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

Лекция №1

1 Числовые поля

1.1 Расширения полей, алгебраические числа

Определение 1. Пусть L и K – поля. Тогда L/K называется расширением полей, если K – подполе в L.

Определение 2. Пусть L/K – расширение полей, $\alpha \in L$. Элемент α называется алгебраическим над полем K, если $\exists\, g \in K[X], g \neq 0$, такой, что $g(\alpha) = 0$.

Пример 1. Рассмотрим $\mathbb{C}/\mathbb{Q}$, i – мнимая единица. Элемент i – алгебраический над $\mathbb{Q}$, так как он является корнем многочлена $g(X) = X^2 + 1 \in \mathbb{Q}[X]$.

Теорема 1. *Пусть α – алгебраический элемент над полем K. Тогда*

1. *$\exists\,!\ \mu_{K,\alpha}(X) \in K[X]$ такой, что $\mu_{K,\alpha}(\alpha) = 0$ и $\mu_{K,\alpha}$ – неприводимый и унитарный. В этом случае $\mu_{K,\alpha}$ называется минимальным многочленом элемента α.*
2. *Если найдётся $f \in K[X]$ такой, что $f(\alpha) = 0$, то $\mu_{K,\alpha} | f$.*

Пример 2. $K = \mathbb{Q}(\sqrt{2}), L = \mathbb{Q}(i + \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$. Рассмотрим $\alpha = i + \sqrt{2}$. Тогда $\mu_{L,\alpha}(X) = X - \alpha$. Найдём $\mu_{K,\alpha}(X)$. Преобразовав выражение $\alpha = i + \sqrt{2}$, получим $\alpha^2 - 2\alpha\sqrt{2} + 3 = 0$. Следовательно, α является корнем многочлена $X^2 - 2\sqrt{2}X + 3 \in K[X]$. Вторым корнем является сопряжённый к α, то есть $\overline{\alpha} = \sqrt{2} - i$. Таким образом, данный многочлен неприводим над полем $K[X]$.

Определение 3. Пусть L/K – расширение полей, $\alpha \in L$ – алгебраический элемент над K. Тогда степенью элемента α называется степень многочлена $\mu_{K,\alpha}$.

Пример 3. Степень $\sqrt{2}$ над $\mathbb{Q}$ равна 2, так как $\mu_{\mathbb{Q},\sqrt{2}}(X) = X^2 - 2$.

Определение 4. $\alpha \in \mathbb{C}$ называется алгебраическим числом, если α – алгебраический элемент над $\mathbb{Q}$.

1.2 Порождённые поля

Определение 5. Пусть L/K – расширение полей, $S \subset L$ – подмножество. Расширение поля K, порождённое множеством S, – это пересечение всех подполей в L, содержащих одновременно K и S.

Порождённое расширение обычно записывается как $K(S)$. Если $S = \{s_1, ..., s_n\}$, то $K(s_1, ..., s_n)$.

Лемма 1. *$K(S)$ – подполе поля L. Это наименьшее подполе, содержащее и K, и S.*

Пример 4.

- $\mathbb{R}(i) = \mathbb{C}$.
- Пусть $d \in \mathbb{Q}$, причём d не является квадратом какого-либо числа, и

$$K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}.$$

По критерию подполя K является подполем в $\mathbb{C}$. Далее пусть $L \neq K$. Мы имеем $\mathbb{Q} \subset L, \sqrt{d} \in L$. Из того, что $a, b \in \mathbb{Q}$ (по условию) и $\sqrt{d} \in L$ (по предложению) следует, что $a + b\sqrt{d} \in L$. Окончательно заключаем, что $K \subseteq L$.

1.3 Алгебраические и конечные расширения

Определение 6. Пусть L/K – расширение полей. Это расширение называется алгебраическим, если $\forall\ \alpha \in L$ является алгебраическим над K.

Если L/K – расширение полей, то L – векторное пространство над K.

Определение 7. $[L : K] = \dim_K L$ – степень расширения L/K. Если $[L : K] < \infty$, то L/K называется конечным расширением.

Пример 5.

- Базис расширения $\mathbb{C} = \mathbb{R}(i)$ состоит из двух элементов: $\{1, i\}$. Следовательно, $[\mathbb{C} : \mathbb{R}] = 2$.
- $[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] = 2$, так как базис расширения $\mathbb{Q}(\sqrt{\alpha})$ состоит из двух элементов: $1, \sqrt{\alpha}$.

Теорема 2. *Пусть L/K – конечное расширение полей. Тогда L/K алгебраическое расширение.*

1.4 Простые расширения

Определение 8. Расширение вида $K(\alpha)/K$ называется простым.

Теорема 3. *Пусть L/K – расширение полей, $\alpha \in L$ – алгебраический над K, $\mu_{K,\alpha}$ – минимальный многочлен элемента α, $n = \deg(\mu_\alpha)$. Тогда*

1. $K(\alpha) \cong K[X]/(\mu_\alpha)$.

2. $\{1, \alpha, ..., \alpha^{n-1}\}$ *– базис* $K(\alpha)$ *над* K *и* $[K(\alpha) : K] = deg(\mu_\alpha)$.

Пример 6. Рассмотрим поле $\mathbb{Q}(\sqrt[3]{d}) = \{a + b\sqrt[3]{d} + c(\sqrt[3]{d})^2 | a, b, c \in \mathbb{Q}\}, \alpha = \sqrt[3]{d}$. Минимальный многочлен элемента α равен $\mu_\alpha = X^3 - d$. Так как $\deg(\mu_\alpha) = 3$, базис $\mathbb{Q}(\sqrt[3]{d})/\mathbb{Q}$ состоит из трех элементов: $\{1, \sqrt[3]{d}, (\sqrt[3]{d})^2\}$.