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

Лекция №6

2 Вложения числового поля

2.9 Дискриминанты и базисы

Лемма 1. *Если $\omega_1, ..., \omega_n$ линейно зависимы над $\mathbb{Q}$, то*

$$D(\omega_1, ..., \omega_n) = \Delta(\omega_1, ..., \omega_n) = 0.$$

Кроме того, $\omega_1, ..., \omega_n$ является базисом $K/\mathbb{Q}$ тогда и только тогда, когда $\Delta(\omega_1, ..., \omega_n) \neq 0$.

Лемма 2. *Пусть $c_{ij} \in \mathbb{Q}$, $\beta_i = \sum_{j=1}^{n} c_{ij}\omega_j$. Тогда*

$$D(\beta_1, ..., \beta_n) = det(c_{ij}) \cdot D(\omega_1, ..., \omega_n).$$

Теорема 1. *Пусть K – числовое поле степени n. Тогда*

1. *$K = \mathbb{Q}(\alpha)$, $D(1, \alpha, \alpha^2, ..., \alpha^{n-1}) = \prod_{1\leq i\leq j\leq n}(\alpha_i - \alpha_j)^2$, где α_i, α_j – элементы, сопряжённые с α.*
2. *$\beta_1; ...; \beta_n \in K \Rightarrow$ образуют базис над $\mathbb{Q}$ тогда и только тогда, когда $\Delta(\beta_1, ..., \beta_n) \neq 0$.*

3 Алгебраические целые числа

3.1 Основные определения

$\overline{\mathbb{Q}}$ – множество алгебраических чисел.

Определение 1. $\alpha \in \overline{\mathbb{Q}}$ называется алгебраическим целым, если является корнем унитарного многочлена с целыми коэффициентами.

Обозначим O – множество всех алгебраических целых.

Пример 1. 1. $i \in O$, т.к. $\mu_i(X) = X^2 + 1$.

2. $\alpha = \frac{1+\sqrt{5}}{2} \in O$, т.к. $\mu_\alpha(X) = X^2 - X + 1$.

3. $\alpha = \frac{1}{\sqrt{2}} \notin O$, т.к. $\mu_\alpha(X) = X^2 - \frac{1}{2} \notin \mathbb{Z}[X]$.

Лемма 3. ***(Гаусса)*** *Пусть $f \in \mathbb{Z}$ – унитарный; $g, h \in \mathbb{Q}[X]$ / $f = gh$. Тогда $\exists \lambda \in \mathbb{Q}$ / $G = \lambda g$, $H = \lambda^{-1} h \in \mathbb{Z}[X]$.*

Лемма 4. *Пусть α – алгебраический элемент. Тогда α будет алгебраическим целым тогда и только тогда, когда $\mu_{\mathbb{Q},\alpha} \in \mathbb{Z}[X]$.*

Следствие 1. *Пусть K – числовое поле. $\alpha \in K$ – алгебраическое целое тогда и только тогда, когда выполняется одно из следующих условий:*

1. *α – корень унитарного многочлена $f \in \mathbb{Z}[X]$.*

2. *$\mu_{\mathbb{Q},\alpha}(X) \in \mathbb{Z}[X]$.*

3. *Характеристический многочлен α имеет целые коэффициенты.*

Определение 2. Пусть K – числовое поле. Кольцо $O_K = K \cap O$ называется кольцом целых поля K. При этом $O_{\mathbb{Q}} = Z$ является множеством рациональных целых чисел и $Z \subseteq O_K$.

Предложение 1. Пусть K – числовое поле, $\alpha \in K \Rightarrow \exists$ рациональное целое $m \geq 1 \mid m \cdot \alpha \in O_K$.

3.2 Кольцо целых

Лемма 5. *Пусть α – алгебраическое целое степени d. Тогда для $\forall j > 0 : \alpha^j$ может быть записано как линейная комбинация $1, \alpha, ..., \alpha^{d-1}$ над Z.*

Лемма 6. *Если $\alpha_1, ..., \alpha_n$ – алгебраические целые, то $Z[\alpha_1, ..., \alpha_n]$ конечно порождено как аддитивная абелева группа.*

Лемма 7. *Пусть H – нетривиальная конечно порождённая аддитивная подгруппа в поле $\mathbb{C}$ и $\theta \in \mathbb{C}$, $\theta \cdot H \subseteq H$, тогда θ – алгебраическое целое.*

Теорема 2. *O и O_K – кольца.*