(4) Конечность группы классов

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

$Id(\mathcal{O}_L)$ – группа дробных идеалов кольца $\mathcal{O}_L$,

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

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

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

Δ – минк. (см. следствие 2.3.2 из ANT7):

$h_L = 1 \iff \mathcal{O}_L$ – кольцо гл. идеалов $\iff \mathcal{O}_L$ 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 $\mathbb{C}=\overline{\mathbb{Q}}$, оставл. $\mathbb{Q}$ – неподвижным. Выберем нумерацию так: $\sigma_i(L)\subseteq\mathbb{R} \Leftrightarrow i=1..r$. Тогда вл-я $\sigma_{r+1},\dots\sigma_n$ разбиваются на пары сопряженных, т.к. $\forall$ $\mathbb{Q}$-вл-я $\psi: L\to\mathbb{C}$ т.ч. $\psi(L)\not\subseteq\mathbb{R}$, оп-е $\overline{\psi}: x\to\overline{\psi(x)}$ ← Ком. Сопр., тоже вл-е $\mathbb{Q}$ вложения L в $\mathbb{C}$, отл. от 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 $\sigma: L\to\mathbb{R}^r\times\mathbb{C}^s\simeq\mathbb{R}^n$ сл. образом

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

Сейчас мы докажем т. 1 исходя из предл. 1

Предл. 1 Пусть L – числ. пол. Тогда каждый класс из $Cl(\mathcal{O}_L)$ содержит целый идеал $I \trianglelefteq \mathcal{O}_L$, такой, что

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

Д-во т. 1: Обозн. через C_L константу из правой части (*). В силу и 3 т-мы 2.5.2 из АНТ 3 имеется только кон. число $I \trianglelefteq \mathcal{O}_L$: $\mathbb{N}(I) < C_L$. В силу предл. 1 $\Rightarrow$ имеется только конечное число классов $Cl(\mathcal{O}_L)$ ▣

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

Упр 1* Д-ть следствие 1 воспользовавшись нер-вом (*).

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

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

Д-во: В силу 1 $|d_L| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} > 1 \Rightarrow \exists p \mid d_L$

$\Rightarrow p\mathcal{O}_L$ разветвл. по Т. 2.4.3 из ANT ■

С помощью нер-ва (b) из предл 1 можно искать h_L!

Пример $L = \mathbb{Q}[i]$, $B = \mathcal{O}_L$. Мы знаем, что любой класс D из $Cl(\mathcal{O}_L)$ содержит $I \trianglelefteq B$: $N(I) < C_L$ из (*).

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

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

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

Т. 2 (Эрмит, 1857, о дискриминанте). Для любого $d \in \mathbb{Z}$ существует только конечное число числ. орб. полей L, для которых $\mathrm{disc}(O_L/\mathbb{Z}) = d$. ∎ Упр 2* 1 – по Теореме 2

Опр 1. $H \leq \mathbb{R}^n$ – **РЕШЁТКА**, если найдется л.н. набор $e_1, \dots, e_k \in \mathbb{R}^n$:

$H = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_k$, при $k = n$ решетка наз-ся **полной**.

$T = \{x \in \mathbb{R}^n \mid x = \sum_{i=1}^{n} \alpha_i e_i, 0 \leq \alpha_i < 1\}$ – фундам. параллелепипед полной решетки.

$\mathrm{Vol}(H) := \mathrm{Vol}(T)$ – **объем** полной решетки.

Факт 1: T зависит от выбора базиса $e_1, \dots, e_n$ решетки H, но $\mathrm{Vol}(H) = \mathrm{Vol}\,T$) **нет!** ← без проверок – исключений

Факт 2: $\mathbb{R}^n = \dot{\bigcup}_{h \in H} (h + T)$ для любой полной решетки H.

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

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

Упр 1 Доказать а) $\Leftarrow$ б) $\Rightarrow$

Теорема 3 (Минковский, 1897) Пусть $H \leq \mathbb{R}^n$ полная решетка, S - огран. изм., центр.-симм. выпуклое подмн-во в $\mathbb{R}^n$. Если

а) $\mathrm{Vol}(S) > 2^n \mathrm{Vol}(H)$ или б) $\mathrm{Vol}(S) \geq 2^n \mathrm{Vol}(H)$ и S - компакт,

то $S \cap (H \setminus \{0\}) \neq \emptyset$.

(открытое мн-во)

Пример $H = \mathbb{Z}e_1 + \mathbb{Z}e_2 \leq \mathbb{R}^2$, $e_1 = (1,0)$, $e_2 = (0,1)$ и $S = \{\alpha_1 e_1 + \alpha_2 e_2 \mid -1 < \alpha_i < 1\}$.

Тогда $\mathrm{Vol}(S) = 4 = 2^2 \mathrm{Vol}(H)$, но $S \cap H = \{0\}$. Условие компактности б) обязательно!

Д-во теоремы 3: а) Пусть $S' = \frac{1}{2}S$ (мин. разм. уменьшился в 2 раза

Имеем $\mathrm{vol}(S') = \frac{1}{2^n}\mathrm{vol}(S) > \mathrm{vol}(H) = \mathrm{vol}(T)$, где

T – фунд. парал. для H при каком-то фикс. базисе.

$$R^n = \bigcup_{h\in H}(T+h) \Rightarrow S' = \bigcup_{h\in H} S' \cap (T+h) \Rightarrow \mathrm{vol}(T+h) = \mathrm{vol}(H) \ \forall h$$

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

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

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

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

Сл-но, из счетной аддитивности объема вытекает, что

$\exists h_1, h_2 \in H : h_1 \neq h_2$ и $S_{h_1} \cap S_{h_2} \neq \emptyset$. Тогда
$\exists x \in S_{h_1} \cap S_{h_2} \subseteq T$ 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 $2s_1$ и $2s_2 \in S = 2S'$
$\Rightarrow -2s_2 \in S$ (S - центр сегм.). Тогда

$h = \frac{1}{2}(2s_1) + \frac{1}{2}(-2s_2) = s_1 - s_2 \in H$, что и треб.

$S^{\cap}$ есть выпукл.

#
○

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

Рассмотрим $S_m = (1 + \frac{1}{m})S$ для $m = 1, 2, 3, \ldots$ Имеем
$S_1 \supset S_2 \supset \ldots \supset S_m \supset \ldots$ Пересеч $\bigcap S_m = S$. В силу
$m \geq 1$
комп., выпукл и центр сегм.

и $\mathrm{Vol}(S_m) > \mathrm{Vol}(S)$

По а) $\forall n = 1, 2, \ldots \ \exists\, 0 \neq h_n \in H : h_n \in S_n$

Обозн. $S_n' = S_n \cap (H \setminus \{0\}) \ni h_n$. Имеем

$$S_1' \supseteq S_2' \supseteq \ldots \supseteq S_n' \supseteq \ldots \qquad (*)$$

Заметим, что $S_1 \overset{\neq}{\ni} 0$ орен $\Rightarrow S_1' = S_1 \cap H \setminus \{0\}$ – конечное мн-во (см. факт 3), т.е $(*)$ – убывающая цепочка конечных непустых мн-в. $\Rightarrow$ стабилизируется

и сосем-но $\bigcap_{n \geq 1} S_n' = \left(\bigcap_{n \geq 1} S_n\right) \cap (H \setminus \{0\}) = S$.

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

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

Лемма 1 Пусть $x_1, \dots x_n$ – целый базис над $\mathbb{Q}$, $H = \mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$,

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

Тогда $\sigma(H)$ – полная решетка в $\mathbb{R}^n$ и $\mathrm{Vol}(\sigma(H)) = \frac{1}{2^s}\sqrt{|\mathrm{disc}(\mathcal{O}_L/\mathbb{Z})|}$

Д-во:

Вычислим $\mathrm{Vol}(\sigma(H)) = \left|\det\begin{pmatrix} - & \sigma(x_1) & - \\ & \vdots & \\ - & \sigma(x_n) & - \end{pmatrix}\right|$ и покажем, что здесь

пр-ями совершая её можно привести к треугольному виду

$$\begin{pmatrix} \dots & a_j + b_j i & a_j - b_j i & \dots \end{pmatrix} \to \begin{pmatrix} \dots & 2a_j & a_j - b_j i & \dots \end{pmatrix} \to \begin{pmatrix} 2a_j & -b_j i \end{pmatrix} \Longrightarrow$$

$+$ (стрелка)

$-\frac{1}{2}\times$

$\det(\sigma_i(x_j)) = (-2i)^s \det(\sigma(x_i)) \Rightarrow \mathrm{Vol}(\sigma(H)) =$

$= |\det(\sigma(x_i))| = \frac{1}{2^s} |\det(\sigma_i(x_j))| = \frac{1}{2^s} \sqrt{|D(x_1,\dots x_n)|} =$

см. предл. 2.6.2 из §4 гл 4

$= \frac{1}{2^s} \sqrt{|\mathrm{disc}(\mathcal{O}_L/\mathbb{Z})|} \neq 0$ в частности, $\sigma(x_1)\dots\sigma(x_n)$ — базис решетки $\sigma(H) \Rightarrow \sigma(H)$ — полная решетка ▣

Следствие (Дирихле, 1877) $\mathrm{sign}(\mathrm{disc}(L/\mathbb{Q})) = (-1)^s$.

Д-во: см. св-во пункт 1.

Лемма 2 Пусть $0 \neq I \trianglelefteq \mathcal{O}_L$. Тогда $\sigma(I)$ — полная решетка в $\mathbb{R}^n$ и $\mathrm{Vol}(\sigma(I)) = \frac{1}{2^s} \mathbb{N}(I) \sqrt{d_L}$, где $d_L = |\mathrm{disc}(\mathcal{O}_L/\mathbb{Z})|$

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

Тогда по опр-ю считающей нормы $\mathbb{N}(I) = |O_L/I| = |a_1 \dots a_n|$

$\Rightarrow \sigma(I) = \frac{1}{2^s}|\det(\sigma_i(a_j x_j))| = \frac{1}{2^s}|a_1 \dots a_n||\det(\sigma_i(x_j))| =$

$= \frac{1}{2^s}\mathbb{N}(I)\sqrt{|disc(O_L/I)|}$ ∎ Зам. $disc(O_L/I) \neq 0$, т.к. $L/\mathbb{Q}$ — сепар.

Д-во предл. 1 (см. выше) Пусть $\mathcal{J} \cdot P(O_L) \in Cl(O_L)$, $\mathcal{J} \in Id(O_L)$

Тогда $\mathcal{J}^* = \mathcal{J}^{-1} \in Id(O_L)$, где $\mathcal{J} \cdot \mathcal{J}^* = O_L$ — единица в $Id(O_L)$

Значит, $\mathcal{J}$ можно выбрать так, что $\mathcal{J}^* \trianglelefteq O_L$. Тогда

$vol(\sigma(\mathcal{J}^*)) = \frac{1}{2^s}\mathbb{N}(\mathcal{J}^*)\sqrt{|d_L|}$ по лемме 2. Подберём

$t \in \mathbb{R}_+$: $Vol(B_t) = 2^r \cdot \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} = 2^n Vol(\sigma(\mathcal{J}^*))$ (факт 4)

Заметим, что B_t — компл. центр. симм. выпукл., измеримое мн-во.

$\Rightarrow$ По т. Минковского $\exists_{x \neq 0}\, x \in \mathcal{J}^* : \sigma(x) \in B_t$.

Обозначим $I^{-1}(x)J \subseteq J^*$. Тогда $I \cdot J^* = (x) \cdot J \cdot J^* = (x) \trianglelefteq \mathcal{O}_L$.

$I \trianglelefteq \mathcal{O}_L$, т.к. $I \subseteq J^*$. Остаётся доказать, что $I \in \mathcal{J}\mathcal{P}(\mathcal{O}_L)$.

По п. 2.5.5. $\mathcal{N}((x)) = \mathcal{N}(x\mathcal{O}_L) = N_{L/\mathbb{Q}}(x) \in \mathbb{Z}$. А по т. 2.5.2

$\mathcal{N}((x)) = |\mathcal{N}((x))| \in \mathbb{Z} \Rightarrow |\mathcal{N}((x))| = |N_{L/\mathbb{Q}}(x)|$. Поэтому

$$\mathcal{N}(I) \cdot \mathcal{N}(J^*) = \mathcal{N}(I \cdot J^*) = \mathcal{N}((x)) = |N_{L/\mathbb{Q}}(x)| \overset{\text{пр. 2.5.3 и т. ANT3}}{=}$$

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

$$\leq \left(\frac{|\sigma_1(x)| + \ldots + |\sigma_r(x)| + 2(|\sigma_{r+1}(x)| + \ldots + 2|\sigma_{r+s}(x)|)}{n} \right)^n \leq \frac{t^n}{n^n}$$

$\sqrt[n]{a_1 \cdots a_n} \leq \frac{a_1 + \ldots + a_n}{n}$

по опр-ю B_t, $\forall x \in B_t$.

Итак, $\mathcal{N}(I) \cdot \mathcal{N}(J^*) \leq \frac{t^n}{n^n}$.

Поэтому $\mathbb{N}(I) \leq \frac{1}{n^n} \frac{t^n}{\mathbb{N}(\mathfrak{f}^*)} = \frac{n!}{n^n} \frac{2^{2s}}{\pi^s} \sqrt{|d_K|} = C$ ∎

(вывод, лемма 2 и факт 4.)