Содержание

1. Коммутативная алгебра с прицелом на алгебраическую геометрию

Замечание. Весь раздел пока что не дописан.

1.1 Предварительные сведения и напоминания

Определение 1. 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 2. 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 3. Кольцо R называется *нётеровым*, если оно удовлетворяет условию обрыва **возрастающих** цепочек (ACC) для идеалов. Модуль называется *нётеровым*, если он удовлетворяет ACC для подмодулей.

Лемма 1. 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 1 (Гильберта, о базисе)**.** *Кольцо многочленов от конечного числа переменных над нётеровым кольцом нётерово. Иными словами, если R — нётерово кольцо, то любой идеал в кольцо $R[x_1, \dots, x_n]$ 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 4. 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 5 (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 6. *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 $\mathfrak{Aff}$.

Определение 7. 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 $\mathrm{Hom}_{\mathfrak{Aff}}(X, \mathbb{A}^1_F) \cong F[t_1, \dots, t_n]/I(X)$. Это кольцо называется *аффинной алгерой* многообразия X и обозначается $F[X]$.

[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.

Так как $\mathrm{Hom}_{\mathfrak{Aff}}(\_, \mathbb{A}^1_F)$ является контравариантным функтором, а кольцевые операции определяются на $\mathrm{Hom}_{\mathfrak{Aff}}(X, \mathbb{A}^1_F)$ естественным образом, отображение $X \mapsto F[X]$ определяет контравариантный функтор $\mathfrak{Aff} \to F - \mathfrak{Alg}_{fin.gen.}$ — конечнопорожденные редуцированные алгебры.

Построим функтор в обратную сторону. Рассмотрим $R \in F - \mathfrak{Alg}_{fin.gen.}$ и выберем в ней набор образующих (то есть, выберем эпиморфизм $\pi_R \colon F[t_1, \ldots, t_n]$). Рассмотрим функтор $\mathcal{X} = \mathrm{Hom}_{F-\mathfrak{Alg}_{fin.gen.}}(\_, F) \colon F - \mathfrak{Alg}_{fin.gen.} \to \mathfrak{Set}$.

Множество $\mathcal{X}(A)$ мы можем отождествить с $\mathbb{A}_{F^n}$ по формуле

$$\varphi \mapsto (\varphi(t_1), \ldots, \varphi(t_n)).$$

Таким образом, $\mathcal{X}(R)$ вкладывается в $\mathbb{A}^n_F$ при помощи отображения $\psi \mapsto \psi \circ \pi_R$. Кроме того, множество $\mathcal{X}(R) = V(\mathrm{Ker}\, \pi_R)$ является аффинным алгебраическим многообразием с аффинной алгеброй $F[t_1, \ldots, t_n]/I(V(\mathrm{Ker}\, \pi_R))$. Так мы имеем:

$$\mathcal{X}(F[X]) = \mathcal{X}(A/I(X)) = V(I(X)) = X \quad F[X(R)] = A/I(V(\mathrm{Ker}\, \pi_R)).$$

Последняя алгебра изоморфна R тогда и только тогда, когда $I(V(J)) = J$, где $R \cong A/J$.

Теорема 2 (Теорема Гильберта о нулях). *Пусть $F = F^{alg}$, $J \subset F[t_1, \ldots, t_n]$, а $f \in F[t_1, \ldots, t_n]$. 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 $F[t_1, \ldots, t_n]$ и категории $\mathfrak{Aff}$ и $F - \mathfrak{Alg}_{fin.gen.}$ 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 $\mathrm{Specm}(F[X])$.

1.3 Топология Зарисского на спектре кольца

Пусть R — кольцо, $\mathrm{Specm}\, R$ — его максимальный спектр (множество его максимальных идеалов). Зададим на $\mathrm{Specm}\, R$ набор замкнутых множеств

$$\widetilde{V}(J) \stackrel{\text{def}}{=} \{\mathfrak{m} \in \mathrm{Specm}\, R \mid \mathfrak{m} \supset J\},\ J \subset R.$$

При таком определении топологии X будет гомеоморфно $\mathrm{Specm}(F[X])$ (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;

$$J \subset R, \quad V(J) \stackrel{\text{def}}{=} \{\mathfrak{p} \in \mathrm{Spec}\, R \mid J \subset \mathfrak{p}\}.$$

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 8. 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 2. 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 3. 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 4. $\lambda_* \circ \lambda^* = \mathrm{id}$. 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 1. *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 5. 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 2. *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 $\operatorname{Im} \lambda^* = \operatorname{Spec} R \setminus V(s)$ — открытое подмножество, а $\{\operatorname{Spec} R_s \mid s \in R\}$ — база топологиии Зарисского.

Определение 9. 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 3. *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 10. Множество $M \times S/\sim$, где $(m, s) \sim (m', s') \Leftrightarrow \exists s'' \in S \colon ms's'' = m'ss''$ с ествественно заданными операциями называется *локализацией* модуля M в S.

Лемма 6. $S^{-1}M \cong M \otimes_R S^{-1}R$.

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 11. Модуль называется *плоским*, если тензорное домножение на него — точный функтор.

Предложение 1. *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 3. *Локализация модуля сохраняет ядра, коядра 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 7. 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. $s \notin \mathfrak{m}$)$\colon sr = 0$. Напомним такое определение:

Определение 12. 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 4. *Следующие свойства модулей и их гомоморфизмов являются локальными:*

1. $M = 0$.
2. *φ — инъективен, φ — 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 8. 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 5 (Гамильтона-Кэли). *Пусть $A \in \mathrm{M}_n(R)$, где R — коммутативное кольцо. Тогда $\chi_A(A) = 0$.*

Докажем теперь некоторое его обобщение.

Теорема 6 (Гамильтона-Кэли). *Пусть $\varphi \in \operatorname{End}(M)$ такой, что $\operatorname{Im}\varphi \subset IM$. 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 7 (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 4. *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 13. Аннулятором R-модуля M называется множество $\{r \in R \mid rM = 0\}$.

Лемма 9. Ненулевой простой R-модуль M изоморфен $R/\mathfrak{m}$ для некоторого $\mathfrak{m} \in \mathrm{Specm}\, R$. Таким образом, $\mathrm{Ann}\, M$ является максимальным идеалом кольца R.

Доказательство. □

1.9 Кольца нормирования, кольца дискретного нормирования и Дедекиндовы области

Определение 14. 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 1. Например, кольцами нормирования являются $\mathbb{Z}_{(p)},\ \mathbb{Z}_p,\ F[[x]]$.

Определение 15. 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 8. *1. Пусть υ — нормирование на F, тогда $R \overset{\text{def}}{=} \{x \in F \mid \upsilon(x) \geq 0\}$ — 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.

[2] в аддитивной записи...

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**. □

Предложение 2. *Пусть R — кольцо нормирования, тогда R —- локально и целозамкнуто.*

Доказательство. Положим $\mathfrak{m} \overset{\text{def}}{=} \{a \in R \mid \upsilon(a) > 0\}$. 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 3. *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 10. 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 $\mathfrak{m}R_{\mathfrak{m}} = \operatorname{Rad}(R_{\mathfrak{m}})$). □

[3] тут имеется в виду изоморфизм моноидов.

Теорема 9. *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* $\mathrm{Ideals}(R) = \{0, \mathfrak{m}^k \mid k \in \mathbb{N}_0\}$

Доказательство. $(1) \implies (2)$ мы уже по сути доказали в утверждении 3. Докажем теперь $(2) \implies (3)$. Мы знаем, что $\mathrm{Specm}\, R = \{\mathfrak{m}\}$, возьмём $a \in \mathfrak{m} \setminus \mathfrak{m}^2$ по лемме 10. 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. □

1.10 Дедекиндовы кольца

Предложение 4. *Пусть R — нётерова одномерная область целостности. Тогда следующие условия эквивалентны:*

1. *R целозамкнуто.*
2. *Любой примарный идеал имеет вид $\mathfrak{m}^k$ для некоторого $\mathfrak{m} \in \mathrm{Specm}\, R$.*
3. *$\forall \mathfrak{m} \in \mathrm{Specm}\, R$ кольцо $R_{\mathfrak{m}}$ — кольцо дискретного нормирования.*

Доказательство. $(1) \Leftrightarrow (3)$ просто в силу того, что целозамкнутость — локальное свойство и теоремы 9. 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 9 $R_{\mathfrak{m}}$ — кольцо дискретного нормирования. □

Определение 16. Кольца, удовлетворяющие условию 4 называют *дедекиндовыми.*

Теорема 10. *Пусть Z — Дедекиндово кольцо, Q — его поле частных, F/Q — конечное расщирение (полей), а $R = \mathrm{Int}_F Z$. 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

$$m_\alpha \in \mathrm{End}_{Q-\mathfrak{mod}}(F),\ m_\alpha(x) = \alpha x.$$

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 17. Пусть I — идеал. Тогда его *высота* $h(I)$ — длина наибольшей цепочки вложенных в него простых идеалов.

Теорема 11 (Крулль, о высоте)**.** *Пусть $x \in R$ — нётерово коммутативное кольцо с единицей, $\mathfrak{p}$ — минимальный простой идеал, содержащий $(x) = xR$. Тогда $h(\mathfrak{p}) \leq 1$.*

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 18. 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 11. 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 $\mathfrak{q} \implies h(\mathfrak{q}) = 0 \implies h(\mathfrak{p}) \leq 1$. □

1.12 Пополнения

Пусть A — абелева группа с убывающей фильтрацией

$$A \supset A_0 \supset A_1 \supset \dots A_n \supset$$

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:

$$\dots \xrightarrow{\theta_2} A/A_2 \xrightarrow{\theta_1} A/A_1 \xrightarrow{\theta_0} A/A_0, \quad \widehat{A} \stackrel{\text{def}}{=} \varprojlim A/A_n.$$

Определение 19. Соотвественно, *пополнением* A в топологии, связанной с фильтрацией $\{A_n\}$ называется определённое выше $\widehat{A}$.

Пример 2. 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 12. 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

$$0 \to \widehat{A'} \to \widehat{A} \to \widehat{A''} \to 0.$$

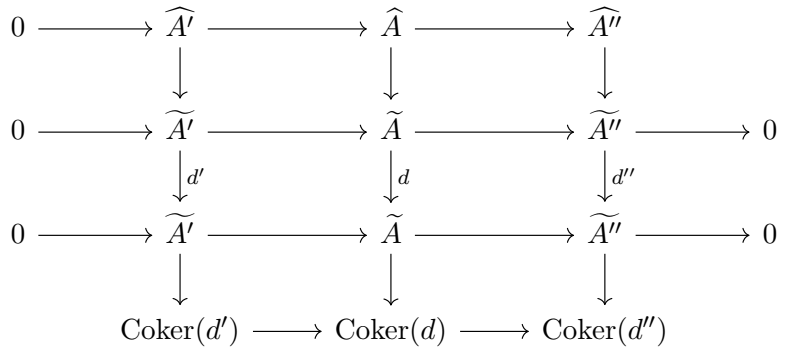
Рабоче крестьянское доказательство. Перейдём к точной последовательности:

$$0 \to A'/A_n \cap A' \to A/A_n \to A''/p(A_n)$$

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



и применить лемму о змее. Засчет сюръективности $\theta'\ \ \forall(b_n)$ 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 5. $\widehat{A}/\widehat{A_n} \cong A/A_n$.

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 6. *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 3. 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 12. $\operatorname{Ker}\left(A \to \widehat{A}\right) = \bigcap_{n=0}^{\infty} A_n$.

[4] что вполне логично.

1.13 Градуированные алгебры и модули

Определение 20. 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 5. *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*:

$$\mathrm{Bl}_I(R) = \bigoplus_{n=1}^{\infty} I^n.$$

2. Алгебраическая теория чисел

2.1 Алгебраические числа и целые алгебраические числа

Определение 21. 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 6. *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 $\exists a_0, \dots, a_n \in \mathbb{Q}$:

$$a_n\alpha^n + \dots + a_1\alpha + a_0 = 0.$$

Домножая на знаменатель, мы имеем нужный многочлен. □

Предложение 7. *Множество алгебраических чисел является полем.*

Доказательство. Пусть α — алгебраическое число. Тогда

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0,\ a_i \in \mathbb{Z}.$$

Но тогда $a_n + \dots + a_1\left(\alpha^{-1}\right)^{n-1} + a_0\left(\alpha^{-1}\right)^n = 0$, 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 22. $\alpha \in \mathbb{C}$ мы будем называть *целым алгебраическим числом*, если существует унитарный многочлен $p \in \mathbb{Z}[x]$, аннулирующий α.

Пример 4. $\sqrt{2}$ — целое алгебраическое число, а вот $\sqrt{2}/2$ — нет!

Предложение 8. *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 13. *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 23. 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.

2.2 След элемента и целый базис кольца $\mathcal{O}_K$

Заведём теперь некоторый полезный аппарат.

Определение 24. 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 $\mathrm{Tr}_{L/K}(\alpha)$.

У этого оператора есть характеристический многочлен χ_α. Выбрав базис L/K, мы можем записать матрицу оператора T_α и тогда

$$\chi_\alpha(t) = \det(Et - T_\alpha) = t^n - \mathrm{Tr}_{L/K}(\alpha)t^{n-1} + \dots$$

Если L/K — расширение Галуа, то можно определять след, как

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Соотвественно, след — это K-линейный функционал $L \to K$, то есть

$$\forall \alpha, \beta \in K \quad \mathrm{Tr}_{L/K}(\alpha a + \beta b) = \alpha \,\mathrm{Tr}_{L/K}(a) + \beta \,\mathrm{Tr}_{L/K}(b).$$

Кроме того, для $\alpha \in K$ $\mathrm{Tr}_{L/K}(\alpha) = [L : K] \cdot \alpha$. Кроме того, след хорошо ведёт себя относительно башни расширений. Если M — расширение K, а K — расширение L, то

$$\mathrm{Tr}_{M/K} = \mathrm{Tr}_{M/L} \circ \mathrm{Tr}_{L/K}.$$

Кроме того, след можно рассматривать и как невырожденную билинейную симметричную форму

$$K \times K \to \mathbb{Q}, \ (x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy).$$

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

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0 \implies (\sigma\alpha)^n + a_{n-1}(\sigma\alpha)^{n-1} + a_0 = 0 \implies \sigma\alpha \in \mathcal{O}_K$$

, 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 9. *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 $\mathbb{Q}$:

$$\alpha^n + c_{n-1}\alpha^{n-1} + \dots + c_1\alpha + c_0 = 0, \quad c_i \in \mathbb{Q}.$$

Запишем $c_i = \frac{b_i}{d}$, $b_i, d \in \mathbb{Z}$. Тогда, домножив равенство выше на d^n, мы получаем

$$(\alpha d)^n + b_{n-1}(\alpha d)^{n-1} + b_{n-2}d(\alpha d)^{n-2} + \dots + b_0 d^{n-1} = 0.$$

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 14. *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 15. *Кольцо $\mathcal{O}_K$ — нётерово.*

Доказательство. В самом деле, по теореме 14 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 5. 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 25. 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 $4(a^2+3b^2)=4a^2+12b^2\in4\mathbb{Z}\implies 12b^2\in4\mathbb{Z}$, 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 6. Если $K=\mathbb{Q}(i)$, то $\mathcal{O}_K=\mathbb{Z}[i]$.

Домашнее задание 1. 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

   $$21=3\cdot7=(1+2\sqrt{-5})(1-2\sqrt{-5})$$

   и покажите: что это два существенно различных разложения в произвдение простых.

2.3 Размерность кольца целых $\mathcal{O}_K$

Докажем теперь, что для любого числового поля K кольцо целых $\mathcal{O}_K$ одномерно.

Лемма 13. Пусть $K/\mathbb{Q}$ — конечное расширение и $0\neq I$ — идеал кольца $\mathcal{O}_K$. Тогда $I\cap\mathbb{Z}\neq0$, то есть I содержит целое число.

Доказательство. Возьмём $\alpha\in I$, $\alpha\neq0$. 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, $a_0\neq0$. 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 7. *Пусть I — ненулевой идеал в $\mathcal{O}_K$. Тогда $\mathcal{O}_K/I$ конечно.*

Доказательство. По лемме 13 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 16. *Кольцо $\mathcal{O}_K$ одномерно, т.е.* $\dim(\mathcal{O}_K) = 1$.

Доказательство. Пусть $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$. Тогда $\mathcal{O}_K/\mathfrak{p}$ — область целостности и конечно по следствию 7. Но тогда по задаче 2 в 1 $\mathcal{O}_K/\mathfrak{p}$ — 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 1, кольцо $\mathcal{O}_K$ далеко не всегда является областью главных идеалов.

2.4 Примеры евклидовых колец целых алгебраических чисел

Предложение 10. *Рассмотрим $K = \mathbb{Q}(\sqrt{-3})$. Тогда $\mathcal{O}_K$ — евклидово.*

Доказательство. Как мы убедились в примере 5,

$$\mathcal{O}_K \cong \mathbb{Z} \oplus \mathbb{Z}\omega, \quad \omega = \frac{1+\sqrt{-3}}{2}.$$

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 11. *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

$$y = a^3 - 6ab^2 = \pm 5 \implies y = \pm 5.$$

□

2.5 “Last Fermat’s theorem” для $n = 3$.

Все мы знаем следующее (важное для истории математики) утверждение:

Теорема 17 (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 12. *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 14. 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,

$$3\left(\frac{a}{3}\right)^2 + b^2 \vdots 3 \implies b \vdots 3,$$

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 слуачае $c = 0$ 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 $c, d \in \mathbb{Z}$. $\square$

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 $x \vdots 2,\ y \nmid 2,\ z \nmid 2$. 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 $q \nmid 3$. Тогда

$$\left(\frac{q}{4}, q^2 + 3p^2\right) = 1 \implies q^2 + 3p^2 = t^3.$$

Соответсвенно, мы попадаем в условие леммы 14:

$$\begin{cases} q^2 + 3p^2 = t^3 \\ p \not\equiv q \pmod 2 \\ (p, q) = 1 \end{cases} \underbrace{\implies}_{\text{Л. } 14} \begin{cases} q = s^3 - 9st^2 \\ p = 3t(s^2 - t^2) \end{cases}$$

С другой стороны, $q/4$ — тоже куб, а тогда

$$2q = 2s(s - 3t)(s + 3t) \text{ — тоже куб.}$$

Так как $q \nmid 3$, $s \nmid 3$. Кроме того, $s - 3t \nmid 2 \implies (s, s - 3t) = (s, s + 3t) = (s + 3t, s - 3t) = 1$, то есть мы имеем

$$\begin{cases} 2s = x_1^3 \\ 3t - s = y_1^3 \\ 3t + s = z_1^3 \implies x_1^3 + y_1^3 = z_1^3. \end{cases}$$

$|x_1|^3 = |2s| \leq |2q| < |x|^3$, 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 14:

$$\begin{cases} p = s(s^2 - 9t^2) \\ r = 3t(s^2 - t^2) \end{cases}.$$

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 $|x|$.

2.6 Целозамкнутость кольца $\mathcal{O}_K$

Определение 26. 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 18. *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 27. 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 7. $\mathbb{Z}$ — целозамкнуто.

Теорема 19. *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. □

2.7 Кольцо целых алгебраических чисел для квадратичного расщирения

Мы уже смотрели на некоторые примеры колец целых для квадратичных расширений. Сейчас мы докажем теорему, полностью описывающую их.

Теорема 20. *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 18, 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.

□

2.8 Разложение идеалов в произведение простых в кольцах целых числовых полей

Лемма 15. 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 28. 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 8. 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 16. 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 15 найдутся такие ненулевые $\mathfrak{p}_1, \dots, \mathfrak{p}_k \in \operatorname{Spec} \mathcal{O}_K$, что $\mathfrak{p}_1 \dots \mathfrak{p}_k \subset (a)$.

Так как I — собственный, а кольцо $\mathcal{O}_K$ одномерно, I лежит в некотором простом идеале $\mathfrak{p}$. Так мы получаем цепочку включений

$$\mathfrak{p}_1 \dots \mathfrak{p}_k \subset (a) \subset \mathfrak{p} \implies \exists i \colon \mathfrak{p}_i \subset \mathfrak{p}.$$

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

$$\mathfrak{p}_2 \dots \mathfrak{p}_k \not\subset (a) \implies \exists b \in \mathfrak{p}_2 \dots \mathfrak{p}_k \setminus (a).$$

Тогда мы можем взять $x = \frac{b}{a}$ и он подойдёт. В самом деле,

$$xI = \frac{b}{a} I \subset \frac{b}{a}\mathfrak{p}_1 \underbrace{\subset}_{b \in \mathfrak{p}_2 \dots \mathfrak{p}_k} \frac{\mathfrak{p}_1 \dots \mathfrak{p}_k}{a} \subset \frac{(a)}{a} = \mathcal{O}_K$$

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 17. 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 $\mathfrak{p} = (u_1, \dots, u_n)$, тогда если $\alpha \in \mathfrak{p}^{-1} \setminus \mathcal{O}_K$ (тут мы пользуемся леммой 16), 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 21 (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 18. 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 17 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 16. 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 29. Пусть $I \subset K$. I называется *дробным идеалом*, если $\exists x \neq 0\colon xI \subset \mathcal{O}_K$ — идеал.

Пример 9. I^{-1} — дробный идеал.

Предложение 13. *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 21 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 10. Для кольца $\mathbb{Z}$ дробные идеалы соотвествуют рациональным числам.

Домашнее задание 2. 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* $\mathfrak{p}$.

2.9 Дискриминант

Определение 30. Пусть K/F — конечное сепарабельное расширение, $[K:F] = n$ и $\alpha_1, \ldots, \alpha_n \in K$. Тогда *дискриминант* набора $\alpha_1, \ldots, \alpha_n$ — это

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \stackrel{\text{def}}{=} \det\bigl(\operatorname{Tr}_{K/F}(\alpha_i\alpha_j)\bigr).$$

Так как расширение K/F сепарабельно, у нас есть ровно $n = [K:F]$ вложений $\sigma_1, \ldots, \sigma_n \colon K \to \mathbb{C}$ (на самом деле, мы знаем, что в $\mathbb{Q}^{alg}$).

Предложение 14. $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = (\det(\sigma_i(\alpha_j))^2$.

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 $(\beta_1, \ldots, \beta_n) = (\alpha_1, \ldots, \alpha_n)M,\ M \in M_n(F)$.

Предложение 15. $\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) \cdot (\det M)^2$.

Доказательство. Действительно, это напрямую следует из предложения 14:

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \det(\sigma_i(\beta_j))^2 = \det\left(\sigma_i(\alpha_j)M\right)^2 = \operatorname{disc}(\alpha_1, \ldots, \alpha_n) \cdot (\det M)^2.$$

□

Предложение 16. $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = 0 \Leftrightarrow \alpha_1, \ldots, \alpha_n$ *— 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 15 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

$$\operatorname{Tr}_{K/F}((x_1\alpha_1 + \ldots + x_n\alpha_n)\alpha_j) = 0, \ldots 1 \leq j \leq n.$$

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[5].

□

[5]Этим утверждением из теорией полей мы пользуемся без доказательств. Доказательство этого утверждения можно прочитать в S. Lang “Algebra”.

Лемма 19. 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 14, $\mathcal{O}_K$ — 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 31. 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

$$(\omega_1, \ldots, \omega_n)M = (u_1, \ldots, u_n), \quad M \in \mathrm{SL}_n(\mathbb{Z}).$$

$$(u_1, \ldots, u_n)M^{-1} = (\omega_1, \ldots, \omega_n)$$

$$\operatorname{disc}(u_1, \ldots, u_n) = \operatorname{disc}(\omega_1, \ldots, \omega_n) \cdot \underbrace{(\det M)^2}_{=1}$$

Определение 32 (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 17. *В описанной выше сиутации* $\operatorname{disc}(1, \theta, \ldots, \theta^{n-1}) = \operatorname{ind}(\theta)^2 \cdot \operatorname{disc}(K)$.

Доказательство. Пусть $\omega_1, \ldots, \omega_n$ — целый базис. Тогда

$$(1, \theta, \ldots, \theta^{n-1}) = (\omega_1, \ldots, \omega_n)M \implies \operatorname{disc}(1, \ldots, \theta^{n-1}) = \operatorname{disc}(K)(\det M)^2.$$

Нетрудно заметить, что по лемме 19 для $\mathbb{Z}[\theta] = B \subset A = \mathcal{O}_K$ мы имеем $|\det M| = \operatorname{ind}(\theta)$.

□

Пример 11. 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 17 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 12. 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 $\frac{\theta+\theta^2}{2} \in \mathcal{O}_K, \notin \mathbb{Z}[\theta]$, $\operatorname{ind}(\theta) \ne 1$. 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 3. Задачи:

1. Предположим, что K/F — расширение Галуа, $[K : F]$ — нечётна. Докажите, что тогда для любого базиса $e_1, \ldots, e_n$ расширения K/F будет выполнено $\operatorname{disc}(e_1, \ldots, e_n) \in F^{*^2}$.

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 30.
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 $\upsilon_p(a_0) = 1$ и $\upsilon_p(a_i) \geq 1$. Докажите, что тогда $p \not| \operatorname{ind}(\theta)$.
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 $\alpha \in K^* \colon \upsilon_{\mathfrak{p}_i}(\alpha) = n_i \; \forall 1 \leq i \leq n_k$.
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 22. *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 $\operatorname{disc}(1, \zeta, \dots, \zeta^{p-2}) = \det\big(\operatorname{Tr}(\zeta^{i+j})\big)_{i,j=1}^{n}$. Ясно, что для каждого $i = 2, \dots, p-2$ найдётся единственный $j = 2, \dots, p-2$ такой, что $i + j \equiv 0 \pmod p$[6]. 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 $\operatorname{disc}(1, \zeta, \dots, \zeta^{p-2}) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

[6] Действительно, это $p - i$.

Теперь воспользуемся одной из домашних задач. Заметим, что в нашем случае совершенно ясно, что минимальный многочлен ζ Эйзенштейнов, а тогда $\mathrm{ind}(\zeta) \not\vdots p$. С другой стороны, по предложению 17 $\mathrm{ind}(\zeta) \mid \mathrm{disc}(1, \zeta, \dots, \zeta^{p-2})(-1)^{\frac{p-1}{2}} p^{p-2}$. Значит, $\mathrm{ind}(\theta) = 1$ то есть

$$|\mathcal{O}_K/\mathbb{Z}[\theta]| = 1 \implies \mathcal{O}_K = \mathbb{Z}[\theta].$$

□

Теорема 23 (Д/З №7, задача 2). *Пусть $K = \mathbb{Q}\big(\sqrt[n]{1}\big)$, 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 20. Пусть $K/\mathbb{Q}$ — конечное сепарабельное расширение, $K = \mathbb{Q}(\theta),\ \theta \in \mathcal{O}_K$, $[K : \mathbb{Q}] = n$. Тогда

$$\mathrm{disc}(1, \theta, \theta^2, \dots, \theta^{n-1}) = \prod_{i \neq j}(\sigma_i(\theta) - \sigma_j(\theta)) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{K/F}(f'(\theta)),\ \text{где}$$

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

$$\mathrm{disc}(1, \theta, \dots, \theta^{n-1}) = \det(\sigma_i(\theta^{j-1}))^2.$$

Так как $\sigma_i(\theta^{j-1}) = \sigma_i(\theta)^{j-1}$, матрица в правой части равенства представляет из себя матрицу Вандермонда, а тогда

$$\det \begin{pmatrix} 1 & \sigma_1(\theta) & \dots & \sigma_1(\theta)^{n-1} \\ 1 & \sigma_2(\theta) & \dots & \sigma_2(\theta)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_n(\theta) & \dots & \sigma_n(\theta)^{n-1} \end{pmatrix} = \prod_{i<j}(\sigma_j(\theta) - \sigma_i(\theta)).$$

Возводя в квадрат, получаем

$$\mathrm{disc}(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j}(\sigma_j(\theta) - \sigma_i(\theta))^2.$$

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

$$\Phi_{p^n}(x)=\frac{x^{p^n}-1}{x^{p^{n-1}}-1},\quad \mathrm{disc}(1,\zeta_{p^n},\dots,\zeta_{p^n}^{\varphi(p^n)-1}).$$

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

$$\begin{pmatrix}\alpha_1&0&0&\dots&0\\ 0&\alpha_2&0&\dots&0\\ 0&0&\alpha_3&\dots&0\\ \vdots&\vdots&\vdots&\ddots&\vdots\\ 0&0&0&\dots&\alpha_{nn}\end{pmatrix}$$

2.10 Норма идеала

Определение 33. Пусть $K/\mathbb{Q}$ — конечное расширение, $0 \neq I \subset \mathcal{O}_K$ — идеал. Тогда, как мы знаем из теоремы 7, $|\mathcal{O}_K/I| < \infty$. *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 18. *Пусть* $a \in \mathcal{O}_K$, *тогда* $\mathrm{N}((a)) = \left|\mathrm{N}_{K/\mathbb{Q}}(a)\right|$.

Доказательство. Пусть $\omega_1, \ldots, \omega_n$ — 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 19 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 3.

Лемма 21 (Задача 5 из ДЗ 3)**.** Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ — максимальные идеалы кольца $\mathcal{O}_K$, $n_1, \ldots, n_k \in \mathbb{Z}$. Докажите, что существует $\alpha \in K^*\colon \upsilon_{\mathfrak{p}_i}(\alpha) = n_i\ \forall 1 \leq i \leq n_k$.

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 22 (Задача 6 из ДЗ 3)**.** 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 21 $\widetilde{y} \in \mathcal{O}_K\colon \upsilon_{\mathfrak{q}_i}(\widetilde{y}) = r_i,\ \upsilon_{\mathfrak{p}_i}(\widetilde{y}) = 0$, 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 24 (Задача 7 из ДЗ 3)**.** *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 22 (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 4 (Осторожно, открытая задача)**.** Существует ли кольцо, в котором каждый идеал порождается тремя элементами, причём, есть идеал, который не порождается двумя элементами.

Теорема 25 (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 22 найдём $x \in K^*$: $xI + J = \mathcal{O}_K$. Тогда воспользуемся теоремой о гомоморфизме и взаимной простотой:

$$|\mathcal{O}_K/J| = |(xI + J)/J| = |xI/xI \cap J| = |xI/xIJ| = |I/IJ|\,.$$

□

2.11 Индекс ветвления и степень инерции

Определение 34. 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 $\mathfrak{p} \in \mathrm{Specm}(\mathcal{O}_K)$, 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 35. Как известно, для $\mathfrak{p} \in \mathrm{Spec}\,\mathcal{O}_K$ 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,

$$p^n = \mathrm{N}_{K/\mathbb{Q}}(p) \underbrace{=}_{\text{Предл. } 18} \mathrm{N}(p\mathcal{O}_K),$$

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:

$$\sum_{i=1}^{k} e_i f_i = n. \tag{1}$$

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 $\mathrm{Specm}\,\mathcal{O}_K$ (т.е. $\forall \mathfrak{p} \in \mathrm{Specm}(\mathcal{O}_K)\ \sigma\mathfrak{p} \in \mathrm{Specm}(\mathcal{O}_K)$), так как $\forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})\ \mathcal{O}_K/\mathfrak{p} \cong \sigma\mathcal{O}_K/\sigma\mathfrak{p} \cong {}^{7}\mathcal{O}_K/\sigma\mathfrak{p}$.

Определение 36. Если $\mathfrak{p} \in \mathrm{Specm}(\mathcal{O}_K)$ 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 26. *Действие* $\mathrm{Gal}(K/\mathbb{Q})$ *на множестве простых идеалов, висящих над простым числом* p.

Доказательство. Предположим, что есть два простых идеала $\mathfrak{p}, \widetilde{\mathfrak{p}}\colon\ \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z} = \widetilde{\mathfrak{p}} \cap \mathbb{Z}$, 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 $\widetilde{\mathfrak{p}} \in \mathrm{Spec}\,\mathcal{O}_K, \exists \tau \in \mathrm{Gal}(K/\mathbb{Q})\colon \tau x \in \widetilde{\mathfrak{p}} \Leftrightarrow x \in \tau^{-1}\widetilde{\mathfrak{p}}$. Но, с дугой стороны, ранее мы отметили, что $\forall \tau \in \mathrm{Gal}(K/\mathbb{Q})\ \tau x \equiv 1 \pmod{\widetilde{\mathfrak{p}}}$. □

Следствие 8. *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. □

[7] В самом начале курса мы уже отмечали, что $\forall \alpha \in \mathcal{O}_K,\ \forall \sigma \in \mathrm{Gal}(K/\mathbb{Q})\ \sigma\alpha \in \mathcal{O}_K$.

Тогда равенство (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 5. 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 $x \in \mathcal{O}_K : px \in \mathbb{Z}[\theta]$. 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 3, 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.

2.12 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 37. 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 27. *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

$$S = \left\{ \sum_{i=1}^{n} x_i\omega_i \;\middle|\; 0 \le x_i \le \left[\mathrm{N}(J)^{\frac{1}{n}}\right] \right\}, \quad |S| > \left(|\,\mathrm{N}(J)|^{\frac{1}{n}}\right)\mathrm{N}(J) = |\mathcal{O}_K/J|.$$

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 13. Вычислим группу классов идеалов для поля $K = \mathbb{Q}\left(\sqrt{-14}\right)$.

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

$$\mathrm{N}_{K/\mathbb{Q}}(a + b\sqrt{-14}) = a^2 + 14b^2 \neq 2 \implies \mathfrak{p}_2 - \text{не может быть главным идеалом,}$$

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: 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 6. 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 $\mathcal{O}_K^* = \{x \in K \mid \operatorname{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z}\ \forall y \in \mathcal{O}_K\}$.
   (a) Доказать, что $\mathcal{O}_K^*$ — дробный идеал и $\mathcal{O}_K \subset \mathcal{O}_K^*$.
   (b) Доказать, что $|\operatorname{disc}(K)| = |\mathcal{O}_K^*/\mathcal{O}_K|$.
   (c) Доказать, что $|\operatorname{disc}(K)|$ есть норма некоторого идеала в $\mathcal{O}_K$.
3. Пусть V — конечномерное векторное пространство над полем F, $A \in \operatorname{End}(V)$, причём A — нильпотентный. Докажите, что тогда $\operatorname{Tr}(A) = 0$.
4. Пусть I — дробный идеал. Докажите, что как абелева группа $d(\mathrm{N}(I))$ (дробный идеал в $\mathbb{Z}$) порождается элементами $\mathrm{N}(x), x \in I$.

2.13 Дифферента и ветвление

Определение 38. 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 неравзетвлено, 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 *неравзветвлённым.*

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 39. *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 19. $\mathrm{N}(\mathcal{D}) = |\mathrm{disc}(K)|$.

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 19 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 28. *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 23 (Задача 3 ДЗ 6)**.** 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 23 мы получим вот такое следствие:

Следствие 9. *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 23 $\mathrm{Tr}(\overline{x}) = 0$ (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 9 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 20. *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 20. 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 20 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

$$\begin{cases} \frac{x}{p} \in \mathfrak{p}^{-1} \\ \mathrm{Tr}\left(\frac{x}{p}\right) \notin \mathbb{Z} \end{cases} \quad \Longrightarrow \ \frac{x}{p} \notin \mathcal{O}_K^* \ \Longrightarrow \ \mathfrak{p}_1^{-1} \not\subset \mathcal{O}_K^* \ \Longrightarrow \ \mathcal{D} \not\subset \mathfrak{p}_1,$$

что мы и хотели доказать. □

Теорема 29. *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 28 $\mathcal{D} \subset \mathfrak{p}_1$, но тогда

$$|\mathrm{disc}(K)| = \mathrm{N}(\mathcal{D}) \vdots \mathrm{N}(\mathfrak{p}_1) = p^{f_1} \ \Longrightarrow \ \mathrm{disc}(K) \vdots p.$$

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, $\mathcal{D} \not\subset \mathfrak{p}_i \ \Longrightarrow \ \mathfrak{p}_i \neq \mathfrak{q}_j$ 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.

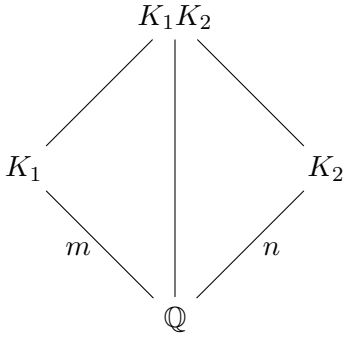
2.14 Кольцо целых композита расширений

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 30. *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 $\tau_i,\ 1 \le i \le m$ — вложения K_1 в $\mathbb{Q}^{alg}$, а $\sigma_i,\ 1 \le i \le n$ — 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 $\mathrm{disc}(K_1) \cdot a_{ij} \in \mathbb{Z}$. Заметим, что такое же рассуждение мы могли проделать, заменив u_i на v_j в определении β_j, и получить, что $\mathrm{disc}(K_1)a_{ij} \in \mathbb{Z}$. Тогда, так как $(\mathrm{disc}(K_1), \mathrm{disc}(K_2)) = 1$, мы имеем $a_{ij} \in \mathbb{Z}$. □

Домашнее задание 7. 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 $\upsilon_p(a_0) = 1$ и $\upsilon_p(a_i) \ge 1$. Докажите, что тогда $p \not| \ \mathrm{ind}(\theta)$. *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.
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 $a_1, \ldots, a_n \in \mathbb{Q}, \quad b_1, \ldots, b_n \in \mathbb{Q},\ b_i > 0, k \ge 2$ 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 31 (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

$$x = a^2 + d, \quad y = \pm a(a^2 - 3d).$$

2.15 Теорема Куммера

Начнём с вот такой полезной леммы:

Лемма 24. Следующие условия равносильны:

1. $p \not| \operatorname{ind}(\theta) = |\mathcal{O}_K/\mathbb{Z}[\theta]|$.
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 $p \not| |\mathcal{O}_K/\mathbb{Z}[\theta]| = \operatorname{ind}(\theta)$.

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 32 (Куммер). *Пусть $K = \mathbb{Q}(\theta)$, $\theta \in \mathcal{O}_K$, а p — такое простое число, что $p \not| \operatorname{ind}(\theta)$. Пусть f — минимальный многочлен θ, причем над полем $\mathbb{Z}/p\mathbb{Z}$ его редукция $\overline{f}$ раскладывается в непривыодимые, 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:

$$\mathcal{O}_K/\mathfrak{p}_i = \mathcal{O}_K/(g_i(\theta), p) \underbrace{=}_{\text{Л. 24.}} \mathbb{Z}[\theta]/(g_i(\theta), p) \cong \mathbb{Z}[t]/(f(t), p, g_i(t)) \cong \mathbb{F}_p[t]/\overline{g_i},$$

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 33. *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 24)

$$\mathbb{Z}[\theta]/(p) \cong \mathcal{O}_K/(p).$$

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 32 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 33 $p \not| \operatorname{ind}(\zeta_m)$, то есть мы можем применить теорему Куммера 32:

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdot \ldots \mathfrak{p}_k, \quad \mathfrak{p}_i = (p, g_i(\zeta_m)).$$

С другой стороны, так как $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ — расширение Галуа, все степени инерции равны. Значит, достаточно вычислить хотя бы одну.

Предложение 21. *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

$$\{1, \theta, \ldots, \theta^{m-1}\} = \langle\theta\rangle \leq (\mathbb{F}_p[x]/(g_1))^*.$$

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 8. Задачи:

1. Рассмотрим кубическое расширение $K = \mathbb{Q}(\sqrt[3]{15}) = \mathbb{Q}(\rho)$.
   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 $K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_k})$, 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.

2.16 Первый случай Last Fermat's theorem

Мы можем полагать, что показатель n — простое число, а также рассматривать уравнение в виде

$$x^p + y^p + z^p = 0, \quad (x,y,z) = 1. \tag{2}$$

Первым случаем Большой теоремы Ферма называют доказательство большой теоремы ферма в предположениии $p \nmid xyz$.

Теорема 34 (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

$$x^p + y^p + z^p = 0 \Leftrightarrow x^{\frac{q-1}{2}} + y^{\frac{q-1}{2}} + z^{\frac{q-1}{2}} = 0., \quad p = \frac{q-1}{2}. \tag{3}$$

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 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 $ABC \not\vdots q$. 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

$$T^{\frac{q-1}{2}} \equiv \pm 1 \pmod q \implies py^{p-1} \equiv \pm 1 \pmod q. \tag{4}$$

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 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 9. 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 22. *Простое число p полностью разветвлено в $\mathbb{Q}(\zeta_p)$.*

Доказательство.

$$x^p - 1 = (x-1)(x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{p-1}) = (x-1)(x^{p-1} + \ldots + x + 1).$$

$$x^{p-1} + \ldots + x + 1 = (x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{p-1})$$

Подставим $x = 1$ и от числового равенства перейдём к равенству идеалов:

$$p\mathcal{O}_K = (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{p-1}).$$

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

$$(1-\zeta) = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_k \implies p\mathcal{O}_K = ((1-\zeta))^{p-1} = \mathfrak{p}_1^{p-1}\mathfrak{p}_2^{p-1}\ldots\mathfrak{p}_k^{p-1},$$

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 25. Пусть p — простое число, не равное двум. Множество корней из единицы[8] 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 $n_0 \vdots p'$,

$$\mathbb{Q}(\zeta_{p'}) \le \mathbb{Q}(\zeta_{n_0}) \le \mathbb{Q}(\zeta_p).$$

Но тогда по предложению 22 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 $\mathbb{Q}(\zeta_{p^a}) \le \mathbb{Q}(\zeta_p)$. С другой стороны, тогда

$$[\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}] = p^a - p^{a-1} \le [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 \implies a = 1 \implies n_0 = p.$$

□

Лемма 26. Пусть $K/\mathbb{Q}$ — конечное расширение, $\sigma_i \colon K \to \mathbb{Q}^{alg}$ — все вложения ($1 \le i \le n$, $n = [K : \mathbb{Q}]$). Предположим, что $\alpha \in \mathcal{O}_K$ и $\forall i\ |\sigma_i\alpha| \le 1$. Тогда α является корнем из единицы какой-то степени. [9]

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 $|\sigma_i(\alpha^k)| \le 1$, 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. □

Лемма 27. 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 26:

$$\rho(v) = \frac{\rho(u)}{\rho(\overline{u})} = {}^{10}\frac{\rho(u)}{\overline{\rho(u)}} \implies |\rho(v)| = 1.$$

Значит, по лемме 26 v — является корнем из единицы какой-то степени, а тогда по лемме 25 $v = \pm\zeta^n$.

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

$$-\overline{u} \equiv \overline{u} \pmod\lambda \implies 2\overline{u} \equiv 0 \pmod\lambda,$$

[8] не обязательно степени p

[9] Обратное утверждение очевидно.

[10] Так как сопряжение — тоже автоморфизм, а группа Галуа абелева, $\rho(\overline{x}) = \overline{\rho(x)}$

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 22, $((1-\zeta)^{p-1}) = p\mathcal{O}_K$, 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 28. 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 $(1-\zeta) \in \operatorname{Specm}(\mathcal{O}_K)$ (что мы доказывали в 22), $\mathfrak{q} = (1-\zeta)$. 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.

Теорема 35. *Пусть $p \nmid |\mathcal{C}\ell(\mathbb{Q}(\zeta_p))$[11]. 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 28, 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 27 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

$$\alpha^p \equiv \underbrace{a_0^p + a_1^p + \ldots + a_{p-2}^p}_{\stackrel{\text{def}}{=} n} \pmod{p}.$$

[11] такие простые числа называются *регулярными*

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.
   (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 40. 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 23.

$$-(n+1)B_n = \binom{n+1}{n-1}B_{n-1} + \ldots + \binom{n+1}{k}B_k + \ldots + \binom{n+1}{1}B_1 + 1.$$

Следствие 10. *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 36. *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 14. 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.

2.17 Алгоритм построения целого базиса

Итак, для $d = \mathrm{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ 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 10. 1.

> **Теорема 37** (Штикельберг)**.** *Дискриминант конечного расширения $K/\mathbb{Q}$ сравним с нулём или единицей по модулю 4.*
> *Hint:* Можно действовать так: $\mathrm{disc}(K) = (\det(\sigma_i))^2$, 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 $\mathrm{disc}(K) = (P-N)^2 = (P+N)^2 - 4PN$. Значит, достаточно показать, что числа $P+N$ и PN — целые. *Hint:* Целое число — это рациональное число, которое еще и целое алгебраическое.

2.

2.18 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 15. Картинка для $L \subset \mathbb{R}^2$.

Предложение 24. *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 25. *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*

$$\Delta = \left\{ \sum_{i=1}^{m} x_i e_i \;\middle|\; 0 \leq x_i < 1 \right\}$$

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

$$m = \dim \operatorname{span}(A_0) \leq \dim \operatorname{span}(A_1) = \dim \langle u_1, \ldots, u_m \rangle.$$

□

Это предложение даёт хороший критерий для проверки, является ли какое-то подпространство решёткой.

Определение 41. Если $L \leq \mathbb{R}^n$ — решётка с порождающим набором $e_1, \ldots, e_m$, то множество

$$\Delta = \left\{ \sum_{i=1}^{m} x_i e_i \;\middle|\; 0 \leq x_i < 1 \right\}$$

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 29. 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

$$\operatorname{Vol}(T) \leq \operatorname{Vol}(\Delta).$$

Доказательство. В самом деле, так как множества $T + \ell$ дизъюнктны,

$$\operatorname{Vol}(\Delta) \geq \sum_{\ell \in L} \operatorname{Vol}(\Delta \cap T_\ell) = \sum_{\ell \in L} \operatorname{Vol}(\Delta_{-\ell} \cap T) = \operatorname{Vol}\left(\bigcup_{\ell \in L} \Delta_\ell \cap T \right) = \operatorname{Vol}(\mathbb{R}^m \cap T) = \operatorname{Vol}(T).$$

□

Лемма 30 (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 $\exists 0 \neq \ell \in L \colon \ell \in T$. Кроме того, если T компактно, то это будет верно и в случае нестрогого неравенства $\operatorname{Vol}(T) \geq 2^n \operatorname{Vol}(\Delta)$.

Доказательство. Рассмотрим тело $\frac{1}{2}T$, тогда $\operatorname{Vol}\left(\frac{1}{2}T\right) = \frac{1}{2^n} \operatorname{Vol}(T) > \operatorname{Vol}(\Delta)$. Тогда по предыдущей лемме 29 $\exists \ell_1, \ell_2 \in L \colon \frac{1}{2}T_{\ell_1} \cap \frac{1}{2}T_{\ell_2} \neq \varnothing$. 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 42. 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 $\operatorname{Im}(\sigma_i) \subset \mathbb{R}$. 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 $\operatorname{disc}(K)$, пользуясь предложением 17

$$\mathrm{Vol}(\Delta) = \left|\det\left(\begin{pmatrix}\varphi(\alpha_1)\\ \varphi(\alpha_2)\\ \vdots\\ \varphi(\alpha_n)\end{pmatrix}\right)\right| = \frac{1}{2^t}\sqrt{|\operatorname{disc}(\alpha_1, \ldots, \alpha_n)|} = \frac{1}{2^t}\sqrt{|\operatorname{disc}(K)| \cdot [\mathcal{O}_K : I]^2} = \frac{1}{2^t}\,\mathrm{N}(I)\sqrt{|\operatorname{disc}(K)|}.$$

Рассмотрим теперь для некоторого фиксированного $a > 0$.

$$T = \left\{(x_1, x_2, \ldots, x_s, y_1, z_1, \ldots, y_t, z_t) \middle| \ |x_1| + \ldots + |x_s| + 2\sqrt{y_1^2 + z_1^2} + \ldots + 2\sqrt{y_t^2 + z_t^2} \le a\right\}.$$

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 $0 \ne I \subset \mathcal{O}_K$ будет выполнено неравенство

$$2^s\left(\frac{\pi}{2}\right)^t\frac{a^n}{n!} > 2^n\frac{\sqrt{|\operatorname{disc}(K)|}}{2^t}\,\mathrm{N}(I). \tag{5}$$

Тогда по лемме Минковского 30 $\exists 0 \ne \alpha \in I$:

$$|\sigma_1(\alpha)| + \ldots + |\sigma_s(\alpha)| + 2|\sigma_{s+1}(\alpha)| + \ldots + 2|\sigma_{s+t}(\alpha)| \le a.$$

Это неравенство мы можем переписать в виде:

$$|\sigma_1(\alpha)| + \ldots + |\sigma_s(\alpha)| + |\sigma_{s+1}(\alpha)| + |\overline{\sigma_{s+1}}(\alpha)| + \ldots + |\sigma_{s+t}(\alpha)| + |\overline{\sigma_{s+t}}(\alpha)| \le a.$$

Тогда по неравенству о средних мы имеем

$$\left|\sigma_1(\alpha)\cdot\ldots\cdot\sigma_s(\alpha)\sigma_{s+1}(\alpha)\overline{\sigma_{s+1}(\alpha)}\cdot\ldots\cdot\sigma_{s+t}(\alpha)\overline{\sigma_{s+t}}(\alpha)\right| \le \left(\frac{a}{n}\right)^n \Leftrightarrow \mathrm{N}(\alpha) \le \left(\frac{a}{n}\right)^n$$

Заметим, что в неравенстве (5) равенство будет достигаться при

$$a^n = \frac{2^n\sqrt{|\operatorname{disc}(K)|}\,\mathrm{N}(I)n!}{2^t 2^s}\cdot\left(\frac{2}{\pi}\right)^t = \left(\frac{4}{\pi}\right)^t n!\,\mathrm{N}(\alpha)\sqrt{|\operatorname{disc}(K)|}.$$

В этом случае будет выполняться неравенство

$$\mathrm{N}(\alpha) \le \left(\frac{a}{n}\right)^n = \left(\frac{4}{\pi}\right)^t\frac{n!}{n^n}\,\mathrm{N}(I)\sqrt{\operatorname{disc} K}.$$

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 38. *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 $\alpha \in I$:

$$\mathrm{N}(\alpha) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\,\mathrm{N}(I)\sqrt{\operatorname{disc} K}.$$

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,

$$|\,\mathrm{N}(\alpha)| \leq \left(\frac{4}{\pi}\right)^t \cdot \frac{n!}{n^n}\,\mathrm{N}(I)\sqrt{|\operatorname{disc}(K)|}.$$

$$\mathrm{N}(\underbrace{\alpha I^{-1}}_{\text{целый}}) = \mathrm{N}(\alpha)\,\mathrm{N}\big(I^{-1}\big) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\operatorname{disc}(K)|}.$$

Но, как мы уже замечали, существует лишь конечное число целых идеалов с ограниченной нормой. Значит, мы получили еще одно (геометрическое) доказательство теоремы 27.

Пример 16. Рассмотрим $K = \mathbb{Q}\big(\sqrt[3]{6}\big)$. 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

$$\operatorname{disc}(K)\cdot(\operatorname{ind}(\theta))^2 = \operatorname{disc}(1,\theta,\theta^2) = \det\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) \\ \mathrm{Tr}(\theta) & \mathrm{Tr}(\theta^2) & \mathrm{Tr}(\theta^3) \\ \mathrm{Tr}(\theta^2) & \mathrm{Tr}(\theta^3) & \mathrm{Tr}(\theta^4) \end{pmatrix} = \det\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 18 \\ 0 & 18 & 0 \end{pmatrix} = -2^2 3^5.$$

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:

$$\mathrm{N}(\underbrace{\alpha I^{-1}}_{\text{целый}}) = \mathrm{N}(\alpha)\,\mathrm{N}\big(I^{-1}\big) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\operatorname{disc}(K)|} = \frac{4}{\pi}\cdot\frac{6}{27}\cdot\sqrt{2^5\cdot 3^5} < \frac{16}{\sqrt{3}} < 10.$$

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 32 легко понять, что

$$2\mathcal{O}_K = (2,\theta)^3 = (\theta-2)^3,$$

так как $\mathrm{N}(\theta - 2) = -2 \implies (\theta - 2)$ — 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, $\mathrm{N}(\theta) = 6,\ \mathrm{N}(\theta - 2) = -2$, откуда $\mathrm{N}\left(\frac{\theta}{\theta-2}\right) = -3$, то есть $\frac{\theta}{\theta-2}$ — простой, висящий над тройкой, $(3, \theta) = \left(\frac{\theta}{\theta-2}\right)$.

Теперь, опять же из теоремы Куммера 32, 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, $\mathrm{N}(\theta - 1) = 5$ 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

$$\frac{7}{\theta + 1} = \frac{7(\theta^2 - \theta + 1)}{\theta^3 + 1} \implies (7, \theta + 1) = (\theta + 1).$$

$$\mathrm{N}(\theta - 3) = 21, \mathrm{N}\left(\frac{\theta}{\theta - 2}\right) = -2 \implies \mathrm{N}\left(\frac{(\theta - 3)(\theta - 2)}{\theta}\right) = -7$$

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 17. 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 11. 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 $\mathrm{Cl}(\mathbb{Q}(\sqrt{-23})) = \mathbb{Z}/3\mathbb{Z}$.

2.19 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 18. 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

$$\mathrm{N}(x + y\sqrt{d}) = x^2 - dy^2 = \pm 1 \tag{6}$$

и из другого описания $\mathcal{O}_K^*$ мы получаем, что все решения уравнения (6) имеют вид $\{\pm\theta^m \mid m \in \mathbb{Z}\}$. Из этого, например, следует, что решений уравнения (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 (6) имеет конечно число решение.

Теорема 39 (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

$$\ell(\alpha) = \big(\log|\sigma_1\alpha|, \log|\sigma_2\alpha|, \dots, \log|\sigma_s\alpha|, \log|\sigma_{s+1}\alpha|^2, \dots, \log|\sigma_{s+t}\alpha|^2\big).$$

Заметим, что это гомоммомрфизм 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:

$$\alpha \in \operatorname{Ker}\ell \Leftrightarrow \forall i = 1, \dots, s+t \quad |\sigma_i\alpha| = 1 \underbrace{\Longrightarrow}_{\text{Л. 26}} \operatorname{Ker}\ell = \mu.$$

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 31. $\operatorname{Im}\ell$ — 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

$$\log|\sigma_j\alpha| \le r\ \forall j \Leftrightarrow |\sigma_j\alpha| \le e^r\ \forall j = 1, \dots, s, \quad |\sigma_j\alpha| < e^{\frac{r}{2}}\ \forall j = s+1, \dots, s+t.$$

Нетрудно заметить, что из этих неравенств следуют неравенства на мнимую и вещественную часть координат $s+1, \dots, s+t$, то есть мы имеем

$$|\sigma_j\alpha| \le e^r\ \forall j = 1, \dots, s, \quad |\operatorname{Im}\sigma_j\alpha| \le e^{\frac{r}{2}},\ |\operatorname{Re}\sigma_j\alpha| \le e^{\frac{r}{2}}\ \forall j = s+1, \dots, s+t.$$

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 24 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 25 $\operatorname{Im}\ell$ — 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, $m \le s+t-1$. 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 $\operatorname{Im}\ell \cong \mathbb{Z}^m, m \le s+t-1$, а значит

$$0 \to \mu \hookrightarrow \mathcal{O}_K^* \xrightarrow{\ell} \mathbb{Z}^m \to 0, \quad m \le s+t-1.$$

откуда $\mathcal{O}_K^* \cong \mu \oplus \mathbb{Z}^m, \quad m \le s+t-1.$ □

Даже слабая форма теоремы Дирихле о единицах позволяет успешно вычислять мультипликативные группы колец целых числовых полей.

Пример 19. Из 2.21 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 $m \le 1$, 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 26. *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 $\mu_2 = \{\pm 1\}$

$$1 - 6\theta + 3\theta^2 = \pm\alpha^d, \quad d \geq 2.$$

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:

$$\pm 1 = \mathrm{N}(\varepsilon) = \varepsilon \cdot \varepsilon' \cdot \varepsilon''.$$

$$\begin{cases} |\varepsilon'| = |\varepsilon''| \\ |\varepsilon\varepsilon'\varepsilon''| = 1 \end{cases} \implies |\varepsilon'| = |\varepsilon''| = \sqrt{|\varepsilon|^{-1}} = \sqrt{|109 + 60\theta + 33\theta^2|} < \sqrt{109 + 60 \cdot 2 + 33 \cdot 4} = \sqrt{361} = \sqrt{19}.$$

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 $|\alpha| = |\varepsilon|^{\frac{1}{d}} < 1$[12], 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,

$$\pm 1 = \mathrm{N}(\alpha) = x^3 + 6y^3 \implies x^3 \equiv \pm 1 \pmod 3 \implies x \equiv \pm 1 \quad (3) \equiv x^3 \equiv \pm 1 \pmod 9,$$

а тогда $y \vdots 9$ и отсюда $y = 0$, но тогда $\alpha = x \in \mathbb{Z}$, что даёт нам противоречие. □

Домашнее задание 12.

- 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.

[12] в том, что $|\varepsilon| < 1$ легко убедиться непосредственно.

Докажем теперь сильную теорему Дирихле о единицах:

Теорема 40. *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 $\operatorname{Im}\ell$ — 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

$$u_1 \mapsto (+,-,-,\ldots,-), u_2 \mapsto (-,+,-,\ldots,-), \ldots u_n \mapsto (-,-,\ldots,+).$$

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:

$$A = \begin{pmatrix} + & - & - & \ldots & - \\ - & + & - & \ldots & - \\ \vdots & \vdots & \ldots & \ldots & \vdots \\ - & - & - & \ldots & + \end{pmatrix}, \quad A \in \mathrm{M}_{s+t-1}(\mathbb{R}).$$

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 32. 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 $u_1, \dots, u_{s+t}$, которые в образе дадут нужные знаки координат. Пусть $n = s+2t$, рассмотрим множество

$$Y = \left\{(x_1, \dots, x_s, y_1, z_1, \dots y_t, z_t), \quad |x_i| < C_i \forall 1 \le i \le s, y_i^2 + z_i^2 < C_{s+i}\right\}.$$

Нетрудно проверить, что Y — ограниченное, выпуклое и центрально-симметричное. Кроме того,

$$\mathrm{Vol}(Y) = 2^s \prod_{i=1}^{s} C_i \cdot \pi^t \cdot \prod_{i=1}^{t} C_{s+i} = 2^s \pi^t \cdot \prod_{i=1}^{s+t} C_i.$$

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 30). В качестве Γ мы возьмём $\mathrm{Im}\,\varphi$, где

$$\varphi(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_s(\alpha), \mathrm{Re}(\sigma_{s+1}(\alpha)), \mathrm{Im}(\sigma_{s+1}(\alpha)), \dots, \mathrm{Re}(\sigma_{s+t}(\alpha)), \mathrm{Im}(\sigma_{s+t}(\alpha))) \in \mathbb{R}^n.$$

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 $\sigma_j \in \{\sigma_1, \dots, \sigma_s, \sigma_{s+1}, \dots, \sigma_{s+t}\}$ и определим

$$C_i = \begin{cases} \varepsilon, i \ne j \\ C \cdot \varepsilon^{-(s+t-1)}, i = j \end{cases}.$$

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 30 $\exists 0 \ne x \in \mathcal{O}_K$:

$$|\sigma_1 x| < C_1, \dots, |\sigma_s x| < C_s, \quad |\sigma_{s+1} x|^2 < C_{s+1}, \dots, |\sigma_{s+t} x|^2 < C_{s+t}.$$

Вычислим норму этого $x \in \mathcal{O}_K$

$$\mathrm{N}(x\mathcal{O}_K) = |\,\mathrm{N}(x)| = |\sigma_1 x| \dots |\sigma_s x| |\sigma_{s+1} x|^2 \dots |\sigma_{s+t} x|^2 < \prod_{i=1}^{s+t} C_i = C.$$

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 $\tau \ne \sigma_j$ 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 $\tau \in \{\sigma_1, \dots, \sigma_s\},\ \tau = \sigma_i$, тогда

$$|\tau u_j| = \frac{|\tau x|}{|\tau a_k|} < \frac{C_i}{\varepsilon} = 1, \text{ так как } i \neq j.$$

- Пусть $\tau \in \{\sigma_{s+1}, \dots, \sigma_{s+t}\}$, тогда

$$|\tau u_j| = \frac{|\tau x|}{|\tau a_j|} < \frac{\sqrt{C_i}}{\sqrt{\varepsilon}} = 1.$$

Таким образом, мы показали, что $\operatorname{Im} \ell$ — полная решетка в гипеплоскости, то есть $\operatorname{Im} \ell \cong \mathbb{Z}^{s+t-1}$, откуда, как мы уже замечали в доказательстве слабой теоремы Дирихле о единицах 39

$$\mathcal{O}_K^* \cong \mu \oplus \mathbb{Z}^{s+t-1}.$$

□

2.20 Контр-пример к принципу Минковского-Хассе

Начнём с вот такого утверждения.

Предложение 27 (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

$$-b = \mathrm{N}(\alpha), \quad (\alpha) = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2} \cdot \dots \implies \mathrm{N}(\alpha) \vdots p,$$

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

$$p^{2n} \cdot \underbrace{\dots}_{\not\vdots p} = b^2 = p^s \cdot \underbrace{\dots}_{\not\vdots p} \implies s = 2n.$$

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 $\upsilon_p(b) = n$

$$\alpha(\alpha^2 + a) = -b = p^n \cdot d, \quad (p, d) = 1, \quad (\alpha(\alpha^2 + a)) = \mathfrak{p}_1^n\mathfrak{p}_2^n\mathfrak{p}_3^n \cdot \underbrace{\dots}_{\not\vdots \mathfrak{p}_3},$$

то есть $\upsilon_p(\alpha(\alpha^2 + a)) = n$, что даёт нам противоречие.

□

Теорема 41. *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

$$x^3 + 6y^3 = 10z^3. \tag{7}$$

Выберем среди таких решений решение с минимальным ненулевым $|z|$. Рассмотрим расширение $K = \mathbb{Q}(\theta)$, где $\theta^3 = 6$. Тогда уравнение 7 выражает тот факт, что

$$\mathrm{N}(x + \theta y) = 10z^3. \tag{8}$$

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[13] 27 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 27 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 32, какие идеалы висят над 2 и 5. Это мы уже делали при вычислении группы классов идеалов $\mathbb{Q}(\sqrt[3]{6})$ (см. пример 16).

$x^3 - 6 \equiv x^2 \pmod 2 \rightsquigarrow 2\mathcal{O}_K = (2, \theta)^3 = (\theta - 2)^3, \quad x^3 - 6 = (x-1)(x^2+x+1) \pmod 5 \rightsquigarrow 5\mathcal{O}_K = (5, \theta - 1)(5, \theta^2 + \theta + 1$

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.

[13] С $\alpha = \alpha\theta$, как бы абсурдно это не звучало.

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 $\theta^3 = 6$,

$$\big(u+v\theta+w\theta^2\big)^3 \equiv u^3 \pmod 3.$$

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

$$\big(u+v\theta+w\theta^2\big)^3 \equiv 0 \pmod 3 \implies x + y\theta \vdots 3 \implies x, y \vdots 3$$

и мы можем сделать спуск. Если

$$\alpha = (\theta-2)(\theta^2+\theta+1)^2\big(u+v\theta+w\theta^2\big)^3 = (\theta^2-3\theta+2)(u+v\theta+w\theta^2)^3 = x + y\theta,$$

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.

□

2.21 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

$$x = p^k \cdot \varepsilon, \quad \varepsilon \in \mathbb{Z}_p^*, k \in \mathbb{N}. \tag{9}$$

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

$$x = p^k \cdot \varepsilon, \quad \varepsilon \in \mathbb{Z}_p^*,\ k \in \mathbb{Z}. \tag{10}$$

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 33 (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 $v_p(f'(y)) = a$. Тогда $v_p(f'(t_n)) = a$ 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 предположнию $v_p(f(t_n)) = 2a + 1 + n$. 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 11 (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 $\exists x \in \mathbb{Z}_p$: $x \equiv x_0 \pmod{p}$, $f(x) = 0$.

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 42. *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 11) 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, $v_9(F(0, 2, -1)) = v_{27}(27) = 1$, 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, $v_5(F(2, -1, 0)) = v_5(20) = 1$, а
$$\frac{\partial F}{\partial x}(2, -1, 0) = 9 \cdot 4 \not\vdots 5.$$

□

2.22 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 28. *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 11, $\exists \xi \in \mathbb{Z}_p\colon f(\xi) = 0$, то есть $\varepsilon = \xi^2$. □

Это предложение позволяет нам определить символ Лежандра для элементов $\mathbb{Z}_p^*$. Действительно, пусть $\varepsilon = a_0 + a_1 p + \ldots$, положим

$$\left(\frac{\varepsilon}{p}\right) = \left(\frac{a_0}{p}\right).$$

Корректность этого определения ясна как раз из предложения 28. Кроме того, если $\eta \in \mathbb{Z}_p^*,\ \eta = b_0 + b_1 p + \ldots$, то

$$\left(\frac{\varepsilon\eta}{p}\right) = \left(\frac{a_0 b_0}{p}\right) = \left(\frac{a_0}{p}\right)\left(\frac{b_0}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{\eta}{p}\right),$$

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 $\xi \in \mathbb{Q}_p^*$, $\xi = p^m\theta = p^(a_0 + a_1 p + \ldots),\ \theta \in \mathbb{Z}_p^*$.

- 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 34. 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 33 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 29. *При $p = 2$ индекс подргуппы 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 43. 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 30. $|Q_p^*/\mathrm{N}| = 2$.

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

$$\mathrm{N} = \{x^2 + y^2 \,|x, y \in \mathbb{Q}_p\}.$$

Но, квадратичная форма $x^2 + y^2$ представляет все элементы $\mathbb{Z}_p^*$[14] 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 $p = 2$. □

[14] Это следует, например, из теоремы Коши-Девенпорта, или еще из чего-нибудь.

2.23 Символ Гильберта

Определение 44. 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 31. *Форма $\langle 1, -a, -b\rangle$ изотропна*[15] *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

$$x_0^2 - ay_0^2 = 0 \implies a = \left(\frac{x_0}{y_0}\right)^2 = c^2 \implies b = x^2 - c^2y^2 = (x - cy)(x + cy), \text{ где } x = \frac{1+b}{2},\ y = \frac{b-1}{2c}.$$

□

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 32. *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 31
$$a_1 = \mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_1), \quad a_2 = \mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_2),\ \alpha_1, \alpha_2 \in \mathbb{Q}_p(\sqrt{b}) \implies$$
$$\implies a_1a_2 = \mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_1)\,\mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_2) = \mathrm{N}_{\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p}(\alpha_1\alpha_2),$$
а тогда, опять же, по предложению 31 $(a_1a_2, b)_p = 1$.
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 30 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 31 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 31 $(a_1a_2, b)_p = 1$.

	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 1: Значения символа Гильберта на $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$.

4. Теперь пусть $p=2$ и $(a_1,b)_p=1,\ (a_2,b)_p=-1$. Тогда по предложению 29 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 29 $|\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}|=8$, 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 32 следует, что

$$(a,b_1b_2)_p=(a,b_1)_p\cdot(a,b_2)_p.$$

Предложение 33. *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 $p\neq2$, докажем второе свойство. Рассмотрим форму

$$f(x,y,z)=x^2-\varepsilon_1y^2-\varepsilon_2z^2.$$

Так как $\varepsilon_1\not\vdots p,\varepsilon_2\not\vdots p$, по теореме Шевалле сравнение

$$x^2-\varepsilon_1y^2-\varepsilon_2z^2\equiv0\pmod p$$

имеет ненулевое (в $\mathbb{Z}/p\mathbb{Z}$) решение, пусть оно (x_0,y_0,z_0). Тогда

$$f(x_0,y_0,z_0)\equiv0\pmod p,\quad \frac{\partial f}{\partial x_1}(x_0,y_0,z_0)=2x_0\not\vdots p,$$

а значит, по лемме Гензеля 33, форма $x^2-\varepsilon_1y^2-\varepsilon_2z^2$ 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

$$f(x,y,z)=x^2-py^2-z^2.$$

$$f(1,1,1)\equiv0\pmod p,\quad \frac{\partial f}{\partial x}(1,1,1)=1\not\vdots p,$$

[15] Из определения ясно, что это равносильно тому, что $(a,b)_p=1$.

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 43 (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 33:

$$(p,q)_p = \left(\frac{q}{p}\right), \quad (p,q)_q = \left(\frac{p}{q}\right), \quad (p,q)_2 = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

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 44. *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:

$$a_1\xi_1^2 + \ldots + a_r\xi_r^2 + p(a_{r+1}\xi_{r+1}^2 + \ldots + a_n\xi_n^2) = 0. \tag{11}$$

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 (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 33 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 (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 12. *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 45. *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 33 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 13. *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 46. *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 12 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 13 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 13 мы получаем, что g изотропна, а значит и f изотропна.

□

2.24 Теорема Минковского-Хассе

Теорема 47 (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 $f \simeq \langle a_1, \ldots, a_n\rangle$, $a_1 \cdot \ldots \cdot a_n \neq 0$.

Пусть $n = \dim f$, случай $n = 1$ тривиален.

Доказательство теоремы 47 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 $a = p_1 \ldots p_k$. Тогда, так как $\forall i\ v_{p_i}(a) = 1$, a не является квадратом ни над каким $\mathbb{Q}_{p_i}$, значит $a = 1$ и $f \simeq \langle 1, -1\rangle$. □

Доказательство теоремы 47 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 31 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 31 форма $\langle 1, -a, -b\rangle$ изотропна над $\mathbb{Q}$. □

Доказательство теоремы 47 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 28 $a^{-1}b_{p_i}$ 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 43, 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 47 в случае $n \geq 5$: Пусть $f \simeq \langle a_1, \dots, a_n\rangle$. Рассмотрим формы

$$g \simeq \langle a_1, a_2\rangle, \quad h \simeq \langle -a_3, -a_4, \dots, -a_n\rangle.$$

Определим множество S аналогичным образом и также, как и в случае $n = 4$ найдём a такое, что формы

$$\langle a_1, a_2, -a\rangle \text{ и } \langle -a_3, \dots, -a_n, -a\rangle$$

изотропны над всеми $\mathbb{Q}_p$, кроме, может быть, $\mathbb{Q}_{p_0}$. Тогда по закону взаимности Гильберта 43 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 12 (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 $\mathbb{Q}_{p_0}$[16], 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 $\mathbb{Q}$. □

[16]Это общий факт, справедливый над любым полем: изотропная форма представляет любой элемент.

Следствие 14. *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 15. *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 $\mathbb{Q}$. □

3. Основы теории гомологий

3.1 Симплициальные гомологии

Определение 45. *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 46. *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 20 (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 $\varepsilon \circ \partial = 0$.

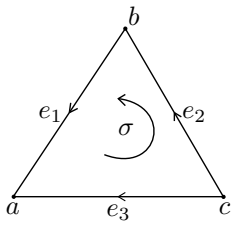
Гомологиями топологического пространства называют гомологии построенного по нему комплекса. В нашем случае

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

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

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

Пример 21 (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.

$$\partial(k_1e_1 + k_2e_2 + k_3e_3) = k_1(b-c) + k_2(a-b) + k_3(a-c) = a(k_2+k_3) + b(k_1-k_2) + c(-k_1-k_3) \Rightarrow$$
$$\Rightarrow \operatorname{Ker} \partial_1 = \langle (k_1, k_2, k_3) \in \mathbb{Z}^3 \mid k_1 = k_2 = -k_3 \rangle$$

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 22 (Спмилициальные гомологии треугольника без внутренности)**.** Пусть теперь всё также, как в примере 21, но у треугольнка нет внутренности. Тогда цепной комплекс будет иметь вид

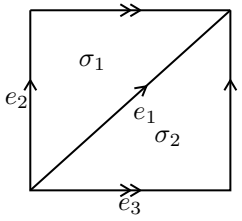
$$\ldots \to 0 \to \mathbb{Z}^3 \to \mathbb{Z}^3 \to \mathbb{Z}$$

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 23 (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.

3.2 Сигнулярные гомологии

Определение 47. 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[17] $C_\bullet$ 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 35. В контексте определения 47 $\partial^2 = 0$.

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 $\partial\partial f = 0$. □

Определение 48. *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*[18], 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.

[17] формально, мы пока еще не знаем, что это комплекс.
[18] позже мы увидим, какая в этом геометрическая интуиция

Теорема 48 (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:

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

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.

3.3 Немного гомологической алгеры

Рассмотрим категорию цепных комплексов $\mathfrak{Ch}$ (в нашем случае абелевых групп, но в принципе, всё что тут будет сказано справедливо 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 36. Сопоставление цепному комплексу его k-й группы гомологий функториально, то есть отображение

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

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

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

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

Тогда нужная нам стрелка получается просто из универсального свойства факторгруппы:

$$\begin{array}{ccccc} \operatorname{Ker}\partial_q & \xrightarrow{f_q} & \operatorname{Ker}\delta_q & \xrightarrow{\pi} & H_q(D_\bullet) \\ & \searrow^{\rho} & & \nearrow_{f_*} & \\ & & H_q(C_\bullet) & & \end{array}$$

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

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 34. *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 49. Пусть X — топологическое пространство. Тогда, если группа $H_k(X)$ конечнопорождена, то

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

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

3.4 Гомотопическая инвариантность гомологий

Определение 50. Пусть $(C_\bullet, \partial), (D_\bullet, \delta) \in \mathfrak{Ch}$ — два цепных комплекса. Их морфизмы $f, g \in \operatorname{Hom}_{\mathfrak{Ch}}((C_\bullet, \partial), (D_\bullet, \delta))$ называются *гомотопными* ($f \sim g$), если сущесвует диагональный морфизм $h\colon C_\bullet \to D_{\bullet+1}$ такой, что

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

$$\begin{array}{ccccccccccc} \dots & \xrightarrow{\partial_{q+2}} & C_{q+1} & \xrightarrow{\partial_{q+1}} & C_q & \xrightarrow{\partial_q} & C_{q-1} & \xrightarrow{\partial_{q-1}} & \dots \\ & \swarrow^{h_{q+1}} & \downarrow{\scriptstyle g_{q+1}} & \swarrow^{h_q} & \downarrow{\scriptstyle g_q} & \swarrow^{h_{q-1}} & \downarrow{\scriptstyle g_{q-1}} & \swarrow^{h_{q+2}} & \\ \dots & \xrightarrow{\delta_{q+2}} & D_{q+1} & \xrightarrow{\delta_{q+1}} & D_q & \xrightarrow{\delta_q} & D_{q-1} & \xrightarrow{\delta_{q-1}} & \dots \end{array}$$

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 49. *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 $x \in \operatorname{Ker} \partial_q$, то

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

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 50. *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 49, 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 16. *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 37. Если X — линейно связно, то $H_0(X) = \mathbb{Z}$.

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

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

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

Следствие 17. *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.

3.5 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 51. 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 52. 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 51 (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[19] □

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 $x + a = \partial(\ldots)$.

[19] 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 18. *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 19. *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.

3.6 Пары Боруска

Определение 53. Пусть X – топологическое пространство, а $A \subset X$ с индуцированной топологией. Тогда говорят, что (X, A) – *пара Борсука* (или, *корасслоение*)[20], 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 54. Пара (X, A) называется *клеточной парой*, если X — клеточное пространство, A — клеточное подпространство X.

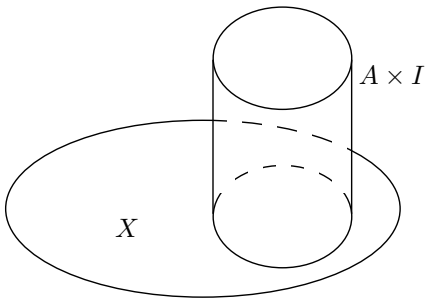
Замечание. Так как очевидно, что $(D^n, \partial D^n)$ — пара Борсука, клеточная пара является парой Борсука.

Нам от пар Борсука понадобится несколько базовых утверждений.

Теорема 52 (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:

[20] 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 $X \times I \to X \cup (A \times I)$[21]. □

Следствие 20. *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 35. *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 21. *Если (X, A) — пара Боруска и A — стягиваемо, то $X \sim X/A$.*

Предложение 36. *Пара (CX, X) — всегда пара Борсука.*

3.7 Относительные гомологии как абсолютные (факторизация)

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

Теорема 53. *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 $[v_0, \ldots, v_n]$. его точки — линейные комбинации вида

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

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

Определение 55. *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 38 (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 50.[22] □

[22] 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 39 (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 38 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 38, 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 40 (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 41. 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 40 □

Наконец, мы можем доказать интересующую нас теорему:

Теорема 54. *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 39 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 41 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 18.

Пусть теперь (X, A) — пара Борсука. Тогда по утверждению 35 $X \cup CA \sim X/A$, а значит, $H_q(X, A) \cong \widetilde{H}_q(X/A)$. □

3.8 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 55 (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 $C_n(A + B)$[23].

Тогда, как мы помним из леммы об измельчении 39 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

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

□

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

3.9 Точная последовательность Майера-Вьеториса

Кроме длинной точной последовательности пары (теорема 51) для вычисления гомологий пары (X, A) есть и другая мощная техника для вычисления гомологий пространства X, тоже представляющая собой длинную точную последовательность.

Теорема 56 (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.

3.10 Гомологии сфер

Теорема 57. *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 54

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

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

Следствие 22. *Сферы разных размерностей негомеоморфны.*

3.11 Гомологии букета и надстройки

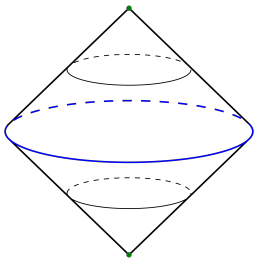
Из стягиваемости конуса сразу следует, что $H_q(CX, X) \cong \widetilde{H}_q(X)$ (достаточно написать точную последовательность для приведенных гомологий).

Определение 56. 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 24. Надстройка над окружностью выглядит следующим образом:



Так как надстройка получается факторизацией конуса по нижнему основанию, из теоремы о факторизации 54 следует, что $H_{q+1}(CX, X) \cong \widetilde{H}_{q+1}(\Sigma X)$. Таким образом, мы получили такое утверждение:

Теорема 58 (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 57.

Теорема 59 (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

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

□

3.12 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 25. 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

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

3.13 Приложения теории гомологий

Теорема 60 (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 61 (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 60. □

Теорема 62 (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 55 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 $m = n$. □

3.14 Симплициальные комплексы

Этот парагарф надо написать из Хатчера.

3.15 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 54 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 63. *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:

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

□

3.16 Степень отображения

Определение 57. 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 $\deg f$.

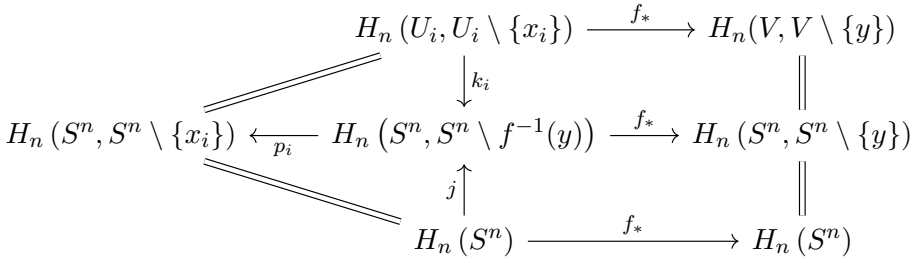
Базовые свойства степени.

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_1^n и Δ_2^n по границе. Тогда n-мерная цепь $\Delta_1^n - \Delta_2^n$ являются образующей n-мерных гомологий, а отображение f переставляет местами Δ_1^n и Δ_2^n, 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 64 (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:



Все отображения на ней индуцируются включениями. Два ихоморфизма в верхней части диаграммы получаются из теоремы о вырезании 55, а два в нижней — из точной последовательности пары 51.

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 65 (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 выразении 55, группа $H_n\big(S^n, S^n \setminus f^{-1}(y)\big)$ — 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

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

□

3.17 Клеточные гомологии

Лемма 42. Пусть X — конечный CW-комплекс. Тогда:

a) $H_k\big(X^n, X^{n-1}\big) = 0$, 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 $\big(X^n, X^{n-1}\big)$ — 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 54 и теоремы 59.

Теперь рассмотрим длинную точную последовательность пары

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

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

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

Тогда, если $k > n$, то

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

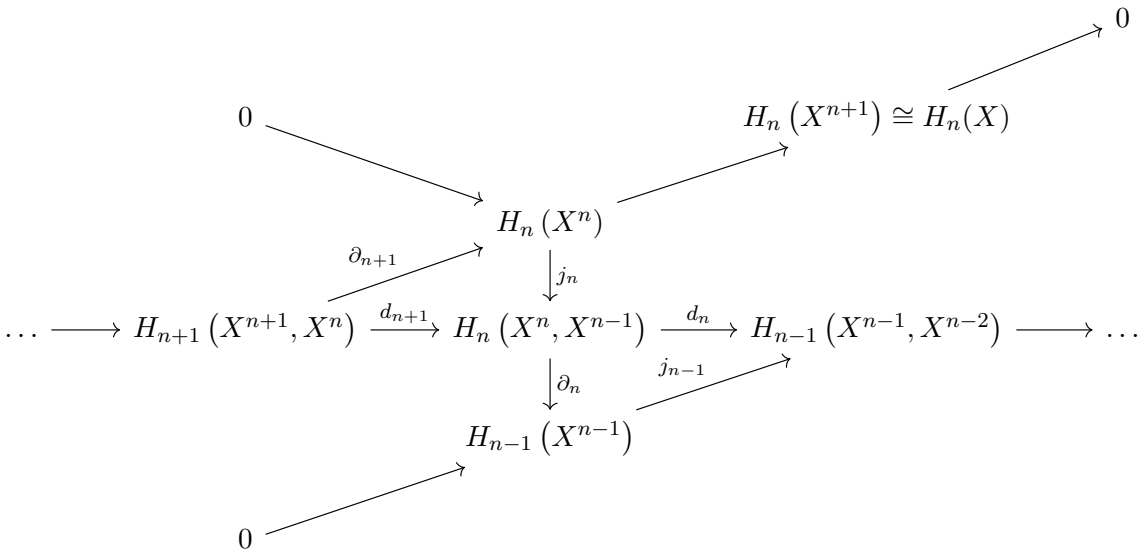
что доказывает пункт b). Если же $k < m$, то тогда

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

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 58. 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 66. *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 23. *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 26. Последний пункт следствия 23 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 37. *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

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

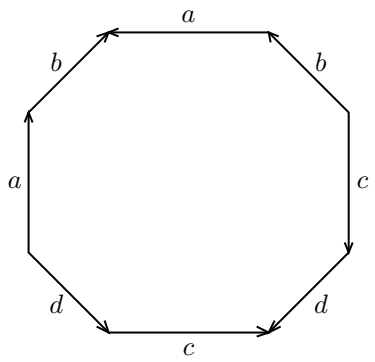
Базис группы $H_{n-1}\big(X^{n-1}, X^{n-2}\big)$ состоит из $(n-1)$-мерных клеток, а отображение $q_{\beta *}$ — это проекция группы $\widetilde{H}_{n-1}\big(X^{n-1}/X^{n-2}\big)$ (которая, как группа гомологий букета окружностей суть прямая сумма $\mathbb{Z}$, где каждое слагаемое соотвествует $(n-1)$-мерной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

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

3.18 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

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

3.19 Пространства Мура

Допишу позже вместе с пространствами Эйленберга-Маклейна.

3.20 Теорема о вложении дисков и сфер

Напомним, что топологическое вложение — гомеоморфизм на образ.

Теорема 67. *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 (56):

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

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

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 56, 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. □

3.21 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.[24] 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 59. 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 границы, 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.

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

3.22 Формула универсальных коэффициентов для когомологий

Пример 27. 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 38. *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

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

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 60. 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 43. 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 43 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 $\operatorname{Ext}(H, G)$[25].

[25]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 68 (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 24. *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 27.

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

Следствие 25. *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. □

3.23 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 44. 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 кограницы (в любом порядке) — кограница:

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

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.

4. Комплексная алгебраическая геометрия

4.1 Комплексные многообразия

Определение 61. *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 28 (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 29. 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 62. 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.

4.2 Векторные рассоления

Определение 63. 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.[26]

Определение 64. 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 30 (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 65. *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 $\Omega^1_{\mathbb{R}}(X)$.

[26] но делать этого мы пока что не будем.

4.3 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 4.1, $|\det \mathcal{J}_{\mathbb{R}}(f)| = |\det \mathcal{J}(f)|^2 \neq 0$ 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 39. *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 66. *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 67. Аналитическим подмножеством V комплексного многообразия M называется подмножество, являющееся локально множеством нулей конечного набора голоморфных функций.

Точка $p \in V$ называется *гладкой*[27] 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 40. *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 41. *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.

4.4 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

$$A^n(M) = \bigoplus_{p+q=n} A^{p,q}(M), \text{ где}$$

[27] 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. □

4.5 Пучки и когомологии

Определение 68. 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 $r_{VU} \colon \mathcal{F}(V) \to \mathcal{F}(U)$[28], 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.

4.6 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 69. *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 70. 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 71. 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 $g = f^a h$.

[28] 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 $\mathrm{ord}_V(g)$.

Ясно, что порядок обладает таким вот свойством:

$$\mathrm{ord}_V(gh) = \mathrm{ord}_V(g) + \mathrm{ord}_V(h).$$

Определение 72. 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

$$\mathrm{ord}_V(f) = \mathrm{ord}_V(g) - \mathrm{ord}_V(h).$$

Замечание. Соотвественно, f имеет нуль порядка a на V, если $\mathrm{ord}_V(f) = a > 0$ и полюс порядка a на V, если $\mathrm{ord}_V(f) = a < 0$.

Определение 73. *Дивизором* (f) мероморфной функции f называют формальную линейную комбинацию

$$(f) = \sum \mathrm{ord}_V(f)V$$

Если f локально представлена в виде $f = g/h$, то *дивизором нулей* называют

$$(f)_0 = \sum \mathrm{ord}_V(g) \cdot V,$$

а *дивизором полюсов* называют

$$(f)_\infty = \sum \mathrm{ord}_V(h) \cdot V,$$

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 $D \in \mathrm{Div}(M)$ — 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 $V \subset M$ $\mathrm{ord}_V f_\alpha = \mathrm{ord}_V f_\beta$ и набор $\{f_\alpha\}$ задаёт дивизор

$$D = \sum \mathrm{ord}_V(f_\alpha) \cdot V,$$

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

$$H^0(M, \mathcal{M}^*/\mathcal{O}^*) \cong \mathrm{Div}(M).$$