

③ Конечность группы классов

Напоминание: L - алг. числовое поле, $\mathcal{O}_L$ - кольцо целых.

$\text{Id}(\mathcal{O}_L)$ - группа главных идеалов кольца $\mathcal{O}_L$,

$P(\mathcal{O}_L) \leq \text{Id}(\mathcal{O}_L)$, сост. из главных идеалов,

$\text{Cl}(\mathcal{O}_L) = \text{Id}(\mathcal{O}_L) / P(\mathcal{O}_L)$ - группа классов кольца $\mathcal{O}_L$,

$h_L = |\text{Cl}(\mathcal{O}_L)|$ - число классов идеалов

Δ -м-рание (см. следствие 2.3.2 из ANT7):

$h_L = 1 \Leftrightarrow \mathcal{O}_L$ - кольцо гл. идеалов $\Leftrightarrow \mathcal{O}_L$ факториально.

Теорема 1 h_L конечно для любого алг. чис. поля L .

Пусть $[L : \mathbb{Q}] = n$ и $\sigma_1, \dots, \sigma_n$ — вложения L в $\mathbb{C} = \overline{\mathbb{Q}}$,

остава. $\mathbb{Q}$ — неограничен. Выберем натуральное T так;

что $\sigma_i(L) \subseteq \mathbb{R} \Leftrightarrow i = 1 \dots r$. Тогда $\sigma_{r+1}, \dots, \sigma_n$

разбрасываются на пары сопряженных, т.е. $\forall \mathbb{Q}$ -ва-я

$\psi : L \rightarrow \mathbb{C}$ т.ч. $\psi(L) \not\subseteq \mathbb{R}$, сг. е $\overline{\psi} : x \rightarrow \overline{\psi(x)}$ ^{← кон. сопр.},

то вместе ψ и $\overline{\psi}$ — $\mathbb{Q}$ вложения L в $\mathbb{C}$, сг. с ψ .

Поэтому $n = r + 2s$ и $\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_s, \overline{\sigma_s}$ — это все $\mathbb{Q}$ -вложения L в $\mathbb{C}$, образы кот. не лежат в $\mathbb{R}$.

Определим $\sigma : L \rightarrow \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n$ с. образом

$$\sigma(x) = (\sigma_1(x), \dots, \sigma_r(x), \operatorname{Re} \sigma_{r+1}(x), \operatorname{Im} \sigma_{r+1}(x), \dots, \operatorname{Re} \sigma_s(x), \operatorname{Im} \sigma_s(x))^T$$

$\forall x \in L.$

Сначала мы покажем т. 1 исходя из пред. 1

Пред. 1 Если L -число арт. поле. Тогда каждый класс из $Cl(\mathcal{O}_L)$ содержит ровно один идеал $I \subseteq \mathcal{O}_L$. Таким, что

$$(*) \quad N(I) \leq \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^S \sqrt{|d_L|}, \text{ где } d_L = \text{disc}(\mathcal{O}_L/\mathbb{Z})$$

Д-во т. 1: Возв. через C_L константу из уравнения (*).

В лемме и в т-ме 2.5.2 из ANT3 имеется только

кон. число $I \subseteq \mathcal{O}_L$: $N(I) < C_L$. В след. предп. 1

$\Rightarrow$ имеется только конечное число классов $Cl(\mathcal{O}_L)$ $\square$

Следствие Если $|L:\mathbb{Q}| = n \geq 2$, то $|d_L| \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4} \right)^{n-1}$.

Упр 1 Δ -до следствие 1 воможно вывести из пер. вом (*).

Следствие 2 Если $|L: \mathbb{Q}| = n \geq 2$, то $\text{disc}(\mathcal{O}_L/\mathbb{Z}) \neq \pm 1$.

В частности, $\exists$ простое $p \in \mathbb{Z}$: $p \mathcal{O}_L$ разлагается в $\mathcal{O}_L$.

Δ -бо: В силу $n \geq 1$ $|d_L| \geq \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1} > 1 \Rightarrow \exists p \mid d_L$
 $\Rightarrow p \mathcal{O}_L$ разлагается по т. 2.4.3 из ANT 8

С помощью леммы-ва (б) из предл 1 можно утверждать h_L !

Пример $L = \mathbb{Q}[\sqrt{-1}]$, $B = \mathcal{O}_L$. Мы знаем, что модуль
класс $\mathcal{D}$ из $\text{Cl}(\mathcal{O}_L)$ содержит $I \trianglelefteq B$: $N(I) < C_L$ из (4).

Так как $n=2$, $\text{Hom}_{\mathbb{Q}}(L, \mathbb{C}) = \{\text{id}, \bar{\alpha}\} \Rightarrow s=1, r=0$ $d_L = 4m = -4$

$\Rightarrow N(I) \leq \frac{2!}{2^2} \cdot \frac{4}{\pi} \cdot \sqrt{4} \ll \frac{4}{3} < 2 \Rightarrow N(I) = 1 \Rightarrow I = B \Rightarrow$

$\Rightarrow \mathcal{D} = 1 = \mathcal{O}_L \Rightarrow h_L = 1 \Rightarrow L$ факториальна!

Т. 2 (Эрмит, 1857, о дискриминанте). Для любого д-ф
 Сусу-е-е только конечное число чисел. а.п. поля L ,
 для которых $\text{disc}(\mathcal{O}_L/\mathbb{Z}) = d$. Упр 2 + 1 - в Теореме 2
Опр 1. $H \subseteq \mathbb{R}^n$ - **решетка**, если найдется л.п. базис $e_1, \dots, e_n \in \mathbb{R}^n$:

$$H = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n, \text{ где } n\text{-н решетка наз-ся } \textbf{полной}.$$

$$T = \{x \in \mathbb{R}^n \mid x = \sum_{i=1}^n d_i e_i, 0 \leq d_i < 1\} - \text{фундаментальный параллелепипед}$$

полной решетки.

$$\text{Vol}(H) := \text{Vol}(T) - \text{объем } \textbf{полной} \text{ решетки}.$$

Факт 1: ТЗависит от базиса базиса $e_1, \dots, e_n$ решетки H , но

$$\text{Vol}(H) = \text{Vol}(T) \text{ не!}$$

← без проверки - неохота

Факт 2: $\mathbb{R}^n = \bigcup_{h \in H} (h + T)$ где h - любой элемент решетки H .

Опр 2 $H \subseteq \mathbb{R}^n$ **дискретна**, если $\forall$ оран. мн-во $X \subseteq \mathbb{R}^n$
выполнено $|H \cap X| < \infty$.

Факт 3: $H \subseteq \mathbb{R}^n$ дискретна $\Leftrightarrow H$ - решетка в $\mathbb{R}^n$.

Лемма 1. Доказано $a) \Leftrightarrow b)^* \Rightarrow$

Теорема 3 (Менковский, 1897). Пусть $H \subseteq \mathbb{R}^n$ полная решетка,
 S - оран. мн., центр - своим выписанное множи-во в $\mathbb{R}^n$. Если
а) $\text{Vol}(S) > 2^n \text{Vol}(H)$ или б) $\text{Vol}(S) \geq 2^n \text{Vol}(H)$ и S - компакт,
то $S \cap (H \setminus \{0\}) \neq \emptyset$.

оран. мн. во.

Пример $H = \mathbb{Z}e_1 + \mathbb{Z}e_2 \subseteq \mathbb{R}^2$ $e_1 = (1, 0)$, $e_2 = (0, 1)$ и $S = \{x_1e_1 + x_2e_2 \mid -1 < x_i \leq 1\}$

Тогда $\text{Vol}(S) = 4 = 2^2 \text{Vol}(H)$, но $S \cap H = \{0\}$. Условие комп-во
обязательно!

1-во Творения 3: а) Пусть $S' = \frac{1}{2} S$ (мин. разн. увеличено в 2 раза)

Умень $\text{vol}(S') = \frac{1}{2} \text{vol}(S) > \text{vol}(H) = \text{vol}(T)$, где T — фигура, перекрывающая H при каждом ϕ из $\mathcal{H}$.

$$R'' = \bigcup_{h \in H} (T + h) \Rightarrow S' = \bigcup_{h \in H} S' \cap (T + h) \Rightarrow \text{vol}(S') = \sum_{h \in H} \text{vol}(S' \cap (T + h))$$

$$\text{vol}(S') = \sum_{h \in H} \text{vol}(S' \cap (T + h))$$

$$\text{Доказн. } \forall h \in H \quad S_h = \underbrace{S' \cap (T + h)}_{\text{сдвиг на } "h"} \subseteq T.$$

$$\text{Заметим, что } \text{vol}(S_h) = \text{vol}(S' \cap (T + h)) \Rightarrow$$

$$\text{vol}(S') = \sum_{h \in H} \text{vol}(S_h) > \text{vol}(T). \quad \text{Но } \bigcup_{h \in H} S_h \subseteq T.$$

Сл. по известной лемме о мере следует, что

$\exists h_1, h_2 \in H: h_1 \neq h_2 \cup S_{h_1} \cap S_{h_2} \neq \emptyset$. Тождество

$\exists x \in S_{h_1} \cap S_{h_2} \subseteq T$ и тогда $x+h_1 = s_1 \in S', x+h_2 = s_2 \in S'$

$\Rightarrow s_1 - s_2 = h_1 - h_2 \in H$. Но $2s_1 \cup 2s_2 \in S = 2S'$

$\Rightarrow -2s_2 \in S$ (S -группа замкн.). Поэтому

$h = \underbrace{\frac{1}{2}(2s_1) + \frac{1}{2}(-2s_2)}_{S^n \text{ как борн-гр.}} = s_1 - s_2 \in H$, что и треб.

○

б) $\text{Vol}(S) = 2^n \text{Vol}(H)$ и S -компакт.

Рассмотрим $S_m = (1 + \frac{1}{m})S$ для $m = 1, 2, 3, \dots$. Чисел

$S_1 \supset S_2 \supset \dots \supset S_m \dots$ Пересечение $\bigcap S_m = S$. б. замкн.

и $\text{Vol}(S_m) > \text{Vol}(S)$

комм., $\lim_{m \rightarrow \infty} S_m = S$ и $\lim_{m \rightarrow \infty} \text{Vol}(S_m) = \text{Vol}(S)$.

Пусть $\forall n=1, 2, \dots \exists 0 \neq h_n \in K : h_n \in S_n$

Отобразим. $S'_n = S_n \cap (K \setminus \{0\}) \ni h_n$. У нас

$$S'_1 \supseteq S'_2 \supseteq \dots \supseteq S'_n \supseteq \dots \quad (*)$$

Заметим, что S_1 ~~не~~ ^{то} ~~является~~ ^{является} $\Rightarrow S'_1 = S_1 \cap (K \setminus \{0\})$ — конечномерный линейный (см. факт 3), т.е. (*) — убывающая последовательность конечномерных л.в. $\Rightarrow$ стабилизируясь

на каком-то n имеет: $\bigcap_{n \geq 1} S'_n = \left(\bigcap_{n \geq 1} S_n \right) \cap (K \setminus \{0\})$
 $\searrow S$ □

Пусть $B_t = \{(y_1, \dots, y_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{i=1}^r |y_i| + 2 \sum_{j=1}^s |z_j| \leq t\}$, $t \in \mathbb{R}^+$
 $n = r + 2s$

Факт 4: $\text{Vol}(B_t) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$ хитрый Δ -в факт 4.

Лемма 1 Пусть $x_1, \dots, x_n$ — линейно независимые над $\mathbb{Q}$, $H = \mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$.

$$\sigma(H) = \{ (\sigma_1(x), \dots, \sigma_r(x), \operatorname{Re} \sigma_{r+1}(x), \operatorname{Im} \sigma_{r+1}(x), \dots, \operatorname{Re} \sigma_{r+s}(x), \operatorname{Im} \sigma_{r+s}(x)) \mid x \in H \}.$$

Тогда $\sigma(H)$ — полная решетка в $\mathbb{R}^n$ и $\operatorname{Vol}(\sigma(H)) = \frac{1}{2^s} \sqrt{|\operatorname{disc}(\sigma/x)|}$

Δ -во:

Вспоминаем $\operatorname{Vol}(\sigma(H)) = \left| \det \begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_n) \end{pmatrix} \right|$ и показываем, что здесь.

из-за линейной независимости x_i можно перейти к ортонормальной базе

$$\underbrace{\begin{pmatrix} \dots & a_j + b_j i & a_j - b_j i & \dots \end{pmatrix}}_{+} \rightarrow \begin{pmatrix} \dots & 2a_j & a_j - b_j i & \dots \end{pmatrix} \xrightarrow{-\frac{1}{2}x} \begin{pmatrix} \dots & 2a_j & -b_j i & \dots \end{pmatrix} \Rightarrow$$

$$\begin{aligned}
 \det(\sigma_i(x_j)) &= (-2i)^s \det(\sigma(x_i)) \Rightarrow \text{Vol}(\sigma(H)) = \\
 &= |\det(\sigma(x_i))| = \frac{1}{2^s} |\det(\sigma_i(x_j))| = \frac{1}{2^s} \sqrt{|D(x_1, \dots, x_n)|} = \\
 &= \frac{1}{2^s} \sqrt{|\text{disc}(\mathcal{O}_L/\mathbb{Z})|} \neq 0 \quad \text{см. лемма 1.8.2 и NT4} \\
 &\quad \text{Базисом } \sigma(x_1), \dots, \sigma(x_n) - \\
 &\quad \text{базис пространства } \sigma(H). \Rightarrow \sigma(H) - \text{линейно независимые} \quad \square
 \end{aligned}$$

Средство (Кронемер, 1877) $\text{sign}(\text{disc}(L/\mathbb{Q})) = (-1)^s$.

D-то: см. гл-во remain 1.

Лемма 2 Пусть $0 \neq I \subseteq \mathcal{O}_L$. Тогда $\sigma(I)$ — линейно независимы в $\mathbb{R}^n$ и $\text{Vol}(\sigma(I)) = \frac{1}{2^s} \text{NV}(I) \sqrt{d_L}$, где $d_L = |\text{disc}(\mathcal{O}_L/\mathbb{Z})|$

Д-во: I — к.ч. $\mathcal{O}_L$ — модуль $\Rightarrow \exists a_1, \dots, a_n \in \mathbb{Z}$, что $a_1 x_1, \dots, a_n x_n$ — базис I и $\exists$ базис $x_1, \dots, x_n$ в $\mathcal{O}_L$ над $\mathbb{Z}$.

Тогда по определению нормировки $IV(I) = |\sigma_L/I| = |a_1 \dots a_n|$
 $\Rightarrow \sigma(I) = \frac{1}{2^s} |\det(\sigma_i(a_j x_j))| = \frac{1}{2^s} |a_1 \dots a_n| |\det(\sigma_i(x_j))| =$
 $= \frac{1}{2^s} IV(I) \sqrt{|disc(\sigma_L/I)|}$ Зам. $disc(\sigma_L/I) \neq 0$, т.к. $L/\mathbb{Q}$ - сеп.
 Δ -во измер. I (см. выше)] $y \in \mathcal{O}_L$

Тогда $y^* = y^{-1} \in Id(\mathcal{O}_L)$, т.е. $y \cdot y^* = 1$ - единица в $Id(\mathcal{O}_L)$

Значит, y делится на y^* , т.е. $y^* \leq \mathcal{O}_L$. Тогда

$vol(\sigma(y^*)) = \frac{1}{2^s} IV(y^*) \sqrt{|d_L|}$ по лемме 2. Пусть берем

$t \in \mathbb{R}_+$: $vol(B_t) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} = 2^n vol(\sigma(y^*))$ (факт)

Заметим, что B_t - комп. центр. сир. сир. в $\mathbb{R}^n$, измеримое мн. в $\mathbb{R}^n$.

$\Rightarrow$ По лемме Бэра $\exists x \in y^* : \sigma(x) \in B_t$.

Обозначим $I \cdot (x) \mathcal{Y} \subseteq \mathcal{Y}^*$. Тогда $I \cdot \mathcal{Y}^* = (x) \cdot \mathcal{Y} \cdot \mathcal{Y}^* = (x) \trianglelefteq \mathcal{O}_L$.
 $I \trianglelefteq \mathcal{O}_L$, т.е. $I \subseteq \mathcal{Y}^*$. Отсюда $\exists$ к-то η -во (с) $\exists$ I , т.е. $I \in \mathcal{Y}P(\mathcal{O}_L)$.

По п. 2.5.1. $N((x)) = N(x\mathcal{O}_L) = N_{L/\mathbb{Q}}(x) \neq \emptyset$. А по п. 2.5.2

$N((x)) = [N((x))] \neq \emptyset \Rightarrow \#N((x)) = |N_{L/\mathbb{Q}}(x)|$. Поэтому

$$N(I) \cdot N(\mathcal{Y}^*) = N(I \cdot \mathcal{Y}^*) = N((x)) = |N_{L/\mathbb{Q}}(x)| \stackrel{\text{п. 2.5.3}}{=} \text{ANS}$$

$$= \left| \prod_{\sigma \in \text{Hom}(L, \mathbb{C})} \sigma(x) \right| = |\sigma_1(x)| \cdot |\sigma_2(x)| \cdot |\sigma_3(x)|^2 \cdot |\sigma_4(x)|^2 \leq$$

$$\leq \left(\frac{|\sigma_1(x)| + |\sigma_2(x)| + 2|\sigma_3(x)| + 2|\sigma_4(x)|}{n} \right)^n \leq \frac{t^n}{n^n} \quad \sqrt[n]{a_1 \dots a_n} \leq \frac{a_1 + \dots + a_n}{n}$$

$$\text{Унас, } \#N(I) \cdot \#N(\mathcal{Y}^*) \leq \frac{t^n}{n^n}.$$

но ord-vo
 B_t , beg
 $x \in B_t$.

Поэтому $\mathbb{N}(I) \leq \frac{1}{n^n} \frac{t^n}{\mathbb{N}(J^*)} = \frac{n!}{n^n} \frac{2^{2s}}{\pi^s} \sqrt{|d_{\mathbb{Z}}|} = C$ 

Вопрос, делить 2 и факт 4.