Введение в теорию полей классов

А.Н.Скоробогатов

Вторая часть

Оглавление

1. Когомологии Тейта

1.1 Когомологии групп

Пусть A - G-модуль, и A^G - подгруппа G-инвариантных элементов.

Задача 1.1.1 Соответствие $A \mapsto A^G$ есть точный слева аддитивный функтор из категории G-модулей в категорию абелевых групп.

Согласно общей философии гомологической алгебры, такой функтор имеет "когомологическое продолжение" - правые производные функторы, обозначаемые $H^i(G,A)$. Напомним коротко их конструкцию. Берется (любая) проективная резольвента тривиального G-модуля $\mathbf{Z}$, т.е. комлекс

$$\ldots \to P_1 \to P_0 \to 0,$$

продолжающийся до точной последовательности:

$$\ldots \to P_1 \to P_0 \to \mathbf{Z} \to 0$$

(т.е. P_i - проективные G-модули = те, для которых функтор $Hom_G(P,\cdot)$ переводит короткие точные последовательности в короткие точные последовательности) и группа $H^i(G,A)$ полагается по определению равной i-той группе когомологий комплекса

$$0 \to Hom_G(P_0,A) \to Hom_G(P_1,A) \to \ldots$$

Задача 1.1.2 $H^0(G,A) = Hom_G(\mathbf{Z},A) = A^G$.

Задача 1.1.3 Доказать, что свободный G-модуль (т.е. изоморфный прямой сумме групповых колец $\mathbf{Z}[G]$) проективен.

Задача 1.1.4 (а) Доказать, что для коиндуцированного модуля $H^i(G,A) = 0, i > 0$. (Модуль A называется коиндуцированным, если $A = Hom(\mathbf{Z}[G],X)$, где X- тривиальный G-модуль.) (б) Доказать, что когомологическое продолжение функтора $A \mapsto A^G$ определено однозначно. Использовать каноническое вложение A в $B = Hom(\mathbf{Z}[G],A_0)$, где A_0 изоморфно A как абелева группа с тривиальным действием G, и достраивая это вложение до короткой точной последовательности

$$0 \to A \to B \to C \to 0$$

отождествить $H^i(G,A)$ с $H^{i-1}(G,C)$. Этот важный прием называется "сдвиг размерности". Он позволяет по индукции доказывать для всех групп когомологий утверждение, верное для H^0. Примеры будут даны ниже.

1.2 Стандартный комплекс

Практически удобно выбрать некоторую стандартную свободную резольвенту $\mathbf{Z}$. Пусть $L_i = \mathbf{Z}[G^{i+1}]$ с диагональным действием G, $d : L_i \to L_{i-1}$ задается как

$$d(g_0, \ldots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \ldots, \hat{g}_j, \ldots, g_i).$$

Отображение $L_0 \to \mathbf{Z}$ переводит все образующие g в 1.

Задача 1.2.1. Доказать точность комплекса $\ldots \to L_1 \to L_0 \to \mathbf{Z} \to 0$.

Определение. $H^i(G, A) = H^i(Hom_G(L, A))$

Из диагональности действия G следует, что функция f из $Hom_G(L_i, A)$ определяется своими значениями на элементах вида $(1, g_1, g_1g_2, \ldots, g_1 \ldots g_i)$. Полагая $\phi(g_1, \ldots, g_i) = f((1, g_1, g_1g_2, \ldots, g_1 \ldots g_i))$ получаем стандартное описание дифференциала для "неоднородных коцепей":

$$(d\phi)(g_1, \ldots, g_{i+1}) = g_1\phi(g_2, \ldots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j \phi(g_1, \ldots, g_jg_{j+1}, \ldots, g_{i+1}) + (-1)^{i+1}\phi(g_1, \ldots, g_i).$$

Отсюда описание 1-коциклов как скрещенных гомоморфизмов и т.д.

Пусть есть гомоморфизм групп $f : G \to G'$. Он порождает гомоморфизм соответствующих комплексов $L(G) \to L(G')$, а значит и гомоморфизмы групп когомологий $f^* : H^i(G', A) \to H^i(G, A)$ (здесь A наделяется структурой G-модуля посредством f). Если f -вложение, то f^* называется ограничением и обозначается Res.

Пусть $H \subset G$ - нормальная подгруппа. Можно показать, что $H^i(H, A)$ имеет естественную структуру G/H-модуля. Спектральная последовательность композиции функторов $A \mapsto A^H$ и $B \mapsto B^{G/H}$ называется спектральной последовательностью Хохшильда-Серра и записывается в виде (E_2-члены)

$$H^p(G/H, H^q(H, A)) \Rightarrow H^{p+q}(G, A).$$

Точная последовательность членов первой степени часто называется последовательностью "ограничение -инфляция":

$$0 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A)$$

Здесь вторая стрелка - ограничение, а первая получается композицией коцикла G/H с естественным отображением $G \to G/H$, а затем вложением этого G-модуля A^H в A.

Задача 1.2.2 Не пользуясь спектральной последовательностью, непосредственно доказать точность последовательности "ограничение-инфляция".

1.3 Гомологии групп

Пусть $A \otimes B$ есть тензорное произведение $\mathbf{Z}$-модулей, а $A \otimes_G B$ есть тензорное произведение G-модулей. Заметьте, что в выражении $A \otimes_G B$, A понимается как правый G-модуль со структурой $ag = g^{-1}a$.

Обозначим $I_G = \langle g-1 \rangle \subset \mathbf{Z}[G]$ - идеал в $\mathbf{Z}[G]$, $A_G = \mathbf{Z} \otimes_G A = A/I_GA$ - наибольший G-инвариантный фактор A.

Задача 1.3.1 Доказать, что $A \otimes_G B = (A \otimes B)_G$.

Теория гомологий групп строится параллельно теории когомологий, $H_i(G, A)$ суть левые производные функторы точного справа функтора $A \mapsto A_G$. Они определяются как группы гомологий комплекса

$$\ldots \to P_1 \otimes_G A \to P_0 \otimes_G A \to 0.$$

Задача 1.3.2 Сформулировать и доказать аналоги задач пункта 1.1 (вместо коиндуцированных модулей надлежит рассматривать индуцированные - вида $\mathbf{Z}[G] \otimes X$, где X- тривиальный G-модуль.)

Задача 1.3.3 $H_1(G, \mathbf{Z}) = G^{ab} = G/[G, G]$.

Аналогично случаю когомологий гомоморфизм групп $f : G \to G'$ и порождаемый им гомоморфизм комплексов $L(G) \to L(G')$ определяют гомоморфизмы групп гомологий $f_* : H_i(G, A) \to H_i(G', A)$. Если f -вложение, то f_* называется коограничением и обозначается $Cores$.

Сдвиг размерности для гомологий устроен так. Высшие гомологии коиндуцированного модуля $B = Hom(\mathbf{Z}[G], A_0)$ равны нулю, имеется каноническая сюръекция $Hom(\mathbf{Z}[G], A_0) \to A$, достраивая ее до короткой точной последовательности

$$0 \to C \to B \to A \to 0$$

можно отождествить $H_i(G, A)$ с $H_{i-1}(G, C)$.

1.4 Группы когомологий Тейта

Пусть G - конечная группа.

Задача 1.4.1 Доказать, что в этом случае $\mathbf{Z}[G] \otimes X = Hom(\mathbf{Z}[G], X)$, где X - тривиальный G-модуль. Что не проходит, если G бесконечна?

Таким образом, в случае конечных групп индуцированные и коиндуцированные модули совпадают.

Пусть $N = \sum_{g \in G} g \in \mathbf{Z}[G]$. Так как $I_G A$ лежит в ядре умножения на N, а образ лежит в G-инвариантной части A, то определен гомоморфизм $N_* : H_0(G, A) \to H^0(G, A)$.

Определение. Группы когомологий Тейта задаются так: $\hat{H}^i(G, A) = H^i(G, A)$, для $i > 0$; $\hat{H}^i(G, A) = H_{-i-1}(G, A)$, для $i < -1$; $\hat{H}^{-1}(G, A) = Ker(N_*)$; $\hat{H}^0(G, A) = Coker(N_*) = A^G/NA$.

Задача 1.4.2 Доказать, что когомологии Тейта индуцированного модуля равны 0.

Задача 1.4.3 Когомологии Тейта можно считать при помощи бесконечной в обе стороны точной последовательности (“полной резольвенты”)

$$\ldots \to P_1 \to P_0 \to P_0^* \to P_1^* \to \ldots,$$

где P^* обозначает $Hom(P, \mathbf{Z})$, а гомоморфизм из P_0 в P_0^* есть композиция проекции $P_0 \to \mathbf{Z}$ с двойственным к ней отображением.

Группы когомологий Тейта имеют много приятных свойств. Во-первых, каждой короткой точной последовательности G-модулей отвечает бесконечная в обе стороны длинная точная последовательность когомологий Тейта. Для этого надо “склеить” между собой соответствующие последовательности для гомологий и когомологий, применив “лемму о змее” (см. самое начало ”Коммутативной алгебры” Бурбаки).

Во-вторых, из совпадения индуцированных и коиндуцированных модулей и задачи 1.4.2 следует, что “сдвиг размерности” работает для когомологий Тейта в обе стороны. Тем самым, для подгруппы $H \subset G$ гомоморфизмы Res и $Cores$ определены для всех $\hat{H}^i(G, A)$.

Задача 1.4.4 Композиция $Cores \circ Res$ совпадает с умножением на индекс H в G. (Подсчитать для $\hat{H}^0(G, A)$ и применить сдвиг размерности.)

Отсюда следует, что порядок любого элемента $\hat{H}^i(G, A)$ делит порядок G. (Взять $H = 1$) Кроме того, если A - конечно порожден, то $\hat{H}^i(G, A)$ конечны (т.к. конечно порождены).

1.5 Когомологии Тейта циклической группы

Пусть G - конечная циклическая группа, $G = \langle g \rangle$. Согласно задаче 1.4.3 когомологии Тейта можно считать при помощи полной резольвенты. Рассмотрим

$$\ldots \to P_1 \to P_0 \to \mathbf{Z} \to 0$$

где все $P_i = \mathbf{Z}[G]$, дифференциалы с четными номерами - умножение на $N = \sum_{g \in G} g$, а с нечетными - на $T = g - 1$. Построенная точная последовательность является свободной резольвентой $\mathbf{Z}$. Полная резольвента выглядит так:

$$\ldots \to \mathbf{Z}[G] \to \mathbf{Z}[G] \to \mathbf{Z}[G] \to \ldots,$$

где стрелки - чередующиеся умножения на N и T. Отсюда

Предложение 1.5.1 Когомологии Тейта конечной циклической группы таковы: $\hat{H}^i(G, A) = A^G/NA$, для $i = 2j$; $\hat{H}^i(G, A) = Ker(N)/I_G A$, для $i = 2j + 1$.

Определение 1.5.2 Если A - G-модуль, когомологии Тейта которого конечны, то обозначим $h_0(A) = |\hat{H}^0(G, A)|$, $h_1(A) = |\hat{H}^1(G, A)|$. Рациональное число $h(A) = h_0(A)/h_1(A)$ называется индексом Эрбрана.

Предложение 1.5.3 Если в точной последовательности G-модулей

$$0 \to A \to B \to C \to 0$$

индекс Эрбрана определен у двух из этих трех модулей, то он определен и у третьего, причем $h(B) = h(A)h(C)$.

Идея доказательства: длинная точная последовательность когомологий Тейта периодична с периодом 6, т.е. сворачивается в точный шестиугольник.

2. Теорема Тейта-Накаямы

2.1 Когомологически тривиальные G-модули

Мы продолжаем считать G конечной группой.

Определение. G-модуль A называется когомологически тривиальным, если $\hat{H}^i(H, A) = 0$ для любой подгруппы $H \subset G$.

Цель этого параграфа - дать необходимые и достаточные условия когомологической тривиальности (см. теорему 2.1.7).

Теорема 2.1.1 Пусть G - p-группа, т.е. порядок G есть степень p, A - G-модуль, такой что $pA = 0$. Тогда следующие утверждения эквивалентны:

(i) A свободен над кольцом $\mathbf{F}_p[G]$;
(ii) A - индуцированный;
(iii) A - когомологически тривиальный;
(iv) $\hat{H}^i(G, A) = 0$ для некоторого i.

Доказательство. Импликации $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv)$ очевидны. Используя сдвиг размерности, построим G-модуль B, $pB = 0$, такой что

$$\hat{H}^n(G, A) = \hat{H}^{n-2-i}(G, B).$$

Тогда B не имеет первой группы гомологий. Мы собираемся доказать, что любой такой модуль свободен над кольцом $\mathbf{F}_p[G]$. Тогда все остальные его группы когомологий Тейта также будут нулевыми, и то же самое будет выполнено для A. Применяя то же утверждение для A получаем (i).

Лемма 2.1.2 Пусть $pA = 0$ и $H^0(G, A) = 0$ или $H_0(G, A) = 0$, тогда $A = 0$.

Доказательство. Утверждение для H^0: Если A ненулевой, то у него есть ненулевой элемент. Порожденный им подмодуль конечен и имеет p^i элементов, он состоит из G-орбит, причем все нетривиальные орбиты состоят из p^j элементов. Значит, число инвариантных элементов делится на p, а так как оно содержит 0, то $A^G \neq 0$. Утверждение для группы гомологий. Пусть $A' = Hom(A, \mathbf{F}_p$, тогда если $A'^G \neq 0$, то A обладает ненулевым G-гомоморфизмом в тривиальный модуль $\mathbf{F}_p$, т.е. $A_G \neq 0$. Значит, $A' = 0$, откуда $A = 0$.

Лемма 2.1.3 Пусть $pA = 0$ и $H_1(G, A) = 0$, тогда A свободен над $\mathbf{F}_p[G]$.

Доказательство. Выберем набор элементов A, образы которых в $H_0(G, A)$ порождают его как векторное пространство над $\mathbf{F}_p$. Пусть A' - подмодуль, порожденный этими элементами, $A'' = A/A'$. Из точной последовательности гомологий тогда следует, что $H_0(G, A'') = 0$, т.е. $A = A'$. Пусть L - свободный $\mathbf{F}_p[G]$-модуль, формально порожденный этими элементами, и $\phi : L \to A$ - соответствующий эпиморфизм. Ясно, что ϕ_* - изоморфизм. Пусть $L' = Ker(\phi)$, тогда из условия леммы и точной последовательности гомологий получаем $H_0(G, L') = 0$, т.е. $A = L$.

Теорема 2.1.1 доказана.

Теорема 2.1.4 Пусть G - p-группа, A - G-модуль без p-кручения. Тогда следующие утверждения эквивалентны:
(i) A - когомологически тривиальный;
(ii) $\hat{H}^i(G, A) = \hat{H}^{i+1}(G, A) = 0$ для некоторого i;
(iii) A/pA - свободен над кольцом $\mathbf{F}_p[G]$.

Доказательство. Импликация $(i) \Rightarrow (ii)$ тривиальна. Из отсутствия в A p-кручения вытекает точность последовательности G-модулей

$$0 \to A \to A \to A/pA \to 0,$$

где первая стрелка есть умножение на p. Соответствующая длинная точная последовательность когомологий Тейта в сочетании с (ii) и Теоремой 2.1.1 дает (iii). Пусть $H \subset G$ - произвольная подгруппа. Та же последовательность показывает, что умножение на p - изоморфизм $\hat{H}^n(H, A)$ для любого n. По задаче 1.4.4 последняя группа убивается умножением на степень p. Единственная возможность совместить эти два свойства - $\hat{H}^n(H, A) = 0$.

Следствие 2.1.5 Пусть A - когомологически тривиальный G-модуль, свободный как $\mathbf{Z}$-модуль; B - G-модуль без кручения. Тогда $Hom(A, B)$ когомологически тривиален.

Доказательство. Ясно, что $N = Hom(A, B)$ не имеет кручения. Покажем, что выполнен пункт (iii) теоремы 2.1.4. Имеем

$$N/pN = Hom(A/pA, B/pB).$$

По теореме 2.1.4 A/pA - индуцированный. Докажем, что всегда, когда M - индуцированный, а N - любой, $Hom(M, N)$ - тоже индуцированный. M есть прямая сумма подгрупп вида gK, где K - подгруппа в M. Но тогда $Hom(M, N)$ есть прямая сумма подгрупп вида

$$Hom(gK, N) = Hom(gK, g^{-1}N) = gHom(K, N),$$

что и требовалось.

Теорема 2.1.6 Пусть G - конечная группа, A - G-модуль, свободный как $\mathbf{Z}$-модуль. Пусть G_p обозначает силовскую p-подгруппу G. Тогда следующие утверждения эквивалентны:
(i) A - когомологически тривиальный G_p-модуль для всех p;
(ii) A - проективный G-модуль.

Доказательство. $(ii) \Rightarrow (i)$: проективный модуль есть прямое слагаемое свободного, следовательно, он когомологически тривиален.

$(i) \Rightarrow (ii)$: возьмем точную последовательность

$$0 \to Q \to F \to A \to 0,$$

где F - свободный G-модуль. A свободен как $\mathbf{Z}$-модуль, поэтому

$$0 \to Hom(A, Q) \to Hom(A, F) \to Hom(A, A) \to 0,$$

- точная последовательность. По следствию 2.1.5 $Hom(A,Q)$ - когомологически тривиален для любой силовской подгруппы. По задаче 1.4.4 любой элемент любой группы его когомологий Тейта убивается умножением на $|G|/|G_p|$, а так как эти числа не имеют общего делителя, то $Hom(A,Q)$ - когомологически тривиален. В частности, $H^1(G, Hom(A,Q)) = 0$, следовательно, отображение $Hom_G(A,F) \to Hom_G(A,A)$ - сюръективно, и тождественное отображение A на себя поднимается до вложения G-модулей $A \to F$, расщепляющего исходную точную последовательность и делающего A прямым слагаемым свободного модуля.

Теорема 2.1.7 G-модуль A когомологически тривиален тогда и только тогда, когда для любого простого p существует целое число n_p, для которого

$$\hat{H}^{n_p}(G_p, A) = \hat{H}^{n_p+1}(G_p, A) = 0.$$

Доказательство. Возьмем точную последовательность

$$0 \to Q \to F \to A \to 0,$$

где F - свободный G-модуль. Из длинной точной последовательности когомологий Тейта следует, что Q удовлетворяет условию (ii) теоремы 2.1.4, значит, это - тривиальный G_p-модуль для всех p. Тогда по теореме 2.1.6 Q - проективный G-модуль, в частности, когомологически тривиальный. Применяя еще раз длинную точную последовательность когомологий Тейта мы докажем утверждение теоремы.

Теорема 2.1.8 Пусть $f : B \to C$ - гомоморфизм G-модулей. Если для любого простого p существует целое число n_p, для которого

$$f_i^* : \hat{H}^i(G_p, B) \to \hat{H}^i(G_p, C)$$

- сюръективно для $i = n_p$, биективно для $i = n_p + 1$ и инъективно для $i = n_p + 2$, то

$$f_i^* : \hat{H}^i(H, B) \to \hat{H}^i(H, C)$$

биективно для любой подгруппы $H \subset G$ и любого i.

Доказательство. Рассмотрим точную последовательность

$$0 \to B \to C \oplus Hom(\mathbf{Z}[G], B_0) \to D \to 0,$$

где первая стрелка есть прямая сумма f и канонического вложения $B \to Hom(\mathbf{Z}[G], B_0)$ (при котором $b \in B$ переходит в $g \mapsto gb$). Длинная точная последовательность групп когомологий показывает, что D удовлетворяет условию теоремы 2.1.7, откуда наше утверждение.

2.2 $\cup$-произведение

Пусть A и B - G-модули, тогда естественное отображение

$$A^G \otimes B^G \to (A \otimes B)^G$$

продолжается единственным образом до семейства гомоморфизмов

$$\hat{H}^i(G, A) \otimes \hat{H}^j(G, B) \to \hat{H}^{i+j}(G, A \otimes B),$$

имеющих следующие свойства.

1) Пусть

$$0 \to A \to A' \to A'' \to 0$$

- точна, равно как и

$$0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0.$$

Тогда если $a'' \in \hat{H}^i(G, A'')$, $b \in \hat{H}^j(G, B)$, то

$$(\delta a'') \cup b = \delta(a'' \cup b).$$

2) Пусть

$$0 \to B \to B' \to B'' \to 0$$

- точна, равно как и

$$0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0.$$

Тогда если $a \in \hat{H}^i(G, A)$, $b'' \in \hat{H}^j(G, B'')$, то

$$a \cup (\delta b'') = (-1)^i \delta(a \cup b'').$$

(Неформально говоря, дифференциал имеет градуировку 1.)

Конструкция $\cup$-произведения требует определенного труда (из-за того, что приходится работать с бесконечными в обе стороны комплексами). Детали можно посмотреть в Касселс-Фрелих, гл. IV.7, в "Гомологической алгебре" Картана-Эйленберга, или "Когомологии групп" Брауна. $\cup$-произведение имеет также следующие свойства.

Предложение 2.2.1 (i) Ассоциативность (понимаемая в смысле канонического изоморфизма $(A \otimes B) \otimes C = A \otimes (B \otimes C)$);

(ii) суперкоммутативность: $a \cup b = (-1)^{dim(a) dim(b)} b \cup a$ (понимаемая в смысле канонического изоморфизма $A \otimes B = B \otimes A$);

(iii) $\cup$-произведение коммутирует с ограничением;

(iv) ("формула проекции") $Cores(a \cup Res(b)) = Cores(a) \cup b$.

Если задан гомоморфизм G-модулей $A \otimes B \to C$, то комбинируя с ним $\cup$-произведение получаем семейство гомоморфизмов

$$\hat{H}^i(G, A) \otimes \hat{H}^j(G, B) \to \hat{H}^{i+j}(G, C),$$

которые также называются $\cup$-произведением.

2.3 Основная теорема

Теорема 2.3.1 Пусть задан гомоморфизм G-модулей $A \otimes B \to C$, $a \in H^i(G, A)$, причем для каждого простого p существует n_p, такое что $\cup$-умножение на $Res_{G/G_p}(a)$:

$$\hat{H}^j(G_p, B) \to \hat{H}^{i+j}(G_p, C)$$

сюръективно для $j = n_p$, биективно для $j = n_p + 1$ и инъективно для $j = n_p + 2$. Тогда $\cup$-умножение на $Res_{G/H}(a)$:

$$\hat{H}^j(H, B) \to \hat{H}^{i+j}(H, C)$$

есть изоморфизм для всех j и всех подгрупп H.

Доказательство получается из теоремы 2.1.8 методом сдвига размерности (см. Касселс-Фрелих)

Теорема Тейта. Пусть A - G-модуль, $a \in H^2(G, A)$, причем для любого простого p имеем

$$H^1(G_p, A) = 0, \quad H^2(G_p, A) = \mathbf{Z}/|G_p \mathbf{Z}|$$

с образующей $Res_{G/G_p}(a)$. Тогда для всех целых n и всех подгрупп $H \subset G$ $\cup$-умножение на $Res_{G/G_p}(a)$ индуцирует изоморфизм

$$\hat{H}^n(H, \mathbf{Z}) \to \hat{H}^{n+2}(H, A)$$

Для доказательства надо взять $B = \mathbf{Z}$, $C = A$, $i = 2$, $n_p = -1$.

3. Формации классов

Пусть имеется группа G и семейство ее подгрупп конечного индекса, причем выполнены свойства:
(а) семейство замкнуто относительно конечных пересечений;
(б) любая подгруппа, содержащая элемент семейства, принадлежит ему;
(в) семейство замкнуто относительно сопряженности подгрупп.

Пусть также дан G-модуль A, удовлетворяющий свойству $A = \cup A^H$, где $H \subset G$ пробегает подгруппы из семейства со свойствами (а,б,в). Такой набор из G, семейства ее подгрупп и G-модуля A, называется формацией. Как обычно (см. гл. 10 первой части или Касселс-Фрелих, гл.5) в этой ситуации A является модулем относительно группы $\hat{G} = lim.proj(G/H)$ - непрерывным модулем в дискретной топологии, причем $\hat{G}$ рассматривается в топологии проконечной группы (здесь H пробегает нормальные подгруппы G из нашего семейства).

Обозначение: пусть $G_2 \subset G_1$ - нормальная подгруппа, тогда $H^i(G_1/G_2) := H^i(G_1/G_2, A^{G_2})$, аналогично обозначаются когомологии Тейта таких факторов. Наряду с $\hat{G}$ можно рассмотреть $\hat{G}_1$ как проективный предел G_1/G_2, где $G_2 \subset G_1$ - нормальна в G_1 и входит в наше семейство. Когомологии проконечной группы $\hat{G}_1$ определяются как индуктивный предел $H^i(G_1/G_2, A^{G_2})$ относительно отображений инфляции

$$H^i(G_1/G_2, A^{G_2}) \to H^i(G_1/G_3, A^{G_3}),$$

где $G_3 \subset G_2 \subset G_1$. Мы будем обозначать этот придел через $H^i(\hat{G}_1, A)$ (собственно говоря, это стандартное определение когомологий проконечной группы).

Аксиомы формации классов:

В придачу к свойствам, которым должна удовлетворять формация, постулируются две следующие аксиомы:

Аксиома I. Если G_2 нормальна в G_1, то $H^1(G_1/G_2) = 0$.

Используя сдвиг размерности (см. лемму 3.1), отсюда легко вывести, что упомянутые выше отображения инфляции инъективны для $i = 2$, т.е. вторые когомологии соответствующих проконечных групп суть просто объединения когомологий их конечных факторов.

Лемма 3.1 $H^i(H, A) = 0$ для $0 < i < n$ влечет точность последовательности "Res-Inf":

$$0 \to H^n(G/H, A^H) \to H^n(G, A) \to H^n(H, A).$$

Доказательство. Вложим A канонически в коиндуцированный модуль и достроим это вложение до короткой точной последовательности

$$0 \to A \to B \to C \to 0.$$

По условию соответствующая последовательность H-инвариантов точна. По предположению индукции утверждение доказано для $n-1$ и C в качестве модуля коэффицентов. Применением дифференциалов - которые суть изоморфизмы - к членам соответствующей последовательности получим искомую последовательность.

Аксиома II. Для любой подгруппы $H \subset G$ из нашего семейства существует инъективный гомоморфизм

$$inv_H : H^2(\hat{H}) \to \mathbf{Q}/\mathbf{Z},$$

такой, что если G_2 нормальна в G_1 индекса n, то

$$inv_{G_1}(H^2(G_1/G_2)) = 1/n\mathbf{Z}/\mathbf{Z},$$

и если H_2 - подгруппа H_1 индекса n, то

$$inv_{H_2} \circ Res_{H_1/H_2} = n \cdot inv_{H_1}.$$

Следствие 3.2 (а) Если $G_2 \subset G_1$ - подгруппы из нашего семейства, то отображение $Res_{G_1/G_2}: H^2(\hat{G}_1) \to H^2(\hat{G}_2)$ сюръективно.

(б) В той же ситуации отображение $Cores_{G_1/G_2}: H^2(\hat{G}_2) \to H^2(\hat{G}_1)$ инъективно, причем $inv_{G_1} \circ Cores_{G_1/G_2} = inv_{G_2}$.

Доказательство (а) легко получается из свойств inv, описанных в Аксиоме II. Отсюда следует (б) ввиду задачи 1.4.4.

Один из двух основных примеров: локальная теория

Пусть k - локальное поле, k_s - его сепарабельное замыкание, $G = Gal(k_s/k)$, $A = k_s^*$, а в качестве подгрупп рассматриваются все подгруппы G конечного индекса, факторы по которым суть группы Галуа конечных расширений k. То, что аксиомы формации удовлетворены следует из теории Галуа. Аксиома I - это теорема Гильберта 90. Гомоморфизм inv в аксиоме II - это локальный инвариант, отождествляющий группу Брауэра $Br(k) = H^2(G, k_s^*)$ (центральные простые алгебры задаются 2-коциклами) с $H^2(Gal(K/k), K^*)$, где K - максимальное неразветвленное расширение k (любая ц.п.а. распадается над неразветвленным расширением). Затем нормирование $K^* \to \mathbf{Z}$ отождествляет последнюю группу с

$$H^2(\hat{\mathbf{Z}}, \mathbf{Z}) = Hom(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z}$$

(Касселс-Фрелих, гл.VI п.1.2) При этом последний изоморфизм задается значением характера на автоморфизме Фробениусе F, соответствующем топологической образующей $1 \in \hat{\mathbf{Z}}$.

Проверим, что выполнены требуемые свойства. Достаточно разобрать по отдельности случаи неразветвленного и вполне разветвленного расширения. В первом - модуль коэффицентов один и тот же, а ограничение происходит на подгруппу индекса n с топологической образующей F^n, откуда следует, что значение инварианта умножается на n. Во втором - группа Галуа одна и та же, а мультипликативная группа одного максимального неразветвленного расширения вкладывается в мультипликативную группу другого так, что нормирование умножается на n - индекс ветвления, равный степени расширения, откуда и вытекает второе равенство. Из него следует первое ввиду Леммы 3.1.

4. Фундаментальные классы и изоморфизм взаимности

Напомним ситуацию для случая произвольной формации классов. Группа $H^2(\hat{H})$, являясь объединением своих подгрупп $H^2(H/H_1)$, вложенных в нее отображением инфляции, гомоморфизмом inv_H вкладывается в $\mathbf{Q}/\mathbf{Z}$. При этом, образ $H^2(H/H_1)$ есть единственная циклическая подгруппа порядка $|H/H_1|$, порожденная элементом $1/|H/H_1|$. Назовем фундаментальным классом $u_{H/H_1} = inv_H^{-1}(1/|H/H_1|) \in H^2(H/H_1)$.

Как связаны фундаментальные классы для разных расширений? Пусть $E \subset F \subset H$ - подгруппы G из нашего семейства. Из определения ясно, что если E и F нормальны в H, то

$$inf(u_{H/F}) = |F/E| u_{H/E}.$$

Из второй части аксиомы II и сюръективности Res следует, что

$$Res(u_{H/E}) = u_{F/E}.$$

Здесь E нормальна в H. В тех же предположениях

$$Cores(u_{F/E}) = |H/F| u_{H/E}.$$

Соотношение для Res вместе с определением формации классов позволяет применить теорему Тейта:

Пусть $F \subset H$ - нормальна, тогда для любого $i \in \mathbf{Z}$ $\cup$-произведение на $u_{H/F}$ задает изоморфизм групп когомологий Тейта

$$\theta_i(H/F) : \hat{H}^i(H/F, \mathbf{Z}) \to \hat{H}^{i+2}(H/F) = \hat{H}^{i+2}(H/F, A^F).$$

Из того, что $Res(a \cup b) = Res(a) \cup Res(b)$ следует, что Res коммутирует с θ, а из $Cores(Res(a) \cup b) = a \cup Cores(b)$ - аналогичное утверждение для $Cores$.

Наиболее важным из этих изоморфизмов, несомненно, является θ_{-2}, отождествляющий $(H/F)^{ab}$ с $A^H/N_{H/F}A^F$. Обратный к нему $a \in A^H \mapsto (a, H/F) \in (H/F)^{ab}$ называется отображением взаимности. Как его вычислить?

Предложение 4.1 $\langle \chi, (a, H/F) \rangle = inv_H(\overline{a} \cup \delta\chi)$, где $\chi \in Hom(H/F, \mathbf{Q}/\mathbf{Z})$ - характер группы H/F, δ - дифференциал в последовательности $0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0$, а $\overline{a}$ - образ a в $\hat{H}^0(H/F, A^F)$.

Доказательство. По определению

$$\overline{a} \cup \delta\chi = u_{H/F} \cup ((a, H/F) \cup \delta\chi) = u_{H/F} \cup \delta((a, H/F) \cup \chi).$$

Утверждается, что $\cup$-произведение $x \cup \chi$, где $x \in \hat{H}^{-2}(H/F, \mathbf{Z}) = (H/F)^{ab}$ совпадает со значением χ на x. Окончание доказательства по модулю этого утверждения очевидно. ($\hat{H}^{-1}(H/F, \mathbf{Q}/\mathbf{Z})$ есть ядро применения "оператора нормы" - умножения на $|H/F|$, на этом ядре δ действует как умножение на $|H/F|$. Это следует из определения соответствующих групп когомологий Тейта и из конструкции бесконечной в обе стороны длинной точной последовательности когомологий Тейта. Применение инварианта устраняет этот появившийся множитель.)

Замечание 4.2 Пусть фундаментальный класс $u_{H/F}$ представляется 2-коциклом $u : H/F \times H/F \to A^F$. Тогда для $s \in H/F$

$$\theta(s) = \sum_{t \in H/F} u(t, s).$$

В случае локальной теории полей классов символ $(a, H/F)$ будем обозначать $(a, K/k)$, где K (соотв. k) - поле инвариантов подгруппы H (соотв. F). Он называется символом норменного вычета - по простой причине, т.к. равен 1 тогда и только тогда когда a есть норма из K в k.

Предложение 4.3 Если K/k неразветвлено, то $(a, K/k) = F^{v(a)}$.

Доказательство. По предложению 4.1 для любого характера χ имеем $\chi((a, K/k)) = inv_k(a \cup \delta\chi)$. Затем воспользоваться явной конструкцией локального инварианта.

Следствие 4.4 Для абелева расширения отображение взаимности переводит подгруппу единиц в группу инерции.

5. Обзор арифметики глобальных полей

(Касселс-Фрелих, гл.2, Ленг "Алгебраические числа", гл.6, Вейль "Основы теории чисел", гл.4)

Пусть $k/\mathbf{Q}$ - числовое поле с кольцом целых O_k. На нем можно рассмотреть множество классов эквивалентности нормирований M_k (аксиомы нормирования: k^* переходит в $\mathbf{R}_+$, мультипликативность, неравенство треугольника; нормирования эквивалентны, если они задают одну и ту же топологию). Элементы M_k называются точками поля k ("places").

Нормирования можно ограничивать на $\mathbf{Q}$. Легко доказать (теорема Островского), что $M_{\mathbf{Q}}$ состоит из p-адических нормирований

$$| x |_p = p^{-val_p(x)}$$

и вещественного нормирования - обычного абсолютного значения.

Нормирование $v \in M_k$ определяет пополнение k по этому нормированию, обозначаемое k_v. Если K/k -конечное расширение, и $u_1, \ldots, u_s$ - нормирования поля K, продолжающие нормирование v поля k, то

$$K \otimes_k k_v = \oplus_{i=1,\ldots,s} K_{u_i}.$$

(Отсюда, в частности, следует, что норма элемента из K есть произведение локальных норм.) При этом единственное нормирование v поля k_v, продолженное на векторное пространство $K \otimes_k k_v$ и ограниченное на K_{u_i}, есть единственное нормирование на K_{u_i}. Это можно применить к расширению $k/\mathbf{Q}$. Пусть

$$||x||_v = | \; Norm_{k_v/\mathbf{Q}_w}(x) \; |_w,$$

$$| \; x \; |_v = (||x||_v)^{1/n_v},$$

где $n_v = [k_v : \mathbf{Q}_w]$ называется локальной степенью. Вторая из этих формул вычисляет v как единственное продолжение нормирования w на k_v. Сравнивая нормы, получаем:

$$|Norm_{k/\mathbf{Q}}(x)|_w = \prod_{v|w} ||x||_v.$$

Точки k, расположенные над p-адическим нормированием $\mathbf{Q}$, задаются дискретным нормированием, связанным с простым идеалом кольца целых O_k, делящим p. Они являются неархимедовыми (удовлетворяют ультраметрическому неравенству). Для таких v обозначим $O_v \subset k_v$ - кольцо целых (целое замыкание $\mathbf{Z}_p$ в k_v); оно компактно (например, потому, что является проконечной группой по сложению). Эквивалентным образом, $O_v = \{x \in k_v, | \; x \; |_v \leq 1\}$. Такие точки называются конечными, они образуют подмножество $M_{k,f} \subset M_k$.

Если v - архимедово, то k_v есть $\mathbf{R}$ или $\mathbf{C}$, и нормирование $| \; x \; |_v$ индуцируется соответствующей вещественной или комплексной нормой. Эти точки называются бесконечными, имеем $M_k = M_{k,\infty} \cup M_{k,f}$.

5.1 *Формула произведения.* Если $a \in k^*$, то

$$\prod_{v \in M_k} ||x||_v = 1,$$

причем лишь конечное число сомножителей отлично от 1. (Взятием нормы сводится к $\mathbf{Q}$, где это очевидно.)

5.2 *Теорема о слабой аппроксимации.* (Обобщение китайской теоремы об остатках) Пусть S - конечное множество точек. Тогда диагональное вложение $k \to \prod_{v \in S} k_v$ имеет всюду плотный образ. (Это практически равносильно тому, что соответствующие нормирования неэквивалентны, Касселс-Фрелих, гл.2, 6.1.)

Адели. Пусть S - конечное множество точек, содержащее все архимедовы. Определим кольцо S-аделей

$$\mathbf{A}_{k,S} = \prod_{v \in S} k_v \prod_{v \notin S} O_v,$$

с покомпонентными операциями сложения и умножения и с топологией прямого произведения. Кольцо аделей $\mathbf{A}_k$ определяется как объединение всех подмножеств $\mathbf{A}_{k,S} \subset \prod_{v \in M_k} k_v$, с топологией, в которой все $\mathbf{A}_{k,S}$ открыты.

Предложение 5.3. Поле k диагонально вкладывается в $\mathbf{A}_k$, образ этого вложения (главные адели) дискретен в $\mathbf{A}_k$, а факторпространство компактно.

Доказательство. Дискретность следует из формулы произведения: если все $||x||_v \leq 1$, а для некоторых v здесь имеется строгое неравенство, то произведение не может быть равно 1, т.е. $x = 0$ - изолированная точка. Для доказательства компактности факторгруппы заметим, что $\mathbf{A}_k = k + \mathbf{A}_{k,M_\infty}$

(следует из китайской теоремы об остатках), и $O_k = k \cap \mathbf{A}_{k,M_\infty}$ (коэффициенты характеристического многочлена - рациональные числа, лежащие во всех $\mathbf{Z}_p$, следовательно они целые). Поэтому фактор-группа $\mathbf{A}_k/k$ есть $\prod_{v \in M_{k,f}} O_v \times (\prod_{u \in M_\infty} k_u)/O_k$. Группа O_k вкладывается в

$$k \otimes_{\mathbf{Q}} \mathbf{R} = \prod_{u \in M_\infty} k_u \simeq \mathbf{R}^{[k:\mathbf{Q}]}$$

как полномерная решетка (k там плотно, а O_k порождает k над $\mathbf{Q}$). Отсюда, и из компактности O_v, следует наше утверждение.

Следствие. Фундаментальную область можно выбрать в виде произведения $W = \prod_{v \in M_{k,f}} O_v \times W_\infty$, где $W_\infty \subset \prod_{u \in M_{k,\infty}} k_u$.

Мера Хаара на аделях. На каждой аддитивной группе k_v есть инвариантная мера: можно, например, взять в архимедовом случае обычную меру Лебега, а в неархимедовом - инвариантную меру μ_v, такую, что $\mu_v(O_v) = 1$. Если определить измеримые множества как произведения измеримых подмножеств в k_v, причем для почти всех v берется O_v, то адельная мера μ задается как произведение локальных мер. Отметим, что при умножении на адель $\{x_v\}$ мера μ умножается на $\prod_{v \in M_k} ||x_v||_v$ (действительно, действие эндоморфизма на конечномерном векторном пространстве умножает меру на абсолютное значение его нормы). Тем самым, действие k сохраняет μ.

5.4. *Теорема о сильной аппроксимации.* Если в определении аделей взять все нормирования кроме одного, то k будет всюду плотно в таком кольце.

Будем называть "ящиком" подмножество в пространстве аделей, задаваемое условиями

$$||x_v||_v \leq ||a_v||_v,$$

для некоторого аделя $\{a_v\}$. Сначала докажем следующее утверждение:

"Лемма Минковского". Пусть $\mu(W)$ - мера фундаментальной области действия k на $\mathbf{A}_k$. Тогда в ящике меры больше $2^n\mu(W)$ есть ненулевой главный адель.

Доказательство. Мера ящика, полученного из нашего ящика умножением на $1/2$ в архимедовых компонентах, будет больше $\mu(W)$, значит в нем найдутся две различные точки, отличающиеся на главный адель. Этот адель лежит уже в нашем ящике.

Доказательство теоремы 5.4. Если заданы все ребра ящика кроме одного, то это последнее ребро можно задать столь большим, что мера полученного ящика будет сколь угодно велика. Пусть фундаментальная область W выбрана как в следствии из предложения 5.3. Пусть v_0 - "недостающее" нормирование, а S - нормирования, в которых мы собираемся аппроксимировать. По лемме Минковского существует ненулевой главный адель λ, очень близкий к 0 в S, и целый вне S и v_0. Область λW - также фундаментальная. Пусть $x_v \in k_v, v \in S$ - числа, которые мы хотим приблизить, тогда адель с такими компонентами в точках S и равный 0 вне S представляется в виде $x + y$, где $x \in \lambda W$, $y \in k$. Из нашего выбора λ и W следует, что $y \in O_v$ при $v \notin S, v \neq v_0$, а также то, что $y - x_v$ сколь угодно близко к 0 в $k_v, v \in S$.

Идели. (Этот термин придумал Шевалле как сокращение словосочетания "идеальный элемент".) Их можно определить как и адели, с заменой k_v на k_v^*, и O_v на группу единиц U_v; обозначение: J_k. Заметим, что хотя как множество J_k естественно вложено в $\mathbf{A}_k$, идельная топология не индуцируется адельной! Если идель x близок к 1 в идельной топологии, то адель $x-1$ близок к 0 в адельной топологии, поэтому из 5.3 вытекает, что k^* дискретно в J_k. Такие идели называются главными, группа $C_k = J_k/k^*$ называется группой классов иделей. Если $x = \{x_v\} \in J_k$, тогда пусть

$$||x|| = \prod_{v \in M_k} ||x_v||_v$$

- гомоморфизм (называемый содержанием) на мультипликативную группу вещественных положительных чисел, и пусть J_k^1 - его ядро. По формуле произведения $k^* \subset J_k^1$.

Предложение 5.5 J_k^1/k^* компактно.

Доказательство состоит из нескольких этапов.

(а) J_k^1 - замкнута в $\mathbf{A}_k$.

Доказательство. Надо для $\{x_v\} \in \mathbf{A}_k \setminus J_k^1$ построить окрестность, непересекающуюся с J_k^1. Если $||\{x_v\}|| < 1$, то надо просто слегка пошевелить в нормированиях, значения которых не равны 1, и взять U_v в остальных. Если содержание больше 1, то пусть S содержит все точки такие, что $||x_v||_v \neq 1$, и все точки над простыми числами $p < 2||\{x_v\}||$. Пусть ϵ столь мало, что из системы неравенств $||y_v - x_v||_v < \epsilon, v \in S$ следует $1 < \prod_{v\in S} ||y_v||_v < 2||\{x_v\}||$. Тогда, добавляя к этой системе неравенства $||y_v|| \leq 1, v \notin S$, получим требуемую окрестность. Действительно, либо для всех $v \notin S$ имеем $||y_v||_v = 1$ и тогда $||\{y_v\}|| > 1$, либо для некоторого $v \notin S$ имеем $||y_v|| = p^a < 1$, где p делит v, и значит, $p^a < 1/2||\{x_v\}||$, откуда $||\{y_v\}|| < 1$.

(б) На J_k^1 идельная и адельная топологии совпадают.

Доказательство. В одну сторону это ясно - открытое множество в идельной топологии открыто и в адельной. В другую: Пусть $\{x_v\} \in J_k^1$, S содержит все архимедовы нормирования и нормирования, в которых $||x_v||_v \neq 1$. Система неравенств

$$||\xi_v - x_v||_v < \epsilon_v, v \in S,$$

$$||\xi_v||_v \leq 1, v \notin S,$$

настолько узких, что из них следует $||\{\xi_v\}|| < 2$, ограниченная на J_k^1, равносильна замене на равенства во второй строчке, т.к. если хотя бы в одном месте неравенство строгое, то содержание уменьшится сразу как минимум в $p > 2$ раз - противоречие.)

(в) Предъявим компакт $K \subset \mathbf{A}_k$, такой что $K \cap J_k^1 \to J_k^1/k^*$ - эпиморфно, тогда J_k^1/k^* компактно как непрерывный образ компакта. Пусть K - ящик меры больше $2^n\mu(W)$. Пусть $\{x_v\} \in J_k^1$, тогда эпиморфность следует из леммы Минковского, примененной к ящику, получаемому из K умножением на идель $\{x_v^{-1}\}$.

Группа классов идеалов. Сопоставление иделю $\{x_v\}$ дробного идеала $\prod_{v\in M_{k,f}} \mathcal{P}_v^{val_v(x_v)}$, где $\mathcal{P}_v$ - идеал нормирования v, задает непрерывный гомоморфизм из J_k на группу идеалов k, наделенную дискретной топологией. Обозначим ее I_k. Группа классов идеалов есть факторгруппа I_k по главным идеалам.

Следствие 5.6 Группа классов идеалов конечна.

Доказательство. Гомоморфизм $J_k^1 \to I_k$ сюръективен. Переходя к факторам, заключаем, что группа классов идеалов конечна, т.к. дискретна, и, в то же время, непрерывный образ компакта, т.е. компакт.

Число элементов этой группы обозначается $h = h_k$ и называется числом классов поля k.

Определение. Пусть S - конечное множество точек, содержащее все архимедовы. S-единицами поля k называются элементы $k^* \cap J_{k,S}$ (где $J_{k,S} = \prod_{v\notin S} U_v \times \prod_{v\in S} k_v^*$). Если $S = M_{k,\infty}$, то $k_S = O_k^*$.

5.7. *Теорема Дирихле о единицах.* Пусть n - число элементов в S. Тогда k_S изоморфно произведению (циклической) группы единиц поля k и $\mathbf{Z}^{n-1}$.

Лемма. x - корень из 1 в k тогда и только тогда, когда $|x|_v = 1$ для всех нормирований v поля k. (Пересечение компактной подгруппы с дискретной - конечно.)

Рассмотрим гомоморфизм $J_{k,S} \to \mathbf{R}^n$, переводящий идель $\{x_v\}$ в $\{log(||x_v||_v)\}, v \in S$. Он непрерывен и имеет группу единиц в качестве ядра. По формуле произведения образы иделей из $J_{k,S} \cap J_k^1$ имеют нулевую сумму координат. При этом, образ k_S - дискретен (пересечение любого "ящика" с образом группы S-единиц конечно, т.к. его прообраз в группе иделей компактен и пересекается с дискретной подгруппой k^* по конечному множеству). Образ $J_{k,S}$ есть прямая сумма $\mathbf{Z}$ для неархимедовых v, и $\mathbf{R}$ -

для архимедовых, а образ $J_{k,S} \cap J_k^1$ изоморфен $\mathbf{Z}^a \times \mathbf{R}^{n-a-1}$. Далее, фактор образа $J_{k,S} \cap J_k^1$ по образу k_S компактен как непрерывный образ $(J_{k,S} \cap J_k^1)/k_S$ - открытой подгруппы в J_k^1/k^* (открытой, следовательно, замкнутой, следовательно, компактной). Отсюда следует, что образ S-единиц - полномерная решетка в $\mathbf{Z}^a \times \mathbf{R}^{n-a-1}$, что и требовалось.

6. Первое неравенство

6.1. Характеры Дирихле

Пусть $Hom(C_k, S^1)$ - группа непрерывных характеров группы классов иделей со значениями в $S^1 = \{z \in \mathbf{C}^*, ||z|| = 1\}$. Мы будем рассматривать их как характеры J_k, тривиальные на k^*. Топологическая группа J_k имеет систему окрестностей единицы, состоящую из открытых подгрупп (т.е. вполне несвязна). Следовательно, по непрерывности, каждый характер ψ тривиален на некоторой открытой подгруппе (содержащейся в прообразе малой окрестности 1). Пусть S - наименьшее множество нормирований, такое, что ψ тривиален на $\prod_{v \notin S} O_v$, вложенной в J_k так, что на местах $v \in S$ стоят 1. Это S назовем исключительным множеством для ψ. Ограничение ψ на v-ую компоненту дает непрерывный характер ψ_v группы k_v^*. Эта группа также вполне несвязна, и ψ_v тривиален на подгруппе $U_v^i = 1 + \mathcal{P}_v^i = 1 + \pi_v^i O_v$ для некоторого i (здесь $\mathcal{P}_v$ - идеал нормирования v, а π_v - униформизующая). Пусть m_v - минимальное такое i. Понятно, что $m_v = 0$ для $v \notin S$. Идеал $f_\psi = \prod_{v \in S} \mathcal{P}_v^{m_v}$ называется кондуктором характера ψ (“Führer”).

До изобретения иделей использовался язык характеров группы идеалов. При этом приходится фиксировать некоторый идеал (“модуль”) M, такой, что кондуктор f_ψ делит M. Пусть I^S - группа дробных идеалов k, взаимно простых с идеалами из S; она свободно порождена неархимедовыми нормированиями, не лежащими в S. Имеется сюръективный гомоморфизм $J_k \to I^S$, переводящий $x = \{x_v\}$ в $(x)^S := \prod_{v \notin S} \mathcal{P}_v^{val_v(x_v)}$. Ограничение ψ на идели с локальными компонентами 1 в точках S факторизуется через гомоморфизм $x \mapsto (x)^S$, $\psi(x) = \chi((x)^S)$. Такие характеры χ группы I^S называются *характерами Гекке.*

Характером Дирихле называется характер Гекке, происходящий из ψ, тривиального на связной компоненте 1 в группе иделей, т.е. такого, что для архимедовых v характер ψ_v имеет дискретный образ (попросту говоря, ψ_v тривиален для комплексных нормирований, а для вещественных - тривиален либо равен знаку соответствующего вещественного вложения). Пусть M - целый идеал k, делящийся лишь на простые идеалы из S, и пусть $a \in k$ сравнимо с 1 по модулю M. Тогда главный идеал $(a) \in I^S$. Легко видеть, что в этом случае

$$\chi((a)) = \prod_{v \in M_{k,\infty}} \psi_v(a^{-1}).$$

Таким образом, χ тривиален на подгруппе H^M, состоящей из главных идеалов (a), таких, что $a \cong 1 mod M$ и $a > 0$ при всех вещественных вложениях k.

Предложение 6.1. Пусть S - конечное множество точек поля k, $M_{k,\infty} \subset S$. Построенное соответствие есть биекция между

(i) характерами $\psi \in Hom(C_k, S^1)$ с исключительным множеством S, тривиальными на связной компоненте 1;

(ii) характерами Дирихле, т.е. характерами I^S, поднятыми с факторгруппы I^S/H^M для некоторого целого идеала M, делящегося лишь на простые идеалы из S, причем H^M состоит из главных идеалов (a), таких, что

а) $a \cong 1 mod M$,

б) $i(a) > 0$ для всех вложений $i : k \hookrightarrow \mathbf{R}$.

Доказательство. Построим k^*-инвариантный характер ψ группы J_k по χ. Пусть $\{x_v\}$ - идель. По теореме о слабой аппроксимации можно найти $y(x) \in k$ сколь угодно близкое к x_v для всех $v \in S$. Если $y(x)$ и $y'(x)$ - два такие числа, то $y(x)/y'(x)$ удовлетворяет (а) и (б), т.е. $\chi(y(x)) = \chi(y'(x))$. Поэтому имеет смысл определение $\psi(x) = \chi((y(x)^{-1}x)^S)$. Легко проверяется, что все свойства выполнены.

6.2. Вывод первого неравенства из свойств L-функций

Пусть s - комплексная переменная. Абсолютная норма $N(A)$ идеала A - это его норма в $\mathbf{Q}$, для целого идеала A имеем $N(A) = |O_k/A|$.

Определение. ζ-функция Дедекинда числового поля k определяется так:

$$\zeta_k(s) = \sum N(A)^{-s} = \prod (1 - N(P)^{-s})^{-1},$$

где сумма берется по всем ненулевым целым идеалам, а произведение - по простым.

Определение. L-функция, отвечающая характеру Дирихле χ, определяется так:

$$L(s,\chi) = \sum \chi(A) N(A)^{-s} = \prod (1 - \chi(P) N(P)^{-s})^{-1},$$

где χ продолжается нулем вне I^S.

Эти суммы и произведения абсолютно сходятся в полуплоскости $Re(s) > 1$, причем $\zeta_k(s)$ имеет в 1 простой полюс, а $L(s,\chi)$ для $\chi \neq 1$ имеет в 1 конечный предел, отличный от 0 (теорема Дирихле).

Пусть K/k - конечное расширение Галуа степени n. Пусть $H(K,M) \subset I^S$ - подгруппа, порожденная H^M и идеалами в I^S, являющимися нормами идеалов K.

Предложение 6.2.1. (*"Первое неравенство".)* $|I^S/H(K,M)| \leq n$.

Доказательство. Вычислим главный член разложения ряда в 1

$$\sum_{P \in H(K,M)} N(P)^{-s}.$$

Имеем

$$ln\ L(s,\chi) = \sum_P \chi(P) N(P)^{-s} + O(1).$$

Суммируя главные части по характерам, тривиальным на $H(K,M)$, получим

$$\sum_{P \in H(K,M)} N(P)^{-s} = |I^S/H|^{-1} ln((s-1)^{-1}) + O(1).$$

При этом используется ограниченность L-функции в окрестности 1 и ее необращение в ноль в 1, и то, что $ln\ \zeta_k(s) = ln((1-s)^{-1}) + O(1)$. С другой стороны,

$$\sum N(P)^{-s} = n^{-1} ln((s-1)^{-1}) + O(1),$$

где суммирование идет по простым идеалам в I^S, полностью распадающимся в K. (Только идеалы K, лежащие над ними, вносят вклад в основной член разложения в единице ζ-функции Дедекинда поля K.) Такие идеалы являются нормами из K, т.е. главный член последнего разложения не больше главного члена в предыдущей формуле, откуда и следует наше утверждение.

Смысл полученной оценки можно выразить в терминах иделей.

Предложение 6.2.2. Имеем $C_k/N_{K/k}(C_K) = I^S/H(K,M)$ для некоторого достаточно большого M, делящегося на $D_{K/k}$ - дискриминант расширения K/k (идеал O_k), при этом S состоит из архимедовых точек и простых идеалов, делящих M.

Доказательство. Поскольку вне S ветвления нет, $H(K,M)$ порождена H^M и $\mathcal{P}_v^{f_v}$, $v \notin S$, где f_v - степень расширения поля вычетов. Это согласуется с тем, что если точка w поля K делит $v \notin S$, то $N_{K_w/k_v}(K_w^*) \subset k_v^*$ порождается O_v^* и $\pi_v^{f_v}$. Применяя теорему о слабой аппроксимации в k, можно считать, что локальные компоненты иделя в точках S столь близки к 1, что попадают в образ норменного отображения (открытую окрестность 1).

Следствие 6.2.3. Если K/k - конечное расширение Галуа степени n с группой G, то порядок $\hat{H}^0(G, C_K)$ не превосходит n.

Доказательство. По теореме Гильберта 90 имеем $H^1(G, K^*) = 0$, поэтому последовательность

$$0 \to H^0(G, K^*) \to H^0(G, J_K) \to H^0(G, C_K) \to 0$$

точна. Так как $K^G = k$, $(J_K)^G = J_k$, то $(C_K)^G = C_k$. Поэтому $C_k/N_{K/k}(C_K) = \hat{H}^0(G, C_K)$.

7. Второе неравенство. Локально-глобальный принцип

7.1. Второе неравенство

Теорема 7.1 Пусть K/k - циклическое расширение степени n, тогда индекс Эрбрана $h(G, C_K)$ равен n.

Доказательство. Пусть $S \subset M_k$ содержит $M_{k,\infty}$, нормирования, ветвящиеся в K/k, а также нормирования поля k, лежащие под конечным множеством простых идеалов K, которые порождают группу классов идеалов поля K. Пусть $T \subset M_K$ - все нормирования K, лежащие над S. Как обычно, обозначим $J_{K,T}$ открытую подгруппу в J_K вида

$$J_{K,T} = \prod_{v \in S} (\prod_{w|v} K_w^*) \times \prod_{v \notin S} (\prod_{w|v} O_w^*),$$

тогда $J_K = J_{K,T} K^*$ и $C_K = J_{K,T}/K_T$, где $K_T = J_{K,T} \cap K^*$ обозначает группу T-единиц поля K. По предложению 1.5.3, $h(G, C_K)$ можно вычислять как $h(G, J_{K,T})/h(G, K_T)$, конечно, при условии, что эти два числа определены. Обозначим через G_w группу разложения нормирования w, т.е. $\{x \in G | xw = w\}$, она естественно вкладывается в $Gal(K_w/k_v)$, и это вложение является изоморфизмом. Это легко следует из того, что степень расширения $n = |G|$ равна сумме локальных степеней $n_v = |Gal(K_w/k_v)|$, т.е. n_v, умноженному на число нормирований $w|v$. Кроме того, тот же аргумент показывает, что G транзитивно действует на множестве таких w. Когомологии коммутируют с прямым произведением, поэтому по лемме Шапиро

$$h(G, J_{K,T}) = \prod_{v \in S} h(G, \prod_{w|v} K_w^*) \times \prod_{v \notin S} h(G, \prod_{w|v} O_w^*)$$

$$= \prod_{v \in S} h(G_v, K_w^*)) \times \prod_{v \notin S} h(G_v, O_w^*),$$

причем в последней строчке берется одно какое-то $w|v$. В конце гл. 13 первой части было доказано, что если v неразветвлено в K/k, то для всех i

$$H^i(G_v, O_w^*) = 0.$$

Кроме того, $H^1(G_v, K_w^*) = 0$ по теореме Гильберта 90, а $H^2(G_v, K_w^*)$ изоморфно $\mathbf{Z}/n_v$ как часть $Br(k_v)$, состоящая из алгебр, убиваемых ограничением на K_w. Отсюда

$$h(G, J_{K,T}) = \prod_{v \in S} n_v.$$

Прежде, чем вычислять $h(G, K_T)$, докажем несколько вспомогательных лемм из теории когомологий Тейта циклических групп.

Лемма 7.2. Если A - конечный G-модуль, то $h(A) = 1$. Доказательство. $|A_G| = |A^G|$ как коядро и ядро умножения на $g - 1$, где $G = \langle g \rangle$. Далее, $\hat{H}^{-1}(G, A) = Ker(N_*)$, $\hat{H}^0(G, A) = Coker(N_*)$, где N_* - умножение на "норму" $A_G \to A^G$. Остается еще раз применить тот же аргумент.

Следствие 7.3. Индекс Эрбрана не меняется при переходе к фактормодулю (соотв. подмодулю) с конечным ядром (соотв. факторомодулем).

Лемма 7.4. Два конечномерных $\mathbf{Q}$-представления конечной группы, изоморфные над $\mathbf{R}$, изоморфны уже над $\mathbf{Q}$.

Доказательство. Ясно, что

$$Hom_G(A_1, A_2) \otimes \mathbf{R} = Hom_G(A_1 \otimes \mathbf{R}, A_2 \otimes \mathbf{R}).$$

Если здесь существует невырожденный оператор с вещественными коэффициентами, то малым шевелением эти коэффициенты можно сделать рациональными, так, чтобы оператор остался невырожденным.

Следствие 7.5. Пусть есть два целочисленных представления циклической группы, порождающих одно и то же конечномерное вещественное пространство. Тогда индексы Эрбрана равны.

Доказательство следует из 7.3 и 7.4.

Вернемся к вычислению $h(G, K_T)$. На пространстве $\mathbf{R}^T$ есть два естественных действия G: одно - перестановками точек T, оно сохраняет очевидную целочисленную решетку. Легко подсчитать, что соответствующий индекс Эрбрана равен $\prod_{v \in S} n_v$. Другая решетка - логарифмическая решетка единиц, порождающая подпространство с нулевой суммой координат. Так как ядро отображения $\{log||x||_w\}_{w \in T} : K_T \to \mathbf{R}^T$ состоит из корней из 1 в K, оно конечно и не меняет индекса Эрбрана по 7.3. Добавим $\mathbf{Z}$, порожденную вектором из одних единиц, к этой решетке, тогда получится полномерная решетка с индексом Эрбрана

$$h(\mathbf{Z})h(K_T) = nh(K_T).$$

Теперь теорема 7.1 следует из 7.5.

Следствие 7.6. Для циклического расширения имеем

$$|\hat{H}^0(G, C_K)| = |H^2(G, C_K)| = n, H^1(G, C_K) = 0.$$

Следствие 7.7. Для произвольного конечного расширения Галуа K/k имеем $H^1(G, C_K) = 0$.

Доказательство. Ядро гомоморфизма ограничения на силовскую p-подгруппу Res_{G/G_p} аннулируется умножением на индекс этой подгруппы, т.е. на число, взаимно простое с p, т.е. Res_{G/G_p} вкладывает p-компоненту конечной абелевой группы $H^1(G, C_K)$ в $H^1(G_p, C_K)$. Докажем, что $H^1(G_p, C_K) = 0$. Любая конечная p-группа имеет нетривиальный центр (группа действует на себе сопряжением; мощности орбит, не сводящихся к одному элементу, делятся на p; значит, число неподвижных элементов тоже делится на $p > 1$, т.е. имеется неподвижный элемент, отличный от 1). Переходя к факторгруппе и повторяя то же самое, построим нормальный ряд с абелевыми факторами (хорошо известный факт - все p-группы разрешимы, Ван дер Варден, гл.7), который можно уплотнить так, чтобы все факторы были изоморфны $\mathbf{Z}/p$. Следовательно, G_p, как и любая p-группа, имеет нормальную подгруппу H индекса p. Пусть наше утверждение доказано для всех p-групп меньшего порядка. Тогда требуемое вытекает из последовательности "ограничение-инфляция" для G_p и H и последнего утверждения следствия 7.6.

7.2. Локально-глобальный принцип

Ввиду следствия 7.7 длинная точная последовательность когомологий, связанная с точной последовательностью

$$1 \to K^* \to J_K \to C_K \to 1,$$

дает вложение

$$H^2(G, K^*) \hookrightarrow \oplus_{v \in M_k} H^2(G_v, K_w^*).$$

(Отождествление $H^2(G, J_K) = \oplus_{v\in S} H^2(G_v, K_w^*)$ было проведено в ходе доказательства теоремы 7.1. Переходя к индуктивному пределу - беря объединение - по возрастающей последовательности конечных подмножеств $S \subset M_k$, получаем $H^2(G, J_K) = \oplus_{v\in M_k} H^2(G_v, K_w^*)$.) Индуктивный предел по возрастающей системе конечных групп G дает вложение

$$Br(K) \hookrightarrow \oplus_{v\in M_k} Br(k_v).$$

Оно традиционно формулируется как

Теорема Брауэра-Хассе-Нетер. Центральная простая алгебра над числовым полем тривиальна тогда и только тогда, когда она тривиальна над всеми его пополнениями.

Теорема Хассе о нормах. Пусть K/k - циклическое расширение. Элемент $a \in k$ является нормой некоторого элемента из K тогда и только тогда, когда для каждого $v \in M_k$ существует $b_v \in K_w$ (для некоторого $w|v$) такой, что $a = N_{K_w/k_v}(b_v)$.

Доказательство. Воспользовавшись периодичностью когомологий Тейта циклической группы, мы получаем вложение

$$\hat{H}^0(G, K^*) \hookrightarrow \oplus_{v\in M_k} \hat{H}^0(G_v, K_w^*),$$

что и дает требуемое.

Задача. Эта теорема не переносится на случай произвольных расширений Галуа. Доказать, что расширение $\mathbf{Q}(\sqrt{13}, \sqrt{17})/\mathbf{Q}$ дает контрпример.

Следующий результат может быть сформулирован как то, что "принцип Хассе выполнен для плоских коник".

Теорема Минковского-Хассе о квадратичных формах от 3 переменных. Квадратичная форма от 3 переменных представляет 0 в числовом поле тогда и только тогда, когда она представляет 0 во всех его пополнениях.

Доказательство. Диагонализуя ($char(k) \neq 2$) и домножая на постоянный множитель, можно считать форму равной $x^2 - ay^2 - bz^2$. Если показать, что b является локальной нормой для всех пополнений k относительно расширения $k(\sqrt{a})$, то все будет следовать из теоремы Хассе о нормах. Если a - квадрат в k_v, то проверять нечего, а если нет, то в представлении 0

$$x^2 - ay^2 - bz^2 = 0$$

z не может быть нулем, следовательно, b - локальная норма в v.

Отсюда чисто алгебраически можно вывести аналогичный результат для форм от 4 переменных, и, с использованием теоремы о слабой аппроксимации, для форм от 5 и более переменных (см. упражнение 4 в Касселс-Фрелих).

8. Лемма Ван дер Вардена

Запись $a||b$ означает, что a делит b, и b/a не делится на a. Если ζ - корень из 1, то будем обозначать через $ord(\zeta)$ порядок ζ, т.е. наименьшее n, такое, что $\zeta^n = 1$. Аналогичное обозначение будем применять и к характеру со значением в корнях из 1. Мы будем рассматривать "мультипликативные характеры" $\mathbf{Z}$ по модулю m, т.е. функции $\mathbf{Z} \to S^1 \subset \mathbf{C}$, поднятые с некоторого характера $(\mathbf{Z}/m)^*$, и продолженные нулем на числа, которые не взаимно просты с m. Характер ψ будем называть четным, если $\psi(-1) = 1$, и нечетным, если $\psi(-1) = -1$. Сразу отметим, что характер нечетного порядка обязательно четен.

Лемма. Пусть $a_1, \ldots, a_r$ и N - целые числа ≥ 2. Тогда существует такой нечетный мультипликативный характер ψ, что $N|ord(\psi(a_i))$ для всех $i = 1, \ldots, r$.

Доказательство состоит из ряда этапов.

а) Достаточно для каждого простого делителя $l|N$, $l^{\alpha_l}||N$, построить характер ψ_l, такой, что $ord(\psi_l)$ - степень l, $l^{\alpha_l}|ord(\psi_l(a_i))$, и ψ_2 - нечетен, тогда можно взять $\psi = \prod_{l|n} \psi_l$. Таким образом, все сводится к случаю когда $N = l^n$ - степень простого числа.

При разборе случая $l = 2$ будет удобно считать, что $a_i \cong 0$ или $1 mod 4$. Это достигается переходом к a_i^2.

б) Утверждается, что для каждого целого числа $a \geq 2$, $a_i \cong 0$ или $1 mod 4$, и любого простого l существует бесконечная последовательность простых чисел $\{p_\nu\}$, таких, что образ a в $(\mathbf{Z}/p_\nu)^*$ имеет порядок l^ν.

Идея решения: понятно, что p_ν надо искать среди простых делителей $a^{l^\nu} - 1$, которые не делят $a^{l^{\nu-1}} - 1$. На самом деле можно взять в качестве p_ν любой отличный от l делитель числа

$$(a^{l^\nu} - 1)/(a^{l^{\nu-1}} - 1)$$

(проверяется, что их множество непусто, и что такое простое не делит $a^{l^{\nu-1}} - 1$).

в) Пусть $\rho \in \mathbf{Z}$ достаточно велико, как и $\nu_i \geq n + \rho - 1$ для каждого a_i, тогда обозначим $p_i := p_{\nu_i}$ соответствующее простое число для a_i. Попросим, чтобы все они были различны и взаимно просты с $a_1, \ldots, a_r$. Тогда некоторая степень образующей группы $Hom((\mathbf{Z}/p_i)^*, \mathbf{C}^*)$ даст мультипликативный характер ψ_i по модулю p_i, такой, что $ord(\psi_i)$ есть степень l, и $ord(\psi_i(a_i)) = l^{n+\rho-1}$. Обозначим через A подгруппу $(\mathbf{Z}/\prod p_i)^* = \prod(\mathbf{Z}/p_i)^*$, порожденную образами $a_1, \ldots, a_r$; и пусть $A^* = Hom(A, \mathbf{C}^*)$ - ее группа характеров. Пусть m - целое число, столь большое, что $ord(\psi_i)|l^m$ для всех i. Построим гомоморфизм $(\mathbf{Z}/l^m)^r$ на подгруппу $\Psi \subset A^*$, порожденную $\psi_1, \ldots, \psi_r$:

$$x = (x_1, \ldots, x_r) \mapsto \psi^x := \prod_{i=1}^{r} \psi_i^{x_i}.$$

Для фиксированного j оценим число $x \in (\mathbf{Z}/l^m)^r$, таких, что $ord(\psi^x(a_j)) \leq l^{n-1}$. Пусть x_i для $i \neq j$ чему-то равны. Тогда это неравенство есть условие на x_j, которое означает принадлежность x_j смежному классу по подгруппе $l^\rho \mathbf{Z}/l^m$, т.е. число решений этого неравенства равно $l^{rm-\rho}$ или нулю. Когда j пробегает числа от 1 до r, число "плохих" ψ^x не превосходит $rl^{rm-\rho} < l^{rm}$ при условии, что $l^\rho > r$, что можно обеспечить выбором ρ. Мы доказали существование требуемого характера, за исключением условия нечетности для $l = 2$.

г) Покажем, как "подправить" ψ^x в этом случае, если этот характер оказался четен. Пусть p_0 - простое число, сравнимое с -1 по модулю 4, и взаимно простое со всеми a_i. Единственный характер второго порядка по модулю p_0 нечетен. Надо домножить ψ^x на этот характер, а поскольку порядки $\psi^x(a_i)$ делятся на 2^n, то при $n > 2$ (чего всегда можно добиться) они делятся на 4 и не изменятся при умножении на -1. Доказательство закончено.

Напомним, что чисто мнимым (соотв. вполне вещественным) называется числовое поле, не имеющее вещественных (соотв. комплексных) пополнений.

Следствие. Для любого конечного множества простых чисел существует чисто мнимое циклическое расширение $\mathbf{Q}$, локальные степени которого в этих простых делятся на сколь угодно большое число. Это расширение можно выбрать лежащим в круговом поле $\mathbf{Q}(\zeta)$, где ζ - примитивный корень из 1 степени m, не делящейся на наши простые числа.

Доказательство. В предыдущей лемме возьмем в качестве $a_1, \ldots, a_r$ упомянутые простые числа. Характер ψ имеет некоторый модуль m, взаимно простой с $a_1, \ldots, a_r$. Хорошо известно, что круговое поле $\mathbf{Q}(\zeta)$, где ζ - примитивный корень степени m из 1, имеет группу Галуа

$$Gal(\mathbf{Q}(\zeta)/\mathbf{Q}) = (\mathbf{Z}/m)^*$$

с действием на корнях из 1, задаваемым возведением в степень. Проинтерпретируем ψ как характер $Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$. Тогда поле инвариантов $Ker(\psi)$ есть циклическое круговое расширение $K/\mathbf{Q}$ с группой $Gal(K/\mathbf{Q}) = (\mathbf{Z}/m)^*/Ker(\psi)$. Фробениус в $p, (p, m) = 1$, для $\mathbf{Q}(\zeta)/\mathbf{Q}$ (такие p неразветвлены) есть

$p \in (\mathbf{Z}/m)^*$, а так как Фробениус в $p, (p,m) = 1$, для $K/\mathbf{Q}$ есть его образ при естественной сюръекции $Gal(\mathbf{Q}(\zeta)/\mathbf{Q}) \to Gal(K/\mathbf{Q})$, то он равен $\psi(p)$. Поскольку порядок Фробениуса равен локальной степени в p ($a_1, \ldots, a_r$ - неразветвлены, так как взаимно просты с m), то осталось только разобраться с архимедовыми нормированиями. Фробениус в бесконечности для $\mathbf{Q}(\zeta)/\mathbf{Q}$ равен -1 (он действует сопряжением на корнях из 1), и аналогичное рассуждение показывает, что Фробениус в бесконечности для $K/\mathbf{Q}$ равен $\psi(-1)$, т.е. локальная степень в бесконечности равна 2, и нечетный характер дает чисто мнимое циклическое расширение.

9. Законы взаимности Артина и Хассе

Пусть k - числовое поле.

Теорема 9.1. Любая ц.п.а. над k распадается над некоторым чисто мнимым циклическим расширением k, которое можно выбрать в виде композита k и чисто мнимого циклического подрасширения $k(\zeta)$, где ζ - примитивный корень из 1 степени m, и m взаимно просто со всеми нормированиями, в которых алгебра разветвлена (= имеет ненулевой локальный инвариант).

Доказательство. Определим $S \subset M_k$ как множество неархимедовых точек v таких, что $inv_v(A) \neq 0 \in \mathbf{Q}/\mathbf{Z}$. По теореме Брауэра-Хассе-Нетер нам нужно подобрать такое глобальное расширение L/k, что класс алгебры $A \otimes L_w$ в $Br(L_w)$ равен 0 для всех $w \in M_L$. Для этого достаточно, чтобы для $w|v \in S$ локальная степень $[L_w : k_v]$ делилась бы на знаменатель $inv_v(A)$ (при ограничении локальный инвариант умножается на степень расширения, см. гл. 3 второй части). Пусть $[k : \mathbf{Q}] = n$. По следствию из леммы Ван дер Вардена существует чисто мнимое циклическое круговое расширение $K/\mathbf{Q}$ с локальными степенями в точках $\mathbf{Q}$, лежащих под S, делящимися на $n.inv_v(A)$. Пусть $L = Kk$. Подсчитав локальную степень L над $\mathbf{Q}$ двумя способами, видим, что $[L_w : k_v]$ делится на $inv_v(A)$. Для архимедовых $w \in M_L$ имеем $A \otimes L_w = A \otimes \mathbf{C} = 0$, т.к. K, а значит и L, - чисто мнимое, а $Br(\mathbf{C}) = 0$.

Теорема 9.2. *Закон взаимности Хассе.* Сумма локальных инвариантов ц.п.а. равна 0.

Доказательство. По предыдущей теореме, класс $[A]$ лежит в $H^2(G, L^*)$, где L/k - расширение степени n с циклической группой Галуа G, $L \subset k(\zeta)$, $\zeta^m = 1$. Группа $H^2(G, \mathbf{Z}) = Hom(G, \mathbf{Q}/\mathbf{Z})$ циклическая порядка n, она порождается некоторым характером χ. Этот характер можно рассматривать как характер группы $Gal(k(\zeta)/k)$ (при желании, как характер всей группы $Gal(\overline{\mathbf{Q}}/k)$), тогда L есть поле инвариантов $Ker(\chi)$.

По периодичности когомологий Тейта циклических групп $\cup$-произведение с $\delta\chi \in H^2(G, \mathbf{Z})$ дает изоморфизм $\hat{H}^0(G, L^*) \to H^2(G, L^*)$, т.е. класс A записывается в виде $[A] = \overline{a} \cup \delta\chi$ для некоторого $a \in k^*$. Покажем, что для данного $\overline{a}$ число a можно выбрать в сколь угодно малой окрестности 1 относительно нормирований $v \in M_k$, лежащих над простыми делителями m.

Вспомним, что m взаимно просто с простыми $v \in M_k$, в которых $inv_v(A) \neq 0$. Иными словами, если v лежит над простым делителем m, то $inv_v(A) = 0$. Пусть $\theta_v : k_v^* \to G_v$ - локальное отображение взаимности для k_v ($G_v = Gal(L_w/k_v) \subset G$ - группа разложения v). По предложению 4.1 - основной формуле, связывающей локальный инвариант и локальное отображение взаимности - имеем:

$$inv_v(\overline{a} \cup \delta\chi) = \chi(\theta_v(a)).$$

Отсюда для $v|m$ получаем $\theta_v(a) = 1$, т.е. $a = N_{L_w/k_v}(c_w)$ для некоторого $c_w \in L_w$, для каждого $w \in M_L$, $w|v$. Во множестве нормирований $w \in M_L$, лежащих над данным $v|m$, выберем одно и для него положим $c'_w = c_w$, а для остальных - $c'_w = 1$. Применим теорему о слабой аппроксимации в L к набору чисел $c'_w \in L_w$ для $w \in M_L$, $w|m$, и найдем $c \in L$ достаточно близкий ко всем c'_w. Тогда $N_{L/k}(c) = \prod_{w|v} N_{L_w/k_v}(c)$ будет сколь угодно близок к a, а $a/N_{L/k}(c)$ сколь угодно близок к 1 для $v|m$. В частности, потребуем, чтобы абсолютная норма $N_{k/\mathbf{Q}}(a)$ была достаточно близка к 1 для всех простых $p|m$.

Дальнейшее рассуждение состоит в редукции к случаю кругового расширения поля рациональных чисел. Очевидным образом, $Gal(\overline{\mathbf{Q}}/k)$ вложена в $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$, откуда получается вложение факторгрупп $Gal(k(\zeta)/k) \subset Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$. В теореме 9.1 поле L строится как композит k и некоторого промежуточного циклического расширения $\mathbf{Q} \subset K \subset \mathbf{Q}(\zeta)$. Поэтому характер χ есть ограничение некоторого характера χ' группы $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ на подгруппу $Gal(\overline{\mathbf{Q}}/k)$. ($K$ есть поле инвариантов $Ker(\chi')$.)

Пусть $v \in M_k$ лежит над p-адическим нормированием $\mathbf{Q}$ (рассуждение для бесконечных нормирований аналогично). Тогда

$$inv_v(A) = inv_v(\overline{a} \cup \delta\chi) = inv_v(\overline{a} \cup Res_{k_v/\mathbf{Q}_p}(\delta\chi')) = inv_p(Cores_{k_v/\mathbf{Q}_p}(\overline{a} \cup \delta\chi')) = inv_p(Cores_{k_v/\mathbf{Q}_p}(\overline{a}) \cup \delta\chi'),$$

где третье равенство следует из 3.2 (б), а последнее - из свойств $\cup$-произведения. Понятно, что $Cores_{k_v/\mathbf{Q}_p}(a)$ есть норма $N_{k_v/\mathbf{Q}_p}(a)$, и учитывая то, что

$$\prod_{v|p} N_{k_v/\mathbf{Q}_p}(a) = N_{k/\mathbf{Q}}(a),$$

достаточно проверить, что

$$\sum_{v \in M_k} inv_v(A) = \sum_{u \in M_{\mathbf{Q}}} inv_u(\overline{b} \cup \delta\chi') = 0,$$

где $b = N_{k/\mathbf{Q}}(a)$. При этом a было выбрано так, что b лежит в сколь угодно малой окрестности 1 в p-адической топологии для всех $p|m$ (в частности, b сравнимо с 1 по модулю m). Поэтому в силу предложения 4.1 и непрерывности локальных отображений взаимности имеем

$$\sum_{v \in M_k} inv_v(A) = \sum_{u \in M_{\mathbf{Q}}} inv_u(\overline{b} \cup \delta\chi') = \chi'(\prod_{u \in M_{\mathbf{Q}}} \theta_u(b)) = \chi'(\theta_\infty(b) \prod_{(p,m)=1} \theta_p(b)).$$

Простые, не делящие m, не разветвлены в $\mathbf{Q}(\zeta)/\mathbf{Q}$, а следовательно и в $K/\mathbf{Q}$. Из предложению 4.3, описания Фробениусов для кругового расширения и функториальности (см. конец предыдущей главы) следует, что для таких простых $\theta_p(b)$ есть канонический образ $p^{val_p(b)} \in (\mathbf{Z}/m)^* = Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$ в фактор-группе $Gal(K/\mathbf{Q})$. Таким же образом, $\theta_\infty(b)$ есть образ $sgn(b) \in (\mathbf{Z}/m)^* = Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$ в $Gal(K/\mathbf{Q})$. Отсюда $\theta_\infty(b) \prod_{(p,m)=1} \theta_p(b)$ есть образ $sgn(b) \prod_{(p,m)=1} p^{val_p(b)} = b \in (\mathbf{Z}/m)^* = Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$, однако b сравнимо с 1 по модулю m, и, следовательно, $\theta_\infty(b) \prod_{(p,m)=1} \theta_p(b) = 1$, что и требовалось доказать.

Как следствие получаем, что последовательность

$$0 \to Br(k) \to \oplus_{v \in M_k} Br(k_v) \to \mathbf{Q}/\mathbf{Z} \to 0,$$

где правая стрелка есть сумма локальных инвариантов (будем считать, что для вещественных точек локальный инвариант принимает значения 0 и 1/2), является комплексом. Ее точность в левом члене следует из теоремы Брауэра-Хассе-Нетер. Можно доказать, что эта последовательность точна.

Следствие 9.3. *Закон взаимности Артина.* Пусть K/k - расширение Галуа с группой G. Произведение локальных отображений взаимности - "глобальное отображение взаимности" - дает гомоморфизм группы иделей J_k в G^{ab}, тривиальный на главных иделях.

(Надо скомпоновать локальные отображения взаимности θ_v с естественным гомоморфизмом $G_v^{ab} \to G^{ab}$ и взять произведение. Иначе говоря, если $\chi \in Hom(G, \mathbf{Q}/\mathbf{Z})$, то $\prod_{v \in M_k} \chi(\theta_v(z_v))$ равно 1 на главных иделях.)

Доказательство следует из закона взаимности Хассе взятием $\cup$-произведения с $\delta\chi$.

Таким образом, глобальное отображение взаимности происходит из гомоморфизма

$$\theta := \prod_{v \in M_k} \theta_v : C_k/N_{K/k}(C_K) \to G^{ab}.$$

Можно доказать, что это изоморфизм.