Листок 7
Тема 7 (2.3). Корни из единицы. Круговой многочлен

Упражнения и задачи

1. Пусть k — поле, $f = a_n x^n + \cdots + a_1 x + a_0 \in k[x]$, $f' = n a_n x^{n-1} + \cdots + a_1 \in k[x]$ — формальная производная f. Докажите следующие свойства:
   - $(f+g)' = f' + g'$;
   - $(fg)' = f'g + fg'$.
2. Пусть k — поле, $f \in k[x]$. докажите, что $\alpha \in k$ — кратный корень $\Leftrightarrow f'(\alpha) = 0$.
3. Пусть $f \in \mathbb{F}_{p^m}[x]$. Докажите, что $f \in \mathbb{F}_p \Leftrightarrow (f(x))^p = f(x^p)$.
4. Докажите, что если $d|n$ и Φ_n определен, то $\Phi_n \mid \dfrac{x^n - 1}{x^d - 1}$.
5. Пусть $f \in \mathbb{F}_q[x]$ — неприводимый, $\deg f = m$. Докажите, что $f \mid x^{q^n} - x \Leftrightarrow m|n$.
6. Докажите, что $\prod' f = x^{q^n} - x$, где произведение берется по всем неприводимым унитарным многочленам $f \in \mathbb{F}_q[x]$ таким, что $\deg f \mid n$. Сделайте вывод о числе неприводимых унитарных многочленов степени d в $\mathbb{F}_q[x]$ (на этот раз для произвольного конечного поля, $q = p^n$).
7. Докажите, что если $\operatorname{char} k = p \not| \, n$, то $\Phi_n = \prod\limits_{d|n} (x^d - 1)^{\mu(n/d)}$.
8. Докажите, что $\mathbb{F}_q$ есть $(q-1)$-е круговое поле над любым своим подполем.
9. Пусть $\alpha \in \mathbb{F}_q$, $n \in \mathbb{Z}$. Докажите, что $x^q - x + \alpha \mid x^{q^n} - x + n\alpha$.
10. Пусть $f \in \mathbb{F}_q[x]$, $q = p^n$. Докажите, что $f'(x) = 0 \Leftrightarrow f = g^p$ для некоторого $g \in \mathbb{F}_q[x]$.
11. Пусть $f \in \mathbb{F}_q[x]$, $q = p^n$, $\deg f = m \geqslant 1$, $f(0) \neq 0$. Докажите, что $\exists e \in \mathbb{Z}_+ \; e \leqslant q^m - 1$ такое что $f(x) \mid x^e - 1$. Наименьшее такое e называется порядком многочлена $f(x)$ в $\mathbb{F}_q[x]$. Докажите также следующие свойства:
    - Пусть $f \in \mathbb{F}_q[x]$ — неприводимый, тогда порядок f равен порядку $\alpha \in \mathbb{F}_{q^m}^*$, α — корень f;
    - Пусть $f \in \mathbb{F}_q[x]$ — неприводимый, тогда порядок f делит $x^e - 1$;
    - Пусть $c \in \mathbb{Z}_+$, e — порядок f, тогда $f(x) \mid x^c - 1 \Leftrightarrow e|c$;
    - Пусть $e_1, e_2 \in \mathbb{Z}_+$, тогда наибольший общий делитель многочленов $x^{e_1} - 1$, $x^{e_2} - 1$ в $\mathbb{F}_q[x]$ равен $x^d - 1$, где $d = (e_1, e_2)$.

SageMath

- Исследуйте основные функции SageMath связанные с работой в кольцах многочленов над конечными полями:
  - Кольцо многочленов: `PolynomialRing()`;
  - Неприводимость многочлена: `is_irreducible()`;
  - Разложение многочлена на множители: `factor()`;
  - Корни многочлена: `roots()`;
  - Круговой многочлен: `cyclotomic_polynomial()`.

Темы для самостоятельного изучения

- Изучите "элементарные"доказательство неприводимости кругового многочлена $\Phi_n(x)$ в $\mathbb{Z}[x]$. (см. например `https://www.lehigh.edu/ shw2/c-poly/several_proofs.pdf`)

- Теорема Веддербёрна: Всякое конечное кольцо с единицей, в котором каждый ненулевой элемент обратим, является полем. ([LN], [The Book]).