

Вычисления групп Галуа

Задача 1. Пусть \mathbb{F}_q – конечное поле из $q = p^k$ элементов.

(а) Докажите, что для любого n существует неприводимый многочлен степени n над полем \mathbb{F}_q .

(б) Найдите поле разложения неприводимого многочлена степени n над \mathbb{F}_q и его группу Галуа.

(в) Пусть $\xi \in \mathbb{F}_q^*$ – примитивный элемент мультипликативной группы, а l – простой делитель $q - 1$. Докажите, что многочлен $x^l - \xi$ неприводим над \mathbb{F}_q .

(г) Пусть $0 \neq a \in \mathbb{F}_q$. Докажите, что многочлен $x^p - x - a$ неприводим над \mathbb{F}_q или раскладывается на линейные множители.

Задача 2.

(а) Докажите, что многочлен $x^5 - x - 1$ неприводим над \mathbb{F}_5 и над \mathbb{Q} ;

(б) Разложите этот многочлен на неприводимые над \mathbb{F}_2 и \mathbb{F}_3 ;

(в) Докажите, группа Галуа этого многочлена над \mathbb{Q} есть S_5 .

Задача 3. Можно ли построить следующие правильные многоугольники циркулем и линейкой:

(а) пятиугольник;

(б) семиугольник;

(в) девятиугольник;

(г) семнадцатиугольник?