Листок 5
Тема 5(2.1). Конечные поля. Соответствие Галуа

Упражнения и задачи

1. Завершите доказательство предложения: 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 если расширение L/K конечной степени $[L:K]$, то L/K — алгебраическое.

3. Докажите, что
   - для $a \in \mathbb{Z}\ a^l - 1 | a^m - 1 \Leftrightarrow l|m$
   - в $\mathbb{F}_q[x]\ x^l - 1 | x^m - 1 \Leftrightarrow l|m$

4. Пусть p, q — различные простые. Чему равно число неприводимых многочленов степени q в $\mathbb{F}_p[x]$?

5. 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
   - $\sum\limits_f \dfrac{\sigma_0(f)}{(Nf)^s} = \dfrac{1}{(1-q^{1-s})^2}$;
   - $\sum\limits_f \dfrac{\sigma_1(f)}{(Nf)^s} = \dfrac{1}{(1-q^{1-s})(1-q^{2-s})}$.

6. 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.

7. Как выглядит подгруппа всех квадратов в $\mathbb{F}_{2^n}$?

8. Пусть $n|q-1$, докажите, что $G = \{\alpha \in \mathbb{F}_q^* : x^n = \alpha$ — разрешимо$\}$ — подгруппа в $\mathbb{F}_q^*$, $|G| = \frac{q-1}{n}$.

9. 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.

10. Пусть K/F — расширение конечных полей, $\operatorname{char} F \neq 2$, $[K:F] = 3$. Докажите, что если α не является квадратом в F, то α не является квадратом и в K.

11. 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 $(n, [K:F]) = 1$.

12. 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()`.