# Конечные поля

**Задача 1.** a) Сколько элементов содержит векторное пространство размерности $n$ над полем из $q$ элементов?

b) Докажите, что если в поле $q$ элементов, то $q$ — степень простого целого числа.

**Задача 2.** Рассмотрим многочлен $P_n = x^{p^n} - x$.

a) Докажите, что $P_n$ не имеет кратных корней над полем характеристики $p$.

b) Докажите, что всякий элемент поля из $p^n$ элементов является корнем $P_n$.
*Hint: Воспользуйтесь теоремой Лагранжа.*

c) Докажите, что корни $P_n$ в поле характеристики $p$ образуют подполе.

d) Докажите, что поле разложения $P_n$ над полем $\mathbb{Z}/p\mathbb{Z}$ состоит из $p^n$ элементов.

e) Докажите, что всякое поле из $p^n$ элементов изоморфно полю разложения $P_n$ над полем $\mathbb{Z}/p\mathbb{Z}$.

**Определение 1** Единственное с точностью до изоморфизма поле из $q = p^n$ элементов обозначим $\mathbb{F}_q$.

**Задача 3.** a) Докажите, что мультипликативная группа $\mathbb{F}_q$ циклическая.
*Hint: Воспользуйтесь тем, что многочлен степени $k$ имеет не более $k$ корней.*

b) Докажите, что если $p > 2$, то $x \in \mathbb{F}_{p^n}$ является квадратом тогда и только тогда, когда $x^{\frac{p^n-1}{2}} = 1$. Какие элементы являются квадратами при $p = 2$?

**Задача 4.** a) При каких $m$ и $n$ многочлен $x^{p^n} - x$ делится на $x^{p^m} - x$ над полем характеристики $p$?

b) Докажите, что $\mathbb{F}_{p^n}$ содержит подполе, изоморфное $\mathbb{F}_{p^m}$ тогда и только тогда, когда $n$ делится на $m$.

c) Докажите, что такое подполе единственно.

**Задача 5*.** *a**) Докажите, что в $\mathbb{F}_q$ неразложимый многочлен $Q$ делит $x^{q^n} - x$ тогда и только тогда, когда степень $Q$ делит $n$.

*b**) Пусть $r$ — простое число. Докажите, что всего существует $\frac{q^r - q}{r}$ неразложимых многочленов степени $r$ с точностью до умножения на константу.

*c**) Как посчитать количество неразложимых многочленов произвольной степени над $\mathbb{F}_q$?

**Определение 2** Пусть $q = p^n$. Определим *автоморфизм Фробениуса* $\mathcal{F} : \mathbb{F}_q \to \mathbb{F}_q$ как отображение, переводящее $x$ в $x^p$.

**Задача 6.** a) Докажите, что $\mathcal{F}$ является изоморфизмом полей.

b) Докажите, что всякий изоморфизм из $\mathbb{F}_q$ в $\mathbb{F}_q$ совпадает с некоторой степенью $\mathcal{F}$.
*Hint: Воспользуйтесь тем, что $\mathbb{F}_q^*$ циклическая.*

c) Сколько элементов $\mathcal{F}^k$ переводит в себя?

d) Сколько существует вложений $\mathbb{F}_{p^n}$ в $\mathbb{F}_{p^{kn}}$?

**Задача 7.** a) Вычислите группу Витта $\mathbb{F}_q$.

*b**) Вычислите кольцо Витта $\mathbb{F}_q$.