Лекции 4 . Алгебраические основы помехоустойчивых кодов. Понятия группы, кольца и поля. Простое и расширенное поле.
Операции над многочленами в поле двоичных чисел и их реализация.
Поля Галуа и их свойства.

Алгебраические основы теории помехоустойчивых кодов.

В основе современной теории помехоустойчивого кодирования лежат такие понятия высшей алгебры как *группа, кольцо* и *поле*.

Группой **называется множество *G* объектов или элементов (числа, матрицы, подстановки и т. д.), для которых определена некоторая операция, позволяющая для каждых двух элементов *a* и *b* группы найти третий элемент *c* той же группы по однозначной функциональной зависимости *f(a, b) = c*.**

Операцию называют сложением, если между элементами группы выполняется зависимость *a + b = c* или умножением при *a·b = c*. Как правило, эти операции не являются арифметическим сложением или арифметическим умножением.

Для элементов группы должны выполняться следующие аксиомы:

1. *Условие замкнутости*: для любых двух элементов a и b группы существует вполне определенный, принадлежащий этой же группе элемент c, который может быть представлен как $c = a + b$ для операции сложения или $c = a \cdot b$ для операции умножения.
2. *Условие сочетательности или ассоциативности*: для любых трех элементов a, b и c группы $(a + b) + c = a + (b + c)$ (для операции сложения) или $(a \cdot b)\, c = a\, (b \cdot c)$ (для операции умножения).
3. *Условие существования единичного элемента*. Если операция названа сложением, то единичный элемент называется нулем, обозначается 0 и определяется из уравнения $0 + a = a + 0 = a$, которое должно выполняться для любого элемента группы. Если операция названа умножением, то единичный элемент называется единицей, обозначается e и определяется из уравнения $e \cdot a = a \cdot e = a$.

4. *Условие существования обратного элемента*. Если операция называется сложением, то обратный элемент, соответствующий элементу a, обозначается $(-a)$ и определяется из уравнения $a + (-a) = (-a) + a = 0$. Если операция называется умножением, то обратный элемент обозначается a^{-1} и определяется из уравнения $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Кроме перечисленных аксиом, элементы группы могут удовлетворять условию **коммутативности** или переместительности, т. е. равенству $a + b = b + a$, если операция называется сложением, или равенству $a \cdot b = b \cdot a$, если операция названа умножением. В этом случае группа называется абелевой или коммутативной.

Группа называется конечной, если она состоит из конечного числа элементов; в противном случае она называется бесконечной.

Число элементов конечной группы называется ее порядком.

Кольцо. Пусть R − некоторое множество элементов a, b, c ,.. . Эти элементы могут быть самой разнообразной природы: числа, матрицы, многочлены и др. Множество R называется кольцом, если:

а) выполняется замкнутость множества R по отношению к операциям сложения и умножения, т. е. сумма $a + b$ и произведение $a \cdot b$ любых двух элементов a, b являются также элементами множества R;

б) выполняются сочетательные (ассоциативные) законы $(a + b) + c = a + (b + c)$ и $(ab)\, c = a\,(bc)$ для любых элементов a, b и c из множества R;

в) операция сложения перестановочна (коммутативна) $a + b = b + a$ для любых элементов a и b из множества R;

г) выполняется **обратимость сложения**, т. е. для любых элементов a и b из множества R уравнение $a + x = b$ разрешимо, где x принадлежит множеству R;

д) выполняется распределительный (дистрибутивный) закон: $a(b + c) = ab + ac$ и $(b + c)a = ba + ca$ для любых элементов a, b и c из множества R.

Если коммутативный закон также справедлив для операции умножения для любых элементов a и b из множества R, т. е. $ab = ba$, то кольцо называется *коммутативным*.

Полем называется такое коммутативное кольцо, в котором уравнение $ax = b$ при $a \neq 0$ всегда разрешимо (т. е. удовлетворяется выполнимость деления). При этом поле, кроме нуля 0 ($a + 0 = a$) и противоположных элементов a и $(-a)$ [$a + (-a) = 0$], содержит также единичный элемент e и обратные элементы a^{-1}, для которых справедливо: $ae = ea = a$; $a \cdot a^{-1} = e$. Элемент поля 0 называют аддитивной единицей, а элемент e – мультипликативной единицей.

Все элементы конечного поля удовлетворяют свойствам группы по операции сложения и поэтому их можно считать *аддитивной группой* в составе конечного поля. Следовательно, порядок этой аддитивной группы совпадает с порядком конечного поля.

Одновременно элементы конечного поля, кроме нулевого, удовлетворяют свойствам конечной группы по умножению, поэтому все ненулевые элементы поля представляют собой *мультипликативную группу* в составе конечного поля. При этом порядок такой мультипликативной группы будет на 1 меньше порядка конечного поля.

Аксиомы (законы) для элементов **поля**

Аксиомы	Операция (*)	
	Сложение(*=+)	Умножение (*=×)
Замкнутость:для каждой пары элементов a и $b \in M$ существует единственный элемент $c \in M : c=a*b$	A1 $a+b=c$	M1 $a \times b=c$
Ассоциативность: $(a*b)*c = a*(b*c)$	A2 $(a+b)+c=a+(b+c)$	M2 $(a \times b) \times c=a \times (b \times c)$
Коммутативность: $a*b = b*a$	A3 $a+b=b+a$	M2 $a \times b = b \times a$
Наличие единичного элемента: $e \in M$, такого, что $a*e = e*a = a$, где $a \in M$	A4 $a+e=e+a=a;\ (e=0)$	M4 $a \times e=e \times a=a;$ $(e=1)$
Наличие обратного элемента: для любого $a \in M$ существует элемент $\overline{a} \in M$ такой, что $a*\overline{a}=\overline{a}*a = e$	A5 $a+\overline{a} = \overline{a} +a=0;$ $(\overline{a} = -a)$	M5 $a \times \overline{a} = \overline{a} \times a=1;$ $(\overline{a} = a^{-1},\ a \neq 0)$
Дистрибутивность	D1: $a(b+c) = ab + ac$ D2: $(b+c)a = ba + ca$	

Итак, *группа* – это система, в которой заданы одна основная операция и операция, ей обратная, например сложение и обратная операция – вычитание; или умножение и обратная операция – деление. В *кольце* определены две основные операции – сложение и умножение, и операция, обратная первой из этих операций – вычитание. В *поле* определены две основные операции, а именно, сложение и умножение, и операции, обратные к ним обеим, т. е. вычитание и деление.

Группа, имеющая конечное число элементов, называется конечной группой. Число элементов группы называется *порядком конечной группы*.

Поле, содержащее конечное число элементов q, называется конечным полем и обозначается GF(q) (GF – Galois Field – поле Галуа). Число элементов поля называется *порядком конечного поля.*

Простые поля. Характеристика поля. Пусть имеется некоторое поле R. Известно, что пересечение произвольного множества подполей поля R также является подполем. На рис. 3.1 $k1$, $k2$, $k3$ – подполя поля R; p – пересечение этих подполей.

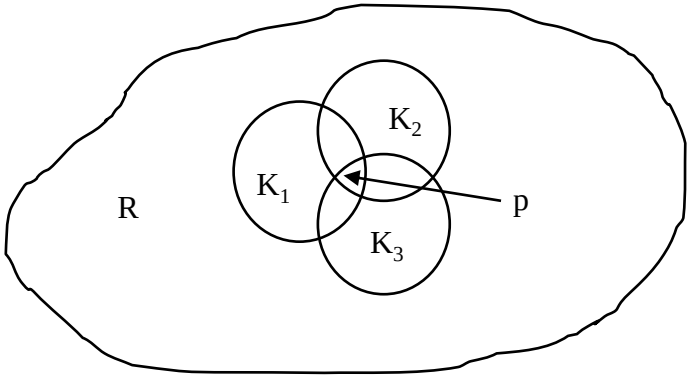


Рис. 3.1. Графическое изображение поля.

Пересечение p всех подполей поля R есть наименьшее подполе, которое не содержит в себе других подполей, отличных от p. Рассмотренный на рис 3.1 пример полей называют полями с характеристикой p ($p > 0$), где число p должно быть простым.

Операции сложения и умножения над элементами простого поля GF(p), (а также над элементами группы) производятся по mod$p$. Часто операции сложения и умножения обозначают $\oplus$ и $\otimes$ соответственно и представляют *таблицами Кэли.* Для примера приведем таблицы Кэли для $p=2$ (наиболее часто применяется) и $p=3$:

а) $p = 2$

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

$-1 = -1+2 = +1$

$-1 = 1 \pmod 2$

б) $p = 3$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$-1 = -1+3 = +2$

$-1 = 3 \pmod 3$

$-a = -a+p \pmod p$

Например: $2 \oplus 2 = 4 \equiv 1 \pmod 3$ $\quad$ $2 \otimes 2 = 4 \equiv 1 \pmod 3$

- сложение $\oplus$ по модулю p :

$$a \oplus b = (a+b) \bmod p \equiv rest\left[\frac{a+b}{p}\right];$$

- умножение $\otimes$ по модулю p :

$$a \otimes b = (a \cdot b) \bmod p \equiv rest\left[\frac{a \cdot b}{p}\right].$$

Основные действия над многочленами в поле двоичных чисел и их реализация

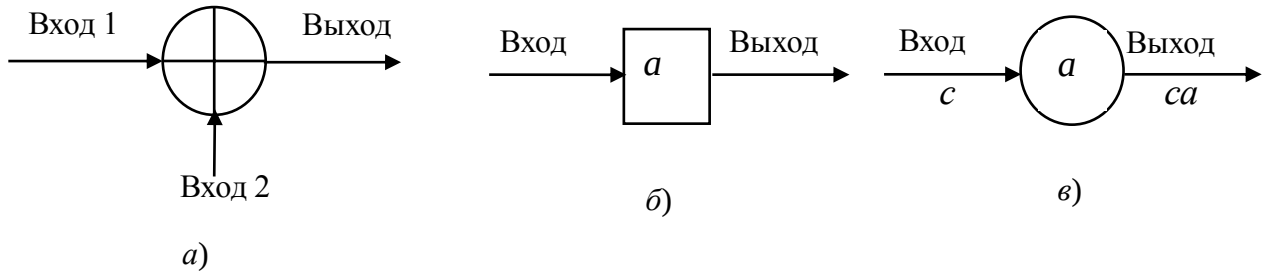


Рис. 3.2. Составные элементы устройств умножения и деления многочленов: сумматор (*а*), запоминающее устройство (*б*) и устройство умножения (*в*)

Сложение многочленов

Правило сложения многочленов сводится к суммированию коэффициентов при одинаковых степенях x и приведению суммы по модулю p. Пусть

$$f_1(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}, \quad f_2(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1},$$

где коэффициенты a_i и b_i принимают значения 0, 1,2, ..., $(p-1)$. Тогда сумма многочленов будет:

$$f_1(x) + f_2(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_{n-1} + b_{n-1})x^{n-1} =$$
$$= c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1}, \text{ где } (a_i + b_i) = c_i \pmod p.$$

Пример. Сумма полиномов $f_1(x) = 1 + x^3 + x^5$ и $f_2(x) = x + x^3 + x^7$ с коэффициентами – вычетами по модулю $p=2$, будет равна:

$$f_1(x) + f_2(x) = 1 + x + x^5 + x^7.$$

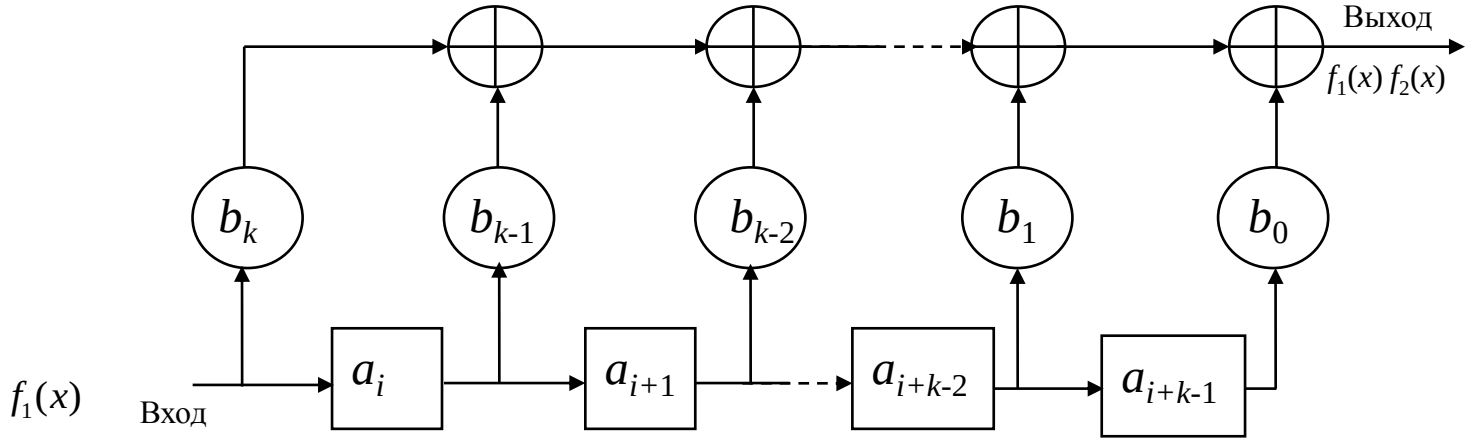
Умножение многочленов.

$f_1(x)\cdot f_2(x) = (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots + a_{n-1}b_{n-1}x^{2n-2} \equiv$

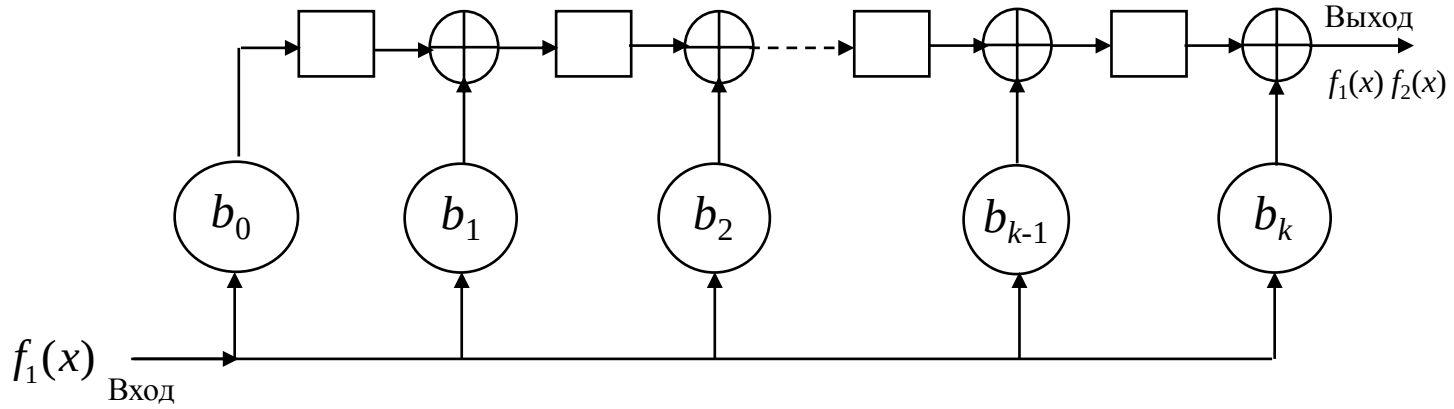
$\equiv c_0 + c_1x + c_2x^2 + \ldots + c_{2n-2}x^{2n-2} \pmod p.$

Таким образом, коэффициент при x^i будет равен

$c_i \equiv (a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \ldots + a_{i-1}b_1 + a_ib_0) \pmod p.$



а)



б)

Рис. 3.3. Умножение с вынесенными (*а*) и встроенными (*б*) сумматорами

Процедура перемножения многочленов по тактам Таблица 3.1.

№ такта	Вход	Выход
1	a_n	$a_n b_k$
2	a_{n-1}	$a_{n-1} b_k + a_n b_{k-1}$
3	a_{n-2}	$a_{n-2} b_k + a_{n-1} b_{k-1} + a_n b_{k-2}$
4	a_{n-3}	$a_{n-3} b_k + a_{n-2} b_{k-1} + a_{n-1} b_{k-2} + a_n b_{k-3}$
……	…….	…….
$n+k-1$	0	$a_0 b_1 + a_1 b_0$
$n+k$	0	$a_0 b_0$

Рассмотрим некоторые характерные особенности построения этих схем для многочленов с двоичными коэффициентами, а именно с коэффициентами 0 и 1. Умножение на величину b_i производим по правилу:
для $b_i=0$: $a_j \cdot b_i = a_j \cdot 0 = 0$ и для $b_i = 1$: $a_j \cdot b_i = a_j \cdot 1 = a_j$.
Таким образом, умножение на 0 соответствует разорванной цепи, а умножение на 1 – короткому замыканию.

Пример умножения. Пусть даны два многочлена с коэффициентами из двоичного поля

$f_1(x) = 1 + x^3 + x^4 + x^6 + x^8$, $f_2(x) = x + x^2 + x^3$

Их произведение после приведения коэффициентов по модулю 2 будет равно:

$f(x) = f_1(x) \cdot f_2(x) = x + x^2 + x^3 + x^4 + x^8 + x^{10} + x^{11}$

Многочлену $f_1(x)$ соответствует комбинация (100110101), а многочлену $f_2(x)$ – (0111). Начало комбинации соответствует младшему разряду, т. е. нулевой степени x.

Умножение $f_1(x) \cdot f_2(x)$ в двоичном представлении:

$f_1(x) \rightarrow$(1 0 0 1 1 0 1 0 1)
$\times 0$ 0 0 0 0 0 0 0 0 0
$\times 1(x)$ 1 0 0 1 1 0 1 0 1 $\times f_2(x)$
$\times 1(x^2)$ 1 0 0 1 1 0 1 0 1
$\times 1(x^3)$ 1 0 0 1 1 0 1 0 1
(0 1 1 1 1 0 0 0 1 0 1 1);

Пусть, например, $f_2(x) = 1 + x + x^3 + x^5$, т. е. $b_0 = 1$, $b_1 = 1$, $b_2=0$, $b_3= 1$, $b_4 = 0$, $b_5 = 1$.

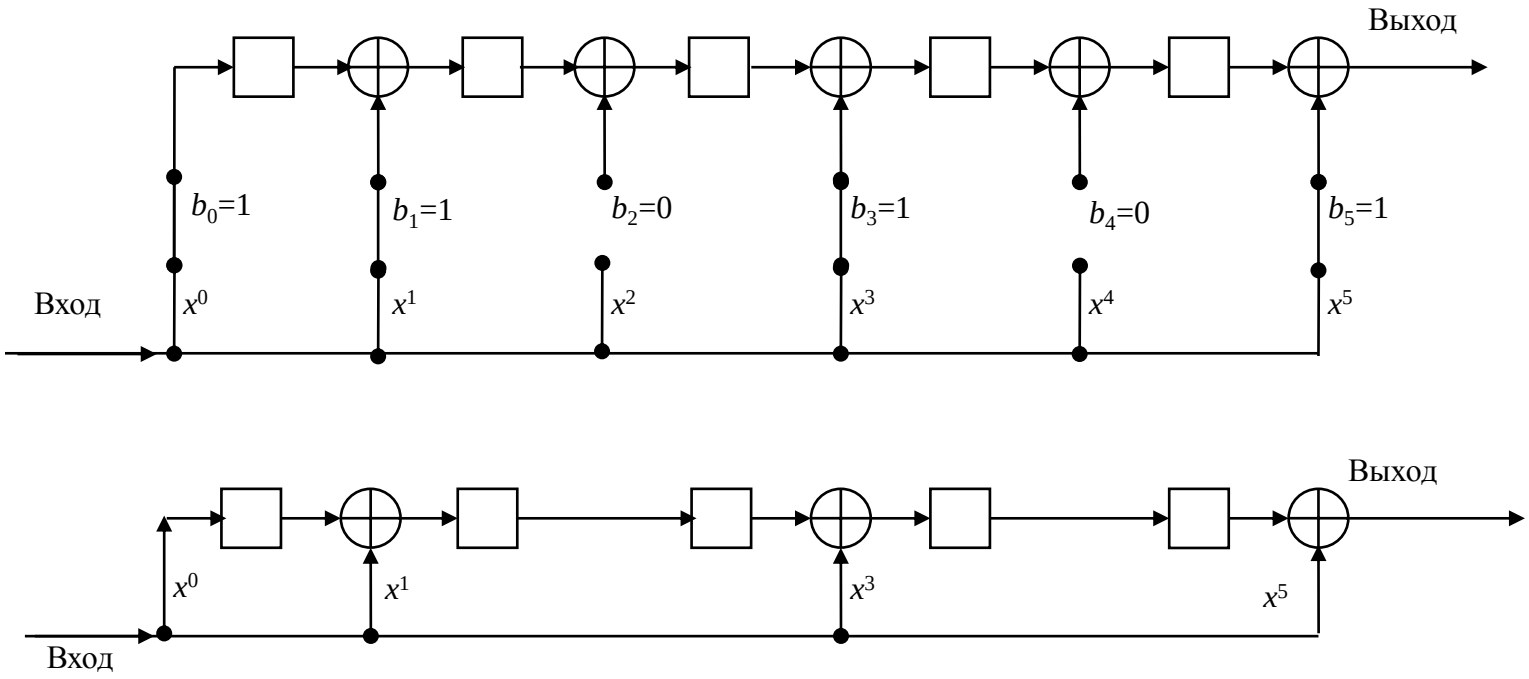


Рис. 3.4. Пример реализации умножения на основе регистра со встроенными сумматорами.

Аналогично строится регистр умножения с вынесенными сумматорами.

Деление многочленов

Операция деления многочленов осуществляется по обычным правилам деления с приведением коэффициентов по mod$p$. Например, деление двоичных многочленов (p = 2) осуществляется следующим образом:

$$
\begin{array}{l|l}
x^8+x^6+x^4+x^3+1 & x^3+x^2+x \\
\cline{2-2}
x^8+x^7+x^6 & x^5+x^4+x^3+1 \\
\cline{1-1}
x^7+x^4+x^3+1 & \\
x^7+x^6+x^5 & \\
\cline{1-1}
x^6+x^5+x^4+x^3+1 & \\
x^6+x^5+x^4 & \\
\cline{1-1}
x^3+1 & \\
x^3+x^2+x & \\
\cline{1-1}
x^2+x+1\ (\textit{остаток}) &
\end{array}
$$

Деление $f_1(x)$:$f_2(x)$ в двоичном виде.

При делении комбинации $f_1(x)$ и $f_2(x)$ записывают в двоичной форме со старшего разряда и делят следующим образом:

$f_1(x)$	$f_2(x)$	
101011001	1110	
1110		
1001		
1110		
1111		
1110		
0010		
1110		
0100		
1110		
1001		
1110		
111 $\rightarrow x^2+x+1$ (остаток)	111001	$\rightarrow x^5+x^4+x^3+1$ (частное)

В общем виде операция деления может быть записана так:

$$\begin{array}{l|l} a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 & b_k x^k + b_{k-1}x^{k-1} + \ldots + b_1 x + b_0 \\ \hline \frac{a_n}{b_k} b_k x^n + \frac{a_n}{b_k} b_{k-1} x^{n-1} + \ldots + \frac{a_n}{b_k} b_0 x^{n-k} & \frac{a_n}{b_k} x^{n-k} + \ldots. \end{array}$$

$$(a_{n-1} - \frac{a_n}{b_k} b_{k-1}) x^{n-1} + \ldots + (a_{n-k} - \frac{a_n}{b_k} b_0) x^{n-k} + \ldots + a_1 x + a_0$$

$$- -$$

При этом коэффициенты $(a_{n-1} - \frac{a_n}{b_k} b_{k-1}), \ldots (a_{n-k} - \frac{a_n}{b_k} b_0)$ приводятся по модулю p.

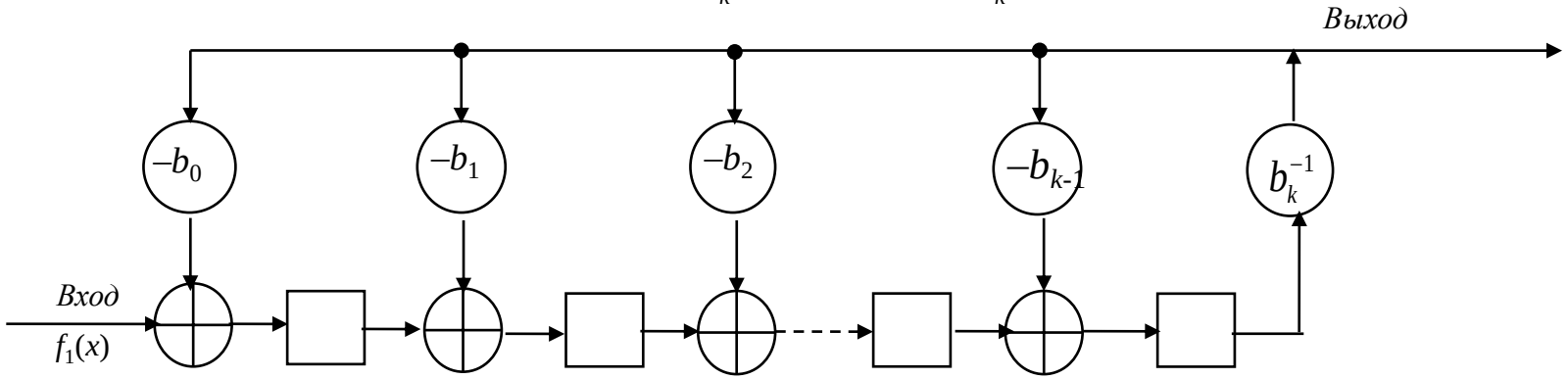


Рис. 3.5. Схема деления на многочлен $f_2(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_k x^k$

Пример. Пусть $f_2(x) = 1 + x^2 + x^4 + x^5$, т. е. $b_0 = 1$, $b_1 = 0$, $b_2 = 1$, $b_3 = 0$, $b_4 = 1$, $b_5 = 1$. На рис. 3.6 представлена схема деления на заданный многочлен.

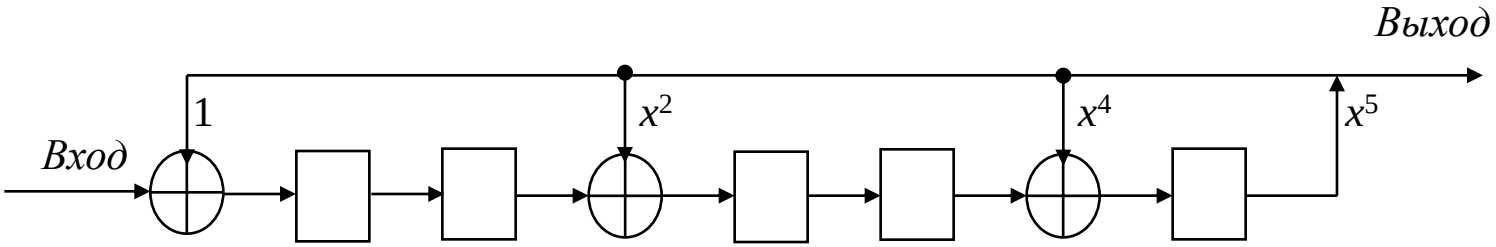


Рис. 3.6

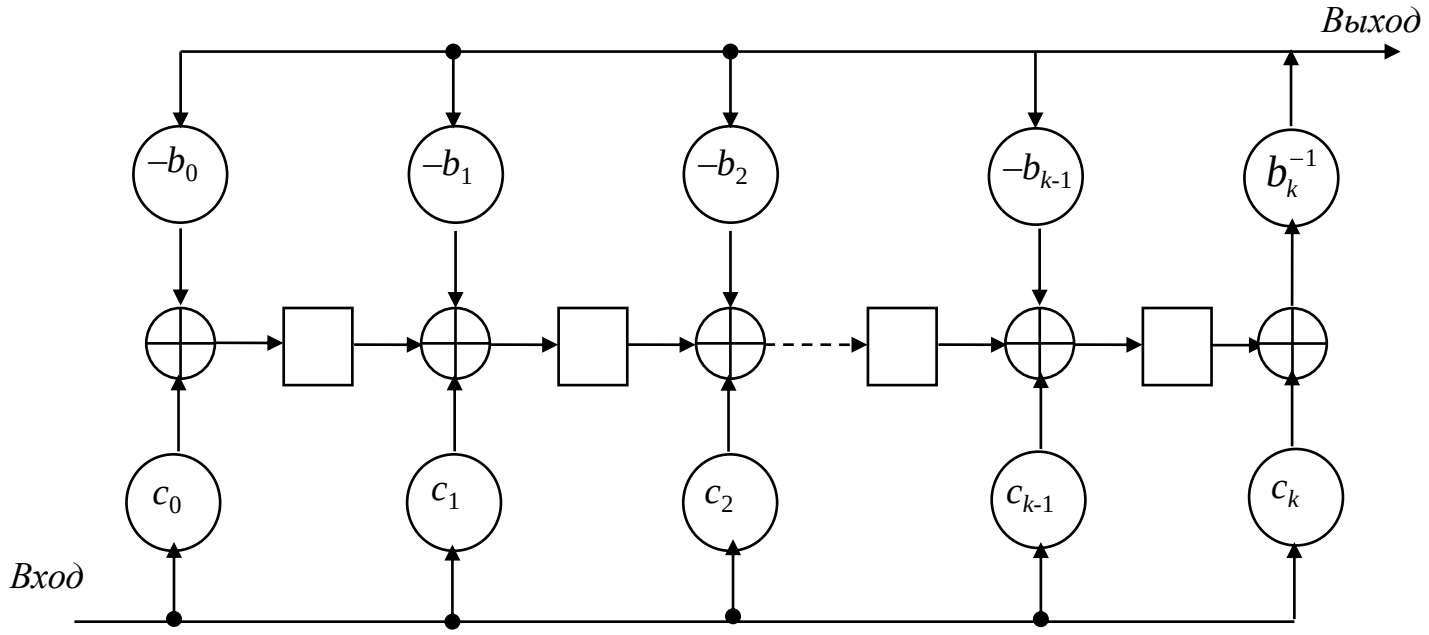
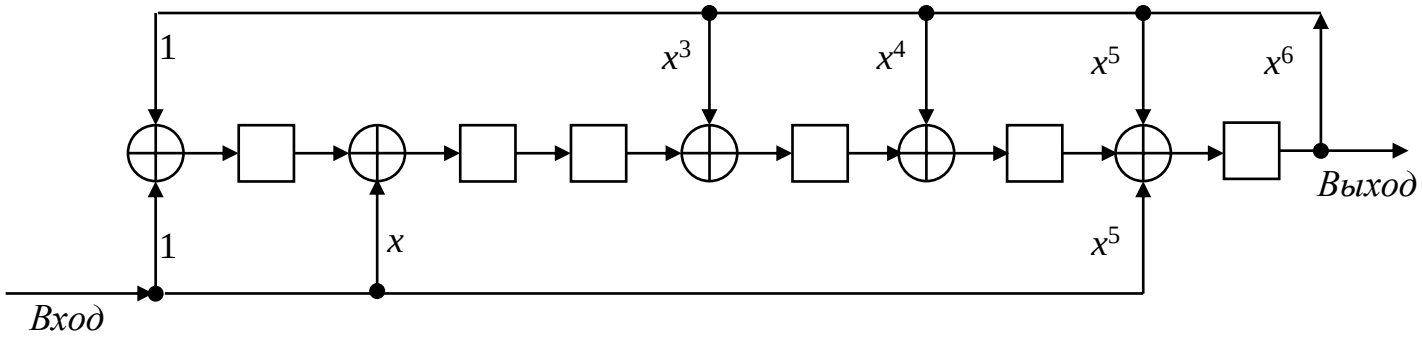
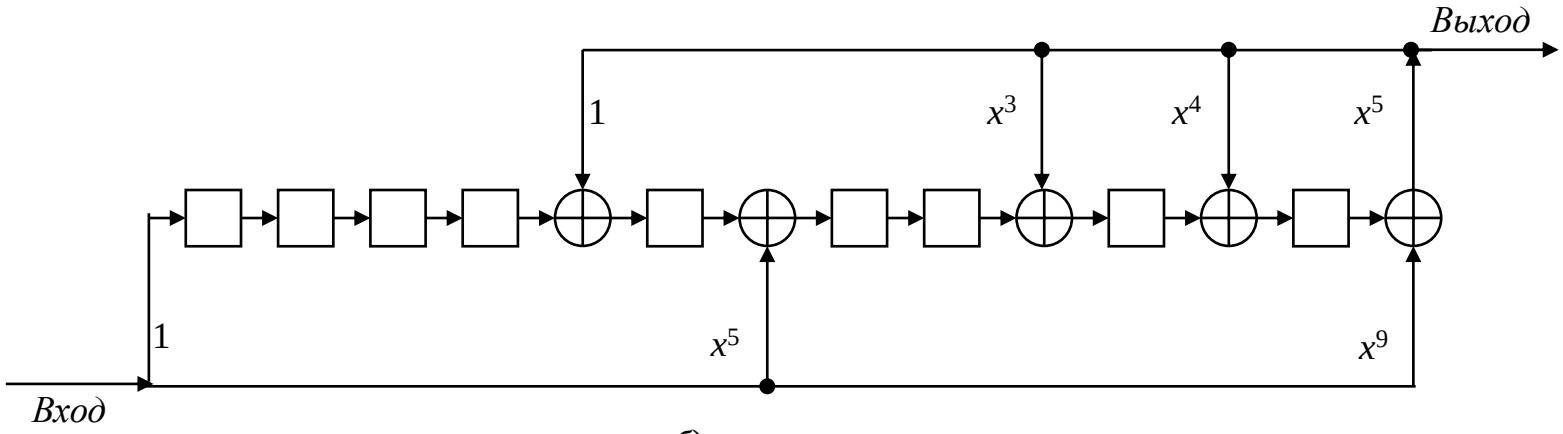


Рис. 3.7. Схема, реализующая одновременное умножение на многочлен $h(x) = c_0 + c_1x + .. + c_kx^k$ и деление на многочлен $g(x) = b_0 + b_1x + b_2x^2 + ... + b_kx^k$

Реализация операций одновременного умножения и деления многочленов в поле двоичных чисел.



а)



б)

Рис. 3.8. Примеры схем, реализующих одновременное умножение на многочлен $h(x)$ и деление на многочлен $g(x)$ для:

а) $h(x)= 1+ x + x^5$ и $g(x)=1+x^3+x^4+ x^5+ x^6$;

б) $h(x)= 1+ x^5 + x^9$ и $g(x)=1+x^3+x^4+ x^5$

Определение 1. Полином $A(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$

называется полиномом над полем GF(p), если его коэффициенты a_i принадлежат полю GF(p).

Определение 2. ***Сравнение полиномов по модулю F(x).*** Полином $A(x)$ сравним с полиномом $B(x)$ по модулю $F(x)$, т.е. $A(x) \equiv B(x) \bmod F(x)$, если разность $A(x) - B(x)$ делится на $F(x)$ без остатка.

Определение 3. ***Сравнение полиномов по двойному модулю F(x) и p.*** Если при сравнении полиномов $A(x)$ и $B(x)$ по модулю $F(x)$ все коэффициенты, кроме того, приводятся по модулю p, то тогда говорят, что полином $A(x)$ сравним с полиномом $B(x)$ по двойному модулю ($F(x)$, p),что записывается как $A(x) \equiv B(x) \bmod(F(x),p)$.

Определение 4. Если дан полином $F(x)$ степени n над полем GF(p), то любому полиному $A(x)$ степени m ($m \geq n$) будет соответствовать остаток $R(x)$ от деления $A(x)$ на $F(x)$, т.е. $A(x) \equiv R(x) \bmod(F(x),p)$. При этом $R(x)$ – это вычет по двойному модулю $\bmod(F(x),p)$, который представляет собой полином степени не выше (n-1)

$$R(x) = \sum_{i=0}^{n-1} r_i x^i = r_0 + r_1 x + r_2 x^2 + \ldots + r_{n-1} x^{n-1}$$

где $r^i \in$ GF(p).

Эварист Галуа. Нестандартность. Путь гения.

Эварист Галуа (26 октября 1811 – 31 мая 1832) – выдающийся французский математик, основатель современной высшей алгебры

Галуа успел в свои 21 год состояться как математик, да такой что не знала Франция со времен Декарта. Был убит на глупой дуэли. Его заметки опубликовали через 15 лет. Стали нужны математике еще через 50 лет. Маленький ручеёк идеи стал огромной рекой. Обычная судьба гения.

За 20 лет жизни Галуа успел сделать открытия, ставящие его на уровень крупнейших математиков XIX века. Решая задачи по теории алгебраических уравнений, он заложил основы современной алгебры, вышел на такие фундаментальные понятия, как группа (Галуа первым использовал этот термин, активно изучая симметрические группы) и поле (конечные поля носят название полей Галуа).

Эварист Галуа предсмертное стихотворение в 21 год

И жизнь пройдет, как тихие дожди,
Загадка, не разгаданная нами…
Осталось на костёр судьбы взойти
И кануть в пожирающее пламя…
Сгореть нестрашно, страшно дымом стать…
Развеяться, растаять, раствориться,
Исчезнуть, до конца сумев понять,
Что в этой жизни есть к чему стремиться…
Мир нем и глух, застлал глаза туман.
Как страшно все, и все-таки я верю,
Что вечность есть, что это не обман,
Что найдены распахнутые двери.
И что разгадки тайн всегда просты.
И стали вдруг доступны пониманью
Возможность нереальная мечты
И хрупкость моего существованья…

Поля Галуа и их свойства. Конечное поле, называемое именем французского математика Эвариста Галуа и обозначаемое GF(q) (GF – Galois Field – поле Галуа), представляет собой конечное множество, состоящее из q элементов, обладающих свойствами поля. Число элементов поля GF(q) может быть простым числом или степенью простого числа. Если q – простое число, то поле GF(q) будет простым с характеристикой q, элементами которого будут числа 0,1,2,…,(q–1), представляющие собой полную систему вычетов по модулю простого числа q. *Порядок такого простого поля равен* q. При этом в соответствии со свойствами поля сложение и умножение элементов такого поля осуществляется с приведением по модулю q.

Если же q является степенью, например, простого числа p, т.е. $q= p^m$, где m – целое, то конечное поле GF(p^m) будет **расширением** простого поля, а элементами расширенного поля будут многочлены степени (m – 1) вида

$$a_0 + a_1x + a_2x^2 + ... + a_{m-1}x^{m-1}\ , \qquad (3.1)$$

где все коэффициенты a_i пробегают полную систему вычетов по модулю p, т.е. принадлежат простому полю GF(p).

Сложение двух элементов

$A = a_0 + a_1x + a_2x^2 + ... + a_{m-1}x^{m-1}$;

$B = b_0 + b_1x + b_2x^2 + ... + b_{m-1}x^{m-1}$

производится с приведением коэффициентов по модулю p. Тогда элемент $C = c_0 + c_1x + c_2x^2 + ... + c_{m-1}x^{m-1}$ будет суммой двух элементов A и B, т. е. $C = A + B$, где $c_i \equiv (a_i+b_i) \bmod p$.

Для **умножени**я двух элементов поля A и B перемножим их алгебраически как многочлены независимой переменной x, затем найдем остаток D от деления произведения $A \cdot B$ на некоторый специальный многочлен $P(x)$ степени m с коэффициентами, принадлежащими простому полю GF(p). Этот многочлен должен обладать тем свойством, что его нельзя разложить на множители, используя только многочлены с коэффициентами из простого поля GF(p). Такой многочлен называют неприводимым. Тогда полученный остаток D с коэффициентами, принадлежащими простому полю GF(p), можно рассматривать как вычет по двойному модулю – по и mod$P(x)$ и mod$p$, т.е. $A \cdot B \equiv D[\text{modd } P(x), p]$. При таких правилах сложения и умножения совокупность рассматриваемых p^m элементов вида (3.1) образует конечное поле, называемое полем Галуа и обозначаемое как GF(p^m).

Итак, *полная система вычетов по двойному модулю* [modd $P(x)$, p] *образует конечное поле Галуа, содержащее* p^m *элементов, которое обозначают* GF(p^m) *и называют расширенным полем или расширением степени* m *простого поля* GF(p).

Таблица 3.2. Формы представления элементов поля GF(2^4)

Выберем в качестве порождающего поле **GF(2^4)** неприводимый по модулю 2 примитивный многочлен четвертой степени
***P*(*x*) = 1+ *x* + x^4**. Пусть ε является корнем данного многочлена
$P(\varepsilon)=0$.
Тогда **$1+\varepsilon+\varepsilon^4=0$**
$\varepsilon^4 = 1+\varepsilon \pmod{2, P(\varepsilon)}$

В полиномиальной форме представления:

$\varepsilon^i=a_0+a_1\varepsilon+a_2\varepsilon^2+a_3\varepsilon^3$.

В векторной форме представления:
$(a_0a_1a_2a_3)$

Степенная	Полиномиальная	Целочисленная	Векторная $(a_0a_1a_2a_3)$
ε-∞	0	0	(0000)
ε^0	1	1	(1000)
ε^1	ε	2	(0100)
ε^2	ε^2	3	(0010)
ε^3	ε^3	4	(0001)
ε^4	$1+\varepsilon$	5	(1100)
ε^5	$\varepsilon+\varepsilon^2$	6	(0110)
ε^6	$\varepsilon^2+\varepsilon^3$	7	(0011)
ε^7	$1+\varepsilon+\varepsilon^3$	8	(1101)
ε^8	$1+\varepsilon^2$	9	(1010)
ε^9	$\varepsilon+\varepsilon^3$	10	(0101)
ε^{10}	$1+\varepsilon+\varepsilon^2$	11	(1110)
ε^{11}	$\varepsilon+\varepsilon^2+\varepsilon^3$	12	(0111)
ε^{12}	$1+\varepsilon+\varepsilon^2+\varepsilon^3$	13	(1111)
ε^{13}	$1+\varepsilon^2+\varepsilon^3$	14	(1011)
ε^{14}	$1+\varepsilon^3$	15	(1001)
ε^{15}	1		

СВОЙСТВА ПОЛЯ

Многочлены $P(x)$ и элементы поля GF(p^m) обладают целым рядом свойств, используемых при построении и описании циклических кодов. Приведем основные из этих свойств.

Свойство 1.1. Все отличные от нуля элементы поля GF(p^m) образуют мультипликативную циклическую группу порядка $p^m - 1$. Тогда, для любого ненулевого элемента поля ε имеет место равенство $\varepsilon^{p^m-1} = 1.$

Свойство 1.2. В поле GF(p^m) всегда существует первообразный элемент ε, т. е. элемент, порядок которого равен $p^m - 1$. При этом каждый ненулевой элемент поля может быть представлен как некоторая степень одного и того же первообразного элемента ε. Иными словами: мультипликативная группа поля Галуа циклична.

Свойство 1.3. Всякий неприводимый по модулю p многочлен $P(x)$ степени m, если он существует, есть делитель по этому модулю двучлена $x^{p^m-1} - 1$

Примитивным называется такой неприводимый по модулю p многочлен $P(x)$ степени m, корни которого являются первообразными элементами поля GF(p^m), т .е. имеющими порядок $p^m - 1$.

Порядок корней неприводимого по модулю p многочлена называют *показателем*, к которому этот многочлен принадлежит. Если неприводимый многочлен принадлежит показателю k, то он является делителем многочлена $x^k - 1$, но не является делителем многочленов вида $x^n - 1$, где $n < k$.

Следовательно, неприводимый многочлен $P(x)$ степени m является примитивным тогда и только тогда, когда он принадлежит показателю $p^m - 1$.

Свойство 1.4. В простом поле характеристики p имеет место равенство $(a + b)^p = a^p + b^p$.
Действительно, $(a+b)^p = a^p + C_p^1 a^{p-1}b + C_p^2 a^{p-2}b^2 + \ldots + C_p^{p-1} ab^{p-1} + b^p$

Но, так как для всех $0 < i < p$ имеем $C_p^i = 0 \pmod p$, то, следовательно, получаем

$(a+b)^p = a^p + b^p$, что и требовалось доказать.

Аналогичным образом доказывается, что в поле характеристики p имеют место формулы:

$$\left(a+b\right)^{p^n} = a^{p^n} + b^{p^n}$$

$$\left(a_1 + a_2 + a_3 + \ldots + a_n\right)^p = a_1^p + a_2^p + a_3^p + \ldots + a_n^p$$

Важной является также *малая теорема Ферма* [11,12], которая гласит:
Для каждого класса вычетов a по модулю p, взаимно простого с модулем, выполняется сравнение $a^{\varphi(p)} \equiv 1 \pmod p$, *где* $\varphi(p)$ *– функция Эйлера. Если p простое число, то функция Эйлера* $\varphi(p) = p - 1$ *и тогда* $a^{p-1} \equiv 1 \pmod p$.
На основании этой теоремы и свойства 1.4 легко доказывается следующее важное для теории циклических кодов свойство:
Свойство 1.5. Для простого модуля p существует сравнение

$$[P(x)]^p \equiv P(x^p) \pmod p,$$

где $P(x)$ – произвольный многочлен, коэффициенты которого принадлежат простому полю GF(p).

Пусть теперь элемент ε поля GF(p^m) является корнем неприводимого многочлена $P(x)$ степени m. Тогда $P(\varepsilon) = 0$, а по свойству 1.5 $[P(\varepsilon)]^p = P(\varepsilon^p) = 0$.
Следовательно, если ε корень неприводимого многочлена $P(x)$, то ε^p является также его корнем. Аналогично можно показать, что для неприводимого многочлена $P(x)$ степени m корнями будут также элементы поля $\varepsilon^{p^2}, \varepsilon^{p^3}, \ldots, \varepsilon^{p^{m-1}}$

Таким образом, доказано следующее свойство полей Галуа:
Свойство 1.6. Если элемент ε поля GF(p^m) является корнем неприводимого по модулю p многочлена $P(x)$ степени m, то остальными корнями многочлена $P(x)$ будут так называемые *p-сопряжённые элементы*

$$\varepsilon^{p}, \varepsilon^{p^2}, \varepsilon^{p^3}, \ldots, \varepsilon^{p^{m-1}}$$

Свойство 1.7. Многочлен $x^k - 1$ является делителем многочлена $x^n - 1$, если k – делитель n.
По этому свойству в поле GF(p^m) будут иметь место элементы ε^i, которые относятся к показателю k, являющимся делителем порядка $p^m - 1$. Такие элементы не будут первообразными элементами поля GF(p^m), они будут корнями двучлена $x^k - 1$, т.е. $(\varepsilon^i)^k = 1$, а их количество будет равно функции Эйлера $\varphi(k)$.
Свойство 1.8. Если неприводимый по модулю p многочлен $P_1(x)$ степени k является делителем двучлена $\chi^{p^m-1} - 1$, то степень k должна быть делителем числа m. И наоборот: всякий неприводимый по модулю p многочлен $P_1(x)$, степень которого k есть делитель числа m, будет делителем по модулю p двучлена $\chi^{p^m-1} - 1$.

Свойство 1.9. Всякий неприводимый по модулю p многочлен $P_1(x)$, который является делителем двучлена $x^{p^m-1}-1$, входит в состав этого двучлена однократно.

Таким образом, двучлен $x^{p^m-1}-1$ раскладывается на ряд различных неприводимых сомножителей-многочленов, степени которых d будут делителями числа m. Сомножители, имеющие степень, равную некоторому определенному делителю d, обозначим через $\Phi_d(x)$. Тогда в числовом поле по модулю p существует равенство

$$x^{p^m-1}-1 = \Pi\Phi_d(x), \qquad (3.2)$$

где произведение П распространяется на все d делители числа m, включая d=1. Многочлены $\Phi_d(x)$ называются *многочленами деления круга*.

Свойство 1.10. Для любого простого числа p и любого неприводимого по модулю p многочлена $P(x)$ степени m существует только одно поле Галуа GF(p^m), иными словами, поля Галуа GF(p^m), образованные различными неприводимыми примитивными многочленами степени m, изоморфны.

Свойство 1.11. Для каждого делителя $n > 0$ числа m в поле GF(p^m) существует подполе GF(p^n). Элемент ε^i поля GF(p^m) принадлежит подполю GF(p^n), если он удовлетворяет уравнению $(\varepsilon^i)^{p^n-1}=1$, т. е. если его порядок (в мультипликативной группе поля GF(p^m)) является делителем числа $p^n - 1$.

Тогда все ненулевые элементы поля GF(p^m), принадлежащие подполю GF(p^n), должны быть корнями двучлена $x^{p^n-1}-1$. Следовательно, двучлен $x^{p^n-1}-1$ должен быть делителем многочлена $x^{p^m-1}-1$, а по свойству 1.7 число ($p^n - 1$) должно быть делителем числа ($p^m - 1$), а n делителем m.

Все приведенные выше свойства полностью характеризуют поля Галуа и позволяют их построить.

Пример 1.

Выберем в качестве порождающего поле **GF(2^4)** неприводимый по модулю 2 примитивный многочлен четвертой степени из таблиц:
$\boldsymbol{P(x) = 1 + x + x^4}$.
Пусть ε является корнем данного многочлена
$P(\varepsilon) = 0$.
Тогда $\mathbf{1} + \boldsymbol{\varepsilon} + \boldsymbol{\varepsilon^4} = \mathbf{0}$
$\boldsymbol{\varepsilon^4} = \mathbf{1} + \boldsymbol{\varepsilon}$ (modd2,P(ε))

В полиномиальной форме представления:

$\boldsymbol{\varepsilon^i = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3}$.

В векторной форме представления:

$\boldsymbol{(a_0 a_1 a_2 a_3)}$

Таблица 3.2. Формы представления элементов поля GF(2^4)

Степенная	Полиномиальная	Целочисленная	Векторная ($a_0 a_1 a_2 a_3$)
	0	0	(0000)
ε^0	1	1	(1000)
ε^1	ε	2	(0100)
ε^2	ε^2	3	(0010)
ε^3	ε^3	4	(0001)
ε^4	$1+\varepsilon$	5	(1100)
ε^5	$\varepsilon+\varepsilon^2$	6	(0110)
ε^6	$\varepsilon^2+\varepsilon^3$	7	(0011)
ε^7	$1+\varepsilon+\varepsilon^3$	8	(1101)
ε^8	$1+\varepsilon^2$	9	(1010)
ε^9	$\varepsilon+\varepsilon^3$	10	(0101)
ε^{10}	$1+\varepsilon+\varepsilon^2$	11	(1110)
ε^{11}	$\varepsilon+\varepsilon^2+\varepsilon^3$	12	(0111)
ε^{12}	$1+\varepsilon+\varepsilon^2+\varepsilon^3$	13	(1111)
ε^{13}	$1+\varepsilon^2+\varepsilon^3$	14	(1011)
ε^{14}	$1+\varepsilon^3$	15	(1001)
ε^{15}	1		

Пример 2. Определить делители двучлена , где $p = 2$, а $m = 4$.

Из свойства 1.8 следует, что делителями многочлена будут все неприводимые многочлены, степень которых является делителем числа m. В примере делителями числа $m = 4$ будут 4, 2, 1. Находим по таблицам все неприводимые многочлены этих степеней. Они и дают разложение двучлена $(x^{15} - 1)$ на множители:

$(x^{15} - 1) = (x - 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$.

Пример 3. При построении поля Галуа $GF(2^4)$ был выбран неприводимый примитивный многочлен $P(x) = 1 + x + x^4$, ε – корень этого многочлена. Определить, какие элементы поля $GF(2^4)$ относятся к каждому из множителей в разложении двучлена $x^{15} - 1$, т. е.. найти корни для каждого из множителей, приведенных в примере 2, а также определить порядок корней $N(\varepsilon^i)$.

При решении этой задачи необходимо использовать свойства 1.6 и 1.7. Корнями многочлена $P(x)$ будут элементы: ε, ε^2, ε^4, ε^8.

Таблица 3.3.

Многочлен	Степень многочлена	Корни многочлена
$P(x)$	4	$\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^8$
$P_1(x)$	4	$\varepsilon^3, \varepsilon^6, \varepsilon^9, \varepsilon^{12}$
$P_2(x)$	2	$\varepsilon^5, \varepsilon^{10}$
$P_3(x)$	4	$\varepsilon^7, \varepsilon^{11}, \varepsilon^{13}, \varepsilon^{14}$
$P_4(x)$	1	$\varepsilon^{15}=1$

Для определения порядка элемента поля ε^i можно использовать формулу:

$$N(\varepsilon^i) = \frac{p^m - 1}{НОД(i, p^m - 1)}$$

Задание для самостоятельной работы: найти значения многочленов $P_i(x)$, зная корни многочленов и используя формулы Виета и значения элементов поля из таблицы примера1.

Свойство 1.12. Если ε –примитивный элемент поля GF(p^m), то мультипликативно обратный ему элемент ε^{-1} также является примитивным (первообразным) элементом, так как $-1 \equiv p^m - 2 (\mathrm{mod}\, p^m - 1)$. а числа p^m-1 и p^m-2 являются взаимно простыми.

Свойство 1.13. Если имеется многочлен $A(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m$ то двойственным ему (взаимным) будет многочлен $\tilde{A}(x) = x^m a_0^{-1} A(x^{-1})$, а его корнями будут элементы поля GF(p^m), мультипликативно обратные корням многочлена $A(x)$.

Функция-след элементов поля GF(p^m)

Функций-след (следом) элемента ε поля GF(p^m) в простом поле GF(p) называют сумму следующих p-сопряжённых элементов поля :

$$Tr(\varepsilon^i) = \sum_{k=0}^{m-1} (\varepsilon^i)^{p^k} = \varepsilon^i + (\varepsilon^i)^p + (\varepsilon^i)^{p^2} + \ldots + (\varepsilon^i)^{p^{m-1}}.$$

Свойства функции-след:

Свойство 1. Функция-след является отображением расширенного поля GF(p^m) в простое поле GF(p) $\varepsilon^i \in GF(p^m) \Rightarrow Tr(\varepsilon^i) \in GF(p).$

Свойство 2. Когда ε^i пробегает все элементы расширенного поля GF(p^m), функция-след Tr(ε^i) принимает каждое из значений простого поля GF(p) ровно p^{m-1} раз.

Свойство 3. Функция-след от суммы элементов расширенного поля равна сумме функций-след от каждого из этих элементов: $Tr(\varepsilon^i + \ldots + \varepsilon^j) = Tr(\varepsilon^i) + \ldots + Tr(\varepsilon^j)$