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

Лекция №2 (14.09.20)

---

1. Алгебраические числовые поля.

1.2. Алгебраические числа и числовые поля.

Определение 1. *Алгебраическим числом называется число α, такое, что α – алгебраическое над $\mathbb{Q}$. Другими словами, существует ненулевой многочлен $g \in \mathbb{Q}[X]$, такой что $g(\alpha) = 0$.*

Пример 1. $x \in \mathbb{Q}$, $1 + i$, $\sqrt{3}i$ *– алгебраические числа.*

Определение 2. *Алгебраическим числовым полем (числовым полем) называется подполе поля $\mathbb{C}$, которое конечно, как расширение поля $\mathbb{Q}$. Кроме того, $\alpha \in \mathbb{C}$ - алгебраический $\Leftrightarrow \mathbb{Q}(\alpha)$ – числовое поле.*

Пример 2. *Пусть α свободно от квадратов. Рассмотрим квадратичное поле $\mathbb{Q}(\sqrt{\alpha}) = \{a+b\sqrt{\alpha} | a, b \in \mathbb{Q}\}$. Степень расширения данного поля равна $[\mathbb{Q}(\sqrt{(\alpha)}) : \mathbb{Q}] = 2$.*

Отметим, что $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{8})) = \mathbb{Q}(\sqrt{18})$.

Предложение 1. *Числовое поле K, такое, что $[K : \mathbb{Q}] = 2$, имеет вид $K = \mathbb{Q}(\sqrt{d})$ для единственного свободного от квадратов целого $d \neq 1$.*

1.3. Расширение числовых полей.

Предложение 2. *Пусть K – числовое поле, $\alpha \in \mathbb{C}$ – алгебраический над полем K. Тогда $K(\alpha)$ – числовое поле.*

Обозначим L/K – расширение полей. Рассмотрим конечное множество $S = \{a_1, ..., a_n\} \subset L$, тогда $K(S) = K(a_1, ..., a_n)$ – наименьшее расширение поля K, лежащее в L и содержащее S.

Пример 3. *Рассмотрим* $K/\mathbb{Q} \subset \mathbb{Q}(i, \sqrt{2}) \subset \mathbb{C}$. *Здесь* $S = \{i, \sqrt{2}\}$.

Следствие 1. *Пусть S – конечное множество алгебраических чисел. Если мы расширим с помощью этих чисел поле $\mathbb{Q}$, то $\mathbb{Q}(S)$ – числовое поле.*

Теорема 3. *Множество всех алгебраических чисел – поле.*

1.4. Числовые поля и матрицы.

Пусть K – числовое поле, $\alpha \in K$. Ассоциируем α с некоторым линейным оператором $m_\alpha : K \to K$.

Пример 4. *Пусть $K = \mathbb{Q}(\sqrt{d})$ – квадратичное поле, тогда $1, \sqrt{d}$ – базис K над $\mathbb{Q}$. Если $\alpha \in K$, то $\alpha = a \cdot 1 + i\sqrt{d}$. При этом*

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

$$m_\alpha(\sqrt{d}) = \sqrt{d}\alpha = bd \cdot 1 + \alpha \cdot \sqrt{d}.$$

Матрицей, соответствующей действию оператора m_α, является $\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$.

Предложение 4. *Пусть – числовое поле. Тогда:*

1. *$\alpha \to m_\alpha$ – инъективно и линейно над $\mathbb{Q}$; также его можно рассматривать как гомоморфизм, действующий из K в кольцо $\mathbb{Q}$-линейных операторов над K.*

2. *Если g – характеристический многочлен оператора m_α, то $g(\alpha) = 0$.*

Пример 5. *Пусть $K = \mathbb{Q}(\theta)$ и θ – единственный действительный корень многочлена $f(X) = X^3 + X + 1$. Тогда $[K : \mathbb{Q}] = 3$, а значит, $1, \theta, \theta^2$ – базис K над $\mathbb{Q}$.*

Рассмотрим произвольный элемент α поля K, такой, что $\alpha = 1+3\theta^2$. Тогда

$$m_\alpha(1) = 1 + 3\theta^2,$$

$$m_\alpha(\theta) = \theta + 3\theta^3 = \theta + 3(-\theta - 1) = -2\theta - 3,$$

$$m_\alpha(\theta^2) = -2\theta^2 - 3\theta.$$

Соответственно, матрица линейного оператора имеет вид: $M = \begin{pmatrix} 1 & -3 & 0 \\ 0 & -2 & -3 \\ 3 & 0 & -2 \end{pmatrix}$

1.5. Вложения.

Определение 3. *Вложением числового поля K называется гомоморфизм колец, действующий из K в $\mathbb{C}$, обозначается $K \hookrightarrow \mathbb{C}$.*

Пример 6. *Рассмотрим автоморфизмы $\mathbb{Q}(\sqrt{3}) \to \mathbb{C}$. Элементы в $\mathbb{Q}(\sqrt{3})$ имеют вид $a + b\sqrt{3}$. Тогда*

$$\varphi_1(a + b\sqrt{3}) = a - b\sqrt{3},$$

$$\varphi_2(a + b\sqrt{3}) = a - b\sqrt{3}.$$

То есть каждый элемент переходит в корень его минимального многочлена.

Замечание 1. *Если L/K – расширение полей, то любое вложение поля $L \hookrightarrow \mathbb{C}$ можно сузить на вложение $K \hookrightarrow \mathbb{C}$.*

Пример 7. *Рассмотрим $K = \mathbb{Q}(\sqrt{2})$ и $\varphi : K \hookrightarrow \mathbb{C}$, $a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Рассмотрим расширение $L = \mathbb{Q}(\sqrt{2}, i)$ поля K. Базис L над $\mathbb{Q}$ есть $1, \sqrt{2}, i, i\sqrt{2}$.*

Пусть $\alpha \in L$, тогда $\alpha = a + b\sqrt{2} + ci + di\sqrt{2}$, где $a, b, c, d \in \mathbb{Q}$. Вложения Φ_1 и Φ_2 поля L можно сузить до вложения φ поля K:

$$\Phi_1(a+b\sqrt{2}+ci+di\sqrt{2}) = \Phi_1((a+ci)+(b+di)\sqrt{2}) = a+ci-(b+di)\sqrt{2} = a-b\sqrt{2}+ci-di\sqrt{2}.$$

Вложение Φ_2 определить самостоятельно.

Лемма 1. *Пусть K – числовое поле, $f \in K[X]$ – неприводимый многочлен и $deg(f) = d \geq 1$. Пусть φ – вложение поля K. Обозначим $\varphi(f) \in \mathbb{C}[X]$ – многочлен, полученный применением φ к коэффициентам f. Тогда $\varphi(f)$ имеет d-рациональных корней в $\mathbb{C}$.*

Предложение 5.

1. *Пусть L/K – расширение числовых полей. Для любого вложения $\varphi : K \hookrightarrow \mathbb{C}$ существует в точности $[L : K]$ рациональных вложений поля L, продолжающих φ.*

2. *Любое числовое поле K имеет $[K : \mathbb{Q}]$ вложений.*

Определение 4. *Пусть α – алгебраическое число, f_α – его минимальный многочлен. Корни f_α, лежащие в $\mathbb{C}$, называются сопряженными к α. Если $\varphi_1, ..., \varphi_d$ – вложения $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$, то сопряженные к α есть $\alpha_1 = \varphi_1(\alpha), ..., \alpha_d = \varphi_d(\alpha)$.*

Пример 8. $K = \mathbb{Q}(\sqrt{2}+\sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. *Тогда* $[K : \mathbb{Q}] = 4$. *Рассмотрим* $\alpha = \sqrt{2}+\sqrt{5}$. *Сопряженными к α являются элементы* $\sqrt{2}-\sqrt{5}$, $-\sqrt{2}+\sqrt{5}$, $-\sqrt{2} - \sqrt{5}$. *Тогда минимальный многочлен элемента α равен* $f_\alpha = (X - (\sqrt{2} + \sqrt{5})) \cdot (X - (\sqrt{2} - \sqrt{5})) \cdot (X - (-\sqrt{2} + \sqrt{5})) \cdot \ldots \cdot (X - (-\sqrt{2} - \sqrt{5})) = X^4 - 14X^2 + 9$.