Конечные поля

Задача 5.1. Выпишите явно таблицы сложения и умножения полей из 4 и 8 элементов.

Задача 5.2. Для каких q_1 и q_2 существует гомоморфизм $\mathbb{F}_{q_1} \to \mathbb{F}_{q_2}$?

Задача 5.3. Группа автоморфизмов поля $\mathbb{F}_{p^n}$ порождена автоморфизмом Фробениуса $x \mapsto x^p$. (Какой, кстати, порядок этой группы?)

Задача 5.4. а) Если многочлен $x^p - x - a$ имеет в поле характеристики p хотя бы один корень, то он разлагается на линейные множители.

б) Над полем $\mathbb{F}_p$ этот многочлен неприводим (при $a \neq 0$).

Задача 5.5. Разложим на неприводимые множители над $\mathbb{F}_p$ все многочлены вида $x^{p^n} - x$. Все ли неприводимые многочлены при этом встретятся?

* * *

▷ Обозначим через Φ_n многочлен $\prod(x - \zeta_n)$, где произведение берется по всем примитивным комплексным корням степени n из единицы ("n-й круговой многочлен").

Задача 5.6. а) $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$.

б) Выпишите многочлены $\Phi_4(x)$ и $\Phi_6(x)$.

в) $\Phi_n(x)$ — многочлен с *целыми* коэффициентами и старшим коэффициентом 1.

Задача 5.7. а) Если характеристика поля k не делит n, то корни Φ_n в k суть элементы порядка n в группе $k^\times$.

б*) Пусть Φ_n разложен над $\mathbb{F}_p$ (p не делит n) на неприводимые множители. Тогда если ζ — корень одного из этих множителей (в $\mathbb{F}_{p^k}$), то ζ^p — корень *того же* множителя.

в*) Над $\mathbb{Z}$ многочлен Φ_n неприводим.

Задача 5.8. а) Если a — целое число, p — простой делитель числа $\Phi_n(a)$, не делящий n, то $p \equiv 1 \pmod{n}$.

б) Для любого целого n существует бесконечно много простых чисел, сравнимых с единицей по модулю n.

(Напомним, что *теорема Дирихле* утверждает, что единицу в последнем утверждении можно заменить на любой обратимый остаток по модулю n.)