Введение в теорию полей классов

А.Н.Скоробогатов

Нижеследующий текст представляет собой слегка отредактированные записки лекций, прочитанных в Независимом Московском Университете весной и осенью 1995 года. У слушателей не предполагалось почти никаких предварительных знаний, выходящих за рамки стандартного университетского курса. Я ставил своей целью дать общий взгляд на алгебраическую теорию чисел, надеясь, что эти лекции помогут в самостоятельном освоении столь важной дисциплины, какой является теория полей классов, со времен Кронекера, Вебера, Гильберта и до наших дней являющаяся источником множества фундаментальных математических понятий и основой для всех выдающихся достижений теории чисел последних лет. По теории полей классов имеются прекрасные, ставшие классическими книги: "Алгебраическая теория чисел" (под ред. Дж.Касселса и А.Фрелиха), "Основы теории чисел" Андрэ Вейля и до сих пор не переведенная на русский язык "Corps locaux" Ж.-П. Серра. За те около 20 лекций, которые были прочитаны, стараться переизлагать содержание любой из них было бы невыполнимой задачей. Поэтому автор избрал способ изложения материала, лежащий где-то между техникой "patchwork" и стилем неподражаемого "Краткого курса" ("Советский народ одобрил разгром бухаринско-троцкистской банды и перешел к очередным делам"). Мне не удалось продвинуться так далеко, как хотелось бы. Курс завершается доказательством закона взаимности, чего, впрочем, достаточно для некоторых приложений, таких, как, например, конструкция препятствия Манина к принципу Хассе для многообразий над глобальными полями.

Мне приятно поблагодарить всех студентов, посещавших эти лекции, за критические замечания и моральную поддержку.

Часть первая

Оглавление

1. Целые элементы

Обозначения и соглашения: Все кольца предполагаются коммутативными и с единицей (если не оговорено противное). Целостное кольцо - это то же самое, что кольцо без делителей нуля. Модуль M над кольцом A имеет конечный тип, если он порожден конечным числом своих элементов.

Пусть $A \subseteq B$ - целостные кольца. Элемент $x \in B$ называется *целым* над A, если он является корнем многочлена со старшим коэффициентом 1:

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0,\ \ a_i \in A.$$

Предложение 1.1 Следующие свойства эквивалентны:
(a) x цел над A,

(б) $A[x]$ - A-модуль конечного типа,
(в) существует A-модуль конечного типа $M \subseteq B, M \neq 0$, такой, что $xM \subseteq M$ и $A \subseteq M$.

Доказательство. (а⇒б) A-модуль $A[x]$ порожден $1, x, \ldots, x^{n-1}$.
(б⇒в) Взять $M = A[x]$.
(в⇒а) Пусть M порожден $v_1, \ldots, v_m$. Действие x на $v_1, \ldots, v_m$ задается некоторой матрицей S. Тогда $xId - S$ аннулирует вектор-столбец $(v_1, \ldots, v_m)^t$. Отсюда x - корень многочлена $det(tId - S) = 0$. (Действительно, пусть T - присоединенная матрица для $xId - S$, так, что $T(xId - S) = det(xId - S)Id$. Значит, $det(xId - S) \in B$ аннулирует M. Однако $1 \in A \subseteq M$, поэтому $det(xId - S) = 0$, т.к. A не имеет делителей нуля.)

Определение 1.2 Целостное кольцо B, $A \subseteq B$, называется *целым* над A, если каждый его элемент цел над A.

Предложение 1.3 (а) Если B цело над A и является A-алгеброй конечного типа, то B - A-модуль конечного типа. (Применить индукцию по числу образующих.)
(б) Если B цело над A, C цело над B, то C цело над A. (Взять в качестве M из 1.1 (в) A-алгебру, порожденную элементом $x \in C$, целым над B, и коэффициентами многочлена над B со старшим коэффициентом 1, корнем которого он является.)

Определение 1.4 Пусть $A \subseteq B$ - целостные кольца. Множество элементов из B, целых над A, называется *целым замыканием* A в B.

Важное свойство целого замыкания состоит в том, что это множество является кольцом. (Замкнутость относительно произведения получается рассмотрением M_1M_2, где M_i - как в 1.1 (в).)

Определение 1.5 Кольцо A *целозамкнуто* в B, если целое замыкание A в B есть A. Кольцо A *целозамкнуто*, если оно целозамкнуто в своем поле частных.

Упражнение 1.6 Доказать, что кольцо целых чисел целозамкнуто. То же для любого кольца с однозначным разложением на простые множители. Напомним, что любое целостное кольцо главных идеалов является кольцом с однозначным разложением на простые множители (Ленг, “Алгебра”, гл. 2)

Упражнение 1.7 Доказать, что целое замыкание A в B целозамкнуто в B. (Использовать 1.3 (б).)

2. Нетеровы кольца

Определение 2.1 Нетеровым называется кольцо, удовлетворяющее одному из следующих эквивалентных условий:
(а) любая возрастающая цепочка идеалов стационарна,
(б) любое множество идеалов содержит максимальный элемент,
(в) любой идеал конечно порожден (как модуль).

Доказательство. Эквивалентность (а) и (б) - простое общее утверждение о частично упорядоченных множествах. (в⇒а) : Взять объединение всех идеалов цепочки. (б⇒в) : Пусть I - не конечно порожденный идеал, тогда рассмотрим множество его конечно порожденных подидеалов. Оно непусто (т.к. содержит 0), его максимальный элемент J отличен от I. Пусть $x \in I \setminus J$, тогда $J + Ix$ строго содержит J, но при этом $J + Ix$ конечно порожден - противоречие. (Этот прием называется “нетеровой индукцией”.)

Пример 2.2 Любое кольцо главных идеалов нетерово. (2.1 (в))

Теорема Гильберта о базисе утверждает, что если A нетерово, то нетеровыми являются также кольцо многочленов $A[x]$ и кольцо формальных степенных рядов $A[[x]]$.

Упражнение 2.3 Кольцо многочленов от бесконечного число переменных не является нетеровым.

3. Кольца Дедекинда

Определение 3.1 Целостное кольцо A называется *дедекиндовым*, если оно

1) нетерово,
2) целозамкнуто,
3) любой ненулевой идеал A максимален.

Упражнение 3.2 Доказать, что любое кольцо главных идеалов дедекиндово. (Примеры: $\mathbf{Z}$, $k[x]$, где k - поле.) Являются ли дедекиндовыми следующие кольца: $\mathbf{Z}[x]$, $k[x, y]$?

Теорема Крулля утверждает, что целое замыкание дедекиндова кольца в конечном сепарабельном замыкании его поля частных - дедекиндово.

4. Дробные идеалы

Определение 4.1 Пусть A - целостное кольцо, K - его поле частных. A-подмодуль $M \subset K$ называется *дробным идеалом*, если для некоторого $c \in A, c \neq 0$, имеет место включение $cM \subseteq A$. Дробный идеал M *обратим*, если существует дробный идеал N, такой, что $MN = A$.

Дробный идеал M является идеалом в обычном смысле слова (говорят также - *целым* идеалом) тогда и только тогда, когда $M \subseteq A$.

Эквивалентное определение колец Дедекинда дается следующей теоремой.

Теорема 4.2 Кольца Дедекинда - это в точности те целостные кольца, в которых любой ненулевой идеал обратим.

Упражнение 4.3 Пусть A - целостное кольцо, M - его дробный идеал. Положим

$$M^{-1} = \{x \in K \mid xM \subset A\}.$$

Доказать, что M^{-1} - дробный идеал.

Упражнение 4.4 Если A - нетерово, то A-подмодуль $M \subset K$ - дробный идеал тогда и только тогда, когда M - A-модуль конечного типа.

Фундаментальное свойство колец Дедекинда состоит в следующем описании структуры его дробных идеалов.

Теорема 4.5 В кольце Дедекинда дробные идеалы образуют группу по умножению, причем любой дробный идеал однозначно представляется в виде произведения конечного числа простых идеалов в целых степенях.

5. Локализация и локальные кольца

Обозначение: A^* - множество обратимых элементов кольца A. Они иногда также называются *единицами* кольца A.

Определение 5.1 *Мультипликативным* подмножеством кольца A называется его подмножество, содержащее 1 и замкнутое относительно умножения.

Для подмножества $S \subseteq A$ через $\overline{S}$ будем обозначать наименьшее мультипликативное подмножество A, содержащее S.

Определение 5.2 Локализация A в S определяется как множество классов эквивалентности на $A \times \overline{S}$: $(a, b) \sim (a', b')$ тогда и только тогда, когда существует $t \in \overline{S}$, такой, что $t(ab' - a'b) = 0$. Операции сложения и умножения вводятся по образцу сложения и умножения обычных дробей - паре (a, b) соответствует дробь a/b. Полученное кольцо обозначается $A[S^{-1}]$.

Имеется канонический гомоморфизм $i : A \to A[S^{-1}]$, $i(a) = (a, 1)$. Убедиться в том, что если $x \in S$, то $i(x) \in A[S^{-1}]^*$, и что любой гомоморфизм $j : A \to B$, такой, что $j(S) \subseteq B^*$ пропускается через i (т.е. существует единственный гомоморфизм $A[S^{-1}] \to B$, композиция которого с i дает j). Это - "универсальное свойство" $A[S^{-1}]$.

Если S - мультипликативное множество, то наряду с $A[S^{-1}]$ используется обозначение $S^{-1}A$.

Упражнение 5.3 (а) i - инъективен тогда и только тогда, когда S не содержит делителей нуля.
(б) i - биективен тогда и только тогда, когда $S \subset A^*$.

Упражнение 5.4 Идеалы и локализация. Пусть

$$\alpha : I \mapsto i^{-1}(I \cap i(A))$$

- отображение $\{$*идеалы* $S^{-1}A\} \to \{$*идеалы* $A\}$, и

$$\beta : J \mapsto i(J)S^{-1}A$$

- отображение в обратную сторону. Доказать, что $\beta\alpha = Id$. Показать, что α задает биекцию

$$\{\textit{простые идеалы } I \subset S^{-1}A\} = \{\textit{простые идеалы } J \subset A | J \cap S = \emptyset\}.$$

Отсюда понятно, что нетеровость сохраняется при локализации.

Упражнение 5.5 Целозамкнутость сохраняется при локализации.

Вот два стандартных примера мультипликативных подмножеств:
1) Пусть A - целостное, $S = A \setminus 0$, тогда $S^{-1}A$ - поле частных A.
2) Пусть $\mathcal{P}$ - простой идеал в A, тогда $S = A \setminus \mathcal{P}$ - мультипликативное подмножество. Обозначение: $A_{\mathcal{P}} := (A \setminus \mathcal{P})^{-1}A$.

Определение 5.6 *Локальное* кольцо - это кольцо, удовлетворяющее одному из следующих эквивалентных свойств (доказать их эквивалентность!):
(а) $A \setminus A^*$ - идеал,
(б) A имеет единственный максимальный идеал ($\neq A$).
Факторкольцо по единственному максимальному идеалу называется *полем вычетов* локального кольца.

Упражнение 5.7 Доказать, что $A_{\mathcal{P}}$ - локальное кольцо ("локализация A в $\mathcal{P}$"). Пусть $\mathcal{M}_{\mathcal{P}}$ - его максимальный идеал. Доказать, что $\mathcal{M}_{\mathcal{P}} = i(\mathcal{P})A_{\mathcal{P}}$ и $i^{-1}(\mathcal{M}_{\mathcal{P}}) \cap i(A)) = \mathcal{P}$. Поле вычетов $A_{\mathcal{P}}/M_{\mathcal{P}}$ изоморфно полю частных целостного кольца $A/\mathcal{P}$.

Упражнение 5.8 Разобрать следующие примеры локальных колец: (а) Рациональные числа, в знаменатель которых не входит простое число p. То же с многочленами над полем. (б) Кольцо формальных степенных рядов от одной или нескольких переменных над локальным кольцом (например, над полем).

6. Кольца дискретного нормирования

Определение 6.1 Кольцо дискретного нормирования - это целостное кольцо главных идеалов с единственным простым идеалом.

Очевидно, что такие кольца локальны. Ясно также, что локальное кольцо главных идеалов - кольцо дискретного нормирования. Подобно тому, как локальные кольца естественным образом появляются при локализации по простому идеалу, кольца дискретного нормирования появляются из нормирований полей. Поле K - поле. Его *дискретным нормированием* называется сюръективный гомоморфизм $v : K \to \mathbf{Z}$, удовлетворяющий условию

$$v(x+y) \geq inf\{v(x), v(y)\}$$

("ультраметрическое неравенство"). Полагаем $v(0) = \infty$. Пусть

$$O_v = \{x \in K | v(x) \geq 0)\},\ U_v = \{x \in K | v(x) = 0)\},\ \mathcal{P}_v = \{x \in K | v(x) > 0)\}.$$

Упражнение 6.2 (а) Доказать, что если $v(x) \neq v(y)$, то $v(x+y) = inf\{v(x), v(y)\}$.
(б) Доказать, что O_v - кольцо с полем частных K, что $U_v = O_v^*$, и что $\mathcal{P}_v$ - идеал O_v.

Предложение 6.3 (а) O_v - кольцо дискретного нормирования.

(б) Пусть A - кольцо дискретного нормирования, тогда на его поле частных существует такое дискретное нормирование v, что $A = O_v$.

Доказательство. (а) Зафиксируем элемент $\pi \in O_v$ такой, что $v(\pi) = 1$ ("униформизующую"). Пусть I - идеал A. Положим $v(I) = inf\{v(x)|x \in I\}$. Докажем, что $I = (\pi^{v(I)})$. Пусть $b \in I$, $v(b) = v(I)$, тогда $b = \pi^{v(I)}u$, где $u \in U_v$. Следовательно, $(b) = (\pi^{v(I)}) \subseteq I$. Обратное включение также очевидно.

(б) Пусть $\mathcal{P}$ - единственный простой идеал A. Он главный, пусть $\mathcal{P} = (\pi)$. В кольце главных идеалов каждый элемент однозначно разлагается на простые множители. В нашем случае π - единственный простой элемент (с точностью до умножения на обратимый элемент). Значит, любой элемент $x \in A$ имеет вид $x = \pi^n u$, $n \geq 0$, $u \in A^*$. Нормирование вводится так: $v(x) = n$ (понятно, что оно естественно продолжается на поле частных).

Дробные идеалы в кольце дискретного нормирования порождаются целыми степенями π. Относительно умножения они образуют бесконечную циклическую группу. Имеется следующая характеризация колец дискретного нормирования.

Теорема 6.4 Кольца дискретного нормирования суть в точности нетеровы целозамкнутые кольца с единственным простым идеалом.

Доказательство см. в Касселс-Фрелих, гл.I, предложение 1.3.

Теорема 6.5 Пусть A - целостное кольцо. Следующие утверждения эквивалентны:

(а) A - дедекиндово,

(б) A - нетерово и для любого простого идеала $\mathcal{P} \subset A$ локализация A в $\mathcal{P}$ является кольцом дискретного нормирования,

(в) дробные идеалы кольца A обратимы.

Доказательство. ($a \Rightarrow б$) 5.4 и 5.5.

($б \Rightarrow в$) Докажем, что II^{-1} (определение I^{-1} см. в (4.3)) не содержится ни в одном максимальном идеале $\mathcal{P}$, построив элемент из $II^{-1} \setminus \mathcal{P}$. По нетеровости I имеет конечный тип, $I = Aa_1 + \ldots + Aa_n$. Пусть v - нормирование, связанное с $\mathcal{P}$. Предположим, что $inf(v)$ достигается, скажем, на a_1. Тогда $v(a_1^{-1}a_i) \geq 0$ и $a_1^{-1}a_i$ записывается в виде x_i/y_i, $x_i \in A$, $y_i \in A$, так, что $y_i \notin \mathcal{P}$. Положим $y = y_2 \ldots y_n$. Так как $\mathcal{P}$ - простой, то $y \notin \mathcal{P}$. С другой стороны, $(ya_1^{-1})a_i \in A$, т.е. $ya_1^{-1} \in I^{-1}$, следовательно, $y \in II^{-1} \setminus \mathcal{P}$.

($в \Rightarrow a$) Нетеровость: пусть $1 = \sum a_i b_i$, где $a_i \in I$, $b_i \in I^{-1}$, тогда I порожден a_i. Целозамкнутость: если $x \in K$ цел над A, то кольцо $A[x]$ - A-модуль конечного типа, а т.к. A - нетерово, то $A[x]$ - дробный идеал (4.4), притом обратимый. Отсюда:

$$A[x] = A[x]A = A[x]A[x]A[x]^{-1} = A[x]A[x]^{-1} = A,$$

следовательно, $x \in A$. Если I - простой идеал, $\mathcal{P}$ - максимальный идеал, в котором I содержится, то $I\mathcal{P}^{-1} \subseteq A$ - целый идеал, $(I\mathcal{P}^{-1})\mathcal{P} = I$. Из того, что I - простой, следует, что либо $\mathcal{P} \subseteq I$, либо $I\mathcal{P}^{-1} \subseteq I$. В первом случае мы получаем, что $\mathcal{P} = I$, что и требовалось. Во втором случае

$$\mathcal{P}^{-1} = I^{-1}I\mathcal{P}^{-1} \subseteq I^{-1}I = A,$$

откуда $\mathcal{P} = A$ - противоречие.

Как следствие получаем теорему 4.2 и первую часть теоремы 4.5.

Окончание доказательства теоремы 4.5. Если целый идеал I содержится в максимальном идеале $\mathcal{P}$, то $I\mathcal{P}^{-1}$ содержится в A, т.е. это тоже целый идеал. Получается возрастающая цепочка идеалов, которая по нетеровости должна в какой-то момент оборваться. Это дает некоторое разложение в произведение простых идеалов. Тот факт, что такое разложение единственно, получается рассмотрением локализаций во всех максимальных идеалах.

7. Расширения полей

Расширение полей L/K называется *конечным*, если $dim_K(L) = n < \infty$, тогда n называется *степенью* расширения L/K. Умножению на элемент $x \in L$ отвечает линейный оператор на L, который будем обозначать A_x. Характеристический многочлен $f_x(t) = det(tId - A_x)$ является степенью минимального многочлена A_x. (Рассмотреть промежуточное расширение $K \subseteq K(x) \subseteq L$ и действие A_x в базисе $x^i\theta_j$, где $\{\theta_j\}$ - базис $L/K(x)$.)

Определение 7.1 *След* элемента $x \in L$ из L в K определяется как след оператора A_x, $Tr_{L/K}(x) := Tr(A_x)$, а *норма* - как определитель A_x, $N_{L/K}(x) := det(A_x)$.

Очевидно, что если $x \in K$, то $Tr_{L/K}(x) = nx$, $N_{L/K}(x) = x^n$.

Определение 7.2 Конечное расширение полей L/K называется *сепарабельным*, если выполнены следующие эквивалентные условия:
(а) существует $x \in L$, такой, что $Tr_{L/K}(x) \neq 0$,
(б) билинейная форма $Tr_{L/K}(xy)$ невырождена,
(в) минимальный многочлен любого элемента $x \in L$ сепарабелен (не имеет кратных корней).

Упражнение 7.3 Конечное расширение степени n, взаимно простой с характеристикой поля K, - сепарабельно. Верно ли обратное?

Упражнение 7.4 Конечное сепарабельное расширение порождено одним элементом.

8. Расширения колец Дедекинда. Ветвление

Мы собираемся изучать следующую ситуацию: A - дедекиндово кольцо с полем частных K, L - конечное сепарабельное расширение K степени n, B - целое замыкание A в L. Вот два основных примера:

1) $A = \mathbf{Z}$, $K = \mathbf{Q}$, L - конечное расширение $\mathbf{Q}$. Такое поле называется *полем алгебраических чисел* или *числовым полем*, B - его *кольцом целых*.

2) $A = k[x]$, где k - поле, $K = k(x)$, L - конечное сепарабельное расширение K. (В простейшем случае в качестве k берется конечное поле.) В этом примере, как и в предыдущем, A - кольцо главных идеалов. Этот случай называют функциональным в отличие от предыдущего, называемого арифметическим.

Поскольку каждый элемент $x \in L$ является корнем многочлена с коэффициентами из K и старшим коэффициентом 1 (например, характеристического), то для некоторого $a \in A$ элемент ax будет корнем многочлена с коэффициентами из A и старшим коэффициентом 1. (Домножить многочлен на произведение знаменателей коэффициентов в степени, равной степени многочлена.) Отсюда $ax \in B$. Поэтому $KB = L$, и, в частности, L есть поле частных B.

Если $x \in B$, то $Tr_{L/K}(x) \in A$. (След равен сумме всех корней $f_x(t)$ в некотором расширении L, каждый из них цел над A, а значит и $Tr_{L/K}(x) \in K$ также цел над A, но A целозамкнуто в K.)

Предложение 8.1 B является A-модулем конечного типа.

Доказательство. Если M - A-подмодуль L, то определим *двойственный* модуль $M^* := \{x \in L | Tr_{L/K}(xy) \in A$ для любого $y \in M\}$. Так как $Tr_{L/K}(B) \subseteq A$, имеем $B \subseteq B^*$. Базис L как векторного пространства над K можно выбрать среди элементов B, пусть V - A-модуль, порожденный этими элементами. Он является свободным A-модулем конечного типа. Тогда $V \subseteq B \subseteq B^* \subseteq V^*$, причем V^* - свободный A-модуль конечного типа. Следовательно, B - A-модуль конечного типа.

Целый идеал B, обратный к дробному идеалу B^*, называется *дифферентой* B над A.

Предложение 8.2 (Теорема Крулля) B - кольцо Дедекинда.

Доказательство. Идеалы B являются A-подмодулями A-модуля B конечного типа, следовательно, они имеют конечный тип как A-модули, тем самым и как B-модули. Это доказывает нетеровость B. Если $I \subset J, I \neq J$, - простые идеалы B, то $A \cap I \neq A \cap J$. (От противного: отфакторизовав по I, можно считать, что $I = 0$; пусть $x^n + a_{n-1}x^{n-1} + \ldots + a_0$ - минимальный многочлен $x \in J$, $x \neq 0$, $a_i \in A$,

$a_0 \neq 0$, но $a_0 \in A \cap J = A \cap I = 0$ - противоречие.) Поскольку A не содержит двух ненулевых простых идеалов, один из которых содержит другой, то это же верно и для B.

Напомним следующий факт:

8.3 *Китайская теорема об остатках.* Пусть $I_1, \ldots, I_n$ - идеалы кольца A, такие, что если $i \neq j$, то $I_i + I_j = A$. Тогда для любых $x_1, \ldots, x_n$ из A существует элемент $x \in A$, такой, что x сравнимо с x_i по модулю идеала I_i. (Ленг, "Алгебра", гл.II, 2)

Следствие: $A/\cap_i I_i = \prod_i A/I_i$.

8.4 Другой факт: модуль конечного типа без кручения (если $am = 0$, $a \in A$, $m \in M$, $m \neq 0$, тогда $a = 0$) над кольцом главных идеалов свободен. (Ленг, "Алгебра", гл. XV,2) Например, конечно порожденная абелева группа без кручения изоморфна $\mathbf{Z}^n$.

Отсюда, из 8.1 и из того, что $KB = L$, следует, что кольцо целых числового поля изоморфно $\mathbf{Z}^n$. Соответствующий аналог верен и в функциональном случае.

Используется следующая терминология: пусть $\mathcal{B}$ - ненулевой простой идеал B, тогда $\mathcal{P} = \mathcal{B} \cap A$ - ненулевой простой идеал A. Говорят, что $\mathcal{B}$ *лежит над* $\mathcal{P}$, или, что $\mathcal{B}$ *делит* $\mathcal{P}$; обозначение: $\mathcal{B}|\mathcal{P}$. В силу однозначности разложения имеем $\mathcal{P}B = \prod \mathcal{B}^{e_\mathcal{B}}$, $e_\mathcal{B}$ называется *индексом ветвления* $\mathcal{B}$ в расширении L/K. Факторкольцо $B/\mathcal{B}$ есть поле, содержащее поле $A/\mathcal{P}$; это расширение конечной степени (т.к. B - A-модуль конечного типа). Обозначим степень этого расширения $f_\mathcal{B}$. Если $e_\mathcal{B} = 1$ для всех $\mathcal{B}|\mathcal{P}$ и соответствующие расширения полей вычетов сепарабельны, то $\mathcal{P}$ называется неразветвленным для данного расширения. Если же $\mathcal{B}$ - единственный идеал, делящий $\mathcal{P}$, и $f_\mathcal{B} = 1$, то $\mathcal{P}$ называется вполне разветвленным.

Теорема 8.5 Пусть $\mathcal{P}$ - простой идеал A. Кольцо $B/\mathcal{P}B$ является алгеброй над полем $A/\mathcal{P}$ размерности n, эта алгебра изоморфна прямой сумме алгебр $B/calB^{e_\mathcal{B}}$ по всем $\mathcal{B}|\mathcal{P}$. При этом

$$n = \sum_{\mathcal{B}|\mathcal{P}} e_\mathcal{B} f_\mathcal{B}.$$

Доказательство. Первое утверждение: пусть $B' = (A \setminus \mathcal{P})^{-1}B$. По 8.1 B' - $A_\mathcal{P}$-модуль конечного типа. Так как $A_\mathcal{P}$ - кольцо главных идеалов, поэтому B' - свободный $A_\mathcal{P}$-модуль (8.4). При этом его ранг равен n, т.к. B' порождает векторное пространство L над K размерности n. Переходя к фактору по $\mathcal{P}$ убеждаемся, что $B/\mathcal{P}B = B'/\mathcal{P}B'$ - векторное пространство над $A/\mathcal{P}$ размерности n. Второе утверждение - следствие китайской теоремы об остатках. Размерность $B/\mathcal{B}^{e_\mathcal{B}}$ вычисляется рассмотрением фильтрации степенями $\mathcal{B}$ с учетом изоморфизма $\mathcal{B}^{i+1}/\mathcal{B}^i = B/\mathcal{B}$.

Упражнение 8.6 $B' = (A \setminus \mathcal{P})^{-1}B$ - кольцо главных идеалов. (Как и всякое дедекиндово кольцо с конечным числом простых идеалов - воспользоваться китайской теоремой.)

Еще один стандартный факт из коммутативной алгебры:

Лемма 8.7 (Лемма Накаямы) Пусть A - кольцо, M - A-модуль конечного типа, I - идеал A, содержащийся во всех максимальных идеалах (например, I - единственный максимальный идеал локального кольца). Если $IM = M$, то $M = 0$.

Доказательство. От противного: предположим, что $M \neq 0$, и выберем некоторую минимальную систему образующих этого модуля $v_1, \ldots, v_n$. Тогда $v_1 = \sum a_i v_i$, где $a_i \in I$, но $1 - a_1 \in A^*$ - иначе 1 лежала бы в некотором максимальном идеале - т.е. M порождается $v_2, \ldots, v_n$. Противоречие.

Следствие 8.7.1 Если N - подмодуль M, то $N + IM = M$ влечет $M = N$.

Следствие 8.7.2 Пусть A - локальное кольцо с максимальным идеалом $\mathcal{M}$, тогда если $x_1, \ldots, x_n \in M$ таковы, что их образы порождают $M/\mathcal{M}M$ как векторное пространство над $A/\mathcal{M}$, то сами $x_1, \ldots, x_n$ порождают M.

Изучим ветвление с локальной точки зрения. Рассмотрим случай расширений, порожденных одним элементом. (Таковы все конечные сепарабельные расширения.)

Пусть A - локальное кольцо с максимальным идеалом $\mathcal{M}$ и полем вычетов $k = A/\mathcal{M}$. Пусть $B = A[x]/(f(x))$, где $f(x) \in A[x]$ имеет старший коэффициент 1. Пусть $\overline{f}(x)$ - многочлен, получающийся редукцией коэффициентов по модулю $\mathcal{M}$, и $\overline{f}(x) = \prod_i \phi_i(x)^{e_i}$ - разложение $\overline{f}(x)$ на неприводимые сомножители в $k[x]$.

Лемма 8.8 Пусть $g_i(x) \in A[x]$ таковы, что $\overline{g_i}(x) = \phi_i(x)$. Максимальные идеалы B суть в точности $\mathcal{M}_i = (\mathcal{M}, g_i(x))$, причем $B/\mathcal{M}_i = k[x]/(\phi_i(x))$.

Доказательство. Максимальность $\mathcal{M}_i$ следует из неприводимости $\phi_i(x)$. Поскольку $\mathcal{M}_i$ суть в точности максимальные идеалы, содержащие $\mathcal{M}B$, достаточно доказать, что любой максимальный идеал $\mathcal{N} \subset B$, содержит $\mathcal{M}B$. В противном случае $\mathcal{N} + \mathcal{M}B = B$, и по следствию из леммы Накаямы $\mathcal{N} = B$. Противоречие.

Пусть теперь A - кольцо дискретного нормирования (к предыдущему добавляется условие, чтобы A было кольцом главных идеалов), в частности, A - дедекиндово.

Следствие 8.9 Идеал $\mathcal{M}$ неразветвлен тогда и только тогда, когда $\overline{f}(x)$ не имеет кратных корней.

Доказательство. По формуле $n = \sum_{\mathcal{B}|\mathcal{M}} e_{\mathcal{B}} f_{\mathcal{B}}$ (8.5) неразветвленность эквивалентна тому, что $n = \sum_{\mathcal{B}|\mathcal{M}} f_{\mathcal{B}}$.

Примеры. (а) Если $\overline{f}(x)$ неприводим в $k[x]$, то по 8.8 B - также кольцо дискретного нормирования с полем вычетов $k[x]/(\overline{f}(x))$. Максимальный идеал B порожден $\mathcal{M}$. Если имеет место другая крайность - $\overline{f}(x)$ распадается в произведение линейных множителей, то говорят, что $\mathcal{M}$ полностью распадается.

(б) Пусть $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_i \in \mathcal{M}$, $a_0 \in \mathcal{M} \setminus \mathcal{M}^2$, - "многочлен Эйзенштейна". Максимальный идеал B есть $(\mathcal{M}, x) = (x)$, т.к. $a_0 \in (x)$ и a_0 порождает $\mathcal{M}$. Здесь $f_{\mathcal{B}} = 1$, следовательно, $e_{\mathcal{B}} = n$, и идеал $\mathcal{M}$ вполне разветвлен.

Как узнать, какие простые идеалы разветвлены в данном расширении?

Для ответа на этот вопрос рассмотрим понятие дискриминанта расширения L/K. В простейшем случае, когда A - кольцо главных идеалов, B, как и всякий A-модуль без кручения, является свободным A-модулем. Пусть $w_1, \ldots, w_n$ - его базис (понятно, что это будет также базис L как векторного пространства над K), и пусть

$$D(w_1, \ldots, w_n) := det(Tr_{L/K}(w_i w_j))$$

- определитель матрицы Грама квадратичной формы $Tr_{L/K}(x^2)$ в этом базисе. Определитель матрицы перехода от одного базиса к другому лежит в A^*, т.е. с точностью до квадратов в A^* определен элемент A, называемый *дискриминантом* расширения L/K. Это рассуждение проходит, например, в случае $A = \mathbf{Z}$, тогда полученное целое число, свободное от квадратов, называется абсолютным дискриминантом поля L.

В общем случае B - не обязательно свободный A-модуль. Тогда дискриминант $D_{L/K}$ определяется как идеал A, порожденный элементами $det(Tr_{L/K}(w_i w_j))$ для всевозможных базисов $w_1, \ldots, w_n$ векторного пространства L над K, таких, что $w_i \in B$. Конструкция дискриминанта коммутирует с локализацией, поэтому можно вычислять дискриминант локально, воспользовавшись тем, что кольца дискретного нормирования являются кольцами главных идеалов, в силу чего на локальном уровне применимо предыдущее рассуждение.

Теорема 8.10 Простой идеал $\mathcal{P}$ не делит $D_{L/K}$ тогда и только тогда, когда $\mathcal{P}$ неразветвлен в L (и все расширения полей вычетов над $\mathcal{P}$ сепарабельны).

Из этой теоремы вытекает, что лишь конечное число простых идеалов разветвлено в L.

Доказательство. Пусть $\mathcal{P}$ - простой идеал A. Построим удобный для вычислений базис свободного $A_{\mathcal{P}}$-модуля $B' = (A \setminus \mathcal{P})^{-1}B$. По теореме 8.5 $B/\mathcal{P}B$ - n-мерное векторное пространство над $A/\mathcal{P}$. Имеем

$$\mathcal{P}B = \prod_{i=1}^{m} \mathcal{B}_i^{e_i}.$$

По китайской теореме об остатках существуют элементы $\Omega_{ij} \in B$, $i = 1, \ldots, m$, $j = 1, \ldots, f_i$, такие, что для данного i их классы вычетов образуют базис $B/\mathcal{B}_i$, а при $i' \neq i$ имеем $\Omega_{i'j} \in \mathcal{B}_i^{e_i}$. По той же теореме существуют $\pi_i \in B$, такие, что $\pi_i \in \mathcal{B}_i \setminus \mathcal{B}_i^2$ и $\pi_i \in B \setminus \mathcal{B}_{i'}$ при $i \neq i'$. Рассмотрим n элементов $\Omega_{ij}\pi_i^s$, $s = 0, \ldots, e_i - 1$. Их образы в $B/\mathcal{P}B$ линейно независимы и, значит, образуют базис этого векторного пространства над полем $A/\mathcal{P}$. По следствию 8.7.2 из леммы Накаямы сами эти элементы образуют базис $A_\mathcal{P}$-модуля B'.

Прежде того, как мы вычислим определитель, докажем, что для $x \in B'$ класс вычетов $Tr_{L/K}(x) \in A_\mathcal{P}$ по модулю $\mathcal{P}$ равен сумме $e_i Tr_{(B/\mathcal{B}_i)/(A/\mathcal{P})}$ от класса вычетов x по модулю $\mathcal{B}_i$. Пусть $f_x(t) \in A_\mathcal{P}$ - характеристический многочлен, $\overline{f_x}(t) \in A/\mathcal{P}$ - его редукция по модулю $\mathcal{P}$. Пусть, далее, $\phi_i(t) \in B/\mathcal{B}_i[t]$ - характеристический многочлен класса вычетов x по модулю $\mathcal{B}_i$. Расписывая умножение на x в нашем базисе, мы приходим к блочно-треугольной матрице. Вычисляя ее определитель, получим $\overline{f_x}(t) = \prod_{i=1}^m \phi_i(t)^{e_i}$, откуда и следует требуемое.

Закончим доказательство теоремы. Если $e_i > 1$ для некоторого i, то среди элементов нашего базиса есть хотя бы один элемент вида $\Omega_{ij}\pi_i^s$, $s \neq 0$, имеющий, как легко видеть, нулевой вычет по модулю всех $\mathcal{B}_j$, откуда $Tr_{L/K}$ от его произведения с любым другим элементом базиса равен 0 по модулю $\mathcal{P}$. Следовательно, дискриминант, как определитель соответствующей матрицы, также равен 0 по модулю $\mathcal{P}$. С другой стороны, если $\mathcal{P}$ неразветвлен, т.е. все $e_i = 1$ и все расширения полей вычетов сепарабельны, то все билинейные формы $Tr_{(B/\mathcal{B}_i)/(A/\mathcal{P})}(xy)$ невырождены, и определители их матриц Грама отличны от 0. Отсюда и из конструкции нашего базиса легко следует, что дискриминант не равен 0 по модулю $\mathcal{P}$.

9. Случай расширений Галуа

Теперь мы предположим, что L/K является расширением Галуа с группой Галуа $G = Gal(L/K)$. Напомним, что это означает, что группа автоморфизмов L над K имеет максимально возможное число элементов - $n = [L : K]$ (это и есть группа Галуа). Эквивалентным образом, если $x \in L$, то все корни характеристического многочлена x лежат в L. В частности,

$$Tr_{L/K}(x) = \sum_{\sigma \in G} \sigma(x), \quad N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x).$$

Предложение 9.1 На множестве простых идеалов $\mathcal{B}$ кольца целых поля L, лежащих над данным простым идеалом $\mathcal{P}$ кольца целых поля K, группа G действует транзитивно.

Доказательство. Пусть $\mathcal{B}|\mathcal{P}$, $\mathcal{B}'|\mathcal{P}$, но $\mathcal{B}$ и $\mathcal{B}'$ не лежат в одной орбите G. По китайской теореме об остатках найдется $x \in \mathcal{B}' \setminus \cup_{\sigma \in G}\mathcal{B}$. Тогда $N_{L/K}(x) \in \mathcal{B}'$, но $N_{L/K}(x) \notin \mathcal{B}$. Но это противоречит тому, что $\mathcal{B} \cap A = \mathcal{B}' \cap A = \mathcal{P}$.

Следствие 9.2 В расширении Галуа индексы ветвления и степени расширения полей частных не зависят от выбора $\mathcal{B}$ над $\mathcal{P}$ - они зависят лишь от $\mathcal{P}$. Обозначая эти числа $e_\mathcal{P}$ и $f_\mathcal{P}$, получаем соотношение

$$n = e_\mathcal{P} f_\mathcal{P} g_\mathcal{P},$$

где $g_\mathcal{P}$ - число простых идеалов над $\mathcal{P}$.

Группа разложения $\mathcal{B}|\mathcal{P}$ в расширении L/K - это подгруппа в G, определяемая как стационарная подгруппа $\mathcal{B}$:

$$D_\mathcal{B} := \{g \in G | g(\mathcal{B}) = \mathcal{B}\}.$$

Индекс $D_\mathcal{B}$ в G равен $g_\mathcal{P}$. Группа разложения $D_\mathcal{B}$, оставляя на месте идеал $\mathcal{B}$, действует автоморфизмами на его поле вычетов $k_\mathcal{B} = B/\mathcal{B}$, т.е. определен гомоморфизм

$$\epsilon : D_\mathcal{B} \to Gal(k_\mathcal{B}/k_\mathcal{P}),$$

где $k_\mathcal{P} = A/\mathcal{P}$. Его ядро $T_\mathcal{B} := Ker(\epsilon)$ называется *группой инерции*.

Предложение 9.3 Предположим, что $k_\mathcal{B}/k_\mathcal{P}$ - сепарабельное расширение. Тогда

(а) $k_{\mathcal{B}}/k_{\mathcal{P}}$ - расширение Галуа,
(б) гомоморфизм ϵ сюръективен.

Доказательство. (а) Требуется доказать, что минимальный многочлен любого элемента $x \in k_{\mathcal{B}}$ полностью разлагается на множители в $k_{\mathcal{B}}$. Пусть $a \in L$ - подъем x, тогда минимальный многочлен a над K полностью разлагается на множители в L. Его редукция по модулю $\mathcal{P}$ - многочлен над $k_{\mathcal{P}}$, корнем которого является x, и все корни которого лежат в $k_{\mathcal{B}}$. Значит, это же верно и для минимального многочлена x.

(б) В тех же обозначениях, пусть $x \in k_{\mathcal{B}}$- примитивный элемент. Его характеристический многочлен над $k_{\mathcal{P}}$ равен его минимальному многочлену. Он полностью распадается в поле $k_{\mathcal{B}}$ и имеет там $f_{\mathcal{P}}$ корней. Группа разложения $D_{\mathcal{B}}$ действует на множестве этих корней, и надо доказать, что это ее действие транзитивно. По китайской теореме об остатках подъем a элемента x можно выбрать так, чтобы $a \in s(\mathcal{B})$ для всех $s \in G \setminus D_{\mathcal{B}}$. Корнями характеристического многочлена $f_a(t)$ являются элементы вида $s(a)$, $s \in G$. Значит, ненулевыми корнями $\overline{f_a}(t) \in k_{\mathcal{P}}[t]$ являются в точности $s(x)$, $s \in D_{\mathcal{B}}$. Следовательно, все корни минимального многочлена x содержатся среди $s(x)$, $s \in D_{\mathcal{B}}$, откуда очевидным образом и следует транзитивность действия группы разложения на их множестве.

Следствие 9.4 Группа инерции тривиальна ($T_{\mathcal{B}} = 1$) тогда и только тогда, когда $\mathcal{P}$ неразветвлен.

Пусть все поля вычетов $k_{\mathcal{P}} = A/\mathcal{P}$ конечны. Если $k_{\mathcal{P}} = \mathbf{F}_q$, то $k_{\mathcal{B}} = \mathbf{F}_{q^f}$, где для краткости $f = f_{\mathcal{P}}$. Группа Галуа $Gal(k_{\mathcal{B}}/k_{\mathcal{P}})$ изоморфна $\mathbf{Z}/f$ с автоморфизмом Фробениуса $Fr_{\mathcal{B}}$ в качестве образующей. Предположим, что $\mathcal{P}$ неразветвлен в L. Тогда группа разложения $D_{\mathcal{B}} \subseteq G$ канонически отождествляется с $Gal(k_{\mathcal{B}}/k_{\mathcal{P}})$ посредством ϵ. Введем обозначение

$$(\mathcal{B}, L/K) = \epsilon^{-1}(Fr_{\mathcal{B}}).$$

Упражнение 9.5 Пусть E - подрасширение L/K, тогда $(\mathcal{B}, L/E) = (\mathcal{B}, L/K)^f$, где f - степень расширения полей вычетов (на уровне E над K). Если E/K - расширение Галуа, то при естественном эпиморфизме $Gal(L/K) \to Gal(E/K)$ символ $(\mathcal{B}, L/K)$ переходит в $(\mathcal{B}', E/K)$, где $\mathcal{B}'$ - пересечение $\mathcal{B}$ с кольцом целых E.

В общем случае $\mathcal{P}$ определяет только класс сопряженности в группе Галуа $G = Gal(L/K)$, состоящий из $(\mathcal{B}, L/K)$, $\mathcal{B}|\mathcal{P}$. Однако, если G абелева, то $(\mathcal{B}, L/K) \in G$ - корректно определенный элемент, зависящий только от $\mathcal{P}$. Обозначим его $(\mathcal{P}, L/K)$. (В общем случае так обозначается упомянутый выше класс сопряженности.) Он называется *символом Артина.* По мультипликативности определяется $(x, L/K)$ для $x \in K$, в разложение которого на простые идеалы не входят идеалы, ветвящиеся в L.

Одним из центральных результатов глобальной теории полей классов является

Закон взаимности Артина. Пусть $\mathcal{P}_1, \ldots, \mathcal{P}_r$ - все простые идеалы K, разветвленные в L. Существуют $n_i > 0$, такие, что если x сравним с 1 по модулю $\mathcal{P}_i^{n_i}$, $i = 1, \ldots, r$, и x положителен при всех вещественных вложениях $K \hookrightarrow \mathbf{R}$ (можно ограничиться теми из них, которые не получаются ограничением вложений $L \hookrightarrow \mathbf{R}$), то $(x, L/K) = 1$. Любой элемент G представляется в виде $(\mathcal{P}, L/K)$ для некоторого простого идеала $\mathcal{P}$.

Теорема плотности Чеботарева утверждает, что $g \in G$ представляется в виде $(\mathcal{P}, L/K)$ для множества простых идеалов, плотность которого равна отношению числа элементов в классе сопряженности g к мощности G.

Пример: случай кругового поля

Пусть $K = \mathbf{Q}$, $L = \mathbf{Q}(\zeta_m)$, где ζ_m - примитивный корень из 1 степени m. Это расширение Галуа с группой G, изоморфной $(\mathbf{Z}/m)^*$ (действие на корнях из 1). Пусть $\sigma(x)$ переводит ζ_m в ζ_m^x, $x \in (\mathbf{Z}/m)^*$ ("циклотомический характер"). Очевидно, что редукция кругового многочлена по модулю p не имеет кратных множителей, если $(p, m) = 1$. По следствию 8.9 такое p неразветвлено в $\mathbf{Q}(\zeta_m)$. Тогда символ Артина $(p, \mathbf{Q}(\zeta_m)/\mathbf{Q}) = \sigma(p)$, откуда по мультипликативности $(x, \mathbf{Q}(\zeta_m)/\mathbf{Q}) = \sigma(x)$. В частности, число простых идеалов $\mathbf{Q}(\zeta_m)$ над p равно $|(\mathbf{Z}/m)^*|$, поделенному на порядок p в группе $(\mathbf{Z}/m)^*$. Закон взаимности Артина выполнен очевидным образом: если x сравнимо с 1 по модулю

m, то $(x, \mathbf{Q}(\zeta_m)/\mathbf{Q}) = 1$. Бесконечность простых чисел такого вида следует из теоремы Дирихле о бесконечности простых в арифметической прогрессии.

10. Проконечные группы

10.1 Проективные пределы

Соглашения: топологические группы предполагаются хаусдорфовыми (или, что то же самое, отделимыми, - это означает, что любые две точки имеют непересекающиеся открытые окрестности). Конечные группы предполагаются наделенными дискретной топологией (все подмножества одновременно открыты и замкнуты).

Определение 10.1 *Направленное множество* - это частично упорядоченное множество I, такое, что для любых $x, y \in I$ существует $z \in I$, $z \geq x$, $z \geq y$. *Проективная система* топологических групп - это семейство групп $\{G_i | i \in I\}$ и непрерывных гомоморфизмов $\pi_{ij} : G_j \to G_i$ для $i \leq j$, причем $\pi_{ik} = \pi_{ij}\pi_{jk}$, если $i \leq j \leq k$. *Проективным пределом* проективной системы топологических групп $\{G_i | i \in I\}$ называется подгруппа в $\prod_{i \in I} G_i$, задаваемая условиями $\pi_{ij}(x_j) = x_i$. Топология на ней вводится так: $\prod_{i \in I} G_i$ наделяется топологией произведения (базу открытых множеств образуют подмножества вида $\prod_{i \in I} U_i$, где U_i открыто в G_i, и $U_i = G_i$ для почти всех i), тогда рассматриваемая подгруппа замкнута, и на ней вводится индуцированная топология. Проективный предел (также говорят - обратный) мы будем обозначать $lim.proj_{i \in I}(G_i)$. *Проконечной группой* называется проективный предел конечных групп. Проконечная группа называется *про-p-группой*, если все G_i - p-группы ($|G_i| = p^{n_i}$), где p - простое число.

Топологическое пространство называется *вполне несвязным*, если связная компонента любой точки состоит из самой этой точки.

Предложение 10.2 Проконечная группа компактна и вполне несвязна.

Доказательство. Теорема Тихонова утверждает, что прямое произведение компактов - компакт. Это применимо к $\prod_{i \in I} G_i$, а т.к. $lim.proj_{i \in I}(G_i)$ замкнуто в $\prod_{i \in I} G_i$, то это тоже компакт. Докажем, что $\prod_{i \in I} G_i$ вполне несвязно: для любого $x \neq 1$ построим окрестность 1 U, одновременно открытую и замкнутую, и такую, что $x \notin U$ (тогда 1 совпадает со своей связной компонентой, значит, то же верно для любой точки). Существует i, такое, что $x_i \neq 1$, тогда можно взять $U = \{1_i\} \times \prod_{j \in I, j \neq i} G_j$. Отсюда $lim.proj_{i \in I}(G_i)$ также вполне несвязно.

Упражнение 10.3 Пусть G - топологическая группа. Всякая открытая подгруппа замкнута. Факторпространство G/H (в фактортопологии) отделимо тогда и только тогда, когда H замкнута. Если H открыта, то G/H дискретно, а если при этом G компактна, то G/H конечно.

Верно также и утверждение, обратное к предложению 10.2. Любая проконечная группа представляется в виде $lim.proj(G/N)$, где N пробегает проективную систему всех открытых нормальных подгрупп G. (Идея доказательства: По предыдущему упражнению $lim.proj(G/N)$ - проконечная группа. Построим гомоморфизм $\theta : G \to lim.proj(G/N)$, $\theta(x) := \{xN\}$. Из того, что G вполне несвязна следует инъективность θ, а из компактности G - его сюръективность.)

Пусть G - произвольная группа. Если имеется проективная система ее нормальных подгрупп, упорядоченных по включению ($i \leq j$, если $N_j \subseteq N_i$), с естественными эпиморфизмами $G/N_j \to G/N_i$ в качестве π_{ij}, то можно рассмотреть соответствующий проективный предел $lim.proj(G/N_i)$. Рассмотрим гомоморфизм $\theta : G \to lim.proj(G/N_i)$, $\theta(x) := \{xN_i\}$. Пусть $G' = G/\bigcap_{i \in I} N_i$, тогда G' наделяется естественной хаусдорфовой топологией с $N_j/\bigcap_{i \in I} N_i$ в качестве базы открытых окрестностей 1. Гомоморфизм θ факторизуется через непрерывный инъективный гомоморфизм $G' \to lim.proj(G/N_i)$, образ которого плотен. Иными словами, $lim.proj(G/N_i)$ является пополнением G' в введенной нами топологии.

Основной пример: Пусть $\{N\}$ - все нормальные подгруппы G конечного индекса, тогда $lim.proj(G/N)$ называется *проконечным пополнением* G, оно обозначается $\hat{G}$. Например,

$$\hat{\mathbf{Z}} = lim.proj_{n \in \mathbf{N}}(\mathbf{Z}/n),$$

где натуральные числа $n \in \mathbf{N}$ частично упорядочены по делимости. Можно включать в нашу проективную систему только нормальные подгруппы, индекс которых есть степень простого числа p. Соответствующая про-p-группа обозначается $\hat{G}_p$. Пример: группа целых p-адических чисел

$$\mathbf{Z}_p = lim.proj(\mathbf{Z}/p^n).$$

Здесь направленное множество есть просто множество натуральных чисел с обычным порядком.

Стандартное определение $\mathbf{Z}_p$ состоит в том, что это есть пополнение $\mathbf{Z}$ по p-адической норме $|x|_p = p^{-val_p(x)}$. (Сначала рассматривается пополнение $\mathbf{Z}$ как метрического пространства, т.е. добавляются пределы последовательностей Коши, затем сложение и умножение определяются по непрерывности.) Топология, задаваемая этой нормой, очевидно совпадает с топологией, в которой базу окрестностей 0 образуют подгруппы $\mathbf{Z}/p^n$. Поле p-адических чисел $\mathbf{Q}_p$ вводится либо как поле частных $\mathbf{Z}_p$, либо как пополнение $\mathbf{Q}$ по p-адической норме. Заметим, что $\mathbf{Q}_p$ уже не компактно.

Если $\mathcal{P}$ - простой идеал дедекиндова кольца A, то пополнение A в $\mathcal{P}$ определяется как $lim.proj(A/\mathcal{P}^n)$, либо, что то же самое, как пополнение A в топологии, задаваемой степенями $\mathcal{P}$. Поле частных этого кольца будет пополнением поля частных A относительно этой топологии.

Упражнение 10.4 Имеется канонический непрерывный изоморфизм

$$\hat{\mathbf{Z}} = \prod_p \mathbf{Z}_p.$$

(Указание: конечная циклическая группа канонически разлагается в произведение циклических p-групп.)

10.2 Группа Галуа бесконечного алгебраического расширения как проконечная группа

Напомним следующий фундаментальный результат:

Основная теорема теории Галуа (для конечных сепарабельных расширений). Пусть L/K - конечное расширение Галуа с группой Галуа $G = Gal(L/K)$. Тогда имеется биекция между подгруппами $H \subseteq G$ и подрасширениями $K \subseteq M \subseteq L$, причем H соответствует подполе инвариантов $M = L^H$, а подполю M - подгруппа G, сотоящая из автоморфизмов L над M. Эти отображения являются взаимно-обратными. При этом нормальным подгруппам отвечают подрасширения Галуа, в этом случае $Gal(M/K) = G/Gal(L/M)$.

Понятно, что пересечению подгрупп соответствует композит расширений.

Как обобщить это на бесконечные расширения?

Определение 10.5 Расширение K/L (возможно, бесконечное) называется расширением Галуа, если оно алгебраично, т.е. каждый элемент является корнем многочлена с коэффициентами из K, и множество неподвижных точек группы автоморфизмов L над K есть само K. Эту группу будем называть группой Галуа и обозначать $Gal(L/K)$.

Предложение 10.6 Пусть L/K - расширение Галуа. Группы Галуа $Gal(M/K)$ его *конечных* подрасширений Галуа, $[M : K] < \infty$, образуют проективную систему, проективный предел которой есть вся группа Галуа

$$Gal(L/K) = lim.proj(Gal(M/K)).$$

Доказательство. Канонические эпиморфизмы $Gal(L/K) \to Gal(M/K)$ задают непрерывный гомоморфизм $\chi : Gal(L/K) \to lim.proj(Gal(M/K))$. Неединичный элемент $Gal(L/K)$ нетривиально действует на некотором $x \in L$. Он содержится в конечном подрасширении (т.к. алгебраичен), откуда инъективность χ. Наоборот, любой элемент из $lim.proj(Gal(M/K))$ есть согласованная система автоморфизмов конечных подрасширений, что эквивалентно заданию автоморфизма из $Gal(L/K)$, т.е. χ сюръективен.

Таким образом, на группе Галуа бесконечного расширения Галуа вводится топология, в которой она является проконечной группой. Теперь можно сформулировать обобщение основной теоремы теории Галуа: оно аналогично конечному случаю, рассматриваются произвольные расширения, но только *замкнутые* подгруппы. (Убедимся, что $Gal(L/M)$ замкнута. Имеем $Gal(L/M) = \cap Gal(L/M')$, где $K \subseteq M' \subseteq M$ и $[M' : K] < \infty$. Поэтому достаточно доказать, что $Gal(L/M')$ замкнута. Если M'' - наименьшее расширение Галуа, содержащее M', то M''/K конечно, $Gal(L/M'')$ открыта, а, значит, $Gal(L/M')$ открыта как объединение смежных классов по $Gal(L/M'')$. Поэтому она также и замкнута.)

Основной пример бесконечного расширения Галуа доставляет сепарабельное замыкание K^s основного поля K. Понятно, что в случае характеристики 0, а также всегда, когда поле K не имеет несепарабельных расширений - такие поля называются *совершенными* - сепарабельное замыкание совпадает с алгебраическим замыканием (последнее обозначается $\overline{K}$). Группа $Gal(K^s/K)$ иногда называется *абсолютной группой Галуа* поля K. Пример: для любого n конечное поле $\mathbf{F}_q$ из q элементов имеет единственное (с точностью до изоморфизма) расширение степени n - поле $\mathbf{F}_{q^n}$, это расширение сепарабельно, поэтому

$$Gal(\overline{\mathbf{F}_q}/\mathbf{F}_q) = \hat{\mathbf{Z}}.$$

Важно отметить, что при этом изоморфизме $1 \in \mathbf{Z} \subset \hat{\mathbf{Z}}$ ("топологическая образующая") переходит в автоморфизм Фробениуса $Fr_q : x \mapsto x^q$.

10.3 Когомологии проконечных групп

Пусть G - проконечная группа. Мы будем рассматривать только *дискретные* G-модули A, т.е. такие, что отображение $G \times A \to A$, задаваемое действием G на A, непрерывно, если A рассматривается в дискретной топологии.

Упражнение 10.7 Доказать, что G-модуль A дискретен тогда и только тогда, когда выполнены следующие эквивалентные условия:

(а) стационарная подгруппа любого элемента A открыта,

(б) $A = \cup_U A^U$, где U пробегает все открытые нормальные подгруппы G, $A^U := \{a \in A | ga = a \textit{ для всех } g \in U\}$.

Группы когомологий $H^n(G, A)$ можно определить как когомологии комплекса, на n-м месте которого стоит группа $Cont(G^n, A)$ непрерывных функций на G^n со значениями в A, а дифференциал $d : Cont(G^n, A) \to Cont(G^{n+1}, A)$ устроен обычным образом:

$$df(g_1, \ldots, g_{n+1}) = g_1 f(g_2, \ldots, g_{n+1}) + \sum_{j=1}^{i} (-1)^j f(g_1, \ldots, g_j g_{j+1}, \ldots, g_{n+1}) + (-1)^{i+1} f(g_1, \ldots, g_n).$$

(В частном случае конечных групп это дает обычное определение.)

Из формулы для d следует, что $H^1(G, A)$ состоит из 1-коциклов - "скрещенных гомоморфизмов" - непрерывных функций $f : G \to A$, таких, что

$$gf(g') = f(gg') - f(g),$$

рассматриваемых с точностью до кограниц, т.е. функций вида $f(g) = ga - a$ для некоторого $a \in A$. Понятно, что если G тривиально действует на A, то $H^1(G, A)$ есть группа непрерывных гомоморфизмов из G в A.

Далее, 2-коцикл - "система факторов" - есть непрерывная функция $f : G \times G \to A$, такая, что

$$gf(g', g'') = f(gg', g'') - f(g, g'g'') + f(g, g').$$

Как связаны когомологии проконечной группы G и когомологии конечных групп, проективным пределом которых она является? Напомним, что $G = lim.proj(G/U)$, где $\{G/U\}$ пробегает проективную систему всех конечных факторгрупп G. Группа G/U действует на A^U, рассмотрим группу когомологий $H^n(G/U, A^U)$. Если $U' \subset U$, то подъем функций с G/U на G/U' дает отображение $H^n(G/U, A^U) \to H^n(G/U', A^U)$, которое можно скомпоновать с естественным вложением G/U'-модулей $A^U \hookrightarrow A^{U'}$. Для каждой пары открытых нормальных подгрупп $U' \subset U$ получаем гомоморфизм

$$\lambda_{U,U'} : H^n(G/U, A^U) \to H^n(G/U', A^{U'}).$$

Группу $H^n(G,A)$ можно определить как "индуктивный предел", т.е. как множество классов эквивалентности на непересекающемся объединении групп $H^n(G/U, A^U)$, так, что $x_1 \in H^n(G/U_1, A^{U_1})$ эквивалентно $x_2 \in H^n(G/U_2, A^{U_2})$ если $\lambda_{U_1, U_1\cap U_2}(x_1) = \lambda_{U_2, U_1\cap U_2}(x_2)$. (Набросок доказательства см. в Касселс-Фрелих, гл. V, 2.4)

Пример: когомологии Галуа

Рассмотрим частный случай, когда A есть сепарабельное замыкание K_s некоторого поля K, $G = Gal(K_s/K)$.

Предложение 10.8 Для всех $n > 0$ имеем $H^n(G, K_s) = 0$.

Доказательство. Достаточно доказать утверждение на конечном уровне. Из теоремы о нормальном базисе следует, что представление $Gal(L/K)$ в L индуцировано с тривиального, откуда наше утверждение следует по лемме Шапиро.

Пусть теперь $A = K_s^*$. Тривиальность $H^1(G, K_s^*)$ - это знаменитая "теорема Гильберта 90" (ее доказательство написано во многих местах, см., например, Касселс-Фрелих, гл. V, 2.6). Группа $H^2(G, K_s^2)$ называется группой Брауэра, ее содержательная интерпретация будет дана в следующем параграфе.

11. Группа Брауэра

Соглашение: все алгебры предполагаются ассоциативными и с единицей (но не обязательно коммутативными). Через $M_n(R)$ будем обозначать алгебру матриц порядка n на кольцом R.

Зафиксируем поле k.

Определение 11.1 Алгебра A над k называется *центральной*, если ее центр совпадает с k; A называется *простой*, если A не имеет нетривиальных двусторонних идеалов. *Обратная* к A алгебра A° изоморфна A как векторное пространство, а произведение в A° элементов x и y определяется как yx (понимаемое как произведение в A).

Предложение 11.2 (a) Тензорное (над k) произведение центральных простых алгебр - центральная простая алгебра. (Ван дер Варден "Алгебра", 103)

(b) Пусть $d = dim_k(A)$, тогда $A \otimes_k A^\circ = M_d(k)$. (Рассмотреть действие $A \otimes_k A^\circ$ на A, при котором A действует умножениями слева, а A° - умножениями на элементы A справа. Так получаются все эндоморфизмы A как k-векторного пространства - использовать центральность A.)

Две центральные простые алгебры A и A' называются *эквивалентными*, если алгебры $A \otimes_k M_n(k)$ и $A' \otimes_k M_{n'}(k)$ изоморфны для некоторых n и n'. Из предыдущего предложения следует, что классы эквивалентности центральных простых алгебр образуют абелеву группу, называемую *группой Брауэра* поля k. Обозначение: $\mathrm{Br}(k)$.

Приведем для полноты краткое резюме структурной теории полупростых алгебр. Рассмотрим ассоциативное кольцо с единицей. Радикалом кольца называется объединение всех его нильпотентных идеалов. Радикал Джекобсона определяется как пересечение всех максимальных левых идеалов, или эквивалентным образом, как пересечение всех двусторонних идеалов (Ван дер Варден, 96). Если наше кольцо - k-алгебра, то оба радикала совпадают (Ван дер Варден, 98). Алгебра без радикала называется полупростой. Такая алгебра представляется в виде прямой суммы конечного числа своих минимальных левых идеалов. (Радикал можно представить как несократимое пересечение конечного числа максимальных левых идеалов A_i. Тогда вся алгебра есть прямая сумма своих левых идеалов $B_i = \cap_{i\neq j} A_j$. При этом A/A_i изоморфно B_i, откуда B_i прост как A-модуль, т.е. является минимальным идеалом. Ван дер Варден, 98) Очевидно, что если M - простой A-модуль, то $End_A(M)$ есть тело (алгебра, являющаяся телом, называется алгеброй с делением), а если M' - простой A-модуль, не изоморфный M, то $Hom_A(M, M') = 0$. Поскольку $End_A(A) = A$ (эндоморфизм A как левого модуля над собой определяется заданием образа единичного элемента - при этом A отождествляется с кольцом правых эндоморфизмов левого A-модуля A), то получаем следующую структурную теорему: каждая полупростая алгебра есть прямая сумма матричных алгебр над телами (теорема Веддерберна, см. Ван дер Варден, 102). При этом, если A - проста, то все B_i изоморфны. Более того, все вообще простые A-модули изоморфны (если M - простой модуль, то $B_i M$ либо нуль, либо M).

Заметим, что из отсутствия некоммутативных конечных тел (другая теорема Веддерберна) вытекает тривиальность группы Брауэра конечного поля.

Упражнение 11.3 Пусть K/k - конечное расширение. Доказать, что $K \otimes_k L$ не содержит нильпотентов (т.е. является полупростой алгеброй) ни для какого расширения L/k тогда и только тогда, когда K/k сепарабельно. Доказать, что $K \otimes_k L$ - простая k-алгебра, т.е. поле, тогда и только тогда, когда $L \cap K = k$.

Предложение 11.4 Тензорное произведение двух простых алгебр над k будет простой алгеброй над k тогда и только тогда, когда произведение их центров - поле (например, если одна из алгебр центральна). (Ван дер Варден, 103)

В частности, если A - центральная простая k-алгебра, и K/k - расширение поля, то $A \otimes_k K$ - центральная простая K-алгебра. Следовательно, имеется гомоморфизм $\mathrm{Br}(k) \to \mathrm{Br}(K)$, ядро которого будем обозначать $\mathrm{Br}(k, K)$. Об элементах из $\mathrm{Br}(k, K)$ говорят, что они *распадаются над* K, а о K - что оно является *полем разложения* такого элемента.

Предложение 11.5 Любая центральная простая k-алгебра A распадается над конечным расширением k. Тем самым, $\mathrm{Br}(K) = \cup_K \mathrm{Br}(k, K)$, где K пробегает все конечные расширения k.

Доказательство. Достаточно рассмотреть случай тел. Каждый элемент не из центра порождает подполе, над которым наше тело приобретает делители нуля (11.3), т.е. становится алгеброй матриц над новым телом, имеющим меньшую размерность над своим центром. Повторяя несколько раз, и беря композит расширений, мы полностью расщепим A.

Следствие 11.6 Размерность алгебры с делением над ее центром является квадратом натурального числа. Оно называется *индексом*.

Теорема 11.7 (Сколем-Нетер) Любой k-изоморфизм между двумя изоморфными простыми k-подалгебрами центральной простой k-алгебры A получается из внутреннего автоморфизма A.

Доказательство: Пусть B - простая алгебра, абстрактно изоморфная двум упомянутым подалгебрам, D - алгебра с делением, такая что $A = M_n(D)$. Рассмотрим два представления (простой!) алгебры $B \otimes_k D^\circ$ на D^n, такие что B действует слева, а D - справа. Поскольку все представления простой алгебры одной размерности эквивалентны, то и два построенных представления получаются друг из друга сопряжением на матрицу из $M_n(D)$, откуда и сопряженность исходных подалгебр.

Пусть, по-прежнему, B - простая алгебра, D - алгебра с делением, причем одна из них центральна. Согласно 11.4, $X = B \otimes_k D^\circ = M_n(E)$ - простая, т.е. имеет единственный простой модуль $M = E^n$ (E - тело). Из того, что $E^\circ = End_X(M)$ (действие, реализованное умножениями справа) - доказать! - следует, что E есть централизатор образа B в X.

Отсюда также легко вывести, что максимальные подполя алгебры с делением имеют степень, равную индексу, и являются полями разложения для данной алгебры. (Ван дер Варден, 112). Действительно, если в качестве B взять максимальное подполе центральной алгебры с делением D, то $E = B$, т.к. централизатор B в K есть само B.

Доказывается, что всегда существует сепарабельное поле разложения (Ван дер Варден, 113). Любое поле разложения алгебры с делением D можно представить как максимальное подполе $M_r(D)$. (там же)

Теорема 11.8 Группа Брауэра $\mathrm{Br}(k)$ канонически изоморфна $H^2(k, k_s^*)$, где k_s^* - сепарабельное замыкание поля k.

Доказательство. Пусть $A \in \mathrm{Br}(k)$, K/k - конечное расширение Галуа с группой G, расщепляющее A. Построим по A коцикл в $H^2(G, K^*)$. Пусть A - тело, и K - максимальное подполе в $M_r(A)$. По теореме Сколема-Нетер действие группы Галуа на K происходит из сопряжения на некоторый элемент $M_r(A)$, пусть при этом элемент $g \in G$ переходит в u_g. Тогда $c_{g,h} = u_{gh}^{-1} u_g u_h$ лежит в централизаторе K, т.е.

в самом K, т.к. это максимальное подполе. Это и есть искомый коцикл. Обратная конструкция: на векторном пространстве $K[G]$ с естественным действием G на K введем умножение по правилу $u_g u_h = u_{gh} c_{g,h}$, где $c_{g,h} \neq 0$. Требование того, чтобы получающаяся алгебра была ассоциативна эквивалентно условию коцикла:

$$c_{g,hl} c_{h,l} = c_{gh,l} l(c_{g,h}).$$

При замене базиса $u'_g = u_g f_g$ соответствующий коцикл меняется на кограницу. Мы опускаем доказательство того, что построенная биекция - изоморфизм групп.

12. Неразветвленные расширения локальных полей

Под *локальными* полями мы будем понимать поля K, снабженные дискретным нормированием (сюръективным гомоморфизмом $v : K^* \to \mathbf{Z}$, удовлетворяющим ультраметрическому неравенству), которые полны в задаваемой этим нормированием топологии (норма x равна $a^{v(x)}$, где $0 < a < 1$). Множество $O_v = \{x \in K^*, v(x) \geq 0\} \cup \{0\}$ образует *кольцо нормирования* v, являющееся кольцом дискретного нормирования, а $m_v = \{x \in K^*, v(x) > 0\} \cup \{0\}$ - его максимальный идеал, называемый *идеалом нормирования*. Факторкольцо $k = O_v/m_v$ называется *полем вычетов*. Мы будем предполагать, что k конечно. В случае характеристики 0 примерами локальных полей являются p-адические числа - пополнение $\mathbf{Q}$ в топологии, задаваемой p-адической нормой $p^{-val_p(x)}$, и более общо, пополнения полей алгебраических чисел относительно топологий, задаваемых нормированиями, связанными с простыми идеалами их колец целых. В случае конечной характеристики аналогичную роль играют поля формальных степенных рядов $\mathbf{F}_q((t))$.

Предложение 12.1 Пусть K'/K - конечное расширение локального поля K. Рассмотрим целое замыкание B кольца O_v в K'. Тогда B - кольцо дискретного нормирования, и поле K' полно в топологии, задаваемой его максимальным идеалом.

Доказательство. Согласно общей теории дедекиндовых колец (теорема Крулля, 8.2) B - дедекиндово, и $m_v B$ разлагается в произведение степеней простых идеалов B. Докажем, что B имеет только один простой идеал. Каждый такой идеал задает норму на K', согласованную со структурой K' как векторного пространства над K, т.е. наделяющую K' структурой нормированного векторного пространства. Так как K полно, то все нормы на K' эквивалентны (Касселс-Фрелих, гл.2 лемма 8.1). Таким образом, все эти нормы задают одну и ту же топологию. Поскольку кольцо нормирования восстанавливается по топологии как множество тех x из K^*, для которых последовательность x^{-n} не стремится к нулю, то отсюда и следует требуемое.

Согласно доказанному, существует ровно одно продолжение нормирования v с K на K', обозначим его w. Его можно явно задать, положив $w(x) = v(N_{K'/K}(x))$. Кольцо B является его кольцом нормирования, $B = O_w$. Как и в общем случае дедекиндовых колец, $m_v O_w = (m_w)^e$ для некоторого e, называемому индексом ветвления. Если $e = 1$, то расширение называется неразветвленным. Так же как и раньше $n = ef$, где f - степень расширения полей вычетов (8.3).

Теорема 12.2 Неразветвленные расширения K' локального поля K взаимно-однозначно задаются своими расширениями поля вычетов k. Имеется эквивалентность категорий, т.е. $Hom_K(K', K'') = Hom_k(k', k'')$. (В этой формуле можно считать, что K'' - произвольное конечное расширение K.)

Доказательство. Для построения расширения K'/K, отвечающего данному расширению (сепарабельному) k'/k надо взять примитивный элемент k', его минимальный многочлен над k, поднять его до многочлена над K, скажем, $f(x)$, и рассмотреть $K' = K[t]/(f(x))$. Тогда, по (8.8, 8.9), K'/K неразветвлено и имеет k' своим полем вычетов. Пусть $\sigma \in Hom_K(K', K'')$, тогда ограничения нормирований $v''(\pi_{v'})v'(x)$ и $v''(\sigma(x))$ поля K' на K совпадают. По 12.1 совпадают сами эти нормирования. Отсюда $\sigma(O_{v'}) \subseteq O_{v''}$ и то же верно для максимальных идеалов этих колец. Переходя к факторам получим гомоморфизм полей вычетов. Пусть, наоборот, имеется гомоморфизм полей вычетов. По лемме Гензеля (Серр, "Курс арифметики", гл. 2, Касселс-Фрелих, гл. 2 добавление В) существует единственный подъем $y \in K'$ образа примитивного элемента k'/k, такой что $f(y) = 0$. Тогда существует единственный гомоморфизм K' в K'', переводящий x в y. Это показывает. что все расширения K с данным расширением поля вычетов изоморфны.

Следствие 12.3 (a) Неразветвленное расширение K' локального поля K является расширением Галуа тогда и только тогда, когда таково k'/k, при этом группы Галуа изоморфны.

(b) Все неразветвленные подрасширения данного конечного расширения K'/K содержатся в одном из них (называемом максимальным неразветвленным подрасширением), его поле вычетов есть k'.

(c) Композит неразветвленных расширений снова неразветвлен.

(d) Все неразветвленные расширения K содержатся в максимальном неразветвленном расширении K_{nr}, оно является расширением Галуа с группой Галуа, изоморфной $\hat{\mathbf{Z}}$.

13. Группа Брауэра локального поля

Теорема 13.1 Любая центральная простая алгебра над локальным полем распадается над некоторым конечным неразветвленным расширением этого поля. Следовательно, $\mathrm{Br}(K) = H^2(\hat{\mathbf{Z}}, K^*_{nr})$.

Прежде, чем приступать к доказательству, изложим конструкцию и некоторые свойства *редуцированной нормы* центральной простой алгебры.

Предложение 13.2 Пусть A - ц.п.а. над полем k, $dim_k(A) = n^2$, тогда существует полиномиальная функция $Nrd : A^* \to k^*$ степени n, такая что для любого расщепляющего расширения L/k, т.е. такого, что $A \otimes_k L = M_n(L)$, имеем $det(a \otimes 1) = Nrd(a)$, $a \in A$. (В частности, редуцированная норма - гомоморфизм.)

Доказательство (набросок): Независимость от выбора неприводимого представления следует из теоремы Сколема-Нетер. Предположим, что L/k - расширение Галуа с группой G (иначе перейдем к наименьшему расширению Галуа, содержащему L). Инвариантность коэффициентов в некотором базисе A относительно G получается так: "скрутим" представление элементом группы Галуа (т.е. подействуем на все матричные элементы) и применим еще раз тот же аргумент.

Упражнение 13.3 (а) Определитель образа $a \in A$ при регулярном представлении A (на себе) есть $Nrd(a)^n$.

(б) Ограничение Nrd на максимальное подполе K совпадает с нормой из K в k.

Теперь применим это к случаю ц.п.а. с делением D над локальным полем K (мы сохраняем обозначения предыдущего пункта). Поскольку все нормы на конечномерном векторном пространстве над полным полем эквивалентны, существует не более одного продолжения v на D - как гомоморфизма w на бесконечную циклическую группу, удовлетворяющего ультраметрическому неравенству. Построим его так: $w(a) = v(Nrd(a))$.

Упражнение 13.4 Доказать ультраметрическое неравенство (опираясь на 13.3 (б)).

Доказательство теоремы 13.1. Пусть $O_D = \{a \in D, w(a) \geq 0\}$. Тогда это - кольцо, а $m_D = \{a \in D, w(a) > 0\}$ - его максимальный идеал. Как и в коммутативном случае, O_D изоморфно $O_v^{n^2}$ как O_v-модуль, и $dim_k(O_D/m_v O_D) = n^2 = ef$, где e - индекс ветвления, а $f = dim_k(O_D/m_D)$. Отметим, что конечное тело O_D/m_D есть на самом деле поле. По лемме Гензеля можно поднять его примитивный элемент в D, где он будет порождать неразветвленное подполе степени f. Отсюда $f \leq n$. Напомним, что максимальные подполя суть в точности подполя степени n. Легко видеть, что подполе D, порожденное элементом m_D, на котором достигается $inf(w(x))$, имеет степень $e \leq n$. Отсюда $e = f = n$ и теорема 13.1 доказана, т.к. мы построили максимальное подполе, являющееся неразветвленным расширением.

Теорема 13.5 (а) Нормирование $v : K_{nr} \to \mathbf{Z}$ индуцирует изоморфизм групп когомологий

$$H^2(\hat{\mathbf{Z}}, K^*_{nr}) = H^2(\hat{\mathbf{Z}}, \mathbf{Z}).$$

(б) Последняя группа естественно изоморфна

$$H^1(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) = Hom(\hat{\mathbf{Z}}, \mathbf{Q}/\mathbf{Z}) = \mathbf{Q}/\mathbf{Z}.$$

Доказательство. (а) Достаточно доказать, что нормирование $v : K_n \to \mathbf{Z}$, где K_n - неразветвленноу расширение степени n с группой Галуа $\mathbf{Z}/n$, индуцирует изоморфизм

$$H^2(\mathbf{Z}/n, K^*_n) = H^2(\mathbf{Z}/n, \mathbf{Z}).$$

Имеется точная последовательность

$$1 \to U_n \to K_n^* \to \mathbf{Z} \to 0,$$

где $U_n = O_n^*$ - группа единиц (обратимых элементов) кольца целых O_n поля K_n. Из длинной точной последовательности когомологий (см. гл. 1 второй части) видно, что достаточно доказать, что $H^i(\mathbf{Z}/n, U_n) = 0$. На группе единиц существует естественная фильтрация подгруппами вида $U_n^m = 1 + \pi^m O_n$, где π - образующая максимального идеала кольца целых $O \subset K$. При этом первый градуированный фактор есть k_n^*, где k_n - поле вычетов K_n - есть расширение степени n поля k, а остальные изоморфны k_n. Мы уже видели в гл. 11.3, что аддитивная группа поля имеет тривиальные когомологии. Мультипликативная группа не имеет первых когомологий - это теорема Гильберта 90. Теперь воспользуемся тем, что k - конечное поле, и, значит, имеет тривиальную группу Брауэра, т.е. вторая группа когомологий также равна нулю. Из периодичности когомологий циклической группы (гл. 1.5 второй части) получаем $H^i(\mathbf{Z}/n, k_n^*) = 0$ для $i > 0$. Остается перейти от когомологий градуированных факторов к когомологиям самой группы U_n. Это делается по индукции, с учетом того, что $U_n = lim.proj(U_n/U_n^m)$ (надо последовательно представлять нашу коцепь как кограницу с точностью до следующего члена фильтрации и т.д., подробности см. в Касселс-Фрелих, гл. VI, лемма 1.3).

(б) Следует из длинной точной последовательности когомологий, связанной с короткой точной последовательностью

$$0 \to \mathbf{Z} \to \mathbf{Q} \to \mathbf{Q}/\mathbf{Z} \to 0,$$

и того, что $\mathbf{Q}$, будучи бесконечно делимым, представляет собой когомологически тривиальный модуль (см. гл.1 второй части). Наконец, последний изоморфизм задается значением характера на топологической образующей $\hat{\mathbf{Z}}$ - автоморфизме Фробениуса.