Семинар 17. Конечные поля

Всюду, где не оговорено дополнительно предполагается, что $\mathbb{F}_q$ – конечное поле характеристики p, состоящее из $q = p^n$ элементов.

Задача 1. Докажите, что

(a) многочлен степени n имеет не более n корней над любым полем,

(b) конечная подгруппа мультипликативной группы поля циклическая.

Задача 2.

(a) Приведите пример многочлена $f(x) \in \mathbb{F}_p[x]$, поле разложения которого имеет p^n элементов.

(b) Докажите, что все поля из p^n элементов изоморфны;

(c) Покажите, что отображение конечных полей $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ существует тогда и только тогда, когда $n|m$.

Задача 3. Сколько различных подполей имеет поле из 3^{30} элементов?

Задача 4. Пусть $\xi \in \mathbb{F}_q^*$ — образующая мультипликативной группы поля из q элементов. Пусть $\mathbb{F}_r \subset \mathbb{F}_q$ его подполе. Докажите, что $\mathbb{F}_q \simeq \mathbb{F}_r[\xi]$. В частности, $\mathbb{F}_q$ является простым расширением $\mathbb{F}_r$.

Задача 5. Пусть $f(x)$ неприводимый многочлен над $\mathbb{F}_q$ степени n. Верно ли, что

(a) если $f(x)$ квадратичен, то он раскладывается на линейные множители над $\mathbb{F}_{q^2}$;

(b) $f(x)$ имеет корень над расширением $\mathbb{F}_{q^m}$ тогда и только тогда, когда $n|m$;

(c) $f(x)$ неприводим над $\mathbb{F}_{q^m}$ тогда и только тогда, когда числа m и n взаимнопросты.

Задача 6. Докажите, что степень поля разложения многочлена $f(x)$ над конечным полем $\mathbb{F}$ равна

(a) его степени, если $f(x)$ – неприводим;

(b) наименьшему общему кратному степеней неприводимых над $\mathbb{F}$ делителей многочлена $f(x)$.

Задача 7. Выпишите все неприводимые

(a) над $\mathbb{F}_3$ многочлены, степень которых не превосходит 3 и уточните, какие из них остаются неприводимыми над $\mathbb{F}_9$;

(b) над $\mathbb{F}_2$ многочлены, степень которых не превосходит 4 и уточните, какие из них остаются неприводимыми над $\mathbb{F}_4$ и $\mathbb{F}_8$ соответственно.

Задача 8. Докажите, что

(a) Неприводимый многочлен $f(x) \in \mathbb{F}_q[x]$ делит $x^{q^n} - x$ тогда и только тогда, когда его степень делит n;

(b) выполнено равенство

$$x^{q^n} - x = \prod_{d|n} \prod_{f_d - \text{неприводим}} f_d(x)$$

произведение берётся по всем унитарным неприводимым многочленам степени делящей n;

(c) $q^n = \sum_{d|n} d\psi(d)$, где $\psi(d)$ – число неприводимых многочленов степени d.

Задача 9. Покажите, что в конечном поле $\mathbb{F}$ характеристики p каждый элемент имеет один и только один корень p-ой степени.