Лекция 3

Конечные поля существуют не при любом количестве элементов, а только в том случае, если число элементов является простым числом или степенью простого числа.

В первом случае конечное поле называется **простым**, во втором - **расширением соответствующего простого поля**. Для каждого допустимого значения q существует только одно поле. Это означает, что правила сложения и умножения, удовлетворяющие всем необходимым требованиям, можно задать только одним способом.

Если $q=p$, где p - простое число, то элементами конечного поля являются числа 0, 1, 2, … , p-1, а сложение и умножение выполняются по модулю числа p.

Простейшее поле Галуа - это поле GF(2), состоящее из двух элементов: 0 и 1. Операции в этом поле выполняются по модулю 2. Правила выполнения арифметических операций в этом поле таковы:

0+0=0; 1+0=1; 0+1=1; 1+1=0 (отсюда 1=-1); 0-0=0; 1-1=0; 0-1=1; 1-0=1;

0•0=0; 0•1=0; 1•0=0; 1•1=1; 0/1=0; 1/1=1.

Поле GF(2) обладает всеми перечисленными выше свойствами. Для двоичных кодов операции над коэффициентами степенных многочленов выполняются в этом поле (операции по модулю 2 выполнялись в предыдущих разделах без упоминания о полях Галуа).

Рассмотрим, например, поле GF(7). Это поле содержит следующие элементы: 0, 1, 2, 3, 4, 5, 6. Для поля GF(7) операции сложения и умножения выполняются по модулю числа 7. Составим таблицы для данных операций (таблицы 8 и 9, соответственно).

Таблица 8

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Таблица 9

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Если q является степенью простого числа ($q=p^m$), то элементами конечного поля будут все многочлены степени m-1 и менее, коэффициенты которых принадлежат простому полю GF(p). Например, для недвоичного кода с основанием $q=2^3=8$ (см. табл. 7) алфавит кода содержит $2^3=8$ трехразрядных символов: 000, 001, 010, 011, 100, 101, 110, 111. Эти восемь символов образуют поле Галуа GF(2^3) . Каждый из этих символов может быть сам представлен в виде степенного многочлена. Если, к примеру, рассмотреть символ 101, то ему соответствует многочлен $x^2+1=1•x^2+0•x^1+1•x^0$, причем коэффициенты при слагаемых этого многочлена (0 и 1) взяты из простого поля Галуа GF(2). Это же относится и к остальным семи символам, образующим алфавит данного кода.

Сложение и умножение такого рода многочленов, образующих алфавит недвоичного кода (заданное поле Галуа), выполняется по обычным правилам сложения и умножения многочленов, но результат приводится по модулю некоторого специального многочлена $p(x)$ степени m. Это означает, что получившееся после выполнения данной операции выражение следует разделить на многочлен $p(x)$ и взять остаток в качестве результата. Многочлен $p(x)$ нельзя разложить на множители, используя только многочлены с коэффициентами из простого поля GF(p). Такие многочлены называются неприводимыми; они аналогичны простым числам. Таблицы неприводимых многочленов представлены в [51].

Многочлен $p(x)=x^3+x+1$ неприводим над полем GF(2) и может быть использован для построения поля GF(2^3) = GF(8).

Пусть $\beta_1=x^2+x$ и $\beta_2=x^2$ два элемента поля GF(2^3).

Можно произвести их суммирование

$\beta_1 + \beta_2 = x^2 + x + x^2 = x$,

или перемножение

$\beta_1 \bullet \beta_2 = (x^2 + x) \bullet x^2 = x^4 + x^3$.

Многочлен $x^4 + x^3$ следует привести по модулю $p(x)$ т. е. поделить на $x^3 + x + 1$ и взять остаток в качестве результата

$$\begin{array}{ll} x^4 + x^3 & \left| \underline{x^3 + x + 1} \right. \\ \oplus \underline{x^4 + x^2 + x} & x + 1 \\ \quad x^3 + x^2 + x & \\ \quad \oplus \underline{x^3 + x + 1} & \\ \quad \textit{остаток}\ x^2 + 1 & \end{array}$$

Таким образом $\beta_1 \bullet \beta_2 = x^2 + 1$ в поле GF(2^3).

В конечных полях как и для обычных чисел используется понятие логарифма. В таких полях существует по крайней мере один элемент, который называется генератором или примитивным элементом, обладающий тем свойством, что любой другой ненулевой элемент поля можно получить путем возведения в некоторую степень примитивного элемента.

Например, элемент 3 является примитивным элементом в поле GF(7), поскольку все ненулевые элементы GF(7): 1, 2, 3, 4, 5, 6 можно получить, возведя число 3 в некоторую степень и приведя результат по модулю числа 7, при этом считается, что $3^0 = 1$:

$3^0 = 1$, $3^2 = 9 \bmod 7 = 2$, $3^1 = 3$, $3^4 = 81 \bmod 7 = 4$, $3^5 = 243 \bmod 7 = 5$,

$3^3 = 27 \bmod 7 = 6$.

Допустим, что α - примитивный элемент поля GF(2^3). Если предположить $\alpha = x$, а в [53] отмечается, что это равенство обеспечивается выбором соответствующего неприводимого многочлена, то любой из семи ненулевых элементов поля GF(2^3) можно представить в виде степенного многочлена, степени примитивного элемента или комбинации двоичных символов следующим образом (табл. 5.10).

Таблица 5.10

Представление элементов в поле GF(2^3)		
В виде степени примитивного элемента	В виде степенного многочлена	В виде комбинации двоичных символов
0	0	000
α^0	1	001
α^1	x	010
α^2	x^2	100
α^3	$x^3 \quad \left\| \underline{x^3 + x + 1} \right.$ $\oplus \underline{x^3 + x + 1} \quad 1$ *остаток* $x + 1 = \alpha^3$	011
α^4	$x^4 \quad \left\| \underline{x^3 + x + 1} \right.$ $\oplus \underline{x^4 + x^2 + x} \quad x$ *остаток* $x^2 + x = \alpha^4$	110

α^5	$x^5 \quad \Big\vert \underline{x^3 + x + 1}$ $\oplus \quad \underline{x^5 + x^3 + x^2} \qquad x^2 + 1$ $x^3 + x^2$ $\oplus \quad \underline{x^3 + x + 1}$ *остаток* $x^2 + x + 1 = \alpha^5$	111
α^6	$x^6 \quad \Big\vert \underline{x^3 + x + 1}$ $\oplus \quad \underline{x^6 + x^4 + x^3} \qquad x^3 + x + 1$ $x^4 + x^3$ $\oplus \quad \underline{x^4 + x^2 + x}$ $x^3 + x^2 + x$ $\oplus \quad \underline{x^3 + x + 1}$ *остаток* $x^2 + 1 = \alpha^6$	101
$\alpha^7 =$ $=\alpha^0 = 1$ и т. д.	$x^7 \quad \Big\vert \underline{x^3 + x + 1}$ $\oplus \quad \underline{x^7 + x^5 + x^4} \qquad x^4 + x^2 + x + 1$ $x^5 + x^4$ $\oplus \quad \underline{x^5 + x^3 + x^2}$ $x^4 + x^3 + x^2$ $\oplus \quad \underline{x^4 + x^2 + x}$ $x^3 + x$ $\oplus \quad \underline{x^3 + x + 1}$ *остаток* $1 = \alpha^7$	001

Наличие логарифмов в полях Галуа позволяет представлять элементы поля в форме, удобной для их сложения, и форме, удобной для умножения. Для сложения удобны формы представления элементов поля в виде степенных многочленов или комбинаций двоичных символов, а для умножения - в виде степеней примитивных элементов.

Например :

$$\alpha^2 + \alpha^5 = \quad 100 = \quad 011 = \alpha^3$$

$$\underline{\oplus\ 111}$$

$$011$$

$$\alpha^2 \cdot \alpha^5 = \alpha^7 = 001$$