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

Лекция №2

1 Числовые поля

1.5 Числовые поля

Определение 9. Числовое поле – это конечное расширение поля $\mathbb{Q}$.

Пример 7. 1. $\mathbb{Q}$ – числовое поле со степенью расширения 1.

2. Пусть $d \in \mathbb{Q}, d \neq 0, 1$ – не квадрат, тогда $\mathbb{Q}(\sqrt{d})$ – числовое поле со степенью расширения 2.

3. Если $d_1, ..., d_m$ – алгебраические числа, то $\mathbb{Q}(d_1, ..., d_m)$ – числовое поле.

Следствие 1. *Если K – числовое поле, то любой $\alpha \in K$ является алгебраическим.*

1.6 Башни полей

Теорема 4. *Пусть $K \subseteq L \subseteq M$ – конечные расширения полей, $l_1, ..., l_r$ – базис L/K, $m_1, ..., m_s$ – базис M/L. Тогда $\{l_i m_j; i = \overline{1, r}, j = \overline{1, s}\}$ – базис M/K. Кроме того, $[M : K] = [L : K][M : L]$.*

1.7 Примеры числовых полей

Лемма 2. *Пусть K – квадратичное поле. Тогда $K = \mathbb{Q}(\sqrt{d})$, где $d \neq 0; 1$ и свободно от квадратов.*

Пример 8. 1. $\mathbb{Q}(\sqrt{-\frac{1}{3}}) = \mathbb{Q}(\sqrt{-12}) = \mathbb{Q}(\sqrt{-3})$.

2. Кубические корни из единицы: $1, \zeta, \zeta^2; \zeta = e^{\frac{2\pi i}{3}}$. Так как $1+\zeta+\zeta^2 = 0 \Rightarrow \zeta$ – корень многочлена $X^2 + X + 1 \Rightarrow \zeta$ – алгебраическое число $\Rightarrow$ $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2 \Rightarrow \mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{d})$ – квадратичное поле.

Определение 10. Пусть n – положительное целое число, $\zeta_n = e^{\frac{2\pi i}{n}}$. Тогда $\mathbb{Q}(\zeta_n)$ – n-е круговое (циклотомическое) поле.

Замечание 1. В общем случае $\mathbb{Q}(\sqrt[3]{d})$ не всегда является кубическим полем.

1.8 Пример $\mathbb{Q}(\sqrt{5}, \sqrt{6})$

Рассмотрим башню полей $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\sqrt{5}, \sqrt{6})$. Степень расширения для первого вложения равна 2, равно как и для второго $\Rightarrow$ по теореме 4 $[\mathbb{Q}(\sqrt{5}, \sqrt{6}) : \mathbb{Q}] = 4$. Значит, в базисе расширения $\mathbb{Q}(\sqrt{5}, \sqrt{6})/\mathbb{Q}$ 4 элемента. При этом:

- Базис $L/K : 1; \sqrt{5}$.
- Базис $M/L : 1, \sqrt{6}$.

Следовательно, базис $M/K : 1, \sqrt{5}, \sqrt{6}, \sqrt{30}$.

Докажем, что $\mathbb{Q}(\sqrt{5}, \sqrt{6}) = \mathbb{Q}(\sqrt{5} + \sqrt{6})$.

(Достаточность): Пусть $\alpha = \sqrt{5} + \sqrt{6}$. Тогда $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{5}, \sqrt{6})$, так как $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}, \sqrt{6}), \alpha \in \mathbb{Q}(\sqrt{5}, \sqrt{6})$.

(Необходимость): Теперь докажем, что $\mathbb{Q}(\sqrt{5}, \sqrt{6}) \subset \mathbb{Q}(\sqrt{5} + \sqrt{6})$.

1. $(\alpha - \sqrt{5})^2 = 6$,
   $\alpha^2 - 2\alpha\sqrt{5} + 5 = 6$,
   $\alpha^2 - 2\alpha\sqrt{5} - 1 = 0$,
   $\sqrt{5} = \frac{\alpha^2-1}{2\alpha} \in \mathbb{Q}(\alpha)$.
2. $(\alpha - \sqrt{6})^2 = 5$,
   $\alpha^2 - 2\alpha\sqrt{6} + 6 = 5$,
   $\alpha^2 - 2\alpha\sqrt{6} + 1 = 0$,
   $\sqrt{6} = \frac{\alpha^2+1}{2\alpha} \in \mathbb{Q}(\alpha)$.

Таким образом, $\mathbb{Q}(\sqrt{5}, \sqrt{6}) \subset \mathbb{Q}(\sqrt{5} + \sqrt{6})$.

Минимальный многочлен элемента α равен $\mu_\alpha(X) = X^4 - 22X^2 + 1$.

1.9 Расширенный пример

Определение 11. Пусть $f \in \mathbb{Q}[X], d_1, ..., d_n$ – корни f в $\mathbb{C}$. Тогда $\mathbb{Q}(d_1, ..., d_n)$ называется полем разложения многочлена f.

Пример 9. Вычислим степень поля разложения многочлена $f = X^3 - 5$ над $\mathbb{Q}$.

- Корни многочлена $f : \theta_1 = \sqrt[3]{5}, \theta_2 = \zeta\sqrt[3]{5}, \theta_3 = \zeta^2\sqrt[3]{5}$, где ζ – примитивный кубический корень из единицы.
- Поле разложения: $\mathbb{Q}(\theta_1, \theta_2, \theta_3)$.

- $K = \mathbb{Q}(\theta_1) \subset L = \mathbb{Q}(\theta_1, \theta_2) \subset M = \mathbb{Q}(\theta_1, \theta_2, \theta_3)$.
- По теореме 4: $[M : \mathbb{Q}] = [K : \mathbb{Q}][L : K][M : L] = 3 \cdot 2 \cdot 1 = 6$.
- Базис $K/\mathbb{Q} : 1, \theta_1, \theta_1^2$.
- Базис $L/K : 1, \frac{\theta_2}{\theta_1} = \zeta$.
- Базис $M/L : 1$.