БФУ им. И. Канта – Методы алгебраической теории чисел в криптографии.
Е.Малыгина (2020 – Осенний семестр)

Лекция №3 (21.09.20)

---

1. Алгебраические числовые поля.

1.6. Примитивные элементы.

Пример 1. *Рассмотрим* $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$. *Роль примитивного элемента в этом случае играет* $\sqrt{2} + i$.

Теорема 1 (Теорема о примитивном элементе)**.** *Для каждого числового поля* K *существует такой элемент* $\alpha \in K$, *что* $K = \mathbb{Q}(\alpha)$. *В этом случае* α *называется примитивным элементом поля* K.

Лемма 1. *Пусть* K *– числовое поле,* α *– примитивный элемент числового поля* K. *Если тождественное вложение поля* K *в* $\mathbb{C}$ *является единственным вложением* φ, *таким, что* $\varphi(\alpha) = \alpha$, *то* α *– примитивный элемент поля* K.

1.7. Нормы и следы.

Пусть как и ранее K – числовое поле, α – элемент поля K и $m_\alpha : K \to K$.

Определение 1. *След и норму элемента* α *определим через соответствующий линейный оператор* m_α*:*

$$Tr_{K/\mathbb{Q}}(\alpha) = Tr(m_\alpha) \in \mathbb{Q},$$

$$N_{K/\mathbb{Q}} = disc(m_\alpha) \in \mathbb{Q}.$$

Пример 2. *1). Рассмотрим $K = \mathbb{Q}(\sqrt{\alpha})$ и вычислим след и норму элемента $\alpha = a + b\sqrt{\alpha}$.*

Действие линейного оператора на базисные элементы:

$$m_\alpha(1) = a + b\sqrt{\alpha},$$

$$m_\alpha(\sqrt{\alpha}) = b\alpha + a\sqrt{\alpha},$$

соответственно, $M = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$. *Имеем*

$$Tr_{K/\mathbb{Q}}(\alpha) = 2a \text{ (сумма элементов главной диагонали)},$$

$$N_{K/\mathbb{Q}}(\alpha) = a^2 - b^2 d \text{ (дискриминант)}.$$

2). Рассмотрим $K = \mathbb{Q}(\theta)$, где θ – корень многочлена $X^3 + X + 1$. При этом $1, \theta, \theta^2$ – базис K над $\mathbb{Q}$. Найдем след и норму элемента $\alpha = 1 + 3\theta^2$. Матрица линейного оператора имеет вид:

$$M = \begin{pmatrix} 1 & -3 & 0 \\ 0 & -2 & -3 \\ 3 & 0 & -2 \end{pmatrix},$$

тогда $Tr(\alpha) = -3$, $N(\alpha) = 4 + 3(+9) = 31$.

Предложение 2. *Пусть K – числовое поле, $\alpha, \beta \in K$. Тогда*

$$Tr_{K/\mathbb{Q}}(\alpha + \beta) = Tr_{K/\mathbb{Q}}(\alpha) + Tr_{K/\mathbb{Q}}(\beta),$$

$$N_{K/\mathbb{Q}}(\alpha \cdot \beta) = N_{K/\mathbb{Q}}(\alpha) \cdot N_{K/\mathbb{Q}}(\beta).$$

Теорема 3. *Пусть $\varphi_1, ..., \varphi_d$ – вложения $K \hookrightarrow \mathbb{C}$, $\alpha \in K$. Характеристический многочлен оператора m_α имеет вид $\prod_{i=1}^{d}(X - \varphi_i(\alpha))$. Тогда*

$$Tr_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^{d} \varphi_i(\alpha),$$

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{d} \varphi_i(\alpha).$$