Методы алгебраической теории чисел в криптографии

БФУ им. И.Канта --- Малыгина Е.С.

Тема. СЛЕДЫ и НОРМЫ.

1. В поле $K = \mathbb{Q}(\alpha, \beta)$, вычислить $Tr_K(\alpha)$, $Tr_K(\beta)$, $N_K(\alpha)$, $N_K(\beta)$.

   1) $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$, 2) $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{1})$, 3) $K = \mathbb{Q}(i, \sqrt{3} \cdot \sqrt[3]{1})$.

2. Вычислить $Tr_{K/k}(\alpha)$ и $N_{K/k}(\alpha)$ для

   1) $K = \mathbb{Q}(\sqrt[4]{3})$, $k = \mathbb{Q}(\sqrt{3})$, $\alpha = \sqrt[4]{3}$,

   2) $K = \mathbb{Q}(\sqrt[4]{3})$, $k = \mathbb{Q}(\sqrt{3})$, $\alpha = \sqrt[4]{3} + \sqrt{3}$,

   3) $K = \mathbb{Q}(\zeta)$, где $\zeta = e^{2\pi i/5}$, $k = \mathbb{Q}$, $\alpha = \zeta + \zeta^2$,

3. Пусть $K = \mathbb{Q}(\theta)$, где θ – корень неприводимого кубического трёхчлена $X^3 - 3X + 1$. Найти норму и след числа θ^2.