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

Лекция №10

7 Группа классов идеалов

Пример 3. 1. Найдём Cl_K для $K = \mathbb{Q}(i)$.
$1, i$ – целый базис $\Rightarrow O_K = \mathbb{Z}[i]$.
$\Delta_K = -4$, $n = 2 \Rightarrow (r, s) = (0, 1)$.

$$B_K = \frac{1}{2} \cdot \frac{4}{\pi} \cdot \sqrt{4} \approx 1.27 < 2.$$

Рассмотрим $(p) = pO_K$, $p < 2 \Rightarrow p = 1 \Rightarrow (p) = (1) = O_K$.
Тогда $Cl_K = \{[O_K]\}$.

2. Пусть $K = \mathbb{Q}(\sqrt{7})$.
$1, \sqrt{7}$ – целый базис $\Rightarrow O_K = \mathbb{Z}[\sqrt{7}]$.
$\Delta_K = 28, n = 2, (r, s) = (2, 0)$.

$$B_K = \frac{1}{2} \cdot \frac{4}{\pi}^0 \cdot \sqrt{28} = \sqrt{7} < 3.$$

Рассмотрим $p \leq B_K, p = 2 : \mu_{\sqrt{7}}(X) = X^2 - 7$.
$X^2 - 7 \equiv X^2 + 1 \equiv (X + 1)^2 \pmod 2$.
Следовательно, $f_1(X) = X + 1$.
По теореме Дедекинда-Куммера: $\mathfrak{p}_2 = (2, \sqrt{7})$, $\mathfrak{p}^2 = (2)$.
$N(\mathfrak{p}_2) = 2$.
Возможно, что $Cl_K = \{[O_K], [\mathfrak{p}_2]\}$. Проверим так ли это: проверим, эквивалентны ли эти классы.
Рассмотрим $\alpha \in \mathfrak{p}_2 \Rightarrow \alpha = a \cdot 2 + b \cdot (\sqrt{7} + 1)$.
Пусть $a = b = 1$, тогда $\alpha = 3 + \sqrt{7} \in \mathfrak{p}_2$.
Получается, что $(3 + \sqrt{7}) \subset \mathfrak{p}_2 \Rightarrow (3 + \sqrt{7})O_K \subset \mathfrak{p}_2 \Rightarrow \mathfrak{p}_2 \sim \varnothing_K \Rightarrow [\mathfrak{p}_2] = [O_K]$.
Следовательно, $Cl_K = \{[O_K]\}$, $h_K = 1$.

3. Пусть $K = \mathbb{Q}(\sqrt{-30})$.
$1, \sqrt{-30}$ – целый базис, $O_K = \mathbb{Z}[\sqrt{-30}]$.
$\Delta_K = -120, n = 2, (r, s) = (0, 1)$.

$$B_K = \frac{1}{2} \cdot \frac{4}{\pi} \cdot \sqrt{120} < 6.$$

$Cl_K = \{[\mathfrak{p}] \mid \mathfrak{p}$ – простой идеал, $N(\mathfrak{p}) \leq B_K\}$

- $p = 2 : \mathfrak{p}_2 = (2, \sqrt{-30})$, $N(\mathfrak{p}_2) = 2$.
- $p = 3 : \mathfrak{p}_3 = (3, \sqrt{-30})$, $N(\mathfrak{p}_3) = 3$.
- $p = 5 : \mathfrak{p}_5 = (5, \sqrt{-30})$, $N(\mathfrak{p}_5) = 5$.

Если $\mathfrak{p}_2$ – главный идеал, то $\mathfrak{p}_2 = (a + b\sqrt{-30})$, где $a, b \in \mathbb{Z}$.
Тогда $N_K(\mathfrak{p}_2) = a^2 + 30b^2 = 2$ – противоречие, таких a, b не существует. Следовательно, $\mathfrak{p}_2$ не эквивалентен O_K.
$\mathfrak{p}_2^2 = (2, \sqrt{-30})(2, \sqrt{-30}) = (4, 2\sqrt{-30}, -30) = (4, 2\sqrt{-30}, 2) = 2(2, \sqrt{-30}, 1) = 2O_K$.
Делаем вывод, что $\mathfrak{p}_2^2 \sim O_K$.
Аналогично и $\mathfrak{p}_3^2, \mathfrak{p}_5^2 \sim O_K$.
$ord(\mathfrak{p}_2) = ord(\mathfrak{p}_3) = ord(\mathfrak{p}_5) = 2$.
Рассмотрим $\mathfrak{p}_2\mathfrak{p}_3$: этот идеал не является главным. Соответственно, $\mathfrak{p}_2\mathfrak{p}_3 \not\sim O_K$.
$[\mathfrak{p}_2] \not\sim [O_K][\mathfrak{p}_3]^{-1}$.
$[\mathfrak{p}_2] \not\sim [\mathfrak{p}_3]$.
Возведём $\sqrt{-30}$ в квадрат: $(\sqrt{-30})^2 = -30 = -2 \cdot 3 \cdot 5$.
Перейдём к идеалам: $(\sqrt{-30})^2 = (2)(3)(5) = \mathfrak{p}_2^2\mathfrak{p}_3^2\mathfrak{p}_5^2$.
$O_K = (\sqrt{-30}) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$. Следовательно, $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5 \sim O_K$.
Из этой эквивалентности получаем: $[\mathfrak{p}_5] = [\mathfrak{p}_2]^{-1}[\mathfrak{p}_3]^{-1} = [\mathfrak{p}_2][\mathfrak{p}_3]$ (так как $ord(\mathfrak{p}_i) = 2) \Rightarrow \mathfrak{p}_5 \sim \mathfrak{p}_2\mathfrak{p}_3$.
$Cl_K = \{[O_K], [\mathfrak{p}_2], [\mathfrak{p}_3], [\mathfrak{p}_2\mathfrak{p}_3]\}$.
Так как $[\mathfrak{p}_2]$ не эквивалентен $[\mathfrak{p}_3] \Rightarrow h_K = 4$.

4. Пусть $K = \mathbb{Q}(\sqrt{-23})$.
$1, \frac{1+\sqrt{-23}}{2}$ – целый базис, $O_K = \mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$.
$\Delta_K = -23, n = 2, (r, s) = (0, 1)$.

$$B_K = \frac{1}{2} \cdot \frac{4}{\pi} \cdot \sqrt{23} \approx 3.1 < 4 \Rightarrow B_K \leq 3.$$

Используем теорему Виета для корней $\frac{1+\sqrt{-23}}{2}$ и $\frac{1-\sqrt{-23}}{2}$.
Тогда $\mu_{\frac{1+\sqrt{-23}}{2}}(X) = X^2 - X + 6$.

- $p = 2 : X^2 - X + 6 \equiv X(X + 1) \Rightarrow (2) = \mathfrak{p}_2\mathfrak{p}_2'$.
  $\mathfrak{p}_2 = (2, \frac{1+\sqrt{-23}}{2})$.
  $\mathfrak{p}_2' = (2, \frac{3+\sqrt{-23}}{2})$.
- $p = 3 : X^2 - X + 6 \equiv X(X + 2) \Rightarrow (3) = \mathfrak{p}_3\mathfrak{p}_3'$.
  $\mathfrak{p}_3 = (3, \frac{1+\sqrt{-23}}{2})$.
  $\mathfrak{p}_3' = (3, \frac{5+\sqrt{-23}}{2})$.

Возможно, что $Cl_K = \langle [O_K], [\mathfrak{p}_2], [\mathfrak{p}_2'], [\mathfrak{p}_3], [\mathfrak{p}_3'] \rangle$. Проверим это.
Сперва проверим, является ли $\mathfrak{p}_2$ главным идеалом.
Если является, то $\mathfrak{p}_2 = (\alpha); \alpha \in O_K \Rightarrow \alpha = a + b\frac{1+\sqrt{-23}}{2}$, где $a, b \in \mathbb{Z}$.
$N_K(\mathfrak{p}_2) = N_K(\mathfrak{p}_2') = 2$.
$N_K(\mathfrak{p}_3) = N_K(\mathfrak{p}_3') = 3$.

$N_K(\mathfrak{p}_2) = (a + \frac{b}{2})^2 + \frac{23b^2}{4} = a^2 + ab + 6b^2$.
Тогда $\frac{(2a+b)^2}{4} + \frac{23b^2}{4} = 2$ и $(2a+b)^2 + 23b^2 = 8$ – не существует таких $a, b \in \mathbb{Z} \Rightarrow \mathfrak{p}_2$ не эквивалентен O_K.
$\mathfrak{p}_2\mathfrak{p}_2' \sim O_K$.
Аналогично, $\mathfrak{p}_2', \mathfrak{p}_3, \mathfrak{p}_3'$ не эквивалентны O_K.
Рассмотрим $\mathfrak{p}_2^2 = (\alpha)$, $\alpha = a + b\frac{1+\sqrt{-23}}{2}$.
$N(\mathfrak{p}_2^2) = 4 = \frac{(2a+b)^2}{4} + \frac{23b^2}{4} \Rightarrow (2a+b)^2 + 23b^2 = 16 \Rightarrow b = 0, a = \pm 2$.
Таким образом, $\mathfrak{p}_2^2 = (2) = \mathfrak{p}_2\mathfrak{p}_2' \Rightarrow \mathfrak{p}_2 = \mathfrak{p}_2'$ – противоречие – значит, $\mathfrak{p}_2^2 \not\sim O_K$.
Рассмотрим $\mathfrak{p}_2^3$. Пусть $\frac{1+\sqrt{-23}}{2} = \theta$. Тогда

$$\mathfrak{p}_2^3 = (2,\theta)(2,\theta)(2,\theta) = (4, 2\theta, \theta^2)(2,\theta) = (4, 2\theta, \theta - 6)(2,\theta) = (4, 2\theta, \theta - 2)(2,\theta) =$$

$$(4, 4, \theta - 2)(2,\theta) = (8, 4\theta, 2\theta - 4) = (8, 8\sqrt{-23}) = 8(1, \sqrt{-23}) = 8O_K.$$

Получается, $\mathfrak{p}_2^3 \sim O_K \Rightarrow ord(\mathfrak{p}_2) = 3$.
$\mathfrak{p}_2\mathfrak{p}_2' = (2) \sim O_K$, тогда $\mathfrak{p}_2' \sim \mathfrak{p}_2^{-1} = \mathfrak{p}_2^2$.
Рассмотрим $\mathfrak{p}_2\mathfrak{p}_3 = (2,\theta)(3,\theta) = (6, 2\theta, 3\theta, \theta - 6) = (6, 2\theta, 3\theta, \theta) = (\theta - \theta^2, \theta) = \theta(1 - \theta, 1) \sim O_K$.
$\mathfrak{p}_3\mathfrak{p}_3' = O_K \Rightarrow \mathfrak{p}_3' \sim \mathfrak{p}_3^{-1} \sim \mathfrak{p}_2$. Следовательно, $Cl_K = \{[O_K], [\mathfrak{p}_2], [\mathfrak{p}_2^2]\}$.

8 Единицы (units)

Пусть R – кольцо в K, R^* – группа обратимых элементов (группа единиц числового поля). Рассмотрим $K^* = \{a \in K \mid a \neq 0\}$. Тогда $K^* = K\{0\}$.

Отметим, что $\mathbb{Z}* = \{\pm 1\}$ и будем обозначать $O_K* = U(K)$.

Предложение 1. Пусть K – числовое поле. Тогда $U(K) = \{\alpha \in O_K \mid N(\alpha) = \pm 1\}$.

Теорема 1. *Пусть $K = \mathbb{Q}(\sqrt{-d})$, d свободно от квадратов и $d > 0$. Тогда*

1. *Если $d = 1$ $(K = \mathbb{Q}(i)) \Rightarrow U(K) = \{\pm 1, \pm i\}$.*
2. *Если $d = 3$ $(K = \mathbb{Q}(\sqrt{-3})) \Rightarrow U(K) = \{\pm 1, \pm\zeta, \pm\zeta^2\}$, где $\zeta = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$.*
3. *Во всех других случаях $U(K) = \{\pm 1\}$.*

Определение 1. Определим $\eta(K) = \{\epsilon \in U(K) \mid ord(\epsilon) < \infty\}$ – группа кручения единиц числового поля. Отметим, что $\eta(K) = \langle\zeta\rangle$ – циклическая, где ζ – корень из единицы.

Если K имеет, как минимум, одно действительное вложение $\sigma : K \hookrightarrow \mathbb{R}$, тогда $\eta(K) = \{\pm 1\}$.

Теорема 2. ***(Дирихле о единицах)*** *Пусть K – числовое поле, (r, s) – подпись K, $t = r+s-1$. Тогда $U(K)$ – конечно порождённая группа ранга t. Кроме того, $\exists \epsilon_1, ..., \epsilon_t \in U(K)$, такие, что $\forall \epsilon \in U(K)$ однозначно представляется в виде: $\epsilon = \omega \cdot \epsilon_1^{n_1} \cdot \epsilon_1^{n_t}$, где $\omega \in \eta(K), n_i \in \mathbb{Z}$.*

Пример 4. Рассмотрим $K = \mathbb{Q}(\sqrt{2})$.
$1 + \sqrt{2}$ – единица в $\mathbb{Z}[\sqrt{2}]$. Следовательно, $1 + \sqrt{2} \in U(K)$.
$U(K) = \{\pm(1 + \sqrt{2})^m \mid m \in \mathbb{Z}\}$, $(r, s) = (2, 0) \Rightarrow t = 1$.
$1 + \sqrt{2} \in O_K = \mathbb{Z}[\sqrt{2}]$.
$N(1 + \sqrt{2}) = -1$ (из произведения сопряжённых).
$1 + \sqrt{2} = \pm\epsilon^n$, $\epsilon = a + b\sqrt{2}$. Тогда $1 + \sqrt{2} = \pm(a + b\sqrt{2})^n$. Рассмотрим $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{R}$. Таким образом, для $u, v \in \mathbb{Q}$.

- $\sigma_1(u + v\sqrt{2}) = u + v\sqrt{2}$.
- $\sigma_2(u + v\sqrt{2}) = u - v\sqrt{2}$

Имеем $1-\sqrt{2} = \pm(a-b\sqrt{2})^n$, тогда $|a+b\sqrt{2}| \leq |1+\sqrt{2}|^{\frac{1}{n}}$ и $|a-b\sqrt{2}| \leq |1-\sqrt{2}|^{\frac{1}{n}}$.
По неравенству треугольника:
$|b| \leq \frac{1}{2\sqrt{2}} \left(|1 + \sqrt{2}|^{\frac{1}{n}} + |1 - \sqrt{2}|^{\frac{1}{n}}\right)$, где $|1 + \sqrt{2}| \approx 2.4$ и $|1 - \sqrt{2}| \approx 0.4$.
Пусть $n \geq 2$, тогда $|1 + \sqrt{2}|^{\frac{1}{n}} \leq |1 + \sqrt{2}|^{\frac{1}{2}} \leq \sqrt{2.5} \leq 1.6$.
Аналогично, $|1 - \sqrt{2}|^{\frac{1}{n}} \leq 1$. Таким образом, $|b| \leq \frac{1.6+1}{2\sqrt{2}} < 1 \Rightarrow b = 0$.
Получаем противоречие, что $N(\epsilon) = a^2 - 2b^2 = \pm 1 \Rightarrow a = \pm 1 \Rightarrow \epsilon = a = \pm 1$.
Значит, $n < 2 \Rightarrow n = 1$.