ВВЕДЕНИЕ В ТЕОРИЮ ПОЛЕЙ КЛАССОВ

Содержание

Многие вопросы теории чисел естественно приводят к изучению конечных расширений поля рациональных чисел. Так, попытки решения уравнений вида $x^p + y^p = 1$ рациональных числах, приводят к рассмотрению кругового поля $\mathbb{Q}(\sqrt[p]{1})$. В терминах этого поля также удобно описывать символ Лежандра, и доказывать квадратичный закон взаимности.

Основное внимание будет уделено явным конструкциям расширений полей, в частности, комплексному умножению и явным законам взаимности, а также их приложениям.

Используемая когомологическая техника и аналогия между числовыми полями и полями функций кривых будут объяснены по ходу дела.

0. Введение: теорема Ферма в некоторых частных случаях

Чтобы увидеть (в историческом контексте), зачем расширять поля, и что нужно знать о расширениях, рассмотрим пример следующего вопроса.

Пример. Будем изучать решения уравнения $x^n + y^n = z^n$ в целых ненулевых числах для всевозможных целых $n \geqslant 3$.

Обозначим через ТФ_n утверждение, о том, что при данном n нужных нам решений нет. Если мы хотим (следуя Ферма) доказать что нужных нам решений нет ни при каких $n \geqslant 3$, то достаточно доказать ТФ_4 и ТФ_p для всех простых $p \geqslant 3$. Можно считать, что $(x, y, z) = 1$, или эквивалентно, $(x, y) = (x, z) = (y, z) = 1$.

Упражнение. Докажите ТФ_4. (*Указание.* Считайте $|xyz| > 0$ минимальным.)

Различают два случая: $p \nmid xyz$ и $p|xyz$. Скажем, что имеет место $\text{ТФ}_p\text{I}$, соотв. $\text{ТФ}_p\text{II}$, если в первом, соотв. во втором, случае решений нет.

Попробуем провести доказательство ТФ_4 в случае ТФ_p для некоторого простого $p \geqslant 3$. Поскольку $x^p + y^p = z^p$, из малой теоремы Ферма следует, что $x + y \equiv z \bmod p$, и следовательно, $(x + y)^p \equiv z^p \bmod p^2$, откуда $(x + y)^p \equiv x^p + y^p \bmod p^2$. Если $p = 3$, то $3|xy(x + y)$, т.е. $3|xyz$, а значит, имеет место $\text{ТФ}_p\text{I}$.

Пусть теперь $p > 3$. Как и в доказательстве ТФ_4, хочется, например, разложить многочлен $x^p + y^p$ на множители и сказать, что эти множители являются p-ыми степенями. Для этого добавим к целым числам элемент $\zeta = \zeta_p = e^{\frac{2\pi i}{p}}$: $\prod_{j=0}^{p-1}(x + \zeta^j y) = z^p$.

Первая неприятность, с которой мы можем встретиться (и действительно встречаемся, например, в случае $\mathbb{Z}[\sqrt{-5}]$: $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ и $3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$) состоит в неоднозначности разложения на простые множители.

Упражнение. Докажите с помощью алгоритма Евклида однозначность разложения на простые множители в кольцах $\mathbb{Z}[\sqrt{-1}]$ и $\mathbb{Z}[\sqrt[3]{1}]$.

Однако мы воспользуемся следующим фактом из коммутативной алгебры дедекиндовых колец: *в кольцах целых числовых полей имеется однозначное разложение идеалов на простые множители.* Например, $(2) = (2, 1 + \sqrt{-5})^2$, $(3) = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$, $(2, 1 + \sqrt{-5})(3, 1 \pm \sqrt{-5}) = (1 \pm \sqrt{-5})$ в $\mathbb{Z}[\sqrt{-5}]$.

Упражнение. Докажите, что $\mathbb{Z}[\sqrt[n]{1}]$ – кольцо целых поля $\mathbb{Q}(\sqrt[n]{1})$ для любого целого $n \geqslant 2$.

Известно, что разложения на простые множители в $\mathbb{Z}[\sqrt[n]{1}]$ однозначно ровно в 29 случаях: $n \in \{1, 3, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84\}$.

Тогда $(x + \zeta y) = \mathfrak{a}^p$, т.к. идеалы $(x + \zeta^j y)$ попарно взаимно просты для любых $0 \leqslant j < s < p$:

$$(x + \zeta^j y, x + \zeta^s y) = (x + \zeta^j y, (1 - \zeta^{s-j})x, (1 - \zeta^{s-j})y) = (x + \zeta^j y, 1 - \zeta^{s-j})$$
$$= \begin{cases} (x + y, 1 - \zeta^s) & \text{если } 0 = j < s < p, \\ (x + \zeta^j y, 1 - \zeta^j) = (x + y, 1 - \zeta^j) & \text{если } 0 < j < s < p, \end{cases}$$

и в любом случае это число делит $(x + y, p) = 1$.

Факт 0.1. *Группа классов идеалов кольца целых любого числового поля конечна.*

Вместо того, чтобы предполагать однозначность разложения на простые множители в кольце $\mathbb{Z}[\zeta_p]$, что бывает крайне редко, мы будем предполагать только, что p не делит число классов идеалов кольца $\mathbb{Z}[\zeta_p]$. В первой сотне только числа 37, 59 и 67 не удовлетворяют этому условию.

Тогда $\mathfrak{a}$ – главный идеал, т.е. $x + \zeta y = \varepsilon\alpha^p$, где $\varepsilon \in \mathbb{Z}[\zeta_p]^\times$ – единица в $\mathbb{Q}(\zeta_p)$, $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ и $a_j \in \mathbb{Z}$.

Лемма 0.2. *Единицы в $\mathbb{Q}(\zeta_p)$ имеют вид $\zeta_p^j\eta$, где $0 \leqslant j < p$ и $\eta \in \mathbb{R}$.*

Упражнение. Докажите, что $1 + \zeta_p \in \mathbb{Z}[\zeta_p]^\times$ – единица в $\mathbb{Q}(\zeta_p)$ для любого простого $p \geqslant 3$.

Согласно малой теореме Ферма, $\alpha^p \equiv a_0 + a_1 + \cdots + a_{p-2} \bmod p$ – вещественно по модулю p, откуда $\zeta_p^{-j}(x+\zeta_p y) \equiv \eta(a_0 + a_1 + \cdots + a_{p-2}) \bmod p$ – также вещественно по модулю p, и значит, $\zeta_p^{-j}(x + \zeta y) \equiv \zeta_p^j(x + \zeta_p^{-1}y) \bmod p$, или $(1 - \zeta_p^{2j})x \equiv \zeta_p(1 - \zeta_p^{2(j-1)})y \bmod p$. При $j = 0$ получим $y \equiv 0 \bmod p$; при $j = 1$ получим $x \equiv 0 \bmod p$; при $1 < j < p$ и $j \neq \frac{p+1}{2}$ получим $x \equiv y \equiv 0 \bmod p$; при $j = \frac{p+1}{2}$ получим $x \equiv y \bmod p$. Таким образом, $x \equiv y \bmod p$, если $xy \not\equiv 0 \bmod p$.

Поменяв ролями y и $-z$, получим аналогично $x \equiv -z \bmod p$, если $xz \not\equiv 0 \bmod p$. Откуда $2x \equiv x + y \equiv z \equiv -x \bmod p$. Таким образом, мы доказали (по модулю некоторых недоказанных утверждений) следующую теорему Куммера.

Теорема 0.3 (Куммер). *Если некоторое простое $p \geqslant 3$ не делит число классов идеалов кольца* $\mathbb{Z}[\zeta_p]$ (такие простые называются регулярными), *то имеет место ТФ$_p$I.* □

Из вышесказанного вытекает, что полезно расширять поля; рассматривать в них кольца целых $\mathcal{O}$, идеалы, смотреть, что с ними происходит при расширениях, изучать группы классов идеалов $\mathrm{Pic}\,\mathcal{O}$, единицы $\mathcal{O}^\times$, основную теоремы арифметики...

Еще один пример класса ситуаций, в которых переход к расширению поля (точнее, к абелевому расширению) проясняет суть дела: *законы взаимности*. Например, символ Лежандра квадратичного вычета по модулю p,

$$\left(\frac{a}{p}\right) = \text{уменьшенное на 1 число решений уравнения } x^2 = a \text{ в } \mathbb{F}_p,$$

удобно описывать с помощью кругового поля $\mathbb{Q}(\zeta_p)$ и его автоморфизмов $G_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} \cong (\mathbb{Z}/p\mathbb{Z})^\times$: если $G = \sum_{j\in(\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{j}{p}\right) e^{\frac{2\pi i j}{p}}$ – сумма Гаусса, а $(\sigma_q : e^{\frac{2\pi i}{p}} \mapsto e^{\frac{2\pi i q}{p}}) \in G_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}$, то $\sigma_q G = \left(\frac{q}{p}\right) G$... Подробности мы обсудим позже, а сейчас приведем приложение к теореме Ферма некоторого обобщения квадратичного закона взаимности на круговые поля. Обратим только внимание на то, что простым $q \in \mathbb{Q}$, неразветвлённым в $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, сопоставляются автоморфизмы кругового расширения $\mathbb{Q}(\zeta_p)$.

Теорема 0.4 (Фуртвэнглер). *Пусть $p, q \geqslant 3$ – некоторые простые числа. Предположим, что $x^p + y^p = z^p$ для некоторых целых x, y, z таких, что $(x, y, z) = 1$, $p \not| xyz$ и $q | xyz$. Тогда $q^{p-1} \equiv 1 \bmod p^2$.* □

Следствие 0.5 (Виферих). *Если $2^{p-1} \not\equiv 1 \bmod p^2$, то имеет место ТФ$_p$I.* □

Факт 0.6. *Если $2^{p-1} \equiv 1 \bmod p^2$ и $p < 3 \cdot 10^9$, то $p \in \{1093, 3511\}$.* □

Теорема 0.7 (Мириманов). *Если $3^{p-1} \not\equiv 1 \bmod p^2$, то имеет место ТФ$_p$I.* □

Из трех последних утверждений следует, что ТФ$_p$I имеет место для всех $p < 3 \cdot 10^9$.

Упражнение. Найдите вычет 3^{1092} по модулю 1093^2. (*Указание.* $3^7 = 2 \cdot 1093 + 1$.)

Ключевой момент в доказательстве теоремы Фуртвэнглера использует закон взаимности Эйзенштейна для символов вычета p-ой степени для кругового поля $\mathbb{Q}(\zeta_p)$.

Таким образом, законы взаимности в различных вариантах и абелевы расширения числовых полей будут в центре нашего внимания.

Если время позволит, мы изучим также аналитический аспект теории – дзета- и L-функции. В частности, следуя Куммеру, мы докажем с их помощью, что $\mathrm{T}\Phi_p\mathrm{II}$ имеет место для регулярных p.

1. Теория Галуа: поля, их расширения и автоморфизмы

1.1. **Общие сведения из теории Галуа,** [K, Jac, ПШ-Ш, Ш, I]. Пусть F – поле, и G – некоторая группа его автоморфизмов. Мы считаем G топологической группой, базу открытых подгрупп которой порождают стабилизаторы элементов F.

Пример. Допустим, что поле F конечно порождено над некоторым подполем k, неподвижным относительно G, т.е. $F = k(S)$ для какого-то конечного подмножества S в F. Тогда G дискретна, поскольку общий стабилизатор элементов множества S открыт и совпадает с общим стабилизатором всех элементов поля F, т.е. равен $\{1\}$.

Упражнение. Докажите, что группа G хаусдорфова и вполне несвязна, т.е. любая окрестность любой точки содержит замкнутую подокрестность. В частности, любая открытая подгруппа замкнута.

Напомним, что по определению,

- расширение полей K/k конечно, если K конечномерно как k-векторное пространство,
- расширение полей K/k алгебраично, если каждый элемент K является корнем некоторого ненулевого многочлена над k,
- алгебраическое расширение K/k сепарабельно, если $\Omega_{k(x)/k} = 0$ для любого $x \in K$,
- алгебраическое расширение K/k нормально, если любой неприводимый многочлен над k становится произведением неприводимых многочленов над K равных степеней,
- K/k – расширение Галуа, если оно нормально и сепарабельно.

Для произвольного гомоморфизма коммутативных колец $B \longrightarrow A$ кэлеровы дифференциалы определяются как формальные суммы $\sum_j f_j dg_j$, где $f_j, g_j \in A$, с соотношениями $(f+g)dh = fdh + gdh$, $hd(f+g) = hdf + hdg$, $hd(fg) = hfdg + hgdf$ (правило Лейбница) и $dc = 0$, если c лежит в образе B. Обозначим через $\Omega_{A/B}$ A-модуль кэлеровых дифференциалов.

Упражнения. 1. Докажите, что конечное расширение полей алгебраично, и порождается корнем некоторого многочлена.

2. Рассмотрим алгебру $A \otimes_B A$ и гомоморфизм умножения $m : A \otimes_B A \xrightarrow{\times} A$. Пусть идеал $\mathfrak{m}$ кольца $A \otimes_B A$ – ядро m. Постройте канонический изоморфизм $\Omega_{A/B} = \mathfrak{m}/\mathfrak{m}^2$.

3. Поле называется совершенным, или если оно характеристики $p > 0$ и каждый его элемент – p-ая степень, или если оно нулевой характеристики. Например, конечные поля совершенны.

а) Докажите, что поле совершенно тогда и только тогда, когда его любое алгебраическое расширение сепарабельно. В частности, алгебраическое расширение совершенного поля совершенно.

б) Докажите, что поле K положительной характеристики совершенно тогда и только тогда, когда $\Omega_{K/\mathbb{Z}} = 0$.

4. Докажите, что любое алгебраическое расширение поля F^H в поле F сепарабельно.

5. Докажите, что конечное расширение полей K/k сепарабельно тогда и только тогда, когда алгебра $K \otimes_k K$ изоморфна прямой сумме полей. Что это за поля, если K/k – расширение Галуа?

Лемма 1.1. *Для автоморфизма σ поля F следующие условия эквивалентны.*

(1) *Существует целое $m \geqslant 1$ такое, что F алгебраично над подполем σ^m-инвариантов.*

(2) *Поле F – расширение Галуа подполя σ-инвариантов.*

(3) *Для любого элемента $y \in F$ существует целое $N \geqslant 1$ такое, что $\sigma^N y = y$.*

Доказательство. Стрелка (2)⇒(1) тривиальна. Для (1)⇒(3) можно взять в качестве N подходящее кратное m.

(3)⇒(2). Рассмотрим произвольный элемент $t \in F$. Пусть $N \geqslant 1$ – минимальное целое такое, что $\sigma^N t = t$. Стандартные симметрические многочлены от $t, \sigma t, \dots, \sigma^{N-1}t$, т.е. коэффициенты многочлена $\prod_{j=1}^{N}(T - \sigma^j t)$, σ-инвариантны, и t алгебраичен (более того, сепарабелен) над порожденным ими полем, а значит, и над полем σ-инвариантов. □

Упражнение. Докажите, что если для автоморфизма σ поля F выполнены эквивалентные условия леммы 1.1, то σ содержится в некоторой компактной группе автоморфизмов поля F.

Для подполя $k \subseteq F$ обозначим через $G_{F/k}$ группу автоморфизмов расширения F/k.

Упражнения. а) Докажите, что для любого флага подполей $k \subseteq K \subseteq F$ топология на $G_{F/K}$ совпадает с ограничением топологии на $G_{F/k}$, а гомоморфизм $G_{\{F,K\}/k} \longrightarrow G_{K/k}$ непрерывен, где $G_{\{F,K\}/k}$ – группа автоморфизмов поля F, сохраняющих K и тождественных на k. Сюръективем ли он?

б) Группа G_{F/F^H} локально компактна тогда и только тогда, когда степень трансцендентности расширения F/F^H конечна. (Вполне несвязная группа локально компактна тогда и только тогда, когда у нее есть хотя бы одна открытая компактная подгруппа.)

в) Для любой компактной G расширение F/F^G – расширение Галуа, и $G_{F/F^G} = G$.

г) Для любого расширение Галуа F/K группа $G_{F/K}$ компактна, и $F^{G_{F/K}} = K$. (Указание. Докажите, что любое проконечное множество компактно, а затем воспользуйтесь методом «деления отрезка пополам», которым доказывается компактность отрезка $[0, 1]$.)

д) Назовем подполе F относительно совершенным, если любое его алгебраическое расширение в F сепарабельно, и его совершенным замыканием – его минимальное относительно совершенное алгебраическое расширение в F.

Докажите существование и единственность совершенного замыкания.

Пусть k – неподвижное подполе в F некоторой группы автоморфизмов.

е) Докажите, что отображение $K \mapsto G_{F/K}$ обращает включения, преобразует композит полей в пересечение подгрупп и отождествляет подполя, над которыми F – расширение Галуа, с компактными подгруппами $G_{F/k}$: [1]

$$\left\{ \begin{array}{c} \text{подполя } K \subset F \text{ над } k \text{ такие,} \\ \text{что } F/K \text{ – расширение Галуа} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{компактные} \\ \text{подгруппы в } G_{F/k} \end{array} \right\};$$

$$\left\{ \begin{array}{c} \text{совершенные замыкания } K \text{ в } F \text{ подполей конечного} \\ \text{типа над } k \text{ такие, что } F/K \text{ – расширение Галуа} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{компактные открытые} \\ \text{подгруппы в } G_{F/k} \end{array} \right\}.^2$$

Обратные отображения задаются правилом $H \mapsto F^H$ (неподвижное подполе в F группы H).

ё) Докажите существование и единственность[3] с точностью до изоморфизма алгебраического и сепарабельного замыкания, т.е. таких алгебраических расширений данного поля, которые алгебраически, соотв. сепарабельно, замкнуты. Докажите, что сепарабельное замыкание нормально,

[1] [ПШ-Ш], §3, лемма 1, или [Ш], предложение 6.11

[2] непосредственно следует из loc.cit., см. также [Ш] предложение 6.12

[3] Несмотря на «единственность», сепарабельное замыкание не канонично, и его выбор следует сравнивать с выбором отмеченной точки в определении фундаментальной группы связного топологического пространства, которая также «не зависит» от отмеченной точки. Аналогия с фундаментальной группой станет еще более уместной, когда мы будем рассматривать неразветвленные расширения. При этом абелев фактор группы Галуа, т.е. группу Галуа максимального абелева расширения, следует расматривать как первые гомологии.

и что группа Галуа сепарабельное замыкания $G_{k_{\mathrm{sep}}/k}$ совпадает с группой автоморфизмов алгебраического замыкания $G_{\overline{k}/k}$.

Полулинейным представлением группы автоморфизмов G поля F называется F-векторное пространство V, снабженное аддитивным полулинейным действием G: $g(u+v) = gu+gv$, $h(f\cdot v) = gf\cdot gv$ для любых $f\in F$, $g\in G$, $u,v\in V$.

Теорема 1.2 (Теорема 90 Гильберта). *Любое полулинейное представление любой конечной группы автоморфизмов G поля F тривиально, т.е. изоморфно прямой сумме копий F.*

Доказательство. Пусть $b=\sum_{g\in G} g : V \longrightarrow V$. Проверим, что образ b порождает V как F-векторное пространство. Пусть $u : V \longrightarrow F$ – F-линейный функционал, зануляющийся на F-линейной оболочке образа b. Тогда $0 = u(b(fv)) = \sum_{g\in G} u(g(fv)) = \sum_{g\in G} u(gf\cdot gv) = \sum_{g\in G} gf\cdot u(gv)$ для любого $f\in F$. Для каждого $v\in V$ получаем F-линейное соотношение между характерами $g : F^{\times} \longrightarrow F^{\times}$. По теореме о независимости характеров, $u(gv)=0$ для всех g,v, т.е. $u=0$. Заметим, что образ b лежит в V^G, т.е. F-базис V можно выбрать в V^G, что означает тривиальность V. □

Упражнение. (например, Ленг, Алгебра) Докажите теорему о линейной независимости характеров.

Пример. Пусть G – некоторая группа автоморфизмов поля F и $\Omega_F := \Omega_{F/\mathbb{Z}}$ (кэлеровы дифференциалы) – полулинейное представление G. Если замыкание G компактно, то F/F^G – расширение Галуа, и $\Omega_F = F\otimes_{F^G}\Omega_{F^G}$ тривиально. Обратное, вообще говоря, неверно. Например, если F совершенно и положительной характеристики, то $\Omega_F = 0$, но G может быть произвольной. Однако, если F – характеристики нуль, то из тривиальности Ω_F как полулинейного представления G следует алгебраичность расширения F/F^G, а также его нормальность.

Определим норму, соотв. след, элемента x конечного расширения K/k как определитель, соотв. след, оператора умножения на x на k-векторном пространстве K. Если $x^m + a_{m-1}x^{m-1} + \dots a_0 = 0$ – минимальный многочлен x над k со старшим коэффициентом 1, то $N_{K/k}(x) = ((-1)^m a_0)^{[K:k(x)]}$ и $\mathrm{tr}_{K/k}(x) = -[K:k(x)]a_{m-1}$. Ясно, что норма и след индуцируют гомоморфизмы $N_{K/k} : K^{\times} \longrightarrow k^{\times}$ и $\mathrm{tr}_{K/k} : K \longrightarrow k$.

Следствие 1.3 (Ещё одна «Теорема 90» Гильберта). *Пусть g – некоторый автоморфизм поля F конечного порядка и $E=F^g$. Тогда для любого элемента $a\in F^{\times}$ с $N_{F/E}(a)=1$ существует $b\in F^{\times}$ такой, что $b/gb=a$.*

Доказательство. Определим одномерное полулинейное представление V группы G, порождённой g, так: $gv = av$ для некоторого вектора $v\neq 0$. Поскольку V тривиально, $g(bv)=bv$ для некоторого $b\in F^{\times}$, т.е. $b/gb=a$. □

Пусть G – вполне несвязная топологическая группа. G-модуль называется гладким (или алгебраическим), если стабилизаторы всех его элементов открыты.

Примеры. а) F и Ω_F гладкие для любого поля F и любой группы G его автоморфизмов.

б) Если G вложена в группу единиц $A^{\times}$ кольца A, и действует на A левым умножением, то A – гладкий G-модуль тогда и только тогда, когда G дискретна. В частности, это относится к групповому кольцу $\mathbb{Z}[G]$.

в) Векторы данного G-модуля, стабилизаторы которых открыты, образуют G-подмодуль (называемой гладкой частью).

Упражнения. 1. Докажите, что гладкие G-модули образуют абелеву категорию.

2. Докажите, что любое гладкое полулинейное представление любой компактной группы автоморфизмов поля F тривиально (тем самым, обобщив теорему 90 Гильберта).

1.2. **Конечные поля.** Упражнение. а) Докажите, что любое конечное расширение конечного поля $\mathbb{F}_q$ из q элементов – циклическое, и автоморфизм Фробениуса, $x \mapsto x^q$, порождает группу его автоморфизмов.

б) Докажите, что группа автоморфизмов алгебраического замыкания поля $\mathbb{F}_q$ канонически изоморфна $\widehat{\mathbb{Z}} := \varprojlim_N \mathbb{Z}/N\mathbb{Z} = \prod_p \mathbb{Z}_p$, где обратная система образована по отношению к редукциям $\mathbb{Z}/MN\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}$, и что автоморфизм Фробениуса порождает плотную подгруппу.

1.3. **Абелевы расширения полей «со многими корнями из единицы»: теория Куммера.** Пусть H – некоторая группа автоморфизмов поля F. Классы изоморфизма одномерных гладких полулинейных представлений группы H образуют группу $\mathfrak{L}$ относительно тензорного умножения над F. Допустим, что целое $n \geqslant 1$ не делится на характеристику поля K, и что K содержит все корни n-ной степени из единицы. Пусть $F = K_{\mathrm{sep}}$ – сепарабельное замыкание поля K и $H = G_{K_{\mathrm{sep}}/K}$. Рассмотрим следующую последовательность

$$1 \longrightarrow K^\times/K^{\times n} \longrightarrow \mathrm{Hom}_{Sm}(G_{K_{\mathrm{sep}}/K}, \mu_n) \longrightarrow \mathfrak{L}, \tag{1}$$

где $K^\times/K^{\times n} \ni [f] \mapsto (\sigma \mapsto \frac{\sigma \sqrt[n]{f}}{\sqrt[n]{f}}) \in \mathrm{Hom}_{Sm}(G_{K_{\mathrm{sep}}/K}, \mu_n)$, Hom_{Sm} обозначает группу гомоморфизмов с открытыми ядрами, и $\varphi \in \mathrm{Hom}_{Sm}(G_{K_{\mathrm{sep}}/K}, \mu_n)$ переходит в одномерное пространство, на котором $G_{K_{\mathrm{sep}}/K}$ действует по формуле $\sigma : x \cdot e \mapsto \varphi(\sigma) \cdot \sigma x \cdot e$ для любых $\sigma \in G_{K_{\mathrm{sep}}/K}$ и $x \in K_{\mathrm{sep}}$, где $e \neq 0$ – некоторый фиксированный вектор.

Упражнение. Проверьте точность этой последовательности.

Согласно теореме 90, $\mathfrak{L} = \{1\}$, а значит, $K^\times/K^{\times n} \xrightarrow{\sim} \mathrm{Hom}_{Sm}(G_{K_{\mathrm{sep}}/K}, \mu_n)$ – изоморфизм.

Упражнение. (Теория Куммера) Докажите, что если K содержит n корней n-ной степени из единицы, то любое циклическое расширение K порядка n получается присоединением корня некоторого неприводимого многочлена вида $x^n - a$ для некоторого $a \in K^\times$. Два таких расширения, соответствующих $a, b \in K^\times$, совпадают тогда и только тогда, когда a и b порождают одну и ту же подгруппу в $K^\times/K^{\times n}$.

Отсюда видна особая роль круговых расширений, и тот факт, что абелевы расширения можно получать как подрасширения расширений Куммера круговых расширений:

$$\begin{array}{ccc} K(\zeta_n) & \xrightarrow{\mathrm{ab}} & L(\zeta_n) \\ \mathrm{ab}\uparrow & & \uparrow \mathrm{ab} \\ K & \xrightarrow{\mathrm{ab}} & L \end{array}$$

Упражнение. Проверьте всё это.

Этот трюк будет использован в доказательствах а) теоремы Чеботарёва о плотности, б) закона взаимности Артина.

Теорема 1.4 (Артин–Шрайер). (1) *Если у поля F нет нетривиальных абелевых расширений (например, если F сепарабельно замкнуто) и порядок любого элемента H конечен, то H содержит не более двух элементов.*

(2) *Если, в предположениях п.1, H содержит два элемента, то неподвижное поле F^H вполне упорядочено. Если же $F^H \ni \sqrt{-1}$, то $H = \{1\}$.*

Доказательство. Мы оставим случай кручения порядка, равного характеристике, в качестве упражнения на теорию Артина–Шрайера, см. ниже, а разберем только остальные случаи.

Предположим, что $\sigma^p = 1$ и $\sigma \neq 1$ для некоторого простого $p \geqslant 3$, отличного от характеристики. Пусть $\sigma\zeta = \zeta^a$ для некоторого примитивного p-го корня из единицы ζ и $a \in \mathbb{F}_p^\times$. Тогда $\sigma^p\zeta = \zeta^{a^p} = \zeta^a$, так что $a = 1$. Далее, из теории Куммера, $F = F^{\langle\sigma\rangle}(x)$ для некоторого $x \in F$ такого, что $x^p \in F^{\langle\sigma\rangle}$, так что $\sigma x = \zeta \cdot x$ для некоторого $\zeta \neq 1$, $\zeta^p = 1$.

Зафиксируем $y \in F$ такой, что $y^p = x$, так что $\sigma y = \xi \cdot y$. Пусть $\sigma\xi = \xi^b$. Тогда $\sigma^p y = \sigma^{p-1}\xi \cdots \xi \cdot y = \xi^{1+b+\cdots+b^{p-1}} \cdot y$. Поскольку $b \equiv 1 + pt \bmod p^2$ для некоторого $t \in \mathbb{F}_p$, получаем $1 + b + \cdots + b^{p-1} \equiv p \bmod p^2$, так что $\sigma^p y = \zeta \cdot y \neq y$.

Предположим, что характеристика отлична от 2, $F^{\langle\sigma\rangle} \ni \sqrt{-1}$ и $\sigma^2 = 1$. Тогда $F = F^{\langle\sigma\rangle}(x^2)$ для некоторого $x \in F$ такого, что $x^4 \in F^{\langle\sigma\rangle}$, так что $\sigma x = \sqrt{-1} \cdot x$, и следовательно, $\sigma^2 x = -x \neq x$.

Предположим теперь, что $\sigma, \tau \in H - \{1\}$. Тогда $\sigma\sqrt{-1} = \tau\sqrt{-1} = -\sqrt{-1}$, и значит, $\sqrt{-1} \in F^{\langle\sigma\tau^{-1}\rangle}$, так что $\sigma = \tau$. $\square$

1.4. **Начальные сведения о (ко-)гомологиях (вполне несвязных) групп,** [АТЧ, С-КГ], **и ещё раз о теории Куммера.** Когомологии дискретной группы G определяются как правые производные функтора G-инвариантов $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, т.е. $H^*(G, M) := \mathrm{Ext}^*_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Гомологии дискретной группы G можно определить как левые производные функтора G-коинвариантов $- \otimes_{\mathbb{Z}[G]} \mathbb{Z}$, т.е. $H_*(G, M) := \mathrm{Tor}_*^{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Как известно, см., например, Гельфанд–Манин, для любого кольца A и любых A-модулей B, C группы $\mathrm{Ext}^*_A(B, C)$ можно рассматривать как правые производные функторы левоточного функтора $\mathrm{Hom}_A(-, C)$ на категории, противоположной категории A-модулей. С другой стороны, правые производные функторы на любой абелевой категории можно вычислять с помощью инъективных резольвент, которые в случае категории, противоположной категории A-модулей, становятся просто проективными резольвентами.

Стандартной резольвентой тривиального G-модуля $\mathbb{Z}$ называется комплекс $\ldots \longrightarrow \mathbb{Z}[G^3] \longrightarrow \mathbb{Z}[G^2] \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$ ($\varepsilon : [g] \mapsto 1$ называется аугментацией) G-модулей с диагональным действием G: $g[(g_0, \ldots, g_q)] \mapsto [(gg_0, \ldots, gg_q)]$ и дифференциалами $\partial : [(g_0, \ldots, g_q)] \mapsto \sum_{j=0}^q (-1)^j[(g_0, \ldots, \widehat{g}_j, \ldots$ Ясно, что G-модули $\mathbb{Z}[G^q]$ свободны.

Упражнение. Проверьте, что любой элемент $g \in G$ задаёт гомотопию $h : [(g_0, \ldots, g_q)] \mapsto [(g, g_0, \ldots, g_q)]$, т.е. такое отображение степени -1, что $\partial h + h\partial = id$ – тождественное отображение. Выведите из этого точность стандартной резольвенты.

Таким образом, $H^*(G, M) = H^*(\mathrm{Hom}_G(\mathbb{Z}[G^\bullet], M))$ и $H_*(G, M) = H_*(\mathbb{Z}[G^\bullet] \otimes_G M)$.

Пример. Пусть G – циклическая группа порядка n, порожденная элементом s. Тогда $\mathbb{Z}[G] = \mathbb{Z}[s]/(s^n - 1) =: \Lambda$. Пусть $T = s - 1$ и $N = \sum_{g\in G} g$. Тогда $\cdots \xrightarrow{T} \Lambda \xrightarrow{N} \Lambda \xrightarrow{T} \Lambda \xrightarrow{\varepsilon} \mathbb{Z}$ – проективная резольвента $\mathbb{Z}$, откуда видно, что гомологии и когомологии G 2-периодичны: $H^q(G, M) = H^{q+2}(G, M)$ и $H_q(G, M) = H_{q+2}(G, M)$ при $q \geqslant 1$. Например, $H^0(G, \mathbb{Z}) = H_0(G, \mathbb{Z}) = \mathbb{Z}$, $H^q(G, \mathbb{Z}) = H_{q+1}(G, \mathbb{Z}) = 0$ при нечетном $q \geqslant 1$ и $H^q(G, \mathbb{Z}) = H_{q-1}(G, \mathbb{Z}) = G$ при четном $q \geqslant 2$. К этому примеру мы еще вернемся в связи с когомологиями Тэйта.

Пусть $H \subseteq G$ – подгруппа, и M – H-модуль. Определим G-модуль, индуцированный H-модулем M, как $\mathrm{Ind}_H^G M = \mathrm{Hom}_H(\mathbb{Z}[G], M)$. Элементы $\mathrm{Ind}_H^G M$ можно считать функциями на G со значениями в M, коммутирующие с действием H. Тогда действие G задаётся правилом $(gf)(x) = f(xg^{-1})$.

Предложение 1.5 (Лемма Шапиро). *$H^*(G, \mathrm{Ind}_H^G M) = H^*(H, M)$ и $H_*(G, \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M) = H_*(H, M)$.* $\square$

Любой гомоморфизм $f : H \longrightarrow G$ индуцирует морфизм стандартных комплексов, а значит, и гомоморфизмы $f^* : H^q(G, M) \longrightarrow H^q(H, M)$ (ограничение) и $f_* : H_q(H, M) \longrightarrow H_q(G, M)$ (коограничение). Если H – нормальная подгруппа в G и $f : G \longrightarrow G/H$, то композиция $\mathrm{Inf} : H^q(G/H, M^H) \longrightarrow H^q(G, M^H) \longrightarrow H^q(G, M)$ называется инфляцией.

Гладкие когомологии гладких G-модулей можно также определить как правые производные функторы левоточного функтора G-инвариантов на категории гладких H-модулей, или как когомологии гладкой части стандартного комплекса.

Нам же понадобятся, в основном, только компактные группы, а для них можно определить когомологии следующим образом.

Упражнение. Докажите, что вполне несвязная группа G компактна тогда и только тогда, когда она проконечна. В этом случае она имеет базу подгрупп, состоящую из открытых *нормальных* подгрупп G_α.

Для топологической группы G, допускающей базу подгрупп, состоящую из открытых нормальных подгрупп G_α, положим $H^*_{Sm}(G, M) := \varinjlim_{\alpha} H^*(G/G_\alpha, M^{G_\alpha})$, где индуктивная система образована по отношению к $H^*(G/G_\alpha, M^{G_\alpha}) \xrightarrow{\mathrm{Res}} H^*(G/G_\beta, M^{G_\alpha}) \longrightarrow H^*(G/G_\beta, M^{G_\beta})$, если $\alpha \leqslant \beta$, т.е. $G_\alpha \supseteq G_\beta$.

Упражнения. а) Докажите, что $H_1(G, \mathbb{Z}) = G/[G, G] =: G^{\mathrm{ab}}$.

б) $H^1(G, M) = \{f : G \longrightarrow M \mid f(gh) = gf(h) + f(g)\}/\{f : g \mapsto gm - m \mid m \in M\}$. Это – множество классов изоморфизма G-торсоров над M, т.е. таких G-множеств V, на которых задано свободное транзитивное действие M: $M \times V \longrightarrow V$, согласованное с действием G. Определите сложение торсоров.

Пример. Пусть G – некоторая группа автоморфизмов поля F, M – группа корней из единицы степени n в F, и $\mathfrak{log}_n(x)$ – множество корней степени n из некоторого элемента $x \in (F^\times)^G$.

Чему в этом случае соответствует сложение торсоров?

в) В обозначениях п. б), пусть M неабелева. Описать $H^1(G, M)$ и, в случае если G-группа M – гладкая, $H^1_{Sm}(G, M)$.

г) Докажите, что если G – некоторая группа автоморфизмов поля F, то $H^1(G, \mathrm{GL}_n F)$, соотв. $H^1_{Sm}(G, \mathrm{GL}_n F)$, параметризует n-мерные полулинейные, соотв. гладкие, представления G.

В частности теорема 90 Гильберта утверждает, что $H^1_{Sm}(G, \mathrm{GL}_n F) = \{*\}$, если G компактна. Если, кроме того, $n = 1$, то утверждение становится $H^1_{Sm}(G, F^\times) = \{1\}$.

д) Докажите, что $H^1_{Sm}(G, \mathrm{SL}_n F) = \{*\}$ для любой компактной группы G автоморфизмов поля F. (Указание: воспользуйтесь короткой точной последовательностью $1 \longrightarrow \mathrm{SL}_n F \longrightarrow \mathrm{GL}_n F \xrightarrow{\det} F^\times \longrightarrow 1$.)

Пример применения когомологий. Точная последовательность (1) появилась бы в теории Куммера более естественно, если бы мы начинали с точной последовательности $G_{K_{\mathrm{sep}}/K}$-модулей[4] $1 \longrightarrow \mu_n \longrightarrow K^\times_{\mathrm{sep}} \xrightarrow{\cdot n} K^\times_{\mathrm{sep}} \longrightarrow 1$, если $n \geqslant 1$ не делится на характеристику поля K. С ней ассоциирована длинная точная последовательность гладких когомологий группы $G_{K_{\mathrm{sep}}/K}$: $1 \longrightarrow \mu_n \cap K^\times \longrightarrow K^\times \xrightarrow{\cdot n} K^\times \longrightarrow H^1_{Sm}(G_{K_{\mathrm{sep}}/K}, \mu_n) \longrightarrow H^1_{Sm}(G_{K_{\mathrm{sep}}/K}, K^\times_{\mathrm{sep}}) = \mathfrak{L}$. Если K содержит все корни n-ной степени из единицы, то μ_n – тривиальный $G_{K_{\mathrm{sep}}/K}$-модуль, а значит, $H^1_{Sm}(G_{K_{\mathrm{sep}}/K}, \mu_n) = \mathrm{Hom}_{Sm}(G_{K_{\mathrm{sep}}/K}, \mu_n)$.

[4]называемой последовательностью Куммера. Это – аналог экспоненциальной последовательности $0 \longrightarrow \mathbb{Z}(1) \longrightarrow \mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times \longrightarrow 1$, поскольку exp – универсальное накрытие, а $\mathbb{C}^\times \xrightarrow{\cdot n} \mathbb{C}^\times$ – конечное.

Предложение 1.6. *Пусть $q \geqslant 1$, и H – нормальная подгруппа в G. Если $H^i(H, M) = 0$ при $1 \leqslant i < q$, то точна последовательность $0 \longrightarrow H^q(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^q(G, M) \xrightarrow{\mathrm{Res}} H^q(H, M)$.*

Идея доказательства. Случай $q = 1$ проверяется непосредственно. При $q > 1$ применяется «сдвиг размерности». А именно, определим G-модуль A как коядро вложения $M \hookrightarrow \mathrm{Ind}_{\{1\}}^G M$, заданного формулой $m \mapsto (g \mapsto gm)$, т.е. с помощью точной последовательности $0 \longrightarrow M \longrightarrow \mathrm{Ind}_{\{1\}}^G M \longrightarrow A \longrightarrow 0$. Тогда $H^i(G, \mathrm{Ind}_{\{1\}}^G M) = H^i(H, \mathrm{Ind}_{\{1\}}^G M) = 0$ для любого $i \geqslant 1$. Из наших предположений следует, что $H^i(H, A) = H^{i+1}(H, M) = 0$ для любого $1 \leqslant i \leqslant q - 2$. Поскольку $H^1(H, A) = 0$, точна последовательность $0 \longrightarrow M^H \longrightarrow (\mathrm{Ind}_{\{1\}}^G M)^H \longrightarrow A^H \longrightarrow 0$. Заметим, что G/H-модуль $(\mathrm{Ind}_{\{1\}}^G M)^H = \mathrm{Hom}(\mathbb{Z}[G/H], M)$ индуцирован, а значит, ацикличен.

По предположению индукции, точна верхняя строка с коммутативной диаграмме

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{q-1}(G/H, A^H) & \xrightarrow{\mathrm{Inf}} & H^{q-1}(G, A) & \xrightarrow{\mathrm{Res}} & H^{q-1}(H, A) \\
 & & \delta \downarrow & & \downarrow \delta & & \downarrow \delta \\
0 & \longrightarrow & H^q(G/H, M^H) & \xrightarrow{\mathrm{Inf}} & H^q(G, M) & \xrightarrow{\mathrm{Res}} & H^q(H, M),
\end{array}$$

где все δ – изоморфизмы. □

1.5. **Теория Артина–Шрайера.**

Теорема 1.7 (теорема о нормальном базисе, Ван дер Варден, Ленг...). *Пусть H – конечная группа автоморфизмов поля F. Тогда существует элемент x поля F, H-орбита которого является базисом F как векторного пространства над полем инвариантов F^H. Элемент x определяет изоморфизм $F^H[H]$-модулей $F^H[H] \longrightarrow F$, $\sum_{h \in H} a_h[h] \mapsto \sum_{h \in H} a_h[h]hx$.*

Теорема 1.8. *Пусть H – конечная группа автоморфизмов поля F. Тогда $\widehat{H}^*(H, F) = 0$.*[5]

Доказательство. По теореме о нормальном базисе, F – индуцированный модуль, а потому его когомологии тривиальны. □

Если p – характеристика поля K, то длинная точная последовательность гладких когомологий группы $G_{K_{\mathrm{sep}}/K}$, ассоциированная с $0 \longrightarrow \mathbb{F}_p \longrightarrow K_{\mathrm{sep}} \xrightarrow{\wp} K_{\mathrm{sep}} \longrightarrow 0$, где $\wp(x) = x^p - x$, даёт (с учётом теоремы 1.8) изоморфизм $K/\wp(K) \xrightarrow{\sim} \mathrm{Hom}_{Sm}(G_{K_{\mathrm{sep}}/K}, \mathbb{F}_p)$.

Упражнение. (Теория Артина–Шрайера) Докажите, что любое циклическое расширение степени p поля K характеристики $p > 0$ получается присоединением корня некоторого неприводимого многочлена вида $x^p - x - a$ для некоторого $a \in K^\times$. Два таких расширения, соответствующих $a, b \in K$, совпадают тогда и только тогда, когда a и b порождают одну и ту же подгруппу в $K/\wp(K)$.

1.6. **Двойственность Понтрягина.** Пусть H – локально компактная абелева группа. Назовём её двойственной группой группу непрерывных характеров $H^\vee := \mathrm{Hom}_{\mathrm{cont}}(H, S^1)$. Зададим базу окрестностей единичного элемента $H^\vee$ системой $U_{\varepsilon,K} = \{\chi \in H^\vee \mid |\chi(g) - 1| < \varepsilon \quad \text{для любого} \quad g \in K\}$, где $\varepsilon > 0$ и K – компактные подмножества в H.

Упражнение. Проверьте, что $H^\vee$ локально компактна.

Теорема 1.9. *а) Имеется биекция между замкнутыми подгруппами H и факторгруппами $H^\vee$, сопоставляющая подгруппе Z факторгруппу $H^\vee/\{\chi \in H^\vee \mid \chi(Z) = \{1\}\} = Z^\vee$.*

б) Гомоморфизм $H \longrightarrow (H^\vee)^\vee$, заданный формулой $h \mapsto (\chi \mapsto \chi(h))$ для любого $\chi \in H^\vee$, – топологический изоморфизм.

---

[5] Это – модифицированные когомологии, или когомологии Тэйта, см. ниже.

Упражнение. а) Найдите двойственные группы для $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\bigcup\limits_{N\geqslant 1}\frac{1}{p^N}\mathbb{Z}=\mathbb{Q}_p/\mathbb{Z}_p$...

б) Докажите, что группа, двойственная к компактной, дискретна.

в) Докажите, что группа, двойственная к проконечной, – группа кручения.

Упражнение. Докажите, что если поле нулевой характеристики F содержит все корни из единицы, то $G_{F_{\mathrm{ab}}/F}\xrightarrow{\sim}\mathrm{Hom}(F^\times,\widehat{\mathbb{Z}}(1))$, где $\widehat{\mathbb{Z}}(1):=\varprojlim_n \mu_n$, и подгруппы

$$H_{a,N}=\{\varphi\in\mathrm{Hom}(F^\times,\widehat{\mathbb{Z}}(1))\mid\varphi(a)\in N\widehat{\mathbb{Z}}(1)\}$$

для всех $N\in\mathbb{N}$ и $a\in F^\times$ порождают базу открытых подгрупп образа.

2. Нормирования и локальные поля

Глобальное поле – это или числовое поле k конечной степени над полем рациональных чисел $\mathbb{Q}$, или функциональное поле от одной переменной над конечным полем констант.

Нормированием называется мультипликативная положительная функция $\varphi:k^\times\longrightarrow\mathbb{R}_+^\times$, удовлетворяющая неравенству треугольника $\varphi(x+y)\leqslant\varphi(x)+\varphi(y)$. В частности, $\varphi(1)=1$. Каждое нормирование определяет некоторую топологию на поле k с базой открытых окрестностей нуля $U_\varepsilon=\{x\in k\mid\varphi(x)<\varepsilon\}$ для всех $\varepsilon>0$. Например, функция $\varphi=1$ задаёт дискретную топологию на k, но далее мы её рассматривать не будем.

Теорема 2.1 (Островский). *Любое нетривиальное нормирование поля $\mathbb{Q}$ имеет вид $|x|_p^\alpha$ для некоторого простого $2\leqslant p\leqslant\infty$ и некоторого положительного $\alpha\in\mathbb{R}$ ($\alpha\leqslant 1$, если $p=\infty$).*

Доказательство. Разберём два случая: 1) существует натуральное n, для которого $\varphi(n)>1$, и 2) $\varphi(n)\leqslant 1$ для всех натуральных n.

В первом случае пусть n_0 – минимально среди таких n, и $\varphi(n_0)=n_0^\alpha$ для некоторого положительного α. Любое натуральное n представляется в виде $n=a_0+a_1n_0+\dots+a_sn_0^s$, где $0\leqslant a_j<n_0$. Тогда $\varphi(n)\leqslant\varphi(a_0)+\varphi(a_1n_0)+\dots+\varphi(a_sn_0^s)\leqslant 1+\varphi(n_0)+\dots+\varphi(n_0^s)=1+n_0^\alpha+\dots+n_0^{s\alpha}=n_0^{s\alpha}(1+n_0^{-\alpha}+\dots+n_0^{-s\alpha})\leqslant Cn^\alpha$, где $C=\frac{1}{1-n_0^{-\alpha}}$. Поскольку $\varphi(n^N)\leqslant Cn^{N\alpha}$, получаем, извлекая корень N-ой степени из обеих частей и переходя к пределу по N, что $\varphi(n)\leqslant n^\alpha$. В обратную сторону, $\varphi(n)\geqslant\varphi(n_0^{s+1})-\varphi(n_0^{s+1}-n)\geqslant n_0^{(s+1)\alpha}-(n_0^{s+1}-n)^\alpha=n_0^{(s+1)\alpha}(1-(1-nn_0^{-s-1})^\alpha)\geqslant C'n^\alpha$. Поскольку $\varphi(n^N)\geqslant C'n^{N\alpha}$, получаем, извлекая корень N-ой степени из обеих частей и переходя к пределу по N, что $\varphi(n)\geqslant n^\alpha$, и значит, $\varphi(n)=n^\alpha$.

Во втором случае пусть p – минимальное среди таких n, что $\varphi(p)<1$. Оно, очевидно, – простое. Если m не делится на p, то для любого натурального N найдутся такие целые x,y, что $m^Nx+p^Ny=1$, а значит, $1=\varphi(m^Nx+p^Ny)\leqslant\varphi(m^Nx)+\varphi(p^Ny)\leqslant\varphi(m)^N+\varphi(p)^N$. Ясно, что при большом N такое может быть только если $\varphi(m)=1$. $\square$

Точкой называется класс эквивалентности нормирований, определяющих одну и ту же топологию. Точка называется неархимедовой, если выполняется неархимедово неравенство треугольника: $\varphi(x+y)\leqslant\max(\varphi(x),\varphi(y))$, и архимедовой – в противном случае.

Будем обозначать точки маленькими готическими буквами $\mathfrak{p}$, а через $k_\mathfrak{p}$ будем обозначать пополнение поля k в точке $\mathfrak{p}$.

С каждой неархимедовой точкой связывается (локальное) кольцо дискретного нормирования, состоящее из элементов, целых в этой точке: $\mathcal{O}_\mathfrak{p}:=\{x\in k\mid\varphi(x)\leqslant 1\}$, и максимальный идеал элементов, целых, но не обратимых в этой точке: $\mathfrak{p}:=\{x\in k\mid\varphi(x)<1\}$. В каждом классе эквивалентности абсолютных значений на таких полях имеется каноническое абсолютное значение $|\ |_\mathfrak{p}$. А именно, для неархимедовой точки и каждого ненулевого $a\in\mathcal{O}_\mathfrak{p}$ можно положить $|a|_\mathfrak{p}=$

$|\mathcal{O}_{\mathfrak{p}}/(a)|$. Среди архимедовых нормирований существуют максимальные, которые определяются вложением в поле комплексных чисел и взятием модуля.

Упражнение. Докажите, что для таких нормирований имеется формула произведения: $\prod_{\mathfrak{p}} |x|_{\mathfrak{p}}^{\delta_{\mathfrak{p}}} = 1$ для любого $x \neq 0$, где $\delta_{\mathfrak{p}} = 2$, если $k_{\mathfrak{p}} \cong \mathbb{C}$, и $\delta_{\mathfrak{p}} = 1$ во всех остальных случаях.

Терминология объясняется в следующем упражнении.

Упражнение. Докажите, что

1) неархимедовы точки взаимно однозначно соответствуют замкнутым схемным точкам (т.е. максимальным идеалам) спектра кольца целых числового поля, или гладкой проективной кривой C с данным полем функций;

2) в случае положительной характеристики все точки неархимедовы, и естественно отождествляются с множеством орбит абсолютной группы Галуа поля констант $\mathbb{F}_q$, действующей на множестве рациональных точек гладкой проективной кривой C над алгебраическим замыканием $\overline{\mathbb{F}_q}$ поля констант.

Определение. Подгруппой разложения точки глобального поля в некоторой группе автоморфизмов называется её стабилизатор.

Другими словами, если k – глобальное поле, $\mathfrak{p}$ – точка k и G – некоторая группа автоморфизмов k, то подгруппа разложения определяется как $G_{\mathfrak{p}} = \{g \in G \mid g(\mathcal{O}_{\mathfrak{p}}) = \mathcal{O}_{\mathfrak{p}}\}$.

В частности, подгруппу разложения можно рассматривать как некоторую группу непрерывных автоморфизмов пополнения глобального поля в данной точке.

Определение. *Локальное поле* – это пополнение глобального поля по нетривиальному нормированию.

Таким образом, это – или вещественное поле $\mathbb{R}$, или комплексное поле $\mathbb{C}$, или конечное расширение p-адического поля $\mathbb{Q}_p$ для некоторого простого числа p, или поле формальных степенных рядов от одной переменной над конечным полем констант.

Можно показать, что локальное поле – это то же самое, что не дискретное локально компактное поле, см., например, А.Вейль, Основы теории чисел, гл. I.

Упражнение. Пусть K/k – конечное сепарабельное расширение степени n локального поля, и φ – нормирование на k. Докажите, что $\varphi(x) = \varphi(N_{K/k}(x))^{1/n}$ для любого $x \in K$ – единственное продолжение φ на K, и что K – локальное поле. Выведите из этого, что продолжения любого нормирования любого глобального поля на его произвольное расширение Галуа образуют (непустую) орбиту группы Галуа.

2.1. **Структура мультипликативной группы поля, полного относительно дискретного нормирования, векторы Витта.** Неархимедовы локальные поля – пример полей, полных относительно дискретного нормирования.

Определение. Дискретным нормированием называется гомоморфизм v из $k^\times$ во вполне упорядоченную группу $\Gamma \subseteq \mathbb{Q}$, удовлетворяющий неархимедову неравенству треугольника: $v(x+y) \geqslant \max(v(x), v(y))$. Как правило, мы будем предполагать, что $\Gamma \cong \mathbb{Z}$.

Дискретное нормирование v определяет нормирование $\varphi = e^{-v}$, а значит, и топологию на k.

Пусть k – поле, полное относительно дискретного нормирования v, $\mathcal{O} = \{x \in k \mid v(x) \geqslant 0\}$ – его кольцо целых, $\mathfrak{p} = \{x \in k \mid v(x) > 0\} = \pi\mathcal{O}$ – максимальный идеал, $\mathcal{O}^\times = \{x \in k \mid v(x) = 0\} = \mathcal{O} \backslash \mathfrak{p}$ – группа единиц, и $\kappa = \mathcal{O}/\mathfrak{p}$ – поле вычетов.

Лемма 2.2. *$\mathcal{O}^\times/(1+\mathfrak{p}) = \kappa^\times$, $(1+\mathfrak{p}^j)/(1+\mathfrak{p}^{j+1}) = \mathfrak{p}^j/\mathfrak{p}^{j+1} = \kappa$, $\overline{x} \mapsto \overline{x-1} \mapsto \overline{(x-1)/\pi^j}$, где π – образующая идеала $\mathfrak{p}$. Если k – локальное поле, то имеется канонический изоморфизм групп $\mathcal{O}^\times = (1+\mathfrak{p}) \times \kappa^\times$.*

Доказательство очевидно.

Упражнение. Докажите, что

а) если характеристика поля вычетов – нулевая, то $\log : 1+\mathfrak{p} \longrightarrow \mathfrak{p}$ – изоморфизм;

б) если характеристика k – нулевая, характеристика поля вычетов равна $p > 0$, то логарифм индуцирует гомоморфизм $\log : 1+\mathfrak{p} \longrightarrow \pi^m\mathcal{O} \supseteq \mathfrak{p}$, где $m = \min\limits_{n\geqslant 0}(p^n - ne_{k/\mathbb{Q}_p}) \leqslant 1$ и $e_{k/\mathbb{Q}_p}$ – индекс ветвления расширения $k/\mathbb{Q}_p$, см. ниже, ядро которого конечно и состоит из корней p-примарных степеней из единицы;

в) если характеристика поля вычетов равна $p > 0$, то $1+\mathfrak{p}$ имеет естественную структуру $\mathbb{Z}_p$-модуля (без кручения, если характеристика поля k равна p).

Пусть R – произвольное коммутативное кольцо с единицей.

Упражнение. Докажите, что любой формальный ряд в $\mathbb{W}(R) := 1 + tR[[t]]$ однозначно представляется в виде $\prod_{s\geqslant 1}(1 - x_s t^s)$. Будем называть x_s координатами.

Сложение в $\mathbb{W}(R)$ определяется как умножение в $1+tR[[t]]$. Умножение в $\mathbb{W}(R)$ определяется формулой $(\prod_{s\geqslant 1}(1 - x_s t^s)) \circ (\prod_{s\geqslant 1}(1 - y_s t^s)) = \prod_{s,e\geqslant 1}(1 - x_s^{e/(s,e)} y_e^{s/(s,e)} t^{[s,e]})^{(s,e)}$.

Упражнение. а) Проверьте, что $\mathbb{W}(R)$ – коммутативное кольцо с единицей. (*Указание.* Рассмотрите сначала случай $R \supseteq \mathbb{Q}$, и покажите, что минус логарифмическая производная: $\prod_{s\geqslant 1}(1 - x_s t^s) \mapsto \sum_{n\geqslant 1} w_n t^{n-1}$, где $w_n = \sum_{d|n} dx_d^{n/d}$, определяет гомоморфизм $\mathbb{W}(R)$ в кольцо формальных рядов с покомпонентными сложением и умножением.)

б) Пусть S – множество натуральных чисел такое, что если $s \in S$ и $d|s$, то $d \in S$. Докажите, что координаты сумм (соотв. произведений) с номерами из S зависят только от координат слагаемых (соотв. множителей) с номерами из S, т.е. множество формальных рядов $\mathbb{W}_S(R)$ вида $\prod_{s\in S}(1 - x_s t^s) \in 1 + tR[[t]]$ также образует кольцо, если учитывать только координаты с номерами из S.

в) Для любого простого p положим $\mathbb{W}_{p,n}(R) := \mathbb{W}_S(R)$, если $S = \{1, p, \dots, p^n\}$, и $\mathbb{W}_p(R) := \mathbb{W}_S(R)$, если $S = \{1, p, p^2, p^3, \dots\}$ Докажите, что $\mathbb{W}_{p,n}(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$, и $\mathbb{W}_p(\mathbb{F}_p) = \mathbb{Z}_p$.

2.2. **Ветвление и фильтрация на локальных группах Галуа.** Пусть G – некоторая группа непрерывных автоморфизмов дискретно нормированного поля k. Например, как следует из варианта упражнения перед §2.1, автоморфизмы любого сепарабельного расширения поля, полного относительно дискретного нормирования, автоматически непрерывны.

Определим убывающую фильтрацию группы G нормальными подгруппами следующим образом. Группа G действует на поле вычетов $\kappa = \mathcal{O}/\mathfrak{p}$, что определяет гомоморфизм из G в группу автоморфизмов κ. Ядро

$$I = \{g \in G \mid gx - x \in \mathfrak{p} \text{ для всех } x \in \mathcal{O}\} = \{g \in G \mid \tfrac{gx}{x} \in 1+\mathfrak{p} \text{ для всех } x \in \mathcal{O}^\times\}$$

этого гомоморфизма называется группой инерции.

Высшими подгруппами ветвления называются $I^j = \{g \in G \mid gx - x \in \mathfrak{p}^{j+1} \text{ для всех } x \in \mathcal{O}\}$.

Ясно, что эта фильтрация – исчерпывающая: если $g \in I^j$ для всех j, то $gx \equiv x \bmod \mathfrak{p}^j$ для любого $x \in \mathcal{O}$, т.е. $g = 1$.

Определение. *Индексом ветвления* дискретного нормирования v расширения K/k называется индекс группы $v(k^\times)$ в $v(K^\times)$.

Если индекс ветвления равен 1, то расширение называется *неразветвлённым*. Если индекс совпадает со степенью расширения, т.е. расширение полей вычетов тривиально, то расширение называется *вполне разветвлённым*.

Упражнения. 1. Пусть K/k – расширение дискретно нормированных полей.

а) Докажите, что композит неразветвлённых расширений поля k в K/k неразветвлён над k.

б) Приведите пример расширения K/k и пары вполне разветвлённых подрасширений, композит которых не является вполне разветвлённым.

в) Докажите, что в K/k любое неразветвлённое подрасширение k^{nr}/k и любое вполне разветвлённое подрасширение k^{tr}/k линейно разделены над k, т.е. естественный гомоморфизм на их композит $k^{\mathrm{nr}} \otimes_k k^{\mathrm{tr}} \longrightarrow k^{\mathrm{nr}}k^{\mathrm{tr}}$ в K является изоморфизмом.

2. Пусть K/k – конечное сепарабельное расширение дискретно нормированных полей степени n и индекса ветвления e. Докажите, что а) K/k неразветвлено тогда и только тогда, когда $\Omega_{\mathcal{O}_K/\mathcal{O}_k} = 0$; б) индекс ветвления делит степень расширения, и их отношение n/e равно степени расширения полей вычетов. (*Указание*: см. доказательство леммы 2.3.)

3. Пусть K/k – конечное расширение Галуа дискретно нормированных полей с группой G.

Докажите, что а) подгруппа инерции в G фиксирует максимальное неразветвлённое подрасширение K^I/k в K/k;

б) неразветвлённые расширения поля k взаимно однозначно соответствуют расширениям его поля вычетов, и в частности, они – циклические, если поле вычетов конечно;

в) индекс ветвления равен порядку подгруппы инерции в G.

4. Докажите, что а) $\mathbb{W}_p(\mathbb{F}_{p^n})$ – кольцо целых в неразветвлённом расширении $\mathbb{Q}_p$ степени n;

б) $\mathbb{W}_p(\overline{\mathbb{F}_p})$ – кольцо целых в *пополнении* максимального неразветвлённого расширения $\mathbb{Q}_p$.

Лемма 2.3. *Пусть K/k – конечное расширение Галуа и π – образующая максимального идеала $\mathfrak{P}$ поля K. Тогда $I^j = \{g \in I \mid g\pi \equiv \pi \bmod \mathfrak{P}^{j+1}\}$.*

Доказательство. Это следует из равенства $\mathcal{O}_K = \mathcal{O}_{K^I}[\pi]$. □

Теорема 2.4. *Пусть K/k – конечное расширение Галуа, и p – характеристика поля вычетов κ поля K. Тогда I^0/I^1 изоморфна (конечной) подгруппе мультипликативной группы поля вычетов κ поля K. В частности, она – циклическая, и её порядок не делится на p.*

Если $p = 0$, то $I^1 = 1$. Если $p > 0$ и $j > 0$, то I^j/I^{j+1} изоморфна подгруппе аддитивной группы κ. В частности, I^1 – p-группа (называемая подгруппой дикого ветвления).

Доказательство. Пусть π – образующая максимального идеала $\mathfrak{P}$ поля K. Отображение $g \mapsto g\pi/\pi \bmod \mathfrak{P}$ – гомоморфизм группы инерции $I = I^0$ в группу $\mathcal{O}_K^\times/(1+\mathfrak{P}) = \kappa^\times$, поскольку это 1-коцикл с тривиальным действием на $\mathcal{O}_K^\times/(1+\mathfrak{P}) = \kappa^\times$. Его ядро $\{g \in I \mid g\pi \equiv \pi \bmod \mathfrak{P}^2\}$, как мы знаем из леммы 2.3, совпадает с I^1.

Отображение $g \mapsto g\pi/\pi \bmod \mathfrak{P}^{j+1}$ – гомоморфизм группы ветвления I^j в группу $(1+\mathfrak{P}^j)/(1+\mathfrak{P}^{j+1}) = \mathfrak{P}^j/\mathfrak{P}^{j+1} = \kappa$, поскольку это 1-коцикл с тривиальным действием на $(1+\mathfrak{P}^j)/(1+\mathfrak{P}^{j+1}) = \kappa$. Его ядро, очевидно, совпадает с I^{j+1}.

Если $p = 0$, то в κ нет конечных подгрупп, т.е. $I^1 = 1$. □

Замечания. 1. Как мы видим, фильтрация ветвления тесно связана с упоминавшейся выше фильтрацией мультипликативной группы поля. В случае абелевых расширений полей, полных относительно дискретного нормирования, точная формулировка этой связи составляет содержание локальной теории полей классов.

2. Если $p = 0$, то группа инерции I естественно вкладывается в группу корней из единицы в поле вычетов κ. Поэтому группа инерции алгебраического замыкания $\overline{\kappa((t))}$ поля рядов Лорана $\kappa((t))$, «геометрическая фундаментальная группа проколотого формального круга», канонически изоморфна $\widehat{\mathbb{Z}}(1) := \varprojlim_N \mu_N \cong \widehat{\mathbb{Z}}$. Из теории Куммера следует, что $\overline{\kappa((t))}$ совпадает с полем рядов Пюизё $\bigcup_{N>1} \overline{\kappa}((t^{1/N}))$ над алгебраическим замыканием κ.

Теорема 2.5 (Шпайзер). *Пусть $\tau \in I$ и $\sigma \in I^j$, $j > 0$. Тогда $[\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} \in I^{j+1}$ тогда и только тогда, когда или $\sigma \in I^{j+1}$, или $\tau^j \in I^1$.*

Доказательство. Пусть π – образующая максимального идеала $\mathfrak{P}$ поля K. Поскольку τ сохраняет максимальный идеал, $\tau\pi = \varepsilon\pi$, где $\varepsilon \in \mathcal{O}_K^\times$. Пусть $\sigma\pi \equiv \pi + \beta\pi^{j+1} \bmod \mathfrak{P}^{j+2}$, где $\beta \in \mathcal{O}_K$. Поскольку $\sigma \in I^j$, получаем $\sigma\varepsilon \equiv \varepsilon \bmod \mathfrak{P}^{j+1}$, откуда $\sigma\tau\pi = \sigma(\varepsilon\pi) \equiv \varepsilon(\sigma\pi) \bmod \mathfrak{P}^{j+2} \equiv \varepsilon\pi + \varepsilon\beta\pi^{j+1} \bmod \mathfrak{P}^{j+2} \equiv \varepsilon\pi + (\varepsilon\pi)^{j+1}\beta\varepsilon^{-j} \bmod \mathfrak{P}^{j+2}$. С другой стороны, $\tau\beta \equiv \beta \bmod \mathfrak{P}$, откуда $\tau\sigma\pi \equiv \tau\pi + (\tau\beta)(\tau\pi)^{j+1} \bmod \mathfrak{P}^{j+2} \equiv \varepsilon\pi + \beta(\varepsilon\pi)^{j+1} \bmod \mathfrak{P}^{j+2}$. Объединив эти два сравнения, получим $(\sigma\tau - \tau\sigma)\pi \equiv (\varepsilon\pi)^{j+1}\beta(\varepsilon^{-j} - 1) \bmod \mathfrak{P}^{j+2}$. Заменив π на $\tau^{-1}\sigma^{-1}\pi$, получим $\pi - \tau\sigma\tau^{-1}\sigma^{-1}\pi \equiv (\varepsilon\pi)^{j+1}\beta(\varepsilon^{-j} - 1) \bmod \mathfrak{P}^{j+2}$. Мы видим, что эквивалентны следующие условия

а) $\tau\sigma\tau^{-1}\sigma^{-1} \in I^{j+1}$,

б) $\beta(\varepsilon^{-j} - 1) \equiv 0 \bmod \mathfrak{P}$,

в) $\beta \equiv 0 \bmod \mathfrak{P}$ или $\varepsilon^j \equiv 1 \bmod \mathfrak{P}$.

Но из определения σ, $\sigma \in I^{j+1}$ тогда и только тогда, когда $\beta \equiv 0 \bmod \mathfrak{P}$.

Поскольку $\tau\varepsilon \equiv \varepsilon \bmod \mathfrak{P}$, получаем $\tau^j\pi \equiv \varepsilon^j\pi \bmod \mathfrak{P}^2$. Это доказывает, что $\tau^j \in I^1$ тогда и только тогда, когда $\varepsilon^j \equiv 1 \bmod \mathfrak{P}$, и завершает доказательство теоремы. □

Следствие 2.6. *Группа I^j/I^{j+1} содержится в центре I^1/I^{j+1}.*

Доказательство. Если $\tau \in I^1$, то $[\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} \in I^{j+1}$. □

Следствие 2.7. *Если K/k абелево и $I^j \neq I^{j+1}$, то порядок e_0 группы I^0/I^1 делит j.*

Доказательство. Выберем подъём $\tau \in I$ образующей группы I^0/I^1 и элемент $\sigma \in I^j \setminus I^{j+1}$. Если e_0 не делит j, то $\tau^j \notin I^1$, а значит, $[\tau, \sigma] \notin I^{j+1}$, что противоречит абелевости K/k. □

2.3. **Явная конструкция абелевых расширений локальных полей и формальные группы: теория Любина–Тэйта.** По определению из предыдущего параграфа, группа Галуа локального поля k является расширением группы Галуа поля вычетов при помощи группы инерции. Поэтому расширение Галуа локального поля является вполне разветвлённым расширением неразветвлённого расширения. Поскольку поле вычетов конечно, все его элементы – корни из единицы степеней, не делящихся на его характеристику p, а все его расширения абелевы и получаются присоединением таких корней из единицы.

По этой причине, неразветвлённые расширения локального поля также получаются добавлением корней из единицы степеней, не делящихся на p.

Осталось научиться строить вполне разветвлённые расширения. Заметим, что в случае нулевой характеристики добавлением корней из единицы p-примарных степеней получается некоторое вполне разветвлённое расширение. Это можно представить следующим образом. Пусть $g(t) = \frac{(1+t)^p - 1}{t}$ и $f(t) = tg(t) = (1+t)^p - 1$. Тогда $k(\mu_{p^n})$ получается присоединением корня $\theta_n(g)$ многочлена $g(f^{(n-1)}(t)) = g((1+t)^{p^{n-1}} - 1) = \frac{(1+t)^{p^n} - 1}{(1+t)^{p^{n-1}} - 1}$. Заметим, что $v(\theta_n(g)) > 0$, и что если $k/\mathbb{Q}_p$ неразветвлено, то $g(t)$, равно как и все $g(f^{(n-1)}(t))$ – многочлены Эйзенштейна.[6]

Как показывает следующее утверждение, расширения полей, полных относительно дискретного нормирования, не очень зависят от многочлена, корни которого мы добавляем.

Лемма 2.8 (Краснер). *Пусть k – поле, полное относительно дискретного нормирования v. Пусть α, β – элементы некоторого алгебраического расширения поля k, и α сепарабелен над*

[6]Многочлен Эйзенштейна над некоторой коммутативной областью – это многочлен со старшим коэффициентом 1, свободный член которого порождает простой идеал $\neq 0$, в котором лежат остальные коэффициенты.

Упражнение. Докажите неприводимость многочленов Эйзенштейна.

$k(\beta)$. Если $v(\beta-\alpha) > v(\alpha'-\alpha)$ для всех сопряжённых α' элемента α, отличных от α, то $\alpha \in k(\beta)$.

Доказательство. Пусть $L/k(\beta)$ – нормальное замыкание расширения $k(\alpha,\beta)/k(\beta)$, и $g \in G_{L/k(\beta)}$. Тогда $v(\beta - g\alpha) = v(\beta-\alpha) > v(\alpha'-\alpha)$, откуда $v(\alpha - g\alpha) \geqslant \min(v(\alpha-\beta), v(\beta - g\alpha)) > v(\alpha'-\alpha)$ для всех сопряжённых α' элемента α, отличных от α. В частности $g\alpha \neq \alpha'$, то есть $g\alpha = \alpha$. □

Упражнение. Докажите, что пополнение алгебраически замкнутого поля по дискретному нормированию, алгебраически замкнуто. В частности, пополнение алгебраического замыкания поля, полного относительно дискретного нормирования, алгебраически замкнуто.

Пусть теперь $g(t)$ – произвольный многочлен Эйзенштейна степени $q-1$, где q – число элементов поля вычетов. Положим $\pi = g(0)$. Пусть $\tilde{g}(t)$ – аналогичный многочлен Эйзенштейна с $\tilde{g}(0) = \pi$. Мы хотим сравнить соответствующие им (вполне разветвлённые сепарабельные) расширения.

Обозначение. Пусть $\mathcal{O}$ – кольцо дискретного нормирования с полем вычетов из q элементов, и π – униформизующая. Тогда $\mathfrak{F}_\pi := X^q + \pi X + \pi X^2\mathcal{O}[[X]] \subset \mathcal{O}[[X]]$.

Лемма 2.9. *Если $f, \tilde{f} \in \mathfrak{F}_\pi$ и $\alpha_1, \dots, \alpha_m \in \mathcal{O}$, то существует единственный формальный ряд $F(X_1,\dots,X_m) \in \mathcal{O}[[X_1,\dots,X_m]]$ такой, что $F(X_1,\dots,X_m) \equiv \alpha_1 X_1 + \dots + \alpha_m X_m$ с точностью до слагаемых степеней > 1, и $f(F(X_1,\dots,X_m)) = F(\tilde{f}(X_1),\dots,\tilde{f}(X_m))$.*

Доказательство. Пусть $F_1 = \alpha_1 X_1 + \dots + \alpha_m X_m$. Докажем, что для каждого $j > 1$ существует единственный многочлен F_j степени $\leqslant j$ такой, что а) $F_j(X_1,\dots,X_m) \equiv F_{j-1}(X_1,\dots,X_m)$ с точностью до слагаемых степеней $\geqslant j$, и б) $f(F_j(X_1,\dots,X_m)) \equiv F_j(\tilde{f}(X_1),\dots,\tilde{f}(X_m))$ с точностью до слагаемых степеней $> j$.

Предположим, что мы это проверили для $F_1,\dots,F_{j-1}$. Пусть $F_j = F_{j-1} + G$, где G – многочлен степени $\leqslant j$. По предположению о единственности $F_1,\dots,F_{j-1}$, многочлен G однороден степени j. Поэтому $f(F_j) \equiv f(F_{j-1}) + \pi G$ с точностью до слагаемых степени $> j$, и $F_j(\tilde{f}(X_1),\dots,\tilde{f}(X_m)) \equiv F_{j-1}(\tilde{f}(X_1),\dots,\tilde{f}(X_m)) + \pi^j G$ с точностью до слагаемых степени $> j$. Поскольку $f(F_{j-1}(X_1,\dots,X_m)) \equiv F_{j-1}(\tilde{f}(X_1),\dots,\tilde{f}(X_m))$ с точностью до слагаемых степеней $\geqslant j$, многочлен G определяется как компонента степени j ряда $\frac{F_{j-1}(\tilde{f}(X_1),\dots,\tilde{f}(X_m)) - f(F_{j-1})}{\pi(1-\pi^{j-1})}$.

Его коэффициенты – целые, так как ряды $f(F_{j-1})$ и F_{j-1}^q, а также $F_{j-1}(\tilde{f}(X_1),\dots,\tilde{f}(X_m))$ и $F_{j-1}(X_1^q,\dots,X_m^q)$ покоэффициентно сравнимы по модулю максимального идела. □

Обозначение. Если $m = 1$, то ряд F, построенный в лемме, обозначается через $[\alpha]_{f,\tilde{f}}$.

Пример. Пусть $g(t)$ и $\tilde{g}(t)$ – такие многочлены Эйзенштейна степени $q-1$, что $g(0) = \tilde{g}(0)$. Пусть $f(t) = tg(t)$ и $\tilde{f}(t) = t\tilde{g}(t)$. Тогда композиции $g(f^{(n-1)}(t)) = g(\underbrace{f(\dots(f}_{n-1}(t))\dots)$ и $\tilde{g}(\tilde{f}^{(n-1)}(t)) = \tilde{g}(\underbrace{\tilde{f}(\dots(\tilde{f}}_{n-1}(t))\dots)$ – также многочлены Эйзенштейна. Пусть $\theta_n(\tilde{g})$ – корень $\tilde{g}(\tilde{f}^{(n-1)}(t))$. Ясно, что он лежит в максимальном идеале. Тогда $[\alpha]_{f,\tilde{f}}(\theta_n(\tilde{g}))$ определено и является корнем многочлена $g(f^{(n-1)}(t))$ для любого $\alpha \in \mathcal{O}^\times$, так как $g(f^{(n-1)}([\alpha]_{f,\tilde{f}}(\theta_n(\tilde{g})))) =$

$g([\alpha]_{f,\tilde f}(\tilde f^{(n-1)}(\theta_n(\tilde g)))) = \frac{[\alpha]_{f,\tilde f}(\tilde f^{(n)}(\theta_n(\tilde g)))}{[\alpha]_{f,\tilde f}(\tilde f^{(n-1)}(\theta_n(\tilde g)))} = 0$, если знаменатель не равен нулю. Знаменатель равен $[\alpha]_{f,\tilde f}(\theta_1(\tilde g)) \equiv \alpha\theta_1(\tilde g) \bmod \mathfrak{p}^2$, то есть не равен нулю, если элемент α обратим.

Следствие 2.10. *Поле $k_\pi^n := k(\theta_n(g))$ зависит только от n и от $\pi := g(0)$.* □

Таким образом, имеется отображение $\mathcal{O}^\times \xrightarrow{\tau_n} G_{k_\pi^n/k}$, $\alpha \overset{\tau_n}{\mapsto} (\theta_n(g) \mapsto [\alpha]_{f,f}(\theta_n(g)))$.

Теорема 2.11 (Любин–Тэйт). (1) *Расширение k_π^n/k абелево и отображение τ_n – гомоморфизм на группу Галуа $G_{k_\pi^n/k}$ с ядром $1+\mathfrak{p}^n$.*

(2) *Пусть $g(t), \tilde g(t)$ – многочлены Эйзенштейна степени $q-1$ над $\mathcal{O}$, и L – неразветвлённое расширение степени $q^{n-1}(q-1)$ поля k в некотором его алгебраическом замыкании. Тогда $L_{g(0)}^n = L_{\tilde g(0)}^n$*

Упражнение. Докажите, что τ_n отождествляет подгруппу $1+\mathfrak{p}^j$ с $V^j := I^{\psi(j)}$, где ψ – единственная непрерывная кусочно-линейная функция на $\mathbb{R}_+$ такая, что $\psi(0)=0$ и $\psi'(u) = [I : I_{[u]}]^{-1}$ для нецелых u ([ ] – целая часть). Здесь I – группа инерции максимального абелева расширения поля k.

Для доказательства теоремы удобно ещё раз вернуться к корням из единицы p-примарных степеней, и заметить, что они образуют подгруппу кручения в $1+\mathfrak{P}$, где $\mathfrak{P}$ – максимальный идеал кольца целых алгебраического замыкания поля k. Группу $1+\mathfrak{P}$ можно отождествить с $\mathfrak{P}$, но с групповым законом $X \dot{+} Y = X + Y + XY$.

Чтобы обобщить эту конструкцию, введём следующее понятие.

Определение. (Одномерной коммутативной) формальной группой над коммутативным кольцом с единицей R называется формальный ряд $F(X,Y) \in R[[X,Y]]$ такой, что $F(X,0) = F(0,X) = X$ (нуль), $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (ассоциативность) и $F(X,Y) = F(Y,X)$ (коммутативность).

Упражнение. Докажите, что если в R нет кручения, т.е. умножение на положительные целые числа инъективно, то коммутативность следует из остальных условий.

Ясно, что $F(X,Y) \equiv X+Y$ с точностью до слагаемых степеней >1 для любой формальной группы $F(X,Y)$. Например, $F(X,Y) = X+Y$ называется формальной аддитивной группой, а $F(X,Y) = X+Y+XY$ – формальной мультипликативной группой.

Назовём R-гомоморфизмом формальных групп $F \longrightarrow G$ формальный ряд $f(X) \in XR[[X]]$ такой, что $f(F(X,Y)) = G(f(X), f(Y))$. Пусть $\mathrm{Hom}_R(F,G)$ – множество R-гомоморфизмов.

Упражнения. а) Для $f, g \in \mathrm{Hom}_R(F,G)$ положим $f \oplus g := G(f(X), g(Y))$. Докажите, что операция $\oplus$ определяет структуру коммутативной группы на множестве $\mathrm{Hom}_R(F,G)$.

б) Рассмотрим $XR[[X]]$ как полугруппу относительно композиции (подстановки) $\circ$. Докажите, что ряд $f(X) \in XR[[X]]$ обратим тогда и только тогда, когда $(f(X)/X)(0) \in R^\times$.

Следствие 2.12. *Для любого элемента $f \in \mathfrak{F}_\pi$ существует единственная формальная группа F_f над $\mathcal{O}$, эндоморфизмом которой он является.*

Доказательство. Согласно лемме 2.9 (при $m=2$), существует единственный формальный ряд $F(X,Y) \in \mathcal{O}[[X,Y]]$ над $\mathcal{O}$ такой, что $F(X,Y) \equiv X+Y$ с точностью до слагаемых степеней >1, и $f(F(X,Y)) = F(f(X), f(Y))$. Из единственности следует коммутативность.

С другой стороны (при $m = 3$), существует единственный формальный ряд $G(X,Y,Z) \in \mathcal{O}[[X,Y]]$ над $\mathcal{O}$ такой, что $G(X,Y,Z) \equiv X+Y+Z$ с точностью до слагаемых степеней > 1, и $f(G(X,Y)) = G(f(X), f(Y), f(Z))$. Поскольку и $F(X, F(Y,Z))$, и $F(F(X,Y),Z)$ удовлетворяют этим условиям, получаем ассоциативность. $\square$

Следствие 2.13. *Для любых элементов $f, \tilde{f}, \tilde{\tilde{f}} \in \mathfrak{F}_\pi$ и любых элементов $\alpha, \beta \in \mathcal{O}$*

(1) $[\alpha]_{f,\tilde{f}} \in \mathrm{Hom}_{\mathcal{O}}(F_{\tilde{f}}, F_f)$;
(2) $[\alpha]_{f,\tilde{f}} \oplus [\beta]_{f,\tilde{f}} = [\alpha+\beta]_{f,\tilde{f}}$;
(3) $[\alpha]_{f,\tilde{f}} \circ [\beta]_{\tilde{f},\tilde{\tilde{f}}} = [\alpha \cdot \beta]_{f,\tilde{\tilde{f}}}$.

В частности, $[-]_{f,f}$ задаёт инъективный гомоморфизм колец $\mathcal{O} \longrightarrow \mathrm{End}_{\mathcal{O}}(F_f)$.

Доказательство. Положим $h(X) := [\alpha]_{f,\tilde{f}} \oplus [\beta]_{f,\tilde{f}} := F_f([\alpha]_{f,\tilde{f}}, [\beta]_{f,\tilde{f}})$. Тогда $h(\tilde{f}(X)) = F_f([\alpha]_{f,\tilde{f}}(\tilde{f}(X)), [\beta]_{f,\tilde{f}}(\tilde{f}(X))) = F_f(f([\alpha]_{f,\tilde{f}}(X)), f([\beta]_{f,\tilde{f}}(X))) = f(F_f([\alpha]_{f,\tilde{f}}(X), [\beta]_{f,\tilde{f}}(X)) = f(h(X))$. Остальное аналогично предыдущему. Инъективность следует из того, что $[\alpha]_{f,f} \equiv \alpha X$ с точностью до слагаемых степеней > 1. $\square$

Ясно, что если $\tilde{R}$ – объединение колец, полных относительно некоторых идеалов, то $F(X,Y)$ задаёт на объединении этих идеалов структуру абелевой группы, нулём которого служит 0.

Возьмём в качестве $\tilde{R}$ кольцо целых сепарабельного замыкания поля k с максимальным идеалом $\mathfrak{m}$, и любой многочлен $f \in \mathfrak{F}_\pi$ степени q. Тогда $\mathfrak{m}$ становится $\mathcal{O}$-модулем относительно группового закона, соответствующего многочлену f.

Например, в случае $k = \mathbb{Q}_p$ и $f = (1+t)^p - 1$ получается формальная мультипликативная группа, и $\mathfrak{m}$ становится $\mathbb{Z}_p$-модулем, канонически изоморфным $1 + \mathfrak{m}$.

Рассмотрим теперь вместо корней из единицы p-примарных степеней $\mathcal{O}$-подмодуль кручения $E_f = \bigcup_n E_f^n$ в $\mathfrak{m}$, где $E_f^n = \{\theta \in \mathfrak{m} \mid [\pi^n]_f(\theta) = f^{(n)}(\theta) = 0\}$. Ясно, что элементы $E_f^n \backslash E_f^{n-1}$ соответствуют $q^n - q^{n-1}$ корням многочлена Эйзенштейна $g(f^{(n-1)}(t))$, где $f(t) = tg(t)$. Поэтому для любого элемента $\theta \in E_f^n \backslash E_f^{n-1}$ инъективный гомоморфизм $\mathcal{O}$-модулей $\mathcal{O}/\mathfrak{p}^n \longrightarrow E_f^n$, $\alpha \mapsto [\alpha]_f(\theta)$, должен быть сюръективным, т.е. изоморфизмом.

Это определяет канонические изоморфизмы $\mathcal{O}/\mathfrak{p}^n = \mathrm{End}_{\mathcal{O}}(E_f^n)$, $\mathcal{O}^\times/(1+\mathfrak{p}^n) = \mathrm{Aut}_{\mathcal{O}}(E_f^n)$ и $\mathcal{O}^\times = \mathrm{Aut}_{\mathcal{O}}(E_f)$.

Упражнение. Докажите, что $\mathcal{O}$-модуль E_f изоморфен $k/\mathcal{O}$, но не канонически.

Следствие 2.14. *Пусть $k_\pi := \bigcup_{n \geqslant 1} k_\pi^n$. Естественный гомоморфизм $G_{k_\pi/k} \xrightarrow{\tau^{-1}} \mathrm{Aut}_{\mathcal{O}}(E_f) = \mathcal{O}^\times$ является изоморфизмом.*

Доказательство. По определению k_π, он инъективен. Группа $(\mathcal{O}/\mathfrak{p}^n)^\times = \mathcal{O}^\times/(1+\mathfrak{p}^n)$ действует точно на поле $k_\pi^n = k(\theta_n(g))$, а значит, $G_{k_\pi^n/k} \longrightarrow \mathrm{Aut}_{\mathcal{O}}(E_f^n) = \mathcal{O}^\times/(1+\mathfrak{p}^n)$ – изомоморфизм. Переход к обратному пределу по n даёт наш изоморфизм τ^{-1}. $\square$

Следствие 2.15. *Расширение $k_\pi k^{\mathrm{nr}}/k$ абелево, и имеется инъективный гомоморфизм $\rho_\pi : k^\times \longrightarrow G_{k_\pi k^{\mathrm{nr}}/k}$, который становится изоморфизмом, если пополнить $k^\times$ по открытым подгруппам конечного индекса.*

Доказательство. Как мы знаем, k_π и k^{nr} линейно разделены над k, поэтому автоморфизмы расширения $k_\pi k^{\mathrm{nr}}/k$ взаимно однозначно соответствуют парам автоморфизмов расширений k_π/k и k^{nr}/k. Любой элемент $a \in k^\times$ однозначно представляется в виде $a = \alpha\pi^m$, где $\alpha \in \mathcal{O}^\times$.

Определим $\rho_\pi(a)$ как Frob_q^m на k^{nr}, и как $\tau(\alpha^{-1})$ – на k_π, где τ – гомоморфизм, обратный к изоморфизму из предыдущего следствия. $\square$

Упражнение. Докажите, что а) в любой топологической группе множества открытых и замкнутых подгрупп конечного индекса совпадают;

б) подгруппы в $k^\times$ конечного индекса, не делящегося на характеристику k, открыты.

Теперь мы хотим доказать, что ни расширение $k_\pi k^{\mathrm{nr}}/k$, ни гомоморфизм ρ_π не зависят от выбора униформизующей π.

Обозначим через K пополнение k^{nr}, и через φ – продолжение по непрерывности автоморфизма Фробениуса $\mathrm{Frob}_q \in G_{k^{\mathrm{nr}}/k} = G_{\overline{\kappa}/\kappa}$ на K. Если $\omega(X) = \sum_m a_m X^m$ – формальный ряд над K, положим $\omega^\varphi(X) = \sum_m \varphi(a_m) X^m$.

Лемма 2.16. *Пусть* $h(X) \in uX + X^2\mathcal{O}[[X]]$, $u \in \mathcal{O}^\times$. *Тогда существует ряд* $\omega(X) \in \mathcal{O}_K^\times X + X^2\mathcal{O}_K[[X]]$ *такой, что* $\omega^\varphi(X) = \omega(h(X))$.

Доказательство оставляется в качестве упражнения, первым шагом которого должна быть проверка точности последовательностей $0 \longrightarrow \mathcal{O} \longrightarrow \mathcal{O}_K \xrightarrow{\varphi - id} \mathcal{O}_K \longrightarrow 0$ и $1 \longrightarrow \mathcal{O}^\times \longrightarrow \mathcal{O}_K^\times \xrightarrow{\varphi - id} \mathcal{O}_K^\times \longrightarrow 1$. Подробности можно найти, например, в книге [И], §4.2, теорема 2; §7.2, лемма 4.

Пусть $\pi' = \alpha\pi$ – другая униформизующая поля k. По лемме 2.16, существует ряд $\omega \in \mathcal{O}_K^\times X + X^2\mathcal{O}_K[[X]]$ такой, что $\omega^\varphi = \omega \circ [\alpha]_{f,f}$.

Лемма 2.17. *Пусть* $h = \omega \circ [\pi']_{f,f} \circ \omega^{-1}$, *где* $f \in \mathfrak{F}_\pi$. *Тогда а)* $h(X) \in \mathfrak{F}_{\pi'}$, *б)* $F_h(\omega(X), \omega(Y)) = \omega(F_f(X,Y))$, *в)* $[\gamma]_{h,h} \circ \omega = \omega \circ [\gamma]_{f,f}$ *для любого* $\gamma \in \mathcal{O}$.

Другими словами, формальные группы F_f *и* F_h *изоморфны над* $\mathcal{O}_K$.

Доказательство. Как следует из точности одной из последовательностей из леммы 2.16, инварианты φ на $\mathcal{O}_K$ совпадают с $\mathcal{O}$. Поскольку для любого $\gamma \in \mathcal{O}$

$$(\omega \circ [\gamma]_{f,f} \circ \omega^{-1})^\varphi = \omega^\varphi \circ [\gamma]_{f,f} \circ (\omega^{-1})^\varphi = \omega \circ [\alpha]_{f,f} \circ [\gamma]_{f,f} \circ [\alpha]_{f,f}^{-1} \circ \omega^{-1} = \omega \circ [\gamma]_{f,f} \circ \omega^{-1},$$

коэффициенты ряда $\omega \circ [\gamma]_{f,f} \circ \omega^{-1}(X)$ лежат в $\mathcal{O}$. Ясно, что $\omega \circ [\gamma]_{f,f} \circ \omega^{-1} \equiv \gamma X \bmod X^2$, и значит, $\omega \circ [\gamma]_{f,f} \circ \omega^{-1} = [\gamma]_{h,h}$. В частности, $h(X) \equiv \pi' X \bmod X^2$. Наконец,

$$\begin{aligned} h(X) = \omega \circ [\pi']_{f,f} \circ \omega^{-1} = \omega \circ [\alpha]_{f,f} \circ [\pi]_{f,f} \circ \omega^{-1} = \\ = \omega^\varphi \circ [\pi]_{f,f} \circ \omega^{-1} = \omega^\varphi \circ f \circ \omega^{-1} \equiv \omega^\varphi((\omega^{-1}(X))^q) \equiv (\omega(\omega^{-1}(X)))^q = X^q \bmod \mathfrak{p}. \end{aligned}$$

Аналогично,

$$(\omega \circ F_f \circ \omega^{-1})^\varphi = \omega^\varphi \circ F_f \circ (\omega^{-1})^\varphi = \omega \circ [\alpha]_{f,f} \circ F_f \circ [\alpha]_{f,f}^{-1} \circ \omega^{-1} = \omega \circ F_f \circ \omega^{-1}, \quad \text{и}$$
$$(\omega \circ F_f \circ \omega^{-1}) \circ h = \omega \circ F_f \circ [\pi']_{f,f} \circ \omega^{-1} = h \circ \omega \circ [\pi']_{f,f}^{-1} \circ F_f \circ [\pi']_{f,f} \circ \omega^{-1} = h \circ (\omega \circ F_f \circ \omega^{-1}),$$

то есть h – эндоморфизм формальной группы $\omega \circ F_f \circ \omega^{-1}$, откуда следует, что $\omega \circ F_f \circ \omega^{-1} = F_h$. □

Следствие 2.18. $k_\pi k^{\mathrm{nr}} = k_{\pi'} k^{\mathrm{nr}}$.

Доказательство. Очевидно, что $k_\pi K = k_{\pi'} K$, т.к. поля, порождённые точками деления групп F_f и F_h совпадают. В частности, совпадают пополнения $\widehat{k_\pi k^{\mathrm{nr}}} = \widehat{k_{\pi'} k^{\mathrm{nr}}}$.

Заметим, что если E – алгебраическое расширение локального поля, и $a \in \widehat{E}$ – элемент его пополнения, алгебраический и сепарабельный над E, то $a \in E$. Это следует из теории Галуа для E^{sep}/E: если $\sigma \in G_{E^{\mathrm{sep}}/E}$, то σ непрерывен, а значит $\sigma a = a$.

Поэтому множество элементов поля $\widehat{k_\pi k^{\mathrm{nr}}} = \widehat{k_{\pi'} k^{\mathrm{nr}}}$, алгебраических и сепарабельных над $k_\pi k^{\mathrm{nr}}$ совпадает с $k_\pi k^{\mathrm{nr}}$. С другой стороны, все элементы поля $k_{\pi'} k^{\mathrm{nr}}$ также алгебраичны и сепарабельны над $k_\pi k^{\mathrm{nr}}$, и значит, $k_\pi k^{\mathrm{nr}} = k_{\pi'} k^{\mathrm{nr}}$. $\square$

Следствие 2.19. $\rho_\pi = \rho_{\pi'}$. Поэтому в дальнейшем будем писать ρ вместо ρ_π.

Доказательство. Покажем, что $\rho_\pi(\pi') = \rho_{\pi'}(\pi')$. Это будет значить, что $\rho_\pi(\pi') = \rho_{\pi'}(\pi') = \rho_{\pi''}(\pi')$. Поскольку все такие π' порождают $k^\times$, получим $\rho_\pi = \rho_{\pi''}$.

По определению, $\rho_\pi(\pi')$ и $\rho_{\pi'}(\pi')$ совпадают на k^{nr} с автоморфизмом Фробениуса φ. Кроме того, $\rho_{\pi'}(\pi')$ – тождественный на $k_{\pi'}$. Осталось вычислить $\rho_\pi(\pi')|_{k_{\pi'}}$.

$k_{\pi'} = k(E_h)$, где $h \in \mathfrak{F}_{\pi'}$. Пусть ω (как и h) – как в лемме 2.17, то есть $\omega : E_f \xrightarrow{\sim} E_h$. Значит, для любого $\lambda \in E_h$ существует единственный элемент $\mu \in E_f$ такой, что $\lambda = \omega(\mu)$. Из равенства

$$\rho_\pi(\pi')\lambda = \rho_\pi(\pi')\omega(\mu) = \rho_\pi(\pi)\rho_\pi(\alpha)\omega(\mu) = \rho_\pi(\pi)\omega([\alpha^{-1}]_{f,f}(\mu)) = \omega^\varphi([\alpha^{-1}]_{f,f}(\mu)) = \omega(\mu) = \lambda$$

видим, что $\rho_\pi(\pi')|_{k_{\pi'}} = \rho_{\pi'}(\pi')|_{k_{\pi'}} = id$. $\square$

Замечание. Пусть k – локальное поле с полем вычетов из q элементов, k^{nr} – его максимальное неразветвлённое расширение, и π – его униформизующая. Нетрудно показать с помощью теории Куммера, что а) любое конечное абелево расширение поля k степени, не делящейся на характеристику p поля вычетов, содержится в $k^{\mathrm{nr}}(\sqrt[q-1]{\pi}) = k_\pi^1 k^{\mathrm{nr}}$; б) если дискретное нормирование v поля k продолжено на k^{ab}, то $v((k^{\mathrm{ab}})^\times) = \frac{1}{q-1}\mathbb{Z}[\frac{1}{p}]v(k^\times) \cong \mathbb{Z}[\frac{1}{p}]$.

Доказательство. Любое конечное абелево расширение является композитом циклических расширений примарных порядков.

Проверим, что любое конечное циклическое расширение K/k степени m, не делящейся на характеристику p поля вычетов, содержится в $k^{\mathrm{nr}}(\sqrt[q-1]{\pi}) = k_\pi^1 k^{\mathrm{nr}}$.

Пусть $\zeta \in k^{\mathrm{nr}}$ – примитивный корень из единицы степени m. Тогда $K(\zeta)/k(\zeta)$ – конечное циклическое расширение поля k степени n, где $n|m$. Согласно теории Куммера, $K(\zeta) = k(\zeta, \sqrt[n]{\xi}) \subset k^{\mathrm{nr}}(\sqrt[n]{\xi})$ для некоторого $\xi \in k(\zeta)^\times$. Поскольку группа единиц $\mathcal{O}_{k^{\mathrm{nr}}}^\times \cong \overline{\kappa}^\times \times (1+\pi\mathcal{O}_{k^{\mathrm{nr}}})$ m-делима, и $(k^{\mathrm{nr}})^\times \cong \mathcal{O}_{k^{\mathrm{nr}}}^\times \times \mathbb{Z}$, имеется включение $K \subset k^{\mathrm{nr}}(\sqrt[n]{\pi})$.

Ясно, что $k(\sqrt[n]{\pi})$ и k^{nr} линейно разделены, т.е. $k^{\mathrm{nr}}(\sqrt[n]{\pi}) = k(\sqrt[n]{\pi})\otimes_k k^{\mathrm{nr}}$, а значит, расщепляется точная последовательность $1 \longrightarrow \mu_n \longrightarrow \Gamma \longrightarrow G_{k^{\mathrm{nr}}/k} \longrightarrow 1$, где $\Gamma = G_{k^{\mathrm{nr}}(\sqrt[n]{\pi})/k}$. Другими словами, $\Gamma \cong \mu_n \rtimes G_{k^{\mathrm{nr}}(\sqrt[n]{\pi})/k}$, где образующая Frob_q группы $G_{k^{\mathrm{nr}}(\sqrt[n]{\pi})/k}$ действует на μ_n возведением в степень q.

Нетрудно вычислить коммутант: $[\Gamma, \Gamma] = \mu_n^{q-1} = \mu_{n/(n,q-1)}$, и значит, любое абелево расширение поля k в $k^{\mathrm{nr}}(\sqrt[n]{\pi})$ содержится в его инвариантах $k^{\mathrm{nr}}(\sqrt[(n,q-1)]{\pi}) \subseteq k^{\mathrm{nr}}(\sqrt[q-1]{\pi})$.

В частности, индексы ветвления абелевых расширений k делят произведения $q-1$ и степеней p. То, что все такие индексы ветвления реализуются, следует из формулы $v(\theta_n(g)) = \frac{v(\pi)}{q^{n-1}(q-1)}$.

Как мы уже знаем, имеются (топологический) изоморфизм $G_{k^\pi k^{\mathrm{nr}}/k} \xrightarrow{\sim} \varprojlim_U k^\times/U$, где U пробегает открытые подгруппы конечного индекса в $k^\times$ и (непрерывный) сюръективный гомоморфизм $G_{k^{\mathrm{ab}}/k} \twoheadrightarrow G_{k^\pi k^{\mathrm{nr}}/k}$. Чтобы установить равенство $k^{\mathrm{ab}} = k^\pi k^{\mathrm{nr}}$ (но не только для этого!), мы достроим эти два отображения до коммутативного квадрата

$$\begin{array}{ccc}
G_{k^{\mathrm{ab}}/k} & \xrightarrow{\sim} & \varprojlim_{[K:k]<\infty} k^\times/N_{K/k}K^\times \\
\downarrow & & \downarrow\cong \\
G_{k^\pi k^{\mathrm{nr}}/k} & \xrightarrow{\sim} & \varprojlim_U k^\times/U
\end{array}$$

Для этого нужно а) доказать, что любая норменная подгруппа в $k^\times$ открыта и конечного индекса, и наоборот, что любая открытая подгруппа в $k^\times$ конечного индекса содержит норменную подгруппу; б) построить изоморфизм $G^{\mathrm{ab}}_{K/k} \xrightarrow{\sim} k^\times/N_{K/k}K^\times$ для каждого конечного расширения Галуа K/k; в) проверить коммутативность диаграммы.

Начнём с пункта б). Как мы знаем, $G^{\mathrm{ab}}_{K/k} = H_1(G_{K/k}, \mathbb{Z})$. Мы интерпретируем $k^\times/N_{K/k}K^\times$ как некоторую группу когомологий (степени 0), но в несколько модифицированном смысле.

2.4. **Когомологии Тэйта и «абстрактная теория полей классов».** Пусть H – конечная группа и, как и прежде, $\Lambda = \mathbb{Z}[H]$ и $N = \sum_{h\in H} h$.

Определение. Модифицированные когомологии, или когомологии Тэйта, определены следующим образом: $\widehat{H}^q(H, M) := H^q(H, M)$ при $q \geqslant 1$, $\widehat{H}^{-q}(H, M) := H_{q-1}(H, M)$ при $q \geqslant 2$, $\widehat{H}^{-1}(H, M) := \ker N^*$ и $\widehat{H}^0(H, M) := \mathrm{coker} N^* = M^H/M_H$, где $N^* : M_H \longrightarrow M^H$.

Упражнение. а) Докажите, что для любой точной последовательности H-модулей $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ имеется каноническая точная последовательность

$$\ldots \longrightarrow \widehat{H}^{q-1}(H, B) \longrightarrow \widehat{H}^{q-1}(H, C) \longrightarrow \widehat{H}^q(H, A) \longrightarrow \widehat{H}^q(H, B) \longrightarrow \widehat{H}^q(H, C) \longrightarrow \ldots$$

б) Если $\ldots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$ – проективная резольвента и $P_j^* = \mathrm{Hom}(P_j, \mathbb{Z})$, то $\widehat{H}^q(H, M) = H^q(\mathrm{Hom}_H(L, M))$, где L – комплекс $\ldots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow P_0^* \longrightarrow P_1^* \longrightarrow \ldots$

в) Докажите, что для любой конечной группы индуцированные модули совпадают с коиндуцированными, и все их когомологии Тэйта – нулевые.

г) Докажите полную 2-периодичность $\widehat{H}^q(H, M)$ для конечных циклических H.

Для конечной циклической группы H и H-модуля M определим *индекс Эрбрана* равенством $h(M) = |\widehat{H}^0(H, M)|/|\widehat{H}^1(H, M)|$, если обе группы конечны.

Упражнение. а) Докажите, что для любой точной последовательности H-модулей $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ если определены два из трех индексов Эрбрана, то определен и третий, и $h(A)h(C) = h(B)$

б) Докажите, что если H-модуль M конечен, то $h(M) = 1$. (Указание: рассмотрите точные последовательности $0 \longrightarrow M^H \longrightarrow M \xrightarrow{T} M \longrightarrow M_H \longrightarrow 0$ и $0 \longrightarrow \widehat{H}^1(H, M) \longrightarrow M_H \xrightarrow{N^*} M^H \longrightarrow \widehat{H}^0(H, M) \longrightarrow 0$.)

Если расширение K/k сепарабельно и L/k – его нормализация Галуа, то норма $N_{K/k} : H^0(G_{L/K}, L^\times) \longrightarrow H^0(G_{L/k}, L^\times)$ и след $\mathrm{tr}_{K/k} : H^0(G_{L/K}, L) \longrightarrow H^0(G_{L/k}, L)$ – частные случаи трансфера $H^q(H, M) \longrightarrow H^q(G, M)$ для G-модуля M и подгруппы конечного индекса H в G.

Предложение 2.20. *Если H – подгруппа конечного индекса n в G, то* $\mathrm{Cor} \circ \mathrm{Res} = n$.

Следствие 2.21. (1) *Если $|G| = n$, то все $\widehat{H}^q(G, -)$ аннулируются умножением на n.*
(2) *Если G-модуль M конечно порожден, то группа $\widehat{H}^q(G, M)$ конечна.*
(3) *Пусть S – силовская p-подгруппа в G. Тогда ограничение на S индуцирует вложение $\widehat{H}^q(G, M)_{p^\infty} \hookrightarrow \widehat{H}^q(S, M) = \widehat{H}^q(S, M)_{p^\infty}$.*
(4) *Для каждого простого p выберем силовскую p-подгруппу S_p в G. Тогда ограничения на S_p индуцируют вложение $\widehat{H}^q(G, M) \hookrightarrow \prod_p \widehat{H}^q(S_p, M)$.*

Теорема 2.22. *Пусть G – конечная группа. Существует единственное семейство гомоморфизмов $\widehat{H}^p(G, A) \otimes \widehat{H}^q(G, B) \longrightarrow \widehat{H}^{p+q}(G, A \otimes B)$ такое, что 1) они функториальны; 2) при $p = q = 0$ они индуцированы $A^G \otimes B^G \longrightarrow (A \otimes B)^G$; 3) если точны последовательности $0 \longrightarrow A \longrightarrow A' \longrightarrow A'' \longrightarrow 0$ и $0 \longrightarrow A \otimes B \longrightarrow A' \otimes B \longrightarrow A'' \otimes B \longrightarrow 0$, то $(\delta a'') \cdot b = \delta(a'' \cdot b)$ (в*

$\widehat{H}^{p+q+1}(G, A\otimes B))$ *и* $b\cdot(\delta a'') = (-1)^q\delta(b\cdot a'')$ *(в* $\widehat{H}^{p+q+1}(G, B\otimes A))$ *для любых* $a''\in \widehat{H}^p(G, A'')$ *и* $b\in \widehat{H}^q(G, B)$.

Доказательство опирается на конструкцию произведения на уровне полной резольвенты $P_\bullet$ для группы G: $\varphi_{p,q} : P_{p+q} \longrightarrow P_p\otimes P_q$.

Свойства $\cup$-произведения: ассоциативность, (супер)коммутативность, мультипликативность ограничения: $\mathrm{Res}(a\cdot b) = \mathrm{Res}(a)\cdot \mathrm{Res}(a\cdot b)$, формула проекции: $\mathrm{Cor}(a\cdot \mathrm{Res}(b)) = \mathrm{Cor}(a)\cdot b$.

Все, что нам нужно из «абстрактной» теории групп для построения локальной и глобальной теорий полей классов, заключено в следующей теореме.

Теорема 2.23 (Тэйт-Накаяма). *Пусть* G *– конечная группа,* A, B, C *–* G*-модули, и* $A\otimes B \longrightarrow C$ *–* G*-гомоморфизм. Пусть* $\alpha\in \widehat{H}^p(G, A)$*. Тогда для каждого* $q\in\mathbb{Z}$ *и каждой подгруппы* $S\subset G$ $\cup$*-произведение с ограничением* α *на* S *задает гомоморфизм* $\alpha_{q,S} : \widehat{H}^q(S, B) \longrightarrow \widehat{H}^{p+q}(S, C)$.

Предположим, что для некоторого q_0 *отображения* $\alpha_{q_0-1,S}$ *сюрьективны,* $\alpha_{q_0,S}$ *биективны, и* $\alpha_{q_0+1,S}$ *инъективны для всех подгрупп* S*. Тогда* $\alpha_{q,S}$ *биективны для всех* q *и всех* S*.*

Схема доказательства. Сдвигом размерности всё сводится к случаю $p = 0$, в котором $\alpha_{q,S}$ – просто отображение, индуцированное некоторым G-гомоморфизмом $f : B \longrightarrow C$. К C можно добавить когомологически тривиальный модуль, в который вкладывается B, например, $\mathrm{Ind}^G_{\{1\}}B$. Другими словами, можно без потери общности считать f инъекцией.

Рассмотрим тогда последовательность когомологий, ассоциированную с точной последовательностью $0\longrightarrow B \xrightarrow{f} C \longrightarrow D \longrightarrow 0$. Из наших предположений следует, что $\widehat{H}^{q_0-1}(S, D) = \widehat{H}^{q_0}(S, D) = 0$ для всех подгрупп S группы G.

Теперь из теории когомологической тривиальности (теорема 9.4, гл. IV, [АТЧ]) следует, что $\widehat{H}^q(S, D) = 0$ для всех q и всех S, что и требовалось. А именно, как мы видели, все сводится к силовским подгруппам. Далее, с помощью последовательности «ограничения-инфляции» (предложение 1.6), по индукции в циклических башнях, к циклическим группам, для которых всё следует из периодичности с периодом 2 (гл. IV, §9, [АТЧ]). $\square$

Точнее, нам потребуется только следующее следствие из теоремы 2.23.

Теорема 2.24 (Тэйт). *Пусть* G *– конечная группа, и* A *–* G*-модуль такой, что* $H^1(S, A) = 0$ *и* $H^2(S, A)$ *– циклическая порядка* $|S|$ *для любой подгруппы* $S\subseteq G$*. Пусть* ζ *– образующая группы* $H^2(G, A)$*. Тогда* $\cup$*- умножение на* ζ *задаёт изоморфизмы* $\cup\zeta : \widehat{H}^q(G,\mathbb{Z}) \xrightarrow{\sim} \widehat{H}^{q+2}(G, A)$ *для всех целых* q*.*

Доказательство. Пусть в теореме 2.23 $p = 2$, $B = \mathbb{Z}$, $C = A$ и $q_0 = 0$. Надо проверить, что $\widehat{H}^{-1}(S,\mathbb{Z}) \xrightarrow{\cup\zeta} \widehat{H}^1(S, A) = 0$ сюрьективно, $\mathbb{Z}/|S|\mathbb{Z} = \widehat{H}^0(S,\mathbb{Z}) \xrightarrow{\cup\zeta} \widehat{H}^2(S, A)$ биективно, и $0 = \widehat{H}^1(S,\mathbb{Z}) \xrightarrow{\cup\zeta} \widehat{H}^3(S, A)$ инъективно для любой подгруппы S. А это очевидно. $\square$

В случае $q = -2$ получаем $\widehat{H}^{-2}(G,\mathbb{Z}) := H_1(G,\mathbb{Z}) = G/[G, G] =: G^{\mathrm{ab}} \xrightarrow{\sim} \widehat{H}^0(G, A)$.

Таким образом, если построить «согласованную» систему $G_{K/k}$-модулей A_K (в частности, $A_K^{G_{K/k}} = A_k$) для всех конечных расширений Галуа K/k некоторого поля k, удовлетворяющую условиям теоремы Тэйта, то группа Галуа максимального абелева расширения поля k, описывается как обратный предел групп $\widehat{H}^0(G_{K/k}, A_K) = A_K^{G_{K/k}}/N_{K/k}A_K = A_k/N_{K/k}A_K$, т.е. пополнение A_k по «норменным» подгруппам.

Чтобы воспользоваться теоремой Тэйта для описания абелевой группы Галуа локальных и глобальных полей, нам предстоит доказать следующие два утверждения.

Теорема 2.25. *Пусть* $A_K = \begin{cases} k^\times, & \text{если } k \text{ – локальное, в т.ч. } \mathbb{R} \text{ или } \mathbb{C} \\ \text{классы иделей поля } k, & \text{если } k \text{ – глобальное.} \end{cases}$

Тогда $A_K^{G_{K/k}} = A_k$, $H^1(G_{K/k}, A_K) = 0$, *и* $H^2(G_{K/k}, A_K) = \mathbb{Z}/[K:k]\mathbb{Z}$ *– циклическая порядка* $[K:k]$ *для любого конечного расширения Галуа* K/k.

Пока мы знаем только, что $(K^\times)^{G_{K/k}} = k^\times$ (теория Галуа) и $H^1(G_{K/k}, K^\times) = 0$ (теорема 90 Гильберта).

Следствие 2.26. *Для любого конечного расширения Галуа* K/k *имеется изоморфизм* $\cup\zeta_{K/k}$: $\widehat{H}^{-2}(G_{K/k}, \mathbb{Z}) = G_{K/k}^{\mathrm{ab}} \xrightarrow{\sim} \widehat{H}^0(G_{K/k}, A_K) = A_k/N_{K/k}A_K$, *где* $\zeta_{K/k}$ *– образующая* $H^2(G_{K/k}, A_K)$.

В этом месте положено вводить понятие формации (см., например, [АТ, С1, Ск]), но мы этого делать не будем.

3. Группа Брауэра

См. [Б, вдВ, В], резюме: [Ск].

Пусть k – поле, A – конечномерная ассоциативная k-алгебра с единицей.

Упражнение. Докажите, что следующие свойства A эквивалентны.

а) В A нет собственных ($\neq 0, A$) двусторонних идеалов, и центр A равен k.

б) Алгебра $A \otimes_k \overline{k}$ изоморфна алгебре матриц $M_n(\overline{k})$ для некоторого n.

б') Существует конечное расширение K/k такое, что алгебра $A \otimes_k K$ изоморфна алгебре матриц $M_n(K)$ для некоторого n. (Например, в качестве K подходит максимальное подполе тела D из п. в), т.е. такое, что $[D:k] = [K:k]^2$.)

в) $A \cong M_n(D)$ для некоторого n и некоторого тела D с центром, равным k. (А именно, все простые A-модули M изоморфны, $A \hookrightarrow \mathrm{End}_k(M)$, $D := \mathrm{End}_A(M)$ – тело с центром, равным k, откуда $A \xrightarrow{\sim} \mathrm{End}_D(M)$. (Веддербёрн).)

Определение. 1. Алгебра A, удовлетворяющая условиям упражнения называется *центральной простой* k-алгеброй.

2. Две центральные простые k-алгебры *эквивалентны*, если тела из п. в) упражнения изоморфны как k-алгебры. (Равносильное условие: $A \sim A'$, если $A \otimes_k M_n(k) \cong A' \otimes_k M_{n'}(k)$ для некоторых n и n'.)

3. $\mathrm{Br}(k) := \left\{ \begin{array}{c} \text{классы эквивалентности} \\ \text{конечномерных центральных} \\ \text{простых } k\text{-алгебр} \end{array} \right\} = \left\{ \begin{array}{c} \text{классы } k\text{-изоморфизма} \\ \text{конечномерных центральных} \\ k\text{-алгебр с делением} \end{array} \right\}.$

Упражнение. Докажите, что $A \otimes_k A'$ – центральная простая k-алгебра для любых двух центральных простых k-алгебр A и A'.

Таким образом, $\otimes_k$ определяет некоторую коммутативную и ассоциативную операцию на $\mathrm{Br}(k)$, относительно которой k является нулём. Пусть A^{op} – k-алгебра, противоположная A, т.е. – то же k-векторное пространство, что и A, но с умножением в обратном порядке: $x \overset{\mathrm{op}}{\cdot} y := y \cdot x$.

Упражнение. Докажите, что $A \otimes_k A^{\mathrm{op}} = M_{\dim A}(k)$, т.е. $[A] + [A^{\mathrm{op}}] = 0$ в $\mathrm{Br}(k)$, т.е. $\mathrm{Br}(k)$ – коммутативная группа.

Ковариантность. Упражнение. Докажите, что для любого расширения K/k тензорное умножение $\otimes_k K$ индуцирует гомоморфизм $\otimes_k K : \mathrm{Br}(k) \longrightarrow \mathrm{Br}(K)$.

Обозначение. $\mathrm{Br}(K/k) := \ker(\otimes_k K)$.

Как мы знаем из упражнения б'), $\mathrm{Br}(k) = \bigcup_{K/k} \mathrm{Br}(K/k)$, где K/k пробегает конечные расширения Галуа. В частности, $\mathrm{Br}(k) = 0$, если k сепарабельно замкнуто.

Теорема 3.1 (Сколем-Нётер). *Любой k-изоморфизм между двумя изоморфными простыми k-подалгебрами центральной простой k-алгебры A индуцирован внутренним автоморфизмом A.*

Следствие 3.2. *Если K/k – расширение Галуа, то*

$$\mathrm{Br}(K/k) = H^2_{Sm}(G_{K/k}, K^\times) = H^1_{Sm}(G_{K/k}, \mathrm{PGL}K).$$

В частности, $\mathrm{Br}(k) = H^2_{Sm}(G_{k_{\mathrm{sep}}/k}, k^\times_{\mathrm{sep}}) = H^1_{Sm}(G_{k_{\mathrm{sep}}/k}, \mathrm{PGL}k_{\mathrm{sep}})$.

Доказательство. Пусть A – центральная простая k-алгебра, и K/k – конечное расщепляющее расширение Галуа, то есть такое, что существует изоморфизм K-алгебр $\varphi : A \otimes_k K \xrightarrow{\sim} M_n(K)$. Согласно теореме Сколема-Нётер, автоморфизмы K-алгебры $M_n(K)$ – внутренние, т.е. $\mathrm{Aut}_K(M_n(K)) = \mathrm{GL}_n K/\text{центр} = \mathrm{PGL}_n K$. Сопоставим алгебре A 1-коцикл $(g \mapsto (m \mapsto \varphi(g\varphi^{-1}(m)))$ на $G_{K/k}$, значениями которого будем считать $G_{K/k}$-группу $\mathrm{PGL}_n K$.

Это задаёт биекцию $\mathrm{Br}(K/k)_n := \{A \mid A \otimes_k K \cong M_n(K)\} \xrightarrow{\sim} H^1_{Sm}(G_{K/k}, \mathrm{PGL}_n K)$.

Связывающий гомоморфизм точной последовательности когомологий короткой точной последовательности $G_{K/k}$-групп $1 \longrightarrow K^\times \longrightarrow \mathrm{GL}_n K \longrightarrow \mathrm{PGL}_n K \longrightarrow 1$ задаёт инъективное, по теореме 90 (упражнение!) отображение $H^1_{Sm}(G_{K/k}, \mathrm{PGL}_n K) \longrightarrow H^2_{Sm}(G_{K/k}, K^\times)$, $(a_g) \mapsto (g\tilde{a}_h \cdot \tilde{a}^{-1}_{gh} \cdot \tilde{a}_g)$, где $\tilde{a}_g$ обозначает произвольный подъём элемента a_g в группу $\mathrm{GL}_n K$.

Пусть $\delta_n : \mathrm{Br}(K/k)_n \xrightarrow{\sim} H^1_{Sm}(G_{K/k}, \mathrm{PGL}_n K) \longrightarrow H^2_{Sm}(G_{K/k}, K^\times)$ – композиция. Нетрудно проверить, что $\delta_{nn'}(A \otimes_k A') = \delta_n(A) + \delta_{n'}(A')$.

Обратно, по 2-коциклу $(c_{g,h}) \in Z^2(G_{K/k}, K^\times)$ строится центральная простая k-алгебра, определяемая как k-векторное пространство $K[G_{K/k}]$ с естественным правилом коммутирования элементов группы $G_{K/k}$ и поля K, следующим умножением элементов группы $G_{K/k}$: $[g] \cdot [h] = c_{g,h}[gh]$. Ассоциативность умножения эквивалентна условию 2-коцикла: $c_{g_1,g_2} \cdot c_{g_1g_2,g_3} = g_1 c_{g_2,g_3} \cdot c_{g_1,g_2g_3}$.

Пример. $\mathrm{Br}(\mathbb{R}) = H^2(G_{\mathbb{C}/\mathbb{R}}, \mathbb{C}^\times)$. В силу 2-периодичности, $\mathrm{Br}(\mathbb{R}) = \widehat{H}^0(G_{\mathbb{C}/\mathbb{R}}, \mathbb{C}^\times)$, и значит, $\mathrm{Br}(\mathbb{R}) = \mathbb{R}^\times/N_{\mathbb{C}/\mathbb{R}}\mathbb{C}^\times = \{\pm 1\}$. Ненулевой элемент соответствует алгебре кватернионов. Как объясняется в следующем упражнении, он также соответствует конике $x^2 + y^2 + z^2 = 0$ на проективной плоскости.

Упражнение. Многообразием Севери–Брауэра над k называется такое V, которое над замыканием k становится изоморфным проективному пространству: $V \times_k \overline{k} \cong \mathbb{P}^n_{\overline{k}}$.

Докажите, что а) n-мерные многообразия Севери–Брауэра над k взаимнооднозначно соответствуют элементам $\mathrm{Br}(K/k)_n \xrightarrow{\sim} H^1_{Sm}(G_{k_{\mathrm{sep}}/k}, \mathrm{PGL}_{n+1}k_{\mathrm{sep}})$;

б) (Шатле) многообразие Севери–Брауэра над k тривиально, т.е. изоморфно проективному пространству, тогда и только тогда, когда имеет точку, рациональную над k. (Это следует из теоремы 90.)

Пример. Если на неособой конике, т.е. гладкой кривой второй степени на проективной плоскости, имеется точка, то коника биективно проектируется из неё на проективную прямую.

3.1. **Группа Брауэра локального поля.**

Теорема 3.3. *Любая центральная простая алгебра над локальным полем k расщепляется над некоторым его неразветвлённым расширением. И значит,*
$$\mathrm{Br}(k) = \mathrm{Br}(k_{\mathrm{nr}}/k) = H^2_{Sm}(G_{k_{\mathrm{nr}}/k}, k_{\mathrm{nr}}^\times) = H^2_{Sm}(\widehat{\mathbb{Z}}, k_{\mathrm{nr}}^\times).$$

Замечание. Аналогичное (но не идентичное) утверждение верно и для глобальных полей.

Доказательство. Пусть D – центральная k-алгебра с делением ранга n, т.е. $[D:k]=n^2$.

Упражнение. Существует единственное продолжение дискретного нормирования поля k на D. А именно, некоторый множитель $v(N_{D/k}(-))$. (Например, это верно для любого подполя в D. Осталось проверить согласованность.)

Тело D полно относительно дискретного нормирования. Как обычно, обозначим через $\mathcal{O}_D := \{a \in D \mid v(a) \geqslant 0\}$ кольцо целых, а через $\mathfrak{m}_D := \{a \in D \mid v(a) > 0\}$ – максимальный идеал кольца целых. Ясно, что $\mathcal{O}_k$-модуль $\mathcal{O}_D$ изоморфен $\mathcal{O}_k^{n^2}$, и значит, $\dim_\varkappa(\mathcal{O}_D/\mathfrak{m}_k\mathcal{O}_D) = n^2 = ef$, где, как обычно, e – индекс ветвления, и $f = \dim_\varkappa(\mathcal{O}_D/\mathfrak{m}_D)$ – степень инерции.

$e \leqslant n$, так как униформизующая π_D, т.е. такой элемент $\mathfrak{m}_D$, на котором дискретное нормирование достигает минимума $1/e$, порождает над k подполе степени e, а как мы знаем, степень над k любого подполя в D не превосходит n.

$f \leqslant n$, так как $\mathcal{O}_D/\mathfrak{m}_D$ – поле, как и все конечные тела, и значит, порождено над $\varkappa$ некоторым элементом $\overline{\alpha}$. Поднимем $\overline{\alpha}$ до некоторого элемента $\alpha \in D$. Расширение $k(\alpha)/k$ неразветвлено, и его степень равна f, а как мы знаем, степень над k любого подполя в D не превосходит n.

Таким образом, $e \leqslant n$ и $f \leqslant n$, поэтому из равенства $n^2 = ef$, следует, что $e = f = n$.

Поскольку $k(\alpha)/k$ – неразветвлённое расширение в D максимальной степени n, алгебра D над ним расщепляется. $\square$

Теорема 3.4. *Дискретное нормирование $v : k_{\mathrm{nr}}^\times \longrightarrow \mathbb{Z}$ индуцирует изоморфизм*
$$H^2_{Sm}(G_{k_{\mathrm{nr}}/k}, k_{\mathrm{nr}}^\times) \xrightarrow{\sim} H^2_{Sm}(G_{k_{\mathrm{nr}}/k}, \mathbb{Z}).$$

Замечание. Как мы знаем, имеется канонический изоморфизм $G_{k_{\mathrm{nr}}/k} \xrightarrow{\sim} \widehat{\mathbb{Z}}$, переводящий в 1 автоморфизм Фробениуса Frob_q. Поэтому из точной последовательности тривиальных $G_{k_{\mathrm{nr}}/k}$-модулей $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$ получаем, с учётом ацикличности однозначно делимого модуля $\mathbb{Q}$, изоморфизм $H^1_{Sm}(G_{k_{\mathrm{nr}}/k}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{Sm}(G_{k_{\mathrm{nr}}/k}, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z} \xrightarrow{\sim} H^2_{Sm}(G_{k_{\mathrm{nr}}/k}, \mathbb{Z})$.

Доказательство. Выбор униформизующей π поля k задаёт изоморфизм $G_{k_{\mathrm{nr}}/k}$-модулей $\mathbb{Z} \times \mathcal{O}_{\mathrm{nr}}^\times \xrightarrow{\sim} k_{\mathrm{nr}}^\times$, $(m,a) \mapsto \pi^m a$. Поэтому достаточно доказать ацикличность $\mathcal{O}_{\mathrm{nr}}^\times$.

Модуль $\mathcal{O}_{\mathrm{nr}}^\times$ фильтрован: $\mathcal{O}_{\mathrm{nr}}^\times \supset (1+\mathfrak{p}_{\mathrm{nr}}) \supset (1+\mathfrak{p}_{\mathrm{nr}}^2) \supset \dots$, с факторами $\overline{\varkappa}^\times = \mathcal{O}_{\mathrm{nr}}^\times/(1+\mathfrak{p}_{\mathrm{nr}})$ и $(1+\mathfrak{p}_{\mathrm{nr}}^i)/(1+\mathfrak{p}_{\mathrm{nr}}^{i+1}) \xrightarrow{\sim} \overline{\varkappa}$, $x \mapsto \frac{x-1}{\pi^i} \bmod \mathfrak{p}_{\mathrm{nr}}$.

Ясно, что $\widehat{H}^0(G_{\varkappa_n/\varkappa}, \varkappa_n^\times) = 0$, где $\varkappa_n$ – расширение степени n конечного поля $\varkappa$. Из теоремы 90 и 2-периодичности когомологий циклических групп следует, что $\widehat{H}^*(G_{\varkappa_n/\varkappa}, \varkappa_n^\times) = 0$, и следовательно, $H^{>0}_{Sm}(G_{k_{\mathrm{nr}}/k}, \overline{\varkappa}^\times) = \varinjlim \widehat{H}^{>0}(G_{\varkappa_n/\varkappa}, \varkappa_n^\times) = 0$.

Что $H^{>0}_{Sm}(G_{k_{\mathrm{nr}}/k}, \overline{\varkappa}) = \varinjlim \widehat{H}^{>0}(G_{\varkappa_n/\varkappa}, \varkappa_n) = 0$, мы уже знаем.

Осталось проверить, что (Упражнение) если M – G-модуль, и (M^i) – убывающая фильтрация такая, что $M \xrightarrow{\sim} \varprojlim M/M^i$ и $\widehat{H}^*(G, M^i/M^{i+1}) = 0$, то $\widehat{H}^*(G,M) = 0$. $\square$

Вывод: построили изоморфизм $\mathrm{inv}_k : \mathrm{Br}(k) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ для любого локального неархимедова поля k.

Опишем этот изоморфизм явно. Пусть D – центральная k-алгебра с делением ранга r, т.е. $\dim_k D = r^2$. Как мы знаем, она содержит расщепляющее поле L, неразветвлённое над k. Из теоремы Сколема–Нётер следует, что все такие L сопряжены, а также все автоморфизмы L/k индуцированы внутренними автоморфизмами D, т.е. существует $\gamma \in D^\times$ такой, что $\gamma L \gamma^{-1} = L$ и $\mathrm{ad}(\gamma)|_L = \mathrm{Frob}_q$. Поскольку $[L:k] = r$, Frob_q^r – тождественный автоморфизм L/k, т.е. γ^r коммутирует с элементами L. Из максимальности подполя L следует, что $\gamma^r =: c \in L^\times$. Такой элемент γ определён однозначно с точностью до домножения на элемент $L^\times$. Поэтому образ элемента $v(\gamma)$ в $\frac{1}{r}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$ не зависит от выбора γ, где $v(\gamma) = \frac{1}{r}v(\gamma^r) = \frac{1}{r}v(c) = \frac{i}{r}$, если $c = \pi^i u$ для некоторой единицы $u \in \mathcal{O}_L^\times$.

Обратно, построим по элементу $\frac{i}{r} \in \mathbb{Q}/\mathbb{Z}$ центральную k-алгебру с делением ранга r. Пусть L – неразветвлённое расширение поля k степени r. Рассмотрим левое L-векторное пространство с базисом $1, T, T^2, \ldots, T^{r-1}$. Пусть элемент T действует на базисе по формуле $T^i \mapsto T^{i+1}$ при $0 \leqslant i \leqslant r-2$, и $T^{r-1} \mapsto \pi^i \cdot 1$ (π – униформизующая поля k), и действует на поле L как Frob_q. Тогда это L-векторное пространство станет центральной k-алгеброй с делением ранга r, с инвариантом $\frac{i}{r} \in \mathbb{Q}/\mathbb{Z}$.

Следствие 3.5. *Если K/k – конечное расширение степени n локальных полей, то диаграмма*

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Br}(K/k) & \longrightarrow & \mathrm{Br}(k) & \xrightarrow{\otimes_k K} & \mathrm{Br}(K) \\
 & & \| & & \|\mathrm{inv}_k & & \|\mathrm{inv}_K \\
0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\times n} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

коммутативна. В частности, $\alpha \in \mathrm{Br}(K/k)$ тогда и только тогда, когда $n \cdot \alpha = 0$. □

3.2. **Локальная теория полей классов.** Таким образом, по теореме Тэйта, $\cup\zeta_{K/k} : G_{K/k}^{\mathrm{ab}} \xrightarrow{\sim} k^\times/N_{K/k}K^\times$ для любого конечного расширения Галуа K/k, где $\zeta_{K/k} = \frac{1}{[K:k]}$ – образующая группы $\mathrm{Br}(K/k) = \frac{1}{[K:k]}\mathbb{Z}/\mathbb{Z}$.

Обратный изоморфизм называется гомоморфизмом взаимности, и обозначается $(\ , K/k) : k^\times \longrightarrow G_{K/k}^{\mathrm{ab}}$. Его ядро совпадает с $N_{K/k}K^\times$, поэтому он называется также символом норменного вычета.

Осталось понять, как они связаны между собой и с отображением $\rho : k^\times \hookrightarrow G_{k_\pi k^{\mathrm{nr}}/k}$. Для этого воспользуемся следующим фактом.

Предложение 3.6. *Пусть $\chi \in \mathrm{Hom}(G_{K/k}, \mathbb{Q}/\mathbb{Z})$, $\delta\chi \in H^2(G_{K/k}, \mathbb{Z})$ – образ χ относительно связывающего гомоморфизма последовательности $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$, $a \in k^\times$, $\overline{a} \in \widehat{H}^0(G_{K/k}, K^\times) = k^\times/N_{K/k}K^\times$ – образ a. Тогда $\chi((a, K/k)) = \mathrm{inv}_k(\overline{a} \cdot \delta\chi)$.*

Доказательство. Положим $s_a = (a, K/k)$; если $s \in G_{K/k}$, пусть $\overline{s} \in G_{K/k}^{\mathrm{ab}}$ обозначает образ s. По определению изоморфизма норменного вычета, $\zeta_{K/k} \cdot \overline{s_a} = \overline{a} \in \widehat{H}^0(G_{K/k}, K^\times)$. Из ассоциативности $\cup$-умножения $\overline{a} \cdot \delta\chi = \zeta_{K/k} \cdot (\overline{s_a} \cdot \delta\chi)$, где $\overline{s_a} \cdot \delta\chi \in \widehat{H}^0(G_{K/k}, \mathbb{Z})$. По одному из основных свойств $\cup$-умножения, $\overline{s_a} \cdot \delta\chi = \delta(\overline{s_a} \cdot \chi)$, где $\overline{s_a} \cdot \chi \in \widehat{H}^{-1}(G_{K/k}, \mathbb{Q}/\mathbb{Z}) = \ker(\mathbb{Q}/\mathbb{Z} \xrightarrow{\times n} \mathbb{Q}/\mathbb{Z}) = \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, если $[K:k] = n$.

Упражнение. Докажите, что $\overline{s_a} \cdot \chi = \chi(\overline{s_a}) = \frac{r}{n}$ для некоторого $r \in \mathbb{Z}$.

Ясно, что $\delta(\frac{r}{n}) = r \in \mathbb{Z}/n\mathbb{Z} = \widehat{H}^0(G_{K/k}, \mathbb{Z})$. Откуда $\zeta_{K/k} \cdot (\overline{s_a} \cdot \delta\chi) = r \cdot \zeta_{K/k}$, и значит, $\mathrm{inv}_k(\zeta_{K/k} \cdot (\overline{s_a} \cdot \delta\chi)) = \frac{r}{n} = \chi(s_a)$. □

Следствие 3.7. *Пусть $L \supset K \supset k$ – конечные расширения, и L/k, K/k – расширения Галуа. Тогда диаграмма*

$$\begin{array}{ccc}
G_{L/k}^{\mathrm{ab}} & \xrightarrow{\cup\zeta_{L/k}} & \widehat{H}^0(G_{L/k}, L^\times) = k^\times/N_{L/k}L^\times \\
\downarrow & & \downarrow \\
G_{K/k}^{\mathrm{ab}} & \xrightarrow{\cup\zeta_{K/k}} & \widehat{H}^0(G_{K/k}, K^\times) = k^\times/N_{K/k}K^\times
\end{array}$$

коммутативна. В частности, определён символ $(\ ,k^{\mathrm{ab}}/k) : k^\times \hookrightarrow G_{k^{\mathrm{ab}}/k}$, *который становится изоморфизмом после пополнения* $k^\times$ *по норменным подгруппам.*

Доказательство. Пусть $\chi \in \mathrm{Hom}(G_{K/k}, \mathbb{Q}/\mathbb{Z}) \subseteq \mathrm{Hom}(G_{L/k}, \mathbb{Q}/\mathbb{Z})$. Как следует из предложения 3.6, $\chi((a, L/k)) = \mathrm{inv}_k(\overline{a} \cdot \delta\chi) = \chi((a, K/k))$, что и требовалось. $\square$

Перейдём теперь к связи с $\rho : k^\times \hookrightarrow G_{k_\pi k^{\mathrm{nr}}/k}$.

Заметим, что π – норма из k_π^n для любого n: $\pi = N_{k_\pi^n/k}(-\theta_n(g))$, т.е. $(\pi, k_\pi^n/k) = 1$ для любого n, и значит, $(\pi, k_\pi/k) = 1$. Таким образом, $(\pi, k_\pi/k) = \rho(\pi)|_{k_\pi} = 1$.

Лемма 3.8. *Если* K/k *неразветвлено, то* $(a, K/k) = \mathrm{Frob}_q^{v(a)}$ *для любого* $a \in k^\times$.

Доказательство. Нужно проверить, что $\chi((a, L/k)) = \chi(\mathrm{Frob}_q) \cdot v(a)$ для любого характера $\chi \in \mathrm{Hom}(G_{K/k}, \mathbb{Q}/\mathbb{Z})$. Слева стоит $\mathrm{inv}_k(\overline{a} \cdot \delta\chi)$. Вспомним определение inv_k. Это – композиция $H^2(G_{K/k}, K^\times) \xrightarrow{v} H^2(G_{K/k}, \mathbb{Z}) \xrightarrow{\sim} H^1(G_{K/k}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$, $(\overline{a} \cdot \delta\chi \mapsto v(a) \cdot \delta\chi \mapsto v(a) \cdot \chi \mapsto v(a) \cdot \chi(\mathrm{Frob}_q)$. $\square$

Таким образом, $(\pi, k^{\mathrm{nr}}/k) = \mathrm{Frob}_q = \rho(\pi)|_{k^{\mathrm{nr}}}$, и значит, $(\pi, k_\pi k^{\mathrm{nr}}/k) = \rho(\pi)$. Поскольку $k_\pi k^{\mathrm{nr}}$ не зависит от π, и все π порождают $k^\times$, получаем $\rho = (\ , k_\pi k^{\mathrm{nr}}/k)$.

Осталось сравнить норменные подгруппы и открытые подгруппы конечного индекса в $k^\times$.

Норменные подгруппы открыты и конечного индекса в $k^\times$, т.к. $N_{K/k} : K^\times \longrightarrow k^\times$ непрерывно и собственно: $N_{K/k}^{-1}(\mathcal{O}_k^\times) = \mathcal{O}_K^\times$, и $k^\times/N_{K/k}K^\times \cong G_{K/k}^{\mathrm{ab}}$ для любого расширения Галуа K/k.

Открытая подгруппа конечного индекса в $k^\times$ содержит $\langle \pi^m, 1{+}\mathfrak{p}^n \rangle$ для некоторых натуральных m и n. Как мы знаем, $\rho : k^\times/\langle \pi^m, 1+\mathfrak{p}^n \rangle \xrightarrow{\sim} G_{k_\pi^n k_m^{\mathrm{nr}}/k}$. Из равенства $\rho = (\ , k_\pi k^{\mathrm{nr}}/k)$ следует, что $\langle \pi^m, 1+\mathfrak{p}^n \rangle = N_{k_\pi^n k_m^{\mathrm{nr}}/k}(k_\pi^n k_m^{\mathrm{nr}})^\times$.

Вывод: $k_\pi k^{\mathrm{nr}} = k^{\mathrm{ab}}$ и $\rho = (\ , k^{\mathrm{ab}}/k)$.

Из формулы проекции $\mathrm{Cor}(a \cdot \mathrm{Res}(b)) = \mathrm{Cor}(a) \cdot b$ следует коммутативность диаграммы

$$(2) \qquad \begin{array}{ccc} K^\times & \xrightarrow{N_{K/k}} & k^\times \\ \downarrow \rho & & \downarrow \rho \\ G_{K^{\mathrm{ab}}/K} & \xrightarrow{|_{k^{\mathrm{ab}}}} & G_{k^{\mathrm{ab}}/k} \end{array} \quad = \quad \begin{array}{ccc} \widehat{H}^0(G_{L/K}, L^\times) & \xrightarrow{\mathrm{Cor}} & \widehat{H}^0(G_{L/k}, L^\times) \\ \uparrow \cup\zeta_{L/K} & & \uparrow \cup\zeta_{L/k} \\ \widehat{H}^{-2}(G_{L/K}, \mathbb{Z}) & \xrightarrow{\mathrm{Cor}} & \widehat{H}^{-2}(G_{L/k}, \mathbb{Z}) \end{array}$$

Другими словами, $(\alpha, L/K) = (N_{K/k}\alpha, L/k)$ для любого $\alpha \in K^\times$.

Упражнение. Для подгруппы H конечного индекса в G определим гомоморфизм переноса, или трансфер, $\mathrm{Ver} : G^{\mathrm{ab}} \longrightarrow H^{\mathrm{ab}}$ формулой $g \mapsto \prod_{t \in H\backslash G} \theta(t) g \theta(tg)^{-1}$, где θ – любое сечение проекции $G \longrightarrow H\backslash G$. Докажите, что коммутативна следующая диаграмма

$$\begin{array}{ccc} k^\times & \xrightarrow{\rho} & G_{k^{\mathrm{ab}}/k} \\ \bigcap & & \downarrow \mathrm{Ver} \cdot \nu \\ K^\times & \xrightarrow{\rho} & G_{K^{\mathrm{ab}}/K}, \end{array} \qquad \text{где } \nu \text{ – множитель несепарабельности.}$$

3.3. **Локальная двойственность и p-расширения локальных полей,** [С-КГ]. Приведём некоторые важные сведения о когомологиях локальных полей, на обсуждение которых не хватило времени.

Теорема 3.9 (Тэйт). *Для любого гладкого* $G_{k^{\mathrm{sep}}/k}$*-модуля* M $H_{Sm}^j(G_{k^{\mathrm{sep}}/k}, M) = 0$ *при* $j \geqslant 3$.

Доказательство. Как видно из спектральной последовательности Серра–Хохшильда $E_2^{a,b} = H_{Sm}^a(G/H, H_{Sm}^b(H, M)) \Rightarrow H_{Sm}^{a+b}(G, M)$ для любого гладкого G-модуля M и любой нормальной замкнутой подгруппы H, задача сводится к следующим двум вопросам: $H^j_{Sm}(G_{k^{\mathrm{sep}}/k^{\mathrm{nr}}}, A) = 0$ и $H^j_{Sm}(G_{k^{\mathrm{nr}}/k}, B) = 0$ при $j \geqslant 2$ для любого гладкого $G_{k^{\mathrm{sep}}/k^{\mathrm{nr}}}$-модуля A и для любого гладкого $G_{k^{\mathrm{nr}}/k}$-модуля B.

Теорема 3.10 (Тэйт). *Для любого конечного гладкого $G_{k^{\mathrm{sep}}/k}$-модуля M положим $M^\vee := \mathrm{Hom}_{\mathbb{Z}}(M, k^\times_{\mathrm{sep}}) = \mathrm{Hom}_{\mathbb{Z}}(M, \mu_\infty)$. Тогда $\cup$-умножение $H^j_{Sm}(G_{k^{\mathrm{sep}}/k}, M) \times H^{2-j}_{Sm}(G_{k^{\mathrm{sep}}/k}, M^\vee) \longrightarrow H^2_{Sm}(G_{k^{\mathrm{sep}}/k}, \mu_\infty) \longrightarrow H^2_{Sm}(G_{k^{\mathrm{sep}}/k}, k^\times_{\mathrm{sep}}) = \mathrm{Br}(k) = \mathbb{Q}/\mathbb{Z}$ невырождено при любом j.*

Теорема 3.11. *Пусть k – p-адическое поле, и $G(p)$ – максимальный про-p-фактор группы $G_{\overline{k}/k}$. Тогда $G(p)$ – свободная про-p-группа ранга $[k : \mathbb{Q}_p] + 1$, если $\mu_p \not\subset k$;*
– про-p-группа Пуанкаре размерности 2 и ранга $[k : \mathbb{Q}_p] + 2$, если $\mu_p \subset k$.

Если k содержит корень из единицы степени p, то из последовательности Куммера $1 \longrightarrow \mu_p \longrightarrow k^\times_{\text{pro-}p} \longrightarrow k^\times_{\text{pro-}p} \longrightarrow 1$, где $k_{\text{pro-}p}$ – максимальное про-p-расширение поля k, получается изоморфизм $H^1_{Sm}(G(p), \mathbb{F}_p) \cong k^\times/k^{\times p}$.

Упражнение. а) Докажите, что $(k^\times : k^{\times n}) = |k^\times_n| \frac{n}{|n|_k}$, где $k^\times_n$ – группа корней из единицы степени, делящей n, в k.

б) Выведите из этого, что ранг группы $G(p)$ равен $[k : \mathbb{Q}_p] + 2$, если k содержит корень из единицы степени p.

4. Символы норменного и степенного вычета

Пусть $k \neq \mathbb{C}$ – локальное поле, и $w = |k^\times_{\mathrm{tors}}|$ – число корней из единицы в нём. Если k неархимедово, пусть p – характеристика его поля вычетов $\varkappa$ и $q = |\varkappa|$. Тогда $w = (q-1)p^c$ для некоторого $c \geqslant 0$. Предполагаем, что $n|w$ и $\mathrm{char}(k) \not| n$.

Мы хотим изучить символ $(\ , K/k)$ для куммеровых расширений степени n.

Положим $(a, b)_n := \frac{\sigma \sqrt[n]{b}}{\sqrt[n]{b}}$, где $\sigma = (a, k(\sqrt[n]{b})/k)$ для всех $a, b \in k^\times$.

Замечание. Если $k(\sqrt[n]{b})/k$ неразветвлено, то $(\pi, b)_n = 1$ тогда и только тогда, когда $b \in k^{\times n}$, т.е. $(\pi,\ )_n$ – символ степенного вычета.

Свойства символа $(a, b)_n$.

(1) $(a, b)_n = 1$ тогда и только тогда, когда a – норма из $k(\sqrt[n]{b})$. Это следует из изоморфизма взаимности. (Замечание. При $n = 2$ это эквивалентно тому, что уравнение $ax^2 + by^2 = 1$ имеет решение в k.)

(2) $(k^\times, a)_n = 1$ тогда и только тогда, когда $a \in k^{\times n}$ (т.к. $\sqrt[n]{a} \in (k^\times_{\mathrm{ab}})^{G_{k_{\mathrm{ab}}/k}}$).

(3) $(aa', b)_n = (a, b)_n \cdot (a', b)_n$ и $(a, bb')_n = (a, b)_n \cdot (a, b')_n$ для любых $a, a', b, b' \in k^\times$.

(4) Соотношения Стейнберга: $(-a, a)_n = (1 - a, a)_n = 1$. *Доказательство.* Из тождества $x^n - a = \prod_{b^n = a} (x - b)$ видно, что $-a$ (при $x = 0$) и $1 - a$ (при $x = 1$) – нормы из $k(\sqrt[n]{a})$. □

(5) $(a, b)_n \cdot (b, a)_n = 1$. *Доказательство.* $(a, b)_n \cdot (b, a)_n = (a, b)_n(-b, b)_n(-a, a)_n \cdot (b, a)_n = (-ab, b)_n(-ab, a)_n = (-ab, ba)_n = 1$. □

(6) $(a, b)_m = (a, b)_n^{n/m}$, если $m|n$, и $(a, b)_w = (a, b)^\alpha_{p^c} \cdot (a, b)^\beta_{q-1}$, если $\alpha(q-1) + \beta p^c = 1$.

(7) $(a, b)_{q-1} \equiv (-1)^{v(a)v(b)} a^{-v(b)} b^{v(a)} \bmod \mathfrak{p}$. *Доказательство.* Из мультипликативности $(a, b)_{q-1} = (a, \pi^{v(b)})_{q-1}(a, \frac{b}{\pi^{v(b)}})_{q-1} = (\pi^{v(a)}, \pi^{v(b)})_{q-1}(\frac{a}{\pi^{v(a)}}, \pi^{v(b)})_{q-1}(a, \frac{b}{\pi^{v(b)}})_{q-1} =$ $= (\pi, -1)^{v(a)v(b)}(\pi, \frac{a}{\pi^{v(a)}})^{-v(b)}_{q-1}(a, \frac{b}{\pi^{v(b)}})_{q-1}$. Поскольку расширения $k(\sqrt[q-1]{a})/k$ и $k(\sqrt[q-1]{b})/k$ неразветвлены, $(c,\ )_{q-1} = \mathrm{Frob}_q^{v(c)}$, и значит, $(\pi, -1)^{v(a)v(b)}(\pi, \frac{a}{\pi^{v(a)}})^{-v(b)}_{q-1}(a, \frac{b}{\pi^{v(b)}})_{q-1} \equiv (-1)^{v(a)v(b)} a^{-v(b)} b^{v(a)} \bmod \mathfrak{p}$. □

(8) Формула сложения: $(a, b)_n = (a, a + b)_n \cdot (a + b, b)_n \cdot (-1, a + b)_n$. *Доказательство.* Правая часть равна $(a + b, -b/a)_n = (a, -b/a)_n = (a, b)_n$. □

(9) Упражнение. Функция $(\ ,\ )_n : k^\times \times k^\times \longrightarrow \mu_n$ непрерывна.

Тут можно было бы взять произвольное поле k, и определить $K_2(k) := (k^\times \otimes k^\times)/\langle a \otimes (1-a) \mid a \in k^\times \setminus \{1\}\rangle$ (свойства 3 и 4).

Поскольку n-ые степени наших символов равны 1, нас интересует $K_2(k)/nK_2(k)$. Как мы знаем из теории Куммера, $k^\times/k^{\times n} \xrightarrow{\sim} H^1_{Sm}(G_{k^{\mathrm{sep}}/k}, \mu_n)$. Поэтому $\cup$-умножение когомологий задаёт гомоморфизм $(k^\times \otimes k^\times)/n \longrightarrow H^2_{Sm}(G_{k^{\mathrm{sep}}/k}, \mu_n^{\otimes 2})$. Басс и Тэйт в некоторых важных частных случаях, а также Меркурьев и Суслин – в общем случае доказали, что он индуцирует изоморфизм $K_2(k)/nK_2(k) = H^2_{Sm}(G_{k^{\mathrm{sep}}/k}, \mu_n^{\otimes 2})$.

4.1. **Явные формулы для символа норменного вычета некоторых круговых расширений.** Если $k = \mathbb{R}$ и $a, b \in \mathbb{R}^\times$, то $(a,b)_2 = (-1)^{\frac{\mathrm{sgn}(a)-1}{2}\frac{\mathrm{sgn}(b)-1}{2}}$.

Теорема 4.1. *Пусть $a, b \in \mathbb{Z}_2^\times$. Тогда $(2,a)_2 = (-1)^{\frac{a^2-1}{8}}$ и $(a,b)_2 = (b,a)_2 = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$.*

Доказательство. Нетрудно проверить (би)мультипликативность этих формул. Из непрерывности следует, что их достаточно проверить для топологического базиса $2, -1, 5$ группы $\mathbb{Q}_2^\times$. Заметим, что $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ неразветвлено. Тогда $(-1,2)_2 = 1$, т.к. $-1 = N(1+\sqrt{2})$; $(2,5)_2 = -1$, т.к. 2 действует на $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ автоморфизмом Фробениуса Frob_4; $(-1,5)_2 = 1$, т.к. $-1 = N(2+\sqrt{5})$ – норма, как и все единицы!; $(5,5)_2 = 1$ по той же причине: $5 = N(5+2\sqrt{5})$; и $(-1,-1)_2 = -1$, т.к. иначе $-1 \equiv x^2 + y^2 \bmod 4$.

Теперь p – нечётное простое, и $k = \mathbb{Q}_p(\zeta)$, где $\zeta = \zeta_p$, и $\pi = 1 - \zeta$. Таким образом, $[k : \mathbb{Q}_p] = p-1$. Поскольку $\frac{p}{\pi^{p-1}} = \prod_{j=2}^{p-1} \frac{1-\zeta^j}{1-\zeta} \equiv (p-1)! \equiv -1 \bmod \pi$, $(p) = (\pi)^{p-1}$, и расширение $k/\mathbb{Q}_p(\zeta)$ вполне разветвлено.

Положим $\eta_j = 1 - \pi^j$ при $j \geqslant 1$.

Лемма 4.2. *$\{\eta_j\}$ порождают топологическую группу $1+\mathfrak{p}$. $\{\eta_j, \zeta_{p-1}, \pi\}$ порождают топологическую группу $k^\times$.*

Доказательство. Поскольку $k/\mathbb{Q}_p$ вполне разветвлено, вторая часть, очевидно, следует из первой. Любая единица $\varepsilon \equiv 1 \bmod \pi$ записывается как $\varepsilon = 1 + a_1\pi + a_2\pi^2 + \dots$, где $a_j \in \mathbb{Z}$, а значит, имеет вид $\varepsilon = (1-\pi)^{-a_1}(1-\pi^2)^{-b_2}(1-\pi^3)^{-c_3}\cdots$, для некоторых $b_2, c_3, \dots \in \mathbb{Z}$. $\square$

Теорема 4.3. *Если $j \neq p$, то $(\eta_j, \pi)_p = 1$; $(\pi, \eta_p)_p = \zeta$.*

Доказательство. Если $p \not| j$, то это следует из равенств $(\eta_j, \pi^j)_p = 1$. Если $j > p$, то $\eta_j \equiv 1 \bmod (\pi^{p+1})$. Поскольку $(\pi^{p+1}) = (p\pi^2)$, композиция изоморфизмов $(1 + (p\pi^2)) \xrightarrow{\log} (p\pi^2) \xrightarrow{\times\frac{1}{p}} (\pi^2) \xrightarrow{\exp} (1 + (\pi^2))$ определяет изоморфизм $(1 + (p\pi^2)) \xrightarrow{\sqrt[p]{\ }} (1 + (\pi^2))$, т.е. η_j – p-ая степень, откуда $(\eta_j, \pi)_p = 1$ при $j \neq p$. (Вариант. $\binom{1/p}{j} \in \frac{p^{-j}}{j!}(1 + p\mathbb{Z}_p)$, т.е. ряд Ньютона для $\sqrt[p]{1+x}$ сходится при $v(x) > \frac{p}{p-1}$.)

Заметим, что $k(\sqrt[p]{\eta_p})/k$ неразветвлено, т.к. $\eta_p \equiv 1 \bmod \pi$, и если положить $b = \frac{\sqrt[p]{\eta_p}-1}{\pi}$, то $(\pi b+1)^p = 1-\pi^p$, или эквивалентно $b^p + \sum_{j=1}^{p-1} \frac{p}{\pi^{p-j}}\binom{p-1}{j-1}\frac{b^j}{j} + 1 = 0$, что становится $b^p - b + 1 \equiv 0$ по модулю π. Поэтому $(\pi, k(\sqrt[p]{\eta_p})/k) = \mathrm{Frob}_p$, и значит, $(\pi, \eta_p)_p = \frac{\mathrm{Frob}_p \sqrt[p]{\eta_p}}{\sqrt[p]{\eta_p}} \equiv \frac{1+\pi b^p}{1+\pi b} \equiv 1 + \pi(b^p - b) \equiv 1 - \pi = \zeta \bmod \pi^2$. Откуда $(\pi, \eta_p)_p = \zeta$. $\square$

Предложение 4.4. $(\eta_i, \eta_j)_p = \prod_{r,s\geqslant 1,\ (r,s)=1} (\pi, \eta_{ri+sj})_p^{r_0 i + s_0 j}$, *где* $rs_0 - sr_0 = 1$.

Доказательство. Поскольку $\eta_j + \pi^j \eta_i = \eta_{i+j}$, из формулы сложения получаем $(\pi^j \eta_i, \eta_j)_p = (\pi^j \eta_i, \eta_{i+j})_p (\eta_{i+j}, \eta_j)_p$, т.к. $-1 = (-1)^p$. Из соотношения Стейнберга следует, что $(\pi^j \eta_i, \eta_j)_p = (\eta_i, \eta_j)_p$, и значит,

$$(\eta_i, \eta_j)_p = (\pi, \eta_{i+j})_p^j (\eta_i, \eta_{i+j})_p (\eta_{i+j}, \eta_j)_p.$$

Из теоремы 4.3 следует корректность правой части. Обозначим её через A_{ij}. Разбив индексы r, s на три группы: $r = s (= 1)$, $r > s$, и $r < s$, видим, что $A_{ij} = (\pi, \eta_{i+j})_p^j A_{i,i+j} A_{i+j,j}$, и значит,

$$\frac{(\eta_i, \eta_j)_p}{A_{ij}} = \frac{(\eta_i, \eta_{i+j})_p}{A_{i,i+j}} \frac{(\eta_{i+j}, \eta_j)_p}{A_{i+j,j}}. \tag{3}$$

Мы знаем, что η_ν – p-ая степень для достаточно больших ν, и потому $(\eta_s, \eta_\nu)_p = (\eta_\nu, \eta_s)_p = A_{s,\nu} = A_{\nu,s} = 1$. Рекуррентное соотношение (3) позволяет выразить $\frac{(\eta_i,\eta_j)_p}{A_{ij}}$ как произведение $\frac{(\eta_\nu,\eta_s)_p}{A_{\nu,s}}$ и $\frac{(\eta_s,\eta_\nu)_p}{A_{s,\nu}}$ для достаточно больших ν, и потому $A_{ij} = (\eta_i, \eta_j)_p$. $\square$

Теорема 4.5. $(\eta_i, \eta_j)_p = \zeta^a$, *где* $a \equiv \sum_{r,s\geqslant 1,\ ri+sj=p} \frac{j}{r} \bmod p$ *($a = 0$, если таких r, s нет).*

Доказательство. В формуле для $(\eta_i, \eta_j)_p$ из предложения 4.4 множители, отличные от единицы соответствуют парам $r, s \geqslant 1$, $(r, s) = 1$, $ri + sj = p$, поэтому $a = \sum_{r,s\geqslant 1,\ ri+sj=p} (r_0 i + s_0 j)$. Осталось заметить, что $r_0 i + s_0 j = \frac{r_0}{r}(ri + sj) + \frac{rs_0 - sr_0}{r} j \equiv \frac{j}{r} \bmod p$, т.к. $rs_0 - sr_0 = 1$. $\square$

Пример. $(\eta_1, \eta_{p-1})_p = \zeta^{-1}$.

Теперь мы можем найти $(\alpha, \beta)_p$ для всех $\alpha, \beta \in k^\times$. Разлагая α и β в произведение степеней π и единиц, видим, что достаточно вычислить символ для единиц и для π.

Редукция 1. Пусть $\alpha, \beta \in \mathcal{O}_k^\times$. Тогда $\alpha^{p-1} \equiv \beta^{p-1} \equiv 1 \bmod \pi$ и $(\alpha^{p-1}, \beta^{p-1})_p = (\alpha, \beta)_p$. Это сводит задачу к случаю $\alpha \equiv \beta \equiv 1 \bmod \pi$.

Редукция 2. Если $\alpha \equiv 1 \bmod \pi$, то $\alpha \equiv 1 + \mu\pi \bmod \pi^2$, где $\mu \in \mathbb{Z}$. Поскольку $\zeta^\mu = (1-\pi)^\mu \equiv 1 - \mu\pi \bmod \pi^2$, получаем $\alpha\zeta^\mu \equiv 1 \bmod \pi^2$. Это сводит задачу к вычислению $(\alpha, \beta)_p$ и $(\zeta, \beta)_p$ при $\alpha \equiv 1 \bmod \pi^2$ и $\beta \equiv 1 \bmod \pi$.

Редукция 3. $(\zeta, \zeta)_p = (-\zeta, \zeta)_p (-1, \zeta)_p = 1$. Это сводит вычисление $(\zeta, \beta)_p$ к случаю $\beta \equiv 1 \bmod \pi^2$.

Замечание. Если L/K – конечное сепарабельное расширение локальных полей, то для любой униформизующей π поля L и единицы $\beta \in \mathcal{O}_L^\times$ отображение $\mathcal{O}_L \xrightarrow{\times \beta d\pi} \Omega_{\mathcal{O}_L/\mathcal{O}_K}$ сюръективно, а его ядро совпадает с $\mathrm{Diff}_{L/K}$ – дифферентой L/K, т.е. аннулятором $\mathcal{O}_L$-модуля $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$.

Для любого кэлерова дифференциала $\omega \in \Omega_{\mathcal{O}_L/\mathcal{O}_K}$ определим $\frac{\omega}{\beta d\pi} \in \mathcal{O}_L/\mathrm{Diff}_{L/K}$ как прообраз ω относительно умножения на $\beta d\pi$. Для любой единицы $\alpha \in \mathcal{O}_L^\times$ положим $d\log\alpha := \frac{d\alpha}{\alpha}$. Заметим, что вообще говоря $d\log\alpha \neq d(\log\alpha)$.

В нашем случае $L = k$, $K = \mathbb{Q}_p$, $\mathrm{Diff}_{L/K} = (\pi^{p-2})$ и $\frac{d\log\alpha}{d\log\zeta} = -\frac{\zeta}{\alpha}\frac{d\alpha}{d\pi}$.

Теорема 4.6 (Артин–Хассе). *Пусть $S : k \longrightarrow \mathbb{Q}_p$ – след. Тогда*

(1) *если $\alpha \equiv 1 \bmod \pi^2$ и $\beta \in \mathcal{O}_k^\times$, то $(\alpha, \beta)_p = \zeta^{-\frac{1}{p}S(\frac{d\log\beta}{d\log\zeta}\cdot\log\alpha)}$;*

(2) *если $\alpha \equiv 1 \bmod \pi$, то $(\zeta, \alpha)_p = \zeta^{\frac{1}{p}S(\log\alpha)}$;*

(3) *если $\alpha \equiv 1 \bmod \pi$, то $(\alpha, \pi)_p = \zeta^{\frac{1}{p}S(\frac{\zeta}{\pi}\cdot\log\alpha)}$.*

Пример. (Хассе) Если $\alpha \equiv 1 \bmod p$ и $\beta \equiv 1 \bmod \pi$, то $(\alpha, \beta)_p = \zeta^{S(\frac{\alpha-1}{p}\frac{\beta-1}{\pi})}$.

Доказательство.

(1) Для проверки корректности заметим, что $\log\alpha \in \pi^2$, и значит, $\frac{1}{p}\frac{d\log\beta}{d\log\zeta}\cdot\log\alpha$ определено по модулю идеала $(\frac{\pi^p}{p}) = (\pi)$. Поэтому $\frac{1}{p}S(\frac{d\log\beta}{d\log\zeta}\cdot\log\alpha)$ определено по модулю идеала $S(\pi) = (p)$, что и требовалось.

Ясно, что обе части бимультипликативны, поэтому тождество достаточно проверить для $(\eta_i,\eta_j)_p$ при $i\geqslant 2$. Из разложения логарифма в степенной ряд получаем $-\frac{1}{p}S(\frac{d\log\eta_j}{d\log\zeta}\cdot\log\eta_i)=\frac{j}{p}S(\zeta\sum_{r,s\geqslant 1}\frac{\pi^{ir+js-1}}{r})$. Пусть $m=ir+js$, $p^\nu|r$, $p^{\nu+1}\not| r$. Тогда $p^\nu\leqslant r$ и $2p^\nu\leqslant m$ (т.к. $i\geqslant 2$). Кроме того, $2r\leqslant m$.

Проверим, что

$$p^{-\nu-1}S(\zeta\pi^{m-1})\equiv\begin{cases}1 \bmod p, & \text{если } m=p \text{ и } \nu=0,\\ 0 \bmod p, & \text{иначе.}\end{cases} \tag{4}$$

Если $m>p$, то $m-1-(p-1)(\nu+1)>0$, т.к. это верно при $\nu=0$ и $m-1-(p-1)(\nu+1)\geqslant 2p^\nu-1-(p-1)(\nu+1)\geqslant 1$ при $\nu\geqslant 1$, поскольку последовательность $2p^\nu-1-(p-1)(\nu+1)$ возрастает. Откуда $p^{-\nu-1}S(\zeta\pi^{m-1})\equiv 0 \bmod p$.

Если $2\leqslant m\leqslant p$ (и значит, $\nu=0$), то $\frac{1}{p}S(\zeta\pi^{m-1})=\frac{1}{p}\sum_{\mu=0}^{m-1}\binom{m-1}{\mu}(-1)^\mu S(\zeta^{\mu+1})=\frac{1}{p}\sum_{\mu=0}^{m-1}\binom{m-1}{\mu}(-1)^\mu(p\cdot\delta_{\mu,p-1}-1)=\begin{cases}1, & \text{если } m=p,\\ 0 \bmod p, & \text{если } m<p.\end{cases}$ Из этого равенства получаем $\frac{j}{p}S(\zeta\sum_{r,s\geqslant 1}\frac{\pi^{ir+js-1}}{r})\equiv j\sum_{r,s\geqslant 1,\ ri+sj=p}\frac{1}{r} \bmod p$, что и требовалось.

(2) $(\zeta,\alpha)_p=(\alpha\zeta^s,\zeta)_p^{-1}$ для любого целого s. Существует такое s, что $\alpha\zeta^s\equiv 1 \bmod \pi^2$, и значит, $(\alpha\zeta^s,\zeta)_p^{-1}=\zeta^{\frac{1}{p}S(\frac{d\log\zeta}{d\log\zeta}\cdot\log(\alpha\zeta^s))}=\zeta^{\frac{1}{p}S(\log\alpha)}$, что и требовалось.

(3) $(\alpha,\pi)_p=(\alpha\zeta^s,\pi)_p$, где $\alpha\zeta^s\equiv 1 \bmod \pi^2$. Поскольку $\log\alpha=\log(\alpha\zeta^s)$, считаем далее, что $\alpha\equiv 1 \bmod \pi^2$, и потому $\frac{\zeta}{\pi}\log\alpha\in(\pi)$, откуда следует корректность. Обе части мультипликативны, поэтому тождество достаточно проверить для $\alpha=\eta_i$ при $i\geqslant 2$. Как и выше, из разложения логарифма в степенной ряд получаем $\frac{1}{p}S(\frac{\zeta}{\pi}\cdot\log(1-\pi^i))=-\sum_{r\geqslant 1}\frac{1}{rp}S(\zeta\pi^{ir-1})$, и сравнение (4) завершает доказательство. $\square$

5. Глобальные поля и степенные законы взаимности

Теперь фиксируем целое $m\geqslant 2$, и рассмотрим глобальное поле K, содержащее примитивный корень степени m из единицы, и некоторую конечную точку $\mathfrak{p}$, не делящую m, с полем вычетов из $q=N\mathfrak{p}$ элементов. Ясно, что корни степени m из единицы остаются различными в поле вычетов, то есть $m|(q-1)$. Для каждого целого $\alpha\in\mathcal{O}_K$, не делящегося на $\mathfrak{p}$, определим «символ Лежандра» $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ как единственный корень степени m, сравнимый с $\alpha^{\frac{q-1}{m}}$ по модулю $\mathfrak{p}$.

Очевидные свойства: а) $\left(\frac{\alpha\beta}{\mathfrak{p}}\right)_m=\left(\frac{\alpha}{\mathfrak{p}}\right)_m\left(\frac{\beta}{\mathfrak{p}}\right)_m$; б) $\left(\frac{\alpha}{\mathfrak{p}}\right)_m=1$ тогда и только тогда, когда $\alpha\equiv\beta^m \bmod \mathfrak{p}$ для некоторого $\beta\in\mathcal{O}_K$.

Обобщением «символа Лежандра» служит следующий «символ Якоби». Для «дробного дивизора» $\mathfrak{b}$ в поле K, носитель которого не пересекается с носителем $m\alpha$ (то есть $\mathfrak{b}$ – формальная целочисленная линейная комбинация конечных точек $\mathfrak{p}$ таких, что $v_\mathfrak{p}(m\alpha)=0$), положим $\left(\frac{\alpha}{\mathfrak{b}}\right)_m=\prod_{\mathfrak{p}:\ \text{конечные}}\left(\frac{\alpha}{\mathfrak{p}}\right)_m^{v_\mathfrak{p}(\mathfrak{b})}$. Очевидно, $\left(\frac{\alpha}{\mathfrak{bc}}\right)_m=\left(\frac{\alpha}{\mathfrak{b}}\right)_m\left(\frac{\alpha}{\mathfrak{c}}\right)_m$.

Хотим найти $\left(\frac{\alpha}{(\beta)}\right)_m\left(\frac{\beta}{(\alpha)}\right)_m^{-1}$. Обозначим через $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_m$ то, что мы раньше обозначали через $(\alpha,\beta)_m$, если $\alpha,\beta\in K_\mathfrak{p}^\times$. Заметим, что здесь точка $\mathfrak{p}$ может быть архимедовой.

Теорема 5.1. $\left(\frac{\alpha}{(\beta)}\right)_m\left(\frac{\beta}{(\alpha)}\right)_m^{-1}=\prod_{\mathfrak{p}\not| m}\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_m^{-1}$, *где $\mathfrak{p}$ пробегает конечные точки.*

Доказательство. Левая часть равна $\prod_{\mathfrak{p}\not| m}\left(\frac{\alpha}{\mathfrak{p}}\right)_m^{v_\mathfrak{p}(\beta)}\left(\frac{\beta}{\mathfrak{p}}\right)_m^{-v_\mathfrak{p}(\alpha)}$. Поскольку $m|(q-1)$, то есть, локальные символы – ручные (см. свойство (7)), $\mathfrak{p}$-множитель в этом произведении совпадает с $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_m^{-1}$, что и требовалось. $\square$

Теорема 5.2 (Закон взаимности в форме Гильберта). *$\prod_{\mathfrak{p}} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_m = 1$ для любых $\alpha, \beta \in K^\times$, где $\mathfrak{p}$ пробегает все, в том числе архимедовы, точки.*

Это следует из закона взаимности Артина, который мы обсудим чуть позже.

Следствие 5.3 (Степенной закон взаимности). *$\left(\frac{\alpha}{(\beta)}\right)_m \left(\frac{\beta}{(\alpha)}\right)_m^{-1} = \prod_{\mathfrak{p}|m,\infty} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_m$, где α, β – такие же, как и выше.*

Если λ делится только на делители m, то $\left(\frac{\lambda}{(\alpha)}\right)_m = \prod_{\mathfrak{p}|m,\infty} \left(\frac{\lambda,\alpha}{\mathfrak{p}}\right)_m$.

5.1. **Квадратичный закон взаимности, закон взаимности Эйзенштейна для круговых полей и приложение к первому случаю теоремы Ферма.** Примеры. 1. **Квадратичный закон взаимности Гаусса.** Пусть $K = \mathbb{Q}$, $m = 2$, a, b взаимно просты и нечётны. Тогда $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \left(\frac{\alpha,\beta}{2}\right)\left(\frac{\alpha,\beta}{\infty}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2} + \frac{\operatorname{sgn}(a)-1}{2}\frac{\operatorname{sgn}(b)-1}{2}}$ и $\left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}$.

2. **Закон взаимности Эйзенштейна.** Пусть $K = \mathbb{Q}(\zeta_p)$, где $p \geqslant 3$ – простое, $\pi = 1 - \zeta_p$ и $m = p$. Тогда $\left(\frac{\alpha}{(\beta)}\right)_p \left(\frac{\beta}{(\alpha)}\right)_p^{-1} = \left(\frac{\alpha,\beta}{(\pi)}\right)_p$, $\left(\frac{\zeta_p}{(\alpha)}\right)_p = \left(\frac{\zeta_p,\alpha}{(\pi)}\right)_p$ и $\left(\frac{\pi}{(\alpha)}\right) = \left(\frac{\pi,\alpha}{(\pi)}\right)_p$, если носители (α) и (β) не пересекаются и не содержат (π). В частности, $\left(\frac{\zeta_p}{(\alpha)}\right)_p = \left(\frac{\zeta_p,\alpha}{(\pi)}\right)_p$, поскольку ζ_p – единица, и значит, $\left(\frac{\alpha}{(\zeta_p)}\right)_p = 1$.

Формулы Артина–Хассе дают явное описание этих выражений.

3. В качестве приложения закона взаимности Эйзенштейна (и формулы Хассе–Артина), докажем теорему Фуртвэнглера 0.4. А именно, $\left(\frac{\alpha}{(\beta)}\right)_p \left(\frac{\beta}{(\alpha)}\right)_p^{-1} = \zeta_p^{S(\frac{\alpha-1}{p}\frac{\beta-1}{\pi})}$ для всех $\alpha, \beta \in \mathbb{Q}(\zeta_p)^\times$ с непересекающимися носителями и такими, что $\alpha \equiv 1 \bmod p$ и $\beta \equiv 1 \bmod \pi$. Пусть, без ограничения общности, $q|y$. Из взаимной простоты $(x + \zeta_p^j y)$ (см. введение) следует, что $(x + \zeta_p^j y) = \mathfrak{a}_j^p$ для некоторых идеалов $\mathfrak{a}_j \subset \mathbb{Z}[\zeta_p]$, $0 \leqslant j < p$. Положим $\beta := \frac{x+\zeta_p y}{x+y} = 1 - \frac{\pi y}{x+y} \equiv 1 \bmod \pi$, где $\pi = 1 - \zeta_p$. Тогда $(\beta) = (\mathfrak{a}_0^{-1}\mathfrak{a}_1)^p$, откуда $\left(\frac{\alpha}{(\beta)}\right)_p = 1$ для всех $\alpha \in \mathbb{Z}[\zeta_p]$ с носителем, не пересекающим носитель β. Пусть $\alpha = q^{p-1}$. Тогда $\left(\frac{\beta}{(\alpha)}\right)_p = \left(\frac{\beta}{(q)}\right)_p^{-1} = 1$. Поэтому из формулы Хассе–Артина получаем $S(\frac{\alpha-1}{p}\frac{\beta-1}{\pi}) \equiv 0 \bmod p$. Поскольку левая часть сравнения равна $-S(\frac{q^{p-1}-1}{p}\frac{y}{x+y}) = (1-p)\frac{q^{p-1}-1}{p}\frac{y}{x+y}$, где $\frac{y}{x+y} \in \mathbb{Z}_p^\times$, видим, что $\frac{q^{p-1}-1}{p}$ делится на p. $\square$

5.2. **Закон взаимности и абелевы расширения глобальных полей.** Пусть L/K – расширение Галуа глобального поля, и $\mathfrak{p}$ – некоторая точка поля L. Тогда подгруппа разложения (см. §2) точки $\mathfrak{p}$ в $G_{L/K}$ канонически изоморфна локальной группе Галуа $G_{L_\mathfrak{p}/K_\mathfrak{p}}$, где $L_\mathfrak{p}$ (соотв. $K_\mathfrak{p}$) – пополнение L в $\mathfrak{p}$ (соотв. в $\mathfrak{p}|_K$). Как упоминалось в §2, продолжения точек поля K на поле L образуют $G_{L/K}$-орбиты. В частности, подгруппы разложения разных продолжений данной точки поля K сопряжены. Пусть теперь расширение L/K – абелево. Тогда подгруппы разложения в $G_{L/K}$ нумеруются точками $\mathfrak{p}$ поля K.

Поскольку разветвлённые точки делят дискриминант, любое конечное расширение разветвлено только в конечном числе точек. Поэтому имеется отображение $\prod'_{\mathfrak{p}} G_{L_{\tilde{\mathfrak{p}}}/K_\mathfrak{p}} \longrightarrow G_{L/K}$, где $\prod'$ означает, что рассматриваются такие наборы элементов $(g_\mathfrak{p})$, что $g_\mathfrak{p}$ лежит в подгруппе инерции для почти всех точек $\mathfrak{p}$.

Как мы уже знаем, имеются гомоморфизмы норменного вычета $(\ , L_{\tilde{\mathfrak{p}}}/K_\mathfrak{p}) : K_\mathfrak{p}^\times \longrightarrow G_{L_{\tilde{\mathfrak{p}}}/K_\mathfrak{p}}$ с плотным образом.

Определение. Группой иделей поля K называется ограниченное произведение $\mathbb{A}_K^\times := \prod'_{\mathfrak{p}} K_\mathfrak{p}^\times$, где $\prod'$ означает, что рассматриваются такие наборы элементов $(a_\mathfrak{p})$, что $a_\mathfrak{p}$ – единица для почти всех точек $\mathfrak{p}$. (Заметим, что это согласуется с ограниченным произведением подгрупп разложения, рассмотренным выше.)

Вывод степенного закона взаимности из закона взаимности Артина. Фиксируем $\alpha, \beta \in K^\times$. Пусть S – конечное множество точек K, содержащее все архимедовы точки, точки ветвления расширения $K(\sqrt[m]{\beta})/K$, и в которых α не является единицей. Тогда $\prod_{\mathfrak{p}} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_m = \prod_{\mathfrak{p}\in S} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_m = \prod_{\mathfrak{p}\in S} \frac{(\alpha, K(\sqrt[m]{\beta})/K)\sqrt[m]{\beta}}{\sqrt[m]{\beta}} = \frac{(\prod_{\mathfrak{p}\in S}(\alpha, K(\sqrt[m]{\beta})/K))\sqrt[m]{\beta}}{\sqrt[m]{\beta}}$. Поэтому, чтобы доказать закон взаимности в виде теоремы 5.2, осталось установить

Теорема 5.4 (Закон взаимности Артина). *Композиция* $K^\times \stackrel{\text{диаг}}{\longrightarrow} \mathbb{A}_K^\times \longrightarrow G_{L/K}$ *тривиальна для любого абелева расширения* L/K.

Проверим это для круговых расширений. Пусть сначала $K = \mathbb{Q}$. В этом случае нетрудно даже проверить точность последовательности $1 \longrightarrow \mathbb{Q}^\times \stackrel{\text{диаг}}{\longrightarrow} \prod'_{p<\infty} \mathbb{Q}_p^\times \times \{\pm 1\} \stackrel{\theta}{\longrightarrow} G_{\mathbb{Q}(\mu_\infty)/\mathbb{Q}} \longrightarrow 1$. Заметим, что элементы $G_{\mathbb{Q}(\mu_\infty)/\mathbb{Q}} = \widehat{\mathbb{Z}}^\times = \prod_{p<\infty} \mathbb{Z}_p^\times$ определяются своими ℓ-компонентами, то есть ограничениями на $\mathbb{Q}(\mu_{\ell^\infty})$. В частности, ℓ-компонента элемента $(a_p, \mathbb{Q}_p(\mu_\infty)/\mathbb{Q}_p)$, то есть $(a_p, \mathbb{Q}_p(\mu_{\ell^\infty})/\mathbb{Q}_p) \in \mathbb{Z}_\ell^\times$, равна а) $p^{v_p(a_p)}$, если $p \neq \ell, \infty$, б) $a_\ell^{-1}|a_\ell|_\ell^{-1}$, если $p = \ell$, в) $\mathrm{sgn}(a_\infty)$, если $p = \infty$.

Таким образом, $\prod_{p\leqslant\infty}(a_p, \mathbb{Q}_p(\mu_{\ell^\infty})/\mathbb{Q}_p) = \prod_{p\neq\ell,\infty} p^{v_p(a_p)} \cdot a_\ell^{-1}|a_\ell|_\ell^{-1} \cdot \mathrm{sgn}(a_\infty) = \prod_{p<\infty} p^{v_p(a_p)} \cdot a_\ell^{-1} \cdot \mathrm{sgn}(a_\infty)$, и значит, ядро θ состоит из иделей $(a_p)_p$ с рациональными координатами $a_\ell \in \mathbb{Q}^\times$, которые не зависят от ℓ, при $\ell < \infty$, и знак которых не зависит от ℓ при $\ell \leqslant \infty$, т.е. из элементов $\mathbb{Q}^\times$.

Квадратичный закон взаимности Гаусса можно вывести прямо отсюда. Для этого нужно заметить, что круговое поле $\mathbb{Q}(\mu_\infty)$ содержит квадратные корни изо всех рациональных чисел. Поскольку группа $\mathbb{Q}^\times$ порождена простыми числами и -1, осталось проверить, что поле $\mathbb{Q}(\mu_\infty)$ содержит $\sqrt{\pm p}$ для всех простых чисел p. Если $p = 2$, это следует из $(1+\sqrt{-1})^2 = 2\sqrt{-1}$. Если p нечётно, то это получается из следующей конструкции. Пусть $\mathbb{F}_q$ – конечное поле характеристики p, χ – его мультипликативный характер, ψ – нетривиальный аддитивный характер.

Определим сумму Гаусса $\Gamma_\psi(\chi) = \sum_{j\in\mathbb{F}_q^\times} \chi(j)\psi(j) \in \mathbb{Z}[\zeta_{p(q-1)}]$. Это – аналог гамма-функции Бернулли–Эйлера $\Gamma(s) = \int_0^\infty t^s e^{-t}\frac{dt}{t}$. Например, $\Gamma_\psi(1) = -1$. Имеется аналог формулы дополнения: $\Gamma_\psi(\chi)\Gamma_\psi(\overline{\chi}) = \chi(-1)q$, если $\chi \neq 1$. (Доопределим $\chi(0) := 0$. Тогда $\Gamma_\psi(\chi)\Gamma_\psi(\overline{\chi}) = \sum_{a,b\in\mathbb{F}_q^\times} \chi(a/b)\psi(a+b) = \sum_{b\in\mathbb{F}_q^\times, c\in\mathbb{F}_q} \chi((c-b)/b)\psi(c) = \chi(-1)\cdot(q-1) + \sum_{b,c\in\mathbb{F}_q^\times} \chi((c-b)/b)\psi(c) = \chi(-1)\cdot(q-1) + (\sum_{a\in\mathbb{F}_q^\times}\chi(a-1))(\sum_{c\in\mathbb{F}_q^\times}\psi(c)) = \chi(-1)\cdot(q-1) + (-\chi(-1))(-1) = \chi(-1)\cdot q$.)

В частности, $\Gamma_\psi(\chi)^2 = \chi(-1)\cdot q = (-1)^{(q-1)/2}q$, если $\chi = \left(\frac{}{\mathbb{F}_q}\right)$ – символ Лежандра квадратичного вычета. (Здесь мы воспользовались нечётностью q.) □

Упражнение. а) Докажите, что аддитивные характеры поля $\mathbb{F}_q$ образуют одномерное $\mathbb{F}_q$-векторное пространство, и $\Gamma_{\alpha\psi}(\chi) = \chi(\alpha)^{-1}\Gamma_\psi(\chi)$ для любого $\alpha \in \mathbb{F}_q^\times$.

б) Докажите, что $\Gamma_\psi(\chi)^\ell \equiv \Gamma_{\ell\psi}(\chi^\ell) \bmod \ell$ для любого простого ℓ, не делящего q.

в) Выведите квадратичный закон взаимности, положив $\chi = \left(\frac{}{\mathbb{F}_q}\right)$.

Из коммутативности первой диаграммы (2) следует, что коммутативна диаграмма

$$\begin{array}{ccccc} K^\times & \longrightarrow & \mathbb{A}_K^\times & \longrightarrow & G_{K(\mu_\infty)/K} \\ \downarrow N_{K/\mathbb{Q}} & & \downarrow N_{K/\mathbb{Q}} & & \downarrow |_{\mathbb{Q}(\mu_\infty)} \text{ – вложение} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{A}_\mathbb{Q}^\times & \longrightarrow & G_{\mathbb{Q}(\mu_\infty)/\mathbb{Q}}. \end{array}$$

Поэтому композиция первой строки равна 1, хотя она не точна, вообще говоря.

Доказательство закона взаимности Артина можно свести к случаю круговых расширений путём отождествления групп Галуа произвольных циклических расширений (а только они нам и нужны, т.к. любое абелево расширение – композит циклических) с группами Галуа циклических круговых расширений помощью следующих элементарных соображений (ван дер Вардена и Артина).

Лемма 5.5. *Пусть $a, r, q \in \mathbb{Z}$, $a \geqslant 2$, $r \geqslant 1$, q – простое, и $(r,q) \neq (1,2)$. Тогда существует такое простое число p, что порядок a в группе $\mathbb{F}_p^\times$ равен q^r.*

Доказательство. Из формулы $T := \frac{a^{q^r}-1}{a^{q^{r-1}}-1} = (a^{q^{r-1}}-1)^{q-1} + q(a^{q^{r-1}}-1)^{q-2} + \cdots + q$ видно, что для любого простое числа p

- если $p|T$ и $p|(a^{q^{r-1}}-1)$, то $p = q$;
- если $q|T$, то $q|(a^{q^{r-1}}-1)$;
- если $q > 2$ или $r > 1$, то T не делится на q^2.

Поскольку $T > q$ и $q^2 \not| T$, существует простой делитель $p \neq q$ числа T, обладающий требуемыми свойствами. □

Лемма 5.6. *Пусть $n = q_1^{r_1} q_2^{r_2} \cdots q_s^{r_s}$ – натуральное и $a \in \mathbb{Z}$, $a \geqslant 2$. Тогда*

- *существует такое натуральное число $m = p_1 p_1' \cdots p_s p_s'$, где $p_1, p_1', \ldots, p_s, p_s'$ – попарно различные простые числа, что порядок a в группе $(\mathbb{Z}/m\mathbb{Z})^\times$ делится на n, и существует такое натуральное число b, порядок которого в группе $(\mathbb{Z}/m\mathbb{Z})^\times$ делится на n, причём a и b независимы в $(\mathbb{Z}/m\mathbb{Z})^\times$.*
- *Можно найти сколь угодно большие простые p_j, p_j', удовлетворяющие этим условиям.*

Лемма 5.7. *Пусть K/k – абелево расширение числовых полей степени n, $\mathfrak{p}$ – неразветвлённая точка поля k, $S \geqslant 2$ – натуральное число. Тогда существует такое натуральное число m, взаимно простое с $\mathfrak{p}$ и S, что*

(1) *порядок автоморфизма Фробениуса $(\mathfrak{p}, k(\mu_m)/k)$ в группе $G_{k(\mu_m)/k}$ делится на n,*
(2) *$K \cap k(\mu_m) = k$ и*
(3) *существует $\tau \in G_{k(\mu_m)/k}$, независимый от $(\mathfrak{p}, K/k)$, порядок которого делится на n.*

Лемма 5.8 (Артин). *Пусть K/k – конечное циклическое расширение числовых полей, $\mathfrak{p}$ – точка поля k, $S \geqslant 2$ – натуральное число. Тогда существуют такое натуральное число m, взаимно простое с $\mathfrak{p}$ и S, и конечное расширение E/k, что*

(1) *$K \cap E = k$,*
(2) *$K(\mu_m) = E(\mu_m)$ и $K \cap k(\mu_m) = k$,*
(3) *$\mathfrak{p}$ вполне распадается в E.*

Лемма Артина используется в сочетании со следующим фактом о поведении символов Артина=автоморфизмов Фробениуса при ограничении.

Предложение 5.9. *Пусть k – числовое поле, K/k – конечное абелево расширение, E/k – конечное расширение; $\mathfrak{p}$ – точка поля k, неразветвлённая в EK, $\mathfrak{q}$ – продолжение точки $\mathfrak{p}$ на* *поле E. Тогда $(\mathfrak{q}, EK/E)|_K = (\mathfrak{p}, K/k)^f$, где f – степень инерции расширения E/k в точке $\mathfrak{q}$, т.е. степень расширения полей вычетов.*

Доказательство. Пусть $\mathfrak{P}$ – продолжение точки $\mathfrak{p}$ на поле K, и $\mathfrak{Q}$ – продолжение точки $\mathfrak{q}$ на поле KE. Тогда для любого $x \in \mathcal{O}_{KE}/\mathfrak{Q}$ и $\sigma := (\mathfrak{q}, KE/E)$: $\sigma x = x^{N\mathfrak{q}}$, $\sigma|_K$ лежит в подгруппе разложения точки $\mathfrak{P}$ и по определению совпадает с $(\mathfrak{p}, K/k)^f$. □

Другой, но тесно связанный с первым, способ состоит в одновременном доказательстве закона взаимности Артина и закона взаимности Хассе.

Теорема 5.10 (Закон взаимности Хассе). *Композиция* $\mathrm{Br}(K) \xrightarrow{\text{диаг}} \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}$ – *нулевая для любого глобального поля K.*

Вывод закона взаимности Артина из закона взаимности Хассе. Пусть K/k – конечное расширение Галуа, $x \in \mathbb{A}_k^\times$, $\overline{x} \in \widehat{H}^0(G_{K/k}, \mathbb{A}_K^\times)$ – образ x, $\delta : H^1(G_{K/k}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G_{K/k}, \mathbb{Z})$ – связывающий изоморфизм. Как мы знаем из предложения 3.6, $\mathrm{inv}_v(\overline{x} \cdot \delta\chi) = \chi(\rho_v(x_v))$, откуда $\sum_v \mathrm{inv}_v(\overline{x} \cdot \delta\chi) = \chi(\theta(x))$. Поскольку $\overline{x} \cdot \delta\chi \in \mathrm{Br}(k)$, если $x \in k^\times$, из закона взаимности Хассе получаем $\chi(\theta(x)) = 0$ для любого характера $\chi \in H^1(G_{K/k}, \mathbb{Q}/\mathbb{Z})$, откуда $\theta(x) = 1$.

Доказательство закона взаимности Хассе для алгебр, расщепляющихся над циклическим круговым расширением K/k. Пусть $\chi : G_{K/k} \hookrightarrow \mathbb{Q}/\mathbb{Z}$ – образующая группы характеров. Тогда $\cup\delta\chi : \widehat{H}^0(G_{K/k}, K^\times) \xrightarrow{\sim} H^2(G_{K/k}, K^\times)$, то есть любая центральная простая k-алгебра, расщепляющаяся над K, происходит из некоторого элемента $\overline{a} \in \widehat{H}^0(G_{K/k}, K^\times)$. Тогда $\mathrm{inv}_v(\overline{a} \cdot \delta\chi) = \chi(\theta(a)) = 0$ для любого $a \in k^\times$.

Остаётся доказать, что любая алгебра расщепляется над некоторым циклическим круговым расширением. Как мы знаем из следствия 3.5, любая центральная простая алгебра над локальным полем с инвариантом $\frac{r}{n}$ расщепляется над любым расширением степени n. Поэтому нужно только проверить, что $\mathrm{Br}(k) \longrightarrow \bigoplus_v \mathrm{Br}(k_v)$ инъективно (и корректно определено; это проделано в §5.3). После чего предъявить циклическое чисто мнимое круговое расширение L любого числового поля k, все локальные степени которого в любом наперёд заданном конечном множестве неархимедовых точек делятся на любое наперёд заданное n.

Это совсем несложно: зафиксируем нечётное простое q, и рассмотрим глобальные поля $k(\mu_{q^r})$. Группы $G_{k(\mu_{q^r})/k}$ согласованно вкладываются в $(\mathbb{Z}/q^r\mathbb{Z})^\times$, а значит, их подгруппы периода $q-1$, если q нечётно, фиксируют циклические расширения $L(q,r)$ q-примарных порядков. В случае $q = 2$ рассмотрим $L(2,r) := k(\zeta_{2^r} - \zeta_{2^r}^{-1})$. Степени соответствующих локальных полей $L(q,r)_v$ также растут, поскольку локальные поля содержат только конечное число корней из единицы, осталось только взять достаточно большое r. Композит таких полей $L(q,r)$ для различных простых q дает требуемое круговое расширение.

5.3. **Когомологии иделей и классов иделей.** Под конечным множеством точек S глобального поля k будем понимать непустое множество, содержащее, в случае числового поля k, все архимедовы точки. Определим группу S-иделей как $J_k^S = \prod_{\mathfrak{p}\in S} k_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_\mathfrak{p}^\times$ с топологией произведения, а группу классов S-иделей, как факторгруппу

$$C_k^S = k^\times J_k^S / k^\times \cong J_k^S / k^\times \cap J_k^S \cong J_k^S / k_S^\times,$$

где $k_S^\times := J_k^S \cap k^\times$ – группа S-единиц поля k, т.е. элементов $k^\times$, являющихся единицами для всех $\mathfrak{p} \notin S$. Заметим, что $C_k/C_k^S \cong J_k/k^\times J_k^S$ изоморфна группе классов дивизоров дедекиндова кольца, образованного элементами поля k, $\mathfrak{p}$-целыми при $\mathfrak{p} \notin S$.

Пусть $J_k := \bigcup_S J_k^S$ – группа иделей с топологией объединения, то есть подгруппа J_k^S открыта в J_k для каждого S. Заметим, что J_k локально компактна, поскольку каждая группа единиц $\mathcal{O}_\mathfrak{p}^\times$ открыта и компактна в $k_\mathfrak{p}$ для каждого неархимедова $\mathfrak{p}$.

Будем обозначать группу классов иделей глобального поля k через C_k. Содержанием иделя $\mathfrak{a}$ называется произведение абсолютных значений его компонент: $\prod_\mathfrak{p} |\mathfrak{a}_\mathfrak{p}|_\mathfrak{p}$. В силу формулы произведения, содержание иделя зависит только от его класса. Обозначим через J_k^1 (соотв., C_k^1) группу иделей (соотв., классов иделей) с содержанием 1.

Из формулу произведения, применённой к $a-1$ при $a \in k^\times$, $a \neq 1$, нетрудно увидеть, что $k^\times$ – дискретная подгруппа в J_k^1. Из теоремы о конечности числа классов и теоремы Дирихле о единицах можно вывести компактность $C_k^1 = J_k^1/k^\times$. Конечно, $C_k/C_k^1 \cong J_k/J_k^1$ изоморфна, соответственно, $\mathbb{R}$ и $\mathbb{Z}$ в случае числового и функционального поля.

Если K – конечное расширение поля k, то имеются инъекции $J_k \hookrightarrow J_K$ и $C_k \hookrightarrow C_K$, и в каждом из этих случаев меньшая группа отображается гомеоморфно на замкнутую подгруппу большей. Если K/k – расширение Галуа, то группа Галуа G действует на K, J_K и C_K, и имеются отождествления $k = K^G$, $J_k = J_K^G$ и $C_k = C_K^G$. Первый из этих изоморфизмов следует из теории Галуа, второй – из определения иделей и вложения $J_k \subset J_K$, и последний – из первых двух, с учетом теоремы 90 Гильберта: $H^1(G, K^\times) = 0$.

Если S – конечное множество простых $\mathfrak{p}$ поля k, то тем же символом S будем обозначать множество простых $\mathfrak{P}$ поля K, которые делят некоторое простое $\mathfrak{p} \in S$. С учётом этих соглашений,

$$J_K^S = \prod_{\mathfrak{P}\in S} K_\mathfrak{P}^\times \times \prod_{\mathfrak{P}\notin S} \mathcal{O}_\mathfrak{P}^\times = \prod_{\mathfrak{p}\in S}(\prod_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}^\times) \times \prod_{\mathfrak{p}\notin S}(\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_\mathfrak{P}^\times),$$

и следовательно,

$$H^r(G, J_K^S) \cong \prod_{\mathfrak{p}\in S} H^r(G, \prod_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}^\times) \times \prod_{\mathfrak{p}\notin S} H^r(G, \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_\mathfrak{P}^\times).$$

Действие G на $\prod_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}^\times$ переставляет множители, и подгруппа G, состоящая из элементов, сохраняющих данный множитель $K_\mathfrak{P}^\times$, – подгруппа разложения $G_\mathfrak{P}$ точки $\mathfrak{P}$. Отсюда следует, что $\prod_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}^\times$ – G-модуль, «индуцированный» $G_\mathfrak{P}$-модулем $K_\mathfrak{P}^\times$, и лемма Шапиро показывает, что для любого фиксированного $\mathfrak{P}$, делящего $\mathfrak{p}$, имеются изоморфизмы

$$H^r(G, \prod_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}^\times) \cong H^r(G_\mathfrak{P}, K_\mathfrak{P}^\times), \quad \text{и аналогично,} \quad H^r(G, \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_\mathfrak{P}^\times) \cong H^r(G_\mathfrak{P}, \mathcal{O}_\mathfrak{P}^\times).$$

Эти изоморфизмы – канонические, получающиеся ограничением с G на $G_\mathfrak{P}$ и проекцией на $\mathfrak{P}$-множитель. Как мы знаем из теории локальных полей, $H^r(G_\mathfrak{P}, \mathcal{O}_\mathfrak{P}^\times) = 0$ при $r > 0$, если $K_\mathfrak{P}$ неразветвлено над $k_\mathfrak{p}$. Следовательно, если наше множество S содержит все простые $\mathfrak{p}$ поля k, разветвлённые в K, то $H^r(G, J_K^S) = \prod_{\mathfrak{p}\in S} H^r(G, \prod_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}^\times) \cong \prod_{\mathfrak{p}\in S} H^r(G_\mathfrak{P}, K_\mathfrak{P}^\times)$. В частности, морфизм G-модулей $k_S^\times \longrightarrow J_k^S$ индуцирует гомоморфизмы $H^r(G, k_S^\times) \longrightarrow \prod_{\mathfrak{p}\in S} H^r(G_\mathfrak{P}, K_\mathfrak{P}^\times)$. Переходя к прямому пределу по всё бóльшим и бóльшим S, получаем при $r > 0$ гомоморфизмы

$$H^r(G, k^\times) \longrightarrow H^r(G, J_K) = \varinjlim_{S} H^r(G, J_K^S) \cong \bigoplus_\mathfrak{p} H^r(G_\mathfrak{P}, K_\mathfrak{P}^\times),$$

где для каждой точки $\mathfrak{p}$ поля k $\mathfrak{P}$ обозначает какую-нибудь точку поля K над $\mathfrak{p}$. Таким образом, когомологии Галуа иделей сводятся к когомологиям локальных полей. Разумеется, построенные изоморфизмы функториальны и коммутируют с ограничением, трансфером и инфляцией в следующем очевидном смысле. Если $k \subset L \subset K$, то глобальное ограничение с $G_{K/k}$ до $G_{K/L}$ отражено в локальных ограничениях с $G_{K_\mathfrak{P}/k_\mathfrak{p}}$ до $G_{K_\mathfrak{P}/L_\mathfrak{r}}$. В обратную сторону, для каждого $\mathfrak{P}$ глобальный трансфер отражен суммой по всем простым $\mathfrak{r}$ поля L, делящим

$\mathfrak{P}$, локальных трансферов. Глобальная инфляция соответствует совокупности всех локальных инфляций.

Заметим, рассмотрев случай $r = 2$, что для доказательства теоремы 5.10 осталось показать, что $H^1(G, C_K) = 0$.

6. Закон взаимности для символа Конту-Каррэра

Законы взаимности возникают также и в более геометрических ситуациях.

Пусть F – алгебраически замкнутое поле, и X – гладкая проективная кривая над F.

Теорема 6.1 (Закон взаимности А.Вейля). *Пусть f, g – рациональные функции на X с непересекающимися носителями их дивизоров. Тогда $f(\mathrm{div}(g)) = g(\mathrm{div}(f))$, где $h(\sum_P n_P P) := \prod_P h(P)^{n_P}$ для любого дивизора $\sum_P n_P P$ и любой функции h, среди нулей и полюсов которой нет таких точек P, что $n_P \neq 0$.*

Мы обобщим это так, что теорема о равенстве нулю суммы вычетов любой мероморфной 1-формы на X станет частным случаем.

Но вспомним сначала формулу (7) на с.28 для символа Гильберта $(\ ,\ )_{q-1}$.

Определение. Пусть K – поле и $v : K^\times \longrightarrow \mathbb{Z}$ – дискретное нормирование. Ручным символом называется отображение $\{\ ,\ \}_v : K^\times \times K^\times \longrightarrow \kappa^\times$, где κ – поле вычетов v, заданное формулой $\{f, g\}_v := (-1)^{v(f)v(g)} f^{-v(g)} g^{v(f)} \bmod \mathfrak{m}_v = (-1)^{v(f)v(g)}(f^{-v(g)} g^{v(f)})(v)$.

Упражнение. Докажите, что ручной символ индуцирует гомоморфизм $K_2(K) \longrightarrow \kappa^\times$.

Заметим, что отношение правой части закона взаимности Вейля к левой равно $\prod_v \{f, g\}_v$, причём это определено для любых $f, g \neq 0$. Здесь мы воспользовались алгебраической замкнутостью поля F, чтобы отождествить (с F) поля вычетов всех нормирований v.

6.1. Соизмеримость.

Пусть A – локальное коммутативное артиново кольцо с максимальным идеалом $\mathfrak{m}$. Пусть $A, B \subset V$ – свободные A-модули.

Определение. Скажем, что A и B *соизмеримы* (и напишем $A \sim B$), если A-модуль $(A + B)/(A \cap B)$ конечно порождён. Ясно, что это – отношение эквивалентности.

Определение. Если $V_+ \subset V$ – свободные A-модули, то $G^V_{V_+} := \{\sigma \in \mathrm{GL}_A(V) \mid V_+ \sim \sigma V_+\}$.

Это – группа, зависящая только от класса соизмеримости V_+.

Пусть $V_+ \subset V$ – свободные A-модули, $\sigma_0, \sigma_1 \in G^V_{V_+}$ коммутируют; $P_i \subseteq V_+ \cap \sigma_i V_+$ – такие свободные A-модули, что V_+/P_i и $\sigma_i V_+/P_i$ – конечного ранга; $R \subseteq P_0 \cap P_1 \cap \sigma_1 P_0 \cap \sigma_0 P_1$ – такой свободный A-модуль, что P_i/R и $\sigma_i P_{1-i}/R$ – конечного ранга.

Зафиксируем базисные элементы a_i, b_i, c_i, d_i детерминантов A-модулей V_+/P_i, $\sigma_i V_+/P_i$, P_i/R и $\sigma_{1-i}P_i/R$, и положим $\{\sigma_0, \sigma_1\}^V_{V_+} := \frac{d_1 \otimes \sigma_0 b_1}{d_0 \otimes \sigma_1 b_0} \cdot \frac{c_0 \otimes b_0}{d_1 \otimes \sigma_0 a_1} \cdot \frac{c_1 \otimes a_1}{c_0 \otimes a_0} \cdot \frac{d_0 \otimes \sigma_1 a_0}{c_1 \otimes b_1}$, где четыре множителя – отношения разных базисных элементов детерминантов A-модулей $\sigma_0\sigma_1 V_+/R$, $\sigma_0 V_+/R$, V_+/R и $\sigma_1 V_+/R$. Очевидно, $\{\sigma_0, \sigma_1\}^V_{V_+}$ не зависит от базисов.

Свойства символа $\{\sigma, \tau\}^V_{V_+}$. Пусть $\sigma_0, \sigma_1, \tau_0, \tau_1 \in G^V_{V_+}$ – такие, что $[\sigma_i, \tau_j] = 1$. Тогда

(1) $\{\sigma_0, \sigma_0\}^V_{V_+} = 1$.
(2) $\{\sigma_0, \tau_0\}^V_{V_+} = (\{\tau_0, \sigma_0\}^V_{V_+})^{-1}$.
(3) $\{\sigma_0\sigma_1, \tau_0\}^V_{V_+} = \{\sigma_0, \tau_0\}^V_{V_+} \cdot \{\sigma_1, \tau_0\}^V_{V_+}$, и значит, $\{\sigma_0, \tau_0\tau_1\}^V_{V_+} = \{\sigma_0, \tau_0\}^V_{V_+} \cdot \{\sigma_0, \tau_1\}^V_{V_+}$.
(4) $\{\sigma_0, \tau_0\}^V_{V_+}$ зависит только от класса соизмеримости V_+.
(5) Если $\sigma_0 V_+ = V_+ = \tau_0 V_+$, то $\{\sigma_0, \tau_0\}^V_{V_+} = 1$.
(6) Если $V_+ = 0$ или $V_+ = V$, то $\{\sigma_0, \tau_0\}^V_{V_+} = 1$.

Доказательство использует интерпретацию $\{\sigma,\tau\}^V_{V_+}=[\widetilde{\sigma},\widetilde{\tau}]$, где $\widetilde{\sigma},\widetilde{\tau}$ – произвольные подъёмы σ,τ на центральное расширение $1\longrightarrow A^\times\longrightarrow \widetilde{G^V_{V_+}}\longrightarrow G^V_{V_+}\longrightarrow 1$, заданное 2-коциклом, значения которого на коммутирующих σ,τ совпадают с $\{\sigma,\tau\}^V_{V_+}$. (Подробности описаны в [AP].)

Пусть F и X – такие же, как и прежде, A – локальная артинова F-алгебра, $s\in X$, $R_s:=A\otimes_F F(X)\hat{_s}$– пополнение алгебры $R:=A\otimes_F F(X)$ в точке s. Пусть $w_s: R_s^\times\longrightarrow (F(X)\hat{_s})^\times\xrightarrow{v_s}\mathbb{Z}$ – «нормирование». Выбор униформизующей t в s определяет изоморфизм $A((t))\xrightarrow{\sim}R_s$.

Определение. Для $f,g\in R_s^\times$ определим *символ Конту-Каррэра* формулой

$$\langle f,g\rangle_s=(-1)^{w(f)w(g)}\{f,g\}^{R_s}_{A\otimes_F\mathcal{O}_{\hat{X},s}}\in A^\times,$$

где $R_s^\times\hookrightarrow G^{R_s}_{A\otimes_F\mathcal{O}_{\hat{X},s}}$– естественное вложение. Как следует из свойств $\{\sigma,\tau\}^V_{V_+}$, это – гомоморфизм $A((t))^\times\otimes A((t))^\times\longrightarrow A^\times$.

Вычислим его в координатах.

Предложение 6.2. *Любой элемент группы $A((t))^\times$ однозначно представим в виде $f(t)=t^{w(f)}a_0\prod_{0\neq i\in\mathbb{Z}}(1-a_it^i)$, где $a_i\in A$, $a_i\in\mathfrak{m}$ при $i<0$, $a_0\in A^\times$ и $a_i=0$ при $i\ll 0$.*

Элементы $a_i\in A$ называются *координатами Витта*.

Теорема 6.3. *Пусть f и g элементы группы $A((t))^\times$ с координатами Витта (a_i) и (b_i). Тогда*

$$\langle f,g\rangle=(-1)^{w(f)w(g)}\frac{b_0^{w(f)}}{a_0^{w(g)}}\prod_{i,j\geqslant 1}\left(\frac{1-a_{-i}^{j/(i,j)}b_i^{i/(i,j)}}{1-a_i^{j/(i,j)}b_{-i}^{i/(i,j)}}\right)^{(i,j)}.$$

Примеры. 1. Если $A=F$, то это – ручной символ.

2. Если $A=F[\varepsilon]/(\varepsilon^3)$, то $\langle 1-\varepsilon f,1-\varepsilon g\rangle=1+\varepsilon^2\mathrm{Res}_{t=0}(gdf)$ для любых $f,g\in F((t))$.

3. Если A – $\mathbb{Q}$-алгебра, и $f\in 1+\mathfrak{m}((t))$, то $\langle f,g\rangle=\exp\mathrm{Res}_{t=0}(\log f\cdot d\log g)$ для любого $g\in A((t))^\times$.

Свойства символа Конту-Каррэра. Пусть $f,g\in A((t))^\times$. Тогда

(1) $\langle f,gh\rangle=\langle f,g\rangle\langle f,h\rangle$.
(2) $\langle f,g\rangle=\langle g,f\rangle^{-1}$.
(3) $\langle f,-f\rangle=1$.
(4) $\langle f,1-f\rangle=1$, если $1-f\in A((t))^\times$.
(5) Если $\varphi\in A((t))^\times$ и $w(\varphi)>0$, то $\langle f,g\circ\varphi\rangle=\langle N_\varphi f,g\rangle$, где $N_\varphi: A((t))^\times\longrightarrow A((t))^\times$ – норма (рассматриваем $A((t))$ как свободный $A((t))$-модуль ранга $w(\varphi)$ относительно вложения $h\mapsto h\circ\varphi$). В частности, $\langle f\circ\tau,g\circ\tau\rangle=\langle f,g\rangle$, если $\tau\in A((t))^\times$ и $w(\tau)=1$.

Теорема 6.4 (Закон взаимности). $\prod_{s\in X}\langle f,g\rangle_s=1$ *для всех $f,g\in R^\times:=(A\otimes_F F(X))^\times$.*

Доказательство. Пусть $S\subset X$ – конечное множество точек, содержащее все нули и полюса f и g. Выбор униформизующих в точках S определяет вложение F-алгебр $R_0':=\Gamma(X\backslash S,\mathcal{O}_X)\hookrightarrow F((t))^S=:V$ (прямая сумма копий $F((t))$, пронумерованных множеством S). Ясно, что существует такое F-подпространство $M_0\subset F((t))^S$, соизмеримое с $V_+:=F[[t]]^S$, что $F((t))^S=M_0\oplus R_0'$. (Это следует из того, что ядро и коядро сложения $F[[t]]^S\oplus R_0'\longrightarrow F((t))^S$ конечномерны, т.к. изоморфны, соответственно, $F[[t]]^S\cap R_0'=\Gamma(X,\mathcal{O}_X)$ и $\frac{F((t))^S}{R_0'+F[[t]]^S}=H^1(X,\mathcal{O}_X)$.) Положим $M=M_0\otimes_F A$. Тогда $V=M\oplus R'$, где $R':=R_0'\otimes_F A$, и $M\sim V_+$.

Будем рассматривать элементы R' как операторы умножения на них на модуле $A((t))^S$.

Поскольку $\{\sigma,\tau\}^V_{V_+}$ зависит только от класса соизмеримости V_+ (свойство (4)), получаем $\{f,g\}^V_{V_+} = \{f,g\}^V_M$. Из свойства (5) следует, что $\{f,g\}^V_{R'} = 1$. Следующий факт утверждает, что $\{f,g\}^V_M\{f,g\}^V_{R'} = 1$, и значит, $\{f,g\}^V_{V_+} = 1$.

Предложение 6.5. *Пусть $V = V_+\oplus V_-$ – разложение в прямую сумму свободных A-модулей, и $\sigma,\tau \in G^V_{V_+}\cap G^V_{V_-}$ коммутируют. Тогда $\{\sigma,\tau\}^V_{V_+}\{\sigma,\tau\}^V_{V_-} = (-1)^{\mu_+\nu_-+\mu_-\nu_+}$, где $\mu_\pm := \mathrm{ind}^V_{V_\pm}\sigma$, $\nu_\pm := \mathrm{ind}^V_{V_\pm}\tau$ и $\mathrm{ind}^V_{V_+} : G^V_{V_+} \longrightarrow \mathbb{Z}$, $\sigma \mapsto \mathrm{rk}(V_+/P) - \mathrm{rk}(\sigma V_+/P)$ для любого свободного A-модуля $P \subset V_+\cap\sigma V_+$ с конечно порождёнными факторами V_+/P и $\sigma V_+/P$.*

(Это не зависит от P, зависит только от класса соизмеримости V_+, и $\mathrm{ind}^V_{V_+}$ – гомоморфизм.)

Пример. $\mathrm{ind}^{A((t))}_{A[[t]]} f = \mathrm{ind}^{(A/\mathfrak{m})((t))}_{(A/\mathfrak{m})[[t]]} f = -w(f)$.

Из бимультипликативности (свойство (3)) и следующего утверждения получается тождество $\{f,g\}^V_{V_+} = \prod_{s\in S}\{f_s,g_s\}^{A((t))}_{A[[t]]}(-1)^{\sum_{s\neq s'\in S} w_s(f)w_{s'}(g)} = (-1)^{(\sum_{s\in S} w_s(f))(\sum_{s\in S} w_s(g))}\prod_{s\in S}\langle f_s,g_s\rangle$.

Останется только заметить, что $\sum_{s\in S} w_s(f)$ – степень главного дивизора, т.е. 0.

Предложение 6.6. *Пусть $V = V_0\oplus V_1$ – разложение в прямую сумму свободных A-модулей, и $V_{i+} = V_i \cap V_+$. Предположим, что $V_+ = V_{0+}\oplus V_{1+}$. Пусть $\sigma_0,\sigma_1 \in \begin{pmatrix} G^{V_0}_{V_{0+}} & 0 \\ 0 & \mathbf{1}_{V_1}\end{pmatrix} \subseteq G^V_{V_+}$, т.е. $\sigma_i|_{V_0} \in G^{V_0}_{V_{0+}}$ и $\sigma_i|_{V_1} = 1$. Пусть $\tau \in \begin{pmatrix} \mathbf{1}_{V_0} & 0 \\ 0 & G^{V_1}_{V_{1+}}\end{pmatrix} \subseteq G^V_{V_+}$, т.е. $\tau|_{V_1} \in G^{V_1}_{V_{1+}}$ и $\tau|_{V_0} = 1$. Тогда $\{\sigma_0|_{V_0},\sigma_1|_{V_1}\}^{V_0}_{V_{0+}} = \{\sigma_0,\sigma_1\}^V_{V_+}$ и $\{\sigma_0,\tau\}^V_{V_+} = (-1)^{\nu_0\nu_1}$, где $\nu_0 := \mathrm{ind}^{V_0}_{V_{0+}}\sigma_0|_{V_0} = \mathrm{ind}^V_{V_+}\sigma_0$ и $\nu_1 := \mathrm{ind}^{V_1}_{V_{1+}}\tau|_{V_1} = \mathrm{ind}^V_{V_+}\tau$.*

7. p-адические периоды

Неархимедовы локальные поля (т.е. $\mathbb{R}$ и $\mathbb{C}$) возникли в анализе, и естественно спросить, насколько основные понятия анализа переносятся на p-адическую ситуацию. В частности, нельзя ли построить p-адическое интегрирование?

Точнее, пусть X – многообразие над p-адическим полем k, $\omega \in \Gamma(X,\Omega^q_{X/k})$ – регулярная q-форма на X, и мы хотим проинтегрировать ω по «циклу». Ясно, что из-за полной несвязности поля k обычные циклы смысла не имеют, кроме как если $q = 0$. В этом случае «интеграл 0-формы ω по циклу P» – это значение $\omega(P)$.

Рассмотрим теперь случай $q = 1$. Что такое 1-циклы? Как известно, первые гомологии связного топологического пространства совпадают с максимальным абелевым фактором его фундаментальной группы, т.е. группы автоморфизмов его универсального абелева накрытия, другими словами, с группой автоморфизмов его универсального абелева накрытия. В алгебраической ситуации у нас нет универсальных накрытий, но их можно приближать произвольными конечными. Определим $\pi_1^{\mathrm{alg}}(X) := \varprojlim \mathrm{Aut}(X'/X)$, где X' пробегает все связные неразветвлённые накрытия Галуа X. Ясно, что если X – комплексное многообразие, то $\pi_1^{\mathrm{alg}}(X)$ – проконечное пополнение обычной фундаментальной группы $\pi_1(X)$. Определим $H_1^{\text{ét}}(X) := \varprojlim \mathrm{Aut}(X'/X)$, где X' пробегает все связные неразветвлённые абелевы накрытия X. В дальнейшем мы будем использовать обозначение $\overline{X} := X\times_k \overline{k}$.

Примеры. 1. Если $X = \mathbb{G}_{m,k} := \mathbf{Spec}k[x,\frac{1}{x}] = \mathbb{A}_{\overline{k}}\backslash\{0\}$, то $H_1^{\text{ét}}(\overline{X}) = \pi_1^{\mathrm{alg}}(\overline{X}) = \varprojlim \mu_N =: \widehat{\mathbb{Z}}(1) <<= \log 1 >>$, т.к. по теории Куммера поле функций циклического накрытия степени N получается присоединением корня N-ой степени из некоторой функции, а неразветвлённость означает, что такой функцией может быть только кратное степени x.

2. Если X – гладкое проективное многообразие над k, то $H_1^{\text{ét}}(\overline{X}) := \varprojlim \mathrm{Alb}(\overline{X})_N \cong \widehat{\mathbb{Z}}^{b_1}$ – обратный предел подгрупп кручения порядка N в многообразии Альбанезе $\mathrm{Alb}(\overline{X})$, где $b_1 = 2\dim_k \Gamma(X, \Omega^1_{X/k})$. Многообразие $\mathrm{Alb}(X)$ (и отображение Альбанезе) определяется как единственное абелево многообразие (и отображение в него) (переводящее в нуль какую-нибудь отмеченную точку), через которое пропускается (единственным образом) отображение из X в любое абелево многообразие.

Заметим, что $G_{\overline{k}/k}$ естественно действует на $H_1^{\text{ét}}(\overline{X})$.

Чем бы ни было интегрирование 1-форм, хотелось бы, чтобы это было естественным непрерывным билинейным отображением $\Gamma(X, \Omega^1_{X/k}) \times H_1^{\text{ét}}(\overline{X}) \longrightarrow A$, где A – некоторая группа значений. Если группа A – p-адическая, т.е. $A = \varprojlim A/p^N A$, то из условия непрерывности следует, что интегрирование пропускается через фактор $H_1^{\text{ét}}(\overline{X}, \mathbb{Z}_p) := \varprojlim \mathrm{Aut}(X'/X) = \varprojlim \mathrm{Alb}(\overline{X})_{p^N}$, где X' пробегает все связные неразветвлённые абелевы накрытия X p-примарных степеней, группы $H_1^{\text{ét}}(\overline{X})$.

Пример 1 в сочетании со следующим фактом показывает, что $\mathbb{C}_p$ не может быть естественной областью ненулевых значений p-адических интегралов формы $\frac{dx}{x}$. Другими словами, «в $\mathbb{C}_p$ нет числа $2\pi\sqrt{-1}$».

Теорема 7.1 (Тэйт, [T]). *Для любого $\mathbb{Z}_p[G_{\overline{k}/k}]$-модуля M положим $M(i) := M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)^{\otimes i}$ при $i \geqslant 0$ и $M(i) := \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p(1)^{\otimes(-i)}, M)$ при $i < 0$. Тогда* $H^0(G_{\overline{k}/k}, \mathbb{C}_p(i)) = \begin{cases} k, & \text{если } i = 0, \\ 0, & \text{если } i \neq 0. \end{cases}$

Заметим, что $\mathbb{C}_p(i)$ – непрерывное, но не гладкое, полулинейное представление. Теорему 7.1 можно переформулировать как утверждение о том, что гладкая часть $\mathbb{C}_p(i)$ – ненулевая только при $i = 0$, и в этом случае равна k.

Поскольку слои накрытия Галуа $X' \longrightarrow X$ – $\mathrm{Aut}(X'/X)$-торсоры, любой элемент $\pi_1(X)$ определяется парой точек универсального накрытия X с общим образом в X. Алгебраический вариант: парой согласованных наборов точек конечных накрытий $(P_\alpha, Q_\alpha \in X_\alpha)$.

Предположим, что все конечные накрытия X' допускают «хорошие» модели $\mathfrak{X}'$ над $\mathcal{O}_{\overline{k}}$. Например, это очевидно верно для $\mathbb{G}_m$.

В наших примерах можно представлять классы в $H_1^{\text{ét}}(\overline{X}, \mathbb{Z}_p)$ как $(P_j \in \mathrm{Alb}(\overline{X})_{p^j})_{j \geqslant 1}$ или $(P_j \in \mu_{p^j})_{j \geqslant 1}$, где $p \cdot P_{j+1} = P_j$. Тогда, если $\omega \in \Gamma(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_k})$, то $(\omega(P_j))_{j \geqslant 1} \in \varprojlim(\Omega^1_{\mathcal{O}_{\overline{k}}/\mathcal{O}_k}, \times p)$, где обратная система образована по отношению к умножению на p.

Теорема Фонтэна (задача 4) экзамена утверждает, что $\varprojlim(\Omega^1_{\mathcal{O}_{\overline{k}}/\mathcal{O}_k}, \times p) = \mathbb{C}_p(1)$, т.е. получается естественное отображение $\Gamma(X, \Omega^1_{X/k}) \otimes_{\mathbb{Z}_p} H_1^{\text{ét}}(\overline{X}, \mathbb{Z}_p) \longrightarrow \mathbb{C}_p(1)$.

Вводится некоторое полное кольцо дискретного нормирования $\mathbf{B}^+_{\mathrm{dR}}$, в которое естественно вложено $\overline{k}$ с плотным образом, и присоединённые факторы степеней максимального идеала которого изоморфны $\mathbb{C}_p(i)$, $i \geqslant 0$ (в частности, поле вычетов отождествлено с $\mathbb{C}_p$).

Определим индуктивно $\mathcal{O}^{(0)}_{\overline{k}} := \mathcal{O}_{\overline{k}}$ и $\mathcal{O}^{(j)}_{\overline{k}}$ – ядро $\mathcal{O}^{(j-1)}_{\overline{k}} \xrightarrow{d} \mathcal{O}_{\overline{k}} \otimes_{\mathcal{O}^{(j-1)}_{\overline{k}}} \Omega^1_{\mathcal{O}^{(j-1)}_{\overline{k}}/\mathcal{O}_k}$. Ясно, что $\mathcal{O}^{(j)}_{\overline{k}}$ – подкольцо в $\mathcal{O}_{\overline{k}}$, содержащее $\mathcal{O}_{k^{\mathrm{nr}}}$. Определим $\mathbf{B}^+_{\mathrm{dR}} := \varprojlim \overline{k}/p^i \mathcal{O}^{(j)}_{\overline{k}}$.

Поле частных $\mathbf{B}_{\mathrm{dR}}$ «$\cong \mathbb{C}_p((2\pi\sqrt{-1}))$» кольца $\mathbf{B}^+_{\mathrm{dR}}$ «$\cong \mathbb{C}_p[[2\pi\sqrt{-1}]]$» называется фонтэновским полем периодов, т.к. оно позволяет сравнить этальные когомологии и когомологии де Рама: $H^i_{\mathrm{dR/k}}(X) = [H^i_{\text{ét}}(\overline{X}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} \mathbf{B}_{\mathrm{dR}}]^{G_{\overline{k}/k}}$.

Приложение A. Экзамен

(1) Докажите, что пополнение $\mathbb{C}_p$ алгебраического замыкания поля p-адических чисел алгебраически замкнуто.

(2) Докажите, что индекс подгруппы n-ых степеней в мультипликативной группе локального поля k равен $|\mu_n(k)| \cdot n \cdot |n|_k^{-1} \leqslant \infty$, где $\mu_n(k)$ – группа корней n-ой степени из единицы в k, и $|n|_k = \begin{cases} |\mathcal{O}_k/(n)|^{-1}, & \text{если } k \text{ неархимедово,} \\ n, & \text{если } k = \mathbb{R}, \\ n^2, & \text{если } k = \mathbb{C}. \end{cases}$

(3) Пусть k – локальное поле. Опишите группу Галуа расширения $k^{\mathrm{ab}}/k(\mu_\infty)$.

(4) Пусть k – p-адическое поле. Рассмотрим обратную (проективную) систему $A_i = \Omega_{\mathcal{O}_{\overline{k}}/\mathcal{O}_k}$, $i \geqslant 0$ с отображениями $A_{i+1} \xrightarrow{\times p} A_i$ умножения на p. Докажите, что обратный предел этой системы $\varprojlim A_i$ канонически изоморфен $\mathbb{C}_p(1) := \mathbb{C}_p \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$, где $\mathbb{Z}_p(1) := \varprojlim \mu_{p^i}$ – обратный предел системы $B_i = \mu_{p^i} \subset \overline{k}$, $i \geqslant 0$ с отображениями $B_{i+1} \xrightarrow{.p} B_i$ возведения в степень p.

Список литературы

[AP] G.W.Anderson, F.Pablos Romo, *Simple proofs of classical explicit reciprocity laws on curves using determinant groupoids over an artinian local ring,* `http://arXiv.org`

F.Pablos Romo, *On the Steinberg property of the Contou-Carrère symbol,* `math.AC/0602374`

[AM] M.F.Atiyah, I.G.Macdonald, **Введение в коммутативную алгебру.** «Мир», 19...

[AT] E.Artin, J.Tate, **Class field theory.** Benjamin, 19...

[АТЧ] **Алгебраическая теория чисел.** (Сб. под ред. Касселса, Фрелиха), Москва, «Мир», 1969.

[Б] Н.Бурбаки, **Алгебра,** гл. VIII, Москва, «Мир», 19...

[В] А.Вейль, **Основы теории чисел.** Москва, «Мир», 1972.

[вдВ] ван-дер-Варден, **Алгебра.** 19...

[C] P.Colmez, *Les nombres algébriques sont dense dans* $\mathbf{B}_{dR}^+$, в Astérisque **223** (1994), 103–111.

[F] J.-M.Fontaine, *Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux,* Invent.Math. **65** (1982), 379–409, `http://gdz.sub.uni-goettingen.de`.

[И] К.Ивасава, **Локальная теория полей классов.** Москва, «Мир», 1983.

[I] Y.Ihara, **On congruence monodromy problems. Vol. 1.** Lecture Notes, No. 1 Dept. of Math., Univ. of Tokyo, 1968.

[Jac] N.Jacobson, **Lectures in abstract algebra, Vol III: Theory of fields and Galois theory.** D. Van Nostrand Co., Inc., Princeton, N.J.-Toronto, Ont.-London-New York 1964.

[K] W.Krull, *Galoissche Theorie der unendlichen algebraischen Erweiterungen,* Math. Ann. 100 (1928), no. 1, 687–698, `http://gdz.sub.uni-goettingen.de`.

[La] С.Ленг, **Алгебраические числа.** «Мир», 1966.

[ПШ-Ш] И.И.Пятецкий-Шапиро, И.Р.Шафаревич, *Теория Галуа трансцендентных расширений и униформизация,* Изв. АН СССР, сер. матем. **30** (1966), 671–704.

[C1] Ж.-П.Серр, **Алгебраические группы и поля классов.** «Мир», 1968.

[С-КГ] Ж.-П.Серр, **Когомологии Галуа.** «Мир», 1968.

[Ск] А.Н.Скоробогатов, **Введение в теорию полей классов.** 1995, `http://www.mccme.ru`.

[Т] Дж.Тэйт, *p-делимые группы,* сб. переводов Математика, 3–25.

[Ш] Г.Шимура, **Введение в арифметическую теорию автоморфных функций,** §6.3, «Мир», 1973.