Домашнее задание по алгебре №9.

Михайлов Никита Маратович, ПМИ-167.

Задание 1.

Постройте явно поле $\mathbb{F}_8$ и составьте для него таблицы сложения и умножения.
Решение. Заметим, что $8 = 2^3$. Следовательно, нам подойдет поле $\mathbb{Z}_2[x]/(x^3+x^2+1)$, т.к. x^3+x^2+1 – неприводим над $\mathbb{Z}_2$. Элементами поля будут многочлены вида $ax^2 + bx + x, a, b, c \in \mathbb{Z}_2$. Построим таблицу сложения:

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

А теперь умножения:

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

Задание 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 $\mathbb{F}_9^\times$.
Решение. Решим в лоб. Построим таблицу умножения:

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

Выпишем элементы, порядок которых равен 8: $x+1, x+2, 2x+1, 2x+2$ – эти элементы и будут порождающими.

Задание 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 $\mathbb{Z}_3[y]/(y^2-y-1)$.
Решение. Так как поле конечно и достаточно маленькое. Давайте просто попробуем подобрать корни для

$x^2 + 1 = 0$. Числа 0, 1, 2 – не подходят. Заметим, что $y^2 - x - 1 = y^2 + 2x + 2 = (y+1)^2 + 1$ – аналогичная ситуация. Корней нет.
Построим таблицу умножения и сделаем там, чтобы элементы одного порядке переходили друг в друга с выполнением линейности(коэфициенты перед x и y одинаковые, чтобы сохранить линейность):

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

1. $\varphi(0) = 0$
2. $\varphi(1) = 1$
3. $\varphi(2) = 2$
4. $\varphi(x) = y + 1$
5. $\varphi(x+1) = y + 2$
6. $\varphi(x+2) = y$
7. $\varphi(2x) = 2y + 2$
8. $\varphi(2x+1) = 2y$
9. $\varphi(2x+2) = 2y + 1$

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.