Алгебраическая теория чисел
БФУ им. И.Канта – Малыгина Е.С.

Лекция №9

5 Нормы идеалов

5.1 Основные определения

Определение 1. Пусть $\mathfrak{a} \neq 0$, $\mathfrak{a} \subset O_K$, тогда $N(\mathfrak{a}) = |O_K/\mathfrak{a}| = (O_K^+ : \mathfrak{a}^+)$.

Лемма 1. *Пусть $\mathfrak{a} \neq 0$ – идеал, $\mathfrak{p} \neq 0$ – простой идеал. Тогда $\exists \alpha \in \mathfrak{a} - \mathfrak{ap}$, такое, что $\mathfrak{a} = (\alpha) + \mathfrak{ap}$.*

Лемма 2. *$(O_K : \mathfrak{p}) = (\mathfrak{a} : \mathfrak{ap})$ – индекс по подгруппе.*

Теорема 1. *1. Пусть $\mathfrak{p}_1; ...; \mathfrak{p}_n$ – ненулевые простые идеалы, тогда*

$$N(\mathfrak{p}_1 \cdot ... \cdot \mathfrak{p}_n) = N(\mathfrak{p}_1) \cdot ... \cdot N(\mathfrak{p}_n).$$

2. Пусть $\mathfrak{a}, \mathfrak{b}$ – ненулевые идеалы, тогда $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

5.2 Вычисление норм идеалов

Теорема 2. *Пусть K – числовое поле степени n, $\mathfrak{a}$ – ненулевой идеал, $\mathfrak{a} \subset O_K$. Тогда $\mathfrak{a}^+$ – подгруппа в O_K^+ ранга n. Кроме того, если $\delta_1, ..., \delta_n$ – целый базис для $\mathfrak{a}$ и $\omega_1, ..., \omega_n$ – целый базис O_K, то*

$$N(\mathfrak{a}) = \left| \frac{D(\delta_1, ..., \delta_n)}{D(\omega_1, ..., \omega_n)} \right|.$$

Теорема 3. *Если $\mathfrak{b} = (\beta)$, $\beta \in O_K$, то $N(\mathfrak{b}) = |N_{K/\mathbb{Q}}(\beta)|$.*

Пример 1. Рассмотрим $K = \mathbb{Q}(\sqrt{15})$. Поскольку $15 \not\equiv 1 \pmod 4$, то $1, \sqrt{15}$ – это целый базис.

Пусть $\mathfrak{a} = (7, 1 + \sqrt{15}) = 7O_K + (1 + \sqrt{15})O_K$.

Так как ранг O_K равен 2, то $O_K = 1 \cdot \mathbb{Z} \oplus \sqrt{15} \cdot \mathbb{Z}$.

$\mathfrak{a}$ порождается элементами $7, \sqrt{15}, 7\sqrt{15}, 1 + \sqrt{15}, \sqrt{15}(1 + \sqrt{15})$.

Обозначим $x_1 = 1, x_2 = \sqrt{15}$. Тогда $\mathfrak{a}$ порождается $7x_1, 7x_2, x_1+x_2, 15x_1+x_2$.

Следовательно, $O_K/\mathfrak{a} \cong \langle x_1, x_2 | 7x_1, 7x_2, x_1 + x_2, 15x_1 + x_2 \rangle$.

Запишем в виде матрицы два вектора коэффициентов перед x_1 и x_2 в элементах, порождающих $\mathfrak{a}$:

$$\begin{pmatrix} 7 & 0 & 1 & 15 \\ 0 & 7 & 1 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \end{pmatrix}.$$

Имеем $O_K/\mathfrak{a} \cong \mathbb{Z}/(1 \cdot \mathbb{Z}) \oplus \mathbb{Z}/(7 \cdot \mathbb{Z}) \cong \mathbb{Z}_7$. Тогда $N(\mathfrak{a}) = (O_K^+ : \mathfrak{a}^+) = 7$.

Докажем, что $\mathfrak{a}$ – не является главным идеалом (от противного). Пусть $\mathfrak{a} = (a \cdot 1 + b \cdot \sqrt{15})$, $a, b \in \mathbb{Z}$, тогда

$$N(\mathfrak{a}) = |N_{K/\mathbb{Q}}(a + b\sqrt{15})| = |(a + b\sqrt{15})(a - b\sqrt{15})| = |a^2 - 15b^2|.$$

Получаем $a^2 - 15b^2 = \pm 7$ и $a^2 \equiv \pm 2 \mod 5$. Очевидно, что не существует $a \in \mathbb{F}_5$, удовлетворяющего данному сравнению. Следовательно, не существует $a + b\sqrt{15}$, такого, что $\mathfrak{a} = (a + b\sqrt{15})$.

Лемма 3. *(1) Пусть $\mathfrak{a} \subset \mathfrak{b}, \mathfrak{a}, \mathfrak{b} \neq 0$ – идеалы в O_K. $\mathfrak{a} = \mathfrak{b}$ тогда и только тогда, когда $N(\mathfrak{a}) = N(\mathfrak{b})$.*

(2) Если $\alpha \in \mathfrak{a} \subset O_K$, то $(\alpha) = \mathfrak{a} \Leftrightarrow N_{K/\mathbb{Q}}(\alpha) = N(\mathfrak{a})$.

Пример 2. Рассмотрим $K = \mathbb{Q}(\sqrt{15}), \mathfrak{a} = (17, 7 + \sqrt{15}), N(\mathfrak{a}) = 17 = N_{K/\mathbb{Q}}(\alpha)$.

Отметим, что если α – алгебраическое целое, то $\alpha = a + b\sqrt{15}$. Соответственно, $17 = |a^2 - 15b^2| \Rightarrow a^2 \equiv \pm 2 \pmod 5$.

6 Теорема Дедекинда-Куммера

Лемма 1. *K – числовое поле, $\mathfrak{a} \neq 0, \mathfrak{a} \subset O_K$. Пусть $a = N(\mathfrak{a})$. Тогда $a \in \mathfrak{a}$.*

Теорема 1. *Пусть $K(\theta)$ – числовое поле, где θ – алгебраическое целое; p – простое и $p \not| (O_K : \mathbb{Z}[\theta])$. Будем считать, то минимальный многочлен элемента θ раскладывается на множители по модулю p:*

$$\mu_\theta(X) \equiv f_1(X)^{e_1} \cdot f_2(X)^{e_2} \cdot ... f_r(X)^{e_r} \pmod p,$$

где $f_i \in \mathbb{Z}[X]$ – унитарные неприводимые над $\mathbb{Z}_p$ и попарно взаимно простые многочлены. Пусть $\mathfrak{p}_i = (p, f_i(\theta))$. Тогда $\mathfrak{p}_i$ – попарно различные простые идеалы и $(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_r^{e_r}$; $N(\mathfrak{p}_i) = p^{deg\, f_i}$.

Пример 1. 1. Рассмотрим $K = \mathbb{Q}(\sqrt{-30})$.
$-30 \not\equiv 1 \pmod 4$, значит, $1, \sqrt{-30}$ – целый базис $\Rightarrow O_K = \mathbb{Z}[\sqrt{-30}]$
$\Rightarrow (O_K : \mathbb{Z}[\sqrt{-30}]) = 1$.
$\mu_{\sqrt{-30}}(X) = X^2 + 30$.

- $p = 2$:
  $X^2 + 30 \equiv X^2 \pmod 2 \Rightarrow (2) = 2O_K = \mathfrak{p}_2^2 = (2, \sqrt{-30})^2$, $N(\mathfrak{p}_2) = 2$.

- $p = 3$:
  $X^2 + 30 \equiv X^2 \pmod 3 \Rightarrow (3) = 3O_K = \mathfrak{p}_3^2 = (3, \sqrt{-30})^2$, $N(\mathfrak{p}_3) = 3$.

- $p = 5$:
  $X^2 + 30 \equiv X^2 \pmod 5 \Rightarrow (5) = 5O_K = \mathfrak{p}_5^2 = (5, \sqrt{-30})^2$, $N(\mathfrak{p}_5) = 5$.

- $p = 7$:
  $X^2 + 30 \equiv X^2 + 2 \pmod 7$ – неприводимый $\Rightarrow (7) = \mathfrak{p}_7$, $N(\mathfrak{p}_7) = 49$.

- $p = 11$:
  $X^2 + 30 \equiv X^2 + 8 \equiv (X + 5)(X + 6) \pmod{11} \Rightarrow (11) = \mathfrak{p}_{11,1} \cdot \mathfrak{p}_{11,2}$;
  $\mathfrak{p}_{11,1} = (11, 5 + \sqrt{-30})$, $N(\mathfrak{p}_{11,1}) = 11$.
  $\mathfrak{p}_{11,2} = (11, 6 + \sqrt{-30})$, $N(\mathfrak{p}_{11,2}) = 11$.
  $N(\mathfrak{p}_{11,1} \cdot \mathfrak{p}_{11,2}) = N(\mathfrak{p}_{11,1})N(\mathfrak{p}_{11,2}) = 121$.

2. Пусть $K = \mathbb{Q}(\theta)$, где $\theta = \sqrt[3]{6}$.
$1, \theta, \theta^2$ – это целый базис $\Rightarrow O_K = \mathbb{Z}[\theta]$.
$\mu_\theta(X) = X^3 - 6$.

- $p = 5$:
  $(5) = 5O_K$.
  $X^3 - 6 \equiv X^3 - 1 \equiv (X - 1)(X^2 + X + 1) \pmod 5$.
  $(X - 1)(X^2 + X + 1) = \mathfrak{p}_{5,1} \cdot \mathfrak{p}_{5,2}$.
  $\mathfrak{p}_{5,1} = (5, \sqrt[3]{6} - 1)$, $N(\mathfrak{p}_{5,1}) = 5$.
  $\mathfrak{p}_{5,2} = (5, (\sqrt[3]{6})^2 + \sqrt[3]{6} + 1)$, $N(\mathfrak{p}_{5,1}) = 25$.
  Вопрос: являются ли $\mathfrak{p}_{5,1}, \mathfrak{p}_{5,2}$ главными идеалами?
  Пусть ζ – корень 3-й степени из единицы.
  $N(\sqrt[3]{6} - 1) = (\sqrt[3]{6} - 1)(\zeta\sqrt[3]{6} - 1)(\zeta^2\sqrt[3]{6} - 1) = 5$, следовательно,

  $$\mathfrak{p}_{5,1} = (\sqrt[3]{6} - 1).$$

  Тогда $5O_K = (\sqrt[3]{6} - 1) \cdot \mathfrak{p}_{5,2}$.

  $$\mathfrak{p}_{5,2} = \left(\frac{6-1}{\sqrt[3]{6}-1}\right) O_K = \left(\frac{(\sqrt[3]{6}-1)((\sqrt[3]{6})^2 + \sqrt[3]{6}+1)}{\sqrt[3]{6}-1}\right) O_K = ((\sqrt[3]{6})^2 + \sqrt[3]{6} + 1)O_K.$$

- $p = 2$:
  $X^3 - 6 \equiv X^3 \pmod 2$.
  $\mathfrak{p}_2 = (2, \sqrt[3]{6})$, $N(\mathfrak{p}_2) = 2$.
  $2O_K = \mathfrak{p}_2^3$.
  $N(2 - \sqrt[3]{6}) = (2 - \sqrt[3]{6})(\zeta 2 - \sqrt[3]{6})(\zeta^2 2 - \sqrt[3]{6}) = 2$.

- $p = 3$:
  $X^3 - 6 \equiv X^3 \pmod 3$.
  $\mathfrak{p}_3 = (3, \sqrt[3]{6})$, $N(\mathfrak{p}_3) = 3$.
  $3O_K = \mathfrak{p}_3^3$.
  $N(3 - \sqrt[3]{6}) = (3 - \sqrt[3]{6})(\zeta 3 - \sqrt[3]{6})(\zeta^2 3 - \sqrt[3]{6}) = 3$.

7 Группа классов идеалов

Определение 1. Пусть K – числовое поле, I_K – группа ненулевых дробных идеалов кольца O_K, P_K – группа ненулевых главных дробных идеалов. Группой классов идеалов числового поля K называется группа $Cl_K = I_K/P_K$, состоящая из классов $[\mathfrak{a}]$.

Замечание 1. $\mathfrak{a} \sim \mathfrak{b}$ (эквивалентны) $\Leftrightarrow \mathfrak{a}, \mathfrak{b} \in [\mathfrak{a}] \Leftrightarrow \mathfrak{a}\mathfrak{b}^{-1}$ – главный $\Leftrightarrow \mathfrak{a} = \gamma\mathfrak{b}, \gamma \in K$.

Теорема 1. ***(Минковского)*** *K – числовое поле степени n с подписью (r, s). Обозначим*

$$B_K = \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^s \cdot \sqrt{|\Delta_K|}.$$

– граница Минковского. Пусть $\mathfrak{a} \neq 0$ – идеал в O_K. Тогда $\mathfrak{a}$ содержит $\alpha \neq 0$, такое, что $N_{K/\mathbb{Q}}(\alpha) \leq B_K \cdot N(\mathfrak{a})$.

Утверждение 1.

1. $|Cl_K| < \infty$.
2. Cl_K порождается $\{[\mathfrak{p}] \mid \mathfrak{p}$ – простой и $N(\mathfrak{p}) \leq B_K\}$.

$h_K = |Cl_K|$ – классовое число (число классов).

Лемма 1. *Пусть $\mathfrak{p}$ – ненулевой простой идеал из O_K. Тогда существует единственное простое p, такое, что $\mathfrak{p}|pO_K$. Кроме того, $N(\mathfrak{p}) = p^f$, где f – некоторое положительное целое.*