

## Листок 5

### Тема 5 (2.1). Конечные поля. Расширения полей

#### Упражнения и задачи

1. Завершите доказательство леммы: пусть  $k$  — поле характеристики  $p$ , тогда  $\forall \alpha, \beta \in k$   
 $\forall d \in \mathbb{Z}_+ (\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$ .
2. Докажите, что многочлен  $x^2 + x + 1$  неприводим над  $\mathbb{F}_2$  (т.е.  $\mathbb{F}_2[x]/(x^2 + x + 1)$  является полем). Выпишите таблицы операций сложения и умножения элементов в этом поле, а также обратные элементы.
3. Найдите все неприводимые многочлены степени 4 над полем  $\mathbb{F}_2$ .
4. Пусть  $L/K$ ,  $M/L$  — конечные расширения (произвольных) полей. Докажите, что расширение  $M/K$  также конечно и  $[M : K] = [K : L][L : K]$ .
5. Докажите, что если  $L/K$  — конечное расширение, то оно является алгебраическим.
6. Пусть  $q = p^n$ ,  $\mathbb{F}_{q^m}/\mathbb{F}_q$  — расширение. Докажите, что если  $f \in \mathbb{F}_q$  — неприводимый, то  $\mathbb{F}_{q^m}$  — поле разложения  $f$ .
7. Пусть  $p, q$  — различные простые. Чему равно число неприводимых многочленов степени  $q$  в  $\mathbb{F}_p[x]$ ?
8. Докажите следующие оценки для числа неприводимых многочленов степени  $n$  над  $\mathbb{F}_p$ :

$$\frac{1}{n}p^n - \frac{p}{n(p-1)}(p^{\frac{n}{2}} - 1) \leq \nu(n) \leq \frac{1}{n}(p^n - p).$$

9. Пусть  $\sigma_j(f) = \sum_{g|f} (Ng)^j$ , где суммирование берется по неприводимым унитарным делителям  $g$  (для  $f \in \mathbb{F}_q[x]$  степени  $\deg f = n$   $Nf = q^n$ ). Докажите, что
  - $\sum_f \frac{\sigma_0(f)}{(Nf)^s} = \frac{1}{(1 - q^{1-s})^2}$ ;
  - $\sum_f \frac{\sigma_1(f)}{(Nf)^s} = \frac{1}{(1 - q^{1-s})(1 - q^{2-s})}$ .
10. Пусть  $\alpha \in \mathbb{F}_q^*$ . Докажите, что  $x^n = \alpha$  разрешимо  $\Leftrightarrow \alpha^{(q-1)/d}=1$ , где  $d = (n, q-1)$ , причем если разрешимо, то  $d$  решений.
11. Как выглядит подгруппа всех квадратов в  $\mathbb{F}_{2^n}$ ?
12. Пусть  $n|q-1$ , докажите, что  $G = \{\alpha \in \mathbb{F}_q^* : x^n = \alpha \text{ — разрешимо}\}$  — подгруппа в  $\mathbb{F}_q^*$ ,  $|G| = \frac{q-1}{n}$ .
13. Пусть  $n|q-1$ ,  $F = \mathbb{F}_q$ ,  $K/F$  — расширение конечных полей,  $[K : F] = n$ . Докажите, что  $\forall \alpha \in F^*$  уравнение  $x^n = \alpha$  имеет  $n$  решений в  $K$ .
14. Пусть  $K/F$  — расширение конечных полей,  $\text{char } F \neq 2$ ,  $[K : F] = 3$ . Докажите, что если  $\alpha$  не является квадратом в  $F$ , то  $\alpha$  не является квадратом и в  $K$ .
15. Пусть  $F = \mathbb{F}_q$ ,  $K/F$  — расширение конечных полей,  $\alpha \in \mathbb{F}_q$ ,  $n|q-1$  и  $x^n = \alpha$  не разрешимо в  $\mathbb{F}_q$ . Тогда  $x^n = \alpha$  не разрешимо в  $K$ , если  $(n, [K : F]) = 1$ .

16. Пусть  $F = \mathbb{F}_q$ ,  $K/F$  — расширение конечных полей,  $[K : F] = 2$ . Докажите, что  $\forall \beta \in K \ \beta^{1+q} \in F$ . Более того,  $\forall \alpha \in F \ \exists \beta \in K: \alpha = \beta^{1+q}$ .

### SageMath

- Исследуйте основные функции SageMath связанные с заданием и свойствами конечных полей
  - Определение конечного поля: `FiniteField()`, `GF()`;
  - Неприводимый многочлен задающий конечное поле: `polynomial()`, опция `modulus` в `FiniteField()` для явного задания неприводимого многочлена модели конечного поля;
  - Решение уравнения  $x^n = \alpha$ : `nth_root()`;
  - Поле разложения: `splitting_field()`;
  - Расширение полей: `extension()`.

### Темы для самостоятельного изучения

- Поле  $\mathbb{F}_q$ ,  $q = p^n$ , однозначно определено в  $\bar{\mathbb{F}}_p$  как поле разложения многочлена  $z^q - z$ . Всякое конечное поле изоморфно одному и только одному  $\mathbb{F}_q$ . ([Степ], [LN])