

Домашнее задание по алгебре

Родигина Анастасия, 167 группа

7 мая 2017

Задача 1

Постройте явно поле \mathbb{F}_8 и составьте для него таблицы сложения и умножения.

Реализуем наше поле как $\mathbb{Z}_2[x]/(x^3 + x + 1)$, где $x^3 + x + 1$ – неприводимый многочлен над \mathbb{Z}_2 .

Таким образом, наше факторкольцо будет являться полем – его элементами будут классы:

$\bar{0}, \bar{1}, \bar{x}, \overline{x+1}, \overline{x^2}, \overline{x^2+1}, \overline{x^2+x}, \overline{x^2+x+1}$

Сделаем для нашего поля таблицу сложения:

+	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$
$\overline{x^2}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\overline{x^2+1}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}
$\overline{x^2+x}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x^2+x+1}$	$\overline{x^2+x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$

Теперь построим таблицу умножения (будем пользоваться тем, что $\overline{x^3} = \overline{x+1}$ и $\overline{x^4} = \overline{x+x^2}$):

\times	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\overline{x^2}$	$\overline{x^2+1}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$
\bar{x}	$\bar{0}$	\bar{x}	$\overline{x^2}$	$\overline{x^2+x}$	$\overline{x+1}$	$\bar{1}$	$\overline{x^2+x+1}$	$\overline{x^2+1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2+1}$	$\overline{x^2+x+1}$	$\overline{x^2}$	$\bar{1}$	\bar{x}
$\overline{x^2}$	$\bar{0}$	$\overline{x^2}$	$\overline{x+1}$	\bar{x}	$\overline{x^2+x}$	\bar{x}	$\overline{x^2+1}$	$\bar{1}$
$\overline{x^2+1}$	$\bar{0}$	$\overline{x^2+1}$	$\bar{1}$	$\overline{x^2}$	\bar{x}	$\overline{x^2+x+1}$	$\overline{x+1}$	$\overline{x^2+x}$
$\overline{x^2+x}$	$\bar{0}$	$\overline{x^2+x}$	$\overline{x^2+x+1}$	$\bar{1}$	$\overline{x^2+1}$	$\overline{x+1}$	$\overline{x^2+x}$	$\overline{x^2}$
$\overline{x^2+x+1}$	$\bar{0}$	$\overline{x^2+x+1}$	$\overline{x^2+1}$	\bar{x}	$\bar{1}$	$\overline{x^2+x}$	$\overline{x^2}$	$\overline{x^2+x+1}$

Задача 2

Реализуем поле \mathbb{F}_9 в виде $\mathbb{Z}_3[x]/(x^2 + 1)$. Перечислите в этой реализации все элементы данного поля, являющиеся порождающими циклической группы \mathbb{F}_9^\times .

Выпишем все элементы поля в данной реализации:

$$0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$$

Для каждого элемента запишем его степени (все и при этом попарно различные) в этом поле и проверим, будет ли он искомым порождающим элементом:

$$0 \Rightarrow \{0\}$$

$$1 \Rightarrow \{1\}$$

$$2 \Rightarrow \{2, 1\}$$

$$x \Rightarrow \{x, 2, 2x, 1\}$$

$$x + 1 \Rightarrow \{x + 1, 2x, 2x + 1, 2, 2x + 2, x, x + 2, 1\}$$

$$x + 2 \Rightarrow \{x + 2, x, 2x + 2, 2, 2x + 1, 2x, x + 1, 1\}$$

$$2x \Rightarrow \{2x, 2, x, 1\}$$

$$2x + 1 \Rightarrow \{2x + 1, x, x + 1, 2, x + 2, 2x, 2x + 2, 1\}$$

$$2x + 2 \Rightarrow \{2x + 2, 2x, x + 2, 2, x + 1, x, 2x + 1, 1\}$$

Таким образом порождающими элементами могут быть только $x + 1, 2x + 2, 2x + 1$ и $x + 2$ (к их степеням добавим нулевой элемент и все будет как надо:)).

Задача 3

Проверьте, что многочлены $x^2 + 1$ и $y^2 - y - 1$ неприводимы над \mathbb{Z}_3 , и установите явно изоморфизм между полями $\mathbb{Z}_3[x]/(x^2 + 1)$ и $\mathbb{Z}_3[y]/(y^2 - y - 1)$.

Для того, чтобы проверить данные многочлены на неприводимость достаточно проверить, будет ли он равен 0 при $x \in \{0, 1, 2\}$. Обозначим за $f(x)$: $x^2 + 1$, а за $g(y)$: $y^2 - y - 1$. Достаточно легко заметить:

$$f(0) = 1; \quad f(1) = 2; \quad f(2) = 2; \quad g(0) = 2; \quad g(1) = 2; \quad g(2) = 1$$

Следовательно наш многочлен не будет раскладываться на линейные множители над \mathbb{Z}_3 , т.е. будет неприводимым. Теперь построим гомоморфизм между двумя этими полями:

Давайте писать вместо второго многочлена: $x_2^2 - x_2 - 1 = x_2^2 + 2x_2 + 2$ (просто добавим слагаемые, которые обнулятся.)

Возьмем такой изоморфизм:

$$\varphi : \mathbb{F} \rightarrow \mathbb{F}'$$

Пусть

$$\varphi(1_2) = 1; \quad \varphi(x_2) = z; \quad \varphi(x_2^2) = z^2$$

То есть:

$$\varphi(ax_2^2 + bx_2 + c) = az^2 + bz + c$$

$$\varphi(x_2^2 + 2x_2 + 2) = z^2 + 2z + 2$$

Пусть

$$\varphi(x_1) = x_2 + 1; \quad \varphi(1) = 1$$

Тогда:

$$\varphi(x_1^2 + 1) = (x_2 + 1)^2 + 1 = x_2^2 + 2x_2 + 2 = 0$$

Получаем с точностью до единств. изоморфизм $\varphi(x_1) = x_2 + 1; \quad \varphi(1) = 1$.

Задача 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.

Воспользуемся фактом, что $(a + b)^p = a^p + b^p$ в данном поле. Пусть λ – корень данного многочлена, а .