Д/з - 9

Чистяков Глеб, группа 167

13 июня 2017 г.

№1

$\mathbb{F}_8 = \mathbb{F}_{2^3} = \mathbb{F}_2[x]/(f(x))$, где $f(x)$ – неприводимый над $\mathbb{F}_2$ и $deg(f(x)) = 3$.
Перечислим все многочлены:
- x^3 – приводимый
- $x^3 + 1$ – приводимый
- $x^3 + x$ – приводимый
- $x^3 + x^2$ – приводимый
- $x^3 + x + 1$ – неприводимый
- $x^3 + x^2 + 1$ – неприводимый
- $x^3 + x^2 + x$ – приводимый
- $x^3 + x^2 + x + 1$ – приводимый

Рассмотрим $S(x) + (x^3 + x + 1)$, где $S(x)$: $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

$\times$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	1	x^2+1	1
x^2+1	0	x^2+1	1	x^2	1	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+1	x^2	$x+1$

№2

Реализуем поле $\mathbb{F}_9$ в виде $\mathbb{Z}_3[x]/(x^2+1)$. А теперь рассмотрим элементы, являющиеся порождающими циклической группы $\mathbb{F}_9^\times$:
Порядки каждого элемента, за исключением нуля, будут:
- $1^1 = 1$
- $2^2 = 4 = 1$
- $x^4 = 1$
- $(x+1)^8 = 1$
- $(x+2)^8 = 1$
- $(2x)^4 = 1$
- $(2x+1)^8 = 1$
- $(2x+2)^8 = 1$

В силу того, что мы можем рассматривать $\mathbb{F}_9 \cong \mathbb{Z}_8$, то порождающими элементами циклической группы $\mathbb{F}_9^\times$ будут элементы порядка 8, а именно – $x+1, x+2, 2x+1, 2x+2$.

№3

Проверим многочлены x^2+1 и y^2-y-1 на неприводимость над $\mathbb{Z}[3]$:
Подставляем $0, 1, 2$ и видим, что они не являются корнями этих многочленов $\Rightarrow$ многочлены неприводимые.

Установим изоморфизм $\mathbb{Z}_3[x]/(x^2+1) \cong \mathbb{Z}_3[y]/(y^2-y-1)$:
$0 \longrightarrow 0$
$1 \longrightarrow 1$
$2 \longrightarrow 2$
$x \longrightarrow a$
Здесь нам достаточно рассмотреть только x, так как если $x \longrightarrow a$, то $x^2+1 \longrightarrow a^2+1$, то есть мы сможем так выразить все элементы.
Рассмотрим $x^2+1=0$, то есть $a^2+1=0$: пусть $a = y+1 \Rightarrow$
$(y+1)^2+1 = 0 \Leftrightarrow y^2+2y+2 = 0 \Leftrightarrow y^2-y-1=0$
Таким образом, мы явно установили изоморфизм $\mathbb{Z}_3[x]/(x^2+1) \cong \mathbb{Z}_3[y]/(y^2-y-1)$.