РАДИОТЕХНИКА

УДК 621.391

ФОРМЫ ПРЕДСТАВЛЕНИЯ ЭЛЕМЕНТОВ КОНЕЧНЫХ ПОЛЕЙ

О.А. Гомцян[1], Б.Ф. Бадалян[1], Г.К. Егоян[1,2], Г.О. Гомцян[2]

[1]*Национальный политехнический университет Армении*
[2]*ЗАО "РЕДИНЕТ"*

Современные методы и устройства кодирования информации базируются на основных моделях высшей (абстрактной) алгебры, теории чисел и таких понятиях (систем), как группы, кольца, поля, сравнения, вычеты и т.п. Все эти понятия в общем случае распространяются на объекты различной природы и на отношения (связи) между ними. В дальнейшем рассматриваются только математические объекты: числа, векторы, многочлены и т.д. Таким образом, математические объекты и описывающие их операции в совокупности образуют математические модели различных физических процессов. Наибольший интерес представляют такие общеизвестные математические модели, как системы целых и действительных чисел, которые символизируют многие физические процессы, например, счет, измерение, сравнение, упорядочение. Конечные поля играют важную роль в системах кодирования, криптографии и цифровой обработки сигналов. Элементы конечных полей представляются в различных формах: степенной, векторной, полиномиальной и др. Наиболее распространенным является построение конечных полей с помощью модульной арифметики, которое, в свою очередь, базируется на известных операциях целочисленной арифметики. В конечных полях операции умножения (деления) являются более сложными, чем операции сложения (вычитания). Для упрощения выполнения операции умножения удобно преобразовать числа в полиномиальную форму. В работе рассмотрен наиболее полный спектр представления элементов в конечных полях. На многочисленных примерах показаны различные способы осуществления основных операций в конечных полях. Показана методика определения примитивных элементов конечных полей.

Ключевые слова: конечные поля, примитивный полином, генераторный многочлен, примитивный элемент, принцип замкнутости, неприводимый полином.

Введение. В настоящее время существует несколько основных форм представления элементов в конечных полях. Для представления этих методов напомним некоторые основные понятия и свойства конечных полей.

Основные свойства конечных полей. В общем случае поле – множество элементов, в котором можно производить операции сложения, вычитания, умножения и деления [1-9]. Как известно, поля могут иметь бесконечное и конечное число элементов. Однако в теории кодирования существенную роль играют поля с определенным числом элементов, которые и называются конечными полями [Finite Fields(FF)]. Итак, пусть имеем поле с конечным числом элементов, равным q, которое также называется порядком поля. Такое поле часто называется полем Галуа [Galois Field] и обозначается $GF(q)$. Это поле обладает

всеми свойствами, перечисленными в [1,3]. Кроме того, конечность числа элементов $GF(q)$ накладывает свой отпечаток на структуру поля.

Рассмотрение полей Галуа начнем с самого простейшего, которое состоит из двух элементов $q=2$. Так как поле должно обязательно обладать нулевым элементом по сложению и единичным элементом по умножению, то, следовательно, поле $GF(2)$ должно содержать $e_{+}=0$ и $e_{x}=1$ соответственно, т.е. это двоичное поле Галуа [2]. При этом операции умножения и сложения определяются следующим образом:

$$\begin{array}{ll} 0+0=0 & 0\cdot 0=0 \\ 0+1=1 & 0\cdot 1=0 \\ 1+0=1 & 1\cdot 0=0 \\ 1+1=0 & 1\cdot 1=1 \end{array} \qquad (1)$$

Из равенств $1+1=0$ и $1\cdot 1=1$ следует, что $-1=1(1=-1)$ и $1^{-1}=1$. Тогда таблицы для вычитания и деления имеют вид

$$\begin{array}{l|l} 0-0=0 & 0:0= \text{ не существуют} \\ 0-1=1 \ [\text{ т.к. } 0-1=0+(1)=1\ ] & 1:0= \\ 1-0=1 & 0:1=0, \text{ т.к. } 0:1=0\cdot 1^{-1}=0 \\ 1-1=0 & 1:1=1. \end{array} \qquad (2)$$

Из сравнения (1) и (2) видно, что операции сложения и вычитания, а также умножения и деления (кроме деления на нуль) равнозначны.

Нетрудно заметить, что (1) представляет собой сложение и умножение по *mod 2*. Сложение и умножение по некоторому *модулю m обеспечивает принцип замкнутости*, т.е. не позволяет выходить за пределы множества. *Это очень важное свойство конечных полей.* Например, обычно $1+1=2$, но $1+1=0\ (mod2)$, т.е. результат операции сложения по mod 2 принадлежит исходному множеству [0,1]. Также отметим, что другого числового поля с $q=2$ не существует [7,8].

Самым примечательным из теории конечных полей можно считать тот факт, что число элементов в этих полях всегда подчиняется условию

$$q=p^{m}, \qquad (3)$$

где p – простое число, $m=1,2,3,\ldots,$.

Итак, конечное поле существует только в том случае, когда число элементов поля равно степени простого числа. При $m=1$ и $p=2$ имеем поле $GF(2)$; при $m=1$ и $p=3$ – поле $GF(3)$; при $m=2$, $p=2$ - $GF(4)$; $m=1$, $p=5$ – $GF(5)$ и т.д. Таким образом, можно построить поле с числом элементов $q=2,3,4,5$ и т.д., но никак нельзя сформировать поле с числом элементов $q=6,10,12,14$ и т.д.

Этот факт приводится и доказывается в многочисленных литературных источниках [1,3,7-9]. При $m=1$ число элементов поля $q=p$, и такое поле часто называется *примитивным*. Элементами такого поля являются числа

$0, 1, 2, \ldots, p-1$ или другие объекты (например, полиномы), которые будут рассмотрены далее.

По всей видимости, самым важным в теории конечных полей является наличие так называемых примитивных элементов (или генераторов, или порождающих элементов, или первообразного корня).

В первом приближении примитивным элементом α поля $GF(q)$ назовем такой элемент, последовательные степени которого образуют $(q-1)$ ненулевых элементов этого поля.

Пример 1. Рассмотрим поле $GF(5)=\{0,1,2,3,4\}$ и составим пять степеней каждого из элементов этого поля. Расчеты сведем в табл.1.

Таблица 1

Поле $GF(5)$

$a=0^1=0$	$a^2=0$	$a^3=0$	$a^4=0$	$a^5=0$
$a=1^1=1$	$1^2=1$	$1^2=1$	$1^4=1$	$1^5=1$
$a=2^1=2$	$2^2=4$	$2^3=8\equiv 3(\text{mod}5)$	$2^4=16=1(\text{mod}5)$	$2^5=32\equiv 2(\text{mod}5)$
$a=3^1=3$	$3^2=9\equiv 4(\text{mod}5)$	$3^3=27\equiv 2(\text{mod}5)$	$3^4=81\equiv 1(\text{mod}5)$	$3^5=243\equiv 3(\text{mod}5)$
$a=4^1=4$	$4^2=16\equiv 1(\text{mod}5)$	$4^3=64\equiv 4(\text{mod}5)$	$4^4=256\equiv 1(\text{mod}5)$	$4^5=1024\equiv 4(\text{mod}5)$

Из табл.1 видно, что $a^5=a$ для всех a и $a^4=1$ для любого a, кроме $a=0$. Более того, при $a=2$ и $a=3$ первые четыре степени образуют элементы исходного поля. Для остальных a этого не наблюдается. Поэтому, согласно предыдущему определению, числа 2 и 3 есть примитивные элементы. В дальнейшем будем рассматривать один примитивный элемент 2, обозначив его через α. Итак, из третьей строки таблицы видно, что элементы поля $GF(5)$ соответствуют следующим степеням примитивного элемента: $\alpha^1=2$; $\alpha^2=4$; $\alpha^3=3$; $\alpha^4=1=\alpha^0$ (из свойств полей).

Таким образом, сумма, например, $3+4=7\equiv 2(\text{mod}5)$, их произведение $3\cdot 4=12\equiv 2(\text{mod}5)$ или, с другой стороны, $3\cdot 4=\alpha^3\cdot\alpha^2=\alpha^{5(\text{mod}4)}=\alpha^1=2$. Наличие $\text{mod}4$ вытекает из $\alpha^4=\alpha^0=1$ [в общем случае для степеней – это $mod(q-1)$].

Отметим, что для случая больших полей нахождение примитивного элемента является достаточно сложной задачей. Поэтому используется полиномиальное представление полей, о котором будет сказано далее.

Многочлены и их применение в теории кодирования. Определим полином над полем (или в поле) $GF(q)$ в виде следующего выражения:

$$a(x)=a_0+a_1x+a_2x^2+\ldots+a_{m-1}x^{m-1}+a_mx^m, \qquad (4)$$

где x – неопределенная переменная; a_i - коэффициенты, которые принадлежат полю $GF(q)$, причем показатели степени при x и индексы при a - это целые числа.

Применим для полиномов над полем обозначение $GF[q,x]$, имея в виду под q - порядок поля, а под x – переменную полинома, которая не принадлежит полю.

Рассмотрим понятие *неприводимого* полинома по аналогии с простым числом. Пусть для полиномов $a(x)$, $b(x)$ и $\varepsilon(x)$ справедливо

$$a(x)=b(x)\cdot\varepsilon(x). \tag{5}$$

Тогда говорят, что $b(x)$ делит $a(x)$ или $a(x)$ делится на $b(x)$. Если имеется полином $p(x)$ степени m, который не делится ни на какой полином степени, меньшей m, но большей 0, то он называется *неприводимым* [3]. Или другое определение: полином $p(x)$ называется неприводимым, если он делится только на $\alpha\cdot p(x)$ или α, где α – любой ненулевой элемент поля $GF(q)$ [6]. Или еще одно определение: полином неприводим в поле $GF(q)$, если он не может быть разложен на полиномы меньшей степени $GF[q,x]$ [4,8].

Конечно, все эти определения имеют один и тот же смысл. Однако очень важно отметить, что приводимость и неприводимость следует определять только по отношению к конкретному заданному полю, т.к. может случиться, что неприводимый полином над этим полем будет приводим над другим [4,8].

Пример 2. Пусть имеем $GF[3,x]$, т.е. множество чисел $\{0,1,2\}$. Тогда полином x^2+x+1 приводим в этом поле, т.к. его можно разложить следующим образом: $x^2+x+1=(x+2)(x+2)=x^2+4x+4=(x^2+x+1)\bmod 3$. Другие полиномы x^2+x+2 и x^2+1 неприводимы в этом поле [4]. С другой стороны, полином x^2+1 неприводим над полем рациональных и действительных чисел, но в поле комплексных чисел он приводим, т.к. $x^2+1=(x-i)(x+i)$.

Отметим несколько важных свойств неприводимых полиномов [4]:

1. Любой полином первой степени неприводим.
2. Если в полиноме коэффициент при старшем члене (т.е. с максимальной степенью x) равен 1, то он называется простым.
3. Всякий полином $f(x)$ степени $m\geq 1$ однозначно разлагается на неприводимые многочлены с точностью до множителей нулевой степени (например, на элементы поля и простые полиномы).
4. Если полином $p(x)$ неприводим, то и любой полином $\alpha\cdot p(x)$ также неприводим, причем α – отличный от нуля элемент поля.

Пусть имеем произвольный элемент $\alpha\in GF(q)$. Если этот элемент подставим в полином $f(x)$ вместо неопределенной переменной x, то получим значение полинома $f(x)$ при $x=\alpha$. Когда $f(\alpha)=0$, то элемент α называется корнем полинома $f(x)$. В общем случае полином может не иметь корней в своем собственном поле.

Пример 3. Пусть имеем полином над полем $GF(2)$ в виде $f(x)=x^2+x+1$. Вычислим его значение при $\alpha=0$ и $\alpha=1$. Тогда $f(0)=1$; $f(1)=1^2+1+1=1$. Это значит, что этот полином не имеет корней в поле $GF(2)$. Аналогично не имеет корней в двоичном поле и полином $f(x)=x^4+x^3+1$.

Если корнем простого полинома является примитивный элемент, то полином называется примитивным [1,4,6]. С другой стороны, для отыскания примитивного полинома можно воспользоваться более строгим определением, а именно, неприводимый полином $p(x)$ степени m из поля $GF[p,x]$, где p – простое число, называется примитивным, если он делит нацело двучлен x^n-1, где $n=p^m-1$ [8].

Пример 4. Пусть имеем полином $p(x)=x^2+x+1$ с $p=2$ и $m=2$. Убедимся, что он примитивный. Для этого проведем деление $x^n-1=x^3-1$ на $p(x)$:

$$\begin{array}{r|l} -\,x^3-1 & \dfrac{x^2+x+1}{x-1} \\ \underline{x^3+x^2+x} & \\ -x^2-x-1 & \\ \underline{-x^2-x-1} & \\ 0 & \end{array}$$

Теперь обратимся к корням полиномов. Корни $\{\alpha_j\}$ примитивного полинома $p(x)$ степени m из $GF[p,x]$, если они существуют, имеют порядок p^m-1. Если любой полином $p(x)$ делится на линейный полином $x-a$, то элемент α является корнем $p(x)$.

Пример 5. Рассмотрим полином $p(x)=x^4+x^3+x+1$ над полем $GF(2)$. Простой проверкой можно убедиться, что его корнем служит элемент $\alpha=1$. Действительно, $p(\alpha)=1^4+1^3+1+1=0$. Следовательно, этот полином должен делиться на $x-1$ или $x+1$, что может быть проверено соответствующим делением. Однако этот полином непримитивный, т.к. легко проверить, что при делении x^7+1 на $p(x)$ получается остаток $x+1$.

Ранее было показано, что числовые поля можно сформировать из последовательных степеней примитивного элемента поля. Покажем, что поле над полиномами можно строить с использованием примитивного полинома.

Пусть имеем следующий примитивный полином из $GF[p,x]$:

$$p(x)=p_0+p_1x+\ldots+p_{m-1}x^{m-1}+x^m. \qquad (6)$$

Допустим, что α - корень этого полинома, что означает

$$p(\alpha) = p_0 + p_1\alpha + \ldots + p_{m-1}\alpha^{m-1} + \alpha^m = 0.$$

Отсюда

$$\alpha^m = -p_0 - p_1\alpha - \ldots - p_{m-1}\alpha^{m-1}. \quad (7)$$

Следовательно, степени m элемента α могут быть представлены в виде полиномов степеней $(m-1)$ или меньше. Поскольку порядок элемента α равен $p^m - 1$, то каждая степень α представляется своим соответствующим полиномом.

Пример 6. Построим поле $GF(8) = GF(2^3)$. Для этого используем примитивный полином $p(x) = x^3 + x + 1$. Пусть α - корень $p(x)$, т.е. $\alpha^3 + \alpha + 1 = 0$ или откуда $\alpha^3 = \alpha + 1$. Тогда степень α и полиномы будут иметь соответствие, показанное в табл. 2.

Используя полиномиальное представление поля $\mathrm{GF}(2^3)$, можем легко осуществить сложение и умножение элементов.

Пример 7. Сложение трех элементов этого поля из табл. 2 имеет вид

$$\alpha^2 + \alpha^4 + \alpha^6 = \alpha^2 + \alpha^2 + \alpha + \alpha^2 + 1 = \alpha^2 + \alpha + 1 = \alpha^5.$$

Умножение двух элементов из этой же таблицы, как было показано ранее, осуществляется следующим образом:

$$\alpha^4 \cdot \alpha^6 = \alpha^{(4+6)\bmod(q-1)} = \alpha^{10(\bmod 7)} = \alpha^3.$$

С другой стороны, теперь уже в форме полиномов, это умножение можно произвести с помощью следующих преобразований:

$$\alpha^4 \cdot \alpha^6 = (\alpha^2 + \alpha)\cdot(\alpha^2 + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha.$$

Далее

$$\begin{array}{l|l} \alpha^4 + \alpha^3 + \alpha^2 + \alpha & \underline{\alpha^3 + \alpha + 1} \\ \underline{\alpha^4 + \alpha^2 + \alpha} & \alpha \end{array}$$

α^3 - остаток.

Следовательно, $(\alpha^2 + \alpha)\cdot(\alpha^2 + 1) = \alpha^3 \bmod p(x)$.

В общем виде это умножение имеет вид

$$(a_0 + a_1\alpha + \ldots + a_m\alpha^m)\cdot(b_0 + b_1\alpha + \ldots + b_m\alpha^m) \bmod p(\alpha),$$

причем здесь коэффициенты a_i и b_i умножаются по правилам умножения в поле $GF(q)$. Такая форма более сложная, поэтому при умножении удобнее пользоваться степенным представлением.

Таблица 2

Поле $GF(8)$ *при* $p(x)=x^3+x+1$

Степени α	Полиномы от α
0	$\alpha^{-\infty}$
$\alpha^0=1$	1
$\alpha^1=\alpha^1$	α
$\alpha^2=\alpha^2$	α^2
$\alpha^3=\alpha^3$	$\alpha^3=\alpha+1$
$\alpha^4=\alpha^4$	$\alpha^4=\alpha^3\cdot\alpha=(\alpha+1)\cdot\alpha=\alpha^2+\alpha$
$\alpha^5=\alpha^5$	$\alpha^5=\alpha^4\cdot\alpha=(\alpha^2+\alpha)\cdot\alpha=\alpha^3+\alpha^2=\alpha^2+\alpha+1$
$\alpha^6=\alpha^6$	$\alpha^6=\alpha^5\cdot\alpha=(\alpha^2+\alpha+1)\cdot\alpha=\alpha^3+\alpha^2+\alpha=\alpha+1+\alpha^2+\alpha=\alpha^2+1$

Пример 8. Продемонстрируем конструкцию поля $GF[4]$. Для этого воспользуемся одним единственно возможным примитивным полиномом этого поля $p(x)=x^2+x+1$. Тогда, если α - корень этого полинома, то $\alpha^2=\alpha+1$. Расчеты сведены в табл. 3.

Полиномиальное представление элементов позволяет также перейти к векторному представлению элементов поля, а именно - полиному $a(x)=a_0+a_1x+a_2x^2+\ldots+a_mx^m$ поставить в соответствие (связать) вектор

$$A=(a_0,a_1,\ldots,a_m)\ , \qquad (8)$$

координаты которого совпадают с коэффициентами полинома (а эти, в свою очередь, взяты из поля $GF(q)$). Например, если имеем двоичное поле $GF(q)$, то вектор A - это последовательность (набор) из m символов 1 и 0, которые отражают соответствующий полином.

Таблица 3

Структура поля $GF(4)$

Численная форма	Степенная форма	Полиномиальная форма
0	$\alpha^{-\infty}$	0
1	α^0	1
2	α^1	α^1
3	α^2	$\alpha+1$

Пример 9. Представим поле $GF(q)=GF(p^m)=GF(2^3)$ в виде векторного пространства – совокупности векторов, соответствующих различным степеням корня α примитивного полинома $p(x)=x^3+x+1$. Для этого используем результаты табл. 2 и предыдущие замечания. Эти построения показаны в табл. 4, где использованы трехразмерные векторы, так как $m=3$.

Отметим, что полиномиальные и векторные формы очень удобны при выполнении сложения, а степенные – при выполнении умножения.

Покажем способы выполнения умножения двух полиномов из табл. 4:

$$\left(\alpha+\alpha^2\right)\cdot\left(1+\alpha^2\right)=\alpha^4\alpha^6.$$

Первый способ – умножение степеней по $\mathrm{mod}(q-1)=7$, т.е. $\alpha^4\alpha^6=\alpha^{10}=\alpha^3$.

Второй способ – непосредственное умножение полиномов и редукция (снижение) степеней в соответствии с табл. 4:

$$\left(\alpha+\alpha^2\right)\cdot\left(1+\alpha^2\right)=\alpha+\alpha^2+\alpha^3+\alpha^4=\alpha+\alpha^2+1+\alpha+\alpha+\alpha^2=1+\alpha=\alpha^3.$$

Третий способ – деление произведения на $p(x)$ и взятие остатка:

$$\begin{array}{l|l}\alpha^4+\alpha^3+\alpha^2+\alpha & \alpha^3+\alpha+1\\ \underline{\alpha^4+\alpha^2+\alpha} & \\ \alpha^3 & \alpha\end{array}$$

Четвертый способ – умножение двоичных векторов и деление на вектор $p(x)$:

$$\begin{array}{r}011\\ \times\\ \underline{101}\\ 011\\ \underline{011}\\ 01111\end{array}\qquad\qquad \begin{array}{r|l}11110 & 1011\\ \underline{1011} & \underline{11}\\ 01000 & \\ \underline{1011} & \\ 11 & \end{array}$$

Таблица 4

Различные формы представления элементов поля $GF(2^3)$

Степенная форма	Полиномиальная форма	Векторная форма
0	0	0 0 0
1	1	1 0 0
α	α	0 1 0
α^2	α^2	0 0 1
α^3	$1+\alpha$	1 1 0
α^4	$\alpha+\alpha^2$	0 1 1
α^5	$1+\alpha+\alpha^2$	1 1 1
α^6	$1+\alpha^2$	1 0 1

Кроме описанных выше представлений элементов полей, используется еще одна логарифмическая форма, которая отражает непосредственно степени или в виде целых чисел, или в виде двоичного кода этих чисел.

Подводя итоги, составим табл. 5, где показаны различные представления элементов конечных полей, например, для случая $GF(4)$.

Целочисленные степени α часто называются логарифмами (иногда индексами). Для удобства принято обозначать $0=\alpha^{-\infty}$ [4]. Экспоненциальная форма

представляет собой двоичный натуральный код индексов (показателей степеней) элемента α.

По всей видимости, в табл. 5 сведены все известные на сегодняшний день формы представления элементов конечного поля.

Таблица 5

Различные формы представления элементов поля $GF(4)$

Символьная форма	Численная форма	Степенная форма	Полиномиальная форма	Векторная форма	Логарифмическая форма	
					индексная	экспоненциальная
0	0	$\alpha^{-\infty}=0$	0	0 0	$-\infty$	0 0
1	1	$\alpha^{0}=1$	1	1 0	0	1 1
a	2	$\alpha^{1}=\alpha$	α	0 1	1	0 1
b	3	$\alpha^{2}=\alpha\alpha$	$1+\alpha$	1 1	2	1 0

Заключение. Проведено обобщение различных способов представления элементов в конечных полях. Представлены примеры, которые позволяют производить расчеты с более сложными полями с целью построения современных систем передачи информации.

Проведен сопоставительный анализ различных методов выполнения арифметических операций в полях целых чисел и многочленов и сделаны предложения по выбору наиболее приемлемого способа выполнения этих операций.

Литература

1. **Берлекэмп Э.** Алгебраическая теория кодирования / Пер. с англ.; Под ред. С.Д. Бермана. - М.: Мир, 1971.- 477 с.
2. **Курош А.Г.** Курс высшей алгебры. – М.: Наука, 1971. – 432 с.
3. **Питерсон У., Уэлдон Э.** Коды, исправляющие ошибки / Пер. с англ.; Под ред. Р.Л. Добрушина и С.И. Самойленко. – М.: Мир, 1976.- 594 с.
4. **Мак-Вильямс Ф.Дж., Слоэн Н.Дж. А**. Теория кодов, исправляющих ошибки / Пер. с англ.; Под ред. Л.А. Бассалыго. - М.: Связь, 1979.- 744 с.
5. **Фрид Э.** Элементарное введение в абстрактную алгебру / Пер с венг. Ю.А. Данилова. - М.: Мир, 1979.- 260 с.
6. **Блейхут Р.** Теория и практика кодов, контролирующих ошибки / Пер с англ.; Под ред. К.Ш. Зигангирова. – М.: Мир, 1986.- 576 с.
7. **Rhee M.Y.** Error Correcting Coding Theory. - N.Y.: McGraw-Hill, 1989.- 461 p.
8. **Wicker S.B.** Error Control Systems for Digital Communication and Storage.- Englewood Cliffs, N. J.: Prentice-Hall, 1994.- 503 p.
9. **Вернер М.** Основы кодирования: Учебник для ВУЗов.- М.: Техносфера, 2004.- 288 с.

Поступила в редакцию 05.09.2017.
Принята к опубликованию 21.12.2017.

ՎԵՐՋԱՎՈՐ ԴԱՇՏԵՐԻ ՏԱՐՐԵՐԻ ՆԵՐԿԱՅԱՑՄԱՆ ՁԵՎԵՐԸ

Հ.Ա. Գոմցյան, Բ.Ֆ. Բադալյան, Գ.Կ. Եղոյան, Գ.Հ. Գոմցյան

Ինֆորմացիայի կոդավորման ժամանակակից մեթոդները և սարքավորումները հիմնվում են բարձրագույն (աբստրակտ) հանրահաշվի հիմնական մոդելների, թվերի

տեսության և այնպիսի հասկացությունների (համակարգերի) վրա, ինչպիսիք են խմբերը, օղակները, դաշտերը, համեմատումները, հանումները և այլն: Բոլոր այդ հասկացությունները, ընդհանուր առմամբ, տարածվում են տարբեր բնույթի օբյեկտների և դրանց միջև եղած հարաբերությունների (կապերի) վրա: Հետագայում դիտարկվում են միայն մաթեմատիկական օբյեկտներ.թվեր, վեկտորներ, բազմանդամներ և այլն: Այդ բոլոր մաթեմատիկական օբյեկտները և դրանք նկարագրող գործողությունները միակցությամբ ձևավորում են ֆիզիկական տարբեր պրոցեսների մաթեմատիկական մոդելներ: Առավել ուշագրավ են այնպիսի հանրահայտ մաթեմատիկական մոդելները, ինչպիսիք են ամբողջ և իրական թվերի համակարգերը, որոնք նկարագրում են բազմաթիվ ֆիզիկական պրոցեսներ, օրինակ՝ հաշվարկ, չափում, համեմատում, կարգավորում: Վերջավոր դաշտերը կարևոր դեր են խաղում կոդավորման, գաղտնագրման և ազդանշանների թվային մշակման համակարգերում: Վերջավոր դաշտերի տարրերը ներկայացվում են զանազան ձևերով. ցուցչային, վեկտորային, բազմանդամային և այլն: Առավել տարածված է վերջավոր դաշտերի կառուցումը մոդուլային թվաբանության միջոցով, որն իր հերթին հիմնվում է ամբողջ թվերի թվաբանության հայտնի գործողությունների վրա: Վերջավոր դաշտերում բազմապատկման (բաժանման) գործողություններն ավելի բարդ են, քան գումարման (հանման) գործողությունները: Բազմապատկման գործողության իրականացման պարզեցման նպատակով հարմար է թվերը ձևափոխել բազմանդամային տեսքի: Դիտարկված է վերջավոր դաշտերում տարրերի ներկայացման առավել ամբողջական սպեկտրը: Բազմաթիվ օրինակներով ցույց են տրված վերջավոր դաշտերում հիմնական գործողությունների իրագործման տարբեր եղանակները: Ներկայացված է վերջավոր դաշտերի պարզունակ տարրերի որոշման մեթոդիկան:

Առանցքային բառեր. վերջավոր դաշտեր, պարզունակ բազմանդամ, գեներատորային բազմանդամ, պարզունակ տարր, պարփակվածության սկզբունք, չբերվող բազմանդամ:

REPRESENTATION FORMS OF FINITE FIELD ELEMENTS

H.A. Gomtsyan, B.F. Badalyan, G.K. Egoyan, G.H. Gomtsyan

Modern methods and devices for coding information are based on the main models of higher (abstract) algebra, the number theory and such concepts (systems) as groups, rings, fields, comparisons, deductions, etc. All these concepts in the general case apply to objects of different nature and relationships (links) between them. Further, we will only consider mathematical objects: numbers, vectors, polynomials, etc. Thus, mathematical objects and the operations describing them together form mathematical models of various physical processes. For us the greatest interest is represented by the well-known mathematical models such as systems of integer and real numbers, representing many physical processes like counting, measuring, comparing, ordering, are of special interest. Finite fields play an important role in coding, cryptography and digital signal processing systems. Elements of finite fields are presented in different forms: power, vector, polynomial, etc. The most common is the construction of finite fields, using modular arithmetic, which in their turn are based on the known operations of integer arithmetic. In finite fields, the operations of multiplication (division) are more complex than are the operations of addition (subtraction). To simplify the operation of multiplication, it is convenient to convert the numbers to the polynomial form. The paper discusses the most comprehensive representation of elements in finite fields. Numerous examples show the different ways of implementing the basic operations in the finite fields. The method of determining the primitive elements of finite fields is shown.

Keywords: finite field, primitive polynomial, generator polynomial, primitive element, principle of closureness, irreducible polynomial.