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

Предложение. G — циклическая группа, $|G| = n < \infty \Rightarrow G \simeq (\mathbb{Z}_n, +)$.

Решение.

$\mathbb{F}_9^{\times} = \mathbb{F}_9 \backslash \{0\} \Rightarrow |\mathbb{F}_9| = 8$.

Тогда, если g принадлежит группе, то $ord(g) = |<g>| \Rightarrow$ множество порождающих элементов $\mathbb{F}_9^{\times}$ то же самое, что и множество элементов порядка 8. Теперь выпишем саму циклическую подгруппу, порождаемую x.

Рассматриваем ${\mathbb{Z}_3}/{(x^2+x+2)}$ с формулой понижения степени: $x^2+x+2=0 \Rightarrow x^2 = -x-2 \Rightarrow x^2 = 2x+1$;

1) $x^1 = x$ 2) $x^2 = 2x+1$ 3) $x^3 = 2x^2 + x = 2(2x+1) + x = 2x+2$ 4) $x^4 = (2x+2)x = 2$
5) $x^5 = 2x$ 6) $2(2x+1) = x+2$ 7) $x^7 = (x+2)x = x+1$ 8) $(x+1)x = 1$

Значит $ord(x)$ действительно 8, и x действительно порождающий.

2. Проверьте, что многочлены $\underbrace{x^2+3}_{f(x)}$ и $\underbrace{y^2+y+1}_{g(y)}$ неприводимы над $\mathbb{Z}_5$, и установите явно изиморфизм между полями $\underbrace{{\mathbb{Z}_5[x]}/{(x^2+3)}}_{F_1}$ и $\underbrace{{\mathbb{Z}_5[y]}/{(y^2+y+1)}}_{F_2}$.

Решение.

Работаем в $\mathbb{Z}_5$:

$f(0) = 3 \neq 0,\quad g(0) = 1 \neq 0;$
$f(1) = 4 \neq 0,\quad g(1) = 3 \neq 0;$
$f(2) = 2 \neq 0,\quad g(2) = 2 \neq 0;$
$f(3) = 2 \neq 0,\quad g(3) = 3 \neq 0;$
$f(4) = 4 \neq 0,\quad g(4) = 1 \neq 0;$

Значит многочлены f и g действительно неприводимы. А ${\mathbb{Z}_5[x]}/{(x^2+3)}$ и ${\mathbb{Z}_5[y]}/{(y^2+y+1)}$ — поля, содержащие по 25 элементов $\Rightarrow F_1 \simeq F_2$. Теперь посторим собственно этот изоморфизм.

Известно, что $\exists \alpha \in F_2$, т. что $f(\alpha) = 0$.

Рассматриваем следующее отображение(гомоморфизм колец): $\mathbb{Z}_5[x] \to F_2, \quad f \to f(\alpha)$.

$Ker\varphi = (h), \quad f(\alpha) = 0 \Rightarrow f \in Ker\varphi \Rightarrow h|f$. Но мы то знаем, что f неприводим $\Rightarrow$

$\left[\begin{array}{l} h = const \text{ — не подходит, так как все многочлены переходили бы в ноль;} \\ h \text{ пропорционален } f \Rightarrow Ker\varphi = (f) \end{array}\right. ; \Rightarrow$
применяем теорему о гомоморфизме: $\exists$ изморфизм $f \to f(\alpha)$:

$\underbrace{{\mathbb{Z}_5[x]}/{(x^2+3)}}_{F_1} \simeq Im\varphi \subseteq F_2$(так как в них по 25 элементов) $\Rightarrow Im\varphi = F_2$.

Осталось только найти $\alpha \in F_2$, такой что $f(\alpha) = 0$ и дело в шляпе. $\alpha = a\overline{y} + b, \quad a, b \in \{0,1,2,3,4\}$.

$f(\alpha) = (a\overline{y} + b)^2 + 3 = 0, \qquad y^2 = -y - 1 = 4y + 4$

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

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

$\begin{cases} 4a^2 + 2ab = 0 \\ 4a^2 + b^2 + 3 = 0 \end{cases} \to \begin{cases} 4a^2 = -2ab \\ 4a^2 + b^2 + 3 = 0 \end{cases} \to \begin{cases} b = 3a \\ 4a^2 + b^2 + 3 = 0 \end{cases} \to \begin{cases} 4a^2 + 9a^2 + 3 = 0 \\ b = 3a \end{cases} \to \begin{cases} 3a^2 = -3 \\ b = 3a \end{cases} \to \begin{cases} a = 2 \\ b = 1 \end{cases} \Rightarrow$

$\alpha = 2\overline{y} + 1 \Rightarrow$ изоморфизм $F_1 \simeq F_2$ выглядит: $a + b\overline{x} \to a + (2\overline{y} + 1)$

3. Перечислите все подполя поля $\mathbb{F}_{262144}$, в которых многочлен $x^3 + x^2 + 1$ имеет корень.

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.