Работа студента группы С18-712 Кольца И. В.

Построение полей Галуа

Цель: описать процесс построения полей Галуа вида $GF((p^m)^k)$, $p \in P; m, k \in Z$.

Опр. *Поле* — это множество, для элементов которого определены операции сложения, умножения, взятия противоположного значения и деления (кроме деления на ноль), причем свойства этих операций близки к свойствам обычных числовых операций.

Хотя названия операций поля взяты из арифметики, следует иметь в виду, что элементы поля не обязательно являются числами, и определения операций могут быть далеки от арифметических. Далее мы рассмотрим, что из себя представляют элементы поля и как можно задать для них арифметические операции.

Пример: полем является множество вещественных чисел R , которые мы умеем складывать, вычитать, делить(«на ноль делить нельзя») и умножать по привычным правилам.

Опр. *Поле Галуа* (или *конечное поле*) — поле, состоящее из конечного числа элементов. Поле Галуа обозначается $GF(q)$, где q - порядок поля — число элементов поля. Порядок конечного поля всегда является степенью какого-нибудь простого числа, то есть $q = p^n$, где p - простое число, а n — любое натуральное число. При этом p будет являться характеристикой этого поля.

Опр. *Характеристика поля* — наименьшее положительное целое число n такое, что сумма n единиц равна нулю: $\underbrace{1+1+...+1}_{n} = n1 = 0$

Рассмотрим структуру поля $GF(p)$.

Элементами поля $GF(p)$ является множество целых чисел $\{0, 1, 2, ..., p-1\}$ - остатки от деления всевозможных целых чисел на простое число p .

Сложение, вычитание и умножение чисел осуществляется с приведение результата по модулю p .

Можно заметить, что результатом всех арифметических операций над элементами конечного поля $GF(p)$ по свойствам модульной арифметики является элемент этого же поля (говорят, что поле *замкнуто* относительно соответствующих арифметических операций).

Обозначим $\%$ - операция взятия остатка от деления; $(mod\ p)$ - арифметические операции осуществляются по модулю p .

I. Рассмотрим поля при $p = 2$, т.е. поля вида $GF((2^m)^k)$

1. Построим поле Галуа $GF(2)$

$GF(2)$ - это поле, элементами которого является числа $\{0, 1\}$ - остатки от деления целых чисел на 2. Сложение и умножение чисел осуществляется с приведение результата по модулю 2.

Разберем выше описанные определения на примере поля $GF(2)$:
Поле конечное — состоит из $q=2$ элементов. $p=2$ является характеристикой поля $GF(2)$ т.е $\underbrace{1+1}_{2}=2\%2=0\ (mod\,2)$

Так как $1+1=0(mod\,2)$ (или в то же время $-1\%2=1$ по определению остатка от деления), то в $GF(2)$ сложение и вычитание — одна и та же операция.

Построим таблицы сложения и умножения для этого поля:

+	**0**	**1**
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

Эта логика лежит в основе двоичной системы компьютера. Обратим внимание, что сложение соответствует битовому оператору XOR (исключающее «ИЛИ»), а умножение — битовому оператору AND (побитовое «И»).

2. Рассмотрим задачу построения поля $GF(16)$.

По определению, $GF(16)$ - это конечное поле, состоящее из $q=16$ элементов. Как было сказано в определении, порядок конечного поля всегда является степенью какого-нибудь простого числа, то есть $q=p^n$. Представим $q=16$ в виде $q=2^4$.

Рассмотрим структуру поля $GF(p^m)$.

Опр. Конечное поле вида $GF(p^m)$ называется *расширением* поля $GF(p)$. Поле $GF(p^m)$ удовлетворяет всем требованиям, которые следуют из определения конечного поля.

Поле $GF(p^m)$ может быть представлено как множество всех полиномов неотрицательной степени не более $m-1$ с коэффициентами в поле $GF(p)$. Т.е. $\forall\, p(x)\in GF(p^m)$, $p(x)=a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+...+a_1x+a_0,\ a_i\in GF(p),\ i=0..m-1$. В этом случае говорят о многочленах «над полем $GF(p)$ ». Можно посчитать, что таких многочленов имеется в точности p^m (m коэффициентов, которые могут принимать одно из p значений, тогда по формуле числа размещений с повторениями получаем p^m).

В отличие от конечных полей, определенных над простыми целыми числами (поля вида $GF(p)$), поле $GF(p^m)$ определенно над *неприводимым многочленом степени* m с коэффициентами в $GF(p)$.

Опр. *Неприводимый многочлен* — многочлен, неразложимый на нетривиальные (то есть не константы) многочлены. Многочлен $p(x)=a_mx^m+...+a_1x+a_0$ называется *неприводимым над полем* $GF(p)$, если он не распадается на множители над этим полем.

Неприводимые многочлен для поля $GF(p^m)$ играет туже роль, что и простое число p для поля $GF(p)$: элементы поля $GF(p^m)$ - остатки от деления всех многочленов всевозможных неотрицательных степеней с коэффициентами из поля $GF(p)$ на неприводимый над полем $GF(p)$ многочлен степени m .

В любом конечном поле существует хотя бы один неприводимый многочлен степени n, $n \in N$.

Так как элементами поля $GF(p^m)$ являются многочлены, сложение и вычитание элементов поля сводится к соответствующим операциям над коэффициентами многочленов.
$\forall\, p(x), q(x) \in GF(p^m): p(x) = a_{m-1}x^{m-1} + ... + a_1 x + a_0;\ q(x) = b_{m-1}x^{m-1} + ... + b_1 x + b_0;$,
$a_i, b_i \in GF(p), i = 0..m-1$

$$p(x) + q(x) = (a_{m-1} + b_{m-1})x^m + ... (a_1 + b_1)x + (a_0 + b_0)$$
$$p(x) - q(x) = (a_{m-1} - b_{m-1})x^m + ... (a_1 - b_1)x + (a_0 - b_0)$$

Для того, чтобы перемножить 2 элемента из $GF(p^m)$, необходимо перемножить соответствующие им полиномы и взять остаток от деления на неприводимый полином (аналог того, как мы берем остаток от деления на простое число p в поле $GF(p)$), с помощью которого мы строили поле.

Можно заметить, что результатом всех вышеперечисленных операций будет является также элемент поля $GF(p^m)$, так как при сложении и вычитании мы осуществляем соответствующую операцию над коэффициентами из поля $GF(p)$, которое замкнуто относительно этих арифметических операций, а при умножении приводим результат по модулю неприводимого полинома степени m, в результате чего получим многочлен степени не более m с коэффициентами в $GF(p)$. Таким образом поле $GF(p^m)$ замкнуто относительно вышеперечисленных арифметических операций.

A. Построим поле $GF(2^4)$

Рассмотрим $GF(2^4)$. $GF(2^4)$ - это множество всех полиномов степени не больше 4 с коэффициентами в $GF(2)$, то есть полиномов вида $p(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$, $a_i \in GF(2), i = 0..3$.

Для того, чтобы задать поле $GF(2^4)$, необходимо найти неприводимый многочлен 4 степени. Чтобы упростить Евклидово деление (деление с остатком), рекомендуется брать многочлены вида $x^m + a x + b$ (если существует неприводимый многочлен такого вида в данном поле). Неприводимый квадратичный полином должен иметь 3 ненулевых коэффициента, так как без свободного члена (константы) полином всегда имеет нулевой корень, а полином формы $x^2 + a$ всегда имеет корень $\sqrt{a}$. На практике удобно пользоваться готовыми таблицами с неприводимыми многочленами (которые можно найти в сети Интернет).

Неприводимых полиномов 4 степени над полем $GF(2)$ существует несколько, найдем некоторые из них.

Проверим, что многочлен $f(x) = x^4 + x + 1$ неприводимый в $GF(2)$.
Пусть $f(x) = g(x)h(x)$, обозначим $deg(p(x))$ - степень произвольного полинома $p(x)$. Так как $deg(f(x)) = 4$ и $deg(f(x)) = deg(g(x)) + deg(h(x))$, то возможен один из следующих вариантов: $deg(g(x)) = 1; deg(h(x)) = 3$ / $deg(g(x)) = 2; deg(h(x)) = 2$ / $deg(g(x)) = 3; deg(h(x)) = 1$. Можно заметить, что в любом случае

один из полиномов будет иметь степень или 1, или 2. Следовательно, нам достаточно проверить делимость $f(x)$ на все полиномы степени ≤ 2 .

Полиномы 1 степени с коэффициентами в $GF(2)$: $x+0=x$, $x+1$

Полиномы 2 степени с коэффициентами в $GF(2)$: $x^2+0x+0=x^2$, $x^2+1x+0=x^2+x$, $x^2+0x+1=x^2+1$, $x^2+1x+1=x^2+x+1$

Так как полином $f(x)$ имеет свободный член, то все многочлены без свободного члена не могут его поделить без остатка, значит их можно отбросить. Остаются следующие многочлены: $x+1$, x^2+1, x^2+x+1 .

Рассмотрим $x+1$:

$$\begin{array}{l|l} x^4+0x^3+0x^2+x+1 & x+1 \\ \hline x^4+1x^3 & x^3+x^2+x \\ \hline x^3+0x^2 & \\ x^3+1x^2 & \\ \hline x^2+x & \\ x^2+x & \\ \hline 0+0+1 & \end{array}$$

$x+1$ не делит $f(x)$ без остатка.

Рассмотрим x^2+1 :

$$\begin{array}{l|l} x^4+0x^3+0x^2+x+1 & x^2+1 \\ \hline x^4+0x^3+1x^2 & x^2+1 \\ \hline x^2+1x+1 & \\ x^2+0x+1 & \\ \hline x & \end{array}$$

x^2+1 не делит $f(x)$ без остатка.

Рассмотрим x^2+x+1 :

$$\begin{array}{l|l} x^4+0x^3+0x^2+x+1 & x^2+x+1 \\ \hline x^4+1x^3+1x^2 & x^2+x \\ \hline x^3+x^2+x & \\ x^3+x^2+x & \\ \hline 0+0+0+1 & \end{array}$$

x^2+x+1 не делит $f(x)$ без остатка.

Можно сделать вывод, что многочлен $f(x)=x^4+x+1$ является неприводимым над $GF(2)$.

Аналогично проверим, что многочлен $q(x)=x^4+x^3+x^2+x+1$ неприводимый в $GF(2)$. Так как это полином 4 степени, имеющий свободный член, то его делителями могут быть, как и в предыдущем случае, следующие многочлены: $x+1$, x^2+1, x^2+x+1 .

Рассмотрим $x+1$:

$x^4+x^3+x^2+x+1$	$x+1$
x^4+x^3	x^3+x
x^2+x	
x^2+x	
$0+0+1$	

$x+1$ не делит $q(x)$ без остатка.

Рассмотрим x^2+1 :

$x^4+1x^3+x^2+x+1$	x^2+1
$x^4+0x^3+x^2$	x^2+x
x^3+x	
x^3+x	
$0+0+1$	

x^2+1 не делит $q(x)$ без остатка.

Рассмотрим x^2+1 :

$x^4+x^3+x^2+x+1$	x^2+x+1
$x^4+x^3+x^2$	x^2
$x+1$	

x^2+x+1 не делит $q(x)$ без остатка.

Можно сделать вывод, что многочлен $q(x)=x^4+x^3+x^2+x+1$ является неприводимым над $GF(2)$.

Покажем, в чем состоит разница при построении полей над различными неприводимыми многочленами. Для этого рассмотрим поле $GF(2^4)$, определенное над неприводимым многочленом $f(x)$ и над неприводимым многочленом $q(x)$.

В обоих случаях, по определению поля $GF(2^4)$, его элементами будет являться множество из 16 полиномов степени не более 4 с коэффициентами в $GF(2)$:

$$\{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1,x^3,x^3+1,x^3+x,x^3+x+1,x^3+x^2,x^3+x^2+1,x^3+x^2+x,x^3+x^2+x+1\}$$

Но в первом случае, когда мы определяем поле $GF(2^4)$ над неприводимым многочленом $f(x)=x^4+x+1$, получаем:

$$x^3+1=x^{-1};x^3+x^2+x=(x+1)^{-1};x^3+x^2+1=(x^2)^{-1};x^3+x+1=(x^2+1)^{-1};x^2+x+1=(x^2+x)^{-1};$$
$$x^3+x^2+x+1=(x^3)^{-1};x^3+x^2=(x^3+x)^{-1}$$

Во втором случае, когда мы определяем поле $GF(2^4)$ над неприводимым многочленом , $q(x)=x^4+x^3+x^2+x+1$ получаем:

$$x^3+x^2+x+1=x^{-1};x^3+x=(x+1)^{-1};x^3=(x^2)^{-1};x^2+x=(x^2+1)^{-1};x^2+x+1=(x^3+1)^{-1};$$
$$x^3+x^2+x=(x^3+x+1)^{-1};x^3+x^2+1=(x^3+x^2)^{-1}$$

Таким образом, роль различных неприводимых многочленов, по модулям которых строится поле, состоит именно в том, что они по-разному "организуют" соотношения между элементами: они по-разному создают пары взаимно обратных элементов. Само же "содержимое" поля зависит только от степени неприводимого многочлена, над которым мы определяем поле, так как она определяет максимальную степень остатка от деления.

Напомним, что элемент x называется взаимно *обратным* к элементу y , если $xy=yx=1$.

Поле можно задать посредством корня неприводимого многочлена.
Пусть $\alpha(x)=x\in GF(2^4)$ - корень неприводимого многочлена $f(x)$, над которым мы строим конечное поле $GF(2^4)$, т.е. $f(\alpha)=0$. Таким образом поле состоит из многочленов от α степени не более 4.

Построим поле $GF(2^4)$ по модулю многочлена $f(x)=x^4+x+1$. Из того, что в поле характеристики 2 выполняется равенство $-1=1\ (mod\,2)$ и $f(\alpha)=0$ получаем, что $\alpha^4=\alpha+1$. Выразим элементы поля через α :

$$\alpha^0=1$$
$$\alpha^1=\alpha$$
$$\alpha^2=\alpha^2$$
$$\alpha^3=\alpha^3$$
$$\alpha^4=\alpha+1$$
$$\alpha^5=\alpha\alpha^4=\alpha(\alpha+1)=\alpha^2+\alpha$$
$$\alpha^6=\alpha\alpha^5=\alpha(\alpha^2+\alpha)=\alpha^3+\alpha^2$$
$$\alpha^7=\alpha\alpha^6=\alpha(\alpha^3+\alpha^2)=\alpha^4+\alpha^3=\alpha+1+\alpha^3=\alpha^3+\alpha+1$$
$$\alpha^8=\alpha\alpha^7=\alpha(\alpha^3+\alpha+1)=\alpha^4+\alpha^2+\alpha=\alpha+1+\alpha^2+\alpha=\alpha^2+2\alpha+1=\alpha^2+1\,(заметим,что\,2\alpha=0\,(mod\,2))$$
$$\alpha^9=\alpha\alpha^8=\alpha(\alpha^2+1)=\alpha^3+\alpha$$
$$\alpha^{10}=\alpha\alpha^9=\alpha(\alpha^3+\alpha)=\alpha^4+\alpha^2=\alpha+1+\alpha^2=\alpha^2+\alpha+1$$
$$\alpha^{11}=\alpha\alpha^{10}=\alpha(\alpha^2+\alpha+1)=\alpha^3+\alpha^2+\alpha$$
$$\alpha^{12}=\alpha\alpha^{11}=\alpha(\alpha^3+\alpha^2+\alpha)=\alpha^4+\alpha^3+\alpha^2=\alpha+1+\alpha^3+\alpha^2=\alpha^3+\alpha^2+\alpha+1$$

$\alpha^{13}=\alpha\alpha^{12}=\alpha(\alpha^3+\alpha^2+\alpha+1)=\alpha^4+\alpha^3+\alpha^2+\alpha=\alpha+1+\alpha^3+\alpha^2+\alpha=\alpha^3+\alpha^2+2\alpha+1=\alpha^3+\alpha^2+1$
$\alpha^{14}=\alpha\alpha^{13}=\alpha(\alpha^3+\alpha^2+1)=\alpha^4+\alpha^3+\alpha=\alpha+1+\alpha^3+\alpha=\alpha^3+2\alpha+1=\alpha^3+1$
$\alpha^{15}=\alpha\alpha^{14}=\alpha(\alpha^3+1)=\alpha^4+\alpha=\alpha+1+\alpha=2\alpha+1=1$

Заметим, что способ представления элементов поля через многочлены от α отличается от способа представления с помощью многочленов от x только тем, что буква x заменена буквой α. Такая замена при обращении с полями Галуа позволяет нам оперировать в терминах корней многочленов, что оказывается намного удобней при осуществлении арифметических операций.

Необходимо ответить, что кроме полученных выше элементов поля, также элементом поля $GF(2^4)$ является ноль. Степени α - корня многочлена $f(x)=x^4+x+1$ - генерируют все *ненулевые* элементы поля.

Рассмотрим далее понятия примитивного элемента поля и примитивного многочлена поля.

Опр. *Порядок элемента* $g\in GF(p^m)$ — это наименьшее целое число $k>0$ такое, что $g^k=1$.

Опр. *Примитивным элементом* конечного поля называется элемент, генерирующий все ненулевые элементы поля. Порядок примитивного элемента поля $GF(p^m)$ равен p^m-1. Любой ненулевой элемент поля может быть представлен как степень примитивного элемента этого поля.

Элемент α является *примитивным элементом поля*, так как минимальное целое k, при котором $\alpha^k=1$ равно $k=2^4-1=15$. Любой другой ненулевой элемент может быть получен как степень α^k, где k - целое число, взаимно простое с $2^4-1=15$.

В свою очередь степень α^k, где k - целое число, взаимно простое с $2^4-1=15$, может быть представлена в виде $b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0$, где α - примитивный элемент, $b_i\in GF(2), i=0..3$.

Опр. *Минимальный многочлен элемента* $g\in GF(p^m)$ — приведенный многочлен минимальной степени над полем $GF(p^m)$, корнем которого является g.

Опр. *Примитивный многочлен* поля — это минимальный многочлен примитивного элемента поля (минимальный многочлен, корнем которого является примитивный элемент поля).

Не любой неприводимый многочлен является примитивным многочленом поля.

Так как α является примитивным элементом поля и многочлен $f(x)=x^4+x+1$ является минимальным, то $f(x)=x^4+x+1$ является примитивным многочленом поля $GF(2^4)$.

Как мы уже упоминали, каждое число представимо в виде $b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0$ и $b_i\in GF(2), i=0..3$, следовательно мы можем задать каждый элемент поля в виде двоичного вектора, в котором каждая цифра соответствует коэффициентам b_i. Например, $\alpha^9=\alpha^3+\alpha$ представим в виде 1010.

Составим таблицу, содержащую все элементы поля (Таблица 1):

0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	1100
α^7	$\alpha^3+\alpha+1$	1011
α^8	α^2+1	0101
α^9	$\alpha^3+\alpha$	1010
α^{10}	$\alpha^2+\alpha+1$	0111
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1101
α^{14}	α^3+1	1001

Как и в поле $GF(2)$, сложение (и вычитывание) в поле $GF(2^4)$ осуществляется с помощью битового оператора XOR (исключающее «ИЛИ»). Построим таблицу сложения в $GF(2^4)$ (для компактности будем использовать двоичную запись)

+	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0001	0001	0000	0011	0010	0101	0100	0111	0110	1001	1000	1011	1010	1101	1100	1111	1110
0010	0010	0011	0000	0001	0110	0111	0100	0101	1010	1011	1000	1001	1110	1111	1100	1101
0011	0011	0010	0001	0000	0111	0110	0101	0100	1011	1010	1001	1000	1111	1110	1101	1100
0100	0100	0101	0110	0111	0000	0001	0010	0011	1100	1101	1110	1111	1000	1001	1010	1011
0101	0101	0100	0111	0110	0001	0000	0011	0010	1101	1100	1111	1110	1001	1000	1011	1010
0110	0110	0111	0100	0101	0010	0011	0000	0001	1110	1111	1100	1101	1010	1011	1000	1001
0111	0111	0110	0101	0100	0011	0010	0001	0000	1111	1110	1101	1100	1011	1010	1001	1000
1000	1000	1001	1010	1011	1100	1101	1110	1111	0000	0001	0010	0011	0100	0101	0101	0111
1001	1001	1000	1011	1010	1101	1100	1111	1110	0001	0000	0011	0010	0101	0100	0111	0110
1010	1010	1011	1000	1001	1110	1111	1100	1101	0010	0011	0000	0001	0110	0111	0100	0101
1011	1011	1010	1001	1000	1111	1110	1101	1100	0011	0010	0001	0000	0111	0110	0101	0100
1100	1100	1101	1110	1111	1000	1001	1010	1011	0100	0101	0110	0111	0000	0001	0010	0011
1101	1101	1100	1111	1110	1001	1000	1011	1010	0101	0100	0111	0110	0001	0000	0011	0010
1110	1110	1111	1100	1101	1010	1011	1000	1001	0110	0111	0100	0101	0010	0011	0000	0001
1111	1111	1110	1101	1100	1011	1010	1001	1000	0111	0110	0101	0100	0011	0010	0001	0000

Как уже говорилось, чтобы перемножить два элемента $a,b \in GF(2^4)$, нам необходимо осуществить перемножение полиномов $a(x)b(x)$ и взять остаток от деления по модулю на примитивный многочлен 4 степени $f(x)=x^4+x+1$, по модулю которого мы строили поле.

Рассмотрим пример:
$(x^3+x+1)(x^3+x^2+x)=x^6+x^5+x^4+x^4+x^3+x^2+x^3+x^2+x=x^6+x^5+2x^4+2x^3+2x^2+x=x^6+x^5+x$
(Напомним, что $2x^k=0(mod\,2)$)

Так как x^6+x^5+x не является элементом поля (напомним, что элементами поля $GF(2^4)$ являются полиномы степени не больше 4 с коэффициентами в $GF(2)$), нам необходимо взять остаток от деления на полином $f(x)=x^4+x+1$:

$$\begin{array}{l|l} x^6+1x^5+0x^4+0x^3+0x^2+x & x^4+x+1 \\ \hline x^6+0x^5+0x^4+1x^3+1x^2 & x^2+x \\ \hline x^5+1x^3+x^2+x & \\ x^5+0x^3+x^2+x & \\ \hline x^3 & \end{array}$$

В итоге получаем: $(x^3+x+1)(x^3+x^2+x)=x^3(mod\quad x^4+x+1)$

Однако на практике умножать элементы таким способом не удобно и не эффективно, поэтому используется (особенно в случае небольших полей) экспоненциальное представление элементов поля как степеней генерирующего элемента α (для теоретического обоснования см. Логарифм Зеха («*Zech's logarithm*»)).

В общем виде формулы для поля $GF(p^m)$ выглядят следующим образом:
$\alpha^m \alpha^n=\alpha^{m+n}$
$(\alpha^m)^{-1}=\alpha^{-m}$
$\alpha^m/\alpha^n=\alpha^{m-n}$

Так как поле конечное и циклическое, то $\alpha^m \alpha^n=\alpha^{m+n}=\alpha^{(m+n)\ \%\ (p^m-1)}$ (аналогично и в случае других операций).

Вернемся к примеру выше: $(x^3+x+1)(x^3+x^2+x)=x^3$, запишем его через примитивный элемент α в виде $(\alpha^3+\alpha+1)(\alpha^3+\alpha^2+\alpha)$. Используя «Таблицу 1» заметим, что $(\alpha^3+\alpha+1)(\alpha^3+\alpha^2+\alpha)=\alpha^7\alpha^{11}=\alpha^{18}=\alpha^{(18\,mod\,15)}=\alpha^3$. Результат совпал с первым способом умножения элементов поля.

Построим таблицу умножения в $GF(2^4)$ (для компактности будем использовать двоичную запись)

*	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
0001	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0010	0000	0010	0100	0110	1000	1010	1100	1110	0011	0001	0111	0101	1011	1001	1111	1101
0011	0000	0011	0110	0101	1100	1111	1010	1001	1011	1000	1101	1110	0111	0100	0001	0010
0100	0000	0100	1000	1100	0011	0111	1011	1111	0110	0010	1110	1010	0101	0001	1101	1001
0101	0000	0101	1010	1111	0111	0010	1101	1000	1110	1011	0100	0001	1001	1100	0011	0110

0110	0000	0110	1100	1010	1011	1101	0111	0001	0101	0011	1001	1111	1110	1000	0010	0100
0111	0000	0111	1110	1001	1111	1000	0001	0110	1101	1010	0011	0100	0010	0101	1100	1011
1000	0000	1000	0011	1011	0110	1110	0101	1101	1100	0100	1111	0111	1010	0010	1001	0001
1001	0000	1001	0001	1000	0010	1011	0011	1010	0100	1101	0101	1100	0110	1111	0111	1110
1010	0000	1010	0111	1101	1110	0100	1001	0011	1111	0101	1000	0010	0001	1011	0110	1100
1011	0000	1011	0101	1110	1010	0001	1111	0100	0111	1100	0010	1001	1101	0110	1000	0011
1100	0000	1100	1011	0111	0101	1001	1110	0010	1010	0110	0001	1101	1111	0011	0100	1000
1101	0000	1101	1001	0100	0001	1100	1000	0101	0010	1111	1011	0110	0011	1110	1010	0111
1110	0000	1110	1111	0001	1101	0011	0010	1100	1001	0111	0110	1000	0100	1010	1011	0101
1111	0000	1111	1101	0010	1001	0110	0100	1011	0001	1110	1100	0011	1000	0111	0101	1010

При необходимости, аналогичным образом можно задать таблицы для оставшихся операций. Автор работы надеется, что читатель без труда справиться с этим самостоятельно.

Теперь построим поле $GF(2^4)$ по модулю многочлена $q(x)=x^4+x^3+x^2+x+1$ и сравним с предыдущем способом.

Пусть $\lambda \in GF(2^4)$ - корень неприводимого многочлена $q(x)$, над которым мы строим конечное поле $GF(2^4)$, т.е. $q(\lambda)=0$.
Попробуем построить поле, возводя в степень λ. Из того, что $q(\lambda)=0$, получаем $\lambda^4=\lambda^3+\lambda^2+\lambda+1$.

$\lambda^0=1$
$\lambda^1=\lambda$
$\lambda^2=\lambda^2$
$\lambda^3=\lambda^3$
$\lambda^4=\lambda^3+\lambda^2+\lambda+1$
$\lambda^5=\lambda^4+\lambda^3+\lambda^2+\lambda=\lambda^3+\lambda^2+\lambda+1+\lambda^3+\lambda^2+\lambda=2\lambda^3+2\lambda^2+2\lambda+1=1$

Получили, что корень λ порождает не все ненулевые элементы поля $GF(2^4)$, а только подмножество из 5 элементов.

Покажем, что элемент $\lambda+1$ порождает все поле $GF(2^4)$, не забывая, что $\lambda^4=\lambda^3+\lambda^2+\lambda+1$:

$(\lambda+1)^0=1$
$(\lambda+1)^1=\lambda+1$
$(\lambda+1)^2=\lambda^2+1$
$(\lambda+1)^3=(\lambda+1)(\lambda^2+1)=\lambda^3+\lambda^2+\lambda+1$
$(\lambda+1)^4=\lambda^4+1=\lambda^3+\lambda^2+\lambda+1+1=\lambda^3+\lambda^2+\lambda$
$(\lambda+1)^5=(\lambda+1)(\lambda^3+\lambda^2+\lambda)=\lambda^4+\lambda^3+\lambda^2+\lambda^3+\lambda^2+\lambda=\lambda^4+\lambda=\lambda^3+\lambda^2+1$
$(\lambda+1)^6=\lambda^6+\lambda^4+\lambda^2+1=\lambda+\lambda^3+\lambda^2+\lambda+1+\lambda^2+1=\lambda^3$
$(\lambda+1)^7=\lambda^4+\lambda^3=\lambda^3+\lambda^2+\lambda+1+\lambda^3=\lambda^2+\lambda+1$
$(\lambda+1)^8=\lambda^6+\lambda^4+\lambda^2=\lambda+\lambda^3+\lambda^2+\lambda+1+\lambda^2=\lambda^3+1$
$(\lambda+1)^9=\lambda^4+\lambda+\lambda^3+1=\lambda^3+\lambda^2+\lambda+1+\lambda+\lambda^3+1=\lambda^2$
$(\lambda+1)^{10}=\lambda^6+\lambda^4+1=\lambda+\lambda^3+\lambda^2+\lambda+1+1=\lambda^3+\lambda^2$

$(\lambda+1)^{11}=\lambda^4+\lambda^3+\lambda^3+\lambda^2=\lambda^3+\lambda+1$
$(\lambda+1)^{12}=\lambda^6=\lambda$
$(\lambda+1)^{13}=\lambda^2+\lambda$
$(\lambda+1)^{14}=\lambda^3+\lambda^2+\lambda^2+\lambda=\lambda^3+\lambda$
$(\lambda+1)^{15}=\lambda^4+\lambda^2+\lambda^3+\lambda=\lambda^3+\lambda^2+\lambda+1+\lambda^2+\lambda^3+\lambda=1$

Таким образом, поле $GF(2^4)$ построено по модулю неприводимого многочлена $q(x)=x^4+x^3+x^2+x+1$, но в степени возводился не корень этого многочлена λ, а элемент $\lambda+1$.

Добавление единицы к λ ничем не мотивировано и на первый взгляд кажется случайным. Однако рассмотрим элемент $\lambda+1$. По Таблице 1 можно заметить, что корнем многочлена $q(x)=x^4+x^3+x^2+x+1$ является элемент α^3 : $\alpha^{12}+\alpha^9+\alpha^6+\alpha^3+1=0$. Значит, $\lambda=\alpha^3$. Это объясняет порядок элемента λ, равный 5: $(\alpha^3)^5=\alpha^{15}=1$. Тогда $\lambda+1=\alpha^3+1=\alpha^{14}$. Элемент α^{14}, и соответственно элемент $\lambda+1$, является элементом порядка 15: $(\alpha^{14})^{15}=1$, т.е этот элемент генерирует все ненулевые элементы поля. Поэтому естественно искать порождающие элементы в виде $\lambda+x,\ x=a_3\lambda^3+a_2\lambda^2+a_1\lambda+a_0, a_i\in GF(2)$.

В общем случае, когда корень λ некоторого многочлена, по модулю которого строится $GF(p^m)$, не является генерирующим элементом ненулевых элементов поля, можно рассмотреть уравнение $\lambda+x=\alpha^k$, где α^k - порождающий элемент поля $GF(p^m)$, $x=a_{m-1}\lambda^{m-1}+...+a_2\lambda^2+a_1\lambda+a_0,\ a_i\in GF(p)$. По свойствам поля, оно всегда имеет решение и при том единственное.

Операции с элементами поля $GF(2^4)$, построенного по модулю многочлена $q(x)=x^4+x^3+x^2+x+1$, можно осуществлять аналогично предыдущему случаю, с учетом того, что примитивным элементом является элемент $\lambda+1$.

На этом закончим с построением поля $GF(2^4)$.

B. Однако поле $GF(16)$ можно представить и в виде $GF((2^2)^2)$. Построим поле $GF((2^2)^2)$

a) Для этого нам необходимо сначала построить поле $GF(2^2)$. Так как алгоритм построения поля $GF(2^m)$ был рассмотрен в общем виде, а также построено поля $GF(2^4)$, которое можно рассматривать в качестве примера, автор не будет подробно описывать уже рассмотренные вопросы.

$GF(2^2)$ - это множество всех полиномов степени не больше 2 с коэффициентами в $GF(2)$, то есть полиномов вида $p(x)=a_1x+a_0$, $a_i\in GF(2), i=0,1$.

Найдем неприводимый многочлен для построения поля $GF(2^2)$. Согласно рекомендациям по выбору неприводимого многочлена, рассмотрим многочлен x^2+x+1.
Покажем, что он неприводимый в $GF(2)$. Полином 2 степени может быть разложен только в полиномы первой степени. Полиномы 1 степени с коэффициентами в $GF(2)$: $\begin{matrix}x+0=x\\x+1\end{matrix}$.
Так как x^2+x+1 содержит свободный член, то x не может являться его делителем.

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

$x+1$ не делит x^2+x+1 без остатка.

Можно сделать вывод, что многочлен я x^2+x+1 является неприводимым в $GF(2)$.

Пусть $\beta(x)=x\in GF(2^2)$ - корень неприводимого многочлена $f(x)=x^2+x+1$, над которым мы строим конечное поле $GF(2^2)$

Построим поле $GF(2^4)$ по модулю многочлена $f(x)=x^2+x+1$. Из того, что в поле характеристики 2 выполняется равенство $-1=1\ (mod\,2)$ и $f(\beta)=0$ получаем, что $\beta^2=\beta+1$. Выразим элементы поля через β :

$\beta^0=1$
$\beta^1=\beta$
$\beta^2=\beta+1$

$\beta^3=\beta\beta^2=\beta(\beta+1)=\beta^2+\beta=\beta+1+\beta=1$
Минимальное $k>0$, такое что $\beta^k=1$ равно $2^2-1=3$, следовательно β является примитивным элементом, а $f(x)=x^2+x+1$ - примитивным многочленом поля $GF(2^2)$. Любой другой ненулевой элемент может быть получен как степень β^k , где k - целое число, взаимно простое с $2^2-1=3$.

В свою очередь степень β^k , где k - целое число, взаимно простое с $2^2-1=3$, может быть представлена в виде $a_1\beta+a_0$, где β - примитивный элемент, $a_i\in GF(2), i=0,1$. Будем также использовать представление элементов $GF(2^2)$ в виде двоичного вектора $(a_1,a_0), a_i\in GF(2), i=0,1$.

Составим таблицу, содержащую все элементы поля

0	0	00
1	1	01
β	β	10
β^2	$\beta+1$	11

Как и в поле $GF(2)$, сложение (и вычитывание) в поле $GF(2^2)$ осуществляется с помощью битового оператора XOR (исключающее «ИЛИ»). Построим таблицу сложения в $GF(2^2)$:

+	0	1	β	$\beta+1$
0	0	1	β	$\beta+1$
1	1	0	$\beta+1$	β
β	β	$\beta+1$	0	1
$\beta+1$	$\beta+1$	β	1	0

Умножать элементы в $GF(2^2)$ будем аналогично $GF(2^4)$, используя экспоненциальное представление элементов поля как степеней генерирующего элемента β.

Построим таблицу умножения в $GF(2^2)$:

*	0	1	β	$\beta+1$
0	0	0	0	0
1	0	1	β	$\beta+1$
β	0	β	$\beta+1$	1
$\beta+1$	0	$\beta+1$	1	β

При необходимости, аналогичным образом можно задать таблицы для оставшихся операций.

На этом закончим построение поля $GF(2^2)$ и перейдем к построению составного поля $GF((2^2)^2)$.

б) Рассмотрим структуру поля Галуа вида $GF((p^m)^k)$, $p \in P; m,k \in Z$.

Расширение $GF((p^m)^k)$ поля $GF(p^m)$ строится аналогичным образом, как и расширение $GF(p^m)$ поля $GF(p)$, $p \in P; m,k \in Z$.

Напомню, как мы определили элементы поля расширения для $GF(p)$:
«Поле $GF(p^m)$ может быть представлено как множество всех полиномов неотрицательной степени не более $m-1$ с коэффициентами в поле $GF(p)$»

Опр. Назовем *основным полем* («*ground field*») — поле, над которым строится расширение. Если мы строим расширение $GF(p^m)$, то для него основным полем будет $GF(p)$. В случае составного поля $GF((p^m)^k)$ мы строим расширение над полем $GF(p^m)$, то есть поле $GF(p^m)$ является основным для расширения $GF((p^m)^k)$.

Тогда обобщим определение элементов поля расширения для $GF(q^k), q=p^m, p \in P; m,k \in Z$:
Утв1. Поле $GF(q^k)$ может быть представлено как множество всех полиномов степени не более $k-1$ с коэффициентами в основном поле $GF(q)$.

Вспомним также, что:
«В отличие от конечных полей, определенных над простыми целыми числами (поля вида $GF(p)$), поле $GF(p^m)$ определенно над неприводимым многочленом степени m с коэффициентами в $GF(p)$».

Также обобщим это правило на случай $GF(q^k), q=p^m, p \in P; m,k \in Z$:
Утв2. Поле $GF(q^k)$ определено над неприводимым многочленом степени k с коэффициентами в основном поле $GF(q)$.

Теперь, используя *Утв1.* и *Утв2.*, опишем составное поле $GF((2^m)^k)$:
Поле $GF((2^m)^k)$ может быть представлено как множество всех полиномов степени не более $k-1$ с коэффициентами в поле $GF(2^m)$, $m,k \in Z$. Поле $GF((2^m)^k)$ определено над неприводимым многочленом $f(x)$ степени k с коэффициентами в $GF(2^m)$.

В двоичном представлении каждый элемент поля $GF((2^m)^k)$ может быть представлен как битовая строка длины $n=m*k;\ n,m,k\in Z$, которую разбили на k последовательных строк длины m. Каждая строка длины m соответствует коэффициенту из основного поля $GF(2^m)$.

Сложение (и вычитывание) в поле о $GF((2^m)^k)$ осуществляется с помощью битового оператора XOR (исключающее «ИЛИ»). Так как поле $GF(2^m)$ замкнуто относительно операции сложения (в результате сложения элементов поля результат так же принадлежит этому полю), то и поле $GF((2^m)^k)$ замкнуто относительно операции сложения, так как при сложении мы складываем соответствующие коэффициенты полиномов, а коэффициенты принадлежат полю $GF(2^m)$.

Пусть $p(x)=a_{k-1}x^{k-1}+...+a_2x^2+a_1x+a_0;\ q(x)=b_{k-1}x^{k-1}+...+b_2x^2+b_1x+b_0;$ $p(x),q(x)\in GF((2^m)^k), a_i,b_i\in GF(2^m), i=1..k-1$. Для того, чтобы умножить два элемента поля $GF((2^m)^k)$, нам необходимо умножить соответствующие полиномы $p(x),q(x)$ и взять остаток от деления на неприводимый в поле многочлен $f(x)$.

Рассмотри более конкретный случай — произведение в поле вида $GF((2^m)^2)$.
Учитывая рекомендации по подбору неприводимого многочлена(см. пункт А. - «*рекомендуется брать многочлены вида* x^m+ax+b ») будем искать неприводимый полином в виде $f(x)=x^2+sx+k$, где $s,k\in GF(2^m), s,k\neq 0$.
Пусть $a(x)=a_1x+a_0,\ b(x)=b_1x+b_0;\ a_i,b_i\in GF(2^m), i=0,1$, тогда

$$a(x)b(x)=(a_1x+a_0)(b_1x+b_0)=a_1b_1x^2+(a_1b_0+a_0b_1)x+a_0b_0$$

Учитывая, что $x^2=sx+k\ \ mod\ f(x)$, получим

$$a(x)b(x)=a_1b_1(sx+k)+(a_1b_0+a_0b_1)x+a_0b_0=(a_1b_0+a_0b_1+sa_1b_1)x+(ka_1b_1+a_0b_0)$$

Таким образом, произведение в $GF((2^m)^2)$ реализуется с помощью 7 произведений в поле $GF(2^m)$. Так как поле $GF(2^m)$ замкнуто относительно умножения, то и поле $GF((2^m)^2)$ замкнуто относительно умножения, определенного по формуле выше (так как мы определили умножение в $GF((2^m)^2)$ через умножение в $GF(2^m)$).

Наконец перейдем к построение поля $GF((2^2)^2)$.
Поле $GF((2^2)^2)$ может быть представлено как множество всех полиномов степени не более 2 с коэффициентами в поле $GF(2^2)$, то есть $p(x)\in GF((2^2)^2), p(x)=a_1x+a_0$, $a_0,a_1\in GF(2^2)$.

В двоичном представлении каждый элемент поля $GF((2^2)^2)$ может быть представлен как битовая строка длины 4, которую разбили на 2 последовательных строки длины 2. Каждая строка длины 2 соответствует коэффициенту из основного поля $GF(2^2)$.

Например:
Пусть $p(x)\in GF((2^2)^2);\ p(x)=\beta x+1;\ \beta,1\in GF(2^2)$, β - примитивный элемент $GF(2^2)$. Можем представить $p(x)$ в виде набора коэффициентов $[\beta,1]$ или в виде двоичной битовой строки $[10,01]$.

Найдем неприводимый в $GF(2^2)$ многочлен вида x^2+sx+k. Полином 2 степени может быть разложен только в полиномы первой степени. Полиномы 1 степени с коэффициентами в $GF(2^2)$ (напомню, что элементами $GF(2^2)$ является множество $\{0,1,\beta,\beta^2=\beta+1\}$):

$x, x+1, x+\beta, x+\beta^2$

$\beta x, \beta x+1, \beta x+\beta, \beta x+\beta^2$

$\beta^2 x, \beta^2 x+1, \beta^2 x+\beta, \beta^2 x+\beta^2$

Так как в полиноме x^2+sx+k есть свободный член, то все полиномы 1 степени без свободного члена не могут являться его делителями. Тогда остаются следующие полиномы 1 степени:

$x+1, x+\beta, x+\beta^2$

$\beta x+1, \beta x+\beta, \beta x+\beta^2$

$\beta^2 x+1, \beta^2 x+\beta, \beta^2 x+\beta^2$

Проверим полином x^2+x+1.

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

Получили, что $x^2+x+1=(x+\beta)(x+\beta^2)$ в $GF(2^2)$. Таким образом, полином x^2+x+1 не является неприводимым в $GF(2^2)$.

Рассмотрим полином $x^2+x+\beta$.

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

$x+1$ не делит $x^2+x+\beta$ без остатка.

$x^2+x+\beta$	$x+\beta$
$x^2+\beta x$	$x+\beta^2$
$\beta^2 x+\beta$	
$\beta^2 x+1$	
β^2	

$x+\beta$ не делит $x^2+x+\beta$ без остатка.

$$\begin{array}{l|l} x^2+x+\beta & x+\beta^2 \\ \hline x^2+\beta^2 x & x+\beta \\ \hline \quad \beta x+\beta & \\ \quad \beta x+1 & \\ \hline \qquad \beta^2 & \end{array}$$

$x+\beta^2$ не делит $x^2+x+\beta$ без остатка.

$$\begin{array}{l|l} x^2+x+\beta & \beta x+1 \\ \hline x^2+\beta^2 x & \beta^2 x+1 \\ \hline \quad \beta x+\beta & \\ \quad \beta x+1 & \\ \hline \qquad \beta & \end{array}$$

$\beta x+1$ не делит $x^2+x+\beta$ без остатка.

$$\begin{array}{l|l} x^2+x+\beta & \beta x+\beta \\ \hline x^2+x & \beta^2 x \\ \hline 0+0+\beta & \end{array}$$

$\beta x+\beta$ не делит $x^2+x+\beta$ без остатка.

$$\begin{array}{l|l} x^2+x+\beta & \beta x+\beta^2 \\ \hline x^2+\beta x & \beta^2 x+\beta \\ \hline \quad \beta^2 x+\beta & \\ \quad \beta^2 x+1 & \\ \hline \qquad \beta^2 & \end{array}$$

$\beta x+\beta^2$ не делит $x^2+x+\beta$ без остатка.

$$\begin{array}{l|l} x^2+x+\beta & \beta^2 x+1 \\ \hline x^2+\beta x & \beta x+1 \\ \hline \quad \beta^2 x+\beta & \\ \quad \beta^2 x+1 & \\ \hline \qquad \beta^2 & \end{array}$$

$\beta^2 x+1$ не делит $x^2+x+\beta$ без остатка.

$x^2+x+\beta$	$\beta^2 x+\beta$
$x^2+\beta^2 x$	$\beta x+\beta^2$
$\beta x+\beta$	
$\beta x+1$	
β^2	

$\beta^2 x+\beta$ не делит $x^2+x+\beta$ без остатка.

$x^2+x+\beta$	$\beta^2 x+\beta^2$
x^2+x	βx
$0+0+\beta$	

$\beta^2 x+\beta^2$ не делит $x^2+\beta x+1$ без остатка.

В итоге получаем, что полином $f(x)=x^2+x+\beta$ является неприводимым в $GF(2^2)$.

Пусть $\gamma(x)=x\in GF((2^2)^2)$ - корень неприводимого многочлена $f(x)=x^2+x+\beta$, над которым мы строим конечное поле $GF((2^2)^2)$.

Построим поле $GF((2^2)^2)$ по модулю многочлена $f(x)=x^2+x+\beta$. Из того, что в поле характеристики 2 выполняется равенство $-1=1\ (mod\,2)$ и $f(\gamma)=0$ получаем, что $\gamma^2=\gamma+\beta$. Выразим элементы поля через γ :

$\gamma^2=\gamma+\beta$
$\gamma^3=\gamma\gamma^2=\gamma(\gamma+\beta)=\gamma^2+\gamma\beta=\gamma+\beta+\gamma\beta=\beta^2\gamma+\beta$
$\gamma^4=\gamma\gamma^3=\gamma(\beta^2\gamma+\beta)=\beta^2(\gamma+\beta)+\gamma\beta=\beta^2\gamma+\beta^3+\gamma\beta=\beta^2\gamma+\gamma\beta+1=\gamma(\beta^2+\beta)+1=\gamma+1$
$\gamma^5=\gamma\gamma^4=\gamma(\gamma+1)=\gamma^2+\gamma=\beta+\gamma+\gamma=\beta$
$\gamma^6=\gamma\gamma^5=\beta\gamma$
$\gamma^7=\gamma\gamma^6=\beta\gamma^2=\beta(\gamma+\beta)=\beta\gamma+\beta^2$
$\gamma^8=\gamma\gamma^7=\gamma(\beta\gamma+\beta^2)=\beta\gamma^2+\beta^2\gamma=\beta(\gamma+\beta)+\beta^2\gamma=\beta\gamma+\beta^2+\beta^2\gamma=\gamma(\beta^2+\beta)+\beta^2=\gamma+\beta^2$
$\gamma^9=\gamma\gamma^8=\gamma(\gamma+\beta^2)=\gamma^2+\gamma\beta^2=\gamma+\beta+\gamma\beta^2=\gamma(\beta^2+1)+\beta=\beta\gamma+\beta$
$\gamma^{10}=\gamma\gamma^9=\gamma(\beta\gamma+\beta)=\beta\gamma^2+\beta\gamma=\beta(\gamma+\beta)+\beta\gamma=\beta\gamma+\beta^2+\beta\gamma=\beta^2$
$\gamma^{11}=\gamma\gamma^{10}=\gamma\beta^2$
$\gamma^{12}=\gamma\gamma^{11}=\gamma^2\beta^2=\beta^2(\beta+\gamma)=\beta^3+\gamma\beta^2=1+\beta^2\gamma$
$\gamma^{13}=\gamma\gamma^{12}=\gamma(1+\beta^2\gamma)=\gamma+\beta^2\gamma^2=\gamma+\beta^2(\gamma+\beta)=\gamma+\beta^2\gamma+\beta^3=\gamma(\beta^2+1)+1=\beta\gamma+1$
$\gamma^{14}=\gamma\gamma^{13}=\gamma(\beta\gamma+1)=\beta\gamma^2+\gamma=\beta(\gamma+\beta)+\gamma=\beta\gamma+\beta^2+\gamma=\gamma(\beta+1)+\beta^2=\beta^2\gamma+\beta^2$
$\gamma^{15}=\gamma\gamma^{14}=\gamma(\beta^2\gamma+\beta^2)=\beta^2\gamma^2+\beta^2\gamma=\beta^2(\gamma+\beta)+\beta^2\gamma=\beta^2\gamma+\beta^3+\beta^2\gamma=1$

Минимальное $k>0$ такое, что $\gamma^k=1$ равно $2^4-1=15$, следовательно γ является примитивным элементом , а $f(x)=x^2+x+\beta$ - примитивным многочленом поля $GF((2^2)^2)$.

Любой другой ненулевой элемент может быть получен как степень γ^k , где k - целое число, взаимно простое с $2^4-1=15$.

В свою очередь степень γ^k , где k - целое число, взаимно простое с $2^4-1=15$, может быть представлена в виде $a_1\gamma+a_0$, где γ - примитивный элемент, $a_i \in GF(2^2), i=0,1$. Будем также использовать представление элементов $GF((2^2)^2)$ в виде двоичного вектора $(a_1, a_0), a_i \in GF(2^2), i=0,1$, например, полиному $\beta^2 x+1$ соответствует число $[11\ 01]$.

Составим таблицу, содержащую все элементы поля:

0	0	00 00
1	1	00 01
γ	γ	01 00
γ^2	$\gamma+\beta$	01 10
γ^3	$\beta^2\gamma+\beta$	11 10
γ^4	$\gamma+1$	01 01
γ^5	β	00 10
γ^6	$\gamma\beta$	10 00
γ^7	$\beta\gamma+\beta^2$	10 11
γ^8	$\gamma+\beta^2$	01 11
γ^9	$\beta\gamma+\beta$	10 10
γ^{10}	β^2	00 11
γ^{11}	$\beta^2\gamma$	11 00
γ^{12}	$\beta^2\gamma+1$	11 01
γ^{13}	$\beta\gamma+1$	10 01
γ^{14}	$\beta^2\gamma+\beta^2$	11 11

Построим таблицу сложения в $GF((2^2)^2)$ (будем использовать двоичную запись):

+	00 00	00 01	00 10	00 11	01 00	01 01	01 10	01 11	10 00	10 01	10 10	10 11	11 00	11 01	11 10	11 11
00 00	00 00	00 01	00 10	00 11	01 00	01 01	01 10	01 11	10 00	10 01	10 10	10 11	11 00	11 01	11 10	11 11
00 01	00 01	00 00	00 11	00 10	01 01	01 00	01 11	01 10	10 01	10 00	10 11	10 10	11 01	11 00	11 11	11 10
00 10	00 10	00 11	00 00	00 01	01 10	01 11	01 00	01 01	10 10	10 11	10 00	10 01	11 10	11 11	11 00	11 01
00 11	00 11	00 10	00 01	00 00	01 11	01 10	01 01	01 00	10 11	10 10	10 01	10 00	11 11	11 10	11 01	11 00
01 00	01 00	01 01	01 10	01 11	00 00	00 01	00 10	00 11	11 00	11 01	11 10	11 11	10 00	10 01	10 10	10 11
01 01	01 01	01 00	01 11	01 10	00 01	00 00	00 11	00 10	11 01	11 00	11 11	11 10	10 01	10 00	10 11	10 10
01 10	01 10	01 11	01 00	01 01	00 10	00 11	00 00	00 01	11 10	11 11	11 00	11 01	10 10	10 11	10 00	10 01
01 11	01 11	01 10	01 01	01 00	00 11	00 10	00 01	00 00	11 11	11 10	11 01	11 00	10 11	10 10	10 01	10 00
10 00	10 00	10 01	10 10	10 11	11 00	11 01	11 10	11 11	00 00	00 01	00 10	00 11	01 00	01 01	01 01	01 11
10 01	10 01	10 00	10 11	10 10	11 01	11 00	11 11	11 10	00 01	00 00	00 11	00 10	01 01	01 00	01 11	01 10
10 10	10 10	10 11	10 00	10 01	11 10	11 11	11 00	11 01	00 10	00 11	00 00	00 01	01 10	01 11	01 00	01 01
10 11	10 11	10 10	10 01	10 00	11 11	11 10	11 01	11 00	00 11	00 10	00 01	00 00	01 11	01 10	01 01	01 00
11 00	11 00	11 01	11 10	11 11	10 00	10 01	10 10	10 11	01 00	01 01	01 10	01 11	00 00	00 01	00 10	00 11

11 01	11 01	11 00	11 11	11 10	10 01	10 00	10 11	10 10	01 01	01 00	01 11	01 10	00 01	00 00	00 11	00 10
11 10	11 10	11 11	11 00	11 01	10 10	10 11	10 00	10 01	01 10	01 11	01 00	01 01	00 10	00 11	00 00	00 01
11 11	11 11	11 10	11 01	11 00	10 11	10 10	10 01	10 00	01 11	01 10	01 01	01 00	00 11	00 10	00 01	00 00

Можно заметить, что таблицы сложения $GF((2^2)^2)$ и $GF(2^4)$ одинаковы с точностью до способа представления элементов.

Вернемся к произведению:

$\forall a(x),b(x)\in GF((2^2)^2)\colon\ a(x)b(x)=(a_1b_0+a_0b_1+sa_1b_1)x+(a_1b_1k+a_0b_0),\ s,k,a_i,b_i\in GF(2^2),i=0,1$

Так как мы искали полином в виде x^2+sx+k и полином $f(x)=x^2+x+\beta$ является примитивным в $GF(2^2)$, следовательно $s=1,k=\beta$, β - примитивный элемент поля $GF(2^2)$.

Тогда получаем формулу:

$\forall a(x),b(x)\in GF((2^2)^2)\colon\ a(x)b(x)=(a_1b_0+a_0b_1+a_1b_1)x+(a_1b_1\beta+a_0b_0),\ a_i,b_i\in GF(2^2),i=0,1$

Рассмотрим пример:

Пусть $a(x)=\beta x+1,b(x)=x+\beta^2,\ a(x),b(x)\in GF((2^2)^2);\ 1,\beta,\beta^2\in GF(2^2)$.

Тогда по формуле получаем:

$$a(x)b(x)=(\beta\beta^2+1*1+\beta*1)x+(\beta*1*\beta+1*\beta^2)=(\beta^3+1+\beta)x+(\beta^2+\beta^2)=$$

$$=(1+1+\beta)x+0=\beta x$$

Или в двоичном виде: $a(x)=[10\ \ 01],\ b(x)=[01\ \ 11];\quad a(x)b(x)=[10\ \ 00]$

Построим таблицу умножения в $GF((2^2)^2)$ (будем использовать двоичную запись)

*	00 00	00 01	00 10	00 11	01 00	01 01	01 10	01 11	10 00	10 01	10 10	10 11	11 00	11 01	11 10	11 11
00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00
00 01	00 00	00 01	00 10	00 11	01 00	01 01	01 10	01 11	10 00	10 01	10 10	10 11	11 00	11 01	11 10	11 11
00 10	00 00	00 10	00 11	00 01	10 00	10 10	10 11	10 01	11 00	11 10	11 11	11 01	01 00	01 10	01 11	01 01
00 11	00 00	00 11	00 01	00 10	11 00	11 11	11 01	10 10	01 00	01 11	01 01	01 10	10 00	10 11	10 01	10 10
01 00	00 00	01 00	10 00	11 00	01 10	00 10	11 10	10 10	10 11	11 11	00 11	01 11	11 01	10 01	01 01	00 01
01 01	00 00	01 01	10 10	11 11	00 10	01 11	10 00	11 01	00 11	01 10	10 01	11 00	00 01	01 00	10 11	11 10
01 10	00 00	01 10	10 11	11 01	11 10	10 00	01 01	00 11	01 11	00 01	11 00	10 10	10 01	11 11	00 10	01 00
01 11	00 00	01 11	10 01	11 10	10 10	11 01	00 11	01 00	11 11	10 00	01 10	00 01	01 01	00 10	11 00	10 11
10 00	00 00	10 00	11 00	01 00	10 11	00 11	01 11	11 11	11 01	01 01	00 01	10 01	01 10	11 10	10 10	00 10
10 01	00 00	10 01	11 10	01 11	11 11	01 10	00 01	10 00	01 01	11 00	10 11	00 10	10 10	00 11	01 00	11 01
10 10	00 00	10 10	11 11	01 01	00 11	10 01	11 00	01 10	00 01	10 11	11 10	01 00	00 10	10 00	11 01	01 11
10 11	00 00	10 11	11 01	01 10	01 11	11 00	10 10	00 01	10 01	00 10	01 00	11 11	11 10	01 01	00 11	10 00
11 00	00 00	11 00	01 00	10 00	11 01	00 01	10 01	01 01	01 10	10 10	00 10	11 10	10 11	01 11	11 11	00 11
11 01	00 00	11 01	01 10	10 11	10 01	01 00	11 11	00 10	11 10	00 11	10 00	01 01	01 11	10 10	00 01	11 00
11 10	00 00	11 10	01 11	10 01	01 01	10 11	00 10	11 00	10 10	01 00	11 01	00 11	11 11	00 01	10 00	01 10
11 11	00 00	11 11	01 01	10 10	00 01	11 10	01 00	10 11	00 10	11 01	01 11	10 00	00 11	11 00	01 10	10 01

3. Мы представили поле $GF(16)$ с помощью полей $GF(2^4)$ и $GF((2^2)^2)$. Однако можно заметить, что по структуре и способу построения эти поля отличаются. Рассмотрим, какая взаимосвязь между $GF(2^4)$ и $GF((2^2)^2)$.

По *теореме о существовании и единственности конечных полей*, для каждого простого числа p и натурального числа m существует конечное поле из $q=p^m$ элементов и все конечные поля из q элементов *изоморфны*.

Опр. Два поля A и B *изоморфны*, если между их элементами $\alpha\in A$ и $\beta\in B$ существует такое *взаимно однозначное соответствие* (называемое *изоморфизмом*), которое сохраняет операции сложения и умножения.

Пусть map - изоморфизм, т.е. такое преобразование, которое ставит в соответствие элементу $\alpha\in A$ единственный однозначно определенный элемент $map(\alpha)=\beta\in B$ и в то же время - элементу $\beta\in B$ единственный однозначно определенный элемент $map^{-1}(\beta)=\alpha\in A$ и при этом обладает следующими свойствами:

$$map(\alpha+\beta)=map(\alpha)+map(\beta)$$
$$map(\alpha*\beta)=map(\alpha)*map(\beta)$$

Рассмотрим, как задать изоморфизм между двумя полями A и B.
Пусть $\alpha\in A$ есть примитивный элемент поля A, $f(x)$ - его примитивный многочлен степени m, т.е $f(\alpha)=0$. Пусть $\beta\in B$ есть примитивный элемент поля B. Тогда из теории конечных полей следует, что в поле B найдется такой элемент β^k, что $f(\beta^k)=0$. Так как β^k - корень примитивного многочлена $f(x)$, β^k является примитивным элементом. Поле A есть множество многочленов от α степени не выше, чем $m-1$, а поле B есть множество многочленов от β степени не выше, чем $m-1$. Тогда взаимно однозначное соответствие $\alpha\Leftrightarrow\beta^k$ задает изоморфизм полей A и B.

Тогда сохранение операций сложения и умножения, требуемое в определении изоморфизма, при установлении соответствия $\alpha\Leftrightarrow\beta^k$ означает, что $\forall a,b,c\in Z:\alpha^a\Leftrightarrow\beta^a,\alpha^b\Leftrightarrow\beta^b$ выполняются следующие условия: из $\alpha^a+\alpha^b=\alpha^c$ и $(\beta^k)^a+(\beta^k)^b=(\beta^k)^c$ по взаимно однозначному соответствию следует
1) $\alpha^c\Leftrightarrow(\beta^k)^c$
2) $\alpha^{a+b}\Leftrightarrow(\beta^k)^{(a+b)}$

Теперь рассмотрим наши конкретные 2 поля: $GF(2^4)$ и $GF((2^2)^2)$. Тогда согласно описанной выше последовательности действий, полем A является $GF(2^4)$, α - примитивный элемент, $f(x)=x^4+x+1$ - примитивный многочлен этого поля. Полем B является $GF((2^2)^2)$, γ - примитивный элемент этого поля. Найдем γ^k такие, что $f(\gamma^k)=(\gamma^k)^4+\gamma^k+1=0$.

Рассмотрим $k=1,\gamma^1=\gamma$: по таблице сложения получаем $\gamma^4+\gamma+1=0$, следовательно $\alpha\Leftrightarrow\gamma$. Также подходят $k=2,4,8$, читатель может проверить эти значения самостоятельно.

Проверим, что данное соответствие удовлетворяет свойствам изоморфизма:
1) Пусть $a=2,b=6$. Тогда $\alpha^2\Leftrightarrow\gamma^2,\alpha^6\Leftrightarrow\gamma^6$, необходимо проверить, что $\alpha^2+\alpha^6\Leftrightarrow\gamma^2+\gamma^6$.

Имеем по таблицам сложения $\alpha^2+\alpha^6=\alpha^3$ и $\gamma^2+\gamma^6=\gamma^3$. Следовательно $\alpha^2+\alpha^6 \Leftrightarrow \gamma^2+\gamma^6$, $\alpha^3 \Leftrightarrow (\gamma^1)^3$, что и требовалось доказать.

2) Второе свойство проверяется легко по свойствам умножения через экспоненциальное представление элементов поля как степеней генерирующего элемента $\forall n,k \in Z \;\; \alpha^{n+k}=\alpha^n \alpha^k \Leftrightarrow \gamma^n \gamma^k = \gamma^{n+k}$, следовательно $\alpha^{n+k} \Leftrightarrow (\gamma^1)^{(n+k)}$, что и требовалось доказать.

Мы рассмотрели один из способов определения изоморфизма для конченых полей, однако могут возникнуть ситуации, когда удобнее оперировать двоичными векторами, через которые выражаются элементы полей.

Хорошо известно, что элемент в одном поле связан с соответствующим ему элементом в другом поле (рассматриваемые поля изоморфны) линейным преобразованием. Так как преобразование между полями линейное, его можно осуществить с помощью матрицы.

Пусть map - изоморфизм. Линейное преобразование ставит в соответствие элементы изоморфных полей в виде степеней соответствующих примитивных элементов:

$\beta^k = map(\alpha^k)$

$\alpha^k = map^{-1}(\beta^k)$

Опр. *Линейное векторное пространство(ЛВП) над полем* — это множество элементов, называемых *векторами*, для которых определены операции сложения друг с другом и умножения на число (называемое *скаляром*). Эти операции подчинены аксиомам линейного векторного пространства.

Опр. Пусть $a_1,...,a_n \in GF(p^m)$ - скаляры, $v_1,...,v_n \in V$ - векторы, где V - ЛВП над $GF(p^m)$. Тогда выражение вида $a_1 v_1 + a_2 v_2 + ... + a_n v_n$ называется *линейной комбинацией* векторов $v_1,...,v_n$.

Опр. *Базис* — упорядоченный набор векторов в ЛВП, такой, что любой вектор этого пространства может быть единственным образом представлен в виде линейной комбинации векторов из этого набора.

Рассмотрим ЛВП над полем $GF(p^m), p \in P, m \in Z$. Его элементами будут вектора размерности m с координатами в поле $GF(p)$.

Тогда, переход от одного конечного поля к другому сводится к переходу от одного базиса ЛВП к другому базису.

Чтобы перейти от одного базиса ЛВП, необходимо задать матрицу перехода от базиса к базису.

Опр. Если векторы $\vec{e_1}', ..., \vec{e_n}'$ выражаются через векторы $\vec{e}_1, ..., \vec{e}_n$ как:

$$\begin{cases} \vec{e_1}' = \alpha_{11}\vec{e}_1 + ... + \alpha_{n1}\vec{e}_n \\ \vec{e_2}' = \alpha_{12}\vec{e}_1 + ... + \alpha_{n2}\vec{e}_n \\ ... \\ \vec{e_n}' = \alpha_{1n}\vec{e}_1 + ... + \alpha_{nn}\vec{e}_n \end{cases}$$

то матрица перехода от базиса $(\vec{e}_1, ..., \vec{e}_n)$ к базису $(\vec{e_1}', ..., \vec{e_n}')$ будет:

$$T_{e\to e'}=\begin{pmatrix}\alpha_{11} & \alpha_{12} & \dots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n}\\ \dots & \dots & \dots & \dots\\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn}\end{pmatrix}$$

Тогда $x'=T_{e\to e'}x$.

Для больших подробностей читатель может посмотреть теорию по линейной алгебре.

Вернемся к рассматриваемому нами случаю — преобразование из $GF((2^2)^2)$ в $GF(2^4)$ и обратно.

Элементами ЛВП над полем $GF((2^2)^2)$ будут вектора размерности 4, координаты которых принадлежат полю $GF(2)$.

Самым простым и очевидном выбором базиса будет являться набор векторов $e_1=(1,0,0,0)$, $e_2=(0,1,0,0), e_3=(0,0,1,0), e_4=(0,0,0,1)$, который удовлетворяет всем требованиям к базису.

Этот набор векторов соответствует определенным элементам поля $GF((2^2)^2)$:

$e_1=(1,0,0,0)\Leftrightarrow \gamma^6$

$e_2=(0,1,0,0)\Leftrightarrow \gamma$

$e_3=(0,0,1,0)\Leftrightarrow \gamma^5$

$e_4=(0,0,0,1)\Leftrightarrow \gamma^0$

Так как мы хотим отображать элементы в виде степеней соответствующих примитивных элементов ($\alpha^k=map(\gamma^k);\ \gamma^k=map^{-1}(\alpha^k), \gamma\in GF((2^2)^2), \alpha\in GF(2^4)$), то в качестве базиса поля $GF(2^4)$ необходимо взять соответствующие элементы примитивного элемента($\alpha^6, \alpha, \alpha^5, \alpha^0$).

Имеем базис $GF(2^4)$:

$\alpha^6\Leftrightarrow e_1'=(1,1,0,0)=e_1+e_2=\gamma^6+\gamma$

$\alpha\Leftrightarrow e_2'=(0,0,1,0)=e_3=\gamma^5$

$\alpha^5\Leftrightarrow e_3'=(0,1,1,0)=e_2+e_3=\gamma+\gamma^5$

$\alpha^0\Leftrightarrow e_4'=(0,0,0,1)=e_4=\gamma^0$

Получим матрицу перехода:

$$T_{e\to e'}=\begin{pmatrix}1 & 0 & 0 & 0\\ 1 & 0 & 1 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}$$

Матрица перехода от базиса к базису обладает следующим свойством:

$T^{-1}_{e\to e'}=T_{e'\to e}$

Таким образом, матрица преобразования имеет размер $4x4$ и является битовой матрицей, то есть состоит из двоичных чисел. Обратное преобразование осуществляется с помощью

обратной матрицы. Преобразование состоит в умножение по модулю 2 матрицы преобразования на вектор-столбец - двоичное представление элемента поля.

Пусть $a=\gamma^k \in GF((2^2)^2), b=\alpha^k \in GF(2^4), k \in Z$. Тогда:

$b=T_{(2^2)^2 \to 2^4} a$

$a=T^{-1}_{(2^2)^2 \to 2^4} b$,

где a - двоичное представление элемента в $GF((2^2)^2)$, b - двоичное представление элемента в $GF(2^4)$, T - матрица преобразования.

$$T_{(2^2)^2 \to 2^4}=\begin{pmatrix}1&0&0&0\\1&0&1&0\\0&1&1&0\\0&0&0&1\end{pmatrix}$$

Найдем обратную матрицу(напомню, что все значения берем по модулю 2):

$$T^{-1}_{(2^2)^2 \to 2^4}=T_{2^4 \to (2^2)^2}=\begin{pmatrix}1&0&0&0\\1&1&1&0\\1&1&0&0\\0&0&0&1\end{pmatrix}$$

Рассмотрим пример:

α - примитивный элемент $GF(2^4)$, γ - примитивный элемент $GF((2^2)^2)$.

$\alpha^{12}=(1,1,1,1)^T, \gamma^{12}=(1,1,0,1)^T$ - смотри соответствующие таблицы элементов.

$$T_{(2^2)^2 \to 2^4}\gamma^{12}=\begin{pmatrix}1&0&0&0\\1&0&1&0\\0&1&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1\\1\\0\\1\end{pmatrix}=\begin{pmatrix}1\\1\\1\\1\end{pmatrix}(mod\ 2)=\alpha^{12}$$

$$T_{2^4 \to (2^2)^2}\alpha^{12}=\begin{pmatrix}1&0&0&0\\1&1&1&0\\1&1&0&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}=\begin{pmatrix}1\\1\\0\\1\end{pmatrix}(mod\ 2)=\gamma^{12}$$

Проверим условие изоморфизма для случайных элементов:

$\gamma^5=(0010), \gamma^7=(1011)$

$\gamma^5+\gamma^7=(1001)=\gamma^{13}$

$T_{(2^2)^2 \to 2^4}(\gamma^5+\gamma^7)=T_{(2^2)^2 \to 2^4}\gamma^{13}=(1101)=\alpha^{13}$

$T_{(2^2)^2 \to 2^4}\gamma^5+T_{(2^2)^2 \to 2^4}\gamma^7=\alpha^5+\alpha^7=\alpha^{13}$

получаем $T_{(2^2)^2 \to 2^4}(\gamma^5+\gamma^7)=T_{(2^2)^2 \to 2^4}\gamma^5+T_{(2^2)^2 \to 2^4}\gamma^7$

$\alpha^5=(0110), \alpha^7=(1011)$

$\alpha^5+\alpha^7=(1101)=\alpha^{13}$

$T_{2^4 \to (2^2)^2}(\alpha^5+\alpha^7)=T_{2^4 \to (2^2)^2}\alpha^{13}=(1001)=\gamma^{13}$

$T_{2^4 \to (2^2)^2}\alpha^5+T_{2^4 \to (2^2)^2}\alpha^7=\gamma^5+\gamma^7=\gamma^{13}$

получаем $T_{2^4 \to (2^2)^2}(\alpha^5+\alpha^7)=T_{2^4 \to (2^2)^2}\alpha^5+T_{2^4 \to (2^2)^2}\alpha^7$

Следовательно, операция преобразования, заданная нами, изоморфна по сложению.

Для произведения:

$T_{(2^2)^2\to 2^4}(\gamma^5\gamma^7)=T_{(2^2)^2\to 2^4}(\gamma^{13})=\alpha^{13}$

$(T_{(2^2)^2\to 2^4}\gamma^5)(T_{(2^2)^2\to 2^4}\gamma^7)=\alpha^5\alpha^7=\alpha^{13}$

получаем $T_{(2^2)^2\to 2^4}(\gamma^5\gamma^7)=(T_{(2^2)^2\to 2^4}\gamma^5)(T_{(2^2)^2\to 2^4}\gamma^7)$

$T_{2^4\to(2^2)^2}(\alpha^5\alpha^7)=T_{2^4\to(2^2)^2}(\alpha^{13})=\gamma^{13}$

$(T_{2^4\to(2^2)^2}\alpha^5)(T_{2^4\to(2^2)^2}\alpha^7)=\gamma^5\gamma^7=\gamma^{13}$

получаем $T_{2^4\to(2^2)^2}(\alpha^5\alpha^7)=(T_{2^4\to(2^2)^2}\alpha^5)(T_{2^4\to(2^2)^2}\alpha^7)$

Следовательно, операция преобразования, заданная нами, изоморфна по умножению.

Для оставшихся элементов проверка осуществляется аналогично, читатель может их проверить самостоятельно.

4. В качестве еще одного примера, кратко опишем структуру поля $GF((2^4)^2)$

Поле $GF((2^4)^2)$ может быть представлено как множество всех полиномов степени не более 2 с коэффициентами в поле $GF(2^4)$, то есть $p(x)\in GF((2^4)^2), p(x)=a_1x+a_0$, $a_0, a_1\in GF(2^4)$.

В двоичном представлении каждый элемент поля $GF((2^4)^2)$ может быть представлен как битовая строка длины 8, которую разбили на 2 последовательных строки длины 4. Каждая строка длины 4 соответствует коэффициенту из основного поля $GF(2^4)$.

Например:

Пусть $p(x)\in GF((2^2)^2);\ p(x)=\alpha^2x+\alpha;\ \alpha, \alpha^2\in GF(2^4)$, α - примитивный элемент $GF(2^4)$. Можем представить $p(x)$ в виде набора коэффициентов $[\alpha^2, \alpha]$ или в виде двоичной битовой строки $[0100\ \ 0010]$.

Найдем неприводимый в $GF(2^4)$ многочлен вида x^2+sx+k. Использую компьютерную программу, перебором было получено, что многочлен $f(x)=x^2+\alpha^2x+\alpha$, α - примитивный элемент $GF(2^4)$, является неприводимым. Читатель может убедиться в этом самостоятельно, перебрал все возможные делители многочлена $f(x)$. Рассмотрим один из делителей, чтобы напомнить, как осуществляется проверка.

$x^2+\alpha^2x+\alpha$	$\alpha^2x+\alpha$
$x^2+\alpha^{14}x$	$\alpha^{13}x+\alpha^{11}$
$\alpha^{13}x+\alpha$	
$\alpha^{13}x+\alpha^{12}$	
α^{13}	

$\alpha^2x+\alpha$ не делит $f(x)$ без остатка.

Остальные делители проверяются аналогично.

Пусть λ - корень многочлена $f(x)$. Проверим, является ли λ примитивным элементом и, соответственно, $f(x)$ - примитивным многочленом.

Из теории конечных полей известно, что порядком элемента поля $GF(q)$ может быть только один из делителей числа $q-1$.

Для поля $GF((2^4)^2)$ $q=(2^4)^2=256$, таким образом, порядком элемента λ может быть только делитель числа $q-1=255$, т.е. одно из чисел: $1,3,5,15,17,51,85,255$. Поэтому, чтобы проверить, является ли элемент λ примитивным, необходимо найти минимальное целое $k\in\{1,3,5,15,17,51,85,255\}$, при котором $\lambda^k=1$.

Так как возводить элемент λ во все степени вручную может быть несколько утомительно, воспользуемся компьютерной программой. Результаты представлены ниже:

$\lambda^1=\lambda$
$\lambda^3=\lambda+\alpha^3$
$\lambda^5=\alpha^{10}\lambda+\alpha^7$
$\lambda^{15}=\alpha\lambda+\alpha^{14}$
$\lambda^{17}=\alpha$
$\lambda^{51}=\alpha^3$
$\lambda^{85}=\alpha^5$
$\lambda^{255}=1$

Минимальное $k>0$, такое что $\lambda^k=1$ равно $(2^4)^2-1=255$, следовательно λ является примитивным элементом, а - $f(x)=x^2+\alpha^2x+\alpha$ примитивным многочленом поля $GF((2^4)^2)$.

Сложение (и вычитывание) в поле о $GF((2^4)^2)$, как и в общем случае $GF((2^m)^k)$, осуществляется с помощью битового оператора XOR (исключающее «ИЛИ»). Так как поле $GF(2^4)$ замкнуто относительно операции сложения, то и поле $GF((2^4)^2)$ замкнуто относительно операции сложения.

Ранее мы определили произведение в поле вида $GF((2^m)^2)$ в следующем виде:

$\forall a(x),b(x)\in GF((2^m)^2):\ a(x)b(x)=(a_1b_0+a_0b_1+s\,a_1b_1)x+(k\,a_1b_1+a_0b_0),\ s,k,a_i,b_i\in GF(2^2),i=0,1$

Так как мы искали полином в виде x^2+sx+k и полином $f(x)=x^2+\alpha^2x+\alpha$ является неприводимым в $GF(2^4)$, следовательно $s=\alpha^2,k=\alpha$, α - примитивный элемент поля $GF(2^4)$.

Тогда получаем формулу для умножения элементов:

$\forall a(x),b(x)\in GF((2^4)^2):\ a(x)b(x)=(a_1b_0+a_0b_1+\alpha^2a_1b_1)x+(a_1b_1\alpha+a_0b_0),\ a_i,b_i\in GF(2^4),i=0,1$

Рассмотрим пример:
Пусть $a(x)=\alpha^2x+\alpha,b(x)=x+\alpha^3,\ a(x),b(x)\in GF((2^4)^2);\ \alpha,\alpha^2,\alpha^3\in GF(2^4)$.
Тогда по формуле получаем:

$$a(x)b(x)=(\alpha^2*\alpha^3+\alpha*1+\alpha^2*\alpha^2*1)x+(\alpha^2*1*\alpha+\alpha\alpha^3)=(\alpha^5+\alpha+\alpha^4)x+(\alpha^3+\alpha^4)=\alpha^{10}x+\alpha^7$$

Или в двоичном виде: $a(x)=[0100\ \ 0010],\ b(x)=[0001\ \ 1000];\quad a(x)b(x)=[0111\ \ 1011]$

На этом закончим рассмотрение полей вида $GF((2^m)^k)$.

II. Рассмотрим поля при $p=3$, т.е. поля вида $GF((3^m)^k)$

Ранее мы рассмотрим подход к построению полей вида $GF((p^m)^k)$ в общем виде. Поля вида $GF((3^m)^k)$ очевидно строятся по тем же правилам, однако, чтобы у читателя не возникло трудностей с построением произвольных полей вида $GF((p^m)^k)$ из-за привыкания к свойствам полей $GF((2^m)^k)$, кратко рассмотрим подход к построению полей $GF((3^m)^k)$, в частности, поля $GF((3^2)^2)$.

1. Построим поле Галуа $GF(3)$

$GF(3)$ - это поле, элементами которого является числа $\{0,1,2\}$ - остатки от деления целых чисел на 3. Сложение и умножение чисел осуществляется с приведение результата по модулю 3.

Поле конечное — состоит из $q=3$ элементов. $p=3$ является характеристикой поля $GF(3)$ т.е $\underbrace{1+1+1}_{3}=3\%3=0\ (mod\,3)$

В отличие от поля $GF(2)$, в поле $GF(3)$ сложение и вычитание — это разные операции, так как $-1\%3=2$ ($\forall a,b\in GF(3): a-b=a+2b$)

Построим таблицы сложения, умножения и вычитания для этого поля:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

-	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2. Построим поле Галуа $GF(3^2)$

$GF(3^2)$ - это множество всех полиномов степени не больше 2 с коэффициентами в $GF(3)$, то есть полиномов вида $p(x)=a_1x+a_0$, $a_i\in GF(3), i=0,1$.

Найдем неприводимый многочлен для построения поля $GF(3^2)$. Рассмотрим все приведенные многочлены степени 2 с коэффициентами в поле $GF(3)$:

$\{x^2, x^2+1, x^2+2, x^2+x, x^2+x+1, x^2+x+2, x^2+2x, x^2+2x+1, x^2+2x+2\}$

Так как делить полиномы 2 степени могут только полиномы 1 степени, достаточно проверить, является ли какой-нибудь элемент поля $GF(3)$ корнем многочлена. Многочлен, у которого не будет корней в $GF(3)$ будет являться неприводимым над этим полем.

Теперь исключим все полиномы без свободного члена, так как их корнем всегда является ноль.
Остаются следующие полиномы:

$\{x^2+1, x^2+2, x^2+x+1, x^2+x+2, x^2+2x+1, x^2+2x+2\}$

Теперь подставим $1\in GF(3)$ в оставшиеся полиномы:

$1^2+1=2$

$1^2+2=0(mod\,3)\Rightarrow x^2+2=(x+2)(x+1)$ *т.е. не является неприводимым*

$1^2+1+1=0(mod\,3)\Rightarrow x^2+x+1=(x+2)(x+2)$ *т.е. не является неприводимым*

$1^2+1+2=1(mod\,3)$

$1^2+2+1=1(mod\,3)$
$1^2+2+2=2(mod\,3)$

Остаются следующие полиномы:
$\{x^2+1, x^2+x+2, x^2+2x+1, x^2+2x+2\}$
Теперь подставим $2\in GF(3)$ в оставшиеся полиномы:
$2^2+1=2(mod\,3)$
$2^2+2+2=2(mod\,3)$
$2^2+2*2+1=0(mod\,3)$ *т.е. не является неприводимым*
$2^2+2*2+2=1(mod\,3)$

Таким образом, многочлены $\{x^2+1, x^2+x+2, x^2+2x+2\}$ являются неприводимыми над полем $GF(3)$.

Построим поле $GF(3^2)$ по модулю многочлена $f(x)=x^2+1$.

Пусть $\alpha \in GF(3^2)$ - корень неприводимого многочлена $f(x)$, над которым мы строим конечное поле $GF(3^2)$, т.е. $f(\alpha)=0$.
Попробуем построить поле, возводя в степень α . Из того, что $f(\alpha)=0$, получаем
$\alpha^2+1=0; \alpha^2=2$.

$\alpha^0=1$
$\alpha^1=\alpha$
$\alpha^2=2$
$\alpha^3=\alpha\alpha^2=2\alpha$
$\alpha^4=\alpha\alpha^3=2\alpha^2=1(mod\,3)$
Получили, что корень α порождает не все ненулевые элементы поля $GF(3^2)$, а только подмножество из 4 элементов.

Будем искать генерирующий элемент в виде $\alpha+x, x=b_1\alpha+b_0, b_i\in GF(3), i=1,2$.
Рассмотрим элемент $\alpha+1$:
$(\alpha+1)^0=1$
$(\alpha+1)^1=\alpha+1$
$(\alpha+1)^2=\alpha^2+2\alpha+1=2\alpha$
$(\alpha+1)^3=\alpha^3+1=2\alpha+1$
$(\alpha+1)^4=(2\alpha)^2=\alpha^2=2$
$(\alpha+1)^5=(\alpha+1)(\alpha+1)^4=(\alpha+1)*2=2\alpha+2$
$(\alpha+1)^6=(2\alpha)^3=2\alpha^3=2*2\alpha=\alpha$
$(\alpha+1)^7=(\alpha+1)(\alpha+1)^6=(\alpha+1)\alpha=\alpha^2+\alpha=\alpha+2$
$(\alpha+1)^8=((\alpha+1)^4)^2=2^2=1$

Таким образом, поле $GF(3^2)$ построено по модулю неприводимого многочлена $f(x)=x^2+1$, но в степени возводился не корень этого многочлена α , а элемент $\alpha+1$, являющийся генерирующим элементом.

Пусть $p(x), q(x)\in GF(3^2), p(x)=a_1x+a_0, q(x)=b_1x+b_0; a_i, b_i\in GF(3), i=1,2$. Тогда
$p(x)+q(x)=(a_1x+a_0)+(b_1x+b_0)=(a_1+b_1)x+(a_0+b_0)$

$$p(x)q(x)=(a_1x+a_0)(b_1x+b_0)=a_1b_1x^2+a_1b_0x+a_0b_1x+a_0b_0$$

Так как мы строим поле $GF(3^2)$ по модулю $f(x)=x^2+1$, то $x^2=2(mod\,3)$. Получаем:

$$p(x)q(x)=2a_1b_1+(a_1b_0+a_0b_1)x+a_0b_0=(a_1b_0+a_0b_1)x+(a_0b_0+2a_1b_1)$$

Как мы уже говорили, $GF(3^2)$ - это множество всех полиномов вида $p(x)=a_1x+a_0$, $a_i\in GF(3), i=0,1$. Можно представить элемент $p(x)$ поля $GF(3)$ в виде вектора (a_1,a_0) размерности 2 с координатами в $GF(3)$. Например, $2x+1\in GF(3^2)$ можно представить в виде вектора $(2,1)$.

Построим таблицу сложения в $GF(3^2)$ (для компактности будем использовать векторную запись):

+	00	01	02	10	11	12	20	21	22
00	00	01	02	10	11	12	20	21	22
01	01	02	00	11	12	10	21	22	20
02	02	00	01	12	10	11	22	20	21
10	10	11	12	20	21	22	00	01	02
11	11	12	10	21	22	20	01	02	00
12	12	10	11	22	20	21	02	00	01
20	20	21	22	00	01	02	10	11	12
21	21	22	20	01	02	00	11	12	10
22	22	20	21	02	00	01	12	10	11

Например: $1+(2x+2)=2x+3=2x$
$(0,1)+(2,2)=(2,3)mod\,3=(2,0)$

Построим таблицу умножения в $GF(3^2)$ (для компактности будем использовать векторную запись):

*	00	01	02	10	11	12	20	21	22
00	00	00	00	00	00	00	00	00	00
01	00	01	02	10	11	12	20	21	22
02	00	02	01	20	22	21	10	12	11
10	00	10	20	02	12	22	01	11	21
11	00	11	22	12	20	01	21	02	10
12	00	12	21	22	01	10	11	20	02
20	00	20	10	01	21	11	02	22	12
21	00	21	12	11	02	20	22	10	01
22	00	22	11	21	10	02	12	01	20

Например: $(x+2)x=(1*0+2*1)x+(2*0+2*1*1)=2x+2$
$(1,2)*(1,0)=(2,2)$

Также для выполнения арифметических операций можно использовать представление элементов поля через генерирующий элемент $\alpha+1$. Тогда для примера выше:
$(\alpha+2)\alpha=(\alpha+1)^7(\alpha+1)^6=(\alpha+1)^{(13\%(3^2-1))}=(\alpha+1)^5=2\alpha+2\Leftrightarrow(2,2)$.

Используя уже знакомые нам формулы через экспоненциальное представление генерирующего элемента, можно аналогично осуществлять другие арифметические операции.

3. Построим поле Галуа $GF((3^2)^2)$.
Поле $GF((3^2)^2)$ может быть представлено как множество всех полиномов степени не более 2 с коэффициентами в поле $GF(3^2)$, то есть $p(x)\in GF((3^2)^2), p(x)=a_1x+a_0$, $a_0,a_1\in GF(3^2)$.

В векторном представлении каждый элемент поля $GF((3^2)^2)$ может быть представлен как битовая строка длины 4, которую разбили на 2 последовательных строки длины 2. Каждая строка длины 2 соответствует коэффициенту из основного поля $GF(3^2)$.

Например:
Пусть $p(x)\in GF((3^2)^2);\ p(x)=\alpha x+1;\ \alpha,1\in GF(3^2)$, α - корень неприводимого многочлена x^2+1, по модулю которого мы строили поле $GF(3^2)$. Можем представить $p(x)$ в виде набора коэффициентов $(\alpha,1)$ или в виде двоичной битовой строки $(10,01)$.

Найдем неприводимый в $GF(3^2)$ многочлен вида $x^2+sx+k;\ s,k\in GF(3^2)$. Так как делить полиномы 2 степени могут только полиномы 1 степени, достаточно проверить, является ли какой-нибудь элемент поля $GF(3^2)$ корнем многочлена. Многочлен, у которого не будет корней в $GF(3^2)$ будет являться неприводимым над этим полем.

Например:
Рассмотрим полином x^2+1. Тогда $\alpha\in GF(3^2)$ является корнем этого многочлена, так как $\alpha^2+1=2+1=0$.

Рассмотрим другой многочлен - x^2+x+1. Его корнем является $1\in GF(3^2)$: $1^2+1+1=0$.

Использую компьютерную программу, перебором было получено, что многочлен $x^2+x+\alpha$, α - корень неприводимого многочлена x^2+1, по модулю которого мы строили поле $GF(3^2)$, является неприводимым.

Действительно, элементами поля $GF(3^2)$ являются $\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$. Тогда:

0: $0+0+\alpha=\alpha$
1: $1^2+1+\alpha=\alpha+2$
2: $2^2+2+\alpha=\alpha$
α: $\alpha^2+\alpha+\alpha=\alpha^2+2\alpha$
$\alpha+1$: $(\alpha+1)^2+(\alpha+1)+\alpha=2\alpha+2\alpha+1=\alpha+1$
$\alpha+2$: $(\alpha+2)^2+(\alpha+2)+\alpha=\alpha^2+4\alpha+4+2\alpha+2=2$

2α: $(2\alpha)^2+2\alpha+\alpha=4\alpha^2=4*2=2$
$2\alpha+1$: $(2\alpha+1)^2+(2\alpha+1)+\alpha=(4\alpha^2+4\alpha+1)+1=\alpha+1$
$2\alpha+2$: $(2\alpha+2)^2+(2\alpha+2)+\alpha=(4\alpha^2+8\alpha+4)+2=2\alpha+2$

Что и требовалось доказать.

Пусть $p(x),q(x)\in(GF(3^2)^2), p(x)=a_1x+a_0, q(x)=b_1x+b_0; a_i,b_i\in GF(3^2), i=1,2$. Тогда
$p(x)+q(x)=(a_1x+a_0)+(b_1x+b_0)=(a_1+b_1)x+(a_0+b_0)$

$p(x)q(x)=(a_1x+a_0)(b_1x+b_0)=a_1b_1x^2+a_1b_0x+a_0b_1x+a_0b_0$

Так как мы искали неприводимый полином в виде $x^2+sx+k; s,k\in GF(3^2)$, то
$x^2=-sx-k=2sx+2k$. Тогда получаем формулу в общем виде:

$p(x)q(x)=a_1b_1(2sx+2k)+(a_1b_0+a_0b_1)x+a_0b_0=(2a_1b_1s+a_1b_0+a_0b_1)x+(a_0b_0+2ka_1b_1)$

Так как $x^2+x+\alpha$ неприводимый, то $s=1,\ k=\alpha$. Получим формулу:
$p(x)q(x)=(2a_1b_1+a_1b_0+a_0b_1)x+(a_0b_0+2\alpha a_1b_1)$.

Рассмотрим пример:
$p(x)=(1,1)x+(2,1)\Leftrightarrow(11,21)$
$q(x)=(0,2)x+(1,0)\Leftrightarrow(02,10)$

$p(x)+q(x)=[(1,1)+(0,2)]x+[(2,1)+(1,0)]=(1,0)x+(0,1)$

$p(x)q(x)=[2*(1,1)*(0,2)+(1,1)*(1,0)+(2,1)*(0,2)]x+[(2,1)*(1,0)+2*(1,0)*(1,1)*(0,2)]=$
$=[(1,1)+(1,2)+(1,2)]x+[(1,1)+(1,2)]=(0,2)x+(2,0)$

Пусть γ - корень неприводимого многочлена $x^2+x+\alpha$, по модулю которого мы строили поле. Проверим, является ли γ примитивным элементом.

Из теории конечных полей известно, что порядком элемента поля $GF(q)$ может быть только один из делителей числа $q-1$.

Для поля $GF((3^2)^2)$ $q=(3^2)^2=81$, таким образом, порядком элемента γ может быть только делитель числа $q-1=80$, т.е. одно из чисел: $1,2,4,5,8,10,16,20,40,80$. Поэтому, чтобы проверить, является ли элемент γ примитивным, необходимо найти минимальное целое $k\in\{1,2,4,5,8,10,16,20,40,80\}$, при котором $\gamma^k=1$.

$\gamma^1=\gamma$
$\gamma^2=2\gamma+2\alpha$
$\gamma^4=(2\alpha+2)\gamma+(2\alpha+2)$
$\gamma^5=\alpha+2$
$\gamma^8=2\alpha\gamma+(2\alpha+2)$
$\gamma^{10}=\alpha$
$\gamma^{16}=(2\alpha+2)\gamma$
$\gamma^{20}=2$
$\gamma^{40}=1$

Таким образом, минимальное k , при котором $\gamma^k=1$ равно $40\neq(3^2)^2-1$, следовательно γ не является примитивным элементом поля $GF((3^2)^2)$ и не генерирует все ненулевые элементы поля.

Будем искать генерирующий элемент в виде $\gamma+x$, $x=a_1\gamma+a_0, a_i\in GF(3^2), i=1,2$. Используя компьютерную программу, получили, что элемент $\gamma+(\alpha+1)$ является примитивным элементом поля $GF((3^2)^2)$:

$(\gamma+(\alpha+1))^1=\gamma+(\alpha+1)$
$(\gamma+(\alpha+1))^2=(2\alpha+1)\gamma+\alpha$
$(\gamma+(\alpha+1))^4=(\alpha+2)\gamma$
$(\gamma+(\alpha+1))^5=(2\alpha+2)\gamma+(\alpha+1)$
$(\gamma+(\alpha+1))^8=2\alpha\gamma+1$
$(\gamma+(\alpha+1))^{10}=2\alpha+2$
$(\gamma+(\alpha+1))^{16}=(\alpha+1)\gamma+(\alpha+1)$
$(\gamma+(\alpha+1))^{20}=2\alpha$
$(\gamma+(\alpha+1))^{40}=2$
$(\gamma+(\alpha+1))^{80}=1$

Что и требовалось доказать.

На этом закончим с построением поля $GF((3^2)^2)$.

4. Кратко рассмотрим поле Галуа $GF(3^4)$.
Конечное поле $GF(3^4)$ строится аналогично полю $GF(3^2)$, поэтому мы не будем полностью описывать его строение.

$GF(3^4)$ - это множество всех полиномов степени не больше 4 с коэффициентами в $GF(3)$, то есть полиномов вида $p(x)=a_3x^3+a_2x^2+a_1x+a_0$, $a_i\in GF(3), i=0..3$.

Воспользуемся таблицей примитивных полином для поля $GF(3)$. Полином x^4+x^3+2 является примитивным над полем $GF(3)$.

Данный многочлен выбран не случайно. Для поля $GF(3^4)$, построенного по модулю многочлена x^4+x^3+2 , можно задать изоморфизм с полем $GF((3^2)^2)$, построенного по модулю $x^2+x+\alpha$ (см. пункт 5).

Построим поле $GF(3^4)$ по модулю многочлена $f(x)=x^4+x^3+2$.

Пусть $\beta\in GF(3^4)$ - корень неприводимого многочлена $f(x)$, над которым мы строим конечное поле $GF(3^4)$, т.е. $f(\beta)=0$. Тогда все элементы поля можно представить в виде $a_3\beta^3+a_2\beta^2+a_1\beta+a_0$, где β - примитивный элемент, $a_i\in GF(3), i=0..3$.

Выразим через β первые несколько элементов:

$\beta^0=1$

$\beta^1=\beta$

$\beta^2=\beta^2$

$\beta^3=\beta^3$

$\beta^4=2\beta^3+1$

$\beta^5=\beta^3+\beta+2$

$\beta^6=2\beta^3+\beta^2+2\beta+1$

$\beta^7=2\beta^3+2\beta^2+\beta+2$

И так далее…

Как мы уже упоминали, каждое число представимо в виде $a_3\beta^3+a_2\beta^2+a_1\beta+a_0$ и $a_i\in GF(3), i=0..3$, следовательно мы можем задать каждый элемент поля в виде двоичного вектора, в котором каждая цифра соответствует коэффициентам a_i. Например, $\beta^7=2\beta^3+2\beta^2+\beta+2$ представим в виде 2212.

На этом закончим построение поля $GF(3^4)$. В случае необходимости, читатель может самостоятельно задать арифметические операции в этом поле аналогично случаю $GF(3^2)$

5. Построим изоморфизм между полями $GF((3^2)^2)$ и $GF(3^4)$.
Изоморфизм между полями $GF((3^2)^2)$ и $GF(3^4)$ задается аналогично изоморфизму между полями $GF((2^2)^2)$ и $GF(2^4)$.

Элементами ЛВП над полем $GF(3^4)$ будут вектора размерности 4, координаты которых принадлежат полю $GF(3)$.

Самым простым и очевидном выбором базиса будет являться набор векторов $e_1=(1,0,0,0)$, $e_2=(0,1,0,0), e_3=(0,0,1,0), e_4=(0,0,0,1)$, который удовлетворяет всем требованиям к базису.

Этот набор векторов соответствует определенным элементам поля $GF(3^4)$:

$e_1=(1,0,0,0)\Leftrightarrow\beta^3$

$e_2=(0,1,0,0)\Leftrightarrow\beta^2$

$e_3=(0,0,1,0)\Leftrightarrow\beta^1$

$e_4=(0,0,0,1)\Leftrightarrow\beta^0$

Напомним, что примитивным элементов поля $GF((3^2)^2)$ является $\gamma+(\alpha+1)$, где γ - корень неприводимого многочлена $x^2+x+\alpha$, α - корень неприводимого многочлена x^2+1.

Так как мы хотим отображать элементы в виде степеней соответствующих примитивных элементов ($\beta^k=map((\gamma+(\alpha+1))^k);(\gamma+(\alpha+1))^k=map^{-1}(\beta^k), \gamma\in GF((3^2)^2), \beta\in GF(3^4)$), то в качестве базиса поля $GF((3^2)^2)$ необходимо взять соответствующие элементы примитивного элемента($(\gamma+(\alpha+1))^3,(\gamma+(\alpha+1))^2,(\gamma+(\alpha+1))^1,(\gamma+(\alpha+1))^0$).

Имеем базис $GF((3^2)^2)$:

$(\gamma+(\alpha+1))^3 \Leftrightarrow e_1' = (2,1,0,1) = 2e_1+e_2+e_4$

$(\gamma+(\alpha+1))^2 \Leftrightarrow e_2' = (2,1,1,0) = 2e_1+e_2+e_3$

$(\gamma+(\alpha+1))^1 \Leftrightarrow e_3' = (0,1,1,1) = e_2+e_3+e_4$

$(\gamma+(\alpha+1))^0 \Leftrightarrow e_4' = (0,0,0,1) = e_4$

Получим матрицу перехода:

$$T_{e\to e'} = \begin{pmatrix} 2 & 2 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Преобразование состоит в умножение по модулю 3 матрицы преобразования на вектор-столбец - двоичное представление элемента поля.

Пусть $a = \beta^k \in GF(3^4), b = (\gamma+(\alpha+1))^k \in GF((2^2)^2), k \in Z$. Тогда:

$b = T_{2^4\to(2^2)^2} a$

$a = T^{-1}_{2^4\to(2^2)^2} b$,

где a - двоичное представление элемента в $GF(3^4)$, b - двоичное представление элемента в $GF((3^2)^2)$, T - матрица преобразования.

$$T_{3^4\to(3^2)^2} = \begin{pmatrix} 2 & 2 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Найдем обратную матрицу(напомню, что все значения берем по модулю 3):

$$T^{-1}_{3^4\to(3^2)^2} = T_{(3^2)^2\to 3^4} = \begin{pmatrix} 0 & 1 & 2 & 0 \\ 2 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 1 \end{pmatrix}$$

Не для любого поля $GF(3^4)$ и поля $GF((3^2)^2)$, которое мы определили по модулю многочлена $x^2+x+\alpha$, можно задать изоморфизм в таком виде. Перебором с помощью компьютерной программы было получено, что отображение элементов поля $GF(3^4)$, построенного по модулю x^4+x^3+2 , в элементы поля $GF((3^2)^2)$, построенного по модулю $x^2+x+\alpha$, и обратно будет удовлетворять всем условиям изоморфизма.

Рассмотрим пример:

β - примитивный элемент $GF(3^4)$, $\gamma+(\alpha+1)$ - примитивный элемент $GF((3^2)^2)$.

$\beta^7 = (2,2,1,2)^T, (\gamma+(\alpha+1))^7 = (2,2,0,2)^T$.

$$T_{3^4\to(3^2)^2}\beta^7 = \begin{pmatrix} 2 & 2 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 2 \\ 2 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 0 \\ 2 \end{pmatrix} (mod\ \ 3) = (\gamma+(\alpha+1))^7$$

$$T_{(3^2)^2\to 3^4}(\gamma+(\alpha+1))^7=\begin{pmatrix}0&1&2&0\\2&2&1&0\\1&1&0&0\\2&1&1&1\end{pmatrix}\begin{pmatrix}2\\2\\0\\2\end{pmatrix}=\begin{pmatrix}2\\2\\1\\2\end{pmatrix}(mod\,3)=\beta^7$$

Проверим условие изоморфизма для случайных элементов:

$\beta^4=(2,0,0,1),\beta^5=(1,0,1,2)$

$\beta^4+\beta^5=(0,0,1,0)=\beta$

$T_{3^4\to(3^2)^2}(\beta^4+\beta^5)=T_{3^4\to(3^2)^2}\beta=(0,1,1,1)=(\gamma+(\alpha+1))$

$T_{3^4\to(3^2)^2}\beta^4+T_{3^4\to(3^2)^2}\beta^5=(\gamma+(\alpha+1))^4+(\gamma+(\alpha+1))^5=(\gamma+(\alpha+1))$

получаем $T_{3^4\to(3^2)^2}(\beta^4+\beta^5)=T_{3^4\to(3^2)^2}\beta^4+T_{3^4\to(3^2)^2}\beta^5$

$(\gamma+(\alpha+1))^4=(1,2,0,0),(\gamma+(\alpha+1))^5=(2,2,1,1)$

$(\gamma+(\alpha+1))^4+(\gamma+(\alpha+1))^5=(0,1,1,1)=(\gamma+(\alpha+1))$

$T_{(3^2)^2\to 3^4}((\gamma+(\alpha+1))^4+(\gamma+(\alpha+1))^5)=T_{(3^2)^2\to 3^4}(\gamma+(\alpha+1))=(0,0,1,0)=\beta$

$T_{(3^2)^2\to 3^4}(\gamma+(\alpha+1))^4+T_{(3^2)^2\to 3^4}(\gamma+(\alpha+1))^5=\beta^4+\beta^5=\beta$

получаем $T_{(3^2)^2\to 3^4}((\gamma+(\alpha+1))^4+(\gamma+(\alpha+1))^5)=T_{(3^2)^2\to 3^4}(\gamma+(\alpha+1))^4+T_{(3^2)^2\to 3^4}(\gamma+(\alpha+1))^5$

Следовательно, операция преобразования, заданная нами, изоморфна по сложению.

Произведение проверяется тривиально (аналогично случаю полей $GF((2^2)^2)$ и $GF(2^4)$)

Для оставшихся элементов проверка осуществляется аналогично, читатель может их проверить самостоятельно.

На этом шаге закончим описание процесса построения полей Галуа вида $GF((p^m)^k)$, $p\in P;m,k\in Z$.

Автор надеется, что читатель теперь сможет самостоятельно построить произвольное конечное поле.

Вывод: в данной работе был описан подход к построению полей Галуа вида $GF((p^m)^k)$, $p\in P;m,k\in Z$ и в качестве примера рассмотрены поля при $p=2$ и $p=3$.

Список литературы:

1. Сагалович Ю.Л. Введение в алгебраические коды
2. Kevin M. Greenan, Ethan L. Miller, Thomas J. E. Schwarz, S.J. Optimizing Galois Field Arithmetic for Diverse Processor Architectures and Applications.
3. E. J. Weldon, Jr. Design of an Error Correction Subsystem for Use with a DDS-2 RDAT Tape System, Appendix E, Finite-Field Isomorphisms
4. Peter M. Maurer. Primitive Polynomials for the Field GF(3).

Приложение

В процессе работы автор использовал компьютерные программы, написанные на языке программирования Python 3. В процессе разработки кода использовалась среда Jupyter Notebook. Исходный код можно получить в открытом репозитории GitHub по ссылке «https://github.com/bountyHntr/galois_field/tree/master».

Данный код не претендует на эффективную реализацию соответствующих арифметических операций в полях Галуа и служит лишь для автоматизации подсчетов в относительно больших (с точки зрения порядка поля) полях. Написание программного кода не являлось целью работы. Читатель может воспользоваться кодом для самостоятельных расчетов и экспериментов, а также убедиться, что расчеты автором были произведены верно.