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

Лекция №3

1 Числовые поля

1.10 Расширения числовых полей и поля алгебраических чисел

Лемма 3. *Пусть L – конечное расширение числового поля K. Тогда L – тоже числовое поле.*

Теорема 5. *Пусть $\alpha, \beta \in \mathbb{C}$ – алгебраические. Тогда $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta}$ – тоже алгебраические числа.*

Пример 10. Рассмотрим $\mu_\alpha(X) = X^{10^6} + 3X^9 + 5X^8 - 11X^4 + 72$ и $\mu_\beta(X) = X^{99999} + 7777X - \frac{11111}{35353535}$. В силу теоремы 5 существует $\mu_{\alpha+\beta}(X)$.

Определение 12. $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} | \alpha$ – алгебраическое $\}$.

Теорема 6. $\overline{\mathbb{Q}}$ *– поле.*

1.11 Нормы и следы

Пусть K – числовое поле, $\alpha \in K, K/\mathbb{Q}$ – векторное пространство. Рассмотрим линейный оператор $m_{K,\alpha} : K \to K, \theta \mapsto \alpha\theta$. $\alpha \neq 0$. Тогда m_α – инъективно и сюръективно. Следовательно, m_α – изоморфизм K на себя (как векторного пространства).

Определение 13. $Tr_{K/\mathbb{Q}}(\alpha) = Trace(m_\alpha) \in \mathbb{Q}$, $N_{K/\mathbb{Q}}(\alpha) = det(m_\alpha) \in \mathbb{Q}$.

Лемма 4. *Пусть $d \neq 0; 1$ – целое, свободное от квадратов, $K = \mathbb{Q}(\sqrt{d})$. Тогда $Tr_{K/\mathbb{Q}}(a + b\sqrt{d}) = 2a$, $N_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - b^2 d$.*

Предложение 1. Пусть $\alpha, \beta \in K$, тогда $Tr_{K/\mathbb{Q}}(\alpha+\beta) = Tr_{K/\mathbb{Q}}(\alpha)+Tr_{K/\mathbb{Q}}(\beta)$, $N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$.

Пример 11. Пусть $f = X^3 + 2X + 2, \theta$ – корень f в кубическом расширении $\mathbb{Q}$. Тогда $\theta^3 = -2\theta - 2$, причем $1, \theta, \theta^2$ – базис $\mathbb{Q}(\theta)/\mathbb{Q}$.

- $m_{\theta^2}(1) = 0 \cdot 1 + 0 \cdot \theta + 1 \cdot \theta^2$

- $m_{\theta^2}(\theta) = -2 \cdot 1 - 2 \cdot \theta + 0 \cdot \theta$
- $m_{\theta^2}(\theta^2) = 0 \cdot 1 - 2 \cdot \theta - 2 \cdot \theta^2$

$$M_{\theta^2} = \begin{pmatrix} 0 & -2 & 0 \\ 0 & -2 & -2 \\ 1 & 0 & -2 \end{pmatrix}$$

Соответственно, $Tr(\theta^2) = -4$, $N(\theta^2) = 4$.

1.12 Характеристический многочлен

Определение 14. Пусть K – числовое поле, $\alpha \in K$. $\chi_{K,\alpha} \in \mathbb{Q}[X]$ – характеристический многочлен $m_{K,\alpha}$, и этот многочлен всегда унитарный.

На построении характеристических многочленов основан ещё один метод нахождения следов и норм.

Пример 12. $\mathbb{Q}(\sqrt{d})$, $\alpha = a + b\sqrt{d}$

$$M_\alpha = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}; \qquad \chi_\alpha = \begin{vmatrix} X-a & -bd \\ -b & X-a \end{vmatrix} = X^2 - 2aX + 4X + (a^2 - b^2 d).$$

Теорема 7. *Пусть K – числовое поле, $\alpha \in K$. Тогда*

1. $deg\chi_\alpha = [K : \mathbb{Q}]$.
2. *Пусть* $\chi_\alpha = X^n + a_{n-1}X^{n-1} + ... + a_0$, *тогда* $Tr(\alpha) = -a_{n-1}$, $N(\alpha) = (-1)^n a_0$.
3. $\chi_\alpha(\alpha) = 0$.

Лемма 5. *Пусть $K = \mathbb{Q}(\alpha)$ – числовое поле. Тогда $\chi_\alpha(X) = \mu_\alpha(X)$.*

Пример 13. Пусть α – корень неприводимого над $\mathbb{Q}$ многочлена $X^3 - 2X - 2$. Тогда

- $\mu_{alpha}(X) = X^3 - 2X - 2 = \chi_\alpha(X)$.
- $Tr(\alpha) = 0$.
- $N(\alpha) = (-1)^3(-2) = 2$.

Лемма 6. *Пусть $K \subset L$ – числовые поля, $\alpha \in K$. Тогда $\chi_{L,\alpha}(X) = \chi_{K,\alpha}(X)^{[L:K]}$. В частности, если $K = \mathbb{Q}(\alpha)$, то $\chi_{L,\alpha}(X) = \mu_{K,\alpha}(X)^{[L:K]}$.*

Пример 14. Рассмотрим $\alpha = a + b\sqrt{5}$, $a, b \in \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{5}, \sqrt{6})$. Имеем:

- $m_\alpha(1) = a \cdot 1 + b \cdot \sqrt{5} + 0 \cdot \sqrt{6} + 0 \cdot \sqrt{30}$.

- $m_\alpha(\sqrt{5}) = 5b \cdot 1 + a \cdot \sqrt{5} + 0 \cdot \sqrt{6} + 0 \cdot \sqrt{30}$.
- $m_\alpha(\sqrt{6}) = 0 \cdot 1 + 0 \cdot \sqrt{5} + a \cdot \sqrt{6} + b \cdot \sqrt{30}$.
- $m_\alpha(\sqrt{30}) = 0 \cdot 1 + 0 \cdot \sqrt{5} + 5b \cdot \sqrt{6} + a \cdot \sqrt{30}$.

$$M'_\alpha = \begin{pmatrix} a & 5b & 0 & 0 \\ b & a & 0 & 0 \\ 0 & 0 & a & 5b \\ 0 & 0 & b & a \end{pmatrix}; \qquad M' = \begin{pmatrix} M_{K,\alpha} & \\ & M_{K,\alpha} \end{pmatrix}$$

$\chi_{L,\alpha} = det(I_4 X - M'_{L,\alpha}) = (det(I_2 X - M_{K,\alpha}))^2 = \chi K, \alpha^2 = ((X-a)^2 - 5b^2)^2$.

Пример 15. Рассмотрим $f(X) = X^3 + X + 1$, θ – корень $f(X)$. Тогда $\theta^3 = -\theta - 1$. Если $K = \mathbb{Q}(\theta)$, то $[K : \mathbb{Q}] = 3$ и $1, \theta, \theta^2$ – базис $K/\mathbb{Q}$.

Пусть $\alpha = 1 + \theta + \theta^2$. Имеем:

- $m_\alpha(1) = 1 \cdot 1 + 1 \cdot \theta + 1 \cdot \theta^2$.
- $m_\alpha(\theta) = \theta + \theta^2 + \theta^3 = -1 \cdot 1 + 0 \cdot \theta + 1 \cdot \theta^2$.
- $m_\alpha(\theta^2) = -1 \cdot 1 - 2 \cdot \theta + 0 \cdot \theta^2$.

$$M = \begin{pmatrix} 1 & -1 & -1 \\ 1 & 0 & -2 \\ 1 & 1 & 0 \end{pmatrix}; \qquad det(M) = \begin{vmatrix} X-1 & 1 & 1 \\ -1 & X & 2 \\ -1 & -1 & X \end{vmatrix} = X^3 - X^2 + 4X - 3$$

$\chi_{L,\alpha}(X) = \chi_{K,\alpha}(X)^{[L:K]}, [L : K] = 1 \Rightarrow detM = \mu(\alpha)$.

Замечание 1. Пусть $K \subset L$ – числовые поля, $\alpha \in K$. Тогда

1. $Tr_{L/\mathbb{Q}}(\alpha) = [L : K] \cdot Tr_{K/\mathbb{Q}}(\alpha)$.
2. $N_{L/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\alpha)^{[L:K]}$.