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

Лекция №7

3 Алгебраические целые числа

3.3 Целый базис

Обозначим O_K^+ – аддитивная абелева группа.

Пример 2. Рассмотрим $\mathbb{Z}[i]$ – гауссовы целые числа. Тогда $\mathbb{Z}[i]^+ = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot i \cong \mathbb{Z}^2$.

Определение 3. Целым базисом числового поля K называется множество элементов $\xi_1, ..., \xi_n \in O_K$, которое является $\mathbb{Z}$-базисом кольца O_K.

Для любого $\alpha \in O_K$ справедливо $\alpha = m_1\xi_1 + ... + m_n\xi_n$, $m_i \in \mathbb{Z}$. Тогда $O_K^+ = \mathbb{Z}\cdot\xi_1 \oplus \mathbb{Z}\cdot\xi_2 \oplus ... \oplus \mathbb{Z}\cdot\xi_n$.

Теорема 3. *Пусть G – конечно порождённая аддитивная абелева группа. Тогда существует $r \geq 0, r \in \mathbb{Z}$ (ранг) и положительные целые $d_1|d_2|...|d_k$, такие, что*

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/_{d_1\mathbb{Z}} \oplus ... \oplus \mathbb{Z}/d_k\mathbb{Z}.$$

Группа G является свободной от кручения группой, если в ней существует единственный элемент конечного порядка 0.

Пример 3. Рассмотрим $\mathbb{C}$ как аддитивную абелеву группу, G – подгруппа в $\mathbb{C}$. Если $\alpha \in G$ и $\mathrm{ord}(\alpha) < \infty$, тогда существует $n = \mathrm{ord}(\alpha) | n\cdot\alpha = 0$, $n \geq 1$. Соответственно, $\alpha = 0$.

Следствие 2. *Пусть G – конечно порождённая аддитивная абелева группа, свободная от кручения. Тогда существует $r \geq 0$ – целое, такое, что $G \cong \mathbb{Z}^r$.*

Лемма 8. *Пусть K – числовое поле. Если O_K^+ – конечно порождена, то O_K^+ имеет целый базис.*

Лемма 9. *Пусть K – числовое поле степени n, H – конечно порождённая подгруппа в O_K^+ ранга m. Тогда $m \leq n$.*

Пример 4. Рассмотрим $K = \mathbb{Q}(i)$ с базисом $\{1, i\}$. Тогда $rank(O_K^+) = 2$.

3.4 Целые в квадратичных полях

Лемма 10. *Пусть $d \neq 0; 1$ свободно от квадратов, $\mu \neq 0 \in \mathbb{Q} \mid \mu^2 d \in \mathbb{Z}$. Тогда $\mu \in \mathbb{Z}$.*

Лемма 11. *Пусть $d \neq 0; 1$ свободно от квадратов. Элемент $\frac{1+\sqrt{d}}{2}$ является алгебраическим целым тогда и только тогда, когда $d \equiv 1 (\mod 4)$.*

Лемма 12. *Пусть $K = \mathbb{Q}(\sqrt{d})$.*
1. Если $d \not\equiv 1 (\mod 4)$, то $1, \sqrt{d}$ – целый базис O_K и $O_K = \mathbb{Z}[\sqrt{d}]$. 2. Если $d \equiv 1 (\mod 4)$, то $1, \frac{1+\sqrt{d}}{2}$ – целый базис O_K, и $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Замечание 1. 1. Если $d \not\equiv 1 (\mod 4)$, то $O_K = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

2. Если $d \equiv 1 (\mod 4)$, то $O_K = \{a+b\sqrt{d} \mid \} \cup \{\frac{r}{2} + \frac{s}{2}\sqrt{d} \mid r, s$– нечётные целые$\}$.

3.5 Целые в квадратичных полях

Лемма 13. *Пусть K – числовое поле степени n, H – конечно порождённая подгруппа в O_K^+ ранга n. Пусть также $\{\omega_1, ..., \omega_n\}$ и $\{\eta_1, ..., \eta_n\}$ – базисы H. Тогда их дискриминанты будут совпадать:*

$$\Delta(\omega_1, ..., \omega_n) = \Delta(\eta_1, ...\eta_n) = \Delta(H).$$

Лемма 14. *Пусть K – числовое поле степени n, H – конечно порождённая подгруппа в O_K^+ ранга n. Тогда $|\Delta(H)| \in \mathbb{Z}^{r \geq 0}$.*

Отметим, если G – конечно порождённая подгруппа в O_K^+ и $H \subseteq G$, тогда $\Delta(H) = (G : H)^2 \Delta(G)$.

3.6 Существование целого базиса

Теорема 4. *Пусть K – числовое поле степени n. Тогда O_K имеет целый базис ранга n:*

$$O_K^+ = \mathbb{Z} \cdot \omega_1 \oplus ... \oplus \mathbb{Z} \cdot \omega_n.$$

Определение 4. Дискриминантом δ_K числового поля K называется дискриминант целого базиса кольца O_K.

3.7 Алгоритм вычисления целого базиса

Лемма 15. *Пусть K – числовое поле степени n, $\omega_1, ..., \omega_n \in O_K$ – линейно независимые, но не являются $\mathbb{Z}$-базисом. Тогда существует простое p, такое, что $p^2 | \Delta(\omega_1, ..., \omega_n \in O_K)$, и существует $u_i \in \mathbb{Q}, 0 \leq u_i < p$ (не все u_i равны 0), такие, что*

$$\frac{u_1\omega_1 + ... + u_n\omega_n}{p} \in O_K.$$

Кроме того, если $\eta_1, ..., \eta_n$ *– базис подгруппы, порождённой* $\omega_1, ..., \omega_n$ *и* $\frac{u_1\omega_1+...+u_n\omega_n}{p}$, *то* $\Delta(\eta_1, ..., \eta_n) = \frac{1}{p^2}\Delta(\omega_1, ..., \omega_n)$.

Пример 5. 1. Пусть θ – корень $X^3 + X + 1$. Вычислим целый базис для $K = \mathbb{Q}(\theta)$.

$$\begin{cases} 1, \theta, \theta^2 \in O_K \\ \Delta(1, \theta, \theta^2) = -31 \end{cases} \Rightarrow \tag{1}$$

$\Rightarrow 1, \theta, \theta^2$ – целый базис для O_K.

2. Пусть теперь θ – корень многочлена $X^3 + X^2 - 2X + 8$. Вычислим целый базис для $K = \mathbb{Q}(\theta)$.
$1, \theta, \theta^2$ – базис $K/\mathbb{Q}$.
$\Delta(1, \theta, \theta^2) = -2012 = 2^2503 \Rightarrow 1, \theta, \theta^2$ не является целым базисом.
Пусть G – конечно порождённая подгруппа в O_K^+.
$\Delta(1, \theta, \theta^2) = (O_K^+ : G)^2\Delta(G)$. Индекс G в O_K^+ равен 2.
Существуют u_i, такие, что $0 \leq u_i < 1$ и $\beta = \frac{u_0+u_1\theta+u_2\theta^2}{2} \in O_K$.
Претенденты на добавление к базису:

$$\frac{1}{2}, \frac{1+\theta}{2}, \frac{1+\theta^2}{2}, \frac{\theta}{2}, \frac{\theta+\theta^2}{2}, \frac{1+\theta+\theta^2}{2}.$$

Сразу исключаем некоторые не алгебраические целые, остаются элементы:

$$\frac{1+\theta}{2}, \frac{1+\theta^2}{2}, \frac{\theta+\theta^2}{2}.$$

$$(u_0, u_1, u_2) = \begin{bmatrix} (1,1,0) \\ (1,0,1) \\ (0,1,1) \end{bmatrix}$$

$M_\beta = \frac{u_0}{2}I_3 + \frac{u_1}{2}M_\theta + \frac{u_2}{2}M_{\theta^2}$.

- $N(\frac{1+\theta}{2}) = -1.25 \notin \mathbb{Z} \Rightarrow \frac{1+\theta}{2} \notin O_K$.
- $N(\frac{1+\theta^2}{2}) = 7.25 \notin \mathbb{Z} \Rightarrow \frac{1+\theta^2}{2} \notin O_K$.
- $N(\frac{\theta+\theta^2}{2}) = 10 \in \mathbb{Z} \Rightarrow \frac{\theta+\theta^2}{2} \in O_K$.

Таким образом, $\beta = \frac{\theta+\theta^2}{2}, \chi_\beta(X) = X^3 - 2X^2 + 3X - 10$.
$1, \theta, \theta^2, \beta$ – элементы, порождающие целый базис.
Поскольку $\theta^2 = 2\beta - \theta \Rightarrow 1, \theta, \beta = \frac{\theta+\theta^2}{2}$ – это целый базис K.