Бурмашев Григорий. Алгебра – 9

[ПОСЛЕДНЯЯ]

Номер 1

Расписываем $\mathbb{F}_9$:

$$\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2 + 2x + 2 = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

Заметим, что $x^2 + 2x + 2$ неприводим, т.к у него нет корней

Формула понижения степени:

$$x^2 = x + 1$$

Составим таблицу умножения для $\mathbb{F}_9$:

·	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
2	0	2	1	2x	2x+2	2x+1	x	x+2	x+1
x	0	x	2x	x+1	2x+1	1	2x+2	2	x+2
x +1	0	x+1	2x+2	2x+1	2	x	x+2	2x	1
x + 2	0	x+2	2x+1	1	x	2x+2	2	x+1	2x
2x	0	2x	x	2x+2	x+2	2	x+1	1	2x+1
2x + 1	0	2x+1	x+2	2	2x	x+1	1	2x+2	x
2x + 2	0	2x+2	x+1	x+2	1	2x	2x+1	x	2

Из лекции знаем, что $\forall a \in F_q$ a является корнем многочлена $x^q - x$, а значит $a^{q-1} = 1$, в нашем случае $q = 9$, а значит $a^8 = 1$ и нас интересуют элементы порядка 8, нужно их найти

А теперь для каждого элемента возводим его в степень, пока не придем в единицу. Для возведения будем просто идти по таблице умножения до тех пор, пока не упремся в 1. Таким образом и посчитаем порядок каждого элемента.

Через $\to$ обозначаю возведение исходного числа в очередную степень (т.е x^2 будет $x \to x+1$ соотвественно)

- 0:

  Нас не интересует, т.к не является порождающим

- 1:

  $$1^1 = 1$$

  Т.е порядок 1

- 2:

  $$2 \to 1$$

  Т.е порядок 2

- x:

  $$x \to x+1 \to 2x+1 \to 2 \to 2x \to 2x+2 \to x+2 \to 1$$

  Т.е порядок 8

- $x+1$:

  $$x+1 \to 2 \to 2x+2 \to 1$$

  Т.е порядок 4

- $x+2$:

  $$x+2 \to 2x+2 \to 2x \to 2 \to 2x+1 \to x+1 \to x \to 1$$

  Т.е порядок 8

- $2x$:

  $$2x \to\to x+1 \to x+2 \to 2 \to x \to 2x+2 \to 2x+1 \to 1$$

  Т.е порядок 8

- $2x + 1$:

$$2x + 1 \to 2x + 2 \to x \to 2 \to x + 2 \to x + 1 \to 2x \to 1$$

Т.е порядок 8

- $2x + 2$:

$$2x + 2 \to 2 \to x + 1 \to 1$$

Т.е порядок 4

Посчитали все порядки, по итогу:

Элемент:	Порядок:
1	1
2	2
x	8
x+1	4
x+2	8
2x	8
2x+1	8
2x+2	4

Берем только те, у которых порядок 8

Ответ:

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

Номер 2

Задача с семинара, поэтому делаю как на семинаре:

$$p = 5, n = 2$$
$$h_1 = x^2 + 3$$
$$h_2 = y^2 + y + 2$$

Для начала сделаем легкую часть, проверим на приводимость:

В $\mathbb{Z}_5$ возможные корни:

$$0, 1, 2, 3, 4$$

Проверяем:

- h_1:

$$h_1(0) = 3$$
$$h_1(1) = 4$$
$$h_1(2) = 4 + 3 = 2$$
$$h_1(3) = 4 + 3 = 2$$
$$h_1(4) = 1 + 3 = 4$$

- h_2:

$$h_2(0) = 2$$
$$h_2(1) = 1 + 1 + 2 = 4$$
$$h_2(2) = 4 + 2 + 2 = 3$$
$$h_2(3) = 4 + 3 + 2 = 4$$
$$h_2(4) = 1 + 4 + 2 = 2$$

Нигде не получили нулей, значит они действительно неприводимы над $\mathbb{Z}_5$

Нам нужно построить явно изоморфизм вида:

$$F_1 = \mathbb{Z}_5/(h_1) \simeq F_2 = \mathbb{Z}_5/(h_2)$$

$$\exists \alpha \in F_2 : h_1(\alpha) = 0$$

Гомоморфизм:

$$\varphi : \mathbb{Z}_5[x] \to F_2$$
$$f \Rightarrow f(\alpha)$$

На лекции доказывалось, что:

$$h_1 \in \mathrm{Ker}\varphi \rightsquigarrow \mathrm{Ker}\varphi = (h_1)$$

Теорема о гомоморфизме $\Rightarrow$ изоморфизм вида:

$$F_1 = \mathbb{Z}_p[x]/(h_1) \simeq \mathrm{Im}\varphi \subseteq F_2$$

В F_1 лежит q элементов, в F_2 тоже q, тогда получается, что образ тоже содержит q элементов, а тогда образ совпадает с F_2 и мы действительно получаем изоморфизм.

Остается найти такое $\alpha \in F_2 : h_1(\alpha) = 0$

Знаем, что в F_2:

$$y^2 = -y - 2 = 4y + 3$$

Теперь находим α:

$$\alpha = a\overline{y} + b$$
$$h_1(\alpha) = (a\overline{y} + b)^2 + 3 = a^2\overline{y}^2 + 2a\overline{y}b + b^2 + 3 = 0$$

Пользуемся фактом про понижение степени:

$$a^2(4\overline{y} + 3) + 2a\overline{y}b + b^2 + 3 = 0$$
$$4a^2\overline{y} + 3a^2 + 2a\overline{y}b + b^2 + 3 = 0$$
$$\overline{y}(4a^2 + 2ab) + (3a^2 + b^2 + 3) = 0$$

Получаем СЛУ:

$$\begin{cases} 4a^2 + 2ab = 0 \\ 3a^2 + b^2 + 3 = 0 \end{cases}$$
$$\begin{cases} 2a(2a + b) = 0 \\ 3a^2 + b^2 + 3 = 0 \end{cases}$$

Пытаемся угадать вариант, их не так уж и много в рамках $\mathbb{Z}_5$

- $a = 1$:

$$\begin{cases} 2(2 + b) = 0 \\ b^2 + 1 = 0 \end{cases}$$
$$\begin{cases} b = 3 \\ b^2 + 1 = 3^2 + 1 = 4 + 1 = 0 \end{cases}$$

Все выполняется, а значит угадывание можно останавливать и нам подходит вариант вида:

$$\alpha = \overline{y} + 3$$

Ответ:
изоморфизм $F_1 \simeq F_2$ определяется так:

$$a\overline{x} + b \to a(\overline{y} + 3) + b$$

Вот и всё :(