

④ Конечность групп 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

1-м правило (см. следствие 2.3.2 из АНТБ) :

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

Уско : Д-во, что $h_L < \infty \quad \forall$ алг. числ. 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 r 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 пара $\psi, \overline{\psi}$ — $\mathbb{Q}$ 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 $\sigma : L \rightarrow \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n$ сг. образом

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

$\forall x \in L.$

Лемма 1 Пусть $x_1, \dots, x_n$ — линейно независимые в $\mathbb{Q}$, $H = \mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$.
 Тогда $\sigma(H)$ — полная решетка в $\mathbb{R}^n$ и $\text{Vol}(\sigma(H)) = \frac{1}{2^n} \sqrt{|\text{disc}(x_i/x_j)|}$.

Опр 1 $H \leq \mathbb{R}^n$ — **решетка**, если найдется л.н. набор $e_1, \dots, e_n \in \mathbb{R}^n$:
 $H = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$, при $n = n$ решетка наз-ся **полной**.
 $T = \{x \in \mathbb{R}^n \mid x = \sum_{i=1}^n \alpha_i e_i, 0 \leq \alpha_i < 1\}$ — фундаментальный параллелепипед
 полной решетки.
 $\text{Vol}(H) := \text{Vol}(T)$ — **объем** полной решетки.

Факт 1: ТЗависит от выбора базиса $e_1, \dots, e_n$ решетки H , но
 $\text{Vol}(H) = \text{Vol}(T)$ нет!

Факт 2: $\mathbb{R}^n = \bigcup_{h \in H} (h + T)$ где T — фундаментальный параллелепипед H .

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

Факт 3: $H \subseteq \mathbb{R}^n$ дискретна $\Leftrightarrow H$ - решетка в л.о. $L(H)$.

Упр 1 Δ -во факты 1, 2, 3.

Теорема (Менковская, 1897). Пусть $H \subseteq \mathbb{R}^n$ полная решетка, S - произв. мн-во, выпукл.-симм. относительно 0 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 $S \cap (H \setminus \{0\}) \neq \emptyset$.

произв. 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. в б) обязательно!

Упр 2 Δ -об T -му Мейковскому (или норм-н у Губерца).

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

Факт 4: $\text{Vol}(B_t) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$ Упр 3 Δ -об факт 4.

Вернемся к Δ -обу леммы 1: $x_1, \dots, x_n$ — реальный базис $\langle \ker \mathbb{Q} \rangle$.

Вспомогательный $\text{Vol}(G(H)) = \left| \det \begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_n) \\ -\sigma(x_1) \\ \vdots \\ -\sigma(x_n) \end{pmatrix} \right|$ и покажем, что такое.

Ир-дмн столбцов, их можно переписать к тривиальному базису

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

$$\begin{aligned}
 \det(\sigma_i(x_j)) &= (-2i)^s \det(\sigma(x_i)) \Rightarrow \text{Vol}(\sigma(H)) = \\
 &= |\det(\sigma(x_i))| = \frac{1}{2^s} |\det(\sigma_i(x_j))| \stackrel{\text{см. АНТ?}}{=} \frac{1}{2^s} \sqrt{|D(x_1, \dots, x_n)|} = \\
 &= \frac{1}{2^s} \sqrt{|\text{disc}(\mathcal{O}_L/\mathbb{Z})|} \neq 0 \quad \text{В частности, } \sigma(x_1), \dots, \sigma(x_n) - \\
 &\text{базис векторов } \sigma(H). \Rightarrow \sigma(H) - \text{многообразие} \quad \square
 \end{aligned}$$

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

D-то: см. сб-во remain 1.

Лемма 2 Пусть $0 \neq I \subseteq \mathcal{O}_L$. Тогда $\sigma(I)$ — многообразие
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 $\exists$ глс базиса $x_1, \dots, x_n$ в $\mathcal{O}_L$ над $\mathbb{Z}$.

Тогда по определению нормированности $\mathbb{N}(I) = |\mathcal{O}_L/I| = |a_1 \dots a_n|$
 $\Rightarrow \delta(I) = \frac{1}{2^s} |\det(\sigma_i(a_j x_j))| = \frac{1}{2^s} |a_1 \dots a_n| |\det(\sigma_i(x_j))| =$
 $= \frac{1}{2^s} \mathbb{N}(I) \sqrt{|\text{disc}(\mathcal{O}_L/I)|} \quad \square$

Предл. 1 Пусть L — числовое поле. Тогда канонический идеал $\mathfrak{c}_L$ из $\text{Cl}(\mathcal{O}_L)$ содержит элемент $I \in \mathcal{O}_L$ такой, что

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

Теорема 1 $h_L < \infty$.

1 — из следствия Т. 1 и предложения 1. Обозначим через C_L константу, стоящую в правой части неравенства (*).

В сечу и в T -мн 2.5.2 из АНТХ имеется только
кон. число $I \trianglelefteq \mathcal{O}_L : \mathbb{N}(I) \leq C_L$. В сечу. предп. 1

$\Rightarrow$ имеется только конечное число идеалов $\mathcal{O}_L$ $\square$

1-во предп. 1: Пусть $\gamma \cdot P(\mathcal{O}_L) \in \mathcal{O}_L$, $\gamma \in \text{Id}(\mathcal{O}_L)$

тогда $\gamma^* = \gamma^{-1} \in \text{Id}(\mathcal{O}_L)$, где $\gamma \cdot \gamma^* = \mathcal{O}_L$ — единица в $\text{Id}(\mathcal{O}_L)$

Значит, γ можно выбрать так, что $\gamma^* \trianglelefteq \mathcal{O}_L$. Тогда

$\text{vol}(\sigma(\gamma^*)) = \frac{1}{2^s} \mathbb{N}(\gamma^*) \sqrt{|d_L|}$ по лемме 2. Попробуем

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

Заметим, что B_t — конт. центр. сим. борн., измеримое мн. в $\mathbb{R}^n$.

$\Rightarrow$ по л. Либмана $\exists_{\neq 0} x \in \gamma^* : \sigma(x) \in B_t$.

Обозначим $I \cdot (x) \cdot J \subseteq J^*$. Тогда $I \cdot J^* = (x) \cdot J \cdot J^* = (x) \trianglelefteq \mathcal{O}_L$.
 $I \trianglelefteq \mathcal{O}_L$, т.е. $I \subseteq J^*$. Отсюда $g \rightarrow$ на $\mathbb{Q}$ -ву (в) $g \mapsto I$, т.е. $I \in JP(\mathcal{O}_L)$.

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

$$N(I) \cdot N(J^*) = N(I \cdot J^*) = N((x)) = |N_{L/\mathbb{Q}}(x)| \stackrel{\text{по 1.3.3. и лем. 2}}{=} \quad$$

$$= \left| \prod_{\sigma \in \text{Hom}_{\mathbb{Q}}(L, \mathbb{C})} \sigma(x) \right| = |\sigma_1(x)| \cdot |\sigma_r(x)| \cdot |\sigma_{r+1}(x)|^2 \cdot \dots \cdot |\sigma_s(x)|^2 \leq$$

$$\leq \left(\frac{|\sigma_1(x)| + \dots + |\sigma_r(x)| + 2(|\sigma_{r+1}(x)| + \dots + |\sigma_s(x)|)}{n} \right)^n \leq \frac{t^n}{n^n} \quad \sqrt[n]{|\sigma_{r+1}(x)|^2 \dots |\sigma_s(x)|^2} \leq \frac{2 + \dots + 2}{n}$$

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

по орг-во
 B_t , $\forall g \in B_t$
 $x \in B_t$.

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

Вопрос, делится ли 2 и факт 4.

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

Упр 3 1-го следствие 1 можно переписать в эквив. форме (*).

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 $\mathcal{O}_L$.

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

С помощью крив-БА (6) из Предл 1 можно вывести h_L .

Пример $L = \mathbb{Q}[\sqrt{-2}]$, $B = \mathcal{O}_L$. Мы знаем, что модуль
класс A из $Cl(\mathcal{O}_L)$ содержит $I \trianglelefteq B$: $N(I) < C_L$ из (4).
Так как $k=2$, $\text{Hom}_{\mathbb{Q}}(L, \mathbb{C}) = \{\text{id}, \bar{\text{id}}\} \Rightarrow s=2, r=0$ $d_L = 4m = -8$,
 $\Rightarrow N(I) \leq \frac{2!}{2^2} \cdot \frac{4}{\pi} \cdot \sqrt{8} = \frac{4\sqrt{2}}{8} < 2 \Rightarrow N(I) = 1 \Rightarrow I = B \Rightarrow$
 $\Rightarrow A = 1 = \mathcal{O}_L \Rightarrow h_L = 1 \Rightarrow L$ факториальна!

Т. 2 (Дикс, 1857, о гильберте). Для любого $d \in \mathbb{Z}$

существуют только конечное число чисел арт. полей L ,
для которых $\text{disc}(\mathcal{O}_L/\mathbb{Z}) = d$.

Упр 5. 1 - то Т2. (см. см. ТУБАРЕВА).