K – конечное поле $\Rightarrow \operatorname{char} K = p > 0$ – простое число. Пусть $\langle 1 \rangle \subseteq K$ – циклическая подгруппа по сложению, порождённая 1. Тогда $\langle 1 \rangle$ – подкольцо в K и $\langle 1 \rangle = \mathbb{Z}_p \Rightarrow \langle 1 \rangle$ – подполе в K.
Будем отождествлять $\mathbb{Z}_p$ с $\langle 1 \rangle$ и считать, что $\mathbb{Z}_p \subseteq K$.

Теорема. $|K| = p^n$, где $n = \dim_{\mathbb{Z}_p} K$.

Конструкция поля из p^n элементов. Выберем неприводимый многочлен $h \in \mathbb{Z}_p[x]$, $\deg h = n$. Тогда $F = \mathbb{Z}_p/(h)$ – поле и $[F : \mathbb{Z}_p] = n \Rightarrow$ получаем $|F| = p^n$.

Определение. K – конечное поле, $\operatorname{char} K = p \Rightarrow$
(а) $|K| = p^n$, где $n = \dim_{\mathbb{Z}_p} K$
(б) Отображение $\varphi : K \to K$, $a \mapsto a^p$ называется *автоморфизмом* (изоморфизмом на себя)
Замечание. K – поле и отображение $\psi : K \to K$ – автоморфизм $\Rightarrow$ множество неподвижных точек $K^\psi = \{a \in K \mid \psi(a) = a\}$ является подполем в K.

Теорема. p – простое, $n \in \mathbb{N} \Rightarrow$ существует поле K, такое что $|K| = p^n$.

Обозначение: K – поле $\Rightarrow K^\times = (K \setminus \{0\}, \times)$ – мультипликативная группа K.
Предложение. $K^\times$ является циклической.

Предложение. Существует неприводимый многочлен $h \in \mathbb{Z}_p[X]$ степени $n \in \mathbb{N}$, такой что поле $K \simeq \mathbb{Z}_p[X]/(h)$. В частности $\forall n$ в $\mathbb{Z}_p[X]$ есть неприводимый многочлен.

Пусть p – простое, $n \in N$, K – поле и $|K| = q = p^n$.
Лемма. Все элементы поля K являются корнями многочлена $f = x^q - x$ (и только они). Более того f разлагается на линейные множители в $K[x]$, причём без кратностей.
Теорема. F – поле и $|F| = q = p^n \Rightarrow F \simeq K$. В частности, поле из p^n элементов единственно с точностью до изоморфизма.
Обозначение: $\mathbb{F}_q$ – поле из q элементов.

Теорема. $q = p^n$, p – простое $\Rightarrow$
(а) $F \subseteq \mathbb{F}_q$ – подполе $\Rightarrow |F| = p^m$, где $m \mid n$
(б) $m \mid n \Rightarrow$ существует единственное подполе $F \subseteq \mathbb{F}_q$, такое что $|F| = p^m$

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

1. Мультипликативная группа $\mathbb{F}_9$ содержит 8 элементов, так как $\mathbb{F}_9^\times = (\mathbb{F}_9 \setminus \{0\}, \times)$, а $|\mathbb{F}_9| = 9$. Всякая циклическая группа, порождаемая элементом g, содержит $\mathrm{ord}(g)$ элементов. Значит, для нахождения порождающих элементов группы $\mathbb{F}_9^\times$ нужно рассмотреть все элементы, порядок которых равен 8.

2. Поле состоит из следующих элементов

$$\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+2x+2) = \{0,\ 1,\ 2,\ \bar{x},\ \bar{x}+1,\ \bar{x}+2,\ 2\bar{x},\ 2\bar{x}+1,\ 2\bar{x}+2\}$$

   Другими словами – оно образовано многочленами над $\mathbb{Z}_3$ степени меньшей двух. Соответствующая этому полю мультипликативная группа состоит из элементов

$$\mathbb{F}_9^\times = \{1,\ 2,\ \bar{x},\ \bar{x}+1,\ \bar{x}+2,\ 2\bar{x},\ 2\bar{x}+1,\ 2\bar{x}+2\}$$

   Найдём порядок каждого из описанных элементов группы $\mathbb{F}_9^\times$, используя формулу понижения степени $\bar{x}^2 = \bar{x}+1$, полученную из равенства $\bar{x}^2+2\bar{x}+2=0$.

   – У элемента 1 порядок равен 1: $1 = 1$

   – У элемента 2 порядок равен 2: $2 \cdot 2 = 4 = 1$

   – У элемента $\bar{x}$ порядок равен 8:

$$\bar{x} \overset{\cdot\bar{x}}{\to} \bar{x}^2 = \bar{x}+1 \overset{\cdot\bar{x}}{\to} \bar{x}^2+\bar{x} = 2\bar{x}+1 \overset{\cdot\bar{x}}{\to} 2\bar{x}^2+\bar{x} = 2 \overset{\cdot\bar{x}}{\to}$$
$$\overset{\cdot\bar{x}}{\to} 2\bar{x} \overset{\cdot\bar{x}}{\to} 2\bar{x}^2 = 2\bar{x}+2 \overset{\cdot\bar{x}}{\to} 2\bar{x}^2+2\bar{x} = \bar{x}+2 \overset{\cdot\bar{x}}{\to} \bar{x}^2+2\bar{x} = 1$$

   – У элемента $\bar{x}+1$ порядок равен 4:

$$\bar{x}+1 \overset{\cdot\bar{x}+1}{\to} \bar{x}^2+2\bar{x}+1 = 2 \overset{\cdot\bar{x}+1}{\to} 2\bar{x}+2 \overset{\cdot\bar{x}+1}{\to} 2\bar{x}^2+\bar{x}+2 = 1$$

   – У элемента $\bar{x}+2$ порядок равен 8:

$$\bar{x}+2 \overset{\cdot\bar{x}+2}{\to} \bar{x}^2+\bar{x}+1 = 2\bar{x}+2 \overset{\cdot\bar{x}+2}{\to} 2\bar{x}^2+1 = 2\bar{x} \overset{\cdot\bar{x}+2}{\to} 2\bar{x}^2+\bar{x} = 2 \overset{\cdot\bar{x}+2}{\to}$$
$$\overset{\cdot\bar{x}+2}{\to} 2\bar{x}+1 \overset{\cdot\bar{x}+2}{\to} 2\bar{x}^2+2\bar{x}+2 = \bar{x}+1 \overset{\cdot\bar{x}+2}{\to} \bar{x}^2+2 = \bar{x} \overset{\cdot\bar{x}+2}{\to} \bar{x}^2+2\bar{x} = 1$$

   – У элемента $2\bar{x}$ порядок равен 8:

$$2\bar{x} \overset{\cdot 2\bar{x}}{\to} \bar{x}+1 \overset{\cdot 2\bar{x}}{\to} 2\bar{x}^2+2\bar{x} = \bar{x}+2 \overset{\cdot 2\bar{x}}{\to} 2\bar{x}^2+\bar{x} = 2 \overset{\cdot 2\bar{x}}{\to}$$
$$\overset{\cdot 2\bar{x}}{\to} \bar{x} \overset{\cdot 2\bar{x}}{\to} 2\bar{x}^2 = 2\bar{x}+2 \overset{\cdot 2\bar{x}}{\to} \bar{x}^2+\bar{x} = 2\bar{x}+1 \overset{\cdot 2\bar{x}}{\to} \bar{x}^2+2\bar{x} = 1$$

   – У элемента $2\bar{x}+1$ порядок равен 8:

$$2\bar{x}+1 \overset{\cdot 2\bar{x}+1}{\to} \bar{x}^2+\bar{x}+1 = 2\bar{x}+2 \overset{\cdot 2\bar{x}+1}{\to} \bar{x}^2+2 = \bar{x} \overset{\cdot 2\bar{x}+1}{\to} 2\bar{x}^2+\bar{x} = 2 \overset{\cdot 2\bar{x}+1}{\to}$$
$$\overset{\cdot 2\bar{x}+1}{\to} \bar{x}+2 \overset{\cdot 2\bar{x}+1}{\to} 2\bar{x}^2+2\bar{x}+2 = \bar{x}+1 \overset{\cdot 2\bar{x}+1}{\to} 2\bar{x}^2+1 = 2\bar{x} \overset{\cdot 2\bar{x}+1}{\to} \bar{x}^2+2\bar{x} = 1$$

   – У элемента $2\bar{x}+2$ порядок равен 4:

$$2\bar{x}+2 \overset{\cdot 2\bar{x}+2}{\to} \bar{x}^2+2\bar{x}+1 = 2 \overset{\cdot 2\bar{x}+2}{\to} \bar{x}+1 \overset{\cdot 2\bar{x}+2}{\to} 2\bar{x}^2+\bar{x}+2 = 1$$

3. Таким образом, элементы $\bar{x}$, $\bar{x}+2$, $2\bar{x}$, $2\bar{x}+1$ являются порождающими в группе $\mathbb{F}_9^\times$. Их порядок равен 8.

4. В цепочках преобразований, полученных выше, нетрудно увидеть, что каждый элемент из $\mathbb{F}_9^\times$ может быть представлен в виде $\bar{x}^k$, $(\bar{x}+2)^k$, $(2\bar{x})^k$ и $(2\bar{x}+1)^k$. Получаем, что рассматриваемая циклическая группа $\mathbb{F}_9^\times = \langle\bar{x}\rangle = \langle\bar{x}+2\rangle = \langle 2\bar{x}\rangle = \langle 2\bar{x}+1\rangle$. Другие элементы не могут порождать эту группу, так как их порядок меньше 8.

Ответ: $\bar{x},\ \bar{x}+2,\ 2\bar{x},\ 2\bar{x}+1$

Задание 2. Проверьте, что многочлены x^2+3 и y^2+y+2 неприводимы над $\mathbb{Z}_5$, и установите явно изоморфизм между полями $\mathbb{Z}_5[x]/(x^2+3)$ и $\mathbb{Z}_5[y]/(y^2+y+2)$.

1. Многочлен второй степени неприводим над полем $\Leftrightarrow$ он не имеет корней в этом поле. Обозначим $h_1 = x^2+3$ и $h_2 = y^2+y+2$. Проверим, что h_1 и h_2 не имеют корней в $\mathbb{Z}_5$, то есть неприводимы в $\mathbb{Z}_5[x]$ и $\mathbb{Z}_5[y]$ соответственно.

$$\begin{aligned} h_1(0) &= 3 \neq 0 & \qquad h_2(0) &= 2 \neq 0 \\ h_1(1) &= 4 \neq 0 & \qquad h_2(1) &= 4 \neq 0 \\ h_1(2) &= 2 \neq 0 & \qquad h_2(2) &= 3 \neq 0 \\ h_1(3) &= 2 \neq 0 & \qquad h_2(3) &= 4 \neq 0 \\ h_1(4) &= 4 \neq 0 & \qquad h_2(4) &= 2 \neq 0 \end{aligned}$$

   Получаем, что многочлены неприводимы, значит $\mathbb{Z}_5[x]/(x^2+3)$ и $\mathbb{Z}_5[y]/(y^2+y+2)$ – поля, в каждом из которых по 25 элементов.

2. Обозначим $F_1 = \mathbb{Z}_5[x]/(x^2+3)$ и $F_2 = \mathbb{Z}_5[y]/(y^2+y+2)$. Известно, что существует такой $\alpha \in F_2$, что $h_1(\alpha) = 0$. Рассмотрим следующий гомоморфизм $\varphi : \mathbb{Z}_5[x] \to F_2$, $f \to f(\alpha)$. Отображение φ действительно гомоморфизм – оно сохраняет сумму и произведение (фактически это отображение – взятие значения в точке).

   Найдём ядро этого гомоморфизма: это такие f, что $f(\alpha) = 0$. Ядро является главным идеалом в $\mathbb{Z}_5[x]$, то есть $\ker\varphi = (g)$ для некоторого $g \in \mathbb{Z}_5[x]$. Многочлен h_1 лежит в ядре, так как $h_1(\alpha) = 0$ $\Rightarrow h_1 \vdots g$, но h_1 неприводим над $\mathbb{Z}_5[x]$, значит, либо $g = C$, чего быть не может, так как иначе φ переводит все f в 0, либо пропорционален h_1, то есть $h_1 = g$ и $\ker\varphi = (h_1)$.

   По теореме о гомоморфизме колец получаем, что $F_1 = \mathbb{Z}_5[x]/(h_1) \simeq \operatorname{Im}\varphi \subseteq F_2$, но F_1 и F_2 имеют одинаковое число элементов, то есть $F_1 = \mathbb{Z}_5[x]/(h_1) \simeq \operatorname{Im}\varphi \Rightarrow |\operatorname{Im}\varphi| = |F_1| = |F_2| \Rightarrow \operatorname{Im}\varphi = F_2$. Таким образом, существует изоморфизм, сопоставляющий элемент $f \in \mathbb{Z}_5[x]/(h_1)$ элементу $f(\alpha) \in \mathbb{Z}_5[y]/(h_2)$.

   Исходный гомоморфизм φ был ограничен на факторкольцо, что дало изоморфизм, который по прежнему сопоставляет каждому многочлену f уже из $\mathbb{Z}_5[x]/(h_1)$ многочлен $f(\alpha) \in \mathbb{Z}_5[y]/(h_2)$.

3. Для того, чтобы задать этот изоморфизм явно, нужно найти описанный элемент $\alpha \in F_2$, такой что $h_1(\alpha) = 0$. Известно, что каждый элемент $\mathbb{Z}_5[y]/(h_2)$ представляется в виде многочлена степени не выше $\deg h_2 = 2$ в следующем виде $\alpha = ay + b$, где $a, b \in \mathbb{Z}_5$. Подставим α в h_1 и, используя формулу понижения степени $\bar{y}^2 = 4\bar{y} + 3$, получим:

$$h_1(\alpha) = (a\bar{y}+b)^2 + 3 = a^2\bar{y}^2 + 2ab\bar{y} + b^2 + 3 = (4a^2 + 2ab)\bar{y} + (3a^2 + b^2 + 3) = 0$$

   В данном случае достаточно найти частное решение, например, $a = 1$, $b = 3$. Действительно, $h_1(\bar{y}+3) = (\bar{y}+3)^2 + 3 = \bar{y}^2 + 6\bar{y} + 9 + 3 = 10\bar{y} + 15 = 0$. Получаем $\alpha = \bar{y} + 3$.

Ответ: Изоморфизм $\mathbb{Z}_5[x]/(x^2+3) \xrightarrow{\sim} \mathbb{Z}_5[y]/(y^2+y+2)$ задаётся формулой $a\bar{x} + b \to a(\bar{y}+3) + b$

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

1. Число $262144 = 2^{18}$. Получаем, что $|\mathbb{F}_{262144}| = 2^{18}$. Из последнего следует, что всякое подполе $F \subseteq \mathbb{F}_{262144}$ имеет 2^m элементов, где $m \mid 18$. Также известно, что каждое подполе $F \subseteq \mathbb{F}_{262144}$, такое что $|F| = p^m$ при $m \mid n$ единственно.

   Получаем, что у $\mathbb{F}_{262144}$ всего 6 подполей: $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_{64}, \mathbb{F}_{512}, \mathbb{F}_{262144}$. Построим граф вложенности найденных полей:

$$\begin{array}{ccccc} \mathbb{F}_{2^2} & \subseteq & \mathbb{F}_{2^6} & \subseteq & \mathbb{F}_{2^{18}} \\ \cup| & & \cup| & & \cup| \\ \mathbb{F}_2 & \subseteq & \mathbb{F}_{2^3} & \subseteq & \mathbb{F}_{2^9} \end{array}$$

2. Реализуем поле $\mathbb{F}_8$ в виде $\mathbb{Z}_2[x]/(x^3 + x + 1)$, данная реализация корректна, так как многочлен $x^3 + x + 1$ неприводим в $\mathbb{Z}_2[x]$ (он не имеет корней в $\mathbb{Z}_2$), то есть $\mathbb{Z}_2[x]/(x^3 + x + 1)$ – поле, и $[\mathbb{F}_8 : \mathbb{Z}_2] = \deg(x^3 + x + 1) = 3 \Rightarrow$ выполнено $|\mathbb{F}_8| = 2^3$.

   Описанное поле $\mathbb{Z}_2[x]/(x^3+x+1)$ состоит из $\{0,\ 1,\ \bar{x},\ \bar{x}+1,\ \bar{x}^2,\ \bar{x}^2+1\}$. Из равенства многочлена $\bar{x}^3 + \bar{x} + 1$ нулю в $\mathbb{F}_8$ выражается формула понижения степени: $\bar{x}^3 = \bar{x} + 1$.
   Заметим, что $h(\bar{x}) = \bar{x}^3 + \bar{x} + 1 = \bar{x} + 1 + \bar{x} + 1 = 0$. Это означает, что в данном поле многочлен $x^3 + x + 1$ имеет корень.

3. Поля $\mathbb{F}_{2^6}, \mathbb{F}_{2^9}, \mathbb{F}_{2^{18}}$ являются расширением поля $\mathbb{F}_{2^3}$ (это видно и из графа вложенности), значит, они содержат все элементы из $\mathbb{F}_{2^3}$. В частности, эти поля содержат элемент из $\mathbb{F}_{2^3}$, который является корнем многочлена h. То есть многочлен h имеет корень и в полях $\mathbb{F}_{2^6}$, $\mathbb{F}_{2^9}$, $\mathbb{F}_{2^{18}}$.

4. Покажем, что в полях $\mathbb{F}_2$ и $\mathbb{F}_4$ у многочлена h нет корней.

   Поле $\mathbb{F}_2$ состоит из двух элементов, а в каждом поле есть 0 и 1, значит, $\mathbb{F}_2 = \{0,\ 1\}$. Подставим оба значения в многочлен h и убедимся, что эти элементы не являются его корнями: $h(0) = 1 \neq 0$ и $h(1) = 1 \neq 0$.

   Реализуем поле $\mathbb{F}_4$ в виде $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Многочлен $x^2 + x + 1$ неприводим в $\mathbb{Z}_2[x]$, так как не имеет корней в $\mathbb{Z}_2$. Элементы этого поля равны $\{0,\ 1,\ \bar{x},\ \bar{x}+1\}$. Формула понижения степени в данном поле равна $\bar{x}^2 = \bar{x} + 1$. Покажем, что значения многочлена h от каждого из этих элементов не равно нулю:

$$h(0) = 1 \neq 0 \qquad h(1) = 1 \neq 0$$
$$h(\bar{x}) = \bar{x}^3 + \bar{x} + 1 = (\bar{x} + 1)\bar{x} + \bar{x} + 1 = \bar{x} \neq 0$$
$$h(\bar{x} + 1) = (\bar{x} + 1)^3 + \bar{x} + 1 + 1 = \bar{x}^3 + \bar{x}^2 + \bar{x} + 1 + \bar{x} = (\bar{x} + 1)\bar{x} + \bar{x} + 1 + 1 = \bar{x} + 1 \neq 0$$

   Таким образом, многочлен h не имеет корней в $\mathbb{F}_2$ и $\mathbb{F}_4$.

Ответ: $\mathbb{F}_{2^3},\ \mathbb{F}_{2^6},\ \mathbb{F}_{2^9},\ \mathbb{F}_{2^{18}}$

Задание 4. Пусть p – простое число, $q = p^n$ и $\alpha \in \mathbb{F}_q$. Докажите, что если следующий многочлен $x^p - x - \alpha \in \mathbb{F}_q[x]$ имеет корень, то он разлагается на линейные множители.

1. Характеристика данного поля равна p, это означает, что $(a+b)^p = a^p + b^p$ для всех $a, b \in \mathbb{F}_q$. Рассмотрим подполе $\mathbb{F}_p \subseteq \mathbb{F}_q$, такое подполе существует, так как $p \mid p^n$, и единственно. Для каждого элемента $t \in \mathbb{F}_p$ выполняется $t^p = t$, так как $\mathbb{F}_p^\times$ – мультипликативная циклическая группа порядка $p-1$, а для каждого элемента g этой группы верно $g^{|\mathbb{F}_p^\times|} \cdot g = e \cdot g = g$.

2. Пусть x_0 корень многочлена, $x_0^p - x_0 - \alpha = 0$. Заметим, что тогда $x_0^p - t$, где $t \in \mathbb{F}_p$, также корень этого многочлена:

$$(x_0 - t)^p - (x_0 - t) - \alpha = x_0^p - t^p - x_0 + t - \alpha = x_0^p - t - x_0 + t - \alpha = x_0^p - x_0 - \alpha = 0$$

3. В $\mathbb{F}_p$ всего p элементов. Каждый элемент t этого поля вместе с x_0 образовывает корень $x_0 - t$ многочлена $x^p - x - \alpha \in \mathbb{F}_q[x]$. Получаем, что многочлен степени p имеет p корней, значит, он разлагается на линейные множители.