

Семинар 2. Конечные поля

Введение в теорию чисел, весенний семестр 2023 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Через p в этом листке обозначается простое число, через k — натуральное число.

Задача 1. При каких n кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$ является полем?

Задача 2. Выпишите таблицу умножения для поля из четырёх элементов.

Задача 3 (Тождество ленивого школьника). (а) Докажите, в поле характеристики p для любых двух элементов x и y выполнено тождество:

$$(x + y)^p = x^p + y^p.$$

(б) Выведите из пункта (а) малую теорему Ферма.

Задача 4. Какие из следующих факторколец являются полями? В случае, когда факторкольцо является конечным полем, найдите количество элементов в нём.

(а) $\mathbb{F}_2[x]/(x^2 + 1)$; (б) $\mathbb{F}_3[x]/(x^2 + 1)$; (в) $\mathbb{Z}[x]/(2, x^2 + x + 1)$;

(г) $\mathbb{Z}[i]/(2)$; (д) $\mathbb{Z}[\sqrt{-2}]/(5)$; (е) $\mathbb{Z}[e^{\frac{2\pi i}{3}}]/(2)$.

Задача 5. (а) Докажите, что если поле конечно, то в нём p^k элементов.

(б) Докажите, что если подполе из p^k элементов лежит в подполе из p^ℓ элементов, то k делит ℓ .

Задача 6. Докажите, что конечная область целостности является полем.

Задача 7. Обозначим через \mathbb{F}_q поле из $q = p^k$ элементов. Докажите, что автоморфизм Фробениуса $x \mapsto x^p$ является линейным оператором на \mathbb{F}_q , если \mathbb{F}_q рассматривать как векторное пространство над \mathbb{F}_p . Найдите собственные векторы, собственные числа и характеристический многочлен этого оператора.