Задача 1. Показать, что многочлен $f(x) = x^4 + x^3 + 1$ неприводим над полем $\mathbb{F}_2$. Описать все элементы поля $\mathbb{F}_{16}$, полученного расширением поля $\mathbb{F}_2$ при помощи корня ξ многочлена $f(x)$. Найти минимальные многочлены элементов ξ, ξ^{-1}, ξ^5. Какие из этих элементов являются примитивными?

Решение. Предположим противное: многочлен $f(x)$ не является примитивным. Тогда либо

$$f(x) = (x^2 + a_1x + a_2)(x^2 + b_1x + b_2),$$

либо

$$f(x) = (x - c)(x^3 + d_1x^2 + d_2x + d_3)$$

для некоторых $a_1, a_2, b_1, b_2, c, d_1, d_2, d_3 \in \mathbb{F}_2$. Легко проверить, что $f(0) \neq 0$, $f(1) \neq 0$, следовательно, второе невозможно. Преобразовывая первое равенство, имеем

$$f(x) = x^4 + (a_1 + b_1)x^3 + (a_1b_1 + a_2 + a_3)x^2 + (a_1b_2 + a_2b_1)x + a_2b_2.$$

Следовательно, $a_1 + b_1 = 1$, $a_1b_1 + a_2 + b_2 = 0$, $a_1b_2 + a_2b_1 = 0$, $a_2b_2 = 1$. Из четвертого равенства следует, что $a_2 = b_2 = 1$. Тогда третье равенство перепишется в виде $a_1 + b_1 = 0$, что противоречит первому равенству.

Проверим, является ли многочлен $f(x)$ (элемент ξ) примитивным. Для этого найдем порядок $|\xi|$ элемента ξ. Многочлен $f(x)$ (элемент ξ) будет примитивным тогда и только тогда, когда
$|\xi| = 2^4 - 1 = 15$. Учитывая, что $\xi^4 = -\xi^3 - 1 = \xi^3 + 1$ и $\xi^n + \xi^n = 0$ для любого $n \in \{0, 1, 2, 3, 4\}$ над полем $\mathbb{F}_2$, имеем:

$$\begin{aligned}
&\xi^0 = 1,\\
&\xi^1 = \xi,\\
&\xi^2 = \xi^2,\\
&\xi^3 = \xi^3,\\
&\xi^4 = \xi^3 + 1,\\
&\xi^5 = \xi\xi^4 = \xi^4 + \xi = (\xi^3 + 1) + \xi = \xi^3 + \xi + 1,\\
&\xi^6 = \xi\xi^5 = \xi^4 + \xi^2 + \xi = (\xi^3 + 1) + \xi^2 + \xi = \xi^3 + \xi^2 + \xi + 1,\\
&\xi^7 = \xi\xi^6 = \xi^4 + \xi^3 + \xi^2 + \xi = (\xi^3 + 1) + \xi^3 + \xi^2 + \xi = \xi^2 + \xi + 1,\\
&\xi^8 = \xi\xi^7 = \xi^3 + \xi^2 + \xi,\\
&\xi^9 = \xi\xi^8 = \xi^4 + \xi^3 + \xi^2 = (\xi^3 + 1) + \xi^3 + \xi^2 = \xi^2 + 1,\\
&\xi^{10} = \xi\xi^9 = \xi^3 + \xi,\\
&\xi^{11} = \xi\xi^{10} = \xi^4 + \xi^2 = (\xi^3 + 1) + \xi^2 = \xi^3 + \xi^2 + 1,\\
&\xi^{12} = \xi\xi^{11} = \xi^4 + \xi^3 + \xi = (\xi^3 + 1) + \xi^3 + \xi = \xi + 1,\\
&\xi^{13} = \xi\xi^{12} = \xi^2 + \xi,\\
&\xi^{14} = \xi\xi^{13} = \xi^3 + \xi^2,\\
&\xi^{15} = \xi\xi^{14} = \xi^4 + \xi^3 = (\xi^3 + 1) + \xi^3 = 1,
\end{aligned}$$

Таким образом, $|\xi| = 15$ и, значит, многочлен $f(x)$ (элемент ξ) примитивен.

Поле $\mathbb{F}_{16} = \mathbb{F}_{2^4} = \mathbb{F}_2(\xi)$ представляет собой множество

$$\{g(\xi) = a\xi^3 + b\xi^2 + c\xi + d \mid a, b, c, d \in \mathbb{F}_2\},$$

где элементы $g_1(\xi), g_2(\xi) \in \mathbb{F}_{16}$ умножаются по правилу $g_1(\xi) \cdot g_2(\xi) = \operatorname{res}(g_1(\xi)g_2(\xi)/f(\xi))$. Кроме того, для каждого $g(\xi) \in \mathbb{F}_{16}$ существует $g^{-1}(\xi) \in \mathbb{F}_{16}$, что $g(\xi) \cdot g^{-1}(\xi) = 1$. Поле $\mathbb{F}_{16}$ можно рассматривать как линейное пространство над полем $\mathbb{F}_2$ с базисом $1, \xi, \xi^2, \xi^3$.

Поскольку элемент ξ примитивен, то он порождает мультипликативную группу $\mathbb{F}_{16}^*$ поля $\mathbb{F}_{16}$, т.е.

$$\begin{aligned}
\mathbb{F}_{16}^* &= \langle\xi\rangle = \{1, \xi, \xi^2, \xi^3, \dots, \xi^{14}\},\\
\mathbb{F}_{16} &= \{0, 1, \xi, \xi^2, \xi^3, \dots, \xi^{14}\}.
\end{aligned}$$

Причем $\xi^k = \xi^{\operatorname{res}(k/15)}$ для любого $k \in \mathbb{N} \cup \{0\}$, $\xi^{-n} = \xi^{15-n}$ для любого $n \in \{1, 2, \dots, 14\}$. Выше каждый элемент поля $\mathbb{F}_{16}$ представлен и как степень ξ элемента, и как многочлен из $\mathbb{F}_2[\xi]$.

Минимальным многочленом элемента α поля $\mathbb{F}_{16}$ является многочлен

$$M_\alpha(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)\dots(x - \alpha^{2^{k-1}}),$$

где k — наименьшее натуральное число, такое, что $\alpha^{2^k} = \alpha$, т.е. $|\alpha| = 2^k - 1$ (утверждение **??**).

Поскольку $|\xi| = 2^4 - 1$, то $\deg M_\xi(x) = 4$. Кроме того, $f(\xi) = 0$, значит, многочлен $M_\xi(x)$ делит $f(x)$ и, следовательно, $M_\xi(x) = f(x)$.

Пусть $\beta = \xi^{-1} = \xi^{14}$. Тогда $\beta^2 = \xi^{28} = \xi^{13}$, $\beta^4 = (\xi^2)^2 = \xi^{26} = \xi^{11}$, $\beta^8 = (\xi^4)^2 = \xi^{22} = \xi^7$, $\beta^{16} = (\xi^8)^2 = \xi^{14} = \beta$. Таким образом, $\beta^{2^4} = \beta$, поэтому $k = \deg M_\beta(x) = 4$ и

$$\begin{aligned}
M_\beta(x) &= (x - \beta)(x - \beta^2)(x - \beta^4)(x - \beta^8) =\\
&= x^4 - (\beta + \beta^2 + \beta^4 + \beta^8)x^3 +\\
&+ (\beta\beta^2 + \beta\beta^4 + \beta\beta^8 + \beta^2\beta^4 + \beta^2\beta^8 + \beta^4\beta^8)x^2 -\\
&- (\beta^2\beta^4\beta^8 + \beta\beta^4\beta^8 + \beta\beta^2\beta^8 + \beta\beta^2\beta^4)x + \beta\beta^2\beta^4\beta^8 =\\
&= x^4 - (\xi^{14} + \xi^{13} + \xi^{11} + \xi^7)x^3 +\\
&+ (\xi^{12} + \xi^{10} + \xi^6 + \xi^9 + \xi^5 + \xi^3)x^2 + + (\xi + \xi^2 + \xi^4 + \xi^8)x + 1 =\\
&= x^4 + [(\xi^3 + \xi^2) + (\xi^2 + \xi) + (\xi^3 + \xi^2 + 1) + (\xi^2 + \xi + 1)]x^3 +\\
&+ [(\xi + 1) + (\xi^3 + \xi) + (\xi^3 + \xi^2 + \xi + 1) + (\xi^2 + \xi + 1) +\\
&+ (\xi^3 + \xi + 1) + \xi^3]x^2 + [\xi + \xi^2 + (\xi^3 + 1) +\\
&+ (\xi^3 + \xi^2 + \xi)]x + 1 = x^4 + x + 1.
\end{aligned}$$

Проверка:

$$M_\beta(\beta) = \beta^4 + \beta + 1 = \xi^{11} + \xi^{14} + 1 =$$
$$= (\xi^3 + \xi^2 + 1) + (\xi^3 + \xi^2) + 1 = 0.$$

Поскольку $|\beta| = 2^4 - 1 = 15$, то элемент β является примитивным.

Пусть $\gamma = \xi^5$. Тогда $\gamma^2 = \xi^{10}$, $\gamma^4 = (\xi^2)^2 = \xi^{20} = \xi^5$, Таким образом, $\gamma^{2^2} = \gamma$, поэтому $k = \deg M_\gamma(x) = 2$ и

$$M_\gamma(x) = (x - \gamma)(x - \gamma^2) =$$
$$= x^2 - (\gamma + \gamma^2)x + \gamma\gamma^2 = x^2 - (\xi^5 + \xi^{10})x + 1 =$$
$$x^2 + [(\xi^3 + \xi + 1) + (\xi^3 + \xi)]x + 1 =$$
$$= x^2 + x + 1.$$

Поскольку $|\gamma| = 2^2 - 1 = 3$, то элемент γ не является примитивным.

Ответ. Минимальные многочлены элементов ξ, ξ^{-1}, ξ^5 — это многочлены $f(x), x^4+x+1, x^2+x+1$ соответственно. Элементы ξ, ξ^{-1} являются примитивными, а элемент ξ^5 — нет.

Задача 2. Показать, что многочлен $f(x) = x^2 + x + 2$ неприводим над полем $\mathbb{F}_3$. Описать все элементы поля $\mathbb{F}_9$, полученного расширением поля $\mathbb{F}_3$ при помощи корня ξ многочлена $f(x)$. Доказать, что элемент ξ примитивен и найти минимальные многочлены для элементов $\xi + 2$, $(2\xi + 1)^{-1}$. Являются ли они примитивными?

Решение. Предположим противное: многочлен $f(x)$ не является примитивным. Тогда $f(x) = (x - a)(x - b)$ для некоторых $a, b \in \mathbb{F}_3$. Непосредственная проверка показывает, что $f(0) \neq 0$, $f(1) \neq 0$, $f(2) \neq 0$, следовательно, наше предположение неверно. Докажем, что многочлен $f(x)$ (элемент ξ) примитивный. Многочлен $f(x)$ (элемент ξ) будет примитивным тогда и только тогда, когда $|\xi| = 3^2 - 1 =$
$= 8$. Учитывая, что $\xi^2 = -\xi - 2 = 2\xi + 1$, $m\xi^n = \mathrm{res}\,(m/4)\xi^n$ для любых $m, n \in \mathbb{N} \cup \{0\}$ над полем $\mathbb{F}_3$,
имеем:

$$\xi^0 = 1,$$
$$\xi^1 = \xi,$$
$$\xi^2 = 2\xi + 1$$
$$\xi^3 = \xi\xi^2 = 2\xi^2 + \xi = 2(2\xi + 1) + \xi = 5\xi + 2 = 2\xi + 2,$$
$$\xi^4 = \xi\xi^3 = 2\xi^2 + 2\xi = 2(2\xi + 1) + 2\xi = 6\xi + 2 = 2,$$
$$\xi^5 = \xi\xi^4 = 2\xi,$$
$$\xi^6 = \xi\xi^5 = 2\xi^2 = 2(2\xi + 1) = 4\xi + 2 = \xi + 2,$$
$$\xi^7 = \xi\xi^6 = \xi^2 + 2\xi = (2\xi + 1) + 2\xi = 4\xi + 1 = \xi + 1,$$
$$\xi^8 = \xi\xi^7 = \xi^2 + \xi = (2\xi + 1) + \xi = 3\xi + 1 = 1.$$

Таким образом, $|\xi| = 8$ и, значит, многочлен $f(x)$ (элемент ξ) примитивен.

Поле $\mathbb{F}_9 = \mathbb{F}_{3^2} = \mathbb{F}_3(\xi)$ представляет собой множество

$$\{g(\xi) = a\xi + b \mid a, b \in \mathbb{F}_3\},$$

где элементы $g_1(\xi), g_2(\xi) \in \mathbb{F}_9$ умножаются по правилу $g_1(\xi) \cdot g_2(\xi) =$
$= \mathrm{res}\,(g_1(\xi)g_2(\xi)/f(\xi))$. Кроме того, для каждого $g(\xi) \in \mathbb{F}_9$ существует $g^{-1}(\xi) \in \mathbb{F}_9$, что $g(\xi) \cdot g^{-1}(\xi) = 1$. Поле $\mathbb{F}_9$ можно рассматривать и как линейное пространство над полем $\mathbb{F}_3$ с базисом $1, \xi$.

Поскольку элемент ξ примитивен, то он порождает мультипликативную группу $\mathbb{F}_9^*$ поля $\mathbb{F}_9$, т.е.

$$\mathbb{F}_9^* = \langle\xi\rangle = \{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7, \xi^8\},$$
$$\mathbb{F}_9 = \{0, 1, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7, \xi^8\}.$$

Причем $\xi^k = \xi^{\mathrm{res}(k/8)}$ для любого $k \in \mathbb{N} \cup \{0\}$, $\xi^{-n} = \xi^{8-n}$ для любого $n \in \{1, 2, \ldots, 7\}$. Выше каждый элемент поля $\mathbb{F}_9$ представлен и как степень ξ элемента, и как многочлен из $\mathbb{F}_3[\xi]$.

Минимальным многочленом элемента α поля $\mathbb{F}_9$ является многочлен

$$M_\alpha(x) = (x - \alpha)(x - \alpha^3)(x - \alpha^9)(x - \alpha^{27}) \ldots (x - \alpha^{3^{k-1}}),$$

где k — наименьшее натуральное число, такое, что $\alpha^{3^k} = \alpha$, т.е. $|\alpha| = 3^k - 1$ (утверждение **??**).

Пусть $\beta = \xi + 2 = \xi^6$. Тогда $\beta^3 = \xi^{18} = \xi^2$, $\beta^9 = (\xi^3)^3 = \xi^6 = \beta$, Значит, $\beta^{3^2} = \beta$, $k = \deg M_\beta(x) = 2$ и

$$M_\beta(x) = (x - \beta)(x - \beta^2) =$$
$$= x^2 - (\beta + \beta^3)x + \beta\beta^3 = x^2 - (\xi^6 + \xi^2)x + 1 =$$
$$= x^2 - [(\xi + 2) + (2\xi + 1)]x + 1 = x^2 - (3\xi + 3)x + 1 = x^2 + 1.$$

Проверка: $M_\beta(\beta) = \beta^2 + 1 = \xi^{12} + 1 = \xi^4 + 1 = 2 + 1 = 0$.

Из равенства $|\beta| = 3^2 - 1 = 8$ следует, что элемент β является примитивным.

Пусть, наконец, $\gamma = (2\xi + 1)^{-1} = (\xi^2)^{-1} = 2$. Ясно, что
$M_\gamma(x) = x - 2$ и $|\gamma| = 3^1 - 1 = 2$, откуда следует, что элемент γ не является примитивным.

Ответ. Минимальными многочленами элементов $\xi+2, (2\xi+1)^{-1}$ являются многочлены $x^2+1, x-2$ соответственно. Элемент $\xi+2$ примитивный, а элемент $(2\xi + 1)^{-1}$ — нет.