Листок 6
Тема 6 (2.2). Группа автоморфизмов. Норма и след

Упражнения и задачи

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

2. Завершите доказательсво теоремы о цикличности $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$: покажите, что $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| \leqslant n$.

3. Докажите, что характеристический многочлен $g_\alpha(x)$ и определитель $\det A_\alpha$ не зависят от выбора базиса расширения L/K.

4. Докажите следующие свойства нормы и следа:
   (a) $\mathrm{N}_{L/K}(a) = a^n$, $\mathrm{Tr}_{L/K}(a) = na$, $a \in K$;
   (b) $\mathrm{N}_{L/K}(\alpha\beta) = \mathrm{N}_{L/K}(\alpha)\,\mathrm{N}_{L/K}(\beta)$, $\alpha, \beta \in L$;
   (c) $\mathrm{N}_{L/K}(a\alpha) = a^n\,\mathrm{N}_{L/K}(\alpha)$, $\mathrm{Tr}_{L/K}(a\alpha) = a\,\mathrm{Tr}_{L/K}(\alpha)$, $a \in K$, $\alpha \in L$.

5. Пусть L/K — расширение, $\alpha \in L$, $g_\alpha(x)$ — характеристический многочлен α, M/K — расширение, в котором $g_\alpha(x)$ полностью раскладывается на линейные множители: $g_\alpha(x) = (x - \alpha_1)\dots(x - \alpha_n)$. Докажите, что:
$$\mathrm{N}_{L/K}(\alpha) = \alpha_1 \dots \alpha_n,\ \mathrm{Tr}_{L/K}(\alpha) = \alpha_1 + \dots + \alpha_n.$$

6. Пусть L/K, M/L — конечные расширения, $\gamma \in M$. Докажите, что $\mathrm{N}_{M/K}(\gamma) = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\gamma))$, $\mathrm{Tr}_{M/K}(\gamma) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\gamma))$.

7. Пусть $(\alpha_1, \dots, \alpha_n)$, $(\beta_1, \dots, \beta_n)$ — два базиса расширения L/K. Докажите, что $\Delta(\alpha_1, \dots, \alpha_n) = \gamma^2 \Delta(\beta_1, \dots, \beta_n)$ для некоторого $\gamma \in K^*$.

8. Пусть $q = p^n$. Докажите, что $\forall a \in \mathbb{F}_p$ уравнение $\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(x) = a$ в $\mathbb{F}_q$ имеет $(p^n - 1)/(p - 1)$ решений, а также что для каждого $b \in \mathbb{F}_p$ уравнение $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = b$ имеет p^{n-1} решений.

9. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение конечных полей, $\alpha \in \mathbb{F}_{q^m}$. Докажите, что сопряженные элементы $\alpha, \alpha^q, \alpha^{q^2}, \dots \alpha^{q^{m-1}}$ имеют один и тот же порядок в мультипликативной группе $\mathbb{F}_{q^m}^*$.

10. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение. Докажите, что $\forall c \in \mathbb{F}_q$
$$\sum_{j=0}^{m-1} x^{q^j} - c = \prod_{\alpha \in \mathbb{F}_{q^m}, \mathrm{Tr}(\alpha) = c} (x - \alpha).$$

11. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение, L — линейный оператор на $\mathbb{F}_{q^m}$ как на векторном пространстве над $\mathbb{F}_q$. Докажите, что $\exists! \alpha_0, \dots, \alpha_{m-1} \in \mathbb{F}_{q^m}$: оператор L имеет вид $L(\beta) = \alpha_0\beta + \alpha_1\beta^q + \dots + \alpha_{m-1}\beta^{q^{m-1}}$.

12. Докажите, что число базисов $\mathbb{F}_{q^m}/\mathbb{F}_q$ равно $(q^m - 1)(q^m - q)\dots(q^m - q^{m-1})$.

13. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение, $\alpha \in \mathbb{F}_{q^m}$. Докажите, что

$$\Delta(1, \alpha, \ldots, \alpha^{m-1}) = \prod_{0 \leqslant i < j \leqslant m-1} (\alpha^{q^i} - \alpha^{q^j})^2.$$

14. Пусть $\mathbb{F}_{q^m}/\mathbb{F}_q$ — расширение, $\alpha \in \mathbb{F}_{q^m}$. Докажите, что $\Delta(1, \alpha, \ldots, \alpha^{m-1})$ совпадает с дискриминантом характеристического многочлена $g_\alpha(x)$.

SageMath

- Исследуйте основные функции SageMath связанные с автоморфизмами и расширениями конечных полей:
  - Группа автоморфизмов поля: `End()`;
  - Автоморфизм Фробениуса: `frobenius_endomorphism()`;
  - Базисы расширений конечных полей;
  - Характеристический многочлен `charpoly()`;
  - Норма, след, дискриминант.

Темы для самостоятельного изучения

- Нормальный базис и теорема о нормальном базисе, [LN].