Методы алгебраической теории чисел в криптографии

БФУ им. И.Канта --- Малыгина Е.С.

Тема 1. АЛГЕБРАИЧЕСКИЕ ЧИСЛА

1. Найти минимальный многочлен числа z над полем k.

   1) $z = \sqrt[3]{5}$, $k = \mathbb{Q}$,

   2) $z = 2 - 3i$, $k = \mathbb{R}$,

   3) $z = (1 + i)/\sqrt{2}$, $k = \mathbb{Q}(i)$,

   4) $z = 1 + \sqrt{2}$, $k = \mathbb{Q}(\sqrt{2} + \sqrt{5})$,

   5) $z = (1 + i)/\sqrt{2}$, $k = \mathbb{Q}(\sqrt{-2})$.

2. Найти степень алгебраического числового поля K, порождённого корнями многочлена $f(X)$, указать базис K над $\mathbb{Q}$.

   1) $f(X) = X^3 - 3$,
   2) $f(X) = X^4 - 3$,
   3) $f(X) = (X^3 - 2)(X^2 - 2)$,
   4) $f(X) = X^6 + X^3 + 1$.