Z}_l \rightarrow E^*, \quad \chi \circ e: \mathbf{Z}_l \rightarrow E^*.$$

Но всякий непрерывный гомоморфизм \mathbf{Z}_l в E^* является локально экспоненциальным. Поэтому, заменяя, если нужно, \mathbf{Z}_l на $l^n \mathbf{Z}_l$, можно найти такие элементы $b_1, b_2 \in E$, что

$$f \circ e(z) = \exp(b_1 z), \quad \chi \circ e(z) = \exp(b_2 z)$$

с абсолютно сходящимися экспоненциальными рядами.

Пусть теперь Γ — это множество таких элементов $z \in \mathbf{Z}_l$, что $e(z) \in T(\mathbf{Q})_W$. Поскольку группа $T(\mathbf{Q}_l)/e(\mathbf{Z}_l)$ конечно порождена и $T(\mathbf{Q})_W$ имеет бесконечный ранг, Γ тоже имеет бесконечный ранг. Если $z \in \Gamma$, $e(z) \in T(\mathbf{Q})_W$, то $f \circ e(z)$ алгебраично над \mathbf{Q} . То же самое верно и для $\chi \circ e(z)$, так как χ отображает $T(\mathbf{Q})$ либо в \mathbf{Q}^* , либо в группу F_l^* (определенную выше). Из предложения 1 следует в таком случае, что b_1/b_2 рационально. Это означает, что некоторая целая степень f^N гомоморфизма f с $N \geq 1$ локально совпадает с некоторой целой степенью отображения χ , следовательно, гомоморфизм f почти локально алгебрачен.

ii) Общий случай. Представим T в виде $T = T_1 \dots T_n$, где T_1, \dots, T_n — одномерные подторы тора T . Так как $X(T) \otimes \mathbf{Q}$ является прямой суммой модулей $X(T_i) \otimes \mathbf{Q}$, то достаточно показать, что для каждого i ограничение f_i гомоморфизма f на $T_i(\mathbf{Q}_l)$ почти локально алгебраично. Для этого мы можем выбрать открытые подгруппы $W_{i,p}$ в $T_i(\mathbf{Q}_p)$ так, чтобы $W_{1,p} W_{2,p} \dots W_{n,p} \subset W_p$. Полагая $W_i = (W_{i,p})_{p \in S}$, видим, что f_i принимает алгебраические значения на $T_i(\mathbf{Q})_{W_i}$, следовательно, в силу i) f_i локально алгебрачен, что и требовалось доказать.

Замечание. Если бы можно было освободиться от условия (б) предложения 2, то все результаты этого параграфа можно было бы распространить на произвольные числовые поля. Это можно было бы сделать, если бы иметь достаточно сильный n -мерный вариант предложения 1; тот, который дан в [34], § 2, по-видимому, недостаточен (нужны такие плотностные свойства, которые в рассматриваемом случае еще не известны).

Упражнение. Пусть T — нетривиальный тор над \mathbf{Q} . Показать, что $T(\mathbf{Q})$ является прямой суммой некоторой конечной группы и свободной абелевой группы бесконечного ранга.

3.4. Доказательство теоремы

Возвратимся к обозначениям и предположениям п. 3.1. Пусть

$$\rho: \mathrm{Gal}(\bar{K}/K)^{\mathrm{ab}} \rightarrow \mathrm{Aut} V_l$$

— рациональное полупростое абелево l -адическое представление поля K . Пусть E — пополнение $\bar{\mathbf{Q}}_l$, как в п. 3.3. Представление ρ над E приводится к диагональному виду. Это доставляет семейство (ψ_1, \dots, ψ_n) непрерывных характеров группы $\text{Gal}(\bar{K}/K)^{\text{ab}}$ (а следовательно, и группы идеалей I) со значениями в E^* , где $n = \dim V_l$.

Пусть $f: K_l^* \rightarrow E^*$ — ограничение характера ψ_i на l -ю компоненту K_l^* группы идеалей. Отметим, что $K_l^* = T(\mathbf{Q}_l)$, где T , как обычно, тор, определенный полем K (гл. II, п. 1.1).

ЛЕММА. *Тор T и гомоморфизмы f_i удовлетворяют условиям (а) и (б) предложения 2 п. 3.3.*

Проверка условия (а). Пусть S — конечное множество простых чисел, отличных от l и таких, что для $v \in \Sigma_K$ и $p_v \neq l$, $p_v \notin S$ представление ρ неразветвлено в v и характеристический многочлен $F_{v, \rho}$ имеет рациональные коэффициенты. Если $p \in S$, то, как показывает предложение 1 п. 2.2, существует такая открытая подгруппа W_p группы $K_p^* = T(\mathbf{Q}_p)$, что $\psi_i(W_p) = 1$. Пусть $W = (W_p)_{p \in S}$ и $x \in T(\mathbf{Q})_W$. Так как $x \in K^*$, то $\psi_i(x) = 1$, если отождествить x с соответствующим главным идеалем поля K . С другой стороны, расщепим идеал x на компоненты

$$x = x_\infty \cdot x_l \cdot x_S \cdot x'$$

в соответствии с разложением группы I в произведение

$$I = K_\infty^* \times K_l^* \times K_S^* \times I',$$

где $K_\infty^* = (K \otimes \mathbf{R})^*$, $K_S^* = \prod_{p \in S} K_p^*$ и I' — ограниченное произведение групп K_v^* для $v \in \Sigma_K$, $p_v \neq l$, $p_v \notin S$. Соотношение $\psi_i(x) = 1$ вместе с равенством $\psi_i(x_l) = f_i(x)$ дают

$$f_i(x)^{-1} = \psi_i(x_\infty) \psi_i(x_S) \psi_i(x').$$

По построению имеем $\psi_i(x_S) = 1$, и очевидно, что $\psi_i(x_\infty) = \pm 1$. Поэтому

$$f_i(x) = \pm \psi_i(x')^{-1}.$$

Но мы знаем, что для любого $v \in \Sigma_K$ с $p_v \notin S$, $p_v \neq l$ собственные значения $F_{v,\rho}$ алгебраичны; следовательно, если f_v — идеяль, равный униформизирующему элементу в точке v и 1 всюду вне, то $\psi_i(f_v)$ алгебраично. Пусть $a(v)$ — порядок идеяля x' в точке v , тогда

$$\psi_i(x') = \prod \psi_i(f_v)^{a(v)},$$

следовательно, значения $\psi_i(x')$ и $f_i(x)$ алгебраичны, и условие (а) проверено.

Проверка условия (б). Так как поле K — композит квадратичных полей, то оно является расширением Галуа поля \mathbf{Q} и его группа Галуа есть произведение групп порядка 2. G -модуль характеров $X(T)$ тора T изоморфен регулярному представлению группы G , и очевидно, что $X(T) \otimes \mathbf{Q}$ расщепляется в прямую сумму одномерных G -инвариантных подпространств (каждое из которых соответствует некоторому характеру группы G). Следовательно, T является суммой одномерных торов.

Окончание доказательства теоремы. Пользуясь предложением 2 п. 3.3, находим, что каждое из f_i почти локально алгебраично. Следовательно, существует такое целое число $N \geq 1$, что f_i^N локально алгебраично. Из этого следует (ср. п. 1.1), что ρ^N локально алгебраично, поэтому (см. п. 3.2) само ρ тоже локально алгебраично. Теорема доказана.

Упражнение. Предположим, что K — композит квадратичных полей. Пусть χ — некоторый характер Гекке поля K , и пусть его значения (на идеалах, взаимно простых с кондуктором) являются алгебраическими числами. Показать, что χ принадлежит «типу A » в смысле Вейля [6]. (Воспользоваться тем же методом, что выше, заменив E на C .) Показать, что если значения характера χ лежат в некотором конечном расширении поля \mathbf{Q} , то χ принадлежит «типу A_0 ».

Добавление

Разложения Ходжа—Тейта и локально алгебраические представления

Пусть K —поле характеристики нуль, полное относительно дискретного нормирования с совершенным полем вычетов k характеристики $p > 0$. В этом добавлении мы будем заниматься разложением Ходжа—Тейта p -адических абелевых представлений поля \bar{K} .

В п. Д. 1 и Д. 2 даны инвариантные свойства таких разложений относительно расширений основного поля. В п. Д. 4 определены специальные характеры группы $\text{Gal}(\bar{K}/K)$; они тесно связаны с модулями Ходжа—Тейта (см. Д. 4 и Д. 5) и локальной алгебраичностью (см. п. Д. 6).

Доказательство теоремы Тейта (ср. п. 1.2) дано в последнем пункте.

Д.1. Инвариантность разложений Ходжа — Тейта

Пусть C —пополнение поля \bar{K} (ср. п. 1.2); на нем непрерывно действует группа $\text{Gal}(\bar{K}/K)$. Пусть χ —характер группы $\text{Gal}(\bar{K}/K)$ со значениями в группе p -адических единиц, определенный в гл. I, п. 1.2. Обозначим через K'/K некоторое подрасширение расширения \bar{K}/K , на котором нормирование $\tilde{\sigma}$ поля \bar{K} дискретно; это означает, что K' является конечным расширением неразветвленного расширения поля K . Пусть \hat{K}' —замыкание поля K' в C .

Рассмотрим конечномерное векторное C -пространство W , на котором непрерывно и полулинейно действует группа $\text{Gal}(\bar{K}/K)$ (см. п. 1.2). Обозначим, как и раньше, через W^n (соответственно $W_{K'}^n$) векторное K - (соответственно \hat{K}' -) пространство

$W^n = \{w \in W \mid s(w) = \chi(s)^n w \text{ для всех } s \in \text{Gal}(\bar{K}/K)\}$
(соответственно

$W_{K'}^n = \{w \in W \mid s(w) = \chi(s)^n w \text{ для всех } s \in \text{Gal}(\bar{K}/K')\}$:

Пусть $W(n) = C \otimes_K W^n$ и $W(n)' = C \otimes_{\hat{K}'} W_{K'}^n$. Отож-

действия модули $W(n)$ и $W(n)'$ с их каноническими образами в W , докажем следующую теорему:

Теорема 1. Каноническое отображение $\hat{K}' \otimes_K W^n \rightarrow W_{K'}^n$ является \hat{K}' -изоморфизмом.

Следствие 1. Модули Галуа $W(n)$ и $W(n)'$ совпадают.

Действительно, из теоремы 1 видно, что W^n и $W_{K'}^n$ порождают одно и то же векторное C -подпространство пространства W .

Следствие 2. Модуль Галуа W имеет тип Ходжа — Тейта над K тогда и только тогда, когда он имеет его над \hat{K}' .

Доказательство теоремы 1. Прежде всего заметим, что замена заданного действия группы $\text{Gal}(\bar{K}/K)$ на W на действие вида $(s, w) \mapsto \chi(s)^{-i} sw$, $i \in \mathbf{Z}$, заменяет W^n на W^{n+i} . Этот процесс сдвига сводит задачу к случаю $n=0$, в котором W^n (соответственно $W_{K'}^n$) — это множество элементов, инвариантных относительно $\text{Gal}(\bar{K}/K)$ (соответственно $\text{Gal}(\bar{K}/K')$). Отметим еще, что инъективность отображения $\hat{K}' \otimes W^0 \rightarrow W_{K'}^0$ тривиальна, так как мы знаем, что отображение $C \otimes_K W^0 \rightarrow W$ инъективно (см. п. 1.2).

С другой стороны, легкое прямое рассуждение показывает, что расширение K'/K можно считать либо *конечным расширением Галуа*, либо *неразветвленным расширением Галуа*. В обоих случаях мы имеем дело с полулинейным действием группы $\text{Gal}(K'/K)$ на $W_{K'}^0$, поскольку действие группы $\text{Gal}(\bar{K}/K')$ на $W_{K'}^0$ тривиально. Если расширение K'/K конечно, то, как хорошо известно, $W_{K'}^0$ порождается элементами, инвариантными относительно $\text{Gal}(K'/K)$, т. е. модулями W^0 (это некоммутативный аналог „теоремы 90“ Гильберта, см., например, [33], стр. 159).

Предположим теперь, что расширение Галуа K'/K неразветвлено и G — его группа Галуа. Обозначим через \hat{O}' кольцо целых элементов поля \hat{K}' . Пусть Λ — некоторая \hat{O}' -решетка в $W_{K'}^0$ (т. е. свободный \hat{O}' -подмодуль

максимального ранга модуля W_K^0). Так как G действует на W_K^0 непрерывно, стабилизатор модуля Λ в G открыт, а следовательно, имеет конечный индекс, поэтому у решетки Λ существует только конечное число образов. Обозначим их сумму через Λ^0 , тогда решетка Λ^0 инвариантна относительно G . Пусть e_1, \dots, e_N — ее базис. Имеем

$$s(e_j) = \sum_{i=1}^N a_{ij}(s) e_i, \quad a_{ij} \in \hat{O}',$$

где матрица $a(s) = (a_{ij}(s))$ принадлежит $GL(N, \hat{O}')$. Ясно, что $a(st) = a(s)s(a(t))$, т. е. $\{a(s)\}$ — непрерывный одномерный коцикл группы G со значениями в $GL(N, \hat{O}')$. Напомним, что два таких коцикла a и a' называются когомологичными, если существует такой элемент $b \in GL(N, \hat{O}')$, что $a'(s) = b^{-1}a(s)s(b)$ для $s \in G$. Это задает отношение эквивалентности на множестве всех коциклов, и соответствующее факторпространство обозначается через $H^1(G, GL(N, \hat{O}'))$. Оказывается, что имеет место

Лемма. $H^1(G, GL(N, \hat{O}')) = \{1\}$.

Предположим, что лемма доказана, тогда доказательство теоремы завершается следующим образом. Поскольку коцикл $a(s)$ когомологичен 1, существует $b \in GL(N, \hat{O}')$, такой, что $b = a(s)s(b)$ для всех $s \in G$. Пусть $b = (b_{ij})$, выберем новый базис e'_1, \dots, e'_N пространства W_K^0 , полагая

$$e'_j = \sum_i b_{ij} e_i.$$

Пользуясь тождеством $b = a(s)s(b)$, видим, что элементы e'_1, \dots, e'_N инвариантны относительно G и, стало быть, принадлежат W^0 . Этим доказана сюръективность отображения $\hat{K}' \otimes_K W^0 \rightarrow W_K^0$, а вместе с этим и теорема.

Доказательство леммы. Пусть π — униформизирующий элемент в кольце \hat{O}' . Зададим фильтрацию

в группе $A = GL(N, \hat{O'})$, полагая $A_n = \{a \in A \mid a \equiv 1 \pmod{\pi^n}\}$. Имеем $A/A_1 \cong GL(N, k'/k)$, где k'/k — поле вычетов расширения K'/K . Более того, при $n \geq 1$ имеют место изоморфизмы $A_n/A_{n+k} \cong M_N(k')$, где $M_N(k')$ — аддитивная группа матриц $N \times N$ с коэффициентами из k' . Лемма следует теперь из тривиальности $H^1(G, GL(N, k'))$ и $H^1(G, M_N(k'))$, где k' рассматривается уже с дискретной топологией (так что это обычные когомологии Галуа, см. [33], стр. 158—159).

Д.2. Допустимые характеристы

Пусть $G = \text{Gal}(\bar{K}/K)$ и $\varphi: G \rightarrow K^*$ — некоторый непрерывный гомоморфизм.

Определение. Характер φ называется *допустимым* (обозначение: $\varphi \sim 1$), если существует такой элемент $x \in C$, $x \neq 0$, что $s(x) = \varphi(s)x$ для всех $s \in G$.

Замечания. 1) Допустимые характеристы образуют подгруппу в группе всех характеристик группы G со значениями в K^* ; для любых характеристик φ и φ' мы будем писать $\varphi \sim \varphi'$, если $\varphi^{-1}\varphi' \sim 1$.

2) Пусть $H^1(G, C^*)$ — одномерная группа когомологий группы G с коэффициентами в C^* (когомологии определены с помощью *непрерывных* коцепей, как и в Д.1). Каждый непрерывный характер $\varphi: G \rightarrow K^*$ является одномерным коциклом и, следовательно, определяет некоторый элемент $\tilde{\varphi}$ в $H^1(G, C^*)$. Имеем $\tilde{\varphi} = \tilde{\varphi}'$, если и только если $\varphi \sim \varphi'$.

3) Определим новое действие группы G на C , полагая

$$(s, c) \mapsto \varphi(s)s(c), \quad s \in G, c \in C.$$

Обозначим полученный C - G -модуль через $C(\varphi)$. Характер φ допустим тогда и только тогда, когда $C(\varphi)$ изоморчен C как C - G -модуль.

Предложение 1. Предположим, что существует такой элемент $c \in C^*$, что $\varphi(s) = s(c)/c$ для всех $s \in G$ из некоторой открытой подгруппы N группы инверции в G . Тогда характер φ допустим.

Доказательство. Пусть K'/K — подрасширение расширения \bar{K}/K , соответствующее подгруппе N . Оно является конечным расширением некоторого неразветвленного расширения. Обозначим через $W = C(\varphi)$ модуль, построенный в замечании 3, и пусть W^0 (соответственно $W_{K'}^0$) — подпространство пространства W , состоящее из всех G -инвариантных элементов (соответственно N -инвариантных). По предположению $W_{K'}^0 \neq 0$. Следовательно, по теореме 1 из Д.1 имеем $W^0 \neq 0$, откуда следует, что φ допустим. Доказательство закончено.

Обозначим через U_C подгруппу единиц в C , через U_C^1 — подгруппу единиц, сравнимых с 1 по модулю максимального идеала, и отождествим \bar{k}^* с группой мультипликативных представителей, так что $U_C = U_C^1 \times \bar{k}^*$ (см. [33], стр. 44). Определим логарифмическое отображение

$$\log: U_C \rightarrow C,$$

полагая

$$\log x = \begin{cases} 0, & \text{если } x \in \bar{k}^*, \\ \sum_{n=1}^{\infty} (-1)^{n-1} (x - 1)^n / n, & \text{если } x \in U_C^1. \end{cases}$$

Это непрерывный гомоморфизм и даже локальный изоморфизм. Более того, имеет место

Лемма. (а) Отображение \log сюръективно.

(б) Ядром $\log: U_C \rightarrow C$ является группа $\bar{k}^* \times \mu_{p^\infty}$, где μ_{p^∞} — группа всех корней p^n -степени из единицы с $n = 1, 2, \dots$.

Утверждение (а) следует из того, что C алгебраически замкнуто и группа U_C поэтому делима.

Для доказательства (б) заметим, что если $u \in U_C^1$ — такой элемент, что $\log u = 0$, то $\lim u^{p^N} = 1$, следовательно, для достаточно большого N u^{p^N} принадлежит некоторой подгруппе группы U_C^1 , на которой \log инъективен (например, подгруппе элементов x , сравнимых

с 1 по $\text{mod } p^2$). Следовательно, $u^{p^N} = 1$ и $u \in \mu_{p^\infty}$, что и доказывает (б).

Применим теперь логарифмическое отображение к группам когомологий группы G с коэффициентами в U_C, C, C^*, \dots (когомологии определяются, как обычно, с помощью *непрерывных* коцепей). Прежде всего, поскольку \mathbf{Q} является группой значений нормирования поля C , имеет место точная последовательность

$$1 \rightarrow U_C \rightarrow C^* \rightarrow \mathbf{Q} \rightarrow 1.$$

По теореме Тейта ([41], § 3.3) $H^0(G, C^*) = K^*$, следовательно, имеем точную последовательность групп когомологий

$$K^* \rightarrow \mathbf{Q} \rightarrow H^1(G, U_C) \rightarrow H^1(G, C^*) \rightarrow 0$$

или

$$0 \rightarrow \mathbf{Q}/\mathbf{Z} \xrightarrow{\delta} H^1(G, U_C) \xrightarrow{i} H^1(G, C^*) \rightarrow 0.$$

Положив $N = \text{Ker}(\log)$, получаем точную последовательность

$$H^1(G, N) \xrightarrow{i} H^1(G, U_C) \xrightarrow{\lambda} H^1(G, C),$$

где λ — гомоморфизм, индуцированный \log . Так как $H^1(G, C)$ является векторным C -пространством, то композиция $\lambda \circ \delta: \mathbf{Q}/\mathbf{Z} \rightarrow H^1(G, C)$ равна 0 и, стало быть, существует единственное отображение

$$L: H^1(G, C^*) \rightarrow H^1(G, C),$$

такое, что $L \circ i = \lambda$.

ПРЕДЛОЖЕНИЕ 2. *Отображение $L: H^1(G, C^*) \rightarrow H^1(G, C)$ инъективно.*

Доказательство. В силу точности предыдущих последовательностей достаточно доказать, что гомоморфизм

$$i \circ j: H^1(G, N) \rightarrow H^1(G, C^*)$$

тривиален. Но поскольку N — дискретная подгруппа группы \bar{K}^* , $i \circ j$ пропускается через $H^1(G, \bar{K}^*)$, где \bar{K} .

рассматривается теперь как дискретная группа; но по теореме 90 группа $H^1(G, \bar{K}^*)$ тривиальна и поэтому гомоморфизм $i \circ j$ нулевой. Это доказывает предложение 2.

Пусть теперь $\varphi: G \rightarrow K^*$ — некоторый непрерывный характер. Поскольку образ $\varphi(G)$ компактен, он содержится в U_K , следовательно, в U_C , и $\log \varphi: G \rightarrow C$ является аддитивным 1-коциклом. Его класс когомологий в $H^1(G, C)$ равен $L\bar{\varphi}$, где $\bar{\varphi}$ — класс когомологий характера φ в $H^1(G, C^*)$.

ПРЕДЛОЖЕНИЕ 3. Свойства $\varphi \sim 1$ и $L\bar{\varphi} = 0$ эквивалентны.

Это следует из инъективности отображения L .

Следствие. Если существует такое целое число $n \neq 0$, что $\varphi^n \sim 1$, то $\varphi \sim 1$.

В самом деле, $L\bar{\varphi} = \frac{1}{n} L\bar{\varphi}^n = 0$.

Замечание. Спрингер доказал, что группа $H^1(G, C)$ имеет размерность 1 над C (см. Тейт [41], § 3.3). Следовательно, в качестве базиса для $H^1(G, C)$ можно взять элемент $L\bar{\chi}$, где χ — фундаментальный характер, определенный в гл. I, п. 1.2. В частности, для любого характера $\varphi: G \rightarrow K^*$ существует элемент $c(\varphi)$ в C , такой, что $L\bar{\varphi} = c(\varphi)L\bar{\chi}$. В случае, когда поле K локально компактно, этот элемент $c(\varphi)$ можно вычислить явно (см. п. Д. 6, упр. 2).

Д.3. Критерий локальной тривиальности

Обозначим через E некоторое подполе поля K , обладающее следующими свойствами:

(а) E содержит \mathbf{Q}_p и $[E : \mathbf{Q}_p] < \infty$ (так что E локально компактно).

(б) Вместе с E полю K принадлежат и все \mathbf{Q}_p -сопряженные с E поля.

Пусть Γ_E обозначает множество всех \mathbf{Q}_p -вложений поля E в K . Рассмотрим некоторый непрерывный характер

$$\psi: \text{Gal}(\bar{K}/K) \rightarrow E^*$$

со значениями в E^* . Тогда для каждого $\sigma \in \Gamma_E$ получаем характер $\sigma \circ \psi: G \rightarrow E^* \xrightarrow{\sigma} K^*$ группы $G = \text{Gal}(\bar{K}/K)$ со значениями в K^* .

ПРЕДЛОЖЕНИЕ 4. Следующие два свойства эквивалентны:

(1) ψ равен 1 на некоторой открытой подгруппе группы инерции в G ,

(2) $\sigma \circ \psi \sim 1$ для всех $\sigma \in \Gamma_E$.

Доказательство. Импликация $(1) \Rightarrow (2)$ тривиально следует из результата, установленного в п. Д. 1 (поскольку мы знаем, что допустимость можно определить с помощью открытой подгруппы группы инерции).

$(2) \Rightarrow (1)$. Здесь мы воспользуемся логарифмическим отображением, определенным в п. Д. 2. Заметим, что ψ принимает значения в группе единиц U_E поля E , поэтому $\log \psi: G \rightarrow E$ корректно определен. Пусть I — группа инерции группы G , тогда подгруппа $\log \psi(I)$ компактна в E и, следовательно, изоморфна \mathbf{Z}_p^n для некоторого n . Обозначим через W векторное \mathbf{Q}_p -подпространство в E , порожденное $\log \psi(I)$. Ясно, что $\log \psi(I)$ является решеткой в W и $\dim W = n$. Заметим, что утверждение „ ψ равно 1 на некоторой открытой окрестности 1 в I “ эквивалентно утверждению, что $\log \psi(I) = 0$ (поскольку $\log U_E \rightarrow E$ — локальный изоморфизм). Предположим, что последнее не имеет места, т. е. $n \geq 1$. Выберем \mathbf{Q}_p -линейное отображение $f: E \rightarrow K$, такое, что $\dim f(W) = 1$; ясно, что оно должно существовать. Согласно теории Галуа (независимость характеров), множество Γ_E составляет базис пространства $\text{Hom}_{\mathbf{Q}_p}(E, K)$. Следовательно, существуют такие элементы $k_\sigma \in K$, что

$$f = \sum_{\sigma \in \Gamma_E} k_\sigma \sigma,$$

и имеет место соотношение

$$f \circ \log \psi = \sum k_\sigma \circ \log \psi = \sum k_\sigma \log (\sigma \circ \psi).$$

Согласно предположению (и предложению 3 из п. Д.2), аддитивный 1-коцикл $\log(\sigma \circ \psi): G \rightarrow K$ когомологичен 0. Следовательно, когомологичен нулю и $f \circ \log \psi$.

Но мы можем считать (заменив, если нужно, f на $p^N f$ с достаточно большим N), что существует непрерывный гомоморфизм $F: U_E \rightarrow U_K$, такой, что $f \circ \log = \log \circ F$. Тогда $\log(F \circ \psi) = f \circ \log \psi$ и поэтому (см. предложение 3 из п. Д. 2) $F \circ \psi \sim 1$, т. е. $F \circ \psi$ — допустимый характер. Но $F \circ \psi$ обладает еще тем свойством, что подгруппа $F \circ \psi(I) \subset U_K$ является p -адической группой Ли размерности 1 (произведение \mathbf{Z}_p на некоторую конечную группу). Это противоречит одной теореме Тейта ([41], § 3, теорема 2). Таким образом, все доказано.

Д.4. Характер χ_E

Сохраним те же предположения относительно E и K , что и в предыдущем пункте. Согласно теории полей классов, группа $\text{Gal}(\bar{E}/E)^{\text{ab}}$ может быть отождествлена с пополнением \hat{E}^* группы E^* в топологии открытых подгрупп конечного индекса. В частности, имеет место точная последовательность

$$1 \rightarrow U_E \rightarrow \text{Gal}(\bar{E}/E)^{\text{ab}} \rightarrow \hat{\mathbf{Z}} \rightarrow 1,$$

где $\hat{\mathbf{Z}} \simeq \prod_l \mathbf{Z}_l$ обозначает пополнение группы \mathbf{Z} относительно топологии подгрупп конечного индекса (см., например, Артин — Тейт [2] или Касселс — Фрёлих [15], гл. VI, § 2).

Пусть π — униформизирующий элемент поля E . Образ элемента π в группе $\text{Gal}(\bar{E}/E)^{\text{ab}}$ порождает подгруппу, замыкание которой изоморфно $\hat{\mathbf{Z}}$. Это доставляет изоморфизм

$$\text{Gal}(\bar{E}/E)^{\text{ab}} \simeq U_E \times \hat{\mathbf{Z}}.$$

Пусть $\text{pr}_\pi: \text{Gal}(\bar{E}/E)^{\text{ab}} \rightarrow U_E$ — проекция, ассоциированная с этим разложением (расширение Галуа поля E , соответствующее $\text{Ker}(\text{pr}_\pi)$, является композитом всех конечных абелевых расширений, для которых π является нормой; см. [15], стр. 224—225).

С другой стороны, вложение $E \rightarrow K$ определяет гомоморфизм $\text{Gal}(K/K) \rightarrow \text{Gal}(\bar{E}/E)$, а также гомоморфизм

$$r_E: G \rightarrow \text{Gal}(\bar{E}/E)^{\text{ab}}.$$

Определим $\chi_{E, \pi}$ (сокращенно χ_E) как композицию гомоморфизмов

$$G \rightarrow \text{Gal}(\bar{E}/E)^{\text{ab}} \rightarrow U_E \xrightarrow{i} U_E,$$

где $i(x) = x^{-1}$, $x \in U_E$. Заметим, что ограничение x_E на группу инерции группы G имеет вид

$$x \mapsto r_E(x^{-1})$$

и поэтому не зависит от выбора π .

ПРЕДЛОЖЕНИЕ 5. Пусть F_π — формальная группа Любина — Тейта ([22], см. также [15], гл. VI, § 3), ассоциированная с E и π . Пусть T — ее модуль Тейта, который свободен и имеет ранг 1 над кольцом целых элементов O_E поля E . Тогда действие группы $\text{Gal}(\bar{K}/K)$ на T задается с помощью характера x_E , определенного выше.

Это следует из основной теоремы работы [22] (см. также [15], теорема 3, стр. 231).

Следствие. Если $E = \mathbf{Q}_p$ и $\pi = p$, то характер χ_E совпадает с характером χ , определенным в гл. I, п. 1.2.

В самом деле, группой Любина — Тейта является в этом случае мультипликативная группа \mathbf{G}_m и ее модулем Тейта — модуль $T_p(\mu)$, определенный в гл. I, п. 1.2.

Замечание. Если поле K локально компактно, то можно отождествить G^{ab} с \hat{K}^* и характер χ_E представить в виде

$$\hat{K}^* \xrightarrow{N} \hat{E}^* \xrightarrow{\text{pr}_\pi} U_E \xrightarrow{i} U_E,$$

где $N = N_{K/E}$ — норменное отображение. [Это следует из функториальных свойств „закона взаимности“ в локальной теории полей классов.]

В частности, ограничение χ_E на подгруппу инерции U_K группы G^{ab} имеет вид $x \mapsto N_{K/E}(x^{-1})$.

Д.5. Характеры, ассоциированные с разложением Ходжа — Тейта

В обозначениях предыдущего пункта пусть $\rho: G \rightarrow U_E$ — некоторый непрерывный гомоморфизм. Рассмотрим одномерное векторное пространство V над E и определим

действие G на V формулой

$$(s, y) \mapsto \rho(s)y, \quad s \in G, \quad y \in V.$$

Таким образом, V становится G -модулем. Пусть $W = C \otimes_{\mathbf{Q}_p} V$, где $C = \widehat{\bar{K}}$, как и раньше. W является d -мерным векторным пространством над C , где $d = [E : \mathbf{Q}_p]$. Каждый элемент x поля E определяет C -эндоморфизм a_x пространства W с помощью формулы

$$a_x(\sum c_i \otimes y_i) = \sum c_i \otimes xy_i, \quad c_i \in C, \quad y_i \in V.$$

Мы получаем, таким образом, некоторое представление E в векторном C -пространстве W ; отметим, что действие a_x коммутирует с действием G .

Положим для $\sigma \in \Gamma_E$

$$W_\sigma = \{w \mid w \in W, \quad a_x(w) = \sigma(x)w, \quad x \in E\}.$$

Лемма 1. (а) *Каждое из W_σ является одномерным векторным C -пространством, инвариантным относительно G .*

(б) *Пространство W является прямой суммой подпространств W_σ , $\sigma \in \Gamma_E$.*

(в) *Как модуль Галуа W_σ изоморчен модулю $C(\sigma \circ \rho)$ для любого $\sigma \in \Gamma_E$.*

[Определение „скрученного“ модуля $C(\sigma \circ \rho)$ см. в. п. Д.2, замечание 3.]

Доказательство. Утверждения (а) и (б) являются следствиями того хорошо известного факта, что $C \otimes_{\mathbf{Q}_p} E$ есть произведение d экземпляров поля C , причем проекции $C \otimes_{\mathbf{Q}_p} E \rightarrow C$ соответствуют элементам из Γ_E .

Для доказательства (в) заметим, что такое же разложение имеет место и для $V_K = K \otimes_{\mathbf{Q}_p} V$, поскольку K содержит все поля, \mathbf{Q}_p -сопряженные с E . Следовательно, для каждого $\sigma \in \Gamma_E$ существует элемент $w \in W_\sigma$, содержащийся в V_K . Если w представлен в виде $w = \sum k_i \otimes y_i$, $k_i \in K$, $y_i \in V$, то

$$s(w) = \sum k_i \otimes s(y_i) = \sum k_i \otimes \rho(s)y_i = a_{\rho(s)}w = \sigma \circ \rho(s)w,$$

поскольку w принадлежит W_σ . Отсюда следует, что W_σ изоморфно $C(\sigma \circ \rho)$. Доказательство закончено.

Пусть ρ_1 и ρ_2 — характеристы группы G со значениями в K^* . Будем писать $\rho_1 \equiv \rho_2$, если они совпадают на некоторой подгруппе группы инерции в G .

Теорема 2. *Пусть ρ, V, W — такие же, как выше, и пусть для каждого $\sigma \in \Gamma_E$ задано целое число n_σ . Тогда следующие условия эквивалентны:*

$$(i) \quad \rho \equiv \prod_{\sigma \in \Gamma_E} \sigma^{-1} \circ \chi_{\sigma E}^{n_\sigma};$$

$$(ii) \quad \sigma \circ \rho \sim \chi^{n_\sigma} \text{ для всех } \sigma \in \Gamma_E;$$

(iii) модуль Галуа W_σ изоморчен модулю $C(\chi^{n_\sigma})$ для каждого $\sigma \in \Gamma_E$.

[Напомним, что χ — это характер, определенный в гл. I, п. 1.2, и $\chi_{\sigma E}$ — характер, связанный с подполем $\sigma E \subset K$, как в п. Д.4. Отметим, что, поскольку ограничение характера $\chi_{\sigma E}$ на группу инерции зависит только от σE , условие (i) имеет смысл.]

Следствие. *Модуль V имеет тип Ходжа — Тейта тогда и только тогда, когда существуют такие $n_\sigma \in \mathbf{Z}$, что $\rho \equiv \prod_{\sigma \in \Gamma_E} \sigma^{-1} \circ \chi_{\sigma E}^{n_\sigma}$.*

Это вытекает из (iii) и того факта, что $W = C \otimes V$ является прямой суммой пространств W_σ .

Доказательство теоремы 2. Докажем сначала следующую лемму:

Лемма 2. (а) $\chi_E \sim \chi$.

(б) *Если $\sigma \in \Gamma_E$ не является тождественным вложением, то $\sigma \chi_E \sim 1$.*

Доказательство. Пусть π — унiformизирующий элемент поля E , F_π — группа Любина — Тейта, ассоциированная с E и π , T_π — ее модуль Тейта и $V_\pi = T_\pi \otimes \mathbf{Q}_p$. Так как V_π — одномерное векторное пространство над E и G действует на V_π посредством гомоморфизма $\chi_E: G \rightarrow U_E$ (ср. п. Д.4, предложение 5), то предыдущие конструкции применимы к V_π и χ_E . По теореме Тейта ([41], § 4,

следствие 2 теоремы 3) модуль $W_\pi = C \otimes_{\mathbb{Q}_p} V_\pi$ обладает разложением Ходжа — Тейта вида

$$W_\pi = W_\pi(0) \oplus W_\pi(1),$$

где $\dim W_\pi(0) = d - 1$, $\dim W_\pi(1) = 1$. Точнее, Тейт определяет канонические изоморфизмы $W_\pi(0) = C \otimes_K \text{Hom}_E(t', K)$, где t' есть $d - 1$ -мерное касательное пространство двойственного к F_π объекта, и $W_\pi(1) = (C \otimes_{\mathbb{Q}_p} V_p(\mu)) \otimes_K t$, где t — одномерное касательное пространство к F_π и $V_p(\mu)$ — векторное \mathbb{Q}_p -пространство размерности 1, определенное в гл. I, п. 1.2.

Заметим, что $C \otimes_{\mathbb{Q}_p} V_p(\mu)$ изоморфно $C(\chi)$, поэтому мы получаем изоморфизм

$$W_\pi(1) \simeq C(\chi) \otimes_K t.$$

Все эти изоморфизмы коммутируют с действием E .

Поскольку E действует на t посредством отображения вложения $\sigma_1: E \rightarrow K$, это показывает, что компонента $(W_\pi)_\sigma$ модуля W_π совпадает с $W_\pi(1)$. Поэтому, пользуясь леммой 1, получаем изоморфизм $C(\chi) \simeq C(\chi_E)$, откуда $\chi_E \sim \chi$, что доказывает утверждение (а).

Те же рассуждения показывают, что $(W_\pi)_\sigma$, $\sigma \neq \sigma_1$, содержатся в другом слагаемом $W_\pi(0)$ модуля W_π . Следовательно, $C(\sigma \circ \chi_E) \simeq C(1)$ (где 1 означает, конечно, единичный характер). Это доказывает утверждение (б), а вместе с ним и лемму.

Возвратимся к доказательству теоремы 2. Эквивалентность условий (ii) и (iii) следует из леммы 1. Для того чтобы доказать эквивалентность (i) \Leftrightarrow (ii), заметим прежде всего, что характер $\chi_{\sigma E}$ принимает значения в σE^* , следовательно, $\sigma^{-1} \circ \chi_{\sigma E}$ принимает значения в E^* и то же самое верно для $\rho_1 = \prod_{\sigma \in \Gamma_E} \sigma^{-1} \circ \chi_{\sigma E}^{n_\sigma}$.

Пусть $\tau \in \Gamma_E$. Имеем

$$\tau \circ \rho_1 = \prod_{\sigma \in \Gamma_E} \tau \circ \sigma^{-1} \circ \chi_{\sigma E}^{n_\sigma}.$$

Из леммы 2, примененной к полю σE , следует, что $\tau \circ \sigma^{-1} \circ \psi_{\sigma E} \sim 1$, если $\tau \circ \sigma^{-1}$ не тождественно на σE ,

т. е. если $\tau \neq \sigma$. Если $\tau = \sigma$, то $\tau \circ \sigma^{-1} \circ \psi_{\sigma E} = \chi_{\sigma E} \sim \chi$. Следовательно, $\tau \circ \rho_1 \sim \chi^{\tau}$ и условие (ii) эквивалентно следующему:

$$\tau \circ \rho_1 \sim \tau \circ \rho \quad \text{для всех } \tau \in \Gamma_E.$$

В силу предложения 3 из п. Д.3 последнее эквивалентно условию $\rho_1 \equiv \rho$, что и требовалось доказать.

Д.6. Локально компактный случай

Добавим ко всем предыдущим предположениям относительно K и E еще одно: K конечно над \mathbf{Q}_p (т. е. K локально компактно). Согласно локальной теории полей классов можно тогда отождествить G^{ab} с \hat{K}^* и подгруппу инерции группы G^{ab} с группой единиц U_K поля K .

Пусть T (соответственно T_E , $T_{\sigma E}$) есть \mathbf{Q}_p -тор, ассоциированный с K (соответственно с E , σE , где $\sigma \in \Gamma_E$), см. п. 1.1. Норменное отображение из K в σE определяет алгебраический морфизм

$$N_{K/\sigma E}: T \rightarrow T_{\sigma E}.$$

В композиции с $\sigma^{-1}: T_{\sigma E} \rightarrow T_E$ он дает морфизм

$$r_\sigma = \sigma^{-1} \circ N_{K/\sigma E}: T \rightarrow T_E.$$

ПРЕДЛОЖЕНИЕ 6. (а) $r_\sigma(u^{-1}) = \sigma^{-1} \circ \chi_{\sigma E}(u)$ для всех $u \in U_K$.

(б) Элементы r_σ , $\sigma \in \Gamma_E$, образуют \mathbf{Z} -базис группы $\text{Hom}_{\text{alg}}(T, T_E)$.

[Отметим, что (а) имеет смысл, поскольку группу U_K можно отождествить с группой инерции группы G^{ab} .]

Доказательство. Утверждение (а) следует из замечания в конце п. Д.4. Для доказательства (б) рассмотрим группы характеров $X(T)$ и $X(T_E)$ торов T и T_E соответственно. Характеры $[s]$, $s \in \Gamma_K$ (соответственно $[\sigma]$, $\sigma \in \Gamma_E$), образуют базис группы $X(T)$ (соответственно $X(T_E)$). Морфизм $r_\sigma: T \rightarrow T_E$ определяет посредством транспозиции морфизм

$$X(r_\sigma): X(T_E) \rightarrow X(T).$$

Легко проверить, что на базисе $[\tau]$, $\tau \in \Gamma_E$, морфизм $X(r_\sigma)$ принимает следующие значения:

$$X(r_\sigma)([\tau]) = \sum_{s\sigma=\tau} [s].$$

Утверждение (б) вытекает теперь из следующего факта.

ЛЕММА. Элементы $X(r_\sigma)$, $\sigma \in \Gamma_E$, образуют базис в $\text{Hom}_{\text{Gal}}(X(T_E), X(T))$.

Доказательство. Независимость элементов $X(r_\sigma)$ очевидна. Далее, пусть $\varphi \in \text{Hom}_{\text{Gal}}(X(T_E), X(T))$ — такой элемент, что

$$\varphi([\tau]) = \sum n(\tau, s)[s].$$

Если $a \in \text{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$ действует тождественно на τE , то $a[\tau] = [\tau]$, следовательно, $a\varphi([\tau]) = \varphi([\tau])$, т. е. $n(\tau, as) = n(\tau, s)$ для всех $s \in \Gamma_K$. Это означает, что $n(\tau, s)$ зависит только от элемента $\sigma = s^{-1}\tau$. Положим $n_\sigma = n(\tau, s)$, тогда

$$\varphi([\tau]) = \sum_{\sigma \in \Gamma_E} n_\sigma \sum_{s\sigma=\tau} [s] = \sum_{\sigma \in \Gamma_E} n_\sigma X(r_\sigma)([\tau]),$$

что доказывает лемму.

ПРЕДЛОЖЕНИЕ 7. Пусть ρ и (n_σ) , $\sigma \in \Gamma_E$, такие же, как и в теореме 2 из п. Д.5. Определим морфизм $r: T \rightarrow T_E$ формулой

$$r = \prod_{\sigma \in \Gamma_E} r_\sigma^{n_\sigma}.$$

Тогда равносильные свойства (i), (ii) и (iii) из теоремы 2 эквивалентны следующему:

(iv) Существует такая открытая подгруппа U' подгруппы инерции U_K группы G^{ab} , что $r(u)\rho(u) = 1$, если $u \in U'$.

В самом деле, свойство (iv) является просто перформулировкой свойства (i), так как мы знаем, что $\sigma^{-1} \circ \chi_{\sigma E}(u) = r_\sigma(u^{-1})$, если $u \in U_K$.

Следствие. Следующие условия эквивалентны:

(а) представление ρ локально алгебраично;

(б) модуль Галуа V , связанный с ρ , имеет тип Ходжа — Тейта.

Это вытекает из теоремы 2 в комбинации с предложениями 6 и 7.

Упражнения 1) а) Пусть $A = \text{End}_{\mathbf{Q}_p}(K)$ — пространство \mathbf{Q}_p -линейных эндоморфизмов K . Обозначим через $\text{Tr}(a)$, $a \in A$, след эндоморфизма a и через u_x , $x \in K$, эндоморфизм вида $y \mapsto xy$. Показать, что для любого $a \in A$ существует единственный элемент $c_K(a) \in K$, такой, что

$$\text{Tr}(u_x \circ a) = \text{Tr}_{K/\mathbf{Q}_p}(xc_K(a)) \quad \text{для всех } x \in K.$$

б) Показать, что так определенное отображение $c_K: A \rightarrow K$ является K -линейным в любой из двух естественных структур векторного K -пространства на A .

в) Пусть $\{e_i\}$ — базис K над \mathbf{Q}_p и $\{e'_i\}$ — двойственный ему базис, так что $\text{Tr}_{K/\mathbf{Q}_p}(e_i e'_j) = \delta_{ij}$.

Показать, что

$$c_K(a) = \sum a(e_i) e'_i, \quad a \in A.$$

г) Пусть $L \supset K$ и $a \in A$; показать тогда, что

$$c_L(a \circ \text{Tr}_{L/K}) = c_K(a).$$

Показать также, что $c_K(\text{Tr}_{K/\mathbf{Q}_p}) = 1$.

д) Пусть K — расширение Галуа поля \mathbf{Q}_p ; показать тогда, что $c_K(\sigma) = 0$ для каждого $\sigma \in \text{Gal}(K/\mathbf{Q}_p)$, $\sigma \neq \text{id}$ и $c_K(\text{id}) = 1$.

2) Пусть $\varphi: G^{\text{ab}} \rightarrow K^*$ — некоторый непрерывный гомоморфизм, и пусть a_φ — такой \mathbf{Q}_p -линейный эндоморфизм K , что диаграмма

$$\begin{array}{ccc} U_K & \xrightarrow{\varphi} & U_K \\ \downarrow \log & & \downarrow \log \\ K & \xrightarrow{a_\varphi} & K \end{array}$$

коммутативна. Обозначим через $L\bar{\varphi}$ (соответственно $L\bar{\chi}$) образ гомоморфизма φ (соответственно χ) в одномерном

векторном C -пространстве $H^1(G, C)$, см. п. Д.2. Показать, что $L\bar{\varphi} = cL\tilde{\chi}$, где $c = -c_K(a_\varphi)$. [Сначала проверить это в случае, когда K — расширение Галуа поля \mathbf{Q}_p и $\varphi = \sigma^{-1} \circ \chi_K$, $\sigma \in \text{Gal}(K/\mathbf{Q}_p)$; здесь $a_\varphi = -\sigma^{-1}$ и $c_K(a_\varphi)$ определено в упражнении 1) г).]

В частности, характер φ допустим тогда и только тогда, когда $c_K(a_\varphi) = 0$.

Д.7. Теорема Тейта

Напомним еще раз (см. п. 1.2) ее формулировку (поле K локально компактно).

ТЕОРЕМА 3. *Пусть V — конечномерное векторное пространство над \mathbf{Q}_p и $\rho: G^{ab} \rightarrow \text{Aut } V$ — абелево p -адическое представление поля K . Тогда следующие условия эквивалентны:*

- (1) ρ локально алгебраично,
- (2) ρ имеет тип Ходжа — Тейта и его ограничение на группу инерции полупросто.

Доказательство. Как мы уже отмечали (см. п. 1.1), из (1) следует, что

(*) *ограничение ρ на группу инерции полупросто.* Поэтому мы можем считать, что утверждение (*) выполнено.

Пусть π — униформизирующий элемент поля K и pr_π — проекция группы G^{ab} на ее группу инерции U_K , ассоциированная с выбором π (см. Касселс — Фрёлих [15]). Определим новое представление ρ' группы G^{ab} , полагая

$$\rho' = \rho \circ \text{pr}_\pi.$$

Замена ρ на ρ' не нарушает локальную алгебраичность (очевидно) и не влияет также на свойство иметь тип Ходжа — Тейта (это следует из п. Д.1, следствие 2 теоремы 1). Поскольку из (*) вытекает, что ρ' полупросто, то после замены ρ на ρ' мы можем предполагать, что этим свойством обладает ρ , и даже считать (с помощью легкой редукции), что ρ просто. Обозначим тогда через $E \subset \text{End}(V)$ коммутант представления ρ . Так как ρ

абелево и просто, то E — поле конечной степени над \mathbf{Q}_p и V — одномерное векторное пространство над E ; представление ρ в таком случае задается непрерывным характером $\rho: G \rightarrow E^*$.

Пусть K' — конечное расширение поля K , настолько большое, чтобы содержать все поля, \mathbf{Q}_p -сопряженные с E . Условия (1) и (2) для поля K' обозначим через (1') и (2'). Мы знаем (см. п. 1.1), что $(1) \Leftrightarrow (1')$. С другой стороны, следствие 2 теоремы 1 из п. Д.1 дает $(2) \Leftrightarrow (2')$. Достаточно поэтому доказать, что $(1') \Leftrightarrow (2')$, а это было установлено в п. Д.6 (следствие предложения 7). Теорема полностью доказана.

ГЛАВА IV

l-АДИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ,
СВЯЗАННЫЕ С ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

Пусть K — числовое поле и E — эллиптическая кривая над K . Для простого числа l рассмотрим соответствующее l -адическое представление

$$\rho_l: \mathrm{Gal}(\bar{K}/K) \rightarrow \mathrm{Aut}(V_l(E))$$

(см. гл. I, п. 1.2). Основным результатом этой главы является вычисление алгебры Ли l -адической группы Ли $G_l = \mathrm{Im} \rho_l$. Оно основано на теореме конечности Шафаревича (п. 1.4) в комбинации со свойствами локально алгебраических абелевых представлений (гл. III) и локальной теории Тейта эллиптических кривых с нецелым модулярным инвариантом (добавление, Д.1). Вариация G_l в зависимости от l изучается в § 3.

Аналогичные результаты в локальном случае (т. е. когда K — локальное поле) изложены в добавлении.

§ 1. Предварительные результаты

1.1. Эллиптические кривые (см. Касселс [14], Дой-ринг [12], Игуза [13])

Под эллиптической кривой мы будем понимать одномерное абелево многообразие, т. е. полную неособую связную кривую рода 1 с фиксированной рациональной точкой P_0 , выбираемой за начало группового закона (и часто обозначаемой через 0).

Пусть E — такая кривая. Хорошо известно, что ее можно вложить в проективную плоскость \mathbf{P}_K^2 в виде неособой кубики так, чтобы P_0 стала точкой перегиба (это вложение задается полной линейной системой, содержащей дивизор $3P_0$). При таком вложении сумма

трех точек P_1, P_2, P_3 тогда и только тогда равна 0, когда дивизор $P_1 + P_2 + P_3$ является пересечением кривой E с прямой в \mathbf{P}_K^2 . В подходящим образом выбранной системе координат уравнение кривой E можно записать в вейерштрасовой форме:

$$y^2 = 4x^3 - g_2x - g_3,$$

где x, y — неоднородные координаты. Точка P_0 в этом случае является бесконечно удаленной точкой на оси y . Дискриминант

$$\Delta = g_2^3 - 27g_3^2$$

отличен от нуля.

Коэффициенты g_2 и g_3 определяются с точностью до преобразований $g_2 \mapsto u^4 g_2$, $g_3 \mapsto u^6 g_3$, $u \in K^*$. Модулярный инвариант j кривой E имеет вид

$$j = 2^{6}3^3 \frac{g_2^3}{g_2^3 - 27g_3^2} = 2^{6}3^3 \frac{g_2^3}{\chi}.$$

Две эллиптические кривые имеют один и тот же инвариант тогда и только тогда, когда они становятся изоморфными над алгебраическим замыканием поля K .

[Все это справедливо над любым полем, кроме случаев характеристики 2 или 3, когда уравнение E следует записывать в более общем виде:

$$y^2 + a_1xy + a_3y + x^3 + a_2x^2 + a_4x + a_6 = 0.$$

Здесь также 0 является бесконечно удаленной точкой по оси y , касательная в ней совпадает с бесконечно удаленной прямой. За соответствующими определениями Δ и j мы отсылаем к Дойрингу [12] или Оггу [25]; отметим, однако, что в формуле Огга для Δ имеется ошибка: коэффициент при β_4^3 должен быть -8 вместо -1 .]

1.2. Хорошая редукция

Пусть $v \in \Sigma_K$ — точка числового поля K . Обозначим через O_v (соответственно \mathfrak{m}_v, k_v) соответствующее локальное кольцо (соответственно его максимальный идеал, его поле вычетов).

Пусть E — эллиптическая кривая над K . Будем говорить, что E имеет *хорошую редукцию* в v , если можно выбрать такую систему координат в \mathbf{P}_K^2 , что соответ-

ствующее уравнение f для E имеет коэффициенты в O_v , и его редукция $\tilde{f} \bmod m_v$ определяет *неособую* кубику (следовательно, эллиптическую кривую) \tilde{E}_v , над полем вычетов k_v (иными словами, дискриминант $\Delta(f)$ уравнения f должен быть обратимым элементом кольца O_v). Кривая \tilde{E}_v называется *редукцией* кривой E в точке v , она не зависит от выбора f , при условии, конечно, что $\Delta(f) \in O_v^*$.

Можно доказать, что это определение эквивалентно следующему: существует абелева схема E_v над $\text{Spec } O_v$ в смысле Мамфорда [23], гл. VI, общий слой которой равен E ; схема E_v в таком случае единственна, и ее замкнутый слой есть \tilde{E}_v . Заметим, что \tilde{E}_v определена над конечным полем k_v ; ее эндоморфизм Фробениуса мы обозначим через F_v .

Из любого определения видно, что E имеет *хорошую редукцию почти для всех точек поля K* .

Если E имеет хорошую редукцию в точке v , то ее j -инвариант является целым в v (т. е. принадлежит O_v) и его редукция $\tilde{j} \bmod m_v$ будет j -инвариантом редуцированной кривой \tilde{E}_v .

Обратное почти верно, но не совсем: если j принадлежит O_v , то существует такое конечное расширение L поля K , что $E \times_K L$ имеет хорошую редукцию во всех точках поля L , делящих v (это — „потенциально хорошая редукция“ в смысле Серра — Тейта [36], § 2). Доказательство этого факта можно найти у Дойринга [12], § 4, п. 3.

Замечание. Определение и результаты этого пункта относятся не только к числовым полям. Они имеют смысл для произвольного поля с дискретным нормированием.

1.3. Свойства модуля V_l для хорошей редукции

Пусть l — простое число. Определим, как в гл. I, п. 1.2, модули Галуа T_l и V_l , полагая

$$V_l = T_l \otimes \mathbf{Q}_l, \quad T_l = \varprojlim E_{l^n},$$

где E_{l^n} — ядро эндоморфизма $l^n: E(\bar{K}) \rightarrow E(\bar{K})$.

Обозначим через ρ_l соответствующий гомоморфизм $\text{Gal}(\bar{K}/K)$ в группу $\text{Aut } T_l$. Напомним, что T_l , E_{l^n} и V_l имеют ранг 2 над $\mathbf{Z}/l^n\mathbf{Z}$, \mathbf{Z}_l и \mathbf{Q}_l соответственно.

Пусть v — точка поля K с $p_v \neq l$ и \bar{v} — некоторое ее продолжение в \bar{K} . Обозначим через D (соответственно I) группу разложения \bar{v} (соответственно группу инерции, см. гл. I, п. 2.1). Если E имеет хорошую редукцию в v , то легко видеть, что \bar{v} определяет изоморфизм E_{l^n} с соответствующей группой для редуцированной кривой \tilde{E}_v . В частности, E_{l^n} , T_l , V_l неразветвлены в v (гл. I, п. 2.1), и автоморфизм Фробениуса F_{v, ρ_l} модуля T_l соответствует эндоморфизму Фробениуса F_v кривой \tilde{E}_v . Поэтому

$$\det(F_{v, \rho_l}) = \det(F_v) = Nv$$

и

$$\det(1 - F_{v, \rho_l}) = \det(1 - F_v) = 1 - \text{Tr } F_v + Nv$$

равно числу k_v -точек кривой \tilde{E}_v .

Обратно, имеет место следующий

Критерий Нерона — Огга — Шафаревича. *Если V_l неразветвлено в v для некоторого $l \neq p_v$, то E имеет хорошую редукцию в точке v .*

Доказательство см. Сеpp — Тейт [36], § 1.

Следствие. *Пусть E и E' — эллиптические кривые, изогенные над K . Тогда если одна из них имеет хорошую редукцию в точке v , то этим же свойством обладает и вторая.*

[Напомним, что две кривые E и E' называются изогенными, если существует нетривиальный морфизм $E \rightarrow E'$.]

Это непосредственно вытекает из теоремы, поскольку l -адические представления, ассоциированные с E и E' , изоморфны.

Замечание. Прямое доказательство этого факта имеется у Койцуми — Шимуры [16].

Упражнение. Пусть S — конечное множество точек поля K , в которых E не имеет хорошей редукции. Для $v \in \Sigma_K \setminus S$ обозначим через t_v число k_v -точек редуцированной кривой \tilde{E}_v .

(а) Пусть l — простое и m — целое положительные числа. Показать, что следующие свойства эквивалентны:

- (i) $t_v \equiv 0 \pmod{l^m}$ для всех $v \in \Sigma_K \setminus S$, $\rho_v \neq l$;
- (ii) множество точек $v \in \Sigma_K \setminus S$, таких, что $t_v \equiv 0 \pmod{l^m}$, имеет плотность 1 (см. гл. I, п. 2.2);
- (iii) для каждого $s \in \text{Im } \rho_l$ $\det(1 - s) \equiv 0 \pmod{l^m}$.

[Эквивалентность (ii) и (iii) следует из теоремы о плотности Чеботарева. Импликации (i) \Rightarrow (ii) и (iii) \Rightarrow (i) устанавливаются легко.]

(б) Положим $m = 1$. Показать, что свойства (i), (ii) и (iii) станут эквивалентными следующему:

(iv) существует такая эллиптическая кривая E' над K , что

(α) либо E' изоморфна E , либо существует изогения $E' \rightarrow E$ степени l ;

(β) группа $E'(K)$ содержит элемент порядка l .

[Импликация (iv) \Rightarrow (iii) проста. Для доказательства обратной импликации надо воспользоваться упражнением 2 гл. I, п. 1.1.]

1.4. Теорема Шафаревича

Она заключается в следующем (см. [43]).

Теорема. Пусть S — конечное множество точек поля K . Тогда множество классов изоморфных эллиптических кривых над K , имеющих хорошую редукцию всюду вне S , конечно.

Учитывая тот факт, что изогенные кривые имеют одно и то же множество точек с плохой редукцией (см. п. 1.3), получаем

Следствие. Пусть E — эллиптическая кривая над K . Тогда с точностью до изоморфизма существует только конечное число эллиптических кривых, K -изогенных E .

Для доказательства теоремы Шафаревича нам понадобится следующий критерий хорошей редукции.

Лемма. Пусть S — конечное множество точек поля K , содержащее делители элементов 2 и 3 и такое, что O_S — кольцо S -целых элементов — является кольцом главных идеалов. Тогда эллиптическая кривая E , определенная над K , имеет хорошую редукцию вне S тогда и только тогда, когда ее уравнение может быть приведено к вейерштрасовой форме $y^2 = 4x^3 - g_2x - g_3$ с $g_i \in O_S$ и с $\Delta = g_2^3 - 27g_3^2 \in O_S^*$ (O_S^* — группа единиц кольца O_S).

Доказательство. Достаточность тривиальна. Чтобы доказать необходимость, запишем кривую E в виде

$$y^2 = 4x^3 - g'_2x - g'_3, \quad (*)$$

где $g'_i \in K$. Пусть v — точка поля K , не содержащаяся в S . Тогда, поскольку редукция в v хорошая и делители элементов 2 и 3 содержатся в S , кривая E может быть записана в виде

$$y^2 = 4x^3 - g_{2,v}x - g_{3,v},$$

где $g_{i,v}$ принадлежат локальному кольцу точки v и дискриминант Δ_v является единицей этого кольца. В силу свойств вейерштрасовой формы существует такой элемент $u_v \in K^*$, что $g_{2,v} = u_v^4 g'_2$, $g_{3,v} = u_v^6 g'_3$, $\Delta_v = u_v^{12} \Delta'$; более того, можно считать, что $g_{i,v} = g'_i$ для почти всех v , т. е. $u_v = 1$ для почти всех $v \notin S$. Так как кольцо O_S является кольцом главных идеалов, существует элемент $u \in K^*$ с $v(u) = v(u_v)$ для всех $v \notin S$. Тогда после замены x на $u^{-2}x$, y на $u^{-3}y$ в уравнении $(*)$ кривая E примет вид

$$y^2 = 4x^3 - g_2x - g_3,$$

где $g_2 = u^4 g'_2$, $g_3 = u^6 g'_3$ и $\Delta = u^{12} \Delta'$. Это доказывает лемму, поскольку по построению $g_i \in O_S$ и $\Delta \in O_S^*$.

Доказательство теоремы. Добавив, если нужно, к S конечное число точек, мы можем считать, что S содержит все делители элементов 2 и 3 и что

O_S — кольцо главных идеалов. Если кривая E имеет хорошую редукцию вне S , то по предыдущей лемме ее можно представить в виде

$$y^2 = 4x^3 - g_2x - g_3, \quad (*)$$

где $g_i \in O_S$ и $\Delta = g_2^3 - 27g_3^2 \in O_S^*$. Но поскольку мы можем умножить Δ на любой элемент $u \in (O_S^*)^{12}$ и группа $O_S^*/(O_S^*)^{12}$ конечна, существует такое конечное множество $X \subset O_S^*$, что любую эллиптическую кривую указанного типа можно записать в форме $(*)$ с $g_i \in O_S$ и $\Delta \in X$. Заметим теперь, что при заданном Δ уравнение

$$U^3 - 27V^2 = \Delta$$

определяет некоторую аффинную эллиптическую кривую. По теореме Зигеля (обобщенной Малером и Ленгом [19], гл. VII) это уравнение имеет только *конечное* число решений в O_S . Это завершает доказательство теоремы.

Замечание. Существует много способов выводить теорему Шафаревича из теоремы Зигеля. Изложенный вывод был указан мне Тейтом.

§ 2. Модули Галуа, связанные с кривой E

В этом параграфе через E обозначается эллиптическая кривая, определенная над K . Нас будет интересовать структура модулей Галуа $E_{\ell^n}, T_{\ell}, V_{\ell}$, определенных в п. 1.3.

2.1. Теорема о неприводимости

Напомним прежде всего, что кольцо $\text{End}_K(E)$ K -эндоморфизмы кривой E либо изоморфно \mathbf{Z} , либо имеет ранг 2 над \mathbf{Z} . В первом случае мы будем говорить, что E „не имеет комплексного умножения над K “. Если это остается верным при любом конечном расширении поля K , то будем говорить, что E „не имеет комплексного умножения“.

Теорема. Предположим, что E не имеет комплексного умножения над K . Тогда

- (а) модуль V_l неприводим для любого простого числа l ;
 (б) модуль E_l неприводим для почти всех l .

Для доказательства нам понадобится следующий элементарный результат.

Лемма. Пусть E — эллиптическая кривая, определенная над K с $\text{End}_K(E) = \mathbf{Z}$. Тогда если $E' \rightarrow E$, $E'' \rightarrow E$ суть K -изогении с неизоморфными циклическими ядрами, то E' не изоморфна E'' над K .

Доказательство. Пусть n' и n'' — порядки ядер изогений $E' \rightarrow E$ и $E'' \rightarrow E$ соответственно. Предположим, что существует K -изоморфизм $E' \rightarrow E''$. Пусть $E \rightarrow E'$ — изогения, инверсная к $E' \rightarrow E$. Она тоже имеет циклическое ядро порядка n' , и, следовательно, ядром изогении $E \rightarrow E$, полученной посредством композиции $E \rightarrow E'$, $E' \rightarrow E''$ и $E'' \rightarrow E$, будет некоторое расширение группы $\mathbf{Z}/n''\mathbf{Z}$ при помощи группы $\mathbf{Z}/n'\mathbf{Z}$. Но так как $\text{End}_K(E) = \mathbf{Z}$, то изогения $E \rightarrow E$ должна быть умножением на некоторое целое число a и, следовательно, ее ядро должно иметь вид $\mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/a\mathbf{Z}$. Стало быть, n' и n'' делят a . Так как $a^2 = n'n''$, то $a = n' = n''$, что противоречит предложению.

Доказательство теоремы. (а) Достаточно показать, что если $\text{End}_K(E) = \mathbf{Z}$, то не существует одномерного \mathbf{Q}_l -подпространства пространства V_l , инвариантного относительно группы $\text{Gal}(\bar{K}/K)$. Предположим, что такое подпространство есть. Пусть X — его пересечение с T_l , тогда X будет подмодулем модуля T_l , причем X и T_l/X будут свободными \mathbf{Z}_l -модулями ранга 1. Для $n \geq 0$ рассмотрим образ $X(n)$ модуля X в $E_{l^n} = T/l^nT$. Это циклический подмодуль модуля E_{l^n} порядка l^n , инвариантный относительно $\text{Gal}(\bar{K}/K)$. Следовательно, он соответствует конечной алгебраической K -подгруппе в E и можно построить факторкривую $E(n) = E/X(n)$. Ядро изогении $E \rightarrow E(n)$ является циклическим и имеет порядок l^n . По предыдущей лемме кривые $E(n)$, $n \geq 0$, попарно не изоморфны, что противоречит следствию теоремы Шафаревича (п. 1.4).

(б) Если модуль E_l приводим, то существует подмодуль Галуа X_l в E , имеющий размерность 1 над \mathbf{F}_l . Так же, как и выше, он определяет изогению $E \rightarrow E/X_l$ с циклическим ядром порядка l . Кривые, соответствующие разным l , не изоморфны по предыдущей лемме, и мы опять можем воспользоваться следствием теоремы Шафаревича. Доказательство закончено.

Замечание. Часть (а) этой теоремы можно доказать совершенно иным методом (см. [29], § 3, 4); вместо теоремы Шафаревича используются свойства подгрупп разложения и инерции в $\text{Im } \rho_l$ (см. добавление).

2.2. Вычисление алгебры Ли группы G_l

Пусть $G_l = \text{Im } \rho_l$ — образ группы $\text{Gal}(\bar{K}/K)$ в группе $\text{Aut } T_l$, и пусть $\mathfrak{g}_l \subset \text{End}(V_l)$ — алгебра Ли группы G_l .

Теорема. *Если кривая E не имеет комплексного умножения (см. п. 2.1), то $\mathfrak{g}_l = \text{End}(V_l)$, т. е. группа G_l открыта в группе $\text{Aut } T_l$.*

Доказательство. Теорема о неприводимости из п. 2.1 показывает, что для любой открытой подгруппы U группы G_l модуль V_l неприводим как U -модуль. Следовательно, V_l неприводим и как \mathfrak{g}_l -модуль. По лемме Шура это означает, что централизатор \mathfrak{g}'_l алгебры \mathfrak{g}_l в $\text{End}(V_l)$ является полем, и, так как $\dim V_l = 2$, это поле есть либо \mathbf{Q}_l , либо квадратичное расширение поля \mathbf{Q}_l . Если $\mathfrak{g}'_l = \mathbf{Q}_l$, то \mathfrak{g}_l совпадает либо со всем $\text{End}(V_l)$, либо с подалгеброй $sl(V_l) \subset \text{End}(V_l)$, состоящей из эндоморфизмов со следом 0. Но во втором случае действие \mathfrak{g}_l на $\Lambda^2 V_l$ будет тривиальным, что противоречит тому факту, что модули $\Lambda^2 V_l$ и $V_l(\mu)$ изоморфны (см. гл. I, п. 1.2). Стало быть, случай $\mathfrak{g}_l = sl(V_l)$ невозможен.

Предположим, что \mathfrak{g}'_l — квадратичное расширение поля \mathbf{Q}_l . Тогда V_l — одномерное векторное \mathfrak{g}'_l -пространство и централизатор подалгебры \mathfrak{g}'_l в $\text{End}(V_l)$ совпадает с ней самой. Значит, \mathfrak{g}_l содержится в \mathfrak{g}'_l и потому полуправа и коммутативна (\mathfrak{g}'_l — „неразложимая подалгебра Картана“ в $\text{End}(V_l)$). Заменив, если нужно, K

на некоторое его конечное расширение (что не влияет на \mathbf{g}_l , см. гл. I, п. 1.1), можно считать, что группа G_l тоже коммутативна. Тогда l -адическое представление V_l является полупростым, абелевым и рациональным. Более того, оно локально алгебраично. Чтобы это установить, заметим прежде всего, что в точке v , делящей l , $v(j) \geq 0$, так как в противном случае группа разложения точки v в G_l не будет абелевой по теореме Тейта (см. добавление, Д.1.3). Следовательно, после конечного расширения поля K мы можем считать, что E имеет хорошую редукцию во всех точках v , делящих l (см. п. 1.2). Пусть $E(l)$ есть l -делимая группа, связанная с E в точке v (см. Тейт [41], п. 2.1, пример (а)). Тогда $V_l \simeq V_l(E(l))$ и, как известно (loc. cit., § 4), этот модуль имеет тип Ходжа — Тейта.

Из другого результата Тейта (гл. III, п. 1.2) следует тогда, что представление V_l локально алгебраично, что и утверждалось. (Это можно было установить также, используя вместо теории модулей Ходжа — Тейта локальные результаты из п. Д. 2 добавления.)

Мы можем теперь применить к V_l результаты гл. III, п. 2.3. Согласно им, для каждого простого числа l' существует рациональное абелево полупростое l' -адическое представление $W_{l'}$, согласованное с V_l . С другой стороны, представление $V_{l'}$ полупросто и согласовано с V_l . Значит, оно изоморфно $W_{l'}$ (см. гл. I, п. 2.3). Но мы знаем, что можно выбрать l' так, чтобы W_l являлось прямой суммой $\text{Gal}(\bar{K}/K)$ -инвариантных одномерных подпространств, а это противоречит неприводимости представления $V_{l'}$. Следовательно, должно быть $\mathbf{g}'_l = \mathbf{Q}_l$ и $\mathbf{g}_l = \text{End}(V_l)$, что и требовалось доказать.

Замечание. Если E имеет комплексное умножение и $L = \mathbf{Q} \otimes \text{End}(E \otimes_K \bar{K})$ — соответствующее мнимое квадратичное поле, то легко показать, что \mathbf{g}_l является картановской подалгеброй в $\text{End}(V_l)$, соответствующей полю $L_l = \mathbf{Q}_l \otimes L$. Она разложима тогда и только тогда, когда l распадается в L .

Упражнения. [Здесь мы предполагаем, что E не имеет комплексного умножения. Пусть S — множество

точек $v \in \Sigma_K$, где E имеет плохую редукцию. Если $v \in \Sigma_K \setminus S$, то F_v обозначает эндоморфизм Фробениуса редуцированной кривой \tilde{E}_v ; если $l \neq p_v$, то F_v мы отождествляем с соответствующим автоморфизмом модуля T_l .]

1) Пусть $H(X, Y)$ — многочлен от двух независимых переменных X, Y с коэффициентами из некоторого поля характеристики нуль. Обозначим через V_H множество тех точек $v \in \Sigma_K \setminus S$, для которых $H(\mathrm{Tr}(F_v), Nv) = 0$. Показать, что V_H имеет плотность 0, если многочлен H ненулевой. (Показать, что множество элементов $g \in GL(2, \mathbf{Z}_l)$ с $H(\mathrm{Tr}(g), \det(g)) = 0$ имеет нулевую меру Хаара.)

2) Собственные значения F_v можно отождествить с комплексными числами вида $(Nv)^{\frac{1}{2}} e^{\pm i\varphi_v}$, $0 \leq \varphi_v \leq \pi$ (см. гл. I, добавление, Д.2). Показать, что множество точек v , для которых φ_v принимает заданное значение φ , имеет плотность нуль. (Показать, что $\mathrm{Tr}(F_v)^2 = 4(Nv) \cos^2 \varphi$, и воспользоваться предыдущим упражнением.)

3) Пусть $L_v = \mathbf{Q}(F_v)$ — поле, порожденное F_v . Согласно предыдущему упражнению, L_v является мнимым квадратичным расширением поля \mathbf{Q} во всех точках v , кроме множества плотности нуль.

(а) Фиксируем простое число l . Пусть C — полупростая коммутативная \mathbf{Q}_l -алгебра ранга 2 и X_C — множество элементов $s \in \mathrm{Aut}(V_l)$, таких, что подалгебра $\mathbf{Q}_l[s]$ в $\mathrm{End}(V_l)$, порожденная s , изоморфна C . Показать, что X_C открыто в $\mathrm{Aut} V_l$ и имеет непустое пересечение с каждой открытой подгруппой группы $\mathrm{Aut} V_l$, в частности с G_l .

(б) Показать, что $F_v \in X_C$ тогда и только тогда, когда поле L_v является квадратичным и $L_v \otimes \mathbf{Q}_l$ изоморфно C .

(в) Пусть l_1, \dots, l_n — различные простые числа и для каждого из них задана алгебра C_i , как в упражнении (а). Показать, что множество точек v , для которых $F_v \in X_{C_i}$, $i = 1, \dots, n$, имеет плотность больше нуля.

[Воспользоваться тем фактом, что образ группы $\mathrm{Gal}(\bar{K}/K)$ в любом конечном произведении групп $\mathrm{Aut} V_l$ открыт; это легкое следствие доказанной выше теоремы.]

(г) Вывести из этого, что для любого конечного множества P простых чисел существует бесконечно много точек v , таких, что L_v разветвлено во всех $l \in P$. В частности, имеется бесконечно много различных полей L_v .

2.3. Теорема об изогении

Теорема. Пусть E и E' — эллиптические кривые над K , l — простое число и $V_l(E), V_l(E')$ — соответствующие l -адицеские представления поля K . Предположим, что модули Галуа $V_l(E)$ и $V_l(E')$ изоморфны и что модулярный инвариант j кривой E (см. п. 1.1) не является целым в поле K . Тогда E и E' являются K -изогенными.

Воспользуемся следующим результатом.

Предложение. Пусть E и E' — эллиптические кривые над K . Тогда следующие условия эквивалентны:

(а) модули Галуа $V_l(E)$ и $V_l(E')$ изоморфны для всех l ;

(б) модули Галуа $V_l(E)$ и $V_l(E')$ изоморфны для одного l ;

(в) пусть F_v и F'_v — эндоморфизмы Фробениуса редуцированных кривых \tilde{E}_v и \tilde{E}'_v , тогда $\text{Tr}(F_v) = \text{Tr}(F'_v)$ для всех точек v , в которых существует хорошая редукция;

(г) для некоторого множества точек плотности единица справедливо равенство $\text{Tr}(F_v) = \text{Tr}(F'_v)$.

Доказательство. Ясно, что из (а) следует (б) и из (в) следует (г). Импликация (б) \Rightarrow (в) вытекает из того факта, что $\text{Tr}(F_v)$ определяется, если известно V_l . Для того чтобы доказать импликацию (г) \Rightarrow (а), заметим прежде всего, что представления группы $\text{Gal}(\bar{K}/K)$ в $V_l(E)$ и в $V_l(E')$ имеют одинаковый след в силу теоремы Чеботарева о плотности (см. гл. I, п. 2.2). Более того, $V_l(E)$ (а также $V_l(E')$) полупросто. Последнее очевидно, если E не имеет комплексного умножения над K , так как $V_l(E)$ тогда неприводимо (см. п. 2.1); если же E имеет комплексное умножение, то это следует из замечания п. 2.2. Поскольку $V_l(E)$ и $V_l(E')$ полупросты и

имеют одинаковый след, они изоморфны. Доказательство закончено.

Замечания. 1) Пусть E и E' имеют хорошую редукцию в v ; обозначим через t_v (соответственно t'_v) число k_v -точек кривой \bar{E}_v (соответственно \bar{E}'_v). Тогда имеют место формулы (см. п. 1.3)

$$\begin{aligned} t_v &= 1 - \text{Tr}(F_v) + Nv, \\ t'_v &= 1 - \text{Tr}(F'_v) + Nv. \end{aligned}$$

Следовательно, условие (в) (соответственно (г)) эквивалентно утверждению, что $t_v = t'_v$ для всех v , в которых имеется хорошая редукция (соответственно для множества точек $\{v\}$ плотности 1).

2) Если E и E' K -изогенны, то очевидно, что условия (а), (б) и (г) выполнены.

Доказательство теоремы. В силу замечания 2) достаточно показать, что эквивалентные условия (а), (б), (в) и (г) обеспечивают изогенцию кривых E и E' , если модулярный инвариант j кривой E не является целым в K . Пусть v — такая точка поля K , что $v(j) < 0$ и p — характеристика поля вычетов k_v .

Положим $j' = j(E')$ и покажем вначале, что $v(j')$ тоже меньше нуля. Предположим, что $v(j') \geq 0$. Тогда после подходящей замены поля K на его конечное расширение мы можем считать, что E' имеет хорошую редукцию в точке v .

Теперь если $l \neq p$, то модуль Галуа $V_l(E')$ неразветвлен в v (см. п. 1.3). С другой стороны, модуль $V_l(E)$ разветвлен в v — это следует либо из критерия Нерона — Огга — Шафаревича (п. 1.3), либо из вычисления группы инерции, приведенного в п. Д.1.3 добавления. Это противоречит тому, что модули $V_l(E)$ и $V_l(E')$ изоморфны.

Пусть, далее, q и q' — элементы поля K_v , соответствующие инвариантам j и j' в теории Тейта (см. п. Д.1.1 добавления), и пусть E_q и $E_{q'}$ — соответствующие эллиптические кривые (*loc. cit.*). Так как E и E_q имеют один и тот же модулярный инвариант j , существует конечное расширение K' поля K , над которым они становятся изоморфными; то же самое относится и к кривым E' и

$E_{q'}$. Следовательно, модули Тейта $T_p(E_q)$ и $T_p(E_{q'})$ становятся изоморфными над K' . Но в таком случае справедлива теорема об изогении (см. добавление, п. Д.1.4), т. е. кривые E_q и $E_{q'}$, а также E и E' изогенны над K' . Однако если эллиптические кривые изогенны над некоторым расширением основного поля, то они изогенны уже над некоторым конечным расширением этого поля. Выберем такое расширение L поля K и L -изогению $f: E \times_K L \rightarrow E' \times_K L$. Покажем, что f автоматически определено над K . Для этого достаточно показать, что $f = {}^s f$ для всех $s \in \text{Gal}(\bar{K}/K)$ или, что равносильно, $V(f): V_p(E) \rightarrow V_p(E')$ коммутирует с действием группы Галуа. Но если $G_L = \text{Gal}(\bar{K}/L)$ — открытая подгруппа группы $G = \text{Gal}(\bar{K}/K)$, соответствующая L , то $V(f)$ коммутирует с действием G_L . Достаточно показать тогда, что $\text{Hom}_{G_L}(V, V') = \text{Hom}_G(V, V')$. Так как V и V' изоморфны как G -модули, то мы должны показать, что $\text{End}_{G_L}(V) = \text{End}_G(V)$. А это очевидно. В самом деле подгруппы G и G_L открыты в $\text{Aut } V$ по теореме из п. 2.2 и, следовательно, их централизаторы состоят только из гомотетий, т. е. $\text{End}_{G_L}(V) = \text{End}_G(V) = \mathbf{Q}_p$. Тем самым теорема полностью доказана.

Замечание. Вполне вероятно, что теорема верна без предположения о том, что инвариант j не является целым. Это можно было бы доказать (методом Тейта [40]), если бы верно следующее обобщение теоремы Шафаревича: существует только конечное число (с точностью до изоморфизма) двумерных абелевых многообразий с поляризацией степени 1, имеющих хорошую редукцию вне конечного множества $S \subset \Sigma_K$.

§ 3. Вариация групп G_l и \tilde{G}_l в зависимости от l

3.1. Предварительные результаты

Сохраним обозначения предыдущих параграфов. Для каждого простого числа l обозначим через ρ_l гомоморфизм

$$\text{Gal}(\bar{K}/K) \rightarrow \text{Aut } T_l \cong GL(2, \mathbf{Z}_l),$$

определенным действием группы $\text{Gal}(\bar{K}/K)$ на модуль T_l . Гомоморфизмы (ρ_l) определяют в свою очередь гомоморфизм

$$\rho: \text{Gal}(\bar{K}/K) \rightarrow \prod_l \text{Aut } T_l,$$

где произведение берется по всем простым числам.

Пусть $G = \text{Im } \rho \subset \prod_l \text{Aut } T_l$ и $G_l = \text{Im } \rho_l \subset \text{Aut } T_l$, так что G_l — это образ группы G при проекции на l -й множитель. Обозначим через \tilde{G}_l образ группы G_l в группе $\text{Aut}(E_l) = \text{Aut}(T_l/lT_l) \simeq GL(2, \mathbf{F}_l)$.

Лемма. (1) *Образ группы G при отображении $\det: \prod_l \text{Aut } T_l \rightarrow \prod_l \mathbf{Z}_l^*$ открыт.*

(2) *Для почти всех l имеем $\det(G_l) = \mathbf{Z}_l^*$ и $\det(\tilde{G}_l) = \mathbf{F}_l^*$.*

Мы знаем (см. гл. I, п. 1.2), что гомоморфизм $\det(\rho_l): \text{Gal}(\bar{K}/K) \rightarrow \mathbf{Z}_l^*$ является тем характером χ_l , который определяет действие группы $\text{Gal}(\bar{K}/K)$ на корни l^n -степени из единицы. Следовательно, $\det(G) \subset \prod_l \mathbf{Z}_l^*$ — это группа Галуа $\text{Gal}(K_C/K)$, где $K_C = \mathbf{Q}_C \cdot K$ — расширение, порожденное всеми корнями из единицы. Так как известно, что $\text{Gal}(\mathbf{Q}_C/\mathbf{Q}) = \prod_l \mathbf{Z}_l^*$ (см., например, [18], гл. IV), то мы получаем, что $\det(G)$ является открытой подгруппой группы $\prod_l \mathbf{Z}_l^*$, соответствующей полю $K \cap \mathbf{Q}_l$, что доказывает утверждение (1). Утверждение (2) следует из (1) и из определения топологии произведения.

Предположим теперь, что кривая E не имеет комплексного умножения. Мы знаем (см. п. 2.2), что каждая из групп G_l открыта в $\text{Aut } T_l$. Из этого не следует a priori, что группа G сама открыта. Тем не менее имеет место следующее

Предложение. *Следующие свойства эквивалентны:*

(i) *группа G открыта в $\prod_l \text{Aut } T_l$;*

(ii) *$G_l = \text{Aut } T_l$ для почти всех l ;*

(iii) *$G_l = \text{Aut } E_l$ для почти всех l ;*

(iv) *\tilde{G}_l содержит $SL(E_l)$ для почти всех l .*

Импликации $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv)$ тривиальны. Импликация $(iv) \Rightarrow (i)$ вытекает из следующего теоретико-группового результата, доказательство которого будет дано в п. 3.4.

Основная лемма. Пусть G — замкнутая подгруппа группы $\prod GL(2, \mathbf{Z}_l)$, и пусть G_l и \tilde{G}_l обозначают ее образы в $GL(2, \mathbf{Z}_l)$ и $GL(2, \mathbf{F}_l)$, как и выше.

Предположим, что

- (a) G_l открыта в $GL(2, \mathbf{Z}_l)$ для всех l ;
- (б) образ G при отображении $\det: \prod GL(2, \mathbf{Z}_l) \rightarrow \prod \mathbf{Z}_l^*$ открыт;
- (в) G_l содержит $SL(2, \mathbf{F}_l)$ для почти всех l . Тогда группа G открыта в $\prod GL(2, \mathbf{Z}_l)$.

Замечание. Для каждого целого числа $n \geq 1$ обозначим через E_n подгруппу точек в $E(\bar{K})$ периода n , и пусть \tilde{G}_n — образ канонического отображения $\text{Gal}(\bar{K}/K) \rightarrow \text{Aut } E_n \cong GL(2, \mathbf{Z}/(n))$. Легко видеть, что свойство (i) предложения эквивалентно следующему:

(i') Индекс подгруппы \tilde{G}_n в $\text{Aut } E_n$ ограничен.

3.2. Случай нецелого j

Теорема. Предположим, что модулярный инвариант j кривой E не является целым в K . Тогда E обладает эквивалентными свойствами (i) — (iv) предложения п. 1.3.

Доказательство. Так как j не является целым, можно найти точку v поля K , такую, что $v(j) < 0$. Пусть q — элемент локального поля K_v , соответствующий j в теории Тейта (см. добавление, п. Д. 1.1), и пусть E_q — соответствующая эллиптическая кривая над K_v . Существует конечное расширение K' поля K , над которым кривые E и E_q становятся изоморфными; в качестве K' можно взять даже либо поле K_v , либо некоторое его квадратичное расширение. Пусть v' — нормирование поля K' , продолжающее v ; предположим, что оно нормализовано так, чтобы $v'(K'^*) = \mathbf{Z}$, и пусть

$$n = v'(q) = -v'(j).$$

Имеем $n \geq 1$.

ЛЕММА 1. Предположим, что l не делит n и $I_{v,l}$ — подгруппа инерции группы \tilde{G}_l , соответствующая некоторому продолжению точки v на поле \bar{K} . Тогда $I_{v,l}$ содержит трансвекцию, т. е. элемент, матрица которого в подходящем \mathbf{F}_l -базисе пространства E_l имеет вид $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Эта лемма верна для кривой E_q над K' , согласно добавлению, п. Д.1.5. Справедливость ее для E следует из изоморфизма $E_{/K'} \simeq E_{q/K'}$.

ЛЕММА 2. Пусть H — подгруппа группы $GL(2, \mathbf{F}_l)$, действующая неприводимо на $\mathbf{F}_l \times \mathbf{F}_l$ и содержащая трансвекцию. Тогда H содержит группу $SL(2, \mathbf{F}_l)$.

Доказательство. Для любой трансвекции $s \in H$ пусть D_s обозначает однозначно определенное одномерное подпространство пространства $\mathbf{F}_l \times \mathbf{F}_l$, инвариантное относительно s . Если бы все такие прямые совпадали, то эта общая прямая была бы инвариантна относительно H и представление группы H не было бы неприводимым. Следовательно, должны существовать трансвекции $s, s' \in H$, такие, что $D_s \neq D_{s'}$. В подходящем базисе пространства $\mathbf{F}_l \times \mathbf{F}_l$ элементы s и s' можно представить в виде матриц

$$s = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad s' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Утверждение леммы вытекает теперь из того, что эти матрицы, как хорошо известно, порождают группу $SL(2, \mathbf{F}_l)$.

Доказательство теоремы. Лемма 1 показывает, что для почти всех l группы $I_{v,l}$ и тем более \tilde{G}'_l содержат трансвекции. С другой стороны, мы знаем (см. п. 2.1), что действие группы \tilde{G}_l неприводимо для почти всех l . По лемме 2 тогда \tilde{G}_l содержит $SL(E_l)$ для почти всех l , т. е. кривая E обладает свойством (iv), что и требовалось доказать.

Замечание. Вероятно, условие „ j не цел“ можно заменить более слабым, „кривая E не имеет комплексного умножения“¹⁾.

3.3. Числовой пример

Если кривая E задана явно и имеет нецелый инвариант j , то иногда можно явно определить конечное множество тех l , для которых $\tilde{G}_l \neq GL(2, \mathbf{F}_l)$. Например, возьмем $K = \mathbf{Q}$ и зададим E уравнением

$$y^2 + x^3 + x^2 + x = 0.$$

Это кривая 3^+ в списке Огга [25], ее инвариант j равен $2^{11}3^{-1}$, $\Delta = -2^43$ и „кондуктор“ равен 24 (она 2-изогенна модулярной кривой J_{24} , соответствующей конгруэнц-подгруппе $\Gamma_0(24)$, см. [25]). Существование нетривиальной 2-изогении для E показывает, что $\tilde{G}_l \neq GL(2, \mathbf{F}_l)$ при $l=2$ [\tilde{G}_2 — циклическая группа порядка 2 и соответствует квадратичному полю $\mathbf{Q}(\sqrt{-3})$]. Но если $l \neq 2$, то $\tilde{G}_l = GL(2, \mathbf{F}_l)$. В самом деле, \tilde{G}_l обладает следующими свойствами:

(а) $\det(\tilde{G}_l) = \mathbf{F}_l^*$, см. п. 3.1;

(б) \tilde{G}_l содержит трансвекцию. Это следует из леммы 1 и из того, что n в этом случае равно 1;

(в) \tilde{G}_l неприводимо. Если бы это было не так, то существовала бы изогения $E \rightarrow E'$ степени l (определенная над \mathbf{Q}). Кривая E' имела бы тогда тот же кондуктор 24, значит, совпадала бы с одной из кривых $1^-, 2^+, 3^+, 4^-, 5^-, 6^+$ в таблице Огга. Но Огг показал, что для каждой такой кривой существует изогения $E' \rightarrow E$ степени 1, 2, 4 или 8. Отображение $E \rightarrow E' \rightarrow E$ было бы тогда эндоморфизмом кривой E степени $l, 2l, 4l$ или $8l$, а это невозможно при $l \neq 2$, поскольку $\text{End}(E) = \mathbf{Z}$.

Из леммы 2 и из свойств (а), (б), (в) следует теперь, что $\tilde{G}_l = GL(2, \mathbf{F}_l)$.

¹⁾ Это доказано в статье Serre J.-P. „Progrès galloisiennes des points d'ordre fini des courbes elliptiques“, Inventiones Math., 15 (1972), 259–331. — Прим. ред.

Упражнение. Доказать, что $\tilde{G}_l = GL(2, F_l)$ для всех $l \neq 2$, если $K = \mathbf{Q}$ и E — эллиптическая кривая с кондуктором $3 \cdot 2^\lambda$, где $\lambda \leqslant 6$. (Воспользоваться таблицей 1 Огга. При $\lambda = 5$ показать, что кривые 7^+ и 7^- становятся изоморфными над $\mathbf{Q}(i)$, но не изогенны над \mathbf{Q} . При $\lambda = 6$ воспользоваться аналогичными рассуждениями и показать, что кривые 10^+ и 18^+ имеют разное число точек по $\text{mod } 5$ и поэтому не изогенны над \mathbf{Q} .)

Что происходит при $\lambda = 7, 8$?

3.4. Доказательство основной леммы из п. 3.1

Прежде всего нам понадобится несколько следующих фактов:

Лемма 1. Пусть $S_l = PSL(2, \mathbf{F}_l) = SL(2, \mathbf{F}_l)/(\pm 1)$, $l \geqslant 3$. Тогда S_l проста при $l \geqslant 5$. Каждая собственная подгруппа группы S_l либо разрешима, либо изоморфна знакопеременной группе A_5 ; последнее возможно только в случае $l \equiv \pm 1 \pmod{5}$.

Это хорошо известно, см., например, Бернсайд [4], гл. XX.

Лемма 2. В $SL(2, \mathbf{F}_l)$ нет собственных подгрупп, отображающихся на всю группу $PSL(2, \mathbf{F}_l)$.

Это очевидно при $l = 2$, поскольку $PSL(2, \mathbf{F}_2) = SL(2, \mathbf{F}_2)$. Пусть $l \neq 2$; предположим, что такая подгруппа существует, и обозначим ее через X . Имеем тогда

$$SL(2, \mathbf{F}_l) = \{\pm 1\} \times X.$$

Но это невозможно, поскольку $SL(2, \mathbf{F}_l)$ порождается элементами $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, имеющими порядок l и, следовательно, принадлежащими X .

Лемма 3. Пусть X — замкнутая подгруппа группы $SL(2, \mathbf{Z}_l)$, образ которой в $SL(2, \mathbf{F}_l)$ совпадает с $SL(2, \mathbf{F}_l)$. Предположим, что $l \geqslant 5$. Тогда $X = SL(2, \mathbf{Z}_l)$.

Будем доказывать индукцией по n , что X отображается на всю группу $SL(2, \mathbf{Z}/l^n\mathbf{Z})$. При $n = 1$ это верно

по предположению. Примем, что это верно для n , и докажем для $n+1$. Достаточно показать, что для любого $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z}_l)$, сравнимого с 1 по $\text{mod } l^n$, существует $x \in X$, такой, что $x \equiv s \pmod{l^{n+1}}$. Запишем $s = 1 + l^n u$. Так как $\det(s) = 1$, то $\text{Tr}(u) \equiv 0 \pmod{l}$. Но, как легко видеть, любой такой элемент u сравним по $\text{mod } l$ с суммой матриц u_i , таких, что $u_i^2 = 0$. Поэтому мы можем предполагать, что $u^2 = 0$. По предположению индукции существует такой элемент $y \in X$, что $y = 1 + l^{n-1}u + l^n v$, где v — матрица с коэффициентами из \mathbf{Z}_l . Положим $x = y^l$. Имеем

$$x = 1 + l(l^{n-1}u + l^n v) + \binom{l}{2}(l^{n-1}u + l^n v)^2 + \dots + (l^{n-1}u + l^n v)^l.$$

Если $n \geq 2$, то очевидно, что $x \equiv 1 + l^n u \pmod{l^{n+1}}$. Это верно также и при $n = 1$. Действительно, поскольку $u^2 = 0$ и $u + lv \equiv u \pmod{l}$, то

$$x \equiv 1 + lu + (u + lv)^l \pmod{l^2}.$$

Но $(u + lv)^2 \equiv l(uv + vu) \pmod{l^2}$, следовательно,

$$(u + lv)^2 \equiv l(uv + vu)u^{l-2} \equiv 0 \pmod{l^2},$$

так как $l > 4$.

Это показывает, что $x \equiv 1 + l^n u \pmod{l^{n+1}}$ при всех n и, стало быть, лемма 3 доказана.

Рассмотрим теперь некоторую замкнутую подгруппу G группы $X = \prod_l GL(2, \mathbf{Z}_l)$, обладающую свойствами (а), (б), (в) основной леммы п. 3.1.

ЛЕММА 4. Пусть S — конечное множество простых чисел и $X_S = \prod_{l \in S} GL(2, \mathbf{Z}_l)$. Тогда образ G_S группы G при проекции $X \rightarrow X_S$ открыт в X_S .

Доказательство. Заменив, если нужно, G на некоторую ее открытую подгруппу, мы можем считать, что каждая из G_l , $l \in S$, содержится в группе элемен-

тов, сравнимых с 1 по $\text{mod } l$, следовательно, G_l — про- l -группа. Поскольку группа G_S является подгруппой группы $\prod_{l \in S} G_l$, из этого следует, что она пронильпотентна (является проективным пределом нильпотентных групп), поэтому она есть произведение своих силовских подгрупп. Это показывает, что $G_S = \prod_{l \in S} G_l$, и так как G_l открыта в $GL(2, \mathbf{Z}_l)$, то по свойству (а) G_S открыта в X_S . Прежде чем двигаться дальше, введем некоторое соглашение. Пусть Y — проконечная группа и Σ — конечная простая группа. Будем говорить, что Σ *происходит из* Y , если существуют замкнутые подгруппы Y_1 и Y_2 в Y , такие, что Y_1 — нормальный делитель в Y_2 и факторгруппа Y_2/Y_1 изоморфна Σ . Обозначим через $\text{Occ}(Y)$ множество классов конечных простых неабелевых групп, происходящих из Y . Пусть $Y = \varprojlim Y_\alpha$ и каждое отображение $Y \rightarrow Y_\alpha$ сюръективно, тогда

$$\text{Occ}(Y) = \bigcup \text{Occ}(Y_\alpha).$$

Если Y является расширением Y' при помощи Y'' , то

$$\text{Occ}(Y) = \text{Occ}(Y') \cup \text{Occ}(Y'').$$

Пользуясь этими формулами и леммой 1, получаем

$$\text{Occ}(GL(2, \mathbf{Z}_l)) = \text{Occ}(SL(2, \mathbf{Z}_l)) = \text{Occ}(S_l),$$

где $S_l = PSL(2, \mathbf{F}_l)$, как и выше, и

$$\text{Occ}(S_l) = \emptyset, \quad \text{если } l = 2, 3,$$

$$\text{Occ}(S_l) = \{S_l\} = \{A_5\}, \quad \text{если } l = 5,$$

$$\text{Occ}(S_l) = \{S_l\}, \quad \text{если } l \equiv \pm 2 \pmod{5}, \quad l > 5,$$

$$\text{Occ}(S_l) = \{S_l, A_5\}, \quad \text{если } l \equiv \pm 1 \pmod{5}, \quad l > 5.$$

Пусть теперь S — конечное множество простых чисел, содержащее 2, 3, 5 и такое, что если $l \notin S$, то $\tilde{G}_l \supset SL(2, \mathbf{F}_l)$. Как показывает свойство (в), такое множество существует.

Лемма 5. Группа G содержит группу $\prod_{l \notin S} SL(2, \mathbf{Z}_l)$ (рассматриваемую как подгруппу полного произведения $X = \prod_l GL(2, \mathbf{Z}_l)$).

Доказательство. Достаточно показать, что группа G содержит каждый из множителей $SL(2, \mathbf{Z}_l)$, $l \notin S$. Пусть $H_l = G \cap GL(2, \mathbf{Z}_l)$. Если $l \notin S$, то из того, что \tilde{G}_l содержит $SL(2, \mathbf{F}_l)$, следует, что $S_l \in \text{Occ}(G_l)$, значит, $S_l \in \text{Occ}(G)$. С другой стороны, группа G/H_l изоморфна замкнутой подгруппе произведения $\prod_{l' \neq l} GL(2, \mathbf{Z}_{l'})$, поэтому $S_l \notin \text{Occ}(G/H_l)$ (мы пользуемся тем очевидным фактом, что простые группы S_p , $p \geq 5$, попарно не изоморфны). Так как

$$\text{Occ}(G) = \text{Occ}(H_l) \cup \text{Occ}(G/H_l),$$

то $S_l \in \text{Occ}(H_l)$. Пусть \tilde{H}_l — образ группы H_l в $SL(2, \mathbf{F}_l)$. Ядро гомоморфизма $H_l \rightarrow \tilde{H}_l$ будет про- l -группой, и мы имеем равенство $\text{Occ}(H_l) = \text{Occ}(\tilde{H}_l)$, следовательно, $S_l \in \text{Occ}(\tilde{H}_l)$. Стало быть, \tilde{H}_l отображается на все $S_l = PSL(2, \mathbf{F}_l)$, и по лемме 2 мы имеем $\tilde{H}_l = SL(2, \mathbf{F}_l)$, а по лемме 3 $H_l = SL(2, \mathbf{Z}_l)$. Следовательно, G содержит $SL(2, \mathbf{Z}_l)$, и лемма доказана.

Лемма 6. Группа G содержит некоторую открытую подгруппу группы $\prod_l SL(2, \mathbf{Z}_l)$.

Доказательство. Пусть множество S такое же, как и в лемме 5, G_S — проекция группы G в $\prod_{l \in S} GL(2, \mathbf{Z}_l)$ и G'_S — проекция ее в дополнительное произведение $\prod_{l \notin S} GL(2, \mathbf{Z}_l)$. Пусть $H_S = G \cap \prod_{l \in S} GL(2, \mathbf{Z}_l)$ и $H'_S = G \cap \prod_{l \notin S} GL(2, \mathbf{Z}_l)$, так что $H_S \subset G_S$, $H'_S \subset G'_S$. Тогда имеют место канонические изоморфизмы

$$G_S/H_S \cong G/(H_S \times H'_S) \cong G'_S/H'_S.$$

По лемме 5 группа H'_S содержит $\prod_{l \notin S} SL(2, \mathbf{Z}_l)$, так что факторгруппа G'_S/H'_S абелева. Следовательно, группа G_S/H_S тоже абелева и H_S содержит коммутант (G_S, G_S) группы G_S . В силу леммы 4 группа G_S открыта в $\prod_{l \in S} GL(2, \mathbf{Z}_l)$. Из этого легко следует, что (G_S, G_S) содержит некоторую открытую подгруппу группы $\prod_{l \in S} SL(2, \mathbf{Z}_l)$ (это видно, например, из того, что производная алгебра Ли алгебры gl_2 есть sl_2). Следовательно, H_S содержит некоторую открытую подгруппу U группы $\prod_{l \in S} SL(2, \mathbf{Z}_l)$. Пользуясь леммой 5, видим, что G в таком случае содержит группу $U \times \prod_{l \notin S} SL(2, \mathbf{Z}_l)$, которая открыта в $\prod_l SL(2, \mathbf{Z}_l)$. Лемма 6 доказана.

Конец доказательства основной леммы. Рассмотрим отображение

$$\det: \prod_l GL(2, \mathbf{Z}_l) \rightarrow \prod_l \mathbf{Z}_l^*,$$

ядро которого есть $\prod_l SL(2, \mathbf{Z}_l)$. Предположение (с) означает, что образ группы G при этом отображении открыт и по лемме 6 пересечение $G \cap \text{Ker}(\det)$ открыто в $\text{Ker}(\det)$. Из этого следует, что открыта и сама группа G в $\prod_l GL(2, \mathbf{Z}_l)$, что и требовалось доказать.

Упражнения. 1) а) Обобщить лемму 3 на группу $SL(d, \mathbf{Z}_l)$ для $d \geq 2, l \geq 5$ (метод тот же).

б) Показать, что единственной замкнутой подгруппой группы $SL(d, \mathbf{Z}_3)$, отображающейся на $SL(d, \mathbf{Z}/3^2\mathbf{Z})$, является вся группа $SL(d, \mathbf{Z}_3)$.

в) Показать, что единственной замкнутой подгруппой группы $SL(d, \mathbf{Z}_2)$, отображающейся на $SL(d, \mathbf{Z}/2^3\mathbf{Z})$, является вся группа $SL(d, \mathbf{Z}_2)$.

2) Пусть E — неразветвленное квадратичное расширение поля \mathbf{Q}_2 и O_E — его кольцо целых элементов. Пусть $x \mapsto \bar{x}$ — нетривиальный автоморфизм поля E .

а) Показать, что O_E содержит примитивный корень 3-й степени из единицы z .

б) Показать, что O_E содержит такой элемент u , что $uu = -1$ (взять, например, $u = (1 + \sqrt{5})/2$).

в) Пусть α и β суть \mathbf{Z}_2 -линейные эндоморфизмы, определенные формулами $\alpha(x) = zx$, $\beta(x) = ux$, где z и u — такие же, как и в а) и б). Показать, что α имеет порядок 3, β — порядок 4 и $\beta\alpha\beta^{-1} = \alpha^{-1}$, так что они порождают неабелеву группу G порядка 12.

г) Показать, что группа G содержится в $SL(O_E) \simeq SL(2, \mathbf{Z}_2)$ и что редукция по mod 2 определяет гомоморфизм группы G на группу $SL(2, \mathbf{F}_2)$. (Следовательно, лемма 3 не распространяется на случай $l = 2$.)

3) Пусть $S_9 = SL(2, \mathbf{Z}/9\mathbf{Z})$, $S_3 = SL(2, \mathbf{Z}/3\mathbf{Z})$ и $g = \text{Ker}(S_9 \rightarrow S_3)$. Группа g изоморфна 3-мерному векторному пространству над \mathbf{F}_3 . Пусть $x \in H^2(S_3, g)$ — класс когомологий, соответствующий расширению

$$1 \rightarrow g \rightarrow S_9 \rightarrow S_3 \rightarrow 1.$$

а) Показать, что ограничение x на силовскую 3-подгруппу группы S_3 равно нулю (заметить что $SL(2, \mathbf{Z})$ содержит элемент порядка 3, а именно $\begin{pmatrix} 1 & 1 \\ -3 & -2 \end{pmatrix}$).

б) Вывести из а), что $x = 0$, т. е. что существует подгруппа X в S_9 , которая изоморфно отображается на S_3 . (Прообраз группы X в $SL(2, \mathbf{Z}_3)$ является нетривиальной подгруппой, отображающейся на всю группу S_3 , следовательно, лемма 3 не распространяется на случай $l = 3$.)

Добавление Локальные результаты

Всюду далее K обозначает поле, полное относительно дискретного нормирования v . Через O_K (соответственно k) будем обозначать кольцо целых элементов (соответственно поле вычетов) поля K . Предположим, что поле k совершенно и имеет характеристику $p \neq 0$.

Пусть E — эллиптическая кривая над K и l — простое число, отличное от характеристики поля K . Пусть T_l и V_l — соответствующие модули Галуа, обозначим

через G_l образ группы $\text{Gal}(K_s/K)$ в $\text{Aut } T_l$ и через I_l — подгруппу инерции группы G_l . Алгебры Ли $\mathbf{g}_l = \text{Lie}(G_l)$, $\mathbf{i}_l = \text{Lie}(I_l)$ будут тогда подалгебрами алгебры $\text{End}(V_l)$. Мы вычислим их при подходящих предположениях относительно поля K и нормирования v . Отметим, что алгебра Ли \mathbf{i}_l является идеалом в алгебре \mathbf{g}_l , поскольку I_l — нормальный делитель группы G_l .

Пусть $j = j(E)$ — модулярный инвариант кривой E (см. п. 1.1). Мы будем рассматривать отдельно случаи $v(j) < 0$ и $v(j) \geq 0$.

Д.1. Случай $v(j) < 0$

В этом пункте мы предполагаем, что модулярный инвариант j эллиптической кривой E имеет полюс, т. е. что $v(j) < 0$.

Д.1.1. Эллиптические кривые Тейта. Пусть q — элемент поля K с $v(q) > 0$ и Γ_q — подгруппа группы K^* , порожденная элементом q . Тогда по теории Тейта ультраметрических тета-функций (не опубликовано, но см. статью Морикавы (Morikawa, Nagoya, Math. J., 1962)¹⁾) существует такая эллиптическая кривая E_q , определенная над K , что для любого конечного расширения K' поля K аналитическая группа K'^*/Γ_q изоморфна группе $E_q(K')$ точек кривой E_q со значениями в K' . Кривая может быть задана уравнением

$$y^2 + xy = x^3 - b_2x - b_3,$$

$b_2 = 5 \sum_{n \geq 1} n^3 q^n / (1 - q^n)$ и $b_3 = \sum_{n \geq 1} (7n^5 + 5n^3) q^n / 12(1 - q^n)$ — ряды, сходящиеся в K . Модулярный инвариант $j(q)$ кривой E_q задается обычной формулой

$$j(q) = \frac{(1 + 48b_2)^3}{q \prod_{n \geq 1} (1 - q^n)^{24}} = \frac{1}{q} + 744 + 196884q + \dots,$$

причем этот ряд имеет целые коэффициенты.

¹⁾ См. также Roquette P., Analytic theory of elliptic functions over local fields, Göttingen, 1970. — Прим. ред.

Поле функций на кривой E_q состоит из дробей вида F/G , где F и G — ряды Лорана

$$F = \sum_{-\infty}^{+\infty} a_n z^n, \quad G = \sum_{-\infty}^{+\infty} b_n z^n$$

с коэффициентами в поле K , сходящиеся для всех значений $z \neq 0, \infty$ и такие, что $F(qz)/G(qz) = F(z)/G(z)$.

Так как для заданной кривой E ее модулярный инвариант j обладает свойством $v(j) < 0$ и поскольку ряд $j(q)$ имеет целые коэффициенты, то можно выбрать q так, чтобы $j = j(q)$. Эллиптические кривые E и E_q будут тогда изоморфны над некоторым конечным расширением поля K (которое можно считать квадратичным). Поэтому после подходящей замены поля K его конечным расширением мы можем считать, что $E = E_q$.

Д.1.2. Одна точная последовательность. Сохраним обозначения п. Д.1.1. Пусть E_n — ядро умножения на l^n в группе K_s^*/Γ_q . Обозначим через μ_n группу корней степени l^n из 1 в K_s ; определено вложение $\mu_n \rightarrow E_n$. С другой стороны, если $z \in E_n$, то $z^{l^n} \in \Gamma_q$ и, следовательно, существует такое целое число c , что $z^{l^n} = q^c$. Сопоставляя элементу z образ числа c в $\mathbf{Z}/l^n\mathbf{Z}$, получаем гомоморфизм группы E_n в группу $\mathbf{Z}/l^n\mathbf{Z}$. В результате возникает последовательность

$$0 \rightarrow \mu_n \rightarrow E_n \rightarrow \mathbf{Z}/l^n\mathbf{Z} \rightarrow 0, \quad (1)$$

которая точна как последовательность $\text{Gal}(K_s/K)$ -модулей. Группа $\text{Gal}(K_s/K)$ действует тривиально на $\mathbf{Z}/l^n\mathbf{Z}$. Переходя к пределу, мы получаем точную последовательность модулей Галуа

$$0 \rightarrow T_l(\mu) \rightarrow T_l(E_q) \rightarrow \mathbf{Z}_l \rightarrow 0, \quad (2)$$

где группа $\text{Gal}(K_s/K)$ действует тривиально на \mathbf{Z}_l . Умножая ее тензорно на \mathbf{Q}_l , мы получаем точную последовательность вида

$$0 \rightarrow V_l(\mu) \rightarrow V_l(E_q) \rightarrow \mathbf{Q}_l \rightarrow 0. \quad (3)$$

Покажем, что эта последовательность $\text{Gal}(K_s/K)$ -модулей не расщепляется. Для этого введем некоторый

инвариант x , принадлежащий группе $\varprojlim H^1(G, \mu_n)$, где $G = \text{Gal}(K_s/K)$. Пусть d — кограницный гомоморфизм

$$H^0(G, \mathbf{Z}/l^n\mathbf{Z}) \rightarrow H^1(G, \mu_n),$$

соответствующий точной последовательности (1), и пусть $x_n = d(1)$. Тогда инвариант x как элемент из $\varprojlim H^1(G, \mu_n)$ определяется семейством элементов $\{x_n\}$, $n \geq 1$.

ПРЕДЛОЖЕНИЕ. (а) Изоморфизм Куммера $\delta: K^*/K^{*l^n} \rightarrow \varprojlim H^1(G, \mu_n)$ отображает класс $q \bmod K^{*l^n}$ в элемент x_n .

(б) Элемент x имеет бесконечный порядок.

[Напомним, что δ индуцируется кограницным отображением, связанным с точной последовательностью Куммера

$$1 \rightarrow \mu_n \rightarrow \bar{K}^* \xrightarrow{l^n} \bar{K}^* \rightarrow 1.]$$

Доказательство. Утверждение (а) доказывается простым вычислением. Чтобы доказать утверждение (б), заметим, что нормирование v определяет гомоморфизм

$$f_n: K^*/K^{*l^n} \rightarrow \mathbf{Z}/l^n\mathbf{Z}$$

и, следовательно, гомоморфизм предельных групп

$$f: \varprojlim K^*/K^{*l^n} \rightarrow \mathbf{Z}_l.$$

Если отождествить x с соответствующим элементом группы $\varprojlim K^*/K^{*l^n}$, как в утверждении (а), то мы будем иметь $f(x) = v(q)$, откуда следует, что порядок элемента x бесконечен.

Следствие. Последовательность (3) не расщепляется.

Предположим противное; тогда существует G -инвариантное подпространство X пространства $V_l(E_q)$, изоморфно отображающееся на \mathbf{Q}_l . Пусть $X_I = T_l(E_q) \cap X$. Тогда образ пространства X_I в \mathbf{Z}_l имеет вид $l^N\mathbf{Z}_l$ для некоторого $N \geq 0$. Легко видеть тогда, что $l^N x = 0$, а это противоречит тому, что порядок элемента x бесконечен.

Д.1.3. Вычисление алгебр g_l и i_l . Сохраним обозначения п. Д.1.1 и Д.1.2. Пусть X — одномерное подпространство пространства $V_l = V_l(E)$; обозначим через \mathfrak{r}_X подалгебру алгебры $\text{End}(V_l)$, состоящую из эндоморфизмов u , для которых $u(V_l) \subset X$, и пусть \mathfrak{n}_X — подалгебра алгебры \mathfrak{r}_X , порожденная элементами $u \in \mathfrak{r}_X$, для которых $u(X) = 0$.

Теорема. (а) Если поле k алгебраически замкнуто и $l \neq p$, то существует такое одномерное подпространство X пространства V_l , что $g_l = \mathfrak{n}_X$.

(б) Если k алгебраически замкнуто и $l = p$, то существует такое одномерное подпространство X пространства V_l , что $g_l = \mathfrak{r}_X$.

(в) Если поле k конечно, то $g_l = \mathfrak{r}_X$ для некоторого одномерного подпространства X пространства V_l и $i_l = \mathfrak{n}_X$ (соответственно $i_l = \mathfrak{r}_X$), если $l \neq p$ (соответственно $l = p$).

Доказательство. Заметим прежде всего, что алгебры g_l и i_l не меняются при конечных расширениях поля K , поэтому мы можем предполагать, что $E = E_q$.

(а) В этом случае поле K содержит корни l^n -степени из единицы, поэтому группа $\text{Gal}(K_s/K)$ действует тривиально на $T_l(\mu)$. Следовательно, существует такой базис e_1, e_2 модуля $T_l(E)$, что для каждого $\sigma \in \text{Gal}(K_s/K)$ имеют место равенства $\sigma(e_1) = e_1$, $\sigma(e_2) = a(\sigma)e_1 + e_2$, где $a(\sigma) \in \mathbf{Z}_l$. Кроме того, гомоморфизм $\sigma \mapsto a(\sigma)$ нетривиален, поскольку последовательность (3) нерасщепляема. Отсюда следует, что $\text{Im } a$ является открытой подгруппой группы \mathbf{Z}_l и, значит, $g_l = \mathfrak{n}_X$ для $X = V_l(\mu)$.

(б) Так как $l = p$, то поле K должно иметь характеристику 0, поскольку $l \neq \text{char } K$. В этом случае действие группы $\text{Gal}(\bar{K}/K)$ на $V_l(\mu)$ задается с помощью характера χ_l (см. гл. I, п. 1.2), имеющего бесконечный порядок. Из этого следует, что $g_l = \mathfrak{r}_X$, где $X = V_l(\mu)$. В самом деле, $g_l \supset \mathfrak{n}_X$, поскольку последовательность (3) не расщепляется, а равенство $g_l = \mathfrak{n}_X$ невозможно.

(в) Так как поле k конечно, то действие группы $\text{Gal}(K_s/K)$ на модуль $T_l(\mu)$ не только нетривиально, но имеет даже бесконечный порядок. Поэтому рассуждения,

использованные при доказательстве утверждения (б), показывают, что $\mathbf{g}_l = \mathbf{r}_X$, где $X = V_l(\mu)$. Применяя утверждение (а) к дополнению максимального неразветвленного расширения поля K , получаем, что $\mathbf{i}_l = \mathbf{n}_X$, если $l \neq p$, и $\mathbf{i}_l = \mathbf{r}_X$, если $l = p$. Доказательство закончено.

Упражнение. Показать, что в случае (а) $\operatorname{Im} a = l^n \mathbf{Z}_l$, где l^n — наивысшая степень числа l , которая делит $v(q) = -v(j)$.

Д.1.4. Приложение к изогениям. Здесь мы будем предполагать, что поле k конечно, а поле K имеет характеристику 0 (т. е. K является конечным расширением поля \mathbf{Q}_p).

Теорема. Пусть $q, q' \in K^*$ и $v(q) > 0, v(q') > 0$. Обозначим через $E = E_q$ и $E' = E_{q'}$ соответствующие эллиптические кривые над K . Тогда следующие условия эквивалентны:

- (1) кривая E_q K -изогенна кривой $E_{q'}$;
- (2) существуют такие целые числа $A, B \geq 1$, что $q^A = q'^B$;
- (3) $\operatorname{Gal}(\bar{K}/K)$ -модули $V_p(E)$ и $V_p(E')$ изоморфны.

Доказательство. (2) \Rightarrow (1). Достаточно показать, что кривые E_q и E_{q^A} изогенны над K . Для этого заметим, что каждая мероморфная функция F/G , инвариантная при умножении на q , инвариантна и при умножении на q^A . Следовательно, поле функций кривой E_q содержится в поле функций кривой E_{q^A} , т. е. эти кривые изогенны.

(1) \Rightarrow (3). Тривиально.

(3) \Rightarrow (2). Выберем некоторый изоморфизм $\varphi: V_p(E) \rightarrow V_p(E')$. Так как $V_p(\mu)$ является единственным одномерным подпространством пространства $V_p(E)$ (соответственно $V_p(E')$), инвариантным относительно группы $G = \operatorname{Gal}(\bar{K}/K)$, то φ отображает $V_p(\mu)$ в себя. Более того, после умножения φ на некоторую гомотетию мы можем считать, что φ отображает $T_p(E)$ в $T_p(E')$. Мы

имеем тогда следующую коммутативную диаграмму:

$$\begin{array}{ccccccc} 0 & \rightarrow & T_p(\mu) & \rightarrow & T_p(E) & \rightarrow & \mathbf{Z}_p \rightarrow 0 \\ & & \rho \downarrow & & \varphi \downarrow & & \downarrow \sigma \\ 0 & \rightarrow & T_p(\mu) & \rightarrow & T_p(E') & \rightarrow & \mathbf{Z}_p \rightarrow 0 \end{array} \quad (4)$$

где ρ (соответственно σ) является умножением на некоторое целое p -адическое число r (соответственно s). Пусть x, x' — элементы группы $\lim_{\leftarrow} H^1(G, \mu_n)$, ассоциированные с кривыми E и E' (см. п. Д.1.2), тогда из коммутативности диаграммы (4) следует, что

$$rx = sx'.$$

Так как нормирование v задает гомоморфизм группы $\lim_{\leftarrow} H^1(G, \mu_n) = \lim_{\leftarrow} K^*/K^{*p^n}$ в \mathbf{Z}_p , при котором x переходит в $v(q)$, а x' в $v(q')$, то

$$rv(q) = sv(q').$$

Покажем теперь, что элемент

$$z = q^{v(q')}/q'^{v(q)}$$

является корнем из единицы. Для этого заметим прежде всего, что образ элемента z в группе $\lim_{\leftarrow} K^*/K^{*p^n}$ является корнем p^s -й степени из единицы. Действительно, он имеет вид

$$v(q')x - v(q)x'.$$

Умножая его на s , мы получаем нуль в силу предыдущей формулы. (Отметим, что $\lim_{\leftarrow} K^*/K^{*p^n}$ является \mathbf{Z}_p -модулем, так что умножение на s имеет смысл.) Воспользуемся теперь тем фактом, что ядро гомоморфизма $K^* \rightarrow \lim_{\leftarrow} K^*/K^{*p^n}$ есть в точности группа k^* (рассматриваемая обычным образом как подгруппа группы K^*). Чтобы это установить, представим K^* в виде произведения $\mathbf{Z} \times k^* \times U^1$, где U^1 — группа единиц, сравнимых с 1 по $\text{mod } p$. Функтор $A \rightarrow \lim_{\leftarrow} A/A^{p^n}$ отображает \mathbf{Z} в \mathbf{Z}_p ,

аннулирует k^* , а U^1 оставляет неизменным, поскольку U^1 является конечно порожденным \mathbf{Z}_p -модулем. Стало быть, $z \in k^*$ и является поэтому корнем из единицы. Отсюда следует (2), что и требовалось доказать.

Замечание. Эквивалентность (1) \Leftrightarrow (2) была замечена Тейтом. Она справедлива без всяких предположений на поле K .

Упражнение. Показать, что условие „поле k конечно“ можно заменить более слабым „ k алгебраично над F_q “.

Д.1.5. Существование трансвекций в группе инерции. Пусть E — эллиптическая кривая вида E_q (см. п. Д.1.1), \tilde{G}_l — образ группы $\text{Gal}(K_s/K)$ в группе $\text{Aut}(T_l/lT_l)$ и \tilde{I}_l — подгруппа инерции группы \tilde{G}_l . Предположим, что нормирование v нормализовано, т. е. что $v(K^*) = \mathbf{Z}$.

Предложение. Если l не делит $v(q)$, то \tilde{I}_l содержит трансвекцию, т. е. элемент, задаваемый матрицей $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ в подходящем \mathbf{F}_l -базисе пространства T_l/lT_l .

Доказательство. Заменив, если нужно, поле K на некоторое его расширение, мы можем предполагать, что поле вычетов k алгебраически замкнуто и что K содержит корни l -й степени из единицы. В самом деле, если $l \neq p$, то последнее условие является следствием первого, а если $l = p$, то эти корни надо присоединить, при этом степень полученного расширения будет делить $l - 1$ и, значит, будет взаимно проста с l ; поэтому значение нормирования на элементе q останется взаимно простым с l . В силу сказанного и согласно предположению на $v(q)$, элемент $q^{1/l}$ не принадлежит полю K . Значит, существует такой автоморфизм $s \in \text{Gal}(K_s/K)$, что $s(q^{1/l}) = zq^{1/l}$. Элемент z является в таком случае примитивным корнем степени l из единицы и вместе с $q^{1/l}$ образует базис T_l по модулю lT_l . Так как $s(z) = z$, то образ элемента s в $\tilde{G}_l = \tilde{I}_l$ есть искомая трансвекция.

Д.2. Случай $v(j) \geq 0$

В этом пункте мы будем предполагать, что модулярный j -инвариант эллиптической кривой E является целым, т. е. $v(j) \geq 0$. Следовательно, после подходящей замены поля K на некоторое его конечное расширение можно считать, что кривая E имеет хорошую редукцию (см. п. 1.2.). Мы будем предполагать еще, что K имеет характеристику 0.

Д.2.1. Случай $l \neq p$. Пусть $l \neq p$. Так как кривая E имеет хорошую редукцию, модуль T_l можно отождествить с модулем Тейта $T_l(\tilde{E})$ редуцированной кривой \tilde{E} (см. п. 1.3.). Следовательно, алгебра инерции i_l равна нулю. Если поле вычетов k конечно, то группа G_l порождается как топологическая группа одним элементом — элементом Фробениуса. Стало быть, в этом случае алгебра $g_l = \text{Lie}(G_l)$ является одномерной подалгеброй алгебры $\text{End}(V_l)$.

Д.2.2. Случай $l = p$ с хорошей редукцией высоты 2. Предположим, что редуцированная кривая \tilde{E} имеет высоту 2. Напомним, что высота абелева многообразия A , определенного над полем характеристики p , — это по определению такое целое число h , для которого p^h является несепарабельной частью степени гомотетии „умножения на p “. Эллиптическая кривая имеет высоту 2 тогда и только тогда, когда ее *инвариант Хассе* (см. Дойринг [12]) равен 0. Поскольку кривая E имеет хорошую редукцию, она определяет *абелеву схему* E_v над O_K и, следовательно, некоторую p -делимую группу $E(p)$ над O_K (см. Тейт [41], п. 2.1, см. также [30], § 1, упражнение 2). Модуль Тейта группы $E(p)$ можно отождествить с T_p . Ее связная компонента $E(p)^0$ совпадает с *формальной группой* (над O_K), связанной с групповой схемой E_v : высота кривой \tilde{E} — это высота ее формальной группы (в обычном смысле). В нашем случае $E(p) = E(p)^0$, так как по предложению высота равна 2.

Теорема. Имеем $g_l = i_l$. Алгебра Ли g_l совпадает либо со всей алгеброй $\text{End}(V_p)$, либо с ее неразложимой подалгеброй Картана.

[Напомним, что неразложимая подалгебра Картана алгебры $\text{End}(V_p)$ —это коммутативная подалгебра ранга 2, для которой V_p как модуль над ней неприводим. Она задается некоторым квадратичным подполем в $\text{End}(V_p)$.]

Доказательство. Алгебра Ли \mathbf{g}_p обладает тем свойством, что $\mathbf{g}_p z = V_p$ для любого ненулевого элемента z пространства V_p (см. [31], стр. 128, предложение 8). В частности, V_p является неприводимым \mathbf{g}_p -модулем, его централизатор—это либо квадратичное поле (которое должно в таком случае совпадать с \mathbf{g}_p), либо поле \mathbf{Q}_p . Во втором случае алгебра \mathbf{g}_p a priori должна равняться либо sl_2 , либо gl_2 . Но $\mathbf{g}_p \neq sl_2$, поскольку $\Lambda^2 V_p$ канонически изоморфно пространству $V_p(\mu)$, на которое $\text{Gal}(\bar{K}/K)$ действует посредством характера χ_p , имеющего бесконечный порядок (в самом деле, никакое конечное расширение поля K не может содержать все корни p^n -й степени из единицы, $n = 1, 2, 3, \dots$). Поэтому алгебра Ли \mathbf{g}_p совпадает либо с $\text{End}(V_p)$, либо с неразложимой подалгеброй Картана алгебры $\text{End}(V_p)$. Поскольку все предыдущие рассуждения проходят и для пополнения максимального неразветвленного поля K , то та же альтернатива имеет место и для алгебры \mathbf{i}_p . Кроме того, \mathbf{i}_p содержится в \mathbf{g}_p . Итак, a priori мы имеем три возможности:

- (а) $\mathbf{i}_p = \mathbf{g}_p = \text{End}(V_p)$,
- (б) $\mathbf{i}_p = \mathbf{g}_p$ и совпадает с неразложимой подалгеброй Картана алгебры $\text{End}(V_p)$,

(в) \mathbf{i}_p является подалгеброй Картана, а $\mathbf{g}_p = \text{End}(V_p)$. Однако мы знаем, что \mathbf{i}_p —идеал в \mathbf{g}_p , поэтому случай (в) невозможен и, стало быть, теорема доказана.

Замечания. 1) По теореме Тейта ([41], § 4, следствие 1 теоремы 4) алгебра \mathbf{g}_p является подалгеброй Картана в $\text{End}(V_p)$ тогда и только тогда, когда $E(p)$ обладает „формальным комплексным умножением“, т. е. тогда и только тогда, когда кольцо эндоморфизмов

группы $E(p)$ в подходящем расширении поля K имеет ранг 2 над \mathbf{Z}_p . Существуют эллиптические кривые без комплексного умножения (в обычном алгебраическом смысле), p -полнения которых $E(p)$ имеют формальное комплексное умножение.

2) Предположим, что \mathbf{g}_p — картановская подалгебра алгебры $\text{End}(V_p)$ и $H = \mathbf{g}_p \cap \text{Aut } V_p$ — соответствующая картановская подгруппа группы $\text{Aut } V_p$. Пусть N — нормализатор подгруппы H в $\text{Aut } V_p$, тогда известно, что факторгруппа N/H — циклическая группа порядка 2. Так как $G_p \subset N$, то отсюда следует, что группа G_p тогда и только тогда абелева, когда $G_p \subset H$. Включение $G_p \subset H$ соответствует случаю, когда формальное комплексное умножение определено над K , а альтернатива $G_p \not\subset H$ — случаю, когда такое умножение определено над квадратичным расширением поля K .

3) Предположим, что группа G_p коммутативна и поле вычетов k *конечно*. Пусть F — квадратичное поле формального комплексного умножения (т. е. само \mathbf{g}_p , рассматриваемое как ассоциативная подалгебра в $\text{End}(V_p)$). Обозначим через U_F группу единиц поля F , тогда действие группы $\text{Gal}(\bar{K}/K)$ на V_p будет задаваться гомоморфизмом

$$\varphi: \text{Gal}(\bar{K}/K) \rightarrow U_F.$$

По локальной теории полей классов мы можем отождествить группу инерции группы $\text{Gal}(\bar{K}/K)^{\text{ab}}$ с группой U_K единиц поля K . Поэтому ограничение φ_I гомоморфизма φ на группу инерции является гомоморфизмом группы U_K в группу U_F . Для того чтобы вычислить φ_I , заметим прежде всего, что действие алгебры $\text{End}(E(p))$ на касательном пространстве к $E(p)$ определяется *вложением* F в K . Для этого вложения имеем (ср. гл. III, п. Д. 4)

$$\varphi_I(x) = N_{K/F}(x^{-1}), \quad x \in U_K. \quad (*)$$

В самом деле, согласно результату Любина (*Ann. Math.*, 85, (1967)), существует формальная группа E' , K -изогенная группе $E(p)$ и имеющая в качестве кольца эндомор-

физмов кольцо целых элементов поля F . Но тогда если E'' — группа Любина — Тейта над K (см. Любин, Тейт [22]), то она изоморфна формальной группе E' над дополнением максимального неразветвленного расширения поля K (см. Любин [21], теорема 4.3.2). Поэтому, для того чтобы доказать формулу (*), можно считать, что $E(p)$ — группа Любина — Тейта. Формула (*) следует в таком случае из основного результата работы [22].

Д.2.3. Вспомогательные результаты из теории абелевых многообразий. Пусть A и B — абелевы многообразия над K , обладающие хорошей редукцией, так что определены соответствующие p -делимые группы $A(p)$ и $B(p)$ (это p -делимые группы над кольцом O_K , см. Тейт [41]). Пусть \tilde{A} и \tilde{B} (соответственно $\tilde{A}(p)$ и $\tilde{B}(p)$) — редукции многообразий A и B (соответственно групп $A(p)$ и $B(p)$).

Теорема 1. *Пусть $\tilde{f}: \tilde{A} \rightarrow \tilde{B}$ — морфизм абелевых многообразий и $\tilde{f}(p)$ — соответствующий морфизм группы $\tilde{A}(p)$ в группу $\tilde{B}(p)$. Предположим, что существует такой морфизм $f(p): A(p) \rightarrow B(p)$, что $\tilde{f}(p)$ является его редукцией. Тогда существует морфизм $f: A \rightarrow B$, редукцией которого является \tilde{f} .*

Доказательство этой теоремы „о подъеме“ было дано Тейтом на семинаре в Вудсхолле в 1964 г., но пока еще не было опубликовано. Я надеюсь, что это будет сделано в ближайшее время. Во всяком случае, доказательство слишком длинно для того, чтобы его можно было здесь привести.

Теорема 2. *Предположим, что модуль $T_p(A)$ является прямой суммой \mathbf{Z}_p -модулей ранга 1, инвариантных относительно действия группы $\text{Gal}(\bar{K}/K)$. Тогда каждый эндоморфизм многообразия \tilde{A} поднимается до эндоморфизма многообразия A , т. е. гомоморфизм редукции $\text{End}(A) \rightarrow \text{End}(\tilde{A})$ сюръективен (и, следовательно, биективен, так как инъективность его известна).*

В силу теоремы 1 достаточно показать, что любой эндоморфизм группы $\tilde{A}(p)$ можно поднять до эндомор-

физма группы $A(p)$. Но из предположения, сделанного относительно модуля T_p , следует (см. Тейт [41], п. 4.2), что $A(p)$ является произведением p -делимых групп высоты 1. Следовательно, доказательство теоремы сводится к следующему элементарному результату.

Лемма. *Пусть H_1, H_2 суть p -делимые группы над O_K высоты 1. Тогда отображение редукции $\text{Hom}(H_1, H_2) \rightarrow \text{Hom}(\tilde{H}_1, \tilde{H}_2)$ биективно.*

Доказательство. Если H_1 и H_2 этальны, то утверждение очевидно. Если обе они не этальны, то этальны их двойственные группы и все сводится к предыдущему случаю. Если одна из них этальна, а вторая нет, то нетрудно проверить, что $\text{Hom}(H_1, H_2) = \text{Hom}(\tilde{H}_1, \tilde{H}_2) = 0$.

Следствие. *Предположим, что*

(i) *модуль $V_p(A)$ есть прямая сумма одномерных подпространств, инвариантных относительно $\text{Gal}(\bar{K}/K)$;*

(ii) *поле вычетов k поля K конечно. Тогда абелево многообразие A изогенно произведению абелевых многообразий (СМ)-типа (в смысле Шимуры — Таниумы [46], см. также гл. II, п. 2.8.).*

Доказательство. Из (i) следует, что модуль $T_p(A)$ содержит решетку T' , являющуюся прямой суммой свободных \mathbf{Z}_p -модулей ранга 1, инвариантных относительно $\text{Gal}(\bar{K}/K)$. Поэтому можно найти такую изогенацию $A_1 \rightarrow A$, что модуль $T_p(A_1)$ будет отображаться на T' . Это означает, что после замены A на изогенное многообразие к нему можно применить теорему 2 и получить изоморфизм $\text{End}(A) \xrightarrow{\sim} \text{End}(\tilde{A})$. Но поскольку поле k конечно, то из результата Тейта [40] следует, что $\mathbf{Q} \otimes \text{End}(\tilde{A})$ содержит полупростую коммутативную \mathbf{Q} -подалгебру Λ ранга $2\dim A$ (в явной форме это не содержится в работе [40], однако легко следует из ее основной теоремы). Стало быть, этот факт имеет место и для алгебры $\mathbf{Q} \otimes \text{End}(A)$. Если представить теперь соответствующую подалгебру Λ в виде произведения

полей Λ_a , то A будет изогенно произведению $\prod A_a$, где A_a — абелево многообразие с комплексным умножением типа Λ_a . Доказательство закончено.

Д.2.4. Случай $l=p$ с хорошей редукцией высоты 1. В этом разделе мы предполагаем, что редуцированная кривая \tilde{E} имеет высоту 1, т. е. что ее инвариант Хассе отличен от нуля (см. Дойринг [12]). Связная компонента нуля $E_1 = E(p)^0$ p -делимой группы $E(p)$, связанной с кривой E (см. Тейт [41]), будет тогда группой высоты 1. Поскольку $E(p)$ является расширением группы E_1 с помощью некоторой этальной группы, то мы имеем следующую точную последовательность $\text{Gal}(\bar{K}/K)$ -модулей:

$$0 \rightarrow X \rightarrow V_p \rightarrow Y \rightarrow 0, \quad (*)$$

где X соответствует модулю Тейта группы E_1 , а Y — точкам порядка степени p кривой \tilde{E} .

Теорема. Предположим, что поле вычетов k конечно. Тогда следующие утверждения эквивалентны:

(а) эллиптическая кривая E имеет комплексное умножение над полем K ;

(а') она имеет комплексное умножение над некоторым расширением поля K ;

(б) существует одномерное подпространство D пространства V_p , дополнительное к подпространству X и инвариантное относительно группы G_p ;

(б') существует одномерное подпространство D пространства V_p , дополнительное к X и инвариантное относительно действия алгебры $\mathbf{g}_p = \text{Lie}(G_p)$.

Доказательство. Если подпространство D инвариантно относительно G_p , то оно также инвариантно и относительно ее алгебры Ли \mathbf{g}_p , следовательно, (б) \Rightarrow (б'). Обратно, если D инвариантно относительно \mathbf{g}_p , то при действии G_p оно имеет конечное число образов. Стандартный способ усреднения показывает тогда, что последовательность (*) расщепляется, поэтому (б') \Rightarrow (б). Импликация (б) \Rightarrow (а) (она одна только и нетривиальна) вытекает из следствия теоремы 2 п. Д.2.3. Обратно,

если кривая E имеет комплексное умножение и F — соответствующее мнимое квадратичное поле, то группа $\text{Gal}(\bar{K}/K)$ действует на V_p посредством $F \otimes \mathbf{Q}_p$ (см. гл. II, п. 2.8) и это действие полупросто. Поэтому точная последовательность (*) расщепляется, откуда (а) \Rightarrow (б). Стало быть, аналогично (а') \Rightarrow (б'). Поскольку импликация (а) \Rightarrow (а') тривиальна, то теорема полностью доказана.

Следствие 1. Если кривая E не имеет комплексного умножения, то \mathbf{g}_p является борелевской подалгеброй \mathbf{b}_X алгебры $\text{End}(V_p)$, порожденной таким элементом $u \in \text{End}(V_p)$, что $u(X) \subset X$; алгебра инерции \mathbf{i}_p является подалгеброй \mathbf{r}_X алгебры \mathbf{b}_X , порожденной элементом $u \in \text{End}(E_p)$, таким, что $u(V_p) \subset X$.

Пусть χ_X и χ_Y — характеристики группы $\text{Gal}(\bar{K}/K)$, определяемые одномерными модулями X и Y . Так как поле k конечно, то χ_Y имеет бесконечный порядок. Пусть χ — характер, определяемый действием группы $\text{Gal}(\bar{K}/K)$ на $V_p(\mu)$, тогда изоморфизмы

$$X \otimes Y \simeq \Lambda^2 V_p \simeq V_p(\mu)$$

показывают, что $\chi_X \chi_Y = \chi$. Поэтому ограничение характеров χ_X и $\chi_Y \chi_Y^{-1}$ на подгруппу инерции группы $\text{Gal}(\bar{K}/K)$ имеет бесконечный порядок. Это показывает прежде всего, что \mathbf{g}_p совпадает либо с \mathbf{b}_X , либо с картановской подалгеброй алгебры \mathbf{b}_X . Второй случай невозможен, поскольку из него следовало бы утверждение (б'), значит, $\mathbf{g}_p = \mathbf{b}_X$.

Аналогично доказывается утверждение, касающееся \mathbf{i}_p . Заметим сначала, что \mathbf{i}_p содержится в \mathbf{r}_X , так что ее действие на X нетривиально. Но поскольку она является идеалом в $\mathbf{g}_p = \mathbf{b}_X$, то из этого следует, что $\mathbf{i}_p = \mathbf{r}_X$.

З а м е ч а н и е. Доказательство этого результата дано в работе [29], стр. 245, теорема 1, но там имеется ошибка: алгебра \mathbf{r}_X определена неправильно как порожденная таким u , что $u(X) = 0$ (вместо $u(V_p) \subset X$).

Следствие 2. Если кривая E имеет комплексное умножение, то \mathbf{g}_p является разложимой картановской подалгеброй алгебры $\text{End}(V_p)$. Пусть D — подпространство в V_p , дополнительное к X и инвариантное относительно $\text{Gal}(\overline{K}/K)$, тогда X и D — характеристические подпространства алгебры \mathbf{g}_p и алгебра инерции \mathbf{i}_p является подалгеброй алгебры $\text{End}(V_p)$, порожденной таким элементом $u \in \text{End}(V_p)$, что $u(D) = 0$ и $u(X) \subset X$.

Доказательство аналогично доказательству следствия 1 (и на самом деле проще).

С П И С О К Л И Т Е Р А Т У Р Ы

- [1] Артин (Artin E.), Collected Papers (edited by S. Lang and J. Tate), Addison — Wesley, 1965.
- [2] Артин (Artin E.), Тейт (Tate J.), Class field theory, Harvard, 1961.
- [3] Артин (Artin M.), Гротендик (Grothendieck A.), Cohomologie étale des schémas, Sémin. Géom. alg., IHES, 1963/64, Bures sur Yvette.
- [4] Бернсайд (Burnside W.), The Theory of Groups (Second Edit.), Cambridge Univ. Press, 1911.
- [5] Вейль (Weil A.), Variétés abéliennes et courbes algébriques, Hermann, Paris, 1948.
- [6] Вейль (Weil A.), On a certain type of characters of the idèle-class group of an algebraic number field, Proc. Int. Symp. Tokyo — Nikko, 1955, 1—7.
- [7] Вейль (Weil A.), On the theory of complex multiplication, Proc. Int. Symp. Tokyo — Nikko, 1955, 9—22.
- [8] Вейль (Weil A.), Adèles and algebraic groups (Notes by M. Demazure and T. Ono), Princeton, Inst. Adv. Study, 1961. (Русский перевод: сб. «Математика», 8 : 4 (1964), 3—74.)
- [9] Вейль (Weil A.), Basic Number Theory, Springer-Verlag, 1967.
- [10] Вейль (Weil A.), Ueber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.*, **168** (1967), 149—156.
- [11] Вейль (Weyl H.), Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, **77** (1914), 313—352.
- [12] Дойринг (Deuring M.), Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hamburg*, **14** (1941), 197—272.
- [13] Игуза (Igusa J.), Fibre systems of Jacobian varieties, I, *Amer. J. Math.*, **78** (1956); 171—199. II, id., 745—760; III, id., **81**, 1959, 453—476.
- [14] Касселс (Cassels J.), Diophantine equations with special reference to elliptic curves, *J. Lond. Math. Soc.*, **41** (1966), 193—219. (Русский перевод: сб. «Математика», **12** : 1 (1968), 113—160, и **12** : 2 (1968), 3—48.)
- [15] Касселс (Cassels J.), Фрёлих (Fröhlich A.), Algebraic Number Theory, Academic Press, 1967. (Русский перевод: Алгебраическая теория чисел, изд-во «Мир», 1969.)
- [16] Коизуми (Koizumi S.), Шимура ((Shimura G.), On Specializations of Abelian Varieties, *Sc. Papers Coll. Gen. Ed.*, Univ. Tokyo, **9** (1959), p. 187—211.

- [17] Ленг (Lang S.), *Abelian Varieties*, Intersc. Tracts, № 7, New York, 1957.
- [18] Ленг, Алгебраические числа, изд-во «Мир», 1966.
- [19] Ленг (Lang S.), *Diophantine Geometry*, Intersc. Tracts, № 11, New York, 1962.
- [20] Ленг (Lang S.), *Introduction to transcendental numbers*, Addison-Wesley, New York, 1966.
- [21] Любин (Lubin J.), One parameter formal Lie groups over p -adic integer rings, *Ann. of Math.*, **80** (1964), 464—484.
- [22] Любин (Lubin J.), Тейт (Tate J.), Formal complex multiplication in local fields, *Ann. of Math.*, **81** (1965), 380—387.
- [23] Мамфорд (Mumford D.), *Geometric Invariant Theory*, Ergebnisse der Math., Bd. Springer-Verlag, 1965.
- [24] Мостов (Mostow G. D.), Тамагава (Tamagawa T.), On the compactness of arithmetically defined homogeneous spaces, *Ann. of Math.*, **76** (1962), 446—463.
- [25] Orr (Ogg A. P.), Abelian curves of small conductor, *Journ. für die reine und ang. Math.*, **226** (1967), 204—215.
- [26] Онo (Ono T.), Arithmetic of algebraic tori. *Ann. of Math.*, **74** (1961), 101—139.
- [27] Полиа, Сёре, Задачи и теоремы из анализа.
- [28] Серр (Serre J.-P.), Sur les groupes de congruence des variétés abéliennes, *Изв. АН СССР*, сер. мат., **28** (1964), 3—20.
- [29] Серр (Serre J.-P.), Groupes de Lie p -adiques attachés aux courbes elliptiques. Coll. Clermont-Ferrand, C. N. R. S., 1964, 239—256.
- [30] Серр (Serre J.-P.), Groupes p -divisibles (d'après. J. Tate), Sémin. Bourbaki, 1966/67, exposé 318.
- [31] Серр (Serre J.-P.), Sur les groupes des Galois attachés aux groupes p -divisibles, Proceed. Conf. on Local Fields, Springer — Verlag, 1967, 113—131.
- [32] Серр Ж.-П., Алгебры Ли и группы Ли, изд-во «Мир», 1969.
- [33] Серр (Serre J.-P.), Corps locaux, Hermann, Paris, 1962.
- [34] Серр (Serre J.-P.), Dépendance d'exponentielles p -adiques, Sémin. Delange — Pisot — Poitou, 7 e année, 1965/66, exposé 15.
- [35] Серр (Serre J.-P.), Résumé des cours 1965/66. Annuaire du Collège de France, 1966/67, 49—58.
- [36] Серр (Serre J.-P.), Тейт (Tate J.), Good reduction of abelian varieties and applications, *Ann. of Math.*, **88** (1968), № 3, 492—517.
- [37] Танияма (Taniyama Y.), L functions of number fields and zeta functions of abelian varieties, *J. Math. Soc. Japan*, **9** (1957), 330—366.
- [38] Тейт (Tate J.), Algebraic cycles and poles of zeta functions, Proc. Purdue Univ. Conf., (1963) p. 93—110, New York, 1965. (Русский перевод: УМН, 20, вып. 6(126) (1965), 27—40.)
- [39] Тейт (Tate J.), On the conjecture of Birch and Swinnerton — Dyer and a geometric analog. Sémin. Bourbaki, 1965/66, exposé 306. (Русский перевод: сб. «Математика», 12:6 (1968), 41—55.)
- [40] Тейт (Tate J.), Endomorphisms of Abelian Varieties over finite fields, *Inven. math.*, **2** (1966), 134—144. (Русский перевод: сб. «Математика», 12 : 6 (1968), 31—40.)

- [41] Тейт (Tate J.), *p-divisible groups*. Proc. Conf. on Local Fields, Springer — Verlag, 1967, p. 158—183.
- [42] Чеботарев Н. Г., Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, *Math. Ann.*, **95** (1925), 151—228.
- [43] Шафаревич И. Р., Поля алгебраических чисел, Proc. Intern. Congress Math. Stockholm, 1962, 163—176.
- [44] Шевалле (Chevalley C.), Deux Théorèmes d'arithmétique, *J. Math. Soc. Japan*, **3** (1951), 36—44.
- [45] Шимура (Shimura G.), A reciprocity law in nonsolvable extensions, *J. für die reine und ang. Math.*, **221** (1966), 209—220.
- [46] Шимура (Shimura G.), Танияма (Taniyama Y.), Complex multiplication of abelian varieties and its applications to number theory, *Publ. Math. Soc. Japan*, **6** (1961).

ПРИЛОЖЕНИЕ

П. Делинъ

МОДУЛЯРНЫЕ ФОРМЫ И ℓ -АДИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ

1. Введение

Пусть

$$D(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \prod_{n=1}^{\infty} \tau(n) q^n, \quad |q| < 1,$$

и

$$\Delta(z) = D(e^{2\pi i z}), \quad \operatorname{Im}(z) > 0.$$

Известно, что $\Delta(z)$ является единственной с точностью до постоянного множителя модулярной параболической формой веса 12 относительно группы $SL_2(\mathbf{Z})$.

Для каждого простого числа p положим

$$H_p(X) = 1 - \tau(p)X + p^{11}X^2.$$

Согласно теории Гекке, ряд Дирихле

$$L_{\tau}(s) = \sum \tau(n) n^{-s} = \prod_p \frac{1}{H_p(p^{-s})}$$

продолжается до некоторой целой функции от s , и функция

$$(2\pi)^{-s} \Gamma(s) L_{\tau}(s)$$

инвариантна относительно замены $s \mapsto 12 - s$.

Гипотеза Рамануджана состоит в том, что корни трехчленов H_p по абсолютной величине равны $p^{-11/2}$ (т. е. $|\tau(p)| < 2p^{11/2}$).

Эти свойства функции $L_{\tau}(s)$, доказанные и гипотетические, аналогичны гипотетическим свойствам дзета-функций алгебраических многообразий над \mathbf{Q} . Поэтому естественно попытаться отождествить L_{τ} с некоторой дзета-функцией такого типа.

Для каждого простого числа l обозначим через K_l максимальное расширение поля \mathbf{Q} , неразветвленное вне l ,

и для $p \neq l$ пусть F_p — элемент группы $\text{Gal}(K_l/\mathbf{Q})$, обратный к элементу Фробениуса φ_p , связанному с простым числом p . Последний определен с точностью до сопряжения.

Переводя вышесказанное на язык l -адических когомологий, Серр предположил, что для каждого l существует представление группы $\text{Gal}(K_l/\mathbf{Q})$ в некотором $\bar{\mathbf{Q}}_l$ -пространстве W_l размерности 2, такое, что

$$H_p(X) = \det(1 - F_p X; W_l)$$

для любого простого числа $p \neq l$. Более того, представление W_l должно быть в области применимости гипотезы Вейля, а гипотеза Рамануджана, предположительно, является частным случаем последних.

Эта программа была успешно проведена Кугой и Шимурой [5] в случае модулярных форм относительно некоторых подгрупп группы $SL_2(\mathbf{R})$ с компактным факторпространством. В нашем случае основная идея Сато — Куги — Шимуры состоит в следующем: пусть E — универсальная эллиптическая кривая над схемой модуля S эллиптических кривых (забудем, что ее не существует), и пусть E^k есть k -кратное расслоенное произведение E на себя над S ; тогда $L_\tau(s)$ является по существу частью дзета-функций схемы E^k при $k = 10 = 12 - 2$.

Ниже объясняется, каким образом устраняются трудности, связанные с параболическими точками, и как строятся представления W_l , обладающие указанными выше свойствами. За историческими подробностями и приложениями мы отсылаем к статье Серра [7].

О б о з н а ч е н и я

Обозначим через \mathbf{A} кольцоadelей поля \mathbf{Q} , через \mathbf{A}^f — кольцо „конечных“adelей, т. е. ограниченное произведение полей \mathbf{Q}_p по всем простым числам p . Для любого множества S простых чисел положим

$$\mathbf{A}_S^f = \prod_{p \in S} \mathbf{Q}_p \times \prod_{p \notin S} \mathbf{Z}_p \subset \mathbf{A}^f.$$

При $S = \emptyset$ полагаем $\hat{\mathbf{Z}} = \mathbf{A}_{\emptyset}^f$.

Если X — топологическое пространство (или этальная топология схемы) и G — некоторое множество, то \underline{G} будет обозначать постоянный пучок на X , определяемый множеством G .

Через \mathbf{G}_a и \mathbf{G}_m обозначаются аддитивная и мультипликативная группы соответственно.

Эллиптическая кривая — это абелево многообразие размерности один; в частности, она снабжена отмеченной точкой — нулем группового закона.

Тензорную степень $\mathcal{L}^{\otimes n}$, $n \in \mathbf{Z}$, обратимого пучка \mathcal{L} мы будем обозначать через \mathcal{L}^n .

Через $\bar{\mathbf{Q}}$ обозначается алгебраическое замыкание поля \mathbf{Q} в \mathbf{C} .

Символом ■ отмечается конец доказательства или отсутствие такового.

2. Изоморфизм Шимуры

(2.1) Эллиптическая кривая над комплексным аналитическим пространством S — это по определению собственный и плоский морфизм аналитических пространств $f: E \rightarrow S$, снабженный некоторым сечением e , слоями которого являются эллиптические кривые. Эллиптическая кривая над S обладает одним и только одним S -групповым законом $\mu: E \times_S E \rightarrow E$, единицей которого является сечение e . С каждой эллиптической кривой E ассоциированы:

(а) Обратимый пучок $\omega_E = e^* \Omega_{E/S}^1$. Относительная алгебра Ли $\underline{\text{Lie}}_S(E)$ — это обратимый пучок ω^{-1} , двойственный пучку ω_E . Имеет место изоморфизм $f_* \Omega_{E/S}^1 \xrightarrow{\sim} \omega_E$.

(б) Локальная система свободных \mathbf{Z} -модулей ранга 2 $R^1 f_* \underline{\mathbf{Z}}$. Положим $T_Z(E) = R^1 f_* \underline{\mathbf{Z}}^\vee$ и $T_Q(E) = T_Z(E) \otimes \mathbf{Q}$ (локальная система гомологий кривой E над S).

Экспоненциальное отображение определяет точную последовательность пучков сечений

$$0 \rightarrow T_Z(E) \xrightarrow{\alpha} \omega^{-1} \rightarrow E \rightarrow 0$$

так, что эллиптическая кривая E восстанавливается, если известна стрелка α .

Локальная система $\Lambda^2 R^1 f_* \underline{\mathbf{Z}} \sim R^2 f_* \underline{\mathbf{Z}}$ канонически изоморфна постоянному пучку $\underline{\mathbf{Z}}$. Изоморфизм между $\underline{\mathbf{Z}}^2$ и $R^1 f_* \underline{\mathbf{Z}}$ будем называть *допустимым*, если он индуцирует -1 (sic) на их внешних квадратах.

Обозначим через $\text{Hom}^+(\mathbf{R}^2, \mathbf{C})$ множество изоморфизмов (\mathbf{R} -линейных) между \mathbf{R}^2 и \mathbf{C} , которые не сохраняют (sic) естественных ориентаций пространств \mathbf{R}^2 и \mathbf{C} (определеных посредством $e_1 \wedge e_2 > 0$ и $1 \wedge i > 0$). Каждый такой изоморфизм определяется своим ограничением на $\underline{\mathbf{Z}}^2$ и поэтому

$$\text{Hom}^+(\underline{\mathbf{Z}}^2, \mathbf{C}) = \text{Hom}^+(\mathbf{R}^2, \mathbf{C}).$$

Это множество снабжается структурой комплексного пространства посредством вложения его в комплексное пространство $\text{Hom}(\underline{\mathbf{Z}}^2, \mathbf{C})$. Над ним надстраивается некоторая „универсальная“ точная последовательность

$$0 \rightarrow \underline{\mathbf{Z}}^2 \xrightarrow{a} \mathbf{G}_a \rightarrow E_0 \rightarrow 0.$$

ПРЕДЛОЖЕНИЕ 2.2. (i). *Функтор, сопоставляющий каждому аналитическому пространству S множество классов изоморфных эллиптических кривых E над S , снабженных изоморфизмами $\omega_E \sim \mathbf{G}_a$ и $R^1 f_* \underline{\mathbf{Z}} \sim \underline{\mathbf{Z}}^2$ (последний допустим), представляется аналитическим пространством $\text{Hom}^+(\mathbf{R}^2, \mathbf{C})$, снабженным универсальной эллиптической кривой E_0 .*

(ii) *Функтор, сопоставляющий каждому аналитическому пространству S множество классов изоморфных эллиптических кривых E над S , снабженных допустимым изоморфизмом $R^1 f_* \underline{\mathbf{Z}} \sim \underline{\mathbf{Z}}^2$, представляется аналитическим пространством $X = \overline{\mathbf{C}^*} \times \text{Hom}^+(\mathbf{R}^2, \mathbf{C})$ (полуплоскостью Пуанкаре).*

(iii) *Пространство $\text{Hom}^+(\mathbf{R}^2, \mathbf{C})$ является главным однородным пространством группы \mathbf{G}_m над X .* ■

Пространство X можно также рассматривать как множество комплексных структур на \mathbf{R}^2 . В силу (ii) оно снабжено универсальной эллиптической кривой E_X , локальная система вещественных когомологий которой изоморфна \mathbf{R}^2 . Пусть ω — обратимый пучок, ассоциированный с E_X .

Аналитический когерентный пучок $R^1\bar{f}_*\underline{\mathbf{R}} \otimes_R \mathcal{O}_X$ является пучком относительных когомологий де Рама кривой E_X над X и как таковой включается в точную последовательность (фильтрацию Ходжа)

$$0 \rightarrow \omega \rightarrow R^1\bar{f}_*\underline{\mathbf{R}} \otimes_R \mathcal{O}_X \xrightarrow{q} \omega^{-1} \rightarrow 0$$

(так как по двойственности Серра $\omega^{-1} \sim R^1\bar{f}_*\mathcal{O}$).

Функториальная формулировка утверждения (ii) предложения 2.2 делает очевидным действие справа группы $SL_2(\mathbf{Z})$ на (X, E_X) : элементу $\gamma \in SL_2(\mathbf{Z})$ и эллиптической кривой E , снабженной изоморфизмом $a: \underline{\mathbf{Z}}^2 \xrightarrow{\cong} R^1\bar{f}_*\underline{\mathbf{Z}}$, сопоставляется пара $(E, a \circ \gamma)$. Если рассматривать \bar{X} , снабженное морфизмом

$$q: \underline{\mathbf{R}}^2 \otimes \mathcal{O}_X \sim R^1\bar{f}_*\underline{\mathbf{R}} \otimes_R \mathcal{O}_X \rightarrow \omega^{-1},$$

как классифицирующее пространство комплексных структур на $\underline{\mathbf{R}}^2$, то также очевидным становится действие справа группы $GL_2^+(\mathbf{R})$ на $(X, \underline{\mathbf{R}}^2, \omega, q)$.

(2.3) Выберем базис (x_1, x_2) пространства $\underline{\mathbf{R}}^2$ так, чтобы $x_1 \wedge x_2 > 0$. Тогда точка $(f: \underline{\mathbf{R}}^2 \rightarrow \mathbf{C}, \text{mod } \mathbf{C}^*)$ пространства X определяется числом $z = f(x_1)/f(x_2)$, $\text{Im}(z) > 0$, и стрелка q отождествляется в таком случае с отображением

$$q: \underline{\mathbf{R}}^2 \rightarrow \mathbf{G}_a : ax_1 + bx_2 \mapsto az + b.$$

Это дает очевидную тривиализацию (не эквивариантную) пучка ω^{-1} над X . В этой тривиализации сечение $f(z)$ пучка ω^k над X преобразуется под действием элемента $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1}$ группы $GL^+(\underline{\mathbf{R}}^2)$ (матрицы в базисе x_1, x_2) с помощью формулы

$$f \cdot \begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} (z) = (cz + d)^{-k} f \left(\frac{az + b}{cz + d} \right).$$

Из тождества

$$dz = (cz + d)^2 d \left(\frac{az + b}{cz + d} \right) \cdot \begin{vmatrix} a & b \\ c & d \end{vmatrix}^{-1}$$

следует, что dz является сечением пучка $\omega^{-2} \cdot \Omega_X^1$, инвариантным относительно действия группы $SL_2(\mathbf{R})$. Оно

нигде не обращается в нуль и определяет изоморфизм эквивариантных $SL_2(\mathbf{R})$ -пучков ω^2 и Ω_X^1 .

(2.4) Пусть Γ — дискретная подгруппа группы $SL_2(\mathbf{R})$ без элементов конечного порядка и с конечным объемом факторпространства. Известно тогда, что факторпространство X/Γ отождествляется с гладкой проективной кривой $\overline{X/\Gamma}$ без конечного числа (выколотых) точек. Группа Γ действует на X без неподвижных точек. Поэтому эквивариантная локальная система $\underline{\mathbf{R}}^2$ над X , так же как и эквивариантная точная последовательность

$$0 \rightarrow \omega \rightarrow \underline{\mathbf{R}}^2 \otimes_{\mathbf{R}} \mathcal{O}_X \xrightarrow{q} \omega^{-1} \rightarrow 0,$$

определяет на X/Γ некоторую локальную систему U и точную последовательность

$$0 \rightarrow \omega \rightarrow U \otimes_{\mathbf{R}} \mathcal{O} \rightarrow \omega^{-1} \rightarrow 0. \quad (2.5)$$

В частном случае, когда $\Gamma \subset SL_2(\mathbf{Z})$, эти структуры возникают из эллиптической кривой E на X/Γ , обратным образом которой является эквивариантная эллиптическая кривая E_X над X .

(2.6) Бесконечно удаленные точки кривой X/Γ описываются следующим образом (см. [1]):

(а) Они соответствуют классам сопряженных нетривиальных подгрупп группы Γ , которые являются максимальными среди подгрупп, состоящих из унитентных элементов.

(б) Пусть $\Gamma_0 \subset \Gamma$ — одна из таких подгрупп и (x_1, x_2) — такой базис пространства \mathbf{R}^2 , что в этом базисе Γ_0 состоит из матриц вида

$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}, \quad n \in \mathbf{Z}.$$

Пусть z — координата на X , определяемая базисом (x_1, x_2) , как в п. (2.3). Тогда существует такое N , что часть $X_N = \{z \mid \text{Im}(z) > N\}$ пространства X будет отделена от ее сдвигов на все $\gamma \in \Gamma \setminus \Gamma_0$, так что имеет место вложение $X_N/\Gamma_0 \hookrightarrow X/\Gamma$. Функция $q = e^{2\pi iz}$ устанавливает изоморфизм между X_N/Γ_0 и диском без точки $0 < q < e^{-2\pi N}$.

Если P_{Γ_0} — точка в $\overline{X/\Gamma} \setminus X/\Gamma$, соответствующая подгруппе Γ_0 , то этот изоморфизм продолжается до изоморфизма некоторой окрестности точки P_{Γ_0} с диском $0 \leq q < e^{-2\pi N}$.

Согласно п. (2.3), сечения пучка ω над X_N , инвариантные относительно Γ_0 , отождествляются с голоморфными периодическими функциями периода единицы на X_N . Будем обозначать также через ω обратимый пучок над $\overline{X/\Gamma}$, продолжающий ω и такой, что в окрестности параболической точки P_{Γ_0} сечение, определяемое постоянной функцией 1, продолжается до некоторого обратимого сечения над $\overline{X_N/\Gamma_0}$.

(2.7) Над $\overline{X/\Gamma}$ имеются два обратимых пучка Ω^1 и ω и задан изоморфизм φ п. (2.3) между ограничениями этих пучков на X/Γ . Из формулы

$$dq = de^{2\pi iz} = 2\pi ie^{2\pi iz} dz = 2\pi iq dz$$

следует, что стрелка

$$\varphi: \Omega^1 \rightarrow \omega^2$$

продолжается на $\overline{X/\Gamma}$ и имеет простой нуль в каждой бесконечно удаленной точке.

ОПРЕДЕЛЕНИЕ 2.8. Пространством параболических автоморфных форм веса $k+2$ относительно группы Γ называется пространство глобальных сечений

$$H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k).$$

В силу п. (2.7) это пространство отождествляется также с пространством тех глобальных сечений пучка ω^{k+2} , которые анулируются на бесконечности (т. е. в каждой бесконечно удаленной точке).

(2.9) Обозначим через U^k локальную систему над X/Γ , являющуюся k -й симметрической степенью локальной системы U . Тогда второе отображение из (2.5) индуцирует отображение

$$\iota^k: \omega^k \rightarrow U^k \otimes {}_{\mathbb{R}}\mathcal{O}$$

и еще одно, также обозначаемое через ι^k ,

$$\iota^k: \Omega^1 \otimes \omega^k \rightarrow \Omega^1(U^k),$$

где $\Omega^1(U^k)$ — пучок голоморфных дифференциальных форм на X/Γ с коэффициентами в локальной системе U^k .

Резольвента де Рама для $U^k \otimes_{\mathbb{R}} \mathbb{C}$

$$0 \rightarrow U^k \otimes_{\mathbb{R}} \mathbb{C} \rightarrow U^k \otimes_{\mathbb{R}} \mathcal{O} \xrightarrow{d} U^k \otimes_{\mathbb{R}} \Omega^1 \rightarrow 0$$

индуцирует отображение

$$\delta: H^0(X/\Gamma, \Omega^1(U^k)) \rightarrow H^1(X/\Gamma, U^k \otimes \mathbb{C}).$$

Более того, пространство когомологий $H^1(X/\Gamma, U^k \otimes \mathbb{C})$ снабжено естественным образом комплексным сопряжением так, что δ определяет сопряженное линейное отображение $\bar{\delta}$ пространства, комплексно сопряженного к $H^0(X/\Gamma, \Omega^1(U^k))$, в $H^1(X/\Gamma, U^k \otimes \mathbb{C})$. Мы получаем, таким образом, отображение

$$sh_0: H^0(X/\Gamma, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(X/\Gamma, \Omega^1 \otimes \omega^k)} \rightarrow H^1(X/\Gamma, U^k \otimes \mathbb{C}),$$

где $sh_0 = \delta_0 H^0(\mathfrak{l}^k) \oplus \bar{\delta} H^0(\mathfrak{l}^k)$.

Для любого пучка \underline{F} над пространством Y через $\tilde{H}^i(Y, \underline{F})$ мы будем обозначать образ когомологий с компактным носителем $H_c^i(Y, \underline{F})$ в когомологиях без носителя $H^i(Y, \underline{F})$.

Теорема 4.2.6 статьи [1] по существу эквивалентна следующей теореме (в [1] число k предполагается четным, однако то же самое доказательство проходит и в общем случае);

Теорема 2.10 (Шимура [9]). Существует изоморфизм sh , делающий следующую диаграмму коммутативной:

$$\begin{array}{ccc} H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\overline{X/\Gamma}, \Omega^1 \otimes \omega^k)} & \xrightarrow{sh} & \tilde{H}^1(X/\Gamma, U^k \otimes \mathbb{C}) \\ \cap \downarrow & & \cap \downarrow \\ H^0(X/\Gamma, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(X/\Gamma, \Omega^1 \otimes \omega^k)} & \xrightarrow{sh_0} & H^1(X/\Gamma, U^k \otimes \mathbb{C}) \end{array}$$

Он называется изоморфизмом Шимуры.

(2.11) В частном случае, когда Γ — подгруппа конечного индекса группы $SL_2(\mathbb{Z})$, эллиптическая кривая E над X/Γ возникает из схемы эллиптических кривых над алгебраической кривой X/Γ (т. е. ее модулярный

инвариант мероморфен на бесконечности); она обладает, следовательно, моделью Нерона \bar{E} над \bar{X}/Γ . Можно показать, что слои \bar{E} над бесконечно удаленными точками будут иметь мультипликативный тип и что над всем \bar{X}/Γ имеет место равенство

$$\omega = e^* \Omega^1_{\bar{E}/(\bar{X}/\Gamma)}.$$

В этом частном случае мы имеем $U = R^1 f_* \underline{\mathbf{Z}} \otimes \mathbf{R}$, так что конечный член изоморфизма Шимуры можно переписать в виде

$$\tilde{H}^1(X/\Gamma, U^k \otimes \mathbf{C}) \sim \tilde{H}^1(X/\Gamma, \text{Sym}^k(R^1 f_* \underline{\mathbf{Z}})) \otimes_{\mathbf{Z}} \mathbf{C}.$$

3. Операторы Гекке и фундаментальное l -адическое представление

(3.1) Напомним (см. [2]), что категория *конструктивных локально постоянных* (сокращенно к. л. п.) \mathbf{Z}_l -пучков над схемой S — это категория проективных систем пучков $(F_n)_{n \in \mathbf{Z}}$ в этальной топологии схемы S , удовлетворяющих следующим условиям:

- (i) F_n — локально постоянный пучок $\mathbf{Z}/(l^n)$ -модулей конечного типа;
- (ii) если $n \leq m$, то $F_m \otimes \mathbf{Z}/(l^n) \xrightarrow{\sim} F_n$.

К. л. п. \mathbf{Z}_l -пучки образуют поле в абелевых категориях¹⁾ над S ; фактором этого поля по плотному подполю к. л. п. \mathbf{Z}_l -пучков, аннулируемых некоторой степенью числа l , является поле к. л. п. \mathbf{Q}_l -пучков. Обозначим через $\otimes \mathbf{Q}_l$ канонический функтор из категорий к. л. п. \mathbf{Z}_l -пучков в категорию к. л. п. \mathbf{Q}_l -пучков.

Пусть схема S связна и s — некоторая ее геометрическая точка. Тогда категория к. л. п. \mathbf{Z}_l (соответственно \mathbf{Q}_l) пучков над S эквивалентна, посредством функтора „слоя над s “, категории непрерывных представлений фундаментальной группы $\pi_1(S, s)$ в \mathbf{Z}_l -модуле

¹⁾ „Champ en des catégories abéliennes“. Это расслоенная категория с некоторыми дополнительными условиями; см. J. Giraud, Non abelian cohomology, Springer-Verlag, 1972. — Прим. перев.

конечного типа (соответственно в векторном \mathbf{Q}_l -пространстве конечной размерности).

Пусть T — конечное множество простых чисел. К. л. п. \mathbf{A}_T^f -пучок задается следующим образом: для простых чисел $l \notin T$ он состоит из к. л. п. \mathbf{Z}_l -пучков, а для $l \in T$ — из к. л. п. \mathbf{Q}_l -пучков. Если $T = \emptyset$, то к. л. п. \mathbf{A}_{\emptyset}^f -пучок будем называть к. л. п. $\widehat{\mathbf{Z}}$ -пучком.

Категория к. л. п. \mathbf{A}_T^f -пучков для произвольных T определяется как индуктивный предел категорий к. л. п. $\mathbf{A}_{T'}^f$ -пучков, где $T' \subset T$ — конечные подмножества. Положим

$$\underline{\mathbf{Z}}_l = \varprojlim \underline{\mathbf{Z}}_l(l^n), \quad \underline{\mathbf{Q}}_l = \underline{\mathbf{Z}}_l \otimes \mathbf{Q}_l,$$

$$\underline{\mathbf{Z}} = \coprod (\underline{\mathbf{Z}}_l), \quad \underline{\mathbf{A}}_T^f = \underline{\mathbf{Z}} \otimes \mathbf{A}_T^f.$$

Поле эллиптических кривых с точностью до изогении над S — это поле эллиптических кривых над S с „формальным обращением изогений“. Обозначим через $\otimes \mathbf{Q}$ функтор, сопоставляющий эллиптической кривой ее класс с точностью до изогении. Для квазикомпактной схемы S имеем

$$\mathrm{Hom}(E, F) \otimes \mathbf{Q} \xrightarrow{\sim} \mathrm{Hom}(E \otimes \mathbf{Q}, F \otimes \mathbf{Q}),$$

и если S нормальна, то всякая эллиптическая кривая с точностью до изогении над S происходит из некоторой эллиптической кривой над S .

(3.2) Пусть $f: E \rightarrow S$ — эллиптическая кривая над схемой S . Обозначим через $T_l(E)$ проективную систему ядер E_{l^n} эндоморфизмов умножения на l^n кривой E ; E_{l^n} и E_{l^m} , $n \geq m$, связаны морфизмом умножения на l^{n-m} . То же самое сделаем и для группы \mathbf{G}_m и положим $T_l(\mathbf{G}_m) = \mathbf{Z}_l(1)$. Если l обратимо на S , то $T_l(E)$ и $\mathbf{Z}_l(1)$ будут \mathbf{Z}_l -пучками над S . Определим $T_{\infty}(E)$ как относительную алгебру Ли кривой E над S (это обратимый пучок, двойственный обратному пучку ω из п. (2.1 (а))).

Предположим, что схема S рассматривается в характеристике 0. Определим тогда $\widehat{\mathbf{Z}}$ -пучок $T_f(E)$ над S как систему $T_l(E)$ по всем l и положим $V_f(E) = T_f(E) \otimes \mathbf{A}^f$.

Пусть $u: E \rightarrow F$ — некоторая изогения, тогда u индуцирует изоморфизм $V_f(E)$ с $V_f(F)$ и $T_\infty(E)$ с $T_\infty(F)$. Следовательно, функторы V_f и T_∞ переносятся на категорию эллиптических кривых с точностью до изогении над S .

ПРЕДЛОЖЕНИЕ 3.3. Пусть S — схема характеристики 0. $\underline{E}_1(S)$ — категория эллиптических кривых над S и $\underline{E}_2(S)$ — категория троек, каждая из которых состоит из эллиптической кривой с точностью до изогении E над S , $\widehat{\mathbf{Z}}$ -пучка T — формы пучка $\widehat{\mathbf{Z}}^2$ — и изоморфизма $\beta: V_f(E) \xrightarrow{\sim} T \otimes \mathbf{A}$. Тогда функтор $I: E \rightarrow (E \otimes \mathbf{Q}, T_f(E), V_f(E) \xrightarrow{\sim} T_f(E) \otimes \mathbf{A})$ из категории $\underline{E}_1(S)$ в категорию $\underline{E}_2(S)$ является эквивалентностью категорий.

Это утверждение локально по S , поэтому можно предполагать, что схема S квазикомпактна. Пусть $f: E \rightarrow F$ есть S -морфизм эллиптических кривых. Если f — изогения, то имеет место следующая точная последовательность:

$$0 \rightarrow T_f(E) \rightarrow T_f(F) \rightarrow \text{Ker } f \rightarrow 0. \quad (3.4)$$

Морфизм f делится на n тогда и только тогда, когда он аннулирует ядро E_n умножения на n , так как морфизм „умножения на n “ E/E_n в E является изоморфизмом. По (3.4) это имеет место тогда и только тогда, когда $T_f(f)$ делится на n , и мы получаем, что $\text{Hom}_S(E, F)$ является подгруппой группы $\text{Hom}_S(E \otimes \mathbf{Q}, F \otimes \mathbf{Q})$, порожденной такими морфизмами f , что $V_f(f)$ отображает $T_f(E)$ в $T_f(F)$. Следовательно, функтор I является строго плоским.

Пусть $X \in \text{Ob}(\underline{E}_2(S))$. Локально по S объект X определяется некоторой эллиптической кривой с точностью до изогении $E \otimes \mathbf{Q}$ и „решеткой“ T в $V_f(E)$, которая для почти всех l совпадает с $T_l(E)$. Для любого $q \in \mathbf{Q}$ объект $(E \otimes \mathbf{Q}, T)$ изоморчен объекту $(E \otimes \mathbf{Q}, qT)$, что позволяет считать, что $T_f(E) \subset T$. Фактор $K = T/T_f(E)$ канонически изоморчен тогда некоторой конечной подгруппе в E , и X является образом при морфизме I эллиптической кривой E/K (ср. 3.4). ■

Следствие 3.5. Функтор $F_1(S)$ (соответственно $F'_1(S)$), сопоставляющий каждой схеме S характеристики 0 множество классов изоморфных эллиптических кривых E над S , снабженных изоморфизмом $\alpha: T_f(E) \xrightarrow{\sim} \bar{\mathbf{Z}}^2$ (соответственно и изоморфизмом $\alpha_\infty: T_\infty \xrightarrow{\sim} \bar{\mathbf{G}}_a$), изоморчен функтору $F_2(S)$ (соответственно $F'_2(S)$), сопоставляющему S множество классов с точностью до изогении эллиптических кривых F над S , снабженных изоморфизмом $\beta: V_f(F) \xrightarrow{\sim} \underline{\mathbf{A}}^{f^2}$ (соответственно и изоморфизмом $\beta: T_\infty(F) \xrightarrow{\sim} \bar{\mathbf{G}}_a$).

Предложение 3.6. Функтор F_1 (соответственно F'_1) представляется некоторой схемой M_∞ (соответственно M'_∞) над \mathbf{Q} .

Пусть $n \geq 3$ — целое число. Функтор, сопоставляющий каждой схеме S множество классов изоморфных эллиптических кривых, снабженных изоморфизмом $\alpha_n: E_n \xrightarrow{\sim} (\mathbf{Z}/(n))^2$ (соответственно и $\alpha_\infty: T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$), представляется некоторой аффинной кривой M_n (соответственно некоторой аффинной поверхностью M'_n) над $\text{Spec } \mathbf{Z}[1/n]$. Для $n | m$ морфизм M_m в M_n , определяемый формулой

$$(E, \alpha_m: E_m \xrightarrow{\sim} (\mathbf{Z}/(m))^2) \mapsto \left(E, \frac{n}{m} \alpha_m: E_n \xrightarrow{\sim} (\mathbf{Z}/(n))^2 \right),$$

конечен и этален над $\text{Spec } \mathbf{Z}[1/m]$, поэтому мы имеем $M_\infty = \varprojlim M_n$.

Представимость функтора F'_1 доказывается аналогично. ■

(3.7) Схема M_∞ (соответственно M'_∞) снабжена некоторой универсальной эллиптической кривой $f_\infty: E \rightarrow M_\infty$ и изоморфизмом $\alpha: T_f(E) \xrightarrow{\sim} \bar{\mathbf{Z}}^2$ (соответственно еще и изоморфизмом $\alpha_\infty: T_\infty(E_\infty) \xrightarrow{\sim} \bar{\mathbf{G}}_a$).

Согласно (3.5), схема M_∞ (соответственно M'_∞) представляет функтор F_2 (соответственно F'_2), что делает очевидным действие слева адельной группы $GL_2(\mathbf{A}^f)$ на $(M_\infty, E_\infty \otimes \mathbf{Q}, \alpha \otimes \underline{\mathbf{A}}^{f^2})$ (соответственно $(M'_\infty, E_\infty \otimes \mathbf{Q}, \alpha \otimes \underline{\mathbf{A}}^{f^2}, \alpha_\infty)$), задаваемое на функторе формулой

$$g: (F, \beta: V_f(E) \xrightarrow{\sim} \underline{\mathbf{A}}^2, \beta_\infty) \mapsto (F, g \circ \beta: V_f(E) \xrightarrow{\sim} \underline{\mathbf{A}}^2, \beta_\infty),$$

где $g \in GL_2(\mathbf{A}^f)$.

Этот факт первым заметил Шафаревич.

Пусть Y — схема над \mathbf{C} , являющаяся проективным пределом схем конечного типа Y_i с конечными морфизмами. Локально компактное окольцованное пространство Y^{an} зависит только от Y , а не от представления его в виде проективного предела. Если Y — схема над \mathbf{Q} , являющаяся проективным пределом схем конечного типа над \mathbf{Q} с конечными морфизмами, то мы полагаем $Y^{\text{an}} = (Y \otimes \mathbf{C})^{\text{an}}$. В частности, это относится к пространствам M_∞ и M'_∞ .

ПРЕДЛОЖЕНИЕ 3.8. *Имеют место канонические изоморфизмы*

$$M'^{\text{an}}_\infty \sim \text{Hom}(\mathbf{Q}^2 \otimes \mathbf{A}, \mathbf{C} \times \mathbf{A}^{f^2}) / GL_2(\mathbf{Q}),$$

$$M^{\text{an}}_\infty \sim \mathbf{C}^* \backslash \text{Hom}(\mathbf{Q}^2 \otimes \mathbf{A}, \mathbf{C} \times \mathbf{A}^{f^2}) / GL_2(\mathbf{Q}),$$

или, менее канонические, изоморфизмы

$$M'^{\text{an}}_\infty \sim GL_2(\mathbf{A}) / GL_2(\mathbf{Q}),$$

$$M^{\text{an}}_\infty \sim K_\infty \backslash GL_2(\mathbf{A}) / GL_2(\mathbf{Q}),$$

где K_∞ — максимальная компактная подгруппа, дополненная вещественными гомотетиями. Эти изоморфизмы согласованы с действием групп $GL_2(\mathbf{A}^f)$.

Понятие эллиптической кривой с точностью до изогении вместе с его первоначальными свойствами переносится также и на комплексно аналитический случай. Кроме того, изогения $\phi: E \rightarrow F$ индуцирует изоморфизм ϕ^* между локальными системами рациональных когомологий E и F , что позволяет определить такую систему для кривой с точностью до изогении. Пусть S — комплексно аналитическое пространство. Из (2.1) видно, что задать эллиптическую кривую с точностью до изогении над S — это то же самое, что задать обратимый пучок T_∞ , локальную систему \mathbf{Q} -пространства $T_{\mathbf{Q}}$ и морфизм $u: T_{\mathbf{Q}} \rightarrow T_\infty$, индуцирующий изоморфизм между $T_{\mathbf{Q}} \otimes \mathbf{R}$ и T_∞ .

Пусть n — целое число и K_n — ядро естественного отображения группы $\prod GL_2(\mathbf{Z}_l)$ на $GL_2(\mathbf{Z}/(n))$. Обозначим через G_l функтор, который сопоставляет S множество

классов изоморфных эллиптических кривых $f: E \rightarrow S$ над S , снабженных изоморфизмами $\varphi: \mathbf{Q}^2 \xrightarrow{\sim} T_{\mathbf{Q}}(E)$, $a_\infty: T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$ и $a_n: E_n \xrightarrow{\sim} (\mathbf{Z}/(n))^2$. Как и в (3.3), видим, что G_1 изоморчен функтору G_2 , который сопоставляет пространству S множество классов эллиптических кривых E с точностью до изогении над S , снабженных изоморфизмами $\varphi: \mathbf{Q}^2 \xrightarrow{\sim} T_{\mathbf{Q}}(E)$, $a_\infty: T_\infty(E) \xrightarrow{\sim} \mathcal{O}_S$ и изоморфизмом $V_f(E) \xrightarrow{\sim} \mathbf{A}^2$, заданным локально по S с точностью до композиции с элементом из K_n . Такой объект определяется композицией φ' морфизмов (заданных локально по $\text{mod } K_n$) вида

$$\varphi': \mathbf{Q}^2 \xrightarrow{\varphi} T_{\mathbf{Q}}(E) \rightarrow T_\infty(E) \times V_f(E) \xrightarrow{\sim} \mathcal{O}_S \times \mathbf{A}^{f2}.$$

Имеем

$$E = \mathcal{O}_S / \varphi'(\mathbf{Q}^2 \cap \varphi'^{-1}(T_\infty(E) \times V_f(E))) = \\ = \hat{\mathbf{Z}}^2 \backslash \mathcal{O}_S \times \mathbf{A}^{f2} / \varphi'(\mathbf{Q}^2),$$

так что (ср. 2.2) функторы G_1 и G_2 будут представлены пространством

$$K_n \backslash \text{Isom}(\mathbf{Q}^2 \otimes \mathbf{A}, \mathbf{C} \times \mathbf{A}^{f2}).$$

Предположим теперь, что $n \geq 3$, так что группа $GL_2(\mathbf{Q})$ действует свободно на этом пространстве. Аналитическое пространство M_n^{an} (соответственно $M_n'^{\text{an}}$) представляет тогда соответствующий функтор в аналитической геометрии, аналогичный функтору, представляемому схемой M_n (соответственно M_n'). Действительно, мы знаем, что этот функтор, скажем X , представим и морфизм $X \rightarrow M_n^{\text{an}}$ (соответственно $X \rightarrow M_n'^{\text{an}}$) индуцирует биекцию на множествах точек со значениями в произвольных алгебрах конечного ранга над \mathbf{C} . Тогда из сказанного выше получаем, что

$$M_n'^{\text{an}} \sim K_n \backslash \text{Isom}(\mathbf{Q}^2 \otimes \mathbf{A}, \mathbf{C} \times \mathbf{A}^{f2}) / GL_2(\mathbf{Q}).$$

Проделав то же самое для M_n , мы получим доказательство первого утверждения (3.8) с помощью перехода к пределу по n .

Точка x схемы $\text{Isom}(\mathbf{Q}^2 \otimes \mathbf{A}, \mathbf{C} \times \mathbf{A}^{f_2})/GL_2(\mathbf{Q})$ отождествляется с некоторой „решеткой“ L_x в $\mathbf{C} \times \mathbf{A}^{f_2}$, и кривая, соответствующая точке x , имеет вид

$$E_x \sim \widehat{\mathbf{Z}}^2 \backslash \mathbf{C} \times \mathbf{A}^{f_2} / L_x$$

и снабжена изоморфизмом $V_f(E) \sim L_x \otimes \mathbf{A}^f \xrightarrow{\sim} \mathbf{A}^{f_2}$. Из этого уже легко получить утверждение (3.8). ■

Обозначим через $f_n: E \rightarrow M_n$ универсальную эллиптическую кривую над M_n . Зафиксируем целое число k и введем следующее

Определение 3.9. Обозначим через W (или через ${}^k W$, если есть опасность путаницы) следующее векторное \mathbf{Q} -пространство:

$$W = \varinjlim_n H^1(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*}(\underline{\mathbf{Q}}))) = \varinjlim_n {}_n W.$$

Это пространство зависит только от универсальной эллиптической кривой (с точностью до изогении) $f_\infty: E \rightarrow M_\infty$ так, что, посредством перенесения структуры, оно снабжается действием слева адельной группы $GL_2(\mathbf{A}^f)$.

Для простого числа l векторное пространство $W_l = W \otimes \mathbf{Q}_l$ имеет чисто алгебраическое определение в терминах l -адических когомологий схем над алгебраическим замыканием $\bar{\mathbf{Q}}$ поля \mathbf{Q} , получающихся с помощью расширения поля скаляров из схем M_n :

$$W_l = \varinjlim_n H^1(M_n \otimes \bar{\mathbf{Q}}, \text{Sym}^k(R^1 f_{n*}(\underline{\mathbf{Q}}_l))) = \varinjlim_n {}_n W_l, \quad (3.10)$$

так что группа Галуа $\bar{\mathbf{Q}}$ над \mathbf{Q} действует, посредством перенесения структуры, на W_l и на ${}_n W_l$.

Наконец, пространство M_n^{an} является несвязным объединением факторпространств полуплоскости Пуанкаре по конгруэнцподгруппам группы $SL_2(\mathbf{Z})$, так что, обозначая через ω обратимый пучок над M_n , определенный кривой E , получаем по теореме Шимуры (2.10):

$$W_\infty = W \otimes \mathbf{C} =$$

$$= \varinjlim_n (H^0(\bar{M}_n^{\text{an}}, \Omega^1 \otimes \omega^k) \oplus \overline{H^0(\bar{M}_n^{\text{an}}, \Omega^1 \otimes \omega^k)}). \quad (3.11)$$

Это разложение пространства $W \otimes \mathbf{C}$ в два комплексно сопряженных подпространства, одно из которых является пространством всех голоморфных автоморфных параболических форм веса $k+2$ относительно некоторой конгруэнцподгруппы группы $SL_2(\mathbf{Z})$, аналогично разложению Ходжа („типа $(0, k+1) + (k+1, 0)$ “).

Действие адельной группы коммутирует с действием группы Галуа и сохраняет это разложение.

Хотя l -адическая локальная система $R^1 f^* \underline{\mathbf{Q}}_l$ и три-виальная над M_∞ , я не знаю, существует ли связь между W_l и

$$\lim_{\rightarrow} (\tilde{H}^1(M_n \otimes \bar{\mathbf{Q}}, \underline{\mathbf{Q}}_l)) \otimes \text{Sym}^k(\underline{\mathbf{Q}}_l^2).$$

(3.12) Пусть $n \geq 3$ — целое число и K_n — то же, что и в 3.8. Тогда $W^{K_n} = {}_n W$. Это проверяется переходом к пределу и вытекает из того, что *рациональные* когомологии факторпространства по конечной группе состоят из инвариантных элементов относительно действия этой группы на когомологиях исходного пространства.

Для каждого простого p положим $W^p = W^{GL_2(\mathbf{Z}_p)}$. Переходя к пределу, получаем

$$W^{(p)} = \varinjlim_{(n, p)=1} {}_n W.$$

На этом пространстве когомологий действуют еще:

(i) подгруппа $\prod_{l \neq p} GL_2(\mathbf{Q}_l)$ группы $GL_2(\mathbf{A}^f)$, так как она содержится в централизаторе $GL_2(\mathbf{Z}_p)$;

(ii) алгебра Гекке $\underline{H}(GL_2(\mathbf{Q}_p), GL_2(\mathbf{Z}_p))$ — алгебра целых мер на дискретном пространстве $GL_2(\mathbf{Q}_p)/GL_2(\mathbf{Z}_p)$, левоинвариантных относительно действия группы $GL_2(\mathbf{Z}_p)$: эта подалгебра групповой алгебры группы $GL_2(\mathbf{Q}_p)$ действует на W с сохранением $W^{(p)}$. Эта алгебра действует даже на каждом ${}_n W$, где n взаимно просто с p .

Алгебра Гекке имеет в качестве базиса двойные классы смежности группы $GL_2(\mathbf{Q}_p)$ по подгруппе $GL_2(\mathbf{Z}_p)$ (меры, ассоциированные с их характеристическими функциями), и известно, что

$$\underline{H}(GL_2(\mathbf{Q}_p), GL_2(\mathbf{Z}_p)) = \underline{\mathbf{Z}}[T_p, R_p, R_p^{-1}],$$

где T_p и R_p — двойные классы матриц

$$\begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix} \text{ и } \begin{pmatrix} p^{-1} & 0 \\ 0 & p^{-1} \end{pmatrix}.$$

(3.13) Пусть p — простое число, $n \geq 3$ — целое число, взаимно простое с p , и $F_{n,p}$ — функтор, сопоставляющий каждой схеме S множество классов изоморфных коммутативных диаграмм S -схем вида

$$\begin{array}{ccc}
 & (\mathbb{Z}/(n))^2 & \\
 \alpha \swarrow & & \searrow \alpha' \\
 E_n & \xrightarrow{\quad} & F_n \\
 \downarrow & & \downarrow \\
 E & \xrightarrow{\varphi} & F
 \end{array} \tag{3.14}$$

где φ есть p -изогения эллиптических кривых, а α — изоморфизмы. Обозначим через q_1 и $q_2: F_{n,p} \rightarrow M_n$ морфизмы функторов, сопоставляющие диаграмме (3.14) поддиаграмму (E, E_n, α) и (F, F_n, α') соответственно.

ПРЕДЛОЖЕНИЕ 3.15. Функтор $F_{n,p}$ представляется некоторой схемой $M_{n,p}$, и морфизмы $q_1, q_2: M_{n,p} \rightarrow M_n$ конечны.

Автоморфизм σ функтора $F_{n,p}$, переводящий $\varphi: E \rightarrow F$ в $\varphi': F \rightarrow E$, переставляет q_1 и q_2 ; достаточно, следовательно, рассмотреть морфизм q_1 . Он отождествляет $F_{n,p}$ с функтором подгрупп порядка p универсальной эллиптической кривой над M_n , так что по теории схем Гильберта функтор $F_{n,p}$ представим и схема $M_{n,p}$ собственна над M_n . Пусть s — геометрическая точка схемы M_n , тогда $q_1^{-1}(s)$ — это множество подгрупп порядка p в E_s , состоящее из $p+1$ элементов, если $\text{char}(k(s)) \neq p$, и одного (ядра эндоморфизма Фробениуса), если $\text{char}(k(s)) = p$. ■

Можно показать, что схема $M_{n,p}$ регулярна и что q_1 и q_2 конечны и плоски; мы не будем пользоваться этими тонкими результатами и удовлетворимся лишь замечанием, что над $\text{Spec } \mathbf{Z} \left[\frac{1}{p} \right]$ любое из q_i превращает $M_{n,p}$ в этальное накрытие степени $p+1$ схемы M_n .

Морфизмы q_i включаются в следующую коммутативную диаграмму:

$$\begin{array}{ccccc}
 & q_1^* E & \xrightarrow{\psi} & q_2^* E & \\
 \searrow & & \downarrow u & & \searrow v \\
 E & & M_{n,p} & & E \\
 \swarrow f_n & \searrow q_1 & \downarrow & \searrow q_2 & \swarrow f_n \\
 M_n & & M_{n,p} & & M_n
 \end{array} \quad (3.16)$$

где (ψ, u, v) — часть универсальной диаграммы (3.14).

Обозначим через I_p морфизм схемы M_n в M_n , соответствующий морфизму функторов $(E, a) \rightarrow (E, a/p)$: $I_p^*(E, a) = (E, a/p)$:

$$\begin{array}{ccc}
 E & \longrightarrow & E \\
 \downarrow & & \downarrow \\
 M_n & \xrightarrow{I_p} & M_n
 \end{array} \quad (3.17)$$

Тогда I_p^* является автоморфизмом пространства $\tilde{H}^i(M_n^{\text{an}}, \text{Sym}^k(R^!f_{n*}\mathbf{Z}))$.

Следующий факт требует кропотливого, но рутинного доказательства.

ПРЕДЛОЖЕНИЕ 3.18. (i) Эндоморфизм T_p пространства ${}_nW$ выражается при помощи диаграммы (3.16) как

композиция морфизмов

$$\begin{aligned} \tilde{H}^1(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*} \underline{\mathbf{Q}})) &\xrightarrow{q_2^*} \tilde{H}^1(M_{n,p}^{\text{an}}, \text{Sym}^k(R^1 v_* \underline{\mathbf{Q}})) \xrightarrow{\varphi^*} \\ &\rightarrow \tilde{H}^1(M_n^{\text{an}}, \text{Sym}^k(R_{\mu_*}^1 \underline{\mathbf{Q}})) \xrightarrow{q_1^*} \tilde{H}^1(M_n^{\text{an}}, \text{Sym}^k(R^1 f_{n*} \underline{\mathbf{Q}})), \end{aligned}$$

где q_{1*} — „морфизм следа“ накрытия q_1 .

(ii) Аналогично $R_p = p^k I_p^*$. ■

Недоверчивый читатель может забыть адельные рассуждения и определить T_p с помощью (i).

Для $n=1$ или 2 мы полагаем ${}_n W = W^{K_n}$, так что

$${}_1 W = {}_n W^{GL_2(\mathbb{Z}/(n))}.$$

Пусть S_{k+2} — пространство параболических модулярных форм веса $k+2$ относительно группы $SL_2(\mathbb{Z})$, тогда изоморфизм Шимуры (3.11) индуцирует следующий изоморфизм:

$${}^k W_\infty = {}^k W \otimes \mathbf{C} = S_{k+2} \oplus \bar{S}_{k+2}.$$

Кропотливо, но рутинно доказывается

ПРЕДЛОЖЕНИЕ 3.19. Эндоморфизм T_p пространства ${}_1 W_\infty$ с помощью изоморфизма Шимуры отождествляется с прямой суммой оператора Гекке на S_{k+2} (с множителем p^{k-1}) и его сопряженного. ■

(3.20) Имеют место канонические изоморфизмы

$$\Lambda^2 R^1 f_{n*} \underline{\mathbf{Z}}_l \sim R^2 f_{n*} \underline{\mathbf{Z}}_l \sim \underline{\mathbf{Z}}_l(-1),$$

так что $\text{Sym}^k(R^1 f_{n*} \underline{\mathbf{Z}}_l)$ снабжается некоторой билинейной (симметрической для k четных и кососимметрической для k нечетных) формой со значениями в $\underline{\mathbf{Z}}_l(-k)$. Тензорное умножение на $\underline{\mathbf{Q}}_l$ делает ее невырожденной.

Пусть F — к. л. п. $\underline{\mathbf{Q}}_l$ -пучок над гладкой схемой X чистой размерности n над алгебраически замкнутым полем k , тогда двойственность Пуанкаре дает

$$H^i(X, \underline{F})^\vee \sim H^{2n-i}(X, \underline{\text{Hom}}(\underline{F}, \underline{\mathbf{Q}}_l(n))),$$

$$H_c^i(X, \underline{F})^\vee \sim H_c^{2n-i}(X, \underline{\text{Hom}}(\underline{F}, \underline{\mathbf{Q}}_l(n))),$$

откуда

$$\tilde{H}^t(X, \underline{F})^\vee \sim \tilde{H}^{2n-t}(X, \underline{\text{Hom}}(\underline{F}, \underline{\mathbf{Q}_l}(n))).$$

Полагая здесь $X = \bar{M}_n$ и $\underline{F} = \text{Sym}^k(R^l f_{n*} \underline{\mathbf{Q}_l})$, мы можем определить на ${}_n^h W_l$ невырожденную билинейную форму $n(\cdot, \cdot)$ со значениями в $\underline{\mathbf{Q}_l}(-k-1)$. Она симметрична для нечетных k и кососимметрична для четных. Это l -адический аналог скалярного произведения Петерсона. Если $n|m$ и $\psi: M_m \rightarrow M_n$ — накрытие степени d , то

$$_m(\psi^*x, \psi^*y) = d \cdot {}_n(x, y).$$

4. Формула сравнения

В этом пункте мы фиксируем целые числа $k \geq 0$, $n \geq 3$ и простые числа p, l . Предположим, что p взаимно просто с l и n . Обозначим через $f_n: E \rightarrow M_n$ универсальную эллиптическую кривую над M_n , снабженную изоморфизмом $a: E_n \xrightarrow{\sim} (\mathbf{Z}/(n))^2$.

Для произвольной схемы Y обозначим через a однозначно определенный морфизм схемы Y в $\text{Spec } \mathbf{Z}$ или, при случае, в подсхему схемы $\text{Spec } \mathbf{Z}$.

Если схема Y отделима и конечного типа над $\text{Spec } \mathbf{Z}$ и если \underline{F} есть \mathbf{Z}_l - или \mathbf{Q}_l -пучок над Y , то обозначим через $R^i a_*(Y, \underline{F})$ (соответственно $R^i a_!(Y, \underline{F})$, соответственно $R^i \tilde{a}(Y, \underline{F})$) \mathbf{Z}_l - или \mathbf{Q}_l -пучок над $\text{Spec } \mathbf{Z}$, являющийся i -м прямым образом пучка \underline{F} относительно морфизма \mathbf{Q} (соответственно i -м прямым образом с собственными носителями, соответственно $\text{Im}(R^i a_!(Y, \underline{F}) \rightarrow R^i a_*(Y, \underline{F}))$). Для натурального числа $m \in \mathbf{N}$ положим $Y[1/m] = Y \times \text{Spec } \mathbf{Z}[1/m]$.

Теорема 4.1 (Игуза [3]). *Схема M_n компактифицируется в схему кривых M_n^* , проективную и гладкую над $\text{Spec } \mathbf{Z}[1/n]$, таким образом, что $M_n^* \setminus M_n$ является эталонным накрытием над $\text{Spec } \mathbf{Z}[1/n]$.*

Схема M_n является формально гладкой и, следовательно, гладкой над $\text{Spec } \mathbf{Z}$.

Модулярный инвариант j универсальной эллиптической кривой над M_n определяет морфизм M_n в аффинную прямую A^1 над $\text{Spec } \mathbf{Z}[1/n]$. Морфизм j конечен и эталонно накрывает прямую A^1 вне сечений 0 и 1728. Действительно:

(а) Две эллиптические кривые над алгебраически замкнутым полем с одним и тем же инвариантом j изоморфны ([8], п. 6.3), следовательно, геометрические слои морфизма j конечны. Далее, схемы M_n и A^1 гладки и имеют одинаковую относительную размерность над $\text{Spec } \mathbf{Z}$, следовательно, j квазиконечен и плосок.

(б) Если эллиптическая кривая E над полем частных K кольца дискретного нормирования R имеет целый инвариант $j \in R$ и ее точки порядка n рациональны над K , то E имеет хорошую редукцию. Валюативный критерий собственности показывает тогда, что морфизм j собственный.

(в) Если эллиптические кривые E и F над схемой S имеют один и тот же инвариант j и если j и $j - 1728$ обратимы, то схема $\underline{\text{Isom}}(S; E, F)$ изоморфизмов между E и F будет этална над S (см. [8], п. 6.3). В диаграмме

$$\begin{array}{ccc} \underline{\text{Isom}}(M_n \times_{A^1} M_n; \text{pr}_1^* E, \text{pr}_2^* E) & \sim & M_n \times GL_2(\mathbf{Z}/(n)) \\ \downarrow u & & \downarrow v \\ M_n \times_{A^1} M_n & \xrightarrow{\text{pr}_1} & M_n \end{array}$$

где $j \neq 0, j \neq 1728$, морфизмы u и v эталны и сюръективны. Следовательно, проекция pr_1 также этална и в силу плоского спуска морфизм j этален.

Бесконечно удаленное сечение проективной прямой $P^1 \supset A^1$ над $\text{Spec } \mathbf{Z}[1/n]$ является регулярным дивизором с общей точкой характеристики 0 на регулярной схеме. Из теоремы Абьянкара (см. [6]) следует тогда, что вдоль этого дивизора $j = \infty$, схема M_n умеренно разветвлена над P^1 и что нормализация M_n^* схемы P^1 в M_n удовлетворяет условию (4.1). ■

Из той же теоремы следует, что к. л. п. \mathbf{Z}_l -пучки $R^l f_{n*} \underline{\mathbf{Z}}_l$ над $M_n[1/l]$ умеренно разветвлены на бесконечности. Отсюда, из теоремы 4.1 и из теорем специали-

зации l -адических когомологий (см. [5]) следует, что $R^i a_*(M_n \text{Sym}^k(R^1 f_{n*} \underline{\mathbf{Z}}_l))$, $R^i a_!(M_n, \text{Sym}^k(R^1 f_{n*} \underline{\mathbf{Z}}_l))$ и, следовательно, $R^i \tilde{a}(M_n, \text{Sym}^k(R^1 f_{n*} \underline{\mathbf{Z}}_l))$ будут к. л. п. $\underline{\mathbf{Z}}_l$ -пучками над $\text{Spec } \mathbf{Z}[1/n, 1/l]$, совместимыми с любой заменой базы.

Следствие 4.2. *Модуль Галуа ${}_n W_l$ свободен в геометрической точке $\bar{\mathbf{Q}}$ схемы $\text{Spec } \mathbf{Z}[1/n, 1/l]$ к. л. п. \mathbf{Q}_l -пучка $R^i \tilde{a}(M_n, \text{Sym}^k(R^1 f_{n*} \underline{\mathbf{Z}}_l)) \otimes \mathbf{Q}_l$. Он неразветвлен вне n и l .* ■

Рассмотрим над $M_n \otimes \mathbf{F}_p$ две коммутативные диаграммы

$$\begin{array}{ccc}
 & (\mathbf{Z}/(n))^2 & \\
 \alpha \nearrow & & \searrow \alpha^{(p)} \\
 E_n & \xrightarrow{\quad} & E_n^{(p)} \\
 \downarrow & & \downarrow \\
 E & \xrightarrow{F} & E^{(p)}
 \end{array}$$

$$\begin{array}{ccc}
 & (\mathbf{Z}/(n))^2 & \\
 p\alpha^{(p)} \nearrow & & \searrow \alpha \\
 E_n^{(p)} & \xrightarrow{\quad} & E_n \\
 \downarrow & & \downarrow \\
 E^{(p)} & \xrightarrow{V} & E
 \end{array}$$

или, сокращенно,

$$F: (E, \alpha) \rightarrow (E^{(p)}, \alpha^{(p)}) \quad \text{и} \quad V: (E^{(p)}, p\alpha^{(p)}) \rightarrow (E, \alpha),$$

где F — морфизм Фробениуса, а V — его сопряженный. Эти диаграммы определяют морфизмы Φ_1 и Φ_2 схемы

$M_n \otimes \mathbf{F}_p$ в схему $M_{n,p}$. Морфизмы Φ_1 и Φ_2 конечны, как сечения морфизмов q_1 и q_2 . Они определяют в свою очередь морфизм

$$\Phi = \Phi_1 \sqcup \Phi_2: M_n \otimes \mathbf{F}_p \sqcup M_n \otimes \mathbf{F}_p \rightarrow M_{n,p} \otimes \mathbf{F}_p.$$

Пусть Φ^h — ограничение морфизма Φ на открытые подмножества M_n^h и $M_{n,p}^h$ схем $M_n \otimes \mathbf{F}_p$ и $M_{n,p} \otimes \mathbf{F}_p$, отвечающие кривым с ненулевым инвариантом Хассе.

ПРЕДЛОЖЕНИЕ 4.3. *Морфизм Φ^h является изоморфизмом.*

Пусть $\varphi: E_1 \rightarrow E_2$ есть p -изогения эллиптических кривых с инвариантом Хассе, обратимым на схеме S характеристики p . В каждой геометрической точке схемы S либо ядро $\text{Кег}\varphi$ морфизма φ , либо его двойственное по Картье (изоморфное $\text{Кег}'\varphi$) этально над S . Свойство „ $\text{Кег}\varphi$ этально“ является открытым, так что локально по S $\text{Кег}\varphi$ или $\text{Кег}'\varphi$ чисто инфинитезимально. Единственная инфинитезимальная подгруппа порядка p кривой E_1 или E_2 будет ядром морфизма Фробениуса: в первом случае φ изоморфен $F: E_1 \rightarrow E_1^{(p)}$, а во втором $'\varphi$ изоморфен $F: E_2 \rightarrow E_2^{(p)}$, следовательно, φ изоморфен $V: E_2^{(p)} \rightarrow E_2$. ■

ПРЕДЛОЖЕНИЕ 4.4. (i) *Схема $M_{n,p}$ является гладкой над $\text{Spec } \mathbf{Z}$ вне точек характеристики p , где $h=0$.*

(ii) *Морфизмы q_1 и q_2 индуцируют конечные и плоские морфизмы q'_1 и q'_2 нормализации $M'_{n,p}$ схемы $M_{n,p}$ в M_n .*

(iii) *Морфизм Φ пропускается через сторъективный морфизм*

$$\Phi': M_n \otimes \mathbf{F}_p \sqcup M_n \otimes \mathbf{F}_p \rightarrow M'_{n,p} \otimes \mathbf{F}_p.$$

Автоморфизм σ из п. (3.15) меняет местами φ и $'\varphi$, поэтому достаточно доказать утверждение (i) в тех точках характеристики p схемы $M_{n,p}$, где ядро φ инфинитезимально. Но в этом случае нет никаких препятствий для инфинитезимального поднятия эллиптической

кривой и инфинитезимальной части ядра умножения на p .

Там, где $p = h = 0$, слой конечного морфизма (3.15) $q_i: M_{n,p} \rightarrow M_n$ состоит из одной точки, так что открытое множество гладкости схемы $M_{n,p}$ плотно в $M_{n,p}$ и $M'_{n,p}$ всюду имеет размерность 2. Схема M_n будет регулярной согласно EGA IV 16.5.1, 17.3.5, а морфизм $q_i: M'_{n,p} \rightarrow M_n$ плоский, что доказывает (ii).

Наконец, утверждение (iii) следует из того, что морфизм Φ конечен и $M_n \otimes \mathbf{F}_p$ — нормальная кривая. ■

Эндоморфизм Гекке T_p пространства ${}_nW_l$, указанный явно в (3.18), — это тензорно умноженный на \mathbf{Q}_l слой в геометрической точке $\bar{\mathbf{Q}}$ схемы $\text{Spec } \mathbf{Z}[1/n, 1/l]$ эндоморфизма (обозначаемого также символом T_p) пучка $R^1\tilde{a}(M_n, \text{Sym}^k(R^1f_{n*}\underline{\mathbf{Z}}_l))$, определенного „соответствием“

$$\begin{array}{ccccc}
 q'_1 * E & \xrightarrow{\psi} & q'_2 * E & & \\
 \searrow & u & \swarrow & u & \searrow \\
 & E & M'_{n,p} & E & \\
 f_n \downarrow & q'_1 \downarrow & q'_2 \downarrow & f_n \downarrow & \\
 M_n & & M_n & &
 \end{array} \quad (4.5)$$

$$T_p = q'_{1*} \psi^* q'^{*}_2$$

(ср. 3.18).

Аналогично интерпретируются и эндоморфизмы R_p и I_p .

Лемма 4.6. Пусть над нётеровой схемой S заданы отдельные схемы конечного типа $X, Y, Z_1, Z_2; \mathbf{Z}_l$ -пучок F над X и \mathbf{Z}_l -пучок G над Y . Каждый из структурных морфизмов X, Y, Z_1, Z_2 в S будем обозначать одной и

той же буквой a . Пусть задана коммутативная диаграмма S -схем и морфизмы пучков

$$\begin{array}{ccc}
 & z_1 & \xrightarrow{f} z_2 \\
 & \searrow x_1 & \swarrow x_2 \\
 X & & Y
 \end{array}$$

$$y_1^*G \xrightarrow{z_1} x_1^*F, \quad y_2^*G \xrightarrow{z_2} x_2^*F.$$

Предположим, что $f^*z_2 = z_1$, морфизмы y_1 и y_2 собственны, морфизмы x_1 и x_2 конечны и плоски и что для каждой геометрической точки s схемы Z_2 кратность s в своем слое $x_2^{-1}(x_2(s))$ равна сумме кратностей в своих слоях (относительно x_1) геометрических точек схемы Z_1 — прообразов точки s относительно морфизма f . Тогда следующая диаграмма коммутативна:

$$\begin{array}{ccccccc}
 R^i\tilde{a}(Y, \underline{G}) & \xrightarrow{y_1^*} & R^i\tilde{a}(Z_1, \underline{G}) & \xrightarrow{z_1} & R^i\tilde{a}(Z_1, \underline{F}) & \xrightarrow{x_{1*}} & R^i\tilde{a}(X, \underline{F}) \\
 \parallel & & \uparrow & & \uparrow & & \parallel \\
 R^i\tilde{a}(Y, \underline{G}) & \xrightarrow{y_2^*} & R^i\tilde{a}(Z_2, \underline{G}) & \xrightarrow{z_2} & R^i\tilde{a}(Z_2, \underline{F}) & \xrightarrow{x_{2*}} & R^i\tilde{a}(X, \underline{F})
 \end{array}$$

Эта лемма следует из аналогичных лемм для $R^i a_*$ и $R^l a_*$. Коммутативность первых квадратов тривиальна. Последний переписывается в виде

$$\begin{array}{ccccc}
 R^i\tilde{a}(Z_1, x_1^*F) & \xleftarrow{\sim} & R^i\tilde{a}(X, x_{1*}x_1^*F) & \xrightarrow{\text{Tr}} & R^i\tilde{a}(X, \underline{F}) \\
 \uparrow & & \uparrow & & \parallel \\
 R^i\tilde{a}(Z_2, x_2^*F) & \xleftarrow{\sim} & R^i\tilde{a}(X, x_{2*}x_2^*F) & \xrightarrow{\text{Tr}} & R^i\tilde{a}(X, \underline{F})
 \end{array}$$

и остается вспомнить определение следа для проверки того, что квадрат

$$\begin{array}{ccc}
 x_{1*}x_1^*\underline{F} & \xrightarrow{\text{Tr}} & \underline{F} \\
 \uparrow & & \parallel \\
 x_{2*}x_2^*\underline{F} & \xrightarrow{\text{Tr}} & \underline{F}
 \end{array}$$

коммутативен. ■

(4.7) Обозначим через T_p/\mathbf{F}_p эндоморфизм, индуцированный эндоморфизмом T_p над ограничением на $\text{Spec } \mathbf{F}_p$ к. л. п. \mathbf{Z}_l -пучка $R^1\tilde{a}(M_n, \text{Sym}^k(R^1f_{n*}\mathbf{Z}_l))$. Имеем $R^1\tilde{a}(M_n, \text{Sym}^k R^1f_{n*}\mathbf{Z}_l)|_{\text{Spec } \mathbf{F}_p} \xrightarrow{\sim} R^1\tilde{a}(M_n \otimes \mathbf{F}_p, \text{Sym}^k R^1f_{n*}\mathbf{Z}_l)$.

Морфизм следа для конечного и плоского морфизма совместим с заменой базы, так что эндоморфизм T_p/\mathbf{F}_p может быть построен по модели (3.18), исходя из слоя над \mathbf{F}_p „соответствия“ (4.5). Лемма (4.6), примененная к коммутативной диаграмме

$$\begin{array}{ccc} M_n \otimes \mathbf{F}_p \amalg M_n \otimes \mathbf{F}_p & \xrightarrow{\Phi'} & M_{n,p} \otimes \mathbf{F}_p \\ \searrow & \swarrow q'_1 & \downarrow q'_2 \\ M_n \otimes \mathbf{F}_p & & M_n \otimes \mathbf{F}_p \end{array}$$

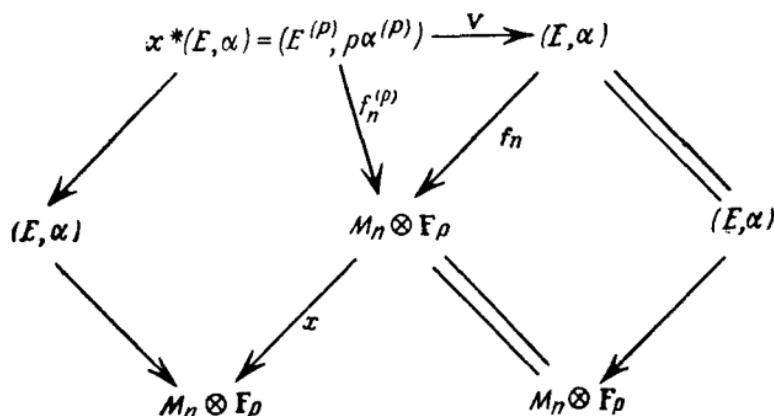
дает тогда разложение T_p/\mathbf{F}_p в сумму эндоморфизмов, определенных следующими соответствиями:

(a)

$$\begin{array}{ccccc} (E, \alpha) & \longrightarrow & (E^{(p)}, \alpha^{(p)}) = F^*(E, \alpha) & & \\ \parallel & & \downarrow & & \\ (E, \alpha) & & M_n \otimes \mathbf{F}_p & & (E, \alpha) \\ \searrow & \swarrow & \downarrow F & \searrow & \swarrow \\ M_n \otimes \mathbf{F}_p & & M_n \otimes \mathbf{F}_p & & M_n \otimes \mathbf{F}_p \end{array}$$

где F — абсолютный морфизм Фробениуса. В этом соответствии узнается геометрический эндоморфизм Фробениуса.

(6)



Стрелка x здесь является композицией $I_p^{-1} \circ F$:

$$\begin{array}{ccccc} (E, \alpha) & \longleftarrow & (E, pa) & \longleftarrow & (E^{(p)}, p\alpha^{(p)}) \\ \downarrow & & \downarrow & & \downarrow \\ M_n \otimes \mathbf{F}_p & \xleftarrow{I_p^{-1}} & M_n \otimes \mathbf{F}_p & \xleftarrow{F} & M_n \otimes \mathbf{F}_p \end{array}$$

Соответствующий эндоморфизм является, следовательно, композицией

$$\begin{aligned} V: R^1\tilde{a}(M_n \otimes \mathbf{F}_p, \text{Sym}^k(R^1f_{n*}\underline{\mathbf{Z}}_l)) &\xrightarrow{V^*} R^1\tilde{a}(M_n \otimes \mathbf{F}_p, \\ \text{Sym}^k(R^1f_{n*}^{(p)}\underline{\mathbf{Z}}_l)) &\xrightarrow{\text{Tr}_F} R^1\tilde{a}(M_n \otimes \mathbf{F}_p, \text{Sym}^k(R^1f_{n*}\underline{\mathbf{Z}}_l)) \end{aligned}$$

и $I_p^* = \text{Tr}_{I_p^{-1}}$ (это эндоморфизм $R^1\tilde{a}(M_n \otimes \mathbf{F}_p, \text{Sym}^k R^1f_{n*}\underline{\mathbf{Z}}_l)$).

ПРЕДЛОЖЕНИЕ 4.8. Имеет место разложение $T_p/\mathbf{F}_p = F + I_p^*V$ и

(i) морфизм F отождествляется с обратным элементом для автоморфизма Фробениуса („арифметического“) φ_p группы Галуа $\text{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$, действующей на $\tilde{H}^1(M_n \otimes \bar{\mathbf{F}}_p, \text{Sym}^k(R^1f_{n*}\underline{\mathbf{Z}}_l))$;

(ii) морфизмы F и V сопряжены относительно скалярного произведения (3.20);

(iii) $FV = VF = p^{k+1}$.

За доказательством утверждения (i) о связи между геометрическим и арифметическим элементами Фробениуса мы отсылаем к докладу Хузеля (SGA, 5. XV). Композиция VF — это композиция следующих морфизмов:

$$\begin{array}{ccccccc}
 E & \xleftarrow{\quad} & E & \xrightarrow{(P)F_E} & E & \xrightarrow{V_E} & E \\
 \downarrow & & \searrow & & \downarrow & & \downarrow \\
 M_n & \xleftarrow{F} & M_n & \xrightarrow{F} & M_n & \xrightarrow{F} & M_n
 \end{array}$$

$$VF = \text{Tr}_F \circ F_E^* \circ V_E^* \circ F^*.$$

Морфизм $F_E^* V_E^* = (F_E V_E)^* = (p, 1_E)^*$ действует на $\text{Sym}^k R^1 f_{n*} \underline{\mathbf{Z}}_l$, как умножение на p^k , таким образом $VF = p^k$. $\text{Tr}_F \circ F^* = p^{k+1}$, поскольку $F: M_n \rightarrow M_n$ имеет степень p .

С помощью перенесения структуры φ_p сохраняет скалярное произведение п. (3.20) со значением в группе $\mathbf{Q}_l(-k-1)$, на которую φ_p действует умножением на p^{-k-1} . Следовательно, имеем

$$(Fx, y) = p^{k+1} (\varphi_p Fx, \varphi_p y) = (x, p^{k+1} F^{-1} y) = (x, Vy). \blacksquare$$

Следующая теорема, по существу совпадающая с предложением (4.8), восходит к Эйхлеру.

Теорема 4.9 (конгруэнцформула). *Пусть $K_{n,l}$ — максимальное подрасширение в $\bar{\mathbf{Q}}$, неразветвленное вне n , и l , φ_p — элемент Фробениуса в $\text{Gal}(K_{n,l}/\mathbf{Q})$, связанный с простым числом p , F — эндоморфизм φ_p^{-1} пространства ${}_n W_l$ и V — сопряженный к F относительно скалярного произведения (3.20). Тогда*

$$T_p = F + I_p^* V, \quad FV = p^{k+1}$$

и

$$1 - T_p X + p R_p X^2 = (1 - FX)(1 - I_p^* V X). \blacksquare$$

5. Из гипотез Вейля следует гипотеза Рамануджана

Пусть p — простое число и X — схема над \mathbf{F}_p . Обозначим через $\bar{\mathbf{F}}_p$ алгебраическое замыкание поля \mathbf{F}_p , через $F: X \rightarrow X$ — эндоморфизм Фробениуса („геометрический“) и положим $\bar{X} = X \otimes \bar{\mathbf{F}}_p$; l всегда будет обозначать простое число, отличное от p .

Под „гипотезами Вейля“ будем понимать следующее.

Пусть X — проективная и гладкая схема над \mathbf{F}_p и l — простое число, отличное от p . Тогда собственные значения эндоморфизма F^* пространств $H^i(\bar{X}, \mathbf{Q}_l)$ являются целыми алгебраическими числами, равными по абсолютной величине $p^{i/2}$.

В обозначениях (4.9) по модулю этих гипотез имеет место следующая (напомним, что $(p, n) = 1$)

Теорема 5.1. *Если гипотезы Вейля верны, то собственные значения эндоморфизма F пространства ${}_n^k W_l$ будут целыми алгебраическими числами (комплексно сопряженными между собой) с абсолютным значением $p^{k+1/2}$.*

Предположим, что гипотезы Вейля верны.

Лемма 5.2. (по модулю гипотез Вейля). *Пусть X — схема, гладкая над \mathbf{F}_p , которая может быть представлена как открытая подсхема в некоторой проективной и гладкой схеме X^* . Тогда собственные значения эндоморфизма F^* пространства $\tilde{H}^i(\bar{X}, \mathbf{Q}_l)$ будут целыми алгебраическими числами с абсолютным значением $p^{i/2}$.*

Естественное отображение из $H_c^i(\bar{X}, \mathbf{Q}_l)$ в $H^i(\bar{X}, \mathbf{Q}_l)$ пропускается через $H^i(\bar{X}^*, \mathbf{Q}_l)$:

$$H_c^i(\bar{X}, \mathbf{Q}_l) \rightarrow H^i(\bar{X}^*, \mathbf{Q}_l) \rightarrow H^i(\bar{X}, \mathbf{Q}_l).$$

Таким образом, $\tilde{H}^i(\bar{X}, \mathbf{Q}_l)$ как $\text{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ -модуль является фактором некоторого подобъекта из $H^i(\bar{X}^*, \mathbf{Q}_l)$. ■

Лемма 5.3 (по модулю гипотез Вейля). *Пусть S — схема, гладкая над \mathbf{F}_p , и $f: A \rightarrow S$ — некоторая абелева схема над S . Предположим, что A может быть представлена как открытая подсхема в проективной и гладкой*

схеме A^* над \mathbf{F}_p . Тогда геометрический эндоморфизм Фробениуса F^* на $\tilde{H}^i(\bar{S}, R^j f_* \underline{\mathbf{Q}}_l)$ имеет в качестве собственных значений целые алгебраические числа, равные по абсолютной величине $p^{i+j/2}$.

Пусть $m > 1$ — целое число. Рассмотрим спектральные последовательности Лере

$$E: E_2^{ij} = H^i(\bar{S}, R^j f_* \underline{\mathbf{Q}}_l) \Rightarrow H^{i+j}(\bar{A}, \underline{\mathbf{Q}}_l),$$

$${}_c E: {}_c E_2^{ij} = H_c^i(\bar{S}, R^j f_* \underline{\mathbf{Q}}_l) \Rightarrow H_c^{i+j}(\bar{A}, \underline{\mathbf{Q}}_l).$$

Эндоморфизм умножения на m : $\psi_m = m1_A$ определяет эндоморфизмы E и ${}_c E$, включающиеся в следующую коммутативную диаграмму:

$$\begin{array}{ccc} {}_c E & \rightarrow & E \\ \downarrow \psi_m^* & & \downarrow \psi_m^* \\ {}_c E & \rightarrow & E \end{array}$$

Морфизм ψ_m^* действует на $R^j f_* \underline{\mathbf{Q}}_l$ как умножение на m^j , так что на членах ${}_c E_r^{ij}$ и E_r^{ij} спектральных последовательностей ${}_c E$ и E эндоморфизм ψ_m^* является умножением на m^j . Отображения d_r ($r \geq 2$) коммутируют с ψ_m^* и переводят E_r^{ij} (соответственно ${}_c E_r^{ij}$) в E_r^{i+j} (соответственно в ${}_c E_r^{i+j}$) с $j \neq j'$. Следовательно, все они нулевые и E_2^{ij} (соответственно ${}_c E_2^{ij}$) отождествляется с подпространством в $H^{i+j}(\bar{A}, \underline{\mathbf{Q}}_l)$ (соответственно в $H_c^{i+j}(\bar{A}, \underline{\mathbf{Q}}_l)$), где $\psi_m^* = m^i$. Поэтому $\tilde{H}^i(\bar{S}, R^j f_* \underline{\mathbf{Q}}_l)$ отождествляется как модуль Галуа с подпространством пространства $\tilde{H}^{i+j}(\bar{A}, \underline{\mathbf{Q}}_l)$, где также $\psi_m^* = m^i$, и можно применить лемму (5.2). Использованный здесь прием принадлежит Либерману. ■

Пусть $f_n: E \rightarrow M_n \otimes \mathbf{F}_p$ — универсальная эллиптическая кривая над $M_n \otimes \mathbf{F}_p$ и $f_{n,k}: E_k \rightarrow M_n \otimes \mathbf{F}_p$ — ее k -кратное расслоенное произведение самой на себя. Формула Кюннета показывает тогда, что $\underline{\mathbf{Q}}_l$ -пучок $R^k f_{n,k*} \underline{\mathbf{Q}}_l$

имеет в качестве прямого слагаемого k -ю тензорную степень пучка $R^1\mathcal{f}_{n*}\underline{\mathbf{Q}}_l$. Она в свою очередь содержит в качестве прямого слагаемого \mathbf{Q}_l -пучок $\text{Sym}^k(R^1\mathcal{f}_{n*}\underline{\mathbf{Q}}_l)$. Теорема (5.1) вытекает теперь из (5.3) и следующей леммы.

ЛЕММА 5.4. Схема E_k является открытой подсхемой гладкой проективной схемы E_k^* над \mathbf{F}_p .

Пусть E^* — минимальная модель Нерона схемы E над $M_n^* \otimes \mathbf{F}_p$ (4.1). Она является гладкой и проективной схемой над \mathbf{F}_p . Поскольку $n \geq 3$ и точки порядка n в E образуют тривиальное накрытие базы $M_n \otimes \mathbf{F}_p$, то эта модель Нерона „полустабильна“ (случай b_m в классификации Нерона). В частности, проекция $f_n: E^* \rightarrow M_n^*$ имеет только конечное число точек негладкости и в этих точках f_n невырождена (имеет обычные квадратичные особенности).

Пусть E_k^{**} есть k -кратное расслоенное произведение E^* на себя над M_n^* . Для доказательства леммы 5.4 достаточно разрешить особенности схемы E_k^{**} , не затрагивая открытой подсхемы E_k . Докажем прежде всего следующий факт.

ЛЕММА 5.5. Пусть V — подмногообразие аффинного пространства над полем k (с координатами $(X_i)_{0 \leq i \leq r}$, $(Y_i)_{0 \leq i \leq r}$, $(T_i)_{1 \leq i \leq s}$), заданное уравнением

$$X_0 Y_0 = X_1 Y_1 = \dots = X_r Y_r.$$

Пусть \mathfrak{m} — подпучок идеалов пучка \mathcal{O}_V , порожденный одночленами, получающимися из одночлена $\prod_{i=0}^r x_i^i$ перестановками координат, сохраняющими пары $\{X_i, Y_i\}$, $0 \leq i \leq r$. Тогда $\mathfrak{m} = \mathcal{O}_V$ вне особых точек многообразия V и многообразие V , получающееся из V раздутием пучка идеалов \mathfrak{m} , гладко над k .

Особые точки — это те точки V , где обращается в нуль четверка координат X_i, Y_i, X_j, Y_j , $i \neq j$. Дополнением

к образу дивизора $\prod_{i=0}^r x_i^l$ является спектр регулярного кольца

$$k[Y_0/Y_1, X_0/X_1, X_1/X_2, \dots, X_{r-1}/X_r, X_r, T_1, \dots, T_s]$$

(для проверки заметим, что $X_i/X_{i+1} = Y_{i+1}/Y_i$), отсюда следует утверждение 5.5 ■

Теперь показывается, что локально в этальной топологии особенности схемы E_k^{**} такие же, как и у многообразия V (при $r = k - 1$). Это позволяет определить на E_k^{**} пучок идеалов, аналогичный пучку \mathfrak{m} на V (см. 5.5). Раздувая этот идеал, мы получаем E_k^* . ■

Некоторое приближение к следующей теореме было доказано Ихарой [4].

Теорема 5.6. *Гипотезы Вейля влекут за собой гипотезу Рамануджана.*

Заметим прежде всего, что теорема (5.1) остается верной при $n = 1$, так как ${}_1^k W_I$ является подмодулем Галуа модуля ${}_m^k W_I$, инвариантным относительно действия группы $GL_2(\mathbf{Z}/m)^2$. Морфизм I_p^* индуцирует на ${}_1^k W_I$ тождественное отображение и утверждения (4.8) сводятся к соотношению

$$1 - T_p X + p^{k+1} X^2 = (1 - FX)(1 - VX).$$

Эндоморфизмы F и V сопряжены друг другу, так что

$$\det(1 - FX; {}_1^k W_I) = \det(1 - VX; {}_1^k W_I).$$

Действие оператора T_p на ${}_1^k W_I$ индуцируется его действием на ${}_1^k W$ и согласовано с разложением ${}_1^k W \otimes \mathbf{C}$ в сумму пространства параболических модулярных форм S_{k+2} веса $k + 2$ относительно группы $SL_2(\mathbf{Z})$ и его комплексно сопряженного. Из эрмитовости оператора T_p (в скалярном произведении Петерсона) и из (3.19) следует тогда, что

$$\det(1 - T_p X + p^{k+1} X^2; {}_1^k W_I) = \det(1 - T_p X + p^{k+1} X^2; S_{k+2})^2$$

и

$$\det(1 - T_p X + p^{k+1} X^2; S_{k+2})^2 = \det(1 - FX; {}_1^k W_I)^2$$

или

$$\det(1 - T_p X + p^{k+1} X^2; S_{k+2}) = \det(1 - FX; {}_1^k W_I). \quad (5.7)$$

Возвратимся к обозначениям п. 1 и положим $k=10$. В силу теории Гекке и предложения (3.19) формулу (5.7) можно переписать в виде

$$H_p(X) = \det(1 - FX; {}_1^{10} W_I)$$

и остается применить теорему 5.1. ■

Точно так же устанавливается, что гипотезы Вейля влекут за собой гипотезы Петерсона.

СПИСОК ЛИТЕРАТУРЫ

- [1] Вердье (Verdier J.-L.), Sur les intégrales attachées aux formes automorphes (d'après G. Shimura), Sémin. Bourbaki, février 1961, exp. 216.
- [2] Жуанолу (Jouanolou J.-P.), Exposés V et VI de SGA 5.
- [3] Игуза (Igusa J.), Kroneckerian model of fields of elliptic modular functions, *Amer. J. of Math.*, **81** (1959), 561—577.
- [4] Ихара (Ihara Y.), Hecke polynomials as congruence zêta functions in elliptic modular case, *Ann. of Math.*, S. 2, **85** (1967), 267—295.
- [5] Кура (Kuga M.), Шимура (Shimura G.), On the zêta function of a fibre variety whose fibres are abelian varieties, *Ann. of Math.*, S. 2, **82** (1965), 478—539.
- [6] Рейно (Raynaud M.) Exposé XIII de SGA 1 et appendice.
- [7] Серр (Serre J.-P.), Une interprétation des congruences relatives à la fonction τ de Ramanujan, Sémin. Delange — Pisot — Poitou, 1967/68, № 14. (Русский перевод: сб. „Математика“ 13: 4 (1969), 3—15.)
- [8] Тейт (Tate J.), Courbes elliptiques: formulaire — mis au gout du jour par P. Deligne, Notes miméographiées par l'IHES.
- [9] Шимура (Shimura G.), Sur les intégrales attachées aux formes automorphes, *J. Math. Soc. Japan* **11** (1959), 291—311.

Условные обозначения

- EGA — Eléments de géométrie algébrique, par A. Grothendieck et J. Dieudonné, Publ. Math. IHES.
- SGA — Séminaire de géométrie algébrique du Bois — Marie, Notes miméographiées par l'IHES, à paraître à North — Holland.

УКАЗАТЕЛЬ

- Алгебраический морфизм, ассоциированный с представлением 71, 76
Анизотропный тор 67
Арифметическая подгруппа 67

Вейерштрассова форма уравнения эллиптической кривой 113
Высота 143

Группа идеалей 42
— инерции 17
— классов идеалей 42
— мультипликативного типа 41
— разложения 17
— характеров 39

Допустимый характер 97

Изогения 115
Изоморфизм Шимуры 161
Индекс ветвления 17
Исключительное множество 22

Комплексное умножение 57, 118
Конгруэнцформула 181
Кондуктор 78
Конструктивные локально постоянные (к. л. п.) пучки 162

Локально алгебраическое представление 71, 76, 82

Локально алгебраичный гомоморфизм 89

Модуль определяющий 77
— Ходжа — Тейта 73
Модулярный инвариант 113

Нерона — Огга — Шафаревича критерий 115
Нормирование неразветвленное 17

Плотность 18
Поле в абсолютных категориях 162
Почти локально алгебраичный гомоморфизм 89
Представление локально алгебраическое 71, 76, 82
— неразветвленное 18
— определенное над k 49
— l -адическое 13
— — рациональное 20, 25
— — целое 20
— λ -адическое 23
Пространство параболических автоморфных форм 160

Равнораспределенность (равномерная распределенность) 28
Редукция 114
Решетка 13

Согласованные представления 22, 25

Строго согласованные представ- ления 22, 25	E_{ln} 114 E_m 43 E_q 136
Тейта теоремы 75, 110	\tilde{E}_v 114
Top 38	$\varphi \sim \varphi'$ 97
Трансвекция 128	φ_l 51
<i>L</i> -функция	F_v, f_v 46 G_l 120 \tilde{G}_l 126 g_l 120, 136
Характер Гекке 56	GL_V 12
Ходжа — Тейта модуль 74	G_m 38
— — разложение 74	I, I_m 42, 43
Хорошая редукция 113	i_l 136
Чеботарева теорема 19	j 113 \bar{K}, K_s 12 $\text{Rep}_k(H)$ 49
Шафаревича теорема 116	S_m 44 Supp (iii) 44 θ_φ 48 $T_l(\mu)$ 15 T_m 44 $T = R_{K/\mathbb{Q}}(G_{m/K})$ 38
Элемент Фробениуса 17, 18	$U_m, U_{v, m}$ 43
Эллиптические кривые 112	$V_l(\mu)$ 15
— — Тейта 136	χ_E 103
Эндоморфизм Фробениуса 58, 114	χ_l 15 $X(T), X(T_m)$ 59, 60 Y, Y^0, Y^-, Y^+ 59, 60, 68 Σ_K 17 $\Sigma_K^\infty, \bar{\Sigma}_K$ 42
$\text{Aut } V$ 12	
C, C_m 42, 43	
$C(\varphi)$ 97	
$c(\varphi)$ 100	
$C = \hat{\bar{K}}$ 73	
c_K 109	
C_∞, c_ω 59	
D 43	
e 44	
e_l 46	

ОГЛАВЛЕНИЕ

Предисловие	5
Из предисловия автора	7
Введение	9
Обозначения	12
 Глава I. l -адические представления	13
§ 1. Понятие l -адического представления	13
1.1. Определение	13
1.2. Примеры	15
§ 2. l -адические представления числовых полей	17
2.1. Предварительные результаты	17
2.2. Теорема плотности Чеботарёва	18
2.3. Рациональные l -адические представления	20
2.4. Представления со значениями в линейной алгебраической группе	24
2.5. L -функции, связанные с рациональными представлениями	26
Добавление. Равнораспределенность и L -функции	28
Д.1. Равнораспределенность	28
Д.2. Связь с L -функциями	31
Д.3. Доказательство теоремы 1	35
 Глава II. Группы S_m	38
§ 1. Предварительные результаты	38
1.1. Тор T	38
1.2. Факторы тора T	39
1.3. Расширения групп	39
§ 2. Построение групп T_m и S_m	42
2.1. Идели и классы идей	42
2.2. Группы T_m и S_m	44
2.3. Каноническое l -адическое представление со значениями в S_m	45
2.4. Линейные представления групп S_m	48
2.5. l -адические представления, ассоциированные с линейным представлением группы S_m	51

2.6. Другая конструкция	54
2.7. Вещественный случай	55
2.8. Пример: комплексное умножение абелевых многообразий	56
§ 3. Строение группы T_m и приложения	59
3.1. Строение группы $X(T_m)$	59
3.2. Морфизм $j^*: G_m \rightarrow T_m$	60
3.3. Строение группы T_m	62
3.4. Как вычислять элементы Фробениуса	63
Добавление. Факторизация по арифметическим группам в торах	66
Д.1. Арифметические группы в торах	66
Д.2. Факторизация по арифметическим подгруппам	67
Глава III. Локально алгебраические абелевы представления	70
§ 1. Локальный случай	70
1.1. Определения	70
1.2. Другое определение „локальной алгебраичности“ с помощью модулей Ходжа — Тейта	73
§ 2. Глобальный случай	75
2.1. Определения	75
2.2. Модуль локального алгебраического абелева представления	77
2.3. Возвращение к S_m	79
2.4. Некоторое собщение	82
2.5. Случай функционального поля	82
§ 3. Случай композита квадратичных полей	85
3.1. Формулировка основного результата	85
3.2. Критерий локальной алгебраичности	85
3.3. Один вспомогательный результат о торах	88
3.4. Доказательство теоремы	91
Добавление. Разложения Ходжа — Тейта и локально алгебраические представления	94
Д.1. Инвариантность разложений Ходжа — Тейта	94
Д.2. Допустимые характеристы	97
Д.3. Критерий локальной тривиальности	100
Д.4. Характер χ_E	102
Д.5. Характеры, ассоциированные с разложением Ходжа — Тейта	103
Д.6. Локально компактный случай	107
Д.7. Теорема Тейта	110

Глава IV. l -адические представления, связанные с эллиптическими кривыми	112
§ 1. Предварительные результаты	112
1.1. Эллиптические кривые	112
1.2. Хорошая редукция	113
1.3. Свойства модуля V_l для хорошей редукции	114
1.4. Теорема Шафаревича	116
§ 2. Модули Галуа, связанные с кривой E	118
2.1. Теорема о неприводимости	118
2.2. Вычисление алгебры Ли группы G_l	120
2.3. Теорема об изогении	123
§ 3. Вариация групп G_l и \tilde{G}_l в зависимости от l	125
3.1. Предварительные результаты	125
3.2. Случай нецелого j	127
3.3. Числовой пример	129
3.4. Доказательство основной леммы из п. 3.1	130
Добавление. Локальные результаты	135
Д.1. Случай $v(j) < 0$	136
Д.1.1. Эллиптические кривые Тейта	136
Д.1.2. Одна точная последовательность	137
Д.1.3. Вычисление алгебр g_l и i_l	139
Д.1.4. Приложение к изогениям	140
Д.1.5. Существование трансвекций в группе инерции	142
Д.2. Случай $v(j) \geq 0$	143
Д.2.1. Случай $l \neq p$	143
Д.2.2. Случай $l = p$ с хорошей редукцией высоты 2	143
Д.2.3. Вспомогательные результаты из теории алгебраических многообразий	146
Д.2.4. Случай $l = p$ с хорошей редукцией высоты 1	148
Список литературы	151
Приложение. Модулярные формы и l -адические представления П. Делинь	154
1. Введение	154
2. Изоморфизм Шимуры	156
3. Операторы Гекке и фундаментальное l -адическое представление	162
4. Формула сравнения	173
5. Из гипотез Вейля следует гипотеза Рамануджана	182
Список литературы	186
Указатель	187

Уважаемый читатель!

Ваши замечания о содержании книги, ее оформлении, качестве перевода и другие просим присыпать по адресу: 129820, Москва, И-110, ГСП, 1-й Рижский пер., д. 2, издательство «Мир».

Ж.-П. Сеpp

АБЕЛЕВЫ

И-АДИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ И ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Редактор Г. М. Цукерман

Художник Д. В. Орлов

Художественный редактор В. И. Шаповалов

Технический редактор Е. Д. Кузнецова

Корректор И. Н. Максимова

Сдано в набор 4/X 1972 г.

Подписано к печати 9/VII 1973 г.

Бумага № 1 84×108^{1/2}=3 бум. л. 10,08 печ. л.

Уч.-изд. л. 8,37. Изд. № 1/6847

Цена 84 коп. Зак. 343

ИЗДАТЕЛЬСТВО «МИР»

Москва, 1-й Рижский пер., 2

Ордена Трудового Красного Знамени

Ленинградская типография № 2

имени Евгении Соколовой Союзполиграфпрома

при Государственном комитете Совета Министров

СССР по делам издательств, полиграфии

и книжной торговли,

г. Ленинград, Л-52, Измайловский проспект, 29