Алгебра

ДЗ 9

Гольдберг Дмитрий Максимович

Группа БПМИ248

Задание 1

Реализуем поле $\mathbb{F}_9$ в виде $\mathbb{Z}_3[x]/(x^2+2x+2)$. Перечислите в этой реализации все элементы данного поля, являющиеся порождающими циклической группы $\mathbb{F}_9^\times$.

Решение:

$$\mathbb{F}_9 = \{0, 1, 2, x, 2x, x+1, 2x+1, x+2, 2x+2\}$$

Очевидно, что $0, 1, 2$ не могут быть порождающими, будем проверять остальные элементы:
1.

$$\begin{gathered} x^1 = x \\ x^2 = x+1 \\ x^3 = 2x+1 \\ x^4 = 2 \\ x^5 = 2x \\ x^6 = 2x+2 \\ x^7 = x+2 \\ x^8 = 1 \\ \Rightarrow x - \text{порождающий} \end{gathered}$$

2.

$$2x = x^5 \Rightarrow \mathrm{ord}(2x) = \frac{8}{\gcd(8,5)} = 8 \Rightarrow 2x - \text{порождающий}$$

3.

$$x+1 = x^2, \gcd(2,8) \neq 1 \Rightarrow x+1 - \text{не ок}$$

4.

$$2x+1 = x^3, \gcd(8,3) = 1 \Rightarrow 2x+1 - \text{порождающий}$$

5.

$$x+2 = x^7, \gcd(8,7) = 1 \Rightarrow x+2 - \text{порождающий}$$

6.

$$2x+2 = x^6, \gcd(8,6) \neq 1 \Rightarrow 2x+2 - \text{не ок}$$

Ответ:

$x, 2x, 2x+1, x+2$

Задание 2

Проверьте, что многочлены x^2+3 и y^2+y+2 неприводимы над $\mathbb{Z}_5$, и установите явно изоморфизм между полями $\mathbb{Z}_5[x]/(x^2+3)$ и $\mathbb{Z}_5[y]/(y^2+y+2)$.

Решение:

$$f(x) = x^2+3, g(y) = y^2+y+2$$
$$f(0) = 3 \neq 0, f(1) = 4 \neq 0, f(2) = 7 \neq 0, f(3) = 12 \neq 0, f(4) = 19 \neq 0$$
$$g(0) = 2 \neq 0, g(1) = 4 \neq 0, g(2) = 8 \neq 0, g(3) = 14 \neq 0, g(4) = 22 \neq 0$$
$$\Rightarrow f \text{ и } g \text{ неприводимы над } \mathbb{Z}_5.$$
$$F = \mathbb{Z}_5[x]/(x^2+3), K = \mathbb{Z}_5[y]/(y^2+y+2)$$

Найдем корень α многочлена f в K. $\alpha = a + by$

$$(a+by)^2+3 = 0$$
$$a^2+2aby+b^2y^2+3 = 0$$
$$a^2+2aby+b^2(-y-2)+3 = 0$$
$$a^2-2b^2+3+y(2ab-b^2) = 0 \Longleftrightarrow$$
$$\Longleftrightarrow \begin{cases} a^2-2b^2+3 = 0 \\ 2ab-b^2 = 0 \end{cases}$$
$$\Rightarrow b(2a-b) = 0 \Rightarrow b = 0; 2a$$
$$1. b = 0 \Rightarrow a^2 = -3 - \text{не имеет решений в } \mathbb{Z}_5$$
$$2. b = 2a \Rightarrow a^2 - 8a^2 + 3 = 0 \Rightarrow 3a^2 = 3 \Rightarrow a^2 = 1 \Rightarrow a = 1; 4$$
$$\text{Пусть } a = 1 \Rightarrow b = 2 \Rightarrow \alpha = 2y+1$$

Тогда изоморфизм $F \simeq K$ задаётся формулой:

$$x \mapsto 2y+1$$
$$a_0 + a_1x \mapsto a_0 + a_1(2y+1)$$

Ответ:

$$x \mapsto 2y+1$$
$$a_0 + a_1x \mapsto a_0 + a_1(2y+1)$$

Задание 3

Перечислите все подполя поля $\mathbb{F}_{262144}$, в которых многочлен $x^3 + x^2 + 1$ имеет корень.

Решение:

$$\mathbb{F}_{262144} = \mathbb{F}_{2^{18}} \Rightarrow \mathbb{F}_{2^m} - \text{подполе, если } \ m \mid 18(\text{утверждение с семинара}) \Rightarrow$$
$$\mathbb{F}_2, \mathbb{F}_{2^2}, \mathbb{F}_{2^3}, \mathbb{F}_{2^6}, \mathbb{F}_{2^9}, \mathbb{F}_{2^{18}} - \text{все подполя.}$$

Заметим, что в $\mathbb{F}_2$ и в $\mathbb{F}_{2^2}$ многочлен не имеет корней, но имеет все три корня в $\mathbb{F}_{2^3}$. Тогда он также будет иметь корни в подполях, где степень двойки делится на 3(по утверждению выше). Итого, он имеет корни в подполях $\mathbb{F}_{2^3}, \mathbb{F}_{2^6}, \mathbb{F}_{2^9}, \mathbb{F}_{2^{18}}$

Ответ:

$\mathbb{F}_{2^3}, \mathbb{F}_{2^6}, \mathbb{F}_{2^9}, \mathbb{F}_{2^{18}}$

Задание 4

Пусть p — простое число, $q = p^n$ и $\alpha \in \mathbb{F}_q$. Докажите, что если многочлен $x^p - x - \alpha \in \mathbb{F}_q[x]$ имеет корень, то он разлагается на линейные множители.

Решение: