Алгебра 2 14.03.2011
Листок 6

Конечные поля

Задача 1. Пусть k – конечное поле характеристики p. Докажите, что k состоит из p^n элементов для некоторого $n \in \mathbb{N}$.

Задача 2. a°) Пусть k – конечное поле из p^n элементов. Докажите, что любой элемент x поля k удовлетворяет уравнению $x^{p^n} - x = 0$.

Пусть K – алгебраически замкнутое поле характеристики p. Обозначим через $\mathbb{F}_{p^n}$ множество решений уравнения $x^{p^n} - x = 0$ в K.

b°) Докажите, что $\mathbb{F}_{p^n}$ содержит ровно p^n элементов.

c°) Докажите, что $\mathbb{F}_{p^n}$ – подполе в K.

d^*) Докажите, что $\mathbb{F}_{p^n}$ не зависит от K и что любое поле из p^n элементов изоморфно $\mathbb{F}_{p^n}$.

Задача 3. Докажите, что мультипликативная группа $\mathbb{F}_{p^n}^*$ конечного поля циклическая.

Подсказка: используйте классификацию конечных абелевых групп и то, что уравнение степени d имеет не более d решений.

Задача 4. Пусть $\mathsf{k} = \mathbb{F}_{p^n}$ – поле. a) Сколько существует в k корней степени m из 1?

b) Сколько существует в k корней степени m из $a \in \mathsf{k}$?

c), d) Те же вопросы для алгебраически замкнутого поля k характеристики p.

Задача 5. a) Разделите с остатком $x^n - 1$ на $x^m - 1$ в $\mathbb{Q}[x]$.

b) Разделите с остатком $x^{p^n} - x$ на $x^{p^m} - x$ в $\mathbb{F}_p[x]$.

c°) При каких n и m поле $\mathbb{F}_{p^n}$ содержит $\mathbb{F}_{p^m}$? d) Найдите $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m}$.

Задача 6*. Пусть $f(x)$ – неприводимый многочлен степени n над $\mathbb{F}_p$, а K – алгебраически замкнутое поле характеристики p. a) Докажите, что все корни f лежат в $\mathbb{F}_{p^n}$.

b) Докажите, что f не имеет кратных корней.

c) Обратно, если $x \in \mathbb{F}_{p^n}$, то x является корнем неприводимого многочлена над $\mathbb{F}_p$ степени d, где $d|n$.

Задача 7*. a) Докажите равенство

$$x^{p^n} - 1 = \prod_{d|n} \prod_{\deg f = d} f(x),$$

где произведение берётся по всем неприводимым над $\mathbb{F}_p$ многочленам со старшим коэффициентом 1.

Пусть $\psi(n)$ – число неприводимых над $\mathbb{F}_p$ многочленов со старшим коэффициентом 1.

b) Покажите, что $p^n = \sum_{d|n} d\psi(d)$.

c) Обращая предыдущее равенство, получите выражение для $\psi(n)$.

d) Докажите, что для любого n существуют неприводимые многочлены степени n над $\mathbb{F}_p$.

Пусть k – поле характеристики p. Обозначим через $\Phi\colon \mathsf{k} \to \mathsf{k}$ отображение Фробениуса: $x \mapsto x^p$.

Задача 8. a°) Покажите, что Φ является гомоморфизмом полей.

b°) Покажите, что для конечного или алгебраически замкнутого поля Φ является автоморфизмом.

c) Приведите пример поля, для которого гомоморфизм Фробениуса не обратим.

d) Докажите, что число сочетаний $C_{p^n}^k$ делится на p при $0 < k < p^n$.

Задача 9. Пусть $\mathsf{k} = \mathbb{F}_{p^n}$ – поле из p^n элементов.

a) Найдите порядок Φ в группе автоморфизмов k.

b) Докажите, что все автоморфизмы k имеют вид Φ^i.

Задача 10. a) Докажите, что поле $\cup_n \mathbb{F}_{p^n}$ алгебраически замкнуто.

b^*) Опишите его автоморфизмы.