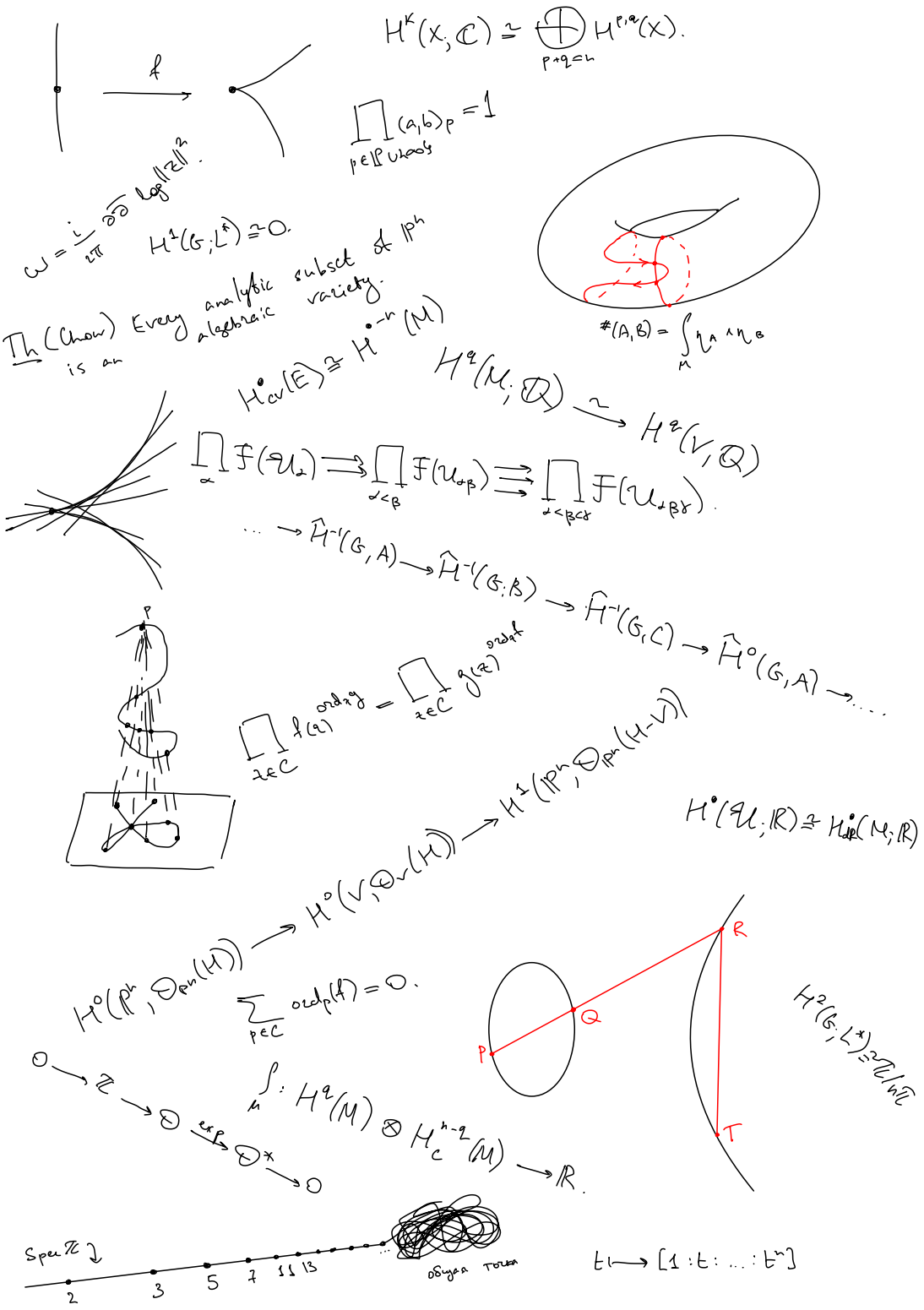
Компендиум по алгебраической геометрии



Предисловие

> По существу бывает только две специальности, на которые нужно учится действительно дого: хирург и алгебраический геометр.
>
> Ф.В. Петров

Данный файл представляет из себя мою записную книжку в изучении комплексной и арифметической геометрии. Так как алгебраическая геометрия — весьма большая наука, здесь записано весьма большое количество пререквизитов (как геометро-топологических, которые необходимы в комплексной геометрии, так и теоретико-числовых, необходимых в диофантовой геометрии).

Так как это по сути личная записная книжка, здесь наверняка крайне много опечаток (и с этим, увы, невозможно побороться). Да и относится серьезно к этому всему тоже не стоит.

Оглавление

1 Алгебраическая топология **7**

1. Сингулярные гомологии . . . 7
   - 1.1 Симплициальные гомологии . . . 7
   - 1.2 Сигнулярные гомологии . . . 9
   - 1.3 Немного гомологической алгеры . . . 10
   - 1.4 Гомотопическая инвариантность гомологий . . . 12
   - 1.5 Относительные гомологии и гомологически точная последовательность пары . . . 13
   - 1.6 Пары Боруска . . . 15
   - 1.7 Относительные гомологии как абсолютные (факторизация) . . . 16
   - 1.8 Вырезание . . . 19
   - 1.9 Точная последовательность Майера-Вьеториса . . . 20
   - 1.10 Гомологии сфер . . . 20
   - 1.11 Гомологии букета и надстройки . . . 21
   - 1.12 Гомологии с коэффициентами . . . 22
   - 1.13 Приложения теории гомологий . . . 22
   - 1.14 Симплициальные комплексы . . . 23
   - 1.15 Эквивалентность симплициальных и сингулярных гомологий . . . 23
   - 1.16 Степень отображения . . . 24
   - 1.17 Клеточные гомологии . . . 26
   - 1.18 Гомологии поверхностей . . . 29
   - 1.19 Пространства Мура . . . 30
   - 1.20 Теорема о вложении дисков и сфер . . . 30
   - 1.21 Когомологии . . . 31
   - 1.22 Формула универсальных коэффициентов для когомологий . . . 32
   - 1.23 Умножение в когомологиях . . . 34
2. Когомологии де Рама . . . 35
   - 2.1 Дифференциальные формы . . . 35
   - 2.2 Когомологии де Рама и компактные когомологии . . . 40
   - 2.3 Дифференциальные формы на многообразиях . . . 41
   - 2.4 Точная последовательность Майера-Виеториса . . . 42
   - 2.5 Лемма Пуанкаре для когомологий де Рама . . . 45
   - 2.6 Когомологии сферы . . . 48
   - 2.7 Лемма Пуанкаре для компактных когомологий . . . 49
   - 2.8 Умножение в когомологиях де Рама . . . 49
   - 2.9 Аргумент Майера-Виеториса . . . 50
   - 2.10 Двойственность Пуанкаре . . . 51
   - 2.11 Формула Кюннета . . . 53
   - 2.12 Двойственный по Пуанкаре к замкнутому подмногообразию . . . 55
   - 2.13 Напоминание про векторные расслоения и класс Тома . . . 56
   - 2.14 Обобщенный принцип Майера-Виеториса и комплекс Чеха-де Рама . . . 60
   - 2.15 Предпучки и когомологии Чеха . . . 66
   - 2.16 Глобальная угловая форма, класс Эйлера, класс Тома . . . 69

2 Аффинная алгебраическая геометрия 73
1. Коммутативная алгебра с прицелом на алгебраическую геометрию . . . 73
1.1 Предварительные сведения и напоминания . . . 73
1.2 Аффинные алгебраиические многообразия . . . 74
1.3 Топология Зарисского на спектре кольца . . . 75
1.4 Словарик алгебраической геометрии . . . 75
1.5 Локализация. Поведение спектра при локализации. . . . 75
1.6 Локализация модуля и плоские модули. Локальный принцип. . . . 77
1.7 Лемма Накаямы . . . 79
1.8 Радикал Джекобсона . . . 80
1.9 Кольца нормирования, кольца дискретного нормирования и Дедекиндовы области . 80
1.10 Дедекиндовы кольца . . . 82
1.11 Hauptidealsatz . . . 83
1.12 Пополнения . . . 83
1.13 Градуированные алгебры и модули . . . 85
2. Аффинные многообразия . . . 86
2.1 Введение. Аффинные алгебраические многообразия. Идеалы, неприводимые многообразия. . . . 86
2.2 Разложение в неприводимые компоненты . . . 88
2.3 Размерность аффинного многообразия . . . 90
2.4 Регулярные функции . . . 92
2.5 Морфизмы алгебраических многообразий . . . 94
2.6 Антиэкивалентность $\mathsf{qAff}^{op} \cong \mathbb{k}\text{-}\mathsf{Alg}$ . . . 95
2.7 Рациональные функции . . . 96
2.8 Главные аффинные окрестности . . . 96
2.9 Эквивалентные определения размерности неприводимого аффинного многообразия 98
2.10 Прямое произведение многообразий и его первые приложения . . . 98
2.11 Размерность редуцированного кольца, в котором каждый необратимый элемент является делителем нуля . . . 100
3. Проективные многообразия . . . 102
3.1 Проективные многообразия . . . 102
3.2 Проективное замыкание аффинного многообразия . . . 105
3.3 Рациональные отображения многообразий . . . 107
3.4 Бирациональная эквивалентность . . . 109
3.5 Рациональные многообразия . . . 110
3.6 Локальное кольцо в точке . . . 111
3.7 Касательное пространство . . . 114
3.8 Разложение в ряд Тейлора . . . 116
3.9 Локальное кольцо точки на неособой кривой. Индексы ветвления и степень инерции. 118
3.10 Конечные морфизмы и нормализация многообразия . . . 120
4. Дивизоры . . . 123
4.1 Дивизоры Вейля . . . 123
4.2 Дивизоры форм . . . 126
4.3 Групповой закон для точек эллиптической кривой . . . 128
5. Комплексная алгебраическая геометрия . . . 130
5.1 Комплексные многообразия . . . 130
5.2 Векторные рассоления . . . 132
5.3 Подмногообразия и аналитические подмножества . . . 134
5.4 Когомологии де Рама и Дольбо . . . 135
5.5 Пучки и когомологии . . . 137
5.6 Дивизоры и линейные расслоения . . . 137

3 Арифметическая и диофантова геометрия **139**
1. Алгебраическая теория чисел, часть I . . . 139
1.1 Алгебраические числа и целые алгебраические числа . . . 139
1.2 След элемента и целый базис кольца $\mathcal{O}_K$ . . . 140
1.3 Размерность кольца целых $\mathcal{O}_K$ . . . 143
1.4 Примеры евклидовых колец целых алгебраических чисел . . . 143
1.5 “Last Fermat’s theorem” для $n = 3$. . . . 144
1.6 Целозамкнутость кольца $\mathcal{O}_K$ . . . 148
1.7 Кольцо целых алгебраических чисел для квадратичного расщирения . . . 149
1.8 Разложение идеалов в произведение простых в кольцах целых числовых полей . . . 149
1.9 Дискриминант . . . 152
1.10 Норма идеала . . . 157
1.11 Индекс ветвления и степень инерции . . . 158
1.12 Группа классов идеалов и её элементарное вычисление . . . 161
1.13 Дифферента и ветвление . . . 164
1.14 Кольцо целых композита расширений . . . 167
1.15 Теорема Куммера . . . 168
1.16 Первый случай Last Fermat’s theorem . . . 171
1.17 Алгоритм построения целого базиса . . . 177
1.18 Геометрия чисел . . . 177
1.19 Мультипликативная группа кольца целых числового поля . . . 183
1.20 Контр-пример к принципу Минковского-Хассе . . . 188
1.21 Поле p-адических чисел и лемма Гензеля . . . 190
1.22 Группа квадратов поля $\mathbb{Q}_p$ и норменная группа . . . 193
1.23 Символ Гильберта . . . 195
1.24 Теорема Минковского-Хассе . . . 200
2. Локальные поля. Введение. . . . 202
2.1 Кольца дискретного нормирования . . . 202
2.2 Продолжение нормирований и ветвление . . . 207
2.3 Целый базис для расширения полного поля . . . 212
2.4 Неравзветвлённые и вполне разветвлённые расширения . . . 214
2.5 Локальные поля . . . 215
3. Когомологии групп . . . 216
3.1 Построение при помощи проективных резольвент . . . 216
3.2 Стандартная резольвента . . . 219
3.3 Когомологии циклической группы . . . 221
3.4 Гомологии групп . . . 223
3.5 Когомологии Тейта . . . 225
3.6 Периодичность когомологий Тейта для циклической группы . . . 226
3.7 Индекс Эрбана . . . 227
3.8 Ограничение и инфляция . . . 228
3.9 Точная последовательность для ограничения и инфляции в старших размерностях . . . 231
3.10 Отображение кограничения . . . 232
3.11 Композиция ограничения и кограничения . . . 234
3.12 Теорема Гильберта-90 . . . 235
4. Применения когомологий групп к теории чисел . . . 236
4.1 Вычисление $H^2(G, L^*)$ . . . 236
4.2 Группа Брауэра . . . 244
4.3 Когомологически тривиальные модули и теорема Тейта . . . 244
4.4 Норменные группы . . . 248
4.5 Теория Куммера . . . 250
4.6 Локальная теорема Кронекера . . . 252

5. Гауссовы суммы 253
5.1 Общие сведения 253
5.2 Количество решений уравнений над конечным полем 255
6. Глобальная теорема Кронекера 256
6.1 Группа и поле инерции для максимального идеала в случае числового поля 256
6.2 Глобальная теорема Кронекера 258

Глава 1

Алгебраическая топология

1. Сингулярные гомологии

1.1 Симплициальные гомологии

Определение 1. *Цепным комплексом* абелевых групп $(C_\bullet, \partial)$ называется последоватекльность абелевых групп и морфизмов вида

$$\dots \xrightarrow{\partial_{q+2}} C_{q+1} \xrightarrow{\partial_{q+1}} C_q \xrightarrow{\partial_q} \dots, \qquad \text{где } C_i - \text{абелевы группы}$$

при условии $\partial_q \circ \partial_{q+1} = 0$. Если комплекс обрывается с одной из сторон, то мы считаем, что он дополнен нулями.

Элементы группы C_q называют q-мерными цепями, а отображение ∂ называют (граничным) дифференциалом.

Замечание. Ясно, что условие $\partial_q \circ \partial_{q+1} = 0$ равносильно тому, что $\operatorname{Ker} \partial_q \supset \operatorname{Im} \partial_{q+1}$.

Замечание. Когда комплекс снабжают отображением $C_0 \xrightarrow{\varepsilon} \mathbb{Z}$, это отображение называют *аугументацией.*

Определение 2. *Гомологиями* комплекса $(C_\bullet, \partial)$ называют абелевы группы

$$H_q(C_\bullet, \partial) \stackrel{\text{def}}{=} \operatorname{Ker} \partial_q / \operatorname{Im} \partial_{q+1}.$$

Если коплекс снабжен аугументацией и обрывается на нулевом члене, то у него также есть *приведённые гомологии*

$$H_0(C_\bullet, \partial) = C_0 / \operatorname{Im} \partial_1, \quad \widetilde{H_0}(C_\bullet, \partial) = \operatorname{Ker} \partial_0 / \operatorname{Im} \partial_1, \quad \widetilde{H}_q = H_q \; \forall q > 0,$$

которые отличаются от обычных только в нулевом члене.

Перед тем как что-то строго определять, посмотрим нестрого на какие-то мотивирующие примеры вычислений. Для этого лучше всего подойдут *симплициальные гомологии.* Неформально, идея состоит в том, что мы разбиваем топологическое пространство X на симплексы всех размерностей и говорим, что $C_q(X, \mathbb{Z})$ — свободная абелева группа, порожденная всеми q-мерными симплексами (то есть, мы рассматриваем целочисленные формальные линейные комбинации симплексов). Дифференциалом ∂ будет оператор взятия границы (топологической).

Пример 1 (Симплицаильные гомологии отрезка (нестрого))**.** Пусть X — отрезок $[a, b]$ с ориентацией из b в a. В нём две нульмерные клетки, значит $C_0(X, \mathbb{Z}) = \mathbb{Z}^2$, одномерная клетка одна — ребро e, то есть $C_1(X, \mathbb{Z}) = \mathbb{Z}$ и комплекс устроен следующим образом:

$$\dots 0 \to C_1 \xrightarrow{\partial_1} C_0 \xrightarrow{\varepsilon} \mathbb{Z},$$

так как мы можем определить аугументацию следующим образом: $x \in C_0 \Rightarrow x = k_1 a + k_2 b$, положим $\varepsilon(x) = k_1 + k_2$. То есть, на самом деле комплекс выглядит вот так:

$$\dots \to 0 \to \mathbb{Z} \xrightarrow[e \to \partial e = a - b]{} \mathbb{Z}^2 \xrightarrow[a \to 1,\; b \to 1]{} \mathbb{Z}.$$

Заметим, что $\varepsilon \circ \partial = 0$.

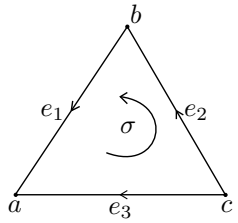
Гомологиями топологического пространства называют гомологии построенного по нему комплекса. В нашем случае

$$H_1(X, \mathbb{Z}) = \operatorname{Ker} \partial_1 / \operatorname{Im} \partial_2 = 0/0 = 0.$$

$$\widetilde{H_0}(X, \mathbb{Z}) = \operatorname{Ker} \varepsilon / \operatorname{Im}_{\partial_1} = \langle a - b \rangle / \langle a - b \rangle = 0.$$

$$H_0(X, \mathbb{Z}) = C_0(X, \mathbb{Z}) = C_0(X, \mathbb{Z}) / \operatorname{Im}_{\partial_1} = \mathbb{Z}^2/\mathbb{Z} = \langle a, b \rangle / \langle a - b \rangle = \langle a \rangle = \mathbb{Z}$$

Пример 2 (Симплицальные гомологии треугольника)**.** Рассмотрим треугольник (abc) с внутренностью σ, ориентированной против часовой стрелки, и рёбрами $b \xrightarrow{e_1} a$, $c \xrightarrow{e_3} a$, $c \xrightarrow{e_2} b$.



Тогда цепной комплекс, построенный по треугольнику будет устроен следующим образом:

$$\ldots \to 0 \to \mathbb{Z} \xrightarrow[\sigma \to e_1 + e_2 - e_3]{\partial_2} \mathbb{Z}^3 \xrightarrow{\partial_1} \mathbb{Z}^3 \xrightarrow{\varepsilon} \mathbb{Z}$$

Из ориентации σ ясно, что $\partial\sigma = e_1 + e_2 - e_3$, $\partial e_1 = b - c$, $\partial e_2 = a - b, \partial e_3 = a - c$. Ясно, что вторые гомологии нулевые:

$$H_2(X, \mathbb{Z}) = \operatorname{Ker} \partial_2 / 0 = 0$$

Посчитаем теперь первые.

$$\partial(k_1 e_1 + k_2 e_2 + k_3 e_3) = k_1(b - c) + k_2(a - b) + k_3(a - c) = a(k_2 + k_3) + b(k_1 - k_2) + c(-k_1 - k_3) \Rightarrow$$
$$\Rightarrow \operatorname{Ker} \partial_1 = \langle (k_1, k_2, k_3) \in \mathbb{Z}^3 \mid k_1 = k_2 = -k_3 \rangle$$

С другой стороны, $\operatorname{Im} \partial_2 = k(e_1 + e_2 - e_3)$. Тем самым, $H_1(X, \mathbb{Z}) = 0$. Аналогичным вычислением мы получаем, что $H_0(X, \mathbb{Z}) = \mathbb{Z}$.

Пример 3 (Спмилициальные гомологии треугольника без внутренности)**.** Пусть теперь всё также, как в примере 2, но у треугольнка нет внутренности. Тогда цепной комплекс будет иметь вид

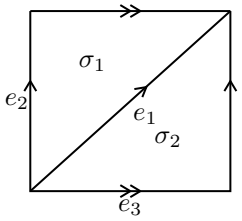
$$\ldots \to 0 \to \mathbb{Z}^3 \to \mathbb{Z}^3 \to \mathbb{Z}$$

Из того, как поменялись отображения, ясно, что поменялись только первые гомологии. Теперь $H_1(X, \mathbb{Z}) = \mathbb{Z}/\{0\} = \mathbb{Z}$, а образующая — это цикл $e_1 + e_2 - e_3$. С другой стороны, $\pi_1(\Delta) = \mathbb{Z}$.

Замечание. Когда-нибудь позже мы докажем, что для любого симплициального пространства X есть отображение

$$\pi_1(X) \to H_1(X) = \pi_1(X)^{ab} = \pi_1(X)/[\pi_1(X), \pi_1(X)].$$

Пример 4 (Симплициальные гомологии тора $\mathbb{T}^2$)**.** Рассмотрим двумерный тор $\mathbb{T}^2$, разбитый на симплексы следующим образом:



Из такой триангуляции ясно, что комплекс будет иметь вид:

$$\ldots \to 0 \to \mathbb{Z}^2 \xrightarrow{\partial_2} \mathbb{Z}^3 \xrightarrow{\partial_1} \mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}$$

Посчитаем дифференциал на двумерных клетках: $\partial\sigma_1 = e_1 - e_3 - e_2,\ \partial\sigma_2 = e_2 + e_3 - e_1$. С другой стороны, ясно, что дифференциал зануляется на любой одномерной клетке, $\partial e_i = a - a = 0$.

$$H_2(\mathbb{T}^2, \mathbb{Z}) = \operatorname{Ker}\partial_2 / 0 = \mathbb{Z}.$$

так как $\partial\sigma_1 = -\partial\sigma_2 \Rightarrow \operatorname{Ker}\partial_2 = \mathbb{Z}$.

Также прямыми вычислениями можно убедиться, что $H_1(\mathbb{T}^2, \mathbb{Z}) = \mathbb{Z}^2 = \pi_1(\mathbb{T}^2)^{ab}$. Образующими первых гомологий будут e_2 и e_3.

Упражнения.

1. Посчиать по определению одномерные гомологии связного дерева.
2. Посчитать по определению все гомологии n-мерного симплекса T^n

$$T^n \stackrel{\text{def}}{=} \left\{ (t_0, \ldots, t_n) \mid t_i \geq 0,\ \sum_{i=1}^{n} t_i = 1 \right\}.$$

3. Покажите, что барицентрическое подразбиение не меняет симплициальных гомологий.

Вообще говоря, далее нужно формально доказывать, что гомологии не зависят от симплициального разбиения пространства (и выяснять, у каких пространств это симплициальное разбиение вообще есть), но мы этим всем заниматься не будем, так как в нашем курсе основной будет другая теория.

1.2 Сигнулярные гомологии

Определение 3. Пусть X — топологическое пространство.

- *Сингулярным q-мерным симплексом* мы будем называть непрерывное отображение $f\colon T^q \to X$.
- Его граница определяется, как формальная линейная комбинация

$$\partial f \stackrel{\text{def}}{=} \sum_{i=0}^{q} (-1)^i \Gamma_i f,$$

  где $\Gamma_i f$ — сужение f на грань $t_i = 0$ (сумма именно такая, так как у q-мерного симплекса $q+1$ грань).
- *Сингулярными q-мерными цепями* $C_q(X, \mathbb{Z})$ мы будем называть формальные целочисленные линейные комбинации конечного числа q-мерных сингулярных симплексов (то есть порожденную ими свободную абелеву группу).
- Дифферецниал комплекса[1] $C_\bullet$ определяется, как продолжение по линейности оператора взятия границы q-мерного сингулярного симплекса.
- Комплекс сингулярных цепей может быть снабжен аугументацией $\varepsilon\colon C_0 \to \mathbb{Z},\ \sum k_i f_i \to \sum k_i$.

Замечание. Формально говоря, мы пока не знаем, что комплекс из сингулярных цепей — это комплекс. Для этого нам понадобится следующая техническая

Лемма 1. В контексте определения 3 $\partial^2 = 0$.

Доказательство. Посчитаем $\partial\partial f$:

$$\partial\partial f = \partial\left(\sum_i (-1)^i \Gamma_i f\right) = \sum_{i,j} (-1)^{i+j} \Gamma_j \Gamma_i f.$$

Ясно, что любую грань коразмерности 2 можно получить взятием границы двумя способами. Действительно, если $j < i$, то $\Gamma_i\Gamma_j = \Gamma_j\Gamma_{i+1}$ (i-я из оставщихся после выкидывания j-й координаты $- i+1$-я изначально), а в сумме слагаемые $\Gamma_i\Gamma_j$ и $\Gamma_j\Gamma_{i+1}$ будут с разным знаком, значит $\partial\partial f = 0$. □

[1] формально, мы пока еще не знаем, что это комплекс.

Определение 4. *Сингулярными гомологиями* топологического пространства X называются гомологии комплекса сингулярных цепей. Мы будем обозначать их, как $H_k(X)$ или $H_{\text{k}}^{\text{sing}}(X)$.

В топологическом контексте группу $Z_q(X) \stackrel{\text{def}}{=} \operatorname{Ker} \partial_q$ часто называют *q-циклами*[2], а группу $B_q(X) \stackrel{\text{def}}{=} \operatorname{Im} \partial_{q+1}$ — *q-границами*. В этом смысле $H_q(X)$ — циклы с точностью до границ.

Замечание. Из определения очевидно, что сингулярные гомологии зависят только от класса гомеоморфизма пространства X (их основной плюс и состоит в том, что тут это очевидно).

Теперь попробем посчитать по определению сингулярные гомологии для какого-нибудь пространства. Оказывается, что по определению сделать это возможно разве что для точки.

Теорема 1 (Сингулярные гомологии точки)**.**

$$H_q^{\text{sing}}(*, \mathbb{Z}) = 0,\ H_0^{\text{sing}}(*, \mathbb{Z}) = \mathbb{Z},\ \widetilde{H}_0^{\text{sing}}(*, \mathbb{Z}) = 0.$$

Итак, как мы помним, $C_q(*)$ — все линейные комбинации отображений $f\colon T^q \to *$. Так как отображений из T^n в точку всего одно, $\forall n\ C_n(X, \mathbb{Z}) = \mathbb{Z}$, а значит, наш комплекс сингулярных цепей $(C_\bullet(*, \mathbb{Z}), \partial)$ будет иметь вид:

$$\ldots \mathbb{Z} \xrightarrow{\partial} \mathbb{Z} \xrightarrow{\partial} \ldots \xrightarrow{\partial_2} \mathbb{Z} \xrightarrow{\partial_1} \mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}.$$

Теперь посчитаем дифференциалы комплекса.

Возьмем $f \in C_1$, это какая-то формальная линейная комбинация отображений из $[a, b] \to \{*\}$ Тогда ∂f — это $f|_a - f|_b = 0$. Впрочем, и сразу ясно, что в случае любого n, так как наше отображение действует в точку (оно постоянно), сужения на все грани будут совпадать и результат в сумме будет зависеть лишь от четности n, то есть дифференциалы комплекса будут иметь вид:

$$\ldots \mathbb{Z} \xrightarrow{\cdot 0} \mathbb{Z} \xrightarrow{\cdot 1} \ldots \xrightarrow{\cdot 1 = \text{id}} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{\varepsilon} \mathbb{Z}$$

Иными словами, $\partial_n = 0$, если n — нечетное и тождественно иначе. Теперь, как нетрудно заметить,

$$\forall q > 0 \quad \operatorname{Ker} \partial_q = \operatorname{Im} \partial_{q+1} \Rightarrow H_q^{\text{sing}}(*, \mathbb{Z}) = 0,\ H_0^{\text{sing}}(*, \mathbb{Z}) = \mathbb{Z},\ \widetilde{H}_0^{\text{sing}}(*, \mathbb{Z}) = 0.$$

Трудности, возникшие при подсчетах, намекают на то, что для отрезка, например, это будет сделать еще гораздо труднее. С другой стороны, если вдруг окажется, что гомологии гомотопически инвариантны, то мы будем знать, какие гомологии у всех стягиваемых пространств (так как для точки мы посчитали).

В дальнейшем, будем использовать для сингулярных гомологий обозначение H_k.

1.3 Немного гомологической алгеры

Рассмотрим категорию цепных комплексов $\mathfrak{Ch}$ (в нашем случае абелевых групп, но в принципе, всё что тут будет сказано справделиво и в случае $R - \mathfrak{Mod}$). Морфизмом цепных комплексов $(C_\bullet, \partial)$ и $(D_\bullet, \delta)$ называется набор отображений $f = \{f_i\}$, где $f_i \in \operatorname{Hom}(C_i, D_i)$ такой, что диаграмма

$$\begin{array}{ccccccccc}
\ldots & \xrightarrow{\partial_{q+2}} & C_{q+1} & \xrightarrow{\partial_{q+1}} & C_q & \xrightarrow{\partial_q} & C_{q-1} & \xrightarrow{\partial_{q-1}} & \ldots \\
\downarrow & & \downarrow{\scriptstyle f_{q+1}} & & \downarrow{\scriptstyle f_q} & & \downarrow{\scriptstyle f_{q-1}} & & \downarrow \\
\ldots & \xrightarrow{\delta_{q+2}} & D_{q+1} & \xrightarrow{\delta_{q+1}} & D_q & \xrightarrow{\delta_q} & D_{q-1} & \xrightarrow{\delta_{q-1}} & \ldots
\end{array}$$

коммутативна, то есть $\forall i\ f_i \circ \partial_{i+1} = \delta_{i+1} \circ f_{i+1}$.

Лемма 2. Сопоставление цепному комплексу его k-й группы гомологий функториально, то есть отображение

$$(C_\bullet, \partial) \mapsto H_k(C_\bullet, \delta)$$

задаёт ковариантный функтор $\mathfrak{Ch} \to \mathfrak{Ab}$.

[2] позже мы увидим, какая в этом геометрическая интуиция

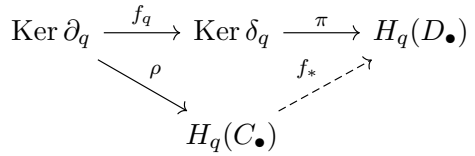
Доказательство. Всё, кроме того, что композиция переходит в композицию — совсем очевидно. Нам надо проверить, что отображение $(C_\bullet, \partial) \xrightarrow{f} (D_\bullet, \delta)$ индуцирует отображение $H_k(C_\bullet) \to H_k(D_\bullet)$, и кроме того,

$$(C_\bullet, \partial) \xrightarrow{f} (D_\bullet, \delta) \xrightarrow{g} (E_\bullet, d) \Rightarrow H_k(f \circ g) = H_k(f) \circ H_k(g).$$

Заметим, что так как $f \in \mathrm{Hom}(C_\bullet, D_\bullet)$, $f_q(\mathrm{Ker}\,\partial_q) \subset \mathrm{Ker}\,\delta_q$. Действительно, если $\partial_q(x) = 0$, то $0 = f_{q-1}(\partial_q(x)) = \delta_q(f_q(x)) \Rightarrow f_q(x) \in \mathrm{Ker}\,\delta_q$. Аналогично $f_{q-1}(\mathrm{Im}\,\partial_q) \subset \mathrm{Im}\,\delta_q$. Действительно, если $x = \partial_q(y)$, то

$$f_{q-1}(x) = f_{q-1} \circ \delta_q(x) = \delta_q(f_q(y)) \in \mathrm{Im}\,\delta_q.$$

Тогда нужная нам стрелка получается просто из универсального свойства факторгруппы:



Действительно, чтоб она существовала, нам нужно, чтоб $\mathrm{Im}\,\partial_{q+1} \subset \mathrm{Ker}(\pi \circ f_q)$. Возьмем $x \in \mathrm{Im}\,\partial_{q+1}$, тогда $f_q(x) \in \mathrm{Im}_{\delta_{q+1}} \Rightarrow f_q(x) \in \mathrm{Ker}\,\pi$, то есть $x \in \mathrm{Ker}\,(\pi \circ f_q)$.

Проверка того, что композиция переходит в композицию тривиальна. □

Замечание. Пусть $X, Y \in \mathfrak{Top}$, $f\colon X \to Y$ — непрерывное отображение. Тогда оно индуцирует морфизм цепных комплексов $f\colon C_\bullet(X) \to C_\bullet(Y)$. Действительно, пусть $g \in C_k(X)$, тогда g — это непрерывное отображение $T_k \to X$ и тогда $f \circ g$ — непрерывное отображение $T_k \to Y$, то есть элемент $C_k(Y)$. Остается проверить, что полученное отоюражение будет коммутировать с дифференциалом.

$$\partial g = \sum_{i=0}^{k} (-1)^i \Gamma_i g.$$

Тогда остается заметить, что взятие грани коммутирует с применением отображения:

$$f(\partial g) = \sum_{i=0}^{k} (-1)^i \Gamma_i f(g) = \partial(fg).$$

Значит, если у нас есть непрерывное отображение $f\colon X \to Y$, то есть и индуцированный морфизм гомологий $f_*\colon H_\bullet(X) \to H_\bullet(Y)$.

Предложение 1. *Если $f\colon X \to Y$ — гомеоморфизм, то $f_*\colon H_k(X) \to H_k(Y)$ — изоморфизм (для всех k).*

Доказательство. Действительно, если f — гомеоморфизм, то все индуцированные отображения между цепями — изоморфизмы, а значит и все индуцированные отображения в гомологиях будут изоморфизмами. □

Замечание. Это утверждение говорит нам о том, что сингулярные гомологии определены для топологических пространств без всякой дополнительной структуры.

Определение 5. Пусть X — топологическое пространство. Тогда, если группа $H_k(X)$ конечнопорождена, то

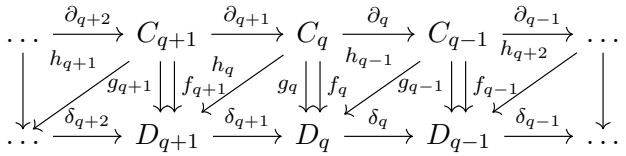
$$H_k(X) \cong \mathbb{Z}^n \oplus \mathrm{Tor}(H^k(X)).$$

Тогда число n (то есть, ранг свободной части) называют k-м числом Бетти b_n. Иными словами, $b_k(X) = \mathrm{rank}(H_k(X))$.

1.4 Гомотопическая инвариантность гомологий

Определение 6. Пусть $(C_\bullet, \partial), (D_\bullet, \delta) \in \mathfrak{Ch}$ — два цепных комплекса. Их морфизмы $f, g \in \mathrm{Hom}_{\mathfrak{Ch}}((C_\bullet, \partial), (D_\bullet, \delta))$ называются *гомотопными* ($f \sim g$), если сущесвует диагональный морфизм $h\colon C_\bullet \to D_{\bullet+1}$ такой, что

$$h_{q-1}\partial_q + \delta_{q+1}h_q = f_q - g_q.$$



Кратко это обычно записывают, как $h\partial + \delta h = f - g$.

Если в категории цепных комплексов $\mathfrak{Ch}(\mathfrak{Ab})$ отождествить гомотопные морфизмы, получится *гомотопическая категория комплексов*, которую обычно обозначают $\mathfrak{K}(\mathfrak{AB})$ (или просто $\mathfrak{K}$).

Теорема 2. *Если морфизмы цепных комплексов гомотопны, то есть $f \sim g$, то индуцированные гомоморфизмы когомологий $f_* = g_*$. Тем самым, функторы гомологий H_k пропускаются через гомотопическую категорию.*

Доказательство. Если $x \in \mathrm{Ker}\,\partial_q$, то

$$f_q(x) - g_q(x) = \delta_{q+1}h_q(x) + \underbrace{h_{q-1}\partial_q(x)}_{=0} \in \mathrm{Im}\,\delta_{q+1},$$

а значит в $H_q(X)$ эти элементы равны. □

Замечание. Гомотопность морфизмов f и g можно определять, как $\delta h \pm h\partial = f - g$, так как при переходе к гомологиям второе слагаемое всё равно обнуляется.

Теорема 3. *Пусть $f, g\colon X \to Y$, $f \sim g$. Тогда $f_* = g_*$.*

Доказательство. У нас есть цепные комплексы сингулярных цепей $(C_\bullet(X), \partial)$ и $(C_\bullet(Y), \partial)$. Так как $f \sim g$, существует непрерывное отображение $H\colon X \times I \to Y$, а тогда $\forall p\colon T_q \to X$ определено непрерывное отобрежение $H(p(\_),\_)\colon T_q \times I \to Y$, причем $H(p,0) = f(p)$ и $H(p,1) = g(p)$. Положим

$$h(p) = \text{сумма симплексов в разбиении призмы } T_q \times I \in C_{q+1}(Y).$$

Взглянув на картинку теперь нетрудно заметить, что

$$f(p) - h(p) = \text{граница всей призмы} - \text{боковые стенки} = \partial h(p) - h\partial(p)$$

Таким образом, мы получили, что индуцированные морфизмы цепных комплексов гомотопны, а значит, по теореме 2, индуцированные гомоморфизмы в гомологиях совпадают. □

Упражнение. Разбить $T_q \times I$ на $q+1$-мерные симплексы формально. А именно, пусть $T_q \times \{0\} = a_0 \dots a_q$. Пусть вершины $T_q \times \{1\}$ — это $a'_0, \dots, a'_q$. Тогда предлагается брать вершины $a_0 \dots a_k a'_k \dots a'_q$.

Следствие 1. *Пусть X — стягиваемое. Тогда $\widetilde{H}_\bullet(X, \mathbb{Z}) = 0$, или, иными словами, $\forall k > 0$ $H_k(X, \mathbb{Z}) = 0$, $H_0(X, \mathbb{Z}) = \mathbb{Z}$.*

Упражнение. Придумайте пример нестягиваемого X с нулевыми приведёнными гомологиями.

Лемма 3. Если X — линейно связно, то $H_0(X) = \mathbb{Z}$.

Доказательство. Выберем в нашем пространстве некоторую фиксированную точку a, тогда

$$\Big(\sum k_i f_i\Big) = \Big(\sum k_i\Big)a \pmod{\mathrm{Im}\,\partial_1},\ \text{(то есть, в } H_0(X))$$

так как все f_i можно соединить путями (а это отображения $T^1 = [0,1] \to X$) с a и значит $\mathrm{Im}\,\partial_1$ будет содержать все разности $f_i - a$. Значит, $H_0(X) \cong \mathbb{Z}$. □

Следствие 2. *Пусть у топологического пространства X n компонент линейной связности. Тогда*

$$H_0(X) \cong \mathbb{Z}^n.$$

Упражнение. Дркажите, что непрерывное отображение между линейно связными пространствами индуцирует изоморфизм нулевых гомологий.

1.5 Относительные гомологии и гомологически точная последовательность пары

Пусть X — топологическое пространство, $A \subset X$, тогда $\forall q\ C_q(A) \subset C_q(X)$ (вложение индуцирует мономорфизм цепей) и мы имеем морфизм цепных комплексов $(C_\bullet(X), \partial)$ и $(C_\bullet(A), \partial)$, то есть коммутативна следующая диаграмма:

$$\begin{array}{ccccccc} \dots & \longrightarrow & C_q(A) & \xrightarrow{\partial_q} & C_{q-1}(A) & \longrightarrow & \dots \\ \downarrow & & \downarrow{\scriptstyle \text{in}} & & \downarrow{\scriptstyle \text{in}} & & \downarrow \\ \dots & \longrightarrow & C_q(X) & \xrightarrow{\partial_q} & C_{q-1}(A) & \longrightarrow & \dots \end{array}$$

Это так просто потому, что если у нас был симплекс $f\colon T^q \to A$, то его граница тоже целиком лежит в A, то есть $\partial f\colon T^{q-1} \to A \in C_{q-1}(A)$.

Глядя на это, возникает естественная идея дополнить до короткой точной последовательности

$$0 \to C_q(A) \to C_q(X) \to C_q(X)/C_q(A) \to 0$$

в каждом столбце.

Определение 7. Факторгруппу $C_q(X, A) \stackrel{\text{def}}{=} C_q(X)/C_q(A)$ называют *относительными цепями.*

Построим цепной комплекс для относительных цепей, для этого надо определить дифференциалы. Это делается стандартно, возьмем $x \in C_q(A)$, тогда $\partial_q(x) \in C_{q-1}(A)$, а значит композиция дифференциала и проекции пропустится через фактор:

$$\begin{array}{ccccc} C_q(X) & \xrightarrow{\partial_q} & C_{q-1}(X) & \xrightarrow{\pi_{q-1}} & C_{q-1}(X)/C_{q-1}(A) \\ & \searrow^{\pi_q} & & \nearrow_{\exists!\delta_q} & \\ & & C_q(X)/C_q(A) & & \end{array}$$

Проверим теперь, что $\delta^2 = 0$. Действительно, из коммутаивной диаграммы выше мы понимаем, что

$$\delta_q(\overline{x}) = \delta_q(\pi_q(x)) = \pi_{q-1}(\partial_q(x)) \Rightarrow \delta_{q-1}(\delta_q(\overline{x})) = \delta_{q-1}(\pi_{q-1}(\partial_q(x))) = \pi_{q-2}(\partial_{q-1}(\partial_q(x))) = 0.$$

Теперь мы построили цепной комплекс и можем определить относительные гомологии.

Определение 8. Пусть $X \subset A$, тогда относительными гомологиями мы будем называть гомологии комплекса относительных цепей, то есть

$$H_q(X, A) \stackrel{\text{def}}{=} \ker \delta_q / \operatorname{Im} \delta_{q+1}.$$

Теперь, попробуем получить для гомологий аппарат, идеологически похожий на теорему Зейферта-Ван-Кампена.

Итак, мы имеем *короткую точную последовательность комплексов*

$$0 \to C_\bullet(A) \to C_\bullet(X) \to C_\bullet(X, A) \to 0$$

В развёрнутом виде она представляет собой коммутативную диаграмму

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_{q+1}(A) & \longrightarrow & C_{q+1}(X) & \longrightarrow & C_{q+1}(X,A) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_q(A) & \longrightarrow & C_q(X) & \longrightarrow & C_q(X,A) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C_{q-1}(A) & \longrightarrow & C_{q-1}(X) & \longrightarrow & C_{q-1}(X,A) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

в которой строки точны, а стлобцы — наши комплексы.

Теорема 4 (Точная последовательность пары)**.** *Существует* связывающий гомоморфизм $\varphi\colon H_q(X,A) \to H_{q-1}(A)$*, и соответственно, имеет место следующая длинная точная последовательность групп гомологий:*

$$\ldots \to H_q(A) \to H_q(X) \to H_q(X,A) \xrightarrow{\varphi} H_{q-1}(A) \to H_{q-1}(X) \to \ldots$$

Доказательство. На самом деле, это утверждение верно для любой точной последовательности комплексов. А именно, если последовательность цепных комплексов

$$0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$$

точна, то имеет место следующая длинная точность последовательность гомологий:

$$\ldots \to H_q(A) \to H_q(B) \to H_q(C) \to H_{q-1}(A) \to H_{q-1}(B) \to \ldots$$

Это можно без труда вывести из леммы о змее, проверив точность строк[3] □

Упражнение. Докажите, что для $X \supset A \supset B$ имеет место следующая длинная точная последовательность групп гомологий

$$\ldots \to H_q(A,B) \to H_q(X,B) \to H_q(X,A) \to H_{q-1}(A,B) \to \ldots$$

Посмотрим, что всё это означает геометрически. Относительные циклы — это элементы

$$\operatorname{Ker}(C_q(X)/X_q(A) \to C_{q-1}(X)/C_{q-1}(A)).$$

Мы взяли представителя в $C_q(X)$, взяли границу и после факторизации по $C_{q-1}(A)$ получили 0, а значит граница нашего цикла полностью лежит в $C_{q-1}(A)$, то есть картинка имеет вид:

С другой стороны, ясно, что $x \in C_q(X)/C_q(A)$ — относительная граница, если $x + a = \partial(\ldots)$.

[3] а так как это делается в абсолютно любом курсе гомологической алгебры, мне лень это сюда писать.

Замечание. У связывающего гомоморфизма $H_q(X, A) \to H_{q-1}(A)$ есть очень естественная интерпретация.

Элементы $H_q(X, A)$ — относительные циклы с точностью до относительных границ. Так как это относительные q-мерные циклы, их граница лежит в A, а значит, при взятии границы, мы получим как раз элемент $H_{q-1}(A)$. То есть, связывающий гомоморфизм $H_q(X, A) \to H_{q-1}(A)$ — взятие границы.

Рассмотрим также еще несколько важных следствий длинной точной последовательности пары.

Следствие 3. *Для любого топологического пространства x и любой его точки $x_0 \in X$ мы имеем*

$$H_n(X, x_0) = \widetilde{H}_n(X) \; \forall n.$$

Доказательство. Запишем длинную точную последовательность приведенных гомологий пары (X, x_0)

$$\ldots \to \widetilde{H}_q(x_0) \to \widetilde{H}_q(X) \to \widetilde{H}_q(X, x_0) \to \widetilde{H}_{q-1}(x_0) \to \ldots$$

Действительно, так как $\widetilde{H}_n(x_0) = 0 \; \forall n$, мы на самом деле имеем

$$\ldots \to 0 \to \widetilde{H}_q(X) \to \widetilde{H}_q(X, x_0) \to 0 \to \ldots,$$

и из точности следует $\widetilde{H}_q(X) \cong \widetilde{H}_q(X, x_0) = H_q(X, x_0)$. □

Следствие 4. *Группы $H_q(X, A)$ измеряют различие между $H_q(X)$ и $H_q(A)$, а именно,*

$$H_q(X, A) = 0 \quad \forall q \Rightarrow H_q(A) = H_q(X) \quad \forall q.$$

Доказательство. Запишем длинную точную последовательность пары (X, A) :

$$\ldots \to H_q(A) \to H_q(X) \to H_q(X, A) \to H_{q-1}(A) \to \ldots$$

В нашем случае она имеет вид:

$$\ldots \to H_q(A) \to H_q(X) \to H_q(X, A) \to H_{q-1}(A) \to \ldots$$

и из точности следует, что $H_q(A) \cong H_q(X)$. □

Упражнение. Убедитесь, что верно и обратное утверждение.

1.6 Пары Боруска

Определение 9. Пусть X – топологическое пространство, а $A \subset X$ с индуцированной топологией. Тогда говорят, что (X, A) – *пара Борсука* (или, *корасслоение*)[4], если $\forall f \colon X \to Y$, $\forall F \colon A \times I \to Y$ такой, что $F|_{A\times 0} = f|_A$ существует $G \colon X \times I \to Y$, причем такое, что $G|_{X\times 0} = f$, $G|_{A\times I} = F$.

Определение 10. Пара (X, A) называется *клеточной парой*, если X — клеточное пространство, A — клеточное подпространство X.

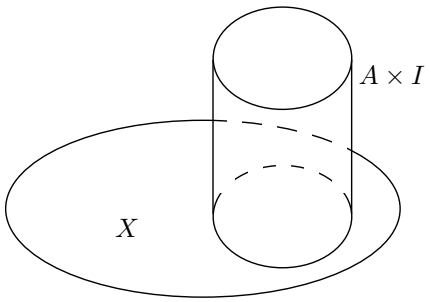
Замечание. Так как очевидно, что $(D^n, \partial D^n)$ — пара Борсука, клеточная пара является парой Борсука.

Нам от пар Борсука понадобится несколько базовых утверждений.

Теорема 5 (Характеризация пар Борсука)**.** *Если (X, A) — пара Борсука, то деформационная ретракция $X \times I$ на $X \cup (A \times I)$. Кроме того, если A — замкнуто, то верно и обратное.*

Доказательство. На картинке это выглядит следующим образом:

[4]Еще говорят «обладает свойством продолжения гомотопии», но это совсем уж длинно.



Положим $Y = X \cup (A \times I)$, $f\colon X \to Y$ — вложение. Рассмотрим теперь гомотопию $F_t(A) = A \times t$. Так как (X, A) — пара Борсука, существует $G\colon X \times I \to Y\colon G|_{A\times I} = F$.

Докажем теперь в другую сторону: пусть для $f\colon X \to Y$ есть гомотопия $F_t\colon A \to Y$, то есть отображение $F\colon X \cup (A \times I) \to Y$. Тогда искомое продолжение гомотопии — композиция F и деформационной ретракции $X \times I \to X \cup (A \times I)$[5]. □

Следствие 5. *Пара $(D^n, \mathrm{Int}(D^n))$ — не пара Борсука.*

Вообще говоря, эта теорема показывает, что было бы хорошо, чтоб A было замкнутым.

Замечание. В нехаусдорфовом случае бывает, что и с незамкнутым A пара (X, A) будет парой Борсука.

Упражнение. Если (X, A) — пара Борсука и X — Хаусдорфово, то A замкнуто.

Предложение 2. *Пусть (X, A) — пара Борсука. Тогда*

$$X \cup CA \sim (X \cup CA)/CA = X/A.$$

Доказательство. Рассмотрим вложение $X \to X \cup CA$. Прогомотопируем A в вершину конуса a. Так как (X, A) — пара Борсука, эта гомотопия продолжается до гомотопии на X. Тогда финальный элемент гомотопии отображает $X \to X \cup CA$ так, что $A \mapsto a$, значит, это отображение пропускается через фактор X/A. С другой стороны ясно, как устроено обратное отображение $X \cup CA \to X/A$ (стягиваем конус в точку). Нетрудно заметить, что два построенных отображения задают гомотопическую эквивалентность. □

Следствие 6. *Если (X, A) — пара Боруска и A — стягиваемо, то $X \sim X/A$.*

Предложение 3. *Пара (CX, X) — всегда пара Борсука.*

1.7 Относительные гомологии как абсолютные (факторизация)

Итак, в этом параграфе нас будет интересовать следующее (весьма полезное в вычислениях утверждение):

Теорема 6. *В общем случае отображение $X \to X \cup CA$ индуцирует изоморфизм*

$$H_q(X, A) \to H_q(X \cup CA, CA) = H_q(X \cup CA, a) = \widetilde{H}_q(X \cup CA),$$

где a — вершина конуса.

Если (X, A) — пара Борсука, то отображение проекции $p\colon X \to X/A,\ A \mapsto a$ индуцирует изоморфизм

$$H_q(X, A) \xrightarrow{p_*} H_q(X/A, a) = \widetilde{H}_q(X/A).$$

Вообще говоря, условие на A во второй части теоремы часто опускают и говорят, что это верно для «хороших пар». Мы доказываем для пар Борсука, можно доказывать для случая, когда A — *окрестностный деформационынй ретракт.*

Для доказательства этой теоремы нам понадобится несколько важных (в общем контексте) лемм.

Сначала посмотрим на геометрическую конструкцию **барицентрического подразбиения**, чтоб иметь геометрическую интуицию в контексте сингулярных симплексов.

Рассмотрим симплекс $[v_0, \dots, v_n]$. его точки — линейные комбинации вида

$$\sum_{i=0}^{n} t_i v_i, \quad \text{где} \sum_{i=0}^{n} t_i = 1,\ t_i \geq 0.$$

[5] вот тут мы пользуемся замкнутостью A, так как нам нужно, чтоб покрытие было фундаментальным.

Определение 11. *Барицентр (центр тяжести)* симплекса — это точка $b \in [v_0, \dots, v_n]$, у которой все барицентрические аоординаты t_i равны, а именно, $t_i = \frac{1}{n+1}\ \forall i$.

Барицентрическое подразбиение (подразделение) симплекса $[v_0, \dots, v_n]$ — это разбиение симплекса $[v_0, \dots, v_n]$ на n-мерные симплексы $[b, w_0, \dots, wn-1]$, где по индукции $[w_0, \dots, w_{n-1}]$ — $(n-1)$-мерный симплекс барицентрического подразбиения грани $[v_0, \dots, \hat{v}_i, \dots, v_n]$.

- Индукция начинается с $n = 0$, когда барицентрическое подразбиение точки $[v_0]$ определяется просто, как сама точка $[v_0]$.
- В случае $n = 1$ отрезок $[v_0 v_1]$ бьется на два отрезка $[v_0 b]$, $[b v_1]$, где b — середина отрезка $[v_0, v_1]$.
- В случае $n = 2$ треугольник $[v_0 v_1 v_2]$ бьется на 6 труегольников, образуемых его вершинами и точкой пересечения медиан b.

Из такого индуктивного определения следует, что вершины симплексов в барицентрическом подразбиении симплекса $[v_0 \dots v_n]$ — в точности барицентры всех k-мерных граней $[v_{i_0} \dots v_{i_k}]$ симплекса $[v_0 \dots v_n]$ для $0 \le k \le n$.

При $k = 0$ это даёт нам просто набор вершин v_i. Барицентр симплекса $[v_{i_0} \dots v_{i_k}]$ имеет барицентрические координаты $t_i = \frac{1}{k+1}$ при $i = i_0, \dots, i_k$ и $t_i = 0$ во всех остальных случаях.

Замечание. Далее нам это не потребуется, но симплексы барицентрического подразбиения задают на симплексе T структуру симплициального комплекса.

Лемма 4 (О барицентрическом подразбиении)**.** Пусть $f\colon T^q \to X$ — сингулярный симплекс. Тогда его барицентрическое поразбиение — это

$$\beta\colon C_q(X) \to C_q(X), \quad \beta f = \sum_{\tau \in S_{q+1}} \operatorname{sign}(\tau) f_\tau,$$

где f_τ определяется следующим образом: исходный симплекс T^q мы можем барицентрически подразбить на симплексы $T'_q = \{x \mid x_{\tau(0)} \le x_{\tau(1)} \le \dots \le x_{\tau(q)}\}$, в которых вершины нумеруются согласно размерностям граней. Тогда мы полагаем $f_\tau \stackrel{\text{def}}{=} f|_{T'_q}$.

Тогда $\partial\beta = \beta\partial$ и $\beta_*([\alpha]) = [\alpha]\ \forall [\alpha] \in H_q(X)$. Иными словами, барицентрическое подразбиение не влияет на гомологический класс.

Доказательство. Для первого утверждения достаточно проверить, что в сумме все внутренние грани встречаются с противоположным знаком, это ясно из картинки. Первое утверждение даёт нам, что $\beta \in \operatorname{Hom}_{\mathfrak{Ch}}(C_\bullet, C_\bullet)$.

Для доказательства второго утверждения мы построим цепную гомотопию $D\colon C_q(X) \to C_{q+1}(X)$ между β и постоянным отображением.

Пусть $f\colon T^q \to X$, тогда $D(f)$ определяется следующим образом: барицентрически разобьем призму $I \times T^q$ на симплексы и рассмотрим проекцию

$$p\colon I \times T^q \to T^q.$$

Тогда $D(f)$ — это $(q+1)$-мерный сингулярный симплекс, являющийся суммой композиций f и проекции p, суженной на симплексы в разбиении $I \times T^q$.

можно нарисовать картинку для отрезка, в принципе.

Из того, как устроена нумерация в барицентрическом разбиении призмы, нетрудно видеть, что D — гомотопия между β и id, то есть

$$f - \beta(f) = D\partial(f) + \partial D(f).$$

Чтоб понять всё это, надо опять позалипать на эту картиночку с призмой, как в теореме 3.[6] □

[6] Возможно, всё это место стоит строго формально переписать из Хачтера.

Следующая лемма говорит нам, что для вычисления сингулярных гомологий достаточно рассматривать лишь *маленькие* сингулярные симплексы. В случае симплициальных гомологий это можно было бы формулировать в терминах диаметров, а в случае сингулярных мы будем говорить об этом в терминах покрытий.

Лемма 5 (Об измельчении)**.** Пусть $\mathcal{U} = \{U_\alpha\}$ — конечное открытое покрытие X. Пусть $C_q^{\mathcal{U}}(X)$ порождено сингулярными симплексами $f \in C_q(X)$ такими, что $\exists \alpha\colon f(T_q) \subset U_\alpha$.

Тогда вложение $i\colon C_q^{\mathcal{U}}(X) \xrightarrow{i} C_q(X)$ индуцирует изоморфизм групп гомологий $H_\bullet(X) \cong H_\bullet^{\mathcal{U}}(X)$.

Доказательство. Заметим, что для достаточно большого n по лемме Лебега $c \in C_q(X) \Rightarrow \beta^n(c) \in C_q^{\mathcal{U}}(X)$. Кроме того, по лемме 4 c и $\beta^n(c)$ гомологичны (то есть, представляют один м тот же класс гомологий). Это даёт нам, что любой гомологический класс мз $H_q(C_\bullet)$ имеет представителя в $C_q^{\mathcal{U}}(X)$, то есть, что отображение $H_q^{\mathcal{U}}(X) \to H_q(X)$ сюръективно.

Кроме того, также по лемме 4, если c — цикл из $C_q^{\mathcal{U}}$, то $c - \beta^n(c)$ — граница цепи из C_{q+1}^U, так как

$$c - \beta^n(c) = \underbrace{D\partial c}_{=0, \text{ так как } c - \text{цикл}} - \partial Dc = \partial(-Dc) \in B_q\big(C_q^{\mathcal{U}}(X)\big).$$

С другой стороны, так как c и $\beta^n(c)$ гомологичны, их разность — граница (элемент $B_q(C_q(X))$). Таким образом, если цепь из $C_q^{\mathcal{U}}$ лежит в $B_q(C_q(X))$, то она лежит и в $B_q\big(C_q^{\mathcal{U}}(X)\big)$. Это даёт нам инъективность отображения $H_q^{\mathcal{U}}(X) \to H_q(X)$. □

Замечание. Заметим, что построенные в доказательстве отображения переводят цепи в A в цепи в A, а значит, выдерживают факторизацию по A. Этот факт даёт нам версию леммы об измельчении для относительных гомологий, которым мы и будем пользоваться.

Обзаведемся еще одним полезным фактом: Посмотрим на такой факт из гомологической алгебры:

Лемма 6 (5-лемма)**.** Рассмотрим диаграмму

$$\begin{array}{ccccccccc} A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & E \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\ A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & E' \end{array}$$

в которой строки точны, f_2, f_4 — изоморфизмы, f_1 — эпиморфизм, f_5 — мономорфизм. Тогда f_3 — изоморфизм.

Доказательство. Есть в любом курсе гомологической алгебры. □

Из неё немедленно следует следующий простой факт:

Лемма 7. Если пара (X, A) гомотопически эквивалентна паре (Y, B), то $H_\bullet(X, A) = H_\bullet(Y, B)$.

Доказательство. Запишем длинную точную последовательность для обоих пар:

$$\begin{array}{ccccccccc} H_k(A) & \longrightarrow & H_k(X) & \longrightarrow & H_k(X, A) & \longrightarrow & H_{k-1}(A) & \longrightarrow & H_{k-1}(X) \\ \| & & \| & & \downarrow & & \| & & \| \\ H_k(B) & \longrightarrow & H_k(Y) & \longrightarrow & H_k(Y, B) & \longrightarrow & H_{k-1}(B) & \longrightarrow & H_{k-1}(Y) \end{array}$$

Тогда всё следует из 5-леммы 6 □

Наконец, мы можем доказать интересующую нас теорему:

Теорема 7. *В общем случае отображение $X \to X \cup CA$ индуцирует изоморфизм*

$$H_q(X, A) \to H_q(X \cup CA, CA) = H_q(X \cup CA, a) = \widetilde{H}_q(X \cup CA),$$

где a — вершина конуса.

Если (X, A) — пара Борсука, то отображение проекции $p\colon X \to X/A,\ A \mapsto a$ индуцирует изоморфизм

$$H_q(X, A) \xrightarrow{p_*} H_q(X/A, a) = \widetilde{H}_q(X/A).$$

Доказательство. Рассмотрим открытое покрытие $X \cup CA$ вида:

$$X \cup CA \subset ((X \cup CA) \setminus X) \cup (X \cup \overline{C}A), \quad \mathcal{U} \stackrel{\text{def}}{=} \{(X \cup CA) \setminus X, (X \cup \overline{C}A)\}$$

где $\overline{C}A$ — нижняя открытая половина конуса CA.

По лемме 5 об измельчении мы вместо $H_q(X \cup CA, CA)$ можем рассматривать $H_q^{\mathcal{U}}(X \cup CA, CA)$.

А теперь, заметим, что по тому, как мы взяли покрытие,

$$C_q^{\mathcal{U}}(X \cup CA, CA) = C_q^{\mathcal{U}}(X \cup CA)/C_q^{\mathcal{U}}(CA) = C_q\big(X \cup \overline{C}A\big)/C_q\big(\overline{C}A\big) = C_q\big(X \cup \overline{C}A, \overline{C}A\big).$$

А значит, из гомотопической эквивалентности и леммы 7 мы имеем

$$H_q(X \cup CA, CA) = H_q(X \cup \overline{C}A, \overline{C}A) = H_q(X, A).$$

Вторая часть первого равенства из условия теоремы следует из следствия 3.

Пусть теперь (X, A) — пара Борсука. Тогда по утверждению 2 $X \cup CA \sim X/A$, а значит, $H_q(X, A) \cong \widetilde{H}_q(X/A)$. □

1.8 Вырезание

Рассмотрим тройку $B \subset A \subset X$. Тогда вложение индуцирует отображение

$$H_k(X - B, A - B) \to H_k(X, A).$$

Вообще говоря, вырезание даёт хорошую технику вычисления относительных гомологий:

Теорема 8 (О вырезании). *Пусть даны пространства $Z \subset A \subset X$, причем $\mathrm{Cl}(Z) \subset \mathrm{Int}(A)$. Тогда вложение $(X - Z, A - Z) \hookrightarrow (X, A)$ индуцирует изоморфизмы*

$$H_n(X - Z, A - Z) \cong H_n(X, A)$$

для всех n. Или, что эквивалентно: для подпространств $A, B \subset X$, внутренности которых покрывают X, включение $(B, A \cap B) \hookrightarrow (X, A)$ индуцирует изоморфизмы

$$H_n(B, A \cap B) \cong H_n(X, A) \quad \forall n.$$

Доказательство. Докажем сначала эквивалентность формулировок. Положим $B = X - Z,\ Z = X - B$. Тогда $A \cap B = A - Z$, а условие $\mathrm{Cl}(Z) \subset \mathrm{Int}(A)$ эквивалентно тому, что $X = \mathrm{Int}(A) \cup \mathrm{Int}(B)$, так как $X - \mathrm{Int}(B) = \mathrm{Cl}(Z)$. Теперь докажем вторую формулировку.

Пусть $X = A \cup B$, обозначим соотвествующее покрытие $\mathcal{U} = \{A, B\}$. Для краткости будем обозначать группы $C_n^{\mathcal{U}}(X)$, как $C_n(A + B)$[7].

Тогда, как мы помним из леммы об измельчении 5 включение

$$C_n(A + B)/C_n(A) \hookrightarrow C_n(X)/C_n(A)$$

индуцирует изоморфизм групп гомологий $H_n(A + B, A) \cong H_n(X, A)$.

Теперь рассмотрим включение

$$C_n(B)/C_n(A \cap B) \hookrightarrow C_n(A + B, A).$$

Оно очевидно индуцирует изоморфизм гомологий, так как обе факторгруппы свободные, а их базис — n-мерные сингулярные симплексы в B, не лежащие в A. Значит, мы получили требуемый изоморфизм

$$H_n(B, A \cap B) \cong H_n(A + B, A) \cong H_n(X, A).$$

□

[7] что на самом деле логично, так как цепи оттуда состоят из суммы цепей из A и цепей из B

1.9 Точная последовательность Майера-Вьеториса

Кроме длинной точной последовательности пары (теорема 4) для вычисления гомологий пары (X, A) есть и другая мощная техника для вычисления гомологий пространства X, тоже представляющая собой длинную точную последовательность.

Теорема 9 (Точная последовательность Майера-Вьеториса, простая версия)**.** *Пусть $X = A \cup B$, где A, B — открытые и $A \cap B = C \neq \varnothing$. Тогда имеет место следующая точная последовательность:*

$$\dots H_q(A \cap B) \to H_q(A) \oplus H_q(B) \to H_q(X) \to H_{q-1}(A \cap B) \to H_{q-1}(A) \oplus H_{q-1}(B) \to \dots$$

Доказательство. Рассмотрим короткую точную последовательность комплексов:

$$0 \to C_\bullet(A \cap B) \xrightarrow[\varphi]{c \to (c,-c)} C_\bullet(A) \oplus C_\bullet(B) \xrightarrow[\psi]{(a,b) \to a+b} C_\bullet(A + B) \to 0$$

Во-первых, заметим, что $\operatorname{Ker} \varphi = 0$, так как цепь в $A \cap B$, которая является нулевой в A (или в B) должна быть нулевой цепью. Во-вторых, очевидно, что $\psi\varphi = 0 \Rightarrow \operatorname{Im} \varphi \subset \operatorname{Ker} \psi$. Заметим, что для $(x, y) \in C_n(A) \oplus C_n(B)$ имеем $x + y = 0 \Rightarrow y = -x$, а значит $x \in C_n(A \cap B)$ и $(x, y) \in \operatorname{Im} \varphi$. Это означает, что $\operatorname{Ker} \psi \subset \operatorname{Im} \varphi$. Точность в последнем члене следует просто из определения $C_n(A + B)$.

Тогда эта короткая точная последовательность комплексов даёт нам точную последовательность гомологий. Остается лишь заметить, что также, как и в теореме о вырезании, $H_\bullet(A + B) = H_\bullet(A \cup B)$. □

Замечание. Эта не самая хорошая версия точной последовательности Майера-Вьеториса, так как условие на открытое покрытие серьезно мешает.

1.10 Гомологии сфер

Теорема 10. *Для $n \neq 0$ гомологии сферы устроены следующим образом:*

$$H_i(S^n) \cong \begin{cases} \mathbb{Z}, & i = n \text{ или } i = n, \\ 0, & \text{иначе.} \end{cases}$$

Или, иными словами,

$$\widetilde{H}_i(S^n) \cong \begin{cases} \mathbb{Z}, & i = n \\ 0, & \text{иначе.} \end{cases}$$

Доказательство. Рассмотрим пару $(X, A) = (D^n, S^{n-1})$, тогда $X/A \cong S^n$. Запишем для этой пары точную послеоватнльность приведенных гомологий:

$$\dots \to \widetilde{H}_q(D^n) \to \widetilde{H}_q\big(D^n, S^{n-1}\big) \to \widetilde{H}_{q-1}\big(S^{n-1}\big) \to \widetilde{H}_{q-1}(D^n) \to \dots$$

Так как D^n стягиваем, $\widetilde{H}_q(D^n) = 0$, а значит, $H_q\big(D^n, S^{n-1}\big) \cong H_{q-1}(S^n)$. С другой строны, так как $(D^n, \partial D^n) = (D^n, S^{n-1})$ — пара Борсука, по теореме о факторизации 7

$$H_q\big(D^n, S^{n-1}\big) \cong \widetilde{H}_q\big(D^n / S^{n-1}\big) \cong \widetilde{H}_q(S^n).$$

Остается замеить, что мы знаем, что утверждение верно для S^0. Таким образом, мы доказали утверждение по индукции. □

Следствие 7. *Сферы разных размерностей негомеоморфны.*

1.11 Гомологии букета и надстройки

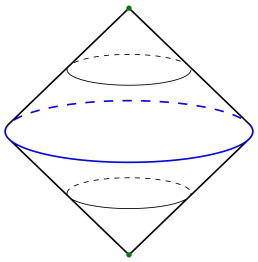
Из стягиваемости конуса сразу следует, что $H_q(CX, X) \cong \widetilde{H}_q(X)$ (достаточно написать точную последовательность для приведенных гомологий).

Определение 12. Пусть X — топологическое пространство. Тогда *надстройкой* над X называется пространство ΣX, определённое, как

$$\Sigma X \cong X \times I/\sim, \text{ где } (x,0) \sim (y,0)\ \forall x,y \in X \text{ и } (x,1) \sim (y,1)\ \forall x,y \in X.$$

Иными словами, мы взяли $X \times I$ и стянули $X \times 1$ и $X \times 0$ в точку.

Пример 5. Надстройка над окружностью выглядит следующим образом:



Так как надстройка получается факторизацией конуса по нижнему основанию, из теоремы о факторизации 7 следует, что $H_{q+1}(CX, X) \cong \widetilde{H}_{q+1}(\Sigma X)$. Таким образом, мы получили такое утверждение:

Теорема 11 (Гомологии надстройки)**.** *Справедливо следующее равенство групп гомологий:*

$$\widetilde{H}_q(X) \cong \widetilde{H}_{q+1}(\Sigma X)$$

Замечание. Так как $\Sigma S^n = S^{n+1}$, мы таким образом получили другое доказательство теоремы 10.

Теорема 12 (Гомологии букета)**.** *Для букета пространств $\bigvee_\alpha X_\alpha$ включения $i_\alpha \colon X_\alpha \hookrightarrow \bigvee_\alpha X_\alpha$ индуцируют изоморфизм гомологий*

$$\bigoplus_\alpha \widetilde{H}_q \cong \widetilde{H}_q\left(\bigvee_\alpha X_\alpha\right).$$

при условии, что если в букете отождествляются точки $\{x_\alpha\}$, то пары (X_α, x_α) — пары Борсука.

Доказательство. Достаточно рассмотреть пару

$$(X, A) = \left(\bigsqcup_\alpha X_\alpha, \bigsqcup_\alpha x_\alpha\right),$$

тогда по тривиальным причинам

$$H_n(X, A) \cong \bigoplus_\alpha \widetilde{H}_n(X_\alpha)$$

и по теореме о факторизации

$$H_n(X, A) \cong \widetilde{H}_n\left(\bigvee_\alpha X_\alpha\right).$$

□

1.12 Гомологии с коэффициентами

У рассматриваемой нами до сих пор теории гомологий есть простое обобщение, котрое иногда даёт техническое преимущество.

Обобщение состоит в рассмотрении цепей $\sum n_i f_i$, где f_i — сингулярные симплексы, а коэффициенты n_i берутся в фиксированной абелевой группе G. Такие n-мерные цепи образуют абелеву группу $C_n(X;G)$ и у неё также есть относительная версия $C_n(X,A;G) \stackrel{\text{def}}{=} C_n(X;G)/C_n(A;G)$.

Дифференциал δ строится также, как и раньше:

$$\partial\left(\sum_i n_i f_i\right) = \sum_{i,j}(-1)^j n_i \Gamma_j f_i.$$

Соотвественно, группы $C_n(X;G)$ и $C_n(X,A;G)$ образуют цепные комплексы и их гомологии обозначают $H_n(X;G)$ и $H_n(X,A;G)$ и называют *гомологиями с коэффициентами в группе G*.

Приведённые группы гомологий $\widetilde{H}(X;G)$ определяются аналогично, аугументация задаётся, как

$$\ldots \to C_0(X;G) \xrightarrow{\varepsilon} G \to 0, \quad \varepsilon\left(\sum_i n_i f_i\right) = \sum_i n_i.$$

Замечание. Часто полезно рассматривать гоиологии с коэффициентами в $\mathbb{Z}/2\mathbb{Z}$, так как нужно считать суммы сингулярных симплексов с коэффициентами 0 и 1, поэтому, отбрасывая члены с коэффициентами 0, можно представлять себе цепи, как конечные «объединения» сингулярных симплексов.

Кроме того, можно больше не заботиться о знаках в формуле для границы, а так как знаки являются алгебраическим выражением ориентации, мы можем игнорировать и ориентации. Это означает, что гомологии с коэффициентами в $\mathbb{Z}/2\mathbb{Z}$ — наиболее естественный инструмент для вычислений в неориентируемом случае.

Отметим, что вся доказанная выше теория переносится на гомологии с коэффициентами в G без проблем и различия между $H_n(X;G)$ и $H_n(X)$ появляются только, когда начинаются вычисления.

Пример 6. Если $X = *$ — точка, то нетрудно заметить, что

$$H_n(*;G) \cong \begin{cases} G, & n = 0 \\ 0, & \text{иначе} \end{cases}$$

Аналогично и в случае сфер S^k мы имеем

$$\widetilde{H}_n(S^k;G) \cong \begin{cases} G, & n = k \\ 0, & \text{иначе} \end{cases}$$

1.13 Приложения теории гомологий

Теорема 13 (Борсук)**.** *Не существует ретракции диска на граничную сферу.*

Доказательство. Предположим, что ретракция $f\colon D^n \to S^{n-1}\colon f$ — непрерывное и $f|_{S^{n-1}} = \mathrm{id}$ существет. Рассмотрим отображение $i\colon S^{n-1} \hookrightarrow D^n$, тогда в гомологиях у нас есть отображение

$$H_{n-1}(S^{n-1}) \xrightarrow{i_*} H_{n-1}(D^n) \xrightarrow{f_*} H_{n-1}(S^{n-1})$$

или, подставляя известные нам результаты:

$$\mathbb{Z} \xrightarrow{i_*} 0 \xrightarrow{f_*} \mathbb{Z}.$$

Так как $f \circ i = \mathrm{id}$, $f_* \circ i_* = \mathrm{id}_* = \mathrm{id}$ и мы приходим к противоречию. □

Теорема 14 (Брауэр, о неподвижной точке). *Пусть $f\colon D^n \to D^n$ — непрерывное отображение. Тогда у него существует неподвижная точка.*

Доказательство. Предположим противное, пусть существует непрерывное $f\colon D^n \to D^n$, не имеющее неподвижных точек. Рассмотрим отображение g, которое переводит $x \in D^n$ в точку пересечения $[f(x), x)$ и ∂D^n. То есть, $g\colon D^n \to \partial D^n$ и $g|_{\partial D^n} = \mathrm{id}$. Тогда g — ретракция D^n на граничную сферу, а этого не бывает по теореме 13. □

Теорема 15 (Брауэр, инвариантность размерности). *Если непустые открытые $U \subset \mathbb{R}^m$, $V \subset \mathbb{R}^n$ открытые и они гомеоморфны, то $m = n$.*

Доказательство. Пусть h — гомеоморфизм $U \to V$, тогда

$$H_k(U, U - x) \cong H_k(V, V - h(x)).$$

По теореме о вырезании 8 для $(X, A) = (\mathbb{R}^m, \mathbb{R}^m - x)$ и $Z = \mathbb{R}^m - U$:

$$H_k(\mathbb{R}^m, \mathbb{R}^m - x) \cong H_k(U, U - x).$$

Тогда мы имеем, что

$$H_k(\mathbb{R}^m, \mathbb{R}^m - x) \cong H_k(\mathbb{R}^n, \mathbb{R}^n - h(x)).$$

Из точной последовательности пары для $(\mathbb{R}^m, \mathbb{R}^m - x)$ мы имеем:

$$\ldots \to H_k(\mathbb{R}^m) \to H^k(\mathbb{R}^m, \mathbb{R}^m - x) \to H_{k-1}(\mathbb{R}^m - x) \to H_{k-1}(\mathbb{R}^m) \to \ldots$$

$$\ldots 0 \to H^k(\mathbb{R}^m, \mathbb{R}^m - x) \to H_{k-1}(\mathbb{R}^m - x) \to 0 \to \ldots,$$

а значит, $H_k(\mathbb{R}^m, \mathbb{R}^m - x) \cong H_{k-1}(\mathbb{R}^m - x) \cong H_{k-1}(S^{m-1})$, так как $\mathbb{R}^m - x$ деформационно ретрагируется на S^{m-1}. Значит, мы получили

$$H_{k-1}(S^{m-1}) \cong H_{k-1}(S^{n-1}),$$

откуда ясно, что $m = n$. □

1.14 Симплициальные комплексы

Этот парагарф надо написать из Хатчера.

1.15 Эквивалентность симплициальных и сингулярных гомологий

Образующая $H_n(S^n)$:

В этом параграфе будем обозначать n-мерный симплекс, как Δ^n. Заметим, что так как $\Delta^n/\partial\Delta^n \cong S^n$, по теореме о факторизации 7 мы имеем изоморфизм

$$H_n(S^n) \cong H_n(\Delta^n, \partial\Delta^n).$$

Покажем, что образующая $H^n(S^n)$ — это отображение $\Delta^n \xrightarrow{\mathrm{id}} \Delta^n$. Нетрудно заметить, что $\mathrm{Im}(\partial f) \subset \partial\Delta^n$, что дает нам, что id вообще представляет какой-то гомологический класс в $H_n(\Delta^n, \partial\Delta^n)$.

Рассмотрим тройку $(\Delta^n, \partial\Delta^n, \Lambda)$, где Λ — это $\partial\Delta^n$ без одной из граней (например, запоолненный треугольник, граница треугольника и граница треугольника без стороны). Напишем точную последовательность тройки:

$$\ldots \to H_n(\partial\Delta^n, \Lambda) \to H_n(\Delta^n, \Lambda) \to H_n(\Delta^n, \partial\Delta^n) \to H_{n-1}(\partial\Delta^n, \Lambda) \to H_{n-1}(\Delta^n, \Lambda) \to \ldots$$

Заметим, что так как Δ^n деформационно ретрагируется на Λ, $H_n(\Delta^n, \Lambda) \cong H_n(\Lambda, \Lambda) = 0$ и то же самое справедливо для $(n-1)$-х гомологий. То есть, наша последовательность на самом деле имеет вид

$$\ldots \to 0 \to H_n(\Delta^n, \partial\Delta^n) \to H_{n-1}(\partial\Delta^n, \Lambda) \to 0 \to \ldots$$

Теперь заметим, что если грань, которую мы выкинули, мы обозначим за Δ', то $H_{n-1}(\partial\Delta^n, \Lambda) \cong H_{n-1}(\Delta', \partial\Delta')$.

Это ценно, так как далее мы можем рассуждать по индукции, ведь если образующая $H_{n-1}(\Delta', \partial\Delta')$ — вложение выкинутой нижней грани Δ', то её прообраз в $H_n(\Delta^n, \partial\Delta^n)$ —- нужное нам тождественное отображение (мы тут пользуемся тем, что мы знаем, что связывающий гомоморфизм в длинной точной последовательности пары/тройки – это просто взятие границы). А для S^0 это утверждение очевидно.

Обозначим симплиаицльные гомологии пространства X за $H_k^\Delta(X)$.

Теорема 16. *Пусть X — конечный симплициальный комплекс. Тогда*

$$H_k^{\text{sing}}(X) \cong H_k^\Delta(X).$$

Доказательство. Пусть X^k — объединение всех симплексов в симплициальном комплексе до размерности k (обозначение аналогично обозначению для CW-комплексов). Напишем точную последовательность пары:

$$\ldots \to H_{n+1}^\Delta\left(X^k, X^{k-1}\right) \to H_n^\Delta\left(X^k\right) \to H_n^\Delta\left(X^k\right) \to H_n^\Delta\left(X^k, X^{k-1}\right) \to \ldots$$

и заметим, что $H_{n+1}^\Delta\left(X^k, X^{k-1}\right) \cong H_{n+1}\left(X^k, X^{k-1}\right) \cong H_{n+1}\left(\bigvee S^k\right)$. Действительно, ясно, что

$$H_{n+1}\left(X^k, X^{k-1}\right) \cong H_{n+1}\left(\bigvee_\alpha S^k\right),$$

где α пробегает k-мерные симплексы в X. Далее,

$$H_{n+1}\left(\bigvee_\alpha S^k\right) \cong \begin{cases} 0, & \text{если } n+1 \neq k \\ \bigoplus_\alpha \mathbb{Z}, & n+1 = k \end{cases}$$

С другой стороны, из определения симплициальных гомологий ясно, что при $n+1 \neq k$ мы имеем $H_{n+1}^\Delta\left(X^k, X^{k-1}\right) \cong 0$, а при $n+1 = k$ эта группа — свободная абелева группа, порожденная всеми k-мерными симплексами в X, то есть, как и в предыдущем случае

$$H_k^\Delta\left(X^k, X^{k-1}\right) \cong \bigoplus_\alpha \mathbb{Z}.$$

Остается заметить, что по доказанному в начале параграфа, мы знаем, что у $H_k\left(\bigvee_\alpha S^k\right)$ такой же набор порождающих.

Теперь будем вести индукцию по размерности симплициального комплекса. По индукционному предположению мы имеем $H_n^\Delta(X^{k-1}) \cong H_n(X^{k-1})$ и тогда мы получаем диаграмму из 5-леммы:

$$\begin{array}{ccccccc} H_{n+1}^\Delta\left(X^k, X^{k-1}\right) & \longrightarrow & H_n^\Delta\left(X^{k-1}\right) & \longrightarrow & H_n^\Delta\left(X^k\right) & \longrightarrow & H_n\left(X^k, X^{k-1}\right) \\ \| & & \| & & \downarrow & & \| \\ H_{n+1}\left(X^k, X^{k-1}\right) & \longrightarrow & H_n\left(X^{k-1}\right) & \longrightarrow & H_n\left(X^k\right) & \longrightarrow & H_n\left(X^k, X^{k-1}\right) \end{array}$$

□

1.16 Степень отображения

Определение 13. Пусть $f\colon S^n \to S^n$ — непрерывное отображение. Тогда оно индуцирует морфизм в гомологиях:

$$f_*\colon H_n(S^n) \to H_n(S^n).$$

Так как f_* — гомоморфизм бесконечной циклической группы в себя, он должен иметь вид

$$f_*(\alpha) = d \cdot \alpha$$

для некоторого фиксированного $d \in \mathbb{Z}$, зависящего только от f. Это число называют *степенью отображения* f и обозначают $\deg f$.

Базовые свойства степени.

1. $\deg \mathrm{id}_{S^n} = 1$.
2. Если f — не сюръекция, то $\deg f = 0$, так как мы можем выбрать $x \in S^n \setminus f(S^n)$ и представить f в виде композиции
$$S^n \to S^n \setminus \{x\} \hookrightarrow S^n,$$
а пространство $S^n \setminus \{x\}$ — стягиваемо, значит $H_n(S^n \setminus \{x\}) = 0$, а значит и $f_* = 0$.
3. Если $f \sim g$, то $\deg f = \deg g$.
4. $\deg f \circ g = \deg f \cdot \deg g$.
5. Если f — гомотопическая эквивалентность, то существует g такое, что $f \circ g \sim \mathrm{id} \Rightarrow \deg f \deg g = 1 \Rightarrow \deg f = \pm 1$.
6. Рассмотрим f, которое тождественно действует на первых n координатах и отправляет x_{n+1} в $-x_{n+1}$. Тогда $\deg f = -1$. Действительно, мы модем реализовать сферу, как склейку двух симплексов Δ^n_1 и Δ^n_2 по границе. Тогда n-мерная цепь $\Delta^n_1 - \Delta^n_2$ являются образующей n-мерных гомологий, а отображение f переставляет местами Δ^n_1 и Δ^n_2, то есть действует на образующую умножением на -1.
7. Степень антиподального отображения: $\deg(x \mapsto -x) = (-1)^{n+1}$
8. Если $f\colon S^n \to S^n$ не имеет неподвижных точек, то $f \sim (x \mapsto -x)$ и соответственно $\deg f = (-1)^{n+1}$. Действительно, если $f(x) \neq x$, то отрезок с концами $f(x)$ и $-x$, который задаётся, как
$$t \mapsto (1-t)f(x) - tx,\ 0 \leq t \leq 1,$$
не проходит через начало координат и формула
$$H(t,x) = \frac{(1-t)f(x) - tx}{\|(1-t)f(x) - tx\|}$$
определяет гомотопию $f(x)$ в постоянное отображение.

Теорема 17 (О причёсывании ежа)**.** *S^n допускает непрерывное ненулевое (касательное) векторное поле тогда и только тогда, когда n — нечетно.*

Доказательство. Предположим, что $x \mapsto V(x)$ — непрерывное поле касательных векторов к сфере. Тогда, если рассматривать вектор $V(x)$, как вектор в начале координат, а не в точке касания, то условие касания означает просто, что $x \perp V(x)$. Если $V(x) \neq 0$, то мы можем нормализовать веторное поле так, что $\|V(X)\| = 1\ \forall x$, тогда векторы
$$(\cos t)x + (\sin t)V(x)$$
лежат на единичной окружности в $\mathrm{span}(x, V(x))$. Соотвественно, при $t \in [0, \pi]$ мы получаем гомотопию тождественного отображения id_{S^n} в антиподальное отображение:
$$H(t,x) = (\cos t)x + (\sin t)V(x).$$
Отсюда следует, что $(-1)^{n+1} = 1$, а значит, n должно быть нечетно. С другой стороны, когда $n = 2k-1$, мы можем положить
$$V(x_1, x_2, \ldots, x_{2k-1}, 2k) = (-x_2, x_1, \ldots, -x_{2k}, x_{2k+1})$$
и это даст нам искомое векторное поле. □

Опишем теперь метод вычисления, который чаще всего применим на практике. Пусть $f\colon S^n \to S^n$ и существует $y \in S^n$ такое, что $f^{-1}(y) = \{x_1, \ldots, x_k\}$, $U_1, \ldots, U_k$ — непересекающиеся окрестности этих точек, которые f переводит в окрестность V точки y. Тогда $f(U_i \setminus x_i) \subset V \setminus y$ и мы имеем коммутативную диаграмму:

$$\begin{array}{ccccc}
 & & H_n(U_i, U_i \setminus \{x_i\}) & \xrightarrow{f_*} & H_n(V, V \setminus \{y\}) \\
 & \nearrow\!\!\nearrow & \downarrow{\scriptstyle k_i} & & \| \\
H_n(S^n, S^n \setminus \{x_i\}) & \xleftarrow[p_i]{} & H_n\left(S^n, S^n \setminus f^{-1}(y)\right) & \xrightarrow{f_*} & H_n(S^n, S^n \setminus \{y\}) \\
 & \searrow\!\!\searrow & \uparrow{\scriptstyle j} & & \| \\
 & & H_n(S^n) & \xrightarrow{\qquad f_* \qquad} & H_n(S^n)
\end{array}$$

Все отображения на ней индуцируются включениями. Два ихоморфизма в верхней части диаграммы получаются из теоремы о вырезании 8, а два в нижней — из точной последовательности пары 4.

Посредством этих четырех гомоморфизмов две верхние группы можно отождествить с $\mathbb{Z}$, тогда верхний гомоморфизм f_* становится умножением на число и это число мы будем называть *локальной степенью* отображения f и обозначать $\deg f|_{x_i}$.

Теорема 18 (Локальность степени)**.** *Пусть $f\colon S^n \to S^n$ и $y \in S^n$ таково, что $f^{-1}(y) = \{x_1, \dots, x_k\}$. Тогда*

$$\deg f = \sum_i \deg f|_{x_i}.$$

Доказательство. По теореме о выразании 8, группа $H_n\left(S^n, S^n \setminus f^{-1}(y)\right)$ — прямая сумма групп $H_n(U_i, U_i \setminus \{x_i\})$, причем k_i — отображение включения i-го слагаемого, а p_i — проекция на i-е слагаемое. Из коммутативности нижнего треугольника мы получаем, что

$$p_i \circ j(1) = 1,$$

а значит, $j(1) = (1, \dots, 1) = \sum_i k_i(1)$. Коммутативность верхнего квадрата говорит, что f_* отображает $k_i(1)$ в $\deg f|_{x_i}$, а коммутативность нижнего квадрата уже дает нам формулу

$$\deg f = \sum_i \deg f|_{x_i}.$$

□

1.17 Клеточные гомологии

Лемма 8. Пусть X — конечный CW-комплекс. Тогда:

a) $H_k\left(X^n, X^{n-1}\right) = 0$, если $k \neq n$ и изоморфно мвободной абелевой группе, если $k = n$. Образующие этой группы — клетки размерности n.
b) $H_k(X^n) = 0$, если $k > n$. В частности, если комплекс конечномерен, то $H_k(X) = 0\ \forall k > \dim X$.
c) Вложение $i\colon X^n \hookrightarrow X$ индуцирует изоморфизм $i_*\colon H_k(X^n) \to H_k(X)$ при $k < n$ и эпиморфизм при $k = n$.

Доказательство. Во-первых, мы знаем, что $\left(X^n, X^{n-1}\right)$ — пара Борсука. Кроме того, $X^n/X^{n-1} \cong \bigvee_\alpha S^n$, где α пробегает все n-мерные клетки. Тогда факт a) следует из теоремы о факторизации 7 и теоремы 12.

Теперь рассмотрим длинную точную последовательность пары

$$\dots \to H_{k+1}\left(X^n, X^{n-1}\right) \to H_k\left(X^{n-1}\right) \to H_k(X^n) \to H_k\left(X^n, X^{n-1}\right) \to \dots.$$

Если $k \neq n$ или $n-1$, то обе внешние группы равны нулю, как группы гомологий букета n-мерных сфер, поэтому мы получаем изоморфизм

$$H_k\left(X^{n-1}\right) \cong H_k(X^n), \quad k \neq n, n-1.$$

Тогда, если $k > n$, то

$$H_k(X^n) \cong H_k\left(X^{n-1}\right) \cong \dots H_k\left(X^0\right) = 0,$$

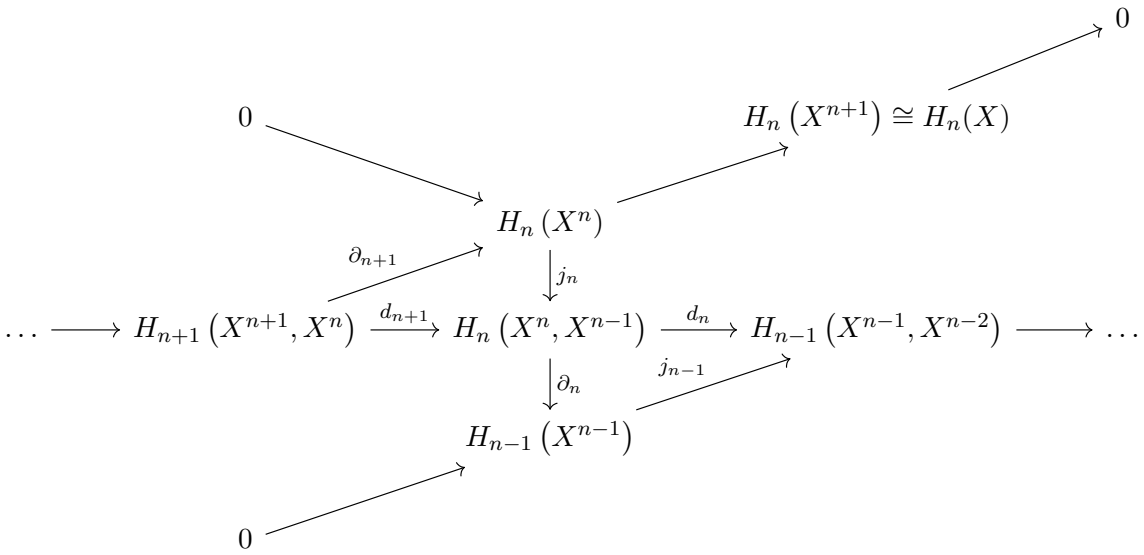
что доказывает пункт b). Если же $k < m$, то тогда

$$H_k(X^n) \cong H_k\left(X^{n+1}\right) \cong \dots \cong H_k\left(X^{n+m}\right)\ \forall m \geq 0,$$

что доказывает c) в случае конечномерного комплекса. □

Замечание. Утверждение c) верно и для бесконечномерных CW-комплкесов (идея состоит в том, что каждая сингулярная цепь имеет компактный образ, а значит пересекается лишь с конечным числом клеток). (Доказательство можно посмотреть в Хатчере).

Теперь мы определим клеточные гомологи — более продвинутый способ вычислять гомологии клеточных пространств. Начнем с такой коммутативной диаграммы:



Её мы получили из точных последовательностей для пар $\left(X^{n+1}, X^n\right)$, $\left(X^n, X^{n-1}\right)$, $\left(X^{n-1}, X^{n-2}\right)$. Морфизмы в нижней строчке определяются, как $d_{n+1} \stackrel{\text{def}}{=} j_n \circ \partial_{n+1}$. Нетрудно заметить, что из точности мы получаем $d_n \circ d_{n+1} = 0$. Таким образом, средняя строчка диаграммы является цепным комплексом (его называют *клеточным цепным комплексом для* X). Как мы уже замечали в доказательстве леммы выше, группа $H_n\left(X^n, X^{n-1}\right)$ — свободная абелева группа с базисом из n-мерных клеток в X.

Определение 14. Рассмотрим построенный выше цепной комлекс с группой k-мерных цепей $C_k^{\mathrm{CW}}(X) \stackrel{\text{def}}{=} H_k\left(X^k, X^{k-1}\right)$. Гомологии этого комплекса называют *клеточным гомологиями пространства* X и обозначают $H_n^{\mathrm{CW}}(X)$.

Замечание. В самом деле, всё происходящее вполне логично — в случае симплициальных гомологий мы рассматриваем свободные абелевы группы, порожденные симплексами всех размерностей, а тут — клетками всех размерностей.

Теорема 19. *Пусть X — CW-комплекс. Тогда имеет место изоморфизм $H_n^{\mathrm{CW}}(X) \cong H_n(X)$.*

Доказательство. Из точности и теоремы о гомоморфимзе мы имеем изоморфизм

$$H_n(X) \cong H_n(X^n)/\operatorname{Im}\partial_{n+1}.$$

Так как j_n — инъекция, $\operatorname{Im}\partial_{n+1} \cong \operatorname{Im} j_n \circ \partial_{n+1} = \operatorname{Im} d_{n+1}$. С другой стороны, $\operatorname{Im} j_n \cong \operatorname{Ker}\partial_n$. Из инъективности j_{n-1} мы имеем $\operatorname{Ker}\partial_n \cong \operatorname{Ker} d_n$. Значит, j_n индуцирует изоморфизм факторгруппы:

$$H_n(X) \cong H_n(X^n)/\operatorname{Im}\partial_{n+1} \cong \operatorname{Ker} d_n/\operatorname{Im} d_{n+1}.$$

□

Следствие 8. *Пусть X — CW-комплекс, тогда:*

1. *$H_n(X) \cong 0$, если в X нет n-мерных клеток.*
2. *Если X — CW-комплекс с k клетками размерности n, то группа $H_n(X)$ порождена не более чем k элементами. В самом деле, так как $H_n\left(X^n, X^{n-1}\right)$ — группа с k образующими, у подгруппы $\operatorname{Ker} d_n$ никак не может быть больше образующих, а значит и в факторгруппе $\operatorname{Ker} d_n/\operatorname{Im} d_{n+1}$ тоже.*

3. *Если X — CW-комплекс, у которого нет пар клеток в соседних размерностях, то $H_n(X)$ — свободная абелева группа с базисом из n-мерных клеток.*

Пример 7. Последний пункт следствия 8 применим, например, к $\mathbb{C}\mathrm{P}^n$, так как клеточная структура для $\mathbb{C}\mathrm{P}^n$ имеет по одной клетке каждой четной размерности до $2n$ (действительно, это заметно из того, что $\mathbb{C}\mathrm{P}^n = \mathbb{C}^n \cup \mathbb{C}\mathrm{P}^{n-1}$). Значит, клеточный цепной комплекс для $\mathbb{C}\mathrm{P}^n$ имеет вид:

$$\mathbb{Z} \to 0 \to \mathbb{Z} \to 0 \to \ldots \to 0 \to \mathbb{Z} \to 0$$

Также при помощи этого же факта можно посчитать гомологии $S^n \times S^n$.

Рассмотрим теперь подробнее клеточный оператор границы d_n. При $n = 1$ это легко, так как

$$d_1 \colon H_1\big(X^1, X^0\big) \to H_0\big(X^0\big)$$

и это просто обычное граничное отображение.

В случае, когда комплекс X связен и имеет лишь одну нульмерную клетку, $d_1 = 0$, так как иначе $H_0(X) \neq \mathbb{Z}$. В общем случае формула для клеточного оператора границы имеет следующий вид:

Предложение 4. *Имеет место равенство:*

$$d_n(e_\alpha^n) = \sum_\beta d_{\alpha\beta} e_\beta^{n-1},$$

где $d_{\alpha\beta}$ — степень отображения $S_\alpha^{n-1} \to X^{n-1} \to S_\beta^{n-1}$, которое является композицией отображения приклеивания клетки e_α^n по границе и отображения фаткоризации, стягивающего $X^{n-1} \setminus e_\beta^{n-1}$ в точку.

Доказательство. Для получения этой формулы рассмотрим такую коммутативную диаграмму:

$$\begin{array}{ccccc}
H_n\left(D_\alpha^n, \partial D_\alpha^n\right) & \xrightarrow{\partial} & \widetilde{H}_{n-1}\left(\partial D_\alpha^n\right) & \xrightarrow{\Delta_{\alpha\beta}} & \widetilde{H}_{n-1}\left(S_\beta^{n-1}\right) \\
\downarrow{\scriptstyle \Phi_{\alpha *}} & & \downarrow{\scriptstyle \varphi_{\alpha *}} & & \downarrow{\scriptstyle q_{\beta *}} \\
H_n\left(X^n, X^{n-1}\right) & \xrightarrow{\partial_n} & \widetilde{H}_{n-1}\left(X^{n-1}\right) & \xrightarrow{q_*} & \widetilde{H}_{n-1}\left(X^{n-1}/X^{n-2}\right) \\
& \searrow^{d_n} & \downarrow{\scriptstyle j_{n-1}} & & \downarrow{\scriptstyle \cong} \\
& & H_{n-1}\left(X^{n-1}, X^{n-2}\right) & \xrightarrow{\cong} & H_{n-1}\left(X^{n-2}/X^{n-2}, X^{n-2}/X^{n-2}\right)
\end{array}$$

Проясним, что за стрелки на ней:

- Φ_α — характеристическое отображение клетки e_α^n, φ_α — её отображение приклеивания.
- $q\colon X^{n-1} \to X^{n-1}/X^{n-2}$ — отображение факторизации.
- $q_\beta\colon X^{n-1}/X^{n-2} \to S_\beta^{n-2}$ — стягивание дополнения клетки e_β^{n-1} в точку и отождествление получившейся сферы с $S_\beta^{n-1} = D_\beta^{n-1}/\partial D_\beta^{n-1}$.
- $\Delta_{\alpha\beta} = q_\beta q \varphi_\alpha$.

Отображение $\Phi_{\alpha *}$ переводит образующую $[D_\alpha^n] \in H_n(D_\alpha^n, \partial D_\alpha^n)$ в образующую слагаемого $\mathbb{Z}$ группы $H_n\big(X^n, X^{n-1}\big)$, соответствующего клетке e_α^n (действительно, такие клетки образуют базис $H_n\big(X^n, X^{n-1}\big)$). Коммутативность левой половины диаграммы даёт нам, что

$$d_n(e_\alpha^n) = j_{n-1}\varphi_{\alpha *}\partial[D_\alpha^n].$$

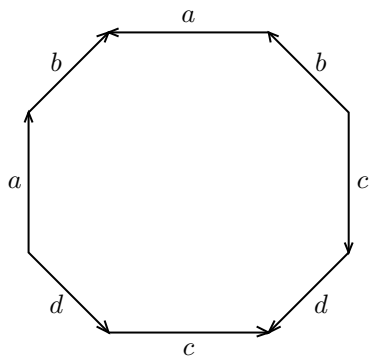
Базис группы $H_{n-1}\big(X^{n-1}, X^{n-2}\big)$ состоит из $(n-1)$-мерных клеток, а отображение $q_{\beta *}$ — это проекция группы $\widetilde{H}_{n-1}\big(X^{n-1}/X^{n-2}\big)$ (которая, как группа гомологий букета окружностей суть прямая сумма $\mathbb{Z}$, где каждое слагаемое соотвествует $(n-1)$-мерной клетке) на её слагаемое $\mathbb{Z}$, соответсвующее e_β^{n-1}.

Теперь формула следует непосредственно из коммутативности правой верхней части диаграммы7 $\square$

1.18 Гомологии поверхностей

В данном параграфе, пользуясь клеточными гомологиями, мы вычислим гомологии поверхностей.

Пусть M_g — компактная ориентируемая поверхность с g ручками. Реализуем её, как склейку $4g$-угольника:



Тогда в её клеточном разбиении:

- 1 двумерная клетка, приклеенная по произведению коммутаторов $[a_1, b_1] \dots [a_g, b_g]$.
- $2g$ одномерных клеток.
- 1 нульмерная клетка.

Значит, цепной клеточный комплекс для M_g будет иметь вид:

$$0 \to \mathbb{Z} \xrightarrow{d_2} \mathbb{Z}^{2g} \xrightarrow{d_1} \mathbb{Z} \to 0$$

Так как комплекс связен и имеет лишь одну нульмерную клетку, $d_1 = 0$. Кроме того, каждое ребро $[a_1, a_2]$, $[a_g, b_g]$ появляется в произведении коммутаторов вместе со своим обратным, а значит, $\Delta_{\alpha\beta}$ гомотопны постоянным отображениям, из чего следует, что $d_2 = 0$.

Таким образом, мы имеем

$$H_k(M_g) = \begin{cases} \mathbb{Z}, & k = 0 \text{ или } k = 2, \\ \mathbb{Z}^{2g}, & k = 1 \\ 0, & \text{иначе} \end{cases}$$

Теперь вычислим гомологии неориентируемой замкнутой поверхности рода g. Она имеет такую клеточную структуру:

- Одна нульмерная клетка.
- g одномерных клеток.
- Одна двумерная клетка, приклеенная по слову $a_1^2 \dots a_g^2$.

Тогда клеточный цепной комплекс имеет вид:

$$0 \to \mathbb{Z} \xrightarrow{d_2} \mathbb{Z}^{g} \xrightarrow{d_1} \mathbb{Z} \to 0$$

Аналогично предыдущему разу, $d_1 = 0$, а вот d_2 задаётся уравнением

$$d_2(1) = (2, \dots, 2),$$

так как каждое ребро a_i появляется в слове приклеивания двумерной клетки со степенью 2, а это значит, что каждое отображение $\Delta_{\alpha\beta}$ гомотопно отображению степени 2. Значит, d_2 инъективно и

$$H_2(N_g) = 0.$$

Выберем в $\mathbb{Z}^g$ такой базис: $(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 1, 0), (1, 1, \dots 1)$. Тогда нетрудно заметить, что

$$H_1(N_g) \cong \mathbb{Z}^{g-1} \oplus \mathbb{Z}/2\mathbb{Z}.$$

1.19 Пространства Мура

Допишу позже вместе с пространствами Эйленберга-Маклейна.

1.20 Теорема о вложении дисков и сфер

Напомним, что топологическое вложение — гомеоморфизм на образ.

Теорема 20. *Пусть* $h\colon D^k \to S^n$ *— вложение. Тогда*

$$\widetilde{H}_i\Big(S^n \setminus h\Big(D^k\Big)\Big) = 0\ \forall i.$$

Кроме того, если $h\colon S^k \to S^n$ *— вложение (и* $k < n$*), то*

$$\widetilde{H}_i\Big(S^n \setminus h\Big(S^k\Big)\Big) = \mathbb{Z},\ i = n-k-1\ \textit{и}\ 0\ \textit{иначе.}$$

Доказательство. Проведём индукцию по k. Случай $k = 0$ тривиален:

$$S^n \setminus h\big(D^0\big) = \mathbb{R}^n.$$

Теперь докажем индукционный переход от противного. Рассмотрим покрытие нашего пространства двумя множествами:

$$A = S^n \setminus h\left(I^k \times \left[0, \frac{1}{2}\right]\right), \quad B = S^n \setminus h\left(I^k \times \left[\frac{1}{2}, 1\right]\right).$$

Заметим, что $A \cup B = S^n \setminus \big(h\big(I^k \times \big[0, \frac{1}{2}\big]\big) \cap h\big(I^k \times \big[\frac{1}{2}, 1\big]\big)\big) = S^n \setminus h\big(I^k \times \frac{1}{2}\big)$ и

$$\widetilde{H}_i(A \cup B) \cong \widetilde{H}_i\left(S^n \setminus h\left(I^k \times \frac{1}{2}\right)\right) = 0,$$

по индукционному предположению. Напишем теперь точную последовательность Майера-Вьеториса (9):

$$\ldots \to H_n(A \cap B) \to H_n(A) \oplus H_n(B) \to H_n(X) \to H_{n-1}(A \cap B) \to \ldots$$

$$\ldots \to H_n\Big(S^n \setminus h\Big(I^{k+1}\Big)\Big) \to H_n(A) \oplus H_n(B) \to \underbrace{H_n\left(S^n \setminus h\left(I^k \times \frac{1}{2}\right)\right)}_{\cong 0} \to H_{n-1}\Big(S^n \setminus h\Big(I^{k+1}\Big)\Big) \to \ldots$$

значит если в $\widetilde{H}_i(A \cap B) = \widetilde{H}_i\big(S^n \setminus \big(I^k \times I\big)\big)$ есть ненулевой класс a, его образ $(a, -a)$ в $\widetilde{H}_n(A) \oplus \widetilde{H}_n(B)$ будет ненулевым, а значит, в $\widetilde{H}_i(A)$ или $\widetilde{H}_i(B)$ тоже будет ненулевым. Далее мы можем также разбить на две части интервал в A или в B (в зависимости от того, где не ноль) и проделать всё полностью аналогично. Таким образом мы получим последовательность вложенных интервалов I_n таких, что

$$\widetilde{H}_i\Big(S^n \setminus h\Big(I^k \times I_n\Big)\Big) \neq 0,\ a \in \widetilde{H}_i\Big(S^n \setminus h\Big(I^k \times I_n\Big)\Big).$$

Тогда, если $p = \bigcap I_n$, то по индукционному предположению

$$\widetilde{H}_i\Big(S^n \setminus h\Big(I^k \times p\Big)\Big),$$

то есть a представляет ноль в этих гомологиях. Но это означает, что он является чьей-то границей, но тогда он является границей и в допредельном случае, что даёт нам противоречие.

Докажем теперь второй пункт. Представим сферу ввиде объединения двух дисков (полусфер):

$$S^k = D^k_+ \cup D^k_-, \quad D^k_- \cap D^k_+ = S^{k-1}.$$

тогда $S^n \setminus h\big(S^k\big) = S^n \setminus h\big(D^k_+ \cup D^k_-\big) = S^n \setminus h\big(D^k_-\big) \cap S^n \setminus h\big(D^k_+\big)$. Запишем опять точную последовательность Майера-Вьеториса 9, полагая

$$A = S^n \setminus h\Big(D^k_+\Big), \quad B = S^n \setminus h\Big(D^k_+\Big).$$

:

$$\ldots \to H_i\Big(S^n \setminus h\Big(S^k\Big)\Big) \to \underbrace{H_i\Big(S^n \setminus h\Big(D^k_-\Big)\Big)}_{=0} \oplus \underbrace{H_i\Big(S^n \setminus h\Big(D^k_+\Big)\Big)}_{=0} \to H_i\Big(S^n \setminus h\Big(S^{k-1}\Big)\Big) \to \ldots$$

Нулевые элементы в точной последовательности у нас их первого утверждения теоремы. Теперь видно, что мы можем вести индукцию по k. □

1.21 Когомологии

Итак, рассмотрим цепной комплекс абелевых групп $(C_\bullet, \partial)$

$$\ldots \to C_k \to C_{k-1} \to C_{k-2} \to \ldots$$

Тогда мы можем рассмотреть группы $C^k \stackrel{\text{def}}{=} \operatorname{Hom}(C_k, G)$, где G — фиксированная абелева группа.[8] Тогда мы получаем цепной комплекс

$$\ldots \leftarrow C^{k+1} \xleftarrow{\delta} C^k \xleftarrow{\delta} C^{k-1} \xleftarrow{\delta} \ldots$$

Естественно, стрелки развернулись, так как мы подействовали на комплекс контравариантным функтором $\operatorname{Hom}(\_, G)$. Действие оператора δ определяется естественным образом:

$$\varphi \in C^k,\ \delta\varphi\colon C_{k+1} \xrightarrow{\partial} C_k \xrightarrow{\varphi} G,\ \delta\varphi = \varphi \circ \partial.$$

Замечание. Сразу же нетрудно заметить, что $\delta^2 = 0$, то есть построенный комплекс действительно будет комплексом. Действительно,

$$\delta_k \circ \delta_{k-1}(\varphi(c)) = \delta_k(\varphi(\partial_{k-1}c)) = \varphi(\partial_k\partial_{k-1}c) = 0.$$

Определение 15. Группы гомологий коцепного комплекса $(C^\bullet, \delta) = (\operatorname{Hom}(C_\bullet), G), \delta)$ называют *группами когомологий* комплекса $(C_\bullet, \partial)$ с коэффициентами в группе G и обозначаются $H^k(C_\bullet; G)$. Как и в случае с гомологиями, $\operatorname{Im}\delta_k$ называют k-мерными кограницами, $\operatorname{Ker}\delta_k$ — k-мерными коциклами, а C^k — k-мерными коцепями.

Таким образом, мы определили и *сингулярные когомологии* пространства X (так как они строятся по сингулярным гомологиям). Заметим, что так как функтор Hom контравариантен, логично ожидать, что и когомологии будут контраваринатным функтором. Действительно, если $f\colon X \to Y$ — непрерывное отображение, то у нас есть индуцированный морфизм

$$f_*\colon C_k(X) \to C_k(Y)$$

и действием функтора Hom мы получаем индуцированный морфизм $f^*\colon C^k(Y) \to C^k(X)$:

$$\varphi \in C^k(Y),\ \varphi\colon C^k(Y) \to G,\ f^*(\varphi) \stackrel{\text{def}}{=} \varphi \circ f\colon C^k(X) \to G,\ f^*(\varphi) \in C^k(X).$$

Покажем теперь, что у нас будет и индуцированный морфизм в когомологиях:

$$f^*\colon H^k(Y) \to H^k(X)$$

Для этого надо проверить, что отображение уважает добавление кограницы, то есть, если мы выберем другого представителя того же когомологического класса, мы полужем тот же образ, что и до этого. Действительно,

$$f^*(c_k + \delta c_{k-1}) = f^*(c_k) + \delta f^*(c_{k-1})$$

Замечание. Формально, как и в гомологиях, нам надо проверить, что $f^*\delta = \delta f^*$. Действительно, пусть $\varphi \in C^k(X)$, тогда

$$f^*(\delta\varphi) = f^*(\varphi\partial) = \varphi\partial f = \varphi f\partial = \delta f^*(\varphi).$$

В третьем равенстве мы пользуемся тем, что в начале курса мы уже проверяли, что граничный оператор коммутирует с непрерывными отображениями.

[8] В нашем, топологическом контексте, это группа коэффициентов.

1.22 Формула универсальных коэффициентов для когомологий

Пример 8. Рассмотрим следующий комплекс:

$$0 \to \underbrace{\mathbb{Z}}_{C_3} \xrightarrow{\cdot 0} \underbrace{\mathbb{Z}}_{C_2} \xrightarrow{\cdot 2} \underbrace{\mathbb{Z}}_{C_1} \xrightarrow{\cdot 0} \underbrace{\mathbb{Z}}_{C_0} \to 0$$

После применения функтора $\mathrm{Hom}(\_, \mathbb{Z})$ мы получим такой комплекс:

$$0 \leftarrow \underbrace{\mathbb{Z}}_{C^3} \leftarrow \underbrace{\mathbb{Z}}_{C^2} \leftarrow \underbrace{\mathbb{Z}}_{C^1} \leftarrow \underbrace{\mathbb{Z}}_{C^0} \leftarrow 0$$

Посмотрим, какие в новом комплексе отображения. Действительно, пусть $\varphi\colon C_1 \to \mathbb{Z}$, $\psi\colon C_2 \to C_1, \psi(x) = 2x$, тогда $\varphi\psi\colon C_2 \to \mathbb{Z} \in C^2$. Нетрудно заметить, что $\varphi(\psi(x)) = \varphi(2x) = 2\varphi(x)$. Значит, мы получили вот такой комплекс:

$$0 \leftarrow \underbrace{\mathbb{Z}}_{C^3} \xleftarrow{\cdot 0} \underbrace{\mathbb{Z}}_{C^2} \xleftarrow{\cdot 2} \underbrace{\mathbb{Z}}_{C^1} \xleftarrow{\cdot 0} \underbrace{\mathbb{Z}}_{C^0} \leftarrow 0$$

Вычислим сначала гомологии:

$$H_0(C_\bullet) = \mathbb{Z},\ H_1(C_\bullet) = \mathbb{Z}/2\mathbb{Z},\ H_2(C_\bullet) = 0,\ H_3(C_\bullet) = \mathbb{Z}.$$

Теперь вычислим когомологии:

$$H^0(C_\bullet) = \mathbb{Z},\ H^1(C_\bullet) = 0, H_2(C_\bullet) = \mathbb{Z}/2\mathbb{Z}, H_3(C_\bullet) = \mathbb{Z}.$$

То есть, сами группы не изменились, но изменилась градуировка.

Это вполне естественно, так как, на самом деле, любой цепной комплекс конечно-порожденных свободных абелевых групп является прямой суммой комплексов

$$0 \to \mathbb{Z} \to 0 \text{ и } 0 \to \mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z} \to 0$$

и в силу того, что функтор Hom аддитивен на конечных копроизведениях, применяя $\mathrm{Hom}(\_, \mathbb{Z})$ к исходному комплексу, мы получаем прямую сумму комплексов

$$0 \leftarrow \mathbb{Z} \leftarrow 0 \text{ и } 0 \leftarrow \mathbb{Z} \xleftarrow{\cdot m} \mathbb{Z} \leftarrow 0$$

Таким образом, мораль всего этого дела в том, что группы когомологий — тоже самое, что группы гомологий, за исключением того, что кручение смещается на олну размерность.

Предложение 5. *Пусть $(C_\bullet, \partial)$ — цепной комплекс. Тогда существует гомоморфизм*

$$h\colon H^n(C; G) \to \mathrm{Hom}(H_n(C), G).$$

Доказательство. Рассмотрим когомологический класс $[\varphi] \in H^n(C_\bullet; G)$, $\varphi\colon C_n \to G$, $\delta\varphi = 0$.

$$\delta\varphi = \varphi\partial \Leftrightarrow \varphi|_{\mathrm{Im}\,\partial_{n+1}} = 0$$

Ограничение $\varphi_0 = \varphi|_{\mathrm{Ker}\,\partial_n}\colon \mathrm{Ker}\,\partial_n \to G$ индуцирует гомоморфизм факторизации

$$\overline{\varphi_0}\colon \mathrm{Ker}\,\partial_n/\,\mathrm{Im}\,\partial_{n+1} \to G, \quad \overline{\varphi_0} \in \mathrm{Hom}(H_n(C_\bullet), G).$$

Таким образом, полагая $h(\varphi) = \overline{\varphi}_0$, мы получаем нужное. □

Упражнение. h — эпиморфизм.

Рассмотрим теперь короткую точную последовательность

$$0 \to Z_{n+1} \to C_{n+1} \xrightarrow{\partial} B_n \to 0$$

Применяя функтор $\mathrm{Hom}(-, G)$ мы получаем точную последовательность

$$0 \leftarrow Z^{n+1} \leftarrow C^{n+1} \leftarrow B^{n+1} \leftarrow 0$$

На самом деле, мы имеем коммутативную диаграмму

$$\begin{array}{ccccccccc} 0 & \longleftarrow & Z^{n+1} & \longleftarrow & C^{n+1} & \longleftarrow & B^n & \longleftarrow & 0 \\ & & \uparrow{\scriptstyle 0} & & \uparrow{\scriptstyle \delta} & & \uparrow{\scriptstyle 0} & & \\ 0 & \longleftarrow & Z^n & \longleftarrow & C^n & \longleftarrow & B^{n-1} & \longleftarrow & 0 \end{array}$$

Видно, что эта диаграмма — часть короткой точной последовательности комплексов. Она даёт нам длинную точную последовательность:

$$\ldots \leftarrow B^n \leftarrow Z^n \leftarrow H^n(C_\bullet, G) \leftarrow B^{n-1} \leftarrow Z^{n-1} \leftarrow \ldots$$

Разбивая длинную точную последовательность на короткие точные последовательности мы получаем:

$$0 \leftarrow \operatorname{Ker}(Z^n \to B^n) \xleftarrow{h} H^n(C_\bullet; G) \leftarrow \operatorname{Coker}\bigl(Z^{n-1} \to B^{n-1}\bigr) \leftarrow 0$$

А теперь заметим, что $\operatorname{Ker}(Z^n \to B^n) = \operatorname{Hom}(H_n(C_\bullet), G)$. Таким образом, мы получаем расщепимую точную последовательность:

$$0 \to \operatorname{Coker}\bigl(Z^{n-1} \to B^{n-1}\bigr) \to H^n(C_\bullet; G) \to \operatorname{Hom}(H_n(C_\bullet), G) \to 0.$$

Определение 16. Пусть H — абелева группа. Тогда её *свободная резольвента* — это точная последовательность

$$\ldots \to F_2 \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} H \to 0,$$

в которой каждая группа F_n свободная.

Применяя к этой точной последовательности функтор $\operatorname{Hom}(-, G)$ мы можем потерять точность, но во всяком случае, получим цепной комплекс:

$$\leftarrow F_2^* \xleftarrow{f_2^*} F_1^* \xleftarrow{f_1^*} F_0^* \xleftarrow{f_0^*} H^* \leftarrow 0$$

Будем обозначать группы когомологий свободной резольвенты, как $H^n(F, G)$. Нам понадобится следующее утверждение из гомологической алгебры:

Лемма 9. Пусть даны свободные резольвенты F и F' абелевых групп H и H'. Тогда любой гомоморфизм $\alpha\colon H \to H'$ можно продолжить до цепного отображения $F \to F'$. Кроме того, любые два таких цепных отображения, продолжающие гомоморфизм α, цепно гомотопны.

Для любых двух свободных резольвент F и F' группы H существуют канонические изоморфизмы

$$H^n(F; G) \cong H^n(F'; G).$$

У любой абелевой группы H есть свободная резольвента вида

$$0 \to F_1 \to F_0 \to H \to 0$$

с $F_i = 0$ при $i > 1$, которую мы сейчас построим.

Выберем в H набор образующих и пусть F_0 — группа, свободно порожденная этими образующими. Тогда у нас есть сюръективный гомоморфизм $f_0\colon F_0 \to H$, переводящий элементы базиса в образующие H. Его ядро будет свободно, как подгруппа свободной группы, поэтому мы можем положить $F_1 = \operatorname{Ker} f_0$, а в качестве f_1 взять включение $\operatorname{Ker} f_0 \hookrightarrow F_0$.

Для этой свободной резольвенты мы имеем $H^n(F; G) = 0\ \forall n > 1$, поэтому, из леммы 9 мы получаем, что это должно быть верно для всех свободных резольвент.

Таким образом, единственная интересная группа из $H^n(F; G)$ — это $H^1(F; G)$. Эта группа зависит лишь от H и G, поэтому обычно её обозначают $\operatorname{Ext}(H, G)$[9].

[9]Вообще говоря, в гомологической алгебре функтор Ext обычно интерпретируют, как множество классов эквивалентности расширений G посредством H, но в алгебраической топологии такая интерпретация редко нужна.

Так вот, из построения свободной резольвенты для группы H и определения когомологий мы теперь наконец можем заметить, что

$$\operatorname{Coker}\bigl(Z^{n-1} \to B^{n-1}\bigr) = \operatorname{Ext}(H_{n-1}(C_\bullet), G).$$

Теперь мы наконец можем заключить, что мы доказали формулу универсальных коэффициентов для когомологий:

Теорема 21 (Об универсальных коээфициентах для когомологий)**.** *Пусть $C_\bullet$ — цепной комплекс. Тогда его группы когомологий определяются расщепимыми короткими точными последовательностями*

$$0 \to \operatorname{Ext}(H_{n-1}(C_\bullet), G) \to H^n(C; G) \to \operatorname{Hom}(H_n(C), G) \to 0$$

Вообще говоря, это утверждение достаточно полезно, потому что на конечнопорожденных абелевых группах функтор Ext несложно посчитать:

- $\operatorname{Ext}(H \oplus H', G) \cong \operatorname{Ext}(H, G) \oplus \operatorname{Ext}(H', G)$.
- $\operatorname{Ext}(H, G) = 0$, если H — свободна.
- $\operatorname{Ext}(\mathbb{Z}/n\mathbb{Z}, G) \cong G/nG$.
- Если H конечно порождена, то имеет место изоморфизм

$$\operatorname{Ext}(H, \mathbb{Z}) \cong \operatorname{Tor}(H).$$

Кроме того, теорема об универсальных коэффициентов позволяет вычислять когомологии, зная только гомологии.

Следствие 9. *Если группы гомологий $H_n(C)$ и $H_{n-1}(C)$ комплекса C, состоящего из свободных абелевых групп, конечно порождены и $T_n \subset H_n$ и $T_{n-1} \subset H_{n-1}$ — подгруппы кручения, то*

$$H^n(C; \mathbb{Z}) \cong (H_{n-1}(C)/T_n) \oplus T_{n-1}.$$

Это следствие даёт нам обобщение и формализацию примера 8.

Кроме того, из всего этого дела есть еще одно замечательное следствие:

Следствие 10. *Если $f\colon C_\bullet \to C'_\bullet$ индуцирует изоморфизм всех групп гомологий $H_k(C_\bullet) \cong H_k(C'_\bullet)$. Тогда отображения $f^*\colon H^k(C_\bullet; G) \cong H^k(C'_\bullet; G)$.*

Доказательство. Действительно, достаточно заметить, что из свойств свободной резольвенты мы знаем, что отображение цепных комплексов индуцирует такую вот диаграмму:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Ext}\left(H_{n-1}(C), G\right) & \longrightarrow & H^n\left(C; G\right) & \xrightarrow{h} & \operatorname{Hom}\left(H_{n-1}(C), G\right) & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \operatorname{Ext}\left(H_{n-1}(C'), G\right) & \longrightarrow & H^n\left(C'; G\right) & \xrightarrow{h} & \operatorname{Hom}\left(H_{n-1}(C'), G\right) & \longrightarrow & 0
\end{array}$$

Применяя 5-лемму и индукцию, мы получаем нужное. □

1.23 Умножение в когомологиях

Пусть R — коммутативное и ассоциативное кольцо.

Пусть $\varphi \in C^k(X; R),\ \psi \in C^\ell(X; R)$. Тогда их произведением определяется таким образом:

$$\varphi \smile \psi \in C^{k+\ell}, \quad (\varphi \smile \psi)(\sigma) = \varphi(\sigma|_{[v_0 \dots v_k]}) \cdot \psi(\sigma|_{[v_k \dots v_{k+\ell}]}),$$

где $\sigma\colon \Delta^{k+\ell} \to X$ — сингулярный симплекс.

Лемма 10. Для кограницы $\smile$-произвения справедлива следующая формула:

$$\delta(\varphi \smile \psi) = \delta\varphi \smile \psi + (-1)^k \varphi \smile \delta\psi.$$

Доказательство. Пусть $\sigma\colon \Delta^{k+\ell} \to X$ — сингулярный симплекс. Тогда

$$(\delta\varphi \smile \psi)(\sigma) = \sum_{i=0}^{k+1}(-1)^i\varphi(\sigma|_{[v_0,\dots,\hat{v_i},\dots,v_{k+1}]})\psi(\sigma|_{[v_{k+1}\dots v_{k+\ell+1}]})$$

Распишем теперь второй кусок:

$$(-1)^k(\varphi \smile \delta\psi) = \sum_{i=k}^{k+\ell+1}(-1)^i\varphi(\sigma|_{[v_0\dots v_k]})\psi(\sigma|_{[v_k,\dots,\hat{v_i},\dots,v_{k+\ell+1}]})$$

Когда мы сложим эти две суммы, последнее слагаемое первой суммы сократится с первым слагаемым второй, а всё, что останется — как раз $\delta(\varphi \smile \psi)(\sigma) = (\varphi \smile \psi)(\partial\sigma)$. □

Замечание. Таким образом, $\delta(\varphi \smile \psi) = \delta\varphi \smile \psi \pm \delta\psi \smile \varphi$. Из этого следует, что произведение коциклов — коцикл. Также это сразу даёт нам, что произведение коцикла и когранцы (в любом порядке) — когранца:

$$\varphi \smile \delta\psi = \pm\delta(\varphi \smile \psi)$$

Это даёт нам ассоциативное дистрибутивное умножение

$$\smile\colon H^k(X;R) \times H^\ell \to H^{k+\ell}(X;R).$$

Таким образом, при помощи $\smile$-произведения, мы наделили

$$H^*(X;R) = \bigoplus_{n=0}^{\infty} H^n(X;R)$$

структурой кольца (а на самом деле, градуированной алгебры).

Если в кольце R есть единица, то единицей относительно $\smile$-произведения будет нольмерный коцикл $1 \in H^0(X;R)$, принимающий значение 1 на любом нульмерном сингулярном симплексе.

Замечание. Это показывает нам отдельную пользу когомологий: например, у $\mathbb{C}\mathrm{P}^2$ и $S^4 \vee S^2$ все группы гомологий и группы когомлогий совпадают, а кольца когомологий отличаются.

2. Когомологии де Рама

2.1 Дифференциальные формы

Начнём с определения дифференциальных форм.

Определение 17. *Дифференциальная 1-форма* на $\mathbb{R}^n$ — это объект вида

$$\omega = \sum_{i=1}^{n} f_i(x)\mathrm{d}x_i, \quad x = (x_1,\dots,x_n) \in \mathbb{R}^n,\ f_i \in C^\infty(\mathbb{R}^n),$$

где $\mathrm{d}x_i$ — «значки», которые пока что ничего не означают и преобразуются по формальным правилам.

Соотвественно, каждой точке x ω_x — просто элемент $\mathbb{R}$-векторного пространства, натянутого на $\mathrm{d}x_1,\dots,\mathrm{d}x_n$. Пространство 1-форм имеет естественную структуру $C^\infty(\mathbb{R}^n)$-модуля, его мы будем обозначать как $\Omega^1(\mathbb{R}^n)$.

Если $g\colon \mathbb{R}^k \to \mathbb{R}^n$ (а координаты в $\mathbb{R}^k$ — это $y_1,\dots,y_k$) — гладкое отображение, то $x_i = x_i(y_1,\dots,y_k)$ и мы будем полагать, что в таком случае $\mathrm{d}x_i$ изменяются вот по таким правилам:

$$\mathrm{d}x_i = \sum_{j=1}^{k}\frac{\partial x_i}{\partial y_j}\mathrm{d}y_j.$$

Тогда для $\omega = \sum f_i \mathrm{d}x_i$ её *пулл-бэк* или *pull-back* вдоль g мы определим, как

$$g^*(\omega) \stackrel{\text{def}}{=} \sum_{i=1}^{n} f_i \sum_{j=1}^{k} \frac{\partial x_i}{\partial y_j} \mathrm{d}y_j.$$

Соотвественно, для пути $\gamma\colon [0,1] \to \mathbb{R}^n$ мы можем интгерал формы ω вдоль γ следующим образом:

$$\int\limits_{\gamma} \omega \stackrel{\text{def}}{=} \int\limits_{[0,1]} \gamma^*\omega = \int\limits_{[0,1]} \sum f_i \cdot \gamma_i' \mathrm{d}t = \int\limits_{[0,1]} \gamma' \cdot (f_1, \ldots, f_n) \mathrm{d}t$$

Определение 18. Дифференциальная k-форма на $\mathbb{R}^n$ — это формальная линейная комбинация

$$\omega = \sum_{|I|=k} f_I(x)\ \mathrm{d}x_{i_1} \wedge \mathrm{d}x_{i_2} \wedge \ldots \wedge \mathrm{d}x_{i_k}, \quad f_I \in C^\infty(\mathbb{R}^n)$$

где $\wedge$-произведение как и обычно антисимметрично: $\mathrm{d}x_i \wedge \mathrm{d}x_j = -\mathrm{d}x_j \wedge \mathrm{d}x_i$.

Пространство k-форм мы будем обозначать, как $\Omega^k(\mathbb{R}^n)$.

Из соображений антисимметричности внешнего произведения, достаточно полагать наборы монотонными, то есть $i_1 < i_2 < \ldots < i_k$.

Опять же, если есть отображение $\gamma\colon [0,1]^k \to \mathbb{R}^n$ и k-форма $\omega = \sum_{|I|=k} f_I\ \mathrm{d}x_{i_1} \wedge \ldots \mathrm{d}x_{i_k}$, то можно определить

$$\int\limits_{\gamma} \omega \stackrel{\text{def}}{=} \int\limits_{[0,1]^k} \gamma^*\omega, \text{ где } \gamma^*(\mathrm{d}x_1 \wedge \ldots \wedge \mathrm{d}x_k) = \gamma^*(\mathrm{d}x_1) \wedge \ldots \wedge \gamma^*(\mathrm{d}x_k).$$

Пример 9. Пусть $\gamma\colon [0,1]^2 \to \mathbb{R}^3,\ \gamma(t_1, t_2) = (t_1, t_2, t_1t_2)$, в $[0,1]^2$ у нас координаты (t_1, t_2), а в $\mathbb{R}^3$ у нас координаты (x, y, z).

Рассмотрим форму $\omega = xy\mathrm{d}y \wedge \mathrm{d}z$, её пулл-бэк:

$$\gamma^*(\omega) = t_1t_2\mathrm{d}t_2 \wedge \mathrm{d}(t_1t_2)$$

$$d(t_1t_2) = \frac{\partial(t_1t_2)}{\partial t_1}\mathrm{d}t_1 + \frac{\partial(t_1t_2)}{\partial t_2}\mathrm{d}t_2 = t_2\mathrm{d}t_1 + t_1\mathrm{d}t_2 \rightsquigarrow \gamma^*(\omega) = t_1t_2\mathrm{d}t_2 \wedge (t_2\mathrm{d}t_1 + t_1\mathrm{d}t_2) = -t_1t_2^2\mathrm{d}t_1 \wedge \mathrm{d}t_2.$$

Замечание. Из определения мы видим, что пулл-бэк k-формы — k-форма.

В частности, из нашей игры с обозначениями сразу следует, что

$$\int\limits_{[0,1]^k} f\ \mathrm{d}x_1 \wedge \ldots \wedge \mathrm{d}x_k = \int\limits_{[0,1]^k} f\ \mathrm{d}x_1 \ldots \mathrm{d}x_k$$

Абстрактно всё озвученное выше можно воспринимать следующим образом: k — формы — это сечения $\Lambda^k T^*\mathbb{R}^n$ (и, с формальной точки зрения, все выписанные выше формулы будут абсолютно такими же).

Теперь рассмотрим $\omega \in \Omega^1(\mathbb{R}^n)$, в каждой точке $x \in \mathbb{R}^n$ это

$$\omega_x = \sum_i a_i \mathrm{d}x_i.$$

Тогда значок $\mathrm{d}x_i$ можно понимать, как функционал на $T_x\mathbb{R}^n$, действующий как

$$v \in T_x\mathbb{R}^n,\ v = (v_1, \ldots, v_n) \quad \mathrm{d}x_i(v_1, \ldots, v_n) = v_i.$$

Тогда $\sum_i a_i \mathrm{d}x_i$ — тоже функционал на $T_x\mathbb{R}^n$. Кроме того, если же V — векторное поле на $\mathbb{R}^n$, то тогда $\mathrm{d}x_i(v)$ — функция на $\mathbb{R}^n$ (в каждой точке вычисляющая $v(x)_i$).

Теперь определим **внешний дифференциал**. Пусть $\omega \in \Omega^k(\mathbb{R}^n)$, $\omega = \sum_{|I|=k} f_I \mathrm{d}x_I$, тогда $d\omega$ определяется, как

$$\mathrm{d}\omega = \sum_{|I|=k} \sum_{i=1}^{n} \frac{\partial f_I}{\partial x_i} \mathrm{d}x_i \wedge \mathrm{d}x_I \in \Omega^{k+1}(\mathbb{R}^n).$$

Нетрудно видеть, что внешний дифференциал — это линейное отображение

$$\mathrm{d}\colon \Omega^k(\mathbb{R}^n) \to \Omega^{k+1}(\mathbb{R}^n).$$

Кроме того, если $f \in C^\infty(\mathbb{R}^n)$, то справедлива формула

$$\mathrm{d}(f \cdot \omega) = \mathrm{d}f \wedge \omega + f\mathrm{d}\omega.$$

Домашнее задание 1. Внешний дифференциал коммутирует с пулл-бэком, то есть если $g \in \mathbb{R}^m \to \mathbb{R}^n$, а $\omega \in \Omega^k(\mathbb{R}^n)$, то

$$\mathrm{d}g^*(\omega) = g^*\mathrm{d}\omega.$$

Определение 19. Если $\mathrm{d}\omega = 0$, то форму ω мы будем называть *замкнутой*. Если $\omega = \mathrm{d}\alpha$ для некоторой α, то форму ω мы будем называть *точной*.

Лемма 11. $d^2 = 0$ (т.е., как отображение $\Omega^k(\mathbb{R}^n) \to \Omega^{k+2}(\mathbb{R}^n)$ это умножение на 0).

Доказательство. Пусть $\omega = \sum_I f_I \mathrm{d}x_I$. В силу линейности достаточно проверить утверждение для $f_I \mathrm{d}x_I$.

$$f_I \mathrm{d}x_I \mapsto \sum_i \frac{\partial f}{\partial x_i} \mathrm{d}x_i \wedge \mathrm{d}x_I \mapsto \sum_j \sum_i \frac{\partial f}{\partial x_j \partial x_i} x_j \wedge x_i \wedge x_I.$$

Остаётся заметить, что каждому слагаемому $\ldots \mathrm{d}x_j \wedge \mathrm{d}x_i$ будет соотвествовать слагаемое $-\mathrm{d}_i \wedge \mathrm{d}x_j$ (и они сократятся). □

Это означает, что d — дифференциал в смысле гомологической алгебры, а

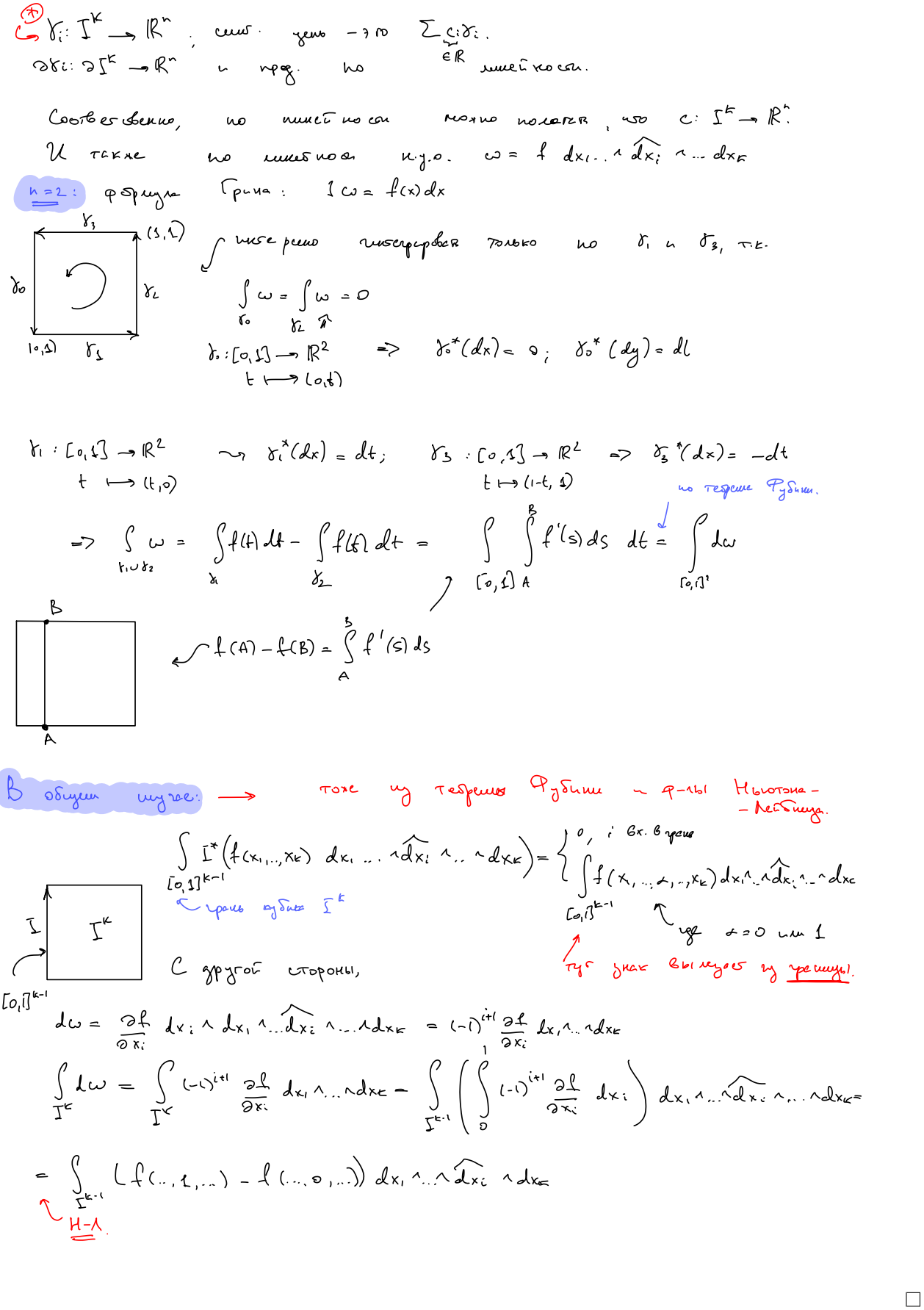
$$\Omega^0(\mathbb{R}^n) \xrightarrow{d} \Omega^1(\mathbb{R}^n) \to \ldots \xrightarrow{d} \Omega^n(\mathbb{R}^n) \to \ldots$$

это *дифференциальный комплекс*.

Теорема 22 (Стокс)**.** *Пусть c — k-мерная сингулярная цепь, а ω — $(k-1)$-форма, тогда*

$$\int_c \mathrm{d}\omega = \int_{\partial c} \omega.$$

Доказательство. Вот же оно:



□

Пример 10. Посмотрим на дифференциальные формы на $\mathbb{R}^3$.

- $\Omega^0(\mathbb{R}^3) = C^\infty(\mathbb{R}^3)$.
- $\Omega^1(\mathbb{R}^3) = \{f_1\mathrm{d}x + f_2\mathrm{d}y + f_3\mathrm{d}z,\ f_i \in C^\infty(\mathbb{R}^3)\}$.
- $\Omega^2(\mathbb{R}^3) = \{f_1\mathrm{d}x \wedge \mathrm{d}y + f_2\mathrm{d}y \wedge \mathrm{d}z + f_3\mathrm{d}z \wedge dx,\ f_i \in C^\infty(\mathbb{R}^3)\}$.
- $\Omega^3(\mathbb{R}^3) = \{f\mathrm{d}x \wedge \mathrm{d}y \wedge \mathrm{d}z,\ f \in C^\infty(\mathbb{R}^3)\}$.

Видно, что у нас есть отождествления $C^\infty(\mathbb{R}^3) \cong \Omega^0(\mathbb{R}^3) \cong \Omega^3(\mathbb{R}^3)$.
Кроме того, как мы помним, гладкие векторные поля на $\mathbb{R}^3$ — это

$$\left\{ f_1\frac{\partial}{\partial x} + f_2\frac{\partial}{\partial y} + f_3\frac{\partial}{\partial z},\ f_i \in C^\infty(\mathbb{R}^n) \right\}.$$

Видно, что гладкие векторные поля можно (не канонически) отождествить с $\Omega^1(\mathbb{R}^3)$. Кроме того, их можно отождествить с $\Omega^2(\mathbb{R}^3)$ посредством

$$f_1\frac{\partial}{\partial x} + f_2\frac{\partial}{\partial y} + f_3\frac{\partial}{\partial z} \mapsto f_1\mathrm{d}y \wedge \mathrm{d}z + f_2\mathrm{d}z \wedge \mathrm{d}x + f_3\mathrm{d}x \wedge \mathrm{d}y.$$

Но, это отождествление, как видно, не каноническое: когда мы меняем координаты, векторные поля будут менятся по одному правилу, а формы по другому правилу.

Какой же смысл можно придать этим отождествлениям? Например, такой, что есть вот такой коммутативный квадрат:

$$\begin{array}{ccc} C^\infty(\mathbb{R}^3) \ni f & \longmapsto & f \in \Omega^0(\mathbb{R}^3) \\ \downarrow & & \downarrow \\ \left(\dfrac{\partial f}{\partial x}, \dfrac{\partial f}{\partial y}, \dfrac{\partial f}{\partial z}\right) & \longleftarrow\!\shortmid & \mathrm{d}f = \dfrac{\partial f}{\partial x}\mathrm{d}x + \dfrac{\partial f}{\partial y}\mathrm{d}y + \dfrac{\partial f}{\partial z}\mathrm{d}z \in \Omega^1(\mathbb{R}^3) \end{array}$$

Он показывает, что композиция этих отождествленйи уже вполне каноническая (так как градиент функции не зависит от выбора координат).

Если же мы рассмотрим векторное $(f_1, f_2, f_3) = V$, изготовим из него 1-форму, продифференцируем её и перегоним обратно в векторное поле, получится *ротор* векторного поля V:

$$\begin{array}{ccc} (f_1, f_2, f_3) = V & \longrightarrow & f_1\mathrm{d}x + f_2\mathrm{d}y + f_3\mathrm{d}z \in \Omega^1(\mathbb{R}^3) \\ \downarrow{\scriptstyle \mathrm{rot}} & & \downarrow{\scriptstyle \mathrm{d}} \\ \mathrm{rot}V = \left(\dfrac{\partial f_3}{\partial y} - \dfrac{\partial f_2}{\partial z}, \dfrac{\partial f_1}{\partial z} - \dfrac{\partial f_3}{\partial x}, \dfrac{\partial f_2}{\partial x} - \dfrac{\partial f_1}{\partial y}\right) & \longleftarrow & \left(\dfrac{\partial f_3}{\partial y} - \dfrac{\partial f_2}{\partial z}\right)\mathrm{d}y \wedge \mathrm{d}z + \left(\dfrac{\partial f_1}{\partial z} - \dfrac{\partial f_3}{\partial x}\right)\mathrm{d}z \wedge \mathrm{d}x + \left(\dfrac{\partial f_2}{\partial x} - \dfrac{\partial f_1}{\partial y}\right)\mathrm{d}x \wedge \mathrm{d}y \end{array}$$

Аналогичное можно селать и с дивергенцией.

$$\begin{array}{ccc} (f_1, f_2, f_3) = V & \longrightarrow & f_1\mathrm{d}y \wedge \mathrm{d}z + f_2\mathrm{d}z \wedge \mathrm{d}x + f_3\mathrm{d}x \wedge \mathrm{d}y \in \Omega^2(\mathbb{R}^3) \\ \downarrow{\scriptstyle \mathrm{div}} & & \downarrow{\scriptstyle \mathrm{d}} \\ \dfrac{\partial f_1}{\partial x} + \dfrac{\partial f_2}{\partial y} + \dfrac{\partial f_3}{\partial z} & \longleftarrow & \left(\dfrac{\partial f_1}{\partial x} + \dfrac{\partial f_2}{\partial y} + \dfrac{\partial f_3}{\partial z}\right)\mathrm{d}x \wedge \mathrm{d}y \wedge \mathrm{d}z \in \Omega^3(\mathbb{R}^3) \end{array}$$

То есть, мы только что поняли, что

- $\mathrm{d}(0\text{-формы})$ = градиент,

- $\mathrm{d}(1\text{-формы})$ = ротор,
- $\mathrm{d}(2\text{-формы})$ = дивергенция,

К слову, отсюда мы бесплатно получили вот такие свойство:

$$\operatorname{rot}\nabla f = 0, \quad \operatorname{div}\operatorname{rot} V = 0.$$

2.2 Когомологии де Рама и компактные когомологии

Определение 20. Комплекс $\Omega^\bullet(\mathbb{R}^n)$ вместе с оператором d называется *комплексом де Рама* на $\mathbb{R}^n$.

Соответственно, когомологии этого комлпекса называют *когомологиями Де Рама* $\mathbb{R}^n$:

$$H^q_{\mathrm{dR}}(\mathbb{R}^n) = \ker\big(\mathrm{d}\colon \Omega^q((\mathbb{R}^n)) \to \Omega^{q+1}(\mathbb{R}^n)\big)/\mathrm{Im}\big(\mathrm{d}\colon \Omega^{q-1}(\mathbb{R}^n) \to \Omega^q(\mathbb{R}^n)\big).$$

Замечание. То, что это комплекс, гарантируется тем, что $\mathrm{d}^2 = 0$ (и, соотвественно, в связи с этим мы имеем $\ker\mathrm{d} \supset \mathrm{Im}\,\mathrm{d}$).

Замечание. Видно $\ker\mathrm{d}$ — это замкнутые формы, а образ d — точные формы. Например, $f(x,y)\mathrm{d}x + g(x,y)\mathrm{d}y$ замкнута тогда и только тогда, когда

$$\frac{\partial f}{\partial y} - \frac{\partial g}{\partial x} = 0.$$

Класс когомологий формы ω мы будем обозначать $[\omega]$.

Замечание. Всё то же самое можно делать для открытого $U \subset \mathbb{R}^n$ таким образом:

$$\Omega^\bullet(U) = C^\infty(U) \otimes_{\mathbb{R}} \Omega^\bullet(\mathbb{R}^n).$$

Таким образом, мы можем говорить о когомологиях де-Рама $H^q_{\mathrm{dR}}(U)$ для любого открытого подмножества $\mathbb{R}^n$.

Заметим, что гладкое отображение $f\colon U \to V$, где U, V — открытые подмножества $\mathbb{R}^n$, индуцирует отображение на формах

$$f^*\colon \Omega^q(V) \to \Omega^q(U),\ \omega \mapsto f^*(\omega),$$

а так как дифференциал коммутирует с пуллбеком (т.е. $\mathrm{d}f^*(\omega) = f^*(\mathrm{d}\omega)$, f^* даст нам цепное отображение $\Omega^\bullet(V) \to \Omega^\bullet(U)$:

$$\begin{array}{ccccccc}
\ldots & \longrightarrow & \Omega^q(V) & \xrightarrow{\mathrm{d}} & \Omega^{q+1}(V) & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle f^*} & & \downarrow{\scriptstyle f^*} & & \\
\ldots & \longrightarrow & \Omega^q(U) & \xrightarrow{\mathrm{d}} & \Omega^{q+1}(U) & \longrightarrow & \ldots
\end{array}$$

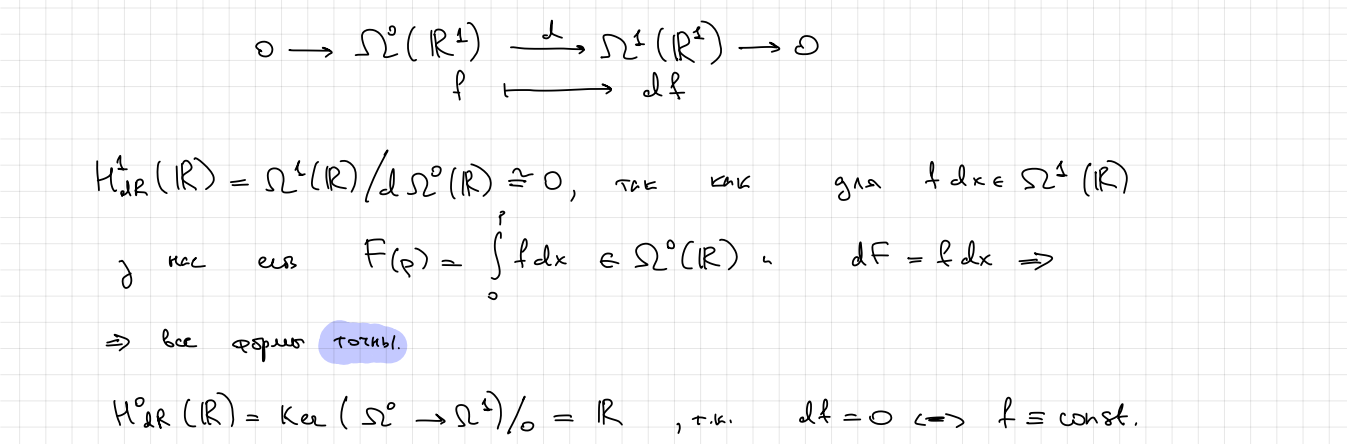
Определение 21. *Когомологии с компактным носителем* определяются следующим образом: рассмотрим комплекс дифференциальных форм с компактным носителем:

$$\Omega^\bullet_c(\mathbb{R}^n) \stackrel{\mathrm{def}}{=} C^\infty_0(\mathbb{R}^n) \otimes_{\mathbb{R}} \Omega^\bullet(\mathbb{R}^n).$$

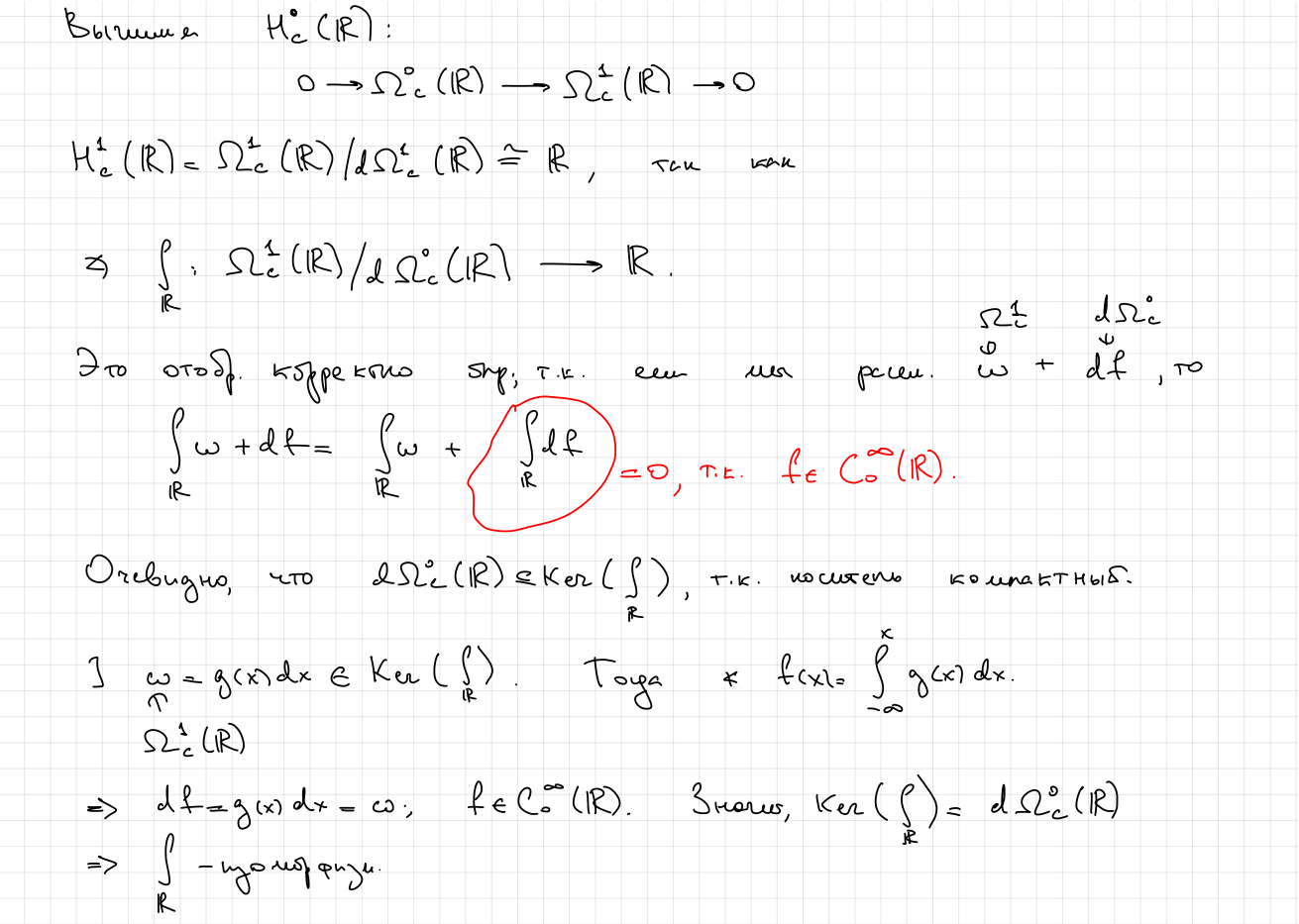
Тогда когомологии с компактным носителем — это когомологии этого комплекса, мы будем обозначать их $H^q_c(\mathbb{R}^n)$.

Замечание. Тут всё также корректно, так как $\mathrm{d}^2 = 0$. Но тут есть свои тонкости: нужно поступать аккуратнее с пуллбэком, так как пуллбэк формы с компактным носителем не обязан иметь компактный носитель. С другой стороны, если мы рассматриваем пулл-бэк при собственном отображении (т.е. таком, что прообраз компакта – компакт), то всё выживает.

Пример 11. Вычислим $H^\bullet_{\mathrm{dR}}(\mathbb{R})$.



Теперь вычислим компактные когомологии $H_c^\bullet(\mathbb{R})$:



2.3 Дифференциальные формы на многообразиях

На самом деле, тот факт, что гладкое отображение $f\colon U \to V$ индуцирует морфизм $f^*\colon \Omega^\bullet(V) \to \Omega^\bullet(U)$ (т.е., что дифференциал коммутирует с пуллбэком) на более изысканном языке означает, что Ω^* является контравариантным функтором из категории евклидовых пространств (и гладких отображений между ними) в категорию коммутативных дифференциальных градуированных алгебр. Коммутативность тут имеется в виду кососимметричная, то есть

$$\tau \wedge \omega = (-1)^{\deg\tau\cdot\deg\omega}\omega\wedge\tau$$

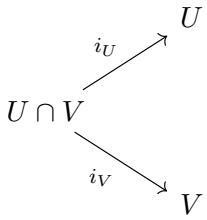
Более того, единственный такой функтор, совпадающий в нулевом члене с $C^\infty(\mathbb{R}^n)$ — это как раз $\Omega^\bullet$.

Действительно, из-за того, что $\Omega^0(\mathbb{R}^n) = C^\infty(\mathbb{R}^n)$, у нас сразу фиксирован базис из нужных $\mathrm{d}x_i$ (после того, как мы выбрали координатыне функции x_i), а дальше по линейности мы получаем всё те же 1-формы (и дальше по индукции).

Этот функтор однозначно продолжается на категорию гладких многообразий.

Определение 22. Пусть M — гладкое многообразие, покрытое картами $\{(U_\alpha, \varphi_\alpha)\}_\alpha$. Тогда дифференциальная форма ω на M задаётся набором форм ω_α, каждая из которых задана в карте $U_\alpha \cong \mathbb{R}^n$, причём они согласованы на пересечении.

Формальнее, у нас есть отображения



и мы требуем, чтоб $i_U^*\omega_U = i_V^*\omega_V$ на $U \cap V$.

Пример 12. Приведём несколько примером дифференциальных форм на многообразиях:

2.4 Точная последовательность Майера-Виеториса

Начнём с напоминания про пуллбэк: если $f\colon M \to N$, причем в M координаты $x_1, \ldots, x_m$, а в N координаты $y_1, \ldots, y_n$, то

$$f^*(\mathrm{d}y_i) = \sum_{j=1}^{n} \frac{\partial y_i}{\partial x_j} \mathrm{d}x_j.$$

Тогда мы сможем считать и пуллбэки форм:

$$f^*(F(y_1, \ldots, y_n)\mathrm{d}y_1 \wedge \ldots \wedge \mathrm{d}y_k) = F(y_1(x_1, \ldots, x_m), \ldots) f^*(\mathrm{d}y_1) \wedge \ldots \wedge f^*(\mathrm{d}y_k).$$

Но можно говорить и иначе (мы немного говорили про этот подход в первом параграфе). А именно, как мы помним, формы $\mathrm{d}y_i$ можно вычислять на касательных векоторах $\sum a_j \frac{\partial}{\partial y_j}$, как

$$\mathrm{d}y_i \left(\sum a_j \frac{\partial}{\partial y_j} \right) = a_i.$$

Тогда k-формы у нас действуют на наборах из k векторов (как элемент $\Lambda^k T^*M$).

Пусть $f_* = \mathrm{d}f\colon TM \to TN$, тогда

$$f_* \left(\frac{\partial}{\partial x_j} \right) = \left(\frac{\partial y_1}{\partial x_j}, \ldots, \frac{\partial y_n}{\partial x_j} \right).$$

Соответственно, пуллбэк $f^*(\omega)$ мы тогда можем определить, как k-форму, действующую на наборах из k векторов следующим образом:

$$f^*(\omega)(v_1, \ldots, v_k) \stackrel{\text{def}}{=} \omega(f_* v_1, \ldots, f_* v_k).$$

Проверим, что для 1-форм это определение совпадает с предыдущим:

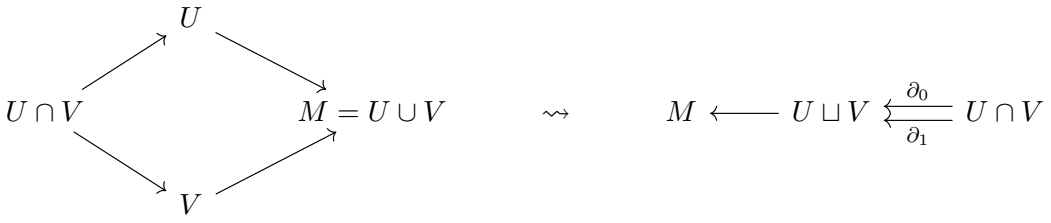
$$f^*(\mathrm{d}y_i) = \sum a_j \mathrm{d}x_j, \quad a_j = \mathrm{d}y_i \left(f_* \frac{\partial}{\partial x_j} \right) = \mathrm{d}y_i \left(\frac{\partial y_1}{\partial x_j}, \ldots, \frac{\partial y_n}{\partial x_j} \right) = \frac{\partial y_i}{\partial x_j},$$

а этот коэффициент совпадает с тем, который был в предыдущем определении. Отсюда сразу следует, что это определение совпадает предыдущим и для k-форм.

Замечание. Как мы уже отмечали, для форм с компактным носителем пулбэк определён только для собственных отображений. Зато определён *пушфорвадр* (т.е. отображение в другую сторону) для открытых вложений (и, соответственно, пуллбэк для обратных отображений). Отсюда следует, в частности, что мы можем корректно (и так же как в обычном случае) определять формы с компактным носителем для многообразий.

Перейдём к **точной последовательности Майера-Виеториса:**

Пусть $M = U \cup V$, U и V — открытые. Тогда у нас есть диаграммы:



Применяя функтор $\Omega^\bullet$, имеем

$$\Omega^*(M) \longrightarrow \Omega^*(U) \oplus \Omega^*(V) \underset{\partial_1^*}{\overset{\partial_0^*}{\rightrightarrows}} \Omega^*(U \cap V)$$

Последовательностью Майера-Вьеториса называется последовательность комплексов

$$0 \longrightarrow \Omega^*(M) \longrightarrow \Omega^*(U) \oplus \Omega^*(V) \xrightarrow[(\omega,\tau)\mapsto\tau-\omega]{} \Omega^*(U \cap V) \longrightarrow 0$$

Замечание. Стрелка $\Omega^*(M) \to \Omega^*(U) \oplus \Omega^*(V)$ — это сужение: $\omega \mapsto \omega|_U \oplus \omega|_V$. И, в следующей стрелке, когда мы берём разность, её мы тоже сужаем на $U \cap V$.

Отметим, что под сужением на подмногообразие мы понимаем пулбек индуцированный вложением.

Лемма 12. Последовательность Майера-Виеториса точна.

Доказательство. Точность в первых двух членах очевидна (дольше писать, чем думать):

Проверим, что стрелка $\Omega^*(M) \to \Omega^*(U) \oplus \Omega^*(V)$ инъективна. Действительно, если $\omega|_U = 0$ и $\omega|_V = 0$, то $\omega = 0$ (так как $M = U \cup V$).

Теперь проверим точность в среднем члене. $\mathrm{Ker}(\Omega^*(U) \oplus \Omega^*(V) \to \Omega^*(U \cap V))$ — это формы $\tau \in \Omega^*(V)$ и $\omega \in \Omega^*(U)$, которые совпадают на $U \cap V$. Тогда просто по определению, так как формы согласованы на пересечении, из них можно склеить одну на M (это доказывает включение $\mathrm{Ker}(\Omega^*(U) \oplus \Omega^*(V) \to \Omega^*(U \cap V)) \subset \mathrm{Im}(\Omega^*(M) \to \Omega^*(U) \oplus \Omega^*(V))$). С другой же стороны, если мы возьмём $\omega \in \Omega^*(M)$ и пройдём по двум стрелкам подряд, мы получим ноль:

$$\omega \mapsto (\omega|_U, \omega|_V) \mapsto (\omega|_U - \omega|_V)|_{U\cap V} = \omega|_{U\cap V} - \omega|_{U\cap V} = 0.$$

Так мы получаем, что $\mathrm{Im}(\Omega^*(M) \to \Omega^*(U) \oplus \Omega^*(V)) \subset \mathrm{Ker}(\Omega^*(U) \oplus \Omega^*(V) \to \Omega^*(U \cap V))$.

Теперь докажем точность в правом члене. Для этого воспользуемся разбиением единицы.

Докажем сначала для функций (для форм отсюда будет следовать афтоматически). Пусть $f \in \Omega^0(U \cap V)$, представим её в виде разности функций из $\Omega^0(U)$ и $\Omega^0(V)$. Пусть $\{\rho_U, \rho_V\}$ — разбиение единицы, подчиненное покрытию $\{U, V\}$. Тогда мы определим $f_U = f \cdot \rho_V$, $f_V = -f \cdot \rho_U$. Тогда

$$f\rho_V - (-f\rho_U) = f \cdot (\rho_U + \rho_V) = f \text{ на } U \cap V.$$

□

Теперь вспомним, что короткая точная последовательность комплексов индуцирует длинную точную последовательность когомологий.

$$\begin{array}{l} \ldots \longrightarrow H^k(M) \longrightarrow H^k(U)\oplus H^k(V) \longrightarrow H^k(U\cap V) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \big\downarrow \mathrm{d}^* \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad H^{k+1}(M) \longrightarrow H^{k+1}(U)\oplus H^{k+1}(V) \longrightarrow H^{k+1}(U\cap V) \longrightarrow \ldots \end{array}$$

Её также называют **точной последовательностью Майера-Виеториса**.

Опишем явно, как выглядит связывающий кограничный гомоморфизм). Для этого нужно выполнить несложный диаграммный поиск. А именно, возьмём класс когомологий $[\omega] \in H^k(U\cap V)$ и выберем какого-то представителя $\omega \in \Omega^k(U\cap V)$. Отправим его наверх; так как это класс когомологий, $\mathrm{d}\omega = 0$. Теперь посмотрим из кого он пришёл и снова перейдём вверх. Так мы получим, что из пара форм $(\mathrm{d}(\rho_V\omega), -\mathrm{d}\rho_U\omega))$ согласована на пересечении и приходит из некоторой формы, которая и является $\mathrm{d}^*\omega$.

$$\begin{array}{ccccccccc} & & \mathrm{d}^*\omega & \longmapsto & (\mathrm{d}(\rho_V\omega), -\mathrm{d}(\rho_U\omega)) & \longmapsto & \mathrm{d}\omega = 0 & & \\ & & & \nearrow & & \nwarrow & & & \\ 0 & \longrightarrow & \Omega^{k+1}(U\cup V) & \longrightarrow & \Omega^{k+1}(U)\oplus\Omega^{k+1}(V) & \longrightarrow & \Omega^{k+1}(U\cap V) & \longrightarrow & 0 \\ & & \uparrow \mathrm{d} & & \uparrow \mathrm{d} & & \uparrow \mathrm{d} & & \\ 0 & \longrightarrow & \Omega^{k}(U\cup V) & \longrightarrow & \Omega^{k}(U)\oplus\Omega^{k}(V) & \longrightarrow & \Omega^{k}(U\cap V) & \longrightarrow & 0 \\ & & & \searrow & & \swarrow & & & \\ & & & & (\rho_V\omega, -\rho_U\omega) & \longmapsto & \omega & & \end{array}$$

Более того, слово «некоторый» тут исключительно в художественных целях, на самом то деле, как легко видеть из диаграммного поиска:

$$\mathrm{d}^*[\omega] = \begin{cases} [-\mathrm{d}(\rho_V\omega)] \text{ на } U \\ [\mathrm{d}(\rho_U\omega)], \text{ на } V \end{cases} .$$

Последовательность Майера-Виеториса для форм с компактным носителем:

Напомним, что функтор $\Omega^\bullet_c(\_)$ удовлетворяет таким свойствам:

- $\Omega^\bullet_c(\_)$ является контравариантным функтором относительно *собственных отображений.*
- $\Omega^\bullet_c(\_)$ является ковариантным функтором относительно *открытых вложений.*

В дальнейшем мы будем использовать именно ковариантную версию этого функтора. Тогда диаграмма

$$M \longleftarrow U\sqcup V \lessdot U\cap V$$

индуцирует короткую точную последовательность комплексов

$$0 \longleftarrow \Omega^\bullet_c(M) \xleftarrow[(\alpha,\beta)\mapsto\alpha+\beta]{} \Omega^\bullet_c(U)\oplus\Omega^\bullet_c(V) \xleftarrow[\alpha\mapsto(\alpha,-\alpha)]{} \Omega_c(U\cap V) \longleftarrow 0$$

Лемма 13. Последовательность Майера-Виеториса для форм с компактным носителем точна.

Доказательство. Здесь всё гораздо проще, чем в предыдущий раз. Обсудим точность в последнем члене. Гомоморфизм $\Omega_c^\bullet(M) \leftarrow \Omega_c^\bullet(U) \oplus \Omega_c^\bullet(V)$ сюръективен, так как прообразом формы ω является пара $(\rho_U\omega, \rho_V\omega)$ (где $\{\rho_U, \rho_V\}$ — разбиение единицы, подчинённое покрытию $\{U, V\}$). □

Замечание. Отметим, что в случае последовательности Майера-Виеториса для всех форм из формы на многообразии форму на кусочках мы получали так:

$$\omega \mapsto (\rho_V\omega, -\rho_U\omega).$$

В то же время, в компактном случае мы поступаем несколько иначе

$$(\omega\rho_U, \omega\rho_V) \mapsto \omega.$$

Тогда короткая точная последовательность комплексов индуцирует длинную точную последовательность когомологий (но, в другую сторону!)

$$\begin{array}{ccccccc}
 & & & & H_c^{k+1}(U\cap V) & & \\
 & & & & \uparrow{\scriptstyle \mathrm{d}^*} & & \\
\vdots & & & & H_c^k(M) & \longleftarrow & H_c^k(U)\oplus H_c^k(V) \longleftarrow H_c^k(U\cap V) \\
\uparrow & & & & & & \uparrow \\
H_c^{k+1}(M) & \longleftarrow & H_c^{k+1}(U)\oplus H_c^{k+1}(V) & \longleftarrow & & & \vdots
\end{array}$$

Пример 13. Переписать из книжки пример про окружность.

2.5 Лемма Пуанкаре для когомологий де Рама

Замечание. В этом параграфе мы не пользуемся обозначением $\wedge$ для внешнего произведения. А может быть, стоило.

Рассмотрим диаграммы:

$$\begin{array}{ccc}
\mathbb{R}^n\times\mathbb{R} & & \Omega^\bullet(\mathbb{R}^n\times\mathbb{R}) \\
\pi\downarrow \quad \uparrow s & \rightsquigarrow & \pi^*\uparrow \quad \downarrow s^* \\
\mathbb{R} & & \Omega^\bullet(\mathbb{R}^n)
\end{array}$$

где π — проекция на первые n координат (т.е. $\pi(x,t) = x$), а s — сечение, т.е. $s(x) = (x, 0)$. Покажем, что отображения $\pi \circ s$ и $s \circ \pi$ индуцируют изоморфизм на когомологиях.

Во-первых, по очевидным причинам $\pi \circ s = \mathrm{id}$, откуда $s^* \circ \pi^* = \mathrm{id}$ (т.е. отображение тождественно уже на уровне форм, а значит, индуцирует изоморфизм на когомологиях). Но вот $s \circ \pi(x,t) = (x, 0)$ и отображение $\pi^* \circ s^*$ уже не тождественно на уровне форм (например, оно переводит $f(x,t)$ в $f(x,0)$). Но изоморфизм в когомологиях оно всё-таки индуцирует. Чтоб доказать это, мы покажем, что $\pi^* \circ s^*$ цепно-гомотопно тождественному:

$$\mathrm{id} - \pi^* \circ s^* = \pm(\mathrm{d}K \pm K\mathrm{d}).$$

Как мы помним, цепно-гомотопные отображения индуцируют одинаковые отображения в когомологиях, так что этого достаточно.

Заметим, что любая форма на $\mathbb{R}^n \times \mathbb{R}$ представляется в виде линейной комбинации форм одного из двух видов:

1. $(\pi^*\varphi)f(x,t)$
2. $(\pi^*\varphi)f(x,t)\mathrm{d}t$,

так как там либо есть $\mathrm{d}t$, либо нет.

Посмотрим сначала, как s^* действует на формы. Рассмотрим форму $f(x,t)\mathrm{d}x_I \wedge \mathrm{d}t$. Тогда, так как $s^*(\mathrm{d}t) = 0$, $s^*(f(x,t)\mathrm{d}x_I \wedge \mathrm{d}t) = 0$. Если же сверху у нас форма $f(x,t)\mathrm{d}x_I$, то $s^*(f(x,t)\mathrm{d}x_I) = f(x,0)\mathrm{d}x_I$.

Теперь определим $K\colon \Omega^q(\mathbb{R}^n \times \mathbb{R}) \to \Omega^{q-1}(\mathbb{R}^n \times \mathbb{R})$ следующим образом:

$$K((\pi^*\varphi)f(x,t)) = 0, \quad K((\pi^*\varphi)f(x,t)\mathrm{d}t) = (\pi^*\varphi)\int\limits_0^t f(s,t)\mathrm{d}s.$$

Проверим, что K действительно является оператором цепной гомотопии. Само собой, это достаточно проверять отдельно на функциях двух типов:

- Пусть $\omega = (\pi^*\varphi)f(x,t)$, $\deg\omega = q$. Тогда

  $$(\mathrm{id} - \pi^* \circ s^*)\omega = (\pi^*\varphi)f(x,t) - (\pi^*\varphi)f(x,0).$$

  В то же время, так как K ноль на формах первого типа,

  $$(\mathrm{d}K - K\mathrm{d})\omega = -K\mathrm{d}\omega.$$

  $$\mathrm{d}((\pi^*\varphi)f(x,t)) = \mathrm{d}\pi^*\varphi \cdot f(x,t) + (-1)^q\pi^*\varphi \cdot \left(\sum_{j=1}^n \frac{\partial f}{\partial x_j}(x,t)\mathrm{d}x_j + \frac{\partial f(x,t)}{\partial t}\mathrm{d}t\right).$$

  $$K\left(\mathrm{d}\pi^*\varphi \cdot f(x,t) + (-1)^q\pi^*\varphi \cdot \left(\sum_{j=1}^n \frac{\partial f}{\partial x_j}(x,t)\mathrm{d}x_j + \frac{\partial f(x,t)}{\partial t}\mathrm{d}t\right)\right).$$

  теперь заметим, что в первых двух слагаемых $\mathrm{d}t$ нет, поэтому K их занулит. На остальное он подействует вот так:

  $$-K\left((-1)^q\pi^*\varphi \cdot \frac{\partial f(x,t)}{\partial t}\mathrm{d}t\right) = (-1)^{q-1}\pi^*\varphi\int\limits_0^t \frac{\partial f(x,t)}{\partial t}\mathrm{d}t = (-1)^{q-1}\pi^*\varphi(f(x,t) - f(x,0)).$$

  Таким образом, на формах первого типа мы получили

  $$\mathrm{id} - \pi^* \circ s^* = (-1)^{q-1}(\mathrm{d}K - K\mathrm{d}).$$

- Теперь пусть $\omega = (\pi^*\varphi)f(x,t)\mathrm{d}t$, $\deg\omega = q$. Тогда:

  $$\mathrm{d}\omega = \mathrm{d}\pi^*\varphi \cdot f(x,t)\mathrm{d}t + (-1)^{q-1}\pi^*\varphi \cdot \left(\sum_{j=1}^n \frac{\partial f(x,t)}{\partial x_j}\mathrm{d}x_j\right)\mathrm{d}t$$

  Теперь заметим, что так как $s^*(\mathrm{d}t) = 0$, мы имеем $\pi^* \circ s^*(\mathrm{d}t) = 0$, откуда

  $$(\mathrm{id} - \pi^* \circ s^*)\omega = \omega.$$

  С другой же стороны,

  $$K\mathrm{d}\omega = (\mathrm{d}\pi^*\varphi)\int\limits_0^t f(x,s)\mathrm{d}s + (-1)^{q-1}(\pi^*\varphi)\sum_{j=1}^n\int\limits_0^t \frac{\partial f(x,s)}{\partial x_j}\mathrm{d}x_j\mathrm{d}s$$

  $$\mathrm{d}K\omega = \mathrm{d}\left(\pi^*(\varphi)\int\limits_0^t f(x,s)\mathrm{d}s\right) = \sum_{j=1}^n \pi^*(\varphi)\int\limits_0^t \frac{\partial f(x,s)}{\partial x_j}\mathrm{d}x_j\mathrm{d}s + \mathrm{d}\pi^*(\varphi)\cdot\int\limits_0^t f(x,s)\mathrm{d}s,$$

  откуда видно, что

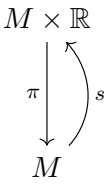
  $$\mathrm{d}K - K\mathrm{d} = (-1)^{q-1}\omega.$$

Таким образом, мы доказали лемму Пуанкаре для когомологий де Рама:

Лемма 14 (Пуанкаре)**.** Когомологии де Рама пространства $\mathbb{R}^n$ имеют следующий вид:

$$H^q_{\mathrm{dR}}(\mathbb{R}^n) = H^q_{\mathrm{dR}}(\mathrm{pt}) = \begin{cases} \mathbb{R}, & q = 0 \\ 0, & \text{иначе.} \end{cases}$$

Дословно повторяя всё то же самое, можно получить такой же результат для:



где M — гладкое многообразие. Действительно, если M покрыть атласом $\{U_\alpha\}$, то $m \times \mathbb{R}$ покроется атласом $U_\alpha \times \mathbb{R}$. Тогда в каждой карте у нас будет происходить всё то же самое, что и в случае $\mathbb{R}^n \times \mathbb{R}$. Так как внешний дифференциал коммутирует с пуллбэком, это не будет зависеть от выбора координат и мы получим, что в каждой карте (а значит и на всём многообразии) у нас вновь есть карты двух типов и мы можем совершенно аналогично построить цепную гомотопию K. Таким образом, получаем

Следствие 11. $H^q_{\mathrm{dR}}(M \times \mathbb{R}) \cong H^q(M)$.

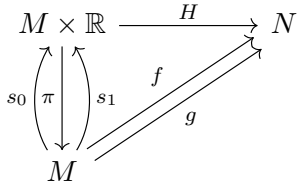
Отсюда мы получаем гомотопиечскую инвариантность когомологий де-Рама:

Следствие 12. *Гомотопные гладкие отображения индуцируют одинакоые отоюражения в когомологиях.*

Замечание. Пусть $f, g\colon M \to N$. Под гладкой гомотопией мы тут понимаем такое отображение $H\colon M \times \mathbb{R} \to N$, что

$$H(x,t) = \begin{cases} f(x), & t \geq 1 \\ g(x), & t \leq 0. \end{cases}$$

Доказательство. Пусть H — гомотопия между f и g. Тогда у нас есть такая диаграмма:



то есть $f = H \circ s_1,\ g = H \circ s_0$. Тогда $f^* = s_1^* \circ H^*$, $g^* = s_0^* \circ H^*$, а тогда, так как s_1^* и s_0^* оба обратные к π^*, отсюда ясно, что $f^* = g^*$. □

Следствие 13. *Гомотопически эквивалентные многообразия имеют однаковые когомологии де Рама.*

Действительно, тут нужно просто воспользоваться функториальностью когомологий.

Замечание. При всех разговорах про гомотопии, мы подразумеваем, что читателю известно, что любое непрерывное отображение гомотопно гладкому, и в частнсоти, что гомотопию тоже можно всегда выбирать гладкой (так как отображения можно сглаживать с фиксацией на подмножестве).

Следствие 14. *В частности, деформационная ретракция индуцирует тождественное отображение в когомологиях.*

2.6 Когомологии сферы

Покроем S^n двумя дисками U и V так, чтоб верхнее немножко наезжало на нижнее и применим точную послеовательность Майера-Виеториса. Перед этим отметим, что $U \cap V \cong S^{n-1} \times \mathbb{R}$. Тогда

$$\begin{array}{ccccc} \dots & & & & \\ \downarrow & & & & \\ H^q(S^n) & \longrightarrow & H^q(U) \oplus H^q(V) & \longrightarrow & H^q(S^{n-1} \times \mathbb{R}) \\ & & & & \downarrow \\ & & & & H^{q+1}(S^n) \longrightarrow H^{q+1}(U) \oplus H^{q+1}(V) \longrightarrow \dots \end{array}$$

Так как диск диффеоморфен $\mathbb{R}^n$, по лемме Пуанкаре $H^q_{\mathrm{dR}}(U) = H^q_{\mathrm{dR}}(V) = 0$ при $q \neq 0$. Кроме того, по следствию леммы Пуанкаре $H^q(S^{n-1} \times \mathbb{R}) = H^q(S^{n-1})$, то есть на самом деле последовательность выглядит вот так:

$$\begin{array}{ccccc} \dots & & & & \\ \downarrow & & & & \\ H^q(S^n) & \longrightarrow & 0 & \longrightarrow & H^q(S^{n-1}) \\ & & & & \downarrow \\ & & & & H^{q+1}(S^n) \longrightarrow 0 \longrightarrow \dots \end{array}$$

Отсюда мы сразу имеем

$$H^{q+1}(S^n) \cong H^q(S^{n-1}),$$

откуда по индукции мы сразу получаем

$$H^q(S^n) = \begin{cases} \mathbb{R}, & q = n \text{ или } 0. \\ 0, & q \neq n. \end{cases}$$

Точнее говоря, случай $q = 0$ нужно разобрать отдельно руками.

Форма объема для сферы

Пусь $\sum x_i^2 = r^2$, тогда форма

$$\omega = \frac{1}{r} \sum_{j=1}^{n} x_j \mathrm{d}x_1 \wedge \ldots \wedge \overline{\mathrm{d}x_j} \wedge \mathrm{d}x_n$$

будет формой объема для сферы, то есть

$$\int\limits_{S^{n-1}} \omega = \mathrm{Vol}_{n-1}(S^{n-1}).$$

Заметим, что $\mathrm{d}\omega \in H^n(S^{n-1})$, а значит, $[\mathrm{d}\omega] = 0$ просто из соображений размерности. С другой же стороны, эта форма не может быть точной, так как если $\omega = \mathrm{d}\alpha$, то тогда по формуле Стокса

$$\int\limits_{S^{n-1}} \omega = \int\limits_{B_1} \mathrm{d}\omega = \int\limits_{B} d^2\alpha = 0.$$

Значит, мы явно нашли образующую $H^n_{\mathrm{dR}}(S^n)$.

2.7 Лемма Пуанкаре для компактных когомологий

Мы будем доказывать, что

$$H_c^{q+1}(\mathbb{R}^n \times \mathbb{R}) = H_c^q(\mathbb{R}^n).$$

Замечание. Рассмотрим сначала общую ситуацию: пусть $\pi\colon M \times \mathbb{R} \to M$ — проекция. Тогда пулбек формы из $\Omega_c^\bullet(M)$ уже не имеет компактного носителя (так как она постоянна вдоль слоёв).

Однако, есть отображение интегрирования вдоль слоя:

$$\pi_*\colon \Omega_c^\bullet(M \times \mathbb{R}) \to \Omega_c^{\bullet-1}(M)).$$

Оно определяется по отдельности на формах двух типов:

- $\pi_*(\varphi f(x,t)) = 0$.
- $\pi_*(\varphi f(x,t)\mathrm{d}t) = \varphi \int\limits_{-\infty}^{+\infty} f(x,t)\mathrm{d}t$.

  Интеграл тут определён корректно, так как форма имела компактный носитель.

Нетрудно проверить, что $\mathrm{d}\pi_* = \pi_*\mathrm{d}$. Определим также отображение

$$e_*\colon \Omega_c^\bullet(M) \to \Omega_c^{\bullet+1}(M \times \mathbb{R}),\ \varphi \mapsto (\pi^*\varphi) \wedge e,$$

где e — это форма с компактным носителем на $\mathbb{R}$ такая, что $\int_{\mathbb{R}} e = 1$.

Очевидно, что $\pi_* \circ e_* = \mathrm{id}$ на $\Omega_c^\bullet(\mathbb{R}^n)$. А вот $e_* \circ \pi_*$ уже не тождественно на уровне форм, но, опять же, цепногомотопно тождественному отображению. Это проверяется также, как и для обычных когомологий де Рама.

Отсюда мы получаем, что

$$H_c^q(\mathbb{R}^n) = \begin{cases} \mathbb{R}, & q = n \\ 0, & \text{иначе} \end{cases}.$$

Причём, изоморфизм тут такой же, как был у нас в случае $\mathbb{R}^1$:

$$\omega \mapsto \int\limits_{\mathbb{R}^n} \omega$$

Образующей $H_c^n(\mathbb{R}^n)$ будет форма

$$e(x_1)\mathrm{d}x_1 \wedge e(x_2)\mathrm{d}x_2 \wedge \ldots \wedge e(x_n)\mathrm{d}x_n.$$

Замечание. Отсюда также можно уследить, что когомологии с компактным носителем не гомотопически инвариантны. Чтоб в этом убедиться, можно, например, вычислить компактные когомологии открытого цилиндра и открытого листа Мёбиуса.

2.8 Умножение в когомологиях де Рама

Вообще говоря, при помощи $\wedge$-произведения можно умножать формы, что наводит на мысль о том, что это может превращать когомологии в градуированное кольцо. Покажем, что это действительно так, то есть, что умножение

$$\wedge\colon \Omega^k(M) \times \Omega^\ell(M) \to \Omega^{k+\ell}(M), \quad (w,v) \mapsto w \wedge v$$

продолжается до умножения в когомологиях. Определим умножение в когомологиях следующим образом:

$$\wedge\colon H^k(M) \times H^\ell(M) \to H^{k+\ell}(M), \quad [w] \wedge [v] = [w \wedge v].$$

Покажем, что это определение корректно, т.е. не зависит от выборов представителей. Нам надо показать, что

$$[(w + \mathrm{d}\alpha) \wedge (v + \mathrm{d}\beta)] = [w \wedge v]$$

для замкнутых форм $w \in \Omega^k(M),\ v \in \Omega^\ell(M)$ и произвольных $\alpha \in \Omega^{k-1}(M),\ \beta \in \Omega^{\ell-1}(M)$. Действительно,

$$(w + \mathrm{d}\alpha) \wedge (v + \mathrm{d}\beta) = w \wedge v + w \wedge \mathrm{d}\beta + \mathrm{d}\alpha \wedge v + \mathrm{d}\alpha \wedge \mathrm{d}\beta.$$

Покажем, что всё кроме первого слагаемого — точная форма. Действительно, рассмотрим

$$\tau = \alpha \wedge v + (-1)^k w \wedge \beta + \alpha \wedge \mathrm{d}\beta.$$

Перед тем, как дифференцировать, напомним, что внешний дифференциал удовлетворяет правилу лейбница, то есть

$$\mathrm{d}(w \wedge v) = \mathrm{d}w \wedge v + (-1)^k w \wedge \mathrm{d}v,\ w \in \Omega^k(M),\ v \in \Omega^\ell(M).$$

Теперь продифференцируем форму τ:

$$\mathrm{d}\tau = \mathrm{d}\alpha \wedge v + (-1)^{k-1}\alpha \wedge \mathrm{d}v + (-1)^k \mathrm{d}w \wedge \beta + w \wedge \mathrm{d}\beta + \mathrm{d}\alpha \wedge \mathrm{d}\beta.$$

Теперь воспользуемся тем, что $\mathrm{d}w = \mathrm{d}v = 0$, тогда

$$\mathrm{d}\tau = \mathrm{d}\alpha \wedge v + w \wedge \mathrm{d}\beta + \mathrm{d}\alpha + \mathrm{d}\beta.$$

Таким образом,

$$(w + \mathrm{d}\alpha) \wedge (v + \mathrm{d}\beta) = w \wedge v + \mathrm{d}\tau \implies [(w + \mathrm{d}\alpha) \wedge (v + \mathrm{d}\beta)] = [w \wedge v].$$

Таким образом, внешнее произведение превращает

$$H^\bullet(M) = \bigoplus_{i=1}^{\infty} H^i(M)$$

в градуированное кольцо.

Теперь пусть у нас есть отображения f и g, которые осуществляют гомотопическую эквивалентность многообразий M и N. Заметим, что тогда просто по определению пуллбека, мы имеем

$$f^*(w \wedge v) = f^*(w) \wedge f^*(v) \quad \forall w \Omega^k(N),\ v \in \Omega^\ell(N).$$

Так как при гомотопической эквивалентности f^* и g^* — изоморфизмы на когомологиях, мы получаем, что f^* — изоморфизм градуированных алгебр $H^\bullet(N)$ и $H^\bullet(M)$.

2.9 Аргумент Майера-Виеториса

Определение 23. Пусть M — многообразие размерности n. Его открытое покрытие $\{U_\alpha\}_\alpha$ называется *хорошим*, если все конечные пересечения $U_{\alpha_0} \cap \ldots U_{\alpha_n}$ диффеоморфны $\mathbb{R}^n$.

Теорема 23. *Любое многообразие имеет хорошее покрытие.*

Набросок доказательства. Во-первых, для этого нам понадобится риманова метрика на многообразии. То, что любое гладкое многообразие метризуемо, следует например из теоремы вложения Уитни. Или, например, можно взять покрытие M координатными шарами U_α, взять гладкую риманову метрику (пулбек стандартного скалярного произведения) $\langle \cdot, \cdot \rangle_\alpha$ из них и сложить с весами из разбиения единицы, подчиненного покрытию U_α:

$$\langle \cdot, \cdot \rangle = \sum_\alpha \rho_\alpha \langle \cdot, \cdot \rangle_\alpha.$$

Так вот, как только у нас есть разбиение единицы, известно, что каждая точка в многообразии имеет геодезически выпуклую окрестность. Тогда, если мы возьмём покрытие геодезически выпуклыми окрестностями (каждая из них диффеоморфна $\mathbb{R}^n$), все конечные пересечения будут диффеоморфны $\mathbb{R}^n$, как мы и хотели. □

Предложение 6. *Если многообразие M имеет конечное хорошее покрытие, тогда его когомологии де Рама (и компактные когомологии) конечномерны.*

Доказательство. Будем использовать индукцию по покрытию и последовательность Майера-Виеториса.
Шаг 1. Запишем последовательность Майера-Виеториса:

$$\begin{array}{ccccccc} \vdots & & & & & & \\ \downarrow & & & & & & \\ H^{q-1}(U\cap V) & \xrightarrow{\mathrm{d}^*} & H^q(M) & \xrightarrow{i^*} & H^q(U)\oplus H^q(V) & \longrightarrow & H^q(U\cap V) \\ & & & & & & \downarrow \\ & & & & & & \vdots \end{array}$$

Заметим, что $H^q(M) \cong \operatorname{Im} i^* \oplus \operatorname{Ker} i^* \cong \operatorname{Im} i^* \oplus \operatorname{Im} \mathrm{d}^*$ по точности последовательности. Тогда ясно, что если когомологии U, V и $U \cap V$ конечномерны, то $H^q(M)$ тоже конечномерны.
Шаг 2. Теперь запустим индукцию по мощности покрытия. Пусть утверждение верно для любого многообразия, допускающего хорошее покрытие из не более чем k элементов. Рассмотрим многообразие M, имеющее хорошее покрытие из $(k+1)$-го элемента $\{U_0, \dots, U_k\}$.

Положим $U = U_p$, $V = U_0 \cup U_1 \cup \dots \cup U_{p-1}$. Тогда по индукционному предположению $H^q(U)$, $H^q(V)$, $H^q(U \cap V)$ конечномерны, откуда по шагу 1 $H^q(U \cup V)$ конечномерны, что мы и хотели. □

2.10 Двойственность Пуанкаре

Пусть V и W конечномерные векторные пространства. Напомним, что спаривание

$$\langle \cdot, \cdot \rangle \colon V \otimes W \to \mathbb{R}$$

называется *невырожденным*, если

$$\langle v, w \rangle = 0 \; \forall w \in W \implies v = 0.$$

Заметим, что это эквивалентно тому, что отображение $v \mapsto \langle v, \cdot \rangle$ определяет изоморфизм $V \cong W^*$.

Теорема 24 (Двойственность Пуанкаре)**.** *Пусть M — ориентируемое многообразие размерности n. Тогда*

$$\forall q \quad H^q(M) \cong \left(H_c^{n-q}(M)\right)^*.$$

Замечание. Мы докажем это в случае, когда M обладает конечным хоршим покрытием, но вообще, это ограничение не по существу (так как принцип Майера-Виеториса можно обобщить на произвольные ориентируемые многообразия). То есть, сформулироавнное в теореме верно и без условия на конечномерность когомологий (но, доказывать это мы не будем).

Доказательство. Для ориентируемого многообразия мы можем определить спаривание

$$\int\limits_M \colon H^q(M) \otimes H_c^{n-q}(M) \to \mathbb{R}, \; [\omega] \otimes [\alpha] \mapsto \int\limits_M \omega \wedge \alpha$$

Тут мы по существу пользуемся ориентируемостью, так как интегрирование корректно продолжается на когомологии при помощи теоремы Стокса.

Мы будем доказывать, что определённое выше спаривание невырождено. Для этого нам понадобится несколько лемм.

Напомним сначала 5-лемму:

Лемма 15 (5-лемма)**.** Рассмотрим диаграмму

$$\begin{array}{ccccccccccccc}
\dots & \longrightarrow & A & \xrightarrow{f_1} & B & \xrightarrow{f_2} & C & \xrightarrow{f_3} & D & \xrightarrow{f_4} & E & \longrightarrow & \dots \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} & & \\
\dots & \longrightarrow & A' & \xrightarrow[f_1']{} & B' & \xrightarrow[f_2']{} & C' & \xrightarrow[f_3']{} & D' & \xrightarrow[f_4']{} & E' & \longrightarrow & \dots
\end{array}$$

Предположим, что строки точны и $\alpha, \beta, \delta, \varepsilon$ — изоморфизмы. Тогда γ тоже изоморфизм.

Лемма 16. Следующая диаграмма коммутативна с точностью до знака:

$$\begin{array}{ccccccccc}
\dots & \longrightarrow & H^q(U\cup V) & \xrightarrow{\text{res}} & H^q(U)\oplus H^q(V) & \xrightarrow{-} & H^q(U\cap V) & \xrightarrow{\mathrm{d}^*} & H^{q+1}(U\cup V) \longrightarrow \dots \\
 & & \otimes & & \otimes & & \otimes & & \otimes \\
\dots & \longleftarrow & H_c^{n-q}(U\cup V) & \xleftarrow{+} & H_c^{n-q}(U)\oplus H_c^{n-q}(V) & \longleftarrow & H_c^{n-q}(U\cap V) & \xleftarrow{\mathrm{d}^*} & H_c^{n-q-1}(U\cup V) \longleftarrow \dots \\
 & & \downarrow{\scriptstyle \int_{U\cup V}} & & \downarrow{\scriptstyle \int_U + \int_V} & & \downarrow{\scriptstyle \int_{U\cap V}} & & \downarrow{\scriptstyle \int_{U\cup V}} \\
 & & \mathbb{R} & & \mathbb{R} & & \mathbb{R} & & \mathbb{R}
\end{array}$$

Доказательство леммы. коммутативность с точностью до знака тут означает следующее: например, если мы возьмём $\omega \in H^q(U\cap V)$ и $\tau \in H_c^{n-q-1}(U\cup V)$, то

$$\int\limits_{U\cap V} \omega \wedge \mathrm{d}_*\tau = \pm \int\limits_{U\cup V} \mathrm{d}^*\omega \wedge \tau.$$

Это означает, что взять форму из верхнего этажа третьего столбца и пойти направо, а потом вниз – это то же самое, что взять форму из нижнего этажа четвертого столбца и пойти направо, а потом вверх.

Проверим например, коммутативность правого квадрата (для левых квадратов тут немного проще). Возьмём $\omega H^q(U\cap V), \tau \in H^{n-q-1}(U\cup V)$. Напомним, что мы знаем явный вид кограничного связывающего гомоморфизма:

$$\mathrm{d}^*\omega = \begin{cases} -\mathrm{d}(\rho_V\omega), & \text{на } U \\ \mathrm{d}(\rho_U\omega), & \text{на } V \end{cases}, \quad \mathrm{d}_*\tau = \begin{cases} \mathrm{d}(\rho_U\tau), & \text{на } U \\ \mathrm{d}(\rho_U\omega), & \text{на } V \end{cases}.$$

Заметим, что так как эти формы из когомологий, они замкнутые, а тогда

$$\mathrm{d}(\rho_V\omega) = \mathrm{d}\rho_V \wedge \omega + \rho_v \mathrm{d}\omega = \mathrm{d}\rho_V \wedge \omega.$$

$$\mathrm{d}(\rho_V\tau) = \mathrm{d}\rho_V \wedge \tau + \rho_V \mathrm{d}\tau = \mathrm{d}\rho_V \wedge \tau.$$

Тогда то, что нам нужно показать сводится к перестановке сомножителей во внешнем произведении

$$\int\limits_{U\cap V} \omega \wedge \mathrm{d}_*\tau = \int\limits_{U\cap V} \omega \wedge \mathrm{d}\rho_V \wedge \tau = (-1)^{\deg\omega} \int\limits_{U\cap V} \mathrm{d}\rho_V \wedge \omega \wedge \tau = (-1)^{\deg\omega+1} \int\limits_{U\cap V} \mathrm{d}^*\omega \wedge \tau.$$

С другой стороны, так как $\mathrm{supp}(\mathrm{d}^*\omega) \subseteq U\cap V$.

Теперь заметим, что приведённая выше лемма означает, что диаграмма ниже коммутативна с точностью до знака:

□

$$\begin{array}{ccccccc} \dots \longrightarrow & H^q(U\cup V) & \longrightarrow & H^q(U)\oplus H^q(V) & \longrightarrow & H^q(U\cap V) & \longrightarrow \dots \\ & \downarrow & & \downarrow & & \downarrow & \\ \dots \longrightarrow & (H_c^{n-q}(U\cup V))^* & \longrightarrow & (H_c^{n-q}(U))^*\oplus(H_c^{n-q}(U))^* & \longrightarrow & (H_c^{n-q}(U\cap V))^* & \longrightarrow \dots \end{array}$$

Если пристально посмотреть на эту диаграмму, можно заметить, что из 5-леммы следует, что если мы знаем, что двойственность Пуанкаре выполнена для $U, V, U\cap V$, то мы знаем это и для $U\cup V$.

Теперь осталось запустить индукцию по размеру хорошего покрытия:

База. Если $M\cong\mathbb{R}^n$, то двойственность Пуанкаре следует из лемм Пуанкаре:

$$H^q(\mathbb{R}^n)=\begin{cases}\mathbb{R}, & q=0\\ 0, & \text{иначе}\end{cases},\qquad H_c^q(\mathbb{R}^n)=\begin{cases}\mathbb{R}, & q=n\\ 0, & \text{иначе}\end{cases}.$$

Переход. Делается также, как в теореме про конечномерность когомологий. □

Замечание. Обратное утверждение, то есть, что

$$H_c^q(M)\cong\big(H^{n-q}(M)\big)^*,$$

верно не всегда. Это связано с тем, что

$$M=\bigsqcup_{i=1}^{\infty}M_i\implies H^q(M)=\prod_{i=1}^{\infty}H^q(M_i),\quad H_c^q(M)\cong\bigoplus_{i=1}^{\infty}H^q(M_i).$$

Но, для компактных многообразий утверждений сохранится.

Из двойственности Пуанкаре сразу следует такой замечательный результат:

Теорема 25. *Пусть M — связное ориентированное многообразие размерности n. Тогда $H_c^n(M)=\mathbb{R}$. В частности, если M компактно, то $H^n(M)=\mathbb{R}$.*

Доказательство. В самом деле, по двойственности Пуанкаре $H_c^n(M)\cong(H^{n-n}(M))^*\cong\mathbb{R}^*\cong\mathbb{R}$. □

2.11 Формула Кюннета

Из двойственности Пуанкаре также можно не слишком сложным образом получить формулу Кюннета:

Теорема 26 (Формула Кюннета)**.** *Пусть M и N — многообразия. Тогда имеет место следующий изоморфизм градуированных колец:*

$$H^\bullet(M\times N)\cong H^\bullet(M)\otimes H^\bullet(N).$$

или же, иными словами,

$$H^n(M\times N)\cong\bigoplus_{p+q=n}H^p(M)\otimes H^q(N).$$

Доказательство. Будем опять пользоваться принципом Майера-Виеториса и 5-леммой. Пусть U и V — открытые подмножества в M, запишем точную последовательность Майера-Виеториса:

$$\dots\longrightarrow H^p(U\cup V)\longrightarrow H^p(U)\oplus H^p(V)\longrightarrow H^p(U\cap V)\longrightarrow\dots$$

Тензорно умножим её на $H^{n-p}(N)$ (так как тензорное произведение – это точный функтор, последовательность останется точной), получим диаграмму

$$\begin{array}{ccc} \dots\longrightarrow H^p(U\cup V)\otimes H^{n-p}(N) & \longrightarrow & H^p(U)\otimes H^{n-p}(N)\oplus H^p(V)\otimes H^{n-p}(N) \\ & & \downarrow \\ & & H^p(U\cap V)\otimes H^{n-p}(N)\longrightarrow\dots \end{array}$$

Просуммируем по p от 0 до n, получим точную последовательность

$$\begin{array}{ccccc} \dots \longrightarrow \bigoplus_{p=0}^{n} H^p(U\cup V)\otimes H^{n-p}(N) & \longrightarrow & \bigoplus_{p=0}^{n}(H^p(U)\otimes H^{n-p}(N))\oplus(H^p(V)\otimes H^{n-p}(N)) & & \\ & & \downarrow & & \\ & & \bigoplus_{p=0}^{n} H^p(U\cap V)\otimes H^{n-p}(F) & \longrightarrow & \dots \end{array}$$

Теперь заметим, что у нас есть следующая коммутативная диаграмма:

$$\begin{array}{ccccc} \bigoplus_{p=0}^{n} H^p(U\cup V)\otimes H^{n-p}(N) & \longrightarrow & \bigoplus_{p=0}^{n}(H^p(U)\otimes H^{n-p}(N))\oplus H^p(V)\otimes H^{n-p}(N) & \longrightarrow & \bigoplus_{p=0}^{n} H^p(U\cap V)\otimes H^{n-p}(N) \\ \downarrow\psi & & \downarrow\psi & & \downarrow\psi \\ H^n((U\cup V)\times N) & \longrightarrow & H^n(U\times N)\oplus H^n(V\times N) & \longrightarrow & H^n((U\cap V)\times F) \end{array}$$

где ψ определён так: у нас есть проекции на обе координаты ,

$$\begin{array}{ccc} M\times N & \xrightarrow{\rho} & N \\ {\scriptstyle\pi}\downarrow & & \\ M & & \end{array}$$

они естественным образом индуцируют отображение

$$\omega\otimes\varphi\mapsto\pi^*\omega\wedge\rho^*\varphi.$$

Это отображение и индуцирует нужное нам отображение в когомологиях:

$$\psi\colon H^\bullet(M)\otimes H^\bullet(N)\to H^\bullet(M\times N).$$

Так вот, в диаграмме выше нужно проверить какую-то коммутативность. Вообще говоря, нужно проверить коммутативность квадратов, например вот этого

$$\begin{array}{ccc} \bigoplus_{p=0}^{n}(H^p(U\cap V)\otimes H^{n-p}(N)) & \xrightarrow{\mathrm{d}^*} & \bigoplus_{p=0}^{n} H^{p+1}(U\cup V)\otimes H^{n-p}(N) \\ \psi\downarrow & & \downarrow\psi \\ H^n((U\cap V)\times N) & \xrightarrow{\mathrm{d}^*} & H^n((U\cup V)\times N) \end{array}$$

Но, делать это очень уж лень. Это делается стандартным образом, короче.

Так вот, по 5-лемме мы опять получаем, что если формула Кюннета верна для $U, V, U\cap V$, то она верна и для $U\cap V$. Далее нужно заметить, что в случае $\mathbb{R}^n$ утверждение следует из леммы Пуанкаре, а дальше нужно сделать такой же индукционный переход, как и в теореме ранее.

□

Похожими техниками можно получить следующее важное обобщение:

Теорема 27 (Лере, Хирш). *Пусть E — локально тривиальное расслоение над M со слоем F. Предположим, что нашлись классы $e_1, \dots, e_n \in H^\bullet(E)$ такие, что для любого вложения слоя $i\colon F \hookrightarrow E$ их пулбеки $i^*(e_1), \dots, i^*(e_n)$ — базис $H^\bullet(F)$ как векторного пространства над $\mathbb{R}$, то $\{e_1, \dots, e_n\}$ — базис $H^\bullet(E)$, как векторного пространства над $H^\bullet(M)$ и*

$$H^\bullet(M) \otimes H^\bullet(F) \cong H^\bullet(E).$$

2.12 Двойственный по Пуанкаре к замкнутому подмногообразию

Пусть M — ориентированное многообразие размерности n, а $S \subset M$ — замкнутое ориентированное подмногообразие[10] размерности k.

Пусть $i\colon S \hookrightarrow M$ — вложение, тогда S мы можем однозначно сопоставить некоторый класс $[\eta_S] \in H^{n-k}(M)$ следующим образом.

Пусть ω — замкнутая k-форма на M с компактным носителем. Так как S замкнутое, $\operatorname{supp}(\omega|_S) \subset S \cap \operatorname{supp}(\omega)$ компактно в M как замкнутое подмножество компакта. Тогда корректно определён интеграл $\int_S i^*\omega$, так как форма $i^*\omega$ имеет компактный носитель в S, $i^*\omega \in \Omega_c^k(S)$.

Соответственно, тогда $\int\limits_S$ индуцирует линейный функционал на $H_c^k(M)$. Тогда, так как по двойственности Пуанкаре $(H_c^k)^* \cong H^{n-k}(M)$, интегрированию по S однозначно соответствует некоторый класс $[\eta_S] \in H^{n-k}(M)$. Более того, как мы помним из конструкции

$$\int\limits_S i^*\omega = \int\limits_M \omega \wedge \eta_S \quad \forall [\omega] \in H_c^k(M).$$

И, как мы помним, это эквивалентное определение. То есть, если мы хотим проверить, что класс какой-то формы является двойственным по Пуанкаре к компактному подмногообразию S, нужно проверять именно это условие.

Этот класс мы и будем называть **(замкнутым) двойственным по Пуанкаре классом к** S.

Теперь пусть S — компактное подмногообразие. В этом случае можно сделать всё то же самое (и, двойственный по Пуанкаре существует), но ситуация несколько улучшается.

В этом случае у S есть еще и **компактный двойственный по Пуанкаре**. Действительно, $\int\limits_S$ определяет линейный функционал на $H^k(M)$ (вот тут мы пользуемся компактностью M), а тогда по двойственности Пуанкаре

$$\exists!\quad [\eta'_S] \in H_c^{n-k}(M).$$

Тут мы предполагаем, что M обладает конечным хорошим покрытием, чтоб выполнялся изоморфизм

$$(H^k(M))^* \cong H_c^{n-k}(M).$$

Компактный двойственный по Пуанкаре класс характеризуется таким свойством:

$$\int\limits_S i^*\omega = \int\limits_M \omega \wedge \eta'_S \quad \forall \omega \in H^k(M).$$

Отсюда видно, что в частности компактный двойственный по Пуанкаре является и замкнутым двойственным по Пуанкаре (как форма). Но отметим тут также, что сами классы в когомологиях могут быть совсем разными (и в задачах у нас есть такие примеры).

Пример 14. Дописать сюда вычисления примеров и разгон про замкнутые гомологии и компактные гомологии.

[10] Тут слово "замкнутое"имеет смысл "замкнутое подмножество"; S далеко не обязано быть компактным.

Пусть теперь мы работаем с компактным случаем, а $W \subset M$ — открытое подмножество, содержащее S. Тогда компактный двойственный по Пуанкаре к S в многообразии W (назовём его $\eta'_{S,W} \in H_c^{n-k}(W)$) продолжается нулём до компактного двойственного по Пуанкаре к S в M (его назовём $\eta'_S \in H_c^{n-k}(M)$):

$$\int_S i^*\omega = \int\limits_W \omega \wedge \eta'_{S,W} = \int\limits_M \omega \wedge \eta'_S.$$

Отсюда следует, что носитель компактного двойственного по Пуанкаре может быть стянут до любой окрестности S! И эту окрестность мы можем выбирать.

2.13 Напоминание про векторные расслоения и класс Тома

Определение 24. Пусть $\pi\colon E \to M$ — сюръективное отображений многообразий, причём $\forall x \in M\ \pi^{-1}(x)$ — векторное пространство.

Тогда (E, π) называется *гладким вещественным векторным расслоением* ранга n, если существует открытое покрытие M множествами $\{U_\alpha\}$ и набор отображений $\{\varphi_\alpha\}_\alpha$ такой что

- $\varphi_\alpha\colon \pi^{-1}(U_\alpha) \cong U_\alpha \times \mathbb{R}^n$ — диффеоморфизм.
- $\forall x \in U_\alpha$ оторбражение $v \mapsto \varphi_\alpha^{-1}(x, v)$ — это линейный изоморфизм между $\mathbb{R}^n$ и $\pi^{-1}(x)$. Говоря короче, на каждом слое отображения φ_α являются линейными изоморфизмами.
- Отображения
$$\varphi_\alpha \circ \varphi_\beta^{-1}\colon (U_\alpha \cap U_\beta) \times \mathbb{R}^n \to (U_\alpha \cap U_\beta) \times \mathbb{R}^n$$
на каждом слое являются автоморфизмами $\mathbb{R}^n$ и таким образом порождают отображения
$$g_{\alpha\beta}\colon U_\alpha \cap U_\beta \to \mathrm{GL}_n(\mathbb{R}), \quad g_{\alpha\beta} = \varphi_\alpha \circ \varphi_\beta^{-1}|_{\{x\}\times\mathbb{R}^n}.$$

Далее все расслоения мы будем полагать именно такими. Кроме того, мы будем полагать, что многообразие M ориентированно, переходы имеют положительный определитель и как следствие, расслоение E также ориентированно (это нам понадобится, чтоб использовать формулу Стокса).

Замечание. Функции перехода $g_{\alpha\beta}$ удовлетворяют следующему условию:

$$g_{\alpha\beta} \circ g_{\beta\gamma} = g_{\alpha\gamma} \text{ на } U_\alpha \cap U_\beta \cap U_\gamma.$$

Вообще говоря, если у нас есть покрытие U_α многообразия и набор гладких отображений перехода $g_{\alpha\beta}\colon U_\alpha \cap U_\beta \to \mathrm{GL}_n(\mathbb{R})$, удовлетворяющих условию

$$g_{\alpha\beta} \circ g_{\beta\gamma} = g_{\alpha\gamma} \text{ на } U_\alpha \cap U_\beta \cap U_\gamma,$$

то при помощи этого набора данных мы можем построить векторное расслоение так:

$$\pi\colon U_\alpha \mapsto U_\alpha \times \mathbb{R}^n.$$

Определение 25. Пусть $\pi\colon E \to M$ — векторное расслоение. Определим $H^\bullet_{cv}(E)$ — *когомологии с компактным носителем в вертикальном направлении.*

Мы будем рассматривать комплекс форм $\Omega^\bullet_{cv}(E)$ — комплекс форм с компактным носителем *в вертикальном направлении.* Это означает, что для $\omega \in \Omega^\bullet_{cv}(E)$ $\forall x\ \omega|_{\pi^{-1}(x)}$ имеет компактный носитель.

Теперь заметим, что если $\omega \in \Omega^\bullet_{cv}(E)$, то $\mathrm{d}\omega \in \Omega^\bullet_{cv}(E)$ (так как дифференциал коммутирует с сужением на слой). Значит, $\Omega^\bullet_{cv}(E)$ — дифференциальный комплекс. Его когомологии мы и будем называть когомологиями с компактным носителем в вертикальном направлении.

Определим отображение *интегрирования вдоль слоя* следующим образом:

$$\pi_*\colon \Omega^\bullet_{cv}(E) \to \Omega^{\bullet-n}(M)$$

Рассмотрим сначала простой случай тривиального расслоения: $E = M \times \mathbb{R}^n$ и пусть $t_1, \ldots, t_n$ — координаты в слое $\mathbb{R}^n$. Определим отображение отдельно на двух типах форм:

- $\pi^*(\varphi) \wedge f(x, t_1, \ldots, t_m)\mathrm{d}t_{i_1} \wedge \ldots \mathrm{d}t_{i_r} \mapsto 0$, если $r < n$. Иными словами, если в форме есть не все $\mathrm{d}t_j$, мы отправляем её в 0.
- $\pi^*(\varphi) \wedge f(x, t_1, \ldots, t_n)\mathrm{d}t_1 \wedge \ldots \wedge \mathrm{d}t_n \mapsto \varphi \int\limits_{\pi^{-1}(x)} f(x, t_1, \ldots, t_n)$,

где f имеет компактный носитель для любого фиксированного $x \in M$ (так как у формы из $\Omega^\bullet_{cv}$ компактный носитель вдоль любого вертикального слоя), $\varphi \in \Omega^\bullet(M)$.

В случае произвольного ориентированного расслоения мы будем определять отображение таким образом в тривиализациях, а после склеим (легко показать, что это не зависит от выбора тривиализации и согласовано на пересечениях, откуда мы получаем в итоге глобальную форму после склейки).

Теорема 28. *Интегрирование вдоль слоя коммутирует с внешним дифференцированием, то есть* $\pi_*\mathrm{d} = \mathrm{d}\pi_*$.

Доказательство. Сначала посмотрим на формы второго типа. Там есть полный набор $\mathrm{d}t_j$, поэтому, когда мы продифференцируем, добавится лишь x_j (а так как интегрируем мы по $\mathrm{d}t_j$, не важно, в каком порядке делать операции).

Теперь посмотрим на формы первого типа. Из определения интегрирования вдоль слоёв: $\mathrm{d}\pi_*\omega = 0$. Чтоб показать, что $\pi_*\mathrm{d}\omega = 0$, разберём два случая:

- Если у нас в форме $\mathrm{d}t_{i_1} \wedge \ldots \wedge \mathrm{d}t_{i_r}$ и $r < n - 1$, то после того, как мы продифференцируем, во всех слагаемых набор $\mathrm{d}t_j$ снова будет неполным и π_* отправит форму в 0.
- Если $r = n - 1$, то когда заметим, что после дифференцирования мы будем применять π_* к

$$(\pi^*\varphi)\frac{\partial \varphi}{\partial t_j}(x, t)\mathrm{d}t_j \wedge \mathrm{d}t_{i_1} \wedge \ldots \wedge \mathrm{d}t_{i_r}$$

а после того, как мы проинтегрируем по слою, каждое слагаемое будет содержать множитель

$$\int\limits_{\mathbb{R}^n} \frac{\partial f(x,t)}{\partial t_j}\mathrm{d}t_j \wedge \mathrm{d}t_{i_1} \wedge \ldots \wedge \mathrm{d}t_{i_r} = \int\limits_{\mathbb{R}^{n-1}} \left(\int\limits_{-\infty}^{+\infty} f(x,t)\mathrm{d}t_j \right) \mathrm{d}t_{i_1} \wedge \ldots \wedge \mathrm{d}t_{i_r},$$

а так как $f(x, t)$ имеет компактный носитель при фиксированном x, мы получаем

$$\int\limits_{-\infty}^{+\infty} f(x,t)\mathrm{d}t_j = f(\ldots, +\infty, \ldots) - f(\ldots, -\infty, \ldots) = 0,$$

откуда видно, что вся сумма равна нулю.

□

Теорема 29 (Формула проекции)**.** *Пусть* $\pi\colon E \to M$ *— ориентированное векторное рассслоение ранга* n*, а* τ *— форма на* M *и* $\omega \in \Omega^\bullet_{cv}(E)$*. Тогда*

$$\pi_*(\pi^*(\tau) \wedge \omega) = \tau \wedge \pi_*\omega.$$

Кроме того, если M *имеет размерность* m*,* $\Omega^q_{cv}(E)$*,* $\tau \in \Omega^{m+n-q}_c(M)$*, то*

$$\int\limits_E (\pi^*\tau) \wedge \omega = \int\limits_M \tau \wedge \pi_*\omega.$$

Первое утверждение, как и обычно, технически проверяется для двух типов форм. Второе же утверждение можно (переходя к разбиению единицы) рассматривать локально, а локально это просто теорема Фубини.

Доказательство леммы Пуанкаре для компактных носителей проводится дословно (пользуясь тем, что мы доказали выше) и даёт следующую лемму

Лемма 17 (Лемма Пуанкаре для компактных вертикальных носителей)**.** Интегрирование вдоль слоя задаёт изоморфизм

$$\pi_*\colon H^\bullet_{cv}(M\times\mathbb{R}^n)\to H^{\bullet-n}(M).$$

А на самом деле, это частный случай следующего весьма общего утверждения:

Теорема 30 (Изоморфизм Тома)**.** *Пусть M — ориентированное многообразие, допускающее конечное хорошее покрытие, а $\pi\colon E\to M$ — ориентированное векторное расслоение. Тогда*

$$H^\bullet_{cv}(E)\cong H^{\bullet-n}(M).$$

Доказательство. Как и обычно, используем принцип Майера-Виеториса. У нас есть точная последовательность комплексов

$$0\longrightarrow\Omega^\bullet_{cv}(E|_{U\cup V})\longrightarrow\Omega^\bullet_{cv}(E|_U)\oplus\Omega^\bullet_{cv}(E|_U)\longrightarrow\Omega^\bullet_{cv}(E|_{U\cap V})\longrightarrow 0$$

Тогда интегрирование вдоль вертикальных слоёв индуцирует вот такую диаграмму:

$$\begin{array}{ccccccccc}
\dots\longrightarrow & H^\bullet_{cv}(E|_{U\cup V}) & \longrightarrow & H^\bullet_{cv}(E|_U)\oplus H^\bullet_{cv}(E|_V) & \longrightarrow & H^\bullet_{cv}(E|_{U\cap V}) & \xrightarrow{\mathrm{d}^*} & H^{\bullet+1}_{cv}(E|_{U\cup V}) & \longrightarrow\dots\\
& \downarrow{\scriptstyle\pi_*} & & \downarrow{\scriptstyle\pi_*} & & \downarrow{\scriptstyle\pi_*} & & \downarrow{\scriptstyle\pi_*} & \\
\dots\longrightarrow & H^{\bullet-n}(U\cup V) & \longrightarrow & H^{\bullet-n}(U)\oplus H^{\bullet-n}(V) & \longrightarrow & H^{\bullet-n}(U\cap V) & \xrightarrow{\mathrm{d}^*} & H^{\bullet+1-n}(U\cup V) & \longrightarrow\dots
\end{array}$$

Вообще говоря, нужно проверять, что она коммутативна. Для первых двух квадратов это очевидно (так там у нас вылазают формы на M, а их мы вдоль слоя не интегрируем, так что порядок не важен), проверим для третьего. Это следует из того, как устроен кограничный оператор и формулы проекции

$$\pi_*\mathrm{d}^*\omega=\pi_*((\pi^*\mathrm{d}\rho_U)\wedge\omega)=(\mathrm{d}\rho_U)\wedge\pi_*\omega=\mathrm{d}^*\pi_*\omega.$$

Если U диффеоморфно $\mathbb{R}^n$, то утверждение сводится к лемме Пуанкаре для когомологий с компактным вертикальным носителем. Из 5-леммы мы знаем, что если утверждение верно для U, V, $U\cap V$, то оно верно для $U\cup V$.

Далее доказательство проводится индукцией по размеру хорошего покрытия (как и обычно). □

Соответственно, рассмотрим изоморфизм Тома, но в другую сторону:

$$\mathcal{T}\colon H^\bullet(M)\to H^{\bullet+n}(E).$$

Класс Тома $\Phi\in H^{\bullet+n}_{cv}(E)$ — образ класса $1\in H^0(M)$, то есть $\mathcal{T}(1)$. Легко видеть, что $\pi_*\Phi=\pi_*\mathcal{T}(1)=1$, откуда

$$\pi_*(\pi^*\omega\wedge\Phi)=\omega\wedge\pi_*\Phi=\omega.$$

Отсюда видно, что изоморфизм тома $\mathcal{T}$ (обратный к интегрированию вдоль вертикальных слоёв) задаётся формулой

$$\mathcal{T}(\omega)=\pi^*(\omega)\wedge\Phi,$$

так как формула выше означает, что $\pi_*\mathcal{T}=\mathrm{id}$.

Заметим также, что сужение класса тома $\Phi\in H^q_{cv}(E)$ на каждый слой F даёт нам образующую $H^q_c(F)$, так как $\pi_*\Phi=1$, что и означает, что

$$\int\limits_{\mathbb{R}^n}\Phi=1.$$

Связь двойственности Пуанкаре и класса Тома.

Пусть S — замкнутое ориентированное подмногообразие размерности k в n. Напомним, что двойственный по Пуанкаре к S класс когомологий $[\eta_S] \in H^{n-k}(M)$ определяется условием

$$\int\limits_S i^*\omega = \int\limits_M \omega \wedge \eta_S \quad \forall \omega \in H^k(M).$$

Пусть W — трубчатая окрестность S в M. Напомним, что она диффеоморфна *нормальному расслоению* — такому векторному ν_S расслоению ранга $n-k$ над S, что последовательность расслоений

$$0 \to TS \to TM|_S \to \nu_S \to 0$$

точна . Как мы помним, это расслоение ориентированно так, что расслоение

$$\nu_S \oplus TS = TM|_S$$

имеет ориентацию прямой суммы.

Применим изоморфизм Тома к нормальному расслоению/трубчатой окрестности $W \cong \nu_S$ над S:

$$H^\bullet(S) \xrightarrow[\mathcal{T}_S(\omega)=\pi^*(\omega)\wedge\Phi_W]{\sim} H^{\bullet+n-k}(W) \xrightarrow[j_*]{} H^{\bullet+n-k}(M)$$

где Φ_W — класс Тома трубчатой окрестности, а j_* — его продолжение нулём на M (тут всё корректно, так как из-за того, что у него компактный носитель вдоль верткиальных слоёв, он нулевой в окрестности границы W).

Предложение 7. $\eta_S = j_*\Phi \in H^{n-k}(M)$.

Доказательство. Нам надо проверить, что

$$\forall \omega \in H^k_c(M) \quad \int\limits_S i^*\omega = \int\limits_M \omega \wedge \eta_S.$$

Пусть $\pi\colon W \to S$ — проекция, а i — вложение $S \hookrightarrow W$ в качестве нулевого сечения. Как мы помним, π деформационно ретрагирует W на S, откуда π^* и i^* — изоморфизы на когомологиях. Тогда формы ω и $\pi^*i^*\omega$ отличаются на точную форму, так как представляют один когомологический класс:

$$\omega = \pi^*i^*\omega + \mathrm{d}\alpha.$$

Осталось написать некоторые вычисления:

$$\int\limits_M \omega \wedge j_*\Phi = \int\limits_W \omega \wedge \Phi = \int\limits_W (\pi^*i^*\omega + \mathrm{d}\alpha) \wedge \Phi =$$

теперь применим формулу Стокса (которая убьет лишнее слагаемое) и после формулу проекции:

$$= \int\limits_W \pi^*i^*\omega \wedge \Phi = \int\limits_S i^*\omega \wedge \pi_*\Phi = \int\limits_S i^*\omega,$$

так как $\pi_*\Phi = 1$. □

2.14 Обобщенный принцип Майера-Виеториса и комплекс Чеха-де Рама

Переформулировка последовательности Майера-Виеториса

Сначала мы переформулируем последовательность Майера-Виеториса на язык бикомплексов.

Как и обычно, рассмотрим покрытие $\mathcal{U} = \{U, V\}$ и построим коцепной бикомплекс $K^{p,q}$, определяемый так

$$K^{0,q} = \Omega^q(U) \oplus \Omega^q(V), \quad K^{1,q} = \Omega^q(U \cap V), \quad K^{p,q} = 0 \text{ при } p \geq 2.$$

Снабдим его двумя дифференциалами: оператор внешнего дифференцирования d будет действовать вертикально, а в горизонтальном направлении будет действовать оператор разности $\delta(w, v) = w - v$.

$$\begin{array}{ccccccccc}
 & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\
 & & \Omega^2(U) \oplus \Omega^2(V) & \xrightarrow{\delta} & \Omega^2(U \cap V) & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \dots \\
 & & \uparrow \mathrm{d} & & \uparrow \mathrm{d} & & \uparrow & & \uparrow \\
 & & \Omega^1(U) \oplus \Omega^1(V) & \xrightarrow{\delta} & \Omega^1(U \cap V) & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \dots \\
 & & \uparrow \mathrm{d} & & \uparrow \mathrm{d} & & \uparrow & & \uparrow \\
 & & \Omega^0(U) \oplus \Omega^0(V) & \xrightarrow{\delta} & \Omega^0(U \cap V) & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \dots
\end{array}$$

Как известно, из биградуированного комплекса всегда можно изготовить его тотализацию суммируя вдоль антидиагоналей

$$K^n \stackrel{\text{def}}{=} \bigoplus_{p+q=n} K^{p,q}, \quad K^0 \to K^1 \to \ldots \to K^n \to K^{n+1},$$

дифференциал в котором определяется таким образом

$$D = \delta + (-1)^p \mathrm{d} \text{ на } K^{p,q}, \quad D \colon K^n \to K^{n+1}.$$

Здесь мы для всего этого дела заведём еще такие обозначения (их смысл можно будет понять потом):

$$C^\bullet(\mathfrak{U}, \Omega^\bullet) = \bigoplus K^{p,q} = \bigoplus C^p(\mathfrak{U}, \Omega^q), \quad K^{0,q} = C^0(\mathfrak{U}, \Omega^q), \quad K^{1,q} = C^1(\mathfrak{U}, \Omega^q).$$

Замечание. В дифференциале D мы альтернируем знак от столбца к столбцу, чтоб он вообще говоря был дифференциалом:

$$D^2 = \mathrm{d}^2 \pm \delta\mathrm{d} \mp \mathrm{d}\delta + \delta^2 = 0.$$

Итак, у нас есть дифференциальный комплекс $(K^\bullet, D) = (C^\bullet(\mathfrak{U}, \Omega^q), D)$.

Теорема 31. *Когомологии комплекса $(C^\bullet(\mathfrak{U}, \Omega^q), D)$ совпадают с когомологиями де Рама многообразия M.*

Доказательство. Рассмотрим отображение сужения

$$r \colon \Omega^\bullet(M) \to K^\bullet, \quad \omega \mapsto (\omega|_U, \omega_V)$$

Во-первых, покажем, что оно индуцирует цепное[11] отображение на комплексах. Для этого нужно проверить коммутативность[12] всех квадратов вот такого вида:

[11] С точностью до знака. На самом деле, ясно, что этого достаточно, так как для вычисления когомологий мы считаем ядра и образы (а они от смены знаков не зависят).

[12] с точностью до знака

$$\begin{array}{ccccccc} \dots & \longrightarrow & \Omega^n(M) & \xrightarrow{\mathrm{d}} & \Omega^{n+1}(M) & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle r} & & \\ \dots & \longrightarrow & K^n & \xrightarrow{D} & K^{n+1} & \longrightarrow & \dots \end{array}$$

Для этого заметим, что $\delta r = 0$, так как отображения действуют вот таким образом:

$$\Omega^\bullet(M) \xrightarrow{r} \Omega^\bullet(U) \oplus \Omega^\bullet(V) \subset K^\bullet \xrightarrow{\delta} \Omega^\bullet(U \cap V) \subset K^\bullet$$

Действительно, $(\omega|_U - \omega|_V)|_{U\cap V} = 0$.

Тогда мы имеем

$$Dr = (\delta + (-1)^p \mathrm{d})r = (-1)^p \mathrm{d}r = (-1)^p r\mathrm{d},$$

что и требовалось.

Значит, r индуцирует отображение в когомологиях

$$r^*\colon H^\bullet_{\mathrm{dR}}(M) \to H^\bullet(C^\bullet(\mathfrak{U}, \Omega^\bullet)).$$

Рассмотрим $\alpha \in K^q$, тогда она может быть представлена в виде

$$\alpha = \alpha_0 + \alpha_1, \quad \text{где } \alpha_0 \in K^{0,q} = \Omega^q(U) \oplus \Omega^q(V),\ \alpha_1 \in K^{1,q-1} = \Omega^{q-1}(U \cap V).$$

Вспомним, что последовательность Майера-Виеториса точна:

$$0 \to \Omega^{q-1}(U \cup V) \to \Omega^{q-1}(U) \oplus \Omega^{q-1}(V) \xrightarrow{\delta} \Omega^{q-1}(U \cap V) \to 0,$$

откуда $\alpha_1 = \delta\beta$ для некоторой $\beta \in \Omega^{q-1}(U) \oplus \Omega^{q-1}(V) = K^{0,q-1}$. Тогда

$$\alpha - D\beta = \alpha_0 - \mathrm{d}\beta \in K^{0,q}.$$

Соотвественно, в комплексе $C^\bullet(\mathfrak{U}, \Omega^\bullet)$ любая коцепь когомологична коцепи с только $(0, q)$-компонентой.

Теперь докажем, что r^* сюръективно. Возьмём $[\varphi] \in H^\bullet(C^\bullet(\mathfrak{U}, \Omega^\bullet))$. По зачмечанию выше, мы можем выбрать представителя когомологического класса так, что он имеет только $(0, q)$ компоненту. Тогда

$$0 = D\varphi = (\mathrm{d} + \delta)\varphi = \mathrm{d}\varphi + \delta\varphi \implies \mathrm{d}\varphi = 0,$$

значит φ замкнута и в качестве прообраза нам подойдёт её класс в когомологиях де Рама (от $U \cup V$, а глобальным мы можем его полагать, так как $\delta\varphi = 0$).

Теперь покажем, что r^* инъективно. Пусть $r^*([\omega]) = 0$, то есть $r^*(\omega) = D\varphi$ для некоторой коцепи $\varphi \in C^\bullet(\mathfrak{U}; \Omega^\bullet)$. Тогда, как мы отмечали, мы можем записать $\varphi = \varphi' + D\varphi''$, где $\varphi \in K^{0,q}$. Тогда $r(\omega) = D\varphi' = \mathrm{d}\varphi'$ и $\delta\varphi' = 0$, откуда ω — точная форма на M.

□

Последовательность Майера-Виеториса для счётного покрытия

Пусть $\mathcal{J}$ — счётное упорядоченное индексное множество, $\mathfrak{U} = \{U_\alpha\}_{\alpha\in\mathcal{J}}$ – пассматриваемое нами открытое покрытие многообразия M.

Введём такие обозначения для пересечений:

$$U_\alpha \cap U_\beta = U_{\alpha\beta}, \quad U_\alpha \cap U_\beta \cap U_\gamma = U_{\alpha\beta\gamma} \text{ и т.д.}$$

Тогда у нас есть такая диаграмма:

$$M \longleftarrow \bigsqcup_{\alpha\in\mathcal{J}} U_\alpha \underset{\partial_1}{\overset{\partial_0}{\leftleftarrows}} \bigsqcup_{\alpha_0<\alpha_1} U_{\alpha_0\alpha_1} \underset{\partial_2}{\overset{\partial_0}{\leftleftarrows}} \bigsqcup_{\alpha_0<\alpha_1<\alpha_2} U_{\alpha_0\alpha_1\alpha_2} \;\substack{\longleftarrow\\ \longleftarrow\\ \longleftarrow\\ \longleftarrow}\; \dots$$

где отображение ∂_i — вложение, игнорирующее i-е открытое множество, т.е.

$$\partial_i(U_{\alpha_1\dots\alpha_i\dots\alpha_k}) = U_{\alpha_1\dots\widehat{\alpha_i}\dots\alpha_k}$$

Например, $\partial_0(U_{\alpha_0\alpha_1\alpha_2}) = U_{\alpha_1\alpha_2}$ и дальше в том же духе. Эта последовательность вложений индуцирует последовательность ограничений форм:

$$\Omega^\bullet(M) \xrightarrow{r} \prod_{\alpha\in\mathcal{J}} \Omega^\bullet(U_\alpha) \;\substack{\longrightarrow\\ \longrightarrow\\ \longrightarrow\\ \longrightarrow}\; \prod_{\alpha_0<\alpha_1} \Omega^\bullet(U_{\alpha_0\alpha_1}) \underset{\delta_2}{\overset{\delta_0}{\rightrightarrows}} \prod_{\alpha_0<\alpha_1<\alpha_2} \Omega^\bullet(U_{\alpha_0\alpha_1\alpha_2}) \;\substack{\longrightarrow\\ \longrightarrow\\ \longrightarrow\\ \longrightarrow}\; \dots$$

Немного поясним, как устроены отображения в ней. например, δ_0 индуцированно вложением

$$\partial_0\colon \prod_\alpha U_{\alpha\beta\gamma} \to U_{\beta\gamma} \rightsquigarrow \delta_0\Omega^\bullet(U_{\beta\gamma}) \to \prod_\alpha \Omega^\bullet(U_{\alpha\beta\gamma})$$

и устроено оно, как сужение.

Определим на этой последовательности оператор разности, который будет действовать

$$\delta\colon \prod_{\alpha_1<\dots<\alpha_p} \Omega^q(U_{\alpha_0\dots\alpha_p}) \to \prod_{\alpha_1<\dots<\alpha_{p+1}} \Omega^q(U_{\alpha_0\dots\alpha_p\alpha_{p+1}})$$

Рассмотрим форму $\omega \in \prod_{\alpha_1<\dots<\alpha_p} \Omega^q(U_{\alpha_0\dots\alpha_p}) \to \prod_{\alpha_1<\dots<\alpha_{p+1}}$. Достаточно определить δ на каждое её компоненте, т.е. сужении $\omega_{\alpha_0\dots\alpha_p} \in \Omega^q(U_{\alpha_0\dots\alpha_p}$. Это мы сделаем так:

$$(\delta\omega)_{\alpha_0\dots\alpha_{p+1}} = \sum_{i=0}^{p+1} (-1)^i \omega_{\alpha_0\dots\widehat{\alpha_i}\dots\alpha_{p+1}}.$$

На самом деле, работает это не очень сложно. Например, если у нас есть форма на из $\prod_\alpha \Omega^q(U_\alpha)$ то у нас есть по форме на каждом куске покрытия и чтоб изготовить по форме на каждом попарном пересечении мы просто берём все попарные разности. В случае с тройками — альтернированные суммы. В общем, нетрудно видеть, что

$$\delta = \sum_i (-1)^i \delta_i.$$

Предложение 8. $\delta^2 = 0$.

Доказательство. Действительно, это очевидно, так как мы просто дважды опускаем индексы α_i и α_j и каждый раз с противоположным знаком (так что всё сократится). □

Замечание. До этого момента мы полагали, что индексы упорядочены монотонно. Теперь для удобства будем допускать и общий случае, но с таким условием: когда мы меняем два индекса местами, форма меняет знак.

Итак, у нас есть послеовательность

$$0 \longrightarrow \Omega^\bullet(M) \xrightarrow{r} \prod_{\alpha\in\mathcal{J}} \Omega^\bullet(U_\alpha) \xrightarrow{\delta} \prod_{\alpha_0<\alpha_1} \Omega^\bullet(U_{\alpha_0\alpha_1}) \xrightarrow{\delta} \prod_{\alpha_0<\alpha_1<\alpha_2} \Omega^\bullet(U_{\alpha_0\alpha_1\alpha_2}) \xrightarrow{\delta} \dots$$

Её называют *обобщенной последовательностью* Майера-Виеториса.

Предложение 9. *Эта последовательность точна.*

Доказательство. Точность в первом члене очевидна: форма из $\prod_\alpha \Omega^\bullet(U_\alpha)$ является глобальной формой на M (т.е.) элементом из $\Omega^\bullet(M)$ тогда и только тогда, когда все её компоненты согласованы на попарных пересечениях элементов покрытия.

Пусть теперь $\{\rho_\alpha\}$ — разбиение единицы, подчинённое покрытию $\mathfrak{U}$. Рассмотрим коцикл

$$\omega \in \prod_{\alpha_0<\ldots<\alpha_p} \Omega^\bullet(U_{\alpha_0\ldots\alpha_p})$$

и покажем, что он является когранице́й. Рассмотрим коцепь τ, определённую так:

$$\tau_{\alpha_0\ldots\alpha_{p-1}} = \sum_{\alpha\in\mathcal{J}} \rho_\alpha \omega_{\alpha\alpha_0\ldots\alpha_{p-1}},$$

тогда мы имеем

$$(\delta\tau)_{\alpha_0\ldots\alpha_p} = \sum_i (-1)^i \tau_{\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_p} \sum_{i,\alpha} (-1)^i \rho_\alpha \omega_{\alpha\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_p}.$$

Так как ω — это коцикл,

$$0 = (\delta\omega)_{\alpha\alpha_0\ldots\alpha_p} = \omega_{\alpha_0\ldots\alpha_p} + \sum_i (-1)^{i+1} \omega_{\alpha\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_p} = 0,$$

откуда мы имеем

$$(\delta\tau)_{\alpha_0\ldots\alpha_p} = \sum_\alpha \rho_\alpha \sum_i (-1)^i \omega_{\alpha\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_p} = \sum_\alpha \rho_\alpha \omega_{\alpha_0\ldots\alpha_p} = \omega_{\alpha_0\ldots\alpha_p} \cdot \sum_\alpha \rho_\alpha = \omega_{\alpha_0\ldots\alpha_p}.$$

Значит, $\omega = \delta\tau$, что нам и требовалось.

□

На самом деле, фактически мы построили оператор цепной гомотопии на этом комплексе:

$$K\omega = \tau, \quad (K\omega)_{\alpha_0\ldots\alpha_{p-1}} = \sum_\alpha \rho_\alpha \omega_{\alpha\alpha_0\ldots\alpha_{p-1}},$$

покажем, что $K\delta + \delta K = \mathrm{id}$. Действительно, легко видеть, что

$$(\delta K\omega)_{\alpha_0\ldots\alpha_p} = \sum_i (-1)^k (K\omega)_{\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_p} = \sum_i (-1)^i \omega_{\alpha\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_p}$$

$$(K\delta\omega)_{\alpha_0\ldots\alpha_p} = \sum_\alpha \rho_\alpha (\delta\omega)_{\alpha\alpha_0\ldots\alpha_p} = \omega_{\alpha_0\ldots\alpha_p} \cdot \sum_\alpha \rho_\alpha + \sum (-1)^{i+1} \rho_\alpha \omega_{\alpha\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_p} = \omega_{\alpha_0\ldots\alpha_p} - (\delta K\omega)_{\alpha_0\ldots\alpha_p}.$$

Соответственно, так как на нашем комплексе есть операт стягивающей гомотопии, когомологии комплекса тривиальны.

Как и в случае двуэлементного покрытия, мы можем интерпретировать эту последовательность в виде бикомплекса $(K^{p,q}, \delta, \mathrm{d})$:

$$\begin{array}{ccccccc}
\vdots & & \vdots & & \vdots & & \\
\uparrow & & \uparrow & & \uparrow & & \\
K^{0,2} & \xrightarrow{\delta} & K^{1,2} & \xrightarrow{\delta} & K^{2,2} & \longrightarrow & \ldots \\
\uparrow{\scriptstyle \mathrm{d}} & & \uparrow{\scriptstyle \mathrm{d}} & & \uparrow{\scriptstyle \mathrm{d}} & & \\
K^{0,1} & \xrightarrow{\delta} & K^{1,1} & \xrightarrow{\delta} & K^{2,1} & \longrightarrow & \ldots \\
\uparrow{\scriptstyle \mathrm{d}} & & \uparrow{\scriptstyle \mathrm{d}} & & \uparrow{\scriptstyle \mathrm{d}} & & \\
K^{0,0} & \xrightarrow{\delta} & K^{1,0} & \xrightarrow{\delta} & K^{2,0} & \xrightarrow{\delta} & \ldots
\end{array}$$

Или, если рисовать в расширенном виде (добавляя -1-й столбец):

$$\begin{array}{ccccccccc}
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \Omega^2(M) & \xrightarrow{r} & \prod\limits_{\alpha} \Omega^2(U_\alpha) & \longrightarrow & \prod\limits_{\alpha_0<\alpha_1} \Omega^2(U_{\alpha_0\alpha_1}) & \longrightarrow & \prod\limits_{\alpha_0<\alpha_1<\alpha_2} \Omega^2(U_{\alpha_0\alpha_1\alpha_2}) \longrightarrow \dots \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \Omega^1(M) & \xrightarrow{r} & \prod\limits_{\alpha} \Omega^1(U_\alpha) & \longrightarrow & \prod\limits_{\alpha_0<\alpha_1} \Omega^1(U_{\alpha_0\alpha_1}) & \longrightarrow & \prod\limits_{\alpha_0<\alpha_1<\alpha_2} \Omega^1(U_{\alpha_0\alpha_1\alpha_2}) \longrightarrow \dots \\
 & & \uparrow & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & \Omega^0(M) & \xrightarrow{r} & \prod\limits_{\alpha} \Omega^0(U_\alpha) & \xrightarrow{\delta} & \prod\limits_{\alpha_0<\alpha_1} \Omega^0(U_{\alpha_0\alpha_1}) & \longrightarrow & \prod\limits_{\alpha_0<\alpha_1<\alpha_2} \Omega^0(U_{\alpha_0\alpha_1\alpha_2}) \longrightarrow \dots
\end{array}$$

Соответственно, мы можем ввести такие же как и для покрытия двух множеств обозначения

$$K^{p,q} = C^p(\mathfrak{U}, \Omega^q) = \prod_{\alpha_1<\ldots<\alpha_p} \Omega^q(U_{\alpha_0\ldots\alpha_p}).$$

Соответственно, комплекс $C^\bullet(\mathfrak{U}, \Omega^\bullet)$ называют *комплексом Чеха-де-Рама* и говорят, что $C^p(\mathfrak{U}, \Omega^q)$ — это p-коцепи со значениями в q-формах.

Как и всегда, можно рассмотреть его тотализацю

$$(K^\bullet, D), \quad K^n = \bigoplus_{p+q=n} K^{p,q}, \quad D = \delta + (-1)^p \mathrm{d}.$$

Предложение 10 (Обобщенный принцип Майера-Виеториса)**.** *Отображение* $r\colon \Omega^\bullet(M) \to C^\bullet(M)$ *индуцирует изоморфизм на когомологиях*

$$H^\bullet_{\mathrm{dR}}(M) \cong H^\bullet(C^\bullet(\mathfrak{U}, \Omega^\bullet)).$$

Доказательство. Доказательство тут аналогично доказательству в случае покрытия из двух множеств. А именно, рассматривая D-коцикл $\varphi \in K^n$ мы представляем её суммой

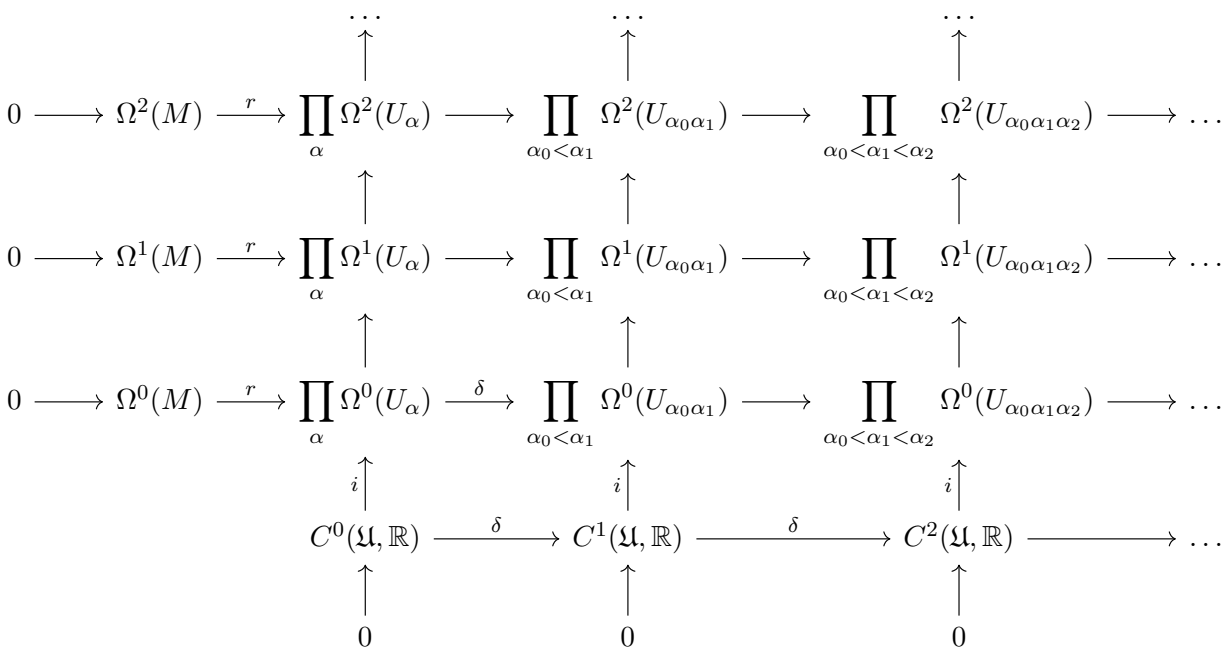
$$\varphi = \alpha_0 + \alpha_1 + \ldots + \alpha_n, \quad \alpha_0 \in K^{0,n}, \alpha_1 \in K^{1,n-1}, \ldots, \alpha_m \in K^{n,0}.$$

Пользуясь точностью строк мы поочередно можем убивать компоненты меньше размерности, а именно, в силу точности нижней строчки диаграммы $\alpha_n = \delta\alpha'_n$, где $\alpha'_n \in K^{n-1,1}$. Тогда если мы рассмотрим $\varphi - D\alpha'_n$, мы останемся в том же когомологическом классе, но получим коцикл без $K^{n,0}$ компоненты. Проделывая так достаточное количество раз мы получим коцикл $\widetilde{\varphi}$ только с $K^{n,0}$ компонентой, оставаясь в том же когомологическом классе. Тогда он будет глобальной замкнутой формой, так как $\mathrm{d}\widetilde{\varphi} = 0,\ \delta\widetilde{\varphi} = 0$ и он из $K^{n,0}$.

Аналогично доказывается и инъективность. □

На самом деле видно, что мы доказали несколько более общее утверждение: *если строки расширенного двойного комплекса точны, то его D-когомологии изоморфны когомологиям начального (-1-го) столбца.*

Теперь добавим к каждому столбцу снизу ядро нижнего дифференциала d, которое мы обозначим как $C^\bullet(\mathfrak{U}, \mathbb{R})$. Как видно из такого определения, $C^p(\mathfrak{U}, \mathbb{R})$ состоит из локально-постоянных функций на $(p+1)$-кратных пересечениях $U_{\alpha_0\ldots\alpha_p}$.



Определение 26. Соотвественно, построенная только что нижняя часть также является дифференциальным комплексом

$$C^0(\mathfrak{U};\mathbb{R}) \xrightarrow{\delta} C^1(\mathfrak{U};\mathbb{R}) \xrightarrow{\delta} C^2(\mathfrak{U};\mathbb{R}) \to \dots,$$

который называется *комплексом Чеха* покрытия $\mathfrak{U}$, а его когомологии, соотвественно, называются *когомологиями Чеха* покрытия $\mathfrak{U}$. Обозначать их мы будем как $H^\bullet(\mathfrak{U},\mathbb{R})$.

Теперь заметим, что если и столбцы расширенного комплекса точны, то "поворотом на $\pi/2$"доказательства предложения 10 мы получаем, что

$$H^\bullet(\mathfrak{U};\mathbb{R}) \cong H^\bullet(C^\bullet(\mathfrak{U},\Omega^\bullet)) \cong H^\bullet_{\mathrm{dR}}(M).$$

Ясно, что столбцы точны совсем не всегда, а препятствие к точности измеряется группами

$$\prod_{q\geq 1,\ \alpha_0\leq\dots\alpha_p} H^q(U_{\alpha_0\dots\alpha_p}).$$

Теперь ясно, какое условие нужно требовать:

Определение 27. Назовём покрытие $\mathfrak{U} = \{U_\alpha\}_\alpha$ *хорошим*, если все его конечные непустые пересечения стягиваемы.

Таким образом, имеем вот такую теорему:

Теорема 32. *Предположим, что многообразие M обладает хорошим покрытием $\mathfrak{U}$. Тогда $H^\bullet_{\mathrm{dR}}(M) \cong H^\bullet(\mathfrak{U};\mathbb{R})$.*

Сделаем теперь несколько забавных наблюдений: можно заметить, что в комплексе Чеха-де-Рама $C^\bullet(\mathfrak{U},\Omega^q)$ мы «смешали» дифференциальную геометрию форм и комбинаторику покрытий. Так вот, из полученного изоморфизма $H^\bullet_{\mathrm{dR}}(M) \cong H^\bullet(\mathfrak{U};\mathbb{R})$ можно делать вот такие интересные выводы:

- Так как при смене хорошего покрытия когомологии де Рама не изменяются, не изменяются и когомологии Чеха (что вообще говоря совсем не очевидно!).
- Так как компактное многообразие допускает конечное хорошее покрытие, а когомологии Чеха такого покрытия конечномерны (по очевидным причинам), конечномерны и когомологии Де Рама (что, как мы видели, вообще говоря. не очевидно).

2.15 Предпучки и когомологии Чеха

Пусть X — топологическое пространство, а $\mathsf{Open}(X)$ — категория открытых множеств в X, морфизмы в которой — вложения открытых множеств.

Определение 28. *Предупочок* на топологическом пространстве X — это контравариантный функтор $\mathcal{F}\colon \mathsf{Open}(X) \to \mathsf{Ab}$.

Иными словами, у нас есть сопоставление каждому открытому $U \subset X$ абелевой группы $\mathcal{F}(U)$ причем такое, что каждому вложению $i_U^V\colon V \to U$ сопоставляется гомоморфизм групп $\mathcal{F}(i_U^V)\colon \mathcal{F}(U) \to \mathcal{F}(V)$, который мы будем называть *ограничением* и это сопоставление функториально.

Гомоморфизм предпучков $\mathcal{F} \to \mathcal{G}$ — это просто естественное преобразование функторов, то есть набор отображений f_U таких, что диаграммы

$$\begin{array}{ccc} \mathcal{F}(U) & \xrightarrow{f_U} & \mathcal{G}(U) \\ {\scriptstyle \rho_V^U}\downarrow & & \downarrow{\scriptstyle \rho_V^U} \\ \mathcal{F}(V) & \xrightarrow{f_V} & \mathcal{G}(V) \end{array}$$

коммутативны.

Пример 15. Приведём несколько примеров:

1. Например, если у нас есть многообразие M, то $\Omega^\bullet(\_)$ задаёт предпучок на нём. И, $C^\infty(\_)$ тоже. В принципе, всякие функции и формы — это основной пример.
2. *Тривиальным предпучком* с группой F называется предпучок $\mathcal{F}$, сопоставляющий каждому открытому связному множеству группу G и каждому вложению $V \hookrightarrow U$ тождественное отображение $G \to G$.
3. *Постоянным предпучком* называется предпучок, изоморфный тривиальному. Предпучок называется *локально постоянным*, если у каждой точки существует окрестность U такая, что $\mathcal{F}|_U$ — постоянный предпучок.
4. *Пучком* называется предпучок, удовлетворяющий *условию склейки*, то есть $\forall U, V \subset X, \forall \sigma \in \mathcal{F}(U),\ \tau \in \mathcal{F}(V)\colon \sigma|_{U\cap V} = \tau|_{U\cap V}$ существует $\rho \in \mathcal{F}(U \cup V)$ такой что $\rho|_U = \sigma$, $\rho|\_V = \tau$.
   Условие склейки вполне естественное. Как мы видели, оно выполняется, например, для дифференциальных форм.
5. Рассмотрим локально тривиальное расслоение $\pi\colon E \to M$. Тогда мы можем рассмотреть вот такой предпучок на M:
   $$\mathcal{H}^q(U) \stackrel{\text{def}}{=} H^q(\pi^{-1}(U)).$$
   Если U — стягиваемое, из формулы Кюннета мы знаем, что
   $$\mathcal{H}^q(U) = H^q(U \times F) \cong H^q(F).$$
   Отсюда ясно, что если M — многообразие, то предпучок $\mathcal{H}^\bullet$ является локально постоянным.
   С другой стороны, если мы рассмотрим $E = M \times F$, то
   $$\mathcal{H}^q(M) = H^q(E) = \bigoplus_{i+j=n} H^i(M) \otimes H^j(F)$$
   и обычно это не совпадает с $H^q(F)$. В общем, это мы всё к тому, что локально постоянный предпучок совсем не обязан быть постоянным. А вот локально постоянный пучок уже обязан быть постоянным.

Перейдём к определению когомологий Чеха.
Пусть X — топологическое пространство, а $\mathfrak{U} = \{U_\alpha\}_\alpha$ — его открытое покрытие.

- 0-коцепями на X со значениями в предпучке $\mathcal{F}$ называются функции, сопоставляющие каждому открытому множеству U_α элемент из $\mathcal{F}(U_\alpha)$, т.е.
  $$C^0(\mathfrak{U}, \mathcal{F}) = \prod_{\alpha\in\mathcal{J}} \mathcal{F}(U_\alpha).$$

- Аналогично, 1-коцепями являются элементы

$$C^1(\mathfrak{U},\mathcal{F}) = \prod_{\alpha<\beta} \mathcal{F}(U_\alpha \cap \mathcal{F}_\beta).$$

- И так далее. p-коцепи определяются, как

$$C^p(\mathfrak{U},\mathcal{F}) = \prod_{\alpha_0<\ldots<\alpha_p} \mathcal{F}(U_{\alpha_0\alpha_1\ldots\alpha_p}).$$

Соответственно, последовательность вложений

$$U_\alpha \;\leftleftarrows\; U_{\alpha\beta} \;\lefteqgtr\; U_{\alpha\beta\gamma} \;\lefteqgtr\; \ldots$$

индуцирует последовательность гомоморфизмов групп (ограничений)

$$\prod_\alpha \mathcal{F}(U_\alpha) \rightrightarrows \prod_{\alpha<\beta} \mathcal{F}(U_{\alpha\beta}) \rightrightarrows \prod_{\alpha<\beta<\gamma} \mathcal{F}(U_{\alpha\beta\gamma}) \rightrightarrows \ldots$$

Теперь определим дифференциал $\delta\colon C^p(\mathfrak{U},\mathcal{F}) \to C^p(\mathfrak{U},\mathcal{F})$ как знакопеременную сумму ограничений, индуцированных вложениями $\delta_i\colon U_{\alpha_0,\ldots\alpha_{p+1}} \to U_{\alpha_0,\ldots\alpha_p}$:

$$\delta = \mathcal{F}(\partial_0) - \mathcal{F}(\partial_1) + \ldots + (-1)^{p+1}\mathcal{F}(\partial_{p+1}).$$

Или, можно еще в явном виде написать:

$$\omega \in C^p(\mathfrak{U},\mathcal{F}) = \prod_{\alpha_0<\ldots<\alpha_p} \mathcal{F}(U_{\alpha_0\ldots\alpha_p}), \quad (\delta\omega)_{\alpha_0\ldots\alpha_{p+1}} = \sum_{i=0}^{p+1} (-1)^i \omega_{\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_{p+1}}.$$

Замечание. Под $\omega_{\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_{p+1}}$ мы подразумеваем сужение $\omega_{\alpha_0\ldots\widehat{\alpha_i}\ldots\alpha_{p+1}}$ на $U_{\alpha_0\ldots\alpha_{p+1}}$.

Лемма 18. $\delta^2 = 0$.

Доказательство. Полностью аналогично случаю комплекса Чеха-де Рама (да и в принципе всем таким доказательствам). □

Определение 29. Соответственно, $(C^\bullet(\mathfrak{U},\mathcal{F}),\delta)$ — коцепной комплекс. Его когомологии мы будем называть *когомологиями Чеха* покрытия $\mathfrak{U}$ со значениями в $\mathcal{F}$. Обозначать их мы будем, как $H^\bullet(\mathfrak{U},\mathcal{F})$.

Обсудим, что произойдёт, если мы сменим покрытие. Напомним, что покрытие $\mathfrak{V} = \{V_\beta\}_{\beta\in\mathcal{J}}$ называется *измельчением* покрытия $\mathfrak{U} = \{U_\alpha\}_{\alpha\in\mathcal{I}}$, если существует такое отображение $\varphi\colon \mathcal{J} \to \mathcal{I}$, что $V_\beta \subset U_{\varphi(\beta)}$. Соответственно, измельчение покрытия индуцирует отображение

$$\varphi^\#\colon C^q(\mathfrak{U},\mathcal{F}) \to C^q(\mathfrak{V},\mathcal{F}), \quad (\varphi^\#\omega)(V_{\beta_0\ldots\beta_q}) = \omega(U_{\varphi_{\beta_0}\ldots\varphi(\beta_q)}).$$

Лемма 19. $\varphi^\#$ — цепное отображение $C^\bullet(\mathfrak{U},\mathcal{F}) \to C^\bullet(\mathfrak{V},\mathcal{F})$.

Доказательство. Нужно проверить, что оно коммутирует с дифференциалом, это стандартная простая выкладка. □

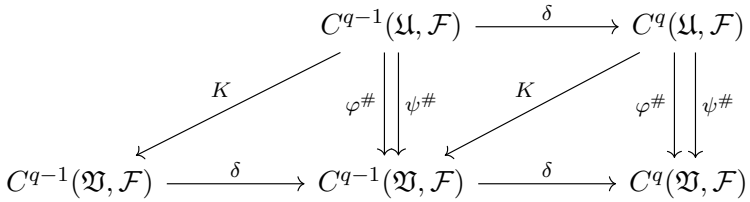
Лемма 20. Пусть $\mathfrak{U} = \{U_\alpha\}_{\alpha\in\mathcal{I}}$ — открытое покрытие, $\mathfrak{V} = \{V_\beta\}_{\beta\in\mathcal{J}}$ — его измельчение, а $\varphi,\psi\colon \mathcal{J} \to \mathcal{I}$ — два отображения измельчения.

Тогда $\varphi^\#$ и $\psi^\#$ цепно гомотопны.

Доказательство. Рассмотрим оператор $K\colon C^q(\mathfrak{U},\mathcal{F}) \to C^{q-1}(\mathfrak{U},\mathcal{F})$, определённый как

$$(K\omega)(V_{\beta_0\dots\beta_{q-1}}) = \sum (-1)^i \omega(U_{\varphi(\beta_0)\varphi(\beta_i)\psi(\beta_i)\dots\psi(\beta_{q-1})}).$$

Покажем, что $\psi^\# - \varphi^\# = \delta K + \delta K$.



В самом деле,

$$(K\delta\omega)(V_{\beta_0\dots\beta_{q-1}}) = \sum (-1)^i (\delta\omega)(U_{\varphi(\beta_0)\dots\varphi(\beta_i)\psi(\beta_i)\dots\psi(\beta_{q-1})}) = \\ = \sum_{i,j} (-1)^{i+j} \omega(U_{\varphi(\beta_0)\dots\varphi(\beta_i)\psi(\beta_i)\dots\psi(\beta_{q-1})}) \text{ где пропущен } j\text{-й индекс.}$$

$$(\delta K\omega)(V_{\beta_0\dots\beta_{q-1})}) = \sum (-1)^i (K\omega)(V_{\beta_0\dots\widehat{\beta_i}\dots\beta_{q-1}}) = \\ = \sum_{i,j} (-1)^{i+j} \omega(U_{\varphi(\beta_0)\dots\varphi(\beta_j)\psi(\beta_j)\dots\psi(\beta_{q-1})}) \text{ где пропущен } i\text{-й индекс.}$$

Как легко видеть, так как в первой сумме мы пропускаем j-й, а во втором i-й, каждое слагаемое $\omega(U_{\varphi(\beta_0)\dots\varphi(\beta_j)\psi(\beta_j)\dots\psi(\beta_{q-1})})$ (кроме $i=j=0$ и $i=j=q$) будет встречаться в первой и во второй сумме с разными знаками. Значит, останутся только

$$\omega(U_{\varphi(\beta_0)\dots\varphi(\beta_{q-1})}) - \omega(U_{\psi(\beta_0)\dots\psi(\psi_{q-1})}) = (\varphi^\#\omega)(V_{\beta_0\dots\beta_{q-1}}) - (\psi^\#\omega)(V_{\beta_0\dots\beta_{q-1}})$$

□

Эта лемма нужна нам затем, чтобы при разных отображениях для одного и того же измельчения в когомологиях получалось одно и то же отображение.

Напомним, что набор $\{G_i\}_{i\in\mathcal{I}}$ называется *индуктивной системой*, если при $\alpha > \beta$ у нас есть отображение $f^\alpha_\beta\colon G_\alpha \to G_\beta$, причём

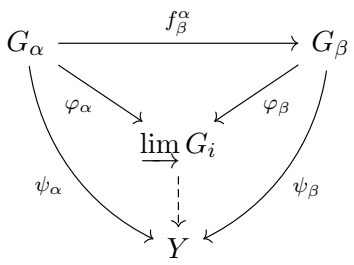
- $f^\alpha_\alpha = \mathrm{id}$
- Если $\gamma < \beta < \alpha$, то $f^\alpha_\gamma = f^\beta_\gamma \circ f^\alpha_\beta$.

Также напомним, что прямым пределом индуктивной системы групп называется

$$\varinjlim G_i = \prod_{i\in\mathcal{I}} G_i / \sim,$$

где $G_\alpha \ni a \sim b \in G_\beta \Leftrightarrow \exists\gamma\colon f^\alpha_\gamma(a) = f^\beta_\gamma(b)$.

Ну или, проще говорить про универсальное свойство:



Так вот, из доказанных выше двух лемм следует, что если $\mathfrak{U} > \mathfrak{V}$, то у нас есть корректно определённое отображение на когомологиях

$$H^\bullet(\mathfrak{U}, \mathcal{F}) \to H^\bullet(\mathfrak{V}, \mathcal{F}).$$

Значит, $\{H^\bullet(\mathfrak{U}, \mathcal{F})\}_{\mathfrak{U}}$ — индуктивная система. Её прямой предел

$$H^\bullet(X, \mathcal{F}) \stackrel{\text{def}}{=} \varinjlim H^\bullet(\mathfrak{U}, \mathcal{F})$$

мы будем называть *когомологиями Чеха пространства X со значениями в предпучке $\mathcal{F}$*.

Лемма 21. Пусть $\mathbb{R}$ — постоянный предпучок на многообразии M. Тогда

$$H^q(M, \mathbb{R}) \cong H^q_{\mathrm{dR}}(M).$$

Доказательство. Начнём с того, что хорошие покрытия образуют кофинальное подмножество в множестве всех покрытий[13], поэтому мы можем рассматривать только хорошие покрытия. Для хороших покрытий мы доказывали, что $H^\bullet(\mathfrak{U}, \mathbb{R}) \cong H^\bullet_{\mathrm{dR}}(M)$. Но тогда ясно, что $H^\bullet(M, \mathbb{R}) \cong H^\bullet_{\mathrm{dR}}(M)$. □

2.16 Глобальная угловая форма, класс Эйлера, класс Тома

В этом параграфе мы явно построим класс Тома ориентированного векторного расслоения $\pi\colon E \to M$ ранга 2 в терминах разбиения единицы на M и функций перехода расслоения E. Пусть E^0 — дополнение нулевого сечения.

Пусть $\{U_\alpha\}$ — открытое покрытие M. Так как у нас есть Риманова метрика на E, на каждом U_α мы можем выбрать ортонормированное оснащение, рассмотреть в слое сферу и завести на $E^0_{U_\alpha}$ полярные координаты r_α и θ_α (их всего две, так как слой плоскость).

Если $x_1, \dots, x_n$ — координаты на U_α, то $\pi^*, \dots, \pi^* x_n, r_\alpha, \theta_\alpha$ — координаты на $E^0|_{U_\alpha}$.

На пересечениях $U_\alpha \cap U_\beta$ радиусы r_α и r_β вообще говоря одинаковы, а вот угловые координаты $\theta_\alpha, \theta_\beta$ могут отличаться на кратное 2π.

Соответственно, определим $\varphi_{\alpha\beta}$ (с точностью до элемента $2\pi\mathbb{Z}$) как угол поворота в направлении против часовой стрелки[14] от α-координатной системы к β-координатной системе

$$\varphi_{\alpha\beta}\colon U_\alpha \cap U_\beta \to [0, 2\pi], \quad \theta_\beta = \theta_\alpha + \pi^*\varphi_{\alpha\beta}.$$

Заметим, что

$$\varphi_{\alpha\beta} + \varphi_{\beta\gamma} - \varphi_{\alpha\gamma} \in 2\pi\mathbb{Z},$$

то есть каждому тройному пересечению $U_{\alpha\beta\gamma}$ мы можем сопоставить целое число:

$$\varepsilon_{\alpha\beta\gamma} = \frac{1}{2\pi}(\varphi_{\alpha\beta} - \varphi_{\alpha\gamma} + \varphi_{\beta\gamma})$$

и набор $\{\varepsilon_{\alpha\beta\gamma}\}$ измеряет отклонение $\varphi_{\alpha\beta}$ от 2-коцикла с смысле Чеха. Видно, что если они все равны нулю, то это Чеховский 2-коцикл (так как дифференциал в комплексе Чеха просто определялся таким образом).

С другой стороны, 1-формы $\mathrm{d}\varphi_{\alpha\beta}$ уже являются коциклами, так как можно найти набор форм ξ_α на U_α , что

$$\frac{1}{2\pi}\varphi_{\alpha\beta} = \xi_\beta - \xi_\alpha.$$

Действительно, можно взять

$$\xi_\alpha = \frac{1}{2\pi}\sum_\gamma \rho_\gamma \mathrm{d}\varphi_{\gamma\alpha},$$

[13] Подмножество $\mathcal{J}$ направленного множества $\mathcal{I}$ называется кофинальным, если для любого $i \in I$ найдется $j \in \mathcal{J}$ такое что $i < j$

[14] об этом мы можем говорить, так как у нас всё ориентированно

где ρ_γ — разбиение единицы, подчиненное покрытию $\{U_\alpha\}$ и тогда

$$\xi_\beta - \xi_\alpha = \frac{1}{2\pi}\sum_\gamma \rho_\gamma(\mathrm{d}\varphi_{\gamma\beta} - \mathrm{d}\varphi_{\gamma\alpha}) = \mathrm{d}\varphi_{\alpha\beta}\cdot\frac{1}{2\pi}\sum_\gamma \rho_\gamma$$

Соответственно, так как $\mathrm{d}^2\varphi_{\alpha\beta} = 0$, мы имеем $\mathrm{d}\xi_\alpha = \mathrm{d}\xi_\beta$ на $U_\alpha \cap U_\beta$. Значит, формы $\mathrm{d}\xi_\alpha$ дают нам глобальную 2-форму e на M.

Определение 30. Когомологический класс формы $e = e(E) \in H^2(M)$ называют *классом Эйлера* расслоения E.

Предложение 11. *Когомологический класс формы e не зависит от выбора форм ξ при построении.*

Доказательство. Пусть $\{\widetilde{\xi_\alpha}\}$ — другой такой набор, тогда

$$\frac{1}{2\pi}\mathrm{d}\varphi_{\alpha\beta} = \widetilde{\xi_\beta} - \widetilde{\xi_\alpha} = \xi_\beta - \xi_\alpha,$$

тогда $\widetilde{\xi_\beta} - \xi_\beta = \widetilde{\xi_\alpha} - \xi_\alpha = \xi$ является глобальной формой (так как согласована на всех пересечениях). Значит, $\mathrm{d}\widetilde{\xi_\alpha}$ и $\mathrm{d}\xi_\alpha$ отличаются на точную форму, как мы и хотели. □

Теперь заметим, что

$$\begin{cases}\theta_\beta = \theta_\alpha + \pi^*\varphi_{\alpha\beta}\\ \frac{1}{2\pi}\varphi_{\alpha\beta} = \xi_\beta - \xi_\alpha\end{cases} \implies \frac{\mathrm{d}\theta_\alpha}{2\pi} - \pi^*\xi_\alpha = \frac{\mathrm{d}\theta_\beta}{2\pi} - \pi^*\xi_\beta \text{ на } E^0|_{U_\alpha\cap U_\beta},$$

поэтому эти формы при слкейке дают глобальную 1-форму ψ на E^0, сужение которой на каждый слой совпадает с угловой формой $\frac{1}{2\pi}\mathrm{d}\theta$.

Вообще говоря, эта глобальная форма ψ замкнутой не является:

$$\mathrm{d}\psi = \mathrm{d}\left(\frac{\mathrm{d}\theta_\alpha}{2\pi} - \pi^*\xi_\alpha\right) = -\pi^*\mathrm{d}\xi_\alpha = -\pi^*\mathrm{d}\xi_\beta \implies \mathrm{d}\psi = -\pi^* e.$$

Если E — тривиальное расслоение, то в качестве ψ можно взять пуллбек формы $\frac{1}{2\pi}\mathrm{d}\theta$ при проекции

$$E^0 = M\times(\mathbb{R}^2\setminus 0) \to (\mathbb{R}^2\setminus 0),$$

в этом случае ψ замкнута и класс Эйлера равен нулю.

В этом смысле класс Эйлера является мерой скрученности расслоения.

Класс Эйлера в терминах функций перехода

Еще класс Эйлера ориентированного векторного расслоения ранга 2 можно задать в терминах переходов. Пусть

$$g_{\alpha\beta}\colon U_\alpha\cap U_\beta \to \mathrm{SO}(2) \cong S^1,$$

а элементы группы $\mathrm{SO}(2)$ мы можем представлять как

$$e^{i\theta} = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}.$$

Тогда угол между α-координатной и β-координатной системой это в точности $\frac{1}{i}\log Cg_{\alpha\beta}$ (так как мы поворачиваем одну систему в другую, применяя $g_{\alpha\beta} = e^{i\theta}$). Соответственно,

$$\theta_\alpha - \theta_\beta = \pi^*\left(\frac{1}{i}\log g_{\alpha\beta}\right) \implies \pi^*\varphi_{\alpha\beta} = -\pi^*\left(\frac{1}{i}\log g_{\alpha\beta}\right).$$

Так как π^* инъективно, отсюда мы получаем

$$\varphi_{\alpha\beta} = -\frac{1}{i}\log g_{\alpha\beta}.$$

Соотвественно, пусть $\{\rho_\gamma\}$ — разбиение единицы, подчиненное покрытию $\{U_\gamma\}$, тогда

$$\xi_\alpha = \frac{1}{2\pi}\sum_\gamma \rho_\gamma \mathrm{d}\varphi_{\gamma\alpha} = -\frac{1}{2\pi i}\sum_\gamma \rho_\gamma \mathrm{d}\log g_{\gamma\alpha},$$

откуда мы получаем вот такую замечательную формулу

$$e(E) = -\frac{1}{2\pi i}\sum_\gamma \mathrm{d}(\rho_\gamma \mathrm{d}\log g_{\gamma\alpha}) \text{ на } U_\alpha.$$

Отсюда мы сразу получаем, что класс Эйлера характеристический:

Предложение 12. *Пусть $f\colon N \to M$ — гладкое отображение, а E — ориентированное векторное расслоение над M ранга 2. Тогда*

$$f^*(e(E)) = e(f^*(E)).$$

Доказательство. Действительно, функции перехода пуллбека расслоения $f^*(E)$ являются функции $f^*g_{\alpha\beta}$ это просто следует из формулы выше. □

Глава 2

Аффинная алгебраическая геометрия

1. Коммутативная алгебра с прицелом на алгебраическую геометрию

Замечание. Весь раздел пока что не дописан.

1.1 Предварительные сведения и напоминания

Определение 31. Собственный идеал I в кольце R называется *простым*, если $ab \in I \implies a \in I$ или $b \in I$.

Собственный идеал I в кольце R называется *максимальным*, если он не содержится ни в каком другом собственном идеале.

Простейшие свойства:

1. Для любого собственного идеала существует максимальный идеал, содержащий его.
2. Любой максимальный идеал является простым.
3. Собственный идеал I является простым тогда и только тогда, когда R/I — область целостности.
4. Собственный идеал I является максимальным тогда и только тогда, когда R/I — поле.

Определение 32. Элементы a и b называются *ассоциированными*, если $aR = bR$.

Необратимый элемент $a \in R$ называется *неприводимым*, если из равенства $a = bc$ следует, что или b или c ассоциирован с a.

Элемент называется *простым*, если главный идеал (a) простой.

Замечание. Простой $\implies$ неприводимый. Обратное, вообще гооворя, неверно.

Определение 33. Кольцо R называется *нётеровым*, если оно удовлетворяет условию обрыва **возрастающих** цепочек (ACC) для идеалов. Модуль называется *нётеровым*, если он удовлетворяет ACC для подмодулей.

Лемма 22. Следующие условия на кольцо R эквивалентны:

1. R нетерово.
2. Любой идеал в R конечнопорожден.
3. Любой подмодуль коненчопрожденного R-модуля конечнопрожден.
4. Любой конечнопорожденный R-модуль нетеров.

Теорема 33 (Гильберта, о базисе)**.** *Кольцо многочленов от конечного числа переменных над нётеровым кольцом нётерово. Иными словами, если R — нётерово кольцо, то любой идеал в кольцо $R[x_1, \ldots, x_n]$ порожден конечным числом многочленов.*

1.2 Аффинные алгебраиические многообразия

Я думаю, что как только я нормально послушаю курс алгебриаческой, этот параграф будет переписан.

Пусть F — поле, $\mathbb{A}^n_F = F^n$ — аффинное пространство над ним.

Пусть $J \subset A = F[t_1, \dots, t_n]$, обозначим через $V(J)$ множество всех общих нулей всех многочленов из идеала J, то есть

$$V(J) = \{x \in \mathbb{A}^n_F \mid f(x) = 0 \; \forall f \in J\}.$$

Определение 34. Пусть I — идеал в колцье R. *Радикал* идеала I определяется, как

$$\sqrt{I} \stackrel{\text{def}}{=} \{f \in R \mid \exists n \in \mathbb{N}\colon f^n \in I\}.$$

Идеал I называется *радикальным*, если он совпадает со своим радикалом.

Замечание. Другими словами, I — радикальный идеал $\Leftrightarrow R/I$ — редуцированное кольцо (т.е. без нильпотентных элементов).

Несложно заметить, что $V(J) = V(AJ)$, где $AJ = \sum_{f \in J} Af$. Действительно, если $f(x) = 0, g(x) = 0$, то $\forall q, p \in F[t_1, \dots, t_n]\ fq + pg = 0 \Rightarrow V(J) = V(AJ)$. Соотвественно, так как $f^m(x) = 0 \implies f(x) = 0$, мы имеем $V(J) = V(\sqrt{AJ})$, а это говорит нам, что имеет смысл рассматривать только радикальные идеалы.

Определение 35 (Топология зарисского)**.** Определим на $\mathbb{A}^n_F$ *топологию Зарисского*: набором замкнутых множеств будет

$$\{V(J) \subset \mathbb{A}^n_F \mid J - \text{радикальный идеал в } F[t_1, \dots, t_n]\}.$$

Замкнутые подмножества $\mathbb{A}^n_F$ в этой топологии называют *аффинными алгебраическими многообразиями (affine algebraic variety)*.[1]

Замечание. Проверим, что это удовлетворяет аксиомам топологии:

- $V(1) = \varnothing$.
- $V(0) = \mathbb{A}^n_F$.
- $V(\bigcup_k J_k) = \bigcap_k V(J_k)$, то есть пересечение замкнутых замкнуто.

Для подмножества $X \subset \mathbb{A}^n_F$ определим $I(X) = \{f \in F[t_1, \dots, t_n] \mid f(x) = 0 \; \forall x \in X\}$. Легко видеть, что $V(I(X)) = \mathrm{Cl}(X)$ в топологии Зарисского. Совершенно ясно, что $I(X)$ — идеал в кольце $F[t_1, \dots, t_n]$.

Определение 36. *Морфизмом* аффинных алгебраических многообразий $X \subset \mathbb{A}^n_f, Y \subset \mathbb{A}^n_F$ называется полиномиальное отображение $X \to Y$.

Аффинные многообразия с таким набором морфизмов образуют категорию Aff.

Определение 37. Так как $\mathbb{A}^1_F = F$, морфизмы $X \to \mathbb{A}^1_F$ — просто какие-то элементы $F[x_1, \dots, x_n]$. Соотвественно, морфизмы f и g совпадают, если $f - g \in I(X)$, то есть $\mathrm{Hom}_{\mathsf{Aff}}(X, \mathbb{A}^1_F) \cong F[t_1, \dots, t_n]/I(X)$. Это кольцо называется *аффинной алгерой* многообразия X и обозначается $F[X]$.

Так как $\mathrm{Hom}_{\mathsf{Aff}}(\_, \mathbb{A}^1_F)$ является контравариантным функтором, а кольцевые операции определяются на $\mathrm{Hom}_{\mathsf{Aff}}(X, \mathbb{A}^1_F)$ естественным образом, отображение $X \mapsto F[X]$ определяет контравариантный функтор $\mathsf{Aff} \to F - \mathsf{Alg}_{fin.gen.}$ — конечнопорожденные редуцированные алгебры.

Построим функтор в обратную сторону. Рассмотрим $R \in F - \mathsf{Alg}_{fin.gen.}$ и выберем в ней набор образующих (то есть, выберем эпиморфизм $\pi_R\colon F[t_1, \dots, t_n]$). Рассмотрим функтор $\mathcal{X} = \mathrm{Hom}_{F-\mathsf{Alg}_{fin.gen.}}(\_, F)\colon F - \mathsf{Alg}_{fin.gen.} \to \mathsf{Set}$.

Множество $\mathcal{X}(A)$ мы можем отождествить с $\mathbb{A}_{F^n}$ по формуле

$$\varphi \mapsto (\varphi(t_1), \dots, \varphi(t_n)).$$

[1] вообще говоря, кажется, что это не вполне правильное определение, так как тут это просто алгебраическое множество, а вот аффинное многообразие — окольцованное пространство. Поговорим об этом позже.

Таким образом, $\mathcal{X}(R)$ вкладывается в $\mathbb{A}^n_F$ при помощи отображения $\psi \mapsto \psi \circ \pi_R$. Кроме того, множество $\mathcal{X}(R) = V(\operatorname{Ker}\pi_R)$ является аффинным алгебраическим многообразием с аффинной алгеброй $F[t_1,\dots,t_n]/I(V(\operatorname{Ker}\pi_R))$. Так мы имеем:

$$\mathcal{X}(F[X]) = \mathcal{X}(A/I(X)) = V(I(X)) = X \quad F[X(R)] = A/I(V(\operatorname{Ker}\pi_R)).$$

Последняя алгебра изоморфна R тогда и только тогда, когда $I(V(J)) = J$, где $R \cong A/J$.

Теорема 34 (Теорема Гильберта о нулях)**.** *Пусть $F = F^{alg}$, $J \subset F[t_1,\dots,t_n]$, а $f \in F[t_1,\dots,t_n]$. Тогда $f(V(J)) = 0 \Leftrightarrow f \in \sqrt{RJ}$. Иными словами, $f \in I(V(J)) \Leftrightarrow f \in \sqrt{RJ}$.*

Другими словами, теорема Гильберта о нулях говорит нам, что над алгебраически замнутым полем F аффинные алгебраические многообразия (замкнутые подмножества $\mathbb{A}^n_F$) взаимно однозначно соотвествуют радикальным идеалам в $F[t_1,\dots,t_n]$ и категории Aff и $F - \mathsf{Alg}_{fin.gen.}$ антиэквивалентны.

Аналогичные рассуждения можно провести и для замкнутых подмножеств аффинного многообразия X и радикальных идеалов его аффинной алгебры $F[X]$. При этом точкам аффинного многообразия X соотвествуют максимальные идеалы $F[X]$, то есть, элементы $\operatorname{Specm}(F[X])$.

1.3 Топология Зарисского на спектре кольца

Пусть R — кольцо, $\operatorname{Specm} R$ — его максимальный спектр (множество его максимальных идеалов). Зададим на $\operatorname{Specm} R$ набор замкнутых множеств

$$\widetilde{V}(J) \stackrel{\text{def}}{=} \{\mathfrak{m} \in \operatorname{Specm} R \mid \mathfrak{m} \supset J\},\ J \subset R.$$

При таком определении топологии X будет гомеоморфно $\operatorname{Specm}(F[X])$ (как мы и отмечали выше, точки соотвествуют максимальным идеалам).

В случае незамкнутого поля или бесконечнопорожденных алгебр правильно вместо максимального спектра рассматривать простой спектр. Топология Зарисского на нём определяется следующим образом;

$$J \subset R, \quad V(J) \stackrel{\text{def}}{=} \{\mathfrak{p} \in \operatorname{Spec} R \mid J \subset \mathfrak{p}\}.$$

1.4 Словарик алгебраической геометрии

Геометрия	Алгебра
Замкнутые подмножества X	Идеалы в $F[X]$
Точки X	Максимальные идеалы в $F[X]$
Неприводимые замкныте подмножества в X	Простые идеалы в $F[X]$
will be upd	will be upd.

1.5 Локализация. Поведение спектра при локализации.

Напомним основные примеры локализаций:

1. Для $s \in R$ можно рассмотреть мультипликативное подмножество $\langle s\rangle = \{s^n \mid n \in \mathbb{N}\}$. Локализация $\langle s\rangle^{-1}R$ называется *главной локализацией* и обозначается R_s.
2. Если $\mathfrak{p}$ — простой идеал кольца R, то $R \setminus \mathfrak{p}$ — мультипликативное подмножество. В этом случае локализация $R_{\mathfrak{p}} \stackrel{\text{def}}{=} (R \setminus \mathfrak{p})^{-1}R$ называется локализацией кольца R в простом идеале $\mathfrak{p}$.

Определение 38. Кольцо называется *локальным*, если оно имеет ровно один максимальный идеал и *полулокальным*, если максимальных идеалов конечное число.

Если $\mathfrak{p}$ — прсотой идеал, то $R_{\mathfrak{p}}$ — локальное кольцо с единственным максимальным идеалом $\mathfrak{p}R_{\mathfrak{p}}$.

Пусть теперь $\varphi\colon R \to A$ — гомоморфизм коолец, тогда он индуцирует следующие отображения на идеалах:

- $\varphi^*\colon \operatorname{Ideals} A \to \operatorname{Ideals} R,\ \varphi^*(J) \stackrel{\text{def}}{=} \varphi^{-1}(J)$.
- $\varphi_*\colon \operatorname{Ideals} R \to \operatorname{Ideals} A,\ \varphi_*(I) \stackrel{\text{def}}{=} \varphi(I)A$.

Заметим, что так как прообраз простоого идеала прост, φ^* можно сузить до отображения $\operatorname{Spec} A \to \operatorname{Spec} R$.

Лемма 23. Если $I \in \operatorname{Im}\varphi^*$, то $I = \varphi^*(\varphi_*(I))$.

Доказательство. Пусть $I = \varphi^*(J) = \varphi^{-1}(J)$, тогда $\varphi(I) \subseteq J \implies \varphi_*(I) = \varphi(I)A \subseteq JA \subseteq J$. Но тогда $\varphi^*(\varphi_*(I)) \subseteq \varphi^{-1}(J) = I$. С другой стороны, $I \subseteq \varphi^{-1}(\varphi(I)) \subseteq \varphi^*(\varphi_*(I))$. □

Предыдущее утверждение можно *сузить* на простые идеалы:

Лемма 24. Пусть $\varphi\colon R \to A$ — произвольный гомоморфизм колец. Тогда $\mathfrak{p} \in \varphi^*(\operatorname{Spec} A)$ тогда и только тогда, когда $\mathfrak{p} = \varphi^*(\varphi_*(\mathfrak{p}))$.

Теперь посмотрим на поведение спектра кольца при локализации. Пусть $\lambda\colon R \to S^{-1}R$ — локализационный гомоморфизм.

Лемма 25. $\lambda_* \circ \lambda^* = \mathrm{id}$. Следовательно, λ^* инъективно, а λ_* — сюръективно.

Доказательство. Пусть $I \trianglelefteq S^{-1}R$, тогда ясно, что $\lambda_*(\lambda^*(I)) \subset I$. Действительно,

$$\lambda_*(\lambda^*(I)) = \lambda(\lambda^{-1}(I))S^{-1}R \subset IS^{-1}R \subset I.$$

Теперь докажем включение в другую сторону. Пусть $\frac{r}{s} \in I$, тогда $s \cdot \frac{r}{s} = \frac{r}{1} \in I \supset \lambda(\lambda^{-1}(I)) \implies \frac{r}{1} \in \lambda(\lambda^{-1}(I)) \implies \frac{r}{1} \cdot \frac{1}{s} \in \lambda(\lambda^{-1}(I))S^{-1}R = \lambda_*(\lambda^*(I))$. □

Следствие 15. *Локализация нётерова кольца нётерова.*

Доказательство. Действительно, по предыдущей лемме $J = \lambda_*(\lambda^*(J)) = \lambda_*(I) = \lambda^(I)S^{-1}R$, а так как I — конечнопорождён, $\lambda^(I)S^{-1}R$ — конечнопорождён. □

Лемма 26. Идеал $I \trianglelefteq R$ лежит в образе λ^* (т.е. является прообразом какого-то идеала из локализации) тогда и только тогда, когда образ S в R/I не содержит делителей нуля.

Доказательство. Итак, как мы помни, $I \in \operatorname{Im}\lambda^* \Leftrightarrow I = \lambda^*(\lambda_*(I))$. Пусть ρ — гомоморфизм факторизации $R \to R/I$. Пусть для некоторых $r \in R,\ s \in S$ $\rho(r)\rho(s) = 0$. Тогда $\rho(rs) = 0 \implies rs = j \in I$. Тогда $\frac{r}{1} = \frac{\lambda(j)}{s} \in \lambda_*(I) \implies r \in \lambda^*(\lambda_*(I)) = I \implies \rho(r) = 0$, то есть $\rho(s)$ — не делитель нуля.

Пусть $r \in \lambda^*(\lambda_*(I)) \setminus I$. Тогда мы можем его представить в виде $\lambda(r) = \lambda(j)\frac{t}{s}, t \in R, s \in S, j \in I$. Но тогда $\exists s' \in S\colon rss' = jts' \implies \rho(r)\rho(ss') = \rho(j)\rho(ts') = 0$, а так как $\rho(r) \neq 0$ по предположению, $\rho(ss')$ — делитель нуля. □

Отсюда мы получаем такое следствие.

Следствие 16. *Отображение $\lambda^*\colon \operatorname{Spec} S^{-1}R \to \operatorname{Spec} R$ инъективно, а его образ равен множеству простых идеалов, не пересекающихся с S.*

Сужение λ_* на множество простых идеалов R, не пересекающихся с S, инъективно.

Таким образом, λ^* и λ^* — взаимнообратные биекции между $\operatorname{Spec} S^{-1}R$ и множеством простых иедалов кольца R, не пересекающихся с S.

Применяя это к главной локализации $\langle s \rangle$, мы получаем, что $\operatorname{Im}\lambda^* = \operatorname{Spec} R \setminus V(s)$ — откртое подмножество, а $\{\operatorname{Spec} R_s \mid s \in R\}$ — база топологиии Зарисского.

Определение 39. Пусть $I \trianglelefteq R$ — идеал в кольце R. Его *радикалом* называется

$$\sqrt{I} \stackrel{\text{def}}{=} \{x \in R \mid \exists n\colon x^n \in I\}.$$

Нильпотентным радикалом кольца R называется $\operatorname{NRad}(R) = \sqrt{0}$ — множество всех нильпотентных элементов кольца R.

Теорема 35. *Пусть $I \trianglelefteq R$. Тогда $\sqrt{I}$ равен пересечению всех простых идеалов, содержащих I, то есть*

$$\sqrt{I} = \bigcap_{\mathfrak{p}\in\operatorname{Spec} R,\ \mathfrak{p}\supset I} \mathfrak{p}.$$

В частности, нильпотентный радикал равен пересечению всех простых идеалов кольца R.

Доказательство. Начнём с того, что если $\mathfrak{p} \supset I$, то $\mathfrak{p} \supset \sqrt{I}$, так как если $x \in \sqrt{I}$, то для некоторого n мы имеем $x^n \in I \implies x^n = x \cdot \ldots \cdot x \in \mathfrak{p} \implies x \in \mathfrak{p}$. То есть, радикал $\sqrt{I}$ идеала I содержится в любом простом идеале $\mathfrak{p}$, содержащем сам I.

Пусть сначала $I = 0$, т.е. Возьмём

$$f \in \bigcap_{\mathfrak{p}\in\operatorname{Spec} R} \mathfrak{p}$$

Тогда из предыдещего следствия $\operatorname{Spec} R_f = \varnothing$, так как с $\langle f\rangle$ пересекаются все простые идеалы. Отсюда $R_f = 0$. Но тогда мы имеем равенство

$$\frac{1}{1} = \frac{0}{1} \implies \exists n\colon f^n = 0.$$

Теперь рассмотрим для произвольного идеала I каноническую проекцию $\rho\colon R \to R/I$. Заметим, что

$$\rho^{-1}(\operatorname{NRad}(R/I)) = \sqrt{I}.$$

В самом деле, $\rho(y) = x \in \operatorname{NRad}(R/I) \Leftrightarrow \exists n\colon \rho(y^n) = x^n = 0$ в $R/I \Leftrightarrow \rho^{-1}(y)^n \in I$.

Теперь вспомним, что при эпиморфизме прооораз простого идеала прост, то есть $\rho^{-1}(\mathfrak{p})$ — простой идеал $\forall \mathfrak{p} \in \operatorname{Spec}(R/I)$. Ну и кроме того, он содержит I (так как содержит 0). Тогда мы имеем такую цепочку включений:

$$\sqrt{I} \subset \bigcap_{I\subset\mathfrak{q}\in\operatorname{Spec} R} \mathfrak{q} \subset \bigcap_{\mathfrak{p}\in\operatorname{Spec} R/I} \rho^{-1}(\mathfrak{p}) = \rho^{-1}\left(\bigcap_{\mathfrak{p}\in\operatorname{Spec} R/I} \mathfrak{p}\right) = \rho^{-1}(\operatorname{NRad}(R/I)) = \sqrt{I}.$$

□

1.6 Локализация модуля и плоские модули. Локальный принцип.

Пусть $M - R$-модуль, а $S -$ мультипликативное подмножество в R.

Определение 40. Множество $M \times S/\sim$, где $(m, s) \sim (m', s') \Leftrightarrow \exists s'' \in S\colon ms's'' = m'ss''$ с естественно заданными операциями называется *локализацией* модуля M в S.

Лемма 27. $S^{-1}M \cong M \otimes_R S^{-1}R$.

Доказательство. Рассмотрим отображение $\varphi\colon S^{-1}M \to M \otimes_R S^{-1}R$, заданное как

$$\frac{m}{s} \mapsto m \otimes \frac{1}{s}.$$

Ясно, что это сюръективный и инъективный гомоморфизм модулей. □

Определение 41. Модуль называется *плоским*, если тензорное домножение на него — точный функтор.

Предложение 13. *Локализация $S^{-1}R$ плоска, как R-модуль.*

Доказательство. Ясно, что достаточно показать, что оно переводит мономорфизмы в мономорфизмы (т.к. точность справа есть всегда).

Пусть $\varphi\colon M \to N -$ мономорфизм R-модулей. Рассмотрим

$$\varphi_S\colon S^{-1}M = M \otimes S^{-1}R \to N \otimes S^{-1}R = S^1N.$$

Тогда $\varphi_S\left(\frac{m}{s}\right) = 0 \Leftrightarrow \frac{\varphi(m)}{s} = 0 \Leftrightarrow \exists s' \in S\colon s'\varphi(m) = 0$. Тогда $\varphi(s'm) = 0$, а так как φ инъективен, отсюда $s'm = 0 \implies \frac{m}{s} = 0$. □

Следствие 17. *Локализация модуля сохраняет ядра, коядря и конечные пересечения пдодмодулей.*

Доказательство. Тензорное умножение на $S^{-1}R$ является точным функтором, а точный функтор всегда сохраняет ядра и коядра.

Рассмотрим пересечение $\bigcap_{i=1}^{n} M_i \subset M$. Тогда

$$\bigcap_{i=1}^{n} M_i = \operatorname{Ker}\left(M \to \bigoplus_{i=1}^{n} M/M_i\right),$$

а ядра, как мы уже убедились, локализация сохраняет. □

Лемма 28. Отображение

$$M \to \prod_{\mathfrak{m} \in \operatorname{Specm} R} M_{\mathfrak{m}}$$

инъективно.

Доказательство. Пусть есть $m \in M$ такой, что $m \mapsto 0$. Это означает, что $\forall \mathfrak{m} \in \operatorname{Specm} R \; \exists s \in S = R \setminus \mathfrak{m}$ (т.е. $s \notin \mathfrak{m}$): $sr = 0$. Напомним такое определение:

Определение 42. Пусть $M - R$-модуль, $N \subset M$. Тогда *аннулятор* N определяется как

$$\operatorname{Ann}(N) \stackrel{\text{def}}{=} \{r \in R \mid rn = 0 \; \forall n \in N\}.$$

Замечание. Если $N \leq M$, то $\operatorname{Ann}(N) -$ идеал в R.

Так вот, предыдущее равенство означает, что $s \in \operatorname{Ann}(r) \setminus \mathfrak{m}$. Но так как $\operatorname{Ann}(r) -$ идеал, а мы имеем такое для любого максимального идеала $\mathfrak{m}$, это означает, что $\operatorname{Ann}(r) = R$, откуда $r = 0$. □

Свойство $\mathfrak{P}$ для R-модулей называется *локальным*, если

$$\mathfrak{P}(M) \Leftrightarrow \forall \mathfrak{p} \in \operatorname{Spec} R \quad \mathfrak{P}(M_{\mathfrak{m}}).$$

Теорема 36. *Следующие свойства модулей и их гомоморфизмов являются локальными:*

1. $M = 0$.
2. $\varphi -$ *инъективен,* $\varphi -$ *сюръективен.*
3. $M -$ *плоский.*
4. $M -$ *проективный.*

Доказательство. Вообще говоря, во всех этих свойствах достаточно пользоваться $\operatorname{Specm} R$.

(1.) В одну сторону очевидно, докажем в другую. Пусть $M_{\mathfrak{m}} = 0 \; \forall \mathfrak{m} \in \operatorname{Specm} R$. Тогда нужно сделать примерно то же самое, что мы уже делали в доказательстве предыдущего утверждения. Условие выше означает, что $\forall x \in M \; \exists s \in R \setminus \mathfrak{m}\colon sx = 0$, откуда следует, что $\operatorname{Ann}(x) \not\subset \mathfrak{m} \; \forall \mathfrak{m} \in \operatorname{Specm} R$, а аннулятор элемента — идеал кольца R. Значит, $\operatorname{Ann}(x) = R \implies x = 0$.

(2.) В одну сторону это будет выполнено просто в силу того, что локализация плоская. Докажем теперь в другую сторону. Пусть $\forall \mathfrak{m} \in \operatorname{Specm} R \; \varphi_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ инъекьивен. Так как локализация сохраняет ядра, это означает, что

$$\forall \mathfrak{m} \in \operatorname{Specm} R \quad \operatorname{Ker}(\varphi_{\mathfrak{m}}) = \operatorname{Ker}(\varphi)_{\mathfrak{m}} = 0.$$

Т.е. $\forall \mathfrak{m} \in \operatorname{Specm} R \; \operatorname{Ker}(\varphi)_{fm} = 0$. Тогда по пункту **(1.)** мы имеем $\operatorname{Ker}(\varphi) = 0$. Для сюръектвности нужно совершенно аналогично доказать, что коядро будет нулевым.

(3.) Заметим, что если $M -$ плоский, то так как $R_{\mathfrak{m}} -$ плоскй,

$$M \otimes R_{\mathfrak{m}} = M_{\mathfrak{m}}$$

тоже будет плоским.

Теперь докажем в обратную сторону. Надо доказать, что если функтор $\_ \otimes M_{\mathfrak{m}}$ точен $\forall \mathfrak{m} \in \operatorname{Specm} R$, то функтор $\_ \otimes M$ будет точным. Так как достаточно проверять, что моно переходит в моно, можно просто воспользоваться пунктом **(2)**. □

Лемма 29. Для любого $\mathfrak{p} \in \operatorname{Spec} R \; M_{\mathfrak{p}} \neq 0 \Leftrightarrow \operatorname{Ann}(M) \leq \mathfrak{p}$.

1.7 Лемма Накаямы

Пусть $I \subset R$ — идеал, M — конечнопорожденный R-модуль.

Из базового курса алгебры мы знаем такой факт:

Теорема 37 (Гамильтона-Кэли). *Пусть $A \in \mathrm{M}_n(R)$, где R — коммутативное кольцо. Тогда $\chi_A(A) = 0$.*

Докажем теперь некоторое его обобщение.

Теорема 38 (Гамильтона-Кэли). *Пусть $\varphi \in \mathrm{End}(M)$ такой, что $\mathrm{Im}\,\varphi \subset IM$. Тогда существует многочлен $p(t) = t^n + \alpha_{n-1}t^{n-1} + \ldots + \alpha_0$ такой что:*

- $\alpha_i \in I^{n-i}$.
- $p(\varphi) = 0$.

Доказательство. Пусть у модуля M есть n образующих, тогда есть сюръективное отображение $R^n \twoheadrightarrow M$ (а значит и $IR^n \twoheadrightarrow IM$) и вообще есть следующая коммутативная диаграмма:

$$\begin{array}{ccc} R^n & \xrightarrow{\psi} & IR^n \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ M & \xrightarrow{\varphi} & IM \end{array}$$

Верхняя стрелка ψ есть из универсального свойства свободного модуля. Так как каждый базисный элемент переходит в элемент с коэффициентами из I, $\psi \in M_n(I)$. Положим $p = \chi_\psi$. Тогда, так как f — сюръективно, $\forall m \in M\ \exists x\colon f(x) = m$. Тогда:

$$p(\varphi)(m) = p(\varphi)(f(x)) = p(\psi)(g(x)) = 0 \implies p(\varphi) = 0.$$

□

Теорема 39 (Лемма Накаямы). *Пусть $M = IM$. Тогда $\exists a \in M\colon \forall m \in I\ am = m$*

Доказательство. $\mathrm{id}_M(M) = IM \implies$, а значит, по теореме Гамильтона-Кэли $\exists p(t) = t^n + \alpha_{n-1}t^{n-1} + \ldots + \alpha_0,\ \alpha_i \in I\colon p(\mathrm{id}_M) = 0$. Тогда

$$\mathrm{id}_M(1 + \alpha_{n-1} + \ldots + \alpha_0) = 0 \implies \mathrm{id}_M(-(\alpha_{n-1} + \ldots + \alpha_0)) = 1.$$

Тогда $a = -(\alpha_{n-1} + \ldots + \alpha_0)$ подходит. В самом деле,

$$am = \mathrm{id}_M(m) = m \quad \forall m \in M.$$

□

Следствие 18. *Если $\varphi \in \mathrm{End}(M)$ и φ — эпиморфизм, то φ — изоморфизм.*

Доказательство. Определим действие $R[t]$ на M при помощи гомоморфизма θ:

$$\theta\colon R[t] \to \mathrm{End}(M) \quad \theta(t) = \varphi.$$

Так как φ — эпиморфизм, $tR[t]M = M$.

Тогда по лемме Накаямы существует $f \in (t) = tR[t]$ такой, что $fm = m\ \forall m \in M$. Запишем $f = tg$ для некоторого $g \in R[t]$ и спроектируем результат в $\mathrm{End}(M)$:

$$tg(t) \cdot m = m \implies \varphi(g(\varphi)(m)) = m \Leftrightarrow \varphi \circ g(\varphi) = \mathrm{id}\,.$$

Но, по определению, $g(\varphi) = \varphi(g)$, тогда

$$g(\varphi)(\varphi(m)) = m,$$

$g(\varphi)$ — обратный к φ. □

1.8 Радикал Джекобсона

Кольцо R, рассматриваемое, как модуль над собой, называется *регулярным* R-модулем.

Определение 43. Аннулятором R-модуля M называется множество $\{r \in R \mid rM = 0\}$.

Лемма 30. Ненулевой простой R-модуль M изоморфен $R/\mathfrak{m}$ для некоторого $\mathfrak{m} \in \operatorname{Specm} R$. Таким образом, $\operatorname{Ann} M$ является максимальным идеалом кольца R.

Доказательство. □

1.9 Кольца нормирования, кольца дискретного нормирования и Дедекиндовы области

Определение 44. Пусть R — область целостности, F — её поле частных. R называется *кольцом нормирования*, если $R \cup (R \setminus 0)^{-1} = F$. То есть, $\forall x \in F$ либо $x \in R$, либо $x^{-1} \in R$.

Пример 16. Например, кольцами нормирования являются $\mathbb{Z}_{(p)},\ \mathbb{Z}_p,\ F[[x]]$.

Определение 45. Пусть F — поле, а функция $\upsilon\colon F^* \to \Gamma$, где Γ — линейно упорядоченная абелева группа, гомоморфизм, т.е. $\upsilon(ab) = \upsilon(a) + \upsilon(b)$, причём выполнено $\upsilon(a+b) \geq \min(\upsilon(a), \upsilon(b))$ называется *нормированием*.

Если υ действует в $\mathbb{Z}$ и сюръективна, то её называют *дискретным нормированием* на F.

Следующая теорема устанавливает связь между нормированием на поле и кольцами нормирования.

Теорема 40. *1. Пусть υ — нормирование на F, тогда $R \stackrel{\text{def}}{=} \{x \in F \mid \upsilon(x) \geq 0\}$ — кольцо нормирования.*

2. Если R — кольцо нормирования с полем частных F, то можно положить $\Gamma = F^*/R^{*2}$ и задать на ней порядок следующим образом:

$$aR^* \geq bR^* \Leftrightarrow ab^{-1} \in R.$$

и задать $\upsilon\colon F^* \to F^*/R^*$. Тогда такое υ будет нормированием.

3. Процедуры из пунктов (1) и (2) взаимнообратны с точностью до изоморфизма на $\operatorname{Im}\upsilon$ (как упорядоченных групп).

Доказательство. Докажем сначала (1):

$$\upsilon(x) + \upsilon(x^{-1}) = 0 \implies \upsilon(x) \geq 0 \text{ или } \upsilon(x^{-1}) \geq 0 \Leftrightarrow x \in R \text{ или } x^{-1} \in R.$$

Теперь докажем (2). Действительно, если R — кольцо номрирования, то либо $ab^{-1} \in R$, откуда $\upsilon(a) \geq \upsilon(b)$, либо $a^{-1}b \in R$, откуда $\upsilon(b) \geq \upsilon(a)$, то есть на $\Gamma = F^*/R^*$ порядок будет линейным. Кроме того,

$$\begin{cases} \upsilon(a) \geq \upsilon(b) \\ \upsilon(b) \geq \upsilon(a) \end{cases} \Leftrightarrow ab^{-1} \in R^* \Leftrightarrow aR^* = bR^* \Leftrightarrow \upsilon(a) = \upsilon(b),$$

что показывает антисимметричность.

Кроме того, $\upsilon(a+b) \geq \upsilon(a)$, либо $\upsilon(a+b) \geq \upsilon(b)$, откуда

$$\frac{a+b}{a} = 1 + \frac{b}{a} \in R, \text{ либо } \frac{a+b}{b} = 1 + \frac{a}{b} \in R.$$

Доказательство взаимной обратности остается в качестве простого **упражнения**. □

[2] в аддитивной записи...

Предложение 14. *Пусть R — кольцо нормирования, тогда R —- локально и целозамкнуто.*

Доказательство. Положим $\mathfrak{m} \stackrel{\text{def}}{=} \{a \in R \mid \upsilon(a) > 0\}$. Ясно, что $\forall x \in R, a \in \mathfrak{m}\ \upsilon(ax) = \upsilon(a) + \upsilon(x) \geq \upsilon(a) > 0$ и $\forall a, b \in \mathfrak{m}\ \upsilon(a+b) \geq \min(\upsilon(a), \upsilon(b)) > 0$, что показывает нам, что $\mathfrak{m}$ — идеал. Все остальные элементы имеют нормирвоание, равное нулю, и поэтому они обратимы (просто по определению), значит $\mathfrak{m}$ — единственный максимальный идеал кольца R.

Теперь докажем целозамкнутость. Действительно, пусть $a \in F$

$$a^n + r_{n-1}a^{n-1} + \ldots + r_0 = 0,\ r_i \in R \implies a^n = r'_{n-1}a^{n-1} + \ldots + r'_0 \implies \upsilon\left(\sum_{i=1}^{n-1} r'_i a^i\right) \geq$$
$$\geq \min \upsilon\left(r'_i a^i\right) \geq \min \upsilon\left(a^i\right) = \min(i \cdot \upsilon(a)) \implies \upsilon(a) \geq 0 \implies a \in R.$$

□

Предложение 15. *Пусть R — кольцо дискретного нормирования с нормированием R. Тогда*

1. $R \setminus \{0\} \cong R^* \times \langle\pi\rangle$[3]
2. $\operatorname{Ideals}(R) = \{0, R, \pi^n R,\ \text{где } n \in \mathbb{N}\}$.
3. $\operatorname{Spec} R = \{0, \pi R\}$.
4. $\operatorname{Specm} R = \{\pi R\}$.

Доказательство. Докажем сначала (1). Возмём $\pi\colon \upsilon(\pi) = 1$ (мы можем так сделать, так как дискретное нормирование сюръективно). Возьмём $a \in R$, $\upsilon(a) = n \in \mathbb{Z} \implies \upsilon(a\pi^{-n}) = 0 \Leftrightarrow a\pi^{-n} \in R^* \Leftrightarrow a \in \pi^n R$ (причем очевидно, что такое представление единственно.

Рассмотрим $I \in \operatorname{Ideals}(R)$, возьмём $n = \min_{a \in I} \upsilon(a) = \upsilon(b) = \upsilon(\pi^n \alpha)$, где $\alpha \in R^*$, а значит, $\forall c \in I\colon c = \pi^k \beta,\ k \geq n \implies c \in \pi^n R$. □

Лемма 31. Пусть R — нётерова область целостности, $\mathfrak{m} \in \operatorname{Specm} R,\ \mathfrak{m} \neq 0$, тогда $\mathfrak{m}^k \neq \mathfrak{m}^{k+1}\ \forall k \in \mathbb{N}$.

Доказательство. Рассмотрим $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ — векторное пространство над $R/\mathfrak{m}$. Тогда

$$\mathfrak{m}^k/\mathfrak{m}^{k+1} \otimes_R R_{\mathfrak{m}} \cong (\mathfrak{m}R_{\mathfrak{m}})^k/(\mathfrak{m}R_{\mathfrak{m}})^{k+1} = 0 \implies \mathfrak{m}R_{\mathfrak{m}}(\mathfrak{m}^k R) = (\mathfrak{m}^k R_{\mathfrak{m}}) \implies \mathfrak{m}^k R_{\mathfrak{m}} = 0 \implies \mathfrak{m} = 0.$$

В предпоследнем переходе мы используем лемму Накаямы (там конечнопорожденный модуль $\mathfrak{m}^k R_{\mathfrak{m}}$ умножается на $\mathfrak{m}R_{\mathfrak{m}} = \operatorname{Rad}(R_{\mathfrak{m}})$). □

Теорема 41. *Пусть R — область целостности. Тогда следующие условия эквивалентны:*

1. *R — кольцо дискретного нормирования.*
2. *R — нётерово локальное целозамкнутое кольцо размерности Крулля 1.*
3. *R — локальное нётерово неполе, в котором максимальный идеал главный.*
4. *R — факториальное кольцо с единственным (с точностью до ассоциированности) неприводимым элементом.*
5. *Локальное неполе, идеалы которого имеют вид $\operatorname{Ideals}(R) = \{0, \mathfrak{m}^k \mid k \in \mathbb{N}_0\}$*

Доказательство. (1) $\implies$ (2) мы уже по сути доказали в утверждении 15. Докажем теперь (2) $\implies$ (3). Мы знаем, что $\operatorname{Specm} R = \{\mathfrak{m}\}$, возьмём $a \in \mathfrak{m} \setminus \mathfrak{m}^2$ по лемме 31. Рассмотрим $aR \subset \mathfrak{m}$. Из примарного разложения aR следует, что aR — $\mathfrak{m}$-примарный. Тогда существует $k\colon \mathfrak{m}^k \subset aR \subset \mathfrak{m}$, выберем наименьшее из таких k. Теперь заметим, что

$$b \in \mathfrak{m}^{k-1} \setminus aR \Leftrightarrow \frac{b}{a} \in \frac{\mathfrak{m}^{k-1}}{a}$$

Дописать этот кусок.

(3) $\implies$ (4) : Возьмём $\pi \in R$ — неприводимый, тогда $\pi \in \mathfrak{m} = aR$, а значит, π — ассоциирован с a.

□

[3] тут имеется в виду изоморфизм моноидов.

1.10 Дедекиндовы кольца

Предложение 16. *Пусть R — нётерова одномерная область целостности. Тогда следующие условия эквивалентны:*

1. *R целозамкнуто.*
2. *Любой примарный идеал имеет вид $\mathfrak{m}^k$ для некоторого $\mathfrak{m} \in \operatorname{Specm} R$.*
3. *$\forall \mathfrak{m} \in \operatorname{Specm} R$ кольцо $R_\mathfrak{m}$ — кольцо дискретного нормирования.*

Доказательство. $(1) \Leftrightarrow (3)$ просто в силу того, что целозамкнутость — локальное свойство и теоремы 41. Ну и, в силу того, что $R_\mathfrak{m}$ — нётеровы одномерные локальные.

$(3) \implies (2)$: В таком кольце любой ненулевой примарный идеал I является $\mathfrak{m}$-примарным, а такие однозначно соотвествуют примарным идеалам локализации $R_\mathfrak{m}$. Так как $R_\mathfrak{m}$ — DVR, там все примарные идеалы имеют вид $\mathfrak{m}^n R_\mathfrak{m}$ (так как $R_\mathfrak{m}$ — локальное кольцо с единственным максимальным идеалом $\mathfrak{m}R_\mathfrak{m}$), а λ_* — биекция на множестве примарных идеалов, не пересекающихся с мультипликативным подмножеством (которое тут $R \setminus \mathfrak{m}$, да), мы имеем $\lambda_*(I) = \lambda_*(\mathfrak{m}^n) \implies I = \mathfrak{m}^n$.

$(2) \implies (3)$: Любой идеал в $R_\mathfrak{m}$ имеет примарное разложение $\implies$ является примарным. $\lambda^*(J)$ — $\mathfrak{m}$-примарный $\implies \lambda^*(J) = \mathfrak{m}^n \implies \lambda_*(\lambda^*(J)) = \lambda_*(\mathfrak{m}^n) = (\mathfrak{m}R_\mathfrak{m})^n$, откуда по теореме 41 $R_\mathfrak{m}$ — кольцо дискретного нормирования. □

Определение 46. Кольца, удовлетворяющие условию 16 называют *дедекиндовыми.*

Теорема 42. *Пусть Z — Дедекиндово кольцо, Q — его поле частных, F/Q — конечное расщирение (полей), а $R = \operatorname{Int}_F Z$. Тогда R — дедекиндово.*

Доказательство. Так как R — целое замыкание, $\dim R = 1$. Так как F — конечное расширение, $\forall \alpha \in F$ является корнем многочлена

$$\alpha^n + \frac{a_{n-1}}{b_{n-1}}\alpha^{n-1} + \ldots + \frac{a_0}{b_0} = 0, \quad a_i, b_i \in \mathbb{Z} \implies b\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_0 = 0 \implies (b\alpha)^n + d_{n-1}(b\alpha)^{n-1} + \ldots + d_0 = 0$$

Значит, $b\alpha \in R$, откуда $\alpha \in (Z \setminus 0)^{-1}R$.

Так как F — поле частных R, R целозамкнуто. Для дедекиндовости нам не хватает Нётеровости.

Рассмотрим F, как векторное пространство над Q. Рассмотрим оператор

$$m_\alpha \in \operatorname{End}_{Q-\mathfrak{mod}}(F),\ m_\alpha(x) = \alpha x.$$

Далее доказательство приводится только для случая сепарабельного расширения. Так вот, если расширение сепарабельно, $\exists \alpha \in F\colon \operatorname{Tr} m_\alpha \neq 0$. Рассмотрим невырожденную билинейную форму $B(x, y) = \operatorname{Tr} m_{xy}\colon F \times F \to Q$.

Возьмём базис $u_1, \ldots, u_n$ — базис F над Q (можно полагать, что $u_i \in R$) и $v_1, \ldots, v_n$ — двойственный базис относительно B. Возьмём $x \in F$, тогда

$$x = \sum_{k=1}^{n} B(x, u_k)v_k.$$

$x \in R,\ u_k \in R$, тогда $xu_k \in R$, а значит, его минимальный многочлен над Q имеет коэффициенты из Z (была такая теорема, надо найти и вставить ссылку). В то же время ясно, что минимальный многочлен xu_k равен минимальному многочлену эндоморфизма m_{xu_k}. Собственные числа m_{xu_k} — это корни минимального многочлена, а они являются целыми над Z, следовательно и их сумма (с учетом кратности) — целая над Z, а это в точности след. Значит, R — подмодуль конечнопорожденного Z-модуля, а значит, так как Z — дедекиндово, R конечнопорождено, как Z-модуль $\implies R$ — нётерово. □

В случае $Z = \mathbb{Z}$, кольцо R называется дедекиндовым кольцом *арифметического типа* или *кольцом целых числового поля.* В случае $Z = K[t]$ кольцо R называется дедекиндовым кольцом *функционального* типа.

1.11 Hauptidealsatz

Определение 47. Пусть I — идеал. Тогда его *высота* $\operatorname{ht}(I)$ — длина наибольшей цепочки вложенных в него простых идеалов.

Теорема 43 (Крулль, о высоте)**.** *Пусть $x \in R$ — нётерово коммутативное кольцо с единицей, $\mathfrak{p}$ — минимальный простой идеал, содержащий $(x) = xR$. Тогда* $\operatorname{ht}(\mathfrak{p}) \leq 1$.

Доказательство. Во-первых, условие теоремы располагает к замене R на $R_{\mathfrak{p}}$, т.е. далее будем считать, что R — локально с единственным максимальным идеалом $\mathfrak{p}$. Так что $\mathfrak{p}$ — единственный минимальный простой, содержащий xR, а xR — $\mathfrak{p}$-примарным, откуда $\dim(R/xR) = 0$. Значит, R/xR — нульмерное нётерово, то есть Артиново. Действительно, $\sqrt{xR} = \mathfrak{p} \implies \exists n \in \mathbb{N}\colon \mathfrak{p}^n = xR$, откуда $(\mathfrak{p}/xR)^n = 0$. Значит, если $p' \in \operatorname{Spec} R/xR$, то

$$(\mathfrak{p}/xR)^n \subset \mathfrak{p}' \subset \mathfrak{p}/xR \implies \mathfrak{p}/xR \subset \mathfrak{p}' \subset \mathfrak{p}/xR.$$

Определение 48. Пусть $\mathfrak{q} \in \operatorname{Spec} R,\ \lambda = \lambda_{\mathfrak{q}}\colon R \to R_{\mathfrak{q}}$. Тогда *символическая степень* идеала $\mathfrak{q}$ используется, как

$$\mathfrak{q}^{(n)} \stackrel{\text{def}}{=} \lambda^*(\lambda_*(\mathfrak{q}^n)).$$

Лемма 32. Идеал $\mathfrak{q}^{(n)}$ — примарный.

Доказательство. $\lambda_*(\mathfrak{q}) \in \operatorname{Spec} R_{\mathfrak{q}} \implies \lambda_*(\mathfrak{q}^n) = \lambda_*(\mathfrak{q})^n$ — примарный, а λ^* отображает примарные в примарные. □

Пусть $\bar{\cdot}\colon R \to R/xR$ — канонический гомоморфизм. Рассмотрим в R/xR такую убывающую цепочку идеалов:

$$\overline{q} \supset \overline{\mathfrak{q}^{(2)}} \supset \ldots \supset \overline{\mathfrak{q}}^{(n)} = \overline{\mathfrak{q}}^{n+1},$$

так как R/xR — артиново. Возьмём $q^{(n)} \ni z = y + xr,\ y \in \mathfrak{q}^{(n+1)}, r \in R$. Тогда $xr\mathfrak{q}^{(n)}$ и $x \notin \mathfrak{q} = \sqrt{\mathfrak{q}^{(n)}}$. Тогда отсюда следует, что $r \in q^{(n)}$

Теперь $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} + x \cdot \mathfrak{q}^{(n)}$. Тогда в $R/\mathfrak{q}^{(n+1)}$ мы имеем $\widetilde{x}\widetilde{q^{(n)}} = \widetilde{\mathfrak{q}^{(n)}},\ \widetilde{x} \in \operatorname{Rad} R/\mathfrak{q}^{(n+1)}$ и тогда по лемме Накаямы $\mathfrak{q}^{(n)} = 0$.

Значит, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)} \implies \lambda^*(\lambda_*(\mathfrak{q}^n)) = \lambda^*(\lambda_*(\mathfrak{q}^{n+1})) \implies \lambda_*(\mathfrak{q})^n = \lambda_*(\mathfrak{q})^n \cdot \lambda_*(\mathfrak{q})$, а $\lambda_*(\mathfrak{q}) \subset \operatorname{Rad}(R_{\mathfrak{q}})$ и тогда опять же по лемме Накаямы мы имеем $\lambda^*(\mathfrak{q}^n) = 0$.

Значит, $\operatorname{Spec} R_{\mathfrak{q}} = \{\mathfrak{q}\} \implies$ в R нет простых, содержащихся в $\mathfrak{q} \implies \operatorname{ht}(\mathfrak{q}) = 0 \implies \operatorname{ht}(\mathfrak{p}) \leq 1$. □

1.12 Пополнения

Пусть A — абелева группа с убывающей фильтрацией

$$A \supset A_0 \supset A_1 \supset \ldots A_n \supset$$

A можно сделать топологической группой, взяв в качестве базы окрестностей нуля $\{A_n\}$. В нашем случае A обычно будет кольцом или модулем, а фильтрация будет степенями идеала.

Ясно, что если $0 \neq a \in \bigcap A_i$, то её отделить от остальных не получится. Соотвественно, можно просто декларировать, что топология, заданная этой фильтрацией Хаусдорфова тогда и только тогда, когда

$$\bigcap_i A_i = 0.$$

Также заметим, что в этой топологии каждая A_i будет не только открытой, но и замкнутой, так как все их сдвиги $x + A_i$ открыты, значит все смежные классы открыты и достаточно перейти к дополнению всех, кроме одного, откуда мы получим, что этот один смежный класс $y + A_j$ замкнут, следовательно A_j замкнуто.

Возьмём теперь пополнение по этой топологии. А именно, возьмём прямой предел по следующей последовательности:

$$\ldots \xrightarrow{\theta_2} A/A_2 \xrightarrow{\theta_1} A/A_1 \xrightarrow{\theta_0} A/A_0, \quad \widehat{A} \stackrel{\text{def}}{=} \varprojlim A/A_n.$$

Определение 49. Соотвественно, *пополнением* A в топологии, связанной с фильтрацией $\{A_n\}$ называется определённое выше $\widehat{A}$.

Пример 17. Например, $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z}$ или $F[[t]] = \varprojlim F[t]/(t)^n$.

Говорят, что фильтрации (A_n) и (B_n) имеют ограниченую разность, если

$$\exists n_0 \in \mathbb{N}\colon A_{n+n_0} \subset B_n \text{ и } B_{n+n_0} \subset A_n \ \forall \mathbb{N}.$$

Ясно, что такие фильтрации задают одну и ту же топологию, но, на самом деле это условие сильнее (это мы поймём чуть попозже).

Напомним лемму о змее:

сюда диаграмму про лемму о змее

Лемма 33. Рассмотрим точную последовательность

$$0 \to A' \to A \to A'' \xrightarrow{p} 0,$$

(A_n) — фильтрация на A, $((A_n) \cap A')$ — фильтрация на A' и $(p(A_n))$ на A". Тогда после перехода к пополнениям мы также получим точную последовательность

$$0 \to \widehat{A'} \to \widehat{A} \to \widehat{A''} \to 0.$$

Рабоче крестьянское доказательство. Перейдём к точной последовательности:

$$0 \to A'/A_n \cap A' \to A/A_n \to A''/p(A_n)$$

Определим теперь $\widetilde{A}$ и гомоморфизм d, как

$$\widetilde{A} = \prod_{n=0}^{\infty} A/A_n \xrightarrow{d} \widetilde{A}, \quad d((c_n)) = (c_n - \theta(c_{n+1})).$$

Несложно заметить, что $\operatorname{Ker} d = \widehat{A}$. Соотвественно, надо рассмотреть диаграмму

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{A'} & \longrightarrow & \widehat{A} & \longrightarrow & \widehat{A''} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \widetilde{A'} & \longrightarrow & \widetilde{A} & \longrightarrow & \widetilde{A''} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d'} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d''} & & \\
0 & \longrightarrow & \widetilde{A'} & \longrightarrow & \widetilde{A} & \longrightarrow & \widetilde{A''} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{Coker}(d') & \longrightarrow & \operatorname{Coker}(d) & \longrightarrow & \operatorname{Coker}(d'') & &
\end{array}$$

и применить лемму о змее. Засчет сюръективности θ' $\forall(b_n)$ мы сможем подобрать (c_n) такие, что $d'(c_n) = (b_n)$. А если d' сюръективен, то $\operatorname{Coker} d' = 0$ и из леммы о змее мы получаем нужную диаграмму:

$$0 \to \widehat{A'} \to \widehat{A} \to \widehat{A''} \to \operatorname{Coker} d' = 0.$$

□

Умновое доказательство. Оказывается, если существуют пределы $\lim X_n, \lim Y_n, \lim Z_n$ (где речь идет об объектах абелевой категории), то последовательность

$$0 \to \lim X_n \to \lim Y_n \to \lim Z_n$$

точна вообще всегегда, так как ядро — это предел, а пределы коммутируют, так как предельный функтор сопряжен к диагональному, а значит, сохраняет пределы. □

Следствие 19. $\widehat{A}/\widehat{A_n} \cong A/A_n$.

Доказательство. Из прошлой леммы, полагая $A' = A_n$, мы получаем короткую точную последовательность

$$0 \to \widehat{A_n} \to \widehat{A} \to \widehat{A/A_n} \to 0$$

А теперь заметим, что

$$(A/A_n) \supset A_1/A_n \supset \ldots \supset A_n/A_n \supset 0 \supset \ldots,$$

откуда $\widehat{A/A_n} = A/A_n$ и из точности последоватльности выше мы получаем нужное. □

Следствие 20. *Переходя в предыдущем следствии к пределу, мы получаем, что*

$$\widehat{\widehat{A}} = \varprojlim \widehat{A}/\widehat{A_n} \cong \widehat{A},$$

то есть пополение полно[4]

Пример 18. На простых примерах видна некоторая эвристика: $\mathbb{Z} \hookrightarrow \mathbb{Z}_p,\ F[t] \hookrightarrow F[[t]]$.

На самом деле, верно такое общее утверждение

Теорема 44. $\operatorname{Ker}\Big(A \to \widehat{A}\Big) = \bigcap_{n=0}^{\infty} A_n$.

1.13 Градуированные алгебры и модули

Определение 50. Пусть $R_i - A$-модули. R называют $\mathbb{N}$-*градуированной* A-*алгеброй*, если

$$R = \bigoplus_{i=0}^{\infty} R_i, \quad R_i \cdot R_j \subset R_{i+j}.$$

Градуированным R-модулем называют $M = \bigoplus M_i$ с условием $R_i M_j \subset M_{i+j}$.

Предложение 17. *Градуированное кольцо R является Нётеровым тогда и только тогда, когда R_0 — нётерово и R — конечнопорожденная R_0-алгебра.*

Доказательство. В обратную сторону это почти очевидно: достаточно применить теорему Гильберта о Базисе и то, что нётеровость сохраняется при эпиморфизме.

Теперь докажем в обратную сторону. Положим

$$R_+ = \bigoplus_{n=1}^{\infty} R_n \trianglelefteq R,$$

пусть R_+ порождён $\{x_1, \ldots, x_s\}$ над R. Эти x_i можно считать однородными, т.к. иначе разобьем на однородные компоненты, которые всё еще будут порождать. Таким образом, $x_i \in R_{k_i}$ для некоторого k_i. Возмём $y \in R_n$,

$$y = \sum_{j=1}^{m} x_j z_j, \quad z_j \in R_{n-k_j}.$$

По индукционному предположению $z_j \in R_0[x_1, \ldots, x_s] \implies y \in R_0[x_1, \ldots, x_s]$. □

Пусть $I \trianglelefteq R$, расммотрим *алгебру раздутия*:

$$\mathrm{Bl}_I(R) = \bigoplus_{n=1}^{\infty} I^n.$$

[4] что вполне логично.

2. Аффинные многообразия

2.1 Введение. Аффинные алгебраические многообразия. Идеалы, неприводимые многообразия.

Прежде всего отметим, что в данном курсе будет изучаться аффинная алгебраическая геометрия и речь пойдет об *аффинных*[5] *многообразиях.*

Пусть $\Bbbk$ — алгебраически замкнутое поле, через $\mathbb{A}^n_\Bbbk = \mathbb{A}^n$ мы будем обозначать $\Bbbk^n$, рассматриваемое как множество, и будем называть это множество *n-мерным аффинным пространством* над $\Bbbk$. Определим на нём топологию.

Определение 51. Рассмотрим $T \subset \Bbbk[x_1, \ldots, x_n]$ и определим

$$Z(T) \stackrel{\text{def}}{=} \{(a_1, \ldots, a_n) \in \mathbb{A}^n_\Bbbk | f(a_1, \ldots, a_n) = 0 \quad \forall f \in T\}.$$

Замечание. В случае $T = \varnothing$ естественно полагать $Z(T) = \mathbb{A}^n_\Bbbk$. Кроме того, сразу заметим, что $Z((1)) = \varnothing$.

Замечание. Пусть $I = (T)$ — идеал, порождённый множеством T. В этом случае $Z(T) = Z(I)$, так как если $(a_1, \ldots, a_n)$ является нулём для всех элементов идеала, то для $T \subset I$ уж тем более, и, кроме того, если $(a_1, \ldots, a_n)$ является общим нулём многочленов из T, то $f \in I$ мы можем представить

$$f = \sum g_i h_i, \quad h_i \in T,\ g_i \in \Bbbk[x_1, \ldots, x_n]$$

и тогда ясно, что $f(a_1, \ldots, a_n) = 0$.

Отсюда ясно, что достаточно рассматривать не произвольные подмножества $\Bbbk[x_1, \ldots, x_n]$, а идеалы этого кольца.

Определение 52. Введём на $\mathbb{A}^n_\Bbbk$ *топологию Зарисского* следующим образом: объявим замкнутыми все множества вида $Z(T)$ для некоторого T.

Покажем, что это действительно топология.

1. Ясно, что $Z(T_1) \cup Z(T_2) = Z(T_1 T_2)$, где $T_1 T_2 = \{f_1 f_2 \,|f_1 \in T_1,\ f_2 \in T_2\}$.
   Совсем очевидно, что левая часть лежит в правой. Пусть $f_1 f_2(a_1, \ldots, a_n) = 0\ \forall f_1 \in T_1,\ f_2 \in T_2$. Если $f_1 f_2(a_1, \ldots, a_n) = 0$, то хотя бы один многочлен из произведения зануляется, откуда ясно обратное включение.
2. Кроме того, ясно, что $\bigcap_{i \in I} Z(T_i) = Z\left(\bigcup_{i \in I} T_i\right)$.

Пример 19. Рассмотрим $\mathbb{A}^1_\Bbbk$. Какими могут быть замкнутые множества? Пусть

- Если $T = 0$, то $Z(T) = \mathbb{A}^1$ — замкнутое.
- Если все многочлены из T взаимнопросты, то $Z(T) = \varnothing$.
- Если из T многочлены имеют нетривиальный наибольший общий делитель $f(x) = (x - a_1) \cdot \ldots \cdot (x - a_n)$, то $V(T) = a_1, \ldots, a_n$ — конечный набор точек.

С другой стороны, если у нас есть конечное множество $\{a_1, \ldots, a_n\} \subset \mathbb{A}^1_\Bbbk$, то оно является множеством нулей многочлена

$$f(x) = \prod_{i=1}^{n} (x - a_i).$$

Таким образом, замкнутые подмножества аффинной прямой — в точности все конечные подмножества $\mathbb{A}^1_\Bbbk$, пустое и сама прямая $\mathbb{A}^1_\Bbbk$. Также отсюда ясно, что любые два открытых подмножества пересекаются и топология Зарисского не хаусдорфова.

[5] и квазиафинных, а также, (квази)проективных.

Определение 53. Пусть X — тополгическое пространство, $Y \subset X,\ Y \neq \varnothing$. Y называется *неприводимым*, если из равенства $Y = Y_1 \cup Y_2$, где Y_i замкнуты в Y, следует, что $Y_1 = Y$ или $Y_2 = Y$.

То есть, неприводимые подмножества — в точности те, которые нельзя представить в виде объединения двух замкнутых множеств.

Пример 20. Аффинная прямая $\mathbb{A}^1_{\Bbbk}$ неприводима (просто из соображений мощности).

Теперь докажем такой общетопологический факт:

Предложение 18. *Открытое*[6] *подмножество неприводимого — неприводимо и плотно. Замыкание неприводимого множества неприводимо.*

Доказательство. Пусть $U \subset Y$ — открытое подмножество. Покажем, что оно неприводимо. Пусть

$$U = (U \cap F_1) \cup (U \cap F_2), \quad F_1, F_2 \text{ замкнуты в } Y.$$

Тогда $Y = F_1 \cup F_2 \cup (Y \setminus U)$, а так как Y — неприводимо, Y совпадает с каким-то из этих множеств. С $Y \setminus U$ оно совпасть не может, так как $U \neq \varnothing$. Тогда $Y = F_i \implies U \cap F_i = U \cap Y = U$, что мы и хотели.

Теперь докажем, что $\overline{U} = Y$. Действтельно, $Y = (Y \setminus U) \cup \overline{U}$ и из неприводимости Y и непустоты U следует, что $\overline{U} = Y$. □

Определение 54. Замкнутые непустые подмножества в $\mathbb{A}^n_{\Bbbk}$ мы будем называть *аффинными алгебраическими многообразиями.*[7]

Пример 21. Рассмотрим $\mathbb{A}^1 \setminus \{0\}$. Это множество не является замкнутым в нашей топологии. С другой стороны, есть взаимно-однозначное соотвествие между этим множеством и множеством $\{(x, y) \in \mathbb{A}^2 \mid xy - 1 = 0\}$, которое является аффинным многообразем.

В одну сторону нам надо сделать проекцию графика гиперболы на горизонтальную ось: $(x, y) \mapsto x \in \mathbb{A}^1 \setminus \{0\}$, а в обратную сторону, мы можем отобразить $\mathbb{A}^1 \setminus \{0\} \ni x \mapsto (x, x^{-1})$.

Замечание. Пример выше наводит на мысль о том, что наше определение не достаточно общее. Довольно скоро мы его обобщим. Вообще говоря, в данном конспекте под словом *многообразие* будет пониматься самое общее, что введено к данному моменту курса.

Определение 55. Рассмотрим $Y \subset \mathbb{A}^n_{\Bbbk}$, положим

$$I(Y) \stackrel{\text{def}}{=} \{f \in \Bbbk[x_1, \ldots, x_n] \mid f(y) = 0 \quad \forall y \in Y\}.$$

Совершенно ясно, что $I(Y)$ — идеал. Кроме того, отметим, что для $Y = \mathbb{A}^n_{\Bbbk}\ I(Y) = 0$, а для $Y = \varnothing,\ I(Y) = (1)$. Таким образом, у нас есть отображения

$$\Bbbk[x_1, \ldots, x_n] \supset T \mapsto Z(T), \quad \mathbb{A}^n_{\Bbbk} \supset Y \mapsto I(Y).$$

Предложение 19. *Определённые выше отображения имеют следующие свойства:*

1. $T_1 \subset T_2$, *где* $T_1, T_2 \subset \Bbbk[x_1, \ldots, x_n],\ Z(T_1) \supset Z(T_2)$.
2. *Если* $Y_1 \subset Y_2 \subset \mathbb{A}^n_{\Bbbk}$, *то* $I(Y_1) \supset I(Y_2)$.
3. $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.
4. *Пусть* $I \trianglelefteq \Bbbk[x_1, \ldots, x_n]$, *тогда* $I(Z(I)) = \sqrt{I}$.
5. $Y \subset \mathbb{A}^n_{\Bbbk} \implies Z(I(Y)) = \overline{Y}$.

Доказательство. Перые три пункта очевидны. Четвертый и пятый пункт следуют из (сильной) теоремы Гильберта о нулях:

Теорема 45 (Теорема Гильберта о нулях)**.** *Пусть* $\Bbbk = \Bbbk^{alg}$, $I \trianglelefteq F[t_1, \ldots, t_n]$, *а* $f \in \Bbbk[x_1, \ldots, x_n]$. *Тогда* $f(Z(I)) = 0 \Leftrightarrow f \in \sqrt{I}$. *Иными словами,* $I(Z(I)) = \sqrt{I}$.

[6] непустое...

[7] Отметим, что в книге Хартсхорна все аффинные алгебраические многообразия предполагаются неприводимыми.

Докажем теперь пятый пункт. Включение $\overline{Y} \subset Z(I(Y))$ очевидно, так как $Y \subset Z(I(Y))$, а правое множество замкнуто.

Рассмотрим произвольное замкнутое W, содержащее Y. Так как оно замкнуто, $W = Z(\mathfrak{a})$ для некоторого идеала $\mathfrak{a}$. Тогда $I(Z(\mathfrak{a})) \subset I(Y) \implies \mathfrak{a} \subset I(Y)$ (так как $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}} \supset \sqrt{\mathfrak{a}}$). Тогда мы получили, что $Z(I(Y))$ содержится в любом замкнутом множестве, содержащем Y, то есть $Z(I(Y)) = \overline{Y}$. □

Предложение 20. *Отображения $Y \mapsto I(Y)$ устанавливает взаимно однозначное соотвествие между аффинными многообразиями в $\mathbb{A}^n_{\Bbbk}$ и радикальными идеалами кольца многочленов $\Bbbk[x_1, \ldots, x_n]$.*

При этом, неприводимым аффинным многообразиям соотвествуют простые идеалы и наоборот.

Доказательство. На самом деле, то, что отображения Z и I взаимно обратные, мы уже фактически видели в предложении 19. Покажем инъективность:

$$I(Y_1) = I(Y_2) \implies Y_1 = \overline{Y_1} = Z(I(Y_1)) = Z(I(Y_2)) = \overline{Y_2} = Y_2.$$

Возьмём теперь некоторый радикальный идеал $I = \sqrt{I}$. Пусть $Y = Z(I)$, тогда $I(Y) = \sqrt{I} = I$, что даёт сюръективность отображения.

Пусть теперь Y неприводимо. Покажем, что $I(Y)$ — простой идеал. Рассмотрим $f, g \in \Bbbk[x_1, \ldots, x_n]$, пусть $fg \in I(Y)$. Заметим, что

$$Y = (Y \cap Z(f)) \cup (Y \cap Z(g)),$$

тогда одно из этих множеств совпадает с Y. Пусть, например, $Y = Y \cap Z(f) \implies Y \subset Z(f) \implies f \in I(Y)$.

Наоборот, предположим, что $I(Y)$ — простой идеал. Пусть $Y = Y_1 \cup Y_2$, тогда

$$I(Y) = I(Y_1) \cap I(Y_2) \supset I(Y_1)I(Y_2).$$

Так как идеал простой, не умаляя общности, $I(Y_1) \subset I(Y) \implies Y \subset Y_1 \implies Y = Y_1$, что мы и хотели

□

Посмотрим, куда при этом соотвествии переходят точки. Пусть $P = (a_1, \ldots, a_n)$. Ясно, что

$$I(P) = \{f \mid f(a_1, \ldots, a_n) = 0\} = (x_1 - a_1, \ldots, x_n - a_n).$$

Слабая теорема Гильберта о нулях говорит нам, что все максимальные идеалы $\Bbbk[x_1, \ldots, x_n]$ имеют вид $(x_1 - a_1, \ldots, x_n - a_n)$, а значит, мы только что поняли, что есть соответствие

$$\text{точки } \mathbb{A}^n_{\Bbbk} \longleftrightarrow \operatorname{Specm}(\Bbbk[x_1, \ldots, x_n]).$$

2.2 Разложение в неприводимые компоненты

Определение 56. Топологическое пространство X называется *Нётеровым*, если оно удовлетворяет DCC для замкнутых множеств. Иными словами, если у нас есть цепочка

$$\forall\, Z_0 \supset Z_1 \supset Z_2 \supset \ldots \; \exists n \colon Z_n = Z_{n+1}.$$

Или же, еще более иными словами, в любом семействе замкнутых множеств содержится минимальный (по включению) элемент.

Пример 22. $\mathbb{A}^n_{\Bbbk}$ является Нётеровым, так как по теореме Гильберта о базисе $\Bbbk[x_1, \ldots, x_n]$ — Нётерово кольцо.

В самом деле, если $Z_0 \supset Z_1 \supset \ldots$, то $I(Z_0) \subset I(Z_1) \subset \ldots$. Так как $\Bbbk[x_1, \ldots, x_n]$ — Нётерово, $\exists m \colon I(Z_m) = I(Z_{m+1}) = \ldots$, и, применяя Z, мы имеем $Z_m = Z_{m+1} = \ldots$.

Теорема 46. *Пусть X — нётерово пространство, $Y \subset X$ — замкнутое. Тогда существует единственное разложение $Y = Y_1 \cup Y_2 \cup \ldots \cup Y_m$, где Y_i — замкнутые нприводимые множества и $\forall i, j \; Y_i \not\subset Y_j$.*

Доказательство. **Существование.** Пусть сущестуют замкнутые множества Y, не разлагающиеся в объединение неприводимых. В силу Нётеровости пространства, мы можем выбрать минимальное множество с таким свойством и обозначить его за Y.

Совершенно ясно, что оно не может быть неприводимым. Тогда его можно представить в виде $Y = T_1 \cup T_2$, где T_1, T_2 — замкнутые и не совпадают с Y. Так как $T_1, T_2 \subset Y$, а Y — минимальное, T_i мы уже можем представить в виде объединения неприводимых, а значит, и Y, что даёт нам противоречие.

Единственность. Пусть $Y = Y_1 \cup Y_2 \cup \ldots \cup Y_m = Y_1' \cup \ldots \cup Y_s'$. Тогда

$$Y_1 = \bigcup_i (Y_1 \cap Y_i') \implies Y_1 \subset Y_i'.$$

Проводя аналогичное рассуждение для Y_i', мы получаем, что $Y_i' \subset Y_j$ для некоторого j. Но, так как между компонентами не может быть включений, отсюда $Y_1 = Y_j$ и $Y_1 = Y_i'$. □

Определение 57. Замкуныте неприводимые множества Y_i, определённые в теореме выше, называют *неприводимыми компонентами* Y.

Пусть теперь Y — аффинное алгебраическое многообразие. Поймём, что оно раскладывается в неприводимые компоненты. Так как $\mathbb{A}^n$ нётерово, а $Y \subset \mathbb{A}^n$, по первому пункту 3 оно Нётерово, тогда есть какое-то разложение в непирводимые. Но, так как Нётерово пространство квазикомпактно (по второму пункту 3), их конечное число.

Итак, пусть $Y = Y_1 \cup \ldots \cup Y_m$, тогда $I(Y) \subset I(Y_i)$, а $I(Y_i)$ — простые идеалы (так как Y_i неприводимы). Оказывается, что идеалы $I(Y_i)$ — наименьшие простые идеалы, содержащие $I(Y)$. Действительно, доказать это совсем легко:

Пусть $T \subset Y$ — неприводимое подмножество, тогда

$$T = \bigcup_{i=1}^{m} (T \cap Y_i) \implies T \subset Y_i.$$

Пусть $Y = Z(I)$, а $Y_i = Z(\mathfrak{p}_i)$, $I \subset \mathfrak{p}_i \in \operatorname{Spec}(\Bbbk[x_1, \ldots, x_n])$.

Предположим, что $I \subset \mathfrak{p} \subsetneq \mathfrak{p}_i$ для некотрого $\mathfrak{p} \in \operatorname{Spec}(\Bbbk[x_1, \ldots, x_n])$. Тогда

$$\underbrace{Z(\mathfrak{p})}_{\text{неприводимо}} \subset Z(I) = Y = Z(\mathfrak{p}_1) \cup \ldots Z(\mathfrak{p}_n) \implies \exists j \colon Z(\mathfrak{p}) \subset Z(\mathfrak{p}_j)$$

Но тогда $\mathfrak{p} \supset \mathfrak{p}_j$, то есть

$$\mathfrak{p}_i \subset \mathfrak{p} \subset \mathfrak{p}_j \implies \underbrace{Z(\mathfrak{p}_j)}_{=Y_j} \subset \underbrace{Z(\mathfrak{p}_i)}_{=Y_i},$$

что даёт нам противоречие.

Теперь, возьмём произвольный минимальный простой идеал $\mathfrak{p} \supset I$ и покажем, что он даст нам неприводимую компоненту (т.е., что он будет совпадать с одним из $\mathfrak{p}_i$).

В самом деле, для некоторого i мы имеем $Z(\mathfrak{p}) \subset Z(\mathfrak{p}_i) \implies \mathfrak{p}_i \subset \mathfrak{p}$, откуда по минимальности $\mathfrak{p}$ мы имеем $\mathfrak{p}_i = \mathfrak{p}$.

Таким образом, доказали

Определение 58. Пусть Y — аффинное многообразие. Его *аффинным координатным кольцом* мы будем называть $A(Y) = \Bbbk[x_1, \ldots, x_n]/I(Y)$.

Домашнее задание 2. Задачи:

1. Любое подпространство Нётерова пространства Нётерово.
2. Нётерово пространство квазикомпактно[8].
3. Имеется отображение $f \colon \mathbb{A}^2 \to \mathbb{A}^2$, $f(x, y) = (x, xy)$. Вычислить образ и определить, будет ли этот образ $f(\mathbb{A}^2)$ открытым/замкнутым/плотным подмножеством в $\mathbb{A}^2$.

[8] В алгебраической геометрии это означает просто обычную компактность.

4. Пусть $f\colon \mathbb{A}^3 \to \mathbb{A}^3,\ f(x,y,z) = (x, xy, xyz)$. Вычислить образ и определить, будет ли этот образ $f(\mathbb{A}^2)$ открытым/замкнутым/плотным подмножеством в $\mathbb{A}^3$.
5. Пусть $Y \subset \mathbb{A}^3,\ Y = Z(x^2 - yz, xz - x)$. Найти неприводимые компоненты Y.
6. Вычислить неприводимые компоненты $Y = Z(y^2 - xz, z^2 - y^3)$.
7. Рассмотрим $Y = \{(t^3, t^4, t^5) \in \mathbb{A}^3_{\Bbbk}\}$.
   (a) Y — аффинное многообразие в $\mathbb{A}^3$.
   (b) Докажите, что $I(Y)$ порождается тремя элементами и найдите их.
   (c) Докажите, что $I(Y)$ не порождается двумя элементами.
8. Рассмотрим $Y = Z(y^2 - x^3)$ и аффинное координатное кольцо $A(Y) = \Bbbk[x,y]/I(Y)$. Докажите, что поле частных этого кольца изоморфно $\Bbbk[k](t)$. Выясните, является ли кольцо $A(Y)$ целозамкнутым.

2.3 Размерность аффинного многообразия

Пусть X — топологическое пространство. Тогда его размерность $\dim X$ определяется аналогично размерности Крулля для кольца в коммутативной алгебре. А именно, рассматривается максимальная длина убывающей цепочки замкнутых неприводимых множеств:

$$X_0 \supsetneq X_1 \supsetneq X_2 \ldots \supsetneq X_n.$$

Предложение 21. *Пусть Y — многообразие, а $A(Y)$ — его координатное кольцо. Тогда*

$$\dim Y = \dim A(Y).$$

Доказательство. Замкнутые неприводимые помножества Y соотвествуют простым идеалам кольца $\Bbbk[x_1, \ldots, x_n]$, содержащим $I(Y)$, а они, в свою очередь, соответствуют простым идеалом координатного кольца $A(Y) = \Bbbk[x_1, \ldots, x_n]/I(Y)$. Значит, $\dim Y$ равна наибольшей из длин цепочек отличных друг от друга простых идеалов в $A(Y)$, то есть размерности Крулля $A(Y)$. □

Это предложение показывает, что результаты из теории размерности Нётеровых колец весьма-весьма полезны в алгебраической геометрии.

Теперь напомним такой факт из коммутативной алгебры:

Теорема 47 (Лемма нётер о нормализации)**.** *Пусть B — конечно-порожденная $\Bbbk$-алгебра. Тогда B — конечное расширение кольца многочленов $\Bbbk[x_1, \ldots, x_n]$ для некоторого n.*

Так как при целом расширении размерность не изменяется, $\dim B = \dim(\Bbbk[x_1, \ldots, x_n]) = n$.

Факт о том, что $\dim(\Bbbk[x_1, \ldots, x_n]) = n$ вообще говоря весьма содержателен, напомним его. Он следует из такой теоремы из коммутативной алгебры:

Теорема 48. *Пусть B — конечнопорожденная $\Bbbk$-алгебра. Если B — область целостности, то* $\dim(B) = \operatorname{trdeg}(\Bbbk(B))$.

Пример 23. Отсюда мы сразу получаем, что $\dim \mathbb{A}^n = \dim \Bbbk[x_1, \ldots, x_n] = n$.

Определение 59. *Аффинная алгебра* — это координатное кольцо некотрого аффинного многообразия.

Замечание. Как мы увидим немного позже, эквивалентно можно говорить, что аффинная алгебра — это конечнопорожденная редуцированная алгебра.

Теорема 49. *Пусть B — целостная аффинная алгебра над $\Bbbk$ (или, что эквивалентно, конечно-порожденная целостная $\Bbbk$-алгебра), а $\mathfrak{p} \in \operatorname{Spec} B$. Тогда*

$$\operatorname{ht} \mathfrak{p} + \dim B/\mathfrak{p} = \dim B.$$

Доказательство. Будем вести индукцию по $\dim B$. База ($\dim B = 0$) очевидна.

I. Пусть $B = \Bbbk[x_1, \ldots, x_n],\ \dim B = n$. Возьмём $\mathfrak{p} \in \operatorname{Spec} B$, $\operatorname{ht} \mathfrak{p} = m$, то есть

$$0 \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}_m = \mathfrak{p}.$$

Тогда $\operatorname{ht} \mathfrak{p}_1 = 1$, но тогда идеал $\mathfrak{p}_1$ — главный, т.е. $\mathfrak{p}_1 = (q)$. В самом деле, иначе мы можем взять образующую, разложить её на неприводимые множители (кольцо многочленов факториально) и взять неприводимымй сомножитель, попадающий в $\mathfrak{p}_1$. Так мы получим простой идеал, меньший $\mathfrak{p}_1$ и придём к противоречию.

Рассмотрим тогда $\mathfrak{p}/(q) \trianglelefteq B/(q)$, $\mathfrak{p}/(q) \in \operatorname{Spec} B/(q)$. Так как $\dim A/(q) = \dim B - 1$, мы можем применить индукционное предположение:

$$\operatorname{ht} \mathfrak{p}/(q) + \dim B/\mathfrak{p} = \dim B - 1.$$

Докажем, что $\operatorname{ht} \mathfrak{p}/(q) = \operatorname{ht} \mathfrak{p} - 1$. Очевидно, что $\operatorname{ht} \mathfrak{p}/(q) \geq \operatorname{ht} \mathfrak{p} - 1$. С другой стороны, если $\varphi\colon B \to B/(q)$, то если есть цепочка

$$0 \subset \mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_s = \mathfrak{p}/(q),$$

то есть и цепочка для $\mathfrak{p}$:

$$0 \subset (\mathfrak{q}) \subset \varphi^{-1}(0) \subset \varphi^{-1}(\mathfrak{q}_1) \subset \ldots \subset \varphi^{-1}(\mathfrak{q}_s) = \mathfrak{p}.$$

II. Пусть B — произвольная конечнопорожденная целостная $\Bbbk$-алгебра. Вспомним теорему о спуске:

Теорема 50 (О спуске)**.** *Пусть $A \subset B$ — целостные и B/A — цело. Пусть $\mathfrak{q}_m \in \operatorname{Spec} B,\ \mathfrak{p}_m \in \operatorname{Spec} A$ — простые. Тогда для любой цепочки простых идеалов*

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_m \subset A$$

существует цепочка простых идеалов

$$\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \ldots \subset \mathfrak{q}_m \subset B\colon \mathfrak{q}_i \cap A = \mathfrak{p}_i.$$

Так вот, по лемме Нётер о нормализации B — целое расширение $A = \Bbbk[x_1, \ldots, x_n]$, $\dim B = \dim A$. Тогда по теореме о спуске для $\mathfrak{q} \in \operatorname{Spec} B$ мы имеем $\operatorname{ht} \mathfrak{q} \geq \operatorname{ht} \mathfrak{q} \cap A$. Кроме того, расширение

$$A/\mathfrak{q} \cap A \hookrightarrow B/\mathfrak{q}$$

тоже целое, откуда $\dim A/\mathfrak{q} \cap A = \dim B/\mathfrak{q}$. Тогда мы имеем

$$\dim B/\mathfrak{q} + \operatorname{ht} \mathfrak{q} \geq \operatorname{ht}(\mathfrak{q} \cap A) + \dim(A/\mathfrak{q} \cap A)$$

По пункту I, правая часть равна $\dim A = \dim B$, то есть мы показали, что

$$\dim B/\mathfrak{q} + \operatorname{ht} \mathfrak{q} \geq \dim B.$$

Но, неравенство в другую сторону очевидно.

□

Следствие 21. *Пусть B — целостная конечно-порожденная алгебра, $f \in B,\ f \neq 0$ и f необратим. Пусть $\mathfrak{p}$ — минимальный простой идеал, содержащий f. Тогда*

$$\dim B/\mathfrak{p} = \dim B - 1.$$

Доказательство. По теореме 49 мы имеем

$$\operatorname{ht} \mathfrak{p} + \dim B/\mathfrak{p} = \dim B.$$

Но, по теореме Крулля о главных идеалах (hauptidealsatz), $\operatorname{ht} \mathfrak{p} = 1$, откуда мы имеем нужное. □

Переформулируем это на алгебро-геометрический язык:

Следствие 22. *Пересечение неприводимого многообразия X с гиперповерхностью или пусто, или имеет размерность хотя бы* $\dim X \geq 1$.

Отсюда получаем вот такое следствие:

Предложение 22. *Все неприводимые компоненты $Z(I(X) + (f_1, \ldots, f_m))$ имеют размерность хотя бы* $\dim X - m$.

Следствие 23. *Пусть $f_1, \ldots, f_m \in \Bbbk[x_1, \ldots, x_n]$, $m < n$ и $f_1(0) = \ldots = f_m(0) = 0$. Тогда система*

$$\begin{cases} f_1 = 0 \\ \vdots \\ f_m = 0 \end{cases}$$

имеет ненулевое решение.

Вот про это следствие еще надо всё понять.

2.4 Регулярные функции

Определение 60. Будем говорить, что X — *квазиаффинное многообразие*, если X — открытое подмножество аффинного многообразия.

Определение 61. Пусть $X \subset \mathbb{A}^n_\Bbbk$ — квазиаффинное. Будем говорить, что отображение $f\colon X \to \Bbbk$ — регулярное в точке p, если существует окрестность $U \ni p$ и многочлены $g, h \in A = \Bbbk[x_1, \ldots, x_n]$ такие, что

- h не имеет нулей в U,
- $f|_U = g/h$.

Функция f называется *регулярной* на X, если она регулярна в каждой точке X.

Регулярные функции на X образуют кольцо, которое мы будем обозначать $\mathcal{O}(X)$.

Замечание. Например, все многочлены — регулярные функции на $\mathbb{A}^n$.

Теорема 51. *Пусть X — аффинное многообразие. Тогда*

$$\mathcal{O}(X) \cong A(X) = \Bbbk[x_1, \ldots, x_n]/I(X).$$

Доказательство. Сначала отметим, что каждый многочлен очевидно определяет регулярную функцию на $\mathbb{A}^n$, а значит и на X. Так мы строим гомоморфизм

$$\alpha\colon \Bbbk[x_1, \ldots, x_n] \to \mathcal{O}(X), \quad f \mapsto f.$$

Но, его ядро — это в точности $I(X)$:

$$\operatorname{Ker}\alpha = \{f \in \Bbbk[x_1, \ldots, x_n]\colon f|_X = 0\} = I(X).$$

Значит, у нас есть инъективный гомоморфизм $A(X) \hookrightarrow \mathcal{O}(X)$. Покажем, что он сюръективен.

Рассмотрим $f \in \mathcal{O}(X)$. По определению, у любой точки $x \in X$ существует окрестность U_x и многочлены p_x, q_x такие, что $q_x f = p_x$ в U_x, причём q_x не обращается в 0 на U_x. Так как $X \setminus U_x$ замкнуто, $X \setminus U_x = Z(\mathfrak{a})$ для некоторого идеала $\mathfrak{a}$ и легко видеть, что

$$Z(\mathfrak{a}) \subset X = Z(I(X)) \implies I(X) \subset \mathfrak{a}.$$

Тогда, если мы возьмём $s \in \mathfrak{a} \setminus I(X)$, мы получим, что

$$s \cdot q_x \cdot f = s \cdot p_x \quad \text{на всём } X, \text{ так как}$$

- $s \in Z(\mathfrak{a}) = X \setminus U_x$, что значит, что $s|_{X\setminus U_x} = 0$ и и на $X \setminus U_x$ это равенство превращается в $0 = 0$.
- А на U_x это равенство получается домножением $q_x f = p_x$ на s.

Причём, выберем s так, чтоб $s(x) \neq 0$. Мы можем так сделать, так как если нет, то

$$\begin{cases} \forall s \in \mathfrak{a} \setminus I(X) \quad s(x) = 0 \\ \forall s \in I(X) \quad s(x) = 0 \end{cases} \implies \forall s \in \mathfrak{a} \quad s(x) = 0,$$

но тогда $x \in Z(\mathfrak{a}) = X \setminus U_x$ (что абсурдно).

Итак, выбрав такой s мы построили для любой точки x многочлены p'_x и q'_x такие, что

$$\forall y \in X \quad q'_x(y) f(y) = p'_x(y) \text{ и } q'_x(x) \neq 0.$$

Теперь рассмотрим идеал $\sum_{x\in X}(q'_x) + I(X)$ в кольце $\Bbbk[x_1, \ldots, x_n]$ и покажем, что он совпадает со всем кольцом. Предположим противное, тогда он содержится в некотором максимальном идеале $\mathfrak{m} \in \operatorname{Spec}(\Bbbk[x_1, \ldots, x_n])$. Но тогда

$$Z\left(\sum_{x\in X} q'_x + I(X)\right) \supset Z(\mathfrak{m}) = \mathrm{pt} \in \mathbb{A}^n \implies \forall x \in X \; q'_x(\mathrm{pt}) = 0, \quad \forall h \in I(X) \; h(\mathrm{pt}) = 0.$$

Это даёт провтиворечие, так как

- Если $\mathrm{pt} \notin X$, то не может быть такого, что $\forall h \in I(X) \; h(\mathrm{pt}) = 0$.
- Если же $\mathrm{pt} \in X$, то по построению $q'_{\mathrm{pt}}(\mathrm{pt}) \neq 0$.

Итак, мы показали, что

$$\sum_{x\in X}(q'_x) + I(X) = (1) \implies \sum_{x\in X}(\overline{q'_x}) = (\overline{1}) \text{ в } A(X),$$

откуда сушествуют $\overline{\ell_{x_i}} \in A(X)$ такие, что

$$\sum_{i=1}^{N} \overline{\ell_{x_i}} \cdot \overline{q'_{x_i}} = \overline{1} \quad \text{на } X.$$

Но, ранее мы показали, что $q'_x \overline{f} = p'_x$ на X, то, домножая это равенство на f, мы получаем, что

$$\overline{f} = \sum_{i=1}^{N} \overline{p'_{x_i}} \cdot \overline{\ell_{x_i}} \in A(X).$$

Таким образом, мы построили для каждой регулярной функции прообраз в $A(X)$. □

Предложение 23. *Регулярная функция $f\colon X \to \Bbbk$ непрерывна, если отождествить $\Bbbk$ с $\mathbb{A}^1$ с топологией Зарисского.*

Доказательство. Докажем сначала такую лемму из общей топологии:

Лемма 34. Пусть X — топологическое пространство, $T \subset X$, а U_i — открытое покрытие. Тогда T замкнуто в X тогда и только тогда, когда $\forall i \; T \cap U_i$ замкнуто в U_i.

Доказательство. В самом деле,

$$V = X \setminus T = \bigcup_i (U_i \setminus T) = \bigcup_i \underbrace{(U_i \setminus (T \cap U_i))}_{\text{открытое}}.$$

□

Достаточно показать, что прообраз замкнутого множества замкнут. Как мы видели, замкнутые множества в $\mathbb{A}^1$ — конечные наборы точек, поэтому достаточно показать, что

$$\forall a \in \Bbbk \quad f^{-1}(a) = \{P \in X \mid f(P) = a\} - \text{замкнуто.}$$

Как мы видели в лемме, это достаточно проверять локально. Пусть U — открытое множество, на которо f можно представить в виде g/h, где $g, h \in \Bbbk[x_1, \ldots, x_n]$ и h не имеет нулей в U. Тогда

$$f^{-1}(a) \cap U = \{P \in U \mid g(P)/h(P) = a\}, \quad \text{но } g(P)/h(P) = a \iff (g - ah)(P) = 0,$$

откуда $f^{-a}(a) \cap U = Z(g - ah) \cap U$ — замкнуто в U. □

2.5 Морфизмы алгебраических многообразий

Определение 62. Пусть X, Y — квазиаффинные многообразия, $\varphi\colon X \to Y$ — *морфизм*, если

1. φ непрерывно.
2. Для каждого открытого $V \subset Y$ и каждой регулярной функции $f\colon V \to \Bbbk$ её пуллбек $\varphi^*(f) = f \circ \varphi\colon \varphi^{-1}(V) \to \Bbbk$ — регулярная функция.

Замечание. В частности, теперь у нас определено понятие изоморфизма многообразий. Отметим, что изоморфизм обязательно является биективным и непрерывным в обе стороны морфизмом, однако биективный и бинепрерывный морфизм может и не быть изоморфизмом.

Предложение 24. *Квазиаффинные многообразия (и морфизмы, определенные как в 62) образуют категорию, которую мы будем обозначать* $\mathsf{qAff}_{\Bbbk}$.

Предложение 25. *Пусть X — квазиаффинное многообразие, $Y \subset \mathbb{A}^n_{\Bbbk}$ — аффинное многообразие. Тогда $\psi\colon X \to Y$ является морфизмом в точности тогда и только тогда, когда функции*

$$\psi^*(x_i)\colon X \xrightarrow{\psi} Y \xrightarrow{x_i} \Bbbk$$

являются регулярными на X.

Доказательство. Если ψ — морфизм, то эти функции регулярны просто по определению (морфизма). Докажем утверждение в обратную сторону.

Покажем непрерывность. Возьмём замкнутое $T \subset Y$ и проверим, что $\psi^{-1}(T)$ замкнуто. Достаточно проверить это локально, то есть в окрестности любой точки. Возьмём произвольную точку $x \in X$ и докажем, что существует такая окрестность $U_x \ni x$, что $U_x \cap \psi^{-1}(T)$ замкнуто в U_x.

Так как функции $\psi^*(x_i)\colon X \to \Bbbk$ регулярны, в некоторой окрестности[9] x мы можем представить отображение ψ в виде

$$(x_1, \ldots, x_m) \mapsto \left(\frac{f_1(x_1, \ldots, x_m)}{g_1(x_1, \ldots, x_m)}, \ldots, \frac{f_n(x_1, \ldots, x_m)}{g_n(x_1, \ldots, x_m)}\right)$$

Тогда, если $T = \{y \in Y \mid F_1(y) = \ldots = F_k(y) = 0\}$, то

$$\psi^{-1}(T) \cap U_x = \left\{(x_1, \ldots, x_m) \middle| F_1\left(\frac{f_1}{g_1}(x_1, \ldots, x_m), \ldots, \frac{f_n}{g_n}(x_1, \ldots, x_m)\right) = \ldots = 0\right\},$$

откуда $\psi^{-1}(T) \cap U_x$ замкнуто в U_x.

Теперь надо проверить второе условие. Его также можно проверять локально. Возьмём открытое $U \subset Y$ и рассмотрим на нём регулярную функцию f. Покажем, что $f \circ \psi$ регулярна на $\psi^{-1}(U)$. Мы можем покрыть U окрестнсотями, на которымх f представляется, как отношение многочленов: пусть $U = \bigcup U_i$ и

$$f|_{U_i} = \frac{g_i}{h_i}.$$

Тогда достаточно доказать, что $\psi^*(f|_{U_i})$ регулярны на $\psi^{-1}(U_i)$, а для этого достаточно доказать, что $\psi^*(g_i)$ и $\psi^*(h_i)$ регуярны. Но, это очевидно, так как по условию $\psi^*(x_i)$ регулярны, а g_i и h_i — многочлены от x_i. □

Замечание. Тут условие аффинности Y не существенно (т.е. это верно и для квазиаффинного).

[9] Достаточно взять окрестность из определения для каждой из координат и пересечь их.

2.6 Антиэкивалентность $\mathsf{qAff}^{op} \cong \Bbbk\text{-}\mathsf{Alg}$

Предложение 26. *Пусть X, Y — многообразия, причем Y — аффинное. Имеется естественное биективное отображение (изоморфизм бифункторов)*

$$\mathrm{Hom}_{\mathsf{qAff}}(X, Y) \xrightarrow{\sim} \mathrm{Hom}_{\Bbbk\text{-}\mathsf{Alg}}(A(Y), \mathcal{O}_X).$$

Естественность тут понимается в естественном смысле: а именно, если у нас есть морфизм $X_1 \to X_2$, то мы получим коммутативную диаграмму:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{qAff}}(X_2, Y) & \xleftrightarrow{\sim} & \mathrm{Hom}_{\Bbbk\text{-}\mathsf{Alg}}(A(Y), \mathcal{O}(X_2)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathsf{qAff}}(X_1, Y) & \xleftrightarrow{\sim} & \mathrm{Hom}_{\Bbbk\text{-}\mathsf{Alg}}(A(Y), \mathcal{O}(X_1)) \end{array}$$

И, если же у нас есть морфизм $Y_1 \to Y_2$, то мы получим коммутативную диаграмму:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathsf{qAff}}(X, Y_1) & \xleftrightarrow{\sim} & \mathrm{Hom}_{\Bbbk\text{-}\mathsf{Alg}}(A(Y_1), \mathcal{O}(X)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathsf{qAff}}(X, Y_2) & \xleftrightarrow{\sim} & \mathrm{Hom}_{\Bbbk\text{-}\mathsf{Alg}}(A(Y_2), \mathcal{O}(X)) \end{array}$$

Доказательство. Пусть задан морфизм $\varphi\colon X \to Y$, тогда он переводит регулярные функции на Y в регулярные функции на X (при помощи пуллбека). Значит, он индуцирует отображение $\varphi^*\colon \mathcal{O}(Y) \to \mathcal{O}(X)$:

$$f \in \mathcal{O}(Y), \quad f \mapsto \varphi^*(f) \in \mathcal{O}(X).$$

Совершенно ясно, что это отображение является гомоморфизмом $\Bbbk$-алгебр. По теореме 51, $\mathcal{O}(Y) \cong A(Y)$, так что мы получаем гомомоифизм $A(Y) \to \mathcal{O}(X)$.

Теперь построим обратное отображение. Пусть задан гомоммрфизм $\Bbbk$-алгебр $h\colon A(Y) \to \mathcal{O}(X)$. Y — аффинное, так что $A(Y) = \Bbbk[x_1, \dots, x_n]/I(Y)$. Рассмотрим $\xi_i = h(\overline{x_i}) \in \mathcal{O}(X)$, Эти функции определены на всём X, так что мы можем определить отображение

$$\psi\colon X \to \mathbb{A}^n, \quad \psi(P) = (\xi_1(P), \dots, \xi_n(P)).$$

Покажем, что на самом деле ψ действует в Y. Так как $Y = Z(I(Y))$, достаточно показать, что $\forall f \in I(Y), \forall P \in X\ f(\psi(P)) = 0$. Так как f — многочлен, а h — гомоморфизм $\Bbbk$-алгебр,

$$f(\psi(P)) = f((\xi_1(P), \dots, \xi_n(P))) = h(f(\overline{x_1}, \dots, \overline{x_n}))(P) = 0,$$

так как $f \in I(Y)$. Так по гомоморфизму $\Bbbk$-алгебр $h\colon A(Y) \to \mathcal{O}(X)$ мы построили отображение $\psi\colon X \to Y$. То, что ψ — морфизм, напрямую вытекает из предложения 25. □

Заметим, что если оба многообразия аффинные, то мы получаем соответствие (естественный изоморфизм)

$$\mathrm{Hom}_{\mathsf{qAff}}(X, Y) \xrightarrow{\sim} \mathrm{Hom}_{\Bbbk\text{-}\mathsf{Alg}}(A(Y), A(X)).$$

То есть, мы получаем функтор $\mathsf{qAff}_{\Bbbk}^{op} \to \Bbbk\text{-}\mathsf{Alg}$ (где алгебры конечнопорожденные и редуцированные[10]):

$$A\colon \mathsf{qAff}_{\Bbbk}^{op} \to \Bbbk\text{-}\mathsf{Alg}, \quad X \mapsto A(X).$$

Кроме того, мы видели, что есть и обратный функтор: если $A \in \Bbbk\text{-}\mathsf{Alg}$, то мы можем рассмотреть аффинное многообразие X' такое, что $A(X') \cong A$ и сопоставить $A \to X'$. Этот функтор задан корректно, так как если взять другое многообразие X такое, что $A(X) \cong A(X')$, то изоморфизм алгебр будет индуцировать и изоморфизм многообразий $X \cong X'$ (так как функтор переводит изоморфизмы в изоморфизмы).

Таким образом, мы доказали такую теоремы:

[10] Допуская вольность речи, мы обозначаем эти две категории одинаково и отличаем их в зависимости от контекста.

Теорема 52. *Категория квазиаффинных многообразий* qAff *антиэквивалентна категории конечнопорожденных редуцированных $\Bbbk$-алгебр.*

Переводя это на существенно менее изысканный язык, мы получаем такое следствие

Следствие 24. *Аффинные многообразия X и Y изоморфны тогда и только тогда, когда их аффинные координатные кольца $A(X)$ и $A(Y)$ изоморфны как $\Bbbk$-алгебры.*

2.7 Рациональные функции

Определение 63. Пусть X — неприводимое аффинное многообразие, U, V — непустые открытые подмножества, а f и g — регулярные функции на U и V соотвественно. Тогда будем говорить, что $(U, f) \sim (V, g)$ если $f = g$ на $U \cap V$.

Класс эквивалентности по этому отношению мы будем называть *рациональной функцией.*

Областью определения рациональной функции называется объединение всех U таких, что функция эквивалентна (U, f) для некоторой f.

Замечание. Множество всех рациональных функций на X образует поле, которое мы будет обозначать через $\Bbbk(X)$.

Проверим, что это в самом деле поле. Так как X неприводимо, любые два непустых открытых подмножества X имеют непустое пересечение (по 18) и мы можем определить сложение и умножение, превратив $\Bbbk(X)$ в кольцо. Кроме того, если $(U, f) \in K(X)$ и $f \neq 0$, то мы можем ограничить f на открытое множество $V = U \setminus (U \cap Z(f))$, на котором f не имеет нулей и тогда $1/f$ регулярна на V и пара $(V, 1/f)$ будет обратным элементом к (U, f).

Отметим, что для неприводимого аффинного многообразия X определение поля рациональных функций $\Bbbk(X)$ можно дать несколько иначе от определения 63.

Предположем, что X неприводимо, тогда мы можем рассмотреть поле частных координатного кольца $A(X)$. Кроме того, рассматривая очевидное отображение

$$A(X) \to \Bbbk(X).$$

мы получаем и вложение поле $\mathrm{Frac}(A(X)) \hookrightarrow \Bbbk(X)$. С другой стороны, нетрудно видеть, что это изоморфизм.

2.8 Главные аффинные окрестности

Определение 64. *Главным открытыми множествами (или, аффинными окрестнстями) в $\mathbb{A}^n$* назвают множества вида

$$D(f) \stackrel{\text{def}}{=} \mathbb{A}^n \setminus Z(f),$$

где f — некоторый многочлен из $\Bbbk[x_1, \ldots, x_n]$.

Пусть X — аффинное многообразие, $\overline{f} \in A(X) = \Bbbk[x_1, \ldots, x_n]/I(X)$, тогда определим

$$D(\overline{f}) \stackrel{\text{def}}{=} D(f) \cap X = X \setminus Z\big(\overline{f}\big).$$

Замечание. Ясно, что если $f = 1$, то $D(f) = \mathbb{A}^n$, откуда $D(\overline{f}) = X$.

Для краткости обозначим $A = A(X)$ и рассмотрим главную локализацию

$$A_{\overline{f}} = S^{-1}A, \text{ где } S = \{\overline{f}^n \mid n \in \mathbb{N}\}.$$

Замечание. Отметим, что возможен случай, когда $A_{\overline{f}} = 0$, но тогда $\exists k\colon \overline{f}^k = 0$, а так как $I(X)$ — радикальный идеал, это равносильно тому, что $\overline{f} = 0$, что равносильно тому, что $f \in I(X)$, т.е.

$$D(\overline{f}) = X \setminus Z(\overline{f}) = \varnothing.$$

В случае, когда $D(\overline{f}) \neq \varnothing$, мы полуачем гомоморфизм колец

$$A_{\overline{f}} \to \mathcal{O}(D(\overline{f})), \quad \frac{\overline{a}}{\overline{f}^k} \mapsto \text{ функция } \frac{\overline{a}}{\overline{f}^k}$$

- Этот гомоморфизм инъективен:

$$\frac{\overline{a}}{\overline{f}^k}\Big|_{D(\overline{f})} = 0 \implies \overline{a}|_{D(\overline{f})} = 0 \implies \overline{a} \cdot \overline{f}|_X = 0 \implies af \in I(X) \implies \overline{a}\overline{f} = 0 \in A(X),$$

  откуда $\overline{a}/\overline{f}^k = 0$ в локализации $A(X)_{\overline{f}}$.
- Кроме того, он сюръективен. Пусть $r \in \mathcal{O}\big(D(\overline{f})\big)$, тогда

$$x \in D\big(\overline{f}\big) \quad \exists \text{ окрестность } U_x \ni x,\ \overline{g}_x, \overline{h}_x \in A(X) \colon r\overline{h}_x = \overline{g}_x \text{ на } U_x$$

  и h_x не имеет нулей в U_x.
  Выбирая многочлен $s_x \in A(X)$, не равный нулю в точке x, но обращающийся в ноль на дополнении, мы можем полагать, что наше равенство выполнено на всём X (см. доказательство теоремы 51). Не умаляя общности, будем считать так изначально. Заметим, что

$$Z\left(\sum_{x \in D(\overline{f})} (h_x) + I(X)\right) \subset Z(f),$$

  так как если $y \in \sum_{x \in D(\overline{f})}(h_x) + I(X)$, то $y \in X \setminus D(\overline{f}) = X \cap Z(f)$. Тогда

$$\sqrt{(f)} \subset \sqrt{\sum_{x \in D(\overline{f})} (h_x) + I(X)} \implies f^m \in \sum_{x \in D(\overline{f})} (h_x) + I(X) \implies \overline{f}^m \in \sum_{x \in D(\overline{f})} (h_x)$$

  Значит, мы можем представить $\overline{f}^m$ в виде

$$\overline{f}^m = \sum_{i=1}^{k} \overline{h_{x_i}\ell_i}, \quad x_i \in D\big(\overline{f}\big).$$

  Но тогда, домножая это равенство на r мы получаем

$$\overline{f}^m r = \sum_{i=1}^{k} \overline{g_{x_i}}\,\overline{\ell_{x_i}} \implies r = \frac{\overline{a}}{\overline{f^m}} \in A_{\overline{f}}.$$

Таким образом, мы доказали такое предложение

Предложение 27. $A(X)_{\overline{f}} \cong \mathcal{O}\big(D\big(\overline{f}\big)\big)$.

Полезно также рассмотреть альтернативное доказательство этого факта.

Альтернативное доказательство предложения 27. Рассмотрим отображение

$$A_{\overline{f}} \xrightarrow{\sim} A[t]/\big(\overline{f}t - 1\big), \quad \frac{a}{\overline{f}^k} \mapsto \overline{a}t^k.$$

Легко видеть, что это изоморфизм. Кроме того,

$$A = \Bbbk[x_1, \ldots, x_n]/I(X) \implies A[t]/\big(\overline{f}t - 1\big) \cong \Bbbk[x_1, \ldots, x_n, t]/\big(I(x), \overline{f}t - 1\big),$$

откуда видно, что $A_{\overline{f}}$ — это координатное кольцо многообразия

$$Y = \{(x_1, \ldots, x_n, t) \in \mathbb{A}^{n+1}_{\Bbbk} \mid (x_1, \ldots, x_n) \in X, \quad f(x_1, \ldots, x_n)t - 1 = 0\}.$$

Рассмотрим коммутативную диаграмму:

$$\begin{array}{ccc} A(X)_{\overline{f}} & \xrightarrow{\sim} & A(X)[t]/(\overline{f}t-1) \\ \vdots & & \downarrow \sim \\ \mathcal{O}(D(\overline{f})) & \xrightarrow{\sim} & \mathcal{O}(Y) \end{array}$$

Нижняя горизонтальная стрелка получается из того, что $Y \xrightarrow{\sim} D\big(\overline{f}\big)$ посредством (взаимнообратных) отображений

$$(x_1, \ldots, x_n, t) \mapsto (x_1, \ldots, x_n), \quad (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, 1/f(x_1, \ldots, x_n))$$

Так как горизонтальные и правая вертикальная стрелка — изоморфизмы, левая вертикальная стрелка — тоже изоморфизм.

□

2.9 Эквивалентные определения размерности неприводимого аффинного многообразия

Предложение 28. *Пусть X — неприводимое квазиаффиное многообразие, $U \subset X$ — открытое подмножество. Тогда* $\dim U = \dim X$.

Доказательство. **I.** Пусть X — аффинное. Тогда так как U открытое,

$$U = X \setminus Z(\overline{f_1}, \ldots, \overline{f_n}) \supset X \setminus Z(\overline{f_j}) = D\big(\overline{f_j}\big) \implies D\big(\overline{f_j}\big) \subset U \subset X \implies$$

$$\implies \dim D\big(\overline{f_j}\big) \leq \dim U \leq \dim X.$$

Но, как мы знаем из предложения 27 и теоремы 48, $\dim D\big(\overline{f_j}\big) = \dim A(X)_{\overline{f_j}} = \text{tr. deg Frac } A(X)_{\overline{f_j}}$. Теперь заметим, что

$$\text{tr. deg Frac } A(X)_{\overline{f_j}} = \text{tr. deg Frac } A(X) = \dim X,$$

откуда мы заключаем, что $\dim U = \dim X$.

II. Пусть X квазиаффинное. Тогда $U \subset X \subset \overline{X}$ и $\overline{X}$ — аффинное. Тогда, так как U — открытое подмножество $\overline{X}$, по пункту I мы имеем

$$\dim U = \dim \overline{X}.$$

С другой стороны, $\dim U \leq \dim X \leq \dim \overline{X}$, откуда мы получили нужное. □

Определение 65. Пусть X — квазиаффинное многообразие. Тогда $\dim X$ — наибольшая из размерностей его неприводимых компонент.

2.10 Прямое произведение многообразий и его первые приложения

Пусть $X \subset \mathbb{A}^m,\ Y \subset \mathbb{A}^n$ — аффинные многообразия. Пусть $X = Z(f_1, \ldots, f_k),\ Y = Z(g_1, \ldots, g_\ell)$, то

$$X \times Y = \{(x_1, \ldots, x_m, y_1, \ldots, y_n) | f_i(x_1, \ldots, x_m) = 0,\ g_j(y_1, \ldots, y_n) = 0\ \forall i, j\}.$$

То есть, прямое произведение естественно снабжается структурой аффинного многообразия в $\mathbb{A}^{m \times n}$. Позже мы докажем, что это произведение в категорном смысле.

Также видно, что если X и Y — квазиаффинные, то их прямое произведение тоже квазиаффинное.

Предложение 29. *Пусть $X \subset \mathbb{A}^m,\ Y \subset \mathbb{A}^n$ — неприводимые аффинные многообразия, то $X \times Y$ — неприводимое аффинное многообразие в $\mathbb{A}^m \times \mathbb{A}^n$.*

Доказательство. Предположим противное, то есть, что

$$X \times Y = Z_1 \cup Z_2, \quad Z_i \neq X \times Y.$$

Ясно, что $\forall x \in X \quad x \times Y \cong Y$ — неприводимое, тогда $x \times Y \subset Z_1$ или $x \times Y \subset Z_2$. Но тогда

$$X = X_1 \cup X_2, \quad X_j = \{x \mid x \times Y \subset Z_j\}.$$

Покажем, что множества X_1 и X_2 замкнутые. Для этого достаточно заметить, что

$$X_1 = \bigcap_{y \in X} X_y, \text{ где } X_y = \{x \in X \mid (x, y) \in Z_1\},$$

а X_y — замкнуты, так как если $Z_1 = Z(f_1(x, y), \ldots, f_k(x, y))$, то

$$X_{\widetilde{y}} = Z(f_1(x, \widetilde{y}), \ldots, f_k(x, \widetilde{y})).$$

Тогда мы приходим к противоречию, так как из неприводимости X следует, что $X \subset X_1$ или $X \subset X_2$, откуда $X \times Y = Z_1$ или $X \times Y = Z_2$ (что противоречит нашему предположению).

□

Предложение 30. *Пусть X, Y — неприводимые аффинные многообразия. Тогда* $\dim(X \times Y) = \dim X + \dim Y$.

Доказательство. Пусть $\dim X = r,\ \dim Y = s$. Поле функций $\Bbbk(X)$ порождается ровно r алгебраически независимыми координатными функциями $u_1, \ldots, u_r$. Аналогично, $\Bbbk(Y)$ порождается координатныими функциями $v_1, \ldots, v_s$ и они алгебраически независимы. Тогда совершенно ясно, что

$$\dim(X \times Y) = \operatorname{trdeg}(\Bbbk(X \times Y)) \leq r + s.$$

Остаётся показать, что система $(u_1, \ldots, u_r, v_1, \ldots, v_s)$ будет алгебраически независимой в $\Bbbk(X \times Y)$. Предположим, что

$$\sum f_{i_1 i_2 \ldots i_r}(v_1, \ldots, v_s) u_1^{i_1} \cdot \ldots \cdot u_r^{i_r} = 0.$$

Подставляя $a_i \in \Bbbk$, мы получаем полиномиальное соотношение на u_i :

$$\sum f_{i_1 i_2 \ldots i_r}(a_1, \ldots, a_s) u_1^{i_1} \cdot \ldots \cdot u_r^{i_r} = 0,$$

а так как u_i алгебраически независимы, отсюда следует, что $f_{i_1 \ldots i_r}(a_1, \ldots, a_s) = 0$. По произвольности набора $a_1, \ldots, a_s$, мы получаем, что $f_{i_1 i_2 \ldots i_r}(v_1, \ldots v_s) = 0$, но так как v_i алгебраически независимы, отсюда следует, что $f_{i_1 \ldots i_r} = 0$, что и требовалось. □

Замечание. Здесь мы по существу использовали, что для аффинных $\Bbbk(X) = \operatorname{Frac} A(X)$.

Обсудим, что происходит в случае приводимых многообразий. Если

$$X = \bigcup_i X_i, Y = \bigcup_j Y_j \quad X_i, Y_j \text{ — неприводимые},$$

то $\dim X = \max \dim X_i$, а $\dim Y = \max \dim Y_j$. Тогда у нас есть разложение $X \times Y$ в неприводимые:

$$X \times Y = \bigcup X_i \times Y_j$$

Таким образом, мы получили, что

Предложение 31. *Пусть X, Y — многообразия, тогда* $\dim(X \times Y) = \dim X + \dim Y$.

Теорема 53. *Пусть $Y, Z \subset \mathbb{A}^n_{\Bbbk}$ — неприводимые аффинные многообразия,* $\dim Y = r,\ \dim Z = s$. *Тогда любая компонента $Y \cap Z$ имеет размерность $\geq r + s - n$.*

Доказательство. Рассмотрим диагональное вложение

$$\Delta\colon \mathbb{A}^n \to \mathbb{A}^n \times \mathbb{A}^n = \mathbb{A}^{2n},\ x \mapsto (x, x).$$

Образ $\Delta(\mathbb{A}^n)$ замкнут в $\mathbb{A}^{2n}$, так как он задаётся вот такой системой уравнений:

$$\begin{cases} y_1 = y_{n+1} \\ y_2 = y_{n+2} \\ \vdots \\ y_n = y_{2n} \end{cases} \tag{2.1}$$

Заметим, что имеет место изоморфизм

$$Y \cap Z \xrightarrow{\sim} \Delta(\mathbb{A}^n) \cap (Y \times Z).$$

Так как при изоморфизме неприводимые компоненты переходят в неприводимые компоненты, размерности неприводимых компонент левой и правой частей равны. Заметим, что $\Delta(\mathbb{A}^n)$ — пересечение n гиперповерхностей (как видно из 2.1. Тоогда, пользуясь теоремой 22 (и тем фактом, что $\dim Y \times Z = r + s$), мы получаем нужное.

□

Заметим, что в процессе доказательства мы установили, что $D(\overline{f})$ изоморфно аффинному подмногообразию в $\mathbb{A}^{n+1}$.

Упражнение. Если X, Y — аффинные, то $A(X \times Y) \cong A(X) \otimes_{\Bbbk} A(Y)$.

Замечание. Над алгебраически замкнутым полем тензорное произведение целостных конечно порожденных алгебра — целостная конечно порожденная алгебра. Если поле не алгебраически замкнутое, то это не обязательно так.

2.11 Размерность редуцированного кольца, в котором каждый необратимый элемент является делителем нуля

Лемма 35. Пусть R — нётерово кольцо. Тогда

1. Любой минимальный простой идеал состоит из делителей нуля.
2. Множество всех делителей нуля нётерова кольца R представляет из себя объединение конечного числа ассоциированных простых идеалов $\mathfrak{p}_i$, а $\mathfrak{p}_i = \operatorname{Ann}(a_i)$ для некоторого $a_i \in R$.
3. Пусть R — нётерово кольцо, причем любой его элемент либо обратим, либо делитель нуля и вдобавок R редуцировано (т.е. $\operatorname{NRad}(R) = 0$). Тогда $\dim R = 0$ (т.е. R — артиново кольцо).

Доказательство. Докажем сначала **первый пункт**. Пусть $\mathfrak{p}$ — минимальный простой идеал. Тогда, так как в кольце $R_{\mathfrak{p}}$ идеал $\mathfrak{p}R_{\mathfrak{p}}$ максимальный,

$$\operatorname{NRad}(R_{\mathfrak{p}}) = \mathfrak{p}R_{\mathfrak{p}}.$$

Так $R_{\mathfrak{p}}$ нётерово (локализация нётерова кольца нётерова), значит идеал конечнопорождён: $\mathfrak{p}R_{\mathfrak{p}} = (e_1, \ldots, e_n)$. Тогда, если $\forall j \quad e_j^n = 0$, то

$$\operatorname{NRad}(R_{\mathfrak{p}})^{nm} = 0.$$

Значит, $\forall a \in \mathfrak{p}\ a^{nm} = 0$ в кольце $R_{\mathfrak{p}}$. Тогда $\exists s \in \mathfrak{p}\colon a^N s = 0$ в R, значит a — делитель нуля.

Второй пункт был в курсе коммутативной алгебры.

Теперь докажем **третий** пункт. Возьмём $\mathfrak{m} \in \operatorname{Specm} R$, тогда он полностью состоит из делителей нуля. Тогда по пункту 2:

$$\mathfrak{m} \subset \bigcup_{i=1}^{m} \mathfrak{p}_i \implies \mathfrak{m} \subset \mathfrak{p}_i \implies \mathfrak{m} = \mathfrak{p}_i.$$

Тогда $\mathfrak{m} = \operatorname{Ann}(a)$ для некоторого $a \in R$. Предположим, что $\mathfrak{p} \subsetneq \mathfrak{m}$. Рассмотрим два случая:

1. $a \in \mathfrak{m}$. Тогда $a \in \mathrm{Ann}(a)$, откуда $a^2 = 0$, но это противоречит тому, что $\mathrm{NRad}(R) = 0$.
2. $a \notin \mathfrak{m}$. Возьмём тогда $b \in \mathfrak{m} \setminus \mathfrak{p}$. Тогда $ab = 0$. Заметим, что $a \notin \mathfrak{p}, b \notin \mathfrak{p}$. Но тогда мы получили противоречие с тем, что идеал $\mathfrak{p}$ простой.

□

Теорема 54. *Пусть R — нётерово кольцо, а $S = R[x]$. Пусть $\dim R = d - 1,\ d \geq 1$, а $I \trianglelefteq S$. Тогда $\exists f_1, \ldots, f_d \in I$:*

$$\sqrt{I} = \sqrt{(f_1, \ldots, f_d)}.$$

Доказательство. Пусть $d = 1$, тогда $\dim R = 0$ и $R/\operatorname{NRad}(R)$ — редуцированное артиново кольцо, то есть прямая сумма конечного числа полей

$$R/\operatorname{NRad}(R) = K_1 \oplus K_2 \oplus \ldots K_n.$$

С другой стороны, легко проверить, что $\operatorname{NRad}(R[x]) = \operatorname{NRad}(R)[x]$. Но тогда мы получаем, что

$$S/\operatorname{NRad}(S) \cong K_1[x] \oplus \ldots K_n[x],$$

а справа написана область главных идеалов. Тогда идеал $I + \operatorname{NRad}(S)/\operatorname{NRad}(S)$ главный, пусть он порождается $f \in I$. Тогда

$$I + \operatorname{NRad}(S) = (f) + \operatorname{NRad}(S) \implies \sqrt{I} = \sqrt{I + \operatorname{NRad}(S)} = \sqrt{(f) + \operatorname{NRad}(S)} = \sqrt{(f)}.$$

Поясним равенство $\sqrt{I} = \sqrt{I + \operatorname{NRad}(S)}$. Включение ($\subset$) очевидно, докажем включение ($\supset$). Пусть $x \in \sqrt{I + \operatorname{NRad}(S)}$, тогда $x^m = a + b$, где $a \in I$, $b \in \operatorname{NRad}(S)$. Тогда, так как $b^N = 0$ для некоторого N, $(x^m)^N \in I$, откуда $x \in \sqrt{I}$.

Сделаем теперь переход $d - 1 \mapsto d$. Так как при факторизации по $\operatorname{NRad}(R)$ размерность не меняется, не умаляя общности мы можем полагать, что с самого начала кольцо редуцированное.

Рассмотрим U — множество всех не делителей нуля в R. Рассмотрим локализацию $U^{-1}R = R[U^{-1}]$. Заметим, что в $R[U^{-1}]$ любой элемент либо обратим, либо является делителем нуля. Тогда по лемме 35 это кольцо будет редуцированным нётеровым кольцом размерности 0, то есть произведением конечного числа полей. Тогда

$$S[U^{-1}] = \prod K_i[x],$$

то есть это в частности кольцо главных идеалов. Тогда $IS[U^{-1}] = (f_1)S[U^{-1}]$, где $f_1 \in I$.

Тогда, так как I конечно порожден, $\exists r \in U\colon rI \subset (f_1) \subset S$[11]. Так как r — не делитель нуля, он не лежит в объединении всех минимальных простых идеалов кольца R (тут мы вновь пользуемся леммой 35). Перейдём к фактору и покажем, что

$$\dim R/(r) \leq d - 2$$

В самом деле, если $\dim R/(r) = d - 1$, то у нас есть цепочка

$$\mathfrak{p}_0/(r) \subsetneq \mathfrak{p}_1/(r) \subsetneq \ldots \subsetneq \mathfrak{p}_{d-1}/(r).$$

Тогда, поднимаясь к исходному кольцу, мы получаем такую цепочку:

$$(r) \subset \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_{d-1}.$$

Но тогда идеал $\mathfrak{p}_0$ не может быть минимальным (так как r не лежит ни в каком минимальном), а значит, мы можем увеличить цепочку и получить противоречие.

Теперь мы можем применить к кольцу $R/(r)$ индукционное предположение: $\exists \overline{f_2}, \ldots, \overline{f_d} \in I + (r)/(r)$:

$$\sqrt{I + (r)/(r)} = \sqrt{(\overline{f_1}, \ldots, \overline{f_d})}.$$

[11] Можно считать, что $r \in U$, домножая на НОК знаменателей образующих.

Теперь остается проверить только, что

$$\sqrt{I} = \sqrt{(f_1, \dots, f_d)}.$$

Действительно, если $x \in \sqrt{I}$, то $x^k \in I$, а кроме того, $\overline{x}^m \in \sqrt{(\overline{f_2}, \dots, \overline{f_d})} \cdot R/(r)$, то есть $x^m \in (r, f_2, \dots, f_d)$.

Тогда $x^{k+m} \in x^m I \in (r, f_2, \dots, f_d)I$, но так как $rI \subset (f)1$, то есть

$$x^{k+m} \in x^m I \in (r, f_2, \dots, f_d)I \subset (f_1, \dots, f_d).$$

□

Пусть $X \subset \mathbb{A}^n$ — аффинное многообразие, тогда $I(X) \subset S = \Bbbk[x_1, \dots, x_{n-1}][x_n] = R[x]$, $\dim R = n - 1$. Тогда по предыдущей теореме мы можем найти $f_1, \dots, f_d$ такие, что

$$\sqrt{I(X)} = I(X) = \sqrt{(f_1, \dots, f_d)}.$$

Тогда ясно, что $X = Z(I) = Z(\sqrt{f_1, \dots, f_n}) = Z(f_1, \dots, f_n)$, чего мы и хотели.

Следствие 25. *В $\mathbb{A}^n$ любое аффинное многообразие задаётся не более чем n уравнениями.*

3. Проективные многообразия

3.1 Проективные многообразия

Пусть $\Bbbk$ — наше базовое алгебраически замкнутое поле, рассмотрим проективное пространство $\mathbb{P}^n = \mathbb{P}^n_{\Bbbk}$.

В этом контексте кольцо многочленов $S = \Bbbk[x_0, x_1, \dots, x_n]$ мы будем рассматривать, как градуированное кольцо. Для этого вкратце напомним терминологию:

Определение 66. Кольцо S называется *градуированным*[12], если оно обладает разложением в прямую сумму

$$S = \bigoplus_{d \geq 0} S_d$$

абелевых групп S_d таких, что $S_d \cdot S_e \subset S_{de}$. Элементы из S_d мы будем называть *однородными степени* d.

Идеал $\mathfrak{a} \subset S$ мы будем называть *однородным*, если он представляется в виде

$$\mathfrak{a} = \bigoplus_{d \geq 0} (\mathfrak{a} \cap S_d).$$

Приведём несколько полезных фактов про однородные идеалы:

- Идеал однородный тогда и только тогда, когда он может быть порожден однородными элементами.
- Сумма, произведение, пересечение однородных идеалов, а также радикал однородного идеала однородны.
- Однородный идеал $\mathfrak{a}$ простой тогда и только тогда, когда для любых двух *однородных* f, g из условия fg следует, что либо $f \in \mathfrak{a}$, либо $g \in \mathfrak{a}$.

Кольцо $S = \Bbbk[x_0, x_1, \dots, x_n]$ мы превратим в градуированное так: обозначим за S_d множество всех линейных комбинаций одночленов полной степени d от переменных $x_0, \dots, x_n$.

Кроме того, многочлены мы уже не можем рассматривать как функции на $\mathbb{P}^n$ ввиду неоднозначности координатных представлений точек $\mathbb{P}^n$. Но, заметим, что если f — однородный многочлен, то очевидно, что свойство f обращаться в 0 зависит только от класса эквивалентности $(a_0, \dots, a_n)$. Тем, самым, для однородных многочленов имеет смысл говорить о множестве

$$Z(f) \stackrel{\text{def}}{=} \{P \in \mathbb{P}^n \mid f(P) = 0\}.$$

[12] Если точнее, $\mathbb{N}_{\geq 0}$-градуированным.

Соотвественно, для любого множества T однородных элементов мы определяем

$$Z(T) \stackrel{\text{def}}{=} \{P \in \mathbb{P}^n \mid f(P) = 0 \quad \forall f \in T\}.$$

Если $\mathfrak{a}$ — однородный идеал в S, то определим $Z(\mathfrak{a})$, как $Z(\mathfrak{a}) = Z(T)$, где T — множество всех однородных элементов из $\mathfrak{a}$. В силу нётеровости кольца S любое множество однородных элементов T содержит такое конечное подмножество $f_1, \ldots, f_r$, что $(T) = (f_1, \ldots, f_r)$.

Определение 67. Подмножество проективного пространства $Y \subset \mathbb{P}^n$ называется *проективным алгебраическим многообразием*, если существует такое множество $T \subset S$ однородных элементов, что $Y = Z(T)$.

Таким образом, мы можем задать на $\mathbb{P}^n$ тополгию Зарисского, объявив замкнутыми алгебраические многообразия.

Определение 68. Также, для любого $Y \subset \mathbb{P}^n$ определим его *однородный идеал* $I(Y) \subset S$, как идеал, порожденный множеством однородных элементов $f \in S$ таких, что $f(P) = 0$ для всех $P \in Y$. *Однородное координатное кольцо* $S(Y)$ проективного многообразия Y определим как факторкольцо $S(Y) = S/I(Y)$.

Упражнение. Пусть $S = \Bbbk[x_1, \ldots, x_n]$, обозначим за S^h множество однородных многочленов. Тогда

1. Если $T_1 \subset T_2 \subset S^h$, то $Z(T_2) \subset Z(T_1)$.
2. Если $Y_1 \subset Y_2 \subset \mathbb{P}^n$, то $I(Y_2) \subset I(Y_1)$.
3. $I(Y_1 \subset Y_2) = I(Y_1) \cap I(Y_2)$.
4. Пусть $I \subset S$ — однородный идеал, $Z(I) \neq \varnothing$. Тогда $I(Z(I)) = \sqrt{I}$.
5. Пусть $I \subset S$ — однородный идеал. Тогда следующие условия равносильны:
   (a) $Z(I) = \varnothing$
   (b) $\sqrt{I} = (1)$ или $\sqrt{I} = S+ = \sum_{d>0} S_d$
   (c) $S_d \subset I$ для некоторого d.

Теорема 55 (Однородный Nullstelensatz)**.** *Пусть $I \subset \Bbbk[x_0, \ldots, x_n]$ — однородный идеал, а $f \in \Bbbk[x_0, \ldots, x_n]$ — однородный элемент положительной степени. Пусть $f(P) = 0$. Тогда*

$$\forall P \in Z(I) \subset \mathbb{P}^n \implies \exists m \colon f^m \in I.$$

Это теорема легко сводится к аффинному случаю.

Определение 69. *Квазипроективным многообразием* мы будем называть открытое подмножество проективного многообразия.

Наша дальнейшая цель состоит в том, чтоб показать, что n-мерное проективное пространство обладает открытым покрытием, состоящим из n-мерных аффинных пространств. И, как весьма полезное следствие, что *всякое проективное/квазипроективное многообразие) обладает открытым покрытием состоящие из аффинных/квазиаффинных многообразий* (это очень удобно, если мы доказываем что-то локально).

Пусть $H_i = Z(x_i)$ — координатные гиперплоскости. Рассмотрим множества

$$U_i = \mathbb{P}^n \setminus H_i = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}.$$

Совершенно ясно, что $\mathbb{P}^n$ покрывается множествами U_i (так как у любой точки хотя бы одна из однородных координат отлична от нуля). Рассмотрим отображение

$$\varphi_i \colon U_i \to \mathbb{A}^n, \quad (a_0 : \ldots : a_n) \mapsto \left(\frac{a_0}{a_i} : \ldots : \frac{a_n}{a_i}\right).$$

Отметим, что это отображение опредедлено корректно, так как частное a_j/a_i не зависит от выбора однородных координат.

Предложение 32. *Отображение φ_i осуществляет гомеоморфизм $U_i \xrightarrow{\sim} \mathbb{A}^n$.*

Доказательство. Очевидно, что оно биективно. Достаточно показать, что замкнутые множества в U_i соотвествуют замкнутым множествам в $\mathbb{A}^n$. Не умаляя общности, $i = 0, U_0 = U,\ \varphi_0 = \varphi$.

Пусть $A = \Bbbk[y_1, \dots, y_n]$. Рассмотрим отображения

$$\alpha\colon S^h \to A, \quad \alpha(f) = f(1, y_1, \dots, y_n),\ \beta\colon A \to S^h, \quad \beta(g) = x_0^{\deg g} \cdot g\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

Пустть $Y \subset U$ — замкнутое подмножество.Тогда $\overline{Y}$ (тут замыкание берётся в $\mathbb{P}^n$) — проективное многообразие, то есть $\overline{Y} = Z(T)$ для некотрого $T \subset S^h$. Положим $\alpha(T) = T'$. Тогда непосредственно проверяется, что $\varphi(Y) = Z(T')$. И обратно, если W — замкнутое подмножество в $\mathbb{A}^n$, то $W = Z(T')$ для некоторого $T' \subset A$ и легко проверить, что

$$\varphi^{-1}(W) = Z(\beta(T')) \cap U..$$

Значит и φ и φ^{-1} замкнутые, что и требовалось. □

Следствие 26. *Пусть Y — проективное (квазипроективное) многообразие. Тогда Y покрывается открытыми множествами $Y \cap U_i$, гомеоморфными аффинным (квазиаффинным) многообразиям, причем гомеоморфизм осуществляется определённым выше отображением φ_i.*

Определение 70. Пусть X — квазипроективное многообразие. Функция $f\colon X \to \Bbbk$ называется *регулярной* в точке $P \in Y$, если существует такая открытая окрестность $U \subset X$ точки P и такие **однородные** многочлены $g, h \in \Bbbk[x_0, \dots, x_n]$ **одной и той же степени**, что

- h не имеет нулей в U.
- $f = g/h$ в U.

Функция f *регулярна на* Y, если она регулярна в каждой точке Y.

Замечание. Отметим, что в этом случае сами f и g не являются функциями на $\mathbb{P}^n$, но вот их отношение (при $h \neq 0$) определено корректно, так как они имеют одинаковую степень однородности.

Пример 24. Например, если $X = U_0$, то функция $f(x_0, \dots, x_n) = x_1/x_0$ регулярна на X.

Определение морфизма на квазипроективные многообразия переносится без изменений:

Определение 71. Пусть X, Y — квазипроективные многообразия, $\varphi\colon X \to Y$ — *морфизм*, если

1. φ непрерывно.
2. Для каждого открытого $V \subset Y$ и каждой регулярной функции $f\colon V \to \Bbbk$ её пуллбек $\varphi^*(f) = f \circ \varphi\colon \varphi^{-1}(V) \to \Bbbk$ — регулярная функция.

Предложение 33. *Пусть $U_i \subset \mathbb{P}^n$ — определённое выше открытое множество. Тогда отображение $\varphi_i\colon U_i \to \mathbb{A}^n$ определённое выше является изоморфизмом.*

Доказательство. Выше мы уже показали, что это отображение — гомеоморфизм. Теперь нужно показать, что на каждом открытом множестве регулярные функции этих многообразий совпадают. Регулярные функции на U_i локально представляются в виде отношений однородных многочленов от $x_0, \dots, x_n$ одинаковой степени, а на $\mathbb{A}^n$ — в виде отношений многочленов от $y_1, \dots, y_n$. Легко видеть, что они отождествляются с помощью отображений α и β, определённых в доказательстве 32. □

Теперь, пусть f — регулярная функция на всём $\mathbb{P}^n$. Тогда $f|_{U_i}$ — регулярная функция на U_i, а так как U_i (по утверждению выше) отождествляется с $\mathbb{A}^n$, $f|_{U_i}$ отождествляется с регулярной функции на $\mathbb{A}^n$ (причем, при помощи определённых нами выше отображений). т=Тогда $f|_{U_i}$ — многочлен от переменных $\frac{x_j}{x_j},\ j \neq i$. Значит, мы можем представить её в виде

$$f = \frac{r_i(x_0, \dots, x_m)}{x_i^m},$$

где r_i — многочлен.

Посмотрим, что происходит на пересечениях. Например,

$$\text{на } U_0 \cap U_1 : \frac{r_0(x_0, \dots, x_n)}{x_0^m} = \frac{r_1(x_0, \dots, x_n)}{x_1^k}$$

Отмюда мы получам, что $f|_{U_0} = C_0$. Аналогично, $f|_{U_i} = C_i$. Так как на пересечениях константы согласованы, функция f постоянна. Итак, мы доказали такое утверждение:

Предложение 34. *Пусть f — регулярная функция на всём $\mathbb{P}^n$. Тогда f постоянна.*

Видно, что можно провести аналогию между этим утверждением и теоремой Лиувилля из комплексного анализа.

Предложение 35. *Любое квазиаффинное многообразие изоморфно некоторому квазипроективному.*

Доказательство. Как мы видели, у нас есть изоморфизм $\mathbb{A}^n \xrightarrow{\sim} U_0$. Причём, при отображении в эту сторону многочлены гомогенизировались:

$$f(y_1, \dots, y_n) \mapsto f^h(x_0, \dots, x_n) = x_0^{\deg f} f\left(\frac{x_0}{x_1}, \dots, \frac{x_n}{x_0}\right).$$

Тогда у нас есть такая коммутативная диаграмма:

$$\begin{array}{ccc} \mathbb{A}^n & \xrightarrow{\sim} & U_0 \\ \uparrow & & \uparrow \\ Z(f) & \dashrightarrow & Z(f^h) \end{array}$$

Значит и соотвествующие открытые куски будут изоморфны. □

Пример 25. Рассмотрим кривую в $C \subset \mathbb{P}^2,\ C = Z(y^2 - xz)$. Рассмотрим отображения

$$\mathbb{P}^1 \to C, (s:t) \mapsto (s^2 : st : t^2), \quad C \to \mathbb{P}^2,\ (x:y:z) \mapsto \begin{cases} (x:y), & x \neq 0 \\ (y:z), & z \neq 0 \end{cases}.$$

Видно, что эти отображения задают изомофизм C и $\mathbb{P}^1$. Но, однородные координатные кольца у этих многообразий — это $S(\mathbb{P}^1) = \Bbbk[x,y],\ S(C) = \Bbbk[x,y,z]/(y^2 - xz)$, а они неизоморфны.

Это наводит нас на мысль о том, что для проективных многообразий нам нужен какой-то структурный инвариант сильнее.

3.2 Проективное замыкание аффинного многообразия

Пусть $T \subset \mathbb{A}^n$ — замкнутое подмножество, попробуем найти $\overline{T} \subset \mathbb{P}^n$.

Первое, что приходит в голову — это просто взять гомогенизацию многочленов, которыми задаётся T, но это не всегда даст $\overline{T} \subset \mathbb{P}^n$, что иллюстрируется следующим примером:

Пример 26. Пусть $T = Z(y - x^2, z - xy) \subset \mathbb{A}^3$. Гомогенизируем все многочлены:

$$\mathbb{P}^3 \supset Z(yw - x^2, zw - xy) \supsetneq Z(yw - x^2, zw - xy, y^2 - xz) \supset = \{(st^2 : s^2t : s^3 : t^3) \mid (s:t) \in \mathbb{P}^1\} T.$$

С другой же стороны,

$$Z(yw - x^2, zw - xy) = \{(st^2 : s^2t : s^3 : t^3) \mid (s:t) \in \mathbb{P}^1\} \cup \{(0:1:0:0)\}.$$

Но, верно следующее

Упражнение. $\overline{T} = Z(\langle f^h \rangle_{f \in I(T)})$.

Ээээ а что дальше???

Доказательство теоремы **??**. Отображение f мы можем разложить в композицию дух:

$$X \xrightarrow{\Gamma_f} X \times Y \xrightarrow{\mathrm{pr}_2} Y, \quad x \mapsto (x, f(x)) \mapsto f(x).$$

Тогда нам достаточно доказать, что

1. $\Gamma_f(X)$ замкнут в $X \times Y$,
2. pr_2 переводит замкнутые множества в замкнутые.

Докажем сначала **первое**. Выделим это в отдельную лемму:

Лемма 36 (О замкнутом графике)**.** Пусть $f\colon X \to Y$ — морфизм, тогда $\Gamma_f(X)$ замкнут в $X \times Y$.

Доказательство леммы. Рассмотрим диагональный морфизм $\Delta\colon Y \to Y \times Y$. Тогда нам достаточно проверить, что $\Delta(Y)$ замкнут в $Y \times Y$, так как если мы это докажем, то можно рассмотреть

$$X \times Y \xrightarrow{(f,\mathrm{id})} Y \times Y$$

и тогда, так как $\Gamma_f(X) = (f, \mathrm{id})^{-1}(\Delta(Y))$, из замкнутости $\Delta(Y$ будет следовать замкнутость графика (просто по непрерывности).

Предположим сначала, что Y аффинное. Тогда всё просто: $\Delta(Y) = \Delta(\mathbb{A}^n) \cap (Y \times Y)$ и оба пересекаемых множества очевидно замкнуты.

Если же Y произвольное, покроем его аффинными: $Y \subset \bigcup U_i$, тогда $Y \times Y \subset \bigcup U_i \times U_i$ и тогда чтоб показать, что $\Delta(Y)$ замкнуто, нам достаточно показать, что $\Delta(Y) \cap (U_i \times U_i)$ замкнуто для всех i. Но это очевидно, так как

$$\Delta(Y) \cap (U_i \times U_i) = \Delta(U_i),$$

а $\Delta(U_i)$ замкнуто по первому шагу доказательства. □

Теперь покажем **второе**.

Прежде всего, можно считать, что $X = \mathbb{P}^n$, так как для произвольного X можно рассматривать композицию

$$X \times Y \hookrightarrow \mathbb{P}^n \times Y \to Y,$$

применить теорему для неё и из этого всё будет следовать.

Покрывая Y аффинными, мы понимаем, что достаточно доказать теорему для случая

$$\mathbb{P}^n \times \mathbb{A}^m \to \mathbb{A}^m.$$

А в этом случае работать существенно проще, так как (из теоремы **??**) мы знаем полное описание замкнутых множеств. Все они имеют вид

$$T = \{(u, y) \mid g_i(u, y) = 0,\ 1 \le i \le t\} \rightsquigarrow \mathrm{pr}(T) = \{y \in \mathbb{A}^m \mid \exists u \in \mathbb{P}^n\ g_i(u, y) = 0\ 1 \le i \le t\},$$

где g_i — однородный многочлен по u.

Пусть $I_s = (u_0, \dots, u_n)^s$. Тогда

$$y \in \mathrm{pr}_2(T) \iff \forall s \quad (g_1(u, y_0), \dots, g_t(u, y_0)) \not\supset I_s,$$

Тогда проекцию мы можем задать, как

$$\mathrm{pr}(T) = \bigcap_s \{y \in \mathbb{A}^m \mid I_s \not\subset (g_1(u, y), \dots, g_t(u, y))\}. \tag{2.2}$$

Значит, нам достаточно доказать, что каждое множество из пересечения замкнуто. Соответственно, по этому поводу зафиксируем s. Пусть $k_i = \deg_{u_i}(g_i)$, $\{M^{(\alpha)}\}_{\alpha \in \mathbb{N}^{n+1},\ \sum \alpha_j = s}$ — все мономы степени s[13]. Посмотрим, что означает условие, противоположное к условию (2.2):

$$I_s \subset (g_1(u, y_0), \dots, g_t(u, y_0)) \Leftrightarrow \forall \alpha\ M^{(\alpha)} = \sum g_i(u, y_0) F_{i,\alpha}(u) \qquad (*)$$

[13]Например, при $n = 2$ есть такой моном: $M^{(2,3,1)} = u_0^2 u_1^3 u_2$

а F_i однородные по переменным u_i. Кроме того, если $s \geq k_i$, то $\deg F_{i,\alpha} = s - k_i$, а если $s < k_i$, то ясно, что $F_{i,\alpha} = 0$. Теперь рассмотрим $\{N_i^{(\beta)}\}_\beta$ — все мономы (от переменных u_i) степени $s - k_i$. Тогда условие $(*)$ означает, что все $M^{(\alpha)}$ — всевозможные линейные комбинации $g_i(u, y_0)N_i^{(\beta)}$. Это, в свою очередь, равносильно тому, что

$$S = \operatorname{span}\{g_i(u, y_0)N_i^{(\beta)}\},$$

где S — пространство однородных многочленов степени α. Тогда ясно, что

$$I_s \not\subset (g_1(u, y_0), \dots, g_t(u, y_0)) \Leftrightarrow S \neq \operatorname{span}\{g_i(u, y_0)N_i^{(\beta)}\} \iff \operatorname{rank} A < \dim S,$$

где A — матрица, состоящая из коэффициентов $g_i(u, y_0)N_i(\beta)$. Тогда ясно, что при фиксированном y это полиномиальное условие (обнуление определителя), так что мы показали замкнутость. □

Следствие 27. *Пусть $X \in \mathsf{Proj}$, $Y \in \mathsf{qProj}$, а $f\colon X \to Y$ — морфизм. Пусть $Z \subset X$ — замкнутое подмножество. Тогда $f(Z)$ замкнуто в Y.*

3.3 Рациональные отображения многообразий

Лемма 37. Пусть X, Y — неприводимые многообразия, а φ, ψ — морфизмы из X в Y. Предположим, что существует такое непустое открытое множество $U \subset X$, что $\varphi|_U = \psi|_U$. Тогда $\varphi = \psi$.

Доказательство. Пусть $Y \subset \mathbb{P}^n$ для некоторого n. Беря композиции морфизмов φ и ψ с вложением $Y \to \mathbb{P}^n$, мы сводим всё к случаю $Y = \mathbb{P}^n$. Рассмотрим $\mathbb{P}^n \times \mathbb{P}^n$ со структурой проективного многообразия, определяемой вложением Сегре (см. **??**). Тогда φ и ψ определяют морфизм

$$X \xrightarrow{\varphi\times\psi} \mathbb{P}^n \times \mathbb{P}^n.$$

Рассмотрим диагональ $\Delta \subset \mathbb{P}^n \times \mathbb{P}^n$. Оно (как и в аффинном случае) замкнуто, так как представляется уравнениями

$$x_i y_j = x_j y_i, \quad i, j = 0, \dots, n.$$

По предположению $(\varphi \times \psi)(U) \subset \Delta$, но U плотно в X (так как X неприводимо), а Δ замкнуто, откуда мы имеем $(\varphi \times \psi)(X) \subset \Delta$, откуда $\psi = \varphi$. □

Определение 72. Пусть X, Y — многообразия, X неприводимо. Рассмотрим множество пар (U, f), где $U \subset X$ — открытое, а $f\colon U \to Y$ — морфизм. На этом множестве мы можем ввести такое отношение эквивалентности:

$$(U_1, f_1) \sim (U_2, f_2) \Leftrightarrow f_1|_{U_1\cap U_2} = f_2|_{U_1\cap U_2}.$$

Класс эквивалентности по этому отношению называется *рациональным* отображением и обозначается, как $f\colon X \dashrightarrow Y$.

Из всех пар (U, f) мы можем выбрать такую, для которой открытое множество U максимально. Это множество U мы будем называть *областью регулярности* рационального отображения.

Замечание. То, что описанное выше отношение — отношение эквивалентности, следует из леммы 37.

Определение 73. Рациональное отображение $f\colon X \dashrightarrow Y$ называется *доминатным*, для некоторой пары (U, f) $f(U)$ плотно в Y.

Замечание. Определение выше корректно, так как если образ плотен для какой-то пары, то это так и для всех (тоже по лемме 37).

Композицию рациональных отображений определить не всегда возможно (по понятным) причинам, а вот с доминатными рациональными отображениями дело обстоит лучше.

Пусть у нас есть доминантные рациональные отображения $X \dashrightarrow Y \dashrightarrow Z$ и они представляются морфизмами $f\colon U \to Y$ и $g\colon V \to Z$. Так как f доминантно, $f(U) \cap V \neq \varnothing$, откуда $W = f^{-1}(V) \cap U \neq \varnothing$. Тогда определим $g \circ f\colon X \dashrightarrow Z$ как класс эквивалентности пары $(W, g \circ f|_W)$.

Отметим также, что композиция доминантных отображений является доминантным. Действительно, предположим противное, а именно, что образ W под действием композиции попадает в некоторое замкнутое $T \subsetneq Z$. Но тогда $f(W) \subsetneq g^{-1}(T) \subsetneq Y$, а это противоречит доминантности.

Значит, квазипроективные многообразия с доминатными рациональными морфизмами образуют категорию.

Кроме того, доминантное рациональное отображение $\varphi\colon X \dashrightarrow Y$ индуцирует гомоморфизм полей рациональных функций

$$\varphi^*\colon \Bbbk(Y) \to \Bbbk(X)$$

Действительно, пусть φ представлено парой (U, φ_U) и пусть $f \in \Bbbk(Y)$ — рациональная функция, представленная парой (V, f), где f регулярна на V. Тогда, посколько $\varphi_U(U)$ плотно в Y, оно пересекается с V и $\varphi^{-1}(V)$ — непустое открытое подмножество X, так что $f \circ \varphi_U$ — регулярная функция на $\varphi_U^{-1}(V)$ (а регуляна она, так как φ_U — морфизм). Она представляет некоторую рациональную функцию на X.

$$\varphi^{-1}(V) \xrightarrow{\varphi} V \xrightarrow{f} \Bbbk.$$

Таким образом, мы построили отображение

$$\Bbbk(Y) \to \Bbbk(X), \quad f \mapsto \varphi^*(f).$$

Пусть C — категория неприводимых многообразий с доминантными рациональными отображениями, а D — категория конечно порожденных расширений поля $\Bbbk$.

Теорема 56. *Для любых неприводимых многообрзий X, Y приведённая выше конструкция осуществляет биективное соотвествие между*

- *множеством доминантных рациональных отображений $X \to Y$*
- *множеством гомоморфизмов $\Bbbk$-адгебр $\Bbbk(Y) \to \Bbbk(X)$.*

Более этого, это соотвествие осуществляет антиэквивалентность категорий C и D:

$$\mathcal{F}\colon \mathsf{C} \to \mathsf{D},\ X \mapsto \Bbbk(X).$$

Доказательство. Построим отображение обратное тому, что было приведено ранее.

Пусть $\theta\colon \Bbbk(Y) \to \Bbbk(X)$ —- гомоморфизм $\Bbbk$-алгебр. Нам надо построить соотвествующее ему доминантное рациональное отображение $X \to Y$.

Так как Y можно покрыть аффинными многообразиям, можно полагать, что Y аффинное. Пусть $A(Y)$ — его аффинное координатное кольцо, а $y_1, \dots, y_n$ — его образующие, как $\Bbbk$-алгебры. Тогда $\theta(y_1), \dots, \theta(y_n)$ являются рациональными функциями на X. Выберем открытое множество $U \subset X$ так, чтобы все функции $\theta(y_i)$ были регулярными на U. В таком случае θ определяет инъективный гомоморфизм $\Bbbk$-алгебр

$$A(Y) \to \mathcal{O}(U).$$

По теореме 52 ему соотвествут морфизм $\varphi\colon U \to Y$, который определяет доминантное[14] рациональное отображение $X \to Y$.

Теперь убедимся, что мы действительно построили антиэквивалентность категорий. Нам надо проверить, что для любого неприводимого многообразия Y поле рациональных функций $\Bbbk(Y)$ конечно порождено над $\Bbbk$ и обратно, что всякое конечно порожденное расщирение $K/\Bbbk$ является полем рациональных функций $K = \Bbbk(Y)$ некоторого неприводимого многообразия Y.

Пусть Y — неприводимое многообразие, тогда $\Bbbk(Y) = \Bbbk(U)$ для любого открытого подмножества $U \subset Y$, так что опять же можно полагать Y аффинным. Тогда $\Bbbk(Y) \cong \operatorname{Frac} A(Y)$ и, как следствие, оно являетя конечно порожденным расширением поля $\Bbbk$ степени трансцендентности $\dim Y$.

С другой стороны, пусть K — конечно порожденное расширение поля $\Bbbk$, а $y_1, \dots, y_n \in K$ — система образующих. Пусть. B — подалгебра в K, порожденная $y_1, \dots, y_n$ над $\Bbbk$. Тогда B является фактором кольца многочленов $\Bbbk[x_1, \dots, x_n]$ по некоторому идеалу I, так что $B \cong A(Y)$ для $Y = Z(I) \subset \mathbb{A}^n$. Y будет неприводимым, так как $A(Y)$ целостное. Значит, $K \cong \Bbbk(Y)$ и теорема доказана. □

[14] Оно будет доминантным, так как инчае отображение $A(Y) \to \mathcal{O}(U)$ не инъективно.

Переводя это на существенно менее изысканный язык, мы получаем такое следствие

Следствие 28. *Неприводимые многообразия X и Y бирационально эквивалентны тогда и только тогда, когда их поля рациональных функций $\Bbbk(X)$ и $\Bbbk(Y)$ изоморфны как $\Bbbk$-алгебры.*

3.4 Бирациональная эквивалентность

Определение 74. *Бирациональным отображением* $\varphi\colon X \to Y$ называется рациональное отображение, которое обладает обратным, т.е. таким рациональным отображением $\psi\colon Y \to X$, что $\psi \circ \varphi = \mathrm{id}_X$, $\varphi \circ \psi = \mathrm{id}_Y$. Многообразия X и Y называются *бирационально эквивалентными*, если существует хотя бы одно бирациональное отображение $X \to Y$.

Следствие 29. *Для любых двух неприводимых многообразий X и Y следующие условия эквивалентны:*

1. *X и Y бирационально эквивалентны,*
2. *существуют открытые подмножества $U \subset X$ и $V \subset Y$ такие, что U изоморфно V,*
3. *$\Bbbk(X) \cong \Bbbk(Y)$ в категории $\Bbbk$-алгебр.*

Доказательство. Сначала докажем $(\mathbf{1}) \implies (\mathbf{2})$. Пусть $\varphi\colon X \to Y$ и $\psi\colon Y \to X$ – бирациональные отображения. Пусть φ представлено парой (U, φ), а ψ — парой (V, ψ). Тогда отображение $\psi\circ\varphi$ представляется парой $(\varphi^{-1}(V), \psi \circ \varphi)$, а так как $\psi \circ \varphi = \mathrm{id}_X$ как раицональное отображение, $\psi \circ \varphi$ тождественно на $\varphi^{-1}(V)$. Аналогично, $\varphi \circ \psi$ тождественно на $\psi^{-1}(U)$. Тогда у нас есть $\varphi^{-1}(\psi^{-1}(U)) \subset X$ и $\psi^{-1}(\varphi^{-1}(U)) \subset Y$ — изоморфные открытые подмножества (изоморфизм осуществляется посредством отображений φ и ψ).

Утверждение $(\mathbf{2}) \implies (\mathbf{3})$ следует из опредления полей функций:

$$\Bbbk(U) \cong \Bbbk(X), \quad \Bbbk(V) \cong \Bbbk(Y), \quad \Bbbk(U) \cong \Bbbk(V) \implies \Bbbk(X) \cong \Bbbk(Y).$$

Утверждение $(\mathbf{3}) \implies (\mathbf{1})$ напрямую следует из теоремы 56. □

Теперь докажем какой-нибудь результат про бирациональную эквивалентность. Напомним несколько фактов из алгебры:

Теорема 57 (О примитивном элементе)**.** *Пусть L — конечное сепарабельное расширение поля K. Тогда существует элемент $\alpha \in L$, порождающий поле L, как расширение над K. Более того, если $\beta_1, \ldots, \beta_n$ — произвольная система образующих L/K и поле K бесконечно, то α можно выбрать α в виде $\alpha = c_1\beta_1 + \ldots + c_n\beta_n$ элементов β_i с коэффициентами $c_i \in K$.*

Определение 75. Расширение $K/\Bbbk$ называется *сепарабельно порожденным*, если существует такой базис трансцендентности $\{x_i\}$ в $K/\Bbbk$, что поле K является сепарабельным алгебраическим расширением поля $\Bbbk(\{x_i\})$. В таком случае $\{x_i\}$ называется *сепарабельным базисом трансцендентности.*

Теорема 58. *Пусть $K/\Bbbk$ — конечно порожденное и сепарабельно порожденное расширение поля $\Bbbk$. Тогда всякое множество образующих расширения $K/\Bbbk$ содержит подмножество, являющееся сепарабельным базисом трансцендентности.*

Теорема 59. *Пусть $\Bbbk$ — алгебраически замкнутое поле. Тогда любое конечно порожденное расширение $K/\Bbbk$ является сепарабельно порожденным.*

Предложение 36. *Всякие неприводимое многообразие X размерности r бирационально эквивалентно гиперповерхности $Y \subset \mathbb{P}^{r+1}$.*

Доказательство. Начнём с того, что поле функций $\Bbbk(X)$ является конечно порожденным расширением поля $\Bbbk$. Тогда по теореме 59 оно сепарабельно порождено над $\Bbbk$. Значит, существует базис трансцендентности $x_1, \ldots, x_r \in \Bbbk(X)$ такой, что $\Bbbk(X)$ — конечное сепарабельное расширение $\Bbbk(x_1, \ldots, x_r)$. Тогда по теореме о примитивном элементе 57 существует $y \in \Bbbk(X)$ такой, что $K = \Bbbk(y, x_1, \ldots, x_r)$. Элемент y алгебраичен над $\Bbbk$, то есть удовлетворяет некоторому полиномиальному уравнению с коэффициентами из поля рациональных функций от переменнвых $\Bbbk(x_1, \ldots, x_r)$. Домножая на знаменатели, мы получим

$$f(y, x_1, \ldots, x_r) = 0,$$

где f — некоторый неприводимый многочлен. Теперь легко видеть, что он определяет гиперповерхность в $\mathbb{A}^{r+1}$ с полем функций $\Bbbk(X)$, а отсюда, по теореме 56, она бирационально эквивалентна X. Проективное замыкание этой гиперповрехности и есть требуема гиперповерхность $Y \subset \mathbb{P}^{r+1}$. □

3.5 Рациональные многообразия

Определение 76. *Рациональным многообразием* мы будем называть многообразие, изоморфное в категории C проективному пространству. Эквивалентно (по теореме 56), можно говорить, что это многообразие, поле функций которого изоморфно $\Bbbk(t_1, \dots, t_n)$.

Пример 27. Например, окружность $x^2 + y^2 = 1$ является рациональным многообразием. Действительно, так как поле алгебраически замкнуто,

$$x^2 + y^2 = (x + iy)(x - iy) = st$$

и окружность задаётся как $st = 1$. Тогда видно, что $\Bbbk(X) \cong \Bbbk(t)$.

А знаем ли мы многообразия, которые не являются рациональными? Рассмотрим *эллиптическую кривую*

$$y^2 = x^3 + ax + b,$$

с условием, что $x^3 + ax + b$ не имеет кратных корней и $\operatorname{char} \Bbbk \neq 2, 3$. Условие про кратные корни гарантированно, например, тем, что $4a^3 + 27b^2 \neq 0$ и $a, b \neq 0$.

Делая линейные замены переменных, мы можем свести ситуацию к

$$y^2 = x(x - 1)(x - \alpha), \quad \alpha \neq 0.$$

Покажем, что эта кривая не является рациональной. Посмотрим на проективное замыкание этой кривой, для этого нужно взять гомогенизацию этого многочлена:

$$y^2 z = x^3 + axz^2 + bz^3.$$

Несложно видеть, что преоктивное замыкание от самой кривой отличается лишь на бесконечно удалённую точку: если $z \neq 0$, то мы получаем все аффинные точки, а если $z = 0$, то мы как раз получаем бесконечно удалённую точку $(0 : 1 : 0)$.

Так как аффинная кривая содержится в проективной, как открытое подмножество, поля функций у них совпадают. Из этого в частности следует, что если мы докажем, что у аффинная кривая не рациональна, то мы получим, что её проективизация не изоморфна $\mathbb{P}^1$.

Теперь докажем, что аффинная кривая не рациональна. Предположим, что $\Bbbk(X) \cong \Bbbk(t)$, и

$$y \mapsto \frac{p_1(t)}{p_2(t)}, \quad x \mapsto \frac{q_1(t)}{q_2(t)}.$$

Не умаляя общности, $(p_1, p_2) = (q_1, q_2) = 1$. Тогда должно быть выполнено соотношение

$$\frac{p_1^2}{p_2^2} = \frac{q_1}{q_2}\left(\frac{q_1}{q_2} - 1\right)\left(\frac{q_1}{q_2} - \alpha\right) \rightsquigarrow p_1^2 \cdot q_2^3 = p_2^2 q_1 (q_1 - q_2)(q_1 - \alpha q_2).$$

Отсюда $p_2^2 \vdots q_2^3$ и $q_2^3 \vdots p_2^2$, откуда они пропорциональны, то есть $q_2^3 / p_2^2 = c \in \Bbbk$, то мы получим

$$c p_1^2 = q_1 (q_1 - q_2)(q_1 - \alpha q_2)$$

и не умаляя общности, c здесь мы можем просто не писать. Отсюда q_2 — квадрат, тогда $q_1, q_2,\ q_1 - q_2,\ q_1 - \alpha q_2$ — квадраты.

Предложение 37. *Пусть Q_1, Q_2 — два взаимнопростых многочлена. Тогда в пространстве $\operatorname{span}_{\Bbbk}(Q_1, Q_2)$ нет четырёх полных квадратов, каждые два из которых непропорциональны.*

Доказательство. Пусть $R_1, R_2 \in \operatorname{span}_{\Bbbk}(Q_1, Q_2)$ непропорциональные квадраты. Так как они пропорциональны, $\operatorname{span}_{\Bbbk}(R_1, R_2) = \operatorname{span}_{\Bbbk}(Q_1, Q_2)$. Тогда оставшиеся два квадрата можно записать в виде $\alpha_1 R_1 + \alpha_2 R_2$ и $\beta_1 R_1 + \beta_2 R_2$. Пусть $R_1 = S_1^2,\ R_2 = S_2^2$ и

$$\alpha_1 R_1 + \alpha_2 R_2 = (\sqrt{\alpha_1} S_1 + \sqrt{\alpha_2} S_2)(\sqrt{\alpha_1} S_1 - \sqrt{-\alpha_2} S_2), \quad \beta_1 R_1 + \beta_2 R_2 = (\sqrt{\beta_1} S_1 + \sqrt{\beta_2} S_2)(\sqrt{\beta_1} S_1 - \sqrt{-\beta_2} S_2)$$

Так как $(S_1, S_2) = 1$, значит взаимно просты и правые части равенств, а отсюда $\sqrt{\alpha_1} S_1 + \sqrt{\alpha_2} S_2$, $\sqrt{\alpha_1} S_1 - \sqrt{-\alpha_2} S_2$, $\sqrt{\beta_1} S_1 + \sqrt{\beta_2} S_2$, $\sqrt{\beta_1} S_1 - \sqrt{-\beta_2} S_2$ — квадраты.

Выберем изначально Q_1, Q_2 с наименьшим максимумом степеней. Тогда мы только что смогли спуститься. □

Предложение 38. *Пусть X — неособая неприводимая кривая, пусть у нас есть рациональное отображение $f\colon X \dashrightarrow \mathbb{P}^n$. Тогда оно регулярно во всех точках.*

Доказательство. Действительно, рассмотрим открытое $U \subset X$, на котором f регулярно, то есть морфизм. Если мы рассмотрим f, как отображение $U \to \mathbb{A}^n_0 \subset \mathbb{P}^n$, то мы знаем, что f мы можем записать, как

$$u \mapsto (1 : f_1(u) : f_2(u) : \ldots : f_n(u)) = (f_0(u) : f_1(u) : f_2(u) : \ldots : f_n(u)), \quad f_i - \text{регулярны на } U.$$

Тогда $f_i \in \Bbbk(X)$. Рассмотрим $P \in X$, тогда $\mathcal{O}_P \subset \Bbbk(X)$. Так как кривая X неособая, $\mathcal{O}_P$ — дискретно нормированное кольцо. Обозначим соответствующее дискретное нормирование за υ_P, пусть $k_i = \upsilon_P(f_i)$, а $k = \min_i\{k_i\}$. В силу симметрии, мы можем считать, что минимум достигается при $i = 0$. Тогда мы можем записать каждую функцию, как

$$f_i = t^{k_i} g_i,$$

где t — локальный параметр, то есть образующая $\mathfrak{m}_P$ (или же, такой элемент, что $\upsilon_P(t) = 1$). Разделим каждую координату на t^{k_0}. Так мы получим другое рациональное отображение $X \dashrightarrow Y$, имеющее вид

$$u \mapsto (g_0(u) : t^{k_1-k_0} f_1(u) : \ldots : t^{k_n-k_0} g_n(u)).$$

Так как локальный параметр не обращается в 0 на некотором открытом множестве, это отображение определено на открытом множестве. Нетрудно видеть, что приведённое выше рациональное отображение регулярно в точке P. Действительно, $\upsilon_P(g_0) = 0$, то есть $g_0 \in \mathcal{O}_P^*$, то есть $g_0 \notin \mathfrak{m}_P$. Это означает, что g_0 определена в точке P и не обращается в 0 (и даже в некоторой окрестности этой точки). Для остальных i мы получаем, что $\upsilon_P(g_i) \geq 0 \implies g_i \in \mathcal{O}_P$, то есть они регулярны в некоторой окрестности P. Тогда мы получаем, что отображение определено в некоторой окрестности точки P и точка P является точкой регулярности (так как в её окрестности не все координаты равны нулю). По произвольности точки P мы имеем нужное.

□

При помощи этого утверждения также можно доказать, что эллиптическая кривая не бирационально изоморфна $\mathbb{P}^1$.

Предположим противное, пусть у нас есть рациональное отображение $C \dashrightarrow \mathbb{P}^1$. Тогда по предыдущему предложению мы можем полагать, что это отображение морфизм. Тогда у нас есть композиция

$$C \xrightarrow{f} \mathbb{P}^1 \xrightarrow{g} C,$$

где f, g — бирациональные изоморфизмы. Тогда на некотором открытом множестве $g \circ f = \mathrm{id}$.

Лемма 38. Если $h_1, h_2\colon X \to Y$ — морфизмы, X неприводимо и h_1 совпадает с h_2 на некотором открытом $U \subset X$. Тогда $h_1 = h_2$.

Тогда мы получаем, что $C \cong \mathbb{P}^1$. Не умаляя общности, можно считать, что $\infty \mapsto \infty$ и тогда достаточно доказывать, что аффинная эллиптическая кривая не может быть изоморфна $\mathbb{A}^1$. Чтоб доказать это, нужно смотреть на кольца регулярных функций. Оказывается, что кольцо регулярных функций на эллиптической кривой не факториально.

3.6 Локальное кольцо в точке

Определение 77. Пусть X — квазипроективное многообразие, $P \ni X$, а $\mathcal{O}(X)$ — его кольцо регулярных функций. Для точки P определим её *локальное кольцо* $\mathcal{O}_P$, как

$$\mathcal{O}_P = \varinjlim_{U \ni P} \mathcal{O}(U).$$

Говоря более изысканно, это кольцо ростков регулярных функций на Y в окрестности P. Или, иными словами, элемент $\mathcal{O}_P$ — это пара (U, f), где U — открытая окрестность P в Y, а f — регулярная функция на U, причём пары (U, f) и $(V, g$ отождествляются, если $f = g$ на $U \cap V$.

Отметим, что кольцо $\mathcal{O}_P$ на самом деле является локальным кольцом: его единственный максимальный идеал $\mathfrak{m}_P$ состоит из всех ростков регулярных функций, обращающихся в нуль в точке P. В самом деле, если $f(P) \neq 0$, то $1/f$ регулярна в некоторой окрестности P и в максимальном идеале лежать не может. Значит, всё вне $\mathfrak{m}_P$ обратимо, то есть $\mathfrak{m}_P$ максимальный. Также несложно видеть, что поле вычетов $\mathcal{O}_P/\mathfrak{m}_P \cong \Bbbk$.

Пусть A — локальное кольцо, $\mathfrak{m}$ — его максимальный идеал. Тогда $\mathfrak{m}/\mathfrak{m}^2$ — векторное пространство над $A/\mathfrak{m}$.

Предложение 39. *Пусть у нас есть набор $x_i \in \mathfrak{m}$ таких, что $(\overline{x_1}, \dots, \overline{x_k}) = \mathfrak{m}/\mathfrak{m}^2$. Тогда $(x_1, \dots, x_k) = \mathfrak{m}$.*

Доказательство. Рассмотрим модуль $M = \mathfrak{m}/(x_1, \dots, x_k)$. Тогда по лемме Накаямы:

$$M = 0 \iff \mathfrak{m}M = M \iff \mathfrak{m}^2 + (x_1, \dots, x_k) = \mathfrak{m},$$

что как равносильно тому, что $(\overline{x_1}, \dots, \overline{x_k})$ — система образующих $\mathfrak{m}/\mathfrak{m}^2$. □

Лемма 39. Пусть A — коммутативное кольцо, $I_1, \dots, I_n$ — набор идеалов ($n \geq 2$), причем среди них есть не более двух **не** простых. И, пусть

$$J \trianglelefteq A, \quad J \trianglelefteq I_1 \cup \ldots \cup I_n.$$

Тогда $J \subset I_k$ для некоторого k.

Доказательство этой леммы предоставляется читателю как упражнение.

Упражнение. Локальное кольцо точки $P = (0, 0)$ для кривой $X = Z(y^2 - x^3)$ не является дискретно нормированным.

Пример 28. Нетрудно заметить,что в случае упражнения выше у нас всё устроено так:

$$\dim X = 1, \quad \mathfrak{m} = (x, y), \quad \dim_{\Bbbk} \mathfrak{m}_P/\mathfrak{m}_P^2 = 2.$$

Возводя в степень максимальный идеал это кольца можно заметить интересную вещь:

$$\mathfrak{m}^3 = (x^3, x^2y, xy^2, y^3) = (y^2, x^2y) \subset (y) \implies \mathfrak{m}^3 \subset (y) \subset \mathfrak{m}$$

Это явление имеет такое коммутативно алгебраическое происхождение:

Теорема 60. *Пусть A — нётерово локальное кольцо. Тогда $\dim A < \infty$ и она равна минимальному такому n, для которого $\exists k,\ x_1, x_2 \dots, x_n \in \mathfrak{m}$ такие, что*

$$\mathfrak{m}^k \subset (x_1, \dots, x_n) \subset \mathfrak{m}.$$

Доказательство. Мы будем доказывать эту теорему для *колец геометрического происхождения*, то есть колец вида $\mathcal{O}_P$. Зафиксируем d и предположим, что для некоторого $k \in \mathbb{N}$ мы имеем

$$\mathfrak{m}_P^k \subset (x_1, \dots, x_d).$$

Шаг 1. Покажем сначала, что в таком случае $\dim \mathcal{O}_P \leq d$.

Так как если мы рассмотрим вместо всего многообразия неприводимую компоненту максимальной размерности, содержащую точку P, то $\dim \mathcal{O}_P$ не изменится, и всё еще будет $\mathfrak{m}_P^k \subset (x_1, \dots, x_d)$, не умаляя общности можно полагать кольцо целостным.

$\operatorname{Specm} A$ — аффинная окрестность, содержащая точку P, а A — её координатное кольцо.

Так как $\mathcal{O}_P = \varinjlim A_a$, мы с самого начала можем полагать, что мы работаем в некоторой локализации A_s. Теперь докажем вот такую лемму:

Лемма 40. Пусть I, J — идеалы в целостном нётеровом кольце A, $\mathfrak{m} \in \operatorname{Specm} A$ и $I_{\mathfrak{m}} \subset J_{\mathfrak{m}}$. Тогда существует $a \in A \setminus \mathfrak{m}$ такой, что $I_a \subset J_a$.

Доказательство леммы. Рассмотрим короткую точную последовательность

$$0 \to J \to I + J \to I + J/J \to 0.$$

Так как локализация — это точный функтор, точной будет и последовательность

$$0 \to J_{\mathfrak{m}} \xrightarrow{\sim} (I + J)_{\mathfrak{m}} \to (I + J/J)_{\mathfrak{m}} \to 0.$$

Тогда, так как $I_{\mathfrak{m}} \subset J_{\mathfrak{m}}$, вторая слева стрелка — изоморфизм, откуда $(I + J/J)_{\mathfrak{m}} = 0$. Рассмотрим конечнопорожденный A-модуль $M = I + J/J$. Так как $M_{\mathfrak{m}} = 0$, существует $a \in A \setminus \mathfrak{m}$ такой, что $M_a = 0$, то есть $(I + J/J)_a = 0$. Но, последовательность

$$0 \to J_a \xrightarrow{\sim} (I + J)_a \to (I + J/J)_a \to 0 \iff 0 \to J_a \xrightarrow{\sim} (I + J)_a \to 0$$

также точна, откуда $I_a \subset J_a$.

□

Применяя эту лемму к $\mathcal{O}_P = A_{\mathfrak{m}_P}$ мы получаем, что $\exists b$: в кольце $B = A_b$ имеется включение идеалов

$$\mathfrak{m}_P^k \subset (x_1, \ldots, x_d).$$

Тогда мы имеем включения

$$\mathfrak{m}_P \subset \sqrt{(x_1, \ldots, x_d)} \subset \mathfrak{m}_P,$$

откуда (так как $\mathfrak{m}_P = I(P)$), мы получаем, что $P = Z(x_1, \ldots, x_d)$. Тогда, если $\dim \mathcal{O}_P > d$, то мы пришли к противоречию, так как $Z(x_1, \ldots, x_d)$ — это пересечение d гиперповерхностей, а оно либо пустое, либо степени $\dim \mathcal{O}_P - d > 0$.

Шаг 2. Покажем, что для $d = \dim \mathcal{O}_P$ существует натуральное k такое, что

$$\mathfrak{m}_P^k \subset (x_1, \ldots, x_d).$$

Будем доказывать это индукцией по d.

База. Случай $d = 0$ очевиден, так как кольцо $\mathcal{O}_P$ локальное, откуда $\mathrm{Rad}(\mathcal{O}_P) = \mathfrak{m}_P$, но в Артиновом кольце радикал Джекобсона нильпотентен, то есть для некоторо N $\mathfrak{m}_P^N = 0$ и условие будет выполнено.

Переход. Рассмотрим элемент x, не лежащий в объединении минимальных простых идеалов. Тогда, как мы видели в одном из параграфов ранее,

$$\dim \mathcal{O}_P/(x) \leq \dim \mathcal{O}_P - 1,$$

так как если у нас есть максимальная цепочка вложенных простых $\overline{\mathfrak{p}_0} \subset \ldots \subset \overline{\mathfrak{p}_n}$, то цепочка $\mathfrak{p}_0 \subset \ldots \subset \mathfrak{p}_n$ уже не будет максимальной, так как идеал $\mathfrak{p}_0$ не минимальный. Тогда по индукционному предположению существует k такое, что

$$\mathfrak{m}_P^k/(x) \subset (\overline{x_1}, \ldots, \overline{x_{d-1}}) \implies \mathfrak{m}_P^k \subset (x, x_1, \ldots, x_d).$$

□

Замечание. Комментарий про $< \infty$ тут по существу, так как произвольное нётерово кольцо, вообще говоря, не обязано быть конечномерным.

Следствие 30 (Из теоремы 60)**.** *Пусть A — нётерово локальное кольцо с максимальным идеалом $\mathfrak{m}$. Тогда*

$$\dim A \leq \dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2.$$

Доказательство. Пусть $\overline{x_1}, \ldots, \overline{x_n}$ — базис $\mathfrak{m}/\mathfrak{m}^2$. Тогда по предложению 39 мы имеем $(x_1, \ldots, x_n) = \mathfrak{m}$, а тогда $\mathfrak{m} \subset (x_1, \ldots, x_n) \subset \mathfrak{m}$. Но тогда по теореме 60 мы имеем $\dim A \leq n$. □

Применяя это к кольцу $\mathcal{O}_P$, мы получаем, что

$$\dim \mathcal{O}_P \leq \dim_{\Bbbk} \mathfrak{m}_P/\mathfrak{m}_P^2.$$

Это наводит на мысль, что полезно рассматривать следующие объекты:

Определение 78. Пусть A — локальное кольцо с максимальным идеалом $\mathfrak{m}$. Оно называется *регулярным*, если $\dim A = \dim_{\Bbbk} \mathfrak{m}/\mathfrak{m}^2$.

Нам понадобятся следующие факты о регулярных локальных кольцах:

1. Регулярное локальное кольцо целостное.
2. Регулярное локальное кольцо факториально.
3. Любая локализация регулярного локального кольца относительно простого идеала — тоже регулярное локальное кольцо.

Некоторые из них мы позже даже докажем. Перед этим, введём объект, который в принципе мотивирует изучение регулярных колец (т.е. поймём, что условие регулярности означает геометрически).

3.7 Касательное пространство

Определение 79. Пусть $X \subset \mathbb{A}^n$ — аффинное многообразие, $I(X) = (f_1, \ldots, f_m),\ P \in X$. Тогда пространство решений системы линейных уравнений

$$\begin{cases} \dfrac{\partial f_1}{\partial x_1}(P)t_1 + \ldots + \dfrac{\partial f_1}{\partial x_n}(P)t_n = 0 \\ \vdots \\ \dfrac{\partial f_m}{\partial x_1}(P)t_1 + \ldots + \dfrac{\partial f_m}{\partial x_n}(P)t_n = 0 \end{cases} \tag{2.3}$$

называется *касательным пространством к многообразию X в точке P*.

Замечание. Определение корректно, то есть оно не зависит от выбора образующих в идеале $I(X)$.

Доказательство. Возьмём $f \in I(X)$ и разложим его по образующим

$$f = f_1 g_1 + \ldots + f_m g_m.$$

Теперь продифференцируем:

$$\frac{\partial f}{\partial x_1}(P) = \sum_{j=1}^{m} \left(\frac{\partial f_j}{\partial x_1}(P) \cdot g_j(P) + \underbrace{f_j(P)}_{=0,\ \text{т.к. } f_j \in I(X)} \cdot \frac{\partial g_j}{\partial x_1}(P) \right) = \sum_{j=1}^{m} \frac{\partial f_j}{\partial x_1}(P) \cdot g_j(P).$$

Тогда отсюда мы заключаем, что

$$\sum_i \frac{\partial f}{\partial x_i} t_i = \sum_{i,j} \frac{\partial f_j}{\partial x_i}(P) g_j(P) t_i = \sum_j g_j(P) \cdot \left(\sum_i \frac{\partial f_j}{\partial x_1}(P) \cdot t_i \right)$$

Теперь заметим, что если $(t_1, \ldots, t_n)$ удовлетворяют системе 2.3, то каждое сллагаемое будет равно нулю. Значит, можно определять касательное пространство более инвариантно: записать бесконечную систему таких уравнений по все $f \in I(X)$, а это — то, что нам нужно. □

Теперь рассмотрим билинейное спаривание

$$\mathfrak{m}_P/\mathfrak{m}_P^2 \times T_p X \to \Bbbk, \quad (\overline{g}, (t_1, \ldots, t_n)) \mapsto \sum_i \frac{\partial g}{\partial x_i}(P) t_i \in \Bbbk.$$

Покажем, что оно невырождено. Для начала, поясним, что это отображение определено корректно.

- Так как $g \in \mathcal{O}_P$, в окрестности точки P мы можем представить g в виде $g = r/s$. Тогда по определению логично думать, что
$$g' = \frac{r's - rs'}{s^2}.$$
- Если $\overline{g_1} = \overline{g_2}$, то $g_1 - g_2 = h \in \mathfrak{m}_P^2$. Тогда
$$h = \sum_j \ell_j \ell_j', \text{ где } \ell_i, \ell_i' \in \mathfrak{m}_P \implies \frac{\partial h}{\partial x_i}(P) = \sum_j \left(\ell_j(P) \frac{\partial \ell_j'}{\partial x_i}(P) + \frac{\partial \ell_j}{\partial x_i}(P) \cdot \ell_j'(P) \right).$$
- Теперь, ддля $g \in \mathcal{O}_P$, $s \in I(X)$, тогда
$$(\overline{g}, (t_1, \ldots, t_n)) = (\overline{g+s}, (t_1, \ldots, t_n)),$$
так как $s \in I(X)$.

Теперь наконец покажем, что оно невырождено.

- Зафиксируем $(t_1, \ldots, t_n) \in T_P X$. Предположим, что
$$\forall g \in \mathfrak{m}_P \quad \sum_i \frac{\partial g}{\partial x_i}(P) t_i = 0.$$
Пусть $P = (p_1, \ldots, p_n)$. Тогда, если мы возьмём $g = x_i - p_i \in \mathfrak{m}_P$, то из равенства выше будет следовать, что $t_i = 0 \; \forall i$.
- Теперь зафиксируем $g \in \mathfrak{m}_P \subset \mathcal{O}_P \subset \Bbbk(x_1, \ldots, x_n)$. Предположим, что
$$\sum_i \frac{\partial g}{\partial x_i}(P) \cdot t_i = 0 \quad \forall (t_1, \ldots, t_n) \in T_p X.$$
Это уравнение является следствием уравнений для касательного пространства, откуда
$$\sum \frac{\partial g}{\partial x_i}(P) t_i = \alpha_1 \ell_1 + \ldots + \alpha_m \ell_m, \text{ где } \ell_i = \sum \frac{\partial f_i}{\partial x_j}(P) t_i.$$
Приравнивая коэффициенты слева и справа мы получаем, что
$$\frac{\partial g}{\partial x_i}(P) = \alpha_1 \frac{\partial f_1}{\partial x_i}(P) + \ldots + \alpha_m \frac{\partial f_m}{\partial x_i}(P) \; \forall i \implies \frac{\partial (g - \sum \alpha_j f_j)}{\partial x_i}(P) = 0.$$
Положим $\widetilde{g} = g - \sum \alpha_j f_j$ и разложим $\widetilde{g}$ по формуле Тейлора в точке P:
$$\widetilde{g}(x_1, \ldots, x_n) = \underbrace{\widetilde{g}(p_1, \ldots, p_n)}_{=0} + \sum_i \underbrace{\frac{\partial \widetilde{g}}{\partial x_i}(P)}_{=0} \cdot (x_i - p_i) + \varepsilon, \quad \varepsilon \in \mathfrak{m}_P^2,$$
откуда $\overline{\widetilde{g}} = 0$ в $\mathfrak{m}_P / \mathfrak{m}_P^2$. С другой стороны, $\sum \alpha_j f_j \equiv 0$ на X, откуда $g \in \mathfrak{m}_P^2$, то есть $\overline{g} = 0$ в $\mathfrak{m}_P / \mathfrak{m}_P^2$, чего мы и хотели.

Значит, мы только что доказали, что
$$T_p X \cong \left(\mathfrak{m}_P / \mathfrak{m}_P^2 \right)^*.$$

Это замечательное наблюдение позволяет нам распространить понятие касательного пространства с аффинного многообразия на произвольное квазипроективное:

Определение 80. Пусть $X \in \mathsf{qProj}$ а $P \in X$. Тогда *касательным пространством к X в точке P* мы будем называть векторное пространство
$$T_p X \stackrel{\text{def}}{=} \left(\mathfrak{m}_P / \mathfrak{m}_P^2 \right).$$

Замечание. Так как идеал $\mathfrak{m}_P$ конечнопорожден, это пространство всегда конечномерное.

Теорема 61. *Регулярное локальное кольцо геометрического происхождения является областью целостности.*

Доказательство. Будем вести индукцию по $\dim R$.
База. Пусть $\dim R = 0$. Тогда, так как R регулярно,

$$\dim R = \dim_{\Bbbk} \mathfrak{m}_P/\mathfrak{m}_P^2 = 0 \iff \mathfrak{m}_P = \mathfrak{m}_P^2.$$

Так как R — нётерово кольцо размерности 0, оно Артиново, а отсюда (и из того факта, что оно локальное) $\mathfrak{m}_p = \mathrm{Rad}(R) = \mathrm{NRad}(R)$, откуда существует такое n, что $\mathfrak{m}_P^n = 0$, но тогда $\mathfrak{m}_P = 0$, то есть R — поле.
Переход. Пусть $\dim R \geq 1$. Рассмотрим элемент $x \in \mathfrak{m}$, не лежащий в объединении минимальных простых и $\mathfrak{m}^2$. Такой существует, так как

$$\mathfrak{m} = \bigcup_{\mathfrak{p} - \text{минимальный простой}} \mathfrak{p} \cup \mathfrak{m}^2 \implies \mathfrak{m} \subset \mathfrak{p} \text{ или } \mathfrak{m} \subset \mathfrak{m}^2.$$

В первом случае $\dim R = 0$. Во втором случае по лемме Накаямы $\mathfrak{m} = 0$, откуда R — поле.

Теперь рассмотрим кольцо $S = R/(x)$. Ясно, что $\dim S \leq \dim R - 1$. Пусть $\dim S = d$. Заметим, что

$$\overline{\mathfrak{m}^2} \subset (\overline{x_1}, \ldots, \overline{x_d}) \subset \overline{\mathfrak{m}} \implies \mathfrak{m}^2 \subset (x, x_1, \ldots, x_d) \subset \mathfrak{m},$$

откуда $\dim S \geq \dim R - 1$. Теперь заметим, что S — регулярное локальное кольцо. То, что оно локальное с единственным идеалом $\overline{\mathfrak{m}}$ ясно. Тогда мы знаем, что

$$\dim S \leq \dim_{\Bbbk} \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2.$$

С другой стороны, мы имеем

$$\dim_{\Bbbk} \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \leq \dim_{\Bbbk} \mathfrak{m}/\mathfrak{m}^2 - 1 = \dim R - 1 = \dim S,$$

так как отображение $\mathfrak{m}/\mathfrak{m}^2 \hookrightarrow \mathfrak{m}/\mathfrak{m}^2 + (x)$ имеет нетривиальное ядро. Значит, кольцо S регулярно. Тогда по индукционному предположению S — область целостности, откуда $(x) \subset R$ — простой идеал. Так как x не лежит ни в одном минимальном простом идеале, существует $\mathfrak{p} \in \mathrm{Spec}\, R$ такой, что $\mathfrak{p} \subseteq (x)$. Рассмотрим $y \in \mathfrak{p}$, тогда $y = ax$ для некоторого $a \in R$. Но, так как $x \notin \mathfrak{p}$, отсюда $a \in \mathfrak{p}$. То есть $\mathfrak{p} = (x)\mathfrak{p}$, откуда по лемме Накаямы $\mathfrak{p} = 0$, то есть R — область целотсности. □

Определение 81. Пусть X — многообразие, $P \in X$. Точка P называется *неособой*, если $\mathcal{O}_P$ регулярно. Многообразие X называтся *неособым*, если каждая его точка неособая.

Точка, в которой локальное кольцо нерегулярно называется *особой точкой*.

3.8 Разложение в ряд Тейлора

Пусть X — многообразие, $P \in X$. Возьмём $f \in \mathcal{O}_P$, тогда ясно, что $f - f(P) \in \mathfrak{m}_P$. Так как идеал $\mathfrak{m}_P$ конечнопорожден, мы можем выбрать какую-то систему образующих $\mathfrak{m}_P = (u_1, \ldots, u_n)$. Тогда

$$f - f(P) = g_1 u_1 + \ldots + g_n u_n, \quad g_i \in \mathcal{O}_P.$$

Аналогично, $g_i \in g_i(P) + \mathfrak{m}_P$, тогда

$$f - f(P) - \sum_{i=1}^{n} g_i(P) u_i \in \mathfrak{m}_P^2 \implies f - f(P) - \sum_{i=1}^{n} g_i(P) u_i = \sum_{i,j=1}^{n} h_{ij} u_i u_j, \quad h_{i,j} \in \mathcal{O}_P.$$

Продолжая в том же духе мы получаем, что

$$\forall g \in \mathcal{O}_P \; \exists F_0 + F_1 + \ldots \in \Bbbk[[x_1, \ldots, x_n]] \colon f - \sum_{i=0}^{s} F_i(u_1, \ldots, u_n) \in \mathfrak{m}_P^{s+1} \; \forall s \in \mathbb{N},$$

где F_i — однородный многочлен степени i от переменных $x_1, \ldots, x_n$.

Определение 82. Полученное выше представление и называется *рядом Тейлора* для функции f относительно системы локальных параметров $u_1, \ldots, u_n$.

Ответим сразу на естественный вопрос о единственности такого представления.

Теорема 62. *Пусть X — многообразие, $P \in X$ — неособая точка, а $\dim \mathcal{O}_P = n$. Выберем систему образующих $\mathfrak{m} = (u_1, \ldots, u_n)$ и рассмотрим функцию $f \in \mathcal{O}_P$. Тогда существует единственный ряд Тейлора для функции f относительно системы $(u_1, \ldots, u_n)$.*

Доказательство. Докажем сначала вот такую лемму:

Лемма 41. Пусть F — s-форма от $x_1, \ldots, x_n$ с коэффициентами из поля $\Bbbk$. Предположим, что $F(u_1, \ldots, u_n) \in \mathfrak{m}_P^{s+1}$. Тогда $F \equiv 0$.

Доказательство леммы. **1)** Предположим сначала, что $F(0, \ldots, 1) = [u_n^s]F \neq 0$. Так как $a_n u_n^s + \ldots \in \mathfrak{m}_P^{s+1}$, $a_n u_n^s + \ldots = G(u_1, \ldots, u_n)$, где G — форма степени s с коэффициентами из $\mathfrak{m}_P$.

$$G(u_1, \ldots, u_n) = H_0 u_n^s + H_1 u_n^{s-1} + \ldots + H_s, \text{ где}$$

H_i — форма от $x_1, \ldots, x_{n-1}$ степени i. Тогда

$$(\underbrace{a_n}_{\in \Bbbk} - \underbrace{H_0(u_1, \ldots, u_{n-1})}_{\in \mathfrak{m}_P}) u_n^s \in (u_1, \ldots, u_{n-1}) \implies u_n^s \in (u_1, \ldots, u_{n-1}),$$

так как $(\underbrace{a_n}_{\in \Bbbk} - \underbrace{H_0(u_1, \ldots, u_{n-1})}_{\in \mathfrak{m}_P}) \in \mathcal{O}_P^*$. Значит, мы получаем

$$\mathfrak{m}_P^s \subset (u_1, \ldots, u_{n-1}) \subset \mathfrak{m}_P,$$

но тогда по лемме 60 мы имеем $\dim \mathcal{O}_P = n - 1$, что приводит нас к противоречию.
2) В общем случае сделаем замену переменных: возьмём

$$G(u_1, \ldots, u_n) = F(\alpha_1 1 u_1 + \ldots + \alpha_{1n} u_n, \ldots, \alpha_{n1} u_1 + \ldots + \alpha_{nn} u_n)$$

где $(\alpha_{ij}) \in \mathrm{GL}_n(\Bbbk)$ и

$$G(0, \ldots, 0, 1) = F(\alpha_{1n}, \ldots, \alpha_{nn}) \neq 0$$

и таким образом сведём ситуацию к **1)**. □

Теперь докажем теорему. Так как нас интересует лишь вопрос единственности, достаточно показать, что у нулевой функции ряд Тейлора также будет нулевым. Пусть $F_0 + F_1 + \ldots$ — ряд Тейлора для нуля. Тогда, так как функция 0 (очевидно) обнуляется в точке P, из определения и леммы мы имеем

$$F_0(u_1, \ldots, u_n) \in \mathfrak{m}_P, \implies F_0 \equiv 0.$$

Пусть теперь $s = 1$. Тогда, так как $F_0 = 0$, отсюда

$$F_1(u_1, \ldots, u_n) \in \mathfrak{m}_P^2 \implies F_1 \equiv 0$$

по лемме. Продолжая пользоваться леммой мы получаем, что $F_j \equiv 0$. □

Итак, выбор системы образующих $\mathfrak{m}_P = (u_1, \ldots, u_n)$ определяет гомоморфизм

$$\tau \colon \mathcal{O}_P \to \Bbbk[[x_1, \ldots, x_n]].$$

Естественно задуматься о том, каково его ядро. Нетрудно видеть, что

$$\tau(f) = 0 \iff f \in \bigcap_{s \in \mathbb{N}} \mathfrak{m}^s,$$

что мотивирует изучить, как устроен идеал справа. Оказывается, в нашем случае он устроен не слишком уж сложно.

Теорема 63. *Пусть A — локальное нётерово кольцо с максимальным идеалом $\mathfrak{m}$. Тогда*

$$\bigcap_{s\in\mathbb{N}} \mathfrak{m}^s = 0.$$

Доказательство. Рассмотрим $\alpha \in \bigcap_{s\in\mathbb{N}} \mathfrak{m}^s = M$. Тогда $\alpha = F_k(u_1, \ldots, u_n)$, где F_k — однородный многочлен из $A[x_1, \ldots, x_n]$ степени k.

Так как $A[x_1, \ldots, x_n]$ нётерово, не умаляя общности, мы можем считать, что

$$(F_1, F_2, \ldots, F_k, \ldots) = (F_1, \ldots, F_s).$$

Но тогда мы получаем, что

$$F_{s+1} = G_1F_1 + \ldots + G_sF_s, \quad G_i \in A[x_1, \ldots, x_n], \deg G_i = s + 1 - i$$

и G_i однородные. Тогда, подставляя $u_1, \ldots, u_n$:

$$\alpha = F_{s+1}(u_1, \ldots, u_n) = \alpha(G_1(u) + \ldots + G_s(u)) \implies \alpha = \alpha a,\ a \in \mathfrak{m}.$$

Но тогда $\mathfrak{m}M = M$ и, применяя лемму Накаямы, мы получаем $M = 0$. □

Таким образом, как мы видим, ядро построенного выше гомомрфизма тривиально и $\mathcal{O}_P \hookrightarrow \Bbbk[[x_1, \ldots, x_n]]$ и отсюда сразу следует целостность кольца $\mathcal{O}_P$.

Отметим также, что из леммы 41 можно извлечь достаточно полезное следствие. А именно, рассмотрим градуированное кольцо

$$\bigoplus_{k=0}^{\infty} \mathfrak{m}_P^k/\mathfrak{m}_P^{k+1}.$$

Тогда, когда P — неособая точка, мы можем рассмотреть гомоморфизм

$$\Bbbk[x_1, \ldots, x_n] \to \sum_{k=0}^{\infty} \mathfrak{m}_P^k/\mathfrak{m}_P^{k+1}, \quad x_i \mapsto u_i.$$

Из леммы следует, что это мономорфизм. Сюръективность очевидна. Значит, мы доказали такое следствие.

Следствие 31. *Пусть $P \in X$ — неособая точка. Тогда имеет место следующий изоморфизм $\Bbbk$-алгебр:*

$$\bigoplus_{k=0}^{\infty} \mathfrak{m}_P^k/\mathfrak{m}_P^{k+1} \cong \Bbbk[x_1, \ldots, x_n]$$

В частности, отсюда следует, что на неособом многообразии градуированная алгебра

$$\bigoplus_{k=0}^{\infty} \mathfrak{m}_P^k/\mathfrak{m}_P^{k+1}$$

не зависит от выбора точки P (что вообще говоря неочевидно).

3.9 Локальное кольцо точки на неособой кривой. Индексы ветвления и степень инерции.

Рассмотри неособоую проективную кривую X и точку $P \in X$. Мы знаем, что в силу того, что кривая неособая, $\dim \mathcal{O}_P = \dim_{\Bbbk} \mathfrak{m}_P/\mathfrak{m}_P^2$, а из этого условия по лемме Накаямы следует, что идеал $\mathfrak{m}_P$ главный.

Тогда ясно (на самом деле это было ясно и из общих соображений[15]), что кольцо $\mathcal{O}_P$ в этом случае — дискретно нормированное кольцо и с каждой точкой кривой у нас ассоциировано нормирование υ_P.

[15] Действительно, если мы рассматриваем к примеру аффинный случай, то $A(X)$ в этом случае Дедекиндово, а любая простая локализация Дедекиндова кольца — это кольцо дискретного нормирования.

Пусть теперь $\varphi\colon Y \to X$ — морфизм неособых кривых и $\varphi^{-1}(P) = \{Q_1, \dots, Q_n\}$. Попробуем понять, как же связаны нормирования υ_P и υ_{Q_i}. Ясно, что в этом случае у нас есть расширение колец $\mathcal{O}_P \to \mathcal{O}_{Q_i}$ и $\mathfrak{m}_P \subset \mathfrak{m}_{Q_i}$, $\mathfrak{m}_P = \mathfrak{m}_{Q_i} \cap \mathcal{O}_{Q_i}$. И, видно, что в этой ситуации нормирования υ_{Q_i} *продолжают* нормирование υ_P. Действительно, мы можем рассмотреть функцию

$$\psi(f) = \upsilon_{Q_i}(\varphi^*(f))\colon \mathcal{O}_P \to \mathbb{Z},$$

она уже возможно не будет дискретным нормированием, но $\operatorname{Im}\psi \leq \mathbb{Z}$ — подгруппа, обозначим её $e\mathbb{Z}$. Нетрудно проверить, что e не может быть равен нулю. Отсюда мы получаем, что

$$\upsilon_{Q_i} = e \cdot \upsilon_P.$$

Число e в этом контексте называют *индексом ветвления* и обозначают $e = e(\mathbb{Q}_{Q_i}/\mathcal{O}_P)$. Сразу видно, что индекс ветвления можно вычислить вот так:

$$\upsilon_{Q_i}(z_P) = e(\mathcal{O}_{Q_i}/\mathcal{O}_P),$$

где $(z_P) = \mathfrak{m}_P$ — локальный параметр для кольца $\mathcal{O}_P$. Или, иными словами, такой элемент, что $\upsilon_P(\pi_P) = 1$.

Степенью инерции называют степень расширения полей вычетов $f_i = [\Bbbk_{Q_i} : \Bbbk_P]$, где поле вычетов — это $\Bbbk_P = \mathcal{O}_P/\mathfrak{m}_P$.

Замечание. Более подробно обо всём этом можно прочесть в конспекте

https://www.overleaf.com/read/khfyxghsbmnn#50fedd

Посмотрим теперь, как в общей ситуации для колец нормирования связаны между собой индексы ветвления, степени инерции и степень расширения. Пусть L/K — конечное сепарабельное расширение, υ — нормирование на K, $\mathcal{O}_\upsilon$ — кольцо нормирования.

В коммутативной алгебре у нас была такая теорема:

Теорема 64. *Пусть A — Дедекиндово кольцо, K — его поле частных, L/K — конечное расширение (полей), а $B = \operatorname{Int}_L A$. Тогда B — дедекиндово.*

В нашей ситуации $A = \mathcal{O}_\upsilon$, а $B = \operatorname{Int}_L(A)$. Пусть $\mathfrak{m}_\upsilon = \mathfrak{p}$ и рассмотрим $\mathfrak{p}B$, он раскладывается в произведение простых:

$$\mathfrak{p}B = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$$

Каждая локализация $B_{\mathfrak{p}_i}$ является дискретно-нормированным кольцом (и, более того, кольцом нормирования w_i). Кроме того, все нормирования w_i, связанные с идеалами $\mathfrak{p}_i$, продолжают нормирование υ (т.е. $w_i \mid \upsilon$) и, это в точности все нормирования, продолжающие нормирование υ.

В самом деле, если w продолжает υ, то $(w|\upsilon \implies \mathfrak{m}_\upsilon \subset \mathfrak{m}_w \implies \mathfrak{m}_\upsilon B \vdots \mathfrak{m}_w)$ $\mathfrak{m}_w \cap B$ — простой идеал, висящий над идеалом $\mathfrak{p}$, то есть, один из $\mathfrak{p}_i$. Пусть $\mathfrak{m}_w \cap B = \mathfrak{p}_i$, тогда $\mathfrak{m}_w \cap B_{\mathfrak{p}_i} = \mathfrak{p}_i B_{\mathfrak{p}_i}$. Тогда $\mathfrak{m}_w \cap \mathcal{O}_{w_i} = \mathfrak{m}_w \cap B_{\mathfrak{p}_i} = \mathfrak{m}_{w_i}$, откуда $w = w_i$.

Как мы уже отмечали, $B_{\mathfrak{p}_i}/\mathfrak{p}_i B_{\mathfrak{p}_i} = \mathcal{O}_{w_i}/\mathfrak{m}_{w_i}$. Положим

$$f_i = [\mathcal{O}_{w_i}/\mathfrak{m}_{w_i} : A/\mathfrak{p}] = [\Bbbk_{w_i} : \Bbbk_\upsilon]$$

и будем (как и в первой части курса) называть f_i **степенью инерции**.

Отметим так же, что, как и в случае колец целых, B — свободный $\mathcal{O}_\upsilon$-модуль ранга n (как и кольцо целых $\mathcal{O}_K$, которое было свободным $\mathbb{Z}$-модулем ранга n).

Теорема 65. *Для индексов ветвления и степеней инерции справедлива следующая формула:*

$$\sum_{i=1}^{k} e_i f_i = n.$$

Доказательство. Пусть $\mathfrak{p} = \mathfrak{m}_v$. Так как B — свободный $\mathcal{O}_v$-модуль ранга n, ясно, что что $B/\mathfrak{p}B$ — векторное пространство над $A/\mathfrak{p}$ размерности n.

$$B/\mathfrak{p}B \cong B/\prod \mathfrak{p}_i^{e_i} = B/\mathfrak{p}_i^{e_1} \times B/\mathfrak{p}_i^{e_2} \times \ldots \times B/\mathfrak{p}_k^{e_k}.$$

Вычисляя размерности обеих частей равенства и приравнивая, мы получаем

$$n = \sum_{i=1}^{k} \dim_{A/\mathfrak{m}} B/\mathfrak{p}_i^{e_i}.$$

Рассмотрим на кольце B фильтрацию степенями идеалов $\mathfrak{p}_i$:

$$\mathfrak{p}_i^{e_i} \subset \mathfrak{p}_i^{e_i-1} \subset \ldots \subset \mathfrak{p}_i \subset B.$$

Посмотрим на факторы этой фильтрации, то есть, на $\mathfrak{p}_i^m/\mathfrak{p}_i^{m+1}$, они являются векторными пространствами над $A/\mathfrak{p}$. Покажем, что $\forall m \geq 1\ B/\mathfrak{p}_i \cong \mathfrak{p}_i^m/\mathfrak{p}_i^{m+1}$. Выберем $x \in \mathfrak{p}_i^m \setminus \mathfrak{p}_i^{m+1}$ и отображение $m_x\colon B/\mathfrak{p}_i \to \mathfrak{p}_i^m/\mathfrak{p}_i^{m+1},\ y \mapsto xy$. Вполне ясно, что это корректно определённый гомоморфизм, вычислим его ядро. Рассмотрим $y \in B$ такой, что $xy \in \mathfrak{p}_i^{m+1}$ и покажем, что тогда $y \in \mathfrak{p}_i$. Рассмотрим главный идеал (xy). Так как $xy \in \mathfrak{p}_i^{m+1}$, его разложение на простые имеет вид

$$(xy) = \mathfrak{p}_i^{m+1} \cdot I.$$

С другой стороны, $(x) = \mathfrak{p}_i^m \cdot J,\ J \not\vdots\ \mathfrak{p}_i$ и тогда $(y) = \mathfrak{p}_i \cdot \widetilde{J}$, откуда $y \in \mathfrak{p}_i$. Значит, мы показали, что $\ker m_x = \{0\}$. Сюръективность отображения m_x следует из того, что $(x) + \mathfrak{p}_i^{m+1} = \mathfrak{p}_i^m$. Так как $x \in \mathfrak{p}_i^m$, очевидно, что левая часть лежит в правой. Тогда $(x) + \mathfrak{p}_i^{m+1} = \mathfrak{p}_i^m \cdot I$, покажем, что $I = (1)$. Предположим противное, тогда

$$I = \mathfrak{p}_i^s \cdot \mathfrak{q}_1^{r_1} \cdot \ldots \mathfrak{q}_\ell^{r_\ell}, \quad \mathfrak{q}_j \neq \mathfrak{p}_i.$$

Тогда $I = \mathfrak{p}_i^s$, откуда $(x) + \mathfrak{p}_i^{m+1} = \mathfrak{p}_i^{m+s}$. Предположим, что s положительно. Тогда $(x) \subset \mathfrak{p}_i^{m+1}$, что противоречит тому, что мы брали $x \in \mathfrak{p}_i^m \setminus \mathfrak{p}_i^{m+1}$. Тогда мы показали, что

$$B/\mathfrak{p}_i \cong \mathfrak{p}_i^m/\mathfrak{p}_i^{m+1},$$

и отсюда уже следует теорема:

$$B/\mathfrak{p}_i^{e_i} \cong \frac{B}{\mathfrak{p}_i} \cdot \frac{\mathfrak{p}_i}{\mathfrak{p}_i^2} \cdot \ldots \frac{\mathfrak{p}_i^{e_i-1}}{\mathfrak{p}_i^{e_i}} \implies$$
$$\implies \dim_{A/\mathfrak{p}} B/\mathfrak{p}_i^{e_i} = \dim_{A/\mathfrak{p}} B/\mathfrak{p}_i + \dim_{A/\mathfrak{p}} \mathfrak{p}_i/\mathfrak{p}_i^2 + \ldots + \dim_{A/\mathfrak{p}} \mathfrak{p}_i^{e_i-1}/\mathfrak{p}_i^{e_i} = e_i \cdot \dim_{A/\mathfrak{p}} B/\mathfrak{p}_i = e_i \cdot f_i.$$

□

3.10 Конечные морфизмы и нормализация многообразия

Теорема 66. *Пусть L/K — сепарабельное конечное расширение, $A \subset K$ и $K = \mathrm{Frac}(A)$. Пусть $B = \mathrm{Int}_L A$ и предположим, что A нётерово и нормально*[16].

Тогда B — конечнопорожденный A-модуль.

Доказательство. Это доказывается стандартным образом. Во-первых, из такой леммы из коммутативной алгебры следует, что $L = \mathrm{Frac}(B)$:

Лемма 42. Пусть Z — дедекиндово кольцо с полем частных Q, F/Q — конечное расширение, а $R = \mathrm{Int}_F Z$. Тогда $F = \mathrm{Frac}(R)$ и, следовательно, R целозамкнуто.

[16]Кольцо называется нормальным, если любая его локализация в простом идеале целозамкнута.

Теперь возьмём $\{\omega_i\}_{i=1}^n$ — базис L/K, причём выберем $\omega_i \in B$. Рассмотрим билинейную форму следа

$$L \times L \to K, \quad (x, y) \mapsto \operatorname{Tr}(xy).$$

Из курса теории полей известно, что так как расширение сепарабельно, эта форма невырожденна. Тогда возьмём двойственный базис к ω_i, то есть рассмотрим такой набор $\{\omega_i^*\}$, что

$$\operatorname{Tr}(\omega_i \omega_j^*) = \begin{cases} 1, & i = j \\ 0, & \text{иначе.} \end{cases}$$

Тогда мы имеем включения

$$A\omega_1 \oplus \ldots \oplus A\omega_n \subset B \subset A\omega_1^* \oplus \ldots \oplus A\omega_n^*.$$

Действительно, первое включение очевидно, докажем второе. Пусть $b = a_1\omega_1^* + \ldots + a_n\omega_n^*$, где $a_i \in K$, мы покажем, что $a_i \in A$. С одной стороны,

$$a_i = \operatorname{Tr}(b\omega_i).$$

Пусть $G = \{\sigma\colon K \to L^{\text{alg}}\}$ — все вложения K в L^{alg}. Тогда если α цел над A, то $\sigma\alpha$ цел над a (это тривиальная проверка), а тогда и $\operatorname{Tr}(\alpha)$ цел над A, так как

$$\operatorname{Tr}(\alpha) = \sum_{\sigma \in G} \sigma\alpha,$$

откуда ясно, что $\operatorname{Tr}(\alpha)$ цело над A. Тогда, так как $\operatorname{Tr}(b\omega_i) \in K$ цело над A, $a_i = \operatorname{Tr}(b\omega_i) \in A$. Тогда мы получили, что B — подмодуль конечнопорожденного модуля над нётеровым кольцом, откуда B — конечнопородженный A-модуль.

□

Теорема 67. *Пусть A — целостная аффинная алгебра, $K = \operatorname{Frac}(A)$, а L/K — конечное расширение. Обозначим $B = \operatorname{Int}_L A$. Тогда B — конечнопорожденный A-модуль.*

Доказательство. По лемме Нётер о нормализации, A — конечное расширение кольца многочленов $\Bbbk[x_1, \ldots, x_n]$. Тогда, так как B цело на A, оно цело и над $\Bbbk[x_1, \ldots, x_n]$, откуда $B = \operatorname{Int}_L \Bbbk[x_1, \ldots, x_n]$.

Кроме того, расширение $L/\operatorname{Frac}(\Bbbk[x_1, \ldots, x_n])$ конечное (это следует из такой леммы):

Лемма 43. Пусть $\varphi\colon A \hookrightarrow B$ — конечное расширение. Тогда расширение $\operatorname{Frac}(B)/\operatorname{Frac}(A)$ конечное.

Доказательство. Рассмотрим мультипликативное подмножество $S = A \setminus \{0\}$. Тогда по лемме из курса коммутативной алгебры расширение $\operatorname{Frac}(A) = S^{-1}A \hookrightarrow \varphi(S)^{-1}B$ конечное. С другой стороны, так как $\varphi(S)^{-1}B$ — конечномерная область целостности над полем $\operatorname{Frac}(A)$, оно является полем (это следует из леммы Зарисского), в которое вкладывается B. Но тогда по универсальному свойству поля частных оно совпадает с $\operatorname{Frac}(B)$ и мы получили, что расширение $\operatorname{Frac}(B)/\operatorname{Frac}(A)$ конечное. □

Из этих рассуждений следует, что мы без ограничений общности можем полагать, что $A = \Bbbk[x_1, \ldots, x_n]$.

Кроме того, без ограничений общности мы можем полагать, что расширение L/K нормальное, так как если мы перейдём к нормальному замыканию $\widetilde{L}/K$ и докажем теорему для него и $\widetilde{B} = \operatorname{Int}_{\widetilde{L}} A \supset B$, то мы докажем теорему и для B.

Теперь, так как L/K нормально, если мы рассмотрим все вложения $G = \{\sigma\colon K \to L^{\text{alg}}\}$, то $\forall \sigma \in G\ \sigma(L) \subset L$ и мы можем рассмотреть башню расширений:

$$\begin{array}{c} L \\ | \\ L^G = F \\ | \\ K \end{array}$$

где верхний этаж — расширение Галуа, а нижний — чисто несепарабельное расширение[17].

Введём соответствующие кольца целых $\mathcal{O}_L = \operatorname{Int}_L A$ и $\mathcal{O}_L = \operatorname{Int}_F A$. Тогда у нас есть расширение

$$\begin{array}{c} \mathcal{O}_L = \operatorname{Int}_L A \\ \Big| \\ \mathcal{O}_L = \operatorname{Int}_F A \\ \Big| \\ A \end{array}$$

Так как расширение L/F сепарабельно, $\mathcal{O}_F$ целозамкнуто, мы можем применить теорему 66 и получить, что $\mathcal{O}_L$ — конечнопорожденный $\mathcal{O}_F$-модуль.

Далее, из общей теории полей следует, что чисто несепарабельное расширение устроено следующим образом:

$$F = \Bbbk\left(y^{\frac{1}{p^{m_1}}}, \dots, y^{\frac{1}{p^{m_s}}}\right), \text{ где } y_i \in A,\ p = \operatorname{char} \Bbbk.$$

Тогда, если мы возьмём $m = \max m_i$, то мы получим

$$y_i = \sum a_I x^I \implies y_i^{\frac{1}{p^m}} = \sum a_I^{\frac{1}{p^m}} x^{I/p^m}, \tag{2.4}$$

так как в характеристике p:

$$\left(\sum a_I^{\frac{1}{p^m}} x^{\frac{I}{p^m}}\right)^{p^m} = \sum \left(a_I^{\frac{1}{p^m}} x^{\frac{I}{p^m}}\right)^{p^m}$$

а так как поле $\Bbbk$ алгебраически замкнуто, $a^{\frac{1}{p^m}} \in \Bbbk$. Но, из (2.4) следует, что

$$F \subset \Bbbk\left(x_1^{\frac{1}{p^m}}, \dots, x_n^{\frac{1}{p^m}}\right).$$

Соответственно, если мы докажем теорему для $\Bbbk\left(x_1^{\frac{1}{p^m}}, \dots, x_n^{\frac{1}{p^m}}\right)$, то мы докажем её и для F, так что далее без ограничений общности можно полагать, что

$$F = \Bbbk\left(x_1^{\frac{1}{p^m}}, \dots, x_n^{\frac{1}{p^m}}\right).$$

Теперь покажем, что $\mathcal{O}_F = \Bbbk\left[x_1^{\frac{1}{p^m}}, \dots, x_n^{\frac{1}{p^m}}\right] = R$. Включение справа налево очевидно. Теперь пусть $\alpha \in \mathcal{O}_F$, тогда α цел над A, значит он цел и над R, откуда $\alpha \in R$ (так как R целозамкнуто и расширение R/A конечно[18]).

Итак, мы показали, что $\mathcal{O}_F/R$ конечно (а так как R/A конечно и $\mathcal{O}_L/\mathcal{O}_F$ конечно), из этого следует теорема.

□

Определение 83. Если в предыдущей теореме $L = K$, то B называется *нормализацией* A.

Замечание. Отметим, что в этом случае B является аффинной $\Bbbk$-алгеброй.

Определение 84. Пусть $\varphi\colon Y \to X$ — морфизм многообразий. Предположим, что у любой точки $x \in X$ есть такая аффинная окрестность U_x, что $\varphi^{-1}(U_x) \cong V_x$, где V_x — аффинная, и расширение $A(U_x) \hookrightarrow A(V_x)$ конечным. Тогда φ называется *конечным морфизмом.*

Определение 85. Пусть X — аффинное многообразие. Тогда X называется *нормальным*, если $X = \operatorname{Specm}(A)$, где A — нормальное.

[17] Вообще говоря, в характеристике 0 такого возникать не может

[18] Его базис состоит из мономов вида $x_1^{k_1/p^m} \cdot \ldots \cdot x_n^{k_n/p^m}$ по $0 \leq k_i \leq p^m - 1$

Замечание. Локализация нормального кольца нормальна.

Определение 86. Неприводимое многообразие X[19] называют *нормальным*, если $\forall P \in X$ кольцо $\mathcal{O}_P$ нормально.

Предложение 40. *Предыдущие два определения нормальности согласованы.*

Доказательство. Нам нужно доказать следующее утверждение: если $\forall \mathfrak{m} \in \operatorname{Specm}(A)$ кольцо $A_{\mathfrak{m}}$ нормально, то A нормально (для целостного кольца A).

Покажем, что $A = \bigcap_{\mathfrak{m}\in\operatorname{Specm}(A)} A_{\mathfrak{m}}$. Действительно, включение слева направо очевидно, а если $x \in \bigcap_{\mathfrak{m}\in\operatorname{Specm}(A)} A_{\mathfrak{m}}$, то $\forall \mathfrak{m} \in \operatorname{Specm}(A)$ найдётся $y_{\mathfrak{m}} \notin \mathfrak{m}$ такой, что $xy_{\mathfrak{m}} \in A$. Тогда, так как никакой y_{fm} не лежит ни в каком максимальном идеале, $(\{y_{\mathfrak{m}}\}_{\mathfrak{m}})$ — единичный идеал. Но тогда

$$1 = \sum y_{\mathfrak{m}} z_{\mathfrak{m}} \implies x = \sum x y_{\mathfrak{m}} z_{\mathfrak{m}} \in A.$$

Тогда, так как каждое кольцо в правой части целозамкнуто, и само A целозамкнуто. □

4. Дивизоры

4.1 Дивизоры Вейля

Начнём с такого примера:

Пример 29. Несложно показать, что все нормирования на $\Bbbk(t) = \Bbbk(\mathbb{P}^1)$, тривиальные на $\Bbbk$ соотвествуют $t - \alpha$ и ∞. Если говорить конкретнее, то

$$f(t) = C \cdot \frac{(t-\alpha_1)^{k_1} \cdot \ldots \cdot (t-\alpha_m)^{k_m}}{(t-\beta_1)^{s_1} \cdot \ldots (t-\beta_n)^{s_n}}$$

и тогда мы имеем

$$\upsilon_{t-\gamma}(f) = \begin{cases} 0, & \gamma \neq \alpha_j, \beta_j \\ k_i & \gamma = \alpha_i \\ s_j, & \gamma = \beta_j \end{cases}, \ \upsilon_\infty = s_1 + \ldots + s_n - k_1 - \ldots - k_m.$$

В частности мы видим, что

$$\forall f \in \Bbbk\big(\mathbb{P}^1\big) \quad \sum_{P\in\mathbb{P}^1} \upsilon_P(f) = 0.$$

Это наблюдение легко обобщить на произвольную неособую проективную кривую X.

Далее пусть X — неособая проективная кривая (и, в дальнейшем всегда так).

Определение 87. *Дивизор на X* — это формальная целочисленная линейная комбинация $\sum_{P\in X} n_P \cdot P$, где $n_P \in \mathbb{Z}$ и почти все из них равны нулю.

Иными словами, группа дивизоров $\operatorname{Div}(X)$ на кривой X — это свободная абелева группа, порожденная точками кривой.

Рассмотрим произвольную рациональную функцию $f \in \Bbbk(X)^*$, тогда в кольце $\mathcal{O}_P$ она представим в виде $f = z_P^{\upsilon_P(f)} \cdot f_0$, где $(z_P) = \mathfrak{m}_P$ — локальный параметр, а $f_0 \in \mathcal{O}_P^*$ (так как кривая неособая и локальное кольцо каждой точки регуляно).

Определение 88. Пусть $f \in \Bbbk(X)^*$ — ненулевая рациональная функция на кривой X. Тогда её *дивизором* называют

$$\operatorname{div}(f) = \sum_{p\in X} \upsilon_p(f) \cdot p$$

А *дивизором нулей* и *дивизором полюсов* называют соотвественно

$$\operatorname{div}(f)_0 = \sum_{p\in X,\ \upsilon_p(x)>0} \upsilon_p(f) \cdot p, \quad \operatorname{div}(f)_\infty = -\sum_{p\in X, \upsilon_p(f)<0} \upsilon_p(f) \cdot p.$$

[19] Уже не обязательно аффинное

Замечание. Нетрудно видеть, что $\operatorname{div}(f)_\infty = \operatorname{div}(1/f)_0$ и $\operatorname{div}(f) = \operatorname{div}(f)_0 - \operatorname{div}(f)_\infty$.

Пример 30. Пусть X — неособая неприводимая проективная кривая, $f \in \Bbbk(X)^*$. Рассмотрим морфизм полей $\Bbbk(t) \to \Bbbk(X)$, $t \mapsto f$. Ему соответствует некоторое доминантное рациональное отображение $X \to \mathbb{P}^1$. Но, мы доказывали, что это отображение будет регулярным во всех точках. Рассмотрим некоторую точку $P \in \mathbb{P}^1$ и $Q_i \in X$ такие, что $Q_i \mapsto P$. Тогда $\upsilon_{Q_i}(f) = e_i \upsilon_P(t) = e_i$. В то же время, степени инерции равны единице (так как поля вычетов алгебраически замкнуты). Тогда по ранее доказанному:

$$\sum_i e_i = [\Bbbk(X) : \Bbbk(f)] = n.$$

Но, с другой стороны, $\{Q_i\} = \{Q \in X \mid \upsilon_Q(f) > 0\}$, то есть дивизор нулей функции f имеет вид

$$\sum \upsilon_{Q_i}(f) \cdot Q_i,$$

откуда мы в частности получаем, что $\deg(\operatorname{div}(f)_0) = [\Bbbk(X) : \Bbbk(f)] = n$.

Пусть X — неособое неприводимое многообразие, $C \subset X$ — неособое подмногообразие коразмерности 1. Тогда мы можем определить локальное кольцо по отношению к C (по аналогии с локальным кольцом точки):

$$\mathcal{O}_C \subset \Bbbk(X), \quad \mathcal{O}_C = \left\{ \frac{f}{g} \mid g|_C \not\equiv 0 \right\}.$$

Тут мы подразумеваем, что g не обращается **тождественно** в 0 на C. Видно, что в случае $C = P$ это определение совпадает с определением локального кольца точки.

Предположим, что X — аффинное многообразие с аффинной алгеброй $A = A(X)$. Тогда подмногообразие C соотвествует некоторому (минимальному) простому идеалу $\mathfrak{p} \subset A$ высоты 1. Тогда $\mathcal{O}_C = A_\mathfrak{p}$ (а тот факт, что знаменатель не обращатся тождественно в 0 на C означает как раз, что мы не попали в идеал $\mathfrak{p}$).

Теперь возьмём $\mathfrak{p} \subset \mathfrak{m} \subset A$, тогда $\mathfrak{m}$ соотвествует какой-то точке C и тогда ясно, что $A_\mathfrak{p}$ получается локализацией кольца $A_\mathfrak{m}$, которое регулярно, так как многообразие неособое. Идеал $\mathfrak{p}A_\mathfrak{m}$ — идеал высоты 1. Регулярное локальное кольцо факториально, а в факториальном локальном кольце простой идеал высоты 1 является главным (как мы уже видели). Значит, $\mathfrak{p}A_\mathfrak{m}$ — главный идеал, тогда $\mathfrak{p}A_\mathfrak{p}$ — главный, а это говорит нам, что кольцо $A_\mathfrak{p}$ является дискретно нормированным.[20]

Определение 89. Пусть X — неособое многообразие. Тогда *группа дивизоров* $\operatorname{Div}(X)$ — свободная абелева группа, образующими которой являются неособые подмногообразия размерности 1.

Пусть $D \in \operatorname{Div}(X)$ — дивизор, $D = \sum_{Z \subset X} n_Z \cdot Z$. Его *носителем* мы будем называть

$$\operatorname{supp} D = \bigcup_{Z \subset X \,:\, n_Z \neq 0} Z.$$

Определение 90. Пусть $f \in \Bbbk(X)^*$. Тогда её *дифизором* мы будем называть

$$\operatorname{div}(f) = \sum_{C \subset X,\ \operatorname{codim} C = 1} \upsilon_C(f) \cdot C$$

где C неприводимо. Дивизоры такого вида мы будем называть *главными*. Нетрудно заметить, что они образуют подгруппу в $\operatorname{Div}(X)$, её мы обозначим через $\operatorname{PDiv}(X)$.

Замечание. Это определение корректно, так как для заданной функции $f \in \Bbbk(X)$ существует лишь конечное число неособых неприводимых подмногообразий C коразмерности таких, что $\upsilon_C(f) > 0$.

Рассмотрим сначала случай, когда X аффинно и $f \in A(X)$. В таком случае, просто по определению, если C не является компонентой $Z(f)$, то $\upsilon_C(f) = 0$. Покажем, что таких C, что $\upsilon_C(f) > 0$ конечное число. Пусть C соотвествует идеалу $\mathfrak{p}$ высоты 1, тогда

$$\upsilon_C(f) > 0 \iff f \in \mathfrak{p}.$$

[20] Формально, тут есть некоторая тонкость, см. Шафаревич.

Рассмотрим $\mathfrak{p}/(f) \subset A/(f)$. заметим, что если $\mathfrak{p}, \mathfrak{q} \trianglelefteq A$, причём $f \in \mathfrak{q}, \mathfrak{p}$ и $\mathfrak{q} \neq \mathfrak{p}$, то $\mathfrak{p}/(f) \neq \mathfrak{q}/(f)$. Тогда нам достаточно доказать, что в $A/(f)$ конечное число минимальных простых идеалов (а это мы знаем).

Если же X всё еще аффинно, но $f \in \Bbbk(X)$, $f = g/h \in A(X)$, то мы видим, что $\upsilon_C(f)$, если C не является компонентой $Z(f)$ или $Z(g)$.

В произвольном случае мы покроем $X = \bigcup U_i$ аффинными (конечным числом) и тогда любое C пересекается хоть с одним из U_i, поэтому $\upsilon_C(f) \neq 0$ только для тех C, которые являются замыканиями таких неприводимых подмногообразий $\widetilde{C} \subset U_i$, что $\upsilon_{\widetilde{C}}(f) \neq 0$. Так как таких U_i конечно, а также $\widetilde{C}$ конечно, определение корректно.

Определение 91. *Группой классов дивизоров* мы будем называть группу $\operatorname{Cl}(X) = \operatorname{Div}(X)/\operatorname{PDiv}(X)$.

Определение 92. Пусть X — неособая проективная кривая, а $L \in \operatorname{Div}(X)$. *Степенью* $\deg L$ дивизора L называется сумма его кратностей.

Предложение 41. *Степень главного дивизора равна нулю, то есть* $\deg(\operatorname{div} f) = 0$.

Доказательство. Поле рациональных функций $\Bbbk(X)$ — это конечно порожденное поле над $\Bbbk$ степени трансцендентности 1. Рассмотрим подполе $\Bbbk(f) \subset \Bbbk(X)$, тогда $\Bbbk(X)/\Bbbk(f)$ — конечное расширение полей. Более того, оно соответствует морфизму

$$X \to \mathbb{P}^1, \quad f \mapsto t \rightsquigarrow \Bbbk(\mathbb{P}^1) = \Bbbk(t) \to \Bbbk(X).$$

Тогда, как мы обсуждали выше

$$\deg(\operatorname{div}(f)_0) = [\Bbbk(X) : \Bbbk(f)], \quad \deg(\operatorname{div}(f)_\infty) = \deg(\operatorname{div}(1/f)_0) = [\Bbbk(X) : \Bbbk(1/f)] = [\Bbbk(X) : \Bbbk(f)],$$

так как $\Bbbk(f) = \Bbbk(1/f)$. Тогда мы получили, что

$$\deg(\operatorname{div}(f)) = \deg(\operatorname{div}(f)_0) - \deg(\operatorname{div}(f)_\infty) = 0.$$

□

Определение 93. Пусть Z — неприводимое неособое подмногообразие в X коразмерности 1. Тогда ему соответствует дивизор $1 \cdot Z$. *Простыми* мы будем называть дивизоры такого вида.

Пусть $U \subset X$ — открытое подмножество, $Z = X \setminus U$. Тогда мы можем определить отображение

$$\operatorname{Div}(X) \to \operatorname{Div}(U).$$

Зададим его на образующих: пусть $T \subset X$ — простой дивизор, тогда если $T \cap U = \varnothing$, отправим его в 0, а если $T \cap U \neq \varnothing$, то $T \cap U$ — простой дивизор в U и мы отправим T в $T \cap U$. Отметим также, что с главными дивизорами при этом отображении происходит также понятная вещь:

$$\operatorname{div}(f) \mapsto \operatorname{div}(f|_U).$$

Значит, мы получили корректно определённое отображение $\operatorname{Cl}(X) \to \operatorname{Cl}(U)$. Заметим теперь, что так как отображение $\operatorname{Div}(X) \twoheadrightarrow \operatorname{Div}(U)$ сюръективно, отображение $\operatorname{Cl}(X) \twoheadrightarrow \operatorname{Cl}(U)$ также сюръективно. Вычислим его ядро. Предположим, что $\sum n_i Z_i \in \operatorname{Ker}(\operatorname{Cl}(X) \to \operatorname{Cl}(U))$, это означает, что он перешел в $\operatorname{div}(f)$ для некоторой f. Тогда $\sum n_i Z_i - \operatorname{div}(f) \mapsto 0$. Но, если $Z_1 \neq Z_2$, то $Z_1 \cap U \neq Z_2 \cap U$ (если $Z_i \cap U \neq \varnothing$ для $i = 1, 2$). Отсюда следует, что ядро состоит из тех неприводимых подмногообразий коразмерности 1, которые не пересекаются с U. А это в точности компоненты $Z = X \setminus U$ коразмерности 1 (в X).

Таким образом, $\operatorname{Ker}(\operatorname{Cl}(X) \twoheadrightarrow \operatorname{Cl}(U)) = \mathbb{Z}^m$, где m — количество неприводимых компонент Z коразмерности 1 в X. В частности, у нас есть точная последовательность

$$\mathbb{Z}^m \to \operatorname{Cl}(X) \to \operatorname{Cl}(U) \to 0.$$

Пример 31. Это наблюдение уже позволяет вычислить группу классов дивизоров для чего-нибудь.

1. Рассмотрим $X = \mathbb{A}^n$ и простой дивизор $T \subset X$. По одной из доказанных ранее теорем любое неприводимое подмногообразие коразмерности 1 в $\mathbb{A}^n$ задаётся одним уравнением: $T = Z(f)$, но тогда $T = \operatorname{div}(f)$ и T главный. Значит, все простые дивизоры главные, откуда следуте, что $\operatorname{Cl}(\mathbb{A}^n) = 0$.
2. Теперь рассмотрим $X = \mathbb{P}^n$ и $U = \mathbb{A}^n$, Тогда, так как $X \setminus U = \mathbb{P}^{n-1}$, мы получаем

$$\mathbb{Z} \hookrightarrow \operatorname{Cl} \mathbb{P}^n \to \operatorname{Cl} \mathbb{A}^n \to 0,$$

а так как левое отображение инъективно,

$$0 \to \mathbb{Z} \to \operatorname{Cl} \mathbb{P}^n \to \underbrace{\operatorname{Cl} \mathbb{A}^n}_{=0} \to 0,$$

мы имеем $\operatorname{Cl} \mathbb{P}^n \cong \mathbb{Z}$.

Определение 94. Дивизор называется *эффективным*, если все его кратности неотрицательны. В таком случае мы пишем $D \geq 0$.

Замечание. Заметим, что если f регулярна, то $\operatorname{div}(f) \geq 0$.

Оказывается, верно и обратное.

Еще небольшой кусок появится тут несколько позже

4.2 Дивизоры форм

Пусть $X \subset \mathbb{P}^N$ — многообразие, F — форма (многочлен). Определим дивизор формы F.

Рассмотрим неприводимое подмногообразие $C \subset X$ коразмерности 1. Выберем форму G той же степени, что и F так, чтоб $G|_C \neq 0$ (т.е. не обращается в 0 полностью). Рассмотрим функцию F/G (так как это частное двух форм, это функция) и положим

$$\upsilon_C(F) \stackrel{\text{def}}{=} \upsilon_C\left(\frac{F}{G}\right).$$

Замечание. Покажем, что это определение корректно. Возьмём две формы G_1 и G_2, удовлетворяющие этим условиям, тогда

$$\upsilon_C\left(\frac{F}{G_2}\right) = \upsilon_C\left(\frac{F}{G_1}\right) + \upsilon_C\left(\frac{G_1}{G_2}\right), \text{ но } \upsilon_C\left(\frac{G_1}{G_2}\right) = 0,$$

откуда мы получаем нужное.

Тогда определим *дивизор формы* F как

$$\operatorname{div}(F) = \sum_{C \subset X} \upsilon_C(F) \cdot C,$$

где сумма как и ранее берётся по всем неприводимым подмногообразиям коразмерности 1.

Пусть теперь X кривая. Тогда мы можем определить *степень дивизора* формы F следующим образом:

$$\deg \operatorname{div}(F) = \sum_{C \subset X} \upsilon_C(F).$$

Рассмотрим теперь формы F_1, F_2 такие, что $\deg F_1 = \deg F_2$. У нас есть очевидное равенство

$$\operatorname{div}(F_1) = \operatorname{div}(F_2) + \operatorname{div}\left(\frac{F_1}{F_2}\right),$$

и применяя степень мы получаем, что

$$\deg \operatorname{div}(F_1) = \deg \operatorname{div}(F_2).$$

Для иллюстрации вычислим дивизор **линейной формы на эллиптической кривой**.

Рассмотрим эллиптическую кривую

$$y^2 = x^3 + ax + b, \quad a, b \neq 0,\ 4a^3 + 27b^3 \neq 0.$$

Рассмотрим точку $P(x_1, y_1) \in C$ и вычислим локальный параметр для кольца $\mathcal{O}_{P_1}$ (т.е. образующую максимального идеала $\mathfrak{m}_P$). Рассмотрим два случая

1. Пусть $y_1 \neq 0$. Тогда покажем, что $x - x_1$ — локальный параметр для кольца $\mathcal{O}_P$. Ясно, что $\mathfrak{m}_P = (x - x_1, y - y_1)$. Попробуем получить одну образующую вместо двух.

$$\begin{cases} y^2 = x^3 + ax + b \\ y_1^2 = x_1^3 + ax_1 + b \end{cases} \implies (y - y_1)(y + y_1) = (x - x_1)(x^2 + xx_1 + x_1^2 + a)$$

$$y - y_1 = \frac{(x - x_1)(x^2 + xx_1 + x_1^2 + a)}{y + y_1}.$$

   Тогда достаточно показать, что $y + y_1 \notin \mathfrak{m}_P$. Действительно, если $y + y_1 \in \mathfrak{m}_P$, но тогда $y_1 \in \mathfrak{m}_P$, а это возможно тогда и только тогда, когда $y_1 = 0$ (а мы предположили, что это не так).
2. Пусть $y_1 = 0$, тогда локальным параметром будет y.

$$x_1^3 + ax_1 + b = 0 \implies y^2 = (x - x_1)(x^2 + xx_1 + x_1^2 + a) \implies x - x_1 = \frac{y^2}{x^2 + xx_1 + x_1^2 + a}.$$

   Покажем, что $x^2 + xx_1 + x_1^2 + a \notin \mathfrak{m}_P$.

$$x^2 + xx_1 + x_1^2 + a \equiv 3x_1^2 + a \pmod{\mathfrak{m}_P}.$$

   Тогда $3x_1^2 + a = 0,\ y_1 = 0$. Но это противоречит тому, что точка $P(x_1, y_1)$ неособая[21].

Теперь, зная локальный параметр, мы можем считать нормирование от любой рациональной функции.

Вычислим степень дивизора линейной формы. Самое простое, что можно сделать с эллиптической кривой — это пересечь её с какой-то прямой. Пусть L — это прямая в $\mathbb{A}^2$. Проективизуем всё, добавляя бесконечно удалённую точку:

$$X\colon y^2 z = x^3 + axz^2 + bz^3.$$

Рассмотрим прямую $L\colon z = 0$. Видно, что $X \cap L$ состоит из одной (бесконечно удалённой) точки. С другой стороны, когда мы пересекаем прямую с эллиптической кривой, точки лежащие в пересечении — корни многочлена третьей степени (так что вообще говоря их должно быть 3). Тут дело всё в том, что у этой бесконечно удалённой точки кратность 3: пусть $P_0 = (0 : 1 : 0)$. Покажем, что

$$\operatorname{div}(L) = 3P_0.$$

Деля на y^3, перейдём в аффинные координаты:

$$\frac{z}{y} = \left(\frac{x}{y}\right)^3 + a\frac{x}{y}\left(\frac{z}{y}\right)^2 + b\left(\frac{z}{y}\right)^3.$$

Обозначим $x/y = x_1,\ z/y = z_1$. Тогда

$$z_1 = x_1^3 + ax_1 z_1^2 + bz_1^3,$$

а P_0 имеет координаты $(0, 0)$. Перепишем это уравнение в немного другом виде:

$$z_1 - bz_1^3 = x_1^3 + ax_1 z_1^2 \implies z_1 = \frac{x_1^3 + ax_1 z_1^2}{1 - bz_1^2}.$$

Так как $z_1 \in \mathfrak{m}_{P_0}$, знаменатель обратим, тогда, так как $\mathfrak{m}_{P_0} = (x_1)$

$$\upsilon_{P_0}(x_1^3) = 3 \implies \upsilon_{P_0}(z_1) \geq 3,$$

но, в то же время, видно, что равенство достигается. Итак,

$$\operatorname{div}(L) = 3P_0.$$

[21] Это проверяется вручную

Это подводит нас гипотезе о том, что дивизор любой линейной формы имеет степень 3.

Действительно, рассмотрим линейную форму $L\colon y = \alpha x + \beta$, тогда

$$x^3 + (ax + b) - (\alpha x + \beta)^2 = 0.$$

Это уравнение имеет три корня (возможно, с кратностью) и эти корни определяют точки пересечения прямой L с эллиптической кривой. Кратности корней будут соответствовать как раз кратностям точек пересечения.

$$x^3 + (ax + b) - (\alpha x + \beta)^2 = (x - x_1)(x - x_2)(x - x_3).$$

Тогда у нас три точки пересечения: $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3 = (x_3, y_3)$. Тогда

$$\operatorname{div}(L) = i_1 P_1 + i_2 P_2 + i_3 P_3, \text{ где } i_j - \text{кратности соответствующих корней.}$$

Упражнение. Докажите это.

Отметим, что мы рассматривали не вертикальную прямую. Вертикальная прямая будет пересекать эллиптическую кривую в двух конечных и бесконечно удалённой точке:

$$\begin{cases} x = x_1 z \\ y^2 z = x^3 + axz^2 + bz^3 \end{cases}$$

и очевидно, что $(0 : 1 : 0)$ лежит в пересечении. Также отметим, что вместо прямой $z = 0$ мы могли бы брать горизонтальную прямую $y = 0$ (и соответственно линейную форму y) и рассматривать её пересечение с такой кривой. В этом случае, когда

$$\operatorname{div}(y) = P_1 + P_2 + P_3$$

4.3 Групповой закон для точек эллиптической кривой

Пусть X — неособая проективная кривая. Мы знаем, что в этом случае любой главный дивизор имеет степень 0, а значит, мы можем рассмотреть отображение

$$\operatorname{Cl}(X) \xrightarrow{\deg} \mathbb{Z} \to 0$$

и, обозначая его ядро через $\operatorname{Cl}^0(X)$ написать короткую точную последовательность

$$0 \to \operatorname{Cl}^0(X) \to \operatorname{Cl}(X) \xrightarrow{\deg} \mathbb{Z} \to 0$$

Пусть X — эллиптическая кривая $y^2 z = x^3 + axz^2 + bz^3$, рассмотрим отображение

$$\varphi\colon X \to \operatorname{Cl}^0(X), \quad P \mapsto [P] - [P_0],$$

где P_0 — это бесконечно удалённая точка. Это поможет нам определить закон сложения точек на эллиптической кривой. Вообще говоря, точки на эллиптической кривой можно складывать так: рассмотрим $P_1, P_2 \in X$, рассмотрим прямую, проходящую через них. Эта прямая пересечёт эллиптическую кривую в третьей точке, её мы симметрично отразим относительно оси абсцисс и объявим результатом сложения то, что получилось. Минус этой конструкции в том, что ассоциативность проверить весьма трудно. В нашем же случае все свойства групповых операций будут унаследованы с группы $\operatorname{Cl}^0(X)$.

Теорема 68. *Отображение $\varphi\colon X \to \operatorname{Cl}^0(X),\ P \mapsto [P] - [P_0]$ взаимно однозначно.*

Доказательство. Докажем сначала вот такую лемму:

Лемма 44. Пусть X — неособая проективная кривая, на которой есть две различные точки $P \neq Q$ такие, что $P - Q$ — главный дивизор. Тогда $X = \mathbb{P}^1$.

Доказательство. Пусть $P - Q = \operatorname{div}(f)$. Но тогда $P = \operatorname{div}(f)_0,\ \operatorname{div}(f)_\infty = Q$. Рассмотрим отображение $X \to \mathbb{P}^1$, которое даёт нам расширение полей $t \mapsto f, \Bbbk(X)/\Bbbk(f)$ и при этом $[\Bbbk(X) : \Bbbk(f)] = \deg \operatorname{div}(f)_0 = 1$. Но тогда $\Bbbk(X) = \Bbbk(f) = \Bbbk(t)$. □

Так как мы доказывали, что эллиптическая кривая не изоморфна $\mathbb{P}^1$, из этого следует инъективность отображения.

Инъективность. Предположим, что $[P] - [P_0] = [Q] - [P_0]$ в $\mathrm{Cl}^0(X)$, тогда $[P] - [Q] = 0$, то есть $P - Q -$ главный дивизор. Тогда по доказанной лемме $X \cong \mathbb{P}^1$ и мы пришли к противоречию.

Сюръективность. Рассмотрим $\sum n_i[P_i] \in \mathrm{Cl}^0(X)$. Так как сумма коэффициентов равна нулю,

$$\sum n_i[P_i] = \sum n_i([P_i] - [P_0])$$

Теперь надо доказать, что для любых $n_i \in \mathbb{Z}$

$$\sum n_i([P_i] - [P_0]) = [S] - [P_0] \in \mathrm{Cl}^0(X)$$

для некоторой $S \in X$. Рассмотрим сначала случай, чтогда все $n_i > 0$. Рассмотрим

$$P_1 - P_0 + P_2 - P_0 \tag{2.5}$$

Теперь заметим, что если мы рассмотрим две произвольные точки P_1 и P_2, проведём через них прямую и получим точку $P_3 \in X$, то $P_1 + P_2 + P_3$ является дивизором линейной формы, а тогда, так как формы одинаковой степени линейно эквивалены (их дивизоры отличаются на дивизор функции),

$$P_1 + P_2 + P_3 = 3P_0 \text{ в } \mathrm{Cl}(X)$$

Рассмотрим точку P_3', симметричную относительно оси абсцисс точке P_3. Проведём вертикальную прямую через P_3 и P_3', она пересечёт X еще в бесконечно удалённой точке отсюда получим:

$$P_3 + P_3' + P_0 = 3P_0 \text{ в } \mathrm{Cl}(X).$$

Из двух этих равенств мы получаем, что (2.5) мы можем переписать вот так:

$$P_1 - P_0 + P_2 - P_0 = P_3' - P_0 \in \mathrm{Cl}(x).$$

Значит, сумму $\sum n_i([P_i] - [P_0])$ мы можем свести к одному равенству. Если же не все коэффициенты положительны, то их мы можем поменять искусственно:

$$P_i - P_0 = -(P_i' - P_0) \in \mathrm{Cl}(X).$$

Итак, мы доказали сюръективность. □

5. Комплексная алгебраическая геометрия

5.1 Комплексные многообразия

Определение 95. *Комплексным многообразием* M называется гладкое многообразие, допускающее такое открытое покрытие $\{U_\alpha\}_{\alpha\in I}$ и такие координатные отображения $\varphi_\alpha\colon U_\alpha \to \mathbb{C}^n$, что все функции перехода $\varphi_\alpha \circ \varphi_\beta^{-1}$ голоморфны на $\varphi_\beta(U_\alpha \cap U_\beta)$.

Функция f на открытом подмножестве $U \subset M$ называется *голоморфной*, если $\forall \alpha \in I$ функция $f \circ \varphi_\alpha^{-1}$ голоморфна в $\varphi_\alpha(U_\alpha \cap U)$.

Набор $z = (z_1, \dots, z_n)$ функций на $U \subset M$ называется *голоморфной системой координат*, если $\varphi_\alpha \circ z^{-1}$ и $z \circ \varphi_\alpha^{-1}$ голоморфны на $z(U \cap U_\alpha)$ и $\varphi_\alpha(U \cap U_\alpha)$ для всех α.

Отображение $f\colon M \to N$, где M и N — комплексные многообразия, называется *голоморфным*, если в голоморфных локальных координатах оно задаётся голоморфными функциями.

Пример 32 (Примеры комплексных многообразий)**.** Приведём какие-нибудь примеры комплексных многообразий:

1. Одномерное комплексное многообразие называют **римановой поверхностью**.
2. $P\mathbb{C}^n = (\mathbb{C}^{n+1} \setminus \{0\})/\{z \sim \lambda z\} = \mathbb{P}^n$ — комплексное проективное пространство. Это пространство компактно, так как есть непрерывное сюръективное отображение $S^n \subset \mathbb{C}^{n+1} \to \mathbb{P}^n$.
3. Пусть $\Lambda = \mathbb{Z}^k \subset \mathbb{C}^n$ — дискретная решётка. Факторгруппа $\mathbb{C}^n/\Lambda$ обладает структурой комплексного многообразия, которую индуцирует проекция $\pi\colon \mathbb{C}^n \to \mathbb{C}^n/\Lambda$. Это многообразие компактно тогда и только тогда, когда $k = 2n$ и в этом случае $\mathbb{C}^n/\Lambda$ называется **комплексным тором**.
4. Тут был еще пример, что при неразветвлённом накрытии структура комплексного многообразия наследуется, но я хз, что такое разветвлённое накрытие.

Касательное пространство к комплексному многообразию.

Пусть M — комплексное многообразие, $p \in M$, а $z = (z_1, \dots, z_n)$ — система голоморфных координат в окрестности p. В случае комплексного многообразия имеются три различных понятия *касательного пространства* к M в точке $p \in M$.

1. Рассмотрим M, как вещественное $2n$-многообразие. Тогда $T_{\mathbb{R},p}M$ — пространство $\mathbb{R}$-линейных дифференцирований кольца $C^\infty(M, \mathbb{R})$ (с носителем в окрестности p). Если мы представим голоморфные координаты в виде $z_j = x_j + iy_j$, то $T_{\mathbb{R},p}M$ будет иметь базис $\{\frac{\partial}{\partial x_j}, \frac{\partial}{\partial y_j}\}$, как векторное пространство над $\mathbb{R}$.
2. Пространство $T_{\mathbb{R},p}M$ можно комплексифицировать при помощи расширения скаляров, то есть рассмотреть
$$T_{\mathbb{C},p}M \stackrel{\text{def}}{=} T_{\mathbb{R},p}M \otimes_{\mathbb{R}} \mathbb{C}.$$
$T_{\mathbb{C},p}M$ называют *комплексифицированным касательным пространством* к M в точке p. Его можно реализовать, как пространство $\mathbb{C}$-линейных дифференцирований кольца $C^\infty(M, \mathbb{C})$ (опять же, фукнции с носителем в окрестности p). Соотвественно, там можно выбрать базис $\{\frac{\partial}{\partial x_j}, \frac{\partial}{\partial y_j}\}$, а при замене базиса на комлпексные обозначения
$$\frac{\partial}{\partial z_j} = \frac{1}{2}\left(\frac{\partial}{\partial x_j} - i\frac{\partial}{\partial y_j}\right),\ \frac{\partial}{\partial \overline{z_j}} = \frac{1}{2}\left(\frac{\partial}{\partial x_j} + i\frac{\partial}{\partial y_j}\right).$$
«более стандартный» базис $\{\frac{\partial}{\partial z_j}, \frac{\partial}{\partial \overline{z_j}}\}$.
3. Подпространство $T'_pM = \operatorname{span}\{\frac{\partial}{\partial z_j}\} \le T_{\mathbb{C},p}M$ называется *голоморфным касательным пространством* к M в точке p. Оно может быть реализовано, как подпространство в $T_{\mathbb{C},p}M$, состоящее из дифференцирований, обращающихся в ноль на антиголоморфных функциях (таких f, что $\overline{f}$ — голоморфна). Соответственно, подпространство $T''_pM = \operatorname{span}\{\frac{\partial}{\partial \overline{z_j}}\}$ называется *антиголоморфным касательным пространством* к M в точке p. Ясно, что
$$T_{\mathbb{C},p}M = T'_pM \oplus T''_pM.$$

Заметим, что для комплексных многообразий M, N любое $f \in C^\infty(M, N)$ индуцирует линейное отображение

$$f_*\colon T_{\mathbb{R},p}M \to T_{\mathbb{R},f(p)}N$$

а значит и линейное отображение

$$f_*\colon T_{\mathbb{C},p}M \to T_{\mathbb{C},f(p)}N,$$

но не отображение $T'_pM \to T'_{f'(p)}N$ для всех $p \in M$.

На самом деле, отображение $f\colon M \to N$ голоморфно тогда и только тогда, когда

$$f_*(T'_pM) \subset T'_{f(p)}N \quad \forall p \in M.$$

То есть, когда голоморфное касательное пространство отображается в голоморфное.

Заметим, что также, поскольку $T_{\mathbb{C},p}M = T_{\mathbb{R},p}M \otimes \mathbb{C}$, операция сопряжения, переводящая

$$\frac{\partial}{\partial z_j} \mapsto \frac{\partial}{\partial \overline{z_j}}$$

корректно определена на $T_{\mathbb{C},p}M$ и, как нетрудно заметить, $T''_pM = \overline{T'_pM}$. Отсюда следует, что проекция

$$T_{\mathbb{R},p}M \to T_{\mathbb{C},p}M \to T'_pM$$

есть $\mathbb{R}$-линейный изоморфизм.

Это обстоятельство позволяет заниматься геометрией исключительно в голоморфном касательном пространстве.

Пример 33. Пусть $z(t)\colon [0,1] \to \mathbb{C}$ — гладкая кривая. Тогда $z(t) = x(t) + iy(t)$ и в качестве касательной мы можем взять

$$x'(t)\frac{\partial}{\partial x} + y'(t)\frac{\partial}{\partial y} \text{ в } T_{\mathbb{R}}\mathbb{C}, \text{ либо } z'(t)\frac{\partial}{\partial z} \text{ в } T'\mathbb{C}.$$

Определение 96. Пусть теперь M, N — комплексные многообразия, $z = (z_1, \ldots, z_n)$ — голомрфные координаты в окрестности точки $p \in M$, а $(w_1, \ldots, w_n)$ — голоморфные координаты в окрестности точки $q = f(p)$, где $f\colon M \to N$ — голоморфное отображение. В связи с различными понятиями касательных пространств, мы имеем и различные понятия *якобиана* f.

1. Пусть $z_j = x_j + iy_j,\ w_k = u_k + iv_k$. Тогда в базисах $\{\frac{\partial}{\partial x_j}, \frac{\partial}{\partial y_j}\}$ и $\{\frac{\partial}{\partial u_k}, \frac{\partial}{\partial v_k}\}$ пространств $T_{\mathbb{R},p}M$ и $T_{\mathbb{R},q}N$ линейное отображение f_* задаётся $2m \times 2n$-матрицей

$$\mathcal{J}_{\mathbb{R}}(f) = \begin{pmatrix} \frac{\partial u_k}{\partial x_j} & \frac{\partial u_k}{\partial y_j} \\ \frac{\partial v_k}{\partial x_j} & \frac{\partial v_k}{\partial y_j} \end{pmatrix}.$$

   В базисах $\{\frac{\partial}{\partial z_j}, \frac{\partial}{\partial \overline{z_j}}\}$ и $\{\frac{\partial}{\partial w_j}, \frac{\partial}{\partial \overline{w_k}}\}$ пространств $T_{\mathbb{C},p}M$ и $T_{\mathbb{C},q}N$ отображение f_* задаётся матрицей

$$\mathcal{J}_{\mathbb{C}}(f) = \begin{pmatrix} \mathcal{J}(f) & 0 \\ 0 & \overline{\mathcal{J}(f)} \end{pmatrix}, \text{ где } \mathcal{J}(f) = \left(\frac{\partial w_k}{\partial z_j}\right)_{k,j}.$$

Замечание. В частности, отметим, что $\operatorname{rank}\mathcal{J}_{\mathbb{R}}(f) = 2\operatorname{rank}\mathcal{J}(f)$ и в случае $m = n$

$$\det\mathcal{J}_{\mathbb{R}}(f) = \det\mathcal{J}(f)\det\overline{\mathcal{J}(f)} = |\det\mathcal{J}(f)|^2 \geq 0,$$

то есть голоморфные отображения **сохраняют ориентацию**.

Мы будем считать, что пространство $\mathbb{C}^n$ естественно ориентированно $2n$-формой

$$\left(\frac{i}{2}\right)^n (\mathrm{d}z_1 \wedge \mathrm{d}\overline{z_1}) \wedge (\mathrm{d}z_2 \wedge \mathrm{d}\overline{z_2}) \wedge \ldots \wedge (\mathrm{d}z_n \wedge \mathrm{d}\overline{z_n}) = \mathrm{d}x_1 \wedge \mathrm{d}y_1 \wedge \ldots \wedge \mathrm{d}x_n \wedge \mathrm{d}y_n.$$

Ясно, что если $\varphi_\alpha\colon U_\alpha \to \mathbb{C}^n$ и $\varphi_\beta\colon U_\beta \to \mathbb{C}^n$ — голоморфные координатные отображения на комплексном многообразии M, то прообразы при φ_α и φ_β естественной ориентации на $\mathbb{C}^n$ согласованы на $U_\alpha \cap U_\beta$.

Соотвественно, любое комплексное многообразие **имеет естественную ориентацию**, которая сохраняется при голоморфных отображениях.

5.2 Векторные рассоления

Определение 97. Пусть M — гладкое многообразие. Комплексным C^∞-расслоением на M называется семейство $\{E_X\}_{x\in M}$ комплексных векторных пространств E_x, параметризованных точками многообразия M, со структурой C^∞ многообразия на

$$E = \bigcup_{x\in M} E_x$$

такой, что выполняются следующие условия:

1. отображение проектирования $\pi\colon E \to M$, переводящее E_x в x принадлежит классу C^∞.
2. $\forall x_0 \in M$ найдутся открытое множество $U \subset M\colon U \ni x_0$ и диффеоморфизм

   $$\varphi_U\colon \pi^{-1}(U) \to U \times \mathbb{C}^k,$$

   который отображает вектоорное пространство E_x изоморфно на $\{x\} \times \mathbb{C}^k$ для всех $x \in U$. Такое отображение φ_U называется *тривиализацей.*

Размерность слоёв E_x расслоения E называется *рангом* E. Расслоение ранга 1 называется *линейным.*

Замечание. Для любой пары тривиализаций φ_U, φ_V *отображение* перехода $g_{uv}(x) = (\varphi_U \circ \varphi_V^{-1})|_{\{x\}\times\mathbb{C}^k\}}\colon U \cap V \to \mathrm{GL}(k)$ принадлежит классу C^∞. Кроме того, они удовлетворяют тождествам:

$$g_{UV}(x)\cdot g_{VU}(x) = I \quad \forall x \in U \cap V$$

$$g_{UV}(x) g_{VW}(X)\cdot g_{WU}(x) = I \quad \forall x \in U \cap V \cap W$$

Обратно, если задано открытое покрытие $\mathcal{U} = \{U_\alpha\}$ многообразия M и C^∞ отображения $g_{\alpha\beta}\colon U_\alpha \cap U_\beta \to \mathrm{GL}(k)$, удовлетворяющие тождествам выше, то найдётся единственное комплексное векторное расслоение $E \to M$ с такими функциями перехода.

Действительно, мы можем положить $E = \bigsqcup_\alpha \big(U_\alpha \times C^k\big)$, в котором мы отождествляем точки $(x,\lambda) \in U_\beta \times \mathbb{C}^k$ и $(x, \lambda g_{\alpha\beta}(x))$, а структура многообразия на E определяется вложениями $U_\alpha \times \mathbb{C}^k \to E$.

Обычно операции над векторными пространствами переносятся и на векторные расслоения:

- Если $E \to M$ — векторное расслоение, то можно определить двойственное раслоение $E^* \to M$, взяв в качесвте слоёв $E_x^* \stackrel{\text{def}}{=} (E_x)^*$. Тривиализации $\varphi_u\colon E_U \to U \times \mathbb{C}^k$ (где $E_u = \pi^{-1}(U)$) индуцируют отображения

  $$\varphi_U^*\colon E_U^* \to U \times (\mathbb{C}^k)^* \cong U \times \mathbb{C}^k,$$

  которые наделяют E^* структурой многообразия. Эту конструкцию проще получить при помощи функций перехода: $E^* \to M$ будет векторным расслоением с функциями перехода $j_{\alpha\beta}(x) =^i g_{\alpha\beta}(x)^{-1}$.
- Пусть $E \to M$ и $F \to M$ — комплексные векторные расслоения рангов k и ℓ с функциями перехода $\{g_{\alpha\beta}\}$ и $\{h_{\alpha\beta}\}$. Тогда мы можем определить $E \oplus F$, как векторное расслоение, заданное функциями перехода

  $$j_{\alpha\beta} = \begin{pmatrix} g_{\alpha\beta}(x) & 0 \\ 0 & h_{\alpha\beta}(x)\end{pmatrix} \in \mathrm{GL}(\mathbb{C}^k \oplus \mathbb{C}^\ell).$$
- Также мы можем определить расслоение $E \otimes F$, как расслоение, заданное функциями перехода

  $$j_{\alpha\beta}(x) = g_{\alpha\beta}(x) \otimes h_{\alpha\beta}(x) \in \mathrm{GL}\Big(\mathbb{C}^k \otimes \mathbb{C}^\ell\Big).$$
- Аналогично, $\Lambda^r E$ — векторное расслоение, заданное формулами

  $$j_{\alpha\beta} = \Lambda^r(g_{\alpha\beta}(x)) \in \mathrm{GL}\Big(\Lambda^r\mathbb{C}^k\Big).$$

  В частности, $\Lambda^k E$ будет линейным расслоением с функциями перехода

  $$j_{\alpha\beta}(x) = \det g_{\alpha\beta}(x) \in \mathrm{GL}(1,\mathbb{C}) = \mathbb{C}^*.$$

Для векторных расслоений можно также определить подрасслоения и прообразы.[22]

Определение 98. Веторные расслоения $E \to M$ и $F \to M$ *изоморфны*, если существует отображение $f\colon E \to F$ такое, что $f_x\colon E_x \to F_x$ — изоморфизмы $\forall x \in M$.

Векторное расслоение $E \to M$ называется *тривиальным*, если оно изоморфно $M \times \mathbb{C}^k$.

Сечением σ векторного расслоения $E \xrightarrow{\pi} M$ над $U \subset M$ называется C^∞ отображение

$$\sigma\colon U \to E\colon \sigma(x) \in E_x \ \forall x \in U.$$

Реперо́м для E над $U \subset M$ называется набор $\sigma_1, \dots, \sigma_k$ сечений E над U таких, что $(\sigma_1(x), \dots, \sigma_k(x))$ является базисом пространства $E_x \ \forall x \in U$.

Репер для E над U, по существу, то же самое, что тривиализация расслоения E над U: при заданной тривиализации $\varphi_U\colon E_U \to U \times \mathbb{C}^k$, то сечения $\sigma_i(x) = \varphi_U^{-1}(x, e_i)$ образуют базис. И обратно, если задан репер $\sigma_1, \dots, \sigma_k$, то можно определить тривиализацию $\varphi_U(\lambda) = (x, (\lambda_1, \dots, \lambda_k))$ для $\lambda = \sum \lambda_i \sigma_i(x)$ в E_x.

Заметим, что при заданной тривиализации φ_U расслоения E над U любое его сечение σ можно единственным образом представить, как векторзначную C^∞-функцию $f = (f_1, \dots, f_k)$, раскладывая $\sigma(x)$ по базису:

$$\sigma(x) = \sum f_i(x) \sigma_U^{-1}(x, e_i).$$

Если же φ_V — тривиализация расслоения E над V и $f' = (f'_1, \dots, f'_k)$ — соотвествуующие представления $\sigma|_{U \cap V}$, то

$$\sum f_i(x) \varphi_U^{-1}(x, e_i) = \sum f'_i(x) \varphi_V^{-1}(x, e_i),$$

так что

$$\sum f_i(x) e_i = \sum f'_i(x) \varphi_U \varphi_V^{-1}(x, e_i) \implies f = g_{UV} f'.$$

Таким образом, при заданных тривиализациях

$$\{\varphi_\alpha\colon E_{U_\alpha} \to U_\alpha \times \mathbb{C}^k\}$$

сечения расслоения E над $\bigcup U_\alpha$ в точности соотвествуют наборам

$$\{f_\alpha = (f_{\alpha_1}, \dots, f_{\alpha_k})\}_\alpha$$

векторзначных C^∞ функций, удовлетворяющих $f_\alpha = g_{\alpha\beta} f_\beta$.

Пример 34 (Векторные расслоения)**.** Рассмотрим некоторые базовые примеры векторных расслоений:

1. **Касательные и кокасательные расслоения:**
   Комплексным касательным расслоением к комплексному многообразию M мы будем называть
   $$TM = \bigsqcup_{z \in M} T_Z M, \text{ где}$$
   $T_z M$ — комплексное касательное пространство к M в точке x. В расслоении TM есть подрасслоения $T'M$ и $T''M$ определяющиеся естественным образом.
2. **Дифференциальные формы:**

   Определение 99. *Дифференциальной формой* степени k называется сечение расслоения $\Lambda^k(TM)^*$. Расслоение комплексных дифференциальных форма степени k мы будет обозначать $\Omega^k_{\mathbb{C}}(M)$ или $\Omega^k_{\mathbb{C},M}$.

   Пусть M — вещественное многообразие. Тогда легко видеть, что если $f \in C^{k-1}(M)$, то $\mathrm{d}f$ — C^{k-1}-гладкое сечение расслоения $\Omega^1_{\mathbb{R}}(M)$. Кроме того, нетрудно видеть, что если $x_1, \dots, x_n$ — локальные координаты в карте $U \subset M$, то k-формы $\mathrm{d}x_I = \mathrm{d}x_1 \wedge \ldots \wedge \mathrm{d}x_{i_k}$, $1 \le i_1 \le \ldots \le i_k \le n$ образуют базис слоя $\Omega^k_{\mathbb{R}}(X)$ в каждой точке откртого множества U. В самом деле, локальные координаты $x_1, \dots, x_n$ задают локальную тривиализацию каательного расслоения TM: соотвествующий локальный базис в слое задаётся в каждой точке дифференцированиями $\left.\frac{\partial}{\partial x_i}\right|_x$. Тогда 1-формы $\mathrm{d}x_i$ образуют двойственный базис в расслоении $\Omega^1_{\mathbb{R}}(X)$.

[22] но делать этого мы пока что не будем.

5.3 Подмногообразия и аналитические подмножества

Докажем теперь несколько классических теорем для случая комплексных многообразий.

Теорема 69 (Об обратном отображении). *Пусть U, V — открытые подмножества в $\mathbb{C}^n$, $0 \in U$ и $f\colon U \to V$ — такое голоморфное отображение, что матрица $\mathcal{J}(f) = (\partial f_i/\partial z_j)$ невырождена в 0.*

Тогда отображение f взаимно однозначно в окрестности точки 0 и обратное отображение f^{-1} голоморфно в некоторой окрестности $f(0)$.

Доказательство. Как мы уже отмечали в 5.1, $|\det \mathcal{J}_{\mathbb{R}}(f)| = |\det \mathcal{J}(f)|^2 \neq 0$ в точке 0, а значит, по обычной теореме об обратном отображении, функция f имеет в окрестности точки 0 обратную $C^\infty(U, V)$ функцию f^{-1}. Заметим, что $f^{-1}(f(z)) = z$, так что, дифференцируя это равенство в нуле мы имеем

$$0 = \frac{\partial}{\partial \overline{z_j}}(f^{-1}(f(z)))_j = \sum_k \frac{\partial f_j^{-1}}{\partial z_k}\frac{\partial f_k}{\partial \overline{z_i}} + \sum_k \frac{\partial f_j^{-1}}{\partial \overline{z_k}}\left(\frac{\partial \overline{f_k}}{\partial \overline{z_i}}\right) = \sum_k \frac{\partial f_j^{-1}}{\partial \overline{z_k}}\left(\frac{\partial \overline{f_k}}{\partial z_i}\right) \quad \forall i, j.$$

Так как матрица $(\partial f_k/\partial z_j)$ была невырождена, отсюда следует, что $\partial f_j^{-1}/\partial \overline{z_k} = 0\ \forall j, k$, что и означает голоморфность функции f. □

Теорема 70 (О неявной функции). *Пусть заданы функции $f_1, \ldots, f_k \in \mathcal{O}_n$, удовлетворяющие условию*

$$\det\left(\frac{\partial f_i}{\partial z_j}(0)\right)_{1 \leq i,\ j \leq k} \neq 0.$$

Тогда существуют такие функции $w_1, \ldots, w_k \in \mathcal{O}_{n-k}$, что в окрестности точки $0 \in \mathbb{C}^n$

$$f_1(z) = \ldots f_k(z) = 0 \Leftrightarrow z_i = w_i(z_{k+1}, \ldots, z_n),\ 1 \leq i \leq k.$$

Доказательство. Как обычно, по обычной теореме о неявной функции в случае C^∞ существуют функции $\omega_1, \ldots, \omega_k$ с нужным свойством. Остается показать голоморфность. Это делается непосредственно вот таким стандартным вычислением вычислением:

$$0 = \frac{\partial}{\partial \overline{z_\alpha}}(f_j(\omega(z), z)) = \ldots = \sum \frac{\partial \omega_\ell}{\partial \overline{z_\alpha}}\frac{\partial f_j}{\partial \omega_\ell} \Rightarrow \frac{\partial \omega_\ell}{\partial \overline{z_\alpha}} = 0\ \forall \alpha, \ell,$$

□

Замечание. Видимо почти всегда, когда мы хотим показать голоморфность, мы тупо считаем в локальных производных антиголоморфную производную.

Теперь мы увидим, что комлексные многообразия в смысле их морфизмов таки имеют свою, отличную от вещественной, специфику:

Предложение 42. *Если $f\colon U \to V$ — взаимно однозначное голоморфное отображение открытых множеств в $\mathbb{C}^n$, то $\det \mathcal{J}(f) \neq 0$, то есть f^{-1} голоморфно.*

Замечание. Мы видели этот факт в обычном комплексном анализе (доказывали, что производная однолистной функции не обнуляется).

Определение 100. *Комплексным подмногообразием S* комплексного многообразия M называется подмножество $S \subset M$, которое локально задается либо как множество нулей совокупности голоморфных функций $f_1, \ldots f_k$ с условием $\operatorname{rank} \mathcal{J}(f) = k$, либо как образ открытого подмножества $U \subset \mathbb{C}^{n-k}$ при отображении $f\colon U \to M$ с условием $\operatorname{rank} \mathcal{J}(f) = n - k$.

Эквивалентность этих определений следует из теоремы о неявной функции 70.

Определение 101. Аналитическим подмножеством V комплексного многообразия M называется подмножество, являющееся локально множеством нулей конечного набора голоморфных функций.

Точка $p \in V$ называется *гладкой*[23] точкой V, если V в некоторой её окрестности задаётся набором голоморфных функций $f_1, \dots, f_k$, причем таким, что $\operatorname{rank} \mathcal{J}(f) = k$.

Множество гладких точек V обозначается V^*, а все точки из $V \setminus V^*$ называются *особыми*. Они формируют *множество особенностей* аналитического подмножества V, которое мы будем обозначать, как V_s.

В частности, если p — точка аналитической гиперповерхности $V \subset M$, задаваемой в локальных координатах z функцией f, определим *кратность* $\operatorname{mult}_p(V)$, как порядок обращения f в нуль в точке p, то есть наибольшее такое m, что

$$\frac{\partial^k f}{\partial z_{i_1} \dots \partial z_{i_k}} = 0 \; \forall k \leq m-1.$$

Предложение 43. *Множество V_s содержится в аналитическом подмножестве многообразия M, не совпадающем с V.*

Замечание. А на самом деле, при аккуратном выборе функций, несложно показать, что V_s — аналитическое подмножество в M.

Запомним также полезный нам в будущем факт:

Предложение 44. *Аналитическое множество V неприводимо тогда и только тогда, когда V^* связно.*

Тут было еще что-то про касательные конусы, пока что забьем на это, лень читать.

5.4 Когомологии де Рама и Дольбо

Пусть M — гладкое многообразие. Обозначим за $A^p(M;\mathbb{R})$ пространство дифференциальных форм степени p на M, а через $Z^p(M;\mathbb{R})$ подпространство замкнутых p-форм.

Так как $d^2 = 0$, у нас есть (ко)цепной комплекс

$$A^0(M;\mathbb{R}) \to \dots \to A^p(M;\mathbb{R}) \to A^{p+1}(M;\mathbb{R}) \to \dots$$

а его группы когомологий называются группами *когомологий де Рама* многообразия M.

Иными словами, группы когомологий де Рама — это факторгруппы замкнутых форм по модулю точных

$$H^p_{\mathrm{DR}}(M;\mathbb{R}) = Z^p(M;\mathbb{R})/dA^{p-1}(M).$$

Совершенно также мы можем рассматривать комплекснозначные формы и давать все соотвествующие определения (используя обозначения $A^p(M)$ и аналогичные, то есть без коэффициентов):

$$H^p_{\mathrm{DR}}(M) = Z^p(M)/dA^{p-1}(M)$$

Замечание. Нетрудно заметить, что как и всегда с коэффициентами,

$$H^p_{\mathrm{DR}}(M) = H^p_{\mathrm{DR}}(M;\mathbb{R}) \otimes \mathbb{C}.$$

Как мы заметили в самом первом параграфе, комплексифицированное кокасательное пространство раскладывается в голоморфную и антиголоморфную часть:

$$T^*_{\mathbb{C},z}M = T^{*'}_z M \oplus T^{*''}_z M,$$

что дает нам разложение

$$\Lambda^n T^*_{\mathbb{C},z}M = \bigoplus_{p+q=n} \Big(\Lambda^p T^{*'}_z(M) \otimes \Lambda^q T^{*''}_z(M)\Big),$$

а это (по определению внешних форм) даёт нам

$$A^n(M) = \bigoplus_{p+q=n} A^{p,q}(M), \text{ где}$$

[23] возможно, корректнее использовать слово регулярная?

$$A^{p,q}(M) = \{\varphi \in A^n(M) \mid \varphi(z) \in \Lambda^p T_z^{*'}(M) \otimes \Lambda^q T_z^{*''}(M)\ \forall z \in M\}.$$

Соотвественно, форму $\varphi \in A^{p,q}$ называют формой типа (p,q). Обозначим за $\pi^{(p,q)}$ проекцию

$$A^*(M) \to A^{p,q}(M),$$

так что для $\varphi \in A^*(M)$ имеем $\varphi = \sum \pi^{(p,q)}\varphi$.

Если $\varphi A^{p,q}(M)$, то для любого $z \in M$

$$\mathrm{d}\varphi(z) \in \left(\Lambda^p T_z^{*'} M \otimes \Lambda^q T_z^{*''} M\right) \wedge T^*_{\mathbb{C},z} M,$$

$$\mathrm{d}\varphi \in A^{p+1,q}(M) \oplus A^{p,q+1}(M).$$

Определоим теперь для этих замечательных дифференциальных форма операторы

$$\overline{\partial}\colon A^{p,q}(M) \to A^{p,q+1}, \quad \partial\colon A^{p,q}(M) \to A^{p+1,q}(M)$$

$$\overline{\partial} = \pi^{(p,q+1)} \circ \mathrm{d}, \quad \partial = \pi^{(p+1,q)} \circ \mathrm{d}, \text{ то есть } d = \partial + \overline{\partial}.$$

В локальных координатах $z = (z_1, \ldots, z_n)$ форма $\varphi \in A^n(M)$ имеет тип (p,q), если она имеет представление в виде

$$\varphi(z) = \sum_{I,J} \varphi_{I,J}(z)\mathrm{d}z_I \wedge \mathrm{d}\overline{z}_J$$

Замечание. Короче говоря, вся эта страшная белиберда была, чтоб сказать, что бывают не только голоморфные дифференциальные формы, но и такие, где один кусок голоморфный, а другой антиголоморфный.

Дифференцировать эти формы можно вполне естественным образом:

$$\overline{\partial}\varphi(z) = \sum_{I,J,j} \frac{\partial}{\partial \overline{z_j}}\varphi_{IJ}(z)\mathrm{d}\overline{z}_j \wedge \mathrm{d}z_I \wedge \mathrm{d}\overline{z}_J, \quad \partial\varphi(z) = \sum_{I,J,i} \frac{\partial \varphi}{\partial z_i}\varphi_{IJ}(z)\mathrm{d}z_i \wedge \mathrm{d}z_I \wedge \mathrm{d}\overline{z}_J.$$

В частности, форма типа $(q,0)$ называется *голоморфной*, если $\overline{\partial}\varphi = 0$. Ясно, что это имеет место тогда и только тогда, когда

$$\varphi(z) = \sum_{I\colon |I|=q} \varphi_I(z)\mathrm{d}z_I, \text{ где}$$

функции $\varphi_I(z)$ голоморфны.

Отметим, что поскольку разложение $T^*_{\mathbb{C},z} = T_z^{*'} \oplus T_z^{*''}$ сохраняется при голоморфных отображениях, тоже самое будет верно и для $A^\bullet = \bigoplus_{(p,q)} A^{(p,q)}$. Действительно, если $f\colon M \to N$ — голоморфное отображение комплексных многообразий, то $f^*(A^{p,q}(N)) \subset A^{p,q}(M)$ и $\overline{\partial} \circ f^* = f^* \circ \overline{\partial}$.

Пусть $Z^{p,q}_{\overline{\partial}}(M)$ — пространство ∂-замкнутых форм типа (p,q). Тогда, так как

$$\frac{\partial^2}{\partial \overline{z_i}\partial \overline{z_j}} = \frac{\partial^2}{\partial \overline{z_j}\partial \overline{z_i}}$$

мы будем иметь $\overline{\partial}^2 = 0$ на $A^{(p,q)}$, откуда мы получим

$$\overline{\partial}(A^{p,q}(M)) \subset Z^{p,q+1}_{\overline{\partial}}(M),$$

что позволяет определить *группы когомологий Дольбо* как

$$H^{p,q}_{\overline{\partial}}(M) = Z^{p,q}_{\overline{\partial}}(M)/\overline{\partial}\big(A^{p,q-1}(M)\big)$$

Теорема 71 ($\overline{\partial}$-лемма Пуанкаре)**.** *Для полидиска $\Delta = \Delta(r) \subset \mathbb{C}^n$ имеет место равенство*

$$H^{p,q}_{\overline{\partial}}(\Delta) = 0, q \geq 1.$$

Доказательство. Какое-то очень уж неприятное. Лучше сначала узнать, как обычная лемма Пуанкаре про то, что в односвзяной области замкнутая форма точна, доказывается. □

5.5 Пучки и когомологии

Определение 102. Пусть X — топологическое пространство. *Пучок* $\mathcal{F}$ на X сопоставляет каждому открытому множеству $U \subset X$ группу (или кольцо) $\mathcal{F}(U)$ (которое мы будем называть группой *сечений* $\mathcal{F}$ над U) и каждой паре $U \subset V$ открытых подмножеств X гомоморфизм $r_{VU}\colon \mathcal{F}(V) \to \mathcal{F}(U)$[24], называемый *гомоморфизмом ограничения*, причём так, что

1. Для любой тройки $U \subset V \subset W$ открытых множеств выполняется
$$r_{WU} = r_{WV} \circ r_{VU}.$$
В силу этого соотношения по аналогии с ограничениями функций принято писать $r_{WU}(\sigma) = \sigma|_U$ (в общем r_{WU} — гомомрфизм сужения с V на U).
2. $r_{UU} = \mathrm{id},\ \mathcal{F}(\varnothing) = 0$.
3. Для любой пары открытых множеств $U, V \subset M$ и сечений $\sigma \in \mathcal{F}(U)$, $\tau \in \mathcal{F}(V)$, таких что $\sigma|_{U\cap V} = \tau|_{U\cap V}$ найдётся такое сечение $\rho \in \mathcal{F}(U \cup V)$, что
$$\rho|_U = \sigma, \quad \rho|_V = \tau.$$
4. Если $\sigma \in \mathcal{F}(U \cup V)$ и $\sigma|_U = \sigma|_V = 0$, то $\sigma = 0$.

Очень хорошие пучки, которые мы будем часто встречать:

1.

5.6 Дивизоры и линейные расслоения

Дивизоры.

Пусть M — n-мерное комплексное многообразие. Тогда любое аналитическое подмножество $V \subset M$ размерности $n-1$ является аналитической гиперповерхностью, то есть в окрестности каждой точки $p \in V \subset M$ оно может быть задано как множество нулей некоторой голоморфной функции f. Кроме того, ясно, что любая голморфная функция g, обращающаяся в нуль на V, делится на f в окрестности точки p.

Пусть V_1^* — компонента связности $V^* = V \setminus V_s$, тогда $\overline{V_1^*}$ — аналитическое подмножество в M. Соответственно, V единственным образом представляется в в виде объединения неприводимых аналитических гиперповерхностей
$$V = V_1 \cup \ldots \cup V_m \quad V_i = \overline{V_i^*}.$$

Определение 103. *Дивизором* D на многообразии M называется локально конечная формальная линейная комбинация
$$D = \sum_i a_i V_i$$
неприводимых аналитических гиперповерхностей в M.

Замечание. Локальная конечность означает, что для любой точки $p \in M$ существует её окрестность, пересекающаяся лишь с конечным числом гиперповерхностей V_i, входящих в D. В случае копактного многообразия дивизоры образуют абелеву группу по сложению, которую мы будем обозначать $\mathrm{div}(M)$.

Определение 104. Дивизор $D = \sum a_i V_i$ называется *эффективным*, если $a_i \geq 0\ \forall i$. Обычно это обозначают, как $D \geq 0$.

Замечание. Если у нас есть аналитическая гиперповерзность V, неприводимые компоненты которой имеют вид $\{V_i\}$, мы отождествляем её с дивизором $\sum V_i$.

Определение 105. Пусть $V \subset M$ — неприводимая аналитическая гиперповерхность, а f — функция, локально определяющая V вблизи p. Тогда для голоморфной g, заданной в окрестности p определим $\mathrm{ord}_{V,p}(g)$, как наибольшее целое число a, при котором в кольце $\mathcal{O}_{M,p}$ имеет место разложение $g = f^a h$.

[24] тут буква r от слова *restriction*.

Замечание. Ясно, что это определение не зависит от точки p, так как взаимнопростые элементы $\mathcal{O}_M$ отаются взаимнопротыми в близких локальных кольцах $\mathcal{O}_{M,p}$. Ясно, что тогда порядок можно обозначать, как $\operatorname{ord}_V(g)$.

Ясно, что порядок обладает таким вот свойством:

$$\operatorname{ord}_V(gh) = \operatorname{ord}_V(g) + \operatorname{ord}_V(h).$$

Определение 106. Пусть f — мероморфная функция на M, записаная локально в виде g/h, где $(g,h) = 1$ и g, h голоморфны. Тогда для неприводимой гиперповерхности V положим

$$\operatorname{ord}_V(f) = \operatorname{ord}_V(g) - \operatorname{ord}_V(h).$$

Замечание. Соотвественно, f имеет нуль порядка a на V, если $\operatorname{ord}_V(f) = a > 0$ и полюс порядка a на V, если $\operatorname{ord}_V(f) = a < 0$.

Определение 107. *Дивизором* (f) мероморфной функции f называют формальную линейную комбинацию

$$(f) = \sum \operatorname{ord}_V(f) V$$

Если f локально представлена в виде $f = g/h$, то *дивизором нулей* называют

$$(f)_0 = \sum \operatorname{ord}_V(g) \cdot V,$$

а *дивизором полюсов* называют

$$(f)_\infty = \sum \operatorname{ord}_V(h) \cdot V,$$

Замечание. Если дивизоры нулей и полюсов корректно определны и $(g,h) = 1$, то

$$(f) = (f)_0 - (f)_\infty.$$

Про дивизоры, конечно же, можно говорить в терминах пучков. Пусть $\mathcal{M}^*$ — мультипликативный пучок мероморфных функций на M, $\mathcal{O}^*$ — его подпучок не обращающихся в нуль (обратимых) голоморфных функций. Тогда дивизор $D \in \operatorname{div}(M)$ — это просто глобальное сечение факторпучка $\mathcal{M}^*/\mathcal{O}^*$.

Действительно, глобальное сечение $\{f_\alpha\}$ факторпучка $\mathcal{M}^*/\mathcal{O}^*$ задаёься открытым покрытием $\{U_\alpha\}$ многообразия M и такими ненулевыми мероморфными функциями f_α на U_α, что

$$f_\alpha / f^\beta \in \mathcal{O}^*(U_\alpha \cap U_\beta).$$

Тогда для любой гиперповерхности $V \subset M$ $\operatorname{ord}_V f_\alpha = \operatorname{ord}_V f_\beta$ и набор $\{f_\alpha\}$ задаёт дивизор

$$D = \sum \operatorname{ord}_V(f_\alpha) \cdot V,$$

где α для каждого V выбран так, что $V \cap U_\alpha \neq \varnothing$.

Теперь рассмотрим дивизор $D = \sum a_i V_i$, по нему можно построить такое открытое покрытие $\{U_\alpha\}$ многообразия M, что в каждом U_α все V_i из D локально определяются функциями $g_{i,\alpha} \in \mathcal{O}(U_\alpha)$. Тогда мы можем положить

$$f_\alpha = \prod_i g_{i,\alpha}^{a_i} \in \mathcal{M}^*(U_\alpha)$$

и получить глобальное сечение факторпучка $\mathcal{M}^*/\mathcal{O}^*$. Соотвественно, вот эти вот функции $\{f_\alpha\}$ называют функциями, локально задающими дивизор. Отсюда мы имеет отождествление

$$H^0(M, \mathcal{M}^*/\mathcal{O}^*) \cong \operatorname{div}(M).$$

Глава 3

Арифметическая и диофантова геометрия

1. Алгебраическая теория чисел, часть I

1.1 Алгебраические числа и целые алгебраические числа

Определение 108. Число $\alpha \in \mathbb{C}$ называется *алгебраическим*, если существует $p \in \mathbb{Z}[x]$, аннулирующий α.

Замечание. Это частный случай общей терминологии, тут речь о том, что α алгебраичен над $\mathbb{Q}$.

Предложение 45. *Пусть $\alpha \in \mathbb{C}$. Тогда следующие утверждения эквивалентны:*

1. *α — алгебраическое.*
2. *$\mathbb{Q}[\alpha]$ — конечномерное векторное пространство над $\mathbb{Q}$.*

Доказательство. $(\mathbf{1}) \implies (\mathbf{2})$: очевидно, так как если α — алгебраичен над $\mathbb{Q}$, базисом $\mathbb{Q}[\alpha]$ над $\mathbb{Q}$ будет множество $\{1, \alpha, \dots, \alpha^{n-1}\}$.

$(\mathbf{2}) \implies (\mathbf{1})$: действительно, если $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha] = n$, то $1, \alpha, \dots, \alpha^n$ линейно зависимы, то есть $\exists a_0, \dots, a_n \in \mathbb{Q}$:

$$a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0.$$

Домножая на знаменатель, мы имеем нужный многочлен. □

Предложение 46. *Множество алгебраических чисел является полем.*

Доказательство. Пусть α — алгебраическое число. Тогда

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,\ a_i \in \mathbb{Z}.$$

Но тогда $a_n + \ldots + a_1\left(\alpha^{-1}\right)^{n-1} + a_0\left(\alpha^{-1}\right)^n = 0$, то есть α^{-1} алгебраическое. Теперь, пусть α и β алгебраические. Тогда $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha, \beta] < \infty \implies \dim_{\mathbb{Q}} \mathbb{Q}[\alpha\beta],\ \dim_{\mathbb{Q}} \mathbb{Q}[\alpha + \beta] < \infty$.

□

Замечание. Искушенный читатель сразу заметит, что это поле — это в точности $\mathbb{Q}^{alg}$.

Определение 109. $\alpha \in \mathbb{C}$ мы будем называть *целым алгебраическим числом*, если существует унитарный многочлен $p \in \mathbb{Z}[x]$, аннулирующий α.

Пример 35. $\sqrt{2}$ — целое алгебраическое число, а вот $\sqrt{2}/2$ — нет!

Предложение 47. *Следующие утверждения эквивалентны:*

1. *α — целое алгебраическое число.*
2. *$\mathbb{Z}[\alpha]$ — конечно-порожденный $\mathbb{Z}$-модуль.*

Доказательство. Опять же, $(\mathbf{1}) \implies (\mathbf{2})$ следует просто из того, что если α — целое алгебраическое, то $\{1, \dots, \alpha^{n-1}\}$ — базис $\mathbb{Z}[\alpha]$ над $\mathbb{Z}$.

Теперь докажем $(\mathbf{2}) \implies (\mathbf{1})$. Ясно, что все образующие $\mathbb{Z}[\alpha]$ над $\mathbb{Z}$ — многочлены от α, пусть они $p_1(\alpha), \dots, p_m(\alpha)$. Пусть $N = \max \deg(p_i)$, тогда

$$\alpha^{N+1} = \sum_{i=1}^{m} a_i p_i(\alpha), \quad \alpha^{N+1} - \sum_{i=1}^{m} a_i p_i(\alpha) = 0.$$

□

Теорема 72. *Множество целых алгебраических чисел является кольцом.*

Доказательство. Возьмём α, β — целые алгебраические. Тогда по предыдущему предложению $\mathbb{Z}[\alpha, \beta]$ — конечнопорожденный $\mathbb{Z}$-модуль, а так как $\mathbb{Z}$ — нётерово, тогда подумодули $\mathbb{Z}[\alpha + \beta]$ и $\mathbb{Z}[\alpha\beta]$ конечнопорождены, откуда $\alpha\beta$ и $\alpha + \beta$ целые алгебраические (также по предыдущему предложению). □

Обозначим кольцо целых алгебраических чисел, как $\mathcal{O}$. В основном в этом курсе мы будем изучать подкольца в $\mathcal{O}$, а именно

Определение 110. Пусть $K/\mathbb{Q}$ — конечное расширение. Тогда

$$\mathcal{O}_K \stackrel{\text{def}}{=} \mathcal{O} \cap K$$

мы будем называть *кольцом целых* числового поля K. Иными словами, $\mathcal{O}_K$ — множество элементов K, для которых существует унитарный целочисленный многочлен, аннулирующий их.

1.2 След элемента и целый базис кольца $\mathcal{O}_K$

Заведём теперь некоторый полезный аппарат.

Определение 111. Пусть L/K — конечное расширение, $[L : K] = n$. Возьмём $\alpha \in L$, его можно рассматривать, как эндоморфизм понятным образом

$$T_\alpha \colon L \to L, \quad x \mapsto \alpha x.$$

Соотвественно, след этого оператора называют следом элемента α относительно расширения L/K и обозначают $\operatorname{Tr}_{L/K}(\alpha)$.

У этого оператора есть характеристический многочлен χ_α. Выбрав базис L/K, мы можем записать матрицу оператора T_α и тогда

$$\chi_\alpha(t) = \det(Et - T_\alpha) = t^n - \operatorname{Tr}_{L/K}(\alpha) t^{n-1} + \dots$$

Если L/K — расширение Галуа, то можно определять след, как

$$\operatorname{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \operatorname{Gal}(L/K)} \sigma(\alpha).$$

Соотвественно, след — это K-линейный функционал $L \to K$, то есть

$$\forall \alpha, \beta \in K \quad \operatorname{Tr}_{L/K}(\alpha a + \beta b) = \alpha \operatorname{Tr}_{L/K}(a) + \beta \operatorname{Tr}_{L/K}(b).$$

Кроме того, для $\alpha \in K$ $\operatorname{Tr}_{L/K}(\alpha) = [L : K] \cdot \alpha$. Кроме того, след хорошо ведёт себя относительно башни расширений. Если M — расширение K, а K — расширение L, то

$$\operatorname{Tr}_{M/K} = \operatorname{Tr}_{M/L} \circ \operatorname{Tr}_{L/K}.$$

Кроме того, след можно рассматривать и как невырожденную билинейную симметричную форму

$$K \times K \to \mathbb{Q}, \ (x, y) \mapsto \operatorname{Tr}_{K/\mathbb{Q}}(xy).$$

Замечание. Если $\alpha \in \mathcal{O}_K$, то $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Действительно, во-первых, $\sigma(\alpha) \in \mathcal{O}_k \ \forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})$, так как если $\alpha \in \mathcal{O}_K$, то

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0 \implies (\sigma\alpha)^n + a_{n-1}(\sigma\alpha)^{n-1} + a_0 = 0 \implies \sigma\alpha \in \mathcal{O}_K$$

, откуда $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathcal{O}_K$.

С другой стороны, по первому определению $\mathrm{Tr}_{K/\mathbb{Q}} \in \mathbb{Q}$, а $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$.

Предложение 48. *Любой элемент поля K представим в виде $\frac{\beta}{d}$, где $\beta \in \mathcal{O}_K$, $m \in \mathbb{Z}$. Иными словами, K — поле частных кольца $\mathcal{O}_K$.*

Доказательство. Во-первых, α является корнем некоторого унитарного многочлена с коэффициентами из $\mathbb{Q}$:

$$\alpha^n + c_{n-1}\alpha^{n-1} + \ldots + c_1\alpha + c_0 = 0, \quad c_i \in \mathbb{Q}.$$

Запишем $c_i = \frac{b_i}{d}$, $b_i, d \in \mathbb{Z}$. Тогда, домножив равенство выше на d^n, мы получаем

$$(\alpha d)^n + b_{n-1}(\alpha d)^{n-1} + b_{n-2}d(\alpha d)^{n-2} + \ldots + b_0 d^{n-1} = 0.$$

Соотвественно, полагая $\beta = d\alpha$ мы видим, что $\beta \in \mathcal{O}_K$ и $\alpha = \beta/d$. □

Так вот, возьмём базис $K/\mathbb{Q}$. Из предыдущего предложения ясно, что можно полагать, что этот базис состоит из элементов $\mathcal{O}_K$. Обозначим их за $\omega_1, \ldots, \omega_n$. Выберем для этого базиса взаимный базис $\omega_1^*, \ldots, \omega_n^*$ относительно формы $\mathrm{Tr}_{K/\mathbb{Q}}$, т.е. такой базис, что

$$\mathrm{Tr}(\omega_i\omega_j^*) = \begin{cases} 0, i \neq j \\ 1, i = j \end{cases} = \delta_{ij}.$$

Покажем, что выполнено

$$\bigoplus_i \mathbb{Z}\omega_i \subset \mathcal{O}_K \subset \bigoplus_i \mathbb{Z}\omega_i^*.$$

Первое включение очевидно, докажем второе. Возмём $\alpha \in \mathcal{O}_K$,

$$\alpha = \sum_{i=1}^n x_i\omega_i^*, \quad x_i \in \mathbb{Q}.$$

Покажем, что на самом деле $x_i \in \mathbb{Z}$.

$$\alpha\omega_j = \sum_{i=1}^n x_i\omega_j\omega_i^* \implies \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega_j) = x_j.$$

С другой стороны, так как $\alpha\omega_j \in \mathcal{O}_K$, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\omega_j) \in \mathbb{Z}$ (как мы отвечали выше). Таким образом, мы имеем

$$\bigoplus_i \mathbb{Z}\omega_i \subset \mathcal{O}_K \subset \bigoplus_i \mathbb{Z}\omega_i^*.$$

Так как слева и справа конечнопорождённые абелевы группы ранга n, мы только что доказали такую теорему:

Теорема 73. *Пусть $\mathcal{O}_K$ — кольцо целых числового поля $K/\mathbb{Q}$, где $K/\mathbb{Q}$ — расширение степени n. Тогда, как абелева группа оно изоморфно конечнопорожденной свободной абелевой группе ранга n:*

$$\mathcal{O}_K \cong \bigoplus_{i=1}^n \mathbb{Z}u_i,$$

где $\{u_i\}$ — базис $K/\mathbb{Q}$, состоящий из элементов кольца $\mathcal{O}_K$.

В данном контексте $\{u_i\}_{i=1}^n$ называют целым базисом.

Из этой теоремы сразу следует вот такой факт:

Теорема 74. *Кольцо $\mathcal{O}_K$ — нётерово.*

Доказательство. В самом деле, по теореме 73 кольцо $\mathcal{O}_K$ конечно порождена, как абелева группа, а значит, любой его идеал $I \subset \mathcal{O}_K$ тоже конечно порожден, как абелева группа, откуда следует, что он конечно порожден и как идеал. □

Пример 36. Рассмотрим поле $K = \mathbb{Q}(\sqrt{-3})$. Чему равно его кольцо целых $\mathcal{O}_K$?

Ясно, что $\mathbb{Z}[\sqrt{-3}] \subset \mathcal{O}_K$, но вот равенства нет, так как можно рассмотреть

$$\alpha = \frac{1+\sqrt{-3}}{2}, \quad 2\alpha - 1 = \sqrt{-3} \implies 4\alpha^2 - 4\alpha + 4 = 0 \implies \alpha^2 - \alpha + 1 = 0,$$

то есть $\alpha \in \mathcal{O}_K$ и $\alpha \notin \mathbb{Z}[\sqrt{-3}]$.

Воспользуемся понятием *нормы*:

Определение 112. Пусть L/K — конечное расширение, $[L : K] = n$. Возьмём $\alpha \in L$, его можно рассматривать, как эндоморфизм понятным образом

$$T_\alpha \colon L \to L, \quad x \mapsto \alpha x.$$

Нормой элемента α относительно расширения L/K мы будем называть $\mathrm{N}_{L/K}(\alpha) = \mathrm{N}(\alpha) = \det(T_\alpha)$. В случае, когда расширение сепарабельно, норму можно определять, как

$$\mathrm{N}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Замечание. Как и в случае со следом, для $\alpha \in \mathcal{O}_K$ $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \in \mathcal{O}_K$ (доказывается это так же, как для следа), а из определения через определитель ясно, что $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$, то есть $\mathrm{N}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Ясно, что в случае квадратичного расширения $\mathbb{Q}(\sqrt{d})$ норма $a + b\sqrt{d}$ норма элемента — произведение его на его сопряженный:

$$\mathrm{N}(a + b\sqrt{d}) = (a + b\sqrt{d}))(a - b\sqrt{d}) = a^2 - db^2$$

Соотвественно, рассмотрим $a + b\sqrt{-3} \in \mathbb{Q}(\sqrt{-3})$ (т.е. $a, b \in \mathbb{Q}$) и пусть $\alpha = a + b\sqrt{-3} \in \mathcal{O}_K$. Тогда

$$\mathrm{N}_{K/\mathbb{Q}}(a+b\sqrt{-3}) = (a+b\sqrt{-3})(a-b\sqrt{-3}) = a+3b^3 \in \mathbb{Z}, \quad \mathrm{Tr}_{K/\mathbb{Q}}(a+b\sqrt{-3}) = (a+b\sqrt{-3})+(a-b\sqrt{-3}) = 2a \in \mathbb{Z}.$$

Соответственно, $2a \in \mathbb{Z}$, то есть или $a = n/2$, где $n \in \mathbb{Z}$ и нечётное, или $a \in \mathbb{Z}$.

1. Пусть $a \in \mathbb{Z}$, тогда так как $a^2 + 3b^2 \in \mathbb{Z}$, $3b^2 \in \mathbb{Z} \implies b \in \mathbb{Z}$.
2. Пусть $2a = 2n + 1$, тогда $4(a^2 + 3b^2) = 4a^2 + 12b^2 \in 4\mathbb{Z} \implies 12b^2 \in 4\mathbb{Z}$, откуда $2b \in \mathbb{Z}$.

Значит, либо a и b одновременно целые, либо a и b одновременно полуцелые. То есть

$$\alpha = \frac{2n+1}{2} + \frac{2m+1}{2}\sqrt{-3} = (n + m\sqrt{-3}) + \frac{1+\sqrt{-3}}{2} = (n-m) + (2m+1)\frac{1+\sqrt{-3}}{2},$$

откуда $\mathcal{O}_K \cong \mathbb{Z} \oplus \mathbb{Z} \cdot \frac{1+\sqrt{-3}}{2}$.

Пример 37. Если $K = \mathbb{Q}(i)$, то $\mathcal{O}_K = \mathbb{Z}[i]$.

Домашнее задание 3. Задачи:

1. Опишите $\mathcal{O}_K$ для $K = \mathbb{Q}(\sqrt{d})$, где $d \in \mathbb{Z}$ и d свободно от квадратов.
2. Докажите, что любое конечное целостное кольцо является полем.
3. Рассмотрим поле $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ и идеал $I = (2, 1+\sqrt{-5})$. Покажите, что он не является главным.
4. Докажите, что кольцо $\mathbb{Z}[\sqrt{-5}]$ не факториальное. А именно, рассмотрите

   $$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

   и покажите: что это два существенно различных разложения в произвдение простых.

1.3 Размерность кольца целых $\mathcal{O}_K$

Докажем теперь, что для любого числового поля K кольцо целых $\mathcal{O}_K$ одномерно.

Лемма 45. Пусть $K/\mathbb{Q}$ — конечное расширение и $0 \neq I$ — идеал кольца $\mathcal{O}_K$. Тогда $I \cap \mathbb{Z} \neq 0$, то есть I содержит целое число.

Доказательство. Возьмём $\alpha \in I$, $\alpha \neq 0$. Тогда

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0, \quad a_i \in \mathbb{Z}.$$

Не умаляя общности, $a_0 \neq 0$. Но тогда

$$a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha) \implies a_0 \in \mathbb{Z} \cap I.$$

□

Следствие 32. *Пусть I — ненулевой идеал в $\mathcal{O}_K$. Тогда $\mathcal{O}_K/I$ конечно.*

Доказательство. По лемме 45 выберем $n \in I \cap \mathbb{Z}$, $n \neq 0$. Тогда $(n) = n\mathcal{O}_K \trianglelefteq I$, значит достаточно доказать, что $\mathcal{O}_K/n\mathcal{O}_K$ конечно. А это сразу же следует из того, что $\mathcal{O}_K$ — это конечнопорожденная свободная абелева группа ранга n. □

Теорема 75. *Кольцо $\mathcal{O}_K$ одномерно, т.е.* $\dim(\mathcal{O}_K) = 1$.

Доказательство. Пусть $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$. Тогда $\mathcal{O}_K/\mathfrak{p}$ — область целостности и конечно по следствию 32. Но тогда по задаче 2 в 3 $\mathcal{O}_K/\mathfrak{p}$ — поле, что равносильно тому, что $\mathfrak{p}$ — максимальынй. □

Замечание. Эквивалентная формулировка этой теоремы состоит в том, что любой ненулевой простой идеал кольца $\mathcal{O}_K$ является максимальным.

Поговорим теперь еще про строение идеалов в кольце $\mathcal{O}_K$. Как мы уже убеждались в задаче 3 Д/З 3, кольцо $\mathcal{O}_K$ далеко не всегда является областью главных идеалов.

1.4 Примеры евклидовых колец целых алгебраических чисел

Предложение 49. *Рассмотрим $K = \mathbb{Q}(\sqrt{-3})$. Тогда $\mathcal{O}_K$ — евклидово.*

Доказательство. Как мы убедились в примере 36,

$$\mathcal{O}_K \cong \mathbb{Z} \oplus \mathbb{Z}\omega, \quad \omega = \frac{1+\sqrt{-3}}{2}.$$

Рассмотрим $a + b\omega$, тогда положим

$$\mathrm{N}(\alpha) = (a + b\omega)(a + b\overline{\omega}) = a^2 + ab + b^2.$$

Пусть $a, b, c, d \in \mathbb{Z}$, тогда

$$\frac{a + b\omega}{c + d\omega} = \alpha + \beta\omega, \quad \alpha, \beta \in \mathbb{Q}.$$

Тогда существуют $u, v \in \mathbb{Z}$ такие, что $|u - \alpha| \leq \frac{1}{2}$, $|v - \beta| \leq \frac{1}{2}$. Положим $\alpha - u = \alpha'$, $\beta - v = \beta'$.

$$a + b\omega = (c + d\omega)(\alpha + \beta\omega) = (c + d\omega)(u + v\omega) + (c + d\omega)(\alpha' + \beta'\omega) = (c + d\omega)(u + v\omega) + r.$$

$$\mathrm{N}(r) = \mathrm{N}((c + d\omega)(\alpha' + \beta'\omega)) = \mathrm{N}(c + d\omega)\,\mathrm{N}(\alpha' + \beta'\omega) = \mathrm{N}(c + d\omega)(\alpha'^2 + \alpha'\beta' + \beta'^2) < \mathrm{N}(c + d\omega),$$

так как $\alpha'^2 + \alpha'\beta' + \beta'^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}$, что и требовалось.

□

Сейчас мы посмотрим

Предложение 50. *Уравнение $y^2 = x^3 - 2$ над $\mathbb{Z}$ в качестве решений имеет лишь $(3, \pm 5)$.*

Доказательство. Во-первых заметим, что можно сразу полагать y нечётным.

Попробуем решить уравнение в $\mathbb{Z}[\sqrt{-2}] = \mathcal{O}_K$ для $K = \mathbb{Q}(\sqrt{-2})$.

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3.$$

Пусть $d = (y + \sqrt{0-2}, y - \sqrt{-2})$. Покажем, что $d = 1$. Действительно,

$$\begin{cases} y + \sqrt{-2} \vdots d \\ y - \sqrt{-2} \vdots d \end{cases} \implies \begin{cases} 2y \vdots d \\ 2\sqrt{-2} \vdots d \end{cases}.$$

Заметим, что $2\sqrt{-2} \vdots d \implies \mathrm{N}(2\sqrt{-2}) \vdots \mathrm{N}(d)$. Пусть $d = a + b\sqrt{-2},\ a, b \in \mathbb{Z}$. Тогда мы имеем $8 \vdots (a^2 + 2b^2)$.

Т.е. $a^2 + 2b^2 = 1, 2, 4$ или 8. Разберём соотвествующие случаи:

1. $a^2 + 2b^2 = 1 \rightsquigarrow a = \pm 1,\ b = 0.$
2. $a^2 + 2b^2 = 2 \rightsquigarrow a = 0,\ b = \pm 1.$
3. $a^2 + 2b^2 = 4 \rightsquigarrow a = \pm 2,\ b = \pm 0.$
4. $a^2 + 2b^2 = 8 \rightsquigarrow a = \pm 0,\ b = \pm 2.$

Заметим, что так как y — нечётное целое,

$$\mathrm{N}(y + \sqrt{-2}) = y^2 + 2 \not\vdots \mathrm{N}(\sqrt{-2}) = 2,$$

откуда следует, что случаи (2) и (4) нам не годятся. Случай (3) нам не подходит просто в силу того, что y нечётное.

Значит, мы доказали, что $y + \sqrt{-2}$ и $y - \sqrt{-2}$ — взаимнопросты, а так как кольцо $\mathbb{Z}[\sqrt{-2}]$ факториально, отсюда мы имеем, что

$$y + \sqrt{-2} = z^3, \quad y - \sqrt{-2} = t^3.$$

Пусть опять же $z = a + b\sqrt{-2}$. Честно возведём в куб:

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a^3 + 3a^2 b\sqrt{-2} - 6ab^2 - 2b^3\sqrt{-2},$$

октуда мы имеем

$$\begin{cases} a^3 - 6ab^2 = y \\ 3a^2 b - 2b^3 = 1 \end{cases}$$

Соотвественно, из второго уравнения ясно, что $b = \pm 1$, откуда либо $3a^2 = 3 \implies a = \pm 1$, либо $3a^2 = -1$, чего быть не может ($a \in \mathbb{Z}$). Соотвественно, мы получили, что

$$y = a^3 - 6ab^2 = \pm 5 \implies y = \pm 5.$$

□

1.5 "Last Fermat's theorem" для $n = 3$.

Все мы знаем следующее (важное для истории математики) утверждение:

Теорема 76 (Last Fermat's theorem)**.** *Для любого натурального $n > 2$ уравнение*

$$x^n + y^n = z^n$$

не имеет решений над $\mathbb{Z}$.

В случае $n = 2$ решения есть и мы даже можем выписать их явно, проделаем это.

$$x^2 + y^2 = z^2 \implies y^2 = (z - x)(z + x)$$

Ясно, что с самого начала можно полагать x, y, z попарно взаимно простыми. Предположим, что $2 \mid y,\ 2 \nmid x$. Тогда мы можем переписать уравнение как

$$\left(\frac{y}{2}\right)^2 = \frac{z - x}{2} \cdot \frac{z + x}{2}$$

Заметим, что $(z, x) = 1 \implies (z - x, z + x) = 1$, откуда

$$\frac{z - x}{2} = b^2, \quad \frac{z + x}{2} = a^2 \implies \begin{cases} z = a^2 + b^2, \\ x = a^2 - b^2 \\ y = 2ab, \end{cases} \quad 0 < b < a,\ (b, a) = 1.$$

Также есть элементарное решение в случае $n = 4$.

Предложение 51. *Уравнение $x^4 + y^4 = z^2$ не имеет нетривиальных решений.*

Доказательство. Предположим противное и рассмотрим нетривиальное решение (x, y, z). В частности, это пифагорова тройка, откуда, как мы уже поняли выше

$$x^2 = 2ab, \quad y^2 = a^2 - b^2, \quad z = a^2 + b^2,\ (a, b) = 1.$$

Рассмотрим решение с минимальным $|z|$. Заметим, что

$$x^2 \vdots 2 \implies x^2 \vdots 4 \implies 2ab \vdots 4 \implies ab \vdots 2$$

Если $b \not\vdots 2$, то $a \vdots 2$ а тогда $y^2 \equiv 0 - 1 \equiv 3 \pmod 4$, чего быть не может. Тогда

$$\begin{cases} y^2 + b^2 = a^2 \\ b \vdots 2 \end{cases} \implies \begin{cases} b = 2uv \\ a = u^2 + v^2 \\ y = u^2 - v^2 \end{cases}, (u, v) = 1.$$

$$x^2 = 2ab = 4uv(u^2 + v^2) \implies \left(\frac{x}{2}\right)^2 = uv(u^2 + v^2) \implies u = s^2 m \quad v = t^2, \quad u^2 + v^2 = r^2,$$

Отсюда получаем $s^4 + t^4 = r^2$, $|r| < |z|$, что даёт нам протворечие.

□

Ясно, что из этого следует, что уравнение $x^4 + y^4 = z^4$ не имеет нетривиальных корней над $\mathbb{Z}$.

Разберёмся теперь с большой теоремой Ферма в случае $n = 3$. Доказательство мы будем проводить в два этапа. Сначала докажем такую вспомогательную лемму:

Лемма 46. Пусть $a, b \in \mathbb{Z}$ — такие, что

- $(a, b) = 1$.
- $a \not\equiv b \pmod 2$
- $\mathrm{N}(a + b\sqrt{-3}) = a^2 + 3b^3$ — полный куб.

Тогда существуют $s, t \in \mathbb{Z}$ такие, что

$$\begin{cases} a = s^3 - 9st^2 \\ b = 3t(s^2 - t^2). \end{cases}$$

Доказательство. Рассмотрим кольцо целых $\mathcal{O}_K$ для поля $K = \mathbb{Q}(\sqrt{-3})$.

Шаг 1: найдём группу обратимых элементов $\mathcal{O}_K^*$:

Пусть ξ — первообразный корень шестой степени из единицы,

$$\xi = \frac{-1+\sqrt{-3}}{2}.$$

Тогда $\pm\xi^i,\ i = 0,1,2$ — обратимые. Докажем, что других обратимых элеемнтов нет. Пусть $u \in \mathcal{O}_K^*$, тогда $u = a + b\xi,\ a,b \in \mathbb{Z}$. Тогда, так как u обратим, $uv = 1$ для некоторого v. Но тогда $\mathrm{N}(u)\,\mathrm{N}(v) = 1$, откуда $\mathrm{N}(u)$ обратима в $\mathbb{Z}$, а так как она неотрицательна, $\mathrm{N}(u) = 1$. Тогда

$$\mathrm{N}(u) = (a+b\xi)(a+b\bar{\xi}) = a^2 + ab + b^2 = 1 \implies (2a+b)^2 + 3b^2 = 4.$$

1. Пусть $b = 0$. Тогда $2a = \pm 2 \implies a = \pm 1 \implies u = \pm 1$.
2. $b = 1 \implies 2a - 1 = \pm 1$, откуда $a = 0$ или $a = 1$ и, в этом случае, $u = -1 + \xi = \xi^2$, либо $u = \xi$.
3. $b = -1 \implies 2a - 1 = \pm 1 \implies a = 1$ или $a = 0$, откуда $u = 1 + \xi = -\xi^2$, или $u = -\xi$.

Шаг 2: докажем, что $(a + b\sqrt{-3}, a - b\sqrt{-3}) = (1)$.

Пусть $a \vdots 3$, тогда $x^3 = a^2 + 3b^2 \vdots 3 \implies x \vdots 3$, откуда $a^2 + 3b^2 = x^3 \vdots 27$, а значит,

$$3\Big(\frac{a}{3}\Big)^2 + b^2 \vdots 3 \implies b \vdots 3,$$

что противоречит тому, что $(a,b) = 1$. Значит, $a \not\vdots 3$.

Предположим, что для некоторого $\alpha \in \mathcal{O}_K$

$$\begin{cases} a + b\sqrt{-3} \vdots \alpha \\ a - b\sqrt{-3} \vdots \alpha \end{cases} \implies \begin{cases} 2a \vdots \alpha \\ 2b\sqrt{-3} \vdots \alpha \end{cases} \implies \begin{cases} \mathrm{N}(2a) \vdots \mathrm{N}(2\alpha) \\ \mathrm{N}(2b\sqrt{-3}) \vdots \mathrm{N}(\alpha) \end{cases} \implies \begin{cases} 4a^2 \vdots \mathrm{N}(\alpha) \\ 12b^2 \vdots \mathrm{N}(\alpha) \end{cases},$$

а так как $a \not\vdots 3$, из этого следует, что $4a^2 \vdots \mathrm{N}(\alpha)$ и $4b^2 \vdots \mathrm{N}(\alpha)$, что даёт нам, что $4 \vdots \mathrm{N}(\alpha)$ (так как $(a,b) = 1$)

Переберём теперь варианты (помня, что мы ищем $\alpha\colon\ \mathrm{N}(\alpha) > 1$):

1. Пусть $\mathrm{N}(\alpha) = 2$. Пусть $\alpha = c + d\omega$, тогда

   $$4\,\mathrm{N}(\alpha) = 4(c^2 + cd + d^2) = (2c+d)^2 + 3d^2 = 8,$$

   а это уравнение не имеет решений в целых числах.
2. Пусть $\mathrm{N}(\alpha) = 4, \alpha = c + d\omega$. Тогда

   $$4\,\mathrm{N}(\alpha) = (2c+d)^2 + 3d^2 = 16.$$

   Пусть $d = 0$, тогла $c = \pm 2$, откуда $\alpha = \pm 2$, но тогда $a + b\sqrt{-3} \vdots 2$, а это возожно только когда a и b одной четности.

   Пусть $d = 2$, тогда $c = 0$, то есть $\alpha = 2\omega$, откуда снова $a + b\sqrt{-3} \vdots 2$.

   И аналогично, когда $d = -2$, так как в этом случае $c = 0$ или $c = 2$, то есть либо $\alpha = -2\omega$, либо $\alpha = 2 - 2\omega$, откуда снова $a + b\sqrt{-3} \vdots 2$.

Шаг 3: Таким образом, так как $a^2 + 3b^2 = (a + b\sqrt{-3})(a - b\sqrt{-3})$ — полный куб, а так как $(a + b\sqrt{-3}, a - b\sqrt{-3}) = 1$, мы получаем, что с точностью до домножения на обратимый $a + b\sqrt{-3}$ и $a - b\sqrt{-3}$ — кубы. Именно чтоб разобраться шаг с домножением на обратимый, мы делали шаг 1. То есть,

$$(\pm\xi)^i(a + b\sqrt{-3}) = (s + t\sqrt{-3})^3, \quad s + t\sqrt{-3} \in \mathcal{O}_K.$$

Пусть $i \neq 0$, тогда

$$(a + b\sqrt{-3}) \cdot \xi^i = (a + b\sqrt{-3}) \cdot \frac{1 \pm \sqrt{-3}}{2} = \frac{a \pm 3b}{2} + \frac{a \pm b}{2}\sqrt{-3}.$$

Тогда s и t оба полуцелые, то есть

$$(a+b\sqrt{-3})(\pm\xi^i)=\left(\frac{c+d\sqrt{-3}}{2}\right)^3=\frac{(c^3-9cd^2)+(3c^2d-3d^3)\sqrt{-3}}{8},\quad c,d\not\vdots 2.$$

Посмотрим на числитель по модулю 8. Так как $c,d\equiv 1\pmod 2$, $c^2\equiv d^2\equiv 1\pmod 8$, а тогда

$$c^3-9c^2d\equiv c^3-cd^2\equiv c(c^2-d^2)\equiv 0\pmod 8.$$

$$3c^2d-3d^3=3d(c^2-d^2)\equiv 3d(1-1)\equiv 0\pmod 8.$$

Таким образом, $a+b\sqrt{-3}=(s+t\sqrt{-3})^3$, но s и t могут быть полуцелые.

Шаг 4: Пусть $c=\frac{2k+1}{2},\ d=\frac{2\ell+1}{2}$, тогда, так как

$$\left(\frac{-1\pm\sqrt{-3}}{2}\right)^3=1\implies(c+d\sqrt{-3})^3=\left((c+d\sqrt{-3})\cdot\frac{-1\pm\sqrt{-3}}{2}\right)^3$$

Вычисляя $(c+d\sqrt{-3})\cdot\frac{-1\pm\sqrt{-3}}{2}$, легко убедиться, что знак всегда можно подобрать так, чтоб $c,d\in\mathbb{Z}$. □

При помощи этой леммы уже совсем несложно доказать большую теоерму ферма для $n=3$. Рассмотрим уравнение

$$x^3+y^3=z^3,\quad (x,y)=1,\ (x,z)=1,\ (y,z)=1.$$

Не умаляя общности, также можно полагать $x\vdots 2,\ y\not\vdots 2,\ z\not\vdots 2$. Выберем решение с минимальным $|x|$. Сделаем такую замену:

$$y=p-q,\quad z=p+q,\ p,q\in\mathbb{Z},\ (p,q)=1,\ p\not\equiv_2 q.$$

Тогда, подставляя это в уравнение, мы имеем

$$x^3=(p+q)^3-(p-q)^3=2q(q^2+3p^2).$$

Так как $x\vdots 2$, $2q(q^2+3p^2)\equiv 0\pmod 8$, откуда $q\equiv 0\pmod 4$. Значит,

$$\left(\frac{x}{2}\right)^3=\frac{q}{4}\left(q^2+3p^2\right).$$

I. Предположим, что $q\not\vdots 3$. Тогда

$$\left(\frac{q}{4},q^2+3p^2\right)=1\implies q^2+3p^2=t^3.$$

Соответсвенно, мы попадаем в условие леммы 46:

$$\begin{cases}q^2+3p^2=t^3\\ p\not\equiv q\pmod 2\\ (p,q)=1\end{cases}\underbrace{\implies}_{\text{Л. 46}}\begin{cases}q=s^3-9st^2\\ p=3t(s^2-t^2)\end{cases}$$

С другой стороны, $q/4$ — тоже куб, а тогда

$$2q=2s(s-3t)(s+3t)\text{ — тоже куб.}$$

Так как $q\not\vdots 3$, $s\not\vdots 3$. Кроме того, $s-3t\not\vdots 2\implies(s,s-3t)=(s,s+3t)=(s+3t,s-3t)=1$, то есть мы имеем

$$\begin{cases}2s=x_1^3\\ 3t-s=y_1^3\\ 3t+s=z_1^3\end{cases}\implies x_1^3+y_1^3=z_1^3.$$

$|x_1|^3=|2s|\le|2q|<|x|^3$, то есть мы получили решение с меньшим модулем x.

II. Пусть $q \vdots 3,\ q = 3r$. Тогда

$$\left(\frac{x}{2}\right)^3 = \frac{q}{4}(q^4 + 3p^2) = \frac{3r}{4}\left(9r^2 + 3p^2\right) = \frac{9r}{4}(3r^2 + p^2).$$

Так как сомножители взаимнопросты, каждый из является кубом. Опять применим лемму 46:

$$\begin{cases} p = s(s^2 - 9t^2) \\ r = 3t(s^2 - t^2) \end{cases}.$$

С другой стороны, $9r/4$ — тоже куб, то есть

$$\ell^3 = \frac{9r}{4} = \frac{27t}{4}(s^2 - t^) \implies 2t(t+s)(s-t) - \text{куб.}$$

Опять же, так как $(2t, t+s) = (s-t, t+s) = (2t, s-t) = 1$, откуда

$$\begin{cases} 2t = x_1^3 \\ s - t = y_1^3 \\ s + t = z_1^3 \end{cases},$$

и опять же, $|x_1|^3 < |2t| < |r| < |q| < |x|^3$, то есть мы снова получили решение с меньшим $|x|$.

1.6 Целозамкнутость кольца $\mathcal{O}_K$

Определение 113. Пусть $f \in \mathbb{Z}[x]$. Тогда *содержание* $f = a_n x^n + \ldots + a_0$ — это $(a_0, \ldots, a_n) \stackrel{\text{def}}{=} \operatorname{cont}(f)$.

Замечание. Как мы помним, $\cong (fg) = \operatorname{cont}(f)\operatorname{cont}(g)$.

Теорема 77. *Пусть α — целое алгебраическое число. Тогда минимальный многочлен α имеет целые коэффициенты.*

Доказательство. Пусть $\alpha \in \mathcal{O}_K$, а f — минимальный многочлен α, p — унитарный многочлен с целыми коэффициентами, аннулирующий α. Тогда $p \vdots f$, то есть существует $g(x) \in \mathbb{Q}[x] \colon p(x) = f(x)g(x)$.

Ясно, что существуют $r_1, r_2 \in \mathbb{Q}$ такие, что $\widetilde{f}(x) = r_1 f(x) \in \mathbb{Z}[x]$ и $\widetilde{g}(x) = r_2 g(x) \in \mathbb{Z}[x]$, причем $\operatorname{cont}(\widetilde{f}) = \operatorname{cont}(\widetilde{g}) = 1$. Тогда старший коэффициент $r_1 r_2 f(x)g(x) = r_1 r_2 p(x)$ равен $r_1 r_2$, откуда $r_1 r_2 \in \mathbb{Z}$.

$$r_1 r_2 \operatorname{cont}(r_1 r_2 p(x)) = \operatorname{cont}(\widetilde{f}(x)\operatorname{cont}(\widetilde{g}(x))) = 1 \implies r_1 r_2 = \pm 1.$$

Изменяя знак, можем добиться, чтоб $r_1 r_2 = 1$.

Тогда старший коэффициент $p(x) = r_1 r_2 p(x) = \widetilde{f}(x)\widetilde{g}(x)$ равен e1, откуда старшие коэффициенты $\widetilde{f}$ и $\widetilde{g}$ равны ± 1. Опять же, меняя знак, можно считать, что старший коэффициент $\widetilde{f}(x)$ равен 1.

$\widetilde{f}(x) = r_1 f(x)$, а старшие коэффциенты f и $\widetilde{f}$ равны, откуда $\widetilde{f}(x) = f(x)$, то есть $f(x) \in \mathbb{Z}[x]$. □

Определение 114. Пусть A — область целостности, K — поле частных A. Пусть $\alpha \in K,\ \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$. Если из этого следует, что $\alpha \in A$, то кольцо A называют *целозамкнутым*.

Пример 38. $\mathbb{Z}$ — целозамкнуто.

Теорема 78. *Пусть $K/\mathbb{Q}$ — конечное расширение. Тогда кольцо $\mathcal{O}_K$ целозамкнуто.*

Доказательство. Пусть $\alpha \in K$, $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$, $a_i \in \mathcal{O}_K$. Покажем, что $\mathbb{Z}[\alpha]$ — конечнопорожденная абелева группа.

В самом деле,

$$\mathbb{Z}[\alpha] \leq \mathbb{Z}[\alpha, a_0, \ldots, a_{n-1}] = \langle \alpha^m a_0^{k_0} \ldots a_{n-1}^{k_{n-1}} \mid m < n,\ k_i < n_i \rangle,$$

где n_i — степень унитарного многочлена с корнем a_i. □

1.7 Кольцо целых алгебраических чисел для квадратичного расширения

Мы уже смотрели на некоторые примеры колец целых для квадратичных расширений. Сейчас мы докажем теорему, полностью описывающую их.

Теорема 79. *Пусть $K = \mathbb{Q}(\sqrt{d})$, где $d \in \mathbb{Z}$, и d свободно от квадратов. Тогда*

$$\mathcal{O}_K \cong \begin{cases} \mathbb{Z}[\sqrt{d}],\ d \not\equiv 1 \pmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right],\ d \equiv 1 \pmod 4. \end{cases}.$$

Доказательство. Во-первых, при $d \equiv 1 \pmod 4$ число $\theta = \frac{1+\sqrt{d}}{2}$ действительно является целым алгебраическим, так как

$$(t-\theta)(t-\overline{\theta}) = t^2 - (\theta+\overline{\theta}) + \theta\overline{\theta} = t^2 - t - \frac{d-1}{4} \in \mathbb{Z}[t].$$

Теперь возьмём $\alpha = x + y\sqrt{d} \in \mathcal{O}_K,\ x, y \in \mathbb{Q}$. Посмотрим на минимальный многочлен α:

$$(t-\theta)(t-\overline{\theta}) = t^2 - (\theta+\overline{\theta}) + \theta\overline{\theta} = t^2 - 2xt + x^2 - dy^2.$$

По теореме 77, он имеет целые коэффициенты, откуда $2x \in \mathbb{Z}$ и $x^2 - dy^2 \in \mathbb{Z}$. Рассмотрим теперь два случая:

- Если $2x$ — четное, то $x \in \mathbb{Z}$ и тогда $dy^2 \in \mathbb{Z}$, а так как d свободно от квадратов, $y \in \mathbb{Z}$. Тогда $\alpha \in \mathbb{Z}[\sqrt{d}]$.
- Если $2x$ — нечётно, то полагая $2x = x'$, мы понимаем, что

  $$n = x^2 - dy^2 = \frac{x'^2}{4} - dy^2 \in \mathbb{Z} \implies 4n = x'^2 - d(2y)^2 \in \mathbb{Z}.$$

  Отсюда $d(2y)^2 \in \mathbb{Z}$, а так как d свободно от квадратов, отсюда $2y \in \mathbb{Z}$.

  $$d(2y)^2 \equiv x'^2 \equiv 1 \pmod 4,$$

  Так как x' — нечётно. Значит, $y' = 2y$ и d нечётные. Но тогда $y'^2 \equiv 1 \pmod 4$, откуда $d \equiv 1 \pmod 4$ (и это значит, что это возможно лишь в этом случае). Тогда мы получаем, что

  $$\alpha = x + y\sqrt{d} = \frac{x'}{2} + \frac{y'}{2}\sqrt{d} = \frac{x'-y'}{2} + y'\frac{1+\sqrt{d}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right],$$

  так как x', y' — нечётные.

□

1.8 Разложение идеалов в произведение простых в кольцах целых числовых полей

Лемма 47. Пусть A — нётерово, $I \subset A$ — ненулевой идеал. Тогда существуют такие простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, что $\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_k \subset I$.

Доказательство. Предположим противное, то есть, что существуют идеаы, для которых не выполнено условие леммы. Выберем среди таких максимальный (мы можем так сделать в силу нётеровости кольца), назовём его I. Заметим, что I — не простой идеал, что означает, что $\exists x, y\colon\ \notin I\colon xy \in I$. Кроме того, I — собственный идеал. Значит,

$$(x) \subsetneq (x) + I, (y) \subsetneq I + (y),$$

Тогда для идеалов $I + (x)$ и $I + (y)$ условие леммы уже выполняется, то есть $\exists \mathfrak{p}_1, \ldots, \mathfrak{p}_k$ и $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ такие, что $\mathfrak{p}_1 \ldots \mathfrak{p}_k \subset I + (x)$, $\mathfrak{q}_1 \ldots \mathfrak{q}_m \subset I + (y)$. Но тогда мы имеем

$$\mathfrak{p}_1 \ldots \mathfrak{p}_k\mathfrak{q}_1 \ldots \mathfrak{q}_m \subset (I + (x))(I + (y)) \subset I, \text{ так как } xy \in I,$$

что даёт нам противоречие. □

Определение 115. Пусть $K/\mathbb{Q}$ — конечное расширение, $0 \neq I \subset \mathcal{O}_K$ — идеал. Тогда введём

$$I^{-1} \stackrel{\text{def}}{=} \{x \in K \mid xI \subset \mathcal{O}_K\}.$$

Свойства:

1. $x, y \in I^{-1} \implies x + y \in I^{-1}$.
2. Если $x \in I^{-1}$, а $a \in \mathcal{O}_K$, то $ax \in I^{-1}$.

Доказательство. Действительно, $(x + y)I \subset xI + yI \subset \mathcal{O}_K$. Если $xI \subset \mathcal{O}_K$, то для $a \in \mathcal{O}_K$ мы получим $axI = xaI = xI$, так как I — идеал в $\mathcal{O}_K$. □

Замечание. Заметим, что I^{-1} — $\mathcal{O}_K$-модуль. Кроме того, если $a \in I$, то aI^{-1} — идеал в $\mathcal{O}_K$. В частности, aI^{-1} конечнопорожден, а значит, aI^{-1} — конечнопорожденный $\mathcal{O}_K$-модуль.

Пример 39. Пусть $K = \mathbb{Q}$, тогда $\mathcal{O}_K = \mathbb{Z}$ и любой идеал $I \subset \mathbb{Z}$ имеет вид $I = (a)$. Тогда $(a)^{-1} = a^{-1}\mathbb{Z}$.

Лемма 48. Пусть $I \subset \mathcal{O}_K$ — ненулевой собственный идеал. тогда $I^{-1} \neq \mathcal{O}_K$.

Доказательство. Докажем, что существует $x \in K$ такой, что $x \notin \mathcal{O}_K$ и при этом $xI \subset \mathcal{O}_K$. Выберем в I ненулевой элемент a. Рассмотрим $(a) \subset I$, по лемме 47 найдутся такие ненулевые $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in \operatorname{Spec} \mathcal{O}_K$, что $\mathfrak{p}_1 \ldots \mathfrak{p}_k \subset (a)$.

Так как I — собственный, а кольцо $\mathcal{O}_K$ одномерно, I лежит в некотором простом идеале $\mathfrak{p}$. Так мы получаем цепочку включений

$$\mathfrak{p}_1 \ldots \mathfrak{p}_k \subset (a) \subset \mathfrak{p} \implies \exists i \colon \mathfrak{p}_i \subset \mathfrak{p}.$$

Так как оба идеала максимальны, это не включение, а равенство. Не умаляя общности, пусть $\mathfrak{p}_1 = \mathfrak{p}$. Теперь, пусть $k = 1$. Тогда мы имеем $\mathfrak{p} \subset (a) \subset I \subset \mathfrak{p} \implies I = \mathfrak{p} = (a) \implies I^{-1} = a^{-1}\mathcal{O}_K$. Значит, $x = a^{-1} \notin \mathcal{O}_K$, так как иначе $I = \mathcal{O}_K$.

Теперь пусть $k \geq 2$, выберем k минимально возможным. Тогда

$$\mathfrak{p}_2 \ldots \mathfrak{p}_k \not\subset (a) \implies \exists b \in \mathfrak{p}_2 \ldots \mathfrak{p}_k \setminus (a).$$

Тогда мы можем взять $x = \frac{b}{a}$ и он подойдёт. В самом деле,

$$xI = \frac{b}{a}I \subset \frac{b}{a}\mathfrak{p}_1 \underbrace{\subset}_{b \in \mathfrak{p}_2 \ldots \mathfrak{p}_k} \frac{\mathfrak{p}_1 \ldots \mathfrak{p}_k}{a} \subset \frac{(a)}{a} = \mathcal{O}_K$$

Остаётся проверить, что $\frac{b}{a} \notin \mathcal{O}_K$.В самом деле, если $\frac{b}{a} \in \mathcal{O}_K$, то $b \in (a)$, что противоречит выбору b. □

Замечание. Ясно, что включение $\mathcal{O}_K \subset I^{-1}$ верно всегда, так как просто по определению идеала: $\forall x \in \mathcal{O}_K\ xI \subset \mathcal{O}_K$

Возьмём $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ и рассмотрим $\mathfrak{p}\mathfrak{p}^{-1}$. С одной стороны, это идеал в $\mathcal{O}_K$, причём он содержит $\mathfrak{p}$.

Лемма 49. Пусть $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$, тогда $\mathfrak{p}\mathfrak{p}^{-1} = (1) = \mathcal{O}_K$.

Доказательство. Предположим противное, тогда в силу максимальности идеала $\mathfrak{p}$ мы имеем $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. Пусть $\mathfrak{p} = (u_1, \ldots, u_n)$, тогда если $\alpha \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$ (тут мы пользуемся леммой 48), то $\alpha u_1 \in \mathfrak{p}$ (так как мы предположили, что $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$) и мы можем написать систему уравнений

$$\begin{cases} \alpha u_1 = \sum\limits_{u=1}^{n} a_{1i} u_i \\ \alpha u_2 = \sum\limits_{u=1}^{n} a_{2i} u_i \\ \vdots \\ \alpha u_n = \sum\limits_{i=1}^{n} a_{ni} u_i \end{cases}$$

В матричной форме эта система будет иметь вид

$$\underbrace{\begin{pmatrix} \alpha - a_{11} & \dots & \dots & \dots \\ \dots & \alpha - a_{22} & \dots & \dots \\ \vdots & \vdots & \ddots & \vdots \\ \dots & \dots & \dots & \alpha - a_{nn} \end{pmatrix}}_{=B} \cdot \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = 0.$$

Значит, $\det B = 0$, что даёт нам унитарный многочлен с коэффициентами из $\mathcal{O}_K$, обнуляющий α. Тогда, так как $\mathcal{O}_K$ — целозамкнуто, $\alpha \in \mathcal{O}_K$, противоречие. □

Теперь мы достаточно подготовились, чтоб доказать, что в кольце $\mathcal{O}_K$ любой идеал единственным образом раскладывается в произведение простых.

Теорема 80 (Основная теорема арифметики для идеалов)**.** *Пусть $0 \neq I \subset \mathcal{O}_K$ — идеал. Тогда I однозначно (с точностью до перестановки сомножителей) раскладывается в произведение простых идеалов.*

Доказательство. Как обычно, проходит в два этапа.
Существование: Предположим, что существуют идеалы, не раскладывающиеся в произведение простых. Среди таких идеалов возьмём максимальный, обозанчим его I (мы можем так сделать, потому что $\mathcal{O}_K$ — нётерово кольцо). Он содержится в некотором максимальном идеале $\mathfrak{p} \in \operatorname{Specm} \mathcal{O}_K$. Тогда $I\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$ — идеал. Значит, нам остаётся показать, что $I\mathfrak{p}^{-1} \neq I$ (кроме того, ясно, что $I \subset \mathfrak{p}^{-1}I$, надо просто показать, что равенства не бывает). Покажем, что $II^{-1} = \mathcal{O}_K$, тогда мы сможем просто домножить и всё получится.

Лемма 50. Для любого идеала $I \subset \mathcal{O}_K$ мы имеем $II^{-1} = \mathcal{O}_K$.

Доказательство. Пусть это не так, тогда $II^{-1} \subset \mathfrak{q}$, где $\mathfrak{q}$ — максимальный идеал. Тогда

$$II^{-1}\mathfrak{q}^{-1} \subset \mathfrak{q}\mathfrak{q}^{-1} = \mathcal{O}_K \implies I^{-1}\mathfrak{q}^{-1} \subset I^{-1}$$

Так как $\mathfrak{q}^{-1}$ не совпадает с $\mathcal{O}_K$, мы можем выбрать $\alpha \in \mathfrak{q}^{-1} \setminus \mathcal{O}_K$. Проделывая рассуждение, аналогичное лемме 49 мы получаем, что $\alpha \in \mathcal{O}_K$, что даёт нам противоречие. □

Итак, если $I\mathfrak{p}^{-1} = I$, то $\mathfrak{p}^{-1} = \mathcal{O}_K$, что противоречит лемме 48. Значит, $I \subset I\mathfrak{p}^{-1}$, следовательно мы можем разложить $I\mathfrak{p}^{-1}$ в произведение простых:

$$I\mathfrak{p}^{-1} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_k \implies I = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_k \cdot \mathfrak{p},$$

что и требовалось.
Единственность: Пусть $\mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_m = \mathfrak{p}\mathfrak{q}_1 \dots \mathfrak{q}_n$, тогда $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_m \subset \mathfrak{q}_1 \implies \exists i \colon \mathfrak{p}_i \subset \mathfrak{q}_i$, а так как они максимальны, $\mathfrak{p}_i = \mathfrak{q}_1$, что даёт нам противоречие. □

Определение 116. Пусть $I \subset K$. I называется *дробным идеалом*, если $\exists x \neq 0 \colon xI \subset \mathcal{O}_K$ — идеал.

Пример 40. I^{-1} — дробный идеал.

Предложение 52. *Ненулевые дробные идеалы образуют группу по умножению.*

Доказательство. Легко заметить, что произведение дробных идеалов — дробный идеал. Обратный определяется как и раньше:

$$I^{-1} \stackrel{\text{def}}{=} \{x \in K \mid xI \subset \mathcal{O}_K\}.$$

Нетрудно убедиться в том, что $II^{-1} = \mathcal{O}_K$. □

Из теоремы 80 следует, что любой дробный идеал раскладывается в произведение простых идеалов (возможно, с отрицательными степенями). Действительно, пусть J — дробный идеал, тогда для некоторого $x \in K$ $xJ = I$ — идеал в $\mathcal{O}_K$, тогда

$$J = (x)^{-1}I = \mathfrak{p}_1^{-1} \dots \mathfrak{p}_k^{-1}\mathfrak{q}_1 \dots \mathfrak{q}_m.$$

Значит, группа дробных идеалов — свободная абелева группа, образующие которой — элементы $\operatorname{Spec} \mathcal{O}_K$.

Пример 41. Для кольца $\mathbb{Z}$ дробные идеалы соотвествуют рациональным числам.

Домашнее задание 4. Задачи:

1. Докажите, что кольцо $\mathcal{O}_K$ факториально тогда и только тогда, когда $\mathcal{O}_K$ — кольцо главных идеалов.
2. Разложите число $33 + 11\sqrt{-7}$ на неприводимые в кольце $\mathcal{O}_K$, где $K = \mathbb{Q}(\sqrt{-7})$.
3. Пусть $\mathfrak{p} \in \operatorname{Specm} \mathcal{O}_K$. Введём на группе дробных идеалов *нормирование* следующим образом: $\upsilon_\mathfrak{p}(I) =$ степень, с которой $\mathfrak{p}$ входит в разложение дробного идеала I. Иными словами,

$$I = \mathfrak{p}^{\upsilon_\mathfrak{p}(I)} \cdot \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_m.$$

Для $a \in K^*$ определим $\upsilon_\mathfrak{p}(a) \stackrel{\text{def}}{=} \upsilon_\mathfrak{p}((a))$. Так вот, докажите, что:

- $\upsilon_\mathfrak{p}(I + J) = \min(\upsilon_p(I), \upsilon_\mathfrak{p}(J))$.
- $\upsilon_\mathfrak{p}(I \cap J) = \max(\upsilon_p(I), \upsilon_\mathfrak{p}(J))$.
- $\upsilon_\mathfrak{p}(a + b) \geq \min(\upsilon_\mathfrak{p}(a), \upsilon_\mathfrak{p}(b))$ и равенство достигается в случае $\upsilon_\mathfrak{p}(a) \neq \upsilon_\mathfrak{p}(b)$.
- $\upsilon_\mathfrak{p}(IJ) = \upsilon_\mathfrak{p}(I) + \upsilon_\mathfrak{p}(J)$.
- $\upsilon_\mathfrak{p}(ab) = \upsilon_\mathfrak{p}(a) + \upsilon_\mathfrak{p}(b)$.

Таким образом, $\upsilon_\mathfrak{p}$ — гомоморфизм $K^* \to \mathbb{Z}$. Этот гомоморфизм называют *дискретным нормированием, соотвествующим идеалу* $\mathfrak{p}$.

1.9 Дискриминант

Определение 117. Пусть K/F — конечное сепарабельное расширение, $[K : F] = n$ и $\alpha_1, \dots, \alpha_n \in K$. Тогда *дискриминант* набора $\alpha_1, \dots, \alpha_n$ — это

$$\operatorname{disc}(\alpha_1, \dots, \alpha_n) \stackrel{\text{def}}{=} \det\bigl(\operatorname{Tr}_{K/F}(\alpha_i\alpha_j)\bigr).$$

Так как расширение K/F сепарабельно, у нас есть ровно $n = [K : F]$ вложений $\sigma_1, \dots, \sigma_n \colon K \to \mathbb{C}$ (на самом деле, мы знаем, что в $\mathbb{Q}^{alg}$).

Предложение 53. $\operatorname{disc}(\alpha_1, \dots, \alpha_n) = (\det(\sigma_i(\alpha_j))^2$.

Доказательство. Положим $(\sigma_i(\alpha_j))_{i,j=1}^n = A$ и рассмотрим A^tA, тогда

$$(A^tA)_{ij} = \sum_{k=1}^n \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^n \sigma_k(\alpha_i\alpha_j) = \operatorname{Tr}_{K/F}(\alpha_i\alpha_j).$$

□

Посмотрим теперь, как дискриминант меняется при линейном преобразовании. Пусть $(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n)M,\ M \in M_n(F)$.

Предложение 54. $\operatorname{disc}(\beta_1, \dots, \beta_n) = \operatorname{disc}(\alpha_1, \dots, \alpha_n) \cdot (\det M)^2$.

Доказательство. Действительно, это напрямую следует из предложения 53:

$$\operatorname{disc}(\beta_1, \dots, \beta_n) = \det(\sigma_i(\beta_j))^2 = \det\left(\sigma_i(\alpha_j)M\right)^2 = \operatorname{disc}(\alpha_1, \dots, \alpha_n) \cdot (\det M)^2.$$

□

Предложение 55. $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0 \Leftrightarrow \alpha_1, \ldots, \alpha_n$ — *линейно зависимы.*

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — линейно зависимы, $e_1, \ldots, e_n$ — базис K/F. Тогда

$$(\alpha_1, \ldots, \alpha_n) = (e_1, \ldots, e_n)M, \quad \det M = 0.$$

Значит, по предложению 54 мы имеем $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0$.

Теперь докажем в обратную сторону. Предположим, что $\alpha_1, \ldots, \alpha_n$ — линейно независимы, но $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det\bigl(\operatorname{Tr}_{K/F}(\alpha_i\alpha_j)\bigr) = 0$. Рассмотрим систему линейных уравнений

$$\operatorname{Tr}_{K/F}((x_1\alpha_1 + \ldots + x_n\alpha_n)\alpha_j) = 0, \ldots 1 \le j \le n.$$

Так как матрица коэффициентов этой системы — $\operatorname{Tr}_{K/F}(\alpha_i\alpha_j)$, а она вырождена, система имеет нетривиальное решение $(x_1, \ldots, x_n)$. Так как $\alpha_1, \ldots, \alpha_n$ — линейно независимы,

$$y = x_1\alpha_1 + \ldots + x_n\alpha_n \neq 0.$$

С другой стороны, $\operatorname{Tr}_{K/F}(y\alpha_j) = 0\ \forall j$. Так как α_i образуют базис K/F, по линейности мы получаем, что $\operatorname{Tr}_{K/F}(yu) = 0\ \forall u \in K$. Но, так как расширение K/F сепарабельно, $\operatorname{Tr}_{K/F}$ должен быть невырожденной формой[1].

□

Лемма 51. Пусть $B \subset A$ — свободные абелевы группы ранга n. Пусть $\omega_1, \ldots, \omega_n$ — базис A, а $\left\{\sum_{j=1}^n a_{ij}w_j\right\}$ — базис B, $a_{ij} \in \mathbb{Z}$. Тогда $|A/B| = |\det(a_{ij})|$.

Доказательство. Приведём матрицу (a_{ij}) нормальной форме Смита. Перечислим теперь элементы A/B: это в точности элементы $x_1\omega_1 + \ldots + x_n\omega_n,\ 0 \le x_i \le a_{ii} - 1$. Если мы докажем, что это в точности все попарно-различные элементы группы A/B, то утверждение будет ясно.

Пусть $\sum_{i=1}^n x_i\omega_i = \sum_{i=1}^n y_i\omega_i$, тогда $\sum_{i=1}^n (x_i - y_i)\omega_i \in B$. Посмотрим на коэффициент при ω_{11}, он может получаться только из первой строки матрицы (так как матрица верхнетреугольная), тогда $\ell a_{11} = x_1 - y_1$, но это равенство возможно только в случае, когда $x_1 = y_1$ (так как есть ограничения на x_i и y_i). Далее мы проделаем аналогичное рассуждение $\sum_{i=2}^n (x_i - y_i)\omega_i \in B$ и в итоге получим, что все такие элементы разлчины.

Теперь рассмотрим $a = x_1\omega_1 + \ldots + x_n\omega_n,\ x_i \in \mathbb{Z}$. Поделим с остатком: $x_1 = a_{11}q + r,\ 0 \le r < a_{11}$, и рассмотрим $x_1\omega_1 + \ldots + x_n\omega_n - q(a_{11}\omega_1 + \ldots + a_{1n}\omega_n) = r\omega_1 + x_2'\omega_2 + \ldots$. Так как мы вычли из a элемент из B, класс $\overline{a} \in A/B$ не изменился, а старшим коэффициентом стал r, лежащий в нужном диапазоне. Продолжая в том же духе, мы полчми, что все коэффициенты лежат в нужном диапазоне. □

Как мы помним из теоремы 73, $\mathcal{O}_K$ — конечнопорожденная свободная абелева группа ранга $n = [K : \mathbb{Q}]$ и $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}\omega_i$, где $\{\omega_i\}$ — целый базис.

Определение 118. Пусть $K/\mathbb{Q}$ — расширение степени n, $\mathcal{O}_K = \bigoplus_{i=1}^n \mathbb{Z}\omega_i$. Тогда

$$\operatorname{disc}(K) \stackrel{\text{def}}{=} \operatorname{disc}(\omega_1, \ldots, \omega_k).$$

Замечание. Дискриминант поля не зависит от выбора целого базиса. Действительно, если у нас есть какой-то другой целый базис $(u_1, \ldots, u_n)$, то

$$(\omega_1, \ldots, \omega_n)M = (u_1, \ldots, u_n), \quad M \in \mathrm{SL}_n(\mathbb{Z}).$$

$$(u_1, \ldots, u_n)M^{-1} = (\omega_1, \ldots, \omega_n)$$

$$\operatorname{disc}(u_1, \ldots, u_n) = \operatorname{disc}(\omega_1, \ldots, \omega_n) \cdot \underbrace{(\det M)^2}_{=1}$$

[1] Этим утверждением из теорией полей мы пользуемся без доказательств. Доказательство этого утверждения можно прочитать в S. Lang “Algebra”.

Определение 119 (Индекс целого алгебраического числа)**.** Пусть $K = \mathbb{Q}(\theta)$, $\theta \in \mathcal{O}_K$, положим $\operatorname{ind}(\theta) = [\mathcal{O}_K : \mathbb{Z}[\theta]] = |\mathcal{O}_K/\mathbb{Z}[\theta]|$.

Предложение 56. *В описанной выше сиутации* $\operatorname{disc}(1, \theta, \dots, \theta^{n-1}) = \operatorname{ind}(\theta)^2 \cdot \operatorname{disc}(K)$.

Доказательство. Пусть $\omega_1, \dots, \omega_n$ — целый базис. Тогда

$$(1, \theta, \dots, \theta^{n-1}) = (\omega_1, \dots, \omega_n)M \implies \operatorname{disc}(1, \dots, \theta^{n-1}) = \operatorname{disc}(K)(\det M)^2.$$

Нетрудно заметить, что по лемме 51 для $\mathbb{Z}[\theta] = B \subset A = \mathcal{O}_K$ мы имеем $|\det M| = \operatorname{ind}(\theta)$.

□

Пример 42. Пусть $K = \mathbb{Q}(\theta)$, где $\theta^3 - \theta - 1 = 0$. Как мы помним из домашнего задания, $\operatorname{disc}(1, \theta, \theta^2) = -23$. Пользуясь предложением 56 мы получаем, что $-23 = (\operatorname{ind}(\theta))^2 \cdot \operatorname{disc} K \implies \operatorname{ind}\theta = 1$, из чего следует, что $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Пример 43. Пусть $K = \mathbb{Q}(\theta)$, где $\theta^3 - \theta - 4 = 0$. Как мы помним, $\operatorname{disc}(1, \theta, \theta^2) = -4 \cdot 107 = (\operatorname{ind}\theta)^2 \cdot \operatorname{disc} K$, Тогда $\operatorname{ind}\theta = 1$ или $\operatorname{ind}\theta = 2$. С другой стороны, так как $\frac{\theta+\theta^2}{2} \in \mathcal{O}_K, \notin \mathbb{Z}[\theta]$, $\operatorname{ind}(\theta) \neq 1$. Значит, $\operatorname{ind}\theta = 2$, из чего мы имеем разложение

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\frac{\theta + \theta^2}{2}.$$

Домашнее задание 5. Задачи:

1. Предположим, что K/F — расширение Галуа, $[K : F]$ — нечётна. Докажите, что тогда для любого базиса $e_1, \dots, e_n$ расширения K/F будет выполнено $\operatorname{disc}(e_1, \dots, e_n) \in F^{*^2}$.
2. Рассмотрим $K = \mathbb{Q}(\sqrt[p]{1})$. Тогда $\zeta, \zeta^2, \dots \zeta^{p-1}$ образуют базис $K/\mathbb{Q}$. Докажите, что $|\operatorname{disc}(\zeta, \zeta^2, \dots, \zeta^{p-1})| = p^{p-2}$. *Hint:* тут можно действовать строго согласно определению 117.
3. Пусть $K/\mathbb{Q}$ — расширение степени n, $K = \mathbb{Q}(\theta)$, где $\theta^n + a_{n-1}\theta^{n-1} + \dots + a_0 = 0$ и пусть p — такое простое число, что $v_p(a_0) = 1$ и $v_p(a_i) \geq 1$. Докажите, что тогда $p \nmid \operatorname{ind}(\theta)$.
4. Докажите, что если $K = \mathbb{Q}(\sqrt[p]{1})$, где p — простое, то $\mathcal{O}_K = \mathbb{Z}[\zeta]$, где $\zeta^p = 1$.
5. Пусть $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ — максимальные идеалы кольца $\mathcal{O}_K$, $n_1, \dots, n_k \in \mathbb{Z}$. Докажите, что существует $\alpha \in K^* \colon v_{\mathfrak{p}_i}(\alpha) = n_i \; \forall 1 \leq i \leq n_k$.
6. Пусть $I \subset \mathcal{O}_K$ — идеал, J — дробный идеал. Докажите, что $\exists x \in K^* \colon xJ + I = \mathcal{O}_K$.
7. Докажите, что любой дробный идеал порождается двумя элементами.

Приведём сейчас другое, конструктивное доказательство того, что $\mathcal{O}_K$ — конечнопорожденная абелева группа.

Возьмем $\omega_1, \omega_2, \dots, \omega_n \in \mathcal{O}_K$, где $\omega_1, \dots, \omega_n$ — базис K на $\mathbb{Q}$. Тогда $\operatorname{disc}(\omega_1, \dots, \omega_n) \in \mathbb{Z}$, возьмем набор $(\omega_1, \dots, \omega_n)$ с минимальным модулем дискриминанта. Докажем, что тогда он и будет целым базисом.

Возьмем $x \in \mathcal{O}_K$, $x = \sum a_i\omega_i$, $a_i \in \mathbb{Q}$ и покажем, что $a_i \in \mathbb{Z}$. Предположим противное, не умаляя общности $a_1 \notin \mathbb{Z}$.

$$x \in \mathcal{O}_K \implies \sum \{a_i\}\omega_i = x - \sum [a_i]\omega_i \in \mathcal{O}_K.$$

Перейдём к набору $(\sum \{a_i\}\omega_i, \omega_2, \dots, \omega_n)$. Покажем, что модуль его дискриминанта уменьшился. Действительно,

$$(\sum \{a_i\}\omega_i, \omega_2, \dots, \omega_n) = (\omega_1, \dots, \omega_n) \cdot \begin{pmatrix} \{a_1\} & 0 & \dots & 0 \\ \{a_2\} & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \{a_n\} & 0 & \dots & 1 \end{pmatrix}.$$

а определитель матрицы, написаной справа равен $\{a_1\} \leq 1$ (так как матрица нижнетреугольная).

Теорема 81. *Пусть p — простое, а $K = \mathbb{Q}\big(\sqrt[p]{1}\big)$. Тогда $\mathcal{O}_K = \mathbb{Z}[\zeta]$, где $\zeta^p = 1$.*

Доказательство. Вычислим сначала $\operatorname{disc}(1,\zeta,\dots,\zeta^{p-2}) = \det\bigl(\operatorname{Tr}(\zeta^{i+j})\bigr)_{i,j=1}^{n}$. Ясно, что для каждого $i = 2,\dots,p-2$ найдётся единственный $j = 2,\dots,p-2$ такой, что $i+j \equiv 0 \pmod p$[2]. Значит, в каждом столбце, кроме второго, будет стоять элемент $\operatorname{Tr}(\zeta^0) = \operatorname{Tr}(1) = [K:\mathbb{Q}] = p-1$, причем ровно один раз (и аналогичное верно для строк).

Минимальным многочленом для ζ является

$$\frac{t^p-1}{t-1} = 1 + \dots + t^{p-1},$$

откуда $\operatorname{Tr}(\zeta^k) = 0, k = 1,\dots,p-2$. Значит, нам нужно вычислить вот такой определитель:

$$\det\begin{pmatrix} p-1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & -1 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ -1 & -1 & p-1 & \dots & -1 \end{pmatrix}.$$

$$\begin{pmatrix} p-1 & -1 & -1 & \dots & -1 \\ -1 & -1 & -1 & \dots & -1 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ -1 & -1 & p-1 & \dots & -1 \end{pmatrix} \sim \begin{pmatrix} p & 0 & 0 & \dots & 0 \\ -1 & -1 & -1 & \dots & -1 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & p & \dots & 0 \end{pmatrix} \sim \begin{pmatrix} p & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & p & \dots & 0 \end{pmatrix}$$

Отсюда уже ясно, что $\operatorname{disc}(1,\zeta,\dots,\zeta^{p-2}) = (-1)^{\frac{p-1}{2}}p^{p-2}$.

Теперь воспользуемся одной из домашних задач. Заметим, что в нашем случае совершенно ясно, что минимальный многочлен ζ Эйзенштейнов, а тогда $\operatorname{ind}(\zeta) \not\vdots\ p$. С другой стороны, по предложению 56 $\operatorname{ind}(\zeta) \mid \operatorname{disc}(1,\zeta,\dots,\zeta^{p-2})(-1)^{\frac{p-1}{2}}p^{p-2}$. Значит, $\operatorname{ind}(\theta) = 1$ то есть

$$|\mathcal{O}_K/\mathbb{Z}[\theta]| = 1 \implies \mathcal{O}_K = \mathbb{Z}[\theta].$$

□

Теорема 82 (Д/З №7, задача 2)**.** *Пусть $K = \mathbb{Q}\bigl(\sqrt[n]{1}\bigr)$, то $\mathcal{O}_K = \mathbb{Z}[\zeta]$, где $\zeta^{p^n} = 1$*

Доказательство. В доказательстве первообразный корень степени m мы будем обозначать, как ζ_m. Воспользуемся задачей 4 Д/З №5, то есть вот таким фактом

Лемма 52. Пусть $K/\mathbb{Q}$ — конечное сепарабельное расширение, $K = \mathbb{Q}(\theta),\ \theta \in \mathcal{O}_K, [K:\mathbb{Q}] = n$. Тогда

$$\operatorname{disc}(1,\theta,\theta^2,\dots,\theta^{n-1}) = \prod_{i\neq j}(\sigma_i(\theta) - \sigma_j(\theta)) = (-1)^{\frac{n(n-1)}{2}}\operatorname{N}_{K/F}(f'(\theta)),\ \text{где}$$

f — минимальный многочлен θ.

Доказательство леммы. Ясно, что если $\sigma_i,\ i = 1,\dots,n$ — все вложения

$$f(t) = \prod_{i=1}^{n}(t - \sigma_i\theta).$$

С другой стороны, мы знаем, что

$$\operatorname{disc}(1,\theta,\dots,\theta^{n-1}) = \det(\sigma_i(\theta^{j-1}))^2.$$

Так как $\sigma_i(\theta^{j-1}) = \sigma_i(\theta)^{j-1}$, матрица в правой части равенства представляет из себя матрицу Вандермонда, а тогда

$$\det\begin{pmatrix} 1 & \sigma_1(\theta) & \dots & \sigma_1(\theta)^{n-1} \\ 1 & \sigma_2(\theta) & \dots & \sigma_2(\theta)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\theta) & \dots & \sigma_n(\theta)^{n-1} \end{pmatrix} = \prod_{i<j}(\sigma_j(\theta) - \sigma_i(\theta)).$$

[2] Действительно, это $p-i$.

Возводя в квадрат, получаем

$$\operatorname{disc}(1,\theta,\dots,\theta^{n-1}) = \prod_{i<j}(\sigma_j(\theta)-\sigma_i(\theta))^2.$$

Теперь продифференцируем f:

$$f(t) = \prod_{i=1}^{n}(t-\sigma_i\theta) \implies f'(\sigma_i(\theta)) = \prod_{j\neq i}(\sigma_j(\theta)-\sigma_i(\theta)).$$

Перемножим эти равенства по $i = 1,\dots,n$:

$$\prod_{i=1}^{n} f'(\sigma_i(\theta)) = \prod_{i=1}^{n}\prod_{j\neq i}(\sigma_j(\theta)-\sigma_i(\theta)).$$

Перепишем правую часть равенства, объединяя

$$(\sigma_j(\theta)-\sigma_i(\theta)) \text{ и } (\sigma_i(\theta)-\sigma_j(\theta)) \rightsquigarrow -(\sigma_j(\theta)-\sigma_i(\theta))^2.$$

Так как пар, где $i<j$ всего $\binom{n}{2} = \frac{n(n-1)}{2}$, мы получаем

$$\prod_{i=1}^{n}\prod_{j\neq i}(\sigma_j(\theta)-\sigma_i(\theta)) = (-1)^{\frac{n(n-1)}{2}}\prod_{i<j}(\sigma_j(\theta)-\sigma_i(\theta))^2$$

и отсюда мы имеем

$$\prod_{i<j}(\sigma_j(\theta)-\sigma_i(\theta))^2 = (-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n} f'(\sigma_i(\theta)).$$

Остаётся заметить, что так как σ_i — гомоморфизмы, а f' — многочлен, мы имеем

$$\prod_{i=1}^{n} f'(\sigma_i(\theta)) = \prod_{i=1}^{n}\sigma_i(f'(\theta)) = \mathrm{N}_{K/\mathbb{Q}}(f'(\theta)),$$

что завершает доказательство.

□

Минимальный многочлен ζ_{p^n} — это

$$\Phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1}, \quad \operatorname{disc}(1,\zeta_{p^n},\dots,\zeta_{p^n}^{\varphi(p^n)-1}).$$

Значит, нам надо вычислить норму числа

$$\Phi'_{p^n}(\zeta_{p^n}) = \frac{p^n\zeta_{p^n}^{p^n-1}}{\zeta_{p^n}^{p^{n-1}}-1} = \frac{p^n\zeta_{p^n}^{-1}}{\zeta_{p^n}^{p^{n-1}}-1} = \frac{p^n\zeta_{p^n}^{-1}}{\zeta_p-1}.$$

так как $\zeta_{p^n}^{p^{n-1}} = \zeta_p$. Теперь, так как $p^n\in\mathbb{Q}$, а $[\mathbb{Q}(\zeta_{p^n}):\mathbb{Q}] = p^n-p^{n-1}$, мы имеем

$$\mathrm{N}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}(p^n\zeta^{-1}) = p^{n(p^n-p^{n-1})}.$$

Так как $\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p-1) = p$. Тогда мы можем вычислить норму телескопически. Так как $\zeta_p-1\in\mathbb{Q}(\zeta_p)$, а $[\mathbb{Q}(\zeta_{p^n}):\mathbb{Q}(\zeta_p)] = p^{n-1}$, мы имеем

$$\mathrm{N}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}(\zeta_p-1) = \mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\Big(\mathrm{N}_{\mathbb{Q}(\zeta_{p^n}/\mathbb{Q}(\zeta_p)}(\zeta_{p-1})\Big) = \mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p-1)^{p^{n-1}} = \big(\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p-1)\big)^{p^{n-1}} = p^{p^{n-1}}.$$

Таким образом, мы наконец получаем, что

$$\mathrm{N}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}\left(\frac{p^n\zeta_{p^n}^{-1}}{\zeta_p-1}\right) = \frac{p^{n(p^n-p^{n-1})}}{p^{p^n-1}} = p^{p^{n-1}(np-n-1)}.$$

□

Напоминание про нормальную форму Смитта:
Пусть $B \subset A$ — свободные абелевы группы ранга n, причем $A = \bigoplus \mathbb{Z}x_i$, $B = \langle \sum_{j=1}^{n} a_{ij}x_j,\ 1 \le i \le n \rangle$. Тогда мы можем явно вычислить задание факторгруппы A/B образующими и соотношениями.

Рассмотрим матрицу

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \dots & \dots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

Рассмотрим автоморфизм группы A, который переводит x_1 в $x_1 + cx_2,\ c \in \mathbb{Z}$, а остальные образующие переводит в себя. Что произойдет с матрцией в результате этого изоморфизма? Ко второму столбцу прибавится первый, умноженный на c. Аналогично мы можем делать для любых столбцов. Кроме того, мы можем менять их местами посредством изоморфизмов вида $x_1 \mapsto x_2, x_2 \mapsto x_1$. При таких преобразованиях факторгруппа B/A будет оставаться такой же, так как: $A/B \cong A/f(B)$. Соотвественно, с помощью таких операций матрицу мы можем диагонализовать. В итоге мы получим диагональную матрциу

$$\begin{pmatrix} \alpha_1 & 0 & 0 & \dots & 0 \\ 0 & \alpha_2 & 0 & \dots & 0 \\ 0 & 0 & \alpha_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \alpha_{nn} \end{pmatrix}$$

1.10 Норма идеала

Определение 120. Пусть $K/\mathbb{Q}$ — конечное расширение, $0 \neq I \subset \mathcal{O}_K$ — идеал. Тогда, как мы знаем из теоремы 32, $|\mathcal{O}_K/I| < \infty$. *Нормой идеала* I мы будем называть целое число

$$\mathrm{N}_{K/\mathbb{Q}}(I) \stackrel{\text{def}}{=} |\mathcal{O}_K/I|$$

Замечание. Вообще говоря, норма идеала определяется для любого дедекиндова кольца, соответствующего некоторому расширению и обычно является идеалом. В нашем случае мы рассматриваем кольцо целых, где для любого идеала можно выбрать наименьшую по модулю неотрицательную порождающую, поэтому у нас норма — число.

Хотелось бы, чтоб норма главного идеала была равна норме порождающего его элемента (в смысле нормы для расширения полей).

Предложение 57. *Пусть $a \in \mathcal{O}_K$, тогда* $\mathrm{N}((a)) = \left|\mathrm{N}_{K/\mathbb{Q}}(a)\right|$.

Доказательство. Пусть $\omega_1, \dots, \omega_n$ — целый базис $\mathcal{O}_K$, а

$$a\omega_i = \sum_{j=1}^{n} b_{ij}\omega_j,\ b_{ij} \in \mathbb{Z}$$

Тогда с одной стороны мы посчитали оператор умножения на a на базисных векторах, то есть по определению $\mathbb{N}_{K/\mathbb{Q}}(a) = \det((b_{ij}))$.

С другой стороны, по предложению 51 мы имеем $|\det(b_{ij})| = |\mathcal{O}_K/a\mathcal{O}_K|$, что и требовалось. □

Заметим, что тогда мы получаем и мультипликативность для главных идеалов:

$$\mathrm{N}((a))\,\mathrm{N}((b)) = |\,\mathrm{N}_{K/\mathbb{Q}}(a)||\,\mathrm{N}_{K/\mathbb{Q}}(b)| = |\,\mathrm{N}_{K/\mathbb{Q}}(ab)| = \mathrm{N}((ab)).$$

Хотелось бы теперь обобщить это на произвольные идеалы. Для этого нам понадобятся задачи из ДЗ 5.

Лемма 53 (Задача 5 из ДЗ 5)**.** Пусть $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ — максимальные идеалы кольца $\mathcal{O}_K, n_1, \dots, n_k \in \mathbb{Z}$. Докажите, что существует $\alpha \in K^*$: $\upsilon_{\mathfrak{p}_i}(\alpha) = n_i\ \forall 1 \le i \le n_k$.

Доказательство. Заметим, что идеалы $\mathfrak{p}_i^{n_i}$ попарно взаимнопросты. Выберем $x_i \in \mathfrak{p}_i^{n_i} \setminus \mathfrak{p}_i^{n_i+1}$. Тогда по КТО существует $x \equiv x_i \pmod{\mathfrak{p}_i^{n_i+1}}$. Тогда

$$\upsilon_{\mathfrak{p}_i}(x) = \upsilon_{\mathfrak{p}_i}((x - x_i) + x_i) = \min(\upsilon_{\mathfrak{p}_i}(x - x_i), \upsilon_{\mathfrak{p}_i}(x_i)) = \min(n_i, n_i + 1) = n_i.$$

□

Лемма 54 (Задача 6 из ДЗ 5)**.** Пусть $I \subset \mathcal{O}_K$ — идеал, J — дробный идеал. Докажите, что $\exists x \in K^* \colon xJ + I = \mathcal{O}_K$.

Доказательство. Во-первых, J сразу можно полагать целым, так как мы можем сначала домножить его на элемент, превращающий его в целый, а потом уже что-то с ним делать. Разложим I в произведение простых:

$$I = \mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_m^{k_m}.$$

Соотвественно, легко найти $y \in K^* \colon \upsilon_{\mathfrak{p}_i}(yJ) = 0$. Проблема в том, что yJ может оказаться не целым идеалом. Предположим, что это так.

$$yJ = \prod_{i=1}^{\ell} \mathfrak{q}_i^{-r_i} \cdot \prod_{j=1}^{r} \mathfrak{r}_j^{\ell_i}, \text{ где } \ell_i \geq 0,\ r_i \geq 0.$$

По лемме 53 $\widetilde{y} \in \mathcal{O}_K \colon \upsilon_{\mathfrak{q}_i}(\widetilde{y}) = r_i,\ \upsilon_{\mathfrak{p}_i}(\widetilde{y}) = 0$, тогда ясно, что $y\widetilde{y}J$ — целый идеал, который не делится на $\mathfrak{p}_i$, следовательно он взаимнопрост с I, что и требовалось. □

Теорема 83 (Задача 7 из ДЗ 5)**.** *Любой дробный идеал I порождается двумя элементами.*

Доказательство. Возьмем $x \in \mathcal{O}_K$ такой, что $xI^{-1} \subset \mathcal{O}_K$ — целый идеал. Тогда по лемме 54 (тут у нас xI^{-1} — целый идеал, I^{-1} — дробный) найдётся $y \in K^*$ такой, что

$$xI^{-1} + yI^{-1} = \mathcal{O}_K \implies xI^{-1}I + yI^{-1}I = I \implies I = (x) + (y) = (x, y).$$

□

Домашнее задание 6 (Осторожно, открытая задача)**.** Существует ли кольцо, в котором каждый идеал порождается тремя элементами, причём, есть идеал, который не порождается двумя элементами.

Теорема 84 (Мультипликативность нормы идеала)**.** *Если I, J — два ненулевых идеала в $\mathcal{O}_K$, то для их норм верно равенство* $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$.

Доказательство. Сравним индексы: $|\mathcal{O}_K/IJ| = |\mathcal{O}_K/I| \cdot |I/IJ|$. Значит, остаётся показать, что $|\mathcal{O}_K/J| = |I/IJ|$. По лемме 54 найдём $x \in K^* \colon xI + J = \mathcal{O}_K$. Тогда воспользуемся теоремой о гомоморфизме и взаимной простотой:

$$|\mathcal{O}_K/J| = |(xI + J)/J| = |xI/xI \cap J| = |xI/xIJ| = |I/IJ|\,.$$

□

1.11 Индекс ветвления и степень инерции

Определение 121. Возьмем простое число $p \in \mathbb{Z}$ и рассмотрим главный идеал $(p) = p\mathbb{Z} \subset \mathbb{Z}$. Этот же идеал мы можем рассматривать, как главный идеал в кольце $\mathcal{O}_K$. Там он уже не обязательно будет простым, но будет раскладываться в произведение простых:

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdot \ldots \cdot \mathfrak{p}_k^{e_k},$$

причем набор идеалов $\mathfrak{p}_i$ будет своим для каждого простого числа p (т.е. для различных простых чисел эти наборы не будут пересекаться, так как $p\mathcal{O}_K$ и $q\mathcal{O}_K$ взаимнопросты для простых p и q). Тогда число e_i называют *индексом ветвления* идеала $\mathfrak{p}_i$.

Пусть теперь $\mathfrak{p} \in \operatorname{Specm}(\mathcal{O}_K)$, тогда $\mathfrak{p} \cap \mathbb{Z}$ — простой идеал в $\mathbb{Z}$, значит $\mathfrak{p} \cap \mathbb{Z} = (p)$ для некоторого простого $p \in \mathbb{Z}$, при том $(p) \subset \mathfrak{p} \implies (p)\mathfrak{p}^{-1} \subset \mathcal{O}_K$ — идеал. Его мы можем разложить на простые:

$$(p)\mathfrak{p}^{-1} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdot \ldots \cdot \mathfrak{p}_k^{e_k} \implies (p) = \mathfrak{p} \cdot \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}$$

Таким образом, простые идеалы в $\mathcal{O}_K$ находятся в соотвествии с простыми числами.

Определение 122. Как известно, для $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ факторкольцо $\mathcal{O}_K/\mathfrak{p}$ будет полем. Это поле — конечное расширение $\mathbb{F}_p$ так как у нас есть естественное вложение $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$. Значит, $|\mathcal{O}_K/\mathfrak{p}| = p^f$. Число f называется *степенью инерции* идеала $\mathfrak{p}$. Иными словами, *степень инерции* — это $[\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$.

Замечание. Заметим, что сразу из нашего определения нормы идеала мы имеем $|\mathcal{O}_K/\mathfrak{p}| = \mathrm{N}(\mathfrak{p})$.

Возьмем простое число p и рассмотрим главный идеал $p\mathcal{O}_K$. Тогда если $n = [K : \mathbb{Q}]$, то с одной стороны,

$$p^n = \mathrm{N}_{K/\mathbb{Q}}(p) \underbrace{=}_{\text{Предл. } 57} \mathrm{N}(p\mathcal{O}_K),$$

а с другой стороны мы имеем

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}, \quad \mathrm{N}(\mathfrak{p}_i) = |\mathcal{O}_K/\mathfrak{p}_i| = p^{f_i}$$

применяя к этому равенству норму, и, пользуясь её мультипликативностью, имеем

$$p^n = \mathrm{N}(p\mathcal{O}_k) = \prod_{i=1}^{k} \mathrm{N}(\mathfrak{p}_i)^{e_i} = \prod_{i=1}^{k} \left(p^{f_i}\right)^{e_i}.$$

Тогда, приравнивая степени, мы получаем формулу, устанавливающую соотношение между *индексом ветвления*, *степенью инерции* и степенью расширения:

$$\sum_{i=1}^{k} e_i f_i = n. \tag{3.1}$$

Из этой формулы можно сделать много полезных выводов. Нетрудно заметить, что случае квадратичного расширения индекс ветвления, как и степень инерции, будут равны единице. Также ясно, что $1 \leq e_i f_i \leq n$, то есть, эти числа не могут быть произвольными.

Ветвление при расширении Галуа:

Пусть $K/\mathbb{Q}$ — конечное расширение. Тогда группа Галуа $\mathrm{Gal}(K/\mathbb{Q})$ действует и на идеалах кольца $\mathcal{O}_K$. Кроме того, она оставляет на месте $\operatorname{Specm} \mathcal{O}_K$ (т.е. $\forall \mathfrak{p} \in \operatorname{Specm}(\mathcal{O}_K)\ \sigma\mathfrak{p} \in \operatorname{Specm}(\mathcal{O}_K)$), так как $\forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})\ \mathcal{O}_K/\mathfrak{p} \cong \sigma\mathcal{O}_K/\sigma\mathfrak{p} \cong {}^3\mathcal{O}_K/\sigma\mathfrak{p}$.

Определение 123. Если $\mathfrak{p} \in \operatorname{Specm}(\mathcal{O}_K)$ и $\mathfrak{p} \cap \mathbb{Z} = (p)$, то будем говорить, что идеал $\mathfrak{p}$ *висит* или *сидит* над простым числом $p \in \mathbb{Z}$.

Теорема 85. *Действие* $\mathrm{Gal}(K/\mathbb{Q})$ *на множестве простых идеалов, висящих над простым числом* p.

Доказательство. Предположим, что есть два простых идеала $\mathfrak{p}, \widetilde{\mathfrak{p}}$: $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z} = \widetilde{\mathfrak{p}} \cap \mathbb{Z}$, для которых утверждение теоремы не верно. То есть, $\forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})\ \sigma\mathfrak{p} \neq \widetilde{\mathfrak{p}}$. Тогда

$$\{\sigma\mathfrak{p} \mid \sigma \in \mathrm{Gal}(K/\mathbb{Q})\} \cap \{\sigma\widetilde{\mathfrak{p}} \mid \sigma \in \mathrm{Gal}(K/\mathbb{Q})\} = \varnothing.$$

По КТО мы можем выбрать такой элемент $x \in \mathcal{O}_K$, что

$$x \equiv 0 \pmod{\sigma\mathfrak{p}} \quad x \equiv 1 \pmod{\sigma\widetilde{\mathfrak{p}}} \quad \forall \sigma \in \mathrm{Gal}(K/\mathbb{Q}).$$

Применим теперь норму:

$$\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{\tau \in \mathrm{Gal}(K/Q)} \tau x \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z} = \widetilde{\mathfrak{p}} \cap \mathbb{Z} \implies \mathrm{N}_{K/\mathbb{Q}}(x) \in \widetilde{\mathfrak{p}}.$$

Значит, так как $\widetilde{\mathfrak{p}} \in \operatorname{Spec} \mathcal{O}_K$, $\exists \tau \in \mathrm{Gal}(K/\mathbb{Q})$: $\tau x \in \widetilde{\mathfrak{p}} \Leftrightarrow x \in \tau^{-1}\widetilde{\mathfrak{p}}$. Но, с дугой стороны, ранее мы отметили, что $\forall \tau \in \mathrm{Gal}(K/\mathbb{Q})\ \tau x \equiv 1 \pmod{\widetilde{\mathfrak{p}}}$. □

[3] В самом начале курса мы уже отмечали, что $\forall \alpha \in \mathcal{O}_K$, $\forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})\ \sigma\alpha \in \mathcal{O}_K$.

Следствие 33. *Пусть $K/\mathbb{Q}$ — расширение Галуа, p — простое и*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdot\ldots\cdot\mathfrak{p}_k^{e_k}$$

Тогда все индексы ветвления и все степени инерции равны.

Доказательство. Так как действие транзитивно, для любой пары $\mathfrak{p}_i, \mathfrak{p}_j$ найдётся $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ такой, что $\sigma\mathfrak{p}_i = \mathfrak{p}_j$. Тогда

$$p^{f_i} = |\mathcal{O}_K/\mathfrak{p}_i| = |\sigma\mathcal{O}_K/\sigma\mathfrak{p}_i = \mathcal{O}_k/\mathfrak{p}_j| = p^{f_j} \implies f_i = f_j.$$

Теперь докажем, что равны индексы ветвления. В самом деле,

$$p\mathcal{O}_K = \mathfrak{p}_i^{e_i}\mathfrak{p}_j^{e_j}\cdot\ldots\cdot\mathfrak{p}_k^{e_k} = \sigma(p\mathcal{O}_K) = \sigma(\mathfrak{p}_i)^{e_i}\sigma(\mathfrak{p}_j)^{e_i}\cdot\ldots = \mathfrak{p}_j^{e_i}\cdot\ldots,$$

Тогда, в силу единственности разложения, мы имеем $e_i = e_j$. Делая так для всех пар индексов, получаем нужное. □

Тогда равенство (3.1) примет весьма простой вид: $efk = n$.

Ветвление при квадратичном расширении:

Пусть $p \neq 2$ — простое число, рассмотрим расширение $\mathbb{Q}\left(\sqrt{d}\right)/\mathbb{Q}$, где d — целое и свободно от квадратов. Тогда в силу формулы $\sum e_i f_i = 2$ мы получаем, что возможны такие варианты разложения:

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2,\ \mathfrak{p}_1 \neq \mathfrak{p}_2, \quad p\mathcal{O}_K = \mathfrak{p}, \quad p\mathcal{O}_K = \mathfrak{p}^2.$$

Пусть $p \mid d$, тогда $p\mathcal{O}_K = (p, \sqrt{d})^2$. Действительно, нам надо проверить

$$(p) = (p^2, p\sqrt{d}, d) \Leftrightarrow (1) = \left(p, \sqrt{d}, \frac{d}{p}\right),$$

а это так, потому что $(p, \frac{d}{p}) = 1$ (так как d свободно от квадратов). Кроме того, заметим, что отсюда в частности следует, что идеал $(p, \sqrt{d})^2$ — простой.

Теперь рассмотрим случай, когда $p \not| d$. Начнём со случая, когда $\left(\frac{d}{p}\right) = 1$. Тогда $x^2 - d = pm$. Тогда

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2, \text{ где } \mathfrak{p}_1 = (p, x + \sqrt{d}),\ \mathfrak{p}_2 = (p, x - \sqrt{d}).$$

Действительно, перемножим эти идеалы:

$$\mathfrak{p}_1\mathfrak{p}_2 = (p^2, p(x - \sqrt{d}), p(x + \sqrt{d}), pm) = (p) \Leftrightarrow (p, x - \sqrt{d}, x + \sqrt{d}, m) = (, 2x, x + \sqrt{d}, m) = (1),$$

так как $(p, 2x) = 1$, а это так в силу того, что $x^2 = d + pm,\ d \not\vdots p \implies 2x \not\vdots p$ (тут мы предположили, что $p \neq 2$, этот случай надо разбирать отдельно).

Остаётся случай, когда $\left(\frac{d}{p}\right) = -1$. Предположим, что $d \not\equiv 1 \pmod 4$. Тогда

$$\mathcal{O}_K = \mathbb{Z}\left[\sqrt{d}\right] = \mathbb{Z}[x]/(x^2 - d) \implies \mathcal{O}_K/(p) \cong \mathbb{Z}[x]/(x^2 - d, p) = \mathbb{F}_p[x]/(x^2 - d) - \text{поле},$$

так как $x^2 - d$ неприводим над $\mathbb{F}_p$. Ясно, что отсюда следует, что $p\mathcal{O}_K$ максимален. Тепеь, если $d \equiv 1 \pmod 4$,

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right] \implies \mathcal{O}_K \Big/ (p) \cong \mathbb{Z}[x] \Big/ \left(x^2 - x + \frac{1-d}{4}, p\right) \cong \mathbb{F}_p \Big/ \left(x^2 - x + \frac{1-d}{4}\right) - \text{поле},$$

так как дискриминант многочлена $x^2 - x + \frac{1-d}{4}$ равен d, а d — невычет по модулю p.

Домашнее задание 7. Задачи:

1. Разобрать случай $p = 2$ в выкладках выше.
2. Пусть $K/\mathbb{Q}$ — расширение степени n, $K = \mathbb{Q}(\theta)$, где $\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_0 = 0$ и пусть p — такое простое число, что $\upsilon_p(a_0) = 1$ и $\upsilon_p(a_i) \geq 1$. Докажите, что тогда $p \not| \operatorname{ind}(\theta)$. *Hint 1:* рассмотрите $x \in \mathcal{O}_K \colon px \in \mathbb{Z}[\theta]$. Покажите, что достаточно доказать, что в этом случае $x \in \mathbb{Z}[\theta]$. *Hint 2:* докажите, что если $\mathfrak{p} \mid (p)$, то $\upsilon_{\mathfrak{p}}(\theta) = 1$ и индекс ветвления числа p равен n. *Hint 3:* $px = b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1}$. Предположите, что не все b_i делятся на p и прийдите к противоречию.
3. Исследуйте разложение идеала $2\mathcal{O}_K$, где $K = \mathbb{Q}\left(\sqrt{d}\right)$.
4. Пусть K/F — конечное сепарабельное расширение, $K = F(\theta)$, $[K : F] = n$. Докажите, что

$$\operatorname{disc}(1, \theta, \theta^2, \ldots, \theta^{n-1}) = \prod_{i \neq j}(\sigma_i(\theta) - \sigma_j(\theta)) = \mathrm{N}_{K/F}(f'(\theta)), \text{ где}$$

   f — минимальный многочлен θ.
5. Докажите, что для $\zeta = \sqrt[p^n]{1}$ и $K = \mathbb{Q}(\zeta)$ будет справедлив результат, аналогичный 5, то есть $\mathcal{O}_K = \mathbb{Z}[\zeta]$.
6. Пусть $f, g \in \mathcal{O}_K[x]$, то $\operatorname{cont}(fg) = \operatorname{cont}(f) \cdot \operatorname{cont}(g)$. *Hint:* применить локальный принцип.

1.12 Группа классов идеалов и её элементарное вычисление

Понятие нормы легко распространить на дробные идеалы: если $I, J \subset \mathcal{O}_K$ — целые идеалы, то мы можем положить

$$\mathrm{N}(IJ^{-1}) \stackrel{\text{def}}{=} \frac{\mathrm{N}(I)}{\mathrm{N}(J)}$$

Проверим, что это определение корректно. Действительно, пусть $I_1 J_1^{-1} = I_2 J_2^{-1}$, тогда $I_1 J_2 = I_2 J_1$, что означает, что

$$\mathrm{N}(I_1)\,\mathrm{N}(J_2) = \mathrm{N}(I_2)\,\mathrm{N}(J_1) \implies \mathrm{N}(I_1)\,\mathrm{N}(J_1)^{-1} = \mathrm{N}(I_2)\,\mathrm{N}(J_2)^{-1}.$$

Определение 124. Как мы помним, у нас есть понятие группы дробных идеалов $\mathrm{I}(K)$ (и в силу основной теоремы арифметики, она порождена простыми идеалами).В ней есть подгруппа из *главных дробных идеалов* $a\mathcal{O}_K,\ a \in K^*$. Эту подгруппу мы будем обозначать, как $\mathrm{PI}(K)$. Факторгруппу $\mathrm{I}(K)/\mathrm{PI}(K)$ называют *группой классов идеалов* и обозначают

$$\mathcal{C}\ell(K) \stackrel{\text{def}}{=} \mathrm{I}(K)/\mathrm{PI}(K).$$

Теорема 86. *Пусть $K/\mathbb{Q}$ — конечное расширение. Тогда группа $\mathcal{C}\ell(K)$ конечна.*

Доказательство. Итак, пусть $n = [K : \mathbb{Q}]$, $\omega_1, \ldots, \omega_n$ — целый базис. Пусть $\sigma_i \colon K \to \mathbb{C}$ — все вложения K в $\mathbb{C}$, а $C = \max|\sigma_i(\omega_j)| > 0$. Возьмём произвольный элемент $\alpha \in \mathcal{C}\ell(K)$, тогда

$$\alpha^{-1} = [J],\ J \text{ — целый идеал в кольце } \mathcal{O}_K.$$

Тогда $\alpha = [J^{-1}]$. Рассмотрим множество

$$S = \left\{ \sum_{i=1}^{n} x_i\omega_i \;\middle|\; 0 \leq x_i \leq \left[\mathrm{N}(J)^{\frac{1}{n}}\right] \right\}, \quad |S| > \left(|\,\mathrm{N}(J)|^{\frac{1}{n}}\right)\mathrm{N}(J) = |\mathcal{O}_K/J|.$$

Из оценки на порядок следует, что найдутся $\sum_{i=1}^{n} x_i\omega_i,\ \sum_{j=1}^{n} y_i\omega_i \in S$ такие, что

$$z = \sum_{i=1}^{n}(x_i - y_i)\omega_i \in J.$$

Рассмотрим идеал $I = zJ^{-1}$, это целый идеал кольца $\mathcal{O}_K$ (так как $z \in J$), $[I] = [J^{-1}] = \alpha$, так как они отличаются на главный идеал. Рассмотрим $[I] \cdot [J] = (z) = z\mathcal{O}_K$ и оценим норму этого главного идеала:

$$\mathrm{N}(I)\,\mathrm{N}(J) = \mathrm{N}(IJ) = \mathrm{N}((z)) = |\mathrm{N}(z)| = \prod_{j=1}^{n} \left|\sigma_j\left(\sum_{i=1}^{n}(x_i - y_i)\omega_i\right)\right| \le \prod_{j=1}^{n}\left(\sum_{i=1}^{n}|x_i - y_i|\,|\sigma_j(\omega_i)|\right) \le$$

$$\underbrace{\le}_{|x_i - y_i| < 2\,\mathrm{N}(J)^{\frac{1}{n}},\ |\sigma_j(\omega_i) < C|} \prod_{j=1}^{n}\left(n \cdot 2\,\mathrm{N}(J)^{\frac{1}{n}} \cdot C\right) = 2n^n C^n\,\mathrm{N}(J) \implies \mathrm{N}(I) \le 2n^n \cdot C^n.$$

Таким образом мы показали, что для любого класса из $\mathcal{C}\ell(K)$ мы можем выбрать представителя с ограниченной нормой. Но, идеалов с ограниченной нормой лишь конечное число, так как

$$I = \mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_m^{k_m} \implies \mathrm{N}(I) = \prod_{i=1}^{m} \mathrm{N}(\mathfrak{p}_k)^{k_i} \le 2 \cdot n^n C^n.$$

, а для выполнения этого неравенства можно подобрать лишь конечное число $\mathfrak{p}_i$, так как $\mathrm{N}(\mathfrak{p}_i) = |\mathcal{O}_K/\mathfrak{p}_i| \ge p$ (так как $\mathcal{O}_K/\mathfrak{p}_i$ — это векторное пространство над $\mathbb{F}_p$, где $p\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}_i$). Это даёт нам, что у нас конечное число классов идеалов.

□

Пример 44. Вычислим группу классов идеалов для поля $K = \mathbb{Q}\big(\sqrt{-14}\big)$.

Основной **факт** состоит в том, что произвольный $\mathfrak{p} \in \operatorname{Spec}\mathcal{O}_K$ выражается через максимальные идеалы, висящие только над (2) и (3). Пока что поверим в это и посчитаем при помощи этого факта группу $\mathcal{C}\ell(K)$.

Нетрудно убедиться в том, что

$$2\mathcal{O}_K = (2) = (2, \sqrt{-14})^2 = \mathfrak{p}_2^2, \quad \mathrm{N}(\mathfrak{p}_2) = 2.$$

Так как $\left(\frac{-14}{3}\right) = 1$, $3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_3'$. Как мы знаем, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$, а в этом кольце

$$\mathrm{N}_{K/\mathbb{Q}}(a + b\sqrt{-14}) = a^2 + 14b^2 \ne 2 \implies \mathfrak{p}_2 - \text{не может быть главным идеалом,}$$

из чего следует, что образ $\mathfrak{p}_2$ нетривиален в группе $\mathcal{C}\ell(K)$.

Кроме того, так как $\mathrm{N}((3)) = 9$, $\mathrm{N}(\mathfrak{p}^3) = \mathrm{N}(\mathfrak{p}_3') = 3$, что даёт нам то же самое. Заметим, что $\mathfrak{p}_3^2$ не является главным идеалом, но $[\mathfrak{p}_3^2] = [\mathfrak{p}_2]$. Действительно, возьмем $(2 + \sqrt{-14})$, $\mathrm{N}((2 + \sqrt{-14}) = 18$, но идеал $(2 + \sqrt{-14})$ раскладывается в произведение максимальных, лежащих либо над (2), либо над (3), так $\mathrm{N}(2 + \sqrt{-14}) = 18 = 2 \cdot 3^2$. Это даёт нам, что

$$(2 + \sqrt{-14}) = \mathfrak{p}_2\mathfrak{p}_3^{(?)}\mathfrak{p}_3^{(?)}.$$

Так как $(1 + \sqrt{-14})(1 - \sqrt{-14}) = 15$, мы можем положить $\mathfrak{p}_3 = (3, 1 + \sqrt{-14})$, а $\mathfrak{p}_3' = (3, 1 - \sqrt{-14})$. Так как $(2 + \sqrt{-14}) \in (3, 1 - \sqrt{-14})$, мы можем заключить, что $\mathfrak{p}_2\mathfrak{p}_3^{(?)}\mathfrak{p}_3^{(?)} \subset \mathfrak{p}_3'$, что даёт нам

$$[\mathfrak{p}_2][\mathfrak{p}_3']^2 = [1], \quad [\mathfrak{p}_2] = [\mathfrak{p}_3]^2$$

Теперь докажем озвученный в начале примера **факт** индукцией по p: $p\mathbb{Z} = \mathbb{Z} \cap \mathfrak{p}$.

$$\mathfrak{p}_2^2 = (2), \quad \mathfrak{p}_7^2 = (7), \quad \mathfrak{p}_2^2\mathfrak{p}_7^2 = (14) = (\sqrt{-14})^2 \implies \mathfrak{p}_2\mathfrak{p}_7 = (\sqrt{-14}) \implies [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_7] \implies [\mathfrak{p}_2] = [\mathfrak{p}_2]^{-1} = [\mathfrak{p}_7].$$

Теперь рассмотрим остальные простые числа. Все они делятся на две группы: по модулю которых -14 — квадратичный вычет и по модулю которых соответственно невычет.

Пусть сначала -14 — невычет по модулю p. Тогда идеал $p\mathbb{Z}$ остаётся простым в $\mathcal{O}_K$. Таким образом, мы имеем единственный простой идеал, сидящий над p и этот идеал главный, что даёт нам что $[\mathfrak{p}]$ тривиален в $\mathcal{C}\ell(K)$.

Теперь пусть -14 — квадратичный вычет по модулю p. Тогда $\exists x \in \mathbb{Z}\colon p \mid x^2 + 14$. Можно считать, что $0 \leq x \leq \frac{p-1}{2}$. Тогда мы имееем, что $x^2 + 14 = pm \leq \left(\frac{p-1}{2}\right)^2 + 14$. Кроме того, в этом случае

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2, \quad \mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_2) = p, \quad \mathfrak{p}_1' = (p, x + \sqrt{-14}),\ \mathfrak{p}_2' = (p, x - \sqrt{-14}).$$

Если $p \geq 5$, то $m < p$, так как будут справделивы такие неравенства:

$$m < \frac{\frac{p^2}{4} + 14}{p} < p.$$

Кроме того, $(x + \sqrt{-14}) \subset \mathfrak{p}_1' \implies (x + \sqrt{-14}) \subset \mathfrak{p}_1' I$. Заметим, что $pm = \mathrm{N}(x + \sqrt{-14}) = \mathbb{N}(\mathfrak{p}_1')\,\mathrm{N}(I)$, а $\mathrm{N}(\mathfrak{p}_1') = p$, то есть $\mathrm{N}(I) = m < p$. Это даёт нам, что в разложении I на максимальные лежат только идеалы, лежащие над меньшими простыми числами. Иными словами, если

$$I = \mathfrak{q}_1^{k_1} \cdot \ldots \cdot \mathfrak{q}_s^{k_s},\ \mathfrak{q}_i \cap \mathbb{Z} = q_i\mathbb{Z},\ q_i \leq p, q_i - \text{простое}.$$

А это, в свою очередь, даёт нам возможность применить индукционное предположение: $[\mathfrak{q}_i]$ выражаются только через $\mathfrak{p}_2$ и $\mathfrak{p}_3$. Теперь заметим, что $[\mathfrak{p}_1'] = [I^{-1}]$, из чего следует, что $\mathfrak{p} = \mathfrak{p}_1'\mathfrak{p}_2'$ тоже выражается через $\mathfrak{p}_2$ и $\mathfrak{p}_3$, что и требовалось.

Группа классов идеалов мнимого квадратичного поля $\mathbb{Q}\left(\sqrt{d}\right)$

1. Если $d = -1, -2, -3, -7$, то $\mathcal{O}_K$ — еклидово, а значит, кольцо главных идеалов, то есть $\mathcal{C}\ell(K) = e$.
2. Если $d = -11, -19$, то справедлив аналогичный результат. Кольцо $\mathbb{Z}\left[\sqrt{-11}\right]$ также евклидово, но установить это сложнее. Кольцо $\mathbb{Z}[\sqrt{-19}]$ уже не является евклидовым, но является кольцом главных идеалов. Аналогичное верно и для $d = -43, -67, -163$.
3. Невероятно, но выполняется следующий факт:
$$\frac{\log\left|\mathcal{C}\ell(\mathbb{Q}\sqrt{-d})\right|}{\log\sqrt{\operatorname{disc} K}} \xrightarrow{d\to\infty} 1.$$
4. Табличку с группами классов идеалов мнимых квадратичных полей можно найти в конце книжки Боревич-Шафаревич.

Следствия из теоремы о конечности групп классов идеалов:

1. Если $h = |\mathcal{C}\ell(K)|$, то для любого дробного идеала $I\colon I^h$ является главным.

2. Если $(\ell, h) = (1)$ и I^ℓ главный, то I — главный. Действительно,

$$a\ell + bh = 1 \implies I = I^{a\ell+bh} = \left(I^\ell\right)^a \left(I^h\right)^b.$$

3. Существует такое конечное расщирение L/K, что для любого дробного идеала I кольца $\mathcal{O}_K$ идеал $I\mathcal{O}_L$ будет главным.

Доказательство. Итак, пусть $I_1, \ldots, I_m$ — представители группы классов идеалов. Пусть $I_i^h = (x_i)$. В качестве поля L мы возьмём:

$$L = K(\sqrt[h]{x_1}, \ldots, \sqrt[h]{x_m}).$$

$$I_j^h\mathcal{O}_L = \left(\sqrt[h]{x_j}\right)^h\mathcal{O}_L \implies I_j\mathcal{O}_L = (\sqrt[h]{x_j})\mathcal{O}_L.$$

□

Домашнее задание 8. Задачи:

1. Вычислите группу классов идеалов для $K = \mathbb{Q}\left(\sqrt{-5}\right),\ \mathbb{Q}\left(\sqrt{-6}\right),\ \mathbb{Q}\left(\sqrt{10}\right),\ \mathbb{Q}\left(\sqrt{-19}\right)$.
2. Положим $\mathcal{O}_K^* = \{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z}\ \forall y \in \mathcal{O}_K\}$.
   (a) Доказать, что $\mathcal{O}_K^*$ — дробный идеал и $\mathcal{O}_K \subset \mathcal{O}_K^*$.

(b) Доказать, что $|\mathrm{disc}(K)| = |\mathcal{O}_K^*/\mathcal{O}_K|$.
(c) Доказать, что $|\mathrm{disc}(K)|$ есть норма некоторого идеала в $\mathcal{O}_K$.

3. Пусть V — конечномерное векторное пространство над полем F, $A \in \mathrm{End}(V)$, причём A — нильпотентный. Докажите, что тогда $\mathrm{Tr}(A) = 0$.
4. Пусть I — дробный идеал. Докажите, что как абелева группа $d(\mathrm{N}(I))$ (дробный идеал в $\mathbb{Z}$) порождается элементами $\mathrm{N}(x), x \in I$.

1.13 Дифферента и ветвление

Определение 125. Пусть $K/\mathbb{Q}$ — конечное расширение. Простое число p называется *неразветвлённым* в числовом поле K, если

$$p\mathcal{O}_k = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_k,\ \mathfrak{p}_i \neq \mathfrak{p}_j - \text{максимальные}.$$

Иными словами, p неразветвлено, если все индексы ветвления равны единице.

Если же выполнкено

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2^{e_2} \cdot \ldots,$$

то идеал $\mathfrak{p}_1$ называется *неразвветвлённым.*

Рассмотрим $\mathcal{O}_K^* = \{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z}\ \forall y \in \mathcal{O}_K\}$ и покажем, что это дробный идеал.
Пусть $\omega_1, \ldots, \omega_n$ — целый базис, а $\omega_1^*, \ldots, \omega_n^*$ — взаимный базис, то есть

$$\mathrm{Tr}(\omega_i\omega_j^*) = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$$

Возьмём $x \in \mathcal{O}_K^*$ и разложим его по взаимному базису;

$$x = a_1\omega_1^* + \ldots + a_n\omega_n^*,\ a_i \in \mathbb{Q}.$$

Тогда $\mathrm{Tr}(x\omega_i) = a_i \implies a_i \in \mathbb{Z}$ по определению $\mathcal{O}_K^*$. Таким образом мы показали, что

$$\mathcal{O}_K^* \subset \bigoplus \mathbb{Z}\omega_i^*.$$

Теперь рассмотрим $\sum a_i\omega_i^*$, тогда

$$\mathrm{Tr}\Big(\sum a_i\omega_i^*\omega_j\Big) = a_j \in \mathbb{Z} \implies \forall y \in \mathcal{O}_K\ \ \mathrm{Tr}(\sum a_i\omega_i^* y) \in \mathbb{Z}$$

по линейности следа. Это доказывает, что $\bigoplus \mathbb{Z}\omega_i^* \subset \mathcal{O}_K^*$.

Таким образом, $\mathcal{O}_K^*$ — просто свободная абелева группа, порожденная взаимным базисом. Заметим также, что $\forall y \in \mathcal{O}_K,\ x \in \mathcal{O}_K^*\ yx \in \mathcal{O}_K^*$. Действительно,

$$\mathrm{Tr}(xy\mathcal{O}_K) = \mathrm{Tr}(x\mathcal{O}_K) \subset \mathbb{Z} \implies yx \in \mathcal{O}_K^*.$$

Так как K — поле частных кольца $\mathcal{O}_K$, каждую образующую $\mathcal{O}_K^*$ мы можем записать в виде $\omega_i^* = \frac{u_i}{v_i}$, где $u_i, v_i \in \mathcal{O}_K$. Положим $x = v_1 \ldots v_n$, тогда $x\mathcal{O}_K^*$ — целый идеал, так как

$$x\mathcal{O}_K = x\left(\frac{u_1}{v_1}, \ldots, \frac{u_n}{v_n}\right) \subset \mathcal{O}_K,$$

а то, что оно уважает домножение на элементы $\mathcal{O}_K$ мы уже проверили выше. Таким образом, $\mathcal{O}_K^*$ — дробный идеал.

Определение 126. *Дифферентой* числового поля K называют идеал $\mathcal{D} = \mathcal{O}_K^{*^{-1}}$.

Как мы помним, дискриминант числового поля K — это

$$\mathrm{disc}(K) = \det(\mathrm{Tr}(\omega_i\omega_j))_{i,j=1}^n,\ \text{где } \{\omega_i\} - \text{ целый базис.}$$

Предложение 58. $\mathrm{N}(\mathcal{D}) = |\mathrm{disc}(K)|$.

Доказательство. Будем действовать строго по определению:

$$\mathrm{N}(\mathcal{D}) = |\mathcal{O}_K/\mathcal{D}| = \left|\mathcal{O}_K/\mathcal{O}_K^{*^{-1}}\right| = |\mathcal{O}_K^*/\mathcal{O}_K|$$

Как мы уже замечали выше, $\mathcal{O}_K = \bigoplus \omega_i\mathbb{Z} \subset \bigoplus \mathbb{Z}\omega_i^* = \mathcal{O}_K^*$. Разложим элемент целого базиса по взаимному базису:

$$\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j^* \implies \mathrm{Tr}(\omega_i\omega_j) = a_{ij}.$$

Тогда по лемме 51 об индексе подгруппы ранга n в свободной абелевой группе ранга n мы имеем нужное:

$$|\mathcal{O}_K^*/\mathcal{O}_K| = \det(\mathrm{Tr}(\omega_i\omega_j))_{i,j=1}^n = |\mathrm{disc}(K)|\,.$$

□

Сейчас мы покажем, что дифферента числового поля K отвечает за ветвление и выведем из этого хороший критерий разветвлённости простых чисел.

Теорема 87. *Максимальный идеал $\mathfrak{p} \subset \mathcal{O}_K$ разветвлён тогда и только тогда, когда $\mathcal{D} \subset \mathfrak{p}$.*

Доказательство. В процессе доказательства нам понадобиться несколько лемм. Докажем сначала импликацию ($\Rightarrow$):

Лемма 55 (Задача 3 ДЗ 8)**.** Пусть V — конечномерное векторное пространство над полем F, $A \in \mathrm{End}(V)$, причём A — нильпотентный. Докажите, что тогда $\mathrm{Tr}(A) = 0$.

Доказательство леммы. Приведём, например, доказательство без Жордановой формы. Ясно, что достаточно показать, что характеристический многочлен является чистой степенью переменной t.

$$t^m E - A^m = (tE - A)((tE)^{m-1} + (tE)^{m-2}A + \ldots) = (tE - A) \cdot B.$$

Применим к этом равенству $\det$:

$$t^{mn} = \det\left(t^m E - A^m\right) = \det(tE - A)\det(B) \implies \det(tE - A) = t^n.$$

□

Пусть p — простое число. Тогда, как мы помним, $\mathcal{O}_K/p\mathcal{O}_K$ — векторное пространство над $\mathbb{F}_p$. Пусть $x \in \mathcal{O}_K$, а $\overline{x} = x + p\mathcal{O}_K$ — его образ в факторкольце. Рассмотрим оператор умножения на $\overline{x}$:

$$\mathcal{O}_K/p\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K,\ y + p\mathcal{O}_K \mapsto xy + \mathcal{O}_K.$$

Тогда ясно, что $\mathrm{Tr}(\overline{x}) = \mathrm{Tr}(x) + p\mathbb{Z}$. Тогда из леммы 55 мы получим вот такое следствие:

Следствие 34. *Пусть $x \in \mathcal{O}_K$, $x^m \in p\mathcal{O}_K$. Тогда $\mathrm{Tr}_{K/\mathbb{Q}}(x) \in p\mathbb{Z}$.*

Доказательство следствия. Действительно, так как $x^m \in p\mathcal{O}_K$, умножение $\overline{x}$ будет нильпотентным оператором $\mathcal{O}_K/p\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$, а значит, по лемме 55 $\mathrm{Tr}(\overline{x}) = 0$ (в $\mathbb{Z}/p\mathbb{Z}$), что и означает, что $\mathrm{Tr}(x) \in p\mathbb{Z}$. □

Перейдём теперь к доказательству теоремы. Пусть $\mathfrak{p}_1$ разветвлён, то есть

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}, e_1 > 1.$$

Докажем, что $\forall x \in \mathfrak{p}_1^{-1}$ выполнено $\mathrm{Tr}(x) \in \mathbb{Z}$. Этого будет достаточно, так как тогда

$$\forall y \in \mathcal{O}_K,\ \forall x \in \mathfrak{p}_1^{-1} \quad \left(xy \in \mathfrak{p}_1^{-1} \implies \mathrm{Tr}(xy) \in \mathbb{Z}\right) \implies x \in \mathcal{O}_K^* \implies \mathfrak{p}_1^{-1} \subset \mathcal{O}_K^* = \mathcal{D}^{-1} \implies \mathcal{D} \subset \mathfrak{p}_1.$$

Докажем теперь само утверждение. Заметим, что так как $x \in \mathfrak{p}_1^{-1}$, $px \in \mathfrak{p}_1^{e_1-1}\mathfrak{p}_2^{e_2} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}$, а тогда

$$(px)^2 \in \mathfrak{p}_1^{2(e_1-1)}\mathfrak{p}_2^{2e_2} \cdot \ldots \cdot \mathfrak{p}_k^{2e_k}$$

Так как $2(e_1 - 1) \geq e_1$, мы получаем, что

$$(px)^2 \in \mathfrak{p}_1^{2(e_1-1)}\mathfrak{p}_2^{2e_2} \cdot \ldots \cdot \mathfrak{p}_k^{2e_k} \subset p\mathcal{O}_K.$$

Тогда, по следствию 34 мы получаем, что $\mathrm{Tr}(px) \in p\mathbb{Z} \implies \mathrm{Tr}(x) \in \mathbb{Z}$.

Докажем теперь импликацию ($\Leftarrow$). Вспомним для начала такое утверждение:

Предложение 59. *Если F — конечное поле, а L/F — конечное расширение, то $\mathrm{Tr}_{L/F} \neq 0$.*

Замечание. В случае характеристики 0 это утверждение очевидно, так как можно рассматривать след единицы.

Доказательство предложения 59. Если $|F| = q$, то $\mathrm{Gal}(L/F) = \langle\sigma\rangle$ — циклическая и она порождена автоморфизмом Фробениуса $\sigma(x) = x^q$ (множество неподвижных элементов — как раз поле). Предположим, что $[L\colon F] = m$. Тогда Группа Галуа будет иметь вид

$$\mathrm{Gal}(L/F) = \langle \mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{m-1}\rangle,$$

а значит, след будет иметь вид

$$\mathrm{Tr}(x) = x + \sigma x + \sigma^2 x = \ldots + \sigma^{m-1}x = x + x^q + x^{q^2} + \ldots + x^{q^{m-1}}.$$

Заметим, что многочлен выше не может быть тождественно нулём. Действительно, он имеет не больше, чем q^{m-1} корней, а $|L| = q^m > q^{m-1}$. □

Итак, вернёмся к доказательству теоремы. Предположим, что $\mathfrak{p}_1$ неразветвлён, то есть

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^{e_2} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}.$$

По китайской теореме об остатках:

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p}_1 \oplus \mathcal{O}_K/\mathfrak{p}_2^{e_2} \oplus \cdot \ldots \cdot \oplus \mathcal{O}_K/\mathfrak{p}_k^{e_k}.$$

Пусть $x \in \mathfrak{p}_2^{e_2} \cdot \mathfrak{p}_3^{e_3} \cdot \ldots \mathfrak{p}_k^{e_k} \setminus \mathfrak{p}_1$. Тогда в разложении в прямую сумму такой x будет иметь лишь одну ненулевую координату (первую). Значит, так как след можно вычислять покоординатно, достаточно посчитать след в первом прямом слагаемом, которое является полем (так как мы факторизуем по максимальному идеалу), причём, конечным расширением $\mathbb{Z}/p\mathbb{Z}$. По утверждению 59 существует такой $\overline{x} \in \mathcal{O}_K/\mathfrak{p}_1$, что $\mathrm{Tr}(\overline{x}) \neq 0$ в $\mathbb{Z}/p\mathbb{Z}$. Тогда существует $x \in \mathcal{O}_K$ такой, что $\mathrm{Tr}(x) \notin p\mathbb{Z}$, то есть $\mathrm{Tr}\left(\frac{x}{p}\right) \notin \mathbb{Z}$. Но тогда

$$\begin{cases} \frac{x}{p} \in \mathfrak{p}^{-1} \\ \mathrm{Tr}\left(\frac{x}{p}\right) \notin \mathbb{Z} \end{cases} \implies \frac{x}{p} \notin \mathcal{O}_K^* \implies \mathfrak{p}_1^{-1} \not\subset \mathcal{O}_K^* \implies \mathcal{D} \not\subset \mathfrak{p}_1,$$

что мы и хотели доказать. □

Теорема 88. *Простое число p разветвлено тогда и только тогда, когда $p \mid \mathrm{disc}(K)$.*

Доказательство. Докажем сначала ($\Rightarrow$). Так как p разветвлено, по определению

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_2^{e_2} \cdot \ldots \cdot \mathfrak{p}_k^{e_k}, e_1 > 1.$$

Тогда по теореме 87 $\mathcal{D} \subset \mathfrak{p}_1$, но тогда

$$|\mathrm{disc}(K)| = \mathrm{N}(\mathcal{D}) \vdots \mathrm{N}(\mathfrak{p}_1) = p^{f_1} \implies \mathrm{disc}(K) \vdots p.$$

Теперь докажем ($\Leftarrow$). Теперь пусть p неравзеветвлено, то есть

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_k,\ \mathcal{D} \not\subset \mathfrak{p}_1.$$

Разложим дифференту в поизведение постых идеалов.

$$\mathcal{D} = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_m.$$

Так как каждый $\mathfrak{p}_i$ неравзетвлён, $\mathcal{D} \not\subset \mathfrak{p}_i \implies \mathfrak{p}_i \neq \mathfrak{q}_j$ для всех i и j.

Применим к этому равенству норму:

$$|\mathrm{disc}(K)| = \mathrm{N}(\mathcal{D}) = \mathrm{N}(\mathfrak{q}_1) \cdot \mathrm{N}(\mathfrak{q}_2) \cdot \ldots \cdot \mathrm{N}(\mathfrak{q}_m) = p_1^{f_1} \cdot p_2^{f_2} \cdot \ldots \cdot p_m^{f_m},\ p_i \neq p - \text{простые}.$$

Значит, $\mathrm{disc}(K) \not\vdots p$. □

Отсюда ясно, что для каджого расщирения разветвлённых простых чисел только конечное число — простые делители дискриминанта. Иными словами, для каждого конкретного расширения почти все простые числа являются неравзетвленными.

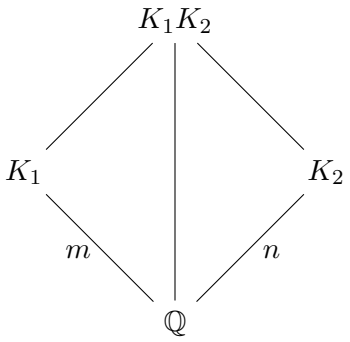
1.14 Кольцо целых композита расширений

В общем случае о вычислении кольца целых композита расширений сказать что-то сложно. Мы будем рассматривать один из частых случаев, который также весьма полезен при вычислении колец целых числовых полей.

Теорема 89. *Рассмотрим композит расщирений $K_1/\mathbb{Q}$ степени m и $K_2/\mathbb{Q}$ степени n, причем таких, что $[K_1K_2 \colon \mathbb{Q}] = mn$ (что равносильно тому, что $K_1K_2 = K_1 \otimes_{\mathbb{Q}} K_2$), а также $(\mathrm{disc}(K_1), \mathrm{disc}(K_2)) = 1$.*

Пусть $\{u_i\}$ — целый базис $\mathcal{O}_{K_1}$, а $\{v_i\}$ — целый базис $\mathcal{O}_{K_2}$. Тогда $\{u_iv_j\}$ — целый базис $\mathcal{O}_{K_1K_2}$.

Доказательство. Нарисуем композит расширений:



Пусть $\tau_i,\ 1 \leq i \leq m$ — вложения K_1 в $\mathbb{Q}^{alg}$, а $\sigma_i,\ 1 \leq i \leq n$ — вложения K_2 в $\mathbb{Q}^{alg}$. Во-первых, заметим, что $\{u_iv_j\}$ — базис композита K_1K_2 над $\mathbb{Q}$. Тогда элементы

$$\tau_i \otimes \sigma_j(u_kv_\ell) = \sigma_j(u_k)\tau_i(v_\ell)$$

будут попапрно различными, а $\tau_i \otimes \sigma_j$ будут давать все вложения $K_1K_2 \to \mathbb{Q}^{alg}$. Рассмотрим $\alpha \in \mathcal{O}_{K_1K_2}$, разложим его по базису:

$$\alpha = \sum a_{ij}u_iv_j \in \mathcal{O}_{K_1K_2},\ a_{ij} \in \mathbb{Q}$$

и докажем, что $a_{ij} \in \mathbb{Z}$.

Рассмотрим $\beta_j = \sum_{i=1}^m a_{ij}u_j$. Тогда выполняется следующее матричное тождество (которое мы преобразовываем далее, домножая на транспонированную, а после на взаимную к A^tA):

$$\underbrace{(\sigma_iv_j)}_{A} \cdot \begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix} = \begin{pmatrix}(1\otimes\sigma_1)(\alpha)\\ (1\otimes\sigma_2)(\alpha)\\ \vdots\\ (1\otimes\sigma_n)(\alpha)\end{pmatrix} \implies A^tA\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix} = A^t \cdot \begin{pmatrix}(1\otimes\sigma_1)(\alpha)\\ (1\otimes\sigma_2)(\alpha)\\ \vdots\\ (1\otimes\sigma_n)(\alpha)\end{pmatrix} \implies \mathrm{disc}(K_2) \cdot \begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix} = \begin{pmatrix}\gamma_1\\ \gamma_2\\ \vdots\\ \gamma_n\end{pmatrix},$$

где $\gamma_i \in \mathcal{O}_{K_1}$. Тогда $\operatorname{disc}(K_1) \cdot a_{ij} \in \mathbb{Z}$. Заметим, что такое же рассуждение мы могли проделать, заменив u_i на v_j в определении β_j, и получить, что $\operatorname{disc}(K_1)a_{ij} \in \mathbb{Z}$. Тогда, так как $(\operatorname{disc}(K_1), \operatorname{disc}(K_2)) = 1$, мы имеем $a_{ij} \in \mathbb{Z}$. □

Домашнее задание 9. Задачи:

1. Пусть $K/\mathbb{Q}$ — расширение степени n, $K = \mathbb{Q}(\theta)$, где $\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_0 = 0$ и пусть p — такое простое число, что $v_p(a_0) = 1$ и $v_p(a_i) \geq 1$. Докажите, что тогда $p \nmid \operatorname{ind}(\theta)$. *Hint 1:* рассмотрите $x \in \mathcal{O}_K : px \in \mathbb{Z}[\theta]$. Покажите, что достаточно доказать, что в этом случае $x \in \mathbb{Z}[\theta]$. *Hint 2:* докажите, что если $\mathfrak{p} \mid (p)$, то $v_{\mathfrak{p}}(\theta) = 1$ и индекс ветвления числа p равен n. *Hint 3:* $px = b_0 + b_1\theta + \ldots + b_{n-1}\theta^{n-1}$. Предположите, что не все b_i делятся на p и прийдите к противоречию.
2. Докажите, что если $K = \mathbb{Q}\big(\sqrt[n]{1}\big)$, то $\mathcal{O}_K = \mathbb{Z}[\zeta]$, где $\zeta^{p^n} = 1$.
3. Пусть $a_1, \ldots, a_n \in \mathbb{Q}, \quad b_1, \ldots, b_n \in \mathbb{Q},\ b_i > 0, k \geq 2$ и $\sqrt[k]{\frac{b_i}{b_j}} \notin \mathbb{Q}$. Предположим, что

$$a_1 \sqrt[k]{b_1} + \ldots + a_n \sqrt[k]{b_n} = 0.$$

   Докажите, что тогда $a_i = 0 \quad \forall i$.
4.

   Теорема 90 (Баше). *Пусть $d \in \mathbb{N}$, d свободно от квадратов, $d \not\equiv_4 3$ и $|\mathcal{C}\ell(\mathbb{Q}(\sqrt{-d}))| \not\vdots 3$. Тогда*

$$y^2 = x^3 - d$$

   не имеет решений в $\mathbb{Z}$, если d не имеет вид $3a^2 \pm 1,\ a \in \mathbb{Z}$. А если $d = 3a^2 \pm 1$, то уравнение имеет целое решение

$$x = a^2 + d, \quad y = \pm a(a^2 - 3d).$$

1.15 Теорема Куммера

Начнём с вот такой полезной леммы:

Лемма 56. Следующие условия равносильны:

1. $p \nmid \operatorname{ind}(\theta) = |\mathcal{O}_K/\mathbb{Z}[\theta]|$.
2. $\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \to \mathcal{O}_K/p\mathcal{O}_K$ — изоморфизм.

Доказательство. Сначала докажем $(2) \implies (1)$. Так как у нас есть изоморфизм $\mathbb{Z}[\theta]/p\mathbb{Z}[\theta] \cong \mathcal{O}_K/p\mathcal{O}_K$, мы имеем

$$(\mathcal{O}_k/\mathbb{Z}[\theta])/p(\mathcal{O}_k/\mathbb{Z}[\theta]) = 0 \implies \mathcal{O}_k/\mathbb{Z}[\theta] = p\mathcal{O}_k/\mathbb{Z}[\theta],$$

отукда, так как $|\mathcal{O}_K/\mathbb{Z}[\theta]| < \infty$, в $\mathcal{O}_K/\mathbb{Z}[\theta]$ нет элементов p-кручения, то есть $p \nmid |\mathcal{O}_K/\mathbb{Z}[\theta]| = \operatorname{ind}(\theta)$.

Теперь докажем $(1) \implies (2)$. Так как $\mathcal{O}_K/\mathbb{Z}[\theta]$ не имеет p-кручения, $\mathcal{O}_k/\mathbb{Z}[\theta] = p\mathcal{O}_k/\mathbb{Z}[\theta]$ (у гомоморфизма факторизации тривиальное ядро). Но тогда отображение $\mathbb{Z}[\theta]/(p) \to \mathcal{O}_K/(p)$ — эпиморфизм (так как $(\mathcal{O}_K/(p))/(\mathbb{Z}[\theta]/(p)) \cong (\mathcal{O}_K/\mathbb{Z}[\theta])/(p) \cong 0$). Но тогда это эпиморфизм векторных пространств над $\mathbb{F}_p$ одинаковой размерности (в самом деле, $\mathbb{Z}[\theta] \cong \mathbb{Z}^n$ и $\mathcal{O}_K \cong \mathbb{Z}^n$, где $n = [K : \mathbb{Q}]$). Тогда

$$\mathbb{Z}[\theta]/(p) \cong \mathbb{F}_p^n \cong \mathcal{O}_K/(p),$$

как векторные пространства, значит, у нас есть и изоморфизм. □

Теорема 91 (Куммер). *Пусть $K = \mathbb{Q}(\theta)$, $\theta \in \mathcal{O}_K$, а p — такое простое число, что $p \nmid \operatorname{ind}(\theta)$. Пусть f — минимальный многочлен θ, причем над полем $\mathbb{Z}/p\mathbb{Z}$ его редукция $\overline{f}$ раскладывается в неприводимые, как*

$$\overline{f} = \prod_i \overline{g_i}^{a_i} \in \mathbb{F}_p[t],\ \deg g_i = d_i,\ g_i \text{ — унитарные.}$$

Тогда:

1. *Идеалы $\mathfrak{p}_i = (g_i(\theta), p)$ — все простые идеалы, висящие над простым числом p. Причём, они попарно различны.*
2. *$|\mathcal{O}_K/\mathfrak{p}_i| = p^{d_i}$, а значит, d_i — степень инерции идеала $\mathfrak{p}_i$.*
3. *$p\mathcal{O}_K = \prod \mathfrak{p}_i^{a_i}$, то есть a_i есть индексы ветвления идеалов $\mathfrak{p}_i$.*

Доказательство. **I.** Покажем, что $\mathfrak{p}_i$ максимальны. Для этого достаточно проверить, что фактор — поле. Действительно, это простое вычисление:

$$\mathcal{O}_K/\mathfrak{p}_i = \mathcal{O}_K/(g_i(\theta), p) \underbrace{=}_{\text{Л. } 56.} \mathbb{Z}[\theta]/(g_i(\theta), p) \cong \mathbb{Z}[t]/(f(t), p, g_i(t)) \cong \mathbb{F}_p[t]/\overline{g_i},$$

которое является полем, так как многочлен g_i неприводим над $\mathbb{F}_p$.

II. Теперь покажем, что $\mathfrak{p}_i \neq \mathfrak{p}_j$ при $i \neq j$. Предположим противное. Тогда

$$\mathfrak{p}_i = \mathfrak{p}_j = (g_i(\theta), p, g_j(\theta)).$$

Но, $\overline{g_i}$ и $\overline{g_j}$ — различные неприводимые многлчлены из $\mathbb{F}_p[t]$, а мы можем линейно представить их НОД:

$$\exists \overline{h_i}, \overline{h_j} \colon \overline{h_i}\overline{g_i} + \overline{h_j}\overline{g_j} = \overline{1} \implies h_i g_i + h_j g_j = 1 + p \cdot q(t) \in \mathbb{Z}[t].$$

Подставляя в последнее равенство θ, мы получаем, что $1 \in (g_i(\theta), g_j(\theta), p) = \mathfrak{p}_i = \mathfrak{p}_j$, что противоречит тому, что $\mathfrak{p}_i$ и $\mathfrak{p}_j$ максимальны.

III. Теперь провреим, что d_i — степень инерции. Действительно,

$$\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{F}_p[t]/(\overline{g_i}) \implies |\mathcal{O}_K/\mathfrak{p}_i| = p^{d_i},$$

так как $\mathbb{F}_p[t]/(\overline{g_i})$ — расширение $\mathbb{F}_p$ степени d_i (так как многочлен g_i неприводим).

Из условия теоремы мы знаем, что

$$f(t) = \prod g_i(t)^{a_i} + ph(t) \implies 0 = f(\theta) = \prod g_i(\theta)^{a_i} + ph(\theta) \implies \prod g_i(\theta)^{a_i} \in p\mathcal{O}_K \implies \prod \mathfrak{p}_i^{a_i} \subset p\mathcal{O}_K.$$

Отсюда уже видно, что над p не висит никаких других идеалов. Действительно,

$$p\mathcal{O}_K \subset \mathfrak{q} \implies \prod \mathfrak{p}_i^{a_i} \subset \mathfrak{q} \implies \mathfrak{p}_i \subset \mathfrak{q} \implies \mathfrak{p}_i = \mathfrak{q}.$$

Значит, $\prod \mathfrak{p}_i^{a_i} = p\mathcal{O}_K \cdot I$. Из этого следует, что $a_i \geq e_i$. Остается заметить, что

$$\sum a_i d_i = n, \quad a_i \geq e_i \implies a_i = e_i \forall n.$$

□

Имеет смысл разобрать полезный частный случай этой теоремы: когда все a_i равны 1.

Теорема 92. *Пусть $K = \mathbb{Q}(\theta)$, $\theta \in \mathcal{O}_K$, f — минимальный многочлен θ, а p — простое число. Предположим, что*

$$\overline{f} = \overline{g_1} \cdot \overline{g_2} \cdot \ldots \cdot \overline{g_k} \in \mathbb{F}_p[t], \text{ причем}$$

$\overline{g_i}$ — попарно различые и унитальные. Тогда $p \not| \operatorname{ind}(\theta)$.

Доказательство. Пусть $I = (p, g_i(\theta)) = I \trianglelefteq \mathbb{Z}[\theta]$ — идеал. По тем же соображениям, что и в предыдущей теореме, $I \in \operatorname{Specm}(\mathbb{Z}[\theta])$:

$$\mathbb{Z}[\theta]/(g_i(\theta), p) \cong \mathbb{Z}[t]/(f(t), p, g_i(t)) \cong \mathbb{F}_p[t]/\overline{g_i}.$$

Покажем, что $I\mathcal{O}_K \neq \mathcal{O}_K$. Предположим противное и выберем в $\mathcal{O}_K$ целый базис $\omega_1, \ldots, \omega_n$. Тогда мы можем записать каждый элемент базиса с коэффициентами из идеала:

$$\omega_i = \sum a_{ij}\omega_j$$

Перенося всё в одну часть и обозначая $A = (a_{ij})$, мы имеем такую систему уравнений:

$$(E - A) \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

В таком случае $\det(E - A) = 0$, из чего следует, что $1 \in I$ (так как $\det(E - a) \in 1 + I$), что противоречит тому, что $I \in \operatorname{Specm}(\mathbb{Z}[\theta])$.

Тогда $I\mathcal{O}_K$ — собственный идеал в $\mathcal{O}_K$, а значит, содержится в некотром максимальном идеале, $(p, g_i(\theta)) \subset \mathfrak{p}_i \subset \mathcal{O}_K$. Теперь нам достаточно показать, что (по лемме 56)

$$\mathbb{Z}[\theta]/(p) \cong \mathcal{O}_K/(p).$$

Рассмотрим следующую коммутативную диаграмму:

$$\begin{array}{ccc} \mathbb{Z}[\theta]/(p) & \xrightarrow{\varphi} & \mathcal{O}_K/(p) \\ \downarrow{\scriptstyle \psi} & & \downarrow \\ \mathbb{Z}[\theta]/(p, g_i(\theta)) & \hookrightarrow & \mathcal{O}_K/\mathfrak{p}_i \end{array}$$

Достаточно проверить, что $\operatorname{Ker}\varphi = 0$. Действительно, пусть $\overline{\alpha} \in \operatorname{Ker}\varphi$, тогда $\psi(\overline{\alpha}) = 0$, а значит, $\alpha \in (p, g_i(\theta))\ \forall i$, из чего следует, что

$$\alpha^k \in \prod_i (p, g_i(\theta)) \in p\mathbb{Z}[\theta] \implies \overline{\alpha}^k = \overline{0} \text{ в } \mathbb{Z}[\theta]/(p),$$

то есть мы нашли нильпотентный элемент. С другой стороны,

$$\mathbb{Z}[\theta]/(p) \cong \mathbb{F}_p[t]/(\overline{f}) \cong \bigoplus \mathbb{F}_p[t]/(\overline{g_i}),$$

а то, что написано справа — прямое произведение полей. Значит, $\overline{\alpha} = 0$ и ядро тривиально. □

Ветвление при круговом расширении

Оказывается, теорема Куммера 91 позволяет полностью исследовать ветвление при круговом расширении.

Пусть p — простое число, $K = \mathbb{Q}(\zeta_m)$ и $m \not\vdots p$. Как мы знаем, минимальный многочлен ζ_m — это круговой многочлен Φ_m. Ясно, что

$$x^m - 1 \vdots \Phi_m,$$

так как Φ_m — минимальный. С другой стороны, многочлен $\overline{x^m - 1}$ имеет m попарно различных корней в $\mathbb{F}_p^{alg}$, так как он взаимнопрост со своей производной:

$$(x^m - 1, (x^m - 1)') = (x^m - 1, mx^{m-1}) = 1.$$

Но тогда, так как $x^m - 1 \vdots \Phi_m$,

$$\overline{\Phi_m} = \overline{g_1} \cdot \ldots \overline{g_n},$$

где $\overline{g_i}$ — попарно различные и неприводимые. Тогда по теореме 92 $p \not| \operatorname{ind}(\zeta_m)$, то есть мы можем применить теорему Куммера 91:

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdot \ldots \mathfrak{p}_k, \quad \mathfrak{p}_i = (p, g_i(\zeta_m)).$$

С другой стороны, так как $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ — расширение Галуа, все степени инерции равны. Значит, достаточно вычислить хотя бы одну.

Предложение 60. *Степени инерции f идеалов $\mathfrak{p}_i$ — это минимальные такие f, что $(p^f - 1) \vdots m$.*

Доказательство. Корни многочлена $\overline{x^m-1}$ образуют циклическую группу, так как это подгруппа в мультипликативной группе конечного расширения $\mathbb{F}_p$. Пусть θ — образующая этой группы, $\theta \in \mathbb{F}_p^{alg}$.

$$x^m-1=\Phi_m(x)\cdot\prod_{k|m,k\neq m}\Phi_k(x)\implies\overline{x^m-1}=\overline{\Phi_m(x)}\cdot\prod_{k|m,k\neq m}\overline{\Phi_k(x)}.$$

Пусть $\Phi_k(\theta)=0$, тогда так как $x^k-1\vdots\Phi_k$, $\theta^k-1=0$, откуда $k\vdots m$ (так как θ — образующая циклической группы из m элементов). Значит, $\overline{\Phi_m}=0$.

Не умаляя общности, пусть $\overline{g_1}(\theta)=0$. Тогда

$$\{1,\theta,\dots,\theta^{m-1}\}=\langle\theta\rangle\leq(\mathbb{F}_p[x]/(g_1))^*.$$

Тогда, если $\deg g_1=f_1$, мы имеем

$$|(\mathbb{F}_p[x]/(g_1))^*|=p^{f_1}-1,\quad\langle\theta\rangle\leq lr*\mathbb{F}_p[x]/(g_1)^*\implies p^{f_1}-1\vdots m,$$

откуда $f_1\geq f$. Теперь докажем, что $f_1\leq f$. Действительно,

$$\begin{cases}\theta^m=1\\ m\mid p^f-1\end{cases}\implies\theta^{p^f-1}=1\implies\theta^{p^f}=\theta.$$

Значит, $\theta\in\mathbb{F}_{p^f}\implies\mathbb{F}_p[x]/(g_1)=\mathbb{F}_p[\theta]\leq\mathbb{F}_{p^f}$, откуда $p^f\vdots p^{f_1}\implies f_1\leq f$. □

Домашнее задание 10. Задачи:

1. Рассмотрим кубическое расщирение $K=\mathbb{Q}(\sqrt[3]{15})=\mathbb{Q}(\rho)$.
   0) Посчитать кольцо $\mathcal{O}_K$.
   а) Вычислить $\mathrm{N}(\rho),\ \mathrm{N}(\rho-1),\ \mathrm{N}(\rho+1),\mathrm{N}(\rho-3)$.
   б) Докажите, что над простым числом 3 лежит ровно один простой идеал ρ_3.
   в) Докажите, что ρ_3 — главный. Найдите его образующую с помощью разложений $(\rho-3)$ и $(\rho+3)$.
   г) Докажите, что $\frac{9(\rho+1)^3}{(\rho-3)^6}\in\mathcal{O}_K^*$.
2. Вычислить $\mathcal{O}_K$, где $K=\mathbb{Q}(\sqrt{p_1},\dots,\sqrt{p_k})$, если p_i — простые и $p_i\equiv 1\pmod 4$.
3. Доказать, что $\upsilon_{\mathfrak{p}}(\mathcal{D})\geq e-1$, где $e=e(\mathfrak{p})$ — индекс ветвления.

1.16 Первый случай Last Fermat's theorem

Мы можем полагать, что показатель n — простое число, а также рассматривать уравнение в виде

$$x^p+y^p+z^p=0,\quad(x,y,z)=1. \tag{3.2}$$

Первым случаем Большой теоремы Ферма называют доказательство большой теоремы ферма в предположениии $p\nmid xyz$.

Теорема 93 (Софи Жермен). *Если простое число p таково, что $2p+1=q$ — простое число, то имеет место первый случай Большой теоремы Ферма.*

Доказательство. Перепишем уравнение в виде

$$y^p+z^p=(-x)^p\Leftrightarrow(y+z)(y^{p-1}-y^{p-2}z+\ldots-yz^{p-1}+z^{p-1})=(-x)^p.$$

Покажем, что $(y+z,y^{p-1}-y^{p-2}z+\ldots+z^{p-1})=1$. Пусть r — простое ($r\neq p$) и такое, что $r\mid y+z,\ r\mid y^{p-1}+y^{p-2}z+\ldots+z^{p-1}$. Тогда

$$y\equiv-z\pmod r\implies y^{p-1}-y^{p-2}z+\ldots-yz^{p-1}+z^{p-1}\equiv py^{p-1}\pmod r\implies y\vdots r\implies z\vdots r,$$

что противоречит тому, что $(y,z)=1$.

$$\begin{cases} y+z=A^p \\ y^{p-1}-y^{p-2}z+\ldots-yz^{p-1}+z^{p-1}=T^p \end{cases}$$

Так как наше условие симметрично относительно переменных, $x+y=B^p,\ x+z=C^p$. Теперь заметим, что по условию

$$x^p+y^p+z^p=0 \Leftrightarrow x^{\frac{q-1}{2}}+y^{\frac{q-1}{2}}+z^{\frac{q-1}{2}}=0., \quad p=\frac{q-1}{2}. \tag{3.3}$$

Заметим, что если $q \nmid x$, то по малой теореме Ферма:

$$x^{q-1}\equiv 1 \pmod q \implies x^{\frac{q-1}{2}}\equiv \pm 1 \pmod q.$$

Отсюда ясно, что не может быть такого, что $q \nmid x,\ q \nmid y,\ q \nmid z$, так как иначе 3.3 выполняться не может. Значит, $q \mid xyz$. Не умаляя общности, пусть $q \mid x$. Тогда

$$2x=B^p+C^p-A^p=B^{\frac{q-1}{2}}+C^{\frac{q-1}{2}}-A^{\frac{q-1}{2}}\equiv 0 \pmod p.$$

Отсюда ясно, что по аналогичным соображениям не может быть такого, что $ABC \nmid q$. С другой стороны, если $B \vdots q$, то $B^p \vdots q$, а тогда

$$\begin{cases} x+y=B^p \vdots q \\ x \vdots q \end{cases} \implies y \vdots q,$$

что противоречит $(x,z)=1$. По аналогичным причинам $q \nmid C$. Тогда $A \vdots q$, откуда $y+z=A^p \vdots q$, откуда $T^p \equiv py^{p-1} \pmod q$. С другой стороны, так как $(A,T)=1$, как мы показали выше, $T \nmid q$, а тогда по малой теореме Ферма

$$T^{\frac{q-1}{2}}\equiv \pm 1 \pmod q \implies py^{p-1}\equiv \pm 1 \pmod q. \tag{3.4}$$

А так как $x \vdots q$, $B^{\frac{q-1}{2}}=B^p=x+y\equiv y \pmod q$, но тогда так как $B \nmid q$, по малой теореме Ферма

$$y\equiv B^{\frac{q-1}{2}}\equiv \pm 1 \pmod q.$$

Подставляя это в 3.4, получаем, что

$$py^{p-1}\equiv p(\pm 1)^{p-1}\equiv p\equiv \pm 1 \pmod q,$$

что даёт нам противоречие, так как $q=2p+1$.

Так как $(A,T)=1$, $q \nmid T$. Тогда $T^{\frac{q-1}{2}} \equiv py^{p-1} \pmod q$, тогда по малой теореме Ферма $\pm 1 = py^{p-1} \pmod q$. Так как $q \mid x$, $B^p=x+y\equiv y \pmod q$. Значит,

$$y\equiv B^{\frac{q-1}{2}}\equiv \pm 1 \pmod 1, \text{ так как } q \nmid B.$$

Знчит, $\pm 1 \equiv \pm p \pmod q$, а этого быть не может, так как $q=2p+1$.

□

Домашнее задание 11. Получите элементарное доказательство случая $p=5$ в первом случае большой теоремы Ферма.

Рассмотрим $K=\mathbb{Q}(\zeta_m)$ над $\mathbb{Q}$. Мы доказывали, что если q простое и $q \nmid m$, то оно неравзетвлено, то есть

$$q\mathcal{O}_K=\mathfrak{p}_1\cdot\mathfrak{p}_2\cdot\ldots\cdot\mathfrak{p}_k.$$

В частности, если $m=p$ — простое, то $q \nmid p$ и это будет выполнено. А вот p будет полностью разветвлено в $\mathbb{Q}(\zeta_p)$. Убедимся в этом:

Предложение 61. *Простое число p полностью разветвлено в $\mathbb{Q}(\zeta_p)$.*

Доказательство.

$$x^p - 1 = (x-1)(x-\zeta)(x-\zeta^2)\dots(x-\zeta^{p-1}) = (x-1)(x^{p-1}+\dots+x+1).$$

$$x^{p-1}+\dots+x+1 = (x-\zeta)(x-\zeta^2)\dots(x-\zeta^{p-1})$$

Подставим $x=1$ и от числового равенства перейдём к равенству идеалов:

$$p\mathcal{O}_K = (1-\zeta)(1-\zeta^2)\dots(1-\zeta^{p-1}).$$

Ясно, что $1-\zeta^j \vdots 1-\zeta$, а так как $\exists i\colon (\zeta^j)^i = \zeta$, $1-\zeta \vdots 1-\zeta^j$, то есть все идеалы в правой части совпадают и мы имеем

$$p\mathcal{O}_K = ((1-\zeta))^{p-1}.$$

Покажем теперь, что $(1-\zeta)$ — простой идеал. Действительно, пусть

$$(1-\zeta) = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_k \implies p\mathcal{O}_K = ((1-\zeta))^{p-1} = \mathfrak{p}_1^{p-1}\mathfrak{p}_2^{p-1}\dots\mathfrak{p}_k^{p-1},$$

откуда индекс ветвления $e_i \geq p-1$, но с другой стороны, $efk = [K:\mathbb{Q}] = p-1$ (так как у нас расширение Галуа), откуда ясно, что

$$p\mathcal{O}_K = ((1-\zeta))^{p-1} = \mathfrak{p}^{p-1}, \quad \mathfrak{p} \in \operatorname{Specm}(\mathcal{O}_K).$$

□

Лемма 57. Пусть p — простое число, не равное двум. Множество корней из единицы[4] в поле $\mathbb{Q}(\zeta_p)$ равно $\{\pm\zeta_p^i\}$.

Доказательство. Возьмем $\zeta_n \in \mathbb{Q}(\zeta_p)$.

1). Предположим, что $n \equiv 0 \pmod 4$. Тогда $i = \zeta_4 \in \mathbb{Q}(\zeta_p)$. Заметим, что $2i = (1+i)^2$ а значит, $(2) = ((1+i))^2$, то есть двойка разветвлена в $\mathbb{Q}(\zeta_p)$ (а это противоречит предыдущему утверждению). Значит $n \not\equiv 0 \pmod 4$.

2). Теперь рассмотрим случай $n = 2n_0$, n — нечётное. Тогда $\zeta_n^i = \pm\zeta_{n_0}^i$ и нам достаточно рассматривать n_0. Пусть у n_0 есть какие-то простые делители, кроме p, например, p'. Тогда, так как $n_0 \vdots p'$,

$$\mathbb{Q}(\zeta_{p'}) \leq \mathbb{Q}(\zeta_{n_0}) \leq \mathbb{Q}(\zeta_p).$$

Но тогда по предложению 61 p' будет полность разветвлено в $\mathbb{Q}(\zeta_{p'})$ и при этом, так как $p' \not| p$, неразветлвено в $\mathbb{Q}(\zeta_p)$, что даёт нам противоречие.

3). Значит, $n_0 = p^a$, а тогда $\zeta_{p^a} \in \mathbb{Q}(\zeta_p)$, то есть $\mathbb{Q}(\zeta_{p^a}) \leq \mathbb{Q}(\zeta_p)$. С другой стороны, тогда

$$[\mathbb{Q}(\zeta_{p^a}):\mathbb{Q}] = p^a - p^{a-1} \leq [\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1 \implies a = 1 \implies n_0 = p.$$

□

Лемма 58. Пусть $K/\mathbb{Q}$ — конечное расширение, $\sigma_i\colon K \to \mathbb{Q}^{alg}$ — все вложения ($1 \leq i \leq n$, $n = [K:\mathbb{Q}]$). Предположим, что $\alpha \in \mathcal{O}_K$ и $\forall i\ |\sigma_i\alpha| \leq 1$. Тогда α является корнем из единицы какой-то степени. [5]

Доказательство. Выпишем многочлен с целыми коэффициентами, корнем которого является α:

$$\prod_i (x - \sigma_i\alpha) \in \mathbb{Z}[x].$$

В силу предположения теоремы, его коэффициенты ограничены, так как они являются симметрическими функциями от $\sigma_i\alpha$. Заметим теперь, что из условия следует, что $|\sigma_i(\alpha^k)| \leq 1$, а значит, для α^k мы также получим многочлен с ограниченными коэффициентами. Заметим, что k — произвольное натуральное, а значит, мы получаем бесконечное число α^k, которые являются корнями коненого набора многочленов над $\mathbb{Z}$ (так как коэффициенты каждого мы можем ограничить одной и той же константой). Значит, $\exists m, n\colon \alpha^m = \alpha^n$, что и даёт нам, что α — корень из 1. □

[4] не обязательно степени p

[5] Обратное утверждение очевидно.

Лемма 59. Пусть $u \in \mathcal{O}_K^* = \mathbb{Z}[\zeta_p]$ для $K = \mathbb{Q}(\zeta_p)$. Тогда $\exists s\colon u\zeta_p^s \in \mathbb{R}$.

Доказательство. Положим $\zeta = \zeta_p$. Рассомтрим $v = u/\overline{u}$ и возьмем $\rho \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$. Тогда по лемме 58:

$$\rho(v) = \frac{\rho(u)}{\rho(\overline{u})} = {}^{6}\frac{\rho(u)}{\overline{\rho(u)}} \implies |\rho(v)| = 1.$$

Значит, по лемме 58 v — является корнем из единицы какой-то степени, а тогда по лемме 57 $v = \pm\zeta^n$.

Положми $\lambda = 1 - \zeta$, тогда

$$\rho(\zeta) \equiv \zeta^k \equiv \zeta \pmod{\lambda} \implies \rho(\zeta^i) \equiv \zeta^i \pmod{\lambda},$$

а так как $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$, мы имеем такое сравнение для всех элементов $\mathcal{O}_K$. В частности, из этого следует, что $\rho(u) \equiv u \pmod{\lambda}$. В частности, мы можем положить $\rho(x) = \overline{x}$ и отсюда получить, что $\overline{u} \equiv u \pmod{\lambda}$. Так как $v = u/\overline{u}$, а $v = \pm\zeta^n$, то есть $u = \pm\zeta^n\overline{u}$, мы имеем

$$\pm\zeta^n = \overline{u} \equiv u \pmod{\lambda}.$$

Предположим, что реализуется знак минус. Тогда, так как $\zeta^n \equiv 1 \pmod{\lambda}$, отсюда мы получаем

$$-\overline{u} \equiv \overline{u} \pmod{\lambda} \implies 2\overline{u} \equiv 0 \pmod{\lambda},$$

а так как $\overline{u}$ обратим, отсюда $2 \vdots \lambda = 1 - \zeta$. Но тогда $2^{p-1} \vdots (1-\zeta)^{p-1}$, а как мы уже видели в предложении 61, $((1-\zeta)^{p-1}) = p\mathcal{O}_K$, то есть $2^{p-1} \vdots p$, что даёт нам противоречие.

Значит, знак минус невозможен и реализуется случай

$$\zeta^n\overline{u} \equiv \overline{u} \equiv u \pmod{\lambda}.$$

Тогда $\zeta^n\overline{u} = u$, значит $u\zeta^s = \zeta^{n+s}\overline{u}$. Попробуем подобрать такое s, что

$$u\zeta^s = \overline{\zeta^{n+s}\overline{u}} \implies \overline{\zeta^{n+s}} = \zeta^s \implies 2s + n \equiv 0 \pmod{p},$$

и достаточно взять $s \equiv -n/2 \pmod{p}$.

□

Лемма 60. Пусть $x^p + y^p = z^p,\ p \nmid xyz,\ (x, y, z) = 1$, разложим левую часть в линейные множители:

$$x^p + y^p = (x + y)(x + \zeta y)\dots(x + \zeta^{p-1}y).$$

Тогда сомножители в правой части равенства попарно взаимнопросты.

Доказательство. Предположим противное, тогда $x + \zeta^i y,\ x + \zeta^j y \in \mathfrak{q}$ для некоторых i, j. Тогда

$$(x + \zeta^i y) - (x + \zeta^j y) = \zeta^i(1 - \zeta^{j-i})y \in \mathfrak{q}.$$

1. Если $y \in \mathfrak{q}$, то, так как $1 + \zeta^i y \in \mathfrak{q}$, мы имеем $x \in \mathfrak{q}$, но по условию $(x, y) = (1)$.
2. Если $(1 - \zeta^{j-i}) \in \mathfrak{q}$, то $1 - \zeta \in \mathfrak{q}$, а так как $(1 - \zeta) \in \mathrm{Specm}(\mathcal{O}_K)$ (что мы доказывали в 61), $\mathfrak{q} = (1 - \zeta)$. Но тогда $x + y \in \mathfrak{q} \implies z^p \in \mathfrak{q} \implies z \in \mathfrak{q}$. Тогда

   $$(z)^{p-1} \vdots \mathfrak{q}^{p-1} = ((1-\zeta))^{p-1} = (p) \implies z \vdots p,$$

   что даёт нам противоречие.

□

Сейчас, пользуясь всей подготовкой выше, мы докажем первый случай большой теоремы Ферма для регулярных простых.

[6] Так как сопряжение — тоже автоморфизм, а группа Галуа абелева, $\rho(\overline{x}) = \overline{\rho(x)}$

Теорема 94. *Пусть $p \nmid |\mathcal{C}\ell(\mathbb{Q}(\zeta_p))$[7]. Тогда имеет место первый случай Великой теоремы Ферма.*

Доказательство. Пусть $x^p + y^p = z^p$, разложим левую часть на множители:

$$\prod_{i=0}^{p-1}(x + \zeta^i y) = z^p.$$

Так как все сомножители в левой части равенства взаимнопросты по лемме 60, все они являются p-ми степенями, в частности для $i = 1$. То есть

$$(x + \zeta y) = I^p,$$

значит I находится в p-кручении $\mathcal{C}\ell(\mathbb{Q}_{\zeta_p})$. Но так как p не делит порядок группы классов, оно тривиально, значит $I-$ главный, то есть $I = (\alpha)$ для некоторого α. Значит,

$$(x + \zeta y) = (\alpha^p) \implies x + \zeta y = \varepsilon\alpha^p, \text{ где } \varepsilon \in \mathbb{Z}[\zeta]^*,$$

Тогда по лемме 59 мы имеем

$$x + \zeta y = \zeta^s u\alpha^p, \quad u \in \mathbb{R}.$$

С другой стороны, $\alpha = a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2},\ a_i \in \mathbb{Z}$. Тогда

$$\alpha^p \equiv \underbrace{a_0^p + a_1^p + \ldots + a_{p-2}^p}_{\stackrel{\text{def}}{=} n} \pmod p.$$

Тогда $x + \zeta y \equiv \zeta^s un \pmod p$. Переходя в этом сравнении к сопряженным, мы получаем

$$\overline{x + \zeta y} = x + \zeta^{-1}y \equiv \zeta^{-s}\overline{u}n = \zeta^{-s}un \pmod p \implies \zeta^s(x + \zeta^{-1}y) \equiv un \pmod p.$$

$$\begin{cases}\zeta^{-s}(x + \zeta y) \equiv un \pmod p \\ \zeta^s(x + \zeta^{-1}y) \equiv un \pmod p\end{cases} \implies \zeta^{-s}(x + \zeta y) \equiv \zeta^s(x + \zeta^{-1}y) \pmod p$$

$$x + \zeta y \equiv \zeta^{2s}(x + \zeta^{-1}y) \pmod p \implies x + \zeta y - \zeta^{2s}x - \zeta^{2s-1}y \in p\mathbb{Z}[\zeta]$$

Теперь рассмотрим несколько случаев:

1. Элементы $S = \{1, \zeta, \zeta^{2s}, \zeta^{2s-1}\}$ попарно различны.
   (a) Если $\zeta^{p-1} \notin S$, то $p \mid x, p \mid y$.
   (b) Если $\zeta^{p-1} = \zeta^{2s-1}$, то $s \vdots p$, а значит $(\zeta - \zeta^{-1})y \in p\mathbb{Z}[\zeta]$ откуда следует, что $p \mid 1 - \zeta^2$, что даёт нам противоречие.
   (c) Если $\zeta^{p-1} = -(1 + \zeta + \ldots + \zeta^{p-2}) = \zeta^{2s}$, а тогда

   $$x+\zeta y+((1+\zeta+\ldots+\zeta^{p-2}))x-\zeta^{p-2}y = 2x+\zeta(x+y)+x\zeta^2+\ldots+x\zeta^{p-3}+(x-y)\zeta^{p-2} \implies 2x \vdots p,$$

   что даёт нам противоречие.
2. Некоторые из этих степеней совпадают.
   (a) $\zeta^{2s} = 1$. В этом случае $s \vdots p$, а как мы уже видели, это влечёт $(\zeta - \zeta^{-1})y \ \vdots\ p$, что невозможно.
   (b) $\zeta^{2s-1} = 1$. В этом случае $x - y + \zeta y - \zeta x \vdots p \implies (x - y)(1 - \zeta) \vdots p \implies x - y \vdots p$, то есть $x \equiv y \pmod p$. Исходное уравнение мы можем записать в виде

   $$z^p + (-y)^p = x^p,$$

   и рассуждая аналогично, мы можем получить, что $(y + z) \vdots p,\ (x + z) \vdots p$. Тогда

   $$0 \equiv x^p + y^p - z^p \equiv x + y - z \equiv 3x \pmod p,$$

   откуда либо $p = 3$ (а в этом случае мы Большую теорему Ферма доказали), либо $p \mid x$, что даёт нам противоречие.

[7] такие простые числа называются *регулярными*

(c) $\zeta = \zeta^{2s-1}$. Тогда $x - \zeta^2 x \vdots p$, откуда следует, что $1 - \zeta^2 \vdots p$, а это, как мы уже видели, противоречие.

□

Дадим теперь хороший критерий для проверки условия теоремы. Этот критерий мы дадим без доказательства, так как он доказывается методами аналитической теории чисел.

Определение 127. Рассмотрим экспоненцальную прозводящую функцию

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_m \frac{t^m}{m!},$$

тогда

Подставим $-t$:

$$\frac{-t}{\frac{1}{e^t} - 1} = \frac{te^t}{e^t - 1} = \frac{t(e^t - 1) + t}{e^t - 1} = t + \frac{t}{e^t - 1}.$$

Отсюда мы можем понять, чему равны коэффициенты:

$$m > 1,\ m \equiv_2 1 \implies B_m = -B_m \implies B_m = 0.$$

Замечание. Так как все нечётные коэффициенты равны нулю, авторы часто используют обозначение B_n для $2n$-го числа Бернулли. Например, известно, что

$$B_n = -n\zeta(1 - n), n > 1.$$

Также отсюда мы имеем такую формулу:

Предложение 62.

$$-(n+1)B_n = \binom{n+1}{n-1} B_{n-1} + \ldots + \binom{n+1}{k} B_k + \ldots + \binom{n+1}{1} B_1 + 1.$$

Следствие 35. *Знаменатели $B_2, B_4, \ldots, B_{p-3}$ не делятся на p.*

Доказательство. Докажем это утверждение по индукци, база очевидна, докажем переход.

$$\upsilon_p\left(\binom{n+1}{n-1} B_{n-1} + \ldots + \binom{n+1}{k} B_k + \ldots + \binom{n+1}{1} B_1 + 1\right) \geq 0 \implies \upsilon_p((n+1)B_n) \geq 0 \implies \upsilon_p(B_n) \geq 0.$$

□

Так вот, нам числа Бернулли полезны, так как справедлива такая теорема:

Теорема 95. *Простое число p — регулярно тогда и только тогда, когда числители всех чисел Бернулли $B_2, B_3, \ldots, B_{p-3}$ не делятся на p.*

Пример 45. Например, таким образом нетрудно показать, что число 7 является регулярным. Действительно,

$$\overline{B_0} = 1,\ \overline{B_1} = \overline{3},\ -3\overline{B_2} = 3\overline{B_1} + \overline{1} = \overline{10} \implies \overline{B_3} = -\frac{\overline{10}}{\overline{3}} = -\overline{1},\ \overline{B_3} = 0,\ \overline{B_4} = 10\overline{B_2} + 5\cdot\overline{3} + 1 = -\overline{1} \implies \overline{B_4} = \frac{\overline{1}}{\overline{5}} = \overline{3}.$$

Теперь, немного отвлечёмся и приведём алгоритм построение целого базиса.

1.17 Алгоритм построения целого базиса

Итак, для $d = \operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ мы наем, что $d\mathcal{O}_k \subset \mathbb{Z}[\alpha] \subset \mathcal{O}_k$, откуда

$$\mathbb{Z}[\alpha] \subset \mathcal{O}_K \subset d^{-1}\mathbb{Z}[\alpha].$$

Тогда, как мы помним, $\bigcup(\omega_i + \mathbb{Z}[\alpha]) = d^{-1}\mathbb{Z}[\alpha]$, причем, каждый класс, либо вообще не содержит целых алгебраических чисел, либо целиком из них состоит. То есть, отсюда мы имеем

$$\mathcal{O}_K = \bigcup_{i \in I}(\omega_i + \mathbb{Z}[\alpha]),$$

откуда следует, что $\mathcal{O}_K$ порождена ω_i и α^s при $0 \leq s \leq n-1$. Значит, $d\mathcal{O}_K$ будет порождена $d\omega_i$ и $d\alpha^s$. С другой стороны, $d\mathcal{O}_K$ — подгруппа свободной абелевой группы $\mathbb{Z}[\alpha]$, значит мы попадаем в контекст нормальной формы Смита.

Домашнее задание 12. 1.

> **Теорема 96** (Штикельберг)**.** *Дискриминант конечного расширения $K/\mathbb{Q}$ сравним с нулём или единицей по модулю 4.*
> *Hint:* Можно действовать так: $\operatorname{disc}(K) = (\det(\sigma_i))^2$, и раскрывая определитель, мы получаем $\det(\sigma_j\omega_j) = P - N$, где P — сумма произведений со знаком +, а N — сумма произведений со знаком минус. Тогда $\operatorname{disc}(K) = (P-N)^2 = (P+N)^2 - 4PN$. Значит, достаточно показать, что числа $P+N$ и PN — целые. *Hint:* Целое число — это рациональное число, которое еще и целое алгебраическое.

2.

1.18 Геометрия чисел

Рассмотрим евклидово пространство $\mathbb{R}^n$, выберем в нём набор из k линейно независимых векторов $e_1, \ldots, e_k$ и рассмотрим порожденную ими свободную абелеву группу:

$$L = \bigoplus_{i=1}^{k} \mathbb{Z}e_i$$

Тогда L мы будем называть *решёткой*, натянутой на вектора $e_1, \ldots, e_k$. В случае $k = n$ решётка L называется *полной*.

Пример 46. Картинка для $L \subset \mathbb{R}^2$.

Предложение 63. *В любом ограниченном подмножестве $\mathbb{R}^n$ лежит конечное число точек решётки.*

Доказательство. В самом деле, можно сделать линейное преобразование, которое переводит произвольную решетку в прямоугольную. Оно будет переводить ограниченное множество в ограниченное, а для прямоугольной решетки необходимое свойство очевидно. □

Оказывается, верно и обратное утверждение.

Предложение 64. *Пусть $A \leq \mathbb{R}^n$ — подгруппа (как абелевой группы), причем такая, что в любом ограниченном подмножестве $\mathbb{R}^n$ лежит конечное число элементов из A. Тогда A — решётка.*

Доказательство. Рассмотрим подпространство $\operatorname{span}(A)$ в $\mathbb{R}^n$. Оно прождено некоторым линейно независимым набором векторов:

$$\operatorname{span}(A) = \langle e_1, \ldots, e_m \rangle,\ e_i \in A - \text{линейно независимы}.$$

Рассмотрим свободную абелеву группу, порожденную этими векторами:

$$A_0 = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_m.$$

Покажем, что A/A_0 конечна. Расммотрим *фундаментальную область*

$$\Delta = \left\{ \sum_{i=1}^{m} x_i e_i \;\middle|\; 0 \le x_i < 1 \right\}$$

Ясно, что $\forall a \in A\ \exists a_0 \in A_0 \colon a - a_0 \in \Delta$. Но так как Δ ограничено, в нём может лежать только конечное число элементов решётки, значит количество значений, которые может принимать $a - a_0$ конечно и A/A_0 конечна.

Значит, $\exists s \in \mathbb{Z} \setminus \{0\} \colon sA \subset A_0$. Тогда

$$A \subset \frac{1}{s} A_0 = \mathbb{Z}\frac{e_1}{s} \oplus \mathbb{Z}\frac{e_2}{s} \oplus \ldots \oplus \mathbb{Z}\frac{e_m}{s} = A_1.$$

Значит, $A_0 \subset A \subset A_1$, а A_0 и A_1 — свободные абелевы группы одного и того же ранга. Значит и A — свободная абелева группа,

$$A = \mathbb{Z}u_1 \oplus \mathbb{Z}u_2 \oplus \ldots \oplus \mathbb{Z}u_m.$$

Остаётся проверить, что $u_1, \ldots, u_m$ будут линейно независимы над $\mathbb{R}$. Но, это так, потому что

$$m = \dim \operatorname{span}(A_0) \le \dim \operatorname{span}(A_1) = \dim \langle u_1, \ldots, u_m \rangle.$$

□

Это предложение даёт хороший критерий для проверки, является ли какое-то подпространство решёткой.

Определение 128. Если $L \le \mathbb{R}^n$ — решётка с порождающим набором $e_1, \ldots, e_m$, то множество

$$\Delta = \left\{ \sum_{i=1}^{m} x_i e_i \;\middle|\; 0 \le x_i < 1 \right\}$$

называют *основным параллелипипедом* решётки или же *фундаментальной областью* решётки.

Если $e_1, \ldots, e_m$ — порождающий набор решётки L, то $\mathbb{R}^m = \operatorname{span}\{e_1, \ldots, e_m\}$ и тогда мы можем вычислить объем фундаментальной области, как

$$\operatorname{Vol}(\Delta) = \det |(a_{ij})|,$$

где $e_i = (a_{i1}, a_{i2}, \ldots, a_{in})$.

Лемма 61. Пусть T — ограниченное измеримое множество в $\mathbb{R}^m$, L — решётка ранга m в $\mathbb{R}^m$, Δ — её фундаментальная область. Предположим, что $\forall \ell_1, \ell_2 \in L$ множества $T + \ell_1$ и $T + \ell_2$ не пересекаются. Тогда

$$\operatorname{Vol}(T) \le \operatorname{Vol}(\Delta).$$

Доказательство. В самом деле, так как множества $T + \ell$ дизъюнктны,

$$\operatorname{Vol}(\Delta) \ge \sum_{\ell \in L} \operatorname{Vol}(\Delta \cap T_\ell) = \sum_{\ell \in L} \operatorname{Vol}(\Delta_{-\ell} \cap T) = \operatorname{Vol}\left(\bigcup_{\ell \in L} \Delta_\ell \cap T \right) = \operatorname{Vol}(\mathbb{R}^m \cap T) = \operatorname{Vol}(T).$$

□

Лемма 62 (Г. Минковский, О выпуклом теле)**.** Пусть T — ограниченное выпуклое центрально-симметричное (относительно нуля) измеримое подмножество $\mathbb{R}^n$, L — решётка ранга n в $\mathbb{R}^n$, Δ — её фундаментальная область. Предположим, что выполнена следующая оценка на объемы:

$$\operatorname{Vol}(T) > 2^n \operatorname{Vol}(\Delta).$$

Тогда $\exists 0 \ne \ell \in L \colon \ell \in T$. Кроме того, если T компактно, то это будет верно и в случае нестрогого неравенства $\operatorname{Vol}(T) \ge 2^n \operatorname{Vol}(\Delta)$.

Доказательство. Рассмотрим тело $\frac{1}{2}T$, тогда $\mathrm{Vol}\left(\frac{1}{2}T\right) = \frac{1}{2^n}\mathrm{Vol}(T) > \mathrm{Vol}(\Delta)$. Тогда по предыдущей лемме 61 $\exists \ell_1, \ell_2 \in L\colon \frac{1}{2}T_{\ell_1} \cap \frac{1}{2}T_{\ell_2} \neq \varnothing$. Это означает, что

$$\exists t_1, t_2 \in T\colon \frac{x_1}{2} + \ell_1 = \frac{x_2}{2} + \ell_2 \implies 0 \neq \frac{x_1 - x_2}{2} = \ell_1 - \ell_2 \in L \cap T.$$

В последнем равенстве $\frac{x_1 - x_2}{2} \in T$ так как T — выпукло и центрально симметрично.

Теперь докажем вторую часть теоремы. Рассмотрим $T_\varepsilon = (1+\varepsilon)T$, для него неравенство уже будет строгим и по первой части теоремы мы получим $0 \neq \ell \in L \cap T_\varepsilon$. Понятно, что если $\ell \in T$, всё доказано. Пусть теперь $\ell \in T_\varepsilon \setminus T$. Вообще говоря, в $T_\varepsilon \setminus T$ лежит лишь конечное число точек из L. Так как T_ε замкнуто, мы можем уменьшить ε так, чтоб все точки из ℓ, лежащие в $T_\varepsilon \setminus T$ уже не лежали там. □

Определение 129. Рассмотрим конечное расширение $K/\mathbb{Q}$, $[K : \mathbb{Q}] = n$. Тогда у нас есть n вложений $\sigma_i\colon K \to \mathbb{Q}^{alg}$. Среди них есть *вещественные* вложения, то есть такие, что $\mathrm{Im}(\sigma_i) \subset \mathbb{R}$. Остальные вложения называют *комплексными* (или, *невещественными*).

С каждым невещественным вложением σ_i связано вложение $\overline{\sigma_i} \neq \sigma_i$. Пронумеруем наши вложения следующим образом:

$\sigma_1, \ldots, \sigma_s$ — вещественные вложения, $\sigma_{s+1}, \overline{\sigma_{s+1}}, \sigma_{s+2}, \overline{\sigma_{s+2}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$ — комплексные вложения.

Так как количество вложений равно степени расширения, $s + 2t = n$.

Рассмотрим отображение $\varphi\colon K \to \mathbb{R}^n$, которое действует так:

$$\alpha \in K,\ \alpha \mapsto (\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_s(\alpha), \mathrm{Re}(\sigma_{s+1}(\alpha)), \mathrm{Im}(\sigma_{s+1}(\alpha)), \ldots, \mathrm{Re}(\sigma_{s+t}(\alpha)), \mathrm{Im}(\sigma_{s+t}(\alpha))) \in \mathbb{R}^n.$$

Пусть I — ненулевой идеал в $\mathcal{O}_K$. Возьмём его базис как абелевой группы — $\alpha_1, \ldots, \alpha_n$. Тогда $\varphi(I)$ — решётка в $\mathbb{R}^n$ с базисом $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$. Нужно проверить равзе что линейную независимость.

Пусть $\sigma_{s+k}(\alpha) = a + bi$, будем делать слудеющие преобразования:

$$(\mathrm{Re}\,\sigma_{s+k}\alpha, \mathrm{Im}\,\sigma_{s+k}\alpha) = (a,b) \mapsto (a, bi) \mapsto (a+bi, bi) \mapsto (a+bi, 2bi) \mapsto (a+bi, -a+bi) \mapsto$$
$$\mapsto (a+bi, a-bi) = (\sigma_{s+k}\alpha, \overline{\sigma_{s+k}\alpha}).$$

Посмотрим, что будет происходить с определителем при проделывании этих операций. Нетрудно проследить, что по итогу определитель умножится на $-2i$. В итоге мы получим, что

$$\det\left(\begin{pmatrix}\varphi(\alpha_1)\\ \varphi(\alpha_2)\\ \vdots\\ \varphi(\alpha_n)\end{pmatrix}\right) = \frac{1}{(2i)^t}\det\begin{pmatrix}\sigma_1(\alpha_1) & \ldots & \sigma_{s+1}(\alpha_1) & \overline{\sigma_{s+1}(\alpha_1)} & \ldots & \overline{\sigma_{s+t}(\alpha_1)} & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_{s+1}(\alpha_n) & \overline{\sigma_{s+1}(\alpha_n)} & \ldots & \overline{\sigma_{s+t}(\alpha_n)} & \end{pmatrix} = \pm\frac{1}{(2i)^t}\sqrt{|\operatorname{disc}(\alpha_1, \ldots, \alpha_n)|}.$$

А теперь заметим, что левая часть — объем фундаментальной области, а правую мы можем переписать в терминах $\mathrm{disc}(K)$, пользуясь предложением 56

$$\mathrm{Vol}(\Delta) = \left|\det\left(\begin{pmatrix}\varphi(\alpha_1)\\ \varphi(\alpha_2)\\ \vdots\\ \varphi(\alpha_n)\end{pmatrix}\right)\right| = \frac{1}{2^t}\sqrt{|\operatorname{disc}(\alpha_1, \ldots, \alpha_n)|} = \frac{1}{2^t}\sqrt{|\operatorname{disc}(K)| \cdot [\mathcal{O}_K : I]^2} = \frac{1}{2^t}\mathrm{N}(I)\sqrt{|\operatorname{disc}(K)|}.$$

Рассмотрим теперь для некоторого фиксированного $a > 0$.

$$T = \left\{(x_1, x_2, \ldots, x_s, y_1, z_1, \ldots, y_t, z_t) |\ |x_1| + \ldots + |x_s| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_t^2 + z_t^2} \leq a\right\}.$$

T — выпуклое, центрально-симметричное и $\mathrm{Vol}(T) = 2^s\left(\frac{\pi}{2}\right)^t \frac{a^n}{n!}$. Подберём a так, что для $0 \neq I \subset \mathcal{O}_K$ будет выполнено неравенство

$$2^s\left(\frac{\pi}{2}\right)^t \frac{a^n}{n!} > 2^n \frac{\sqrt{|\operatorname{disc}(K)|}}{2^t} \operatorname{N}(I). \tag{3.5}$$

Тогда по лемме Минковского 62 $\exists 0 \neq \alpha \in I$:

$$|\sigma_1(\alpha)| + \ldots + |\sigma_s(\alpha)| + 2|\sigma_{s+1}(\alpha)| + \ldots + 2|\sigma_{s+t}(\alpha)| \leq a.$$

Это неравенство мы можем переписать в виде:

$$|\sigma_1(\alpha)| + \ldots + |\sigma_s(\alpha)| + |\sigma_{s+1}(\alpha)| + |\overline{\sigma_{s+1}}(\alpha)| + \ldots + |\sigma_{s+t}(\alpha)| + |\overline{\sigma_{s+t}}(\alpha)| \leq a.$$

Тогда по неравенству о средних мы имеем

$$\left|\sigma_1(\alpha) \cdot \ldots \cdot \sigma_s(\alpha)\sigma_{s+1}(\alpha)\overline{\sigma_{s+1}(\alpha)} \cdot \ldots \cdot \sigma_{s+t}(\alpha)\overline{\sigma_{s+t}}(\alpha)\right| \leq \left(\frac{a}{n}\right)^n \Leftrightarrow \operatorname{N}(\alpha) \leq \left(\frac{a}{n}\right)^n$$

Заметим, что в неравенстве (3.5) равенство будет достигаться при

$$a^n = \frac{2^n\sqrt{|\operatorname{disc}(K)|}\operatorname{N}(I)n!}{2^t 2^s} \cdot \left(\frac{2}{\pi}\right)^t = \left(\frac{4}{\pi}\right)^t n!\operatorname{N}(\alpha)\sqrt{|\operatorname{disc}(K)|}.$$

В этом случае будет выполняться неравенство

$$\operatorname{N}(\alpha) \leq \left(\frac{a}{n}\right)^n = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\operatorname{N}(I)\sqrt{\operatorname{disc} K}.$$

Замечание. Подставим в этом неравенство, например, единичный идеал. Тогда мы получим неравенство

$$1 \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{\operatorname{disc} K}.$$

Например, из этого неравенства следует, что $\operatorname{disc}(K) \neq 1$ (в случае нетривиального расширения).

Теорема 97. *Пусть $K/\mathbb{Q}$ — конечное расширение, $[K:\mathbb{Q}] = n > 1$. Тогда* $\operatorname{disc}(K) \neq 1$. *Кроме того,*

$$\lim_{n\to\infty} \operatorname{disc}(K) = \infty.$$

Получим теперь при помощи новых методов некоторые результаты, связанные с группой классов идеалов числового поля.

Мы доказали, что для ненулевого идеала I в $\mathcal{O}_K$ существует $\alpha \in I$:

$$\operatorname{N}(\alpha) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\operatorname{N}(I)\sqrt{\operatorname{disc} K}.$$

Возьмём класс $[J] \in \mathcal{C}\ell(K)$, для него существует целый идеал I такой, что $[J] = [I^{-1}] \in \mathcal{C}\ell(K)$.Пусть $\alpha \in I$. С одной стороны, αI^{-1} представляет тот же класс в группе классов, а с другой стороны,

$$|\operatorname{N}(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \cdot \frac{n!}{n^n}\operatorname{N}(I)\sqrt{|\operatorname{disc}(K)|}.$$

$$\operatorname{N}(\underbrace{\alpha I^{-1}}_{\text{целый}}) = \operatorname{N}(\alpha)\operatorname{N}\left(I^{-1}\right) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\operatorname{disc}(K)|}.$$

Но, как мы уже замечали, существует лишь конечное число целых идеалов с ограниченной нормой. Значит, мы получили еще одно (геометрическое) доказательство теоремы 86.

Пример 47. Рассмотрим $K = \mathbb{Q}(\sqrt[3]{6})$. Посмотрим сначала на количество вложений. Нетрудно убедиться в том, что $n = 3, t = 1$. Сосчитаем теперь дискриминант K. Для этого покажем, что $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{6}]$. Обозначим $\theta = \sqrt[3]{6}$ и посчитаем $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. Заметим, что минимальный многочлен θ — это $x^3 - 6$, а минимальный многочлен θ^2 — это $x^2 - 36$, а тогда

$$\operatorname{disc}(K) \cdot (\operatorname{ind}(\theta))^2 = \operatorname{disc}(1, \theta, \theta^2) = \det \begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\theta) & \operatorname{Tr}(\theta^2) \\ \operatorname{Tr}(\theta) & \operatorname{Tr}(\theta^2) & \operatorname{Tr}(\theta^3) \\ \operatorname{Tr}(\theta^2) & \operatorname{Tr}(\theta^3) & \operatorname{Tr}(\theta^4) \end{pmatrix} = \det \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 18 \\ 0 & 18 & 0 \end{pmatrix} = -2^2 3^5.$$

Заметим, что многочлен $x^3 - 6$ является многочленом Эйзенштейна относительно и двойки и тройки, а значит, $\operatorname{ind}(\theta)$ не может делиться на 2 и 3, откуда $\operatorname{ind}(\theta) = 1$. Значит, $\operatorname{disc}(K) = -2^5 \cdot 3^5$. Подставим это в полученное выше неравенство:

$$\operatorname{N}(\underbrace{\alpha I^{-1}}_{\text{целый}}) = \operatorname{N}(\alpha) \operatorname{N}\big(I^{-1}\big) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|\operatorname{disc}(K)|} = \frac{4}{\pi} \cdot \frac{6}{27} \cdot \sqrt{2^5 \cdot 3^5} < \frac{16}{\sqrt{3}} < 10.$$

То есть, в любом классе есть целый представитель, норма которого меньше 10. Значит, чтоб показать, что группа классов тривиальна, нам достаточно показать, что любой идеал, висящий над 2, 3, 5, 7 — главный.

Из теоремы Куммера 91 легко понять, что

$$2\mathcal{O}_K = (2, \theta)^3 = (\theta - 2)^3,$$

так как $\operatorname{N}(\theta - 2) = -2 \implies (\theta - 2)$ — простой и он тоже висит над двойкой, откуда $(2, \theta) = (\theta - 2)$.

Аналогичное явление будет и с тройкой:

$$3\mathcal{O}_K = (3, \theta)^3 = \left(\frac{\theta}{\theta - 2}\right)^3 = \left(\frac{6 + 2\theta^2 + 4\theta}{-2}\right)^3 = (3 + \theta^2 + 2\theta)^3.$$

Действительно, $\operatorname{N}(\theta) = 6,\ \operatorname{N}(\theta - 2) = -2$, откуда $\operatorname{N}\left(\frac{\theta}{\theta-2}\right) = -3$, то есть $\frac{\theta}{\theta-2}$ — простой, висящий над тройкой, $(3, \theta) = \left(\frac{\theta}{\theta-2}\right)$.

Теперь, опять же из теоремы Куммера 91, мы получаем, что

$$5\mathcal{O}_K = (5, \theta - 1)(5, \theta^2 + \theta + 1)^2$$

и надо показать, что эти идеалы главные. В самом деле, $\operatorname{N}(\theta - 1) = 5$ и при этом

$$\frac{5}{\theta - 1} = \theta^2 + \theta + 1,$$

откуда $(5, \theta^2 + \theta + 1) = (\theta^2 + \theta + 1),\ (5, \theta - 1) = (\theta - 1)$. Теперь, делаем то же самое над семёркой:

$$x^3 - 6 = x^3 + 1 = (x + 1)(x^2 - x + 1) = (x + 1)(x - 3)(x - 5) \text{ в } \mathbb{F}_7[x].$$

Тогда семёрка будет раскладываться, как

$$7\mathcal{O}_K = (7, \theta + 1)(7, \theta - 3)(7, \theta - 5).$$

Во-первых, заметим, что

$$\frac{7}{\theta + 1} = \frac{7(\theta^2 - \theta + 1)}{\theta^3 + 1} \implies (7, \theta + 1) = (\theta + 1).$$

$$\operatorname{N}(\theta - 3) = 21, \operatorname{N}\left(\frac{\theta}{\theta - 2}\right) = -2 \implies \operatorname{N}\left(\frac{(\theta - 3)(\theta - 2)}{\theta}\right) = -7$$

Этот элемент даёт нам максимальный главный идеал, висящий над семёркой. Нетрудно заметить, что

$$(7, \theta - 3) \subset \left(\frac{(\theta-3)(\theta-2)}{\theta}\right)$$

а так как оба идеала максимальные, они совпадают. Значит и третий идеал главный (так как произведение трех главных идеалов равно главному идеалу).

Таким образом, мы показали, что любой идеал кольца $\mathcal{O}_K$ является главным, то есть, что $\mathcal{C}\ell(\mathbb{Q}(\sqrt[3]{6})) = 0$.

Пример 48. Оказывается, в случае квадратичных расширений оценка Минковского работает существенно лучше оценки, которой мы пользовлись при первом знакомстве с группой классов. Вычислим при её помощи группу $\mathcal{C}\ell(\mathbb{Q}(\sqrt{-14}))$.

Как мы видели выше,

$$\mathrm{N}(\alpha I^{-1}) \leq \left(\frac{4}{\pi}\right)^t \cdot \frac{n!}{n^n}\sqrt{|\operatorname{disc}(K)|}$$

Соотвественно, тут $n = 2$ и $t = 1$. Пусть $\theta = \sqrt{-14}$ и $f(t) = t^2 + 14$ — минимальный многочлен θ. Тогда

$$|\operatorname{disc}(1, \theta)| = |\mathrm{N}(f'(\theta))| = |\mathrm{N}(2\sqrt{-14})| = 4 \cdot |\mathrm{N}(\theta)| = 4 \cdot 14.$$

Отсюда мы имеем

$$\mathrm{N}(J) \leq \frac{4}{\pi} \cdot \frac{2}{4} \cdot 2\sqrt{14} < 5.$$

Значит, нам достаточно рассматривать идеалы, висящие над двойкой и тройкой. Воспользуемся теоремой Куммера:

$$2\mathcal{O}_K = (2, \theta)^2, \quad \mathfrak{p}_2 = (2, \theta), \quad 3\mathcal{O}_K = (3, \theta - 1)(3, \theta + 1) = \mathfrak{p}_3 \cdot \mathfrak{p}_3'.$$

Заметим, что $[\mathfrak{p}^2] = e \in \mathcal{C}\ell(K)$, $[\mathfrak{p}_3\mathfrak{p}_3'] = e \in \mathcal{C}\ell(K)$, откуда $[\mathfrak{p}_3] = [\mathfrak{p}_3'^{-1}]$. Кроме того,

$$(2 + \sqrt{14})\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_3^2,$$

так как $\mathrm{N}(\mathfrak{p}_3^2) = 9$, $\mathrm{N}(\mathfrak{p}_2) = 2$, а $\mathrm{N}(2 + \sqrt{14}) = 18$. Отсюда мы получаем

$$\begin{cases} [\mathfrak{p}_2]^2 = [e], \\ [\mathfrak{p}_2\mathfrak{p}_3^2] = e \end{cases} \implies [\mathfrak{p}_3^4] = e \in \mathcal{C}\ell(K).$$

Докажем, что $[\mathfrak{p}_3^2] \neq 3$. Предположим противное, тогда $\mathrm{N}(\mathfrak{p}_3^2) = \mathrm{N}((\alpha))$ для некоторого $\alpha = a + b\sqrt{-14}$, $a, b \in Z$. Тогда

$$a^2 + 14b^2 = 9 \implies a = \pm 3,\ b = 0,$$

то есть $\mathfrak{p}_3^2 = (3)$, но мы уже убеждались, что это не так.

Таким образом, мы полнотью описали таблицу умножения в группе $\mathcal{C}\ell(K)$ и можем заключить, что $\mathcal{C}\ell(K) \cong \mathbb{Z}/4\mathbb{Z}$ с образующей $[\mathfrak{p}_3]$.

Домашнее задание 13. Задачи:

1. Докажите, что для любого простого p уравнение

$$3x^2 + 4y^3 + 5z^3 = 0$$

имеет ненулевое решение над $\mathbb{F}_p$.
2. Докажите, что $1 - 6\theta + 3\theta^2 \in \mathcal{O}_K^*$, где $K = \mathbb{Q}(\sqrt[3]{6})$.
3. Докажите, что $\mathrm{Cl}(\mathbb{Q}(\sqrt{-23})) = \mathbb{Z}/3\mathbb{Z}$.

1.19 Мультипликативная группа кольца целых числового поля

Пусть числа s и t, связанные с количеством вложений числового поля $K \to \mathbb{Q}^{alg}$ определены как в . В этом параграфе мы докажем, что мультипликативная группа кольца целых числового поля имеет вид

$$\mathcal{O}_K^* \cong \mu \oplus \mathbb{Z}^{s+t-1},$$

где μ — группа корней из единицы. Этот факт будет иметь множество приложений. Этот факт обычно называют *сильной формой теоремы Дирихле о единицах.*

Пример 49. Рассмотрим квадратичное расширение $K = \mathbb{Q}(\sqrt{d})$. Если $\mathbb{Q}(\zeta_n) \subset\in \mathbb{Q}(\sqrt{d})$, то $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq 2$, но с другой стороны $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, откуда $n = 1, 2, 3, 4, 6$. Если $n = 3$, то $d = -3$, если $n = 4$, то $d = -1$, если $n = 6$, то $d = -3$, но $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$, так как $\zeta_6 = -\zeta_3$, а в остальных случаях нетривиальных корней из единицы в этом поле нет.

Пусть s и t опредедлены как тут. Соотвественно, если $d > 0$, то $s = 2, t = 0 \implies s + t - 1 = 1 \implies \mathcal{O}_K^* = \{\pm\theta \mid m \in \mathbb{Z}\}$.

Если $d > 0$ и $d \not\equiv 1 \pmod 4 \implies \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Как мы помним, $u \in \mathcal{O}_K^* \Leftrightarrow \mathrm{N}_{K/\mathbb{Q}}(u) = \pm 1$. В нашем случае

$$\mathrm{N}(x + y\sqrt{d}) = x^2 - dy^2 = \pm 1 \tag{3.6}$$

и из другого описания $\mathcal{O}_K^*$ мы получаем, что все решения уравнения (3.6) имеют вид $\{\pm\theta^m \mid m \in \mathbb{Z}\}$. Из этого, например, следует, что решений уравнения (3.6) бесконечно много.

Вообще говоря, этот самый элемент $\theta = \theta_d$ может иметь очень неприятный вид. Например, $\theta_2 = 1 + \sqrt{2},\ \theta_3 = 2 + \sqrt{3},\ \theta_{94} = 2143295 + 221064\sqrt{94}$.

Если же $d < 0$, то вполне ясно, что $s = 0,\ t = 1 \implies s + t - 1 = 0$, откуда следует, что $\mathcal{O}_K^* = \mu$, откуда, в частности, следует, что уравнение (3.6) имеет конечно число решение.

Теорема 98 (Дирихле, о единицах, *слабая форма*)**.** *Мультипликативная группа кольца целых $\mathcal{O}_K$ числового поля K имеет вид*

$$\mathcal{O}_K^* \cong \mu \oplus \mathbb{Z}^m,\ \textit{где}\ m \leq s + t - 1.$$

Доказательство. Рассмотрим отображение $\ell\colon K^* \to \mathbb{R}^{s+t}$, действующее следующим образом

$$\ell(\alpha) = \big(\log|\sigma_1\alpha|, \log|\sigma_2\alpha|, \ldots, \log|\sigma_s\alpha|, \log|\sigma_{s+1}\alpha|^2, \ldots, \log|\sigma_{s+t}\alpha|^2\big).$$

Заметим, что это гомомомрфизм групп, $\ell(\alpha\beta) = \ell(\alpha) + \ell(\beta)$. Рассмотрим сужение $\ell\colon \mathcal{O}_K^* \to \mathbb{R}^{s+t}$ (чтоб не перегружать обозначения, с этого момента мы называем сужение той же буквой ℓ). Посчитаем ядро этого отображения:

$$\alpha \in \operatorname{Ker}\ell \Leftrightarrow \forall i = 1, \ldots, s+t \quad |\sigma_i\alpha| = 1 \underbrace{\Longrightarrow}_{\text{Л. 58}} \operatorname{Ker}\ell = \mu.$$

Теперь посчитаем $\operatorname{Im}\ell,\ \ell\colon \mathcal{O}_K^* \to \mathbb{R}$. Пусть $\alpha \in \mathcal{O}_K^*$, тогда мы знаем, что $\mathrm{N}(\alpha) = \pm 1$, откуда

$$\log|\mathrm{N}(\alpha)| = \log|\sigma_1\alpha| + \ldots + \log|\sigma_{s+1}\alpha| + \log|\overline{\sigma}_{s+1}\alpha| + \ldots = 0,$$

что даёт нам, что образы всех обратимых элементов лежат в гиперплоскости

$$x_1 + x_2 + \ldots + x_{s+t} = 0.$$

Лемма 63. $\operatorname{Im}\ell$ — решётка в $\mathbb{R}^{s+t}$.

Доказательство. Надо проверить, что $\operatorname{Im}\ell$ — это дискретная подгруппа в $\mathbb{R}^{s+t}$ (то, что это подгруппа — очевидно). Иными словами, нам надо показать, что в любом ограниченном множестве содержится конечное число точек из $\operatorname{Im}\ell$. Ясно, что это достаточно проверять для шаров, рассмотрим шар $\overline{B}_r(0)$.

Ясно, что неравенства

$$\log|\sigma_j\alpha| \leq r\ \forall j \Leftrightarrow |\sigma_j\alpha| \leq e^r\ \forall j = 1, \ldots, s, \quad |\sigma_j\alpha| < e^{\frac{r}{2}}\ \forall j = s+1, \ldots, s+t.$$

Нетрудно заметить, что из этих неравенств следуют неравенства на мнимую и вещественную часть координат $s+1,\dots,s+t$, то есть мы имеем

$$|\sigma_j\alpha| \leq e^r \ \forall j = 1,\dots,s, \quad |\operatorname{Im}\sigma_j\alpha| \leq e^{\frac{r}{2}},\ |\operatorname{Re}\sigma_j\alpha| \leq e^{\frac{r}{2}}\ \forall j = s+1,\dots,s+t.$$

Но, в предыдущем параграфе мы уже рассматривали отображение φ

$$\varphi(\alpha) = (\sigma_1(\alpha),\sigma_2(\alpha),\dots,\sigma_s(\alpha),\operatorname{Re}(\sigma_{s+1}(\alpha)),\operatorname{Im}(\sigma_{s+1}(\alpha)),\dots,\operatorname{Re}(\sigma_{s+t}(\alpha)),\operatorname{Im}(\sigma_{s+t}(\alpha))) \in \mathbb{R}^n,$$

и доказывали, что $\operatorname{Im}\varphi$ — решётка. Тогда по предложению 63 в шаре $\overline{B}_{e^r}$ лежит лишь конечное число точек из образа φ, но тогда, по отмеченному выше, там будет лежать лишь конечное число точек из $\operatorname{Im}\ell$, а тогда по предложению 64 $\operatorname{Im}\ell$ — решётка. □

Значит, $\operatorname{Im}\ell$ порождён m линейно-независимыми в $\mathbb{R}^{s+t}$ векторами и $\operatorname{Im}\ell \cong \mathbb{Z}^m$. С другой стороны, так как $\operatorname{Im}\ell$ лежит в гиперплоскости, $m \leq s+t-1$. Тогда у нас есть короткая точная последовательность

$$0 \to \operatorname{Ker}\ell \hookrightarrow \mathcal{O}_K^* \xrightarrow{\ell} \operatorname{Im}\ell \to 0.$$

Как мы уже выяснили выше, $\operatorname{Ker}\ell \cong \mu$, а $\operatorname{Im}\ell \cong \mathbb{Z}^m, m \leq s+t-1$, а значит

$$0 \to \mu \hookrightarrow \mathcal{O}_K^* \xrightarrow{\ell} \mathbb{Z}^m \to 0, \quad m \leq s+t-1.$$

откуда $\mathcal{O}_K^* \cong \mu \oplus \mathbb{Z}^m, \quad m \leq s+t-1.$ □

Даже слабая форма теоремы Дирихле о единицах позволяет успешно вычислять мультипликативные группы колец целых числовых полей.

Пример 50. Из 1.21 мы знаем, что в $K = \mathbb{Q}(\theta)$, где $\theta^3 = 6$ мы имеем

$$\frac{1}{1-6\theta+3\theta^2} = 109 + 60\theta + 33\theta^2$$

В данном случае $s=1, t=1 \implies s+t-1=1$, откуда $m=1$, так как ясно, что $m \leq 1$, так как если $m=0$, то никаких обратимых элементов, кроме μ в $\mathcal{O}_K$ нет, а из корней из единицы в этом кольце есть только ±1, так как если $\mathbb{Q}(\zeta_n) \subset \mathbb{Q}(\sqrt[3]{6})$, то $\varphi(n)=2$. Таким образом, мы имеем

$$\mathcal{O}_K^* \cong \mu_2 \oplus \mathbb{Z}.$$

Предложение 65. *Элемент $\varepsilon = 1-6\theta+3\theta^2$ — основная единица в $\mathcal{O}_K^*$.*

Доказательство. Во-первых, как мы уже отметили выше, этот элемент обратим и его обратный — это $109+60\theta+33\theta^2$.

Предположим, что основная единица — это α, тогда, так как $\mu_2 = \{\pm1\}$

$$1-6\theta+3\theta^2 = \pm\alpha^d, \quad d \geq 2.$$

Пусть $\omega^3 = 1$, тогда все вложения $K \to \mathbb{Q}^{alg}$ — это

$$\theta \mapsto \theta, \quad \theta \mapsto \omega\cdot\theta, \quad \omega^2\cdot\theta.$$

Рассмотрим ε' и ε'' — образы ε при комплексных вложениях,

$$\varepsilon' = 1-6\theta\omega+3\theta^2\omega^2, \quad \varepsilon'' = 1-6\theta\omega^2+3\theta^2\omega,\ \varepsilon' = \overline{\varepsilon''}.$$

Заметим, что тогда, по определению нормы:

$$\pm1 = \mathrm{N}(\varepsilon) = \varepsilon\cdot\varepsilon'\cdot\varepsilon''.$$

$$\begin{cases} |\varepsilon'| = |\varepsilon''| \\ |\varepsilon\varepsilon'\varepsilon''| = 1 \end{cases} \implies |\varepsilon'| = |\varepsilon''| = \sqrt{|\varepsilon|^{-1}} = \sqrt{|109 + 60\theta + 33\theta^2|} < \sqrt{109 + 60 \cdot 2 + 33 \cdot 4} = \sqrt{361} = \sqrt{19}.$$

Запишем α в виде $\alpha = x + y\theta + z\theta^2,\ x, y, z \in \mathbb{Z}$ и рассмотрим его образы при комплексных вложениях:

$$\alpha' = x + y\theta\omega + z\theta^2\omega^2, \quad \alpha'' = x + y\theta\omega^2 + z\theta^2\omega.$$

Так как $1 + \omega + \omega^2 = 0$, мы имеем

$$y\theta = \frac{\alpha + \alpha''\omega + \alpha'\omega^2}{3}, \quad z\theta^2 = \frac{\alpha + \alpha'\omega + \alpha''\omega^2}{3}.$$

Теперь заметим, что $|\varepsilon| = |\alpha|^d$, откуда $|\alpha| = |\varepsilon|^{\frac{1}{d}}$. Тогда

$$|\alpha'| \leq |\varepsilon'|^{\frac{1}{d}} \leq \sqrt{|\varepsilon'|} < \sqrt{19}, \quad |\alpha''| \leq |\varepsilon''|^{\frac{1}{d}} \leq \sqrt{|\varepsilon''|} < \sqrt{19},$$

так как $d \geq 2$. Оценим теперь $|y|$. Заметим, что $|\alpha| = |\varepsilon|^{\frac{1}{d}} < 1$[8], откуда

$$|y| = \frac{|\alpha + \alpha''\omega + \alpha'\omega^2|}{3|\theta|} \leq \frac{|\alpha + \sqrt{19}|}{3|\theta|} < \frac{1 + \sqrt{19}}{3|\theta|} < 2.$$

Абсолютно аналогичным образом мы получаем, что

$$|z| < \frac{9{,}8}{3|\theta|^2} < 1.$$

Так как $z \in \mathbb{Z}$, отсюда следует, что $z = 0$. Значит, $\alpha = x + \theta y$, $|y| < 2$. Как мы помним,

$$\pm 1 = \mathrm{N}(\alpha) = x^3 + 6y^3 \implies x^3 \equiv \pm 1 \pmod 3 \implies x \equiv \pm 1 \pmod{(3)} \equiv x^3 \equiv \pm 1 \pmod 9,$$

а тогда $y \vdots 9$ и отсюда $y = 0$, но тогда $\alpha = x \in \mathbb{Z}$, что даёт нам противоречие. □

Домашнее задание 14.

- Рассмотрим $K = \mathbb{Q}(\zeta_5)$. Докажите, что $\mathcal{O}_K$ — евклидово.
- Приведите пример неизоморфных расширений K_1, K_2 над $\mathbb{Q}$ одинаковой степени и таких, что $\mathrm{disc}(K_1) = \mathrm{disc}(K_2)$.
  Рассмотрим $K_1 = \mathbb{Q}(\theta),\ \theta^3 - 18\theta - 6 = 0$, $K_2 = K(\xi),\ \xi^3 - 36\xi - 78 = 0$, $K_3 = \theta^3 - 54\theta - 150 = 0$.
- Тут была еще задача, её надо с фотки переписать.

Докажем теперь сильную теорему Дирихле о единицах:

Теорема 99. *Пусть $K/\mathbb{Q}$ — конечное расщирение, $[K : \mathbb{Q}]$, а числа s, t связаны с количествами вещественных и комплексных вложений. Тогда*

$$\mathcal{O}_K^* \cong \mu \oplus \mathbb{Z}^{s+t-1},$$

где μ — группа всех корней из единицы в $\mathcal{O}_K$.

Доказательство. Ясно, что для этого нам достаточно доказать оценку $m \geq s + t - 1$, а это равносильно тому, что $\mathrm{Im}\,\ell$ — полная решётка в гиперплоскости

$$x_1 + x_2 + \ldots + x_{s+t} = 0.$$

Для этого необходимо найти систему из $(s + t - 1)$-го линейно независимого над $\mathbb{R}$ элемента $\ell(\mathcal{O}_K^*)$.

Соотвественно, надо найти $s + t$ элементов $u_1, \ldots, u_{s+t} \in \mathcal{O}_K^*$, которые дадут нам $s + t - 1$ линейно независимый над $\mathbb{R}$ вектор в образе. Мы постараемся найти такие u, что их образы имеют вид

$$u_1 \mapsto (+, -, -, \ldots, -), u_2 \mapsto (-, +, -, \ldots, -), \ldots u_n \mapsto (-, -, \ldots, +).$$

[8] в том, что $|\varepsilon| < 1$ легко убедиться непосредственно.

Обозначение выше означает, что на соовтествующей координате стоит число соотвествующего знака. Покажем сначала, что такие векторы нам подойдут. Возьмём первые $s+t-1$ координату первых $s+t-1$ столбцов матрицы, где $\ell(u_i)$ записаны по строкам и обозначим за A. Для ясности, выпишем еще раз эту матрицу:

$$A = \begin{pmatrix} + & - & - & \dots & - \\ - & + & - & \dots & - \\ \vdots & \vdots & \dots & \dots & \vdots \\ - & - & - & \dots & + \end{pmatrix}, \quad A \in \mathrm{M}_{s+t-1}(\mathbb{R}).$$

Ясно, что достаточно доказать, что эта матрица имеет полный ранг. Заметим, что так как образ лежит в гиперплоскости $x_1 + \ldots + x_{s+t} = 0$ изначально сумма по каждой строке равна нулю, то есть

$$a_{i,1} + a_{i,2} + \ldots + a_{i,s+t} = 0,$$

а так как $\forall i = 1, \ldots, s+t-1 \quad a_{i,s+t} < 0$, в усеченной матрице (которую мы обозначили за A), сумма по каждой строке будет равна

$$a_{i,1} + a_{i,2} + \ldots + a_{i,s+t-1} > 0.$$

Докажем теперь такую лемму:

Лемма 64. Пусть $A \in \mathrm{M}_m(\mathbb{R})$ такая, что $\forall i\ a_{ii} > 0, \forall i \neq j\ a_{ij} < 0,\ \forall i\ \sum_{j=1}^m a_{ij} > 0$. Тогда $\operatorname{rank} A = m$.

Доказательство. Предположим, что $\operatorname{Ker} A \neq \{0\}$, то есть система

$$\begin{cases} a_{11}x_1 + \ldots + a_{1m}x_m = 0 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mm}x_m = 0 \end{cases}.$$

имеет нетривиальное решение.

Не умаляя общности, x_1 — максимальная по модулю координата. Тогда

$$0 = |a_{11}x_1 + \ldots + a_{1m}x_m| \geq |a_{11}x_1| - |a_{12}x_2| - \ldots - |a_{1m}||x_m| \geq |x_1| \underbrace{(a_{11} - |a_{12}| - \ldots - |a_{1m}|)}_{>0} \geq 0,$$

откуда $|x_1| = 0 \implies |x_i| = 0\ \forall i = 1, \ldots, m$. □

Остаётся найти систему $u_1, \ldots, u_{s+t}$, которые в образе дадут нужные знаки координат. Пусть $n = s+2t$, рассмотрим множество

$$Y = \left\{(x_1, \ldots, x_s, y_1, z_1, \ldots y_t, z_t), \quad |x_i| < C_i \forall 1 \leq i \leq s, y_i^2 + z_i^2 < C_{s+i}\right\}.$$

Нетрудно проверить, что Y — ограниченное, выпуклое и центрально-симметричное. Кроме того,

$$\operatorname{Vol}(Y) = 2^s \prod_{i=1}^{s} C_i \cdot \pi^t \cdot \prod_{i=1}^{t} C_{s+i} = 2^s \pi^t \cdot \prod_{i=1}^{s+t} C_i.$$

Пусть Γ — полная решётка, Δ — объем фундаментальной области. Тогда, если

$$2^s \pi^t \prod_{i=1}^{s+t} C_i > 2^n \Delta,$$

то Y будет содержать точку из решетки Γ (по лемме Минковкого о выпуклом теле 62). В качестве Γ мы возьмём $\operatorname{Im} \varphi$, где

$$\varphi(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_s(\alpha), \operatorname{Re}(\sigma_{s+1}(\alpha)), \operatorname{Im}(\sigma_{s+1}(\alpha)), \ldots, \operatorname{Re}(\sigma_{s+t}(\alpha)), \operatorname{Im}(\sigma_{s+t}(\alpha))) \in \mathbb{R}^n.$$

Заметим, что неравенство выше равносильно тому, что

$$\prod_{i=1}^{s+t} C_i > \left(\frac{4}{\pi}\right)^t \cdot \Delta.$$

Возьмём $C > \left(\frac{4}{\pi}\right)^t \Delta$ и рассмотри все главные идеалы $a_i\mathcal{O}_K \subset \mathcal{O}_K$: $\mathrm{N}(a_i\mathcal{O}_K) < C$. Пусть $\varepsilon = \min\left(|\sigma_i a_j|, |\sigma_{s+i} a_j|^2\right) > 0$.

Зафиксируем теперь некоторый $\sigma_j \in \{\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \ldots, \sigma_{s+t}\}$ и определим

$$C_i = \begin{cases} \varepsilon, i \neq j \\ C \cdot \varepsilon^{-(s+t-1)}, i = j \end{cases}.$$

Нетрудно заметить, что всё подрбрано таким образом, что

$$\prod_{i=1}^{s+t} C_i > \left(\frac{4}{\pi}\right)^t \Delta.$$

Тогда по лемме 62 $\exists 0 \neq x \in \mathcal{O}_K$:

$$|\sigma_1 x| < C_1, \ldots, |\sigma_s x| < C_s, \quad |\sigma_{s+1} x|^2 < C_{s+1}, \ldots, |\sigma_{s+t} x|^2 < C_{s+t}.$$

Вычислим норму этого $x \in \mathcal{O}_K$

$$\mathrm{N}(x\mathcal{O}_K) = |\,\mathrm{N}(x)| = |\sigma_1 x| \ldots |\sigma_s x||\sigma_{s+1} x|^2 \ldots |\sigma_{s+t} x|^2 < \prod_{i=1}^{s+t} C_i = C.$$

Значит, для некоторого i мы имеем $x\mathcal{O}_K = a_i\mathcal{O}_K$. Положим $u = \frac{x}{a_i}$. Тогда $\mathrm{N}(u) = 1 \implies u \in \mathcal{O}_K^*$.

Так для каждого σ_j мы находим свой u (назовём его u_j). Проверим, что $\{u_j\}$ подойдут. Пусть $\tau = \sigma_i$,

$$|\tau u_j| = \frac{|\tau x|}{|\tau a_k|},$$

докажем, что для всех $\tau \neq \sigma_j$ будет выполнено $|\tau u_j| < 1$ (это означает, что в соотвествующей координате будет знак минус). Ясно, что этого будет достаточно, так как сумма координат равна нулю. Рассмотрим два случая:

- Пусть $\tau \in \{\sigma_1, \ldots, \sigma_s\},\ \tau = \sigma_i$, тогда

$$|\tau u_j| = \frac{|\tau x|}{|\tau a_k|} < \frac{C_i}{\varepsilon} = 1, \text{ так как } i \neq j.$$

- Пусть $\tau \in \{\sigma_{s+1}, \ldots, \sigma_{s+t}\}$, тогда

$$|\tau u_j| = \frac{|\tau x|}{|\tau a_j|} < \frac{\sqrt{C_i}}{\sqrt{\varepsilon}} = 1.$$

Таким образом, мы показали, что $\mathrm{Im}\,\ell$ — полная решетка в гипеплоскости, то есть $\mathrm{Im}\,\ell \cong \mathbb{Z}^{s+t-1}$, откуда, как мы уже замечали в доказательстве слабой теоремы Дирихле о единицах 98

$$\mathcal{O}_K^* \cong \mu \oplus \mathbb{Z}^{s+t-1}.$$

□

1.20 Контр-пример к принципу Минковского-Хассе

Начнём с вот такого утверждения.

Предложение 66 (ДЗ 11, задача 3). *Пусть* $K = \mathbb{Q}(\alpha),\ \alpha^3 + a\alpha + b = 0$ *где* $a, b \in \mathbb{Z}$. *Пусть* $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ *и* $\alpha \in \mathfrak{p}_1\mathfrak{p}_2$. *Тогда* $\alpha \in \mathfrak{p}_3$.

Доказательство. Перепишем данное равенство, как $\alpha(\alpha^2 + a) = -b$ и возьмём норму от обеих частей:

$$\mathrm{N}(\alpha)\,\mathrm{N}(\alpha^2 + a) = \mathrm{N}(-b) = -b^3.$$

Так как $\mathrm{N}(\alpha) = (-1)^3 b = -b$, отсюда $\mathrm{N}(\alpha^2 + a) = b^2$. Сразу заметим, что $b \vdots p$, так как

$$-b = \mathrm{N}(\alpha), \quad (\alpha) = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2} \cdot \ldots \implies \mathrm{N}(\alpha) \vdots p,$$

так как $\mathrm{N}(\mathfrak{p}_1), \mathrm{N}(\mathfrak{p}_2) \vdots p$, так как они висят над p.

1. Пусть $a \in p\mathbb{Z}$. Тогда, так как $\alpha^3 = a\alpha - b$, а $b \vdots p$, в этом случае $\alpha^3 \vdots p$, откуда $\alpha^3 \in \mathfrak{p}_3$, а так как $\mathfrak{p}_3 \in \operatorname{Spec}\mathcal{O}_K$, $\alpha \in \mathfrak{p}_3$, что мы и хотели.
2. Пусть $a \notin p\mathbb{Z}$. Заметим, что тогда $a \notin \mathfrak{p}_1\mathfrak{p}_2$, так как если a лежит хоть в одном из них, $a \vdots p$. Но тогда $\alpha^2 + a \notin \mathfrak{p}_1\mathfrak{p}_2$. Теперь заметим, что

   $$\mathrm{N}(\alpha^2 + a) = b^2 \vdots p \implies \alpha^2 + a \in p\mathcal{O}_K,$$

   а так как $\alpha^2 + a \notin \mathfrak{p}_1\mathfrak{p}_2$, $\alpha^2 + a \in \mathfrak{p}_3$. Пусть $(\alpha^2 + a) = \mathfrak{p}_3^s\mathfrak{q}$, тогда

   $$b^2 = \mathrm{N}(\alpha^2 + a) = \mathrm{N}(\mathfrak{p}_3)^s \underbrace{\mathrm{N}(\mathfrak{q})}_{\not\vdots p}$$

   Из условия все индексы втевления e_i равны единицы. Но тогда, так как $1 \cdot f_1 + 1 \cdot f_2 + 1 \cdot f_3 = 3$, все степени инерции равны единице, а тогда $\mathrm{N}(\mathfrak{p}_3) = p$. Тогда

   $$p^{2n} \cdot \underbrace{\ldots}_{\not\vdots p} = b^2 = p^s \cdot \underbrace{\ldots}_{\not\vdots p} \implies s = 2n.$$

   То есть $\upsilon_{\mathfrak{p}_3}(\alpha^2 + a) = 2n$. С другой стороны, $\upsilon_{\mathfrak{p}_3}(\alpha) = 0$, откуда $\upsilon_{\mathfrak{p}_3}(\alpha^2 + a) = 2n$. Но тогда, так как $\upsilon_p(b) = n$

   $$\alpha(\alpha^2 + a) = -b = p^n \cdot d, \quad (p, d) = 1, \quad (\alpha(\alpha^2 + a)) = \mathfrak{p}_1^n\mathfrak{p}_2^n\mathfrak{p}_3^n \cdot \underbrace{\ldots}_{\not\vdots \mathfrak{p}_3},$$

   то есть $\upsilon_p(\alpha(\alpha^2 + a)) = n$, что даёт нам противоречие.

□

Теорема 100. *Уравнение* $3x^3 + 4y^3 + 5z^3 = 0$ *не имеет целых решений.*

Доказательство. Предположим противное, пусть

$$3x_1^3 + 4y_1^3 + 5z_1^3 = 0 \implies 6x_1^3 + 8y_1^3 + 10z_1^3 = 0.$$

Сделаем замены переменных $x = 2y_1,\ y = x_1, z = -z_1$, получим уравнение

$$x^3 + 6y^3 = 10z^3. \tag{3.7}$$

Выберем среди таких решений решение с минимальным ненулевым $|z|$. Рассмотрим расширение $K = \mathbb{Q}(\theta)$, где $\theta^3 = 6$. Тогда уравнение 3.7 выражает тот факт, что

$$\mathrm{N}(x + \theta y) = 10z^3. \tag{3.8}$$

Положим $\alpha = x + \theta y$. Предположим, что в разложение идеала (α) на простые входит идеал $\mathfrak{p}_1$, не лежащий над двойкой и пятёркой (т.е. $\mathfrak{p}_1 \not| 2\mathcal{O}_K$, $\mathfrak{p}_1 \not| 5\mathcal{O}_K$) и предположим, что этот $\mathfrak{p}_1$ висит над некоторым простым числом p. То есть, пусть $(\alpha) = \mathfrak{p}_1^m \cdot \mathfrak{q}$. Рассмотрим два случая:

1. Пусть $\mathfrak{q} \not| p\mathcal{O}_K$. Тогда применим норму:

$$\mathrm{N}(\mathfrak{p}_1)^m \cdot \mathrm{N}(\mathfrak{q}) = \mathrm{N}(\alpha) = \mathrm{N}(x + \theta y) = 10z^3.$$

Так как степень инерции не больше степени расширения, $\mathrm{N}(\mathfrak{p}_1) = p^s$, где $s \in \{1, 2, 3\}$. Так как $\upsilon_p(10z^3) \vdots 3$ и $\mathfrak{q} \not| p\mathcal{O}_K$, мы имеем $sm \vdots 3$, значит либо $m \vdots 3$, либо $s = 3$.
Если $s = 3$, то $\mathrm{N}(\mathfrak{p}_1) = p^3$, а тогда $e_1(p) = 1$ и так как степень расширения равна трём, $\mathfrak{p}_1 = (p)$. В таком случае $\alpha \vdots p \implies x \vdots p,\ y \vdots p \implies z \vdots p$, а тогда мы можем сделать спуск.
Отсюда мы заключаем, что $m \vdots 3$.

2. Пусть $(\mathfrak{q}, (p)) \neq (1)$. Тогда $(\alpha) = \mathfrak{p}_1^m \mathfrak{p}_2 \mathfrak{q}'$ (где $\mathfrak{p}_2$ — еще один простой идеал, лежащий над p).

   - Если $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, то попробуем применить предложение[9] 66 для $\alpha\theta = (x + \theta y)\theta$. Проверим, что коэффициент при t^2 минимального многочлена $\alpha\theta$ равен нулю. В самом деле, так как это многочлен, этот коэффициент с точностью до знака равен следу, а след равен

$$\mathrm{Tr}(\alpha\theta) = \mathrm{Tr}(x\theta) + \mathrm{Tr}(y\theta^2) = 0 + 0 = 0.$$

     Тогда по предложению 66 мы имеем $\alpha\theta \in \mathfrak{p}_3$, то есть $\alpha \vdots p$, то есть $x\theta + y\theta^2 \vdots p$, откуда $x \vdots p,\ y \vdots p$ и мы снова можем сделать спуск.
   - Если $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$ или $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^2$. В любом из этих случаев мы получаем $\alpha^2 \vdots p$, но

$$\alpha^2 = x^2 + 2xy\theta + y^2\theta^2 \vdots p \implies x \vdots p,\ y \vdots p$$

     и мы можем сделать спуск.

Итого мы получили, что $(\alpha) = I^3 \cdot \mathfrak{m}$, где $\mathfrak{m}$ — произведение максимальных идеалов, висящих над 2 и 5. Поймём при помощи теоремы Куммера 91, какие идеалы висят над 2 и 5. Это мы уже делали при вычислении группы классов идеалов $\mathbb{Q}(\sqrt[3]{6})$ (см. пример 47).

$$x^3-6 \equiv x^2 \pmod 2 \rightsquigarrow 2\mathcal{O}_K = (2,\theta)^3 = (\theta-2)^3, \quad x^3-6 = (x-1)(x^2+x+1) \pmod 5 \rightsquigarrow 5\mathcal{O}_K = (5,\theta-1)(5,\theta^2+\theta+1$$

Заметим, что $(\theta - 1)$ и $(\theta^2 + \theta + 1)$ не могут входить в $\mathfrak{m}$ одновременно, так как тогда $\alpha \vdots 5$, откуда $x \vdots 5,\ y \vdots 5$ и мы можем спустится.

Так как $\mathrm{N}(\alpha) \vdots 2, \vdots 5$, в разложение α обязательно входит как идеал, всящий над двойкой, так и идеал, висящий над пятеркой.

Посмотрим сначала на идеалы, висящие над двойкой. Заметим, что с самого начала мы можем полагать z нечётным, так как иначе можно сделать спуск. Но тогда $\upsilon_2(10z^3) = \upsilon_p(\mathrm{N}(\alpha)) = 1$. Тогда, так как $\mathrm{N}(\theta-2) = 2$, идеал $(\theta - 2)$ не может входить в разложение (α) в больше чем первой степени.

Теперь посмотрим на идеалы, висящие над пятеркой. $\upsilon_5(\mathrm{N}(\alpha)) = \upsilon_5(10z^3) \equiv 1 \pmod 3$. Но тогда в (α) может входить либо $(\theta - 1)$ в первой степени, так как $\upsilon_5(\mathrm{N}(\theta - 1) = 1)$, либо $(\theta^2 + \theta + 1)^2$, так как $\upsilon_5((\theta^2 + \theta + 1)^2) = 4 \equiv 1 \pmod 5$ и других случаев не бывает.

Соотвественно, α имеет вид

$$\alpha = \alpha_0 \cdot t^3, \quad \alpha_0 \in \{(\theta - 2)(\theta - 1),\ (\theta - 2)(\theta^2 + \theta + 1)^2\} \cdot \{1, \varepsilon, \varepsilon^2, \}.$$

где $\varepsilon = 1 - 6\theta + 3\theta^2$ — основная единица в $\mathcal{O}_K$. Пусть $t = u + v\theta + w\theta^2$. Рассмотрим, например, случай, когда

$$\alpha = (\theta - 2)(\theta - 1)\big(u + v\theta + w\theta^2\big)^3 = (\theta^2 - 3\theta + 2)(u + v\theta + w\theta^2)^3 = x + y\theta.$$

Раскроем скобки и приравняем коэффициенты при соотвествующих степенях θ, а после, перейдём от равенства к сравнению по модулю 3. Так как $\theta^3 = 6$,

$$\big(u + v\theta + w\theta^2\big)^3 \equiv u^3 \pmod 3.$$

[9] С $\alpha = \alpha\theta$, как бы абсурдно это не звучало.

Значит, в левой части равенства коэффициент при θ^2 будет сравним с u^3 по модулю 3. С другой стороны, коэффициент при θ^2 в правой части равен нулю, откуда $u \vdots 3$. Но тогда

$$\left(u + v\theta + w\theta^2\right)^3 \equiv 0 \pmod 3 \implies x + y\theta \vdots 3 \implies x, y \vdots 3$$

и мы можем сделать спуск. Если

$$\alpha = (\theta - 2)(\theta^2 + \theta + 1)^2\left(u + v\theta + w\theta^2\right)^3 = (\theta^2 - 3\theta + 2)(u + v\theta + w\theta^2)^3 = x + y\theta,$$

то будет работать абсолютно такой же аргумент, так как

$$(\theta - 2)(\theta^2 + \theta + 1)^2 \equiv (\theta - 2)(2\theta + 1) \equiv 2\theta^2 - 2 \pmod 3.$$

Остаётся сказать, что если мы вместо единицы возьмём какой-то другой элемент $\mathcal{O}_K^*$, ничего не изменится, так как основная единица $\varepsilon \equiv 1 \pmod 3$.

Таким образом, во всех случаях мы смогли сделать спуск и теорема доказана.

□

1.21 Поле p-адических чисел и лемма Гензеля

Напомним вкратце определение поля $\mathbb{Q}_p$. Как мы помним из курса алгебры, *кольцо целых p-адических чисел* определяется как

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^\ell\mathbb{Z}$$

Соотвественно, его элементы имеют вид $\sum_{k=1}^{\infty} a_k p^k$, а операции определяются покоординатно по модулю p. Кроме того ясно, что элемент $\mathbb{Z}_p$ обратим тогда и только тогда, когда $a_0 \neq 0 \pmod p$, а любой элемент $x \in \mathbb{Z}_p$ единственным образом представялется в виде

$$x = p^k \cdot \varepsilon, \quad \varepsilon \in \mathbb{Z}_p^*, k \in \mathbb{N}. \tag{3.9}$$

Отсюда в частности следует, что кольцо $\mathbb{Z}_p$ локальное с единственным максимальным идеалом (p).

Кольцо $\mathbb{Z}_p$ целостное и его поле частных мы называем полем p-адических чисел $\mathbb{Q}_p$. Также ясно, что любой $x \in \mathbb{Q}_p$ представляется в виде

$$x = p^k \cdot \varepsilon, \quad \varepsilon \in \mathbb{Z}_p^*,\ k \in \mathbb{Z}. \tag{3.10}$$

Отметим также, что кольцо $\mathbb{Z}_p$ является кольцом дискретного нормаирования (со всеми вытекающими из этого хорошими свойствами), нормирование на нём определяется следующим образом:

$$x = p^n u, \quad u \in \mathbb{Z}_p^* \rightsquigarrow \upsilon_p(x) = n.$$

Полагая $\mathcal{U} = \mathbb{Z}_p^*$ мы имеем такую точную последовательность

$$1 \to \mathcal{U} \to \mathbb{Q}_p^* \xrightarrow{\upsilon} \mathbb{Z} \to 0.$$

Кроме того, на $\mathbb{Q}_p$ при помощи этого нормирования можно определить *неархимедову p-адическую норму*

$$|x|_p = \begin{cases} p^{-\upsilon_p(x)}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

Она удовлетворяет всем аксиомам нормы, но вместо неравенства треугольника имеет место более сильное *ультраметрическое неравенство*:

$$\upsilon_p(x + y) \geq \min(\upsilon_p(x), \upsilon_p(y)) \rightsquigarrow |x + y|_p \leq \max(|x|_p, |y|_p).$$

Соотвественно, нетрудно убедиться в том, что $\mathbb{Q}_p$ — пополнение $\mathbb{Q}$ по p-адической норме (и это даёт другую конструкцию этого поля). Одним из самых частых применений p-адических чисел является следующая известная многим со школьных лет лемма:

Лемма 65 (Лемма Гензеля)**.** Пусть для многочлен $F(x_1, \ldots, x_n)$ с целыми p-адическими коэффициентами и набора чисел $y_1, \ldots, y_n \in \mathbb{Z}_p$ при некотором $1 \leq i \leq n$ мы имеем

- $F(y_1, \ldots, y_n) = 0 \pmod{p^{2a+1}}$.
- $\frac{\partial F}{\partial x_i}(y_1, \ldots, y_n) \equiv 0 \pmod{p^a}$
- $\frac{\partial F}{\partial x_i}(y_1, \ldots, y_n) \not\equiv 0 \pmod{p^{a+1}}$,

где $a \in \mathbb{Z}_{\geq 0}$. Тогда существуют целые p-адические числа $z_1, \ldots, z_n$ такие, что

$$F(z_1, \ldots, z_n) = 0, \quad z_i \equiv y_i \pmod{p^{a+1}}.$$

Доказательство. Во-первых, от случая многочлена многих переменных можно моментально перейти к случаю многочлена одной переменной, полагая $y = y_i$ и рассматривая

$$f(x) = F(y_1, \ldots, y_{i-1}, x, y_{i+1}, \ldots, y_n).$$

Тогда для докзательства теоремы нам достаточно показать, что для многочлена $f(x) \in \mathbb{Z}_p[x]$, для которого

$$f(y) \equiv 0 \pmod{p^{2a+1}}, \quad f'(y) = up^a, u \in \mathbb{Z}_p^* \text{ (т.е. } \upsilon_p(f'(y)) = a),$$

найдётся $z \in \mathbb{Z}_p$ такой, что

$$f(z) = 0, \quad z \equiv y \pmod{p^{k+1}}.$$

Существование z мы докажем известным *методом касательных Ньютона.* Положим $t_0 = y$ и построим последовательность $\{t_n\}$, как

$$t_{n+1} = t_n - \frac{f(t_n)}{f'(t_n)}.$$

Сейчас про эту последовательность $\{t_n\}$ мы докажем, что

- $t_n \in \mathbb{Z}_p \quad \forall n \in \mathbb{N}$.
- $f(t_n) \equiv 0 \pmod{p^{2a+1+n}}$, $n \geq 0$.
- $t_n \equiv t_{n-1} \pmod{p^{a+n}}$, $n \geq 1$.

Докажем это мы индукцией по n. Предположим, что дле некоторого $n \geq 0$ это выполнено, сделаем переход. Так как из сравнимости по модулю большей степени следует сравнимость по модулю меньшей степени,

$$t_n \equiv t_{n-1} \pmod{p^{a+n}} \implies t_n \equiv t_{n-1} \pmod{p^{a+n-1}}$$

$$\begin{cases} t_n \equiv t_{n-1} \pmod{p^{a+n-1}} \\ t_{n-1} \equiv t_{n-2} \pmod{p^{a+n-1}} \end{cases} \implies t_n \equiv t_{n-1} \equiv t_{n-2} \pmod{p^{a+n-1}}.$$

Таким образом мы имеем сравнение

$$t_n \equiv t_0 = y \pmod{p^{a+1}} \implies f'(t_n) \equiv f'(y) \pmod{p^{a+1}},$$

а $\upsilon_p(f'(y)) = a$. Тогда $\upsilon_p(f'(t_n)) = a$ и отсюда моментально следует, что

$$t_{n+1} = t_n - \frac{f(t_n)}{f'(t_n)} \in \mathbb{Z}_p,$$

так как по индукционному предположннию $\upsilon_p(f(t_n)) = 2a + 1 + n$. Кроме того,

$$\frac{f(t_n)}{f'(t_n)} \vdots p^{2a+n+1-a} = p^{a+n+1} \implies t_{n+1} \equiv t_n \pmod{p^{a+n+1}}.$$

Теперь разложим $f(x)$ по степеням $(x - t_n)$:

$$f(x) = f(t_n) + f'(t_n)(x - t_n) + (x - t_n)^2 G(x), \quad G(x) \in \mathbb{Z}_p[x].$$

Подставим $x = t_{n+1}$:

$$f(t_{n+1}) = f(t_n) + f'(t_n)(t_{n+1} - t_n) + (t_{n+1} - t_n)^2 G(t_{n+1}) = \left(\frac{f(t_n)}{f'(t_n)}\right)^2 G(t_{n+1}).$$

$$\frac{f(t_n)}{f'(t_n)} \vdots p^{a+n+1} \implies f(t_{n+1}) \vdots p^{2a+n+2},$$

что и требовалось.

Теперь заметим, что так как $v_p(t_n - t_{n-1}) = a + n \to \infty$, последовательность t_n сходится, положим

$$z = \lim_{n\to\infty} t_n.$$

Но тогда, с одной стороны $v_p(f(t_n)) = 2a + n + 1$, откуда $f(t_n) \to 0$, а с другой стороны, по непрерывности,

$$\lim_{n\to\infty} f(t_n) = f(z) \implies f(z) = 0,$$

что и требовалось. □

Оченнь часто лемма Гензеля используется в вот таком виде

Следствие 36 (Лемма Гензеля, упрощенная форма)**.** *Пусть $f \in \mathbb{Z}_p[x]$ и $x_0 \in \mathbb{Z}_p$ таково, что*

- $f(x_0) \equiv 0 \pmod p$
- $f'(x_0) \not\equiv 0 \pmod p$.

Тогда $\exists x \in \mathbb{Z}_p\colon x \equiv x_0 \pmod p,\ f(x) = 0.$

В следующих нескольких параграфах мы займёмся изучением принципа Минковского-Хассе, или локально-глобального приницп.

Локально-глобальным принципом в теории чисел называют рассуждения примерно такого вида:

Уравнение разрешимо над $\mathbb{Z} \Leftrightarrow$ уравнение разрешимо по модулю всех простых p.

Для линейных уравнения это утверждение очевидно выполняется. Также оно выполнено для квадратичных форм: это уже весьма нетривиальное утверждение, доказанное Минковским и Хассе:

Рациональная квадратичная форма представляет ноль над $\mathbb{Q}$ тогда и только тогда, когда она представляет 0 над $\mathbb{R}$, а также представляет 0 над $\mathbb{Q}_p$ для всех простых p.

Это весьма сильное и полезное утверждение мы докажем в следующих параграфах.

Для кубических форм локально-глобальный принцип уже не верен. В ДЗ мы показывали, что уравнение $3x^3 + 4y^3 + 5z^3 = 0$ разрешимо над $\mathbb{F}_p$ для любого простого p. Сейчас, при помощи леммы Гензеля, мы докажем, что оно разрешимо над $\mathbb{Q}_p$ для любого простого p. Доказать, что оно не имеет решений над $\mathbb{Z}$ (и над $\mathbb{Q}$, соотественно) существенно сложнее, это мы проделаем несколько позже.

Теорема 101. *Уравнение $F(x, y, z) = 3x^3 + 4y^3 + 5z^3$ разрешимо над $\mathbb{Z}_p$ для любого простого p.*

Доказательство. Пусть сначала $p \neq 2, 3, 5$. Как мы уже убеждались,

$$\exists x_0, y_0, z_0\colon 3x_0^3 + 4y_0^3 + 5z_0^3 \equiv 0 \pmod p,$$

и x_0, y_0 и z_0 одновременно не делятся на p (иначе это тривиальный корень, такие нас не интересуют). Не умаляя общности, пусть $x_0 \not\vdots p$. Тогда применим лемму Гензеля с $a = 0$ (т.е. следствие 36) к многочлену

$$f(x) = 3x^3 + (4y_0^3 + 5z_0^3).$$

Мы действительно можем её применить, так как $f(x_0) \equiv 0 \pmod p$, как отмечено выше, а

$$f'(x_0) = 9x_0^2 \not\equiv 0 \pmod p.$$

Тогда существует $x_1 \in \mathbb{Z}_p$ такой, что $3x_1^3 + 4y_0^3 + 5z_0^3 = 0$, что мы и хотели.

Теперь разберёмся с $p = 2, 3, 5$.

- При $p = 2$ рассмотрим $(x_0, y_0, z_0) = (1, 0, 1)$, который, очевидно, даст корень и аналогично случаю выше применим лемму Гензеля с $a = 0$. Действительно,
$$\frac{\partial F}{\partial x}(1, 0, 1) = 9 \not\vdots 2.$$
- При $p = 3$ рассмотрим $(x_0, y_0, z_0) = (0, 2, -1)$ и применим леммму Гензеля с $a = 1$. В самом деле, $\upsilon_9(F(0, 2, -1)) = \upsilon_{27}(27) = 1$, а рассматривая
$$\frac{\partial F}{\partial y}(0, 2, -1) = 12 \cdot 2^3 \vdots 3, \not\vdots 9,$$
становится ясно, что лемма Гензеля применима.
- При $p = 5$ рассмотрим $(x_0, y_0, z_0) = (2, -1, 0)$ и применим лемму Гензеля $a = 0$. Действительно, $\upsilon_5(F(2, -1, 0)) = \upsilon_5(20) = 1$, а
$$\frac{\partial F}{\partial x}(2, -1, 0) = 9 \cdot 4 \not\vdots 5.$$

□

1.22 Группа квадратов поля $\mathbb{Q}_p$ и норменная группа

Перед тем, как изучать квадратичные формы, хорошо понимать строение группы квадратов поля $\mathbb{Q}_p$. Её изучением мы сейчас и займёмся. Пусть сначала $p \neq 2$. Так как любое p-адическое число представимо в виде $\alpha = p^m\varepsilon,\ \varepsilon \in \mathbb{Z}_p^*$, если α является квадратом числа $\gamma = p^k\varepsilon_0$, то $m = 2k,\ \varepsilon = \varepsilon_0^2$. Соотвественно, для описания группы квадратов поля $\mathbb{Q}_p$, достаточно понимать, какие элементы $\mathbb{Z}_p$ являются квадратами.

Предложение 67. *Пусть $p \neq 2$, тогда для того что бы целое p-адическое число*

$$\varepsilon = a_0 + a_1p + a_2p^2 + \ldots, \quad 0 \leq a_i < p,\ a_0 \neq 0,$$

было квадратом, необходимо и достаточно, чтоб a_0 было квадратичным вычетом по модулю p.

Доказательство. Ясно, что если $\varepsilon = \xi^2$ и $\xi \equiv b \pmod p$, то $a_0 \equiv b^2 \pmod p$, то есть является квадратичным вычетом по модулю p.

Теперь докажем в другую сторону. Пусть $a_0 \equiv b^2 \pmod p$. Рассмотрим многочлен

$$f(x) = x^2 - \varepsilon, \quad f(b) \equiv 0 \pmod p,\ f'(b) = 2b \not\equiv 0 \pmod p.$$

Значит, по лемме Гензеля 36, $\exists \xi \in \mathbb{Z}_p\colon f(\xi) = 0$, то есть $\varepsilon = \xi^2$. □

Это предложение позволяет нам определить символ Лежандра для элементов $\mathbb{Z}_p^*$. Действительно, пусть $\varepsilon = a_0 + a_1p + \ldots$, положим

$$\left(\frac{\varepsilon}{p}\right) = \left(\frac{a_0}{p}\right).$$

Корректность этого определения ясна как раз из предложения 67. Кроме того, если $\eta \in \mathbb{Z}_p^*,\ \eta = b_0 + b_1p + \ldots$, то

$$\left(\frac{\varepsilon\eta}{p}\right) = \left(\frac{a_0b_0}{p}\right) = \left(\frac{a_0}{p}\right)\left(\frac{b_0}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{\eta}{p}\right),$$

так как обычный (на $\mathbb{Z}$) символ Лежандра мультипликативен.

Изложенное выше поможет нам убедиться в том, что

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, \varepsilon, p, \varepsilon p\}, \quad \varepsilon \in \mathbb{Z}_p^*,\ \left(\frac{\varepsilon}{p}\right) = -1.$$

Во-первых, ясно, что если $\varepsilon \in \mathbb{Z}_p^*$ не является квадратом, то отношение любых из чисел $1, \varepsilon, p, \varepsilon p$ не является квадратом (т.е. это разные классы в фаторгруппе).

Во-вторых, возьмём $\xi \in \mathbb{Q}_p^*,\ \xi = p^m\theta = p^(a_0 + a_1p + \ldots),\ \theta \in \mathbb{Z}_p^*$.

- Если $m \vdots 2$ и a_0, квадратичный вычет, то $[\xi] = 1 \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.
- Если $m = 2k+1$ и a_0 квадратичный вычет, то $\theta = \eta^2$ и

$$\xi = p \cdot p^{2k}\theta = p \cdot (p^k\eta)^2 \implies [\xi] = p.$$

- Если $m = 2k$, но a_0 — квадратичный невычет, то

$$\xi = p^{2k} \cdot \theta = \varepsilon \cdot (\theta\varepsilon^{-1} \cdot p^{2k}) \implies [\xi] = \varepsilon.$$

- Если $m = 2k+1$ и a_0 — квадратичный невычет, то

$$\xi = p \cdot \varepsilon \cdot (\theta\varepsilon^{-1} \cdot p^{2k}) \implies [\xi] = p\varepsilon.$$

В последних двух пунктах мы воспользовались тем, что если ε — квадратичный невычет, то ε^{-1} — тоже, а тогда

$$\left(\frac{\theta\varepsilon^{-1}}{p}\right) = \left(\frac{\theta}{p}\right)\left(\frac{\varepsilon^{-1}}{p}\right) = (-1)^2 = 1.$$

Теперь обратимся к случаю $p = 2$. Сначала докажем такую лемму:

Лемма 66. Элемент $x \in \mathbb{Z}_2^*$ лежит в $\mathbb{Q}_2^{*2}$ тогда и только тогда, когда $x \equiv 1 \pmod 8$.

Доказательство. Необходимость следует из того, что квадрат нечетного числа всегда сравним с 1 по модулю 8.

Теперь докажем достаточность. Рассмотрим многочлен $f(t) = t^2 - x$. Тогда

$$f(1) = 1 - x \equiv 0 \pmod 8, \quad f'(t) = 2t \rightsquigarrow f'(1) = 2 \implies \upsilon_2(f'(1)) = 1.$$

Тогда по лемме Гензеля 65 с $a = 1$ мы имеем нужное. □

Отсюда следует, что $\{1, 3, 5, 7, 2, 6, 10, 14\}$ представляют $\mathbb{Q}_2^*$ по модулю $\mathbb{Q}_2^*$. Действительно, пусть сначала $x \in \mathbb{Z}_2,\ x \not\vdots 2$. Тогда

$$x = a_0 + 2a_1 + 4a_2 + 8y, a_0 \not\vdots 2.$$

Тогда $x \equiv a_0 + 2a_1 + 4a_2 \pmod 8$, а $a_0 + 2a_1 + 4a_2$ обратимо по модулю 8 (так как не делится на 2). Тогда

$$\frac{x}{a_0 + 2a_1 + 4a_2} \equiv 1 \pmod 8 \implies \frac{x}{a_0 + 2a_1 + 4a_2} = z^2,$$

откуда $[x] \in \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ будет иметь вид $[x] = a_0 + 2a_1 + 4a_2$. Так как $a_0 = 1$, а остальные коэффициенты равны единице или нулю, так мы получаем классы $1, 3, 5, 7$. В случае, когда $x \vdots 2$ мы можем применить абсолютно аналогичное рассуждение к $x/2$ и получить классы $2, 6, 10, 14$.

В то же время ясно, что все эти элементы будут различны. Таким образом, мы доказали такое предложение:

Предложение 68. *При $p = 2$ индекс подгруппы квадратов равен $[\mathbb{Q}_p^* : \mathbb{Q}_p^{*2}] = 8$. Кроме того,*

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, 3, 5, 7, 2, 6, 10, 14\}.$$

Определение 130. Пусть $a \in \mathbb{Q}_p^* \setminus \mathbb{Q}_p^{*2}$. Тогда группу

$$\mathrm{N} = \mathrm{N}_a = \{0 \neq x^2 - ay^2 | x, y \in \mathbb{Q}_p\}$$

называют *норменной группой* для квадратичного расширения $\mathbb{Q}_p(\sqrt{a})$.

Замечание. То, что N это в самом деле группа следует из мультипликативности нормы в квадратичном расширении $\mathbb{Q}_p(\sqrt{a})$.

Ясно, что $\mathbb{Q}_p^{*2} \subset \mathrm{N}$, так как можно положить $y = 0$.

Предложение 69. $|Q_p^*/\mathrm{N}| = 2$.

Доказательство. Пусть сначала $p \neq 2$. Сначала докажем, что $\mathrm{N} \neq \mathbb{Q}_p^{*2}$. Если $-a \notin \mathbb{Q}_p^{*2}$, то это очевидно. Предположим, что $-a \in \mathbb{Q}_p^{*2}$. Тогда

$$\mathrm{N} = \{x^2 + y^2 \mid x, y \in \mathbb{Q}_p\}.$$

Но, квадратичная форма $x^2 + y^2$ представляет все элементы $\mathbb{Z}_p^{*}$[10] что даёт нам, что $N \neq \mathbb{Q}_p^{*2}$.

Теперь докажем, что $\mathrm{N} \neq \mathbb{Q}_p^{*}$. Ясно, что нам важен лишь класс a по модулю группы квадратов. Покажем, что каким бы он ни был, найдётся число, которое нельзя будет представить формой $x^2 - ay^2$.

- Пусть $[a] = \varepsilon$. Тогда $x^2 - \varepsilon y^2 = p$ не имеет решений, так как можно перейти к сравнению по модулю p:
$$x^2 - \varepsilon y^2 \equiv 0 \pmod{p} \rightsquigarrow x^2 \equiv \varepsilon y^2 \pmod{p} \implies x, y \vdots p,$$
что даёт нам противоречие, так как тогда
$$\upsilon_p(x^2 - \varepsilon y^2) = 2, \quad \upsilon_p(p) = 1.$$
- Все оставшиеся случае для $a \in \{1, p, p\varepsilon\}$ сводятся к случаю выше.

$$\mathbb{Q}_p^{*2} \leq \mathrm{N} \leq \mathbb{Q}_p^{*} \implies [\mathbb{Q}_p^{*} : \mathbb{Q}_p^{*}] \vdots [\mathbb{Q}_p^{*} : \mathrm{N}],$$

а так как $\mathrm{N} \neq \mathbb{Q}_p^{*2}$ и $\mathrm{N} \neq Q_p^{*}$, мы имеем $[\mathbb{Q}_p^{*} : \mathrm{N}] = 2$.

Доказательство случая $p = 2$ является переборным и будет приведено дальше при доказательстве мультипликативности символа Гильберта в случае $p = 2$. □

1.23 Символ Гильберта

Определение 131. Пусть p — простое число, $a, b \in \mathbb{Q}_p^{*}$. Тогда *символом Гильберта* мы будем называть

$$(a, b)_p = \begin{cases} 1, \text{ если } x^2 - ay^2 - bz^2 \text{ представляет 0 над } \mathbb{Q}_p \\ -1, \text{ иначе.} \end{cases}$$

Замечание. Для квадратичной формы $a_1x_1^2 + \ldots + a_nx_n^2$ в этом параграфе мы будем использовать более удобное обозначение $\langle a_1, \ldots, a_n \rangle$.

Предложение 70. *Форма $\langle 1, -a, -b \rangle$ изотропна*[11] *тогда и только тогда, когда $b = \mathrm{N}_{\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p}(\alpha)$ для некоторого $\alpha \in \mathbb{Q}_p(\sqrt{a})$.*

Доказательство. Ясно, что если $b = \mathrm{N}_{\mathbb{Q}_p(\sqrt{(a)})/\mathbb{Q}_p}(\alpha)$, то

$$b = (x + y\sqrt{a})(x - y\sqrt{a}) = x^2 - ay^2$$

и тогда $(x, y, 1)$ даёт представление нуля.

Теперь докажем в обратную сторону. Пусть для $x_0, y_0, z_0 \in \mathbb{Q}_p$ $x_0^2 - ay_0^2 - bz_0^2 = 0$.

- Предположим, что $z_0 \neq 0$. Тогда
$$b = \left(\frac{x_0}{z_0}\right)^2 - a\left(\frac{y_0}{z_0}\right).$$
- Пусть $z_0 = 0$. Тогда

$$x_0^2 - ay_0^2 = 0 \implies a = \left(\frac{x_0}{y_0}\right)^2 = c^2 \implies b = x^2 - c^2y^2 = (x - cy)(x + cy), \text{ где } x = \frac{1 + b}{2},\ y = \frac{b - 1}{2c}.$$

□

[10] Это следует, например, из теоремы Коши-Девенпорта, или еще из чего-нибудь.

[11] Из определения ясно, что это равносильно тому, что $(a, b)_p = 1$.

	1	3	5	7	$2\cdot1$	$2\cdot3$	$2\cdot5$	$2\cdot7$
1	+	+	+	+	+	+	+	+
3	+	−	+	−	−	+	−	+
5	+	+	+	+	−	−	−	−
7	+	−	+	−	+	−	+	−
$2\cdot1$	+	−	−	+	+	−	−	+
$2\cdot3$	+	+	−	−	−	−	+	+
$2\cdot5$	+	−	−	+	−	+	+	−
$2\cdot7$	+	+	−	−	+	+	−	−

Таблица 3.1: Значения символа Гильберта на $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$.

Замечание. Заметим, что $(a, u^2 - av^2)_p = 1 \quad \forall u, v \in \mathbb{Q}_p$. Действительно:

$$x^2 - ay^2 - (u^2 - av^2)z^2 = 0 \Leftrightarrow x^2 - ay^2 = (u^2 - av^2)z^2$$

и тогда нам очевидно подходит набор $(u, v, 1)$.

В частности, $\forall a \in \mathbb{Q}_p^*\ (a, 1-a)_p = 1$.

Предложение 71. *Символ Гильберта мультипликативен, то есть* $(a_1a_2, b)_p = (a_1, b)_p \cdot (a_2, b)_p$.

Доказательство.

1. Если $(a_1, b)_p = 1$ и $(a_2, b)_p = 1$, то по предложению 70
$$a_1 = \mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_1), \quad a_2 = \mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_2),\ \alpha_1, \alpha_2 \in \mathbb{Q}_p(\sqrt{b}) \implies$$
$$\implies a_1a_2 = \mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_1)\,\mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_2) = \mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_1\alpha_2),$$
а тогда, опять же, по предложению 70 $(a_1a_2, b)_p = 1$.
2. Пусть $(a_1, b)_p = 1,\ (a_2, b)_p = -1$ (или наоборот). Тогда если $(a_1a_2, b)_p = 1$, то по первому пункту
$$1 = (a_1, b)_p \cdot (a_1a_2, b)_p = (a_1^2a_2, b)_p.$$
С другой стороны, совершенно ясно, что символ Гильберта не меняется при доножении на элемент $\mathbb{Q}_p^{*2}$, откуда $(a_1^2a_2, b)_p = (a_2, b)_p = -1$. Таким образом, мы пришли к противоречию.
3. Пусть $p \neq 2$ $(a_1, b)_p = -1$, $(a_2, b)_p = -1$. Ясно, что мы можем полагать $b \notin \mathbb{Q}_p^{*2}$ (иначе всё очевидно). Тогда в предложении 69 мы доказали, что
$$|\,\mathrm{N}_b\,/\mathbb{Q}_p^{*2}| = 2,\ |\mathbb{Q}_p^*/\,\mathrm{N}_b\,| = 2.$$
Тогда, так как $(a_1, b)_p = 1,\ (a_2, b)_p = -1$, по предложению 70 мы имеем $a_1, a_2 \in \mathbb{Q}_p^* \setminus \mathrm{N}_b$, а тогда $a_1a_2 \in \mathrm{N}_b$ и по предложению 70 $(a_1a_2, b)_p = 1$.
4. Теперь пусть $p = 2$ и $(a_1, b)_p = 1,\ (a_2, b)_p = -1$. Тогда по предложению 68 достаточно рассматривать $a_1, a_2, b \in \{1, 3, 5, 7, 2, 6, 10, 14\}$. На этих элементах символ гильберта можно просто вычислить:

□

Замечание. Если внимательно вглядеться в эту таблицу, становится заметно, что в каждой строке ровно 4 плюса и 4 минуса. Значит, $|\,\mathrm{N}\,/\mathbb{Q}_2^{*2}| = 4$, а так как по предложению 68 $|\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}| = 8$, мы получаем, что $|\mathbb{Q}_2^{*2}/\,\mathrm{N}\,| = 4$.

Замечание. Очевидно, что символ Гильберта симметричен, то есть $(a, b)_p = (b, a)_p$. Тогда из предложения 71 следует, что
$$(a, b_1b_2)_p = (a, b_1)_p \cdot (a, b_2)_p.$$

Предложение 72. *Пусть p — нечетное простое, $\varepsilon, \varepsilon_1, \varepsilon_2 \in \mathbb{Z}_p^*$. Тогда справедливы следующие свойства символа Гильберта:*

1. $(p, \varepsilon)_p = \left(\frac{\varepsilon}{p}\right)$.

2. $(\varepsilon_1, \varepsilon_2)_p = 1$.

Если же $p = 2$, они имеют следующий вид:

1. $(2, \varepsilon)_2 = (-1)^{\frac{\varepsilon^2-1}{8}}$.
2. $(\varepsilon_1, \varepsilon_2)_2 = (-1)^{\frac{\varepsilon_1-1}{2}\cdot\frac{\varepsilon_2-1}{2}}$.

Доказательство. Пусть $p \neq 2$, докажем второе свойство. Рассмотрим форму

$$f(x, y, z) = x^2 - \varepsilon_1 y^2 - \varepsilon_2 z^2.$$

Так как $\varepsilon_1 \not\vdots p, \varepsilon_2 \not\vdots p$, по теореме Шевалле сравнение

$$x^2 - \varepsilon_1 y^2 - \varepsilon_2 z^2 \equiv 0 \pmod{p}$$

имеет ненулевое (в $\mathbb{Z}/p\mathbb{Z}$) решение, пусть оно (x_0, y_0, z_0). Тогда

$$f(x_0, y_0, z_0) \equiv 0 \pmod{p}, \quad \frac{\partial f}{\partial x_1}(x_0, y_0, z_0) = 2x_0 \not\vdots p,$$

а значит, по лемме Гензеля 65, форма $x^2 - \varepsilon_1 y^2 - \varepsilon_2 z^2$ изотропна.

Докажем теперь первое свойство. Пусть $\left(\frac{\varepsilon}{p}\right) = 1$, то есть $\varepsilon = \theta^2$. Так как символ Гильберта не именяется при домножении на квадраты, в этом случае $(p, \varepsilon)_p = (p, 1)_p$. Рассмотрим форму

$$f(x, y, z) = x^2 - py^2 - z^2.$$

$$f(1, 1, 1) \equiv 0 \pmod{p}, \quad \frac{\partial f}{\partial x}(1, 1, 1) = 1 \not\vdots p,$$

а значит, по лемме Гензеля она анизотропна, то есть $(p, 1)_p = 1$.

Теперь, предположим, что $(p, \varepsilon)_p = 1$. Тогда существуют $x_0, y_0, z_0 \in \mathbb{Q}_p$ такие, что

$$x_0^2 - py_0^2 - z_0^2 = 0.$$

Ясно, что мы можем полагать, что $x_0, y_0, z_0 \in \mathbb{Z}_p$. Выберем корень с минимальным $\min(\upsilon_p(x_0), \upsilon_p(y_0), \upsilon_p(z_0))$. Если z_0 не делится на p, то $z_0 \in \mathbb{Z}_p^*$ и

$$\varepsilon \equiv \left(\frac{x_0}{z_0}\right)^2 \pmod{p} \implies \left(\frac{\varepsilon}{p}\right) = 1.$$

Если же $z_0 \vdots p$, то так как $x_0^2 - \varepsilon z_0^2 = py_0^2$, видно, что мы можем сделать спуск.

□

Теорема 102 (Закон взаимности для символа Гильберта)**.** *Пусть $a, b \in \mathbb{Q}^*$, тогда*

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} (a, b)_p = 1,$$

Замечание. Под $\mathbb{Q}_\infty$ обычно понимают $\mathbb{R}$ и символ Гильберта $(a, b)_\infty$ определяется аналогично. Отметим, что его вычисление существенно легче в силу того, что над $\mathbb{R}$ есть критерий Сильвестра.

Доказательство закона взаимности для символа Гильберта. В силу мультипликативности достаточно проверить это равенство для пяти случаев:

1. $a = -1, b = -1$.
2. $a = -1, b = 2$.
3. $a = -1, b = q$, где $q \in \mathbb{P} \setminus \{2\}$.
4. $a = 2, b = q$, где $q \in \mathbb{P} \setminus \{2\}$.

5. $a = p,\ b = q$, где $p, q \in \mathbb{P} \setminus \{2\}$ и $p \neq q$.

Проверим, например, формулу в случае 5. Если $r \in \mathbb{P} \setminus \{2, p, q\}$, то ясно, что $(p, q)_r = 1$ (так как в этом случае $p, q \in \mathbb{Z}_r^*$). Рассмотрим остальные случаи. По предложению 72:

$$(p, q)_p = \left(\frac{q}{p}\right), \quad (p, q)_q = \left(\frac{p}{q}\right), \quad (p, q)_2 = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Но так как по квадратичному закону взаимности

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

при перемножении получится 1.

Остальные пункты тоже проверяются непосредственно. □

Теперь докажем некоторую техническую теорему об изотропнсоти квадратичных форм с p-адическими коэффициентами, которая поможет нам в доказательстве теоремы Минковского-Хассе. Рассмотрим неособую квадратичную форму $f \simeq \langle b_1, \ldots, b_n\rangle,\ b_i \in \mathbb{Q}_p^*$. Линейной заменой перменных её всегда можно привести к виду

$$f = f_0 + pf_1 = a_1x_1^2 + \ldots + a_rx_r^2 + p(a_{r+1}x_{r+1}^2 + \ldots + a_nx_n^2), \quad a_i \in \mathbb{Z}_p^*.$$

Если мы говорим об изотропности формы, можно всегда полагать $r \geq n - r$, так как pf и f изотропны одновременно, а $pf \simeq f_1 + pf_0$.

Теорема 103. *Пусть $p \neq$ и $0 < r < n$. Тогда форма f изотропна над $\mathbb{Q}_p$ тогда и только тогда, когда хоть одна из форм f_0 или f_1 изотропна над $\mathbb{Q}_p$.*

Доказательство. Пусть форма f представляет нуль:

$$a_1\xi_1^2 + \ldots + a_r\xi_r^2 + p(a_{r+1}\xi_{r+1}^2 + \ldots + a_n\xi_n^2) = 0. \tag{3.11}$$

Мы можем полагать, что $\xi_i \in \mathbb{Z}_p$ и хотя бы одно из них не делится на p.

- Если не все $\xi_1, \ldots, \xi_r$ делятся на p, то переходя в равенстве (3.11) к сравнению по модулю p мы имеем

  $$f_0(\xi_1, \ldots, \xi_r) \equiv 0 \pmod p, \quad \frac{\partial f_0}{\partial x_1}(\xi_1, \ldots, \xi_r) = 2a_1\xi_1 \not\equiv 0 \pmod p.$$

  Тогда по лемме Гензеля 65 форма f_0 изотропна.
- Пусть $\xi_j \vdots p\ \forall j = 1, \ldots, r$. Тогда

  $$a_1\xi_1^2 + \ldots + \xi_r^2 \equiv 0 \pmod{p^2}.$$

  Тогда перейдём в равенстве (3.11) к сравнению по модулю p^2 и сократим его на p, получится

  $$f_1(\xi_{r+1}, \ldots, \xi_n) \equiv 0 \pmod p,$$

  причём хоть одно из $\xi_{r+1}, \ldots, \xi_n$ не делится на p. Применяя лемму Гензеля аналогично первому случаю, имеем нужное.

□

Следствие 37. *Если $a_1, \ldots, a_n \in \mathbb{Z}_p^*$, то при $p \neq 2$ форма $f = \langle a_1, \ldots, a_r\rangle$ всегда изотропна над $\mathbb{Q}_p$ при $r \geq 3$.*

Доказательство. По теореме Шевалле квадратичная форма от хотя бы трёх переменных всегда имеет нуль в $\mathbb{Z}/p\mathbb{Z}$, значит, сравнение

$$f(x_1, \ldots, x_n) \equiv 0 \pmod p$$

будет иметь нетривиальное решение. Но тогда остаётся лишь применить лемму Гензеля. □

Теперь перейдём к случаю $p = 2$. В этом случае, как и обычно, нужно давать некоторые корректировки.

Теорема 104. *В поле $\mathbb{Q}_2$ квадратичная форма $f = f_0 + 2f_1$ изотропна тогда и только тогда, когда разрешимо сравнение $f \equiv 0 \pmod{16}$ разрешимо с нечетным значением хоть одной переменной.*

Доказательство. Пусть $f(\xi_1, \ldots, \xi_n) \equiv 0 \pmod{16}$ и хотя бы одно ξ_i не делится на 2.

- Предположим, что некоторый ξ_i, где $1 \leq i \leq r$, не делится на 2. Не умаляя общности, пусть это ξ_1.
$$f(\xi_1, \ldots, \xi_n) \equiv 0 \pmod 8, \quad \frac{\partial f}{\partial x_1}(\xi_1, \ldots, \xi_n) = 2a_1\xi_1 \not\equiv 0 \pmod 4.$$
Тогда по лемме Гензеля 65 форма f изотропна.
- Пусть $\xi_1, \ldots, \xi_r \vdots 2$, то есть $\xi_i = 2\eta_i$. Но тогда
$$4(a_1\eta_1^2 + \ldots + a_r\eta_r^2) + 2(a_{r+1}\xi_r^2 + \ldots + a_n\xi_n^2) \equiv 0 \pmod{16}.$$
Сократим это сравнение на 2, получим:
$$2(a_1\eta_1^2 + \ldots + a_r\eta_r^2) + (a_{r+1}\xi_r^2 + \ldots + a_n\xi_n^2) \equiv 0 \pmod 8$$
и хотя бы одно ξ_i, где $r + 1 \leq i \leq n$ не делится на 2. Тогда мы можем в точности, как в первом случае, применить лемму Гензеля и получить, что $f_1 + 2f_0$ изотропна, но $f_1 + 2f_0 \simeq 2f$, а f и $2f$ изотропны одновременно.

□

Из доказательства сразу можно извлечь такое следствие:

Следствие 38. *Если для $f = f_0 + 2f_1$ сравнение $f \equiv 0 \pmod 8$ имеет решение с нечетным значением хоть одной из неизвестных $x_1, \ldots, x_r$, то эта форма изотропна над $\mathbb{Q}_2$.*

Теперь мы наконец можем доказать следующую теорему:

Теорема 105. *В поле p-адических чисел $\mathbb{Q}_p$ всякая неособая квадратичная форма от пяти и более переменных изотропна.*

Доказательство. Не умаляя общности, можем полагать, что наша форма имеет вид
$$f = f_0 + pf_1 = a_1x_1^2 + \ldots + a_rx_r^2 + p(a_{r+1}x_{r+1}^2 + \ldots + a_nx_n^2), \quad a_i \in \mathbb{Z}_p^*.$$
и $r \geq n - r$. Пусть $p \neq 2$. Тогда, так как $n \geq 5,\ n - r \geq 3$ и по следствию 37 форма f_0 изотропна, а значит, и f изотропна вместе с ней.

Теперь, пусть $p = 2$. Если $n - r > 0$, рассмотрим форму
$$g = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + 2a_nx_n^2.$$
Покажем, что такая форма всегда изотропна над $\mathbb{Q}_2$. Так как $a_1 + a_2 = 2\alpha,\ \alpha \in \mathbb{Z}_2$,
$$a_1 + a_2 + 2a_n\alpha^2 \equiv 2\alpha + 2\alpha^2 \equiv 2\alpha(\alpha + 1) \equiv 0 \pmod 4.$$
Значит, $a_1 + a_2 + 2a_n\alpha^2 = 4\beta$, $\beta \in \mathbb{Z}_2$. Тогда мы можем положить $x_1 = x_2 = 1$, $x_3 = 2\beta,\ x_n = \alpha$ и
$$a_1 + a_2 + a_3(2\beta)^2 + 2a_n\alpha^2 \equiv 4\beta + 4\beta^2 \equiv 0 \pmod 8.$$
Тогда по следствию 38 форма g изотропна над $\mathbb{Q}_2$, а значит, и f изотропна над $\mathbb{Q}_2$.

Если же $n = r$, то мы рассмотрим
$$g = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2$$
Если $a_1 + a_2 \equiv a_3 + a_4 \equiv 2 \pmod 4$, то можем положить $x_1 = x_2 = x_3 = x_4 = 1$, а если $a_1 + a_2 \equiv 0 \pmod 4$, то $x_1 = x_2 = 1,\ x_3 = x_4 = 0$. И в том, и в другом случае мы получим
$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 4\gamma, \quad \gamma \in \mathbb{Z}_2.$$
Тогда положим $x_5 = 2\gamma$ и получим
$$g \equiv 4\gamma + 4\gamma^2 \equiv 4\gamma(\gamma + 1) \equiv 0 \pmod 8$$
Тогда по следствию 38 мы получаем, что g изотропна, а значит и f изотропна.

□

1.24 Теорема Минковского-Хассе

Теорема 106 (Принцип Минковского-Хассе)**.** *Пусть f — рациональная квадратичная форма. Тогда f изотропна над $\mathbb{Q}_p$ для всех $p \in \mathbb{P} \cup \{\infty\}$ тогда и только тогда, когда она изотропна над $\mathbb{Q}$.*

Замечание. Ясно, что с самого начала f можно полагать невырожденной и диагональной, то есть $f \simeq \langle a_1, \dots, a_n \rangle$, $a_1 \cdot \ldots \cdot a_n \neq 0$.

Пусть $n = \dim f$, случай $n = 1$ тривиален.

Доказательство теоремы 106 в случае $n = 2$: Ясно, что с самого начала можно полагать $f = \langle 1, -a \rangle$, где $a \in \mathbb{Z}_{>0}$ (так как f изотропна над $\mathbb{R}$). Кроме того, можно считать a свободным от квадратов (так как все квадраты простых, входящих в a, можно занести внутрь переменной, делая линейную замену).

Пусть $a = p_1 \dots p_k$. Тогда, так как $\forall i \; \upsilon_{p_i}(a) = 1$, a не является квадратом ни над каким $\mathbb{Q}_{p_i}$, значит $a = 1$ и $f \simeq \langle 1, -1 \rangle$. □

Доказательство теоремы 106 в случае $n = 3$: По соображениям аналогичным размерности 2, с самого начала можно полагать $f \simeq \langle 1, -a, -b \rangle$, где $a, b \in \mathbb{Z}$, $ab \neq 0$ и a и b свободны от квадратов.

Будем вести индукцию по $|a| + |b|$.

База: Пусть $|a| + |b| = 1$. Тогда $a = \pm 1,\ b = \pm 1$, а так как f изотропна над $\mathbb{R}$, они не могут быть одновременно отрицательными. Но тогда f имеет гиперболическую плоскость $\langle 1, -1 \rangle$ в качестве подформы, а она представляет 0 над $\mathbb{Q}$.

Переход: Не умаляя общности, пусть $|a| \leq |b|$. Пусть

$$b = \pm p_1 p_2 \dots p_k, \quad p_i \neq p_j \text{ при } i \neq j.$$

Тогда, так как f изотропна над каждым $\mathbb{Q}_{p_i}$, a является квадратичным вычетом по модулю каждого p_i, откуда a является квадратом в $\mathbb{Z}/b\mathbb{Z}$. Тогда

$$\exists t, b' \in \mathbb{Z} \colon t^2 - a = bb'.$$

и при этом, ясно, что можно полагать $|t| < b/2$, а отсюда $|b'| \leq |b|/4 + 1$. Рассмотрим форму

$$f' \cong \langle 1, -a, -b' \rangle.$$

$$|a| + |b'| \leq |a| + \left| \frac{|b|}{4} + 1 \right| < |a| + |b|.$$

Чтоб применить индукционное предположение, осталось понять, почему f' изотропна над $\mathbb{Q}_p$ для всех простых p. Действительно, по свойству, отмеченному в этом замечении,

$$1 = (a, t^2 - a)_p = (a, b'b)_p = \underbrace{(a, b)_p}_{=1} \cdot (a, b')_p \implies (a, b')_p = 1.$$

Значит, $\langle 1, -a, -b' \rangle$ изотропна над $\mathbb{Q}_p$ для всех $p \in \mathbb{P} \cup \{\infty\}$. Тогда, по индукционному предположению она изотропна над $\mathbb{Q}$. По предложению 70 это равносильно тому, что

$$b' = \mathrm{N}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\alpha).$$

С другой стороны, так как $bb' = t^2 - a$, $bb' = \mathrm{N}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\beta)$. Но тогда

$$bb'^2 = \mathrm{N}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}(\alpha\beta) \implies b = \mathrm{N}_{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}\left(\frac{\alpha\beta}{b'}\right),$$

откуда по предложению 70 форма $\langle 1, -a, -b \rangle$ изотропна над $\mathbb{Q}$. □

Доказательство теоремы 106 в случае $n = 4$: Пусть $f \simeq \langle a_1, a_2, a_3, a_4\rangle,\ a_i \in \mathbb{Z}$. Так как f изотропна над $\mathbb{R}$, мы можем полагать $a_1 > 0, a_4 < 0$. Рассмотрим формы

$$g \simeq \langle a_1, a_2\rangle, \quad h \simeq \langle -a_3, -a_4\rangle.$$

Заметим, что для доказательства нам достаточно найти такое ненулевое рациональное c, которое представляют обе эти формы, то есть

$$a_1\xi_1^2 + a_2\xi_2^2 = c = -a_3\xi_3^2 - a_4\xi_4^2,$$

Рассмотрим множество S, определённое как

$$S \stackrel{\text{def}}{=} \{2,\ \text{все простые делители } a_i\}.$$

По условию теоремы для каждого простого p сущесвтуют $\xi_{ip} \in \mathbb{Q}_p$ (не все равные нулю) и $b_p \in \mathbb{Z}_p$ такие, что

$$a_1\xi_{1p}^2 + a_2\xi_{2p}^2 = -a_3\xi_{3p}^2 - a_4\xi_{4p}^2 = b_p \neq 0.$$

По китайской теореме об остатках мы можем выбрать такое $a \in \mathbb{Z}_{>0}$, что

$$\forall p_i \in S,\ p_i \neq 2 \quad a \equiv b_{p_i} \pmod{p_i^2},\ a \equiv b_2 \pmod{16}.$$

Так как мы можем полагать, что $0 \leq \upsilon_{p_i}(b_{p_i}) \leq 1$, мы имеем

$$\begin{cases} \upsilon_{p_i}(a) = \upsilon_{p_i}(b_{p_i}) \\ \upsilon_2(a) = \upsilon_2(b_2) \end{cases} \implies b_{p_i} - a = p_i^2 d \rightsquigarrow \frac{b_{p_i}}{a} = 1 + \frac{p_i^2}{a}d \in \mathbb{Z}_p.$$

То есть мы имеем

$$\frac{b_i}{a} \in \mathbb{Z}_{p_i} \text{ и } \frac{b_i}{a} \equiv 1 \pmod{p_i}.$$

Тогда, так как $\left(\frac{1}{p_i}\right) = 1$, по предложению 67 $a^{-1}b_{p_i}$ является квадратом в $\mathbb{Z}_{p_i}$. Аналогично и $a^{-1}b_2$ является квадратом в $\mathbb{Z}_2$.

Теперь заметим, что по определению b_{p_i} формы $\langle a_1, a_2, -b_{p_i}\rangle$ и $\langle -a_3, -a_4, -b_{p_i}\rangle$ изотропны над $\mathbb{Q}_{p_i}$, а так как $a^{-1}b_{p_i}$ — квадрат в $\mathbb{Z}_{p_i}$, формы $\langle a_1, a_2, -a\rangle$ и $\langle -a_3, -a_4, -a\rangle$ изотропны над $\mathbb{Q}_{p_i}$ для всех $p_i \in S$. В самом деле, пусть $a^{-1}b_{p_i} = \theta^2$, тогда $b_{p_i} = a \cdot \theta^2$ и

$$a_1\eta_1^2 + a_2\eta_2^2 - \cdot b_{p_i} = 0 \rightsquigarrow a_1\eta_1^2 + a_2\eta_2^2 - a \cdot \theta^2 = 0,$$

и аналогично для второй формы.

Если же $p \notin S$ и $p \nmid a$, то так как $a_i \not\vdots p$, формы $\langle a_1, a_2, -a\rangle$ и $\langle -a_3, -a_4, -a\rangle$ также будут изотропны над $\mathbb{Q}_p$.

Значит, нам остаётся рассмотреть лишь простые делители a, не лежаще в s. От a мы требовали, чтоб

$$\forall p_i \in S,\ p_i \neq 2 \quad a \equiv b_{p_i} \pmod{p_i^2},\ a \equiv b_2 \pmod{16}, \quad a \in \mathbb{Z}_{>0}.$$

Так как мы свободно можем изменять a на $16p_1^2 \dots p_k^2 \cdot n$, всевозможные подходящие a лежат в арифметической прогрессии $\{c_n\}$, где c_0 , а

$$c_n = c_0 + 16p_1^2 \dots p_k^2 \cdot n = d \cdot \left(\frac{c_0}{d} + \frac{16p_1^2 \dots p_k^2}{d}n\right), \quad d = (c_0, 16p_1^2 \dots p_k^2 \cdot).$$

Тогда по теореме Дирихле о простых в арифметической прогрессии существует n такой, что $c_n = dp_0$, где p_0 — простое. Возьмём в качестве искоимого a этот самый c_n. Так как любой простой делитель d будет лежать в S, всего один простой делитель a не будет лежать там — это p_0.

Заметим, что тогда форма $\langle a_1, a_2, -a\rangle$ изотропна над $\mathbb{Q}_p$ для всех p, кроме p_0. Но тогда, в силу закона взаимности Гильберта 102, они изотропна и над $\mathbb{Q}_{p_0}$. Аналогично и для формы $\langle -a_3, -a_4, -a\rangle$.

Тогда для каждой из них мы можем применить теорему Минковского-Хассе для $n = 3$ и получить, что $\langle a_1, \dots, a_4\rangle$ изотропна над $\mathbb{Q}$. □

Доказательство теоремы 106 в случае $n \geq 5$: Пусть $f \simeq \langle a_1, \ldots, a_n \rangle$. Рассмотрим формы

$$g \simeq \langle a_1, a_2 \rangle, \quad h \simeq \langle -a_3, -a_4, \ldots, -a_n \rangle.$$

Определим множество S аналогичным образом и также, как и в случае $n = 4$ найдём a такое, что формы

$$\langle a_1, a_2, -a \rangle \text{ и } \langle -a_3, \ldots, -a_n, -a \rangle$$

изотропны над всеми $\mathbb{Q}_p$, кроме, может быть, $\mathbb{Q}_{p_0}$. Тогда по закону взаимности Гильберта 102 форма $\langle a_1, a_2, -a \rangle$ будет изотропна над всеми $\mathbb{Q}_p,\ p \in \mathbb{P} \cup \{\infty\}$.

Пусть теперь $n \geq 5$. По следствию 37 (оно применимо, так как $a_3, a_4, a_5 \not\vdots p_0 \implies a_3, a_4, a_5 \in \mathbb{Z}^*_{p_0}$) форма h будет изотропна над $\mathbb{Q}^*_{p_0}$. Значит, она представляет любой элемент $\mathbb{Q}_{p_0}$[12], в частности a. Но, тогда форма $\langle -a_3, -a_4, -a_5, -a \rangle$ изотропна над $\mathbb{Q}_{p_0}$. Значит, по теореме Минковского-Хассе для $n = 4$ она изотропна над $\mathbb{Q}$. Но тогда формы g и h представляют рациональное число a, откуда f изотропна над $\mathbb{Q}$.

Теперь пусть $n > 5$. Тогда достаточно заметить, что нашу форму f можно будет представить в виде $f_0 + f_1$, где f_0 — неопределённая форма от пяти переменных. По доказанному выше она будет изотропна над $\mathbb{Q}$, а значит и f будет изотропна над $\mathbb{Q}$. □

Следствие 39. *Пусть f — рациональная квадратичная форма и f гиперболична над всеми $\mathbb{Q}_p$. Тогда f гиперболична.*

Доказательство. Так как f гиперболична над всеми $\mathbb{Q}_p$, она, в частности, изотропна над всеми $\mathbb{Q}_p$, откуда по теореме Минковского-Хассе она изотропна над $\mathbb{Q}$. Тогда мы можем представить её в виде

$$f = \mathbb{H} \oplus f' \implies f_{\mathbb{Q}_p} = \mathbb{H} \oplus f'_{\mathbb{Q}_p}.$$

С другой стороны, так как f гиперболична над всеми $\mathbb{Q}_p$, мы имеем

$$\underbrace{\mathbb{H} \oplus \ldots \mathbb{H}}_{m \text{ раз}} = f_{\mathbb{Q}_p} = \mathbb{H} \oplus f'_{\mathbb{Q}_p}.$$

Применяя теорему Витта о сокращении, мы получаем, что f' гиперболична, а значит, f гиперболична. □

Следствие 40. *Пусть f, g — рациональные квадратичные формы одинаковой размерности, $\dim f = \dim g = n$. Тогда они эквивалентны над полем рациональных чисел тогда и только тогда, когда они эквивалентны над полями $\mathbb{Q}_p$ для всех $p \in \mathbb{P} \cup \{\infty\}$.*

Доказательство. Так как $f \simeq g$ над $\mathbb{Q}_p$ для всех $p \in \mathbb{P} \cup \{\infty\}$, форма $f \oplus (-g)$ будет гиперболична над $\mathbb{Q}_p$ для всех $p \in \mathbb{P} \cup \{\infty\}$. Тогда по предыдущему следствию $f \oplus (-g)$ будет гиперболична над $\mathbb{Q}$. С другой стороны, форма $g \oplus (-g)$ тоже гиперболична и имеет такую же размерность. Тогда остаётся применить теорему Витта о сокращении:

$$f \oplus (-g) \simeq g \oplus (-g) \implies f \simeq g$$

над полем $\mathbb{Q}$. □

2. Локальные поля. Введение.

2.1 Кольца дискретного нормирования

Определение 132. Пусть F — поле, $\upsilon\colon F^* \to \mathbb{Z}$ — эпиморфизм групп, то есть

- $\upsilon(xy) = \upsilon(x) + \upsilon(y)$.
- $\operatorname{Im}\upsilon = \mathbb{Z}$ или, что то же самое, $\operatorname{Im}\upsilon \ni 1$.

и, кроме того, $\upsilon(x + y) \geq \min(\upsilon(x), \upsilon(y))$.

Тогда υ называют *дискретным нормированием* на поле F.

[12] Это общий факт, справедливый над любым полем: изотропная форма представляет любой элемент.

Замечание. Дискретное нормирование обычно доопределяют на 0, полагая, что $\upsilon(0) = +\infty$.

Пример 51. Мы уже видели, что для конечного расширения $\mathbb{Q}$ можно определять нормирование следующим образом: пусть $\mathfrak{p} \in \operatorname{Specm}(\mathcal{O}_K)$, тогда мы можем определить нормирование на K так:

$$a \in K \quad (a) = \mathfrak{p}^k \cdot \mathfrak{q}_1^{k_1} \cdot \ldots \cdot \mathfrak{q}_m^{k_m},\ \mathfrak{q}_i \neq \mathfrak{p} \rightsquigarrow \upsilon_{\mathfrak{p}}(a) \stackrel{\text{def}}{=} k.$$

Нетрудно проверить, что это в самом деле нормирование.

Действительно, $\exists x \in \mathfrak{p} \setminus \mathfrak{p}^2$, а значит, $\upsilon_{\mathfrak{p}}(x) = 1 \implies \operatorname{Im} \upsilon = \mathbb{Z}$. Кроме того, если $(x) = \mathfrak{p}^m \cdot I,\ (y) = \mathfrak{p}^n \cdot J$ (не умаляя общности, $x, y \in \mathcal{O}_K,\ m \leq n$), то $x \in \mathfrak{p}^m,\ y \in \mathfrak{p}^n \implies x + y \in \mathfrak{p}^m$, откуда $\upsilon_{\mathfrak{p}}(x + y) \geq m$.

Пример 52. Пусть F — поле. Введём нормирование на $F(t)$, которое будет тривиальным на F. Пусть p — неприводимый унитарный многочлен. Тогда $\forall h \in F(t)\ \exists f, g \in F[t]$:

$$h(t) = p^n(t) \cdot \frac{f(t)}{g(t)}, \quad (f, p) = (g, p) = (1).$$

Тогда мы можем положить $\upsilon_p(h) = n$.

Определение 133. Пусть на поле K задано дискретное нормирование υ. Определим по нему *кольцо дискретного нормирования*

$$\mathcal{O}_\upsilon \stackrel{\text{def}}{=} \{x \in K \mid \upsilon(x) \geq 0\}.$$

Сразу можно заметить, что

$$\mathcal{O}_\upsilon^* = \{x \in \mathcal{O}_\upsilon \mid \upsilon(x) = 0\}.$$

Действительно, если x обратим, то $\upsilon(x) + \upsilon(x^{-1}) = \upsilon(1) = 0$, откуда $\upsilon(x) = 0$. И, если же $\upsilon(x) = 0$, то $\upsilon(x^{-1}) = -\upsilon(x) = 0$, откуда $x^{-1} \in \mathcal{O}_\upsilon$.

Кольцо $\mathcal{O}_\upsilon$ является локальным с единственным максимальным идеалом

$$\mathfrak{m}_\upsilon = \{x \in \mathcal{O}_\upsilon \mid \upsilon(x) \geq 1\}.$$

Совершенно ясно, что это идеал. Более того, как мы видим, все элементы $\mathcal{O}_\upsilon$, не лежащие в $\mathfrak{m}_\upsilon$, будут обратимы, откуда ясно, что это единственный максимальный идеал.

Кроме того, этот идеал является главным. Действительно, возьмём элемент $\pi \in \mathcal{O}_\upsilon$, такой, что $\upsilon(\pi) = 1$, тогда $\mathfrak{m}_\upsilon = (\pi)$.

В самом деле, включение $(\pi) \subset \mathfrak{m}_\upsilon$ очевидно, докажем обратное. Возьмём $x \in \mathfrak{m}_\upsilon,\ \upsilon(x) = n > 0$. Тогда

$$\upsilon\Big(\frac{x}{\pi^n}\Big) = 0 \implies \frac{x}{\pi^n} \in \mathcal{O}_\upsilon^* \implies x \in \pi^n \mathcal{O}_\upsilon.$$

Предложение 73. *Кольцо дискретного нормирования $\mathcal{O}_\upsilon$ является локальным кольцом с единственным максимальным идеалом*

$$\mathfrak{m}_\upsilon = \{x \in \mathcal{O}_\upsilon \mid \upsilon(x) \geq 1\}.$$

Мультипликативная группа этого кольца имеет вид

$$\mathcal{O}_\upsilon^* = \{x \in \mathcal{O}_\upsilon \mid \upsilon(x) = 0\}.$$

Упражнение. Любой идеал кольца $\mathcal{O}_\upsilon$ является степенью идеала $\mathfrak{m}_\upsilon$.

Также легко видеть, что $\mathcal{O}_\upsilon$ целозамкнуто и $\dim \mathcal{O}_\upsilon = 1$, так как

$$\operatorname{Spec} \mathcal{O}_\upsilon = \{(0), \mathfrak{m}_\upsilon\}.$$

Кроме того, очевидно, что кольцо $\mathcal{O}_\upsilon$ нётерово (более того, оно является областью главных идеалов).

Есть и обратное утверждение:

Предложение 74. *Если кольцо A — нётерова локальная область целостности, в которой максимальный идеал главный, и A не является полем, то A — кольцо дискретного нормирования*[13].

Доказательство. Покажем сначала, что любой идеал в кольце A является степенью максимального идеала $\mathfrak{m} = (\pi)$. Действительно, рассмотрим идеал $I \subset \mathfrak{m} \subset A$. Выберем такую степень k, что $I \subset \mathfrak{m}^k$, но $I \not\subset \mathfrak{m}^{k+1}$. Такая степень обязательно найдётся, так как

$$\bigcap_{k\in\mathbb{N}} \mathfrak{m}^k = 0,$$

так как если x лежит в этом пересечении, то $x = \pi x_1 = \pi^2 x_2 = \pi^3 x_3$, откуда мы мы получим возрастающую цепочку $(x) \subset (x_1) \subset (x_2) \subset \ldots$, которая обязана стабилизироваться в силу нётеровости. Тогда $(x_n) = (x_{n+1})$, откуда $x_n = \pi x_{n+1} = \pi a x_n$, откуда $x_n(1 - \pi a) = 0$, что противоречит целостности кольца A. Докажем, что тогда $I = (\pi^k)$. Совершенно ясно, что $(\pi^k) \subset I$, а обратное включение также верно, так как $J = I/\pi^k$ содержит элементы, которые не делятся на π (а так как все такие элементы обратимы), $J = A$, откуда $I = (\pi^k)$.

Тогда, если K — поле частных кольца A, то ясно, как определить на нём нормирование:

$$x \in K^*,\ x = \frac{y}{z},\ y, z \in A \rightsquigarrow (x) = (\pi^k),\ (y) = (\pi^m) \rightsquigarrow \upsilon(x) = k - m.$$

И, совершенно очевидно, что $\mathcal{O}_\upsilon = \{x \in K \mid \upsilon(x) \geq 0\}$. □

Часто встречается ситуация, когда нормирований на поле несколько. Например, на поле $\mathbb{Q}$ есть бесконечно много p-адических нормирований υ_p, связанных с простыми числами. Интересно узнать, насколько эти нормирования независимы.

Лемма 67. Пусть υ_1, υ_2 — два нормирования на поле K, причем $\mathcal{O}_{\upsilon_1} \subset \mathcal{O}_{\upsilon_2}$. Тогда $\upsilon_1 = \upsilon_2$.

Доказательство. **1)** Докажем, что $\mathfrak{m}_{\upsilon_2} \subset \mathfrak{m}_{\upsilon_1}$. Возьмём $0 \neq x \in \mathfrak{m}_{\upsilon_2}$, предположим, что $x \notin \mathfrak{m}_{\upsilon_1}$. Тогда $\upsilon_1(x) \leq 0$, откуда $\upsilon_1(x^{-1}) \geq 0 \implies x^{-1} \in \mathcal{O}_{\upsilon_1} \subset \mathcal{O}_{\upsilon_2}$, но это противоречит тому, что $x \in \mathfrak{m}_{\upsilon_2}$.

2) Докажем, что $\mathfrak{m}_{\upsilon_1} = \mathfrak{m}_{\upsilon_2}$. Пусть $\mathfrak{m}_{\upsilon_1} = (\pi_1), x \in \mathfrak{m}_{\upsilon_1}$ тогда $x = \pi_1^n \cdot u$, где $u \in \mathcal{O}^*_{\upsilon_1}$.

Докажем, что $\pi_1 \in \mathfrak{m}_{\upsilon_2}$. Если $\pi_1 \notin \mathfrak{m}_{\upsilon_2}$, то $\pi_1 \in \mathcal{O}^*_{\upsilon_2}$, но тогда, так как $\mathcal{O}^*_{\upsilon_1} \subset \mathcal{O}^*_{\upsilon_2}$, мы имеем $u \in \mathcal{O}^*_{\upsilon_2}$, откуда $x \in \mathcal{O}^*_{\upsilon_2}$. То есть, $\mathfrak{m}_{\upsilon_1} \subset \mathcal{O}^*_{\upsilon_2}$, но при этом $\mathfrak{m}_{\upsilon_2} \subset \mathfrak{m}_{\upsilon_1}$, что даёт нам противоречие.

3) Докажем, что $\mathcal{O}^*_{\upsilon_2} \subset \mathcal{O}_{\upsilon_1}$. Пусть $x \in \mathcal{O}^*_{\upsilon_2}$, тогда, если $x \notin \mathcal{O}_{\upsilon_1}$, то $\upsilon_1(x) < 0$, откуда $\upsilon_1(x^{-1}) > 0 \implies x^{-1} \in \mathfrak{m}_{\upsilon_1} = \mathfrak{m}_{\upsilon_2}$, откуда $\upsilon_2(x^{-1}) > 0 \implies \upsilon_2(x) < 0$, что противоречит тому, что $x \in \mathcal{O}_{\upsilon_2}$. Тогда ясно, что $\mathcal{O}_{\upsilon_1} = \mathcal{O}_{\upsilon_2}$.

4) Докажем, что $\upsilon_1 = \upsilon_2$. Так как $\mathcal{O}_{\upsilon_1} = \mathcal{O}_{\upsilon_2}$, $\mathcal{O}^*_{\upsilon_1} = \mathcal{O}^*_{\upsilon_2}$ и $\mathfrak{m}_{\upsilon_1} = \mathfrak{m}_{\upsilon_2}$. Ясно, что $\upsilon_1(\pi_1) = \upsilon_2(\pi_1) = 1$, а так как любой элемент представим в виде $\pi_1^n \cdot u$, где u обратим, нормирования совпадают на любом элементе. □

Определение 134. Если $\upsilon(x) > 0$, то x называют *нулём порядка* $\upsilon(x)$ относительно υ.

Если $\upsilon(x) < 0$, то x называют *полюсом порядка* $\upsilon(x)$ *относительно* υ.

Лемма 68. Пусть υ_1, υ_2 — два различных нормирования. Тогда $\exists x \in K^*$, который является нулём относительно υ_1 и полюсом относительно υ_2.

Доказательство. По лемме 67 у нас нет включений между $\mathcal{O}_{\upsilon_1}$ и $\mathcal{O}_{\upsilon_2}$. Возьмём $y \in \mathcal{O}_{\upsilon_1} \setminus \mathcal{O}_{\upsilon_2}$ и $z \in \mathcal{O}_{\upsilon_2} \setminus \mathcal{O}_{\upsilon_1}$. Тогда нам подойдёт $x = \frac{y}{z}$. Действительно,

$$\upsilon_1(x) = \underbrace{\upsilon_1(y)}_{>0} - \underbrace{\upsilon_1(z)}_{<0} > 0, \quad \upsilon_2(x) = \underbrace{\upsilon_2(y)}_{<0} - \underbrace{\upsilon_2(z)}_{>0} > 0$$

□

[13] Вообще говоря, есть очень много характеризаций колец дискретного нормирования. Например, такое: нётеровы целозамкнутые локальные кольца размерности 1.

Лемма 69. Пусть $\upsilon_1, \ldots, \upsilon_n$ — попарно различные нормирования. Тогда существует x такой, что $\upsilon_1(x) < 0$, $\upsilon_2(x) > 0, \ldots, \upsilon_n(x) < 0$.

Доказательство. Докажем этот факт индукцией по n. В качестве базы нам подходит предыдущая лемма 68.

Теперь сделаем переход $n-1 \mapsto n$. По предположению индукции мы можем найти $\widetilde{x}\colon \upsilon_1(\widetilde{x}) < 0$, $\upsilon_2(\widetilde{x}) > 0, \ldots, \upsilon_{n-1}(\widetilde{x}) < 0$. По лемме 68 мы можем найти y такой, что $\upsilon_1(y) > 0$, а $\upsilon_n(y) < 0$. Рассмотрим элемент $\widetilde{x} + y^r$. Ясно, что $\upsilon_1(\widetilde{x} + y^r) > 0$. Кроме того, ясно, что число r можно взять достаточно большим, чтоб выполнялось неравенство

$$\forall i \quad 2 \le i \le n \quad \upsilon_i(\widetilde{x} + y^r) < 0,$$

тогда $\widetilde{x} + y^r$ нам подойдет. □

Теперь, по этой лемме выберем элемент $x \in K$ такой, что $\upsilon_1(x) > 0,\ \forall i > 1\ \upsilon_i(x) < 0$. Рассмотрим

$$y = \frac{1}{1+x^m}, \quad y - 1 = \frac{-x^m}{1+x^m}$$

$$\forall i > 1 \quad \upsilon_i(1+x^m) \le -m, \text{ так как } \upsilon_i(x) \le -1 \implies \upsilon_i(y) \ge m.$$

Кроме того, $\upsilon_1(y-1) = m\upsilon_1(x) - \upsilon_1(1+x^m) \ge m$.

Пусть $a_1, \ldots, a_n \in K$, рассмотрим $t = a_1 z_1 + \ldots + a_n z_n$, где z_i такие, что

$$\begin{cases} \upsilon_i(z_i - 1) \ge m \\ \upsilon_j(z_i) \ge m\ \forall j \ne i. \end{cases}$$

Ясно, что мы можем выбрать z_i абсолютно также, как мы выбирали y. Тогда

$$\upsilon_i(t - a_i) = \upsilon_i(a_1 z_1 + \ldots + a_i(z_i - 1) + \ldots + a_n z_n) \ge m + \min(\upsilon_i(a_1), \ldots, \upsilon_i(a_n)).$$

Таким образом, мы доказали такую теорему:

Теорема 107 (Аппроксимационная теорема)**.** *Пусть $a_1, \ldots, a_n \in K,\ N > 0$, а $\upsilon_1, \ldots, \upsilon_n$ — попарно различные нормирования. Тогда $\exists t \in K\colon \upsilon_i(t - a_i) > N$.*

Следствие 41. *Пусть $k_1, \ldots, k_n \in \mathbb{Z}$. Тогда существует $a \in K$ такой, что $\upsilon_i(a) = k_i$.*

Доказательство. Выберем $a_1, \ldots, a_n$, что $\upsilon_i(a_i) = k_i$, а N достаточно большим (больше всех k_i). Тогда по аппроксимационной теореме $\exists a \in K\colon \upsilon_i(a - a_i) > N$. Но тогда

$$\upsilon_i(a) = \upsilon_i(a_i + (a - a_i)) = \min(\upsilon_i(a_i), \upsilon_i(a - a_i)) = \upsilon_i(a_i) = k_i.$$

□

Аппроксимационную теорему можно интерпретировать и топологически. Во-первых, нормирование υ определяет на поле K неархимедову норму: возьмем $0 < c < 1$ и определим её, как

$$|x|_\upsilon = \begin{cases} 0, & x = 0 \\ c^{\upsilon(x)}. \end{cases} \quad .$$

По такой норме можно стандартным образом построить метрику $d_\upsilon(x, y) = |x - y|_\upsilon$ и тогда поле K станет метрическим (в частности, топологическим) пространством.

Следствие 42. *Рассмотрим все нормирования на поле K и произведение $\prod_\upsilon K$ с топологией произведения. Тогда аппроксимационная теорема говорит нам, что множество диагональных элементов $\{(a, \ldots, a) \mid a \in K\}$ плотно в топологии произведения.*

Пример 53. Пусть $\Bbbk$ — поле, $f \in \Bbbk[x,y]$ — неприводимый многочлен. Тогда $A = \Bbbk[x,y]/(f)$ — одномерное целостное кольцо. Пусть $f(x_0,y_0) = 0$, тогда $(f) \subset (x-x_0, y-y_0)$, причем $(x-x_0, y-y_0) = \mathfrak{m}$ — максимальный идеал. Тогда $A_{\mathfrak{m}}$ — одномерное целостное локальное нётерово кольцо. Пусть (x_0,y_0) — неособая точка ($f'_x(x_0,y_0) + f'_y(x_0,y_0) \neq 0$). По формуле Тейлора:

$$f(x,y) = f(x_0,y_0) + f'_x(x_0,y_0)(x-x_0) + f'_y(x_0,y_0)(y-y_0) + \ldots \equiv$$
$$\equiv f(x_0,y_0) + f'_x(x_0,y_0)(x-x_0) + f'_y(x_0,y_0)(y-y_0) \pmod{\mathfrak{m}^2}$$

Тогда в A $f(x_0,y_0) + f'_x(x_0,y_0)(x-x_0) + f'_y(x_0,y_0)(y-y_0) \in \mathfrak{m}^2$. Значит, в фаторе по $\mathfrak{m}^2$ мы получим, что одна образующая идеала $\mathfrak{m}$ выражается через другую, то есть, что

$$\dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1 \implies \mathfrak{m} - \text{главный}.$$

Воспользуемся леммой Накаямы. Пусть $\mathfrak{m}/\mathfrak{m}^2 = (z)$, тогда $(\mathfrak{m}/(z))^2 = \mathfrak{m}/(z)$, откуда по лемме Накаямы 39 $\mathfrak{m}/(z) = 0$, то есть $\mathfrak{m}$ порождается элементом (z). Значит, идеал $\mathfrak{m}$ в кольце $A_{\mathfrak{m}}$ является главным, откуда по теореме 74 кольцо $A_{\mathfrak{m}}$ — кольцо дискретного нормирования.

То есть, по неособой точке на кривой всегда можно построить кольцо дискретного нормирования.

Мы в основном будем заниматься теми нормированиями, относительно которых поле K является полным (как метрическое пространство).

Определение 135. Пусть K — поле, полное относительно υ. Тогда поле $\Bbbk = \mathcal{O}_\upsilon/\mathfrak{m}_\upsilon$ называют *полем вычетов* нормирования υ.

Пусть $S \subset \mathcal{O}_\upsilon$ и S состоит из представителей элементов поля вычетов и $0 \in S$.

Теорема 108. *Пусть $0 \neq x \in K$, $\pi \in \mathcal{O}_\upsilon$ — такой элемент, что $\mathfrak{m}_\upsilon = (\pi)$. Тогда x единственным образом раскладывается в ряд*

$$x = a_n\pi^n + a_{n+1}\pi^{n+1} + \ldots,$$

где число n определено однозначно ($n = \upsilon(x)$).

Доказательство. Заметим, что $\upsilon\left(\frac{x}{\pi^n}\right) = 0$, то есть $x/\pi^n \in \mathcal{O}_\upsilon \setminus \mathfrak{m}_\upsilon$. Тогда для него существует ненулевой ненулевой представитель a_n в поле вычетов. Иными словами,

$$\frac{x}{\pi^n} \equiv a_n \pmod{\mathfrak{m}_\upsilon}.$$

Тогда $m = \upsilon(x - a_n\pi^n) \geq n+1$. Проделывая ту же самую процедуру для $x - a_n\pi^n$ мы получаем

$$\upsilon(x - a_n\pi^n + a_m\pi^m) \geq m+1$$

и так далее. Так мы получаем разложение

$$x = a_n\pi^n + a_{n+1}\pi^{n+1} + \ldots, \quad n = \upsilon(x),\ a_i \in S.$$

Теперь докажем единственность. Пусть

$$x = a_n\pi^n + a_{n+1}\pi^{n+1} + \ldots = b_n\pi^n + b_{n+1}\pi^{n+1} + \ldots,$$

тогда $(a_n - b_n)\pi^n \in (\pi^{n+1}) \implies a_n - b_n \in \mathfrak{m}_\upsilon$, то есть $\overline{a_n} = \overline{b_n}$ в $\Bbbk = \mathcal{O}_\upsilon/\mathfrak{m}_\upsilon$, но тогда, так как мы брали для каждого элемента поля вычетов единственный представитель, отсюда $a_n = b_n$. Аналогично мы получаем равенство всех коэффициентов. □

Домашнее задание 15. Задачи:

1. Опишите все нормирования поля $F(t)$, тривиальные на F.
2. Рассмотрим фильтрацию $U = \mathcal{O}_\upsilon \supset U_1 \supset U_2 \supset \ldots \supset U_n \supset \ldots$, где

$$U_n = \{x \in \mathcal{O}_\upsilon \mid \upsilon(x-1) \geq n\}.$$

(a) Покажите, что U_n — группа.
(b) Докажите, что $U/U_1 \cong \Bbbk$.
(c) Докажите, что $U_n/U_{n+1} \cong \Bbbk$.

3. Пусть $c \in \mathbb{Z}$, p — простое и $c \not\vdots p$. Докажите, что последовательность c^{p^n} сходится в поле $\mathbb{Q}_p$.
4. Пусть $K = \mathbb{Q}_p$. Докажите, что $U_i \cong U$ при $i \geq 1$.
5. Докажите, что $\forall n\ |\mathbb{Q}_p/\mathbb{Q}_p^{*n}| < \infty$.
6. Пусть K — полное поле и $\operatorname{char} \Bbbk \not\vdots m$. Тогда отображение $x \mapsto x^m$ — изоморфизм $U_n \to U_n$.

2.2 Продолжение нормирований и ветвление

Пусть тпеперь L/K — конечное расширение, υ — дискретное номрирование на K, а w —- дискретное нормирование на L.

Пример 54. Пусть $L/\mathbb{Q}$ — конечное расширение. Пусть p — простое число, тогда на $\mathbb{Q}$ у нас есть p-адическое нормирование υ_p. С другой стороны,

$$p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdot \ldots \mathfrak{p}_k^{e_k}$$

и каждому простому соотвествует нормирование $w_{\mathfrak{p}_i}$. Легко видеть, что $w_{\mathfrak{p}_i}(x) = e_i \upsilon_p(x)$.

Предложение 75. *Следующие условия равносильны:*

1. *Существует* $e \in \mathbb{N}$: $\forall x \in K\ w(x) = e\upsilon(x)$.
2. $\mathcal{O}_\upsilon \subset \mathcal{O}_w$.
3. $\mathfrak{m}_\upsilon \subset \mathfrak{m}_w$.
4. $\mathfrak{m}_\upsilon = \mathfrak{m}_w \cap \mathcal{O}_\upsilon$.

Доказательство. Во-первых, ясно, что их первого условия следуют все остальные. Покажем, что **2)** $\implies$ **1)**. Нормирование w на поле L мы можем ограничить на поле K, т.е. рассмотреть $w|_K$. Вообще говоря, такое ограничение может и не быть нормированием, так как, ясно, что $\operatorname{Im} w|_K$ может не совпадать с $\mathbb{Z}$. В то же время, это некоторая подгруппа в $\mathbb{Z}$, предположим, что $\operatorname{Im} w|_K = e\mathbb{Z}$. Во-первых, $e \neq 0$. Действительно, так как L алгебраично над K, любой $x \in L$ мы можем записать, как

$$x^n + a_{n-1}x^{n-1} + a_0 = 0 \implies x^n = -(a_{n-1}x^{n-1} + a_0), \quad a_j \in K.$$

и взяв нормирование слева и справа мы получим противоречие. Действительно, если $w(x) \neq 0$, то

$$w(x^n) = nw(x), \quad w(-a_j x^j) = w(a_j) + jw(x) = w(x),$$

откуда мы получаем, что

$$nw(x) = \min(0, (n-1)w(x)) \implies w(x) = 0$$

и по произвольности $x \in L$ мы получаем, что $w = 0$, что даёт нам противоречие.

Тогда $e > 0$ и мы можем рассмотреть функцию $\upsilon' = \frac{w|_K}{e}$, которая уже будет нормированием на K. Тогда мы получаем, что $\mathcal{O}_\upsilon \subset \mathcal{O}_{\upsilon'}$, а отсюда, по лемме 67, $\upsilon = \upsilon'$.

Равносильность остальных условий доказывается аналогично. □

Определение 136. Если хотя бы одно из этих условий выполнено, то говорят, что $w \mid \upsilon$ (или, что нормирование w *находится над* нормированием υ, или же, w *продолжает* υ).

Пусть L/K — конечное сепарабельное расширение, υ — нормирование на K, $\mathcal{O}_\upsilon$ — кольцо нормирования. Напомним знакомое нам из коммутативной алгебры определение:

Определение 137. Кольцо A называется *дедекиндовым*, если оно

- нётерово
- целостное
- целозамкнутое

- размерности 1.

В коммутативной алгебре у нас была такая теорема:

Теорема 109. *Пусть A — Дедекиндово кольцо, K — его поле частных, L/K — конечное расщирение (полей), а $B = \mathrm{Int}_L A$. Тогда B — дедекиндово.*

В нашей ситуации $A = \mathcal{O}_\upsilon$, а $B = \mathrm{Int}_L(A)$. Пусть $\mathfrak{m}_\upsilon = \mathfrak{p}$ и рассмотрим $\mathfrak{p}B$, он раскладывается в произведение простых:

$$\mathfrak{p}B = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$$

Каждая локализация $B_{\mathfrak{p}_i}$ является дискретно-нормированным кольцом (и, более того, кольцом нормирования w_i). Кроме того, все нормирования w_i, связанные с идеалами $\mathfrak{p}_i$, продолжают нормирование υ (т.е. $w_i \mid \upsilon$) и, это в точности все нормирования, продолжающие нормирование υ.

В самом деле, если w продолжает υ, то $(w|\upsilon \implies \mathfrak{m}_\upsilon \subset \mathfrak{m}_w \implies \mathfrak{m}_\upsilon B \vdots \mathfrak{m}_w)$ $\mathfrak{m}_w \cap B$ — простой идеал, висящий над идеалом $\mathfrak{p}$, то есть, один из $\mathfrak{p}_i$. Пусть $\mathfrak{m}_w \cap B = \mathfrak{p}_i$, тогда $\mathfrak{m}_w \cap B_{\mathfrak{p}_i} = \mathfrak{p}_i B_{\mathfrak{p}_i}$. Тогда $\mathfrak{m}_w \cap \mathcal{O}_{w_i} = \mathfrak{m}_w \cap B_{\mathfrak{p}_i} = \mathfrak{m}_{w_i}$, откуда $w = w_i$.

Как мы уже отмечали, $B_{\mathfrak{p}_i}/\mathfrak{p}_i B_{\mathfrak{p}_i} = \mathcal{O}_{w_i}/\mathfrak{m}_{w_i}$. Положим

$$f_i = [\mathcal{O}_{w_i}/\mathfrak{m}_{w_i} : A/\mathfrak{p}] = [\mathbb{k}_{w_i} : \mathbb{k}_\upsilon]$$

и будем (как и в первой части курса) называть f_i **степенью инерции**.

Отметим так же, что, как и в случае колец целых, B — свободный $\mathcal{O}_\upsilon$-модуль ранга n (как и кольцо целых $\mathcal{O}_K$, которое было свободным $\mathbb{Z}$-модулем ранга n).

Теорема 110. *Для индексов ветвления и степеней инерции справедлива следующая формула:*

$$\sum_{i=1}^{k} e_i f_i = n.$$

Доказательство. Пусть $\mathfrak{p} = \mathfrak{m}_\upsilon$. Так как B — свободный $\mathcal{O}_\upsilon$-модуль ранга n, ясно, что что $B/\mathfrak{p}B$ — векторное пространство над $A/\mathfrak{p}$ размерности n.

$$B/\mathfrak{p}B \cong B/\prod \mathfrak{p}_i^{e_i} = B/\mathfrak{p}_i^{e_1} \times B/\mathfrak{p}_i^{e_2} \times \ldots \times B/\mathfrak{p}_k^{e_k}.$$

Вычисляя размерности обеих частей равенства и приравнивая, мы получаем

$$n = \sum_{i=1}^{k} \dim_{A/\mathfrak{m}} B/\mathfrak{p}_i^{e_i}.$$

Рассмотрим на кольце B фильтрацию степенями идеалов $\mathfrak{p}_i$:

$$\mathfrak{p}_i^{e_i} \subset \mathfrak{p}_i^{e_i-1} \subset \ldots \subset \mathfrak{p}_i \subset B.$$

Посмотрим на факторы этой фильтрации, то есть, на $\mathfrak{p}_i^m/\mathfrak{p}_i^{m+1}$, они являются векторными пространствами над $A/\mathfrak{p}$. Покажем, что $\forall m \geq 1$ $B/\mathfrak{p}_i \cong \mathfrak{p}_i^m/\mathfrak{p}_i^{m+1}$. Выберем $x \in \mathfrak{p}_i^m \setminus \mathfrak{p}_i^{m+1}$ и отображение $m_x \colon B/\mathfrak{p}_i \to \mathfrak{p}_i^m/\mathfrak{p}_i^{m+1}$, $y \mapsto xy$. Вполне ясно, что это корректно определённый гомоморфизм, вычислим его ядро. Рассмотрим $y \in B$ такой, что $xy \in \mathfrak{p}_i^{m+1}$ и покажем, что тогда $y \in \mathfrak{p}_i$. Рассмотрим главный идеал (xy). Так как $xy \in \mathfrak{p}_i^{m+1}$, его разложение на простые имеет вид

$$(xy) = \mathfrak{p}_i^{m+1} \cdot I.$$

С другой стороны, $(x) = \mathfrak{p}_i^m \cdot J$, $J \not\vdots\ \mathfrak{p}_i$ и тогда $(y) = \mathfrak{p}_i \cdot \widetilde{J}$, откуда $y \in \mathfrak{p}_i$. Значит, мы показали, что $\ker m_x = \{0\}$. Сюръективность отображения m_x следует из того, что $(x) + \mathfrak{p}_i^{m+1} = \mathfrak{p}_i^m$. Так как $x \in \mathfrak{p}_i^m$,

очевидно, что левая часть лежит в правой. Тогда $(x) + \mathfrak{p}_i^{m+1} = \mathfrak{p}_i^m \cdot I$, покажем, что $I = (1)$. Предположим противное, тогда

$$I = \mathfrak{p}_i^s \cdot \mathfrak{q}_1^{r_1} \cdot \ldots \mathfrak{q}_\ell^{r_\ell}, \quad \mathfrak{q}_j \neq \mathfrak{p}_i.$$

Тогда $I = \mathfrak{p}_i^s$, откуда $(x) + \mathfrak{p}_i^{m+1} = \mathfrak{p}_i^{m+s}$. Предположим, что s положительно. Тогда $(x) \subset \mathfrak{p}_i^{m+1}$, что противоречит тому, что мы брали $x \in \mathfrak{p}_i^m \setminus \mathfrak{p}_i^{m+1}$. Тогда мы показали, что

$$B/\mathfrak{p}_i \cong \mathfrak{p}_i^m/\mathfrak{p}_i^{m+1},$$

и отсюда уже следует теорема:

$$B/\mathfrak{p}_i^{e_i} \cong \frac{B}{\mathfrak{p}_i} \cdot \frac{\mathfrak{p}_i}{\mathfrak{p}_i^2} \cdot \ldots \frac{\mathfrak{p}_i^{e_i-1}}{\mathfrak{p}_i^{e_i}} \implies$$
$$\implies \dim_{A/\mathfrak{p}} B/\mathfrak{p}_i^{e_i} = \dim_{A/\mathfrak{p}} B/\mathfrak{p}_i + \dim_{A/\mathfrak{p}} \mathfrak{p}_i/\mathfrak{p}_i^2 + \ldots + \dim_{A/\mathfrak{p}} \mathfrak{p}_i^{e_i-1}/\mathfrak{p}_i^{e_i} = e_i \cdot \dim_{A/\mathfrak{p}} B/\mathfrak{p}_i = e_i \cdot f_i.$$

□

Теперь посмотрим, что будет происходить в **несепарабельном** случае.

В этом случае наше расширение раскладывается в башню

$$\begin{array}{c} L \\ | \\ \widetilde{K} \\ | \\ K \end{array}$$

где расширение $L/\widetilde{K}$ чисто несепарабельно. Если $\operatorname{char} K = 0$, то $\widetilde{K} = L$. Если же $\operatorname{char} K = p$,то чисто несепарабельное расширение, в свою очередь, раскладывается в башню *элементарных* чисто несепарабельных расширений:

$$\widetilde{K} \subset K_1 \subset K_2 \subset \ldots \subset K_m \subset L.$$

Каждое из них устроено следующим образом: $K_{i+1} = K_i(\sqrt[p]{a})$, где $a \in K_i$ и a не является p-й степенью, а $p = \operatorname{char} K$.

Докажем, что каждое нормирование на K_i мы можем продолжить на K_{i+1}.

Лемма 70. Пусть $F \subset F_1 \subset F_2$, причем на этих полях есть нормирования υ, υ_1 и υ_2 соответственно. Тогда

$$\begin{cases} \upsilon_1 \text{ продолжает } \upsilon \\ \upsilon_2 \text{ продолжает } \upsilon_1 \end{cases} \implies \upsilon_2 \text{ продолжает } \upsilon.$$

Доказательство. В самом деле, нам известно, что

$$\forall x \in F \; \upsilon_1(x) = e_1\upsilon(x), \quad \forall y \in F_1 \; \upsilon_2(y) = e_2\upsilon_1(y).$$

Тогда мы получаем, что $\forall x \in F \; \upsilon_2(x) = e_2\upsilon_1(x) = e_2e_1\upsilon(x)$, что даёт нам, что υ_2 продолжает υ. □

Лемма 71. Пусть L/F — элементарное чисто несепарабельное расширение, то есть $L = F(\sqrt[p]{a})$, а υ — нормирование на F. Тогда у нормирования υ существует единственное продолжение на L.

Доказательство. Сначала отметим, что возводя элемент поля L в степень p, мы неизбежно получим элемент поля F, так как любой элемент L мы можем записать как

$$x = f_0 + f_1\sqrt[p]{a} + \ldots + f_{p-1}\sqrt[p]{a^{p-1}}.$$

Рассмотрим функцию $\varphi\colon L \to \mathbb{Z}$, $\varphi(x) = \upsilon(x^p)$. Ясно, что φ является гомоморфизмом $L^* \to \mathbb{Z}$. Кроме того,

$$\varphi(x+y) = \upsilon((x+y)^p) = \upsilon(x^p + y^p) \geq \min(\upsilon(x^p), \upsilon(y^p)) = \min(\varphi(x), \varphi(y)).$$

Опять же, тогда $\operatorname{Im}\varphi = f\mathbb{Z}$, где $f \in \mathbb{N}$. Нетрудно заметить, что так как для $x \in F$ $\varphi(x) = p\upsilon(x)$, откуда $p \in \operatorname{Im}\varphi$, то есть, $f = 1$ или $f = p$. Мы можем рассмотреть нормирование

$$w = \frac{\varphi}{f}, \quad x \in F \rightsquigarrow w(x) = \frac{\upsilon(x^p)}{f} = \frac{p}{f}\upsilon(x) \rightsquigarrow w \mid \upsilon.$$

Теперь докажем единственность. Пусть w' продолжает нормирование υ с индексом ветвления e. Возьмём $x \in L$, тогда

$$w'(x^p) = e\upsilon(x^p) = efw(x),$$

а с другой стороны, $w'(x) = pw'(x)$, откуда $w'(x) = \frac{ef}{p}w(x)$. Подставляя в это равенство локальный параметр для нормирования w, мы получаем, что $\frac{ef}{p} = 1$, откуда $w = w'$. □

Лемма 72. Пусть L/F — чисто несепарабельное расширение, а υ — нормирование на F. Тогда у нормирования υ существует единственное продолжение на L.

Доказательство. Разложим наше чисто несепарабельное расширение в башню элементарных чисто несепарабельных:

$$F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_n = L.$$

Тогда, по предыдущей лемме у нас есть последовательнbость нормирований $\upsilon, w_1, \ldots, w_n$, каждое из которых продолжает другое. Соответственно, так мы получаем существование. Теперь проверим единственность.

Пусть w — нормирование на L, продолжающее υ. Докажем, что оно продолжает w_{n-1} (и, отсюда будет следовать, что оно совпадает с w_n). Пусть $w(x) = e\upsilon(x)$ $\forall x \in F$. Заметим теперь, что

$$F_n^p \subset F_{n-1},\ F_{n-1}^p \subset F_{n-2},\ \ldots, F_1^p \subset F_0 \implies F_{n-1}^{p^{n-1}} \subset F.$$

Тогда мы имеем

$$\forall x \in F_{n-1}\ w\left(x^{p^{n-1}}\right) = e\upsilon\left(x^{p^{n-1}}\right) = \frac{ew_{n-1}\left(x^{p^{n-1}}\right)}{e'} = \frac{ep^{n-1}}{e'}w_{n-1}(x).$$

С другой же стороны, $p^{n-1}w(x) = \frac{e}{e'}p^{n-1}w_{n-1}(x)$ $\forall x \in F_{n-1}$. Подставляя в это равенство локальный параметр для нормирования w_{n-1} мы получаем, что $e/e' \in \mathbb{Z}$, откуда $w \mid w_{n-1}$, а значит, $w = w_n$. □

Пусть теперь K — полное поле относительно нормирования υ, а L/K — конечное расширение. Докажем вот такую теорему:

Теорема 111. *В случае полного относительно нормирования υ поля K существует единственное продолжение υ на L. Поле L является полным относительно этого нормирования.*

Доказательство. Рассмотрим L, как векторное пространство над K, пусть $V \subset L$ — ненулевое подпространство. Мы знаем, что какое-то продолжение нормирования υ на L существует, обозначим его за w. Рассмотрим последовательность $\{x_i\},\ x_i \in V$ и обозначим за $\{v_j\}$ базис V. Разложим x_i по базису:

$$x_i = \sum_j a_{ij}v_j, \quad a_{ij} \in K.$$

Лемма 73. Если $x_i \xrightarrow{|\cdot|_w} 0$, то $a_{ij} \xrightarrow{|\cdot|_\upsilon} 0$ для всех j.

Доказательство. Будем вести доказательство индукцией по размерности V. В случае, когда она равна единице, утверждение тривиально. Не умаляя общности, пусть $j = 1$. Предположим, что $a_{i1} \overset{|\cdot|_\upsilon}{\not\longrightarrow} 0$. Тогда, переходя к подпоследовательности, мы можем полагать, что $\exists c > 0 : \forall i \ |a_{i1}|_\upsilon > c$.

Рассмотрим

$$\widetilde{x_i} = \frac{x_i}{a_{i1}} = v_1 + y_{2i}v_2 + \ldots + y_{mi}v_m,$$

где $m = \dim V$.

Ясно, что $\widetilde{x_i} \xrightarrow{|\cdot|_w} 0$. Заметим, что $t_i = \widetilde{x_{i+1}} - x_i \in \operatorname{span}(v_2, \ldots, v_m,)$, а тогда по предположению индукции

$$y_{j,i+1} - y_{j,i} \xrightarrow{|\cdot|_\upsilon} 0 \quad \forall j.$$

Тогда $\{y_{j,i}\}_{i\in\mathbb{N}}$ — последовательность Коши и, так как поле полное, она имеет предел. Пусть

$$\lim_{i\to\infty} \{y_{j,i}\}_{i\in\mathbb{N}} = s_j$$

$$0 \xleftarrow{i\to\infty} \widetilde{x_i} = \frac{x_i}{a_{i1}} = v_1 + y_{2i}v_2 + \ldots + y_{mi}v_m \xrightarrow{i\to\infty} v_1 + s_2v_2 + \ldots + s_mv_m.$$

что противоречит тому, что $\{v_i\}$ — базис.

□

Продолжим доказательство теоремы. Если $\{x_i\}$ — последовательность Коши, то по лемме $\{a_{ij}\}$ — тоже последовательность Коши. Тогда, так как пле полное, $a_{ij} \xrightarrow{i\to\infty} s_j$, откуда

$$x_i = \sum_j a_{ij}v_j \xrightarrow{|\cdot|_w} \sum_j s_jv_j,$$

то есть поле будет полным относительно нормирования w.

Теперь докажем единственность. Пусть $w' \neq w$ — другое продолжение нормирования υ. Тогда по аппроксимационной теореме мы можем найти $x_i \in L$ такие, что

$$x_i \xrightarrow{|\cdot|_w} 0, \quad x_i \overset{|\cdot|_{w'}}{\not\longrightarrow} 0.$$

Но из первого условия по лемме мы имеем $a_{ij} \xrightarrow{|\cdot|_\upsilon}$, а отсюда следует, что $x_i \xrightarrow{|\cdot|_{w'}} 0$, что противоречит предположению выше.

□

Таким образом мы доказали еще и такую теорему:

Теорема 112. *Пусть L/K — конечное расширение, υ — нормирование на K. Тогда υ можно продолжить на L.*

Доказательство. □

Домашнее задание 16. Задачи:

1. Докажите лемму Гензеля для полных полей:

   Теорема 113 (Лемма Гензеля для полных полей)**.** *Пусть (K, υ) — полное поле относительно нормирования υ, $\mathcal{O} = \mathcal{O}_\upsilon$, $\mathfrak{m} = \mathfrak{m}_\upsilon$. Пусть $f \in \mathcal{O}[x]$ и $f \neq 0 \pmod{\mathfrak{m}}$. Предположим, что*

   $$\overline{f_1} = \overline{g_1}\overline{h_1}, \quad (\overline{g_1}, \overline{h_1}) = (1) \text{ над } \mathbb{k} = \mathcal{O}/\mathfrak{m}.$$

   Тогда $\exists g, h \in \mathcal{O}[x]$:
   (a) $f = gh$.
   (b) $\deg g = \deg \overline{g_1}$.
   (c) $\overline{g} = \overline{g_1}$, $\overline{h} = \overline{h_1}$.

2. Докажите следствие из леммы Гензеля:

Следствие 43 (Из леммы Гензеля)**.** *Пусть $f \in K[x]$ — унитарный неприводимый многочлен над полным полем K, $f(0) \in \mathcal{O}_\upsilon$. Тогда $f \in \mathcal{O}_\upsilon[x]$.*

Пусть L/K — конечное расширение, а поле K — полное относительно нормирования υ. Положим $\varphi(x) = \upsilon(\mathrm{N}_{L/K}(x))$. Тогда:

(a) $\varphi\colon L^* \to \mathbb{Z}$ *— гомоморфизм.*
(b) $\varphi(x+y) \geq \min(\varphi(x), \varphi(y))$.
(c) $\frac{\varphi}{f}$ *— нормирование на L, продолжающее υ.*
(d) Пусть (K, υ) — произвольное нормированное поле, а f — мноочлен Эйзенштейна, то есть

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0, \quad \upsilon(a_i) > 0,\ \upsilon(a_0) = 1.$$

Тогда

i. f неприводим.
ii. Нормирование υ однозначно продолжается на поле $L = K[x]/(f)$, причём $e = n,\ f = 1$.

2.3 Целый базис для расширения полного поля

Пусть (K, υ) — полное нормированное поле, L/K — конечное расширение (на которое мы можем продолжить нормирование), а

$$\mathcal{O}_L = \{x \in K^* \mid \upsilon(x) > 0\}, \quad \mathcal{O}_L = \{x \in L^* \mid w(x) > 0\}, \quad w \mid \upsilon.$$

Пусть $\Bbbk = \mathcal{O}_L/\mathfrak{p}_K,\ \ell = \mathcal{O}_L/\mathfrak{p}_L$ — поля вычетов, а

$$f(L/K) = [\ell : \Bbbk], \quad e(L/K) = w(\pi), \text{ где } \pi_K \in \mathcal{O}_K,\ \upsilon(\pi) = 1, \quad w(\pi_L) = 1.$$

В частности, если расширение сепарабельно, то $ef = n$.

Предложение 76. *$\mathcal{O}_L$ — свободный $\mathcal{O}_K$-модуль ранга n.*

Доказательство. Пусть $\omega_1, \ldots, \omega_f \in \mathcal{O}_L$ — такие, что $\overline{\omega_1}, \ldots, \overline{\omega_f}$ — базис $\ell/\Bbbk$. Рассмотрим набор

$$\{\omega_i \pi_L^j\}_{1 \leq i \leq f,\ 0 \leq j \leq e-1}$$

и проверим, что он образует базис $\mathcal{O}_L$ над $\mathcal{O}_K$. Проверим сначала линейную независимость. Рассмотрим линейную комбинацию:

$$\sum_{i,j} a_{ij}\omega_i\pi_L^j = 0 \Leftrightarrow \sum_j \left(\sum_i a_{ij}\omega_i\right)\pi_L^j = 0.$$

Пусть $P_1 = \{0 \leq j \leq e-1 \mid \forall i\ \upsilon(a_{ij}) \geq 1\}$, а $P_2 = \{0 \leq j \leq e-1 \mid \exists i\colon \upsilon(a_{ij}) = 0\}$. Ясно, что они дополняют друг друга, то есть $P_1 \sqcup P_2 = \{0, 1, \ldots, e-1\}$. Заметим, что для $j \in P_1$

$$w\left(\left(\sum_i a_{ij}\omega_i\right)\pi_L^j\right) \geq e \implies w\left(\sum_{j \in P_1}\left(\sum_i a_{ij}\omega_i\right)\pi_L^j\right) \geq e.$$

Если $j \in P_2$, то перейдём к образу в поле вычетов:

$$\sum \overline{a_{ij}\omega_i} \neq 0 \in \ell,$$

так как $\{\overline{\omega_i}\}$ — базис $\ell/\Bbbk$, то есть элемент не лежит в идеале нормирования. Тогда

$$w\left(\sum_i a_{ij}\omega_i\right) = 0 \implies w\left(\left(\sum_i a_{ij}\omega_i\right)\pi_L^j\right) = j.$$

Тогда, суммируя мы получим, что

$$\sum_{j\in P_2}\left(\sum_{j\in P_2} a_{ij}\omega_i\right)\pi_L^j = \min_{j\in P_2} j \le e-1.$$

Так мы приходим к противоречию, так как

$$\sum_{j\in P_1}\left(\sum_{i} a_{ij}\omega_i\right)\pi_L^j = -\sum_{j\in P_2}\left(\sum_{i} a_{ij}\omega_i\right)\pi_L^j.$$

Если $P_2 \neq \varnothing$, то мы пришли к противоречию, так как нормирование левой части $\ge e$, а номрирование правой части $\le e-1$.

Если же $P_2 = \varnothing$, все $a_{ij} \vdots \pi_K$. Тогда мы можем делить коэффициенты на π_K до тех пор, пока хотя бы один из коэффициентов не будет не делиться на π_K. Если коэффициенты ненулевые, то в какой-то момент мы таким образом добьемся, что $P_2 \neq \varnothing$, что нам и нужно.

Покажем теперь, что это система образующих. Возьмём $x_0 = x \in \mathcal{O}_L$, рассмотрим $\overline{x} \in \ell$ и разложим по базису $\ell/\Bbbk$:

$$\overline{x} = \sum_{i=1}^{f} \overline{a_i}\cdot\overline{\omega_i} \rightsquigarrow x_0 = a_{01}\omega_1 + \ldots + a_{0f}\omega_f + \pi_L x_1.$$

Проделаем аналогичную процедуру для элемента $x_1 \in \mathcal{O}_L$:

$$\begin{cases} x_0 = a_{01}\omega_1 + \ldots + a_{0f}\omega_f + \pi_L x_1 \\ x_1 = a_{11}\omega_1 + \ldots + a_{1f}\omega_f + \pi_L x_1 \\ \vdots \\ x_{e-1} = a_{e-1,1}\omega_1 + \ldots + a_{e-1,f}\omega_f + \pi_L x_e. \end{cases}$$

Домножим второе уравнение на π_L, третье на π_{L^2} и так далее, и сложим. Тогда мы получим:

$$x = \sum_{1\le i\le f,\ 0\le j e-1} \alpha_{ij}^{(0)}\omega_i\pi_L^j + \pi_L^e y$$

Так как $\pi_K = \pi_L^e t$, где t обратим, мы можем переписать эту сумму вот в таком виде:

$$x = \sum_{1\le i\le f,\ 0\le j e-1} \alpha_{ij}^{(0)}\omega_i\pi_L^j + \pi_K\widetilde{x_1}, \quad \widetilde{x_1} \in \mathcal{O}_L.$$

Для $\widetilde{x_1}$ мы можем записать аналогичное равенство:

$$\begin{cases} \widetilde{x_1} = \sum_{1\le i\le f,\ 0\le j e-1} \alpha_{ij}^{(1)}\omega_i\pi_L^j + \pi_K\widetilde{x_2}, \quad \widetilde{x_2} \in \mathcal{O}_L \\ \widetilde{x_2} = \sum_{1\le i\le f,\ 0\le j e-1} \alpha_{ij}^{(2)}\omega_i\pi_L^j + \pi_K\widetilde{x_3}, \quad \widetilde{x_3} \in \mathcal{O}_L \\ \vdots \end{cases}$$

Домножим первое равенство на π_k, второе на π_K^2 сложим (тут строчек бесконечное число, но так как общий член стремится у нулю, всё в порядке). Тогда мы получим

$$x = \sum \alpha_{ij}\omega_i\pi_L^j, \quad \alpha_{ij} \in \mathcal{O}_K,$$

что и требовалось. □

Рассмотрим теперь башню полей $E/L/K$. Тогда нетрудно заметить, что

$$e(E/K) = e(E/L)\cdot e(L/K), \quad f(E/K) = f(E/L)\cdot f(L/K).$$

Пусть $\overline{E}$,$\overline{K}$, $\overline{L}$. Тогда второе утверждение — просто лемма о башне, а первое утверждение следует из того, что

$$\pi_K = \pi_L^{e(L/K)}\cdot u,\ u \in \mathcal{O}_L^*, \quad \pi_L = \pi_E^{e(E/L)}v, \quad v \in E^* \rightsquigarrow \pi_K = \pi_E^{e(E/L)\cdot e(L/K)}\cdot s, \quad s \in E^*.$$

Эти равенства оказываются весьма удобными, когда необходимо вычислять индексы ветвления и степени инерции.

С этого момента мы будем повсеместно полагать поле K полным относительно нормирования v.

2.4 Неравзветвлённые и вполне разветвлённые расширения

Обычно выделяют два типа расширений такого поля K:

Определение 138. Пусть K — полное поле, тогда конечное расширение L/K называется *неравзетвлённым*, если $e(L/K) = 1$, а $\ell/\Bbbk$ — сепарабельно.

Оно же называется *вполне разветвлённым*, если $f(L/K) = 1$.

Замечание. В случае, когда поле вычетов конечно (а это как раз интересный нам случай), сепарабельность есть автоматически.

Отметим также, что в случае вполне разветвленного расширения мы не требуем сепарабельности.

Пример 55. Например, если $L = K(\theta)$, где

$$\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_1\theta + a_0 = 0$$

и, минимальный многочлен θ Эйзенштейнов, то есть, $\upsilon(a_i) \geq 1,\ \upsilon(a_0) = 1$. Тогда L/K — вполне равзетвлённое расширение.

Кроме того, верно и обратное: любое равзетвлённое расширение полного поля K получается присоединением корня многочлена Эйзенштейна.

Пример 56. Рассмотрим над $\mathbb{Q}_p$ многочлен $x^2 - pu,\ u \equiv 1 \pmod p,\ u \neq 1$. Тогда, так как $u \in \mathbb{Q}_p^{*2}$, мы всегда получим расширение $\mathbb{Q}_p\big(\sqrt{p}\big)$. Значит, различные многочлены Эйзенштейна могут давать одно и то же расширение.

С другой стороны, если $x^2 - p\varepsilon$, где $\varepsilon \notin \mathbb{Q}_p^{*2}$, мы получаем вполне разветвлеённое расширение $\mathbb{Q}_p\big(\sqrt{p\varepsilon}\big)$.

А вот расширение $\mathbb{Q}_p(\sqrt{\varepsilon})$ будет неразветвлённым.

Оказывается, если поле вычетов конечно (как в этом случае), то существует ровно одно неравзетвлённое расширение заданной степени.

Пример 57. Нетрудно придумать пример, когда поле вычетов будет алгебраически замкнутым. Пусть $\Bbbk$ — алгебраически замкнутое, рассмотрим поле $\Bbbk((t))$. Оно является полным относительно нормирования

$$\upsilon(f) = n, \quad f = t^n(a_0 + a_1 t + \ldots).$$

В данном случае $\mathcal{O}_K = \Bbbk[[t]]$, а $\mathfrak{m}_\upsilon = (t)$, откуда $\mathfrak{m}_\upsilon = \Bbbk$.

Теперь изучим, как строить неравзветвлённые расширения:

Предложение 77. *Пусть $\Bbbk$ — поле вычетов, а $\overline{f}$ — неприводимый сепарабельный (над $\Bbbk$) унитарный многочлен (предположим, что $\Bbbk$ таково, что он существует) степени n. Пусть f — его прообраз, т.е. многочлен над K. Рассмотрим $L = K(\alpha)$, где α — корень f. Тогда L/K — неравзетвлённое расширение степени n.*

Доказательство. Мы можем единственным образом продолжить нормирование υ на поле L и рассмотреть поле вычетов $\ell = \mathcal{O}_L/\mathfrak{m}_L$. Заметим, что

$$[\ell : \Bbbk] \geq [\Bbbk(\overline{\alpha}) : \Bbbk] = n.$$

Отсюда мы имеем $ef = n$, а так как $f = n$, мы получаем $e = 1$, что и хотели. □

Пусть L/K — неравзветвлённое расширение, а расширение $\ell/\Bbbk$ сепарабельно. Тогда $\ell = \Bbbk(\overline{\theta})$, где $\overline{f}(\overline{\theta}) = 0$. Тогда у нас есть башня расширений

$$K \subset K(\theta) \subset L.$$

Так как L/K неравзветвлено, а индекс ветвления мультипликативен относительно башни, отсюда мы получаем, что $K(\theta)/K$ тоже неравзветвлено (тут еще нужно сделать комментарий, что если сепарабельное расширение раскладывается в башню, то все её этажи сепарабельны). Тогда мы получаем, что

$$f(L/K(\theta)) = 1, \quad f(K(\theta)/K) = f(L/K), \quad e(L/K(\theta)) = 1,$$

откуда $L = K(\theta)$.

2.5 Локальные поля

Определение 139. Поле K с дискретным нормированием υ называется *локальным*, если оно полно относительно нормирования υ, а его поле вычетов $\Bbbk = \mathcal{O}_\upsilon/\mathfrak{m}_\upsilon$ конечно.

Пример 58. Например, локальным является поле $\mathbb{Q}_p$ и вообще любое его конечное расширение. Построим пример локального поля в положительной характеристики. Зафиксируем $\mathrm{char} = p > 0$ и рассмотрим $K = \mathbb{F}_q((t))$, где $q = p^n$. Это поле будет полным относительно нормирования ord_t, а полем вычетов будет $\mathbb{F}_q$.

Пусть K — локальное поле, а L/K — неразветвлённое расширение, $\mathrm{char}\,\Bbbk = p$, $|\Bbbk| = q = p^n$, $n = [\ell : \Bbbk]$. Тогда известно, что

$$\ell = \Bbbk[\zeta_{q^n-1}]$$

Покажем, что $L = K(\zeta_{q^n-1})$.

Над ℓ многочлен $x^{q^n} - x$ раскладывается на различные линейные множители:

$$\overline{x^{q^n} - x} = \prod_i (x - \overline{\alpha_i}), \quad \alpha_i \in \ell$$

Вопсользуемся леммой Гензеля: каждый корень над полем вычетов поднимается в корень над $\mathcal{O}_L$. Так мы получаем промежуточное расширение

$$K \subset K(\zeta_{q^n-1}) \subset L.$$

Покажем, что нижний этаж башни — расширение степени n (и из этого всё будет следовать). Посмотрим на поле вычетов:

$$[\Bbbk[\zeta_{q^n-1}] : \Bbbk] \geq n \implies [K(\zeta_{q^n-1}) : K] \geq n,$$

откуда $L = K(\zeta_{q^n-1})$.

Таким образом, мы показали, что над локальным полем есть только одно неразветвлённое расширение степени n и это $K(\zeta_{q^n-1})$.

Домашнее задание 17. Задачи:

1. Пусть L/K — неразветвлённое расширение. Тогда возникают следующие коммутативные диаграммы:
   Докажите, что они коммутативны.
2. Пусть L/K — неравзветвлённое расширение, причем $\ell/\Bbbk$ — расширение Галуа. Тогда L/K — тоже расширение Галуа и, кроме того, есть естественный изоморфизм
   $$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/\Bbbk).$$
3. Пусть K — локальное поле характеристики 0. Пусть $\upsilon(p) = e$, где $p = \mathrm{char}\,\Bbbk$. Положим $e_0 = e/(p-1)$. Докажите, что
   $$U_i \xrightarrow{\sim} U_{i+e} \text{ при } i > e_0,$$
   где изоморфизм — это $x \mapsto x^p$. Также докажите, что
   $$U_i/U_{i+1} \xrightarrow{\sim} U_{pi}/U_{pi+1} \text{ при } i < e_0,$$
   где $x \mapsto x^p$.
4. Пусть L/K — неравзветвлённое расширение локального поля K. Докажите, что $N_{L/K}(U_L) = U_K$.

С этого момента пусть K — локальное поле.;

Теорема 114. *Пусть L/K — конечное расширение локального[14] поля K, $f = f(L/K)$ — степень инерции. Тогда существует промежуточное поле E между K и L, определяемое таким образом: $E = K(\zeta_{q^f-1})$ (где $q = |\Bbbk|$), при этом, E/K — неразветвлённое расширение, и любое неравзветвлённое расширение $K \subset F \subset L$ содержится в E.*

[14] Ясно, что в этом случае поле L также локально.

Доказательство. Так как $\ell = \Bbbk(\zeta_{q^f-1})$, $\zeta_{q^f-1} \in L$, и получим расширение $E = K(\zeta_{q^f-1})/K,\ E \subset L$. Мы доказывали, что такое расширение будет иметь степень ровно f и будет неразветвлённым.

$$f(E/K) = f, \quad e(E/K) = 1 \implies f(L/E) = 1,\ e(L/E) = e = e(L/K),$$

откуда верхний этаж является вполне разветвлённым расширением.

Возьмём произвольное неразветвлённое расширение $K \subset E_1 \subset L$, пусть $f_1 = f(E_1/K) = f_1$. Ясно, что $f_1 f(L/E_1) = f$, откуда $f_1 \mid f$. Из доказанного в конце предыдущей лекции мы знаем, что $E_1 = K(\zeta_{q_1^f-1})$, а так как $f_1 \mid f$, $q^{f_1} - 1 \mid q^f - 1$, откуда $E_1 = K(\zeta_{q^{f_1}-1}) \subset E$, что мы и хотели. □

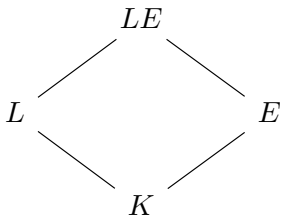
Следствие 44. *Пусть L_1/K и L_2/K — неравзветвлённые расширения. Тогда L_1L_2/K — неравзветвлённое расширение.*

Доказательство. По предыдущей теореме у нас есть максимальное промежуточное неравзвтелённое расширение E такое, что $K \subset E \subset L_1L_2$. В частности, по максимальности $L_1 \subset E$, $L_2 \subset E$, откуда $L_1L_2 \subset E$, а тогда $L_1L_2 = E$, то есть, в частности, композит является неразветвлённым расширением. □

Следствие 45. *Пусть L/K — неразветвлённое расширение, а E/K — конечное расширение. Тогда расширение LE/E также неразветвлённое.*

Доказательство. Предположим, что E/K неравзветвлённое. Тогда по предыдущей теореме LE/K неразветвлённое, но тогда и LE/E неразветвлённое.

Теперь пусть E/K — вполне разветвлённое. Рассмотрим диаграмму



Тогда мы имеем

$$e = e(E/K) = [E : K] \geq [LE : L] \geq e(LE/L) = e(LE/K) = e(E/K) \cdot e(LE/E).$$

Отсюда мы получаем, что $e(LE/E) = 1$, то есть LE/E неразветвлённое. □

Замечание. Отметим, что так как поля здесь локальные, мы не говорим о сепарабельности (так как конечное расширение конечного поля сепарабельно всегда).

Подобные результаты можно получать и не для глобальных полей, но мы этого делать не будем.

На этом мы прервёмся в изучении локальных полей и перейдём к несколько другой технике, которая нам понадобится для классификации абелевых расширений поля $\mathbb{Q}_p$.

3. Когомологии групп

3.1 Построение при помощи проективных резольвент

Пусть G — группа. Через G-Mod обозначим категорию модулей над $\mathbb{Z}[G]$.

Рассмотрим $\mathbb{Z}$, как $\mathbb{Z}[G]$-модуль с тривиальным действием, то есть $\forall g \in G,\ a \in \mathbb{Z}\ g \cdot a = a$. Построим проективную резольвенту $\mathbb{Z}$, как G-модуля.

Накроем $\mathbb{Z}$ сюръективно проективным модулем P_0:

$$P_0 \xrightarrow{d_0} \mathbb{Z} \to 0.$$

Теперь накроем $\operatorname{Ker} d_0$ проективным модулем P_1 и рассмотрим сквозное отображение $d_1\colon P_1 \to \operatorname{Ker} d_1 \to P_0$. Тогда по построению $\operatorname{Im} d_1 = \operatorname{Ker} d_0$, так что комплекс

$$P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} \mathbb{Z} \to 0.$$

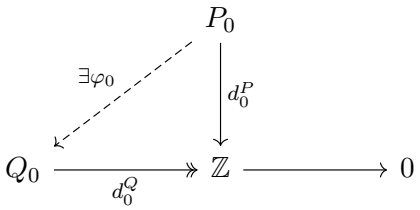
будет точным в нулевом члене. Продолжая эту процедуру мы получим ацикличный комплекс из проективных модулей:

$$\dots P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} \mathbb{Z} \to 0$$

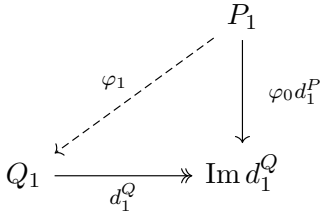
Собственно он и называется *проективной резольвентой* $P_\bullet$.

Замечание. Отметим, что построение выше сильно зависело от всяческих выборов.

Пусть теперь $P_\bullet$ и $Q_\bullet$ — две проективные резольвенты. Построим морфизм цепных комплексов $P_\bullet \to Q_\bullet$. Отображение $P_0 \to Q_0$ строится просто из проективности модуля P_0:



Теперь заметим, что $d_0^Q\varphi_0 d_1^P = \mathrm{id}_{\mathbb{Z}}\, d_0^P d_1^P = 0$, то есть $\operatorname{Im}\varphi_0 d_1^P \subset \operatorname{Ker} d_0^Q = \operatorname{Im} d_1^Q$. Тогда у нас есть вот такая диаграмма:

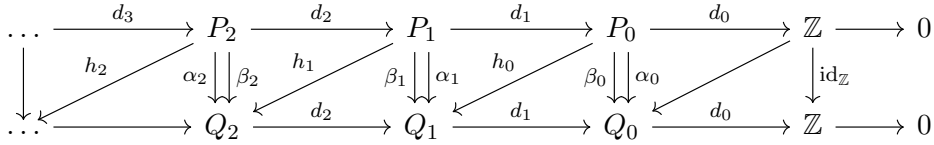


Продолжая в том же духе, получаем морфизм $\varphi\colon P_\bullet \to Q_\bullet$.

Замечание. Отметим, что в этом рассуждении мы нигде не пользовались проективностью резольвенты $Q_\bullet$. Вообще говоря, только что мы доказали несколько более общее утверждение: для любого морфизма модулей $\varphi\colon M \to N$ (где $P_\bullet$ — проективная резольвента M, а $Q_\bullet$ — резольвента N существует морфизм комплексов $\varphi_\bullet\colon P_\bullet \to Q_\bullet$ на нулевых гомологиях) совпадающий в нулевом члене с φ. У нас (здесь и далее) всегда будет $\varphi = \mathrm{id}$.

Теперь покажем, что любые два морфизма между проективными резольвентами цепно-гомотопны. Пусть $\alpha, \beta\colon P_\bullet \to Q_\bullet$ — морфизмы цепных комлпексов, построим связывающую их цепную гопотопию h, то есть $h\colon P_\bullet \to Q_{\bullet+1}$ такое что

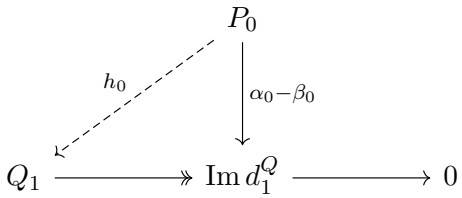
$$\alpha - \beta = dh + hd.$$



Заметим, что

$$d_0^Q\alpha_0 = d_0^Q\beta_0 \implies d_0^Q(\alpha_0 - \beta_0) = 0 \implies \operatorname{Im}\alpha_0 - \beta_0 \subset \operatorname{Ker} d_0^Q = \operatorname{Im} d_1^Q.$$

Тогда по проективности у нас есть отображение h_0:



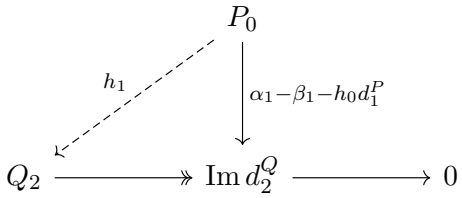
Теперь построим отображение h_1. По построению

$$\alpha_0 - \beta_0 = h_0 d_1^P \implies (\alpha_0 - \beta_0) d_1^P = d_1^Q h_0 d_1^P.$$

Соотвественно, мы имеем

$$d_1^Q(\alpha_1 - \beta_1 - h_0 d_1^P) = d_1^Q(\alpha_1 - \beta_1) - (\alpha_0 - \beta_0) d_1^P = 0,$$

так как α и β — цепные отображения. Значит, $\operatorname{Im} \alpha_1 - \beta_1 - h_0 d_1^P \subset \operatorname{Ker} d_1^Q = \operatorname{Im} d_2^Q$, откуда мы снова имеем вот такую диаграмму:



и из проективности мы снова получаем отображение h_1. Продолжая в том же духе мы построим цепную гомотопию h.

Замечание. Таким образом, мы показали, что любые два морфизма проективных резольвент цепно-гомотопны. Итого, мы знаем, что *между двумя проективными резольвентами G-модуля $\mathbb{Z}$ существует единственный с точностью до гомотопии морфизм, продолжающий* $\mathrm{id}_{\mathbb{Z}}$.

Определение 140. Теперь рассмотрим проективную резольвенту $P_\bullet \to \mathbb{Z}$ и применим к ней функтор $\operatorname{Hom}(\_, A)$, где $A \in G\text{-}\mathsf{Mod}$, тогда мы получим комплекс

$$0 \to \operatorname{Hom}_G(P_0, A) \to \operatorname{Hom}_G(P_1, A) \to \operatorname{Hom}_G(P_2, A) \to \dots$$

Гомологии построенного выше комплекса

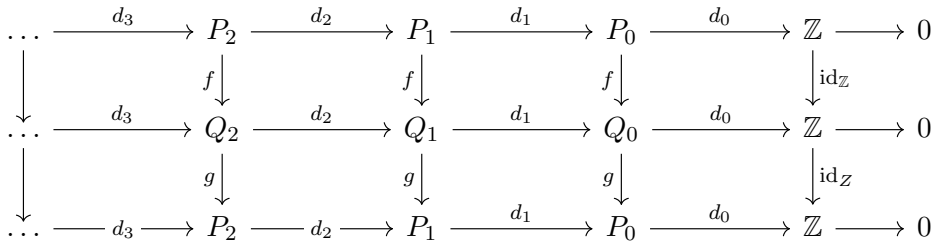
$$0 \to \operatorname{Hom}_G(P_0, A) \xrightarrow{d_0} \operatorname{Hom}_G(P_1, A) \xrightarrow{d_1} \operatorname{Hom}_G(P_2, A) \to \dots$$

мы будем называть группами *когомологий* группы G с коэффициентами в $\mathbb{Z}[G]$-модуле A и обозначать, как $H^i(G, A)$. Если говорить точнее,

$$H^i(G, A) \stackrel{\text{def}}{=} Z^i(G, A)/B^i(G, A), \text{ где } Z^i(G, A) = \ker d_i,\ B^i(G, A) = \operatorname{Im} d_{i-1}.$$

Заметим, что пока что когомологии зависят от выбора резольвенты. Покажем, что это не так. Для этого обозначим когомологии, посчитанные при помощи одной проективной резольвенты за $H^\bullet(G, A)^{(P)}$, а при помощи другой за $H^\bullet(G, A)^{(Q)}$.

Тогда существует морфизм $f\colon P_\bullet \to Q_\bullet$ и $g\colon Q_\bullet \to P_\bullet$.



Тогда, пользуясь нашим замечанием мы получаем, что $f_*g_* \sim \mathrm{id}$ и $g_*f_* \sim \mathrm{id}$. Зафиксируем гомотопию h и заметим, что когда мы применим к диаграмме для неё функтор Hom у нас получится снова гомотопия, но уже для нужного комплекса. Таким образом мы получим

$$H^q(G,A)^{(P)} \xrightarrow{f^*} H^q(G,A)^{(Q)} \xrightarrow{g^*} H^q(G,A)^{(P)}, \text{ и } g^*f^* = \mathrm{id}\,.$$

По симметричности мы получаем, что $H^q(G,A)^{(P)} \cong H^q(G,A)^{(Q)}$.

Как и всегда, стандартным образом из которткой точной последовательности коэффициентов получается длинная точная последовательность когомологий:

Теорема 115 (Длинная точная последовательность когомологий)**.** *Пусть* $0 \to A \to B \to C$ *— точная последовательность* G*-модулей. Тогда имеется естественная длинная точная последовательность групп когомологий:*

$$0 \to H^0(G;A) \to H^0(G;B) \to H^0(G;C) \to H^1(G;A) \to H^1(G;B) \to \ldots \to \\ \to H^n(G;A) \to H^n(G;B) \to H^n(G;C) \to H^{n+1}(G,A) \to \ldots$$

3.2 Стандартная резольвента

Как мы видели в предыдущем параграфе, когомологии группы G с коэффициентами в G-модуле A не зависят от выбора проективной резольвенты. В данном параграфе мы приведём *стандартную резльвенту*, которая часто оказывается весьма удобной при вычислениях. ъ

Определение 141. *Стандратная проективная резольвента* для $\mathbb{Z}$ — это свободная резольвента

$$\ldots \mathbb{Z}[G^i] \to \mathbb{Z}[G^{i+1}] \to \ldots \to \mathbb{Z}[G^2] \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0.$$

Напомним, что $P_i = \mathbb{Z}[G^{i+1}]$ — свободный $\mathbb{Z}[G]$-модуль с базисом $G \times G \times \ldots \times G$ (где произведение берётся $i+1$ раз). Группа G действует на каждый базисный элементы естественным образом:

$$s \cdot (g_0, \ldots, g_i) = (sg_0, \ldots, sg_i).$$

Гомоморфизм $d\colon \mathbb{Z}[G^i] \to \mathbb{Z}[G^{i-1}]$ определяется стандартным образом:

$$d_i(g_0, \ldots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \ldots, g_{j-1}, g_{j+1}, \ldots, g_i).$$

Заметим, что тогда

$$\mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], A) = \{f\colon G^{i+1} \to A \mid f(\sigma g_0, \ldots, \sigma g_i) = \sigma g(g_0, \ldots, g_i)\}.$$

Заметим, что такая функция полностью определяется своими значениями на элементах из G^{i+1} вида $(1, g_1, g_1g_2, \ldots, g_1g_2 \ldots g_i)$. Соответственно, если мы обозначим

$$\varphi(g_1, \ldots, g_i) = f(1, g_1, g_1g_2, \ldots, g_1 \ldots g_i),$$

то дифференциал в комплексе $\mathrm{Hom}_G(\mathbb{Z}[G^\bullet], A)$ можно записать в таком виде:

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

Найдём теперь конструктивное описание некоторых групп когомологий.

Пример 59 (Нулевая группа когомологий)**.** По определению $H^0(G, A) \cong \ker d_1$. Теперь заметим, что из точности последовательности

$$P_1 \to P_0 \to \mathbb{Z} \to 0$$

следует точность последовательности

$$0 \to \mathrm{Hom}_G(\mathbb{Z}, A) \xrightarrow{\varphi} \mathrm{Hom}_G(P_0, A) \xrightarrow{d_0} \mathrm{Hom}_G(P_1, A),$$

откуда $\ker d_0 = \mathrm{Im}\,\varphi$, а так как φ — мономорфизм, $\mathrm{Im}\,\varphi \cong \mathrm{Hom}_G(\mathbb{Z}, A)$. Таким образом,

$$H^0(G, A) \cong \mathrm{Hom}_G(\mathbb{Z}, A).$$

Также отметим, что $\mathrm{Hom}_G(\mathbb{Z}, A) \cong A^G$, где $A^G = \{a \in A \mid ga = a\ \forall g \in G\}$ — неподвижные точки. Второй изоморфизм строится так:

$$\mathrm{Hom}_G(\mathbb{Z}, A) \ni \varphi \mapsto \varphi(1).$$

Сначала заметим, что он вообще действует в A^G, так как $\forall n \in \mathbb{Z}\ \varphi(gn) = g\varphi(n)$ с одной стороны, а с другой, так как $\mathbb{Z}$ у нас действует на G тривиально, $\varphi(gn) = \varphi(n)$, т.е. $\varphi(n) = g\varphi(n)\ \forall n \in \mathbb{Z}$.

Очевидно, что этот гомоморфизм инъективен, покажем, что он сюръективен. Действительно, для $a \in A^G$ положим $\varphi(1) = a$, а далее доопределим φ по линейности и G-эквивариантности (т.е. положим $\varphi(n) = na$). Таким образом,

$$H^0(G, A) \cong A^G.$$

Пример 60 (Первая группа когомологий)**.** При помощи явной формулы для дифференцицала мы сразу видим, что

$$Z^1(G, A) = \ker d_2 = \{\varphi\colon G \to A \mid \varphi(g_1 g_2) = g_1\varphi(g_2) + \varphi(g_1)\}.$$

Т.е. коциклами являются *скрещенные гомоморфизмы*, т.е. отображения $\varphi\colon G \to A$, для которых выполнено тождество $\varphi(g_1 g_2) = g_1\varphi(g_2) + \varphi(g_1)$. Кроме того, сразу видно, что

$$B^1(G, A) = \mathrm{Im}\, d_1 = \{\varphi\colon G \to A \mid \exists a \in A\colon \varphi(g) = ga - a\}.$$

Соответственно, мы имеем $H^1(G, A) = Z^1(G, A)/B^1(G, A)$. Приведём теперь несколько примеров.

Пусть $A = \mathbb{Z}$ с тривиальным действием. Тогда $\varphi(g_1 g_2) = g_1\varphi(g_2) + \varphi(g_1) = \varphi(g_2) + \varphi(g_1)$, и

$$Z^1(G, \mathbb{Z}) = \mathrm{Hom}_{\mathsf{Grp}}(G, \mathbb{Z}).$$

Кроме того, так как $ga - a = a - a = 0$, мы имеем $B^1(G, \mathbb{Z}) = 0$. Таким образом,

$$H^1(G, \mathbb{Z}) \cong \mathrm{Hom}_{\mathsf{Grp}}(G, \mathbb{Z}).$$

- Пусть теперь G — конечная группа. Тогда $\forall g\ \exists n\colon g^n = e$. Тогда $\varphi(g^n) = n\varphi(g) = \varphi(e) = 0$, откуда $\varphi(g) = 0$. Таким образом, $\mathrm{Hom}_{\mathsf{Grp}}(G, \mathbb{Z}) = 0$.
- Если же $G = \mathbb{Z}$, то

$$\mathrm{Hom}_{\mathsf{Grp}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z} \implies H^1(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}.$$

Определение 142. Пусть $A, B \in G$-Mod. Тогда на $\mathrm{Hom}(A, B)$ можно завести структуру G-модуля следующим образом: пусть $\varphi \in \mathrm{Hom}(A, B)$, тогда определим

$$g\varphi\colon A \to B, \quad g\varphi(a) = g \cdot \varphi(g^{-1}a).$$

Замечание. Также заметим, что $\mathrm{Hom}(A, B)^G = \{\varphi \in \mathrm{Hom}(A, B) \mid \forall g \in G g\varphi = \varphi\}$, но в то же время

$$g\varphi = \varphi \Leftrightarrow g\varphi(g^{-1}a) = \varphi(a) \Leftrightarrow \varphi(g^{-1}a) = g^{-1}\varphi(a),$$

откуда видно, что $\mathrm{Hom}(A, B)^G = \mathrm{Hom}_G(A, B)$.

Определение 143. Пусть X — абелева группа с тривиальным действием G. Тогда модуль вида $\mathrm{Hom}(\mathbb{Z}[G], X)$ мы будем называть *коиндуцированным.*

Заметим, что есл $A = \mathrm{Hom}(\mathbb{Z}[G], X)$ — коиндуцированный модуль, то для любого $B \in G\text{-}\mathsf{Mod}$

$$\mathrm{Hom}_G(B, A) \cong \mathrm{Hom}_G(B, X) \Leftrightarrow \mathrm{Hom}_G(B, \mathrm{Hom}(\mathbb{Z}[G], X)) \cong \mathrm{Hom}_G(B, X).$$

Действительно, изоморфизм строится таким образом:

$$\varphi\colon B \to A,\ \varphi \mapsto \psi\colon B \to X,\ \psi(b) = \varphi(b) \cdot 1.$$

Обратное же отображение стротся так:

$$f \in \mathrm{Hom}_G(B, X),\ f \mapsto \varphi\colon b \mapsto s_b \text{ где } s_b(\sigma) = f(\sigma^{-1}b).$$

Легко видеть, что эти отображения взаимнообратны. Теперь мы видим, что наш комплекс (который вычисляет когомологии) приобретает вот такой вид:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_G(P_0, A) & \longrightarrow & \mathrm{Hom}_G(P_1, A) & \longrightarrow & \mathrm{Hom}_G(P_2, A) & \longrightarrow & \dots \\ & & \| & & \| & & \| & & \\ 0 & \longrightarrow & \mathrm{Hom}_G(P_0, X) & \longrightarrow & \mathrm{Hom}_G(P_1, X) & \longrightarrow & \mathrm{Hom}_G(P_2, X) & \longrightarrow & \dots \end{array}$$

Заметим, что проективные модули свободны как абелевы группы (так как являются прямыми слагаемыми свободных), а на них функтор $\mathrm{Hom}_G(\_, X)$ точен. Соответственно, полученный комплекс будет точен в каждом члене, начиная со второго. Соответственно, мы получили, что если A — коиндуцированный модуль, то

$$H^q(G, A) = 0 \quad \forall q \geq 1.$$

Теперь пусть A — произвольный G-модуль, тогда мы можем рассмотреть $A^* = \mathrm{Hom}(\mathbb{Z}[G], A)$. Тогда существует естественное вложение $A \hookrightarrow A^*$ по правилу $a \mapsto \varphi_a$, где $\varphi_a(g) = g^{-1}a$. Соответственно, у нас есть короткая точная последовательность модулей

$$0 \to A \to A^* \to A' \to 0,$$

где $A' = A^*/A$. Если мы напишем длинную точную последовательность когомологий, то, так как $H^q(G, A^*) = 0 \quad \forall q \geq 1$, свзывающий гомоморфизм даст нам изоморфизмы

$$\delta\colon H^q(G, A') \xrightarrow{\sim} H^{q+1}(G, A),$$

что часто позволяет вести индукцию по размерности.

3.3 Когомологии циклической группы

Пусть $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ — короткая точная последовательность коэффициентов. Она индуцирует длинную точную последовательность когомологий

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C) \xrightarrow{\delta} \dots$$

Вспомним, как устроен связывающий гомоморфизм в маленьких размерностях. Возьмём $c \in C^G$, так как j — эпиморфизм, $\exists b\colon j(b) = c$. Тогда

$$j(gb - b) = gc - c = 0, \text{ так как } c \in C^G.$$

Так как $\ker j = \mathrm{Im}\, i$, это означает, что $gb - b = i(a)$ для некоторого $a \in A$. Соответственно, мы можем определить функцию

$$\varphi\colon G \to A, \quad g \mapsto a, \text{ где } a\colon gb - b = i(a).$$

Так как i —мономорфизм, при фиксированном b элемент a определён однозначно. Теперь заметим, что

$$\begin{cases} g_1 b - b = i(a_1) \\ g_2 b - b = i(a_2) \end{cases} \implies g_1 g_2 b - b = g_1(g_2 b - b) + (g_1 b - b) = g_1 i(a_2) + i(a_1) = i(g_1 a_2 + a_1).$$

Таким образом, мы получили, что $\varphi(g_1 g_2) = g_1 \varphi(g_2) + \varphi(g_1)$, то есть φ — 1-коцикл.

Значит, у нас есть отображение $C^G \to Z^1(G, A)$, определённое как $c \mapsto \varphi$. Заметим, что если мы выберем другой прообраз b' вместо b, коцикл φ изменится на когранцу и класс когомологий от этого не изменится. Итого, связывающий гомоморфизм в нулевом члене имеет такой вид:

$$\delta \colon C^G \to H^1(G, A), \quad c \mapsto [\varphi].$$

Приступим теперь к подсчету когомологий $G = C_n = \langle \sigma \rangle,\ \sigma^n = e$.

Определение 144. Положим $N = \sum_{g \in G} g \in \mathbb{Z}[G]$. *Норменным отображением* мы будем называть отображение

$$N \colon \mathbb{Z}[G] \to \mathbb{Z}[G], \quad a \mapsto N \cdot a.$$

Для циклической группы у нас есть такая проективная резольвента:

$$\ldots \xrightarrow{\cdot(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\cdot N} \mathbb{Z}[G] \xrightarrow{\cdot(\sigma-1)} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

где ε — аугументация. Проверим точность:

- Пусть $x = \sum_{i=0}^{n-1} a_i \sigma^i$, тогда если $\varepsilon(x) = 0$, то $\sum_{i=0}^{n-1} a_i = 0$, откуда

  $$x = \sum_{i=0}^{n-1} a_i \sigma^i = \sum_{i=0}^{n-1} a_i \sigma^i - \sum_{i=0}^{n-1} a_i = \sum_{i=0} a_i (\sigma^i - 1),$$

  откуда $x \in (\sigma - 1)\mathbb{Z}[G]$.
- Теперь пусть $(\sigma - 1)\left(\sum_{i=0}^{n-1} a_i \sigma^i\right) = 0$, тогда

  $$a_0 + a_1 \sigma + \ldots + a_{n-1} \sigma^{n-1} = a_0 \sigma + a_1 \sigma^2 + \ldots + a_{n-2} \sigma^{n-1} + a_{n-1}$$

  Приравнивая коэффициенты при базисных элементах мы получаем:

  $$a_1 = a_0, a_2 = a_2, \ldots \implies a_0 = a_1 = \ldots = a_{n-1} = a,$$

  откуда $x = Na$.

и, точность в остальных членах тоже проверяется. Тогда наш комплекс будет иметь вид

$$0 \to \mathrm{Hom}_G(\mathbb{Z}[G], A) \xrightarrow{\cdot(\sigma-1)} \mathrm{Hom}_G(\mathbb{Z}[G], A) \xrightarrow{\cdot N} \mathrm{Hom}_G(\mathbb{Z}[G], A) \to \ldots$$

Теперь вспомним, что $\mathrm{Hom}_G(\mathbb{Z}[G], A) \cong A$ и наш комплекс выглядит немного адекватнее:

$$0 \to A \xrightarrow{\cdot(\sigma-1)} A \xrightarrow{\cdot N} A \xrightarrow{\cdot(\sigma-1)} A \xrightarrow{\cdot N} \ldots,$$

откуда видно, что мы доказали такую теорему

Теорема 116. *Пусть G — циклическая группа порядка n, а $A \in G$-Mod. Тогда*

$$H^0(A, G) = A^G, \quad H^{2i+1}(G, A) \cong \ker N / (\sigma - 1)A, \quad H^{2i}(G, A) \cong A^G / NA.$$

Замечание. Мы тут немножко замяли под ковёр, но впрочем очевидно, что для циклической группы $(\sigma - 1)x = 0 \Leftrightarrow x \in A^G$.

Предложение 78. *Пусть G — конечная группа, $0 \to A \to B \to C$ — короткая точная последовательность. Тогда следующая последовательность точна:*

$$A^G/NA \to B^G/NB \to C^G/NC \xrightarrow{\delta} H^1(G, A) \to \dots$$

Доказательство. Запишем сначала длинную точную последовательность когомологий:

$$0 \to A^G \xrightarrow{i^*} B^G \xrightarrow{j^*} C^G \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C) \xrightarrow{\delta} \dots$$

По точности $\forall c \in C\ \exists b \in B\colon c = j(b)$. Тогда $j(Nb) = Nc$, а так как $Nb \in B^G$, мы получаем, что $Nc \in \operatorname{Im} j^* \subset \ker \delta$. Отсюда мы имеем $NC \subset \operatorname{Ker} \delta$. В остальных членах точность очевидна.

□

3.4 Гомологии групп

Пусть G — группа, $\mathbb{Z}$ мы рассматриваем, как G-модуль с тривиальным действием. Рассмотрим проективную резольвенту

$$\dots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0.$$

Применим к ней функтор $\_ \otimes_{\mathbb{Z}[G]} A$, получим комплекс

$$\dots \to P_1 \otimes_{\mathbb{Z}[G]} A \to P_0 \otimes_{\mathbb{Z}[G]} A \to 0.$$

Тогда $H_i(G, A)$ мы определим, как группы гомологий этого комплекса.

Замечание. Нетрудно проверить, что группы гомологий не зависят от выбора резольвенты.

Пример 61 (Нулевые гомологии)**.** Так как тезнорное произведение $\_ \otimes_{\mathbb{Z}[G]} A$ точно справа, последовательность

$$P_1 \otimes_{\mathbb{Z}[G]} A \to P_0 \otimes_{\mathbb{Z}[G]} A \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \to 0$$

точна. Отсюда $\operatorname{Im}(P_1 \otimes A \to P_0 \otimes A) \cong \ker\big(P_0 \otimes A \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} A\big)$. Соответственно,

$$H_0(G, A) \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A.$$

Пусть $P_0 = \mathbb{Z}[G]$, а отображение $\varepsilon\colon P_0 \twoheadrightarrow \mathbb{Z}$ — аугументация. Тогда, как мы помним, $\ker \varepsilon = I = \langle g - 1 \mid g \in G\rangle$ — аугументационный идеал. Соответственно, у нас есть вот такая короткая точная последовательность:

$$0 \to I \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0.$$

Домножим её тензорно на A над $\mathbb{Z}[G]$, получим точную последовательность

$$I \otimes_{\mathbb{Z}[G]} A \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \to 0,$$

а так как $\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} A \cong A$, мы имеем

$$I \otimes_{\mathbb{Z}[G]} A \to A \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \to 0,$$

а из точности этой последовательности мы заключаем, что

$$\operatorname{Ker}\big(P_0 \otimes_{\mathbb{Z}[G]}\big) A \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \cong IA,$$

откуда $H_0(G, A) \cong A/IA$.

Отметим, что для гомологий короткая точная последовательность коэффициентов $0 \to A \to B \to C \to 0$ также индуцирует длинную точную последовательность когомологий:

$$\dots \to H_q(G, A) \to H_q(G, B) \to H_q(G, C) \xrightarrow{\delta} H_{q-1}(G, A) \to \dots.$$

Теорема 117. $H_1(G, \mathbb{Z}) \cong G^{ab} = G/[G, G]$.

Доказательство. Рассмотрим короткую точную последовательность

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

напишем соотвествующую длинную точную последовательность гомологий:

$$\ldots \to H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}) \to \ldots$$

- Покажем, что $H_1(G, \mathbb{Z}[G]) = 0$. Действительно, если мы напишем проективную резольвенту для $\mathbb{Z}$ и тезнорно умножим её на $\mathbb{Z}[G]$, то полученный комплекс будет точным со второго члена (так как проективные модули свободны как абелевы группы, а тензорное произведение на таких — точный функтор) и все его гомологии (кроме нулевых) будут нулевыми.
- $H_0(G, \mathbb{Z}[G]) \cong \mathbb{Z}$ и $H_0(G, \mathbb{Z}) = \mathbb{Z}$, причем стрелка между ними — изоморфизм.

Значит, наша точная последовательность на самом деле имеет вид

$$0 \to \ldots H_1(G, \mathbb{Z}) \xrightarrow{\sim} H_0(G, I_G) \xrightarrow{\cdot 0} \mathbb{Z} \xrightarrow{\sim} \mathbb{Z} \to \ldots,$$

откуда $H_1(G, \mathbb{Z}) \cong H_0(G, I_G)$. С другой стороны, мы вычисляли нулевые гомологии:

$$H_0(G, I_G) \cong I_G / I_G^2.$$

Остаётся доказать, что $I_G / I_G^2 \cong G^{\mathrm{ab}}$.

Действительно, рассмотрим отображение

$$\varphi \colon G \to I/I^2, \quad g \mapsto g - 1 \pmod{I^2}.$$

Убедимся, что отображение корректно определено:

$$ghg^{-1}h^{-1} - 1 = (gh - hg)g^{-1}h^{-1},$$

но в то же время

$$gh - g - h + 1 = (g-1)(h-1) \in I_G^2, \quad hg - g - h - 1 = (h-1)(g-1) \in I_G^2,$$

$$gh - g - h + 1 - (hg - g - h - 1) = gh - hg.$$

Теперь построим обратное отображение таким образом

$$x = \sum_{g \in G} a_g \cdot g \in I_G, \quad \psi(x) = \prod_{g \in G} g^{a_g} \pmod{G, G}.$$

$$\psi((g-1)(h-1)) = \psi(gh - g - h + 1) = gh \cdot g^{-1} \cdot h^{-1} \equiv 0 \pmod{[G, G]},$$

то есть I_G^2 лежит в ядре. Кроме того, легко видеть, что $\psi \circ \varphi = \varphi \circ \psi = \mathrm{id}$. □

Соотвественно, как и с индуцированными модулями, мы можем рассмотреть

$$0 \to A'' \to A_* \to A \xrightarrow{\varphi} 0, \text{ где } A_* = \mathbb{Z}[G] \otimes_Z A,$$

гомоморфизм φ действует как $\sigma \otimes a \mapsto a$, а $A'' = \ker \varphi$. Соотвественно, рассуждением аналогичным рассуждению для коиндуцированных модулей мы получаем, что гомологии с коэффициентами в A^* тривиальны. Как и в случае с коиндуцированными модулями, при помощи длинной точной последовательности пары мы можем делать сдвиг размерности.

Кроме того, отметим, что если группа G конечна, то $\mathrm{Hom}(\mathbb{Z}[G], X) \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ как G-модули. Действительно, изоморфизм выглядит вот так:

$$\varphi \mapsto \sum_G g \otimes \varphi(g)$$

Соответственно, индуцированный модуль также является и коиндуцированным (и, когомологии в нём также тривиальны).

3.5 Когомологии Тейта

Определение 145. Пусть G — группа, $A \in G$-Mod. Введём группы *когомологий Тейта* с коэффициентами в G-модуле A:

$$\widehat{H}^{-1}(G,A) \stackrel{\text{def}}{=} \ker N_A/IA, \quad \widehat{H}^{-n}(G,A) \stackrel{\text{def}}{=} H_{n-1}(G,A) \text{ при } n \geq 2$$

и, кроме того,

$$\widehat{H}^0(G,A) = A^G/N_A A, \quad \widehat{H}^n(G,A) \stackrel{\text{def}}{=} H^n(G,A) \text{ при } n \geq 1.$$

Пусть $0 \to A \to B \to C$ — короткая точная последовательность. Мы знаем, что тогда есть длинная точная последовательность гомологий и длинная точная последовательность когомологий. Утверждается, что если правильно (т.е. так, как в определении выше) подобрать нулевой и начальные члены, будет длинная точная последовательность для когомологий Тейта (бесконечная в две стороны!):

$$\ldots \to \widehat{H}^{-1}(G,A) \to \widehat{H}^{-1}(G,B) \to \widehat{H}^{-1}(G,C) \to \widehat{H}^0(G,A) \to \widehat{H}^0(G,B) \to \widehat{H}^0(G,C) \to \widehat{H}^1(G,A) \to \ldots$$

Соответственно, точность в отрицательном и в положительном куске мы знаем. Проверим точность на стыках.

- Построим сначала гомоморфизм $\operatorname{Ker} N_C/IC \to A^G/N_A A$. Рассмотрим диаграмму:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N_A} & & \downarrow{\scriptstyle N_B} & & \downarrow{\scriptstyle N_C} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

  Возьмём $c \in \operatorname{Ker} N_C$. У него есть какой-то прообраз при горизонтальном отображении, назовём его b и рассмотрим $N_B b$. В силу коммутативности диаграммы, направо он уйдёт в ноль (так как $c \in \operatorname{Ker} N_C$), а значит, $N_B b$ лежит в образе стрелки $f\colon A \to B$ в нижней части диаграммы. Тогда возьмём какой-то его прообраз a (он определён однозначно, так как $f\colon A \to B$ инъективна).
- Покажем, что это построение корректно. $a \in A^G$, так как $N_B b \in B^G$. Если же мы выберем b' вместо b, как прообраз, то $N_B b - N_B b'$. Тогда $f^{-1}(N_B b - N_B b') \in N_A A$.
- Покажем, что IC попадает в 0 при отображении в $A^G/N_A A$. Проверим это для образующих аугментационного идеала, пусть $c = c'(g-1) \in IC$, тогда $b = b'(g-1)$, но тогда

$$N_B b = \left(\sum_{\sigma \in G} \sigma\right) b'(g-1) = b'\left(\sum_{\sigma \in G} \sigma g - \sum_{\sigma \in G} \sigma\right) = 0,$$

  так как домножение на элемент группы это биекция. Точность проверяется как и обычно, технически.

Тривиальность когомологий Тейта для индуцированного модуля

Пусть G — конечная, группа $A_* \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$, где X — абелева группа (т.е. A_* — индуцированный модуль). Покажем, что

$$H^q(G,A) = 0 \quad \forall q \in \mathbb{Z}.$$

Для $q > 0$ мы это видели в замечании после определения индуцированного модуля. Рассмотрим теперь $q = 0$. Любой элемент $a \in A_*$ мы можем записать в виде

$$a = \sum_g g \otimes x_g, \quad x_g \in X.$$

Если $g'a = a$, то

$$\sum_g (g'g \otimes x_g) = \sum_g g \otimes x_g,$$

в частности, $g' \otimes x_{g'} = g' \otimes x_e$, откуда $x_{g'} = x_e$. Соответственно, если $a \in A_*^G$, то $x_g = x_e \; \forall g \in G$ и отсюда

$$a = \left(\sum_{g \in G} g\right) \otimes x_e = N(e \otimes x_e) \implies a \in N_G A_*.$$

Значит, $\widehat{H}^0(G, A_*) = A_*^G / N A_* = 0$.

Теперь пусть $q < -1$. Пусть $a \in \operatorname{Ker} N$, то есть

$$N_G(\sum_g g \otimes x_g) = 0 \implies \sum_g x_g = 0 \implies \sum_g (g \otimes x_g) = \sum_g ((g-1) \otimes x_g) \in I_G A_*,$$

то есть $H^{-1}(G, A_*) = \operatorname{Ker} N / I_G A_* = 0$.

Пусть теперь $r < -1$. Возьмём для абелевой группы X свободную резольвенту длины 2[15]:

$$0 \to X_1 \to X_0 \to X \to 0.$$

Тезнорно домножим эту последовательность на $\mathbb{Z}[G]$ (так как модули свободны, последовательность останется точной), получим последовательность

$$0 \to A_1 \to A_0 \to A_* \to 0$$

Так как A_1, A_0 — свободные $\mathbb{Z}[G]$-модули,

$$H^q(G, A_1) = H^q(G, A_0) = 0 \quad \forall q < -1.$$

А так как они индуцированные, $\forall q \geq -1$

$$H^q(G, A_1) = H^q(G, A_0) = 0.$$

Таким образом, мы всё доказали.

3.6 Периодичность когомологий Тейта для циклической группы

Так как далее мы будем часто сталкиватся с циклическими группами (в целях теории Галуа), полезно понимать, какие же у них когомологии Тейта.

Теорема 118. *Пусть G — циклическая группа конечного порядка, $A \in G$-Mod. Тогда выбор образующей в G задаёт изоморфизм*

$$\widehat{H}^q(G, A) \cong \widehat{H}^{q+2}(G, A) \quad \forall q \in \mathbb{Z}.$$

Доказательство. Пусть $G = \langle \sigma \rangle$. Тогда имеется следующая короткая точная последовательность:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\cdot(\sigma - 1)} \mathbb{Z}[G] \xrightarrow{\sigma^i \mapsto 1} \mathbb{Z} \longrightarrow 0$$

Так как все члены последовательности, а также, аугументационный идеал $I_G = \operatorname{Ker}(\mathbb{Z}[G] \to \mathbb{Z})$ свободны, как абелевы группы, после тензорного умножения на A последовательнльность останется точной:

$$0 \longrightarrow A \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \longrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \longrightarrow A \longrightarrow 0$$

[15] достаточно накрыть свободной и взять ядро

Она, в свою очередь, разваливается в две короткие точные последовательности:

$$0 \to A \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to N_1 \to 0$$

$$0 \to N_1 \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to A \to 0.$$

Записывая длинную точную последовательность пары мы для каждой из них, мы получаем, что

$$H^q(G, A) \cong H^{q+1}(G, N_2) \cong H^{q+2}(G, A),$$

что и даёт нам нужный факт. □

Замечание. Отметим, что это явление мы уже наблюдали для когомологий, но там была стандартная теория, а тут теория Тейта (и это существенно)!

3.7 Индекс Эрбана

Пусть G конечная группа и предположим дополнительно, что

$$|\widehat{H}^0(G, A)| < \infty, \quad |\widehat{H}^1(G, A)| < \infty.$$

Замечание. Позже мы увидим, что для конечных групп группы когомологий Тейта периодичны, так что это означает, что все когомологии конечны.

Определение 146. Пусть $A \in G\text{-Mod}$. Его *индексом Эрбана* мы будем называть

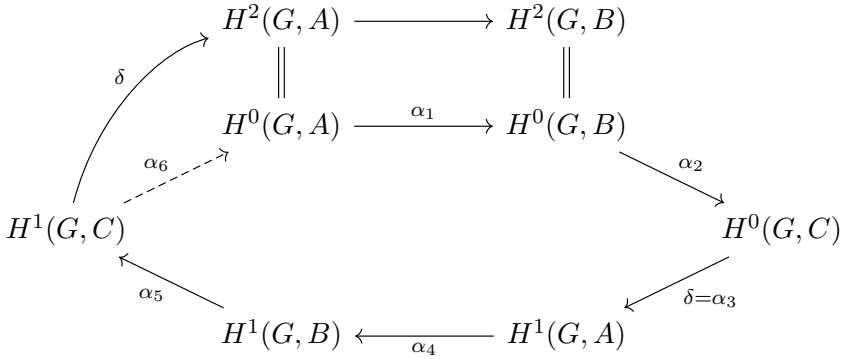
$$h(A) = \frac{|\widehat{H}^0(G, A)|}{|\widehat{H}^1(G, A)|}.$$

Докажем лемму, которая помогает удобно вычислять индекс Эрбана.

Предложение 79. *Пусть G — конечная циклическая группа, а $0 \to A \to B \to C \to 0$ — короткая точная последовательность $\mathbb{Z}[G]$-модулей. Предположим, что два из трё индексов Эрбана $h(A), h(B), h(C)$ определены. Тогда определён и третий и, более того,*

$$h(B) = h(C) \cdot h(A).$$

Доказательство. Так как группа циклическая (и её когомологии периодичны), из длинной точной последовательности пары мы получаем вот такой коммутативный шестиугольник (бензольное кольцо):



Соответственно, обозначая $M_i = \ker \alpha_i = \mathrm{Im}_{\alpha_{i-1}}$, мы получаем такие короткие точные последовательности:

$$\begin{cases} 0 \to M_1 \to H^0(G, A) \to M_2 \to 0 \\ 0 \to M_2 \to H^0(G, B) \to M_3 \to 0 \\ \vdots \\ 0 \to M_6 \to H^1(G, C) \to M_1 \to 0 \end{cases} \implies h(A) = \frac{H^0(G, A)}{H^1(G, A)} = \frac{|M_1| \cdot ||M_2|}{|M_4| \cdot |M_5|},$$

и, аналогичным образом:

$$h(B) = \frac{|M_2| \cdot |M_3|}{|M_5| \cdot |M_6|}, \quad h(C) = \frac{|M_3| \cdot |M_4|}{|M_1| \cdot |M_6|},$$

откуда $h(A) \cdot h(C) = h(B)$. □

Следствие 46. *Пусть G — конечная циклическая группа, и при этом G-модуль A конечный. Тогда $h(A) = 1$.*

Доказательство. Запишем две точные последовательности:

$$0 \to \operatorname{Ker} N \to A \xrightarrow{\cdot N} A^G \to \widehat{H}^0(G, A) \to 0$$

$$0 \to A^G \to A \xrightarrow{\cdot(\sigma-1)} \operatorname{Ker} N \to H^1(G, A) \to 0.$$

Тогда мы имеем

$$|\widehat{H}^0(G, A)| = \frac{|A^G| \cdot |\operatorname{Ker} N|}{|A|}, \quad |\widehat{H}^1(G, A)| = \frac{|A^G| \cdot |\ker N|}{|A|},$$

откуда видно, что $h(A) = 1$. □

Следствие 47. *Пусть $A, B \in G$-Mod, $f \in \operatorname{Hom}_G(A, B)$ и при этом $|\ker f| < \infty$ и $|\operatorname{Coker} f| < \infty$. Тогда если один из индексов Эрбрана $h(A), h(B)$ определён, то они оба определены и совпадают.*

Доказательство. Теперь у нас есть такие короткие точные последовательности:

$$0 \to \operatorname{Ker} f \to A \twoheadrightarrow \operatorname{Im} f \to 0$$

$$0 \to \operatorname{Im} f \to B \to \operatorname{Coker} f \to 0.$$

Не умаляя общности, $h(A)$ определён. Тогда мы получаем, что

$$\Big\{ h(A) \text{ определён } h(\ker f) = 1 \quad \Longrightarrow \ h(\operatorname{Im} f) \text{ определён} .$$

$$\begin{cases} h(\operatorname{Coker} f) = 1 \\ h(\operatorname{Im} f) \text{ определён} \end{cases} \Longrightarrow \ h(b) \text{ определён}$$

и, из формул выше следует, что $h(B) = h(\operatorname{Im} f) \cdot h(\operatorname{Coker} f)$. Но тогда

$$h(B) = h(\operatorname{Im} f) = \frac{h(A)}{h(\ker f)} = h(A).$$

□

3.8 Ограничение и инфляция

Пусть $\varphi\colon H \to G$ — гомоморфизм групп, а $A \in G$-Mod. Тогда A естественно наделяется структурой H-модуля следующим образом:

$$a \cdot h \stackrel{\text{def}}{=} \varphi(h) \cdot a.$$

Тогда у нас есть гомоморфизм $\varphi^*\colon \mathbb{Z}[H] \to \mathbb{Z}[G]$, так как групповое кольцо это функтор, а значит, есть и морфизм комплексов

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Hom}_G(\mathbb{Z}[G], A) & \longrightarrow & \operatorname{Hom}_G(\mathbb{Z}[G^2], A) & \longrightarrow & \operatorname{Hom}_G(\mathbb{Z}[G^3], A) & \longrightarrow & \dots \\
 & & \downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} & & \downarrow{\scriptstyle \varphi^*} & & \\
0 & \longrightarrow & \operatorname{Hom}_H(\mathbb{Z}[H], A) & \longrightarrow & \operatorname{Hom}_H(\mathbb{Z}[H], A) & \longrightarrow & \operatorname{Hom}_H(\mathbb{Z}[H], A) & \longrightarrow & \dots
\end{array}$$

и индуцированный морфизм на когомологиях $\varphi^*\colon H^k(G,A) \to H^k(H,A)$.

Определение 147. Если $H \leq G$ и $\varphi\colon H \hookrightarrow G$ — это вложение, то индуцированный морфизм в когомологиях

$$H^\bullet(G,A) \xrightarrow{\text{res}} H^\bullet(H,A)$$

мы будем называть *гомоморфизмом ограничения* и обозначать res.

Замечание. Этот гомоморфизм, вообще говоря, не обязан быть мономорфизмом.

Пусть теперь $H \leq G$ — нормальная подгруппа, а $A \in G\text{-Mod}$. Тогда A^H можно естественным образом снабдить структурой G/H-модуля:

$$(gh)a = ga.$$

Соответственно, у нас есть диаграмма

$$\begin{array}{ccc} \dots \longrightarrow \operatorname{Hom}_G(\mathbb{Z}[(G/H)^i], A^H) & \longrightarrow & \dots \\ \downarrow & & \\ \dots \longrightarrow \operatorname{Hom}_G(\mathbb{Z}[G^i], A) & \longrightarrow & \dots \end{array}$$

Определение 148. Соответствующий индуцированный морфизм $H^n(G/H, A^H) \xrightarrow{\text{inf}} H^n(G,A)$ в когомологиях мы будем называть *инфляцией.*

Предложение 80. *Пусть $A \in G\text{-Mod}$, H — нормальная подгруппа в G. Тогда следующая последовательность точна:*

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G,A) \xrightarrow{\text{res}} H^1(H,A).$$

Доказательство. **Шаг 1.** Пусть $f \in Z^1(G/H, A^H)$, тогда f удовлетворяет

$$f(\overline{g_1 g_2}) = \overline{g_1} f(\overline{g_2}) + f(\overline{g_1}).$$

Предположим, что отображение

$$\inf(f)\colon G \xrightarrow{\pi} G/H \xrightarrow{f}\to A^H \to A$$

является кограницей (не умаляя общности, назовём его той же буквой), то есть, существует $a \in A$ такой, что $\forall g \in G\ f(\overline{g}) = ga - a$. Проверим, что в таком случае $a \in A^H$.

$$\begin{cases} f(\overline{gh}) = f(\overline{g}) = ga - a \\ f(\overline{gh}) = gha - a \implies gha = ga \implies ha = a \implies a \in A^H. \end{cases}$$

Значит, $f \in B^1(G/H, A^H)$, то есть мы проверили инъективность стрелки inf.
Шаг 2. Докажем, что $\text{res} \circ \text{inf} = 0$. Пусть $f \in Z^1(G/H, A^H)$. Рассмотрим

$$\text{res} \circ \inf(f) = \widetilde{f}\colon H \to G \to G/H \xrightarrow{f} A^H \hookrightarrow A$$

В самом деле, тогда

$$\widetilde{f}(h) = f(\overline{1}) = 0 \implies \text{res} \circ \inf(f) = 0.$$

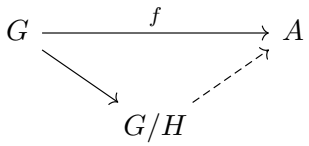
Шаг 3. Пусть теперь $f \in Z^1(G; A)$ и $f \in \ker(\text{res})$. То есть,

$$f(g_1 g_2) = g_1 f(g_2) + f(g_1), \quad \exists a\colon f(h) = ha - a.$$

Рассмотрим кограницу $\ell(g) = ga - a \in B^1(G,A)$. Тогда $[f] = [f - \ell]$, но

$$(f - \ell)(h) = ha - a - (ha - a) = 0,$$

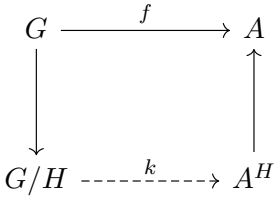
поэтому мы с самого начала можем полагать, что наш представитель $f|_H \equiv 0$. Тогда можно попустить отображение через фактор:



С другой же стороны,

$$f(hg_2) = hf(g_2) + f(h) = hf(g_2),$$

откуда ясно, что отображение пропускается через A^H, т.е. у нас есть вот такая диаграмма



и очевидно, что k — коцикл. □

Теперь распространим гомоморфизм ограничения на отрицательные размерности.

Пусть A — G-модуль, $H \hookrightarrow$, тогда есть отображение $A^G \hookrightarrow A^H$ (действительно, если $a \in A$ неподвижен под действием всех элементов из G, то под действием всех элементов из H уж точно). Тогда есть и корректное отображение

$$A^G/N_G A \to A^H/N_H A.$$

В самом деле, если $x \in N_G A$, то $x = \sum_\sigma \sigma \cdot a$ для некоторого a. Заметим, что

$$G = \bigsqcup_i \sigma_i H.$$

Соответственно, тогда мы имеем

$$N_G a = \sum_{\sigma \in G} \sigma a = \sum_{\tau \in H} \left(\sum_i \sigma_i a \right) = N_H \left(\sum_i \sigma_i a \right) \in N_H A.$$

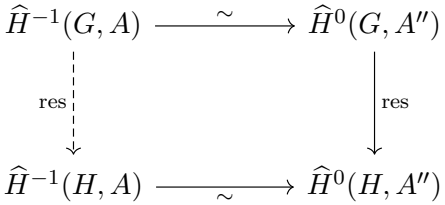
Таким образом мы смогли доопределить ограничение на нулевые когомологии Тейта:

$$\mathrm{res}\colon \widehat{H}^0(G,A) \to \widehat{H}^0(H,A).$$

Осталось распространить его на отрицательные размерности. Рассмотрим короткую точную последовательность

$$0 \to A'' \to A_* \to A \xrightarrow{\varphi} 0, \text{ где } A_* = \mathbb{Z}[G] \otimes_Z A,$$

гомоморфизм φ действует как $\sigma \otimes a \mapsto a$, а $A'' = \ker \varphi$. Так как модуль A_* когомологически тривиален, то есть $\widehat{H}^n(G, A_*) = 0 \ \forall n \in \mathbb{N}$, мы получаем из длинной точной последовательности мы получаем следующую диаграмму (точнее говоря, горизонтальные изоморфимзы в ней)



Тогда определим res в -1-й размерности, как пунктирную стрелочку, замыкающую диаграмму.

Замечание. Вообще говоря, чтоб был у нас был изоморфизм когомологий Тейта для подгруппы H, нужно, чтоб A_* был не только G-индуцированным, но и H-индуцированным. Соответственно, надо проверить, почему же это так.

3.9 Точная последовательность для ограничения и инфляции в старших размерностях

Как мы видели ранее, если $A \in G\text{-Mod}$, а H — нормальная подгруппа в G, то следующая последовательность точна:

$$0 \to H^1(G/H, A^H) \xrightarrow{\inf} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A).$$

В этом параграфе мы понятным образом обобщим этот результат на старшие размерности.

Предложение 81. *Пусть $H \leq G$ — нормальная подгруппа, $A \in G$-Mod, а кроме того*

$$H^1(H, A) = H^2(H, A) = \ldots = H^{q-1}(H, A) = 0.$$

Тогда следующая последовательность точна:

$$0 \to H^q(G/H, A^H) \xrightarrow{\inf} H^q(G, A) \xrightarrow{\text{res}} H^q(H, A).$$

Доказательство. Естественно, будем доказывать утверждение индукцией по q.
База: Для $q = 1$ утверждение мы знаем.
Переход: Рассмотрим короткую точную последовательность

$$0 \to A \to A^* \to A' \to 0,$$

она индуцирует длинную точную последовательность когомологий:

$$0 \to A^H \to (A^*)^H \to (A')^H \to \underbrace{H^1(H, A)}_{=0} \to \ldots$$

Из неё (так как A^* коиндуцированный) мы получаем, что $H^i(H, A') \cong H^{i+1}(H, A)$. Кроме того, из этой же короткой точной последовательности мы стандартным образом получаем, что $H^{q-1}(G, A') \cong H^q(G, A)$.

Обозначим для простоты $F = G/H$. Теперь заметим, что в частности из длинной точной последовательности сверху можно достать короткую точную последовательность

$$0 \to A^H \to (A^*)^H \to (A')^H \to 0,$$

как начальный кусок. Напишем длинную точную последовательность когомологий и для неё:

$$\ldots H^{q-1}(F, (A^*)^H) \to H^{q-1}(F, (A')^H) \to H^q(F, A^H) \to H^q(F, (A^*)^H) \to \ldots.$$

Заметим, что $(A^*)^H = \text{Hom}(\mathbb{Z}[G], A)^H \cong \text{Hom}(\mathbb{Z}[G/H], A)$, откуда следует, что $(A^*)^H - H$-коиндуцированный модуль. Значит, из длинной точной последовательности выше мы заключаем, что

$$H^{q-1}(F, (A')^H) \cong H^q(F, A^H).$$

Соответственно, тогда у нас есть такая коммутативная диаграмма:

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{q-1}(F, (A')^H) & \xrightarrow{\inf} & H^{q-1}(G, A') & \xrightarrow{\text{res}} & H^{q-1}(H, A') \\
 & & \downarrow \sim & & \downarrow \sim & & \downarrow \sim \\
0 & \longrightarrow & H^q(F, A^H) & \xrightarrow{\inf} & H^q(G, A) & \xrightarrow{\text{res}} & H^q(H, A)
\end{array}$$

Верхняя строка точна по индукционном предположению, а вертикальные стрелки — изоморфизмы. Значит, и нижняя строка точна. □

3.10 Отображение кограничения

Определение 149. Пусть $H \leq G$, тогда вложение $H \hookrightarrow G$ индуцирует морфизм цепных комплексов

$$\begin{array}{ccccccc} \ldots & \longrightarrow & \mathbb{Z}[H^2] \otimes_H A & \longrightarrow & \mathbb{Z}[H] \otimes_H A & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \\ \ldots & \longrightarrow & \mathbb{Z}[G^2] \otimes_G A & \longrightarrow & \mathbb{Z}[G] \otimes_G A & \longrightarrow & 0 \end{array}$$

Это цепное отображение индуцирует отображение в когомологиях $H_n(H, A) \to H_n(G, A)$. Это отображение мы будем называть отображением *кограничения* и обозначать cores.

Соответственно, в таком случае отображение кограничения определено $\widehat{H}^{-n}(H, A) \to \widehat{H}^{-n}(G, A)$ для всех $n > 1$.

Доопределим $\mathrm{cores}\colon \widehat{H}^{-1}(H, A) \to \widehat{H}^{-1}(G, A)$.

Пусть $I_G = \ker\left(\mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z}\right)$ — аугументационный идеал, $I_G = \langle g - 1 \mid g \in G \rangle$. Тогда

$$H_0(G, A) \cong A/I_G A \supset \operatorname{Ker} N_G/I_G A \cong \widehat{H}^{-1}(G, A).$$

Соответственно, у нас есть такая диаграмма:

$$\begin{array}{ccc} A/I_H A & \hookleftarrow & \ker N_H/I_H A \\ \Big\downarrow{\scriptstyle \mathrm{cores}} & & \Big\downarrow{\scriptstyle \mathrm{cores}} \\ A/I_G A & \hookleftarrow & \ker N_G/I_G A \end{array}$$

и cores в -1-й размерности определяется как пунктирная стрелка, замыкающая эту диаграмму. Отметим, что эта стрелка есть, так как $G = \bigsqcup_i \sigma_i H$ и тогда

$$\sum_{h \in H} hx = 0 \implies \sum_{g \in G} gx = \sum_i \sigma_i \left(\sum_{h \in H} hx \right) = 0.$$

Таким образом, мы распространили кограничение на -1-ю группу когомологий Тейта.

Теперь распространим кограничение на положительные размерности. Это мы сделаем при помощи коиндуцированных модулей. Пусть $A^* = \mathrm{Hom}(\mathbb{Z}[G], A)$, рассмотрим диаграмму

$$0 \to A \xrightarrow{i} A^* \to A' \to 0,$$

где $i(a) = \varphi_a$, который действует так: $\varphi_a(g) = g^{-1}a$ (ясно, что отображение i инъективно), а $A' = \operatorname{Coker} i$. Тогда из длинной точной последовательности пары мы получаем (и того факта, что коиндуцированный модуль гомологически тривиален), что

$$\widehat{H}^{-1}(G, A') \cong \widehat{H}^0(G, A), \quad \widehat{H}^{-1}(H, A') \cong \widehat{H}^0(H, A).$$

Замечание. Как и в предыдущем рассуждении такого толка тут также нужно проверить, что A^* является не только G-коиндуцированным, но и H-коиндуцированным.

Итак, у нас есть диаграмма

$$\begin{array}{ccc} \widehat{H}^{-1}(H, A') & \xrightarrow{\sim} & \widehat{H}^0(H, A) \\ \Big\downarrow{\scriptstyle \text{cores}} & & \Big\downarrow{\scriptstyle \text{cores}} \\ \widehat{H}^{-1}(G, A') & \xrightarrow{\sim} & \widehat{H}^0(G, A) \end{array}$$

и cores в нулевой размерности мы определяем, как пунктирную стрелочку, замыкающую эту диаграмму.

Теперь при помощи диаграммного поиска выпишем явную формулу для коограничения. Рассмотрим диаграмму

$$\begin{array}{ccccc} \widehat{H}^{-1}(H, A') & \xrightarrow{\sim} & \widehat{H}^0(H, A) & = & A^H/N_H A \\ \Big\downarrow{\scriptstyle \text{cores}} & & \Big\downarrow{\scriptstyle \text{cores}} & & \\ \widehat{H}^{-1}(G, A') & \xrightarrow{\sim} & \widehat{H}^0(G, A) & = & A^G/N_G A \end{array}$$

Возьмём класс $\overline{\varphi} \in \widetilde{H}^{-1}(H, A') \cong \operatorname{Ker} N_H/I_H A' \subset A'/I_H A'$. Рассмотрим вот такую диаграмму:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & A^* & \longrightarrow & A' & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle N} & & \Big\downarrow{\scriptstyle N} & & \Big\downarrow{\scriptstyle N} & & \\ 0 & \longrightarrow & A & \longrightarrow & A^* & \longrightarrow & A' & \longrightarrow & 0 \end{array}$$

Тогда $N_H\overline{\varphi} = 0 \implies N_H\varphi = \varphi_a \in A^*$, где $\varphi_a(g) = g^{-1}a$. Пусть $G = \sqcup_i \sigma_i H$, тогда мы имеем такую диаграмму:

$$\begin{array}{ccc} \ker N_H/I_H A' & \xrightarrow{\sim} & A^H/N_H A \\ \Big\downarrow{\scriptstyle \text{cores}} & & \Big\downarrow{\scriptstyle \text{cores}} \\ \ker N_G/I_G A' & \xrightarrow{\sim} & A^G/N_G A \end{array} \qquad \begin{array}{ccc} \overline{\varphi} \pmod{I_H A'} & \longmapsto & a \\ \Big\downarrow & & \Big\downarrow \\ \overline{\varphi} \pmod{I_G A'} & \longmapsto & \sum_i \sigma_i a \end{array}$$

Покажем, что $\overline{\varphi} \pmod{I_G A'} \mapsto \sum_i \sigma_i a$. Отметим сразу, что из этого будет следовать, что

$$\text{cores}^0(a) = \sum_i \sigma_i a.$$

Теперь докажем требуемый факт. Он следует из нашего замечания выше о том, что $N_H\varphi = \varphi_a$:

$$(N_G\varphi)(g) = \left(\sum_i \sigma_i N_H\varphi\right)(g) = (\sum_i \sigma_i\varphi_a)(g) = \varphi_{\sum_i \sigma_i a}(g),$$

что и требовалось.

3.11 Композиция ограничения и кограничения

Теперь выведем из только что доказанной формулы для $\mathrm{cores}^0(a)$ полезные следствия.

Пусть G – конечная группа, рассмотрим композицию

$$A^G/N_GA \xrightarrow{\mathrm{res}} A^H/N_HA \xrightarrow{\mathrm{cores}} A^G/N_GA$$

Соответственно, идя по композиции мы получаем

$$a \in A^G \mapsto a \in A^H \mapsto \sum_i \sigma_i a,$$

но так как изначально $a \in A^G$, мы имеем $\forall i\ \sigma_i a = a$, откуда

$$\mathrm{cores}(\mathrm{res}(a)) = [G : H] \cdot a.$$

Аналогичные формулы можно получать и в больших размерностях при помощи сдвига (посредством длинной точной последовательности когомологий).

Пусть $q \geq 1$, рассмотрим вновь короткую точную последовательность

$$0 \to A \to A^* \to A' \to 0,$$

где стрелка $A \to A'$ устроена как $a \mapsto \varphi_a,\ \varphi_a(g) = g^{-1}a$, а A' — это коядро этой стрелки.

Соответственно, так как для $q \geq 1$ когомологии с коэффициентами в A^* тривиальны, из длинной точной последовательности когомологий мы можем заключить, что $H^{q-1}(G, A') \cong H^q(G, A)$ (т.е. мы можем сдвинуть размерность). Теперь рассмотрим диаграмму:

$$\begin{array}{ccccc}
H^{q-1}(G, A') & \xrightarrow{\mathrm{cores}} & H^{q-1}(H, A') & \xrightarrow{\mathrm{cores}} & H^{q-1}(G, A') \\
\downarrow\sim & & \downarrow\sim & & \downarrow\sim \\
H^q(G, A) & \xrightarrow{\mathrm{res}} & H^q(H, A) & \xrightarrow{\mathrm{res}} & H^q(G, A)
\end{array}$$

Коммутативность правого квадрата следует из определения cores^q, а коммутативность левого квадрата следует из того, что связывающий гомоморфизм коммутирует с гомоморфизмами точных троек комплексов.

Предположим, что мы доказали требуемую формулу для $q-1$ (т.е. для верхней строчки диаграммы). Тогда по индукционному предположению мы имеем

$$\mathrm{cores}^{q-1} \circ \mathrm{res}^{q-1}(a) = [G : H] \cdot a,$$

и из коммутативности диаграммы отсюда мы можем заключить, что утверждение верно и для q.

Теперь коротко обсудим, что же происходит в отрицательной размерности. Как нетрудно догадаться, там нужно рассмотреть короткую точную последовательность

$$0 \to A'' \to A_* \to A \to 0$$

и воспользоваться тем, что для групп отрицательной размерности когомологии с коэффициентами в модуле A_* тривиальны, а тогда из длинной точной последовательности пары мы заключаем, что

$$\widehat{H}^q(G, A) \cong \widehat{H}^{q-1}(G, A''),$$

откуда следует, что можно делать сдвиг размерности влево.

Итого, в этом параграфе мы доказали такую теорему:

Теорема 119. *Пусть G — конечная группа, $H \leq G$ — подгруппа. Тогда во всех размерностях выполнена такая формула:*

$$\mathrm{cores} \circ \mathrm{res}(a) = [G : H] \cdot a.$$

Следствие 48. *Если $H = e$ — тривиальная подгруппа, то* $\mathrm{res} = 0$ *(так как $H^\bullet(H, A) = 0$), и тогда мы (достаточно внезапно) имеем*

$$|G| \cdot \widehat{H}^q(G, A) = 0,$$

что говорит нам, что для конечных групп группы Тейта периодичны. Или же, что всякий коцикл, умноженный на порядок группы является кограницей.

Теперь поговорим про Силовские подгруппы. Пусть p — простое число, S — Силовская p-подгруппа в G.

Следствие 49. *Отображение ограничения $\widehat{H}^q(G, A) \xrightarrow{\mathrm{res}} H^q(S, A)$ — мономорфизм на p-примарной компоненте $\widehat{H}^q(G, A)$.*

Доказательство. Пусть $|G| = p^\alpha m$, $(p^\alpha, m) = 1$ и пусть x лежит в p-примарной компоненте $\widehat{H}^q(G, A)$. Предположим, что $\mathrm{res}(x) = 0$. Тогда

$$0 = \mathrm{cores} \circ \mathrm{res}(x) = [G : S] \cdot x$$

Таким робразом, $p^\alpha x = 0$ и $mx = 0$, а так как $(p^\alpha, m) = 1$, отсюда мы имеем, что $x = 0$. □

Следствие 50. *Отображение $\widehat{H}^q \xrightarrow{\bigoplus \mathrm{res}_{G/S_p}} \bigoplus_p \widehat{H}^q(S_p, A)$ — мономорфизм (тут S_p пробегает все Силовские p-подгруппы).*

3.12 Теорема Гильберта-90

Пусть L/F — конечное расширение Галуа. Тогда $G = \mathrm{Gal}(L/F)$ действует на L и L^* наделяется структурой G-модуля (как и L^+).

Теорема 120 (Hilbert-90)**.** *Пусть L/F — конечное расширение Галуа. Тогда $H^1(G, L^*) = 0$.*

Перед тем как доказывать эту теорему, сформулируем лемму Артина о линейной независимости характеров, которая поможет нам при доказательстве.

Лемма 74 (Артин)**.** Пусть K — поле H – группа, а $\chi_1, \ldots, \chi_n \colon H \to K^*$ — попарно-различные характеры. Пусть $a_1, \ldots, a_n \in K$ таковы, что

$$a_1\chi_1 + \ldots + a_n\chi_n = 0.$$

Тогда $a_1 = \ldots = a_n$.

Доказательство теоремы Гильберта-90. Рассмотрим $f \in \mathbb{Z}^1(G, L^*)$ и рассмотрим

$$\sum_{\sigma \in G} f(\sigma) \cdot \sigma.$$

Это какая-то линейная комбинация попарно-различных характеров. Значит, по лемме Артина о независимости характеров найдётся $c \in L^*$ такое, что

$$b = \sum_{\sigma \in G} f(\sigma) \cdot \sigma(c) \neq 0.$$

Применим к этому равенству действие какого-то $\tau \in G$ и воспользуемся тем, что так как f — это 1 коцикл (т.е. скрученный гомоморфизм), $f(\tau\sigma) = f(\tau) \cdot \tau f(\sigma)$. Тогда

$$\tau(b) = \sum_{\sigma \in G} (\tau f(\sigma))(\tau\sigma(c)) = \sum_{x \in G} (f^{-1}(\tau) f(\tau\sigma)) \cdot \tau\sigma(c) = f^{-1}(\tau) \sum_{\eta \in G} f(\eta)\eta(c) = f^{-1}(\tau) b.$$

Таким образом, $f(\tau) = \frac{b}{\tau(b)}$, то есть f является 1-кограницей и когомологии тривиальны. □

Замечание. Исторически Гильберт доказал это только для циклических расширений (пользуясь тем, что все элементы это степени какого-то одного), а именно эту версию доказала Эмми Нётер. Но, стоит отметить, что доказательство проходит абсолютно такое же. Гильберт предпочитал понимать эту теорему в такой формулировке: если $x \in L^*$ таков, что $Nx = 1$, то существует $b \in L^*$ такой, что $x = \frac{b}{\sigma(b)}$, где σ — образующая группы Галуа (у него группа Галуа была циклической).

Вообще говоря, в случае конечных полей эту теорему можно доказать и элементарным способом:

Пусть L/F — конечное расширение, $|F| = q = p^k$, $|L| = q^n$. Тогда у нас есть короткая точная последовательность

$$1 \to \operatorname{Ker} N \to L^* \to \operatorname{Im} N \to 1,$$

откуда мы имеем

$$|L^*| = |\operatorname{Im} N| \cdot |\operatorname{Ker} N| \implies |\operatorname{Im} N| = \frac{q^n - 1}{|\operatorname{Ker} N|}$$

$$Nx = \prod_{\sigma \in \mathrm{Gal}(L/F)} \sigma x = \prod_{i=0}^{n-1} \sigma^i(x) = x^{1+q+\ldots+q^{n-1}}.$$

Возьмём $x \in \operatorname{Ker} N$, тогда у нас есть уравнение

$$x^{1+q+\ldots+q^{n-1}} = 1.$$

Количество корней этого уравнения не превосходит $1 + q + \ldots + q^{n-1} = \frac{q^n-1}{q-1}$, откуда

$$|\operatorname{Ker} N| \le \frac{q^n - 1}{q - 1}.$$

Отсюда мы получаем неравенство

$$|\operatorname{Im} N| \ge q - 1 \implies |\operatorname{Im} N| = F^*.$$

4. Применения когомологий групп к теории чисел

4.1 Вычисление $H^2(G, L^*)$

Пусть K — локальное поле, L — конечное расширение Галуа с группой Галуа $G = \mathrm{Gal}(L/K)$. Тогда, как мы помним, по теореме Гильберта-90:

$$H^1(G, L^*) = 0.$$

Вычислим $H^2(G, L^*) \cong \widehat{H}^2(G, L^*)$. Рассмотрим сначала случай неразветвлённого расширения (так как он проще).

Случай неразветвлённого расширения

Как мы помним, в этом случае группа Галуа циклическая, а тогда по 2-периодичности когомологий циклической группы достаточно посчитать $\widehat{H}^0(G, L^*)$. По определению,

$$\widehat{H}^0(G, L^*) = (L^*)^G / NL^* \cong K^*/NL^*,$$

так как просто по определению группы Галуа $(L^*)^G = K^*$. Как мы видели в параграфе про теорему Гильберта-90, в случае конечных полей такой фактор тривиален. Но, вообще говоря это не всегда так.

Таким образом, в случае неразветвлённого расширения мы имеем $H^2(G, L^*) \cong K^*/NL^*$.

Вспомним, что у нас есть такие фильтрации на кольцах $\mathcal{O}_K$ и $\mathcal{O}_L$:

$$\mathcal{O}_K = U_K = U_{K,0} \supset U_{K,1} \supset U_{K,0} \supset \ldots$$

и аналогично для $\mathcal{O}_L = U_L$, где

$$U_{L,i} = \{x \in L \mid v_L(x - 1) \ge 1\} = \{1 + \pi_L^i y \,|y \in \mathcal{O}_L\} = 1 + \mathfrak{m}_L^i.$$

Так как расширение неразветвлено, $\pi_K = \pi_L \implies \mathfrak{m}_L = \mathfrak{m}_K$. Кроме того, мы вычисляли факторы фильтрации

$$U_{L,i}/U_{L,i+1} \cong \begin{cases} \ell^*, & i = 0 \\ \ell^+, & i \geq 1 \end{cases}.$$

Рассмотрим вот такие коммутативные диаграммы:

$$i \geq 0: \qquad \begin{array}{ccc} U_{L,i}/U_{L,i+1} & \xrightarrow{\sim} & \ell^+ \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ U_{K,i}/U_{K,i+1} & \xrightarrow[\sim]{} & \Bbbk^+ \end{array} \qquad\qquad i = 0: \qquad \begin{array}{ccc} U_{L,0}/U_{L,1} & \xrightarrow{\sim} & \ell^* \\ \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} \\ U_{K,0}/U_{K,1} & \xrightarrow[\sim]{} & \Bbbk^* \end{array}$$

В них обоих правый столбец сюръективен, а значит, левый тоже. Значит, для $x \in U_k$ можно найти $y \in U_L$ и $x_1 \in U_{K,1}$ такие, что $x = x_1 \cdot Ny$. Продолжая в том же духе, для x_1 мы находим $y_1 \in U_{L,1}$ и $x_2 \in U_{K,2}$ такие, что $x_1 = x_2 \cdot Ny$. Соответственно, для x_m мы найдём $y_m \in U_{L,m}$ и $x_{m+1} \in U_{K,m+1}$ такие, что $x_m = x_{m+1} \cdot Ny_m$.

Заметим, что так как $x_m \in U_K^m$, $x_m \xrightarrow{m\to\infty} 1$. Значит, произведение

$$\prod_{m=1}^{n} x_m$$

сходится и мы можем перемножить выписанные соотношения на x_i и y_j. Перемножая их, мы получаем

$$x = \mathrm{N}(y_1 y_2 \ldots) \implies \widehat{H}^2(G, U_L) = \widehat{H}^0(G, U_L) = U_k/NU_L = 0.$$

Соответственно, отсюда следует, что

$$\widehat{H}^2(G, U_L) = \widehat{H}^0(G, U_L) = U_K/NU_L = 0.$$

Пусть $n = [L : K]$. Заметим, что тогда у нас есть изоморфизм

$$K^*/NL^* \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto \upsilon_K(x).$$

Сначала заметим, что это отображение корректно определено. Действительно, это следует из формулы

$$\upsilon_L(X) = \frac{\upsilon_K(Nx)}{n} \implies \upsilon_K(Nx) \vdots n.$$

Проверим, что оно сюръективно. Пусть $\upsilon_K(x) = ns$. Тогда

$$\upsilon_K\Big(\frac{x}{\pi^{ns}}\Big) = 0 \implies \frac{x}{\pi^{ns}} \in U_k \implies \frac{x}{\pi^{ns}} \in Ny,$$

где $y \in U_L$ (в последнем переходе мы воспользовались как раз тем, что $H^0(G, U_L) = 0$). Так вот, тогда, так как $\pi^{ns} = N(\pi^s)$, мы получаем $x = N(\pi^s y)$.

Таким образом, мы доказали, что $\widehat{H}^2(G, L^*) \cong \mathbb{Z}/n\mathbb{Z}$.

Дабы не потерять, сформулируем это, как отдельный результат:

Теорема 121. *Пусть L/K — конечное неразветвлённое расширение локального поля с группой Галуа $G = \mathrm{Gal}(L/K)$. Тогда $H^2(G, L^*) \cong \mathbb{Z}/n\mathbb{Z}$.*

Вообще говоря, для общего развития отметим, что это можно доказать и чисто гомологическими методами в два шага.

Шаг 1. Покажем, что $\widehat{H}^1(G, U_L) = 0$.

Рассмотрим короткую точную последовательность

$$1 \to U_{L,i+1} \to U_{L,i} \to U_{L,i}/U_{L,i+1} \to 1.$$

Поскольку $H^1(G, U_{L,0}/U_{L,1}) = H^1(G, \ell^*) = 0$ по теореме Гильберта-90, а $H^1(G, U_{L,i}/U_{L,i+1}) = 0$, так как ℓ^+ — индуцированный модуль Добавить про это комментарий выше под теоремой Гильберта-90!!!, из длинной точной последовательности пары мы получаем, что для любого коцикла $\varphi \in Z^1(G, U_L)$ найдётся $u \in U_L$ и $\varphi_1 \in Z^1(G, U_L)$ такие, что

$$\varphi(\sigma) = \frac{\sigma u}{u}\varphi_1(\sigma).$$

Дальнейшие действия вполне ясны:

$$\begin{cases} \varphi_1(\sigma) = \frac{\sigma u}{u}\varphi_1(\sigma) \\ \vdots \\ \varphi_m(\sigma) = \frac{\sigma u_m}{u_m}\varphi_{m+1}(\sigma) \\ \vdots \end{cases} \quad \Longrightarrow \quad \varphi(\sigma) = \frac{\sigma(uu_1\ldots)}{uu_1u_2\ldots}$$

так как $\varphi_m(\sigma) \in U_{L,m}$ и отсюда $\varphi_m(\sigma) \xrightarrow{m\to\infty} 1$.

Таким образом, мы показали, что наш коцикл является кограницей и отсюда заключаем, что $\widetilde{H}^1(G, U_L) \cong 0$.

Шаг 2. У нас есть короткая точная последовательность

$$1 \to U_L \to L^* \xrightarrow{v_L} \mathbb{Z} \to 0.$$

Она индуцирует длинную точную последовательность когомологий:

$$\begin{array}{ccccccccc} \ldots & \longrightarrow & \widehat{H}^0(G, U_L) & \longrightarrow & \widehat{H}^0(G, L^*) & \xrightarrow{\sim} & \widehat{H}^0(G, \mathbb{Z}) & \longrightarrow & \widehat{H}^1(G, U_L) & \longrightarrow & \widehat{H}^1(G, L^*) & \longrightarrow & \ldots \\ & & \| & & & & \| & & \| & & \| & & \\ & & 0 & & & & \mathbb{Z}/n\mathbb{Z} & & 0 & & 0 & & \end{array}$$

Ясно, что $\widehat{H}^0(G, \mathbb{Z}) \cong \mathbb{Z}^G/N_{\mathbb{Z}}\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$, так как $Na = |G|a$ (так как действие тривиальное), а $\mathbb{Z}^G = \mathbb{Z}$.

Тогда отсюда мы получаем, что $\widehat{H}^0(G, \mathbb{Z}) \cong \widehat{H}^0(G, L^*)$, а дальше нужно вновь воспользоваться сдвигом размерности.

Порядок группы $H^2(G, L^*)$ для циклического расширения

Начнем с такого технического результата:

Предложение 82. *Пусть L/K — конечное расширение Галуа локального поля с группой Галуа $G = \mathrm{Gal}(L/K)$. Тогда существует такой G-подмодуль модуля U_L, что*

- $|U_L/V| < \infty$.
- $\forall q \geq 1 \quad \widehat{H}^q(G, V) = 0$.

Доказательство. Вспомним теорему о нормальном базисе: если L/K — расширение Галуа, то существует такой $\alpha \in L$, что $\{\sigma\alpha\}_{\sigma\in G}$ — базис L/K. Не умаляя общности, можно полагать, что $\alpha \in \mathcal{O}_L$. Рассмотрим G-модуль

$$A = \sum_{\sigma\in G} \mathcal{O}_K \cdot \sigma\alpha \subset \mathcal{O}_L.$$

Так как $\mathcal{O}_L = \omega_1\mathcal{O}_K \oplus \ldots \oplus \omega_n\mathcal{O}_K$ и $\forall i\ \exists N_i\colon \pi_i^N\omega_i \in A$, существует N такое, что $\pi^N\mathcal{O}_L \subset A$. Обозначим $M = \pi^{N+1}A$, тогда

$$M \cdot M = \pi^{2N+2}A \cdot A \subset \pi^{2N+2}\mathcal{O}_L \subset \pi^{N+2}A = \pi M$$

Положим $V = 1 + M \subset U_L$. Заметим, что

$$(1 + m_1)(1 + m_2) = 1 + m_1 + m_2 + m_1m_2 \in 1 + M,$$

и, кроме того, V замкнут относительно взятия обратного.

$$V = 1 + \pi^{N+1}A \supset 1 + \pi^{2N+1}\mathcal{O}_L \implies V \subset U_{L,2N+1}$$
$$\frac{U_L}{U_{L,2N+1}} = \frac{U_L}{V} \cdot \frac{V}{U_{L,2N+1}},$$

а так как $|U_L/U_{L,2N+1}| < \infty$, отсюда мы получаем, что $|U_L/V| < \infty$.

Тривиальность перывх когомологий с коэффициентами в U_L устанавливается таким образом при помощи теоремы о нормальном базисе (которую мы вспоминали в начале доказательства)

$$V_i = 1 + \pi^i M, \quad V = V_0 \supset V_1 \supset V_2 \supset \ldots,$$
$$V_i/V_{i+1} \cong M/\pi M \cong \pi^{N+1}A/\pi^{N+2}A \cong A/\pi A = \sum \Bbbk \cdot \sigma\alpha = \Bbbk[G],$$

то есть это индуцированный модуль. Далее нужно действовать полностью аналогично шагу 1 гомологического доказательства теоремы 121. Таким образом, $\forall q \geq 1\ \widehat{H}^q(G, V) = 0$. □

Пусть теперь L/K — циклическое расширение локального поля с группой Галуа G. Попробуем при помощи доказанного выше предложения понять что-то про порядок группы $H^2(G, L^*)$.

Рассмотрим короткую точную последовательность

$$1 \to V \to U_L \to U_L/V \to 1.$$

Тогда, так как $|U_L/V| < \infty$, по следствию 46 мы имеем $h(U/V) = 1$. С другой стороны, так как $\widehat{H}^q(G, V) = 0$, $h(V) = 1$. Тогда из короткой точной последовательности выше, пользуясь леммой 79 мы заключаем, что $h(U_L) = 1$, что означает, что

$$|\widehat{H}^0(G, U_L)| = |\widehat{H}^1(G, U_L)|.$$

Рассмотрим теперь другую короткую точную последовательность

$$1 \to U_L \to L^* \xrightarrow{\upsilon_L} \mathbb{Z} \to 0$$

Как мы уже отмечали выше, $\widehat{H}^0(G, \mathbb{Z})$, а $\widehat{H}^1(G, \mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Z}) = 0$, так как группа G конечная. Соответственно,

$$h(\mathbb{Z}) = \frac{|\widehat{H}^0(G, \mathbb{Z})|}{|\widehat{H}^1(G, \mathbb{Z})|} = \frac{|\mathbb{Z}/n\mathbb{Z}|}{|\mathrm{Hom}_{\mathsf{Grp}}(G, \mathbb{Z})|} = \frac{n}{1} = n.$$

Тогда из точной последовательности выше по лемме 79 мы получаем, что

$$h(L^*) = h(U_L) \cdot h(\mathbb{Z}) = 1 \cdot n = n.$$

С другой стороны, пользуясь периодичность когомологий Тейта для циклической группы

$$h(L^*) = \frac{|\widehat{H}^0(G, L^*)|}{|\widehat{H}^1(G, L^*)|} = \frac{|\widehat{H}^2(G, L^*)|}{1} = |\widehat{H}^2(G, L^*)|$$

Таким образом, мы доказали такую теорему.

Теорема 122. *Пусть L/K — циклическое расширение локального поля K степени n с группой Галуа $G = \mathrm{Gal}(L/K)$. Тогда $|\widehat{H}^2(G, L^*)| = n$.*

Теперь докажем частный случай известно «неприятной леммы», которая понадобится нам в дальнейшем.

Лемма 75 (Ugly lemma)**.** Пусть G — конечная группа, $A \in G\text{-Mod}$ и выполнены следующие условия

1. Для любой подгруппы $H \leq G$ тривиальны первые когомологии $H^1(H, A) = 0$.
2. Если $H \leq K$ — нормальная подгруппа в подгруппе $K \leq G$ и $|K/H| = p$ (где p — простое), то

$$|H^2(K/H, A^H)| \mid p.$$

Тогда $|H^2(G, A)| \mid |G|$.

Доказательство. **Шаг 1.** Предположим, что G — это p-группа. Будем вести индукцию по $|G|$.
База. Случай $|G| = 1$ очевиден.
Переход. В G существует нормальная подгруппа H индекса p. По индукционному предположению $|H| \vdots |H^2(H, A)|$. Запишем точную последовательность для ограничения и инфляции:

$$0 \to H^2(G/H, A^H) \xrightarrow{\inf} H^2(G, A) \xrightarrow{\text{res}} H^2(H, A)$$

Соответственно, из неё мы заключаем, что

$$\begin{cases} p = |G/H| \vdots |H^2(G/H, A^H)| \text{ (по условию теоремы)} \\ |H| \vdots |H^2(H, A)| \end{cases} \implies |G| \vdots |H^2(G, A)|.$$

Шаг 2. Теперь рассмотрим общий случай. Как мы помним из следствия 50, отображение

$$\widehat{H}^q(G, A) \xrightarrow{\bigoplus \text{res}_{G/S_p}} \bigoplus_p \widehat{H}^q(S_p, A)$$

является мономорфизмом. Отсюда мы заключаем, что

$$\left| \bigoplus_p \widehat{H}^2(S_p, A) \right| \vdots |H^2(G, A)|.$$

С другой стороны, по первому пункту мы знаем, что $|S_p| \vdots |\widehat{H}^2(S_p, A)|$, откуда

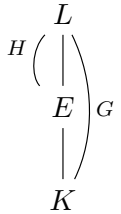
$$|G| = \prod_p |S_p| \vdots \prod_p |\widehat{H}^2(S_p, A)| \vdots |H^2(G, A)|,$$

чего мы собственно и хотели.

□

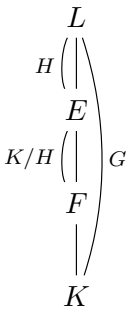
Теперь применим эту замечательную "неприятную"лемму в нашем контексте. Пусть $G = \text{Gal}(L/K)$, $A = L^*$.

1. По соответствию Галуа, любой подгруппе $H \leq G$ соответствует $E/K,\ E \subset L$, причём $\text{Gal}(L/E) = H$.



По теореме Гильберта-90 $H^1(H, L^*) = 0$. Это гарантирует нам выполнение первого условия неприятной леммы.

2. Теперь, второму условию в неприятной лемме соответствует такая башня полей:



Соответственно, по определению группы Галуа: $A^H = (L^*)^H = E^*$ и тогда соответственно

$$H^2(K/H, A^H) \cong H^2(K/H, E^*) \cong H^2(\mathrm{Gal}(E/F), E^*).$$

Так как группа Галуа $\mathrm{Gal}(E/F)$ циклическая, по доказанному ранее (см. 114)

$$p = |\mathrm{Gal}(E/F)| \vdots |H^2(K/H, A^H)|.$$

Тогда по неприятной лемме мы получаем, что

$$|G| \vdots |H^2(G, A)|.$$

Итого, мы доказали такую теорему

Теорема 123. *Пусть L/K — конечное расширение локального поля K с группой Галуа $G = \mathrm{Gal}(L/K)$. Тогда*

$$|G| = [L : K] \vdots |H^2(G, L^*)|.$$

Группа $H^2(G, L^*)$ в общем случае для локального поля

Рассмотрим короткую точную последовательность G-модулей с тривиальным действием

$$0 \to \mathbb{Z} \hookrightarrow \mathbb{Q} \twoheadrightarrow \mathbb{Q}/\mathbb{Z} \to 0$$

Она индуцирует длинную точную последовательность когомологий

$$\ldots \widehat{H}^{q-1}(G, \mathbb{Q}/\mathbb{Z}) \to \widehat{H}^q(G, \mathbb{Z}) \to \widehat{H}^q(G, \mathbb{Q}) \to \widehat{H}^q(G, \mathbb{Q}/\mathbb{Z}) \to \widehat{H}^{q+1}(G, \mathbb{Z}) \to \ldots$$

Заметим, что умножение на $|G|$ индуцирует изоморфизм $\mathbb{Q} \xrightarrow{\sim} \mathbb{Q}$, а он индуцирует отображение

$$\widehat{H}^q(G, \mathbb{Q}) \xrightarrow[\cdot|G|]{\sim} \widehat{H}^q(G, \mathbb{Q})$$

. С другой стороны, мы знаем, что $|G| \cdot \widehat{H}^q(G, \mathbb{Q}) = 0$. Отсюда мы заключаем, что

$$\widehat{H}^q(G, \mathbb{Q}) = 0.$$

Тогда из длинной точной последовательности пары выше мы видим, что

$$\widehat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \cong \widehat{H}^2(G, \mathbb{Z}).$$

Посмотрим внимательнее на группу $H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}^1(G, \mathbb{Q}/\mathbb{Z})/B^1(G, \mathbb{Q}/\mathbb{Z})$. Как мы помним, кограницы — это функции $\varphi\colon G \to \mathbb{Q}/\mathbb{Z}$, для которых существует $a \in \mathbb{Q}/\mathbb{Z}$ такой, что $\varphi(g) = ga - a$. Но, так как действие тривиально, $\varphi(g) = ga - a = a - a = 0$, откуда $B^1(G, \mathbb{Q}/\mathbb{Z}) = 0$. Кроме того, $\mathbb{Z}^1(G, \mathbb{Q}/\mathbb{Z})$ — это скрученные гомоморфизмы $\varphi\colon G \to \mathbb{Q}/\mathbb{Z}$, т.е. отображения вида

$$\varphi(g_1 g_2) = g_1\varphi(g_2) + \varphi(g_1) = \varphi(g_2) + \varphi(g_1),$$

так как действие тривиально. Соответственно, $Z^1(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathsf{Grp}}(G, \mathbb{Q}/\mathbb{Z})$. Значит,

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

Соответственно, мы получили, что

$$H^2(G, \mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

Пример 62. Пусть $G = \langle\sigma\rangle$ — циклическая группа. Пусть $|G| = m$. Рассмотрим отображение

$$\sigma \mapsto \frac{1}{m}$$

индуцирует изоморфизм $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \frac{1}{m}\mathbb{Z}/\mathbb{Z}$.

Пусть теперь L/K — неразветвлённое расширение локального поля K. Тогда

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/\Bbbk)$$

и, если $|\Bbbk| = q$, то группа $\mathrm{Gal}(\ell/\Bbbk$ порождена автоморфизмом Фробениуса

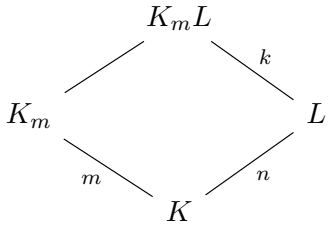
$$\mathrm{Fr}_q \colon \ell \to \ell,\ \mathrm{Fr}_q(x) = x^q.$$

При изоморфизме этот автоморфизм переходит в некоторый элемент $F \in \mathrm{Gal}(L/K)$, причем такой, что

$$F(x) \equiv x^q \pmod{\mathfrak{m}_L} \text{ для } x \in \mathcal{O}_L.$$

Допуская волность речи, этот элемент мы также будем называть автоморфизмом Фробениуса.

Теперь пусть L/K — расширение Галуа локального поля K степени $[L : K] = |G| = n$. Рассмотрим K_m/K — неразветвлённое расширение поля K степени m. Рассмотрим композит расширений

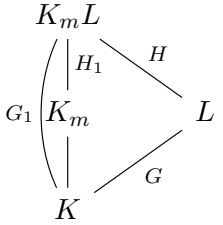


Тогда у нас есть вот такая коммутативная диаграмма:

$$\begin{array}{ccccccc}
H^2(\mathrm{Gal}(K_m/K), K_m^*) & \xrightarrow[\upsilon_{K_m}]{\sim} & H^2(\mathrm{Gal}(K_m/K), \mathbb{Z}) & \xrightarrow{\sim} & \mathrm{Hom}(\mathrm{Gal}(K_m/K), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\sim} & \frac{1}{m}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{res}\circ\mathrm{inf}} & & \downarrow{\scriptstyle e\cdot\mathrm{res}} & & \downarrow{\scriptstyle e\cdot\mathrm{res}} & & \downarrow{\scriptstyle \cdot n} \\
H^2(\mathrm{Gal}(K_mL/K), (K_mL)^*) & \xrightarrow[\upsilon_{K_mL}]{\sim} & H^2(\mathrm{Gal}(K_mL/L), \mathbb{Z}) & \xrightarrow{\sim} & \mathrm{Hom}(\mathrm{Gal}(K_mL/L), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\sim} & \frac{1}{k}\mathbb{Z}/\mathbb{Z}
\end{array}$$

Поясним, что на ней вообще происходит.

- Первое вертикальное отображение происходит из точной последовательности для ограничения и инфляции. Если конкретнее, то у нас есть такая башня:



И из неё мы получаем отображение

$$H^2(G_1/H_1, K_m^*) \xrightarrow{\mathrm{inf}} H^2(G_1, (K_mL)^*) \xrightarrow{\mathrm{res}} H^2(H_2, (K_mL)^*)$$

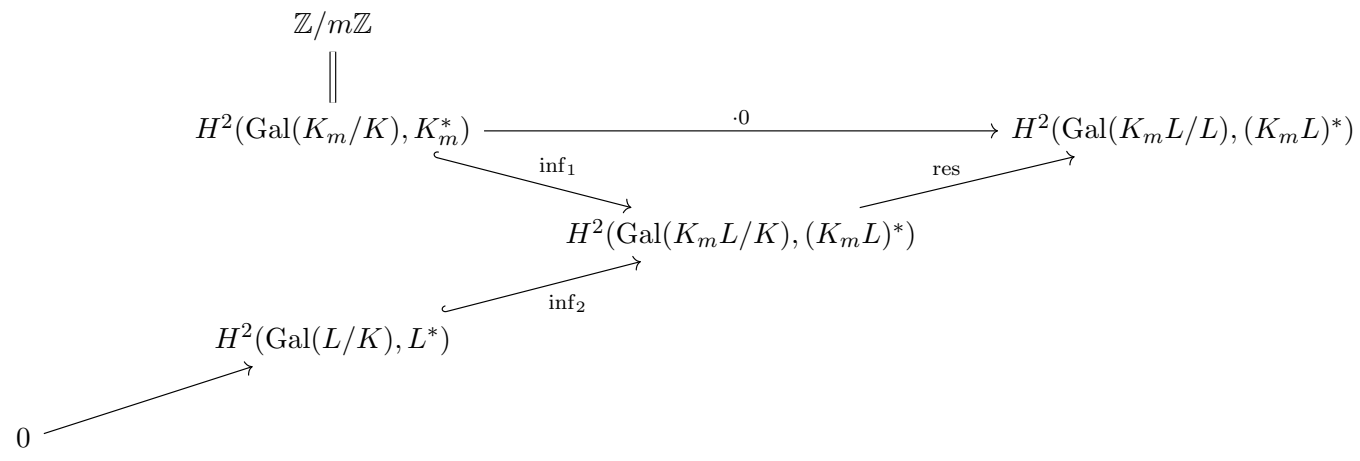
И в качестве стрелки мы берём сквозное отображение.

- Вторую вертикальную стрелку мы на самом деле уже видели. А именно, у нас есть кроткая точная последовательность
$$1 \to U_{K_m} \to K_m^* \xrightarrow{\upsilon_{K_m}} \to \mathbb{Z} \to 0,$$
а так как (как мы видели в вычислении для неразветвлённого расширения) $\widehat{H}^1(\mathrm{Gal}(K_m/K), U_{K_m}) = 0$, мы получаем изоморфизм $\widehat{H}^2(\mathrm{Gal}(K_m/K), K_m^*) \cong \widehat{H}^2(\mathrm{Gal}(K_m/K), \mathbb{Z})$.
Аналогично и для нижнего куска диаграммы, так как мы доказывали, что если расширение K_m/K неразветвлено и является подрасширением в L, то K_mL/L неразветвлено.
- Третья вертикальная стрелка получается из обсуждённого только что изоморфизма
$$H^2(G, \mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$
- Четвёртая вертикальная стрелка также получается из рассуждения выше про $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ для циклической группы (а тут она именно такова, так как расширение неразветвлено).

Поясним теперь, почему эта диаграмма коммутативная.
Пусть $e = e(L/K)$. Коммутативность левого квадрата следует из того, что
$$\forall x \in K_m^* \quad e \cdot \upsilon_{K_m}(x) = \upsilon_{K_mL}(x),$$
так как $e(K_mL/K_m) = e(L/K)$. Соответственно, в частности для 2 коциклов выполнено
$$e\upsilon_{K_m}(f(\sigma_1, \sigma_2)) = \upsilon_{K_mL}(f(\sigma_1, \sigma_2)).$$

Коммутативность второго квадрата следует из согласованности ограничения с длинной точной последовательностью. Коммутативность третьего квадрата следует из того, что
$$n\varphi(F_K) = e \cdot \varphi(F_L),$$
где F_K — автоморфизм Фробениуса. Это в свою очередь равносильно тому, что $f(L/K) \cdot \varphi(F_k) = \varphi(F_L)$ (так как $n = ef$), а это выполнено так как $F_L = F_K^f$, где.

Возьмём теперь $m = n$. В этом случае правое отображение будет нулевым, откуда крайнее левое — тоже. В то же время, в силу теоремы Гильберта-90 последовательность 2-х когомологий для ограничения и инфляции точна
$$0 \to H^2(\mathrm{Gal}(L/K), L^*) \xrightarrow{\mathrm{inf}_2} H^2(\mathrm{Gal}(K_mL/K), (K_mL)^*) \xrightarrow{\mathrm{res}} H^2(\mathrm{Gal}(K_mL/L), (K_mL)^*)$$
(и заметим, что тут имеется в виду другое отображение инфляции между другими группами!).
Соответственно, мы получаем вот такую коммутативную диаграмму:



Из этой диаграммы мы получаем, что $\mathbb{Z}/m\mathbb{Z} \hookrightarrow H^2(\mathrm{Gal}(L/K), L^*)$.. С другой стороны, из неприятной леммы мы знаем, что $m = n : |H^2(\mathrm{Gal}(L/K), L^*)|$, откуда

$$H^2(G, L^*) \cong \mathbb{Z}/m\mathbb{Z}.$$

Итак, мы наконец доказали вот такую теорему:

Теорема 124. *Пусть L/K — конечное расширение Галуа локального поля K степени n с группой Галуа $\mathrm{Gal}(L/K) = G$. Тогда*

$$H^2(G, L^*) = \mathbb{Z}/n\mathbb{Z}.$$

4.2 Группа Брауэра

Этот параграф будет добавлен после девятой и десятой лекций.

4.3 Когомологически тривиальные модули и теорема Тейта

Пусть L/K — расширение Галуа с группой Галуа G, $H \subset G$. Сейчас мы построим следующую коммутативную диаграмму (слева она, справа её когомологическая интерпретация):

$$\begin{array}{ccc} H/[H,H] & \xrightarrow{\sim} & F^*/N_{L/F}L^* \\ \downarrow & & \downarrow N \\ G/[G,G] & \xrightarrow{\sim} & K^*/N_{L/K}L^* \end{array} \quad \rightsquigarrow \quad \begin{array}{ccc} \widehat{H}^{-2}(H;\mathbb{Z}) & \xrightarrow{\sim} & \widehat{H^0}(H;L^*) \\ \downarrow \mathrm{cores} & & \downarrow \mathrm{cores} \\ \widehat{H}^{-2}(G;\mathbb{Z}) & \xrightarrow{\sim} & \widehat{H^0}(G;L^*) \end{array}$$

Для этого нам понадобится следующее понятие:

Определение 150. Пусть G — конечная группа, $A \in G\text{-Mod}$. A называется *когомологически тривиальным*, если $\forall H \subset F,\ \forall n \in \mathbb{Z}\ \widehat{H}^n(H, A) = 0$.

Предложение 83. *Пусть $\exists n \geq 0 \colon \forall H \subset G\ \widehat{H}^n(H;A) = \widehat{H}^{n+1}(H;A) = 0$. Тогда модуль A когомологически тривиален.*

Доказательство. **Шаг 1:** докажем это утверждение, когда G — p-группа.

Будем вести индукцию по $|G|$, база очевидна.

Выберем нормальную подгруппу H индекса p. Так как $|H| \leq |G|$, по индукционному предположению A является когомологически тривиальным H-модулем.

Рассмотрим сначала отдельно случай, когда $n \geq 0$. Тогда (в силу того, что $H^1(H, A) = \ldots = H^{n-1}(H, A) = 0$) мы можем записать точную последовательность для ограничения и инфляции:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^n(G/H; A^H) & \xrightarrow{\inf} & H^n(G;A) & \xrightarrow{\mathrm{res}} & H^n(H,A) \\ & & & & \| & & \| \\ & & & & 0 & & 0 \end{array}$$

из которой мы заключаем, что $H^n(G/H, A^H) = 0$. Аналогично мы понимаем, что $H^{n+1}(G/H, A^H) = 0$

Группа G/H циклическая, а значит, в силу периодичности, из того, что зануляются две соседних группы когомологий следует, что зануляются все группы когомологий, то есть $\widehat{H}^i(G/H, A^H) = 0$, то есть A^H — когомологически тривиальный G/H-модуль (так как G/H — циклическая группа порядка p и нетривиальных подгрупп у неё просто нет).

Теперь пусть $n = 0$. Тогда

$$\widehat{H}^0(G/H; A^H) = (A^H)^{G/H}/N_{G/H}A^H.$$

С другой стороны, мы знаем, что $0 = \widehat{H}^0(G; A) = A^G/N_G A$, и, кроме того, выполнено равенство $(A^H)^{G/H} = A^G$. Кроме того, $N_{G/H} A^H \supset N_G A$, так как

$$G = \bigsqcup \sigma_i H \implies Na = \sum_{g \in G} ga = \sum_{\sigma_i \in G/H} \sigma_i \underbrace{\left(\sum_{h \in H} (ha) \right)}_{\in A^H},$$

откуда одна группа — фактор другой, откуда $\widehat{H}^0(G/H; A^H) = 0$, то есть A^H — когомологически тривиальный G/H-модуль.

Осталось доказать, что что $\widehat{H}^i(G; A) = 0 \; \forall i$.

В случае $i \geq 1$ мы получаем это из точной последовательности для ограничения и инфляции:

$$\begin{array}{ccccc} 0 & \longrightarrow & \widehat{H}^i(G/H; A^H) & \xrightarrow{\inf} & \widehat{H}^i(G; A) \xrightarrow{\text{res}} \widehat{H}^i(H; A) \\ & & \| & & \| \\ & & 0 & & 0 \end{array},$$

так как выше мы показали, что A^H — когомологически тривиальный G/H-модуль, а по индукционному предположению A — когомологически тривиальный H-модуль.

Теперь разберём случай $i \leq 1$. Запишем длинную точную последовательность когомологий, связанную с короткой точной последовательностью

$$0 \to B \to A_* \to A \to 0.$$

При помощи связывающего гомоморфизма из неё мы получим $\widehat{H}^{m+1}(G, B) = \widehat{H}^m(G, A)$.

Тогда по доказанному для $i \geq 1$ мы получаем, что $H^i(G, B) = 0$. В частности, $\widehat{H}^1(G; B) = 0$, но

$$\widehat{H}^0(G, A) = \widehat{H}^1(G, B) = 0.$$

Так мы можем и дальше сдвигать размерности и получать, что

$$\widehat{H}^{-1}(G; A) = \widehat{H}^0(G; B) = 0$$

и так далее. Итак, мы полностью закончили первый шаг доказательства.

Шаг 2: пусть G — произвольная группа. Тогда мы поступим также, как и в ugly-lemma: отображение

$$\widehat{H}^i(G; A) \xrightarrow{\bigoplus \text{res}} \bigoplus_p \widehat{H}^i(G_p; A)$$

является мономорфизмом, а каждое слагаемое справа когомологически тривиально по первому шагу доказательства. □

Замечание. Из рассуждения со сдвигом размерности видно, что требование $n \geq 0$ в теореме не по существу.

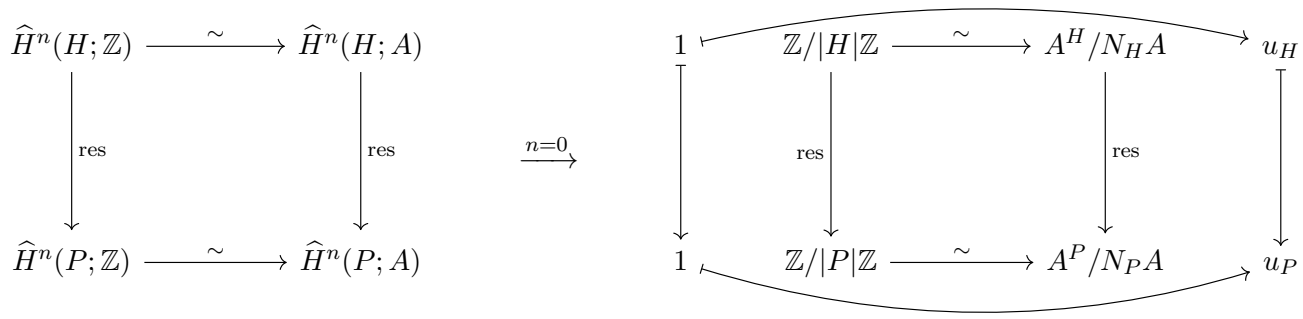
Теперь двинемся дальше. Пусть $A \in G\text{-Mod}$, зададимся следующим вопросом: *когда существует система изоморфизмов $\widehat{H}^n(H; \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^n(H; A)$, индуцированная некоторым морфизмом G-модулей $\mathbb{Z} \to A$?*

Получим необходимое условие существования такой системы для всех $H \subset G$ и $n \in \mathbb{Z}$. Предположим сначала, что

$$\widehat{H}^{-1}(H; \mathbb{Z}) \cong \widehat{H}^{-1}(H; A), \text{ но } \widehat{H}^{-1}(H; A) = \operatorname{Ker} N/\langle \sigma - 1 \rangle A,$$

Соответственно, так как $\mathbb{Z}$ — тривиальный $\mathbb{Z}$-модуль, уже $N(a) = |G|a = 0 \implies a = 0$, октуда $\operatorname{Ker} N = 0$ и группа $\widehat{H}^{-1}(H; \mathbb{Z})$ будет нулевой.

Теперь, пусть у нас есть последовательность подгрупп $P \subset H \subset G$. Тогда у нас есть соответствующая коммутативная диаграмма (и её частный случай для $n = 0$):



То есть, нам нужно, чтоб группы A^H/N_HA были цикличны и имели порядок $|H|$ для всех подгрупп $|H|$, и кроме того, существовали образующие u_H такие, что $\mathrm{res}_{H/P}(u_H) = u_P$.

Еще это условие можно переформулировать таким образом: в A^G/N_GA можно выбрать образующую u_G так, что $\mathrm{res}(u_G) = u_H$. Итого, мы получили два необходимых условия:

1. $\widehat{H}^{-1}(H, 0) = 0$.
2. В A^G/N_GA можно выбрать образующую u_G так, что $\mathrm{res}(u_G) = u_H$

Теорема 125 (Тейт)**.** *Эти условия являются достаточными.*

Доказательство. Итак, рассмотрим наш гомоморфизм, $\mathbb{Z} \to A$, он переводит 1 в прообраз u_G при факторизации.

Рассмотрим короткую точную последовательность

$$0 \to X \to A_* \oplus \mathbb{Z} \to A \to 0,$$

Покажем, что X когомологически тривиален, пользуясь предложением 83. А конкретнее, покажем, что

$$\forall H \leq G \quad \widehat{H}^0(H, X) = \widehat{H}^1(H, X) = 0.$$

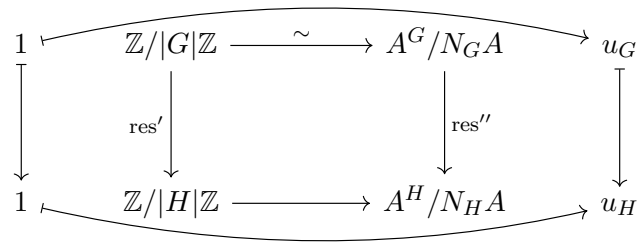
Запишем длинную точную последовательность когомологий:

$$\widehat{H}^{-1}(H; A) \longrightarrow \widehat{H}^0(H; X) \longrightarrow \widehat{H}^0(H; A_* \oplus \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^0(H; A) \xrightarrow{\delta} \widehat{H}^1(H; X) \longrightarrow \widehat{H}^1(H; A_* \oplus \mathbb{Z})$$

$$0 \longrightarrow \widehat{H}^0(H; X) \longrightarrow \mathbb{Z}/|H|\mathbb{Z} \xrightarrow{\sim} A^H/N_HA \longrightarrow \widehat{H}^1(H; X) \longrightarrow 0$$

Поясним, почему на ней всё устроено именно так.

- $H^{-1}(H, A) = 0$ по первому условию.
- $\widehat{H}^0(H, A_* \oplus \mathbb{Z}) \cong \widehat{H}^0(H, A_*) \oplus \widehat{H}^0(H,\mathbb{Z}) \cong \widehat{H}^0(H,\mathbb{Z}) \cong \mathbb{Z}/|H|\mathbb{Z}$.
- В силу условия 2 у нас есть вот такая коммутативная диаграмма:



Так как res'' сюръективен, $\mathbb{Z}/|H|\mathbb{Z} \twoheadrightarrow A^H/N_HA$, но порядок этих групп совпадает и равен $|H|$, откуда мы понимаем, что

$$\widehat{H}^0(H, A_* \oplus \mathbb{Z}) \cong \mathbb{Z}/|H|\mathbb{Z} \cong A^H/N_HA \cong \widehat{H}^0(H, A).$$

- $\widehat{H}^1(H, A_* \oplus \mathbb{Z}) \cong \widehat{H}^1(H, A_*) \oplus \widehat{H}^1(H, \mathbb{Z}) \cong \mathrm{Hom}(H, \mathbb{Z}) = 0.$

Тогда из длинной точной последовательности, написанной выше мы видим, что $\forall H \leq G \quad \widehat{H}^0(H, X) = \widehat{H}^1(H, X) = 0$, а значит, по предложению 83 X — когомологически тривиальный G-модуль. Тогда вновь из длинной точной последовательности когомологий мы получаем, что

$$\widehat{H}^n(H, A_* \oplus \mathbb{Z}) \xrightarrow{\sim} \widehat{H}^n(H, A),$$

но $\widehat{H}^n(H, A_* \oplus \mathbb{Z}) \cong \widehat{H}^n(H, \mathbb{Z})$, так что мы получили, что хотели. □

Следствие 51 (Тейт). *Пусть $A \in G - \mathsf{Mod}$. Предположим, что выполнены следующие условия*

1. *Для любой подгруппы $H \subset G$ мы имеем $H^1(H, A) = 0$.*
2. *Для любой подгруппы $H \subset G$ группа $H^2(H, A)$ — циклическая группа порядка $|H|$.*
3. *$\mathrm{res}_{H/P} u_H = u_P$ для любой подгруппы $P \subset H$.*

Тогда существует система изоморфизмов $H^n(H; A) \to H^{n-2}(H; \mathbb{Z})$, причем эти изоморфизмы согласованы с ограничениями и кограничениями, то есть, следующие диаграммы коммутативны:

$$\begin{array}{ccc} H^n(H; A) & \xrightarrow{\sim} & H^{n-2}(H; \mathbb{Z}) \\ {\scriptstyle \mathrm{res}}\downarrow \uparrow{\scriptstyle \mathrm{cor}} & & {\scriptstyle \mathrm{res}}\downarrow \uparrow{\scriptstyle \mathrm{cor}} \\ H^n(P; A) & \xrightarrow{\sim} & H^n(P; \mathbb{Z}) \end{array}$$

Доказательство. Запишем следующие короткие точные последовательности

$$0 \to A \to A^* \to A' \to 0$$

$$0 \to A' \to (A')^* \to (A')' \to 0$$

Так как модуль по центру коиндуцированный, мы получаем, что

$$H^{n-2}(H; A'') \cong H^{n-1}(H; A') \cong H^n(H; A).$$

Применяя теорему Тейта для A'' мы получаем нужное:

$$H^n(H; A) \cong \widehat{H}^{n-2}(H, (A')') \cong H^{n-2}(H; \mathbb{Z}),$$

чего мы собственно и хотели. □

Возьмём $G = \mathrm{Gal}(L/K)$, $A = L^*$, тогда как мы помним, группа $H^2(H, L^*)$ — циклическая группа порядка $|H|$, то есть условие 1 выполнено. Условие 2 следует из приведённой ранее коммутативной диаграммы для группы Брауэра. Тогда, применяя следствие, мы получаем, в частности, что

$$H^n(G; L^*) \cong H^{n-2}(G; \mathbb{Z}),$$

а в частности

$$\implies \widehat{H}^0(G; L^*) = F^*/N_{L/F}L^* \cong G/[G, G] = \widehat{H}^{-2}(G; \mathbb{Z}).$$

Следствие 52. *Пусть L/K — конечное расширение локального поля K с группой Галуа G. Тогда*

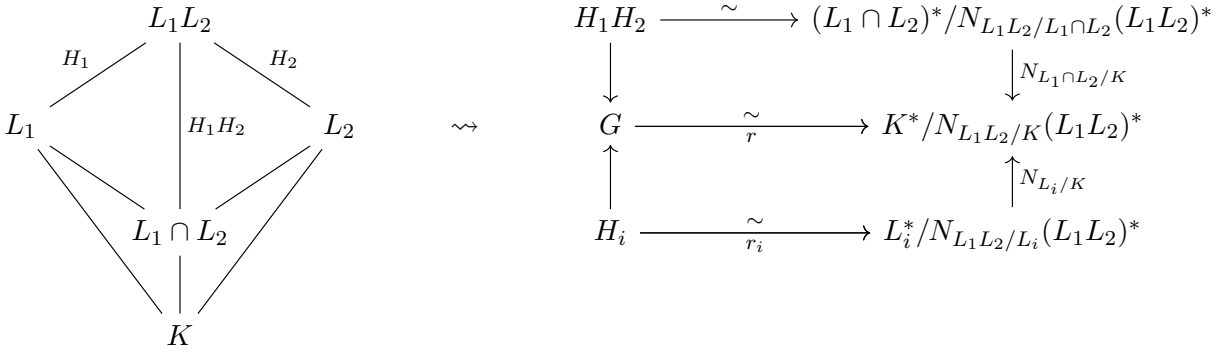
$$K^*/N_{L/K}L^* \cong G^{ab}$$

4.4 Норменные группы

Пусть L/K — расширение Галуа локального поля K с группой Галуа G.

Определение 151. Подгруппа группы K^* называется *норменной*, если существует такое конечное абелево расширение[16] L/K , что эта подгруппа в точности совпадает с $N_{L/K}L^*$.

Рассмотрим два абелевых расширения L_1 и L_2 локального поля K и их композит:



По следствию 52 в правой диаграмме горизонтальные стрелки — изоморфизмы. Тогда из коммутативности мы получаем, что

$$r(H_1H_2) = r(H_1)r(H_2) = N_{L_1/K}(L_1^*/N_{L_1L_2/L_1}(L_1L_2)^*)\cdot N_{L_2/K}(L_2^*/N_{L_1L_2/L_1}(L_1L_2)^*) = \frac{N_{L_1/K}L_1^* \cdot N_{L_2/K}L_2^*}{N_{L_1L_2/K}(L_1L_2)^*}$$

С другой стороны, мы имеем

$$r(H_1H_2) = \frac{N_{L_1\cap L_2/K}(L_1 \cap L_2)^*}{N_{L_1L_2/K}(L_1L_2)^*},$$

а тогда мы имеем равенство

$$N_{L_1\cap L_2/K}(L_1 \cap L_2)^* = N_{L_1/K}L_1^* \cdot N_{L_2/K}L_2^*.$$

С другой стороны, мы знаем, что $H_1 \cap H_2 = 1$. Тогда

$$\frac{N_{L_1L_2/K}(L_1L_2)^*}{N_{L_1L_2/K}(L_1L_2)^*} = r(1) = r(H_1 \cap H_2) = r(H_1) \cap r(H_2) = \frac{N_{L_1/K}L_1^* \cap N_{L_2/K}L_2^*}{N_{L_1L_2/K}(L_1L_2)^*},$$

откуда мы получаем равенство

$$N_{L_1L_2/K}(L_1L_2)^* = N_{L_1/K}L_1^* \cap N_{L_2/K}L_2^*.$$

Таким образом, мы показали, что пересечение и объединение норменных подгрупп — норменная подгруппа.

Что же можно сказать относительно включений? Из общей теории полей следует, что

$$L_1 \subset L_2 \implies N_{L_2/K}L_2^* \subset N_{L_1/K}L_1^*.$$

Оказывается, есть и стрелочка в обратную сторону. Её мы также получим из равенств выше. Действительно, предположим, что $N_{L_2/K}L_2^* \supset N_{L_1/K}L_1^*$, тогда

$$N_{L_1L_2/K}(L_1L_2)^* = N_{L_2/K}L_2^*,$$

а отсюда мы имеем

$$\mathrm{Gal}(L_1L_2/K) \cong K^*/N_{L_1L_2/K}(L_1L_2)^* = K^*/N_{L_2/K}L_2^* \cong \mathrm{Gal}(L_2/K).$$

Но из такого равенства групп Галуа следует, что $L_1L_2 = L_2 \Leftrightarrow L_1 \subset L_2$, что и требовалось.

[16] т.е. расширение Галуа с абелевой группой Галуа

Упражнение. Если $N_{L/K}L^* \subset S \subset K^*$, то S — норменная подгруппа.

Доказательство. Применим соответствие Галуа. Действительно, рассмотрим $\theta_{L/K}\colon K^* \to K^*/N_{L/K}L^* \cong \mathrm{Gal}(L/K)$. Рассмотрим $\theta_L/K(S)$ и поле $F = L^{\theta_L/K(S)}$. Тогда имеет место такая коммутативная диаграмма:

$$\begin{array}{ccc} L & & K^* \xrightarrow{\theta_{L/K}} \mathrm{Gal}(L/K) \\ \Big| \mathrm{Gal}(L/F)\cong\theta_{L/K}(S) & & \| \qquad\qquad \Big\downarrow \mathrm{res} \\ \mathrm{Gal}(L/K) \quad F \quad \rightsquigarrow & & \| \\ \Big| \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) & & \| \\ K & & K^* \xrightarrow{\theta_{F/K}} \mathrm{Gal}(F/K) \end{array}$$

Ну и из соответствия Галуа мы знаем, что

$$\theta_L/K(S) = \mathrm{Ker}(\mathrm{Gal}(L/K) \to \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/F) = \mathrm{Gal}(F/K)) \cong \mathrm{Gal}(L/F).$$

Но тогда мы получаем, что

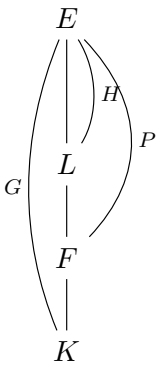
$$S = \theta^{-1}_{L/K}(\mathrm{Gal}(L/F)) = N_{F/K}F^*.$$

□

Теорема 126. *Пусть L/K — конечное сепарабельное[17] расширение[18]. Тогда $N_{L/K}L^*$ является норменной группой.*

Доказательство. Картинка у нас выглядит вот так:

где E — какое-то расширение Галуа поля K, содержащее L в качестве подрасширения, а F/K — максимальное абелево расширение K, содержащееся в L.



Докажем, что $P = H[G,G] = HG'$. Действительно, из диаграммы мы видим, что G/P абелева (так как это группа Галуа расширения F/K), откуда $G' \subset P \implies HG' \subset P$. Теперь применим соответствие Галуа:

$$HG' \leftrightarrow L \cap K_{ab},$$

где K_{ab} — максимальное абелево расширение K, содержащееся в E. Но тогда $F = L \cap K_{ab}$ (просто по определению), тогда, так как соответствие Галуа — антиэквивалентность решеток, $P = HG'$.

Теперь рассмотрим такую коммутативную диаграмму:

[17] это ограничение не по существу, но так доказывать проще (да и работаем мы в характеристике 0)

[18] не обязательно Галуа!

$$\begin{array}{ccc} L^* & \xrightarrow{\theta_{E/L}} & H/H' \cong L^*/N_{E/L}E^* \\ \Big\downarrow{\scriptstyle N_{L/F}} & & \Big\downarrow{\scriptstyle i} \\ F^* & \xrightarrow{\theta_{E/F}} & HG'/(HG')' \cong P/P' \cong F^*/N_{E/F}E^* \\ \Big\downarrow{\scriptstyle N_{F/K}} & & \Big\downarrow{\scriptstyle j} \\ K^* & \xrightarrow{\theta_{E/K}} & G/G' \cong K^*/N_{E/K}E^* \end{array}$$

где $\theta_{E/L}$ — это сюръективное сквозное отображение

$$L^* \to L^*/N_{E/L}E^* \cong H/H'.$$

Мы докажем, что $N_{L/K}L^* = N_{F/K}F^*$. Включение слева направо очевидно, а вот обратное включение — совсем не очевидно. Возьмём $x \in F^*$ и пройдёмся по верхнему коммутативному квадрату

$$\theta_{E/F}(x) = i\theta_{E/L}(y) \cdot \theta_{E/F}(u),\ \theta_{E/F}(u) \in G'/(HG')'.$$

Значит, при факторизации по G' этот элемент уйдёт в 0, то есть $j\theta_{E/F}(u) = 0$, что говорит нам, что если пройти в другом направлении, тоже получится 0, то есть

$$\theta_{E/K}\big(N_{F/K}u\big) = 0 \implies N_{F/K}u \in N_{E/K}E^*.$$

Значит, для некоторого v мы имеем $N_{F/K}u = N_{E/K}v$. Продолжим диаграммный поиск, а именно, вновь пройдём по верхнему квадрату двумя способами:

$$\theta_{E/F}(x) = i\theta_{E/L}(y) \cdot \theta_{E/F}(u) \implies \theta_{E/F}(xu^{-1}) = i\theta_{E/L}(y) = \theta_{E/F}\big(N_{L/F}y\big)$$

Отсюда мы имеем, что

$$\theta_{E/F}(xu^{-1}(N_{L/F}y)^{-1}) = 1 \implies xu^{-1}(N_{L/F}y)^{-1} = xu^{-1}N_{L/F}(y)^{-1} \in N_{E/F}E^*$$

Применим к этому равенству $N_{F/K}$ и воспользуемся тем, что $N_{L/K} = N_{F/K}N_{L/F}$, а также $N_{E/K} = N_{F/K}N_{E/F}$, получим

$$N_{F/K}x \cdot N_{F/K}u^{-1} \cdot N_{L/K}y^{-1} \in N_{E/K}E^*$$

Теперь вспомним, что в самой первой выкладке мы поняли, что $N_{F/K}u^{-1} = N_{E/K}v^{-1}$, что даёт нам

$$N_{F/K}x \cdot N_{E/K}v^{-1} \cdot N_{L/K}y^{-1} \in N_{E/K}E^*,$$

откуда мы имеем

$$N_{F/K}x \cdot N_{L/K}y^{-1} \in N_{E/K}E^*,$$

откуда мы заключаем, что $N_{F/K}x \in N_{L/K}L^*$, что и требовалось.

□

4.5 Теория Куммера

Пусть у нас некоторая подгруппа $A \subset K^*$ индекса m, то есть $|K^*/A| = m$. В таком случае $K^{*m} \subset A$. Тогда для того чтобы доказать, что A — норменная, достаточно показать, что K^{*m} — норменная.

Докажем это в случае поля K характеристики нуль. Сначала сделаем это в предположении $\zeta_m \in K$ (позже мы избавимся от этого предположения).

Пусть $\Bbbk$ — поле, $m \geq 2$ — целое число, $\operatorname{char}\Bbbk \nmid m$ и $\zeta_m \in \Bbbk$.

Рассмотрим B такое, что $\Bbbk^{*m} \subset B \subset \Bbbk^*$ и $|B/\Bbbk^{*m}|$. Через $\Bbbk\Big(\sqrt[m]{B}\Big)$ мы будем обозначать композит всех расширений $\Bbbk\Big(\sqrt[m]{b}\Big)$ по $b \in B$.

Теорема 127 (Куммер). *Расширение* $\Bbbk\Big(\sqrt[m]{B}\Big)/\Bbbk$ *конечно и* $[\Bbbk\Big(\sqrt[m]{B}\Big) : \Bbbk] = |B/\Bbbk^{*m}|$.

В нашей ситуации $B = K^*$ и мы получим, что

$$|K^*/K^{*m}| = [K\Big(\sqrt[m]{K^*}\Big) : K] < \infty.$$

Положим $L = K\Big(\sqrt[m]{K^*}\Big)$, тогда расширение L/K абелево, так как $\forall \sigma, \tau \in \mathrm{Gal}(L/K)$

$$\sigma\big(\sqrt[m]{a}\big) = \zeta^s \sqrt[m]{a}, \quad \tau\big(\sqrt[m]{a}\big) = \zeta^r \sqrt[m]{a},$$

тогда, так как $\zeta \in K$, мы имеем

$$\sigma\tau(\sqrt[m]{a}) = \sigma(\zeta^r \sqrt[m]{a}) = \sigma(\zeta^r)\sigma(\sqrt[m]{a}) = \zeta^{r+s} \sqrt[m]{a}.$$

Тогда $K^*/N_{L/K}L^* \cong G/[G,G] = G$, а но $\forall \sigma \in G\ \sigma^m = 1$. Действительно,

$$\sigma(\sqrt[m]{a}) = \zeta \sqrt[m]{a} \implies \sigma^m(\sqrt[m]{a}) = \sqrt[m]{a} \implies \forall x \in K^* \quad x^m \in \mathrm{N}_{L/K} L^*.$$

Отсюда $K^{*m} \subset N_{L/K}L^*$. С другой стороны, по теореме Куммера индексы этих подгрупп равны

$$|K^*/K^{*m}| = [L : K] = |G| = |K^*/N_{L/K}L^*| \implies K^* = N_{L/K}L^*.$$

Избавимся теперь от предположения про $\zeta \in K$. Действительно, если $K(\zeta_m)^*$ — норменная, то есть $K(\zeta_m)^* = N_{L/K(\zeta_m)}L^*$, то

$$K^* \supset K^{*m} \supset N_{K(\zeta_m)/K}K^*(\zeta_m)^{*m} = N_{L/K}L^*,$$

а значит, K^{*m} — норменная.

Теперь сделаем набросок доказательства теоремы Куммера:

Набросок доказательства. Пусть $G = \mathrm{Gal}(\Bbbk\Big(\sqrt[m]{B}\Big)/\Bbbk)$. Рассмотрим отображение

$$G \times B/\Bbbk^* m \to \mu_m, \quad (\sigma, b) \mapsto \frac{\sigma\Big(\sqrt[m]{b}\Big)}{\sqrt[m]{b}}.$$

оно осуществляет невырожденное спаривание $\mathbb{Z}/m\mathbb{Z}$-модулей. Отсюда мы получаем, что

$$[\Bbbk\Big(\sqrt[m]{B}\Big) : \Bbbk] = |G| = |B/\Bbbk^{*m}|.$$

□

Теперь докажем наконец, что $|K^*/K^{*m}| < \infty$ при $p = \mathrm{char}\,\Bbbk$ (тут $\Bbbk$ — поле вычетов). Обозначим за $U = \mathcal{O}_K^*$, тогда

$$K^* \cong \mathbb{Z} \times U \implies K^{*m} \cong m\mathbb{Z} \times U^m \implies K^*/K^{*m} \cong \mathbb{Z}/m\mathbb{Z} \times U/U^m.$$

По одному из упражнений, отображение

$$U_i \xrightarrow{\sim} U_i,\ x \mapsto x^m$$

является изоморфизмом при $(m, p) = 1$ и $i \geq 1$. Соответственно, тогда

$$|U/U^m| \leq |U/U_1| \leq p.$$

Если же $m = p$, то

$$U_i \xrightarrow{\sim} U_{i+e},$$

если $i > e_0$, где $e = \upsilon_K(p)$. Тогда $U^p \supset U_{e+e_0+1}$, но $|U/U_{e+e_0+1}| < \infty$, что даёт нам, что $|U/U^p| < \infty$.

Итого, из рассуждения выше мы заключаем, что

$$\forall m \in \mathbb{N} \quad |U/U^m| < \infty.$$

4.6 Локальная теорема Кронекера

Пусть теперь $K_i = \mathbb{Q}_p(\zeta_{p^i})$, для краткости обозначим $\zeta = \zeta_{p^i}$. Расширение $K_i/\mathbb{Q}_p$ — вполне разветвлённое:

Упражнение. Постройте неприводимый многочлен над $\mathbb{Q}_p$ с корнем $1-\zeta$ степени $\varphi(p^i)$ (*Hint:* $N(1-\zeta) = p$).

У нас есть фильтрация

$$\mathbb{Q}_p \supset U \supset U_1 \supset \ldots \supset U_i = \{u \in U \mid u \equiv 1 \pmod{p^i}\}.$$

Тогда, так как отображения

$$U_j \to U_{j+1},\ x \mapsto x^p, \quad U_j \to U_j,\ x \mapsto x^m,\ (p,m) = 1$$

являются изоморфизмами, выполняется включение $U_1^{(p-1)p^{i-1}} = U_i$. Действительно, мы просто $i-1$ раз возводим в p-ю степень и так сдвигаем индекс, а после возводим в $(p-1)$-ю и пользуемся тем, что $(p-1,p) = 1$. Отсюда мы получаем

$$U_{K_i} \supset U \supset U_1 \implies N_{K_i/\mathbb{Q}_p}(U_{K_i}) \supset N_{K_i/\mathbb{Q}_p}(U_1) = U_1^{(p-1)p^{i-1}} = U_i,$$

так как на базовом поле норма действует как возведение в степень расширения.

Значит, $U_i \subset N_{K_i/\mathbb{Q}_p}(U_{K_i})$. Тогда, так как

$$|U/U_1| = p-1, \quad |U_j/U_{j+1}| = p,$$

стандатным переходом к последовательным факторам фильтрации мы имеем, что

$$(p-1)\cdot p^{i-1} = |U/U_i| \geq |U/N_{K_i/\mathbb{Q}_p}(U_{K_i})| = |\mathbb{Q}_p^*/N_{K_i/\mathbb{Q}_p}(K_i^*)|$$

откуда (так как индексы совпали) $U_i = N_{K_i/\mathbb{Q}_p}(U_{K_i}) \implies N_{K_i/\mathbb{Q}_p}(K_i^*) = \langle p\rangle \times U_i$.

Пусть теперь $F_m/\mathbb{Q}_p$ — неразветвлённое расширение степени m. Тогда

$$N_{F_m/\mathbb{Q}_p}U_{F_m} = U \implies N_{F_m/\mathbb{Q}_p}F_m^* = \langle p^m\rangle \times U,$$

а тогда по доказанному ранее для норменных подгрупп:

$$N_{K_iF_m/\mathbb{Q}_p}(K_iF_m)^* = N_{K_i/\mathbb{Q}_p}K_i^* \cap N_{F_m/\mathbb{Q}_p}F_m^* = \langle p^m\rangle \times U_i.$$

Теперь пусть $L/\mathbb{Q}_p$ — абелево расширение Галуа степени n. Предположим, что

$$N_{K_iF_m/\mathbb{Q}_p}(K_iF_m)^* \subset \mathbb{Q}_p^{*n},$$

тогда так как $\mathbb{Q}_p^{*n} \subset N_{L/\mathbb{Q}_p}L^*$ мы получаем, что $L \subset K_iF_m$, но так как $K_i = \mathbb{Q}_p(\zeta_{p^i})$ это означает, что $F_m = \mathbb{Q}_p(\zeta_{p^m-1})$, а тогда

$$K_iF_m = \mathbb{Q}_p(\zeta_{p^i(p^m-1)}).$$

Остаётся положить $i = s+1$, $m = n$, где $n = p^s\cdot r$. Тогда мы получаем, что

$$N_{K_iF_m/\mathbb{Q}_p}(K_iF_m)^* = \langle p^n\rangle \times U_{s+1} = \langle p^n\rangle \times U_1^s = \mathbb{Q}_p^{*n},$$

что гарантирует нам условие $N_{K_iF_m/\mathbb{Q}_p}(K_iF_m)^* \subset \mathbb{Q}_p^{*n}$.

Таким образом, мы доказали локальную теорему Кронекера:

Теорема 128 (Локальная теорема Кронекера)**.** *Пусть $L/\mathbb{Q}_p$ — конечное абелево расширение. Тогда $L \subset \mathbb{Q}(\zeta_n)$ для некоторого $n \in \mathbb{N}$.*

5. Гауссовы суммы

5.1 Общие сведения

Определение 152. Пусть p — простое число. *Мультипликативными характерами* группы $\mathbb{F}_p$ мы будем называть гомоморфизмы $\mathbb{F}_p \to \mathbb{C}^*$.

Если мы выбрали некоторый первообразный корень ω, порождающий $\mathbb{F}_p^*$, то характер задаётся тем, в какой первообразынй корень из 1 переходит ω.

Через χ_0 обозначим единичный характер, то есть такой, что $\chi(x) = 1\,\forall x$. Пусть теперь χ – произвольный характер, $a \in \mathbb{Z}, a \not\vdots p$, тогда определён $\chi(\overline{a})$. Доопределим его в нуле следующим образом:

$$\chi(\overline{0}) = \begin{cases} 0, & \chi \neq \chi_0 \\ 1, \chi = \chi_0 \end{cases}.$$

Теперь все наши характеры заданы на $\mathbb{Z}$ как $\chi(a) \stackrel{\text{def}}{=} \chi(\overline{a})$.

Отметим для начала несколько самых простых свойств:

- $\chi(1) = 1$,
- $\forall a\ \chi(a) -$ корень $(p-1)$-й степени из единицы,
- $\chi(a^{-1}) = \overline{\chi(a)}$.

Определение 153. Пусть χ — мультипликативный характер группы $\mathbb{F}_p$. *Суммой Гаусса* соотвествующей характеру χ мы будем называть выражение вида

$$S(\chi, a) = \sum_{x=0}^{p-1} \chi(x)\zeta_p^{ax}.$$

Замечание. Видно, чтто $S(\chi, a)$ зависит лишь от χ и класса $\overline{a} \in \mathbb{F}_p$.

Сделаем сначала несколько наблюдений.

Предложение 84. *Для сумм Гаусса выполняется следующее соотношение*

$$S(\chi, a) \cdot \chi(a) = \begin{cases} S(\chi, 1), & a \not\vdots p,\ \chi \neq \chi_0 \\ 0, & a \not\vdots p,\ \chi = \chi_0 \text{ или } a \vdots p,\ \chi \neq \chi_0 \\ p, & a \vdots p,\ \chi = \chi_0 \end{cases}.$$

Доказательство. Действительно, если $\chi \neq \chi_0$ и $a \not\vdots p$, то

$$\chi(a)S(\chi, a) = \sum_{x=0}^{p-1} \chi(ax)\zeta^{ax} = \sum_{t=0}^{p-1} \chi(t)\zeta^t = S(\chi, t).$$

Если же $a \not\vdots p,\ \chi = \chi_0$, то

$$S(\chi_0, a) = \sum_{x=0}^{p-1} \zeta^{ax} = 0.$$

И, если же $a \vdots p$, то мы имеем

$$S(\chi, 0) = \sum_{x=0}^{p-1} \chi(x) = 0,$$

так как если мы обозначим эту сумму за T и выберем такое $B \in \mathbb{F}_p^*$, что $\chi(b) \neq 1$, мы получим

$$\chi(b) \cdot T = \chi(b) \sum_{x=0}^{p-1} \chi(x) = \sum_{x=0}^{p-1} \chi(bx) = \sum_{t=0}^{p-1} \chi(t) = T \implies T = 0.$$

□

Теперь вычислим модуль Гауссовой суммы. Во-первых, сразу очевидно, что

$$S(\chi_0, 1) \cdot \overline{S(\chi_0, 1)} = 0.$$

Вычислим $\sum_{a=0}^{p-1} S(\chi, a)\overline{S(\chi, a)}$ двумя способами. Во-первых если $a \neq 0$, то заметим, что по предложению выше

$$S(\chi, a) \cdot \overline{S(\chi, a)} = \chi(a^{-1}) \cdot \chi(a) \cdot S(\chi, 1)\overline{S(\chi, 1)} = |S(\chi, 1)|^2.$$

Тогда мы получаем, что

$$\sum_{a=0}^{p-1} S(\chi, a)\overline{S(\chi, a)} = (p-1)|S(\chi, 1)|^2,$$

так как $S(\chi, 0) = 0$. С другой стороны,

$$S(\chi, a) \cdot \overline{S(\chi, a)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay}.$$

Теперь вспомним, что

$$\sum_{t=0}^{p-1} \zeta^{at} = \begin{cases} p, & a \equiv 0 \pmod p \\ 0, & \text{иначе.} \end{cases} \implies \frac{1}{p}\sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta_{xy}.$$

Отсюда получаем, что

$$\sum_{a=0}^{p-1} S(\chi, a) \cdot \overline{S(\chi, a)} = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}\delta_{xy}p = (p-1)p.$$

Отсюда мы получили, что $(p-1)|S(\chi, 1)|^2 = (p-1)p$, откуда

$$|S(\chi, 1)| = \sqrt{p} \implies |S(\chi, a)| = \sqrt{p}.$$

Пример 63. Рассмотрим теперь частный случай $p \neq 2$ и характеров

$$\chi(a) = \left(\frac{x}{a}\right).$$

Тогда мы получаем, что

$$p = |S(\chi, 1)|^2 = \left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\zeta^x\right) \cdot \left(\sum_{y=1}^{p-1}\left(\frac{-y}{p}\right)\zeta^{-y}\right) = \left(\frac{-1}{p}\right)|S(\chi, 1)|^2.$$

Соответственно, если $\left(\frac{-1}{p}\right) = 1$, то $\sqrt{p} \in \mathbb{Q}(\zeta_p)$. Если же $\left(\frac{-1}{p}\right) = -1$, то $\sqrt{-p} \in \mathbb{Q}(\zeta_p) \implies \sqrt{p} \in \mathbb{Q}(\zeta_{4p})$.

Если же $p = 2$, то $2\sqrt{-1} = (1 + \sqrt{-1})^2 \implies \sqrt{2} \in \mathbb{Q}(\zeta_{8p})$.

Теперь рассмотрим произвольное натуральное n, разложим его в произведение простых:

$$n = p_1^{k_1} \cdot \ldots p_s^{k_s},$$

а отсюда $\mathbb{Q}(\sqrt{n}) \subset \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_s})$, а это расширение лежит в каком-то круговом расширении (по выкладке выше).

С другой же стороны, если $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_n)$, то $n \vdots p$ (так как простое число p будет разветвлено в $\mathbb{Q}(\sqrt{p})$, значит будет разветвлено и в $\mathbb{Q}(\zeta_n)$, но, как мы видели в первой части курса, такого не происходит при $n \not\vdots p$).

5.2 Количество решений уравнений над конечным полем

Пусть $F(x_1,\dots,x_n)\in\mathbb{Z}[x_1,\dots,x_n]$, ζ — певообразные корень степени p из единицы. Рассмотрим сумму

$$S=\sum_{(x_1,\dots,x_n)\in\mathbb{F}_p^n}\sum_{x\in\mathbb{F}_p}\zeta^{xF(x_1,\dots,x_n)}.$$

Заметим, что

$$\sum_{x\in\mathbb{F}_p}\zeta^{xF(x_1,\dots,x_n)}=\begin{cases}0, & \text{если } F(x_1,\dots,x_n)\not\equiv 0 \pmod p\\ p, & \text{если } F(x_1,\dots,x_n)\not\equiv 0 \pmod p\end{cases}.$$

Соотвественно, отсюда получаем, что

$$S=\sum_{(x_1,\dots,x_n)\in\mathbb{F}_p^n}\sum_{x\in\mathbb{F}_p}\zeta^{xF(x_1,\dots,x_n)}=p\cdot N,$$

где N — это количество решений уравнения $F(x_1,\dots,x_n)=0$ в $\mathbb{F}_p$.

Рассмотрим теперь случай, когда F имеет диагональный вид:

$$F(x_1,\dots,x_n)=a_1x_1^{r_1}+\dots+a_nx_n^{r_n},\quad a_i\in\mathbb{Z},\ a_i\not\equiv 0 \pmod p.$$

Посчитаем сумму S вторым способом:

$$S=\sum_{(x,x_1,\dots,x_n)\in\mathbb{F}_p^{n+1}}\zeta^{x\left(a_1x_1^{r_1}+\dots+a_nx_n^{r_n}\right)}=p^n+\sum_{x\neq 0}\left(\sum_{x_1=0}^{p-1}\zeta^{xa_1x_1^{r_1}}\right)\left(\sum_{x_2=0}^{p-1}\zeta^{xa_2x_2^{r_2}}\right)\dots\left(\sum_{x_n=0}^{p-1}\zeta^{xa_nx_n^{r_n}}\right)$$

Посмотрим на отдельные сомножители:

$$\sum_{y=0}^{p-1}\zeta^{y^r}=\sum_{z=0}^{p-1}m(z)\zeta^z,$$

где $m(z)$ — число решений уравнения $y^r=z$ над полем $\mathbb{F}_p$ или же число решений сравнения

$$y^r=z \pmod p$$

относительно y. Ясно, что $m(0)=1$. Найдём $m(z)$ явно при $z\not\equiv 0 \pmod p$. Выберем первообразный корень g по модулю p, то есть $\mathbb{F}_p=\langle g\rangle$ и пусть

$$x=g^k \pmod p,$$

где показатель k определён одозначно (по модулю $p-1$, естественно). Пусть также $y=g^u \pmod p$, тогда

$$y^r=z \pmod p\Leftrightarrow ru\equiv k \pmod{p-1}.$$

Это сравнение имеет $d=(r,p-1)$ решений по u или не имеет ни одного решения, в зависимости от того, делится k на d или нет:

$$m(z)=\begin{cases}d, & k\equiv 0 \pmod d\\ 0, & k\not\equiv 0 \pmod d\end{cases}.$$

Но, в аналитическом смысле такая формула не слишком удобна. Получим другую. Выберем некоторый первообразный корень степени d из единицы и обозначим его за ε. Рассмотрим характеры

$$\chi_s(z)=e^{ks},\quad s=0,\dots,d-1$$

где число k для z определяется как выше. Или, эквивалентно можно говорить, что мы задали отображение.

$$\chi_s\colon \mathbb{F}_p^*=\langle g\rangle\to\mu_d,\quad g\mapsto\varepsilon^s.$$

Тогда видим, что если $k \equiv 0 \pmod d$, то каким бы ни было $s = 0, \dots, s-1$, мы имеем $\varepsilon^{ks} = 1$ и

$$\sum_{s=0}^{d-1} \chi_s(z) = d.$$

Если же $k \not\equiv 0 \pmod d$, то так как ε — первообразный корень, $\varepsilon^k \not\equiv 1$, а значит,

$$\sum_{s=0}^{d-1} \chi_s(z) = \sum_{s=0}^{d-1} \varepsilon^{ks} = \frac{\varepsilon^{kd} - 1}{\varepsilon^k - 1} = 0.$$

Итак, мы получили, что

$$m(z) = \sum_{s=0}^{d-1} \chi_s(z).$$

Тогда мы получили, что

$$\sum_{y=0}^{p-1} \zeta^{ay^r} = \sum_{z=0}^{p-1} m(z)\zeta^{az} = 1 + \sum_{z=0}^{p-1}\sum_{s=0}^{d-1} \chi_s(z) = \sum_{s=0}^{d-1} S(\chi_s, a) = \sum_{s=1}^{d-1} S(\chi_s, a).$$

Тогда мы можем оценить модуль этой суммы:

$$\left|\sum_{y=0}^{p-1} \zeta^{ay^r}\right| \le (d-1)|S(\chi_s, a)| = (d-1)\sqrt{p}.$$

Применим это к замечательной формуле

$$S = \sum_{(x,x_1,\dots,x_n)\in\mathbb{F}_p^{n+1}} \zeta^{x\left(a_1x_1^{r_1}+\dots+a_nx_n^{r_n}\right)} = p^n + \sum_{x\neq 0}\left(\sum_{x_1=0}^{p-1}\zeta^{xa_1x_1^{r_1}}\right)\left(\sum_{x_2=0}^{p-1}\zeta^{xa_2x_2^{r_2}}\right)\dots\left(\sum_{x_n=0}^{p-1}\zeta^{xa_nx_n^{r_n}}\right)$$

$$|S - p^n| \le (p-1)\cdot p^{\frac{n}{2}}\cdot(d_1-1)\dots(d_n-1),$$

где $d_i = (r_i, p_i - 1)$.

Значит, мы получили такое неравенство для количества решений:

$$|N - p^{n-1}| \le (p-1)\cdot p^{\frac{n}{2}-1}\cdot(d_1-1)\dots(d_n-1).$$

6. Глобальная теорема Кронекера

6.1 Группа и поле инерции для максимального идеала в случае числового поля

Пусть K — числовое поле (т.е. конечное расширение $\mathbb{Q}$), L/K — расширение Галуа с группой Галуа $G = \mathrm{Gal}(L/K)$.

Пусть $\mathfrak{p}$ — максимальный идеал в $\mathcal{O}_L$, а $\mathfrak{P}$ — такой максимальный идеал в $\mathcal{O}_L$, что $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.

В случае расширения Галуа мы знаем, что у всех идеалов, висящих над $\mathfrak{p}$ одинаковые индексы ветвления и степени инерции, то есть справедлива формула $efr = n$, где

- $e = e(\mathfrak{P}/\mathfrak{p})$ — индекс ветвления,
- $f = f(\mathfrak{P}/\mathfrak{p})$ — степень инерции,
- r — колиество максимальных идеалов в $\mathcal{O}_L$, висящих над $\mathfrak{p}$.

Введём такие обозначения

- $G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$.
- $\Bbbk(\mathfrak{P}) = \mathcal{O}_L/\mathfrak{P}$, $\Bbbk(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$.

Лемма 76. $G_{\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}(\Bbbk(\mathfrak{P})/\Bbbk(\mathfrak{p}))$.

Доказательство. Так как можно заменить K на $Z_{\mathfrak{P}}$ и доказывать, что $G_{\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}(\Bbbk(\mathfrak{P})/\Bbbk\big(\mathfrak{P} \cap \mathcal{O}_{Z_{\mathfrak{P}}}\big))$, достаточно доказывать это рассуждение когда $G_{\mathfrak{P}} = G$.

Соотвественно, покажем, что $\Bbbk\big(\mathfrak{P} \cap \mathcal{O}_{Z_{\mathfrak{P}}}\big) = \Bbbk(\mathfrak{p})$, а для этого докажем, что $f\big(\mathfrak{P} \cap \mathcal{O}_{Z_{\mathfrak{P}}}/\mathfrak{p}\big) = 1$.

Положим $e' = e(\mathfrak{P} \cap \mathcal{O}_{Z_{\mathfrak{P}}}/\mathfrak{p})$, $f' = f\Big(\mathfrak{P} \cap \mathcal{O}_{Z_{\mathfrak{P}}/\mathfrak{p}}\Big)$. Так как $G_{\mathfrak{P}}$ действует на $\mathfrak{P}$ тривиальн, над $\mathfrak{P} \cap \mathcal{O}_{Z_{\mathfrak{P}}}$ есть ровно один максимальный идеал, откуда $\mathfrak{P}$, откуда $e'f' = |G_{\mathfrak{P}}|$. Соотвественно,

$$e = e'e_1,\ f = f'f_1, \quad e_1 = e(\mathfrak{P} \cap \mathcal{O}_{Z_{\mathfrak{P}}}/\mathfrak{p}),\ f_1 = f(\mathfrak{P} \cap \mathcal{O}_{Z_{\mathfrak{P}}}/\mathfrak{p}).$$

Так как $ref = n$, мы получаем $re_1f_1 = r \implies e_1f_1 = 1 \implies f_1$.

Теперь мы считаем, что $G = G_{\mathfrak{P}}$. Заметим, что

$$\Bbbk(\mathfrak{P}) = \Bbbk(\mathfrak{P})(\theta).$$

Пусть $\overline{g}$ — минимальный многочлен для $\overline{\theta}$, а f — минимальный многочлен для θ. Тогда $\overline{f} \vdots \overline{g}$.

$$f(x) = \prod_{\sigma \in G}(x - \sigma\theta) \implies \overline{f}(x) = \prod_{\sigma \in G}(x - \overline{\sigma\theta}),\ \overline{g}(x) = \prod_{\sigma \in \mathrm{Gal}(\Bbbk(\mathfrak{P})/\Bbbk(\mathfrak{p}))}(x - \sigma\overline{\theta}).$$

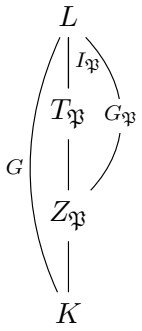
Теперь пусть $\overline{\theta} \in \mathrm{Gal}(\Bbbk(\mathfrak{P})/\Bbbk(\mathfrak{p}))$, тогда $\overline{\theta}(\overline{\theta}) = \overline{\tau(\theta)}$, где $\tau \in G$. Тогда $\overline{\tau} = \overline{\sigma}$.

□

Посмотрим тогда на короткую точную последовательность

$$1 \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \to \mathrm{Gal}(\Bbbk(\mathfrak{P})/\Bbbk(\mathfrak{p})) \to 1$$

точна и рассмотрим подрасщирения, которые соотвествуют этим группам



Заметим, что $[G : G_{\mathfrak{P}}]$ — количество элементов в орбите действия G на $\mathfrak{P}$ (так как индекс стабилизатора равен размеру орбиты действия), то есть $[Z_{\mathfrak{P}} : K] = r$. С другой же стороны,

$$|G_{\mathfrak{P}} : I_{\mathfrak{P}}| = |\mathrm{Gal}(\Bbbk(\mathfrak{P})/\Bbbk(\mathfrak{p}))| = [\Bbbk(\mathfrak{P}) : \Bbbk(\mathfrak{p})] = f \implies [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = f.$$

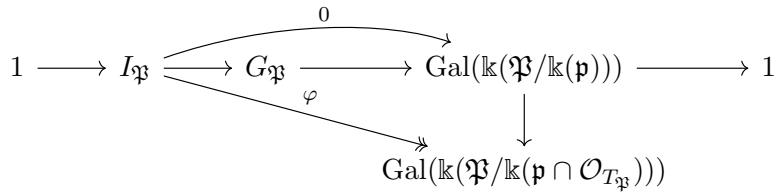
Отсюда получаем, что $|I_{\mathfrak{P}}| = [L : T_{\mathfrak{P}}] = e$. Покажем, что

$$e\big(\mathfrak{P} \cap \mathcal{O}_{T_{\mathfrak{P}}}/\mathfrak{p}\big) = 1,$$

для этого покажем, что $e(\mathfrak{P}/\mathfrak{P} \cap \mathcal{O}_{T_{\mathfrak{P}}}) = e$. Так как $I_{\mathfrak{P}} \subset G_{\mathfrak{P}}$, он действует на $\mathfrak{P}$ тривиально. Тогда нам остаётся доказать, что $f(\mathfrak{P}/\mathfrak{P} \cap \mathcal{O}_{T_{\mathfrak{P}}}) = 1$, что равносильно тому, что группа Галуа $\mathrm{Gal}(\Bbbk(\mathfrak{P})/\Bbbk(\mathfrak{P} \cap \mathcal{O}_{\mathfrak{P}}))$ тривиальна.

Запишем для расширения $L/T_{\mathfrak{P}}$ точную последовательность, как для расширения выше, из неё получим, что $\varphi : I_{\mathfrak{P}} \twoheadrightarrow \mathrm{Gal}(\Bbbk(\mathfrak{P})/\Bbbk(\mathfrak{P} \cap \mathcal{O}_{\mathfrak{P}}))$. С другой стороны, есть такая коммутативная диаграмма:[19]

[19](тут я подразумеваю, что φ это в точности композиция нужных стрелок)



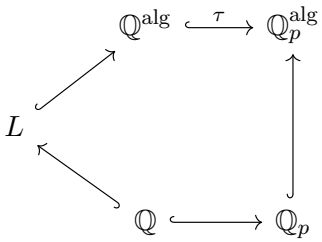
из которой получаем, что $\mathrm{Gal}(\Bbbk(\mathfrak{P})/\Bbbk(\mathfrak{P}\cap\mathcal{O}_{\mathfrak{P}})) = e$.

Определение 154. $I_{\mathfrak{P}}$ называется группой инерции идеала $\mathfrak{P}$, а $T_{\mathfrak{P}}$ — полем инерции идеала $\mathfrak{P}$.

6.2 Глобальная теорема Кронекера

Теорема 129 (Глобальная теорема Кронекера)**.** *Пусть F — абелево расширение поля $\mathbb{Q}$. Тогда $F \subset \mathbb{Q}(\zeta_n)$ для некоторого натурального n.*

Доказательство. Рассмотрим произвольное абелево расширение, построим для него $L\mathbb{Q}_p/\mathbb{Q}_p$ и для начала поясним, что это вообще такое. Под этим мы подразумеваем вот такой композит:



Ясно, что в таком случае $L\mathbb{Q}_p/\mathbb{Q}_p$ — расширение Галуа и

$$\mathrm{Gal}(\tau(L)\mathbb{Q}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(L/\mathbb{Q}),$$

откуда ясно, что это расширение абелево. Совершенно ясно, что эту конструкцию мы используем, чтоб свести глобальную теорему Кронекера к локальной. Теперь преступим непосредственно к доказательству.

Заметим, что существует лишь конечное число простых p, разветвлённых в F. Пронумеруем их: $p_1, p_2, \ldots, p_s$. По локальной теореме Кронекера каждого p_i существует n_{p_i} такое, что

$$\mathbb{Q}_{p_i} \hookrightarrow \mathbb{Q}\big(\zeta_{n_{p_i}}\big).$$

Рассмотрим $n = n_{p_1} \cdot \ldots \cdot n_{p_s} = q_1^{a_1} \cdot \ldots \cdot q_t^{a_t}$ и расширение $K = \mathbb{Q}(\zeta_n)$. Ясно, что расширение $K/\mathbb{Q}$ — абелево. Докажем, что

$$F \hookrightarrow K.$$

Точнее, мы покажем, что $L = KF = K$, откуда это будет следовать. Начнём с того, что покажем, что

$$e_{p_i}(L/\mathbb{Q}) = e_{p_i}(L\mathbb{Q}_{p_i}/\mathbb{Q}_{p_i}).$$

Так как $\mathbb{Q}_{p_i}$ — локальное поле, у нас существует единственное продолжение нормирования на $L\mathbb{Q}_{p_i}$, обозначим его за υ_i. Заметим, что так как $L/\mathbb{Q}$ — расширение Галуа, индекс ветвления равен значению **любого** продолжения нормирования, соответствующего максимальному идеалу. Например,

$$e_{p_i}(L/\mathbb{Q}) = \upsilon_i|_L(p_i).$$

С другой стороны, мы знаем, что

$$e_{p_i}(L\mathbb{Q}_{p_i}/\mathbb{Q}_{p_i}) = \upsilon_i(p_i), \quad \upsilon_i|_L(p_i) = \upsilon_i(p_i).$$

Таким образом,

$$e_{p_i}(L\mathbb{Q}_{p_i}/\mathbb{Q}_{p_i}) = e_{p_i}(L/\mathbb{Q}).$$

Справедливости ради, тут надо пояснять, почему сужение нормирования будет нормированием. Это следует из того, что L плотно в $L\mathbb{Q}_p$.

Теперь заметим, что так как $F\mathbb{Q}_{p_i} \subset K\mathbb{Q}_{p_i}$:

$$L\mathbb{Q}_{p_i} = KF\mathbb{Q}_{p_i} = K\mathbb{Q}_{p_i} \cdot F\mathbb{Q}_{p_i} = K\mathbb{Q}_{p_i}.$$

Соответственно, отсюда

$$e_{p_i}(K\mathbb{Q}_{p_i}/\mathbb{Q}_{p_i}) = e_{p_i}(L\mathbb{Q}_{p_i}/\mathbb{Q}_{p_i}) = e_{p_i}(L/\mathbb{Q}) > 1.$$

С другой стороны,

$$e_{p_i}(K/\mathbb{Q}) = e_{p_i}(K\mathbb{Q}_{p_i}/\mathbb{Q}_{p_i}) = \varphi(q^{a_j}) \text{ если } p_i = q_j.$$

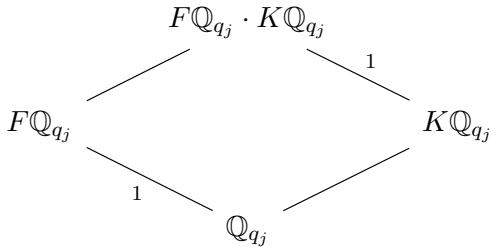
Значит, p_i разветвлено в $K = \mathbb{Q}(\zeta_n)$, откуда $n \vdots p_i$, откуда

$$\{p_1, \ldots, p_s\} \subset \{q_1, \ldots, q_t\}$$

С другой стороны, если для некоторого j мы имеем $q_j \notin \{p_1, \ldots, p_s\}$, то

$$e_{q_j}(L/\mathbb{Q}) = e_{q_j}\big(L\mathbb{Q}_{q_j}/\mathbb{Q}_{q_j}\big) = e_{q_j}\big(F\mathbb{Q}_{q_j} \cdot K\mathbb{Q}_{q_j}/\mathbb{Q}_{q_j}\big) = e_{q_j}(K\mathbb{Q}_{q_j}/\mathbb{Q}_{q_j}) = \varphi(q_j^{a_j}),$$

так как



где на стрелочках подписаны индексы ветвления. Аналогично, если $p \notin \{q_1, \ldots q_t\}$, то

$$e_p(L/\mathbb{Q}) = e_p(K/\mathbb{Q}) = 1.$$

Рассмотрим для каждого j $L_j/\mathbb{Q}$ — поле инерции для q_j, соответственно $L_j \subset L$, притом

$$[L : L_j] = e_{q_j}(L/\mathbb{Q}), \quad e_{q_j}(L_j/\mathbb{Q}) = 1.$$

Тогда рассмотрим $S = L_1 \cap \ldots \cap L_t$. Заметим, что все простые числа неразветвлены в S, так как если $p \in \{q_1, \ldots, q_t\}$, то

$$e_{q_j}(L_j/\mathbb{Q}) = 1,$$

а если $p \notin \{q_1, \ldots, q_t\}$, то $e_p(L/\mathbb{Q}) = 1$ (так как тогда p не разветвлено в L, а $L_j \subseteq L$). Тогда, как мы видели в первой части курса, $L_1 \cap \ldots \cap L_t = \mathbb{Q}$.

С другой стороны,

$$[L : L_1 \cap L_2] \leq [L : L_1] \cdot [L : L_2] \implies [L : L_1 \cap \ldots \cap L_s] \leq \prod_{i=1}^{t} [L : L_i] = e_{q_j}(L/\mathbb{Q}) = \varphi(q_j^{a_j})$$

и тогда по мультипликативности функции Эйлера $[L : \mathbb{Q}] \leq \varphi(n)$, но так как $L \supset K$, а $[K : \mathbb{Q}] = \varphi(n)$, мы получили, что $L = K$. $\square$

Литература

[1] А. Хатчер, *Алгебраическая топология.*

[2] Робин Хартсхорн, *Алгебраическая геометрия*, перевод на русский язык, Москва «Мир», 1981г.

[3] Phillip Griffiths, Joseph Harris, *Principles of Algebraic Geometry,* 2.08.1994.