Домашнее задание на 17.06 (Алгебра)

Емельянов Владимир, ПМИ гр №247

№1 По условию

$$F_9 \;=\; \mathbb{Z}_3[x]\big/\big(x^2+2x+2\big),$$

Обозначим класс многочлена $a+bx$ через пару (a,b), где $a,b\in\{0,1,2\}$.

Так как в $\mathbb{Z}_3$ выполнено $-2\equiv 1 \pmod 3$, из уравнения $x^2+2x+2=0$ следует

$$x^2 \;\equiv\; -2x-2 \;\equiv\; x+1 \pmod 3$$

Порождающие элементы имеют порядок 8. Проверим, что для каждого элемента g:

$$g^1\neq 1,\quad g^2\neq 1,\quad g^4\neq 1.$$

Если это верно, то $g^8=1$, и g — порождающий.

(a) Элемент x:

$$\begin{aligned}
x^1 &= x\neq 1,\\
x^2 &= x+1\neq 1,\\
x^4 &= (x^2)^2=(x+1)^2=x^2+2x+1\\
&=(x+1)+2x+1=3x+2=2\neq 1
\end{aligned}$$

Значит, порядок x равен 8.

(b) Элемент $2x$:

$$\begin{aligned}
(2x)^1 &= 2x\neq 1,\\
(2x)^2 &= 4x^2=4(x+1)=4x+4=x+1\neq 1,\\
(2x)^4 &= (x+1)^2=2\neq 1
\end{aligned}$$

Порядок $2x$ равен 8.

(c) Элемент $x+2$:

$$(x+2)^1 = x+2 \neq 1,$$
$$(x+2)^2 = x^2+4x+4 = (x+1)+x+1 = 2x+2 \neq 1,$$
$$(x+2)^4 = (2x+2)^2 = 4x^2+8x+4 = 2 \neq 1$$

Порядок $x+2$ равен 8.

(d) Элемент $2x+1$:

$$(2x+1)^1 = 2x+1 \neq 1,$$
$$(2x+1)^2 = 4x^2+4x+1 = (x+1)+x+1 = 2x+2 \neq 1,$$
$$(2x+1)^4 = (2x+2)^2 = 2 \neq 1$$

Порядок $2x+1$ равен 8.

Остальные элементы: 1 (порядок 1), 2 (порядок 2), $x+1$ и $2x+2$ имеют порядок 4, так как $(x+1)^4 = 2^2 = 1$ и $(2x+2)^4 = 1$.

Ответ: $x, \quad 2x, \quad x+2, \quad 2x+1$

№2 Многочлен x^2+3 над $\mathbb{Z}_5$:

- $0^2+3 = 3 \neq 0$
- $1^2+3 = 4 \neq 0$
- $2^2+3 = 2 \neq 0$
- $3^2+3 = 2 \neq 0$
- $4^2+3 = 4 \neq 0$

Нет корней, следовательно, x^2+3 неприводим.

Многочлен y^2+y+2 над $\mathbb{Z}_5$:

- $0^2+0+2 = 2 \neq 0$

- $1^2 + 1 + 2 = 4 \neq 0$
- $2^2 + 2 + 2 = 3 \neq 0$
- $3^2 + 3 + 2 = 4 \neq 0$
- $4^2 + 4 + 2 = 2 \neq 0$

Нет корней, следовательно, $y^2 + y + 2$ неприводим.

Обозначим:

- α — корень $x^2 + 3 = 0$ в $\mathbb{Z}_5[x]/(x^2 + 3)$
- β — корень $y^2 + y + 2 = 0$ в $\mathbb{Z}_5[y]/(y^2 + y + 2)$

Найдём подстановку $\beta = a\alpha + b$, удовлетворяющую уравнению $\beta^2 + \beta + 2 = 0$.

После решения системы уравнений получаем два варианта:

- $\beta = \alpha + 2$
- $\beta = 4\alpha + 2$

Выберем $\beta = \alpha + 2$. Тогда изоморфизм $\varphi : \mathbb{Z}_5[x]/(x^2+3) \to \mathbb{Z}_5[y]/(y^2+y + 2)$ задаётся как:

$$\varphi(a + b\alpha) = a + b\beta = a + b(\alpha + 2)$$

Проверим

- $\beta^2 = (\alpha + 2)^2 = \alpha^2 + 4\alpha + 4 = 2 + 4\alpha + 4 = 4\alpha + 1,$
- $\beta^2 + \beta + 2 = (4\alpha + 1) + (\alpha + 2) + 2 = 5\alpha + 5 \equiv 0 \mod 5.$

Изоморфизм сохраняет операции сложения и умножения, так как β удовлетворяет требуемому уравнению.

Ответ: $\varphi(a + b\alpha) = a + b(\alpha + 2)$

№3 Поле $\mathbb{F}_{262144}$ имеет порядок 2^{18}. Подполя этого поля имеют порядки 2^d, где d — делитель 18. Делители 18: $1, 2, 3, 6, 9, 18$.

Соответствующие подполя:

$$\mathbb{F}_2, \quad \mathbb{F}_4, \quad \mathbb{F}_8, \quad \mathbb{F}_{64}, \quad \mathbb{F}_{512}, \quad \mathbb{F}_{262144}$$

Проверим наличие корней в подполях

(a) Подполе $\mathbb{F}_2$

Многочлен $x^3 + x^2 + 1$ в $\mathbb{F}_2[x]$:

- $f(0) = 0 + 0 + 1 = 1 \neq 0$
- $f(1) = 1 + 1 + 1 = 3 \equiv 1 \neq 0$

Корней нет

(b) Подполе $\mathbb{F}_4$

Представим $\mathbb{F}_4$ как $\mathbb{F}_2[\alpha]/(\alpha^2 + \alpha + 1)$. Элементы: $0, 1, \alpha, \alpha + 1$.

- $f(0) = 1 \neq 0$
- $f(1) = 1 \neq 0$
- $f(\alpha) = \alpha^3 + \alpha^2 + 1 = (\alpha + 1) + \alpha + 1 = 1 \neq 0$ (используя $\alpha^2 = \alpha + 1$)
- $f(\alpha + 1) = (\alpha + 1)^3 + (\alpha + 1)^2 + 1 = \alpha + 1 \neq 0$

Корней нет

(c) Подполе $\mathbb{F}_8$

Многочлен $x^3 + x^2 + 1$ неприводим над $\mathbb{F}_2$ (нет корней в $\mathbb{F}_2$). Следовательно, $\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3 + x^2 + 1)$, и корень многочлена существует в $\mathbb{F}_8$

Корень есть

(d) Большие подполя

Подполя $\mathbb{F}_{64}$, $\mathbb{F}_{512}$, $\mathbb{F}_{262144}$ содержат $\mathbb{F}_8$ (поскольку их порядки кратны $8 = 2^3$). Корень из $\mathbb{F}_8$ автоматически принадлежит этим подполям.

Корень существует

Ответ: $\mathbb{F}_8, \mathbb{F}_{64}, \mathbb{F}_{512}, \mathbb{F}_{262144}$

№4 Пусть $\beta \in \mathbb{F}_q$ — корень многочлена $f(x) = x^p - x - \alpha$.

Тогда:

$$\beta^p - \beta = \alpha$$

В поле характеристики p выполняется тождество $(a+b)^p = a^p + b^p$. Для любого $c \in \mathbb{F}_p$:

$$(\beta + c)^p - (\beta + c) = \beta^p + c^p - \beta - c$$

Поскольку $c \in \mathbb{F}_p$, по малой теореме Ферма $c^p = c$. Тогда:

$$(\beta + c)^p - (\beta + c) = \beta^p - \beta = \alpha$$

Это означает, что $\beta + c$ также является корнем $f(x)$

Так как $\beta \in \mathbb{F}_q$ и $c \in \mathbb{F}_p \subseteq \mathbb{F}_q$, все элементы вида $\beta + c$ принадлежат $\mathbb{F}_q$.

Множество

$$\{\beta + c \mid c \in \mathbb{F}_p\}$$

содержит ровно p различных элементов (поскольку $\beta + c_1 = \beta + c_2 \Rightarrow c_1 = c_2$).

Таким образом, многочлен $f(x)$ имеет p корней в $\mathbb{F}_q$, и его можно разложить на линейные множители:

$$f(x) = \prod_{c \in \mathbb{F}_p} (x - (\beta + c))$$