$$a(X) \equiv r(X) \pmod{f(X)} \qquad (3\text{-}27)$$

при фиксированном многочлене $r(X)$, степень которого меньше степени n многочлена $f(X)$, т.е. многочлены, которые при делении на $f(X)$ дают один и тот же остаток $r(X)$, образуют *класс вычетов по модулю многочлена* $f(X)$ $\{r(X)\}$ [3.2, с. 172]. Любой многочлен класса $\{r(X)\}$ называется *вычетом по модулю многочлена* $f(X)$ степени n по отношению ко всем многочленам этого класса.

Из приведенного определения класса вычетов по модулю многочлена $f(X)$ вытекает, что всем многочленам одного и того же класса вычетов соответствует один и тот же остаток $r(X)$, и что все многочлены класса $\{r(X)\}$ можно получить, заставив $q(X)$ в выражении

$$q(X)f(X) + r(X) \qquad (3\text{-}27а)$$

пробегать все возможные многочлены с коэффициентами из $GF(p)$.

Таким образом, если $f(X)$ – многочлен степени n с коэффициентами из $GF(p)$, то всевозможные остатки $r(X)$ являются многочленами степени не выше n - 1:

$$r(X) = a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_1X + a_0, \qquad (3\text{-}28)$$

где каждый коэффициент из совокупности $\{a_{n-1}, a_{n-2}, \ldots, a_1, a_0\}$ может быть любым из p элементов поля $F_0 = GF(p)$.

Из (3-28) следует, что существует точно $|F_0|^n = p^n$ различных многочленов $r(X)$ и, соответственно, имеется столько же классов $\{r(X)\}$.

В соответствии со свойствами сравнений (см. пункты 5) и 6) в примере 3.30), если

$$a(X) \equiv r_1(X) \pmod{f(X)} \quad \text{и} \quad b(X) \equiv r_2(X) \pmod{f(X)},$$

то

$$a(X) + b(X) \equiv r_1(X) + r_2(X) \pmod{f(X)}, \qquad (3\text{-}29)$$

и

$$a(X)b(X) \equiv r_1(X)r_2(X) \pmod{f(X)}. \qquad (3\text{-}30)$$

На основе двух последних соотношений могут быть определены операции сложения и умножения классов вычетов по модулю $f(X)$:

$$\{r_1(X)\} + \{r_2(X)\} = \{r_1(X) + r_2(X)\}, \qquad (3\text{-}31)$$
$$\{r_1(X)\}\{r_2(X)\} = R_{f(X)}[r_1(X)r_2(X)], \qquad (3\text{-}32)$$

где $R_{f(X)}[r_1(X)r_2(X)]$ – остаток от деления $r_1(X)r_2(X)$ на многочлен $f(X)$ [3.1, с. 236].

Легко проверить, что полученная описанным способом из кольца многочленов бесконечного порядка алгебраическая структура конечного порядка $|F_0|^n = p^n$ также является кольцом классов вычетов по модулю многочлена $f(X)$ степени n.

Более того, можно убедиться также в том, что все законы поля, за исключением $M5$, удовлетворяются для операций сложения и умножения классов вычетов при произвольном многочлене $f(X)$ над $GF(p)$. Однако, подобно тому как это имело место при создании конечных полей Z_m порядка m, когда m должно было быть *простым числом*, в рассматриваемом случае закон $M5$ удовлетворяется для ненулевых элементов образованного указанным образом кольца классов вычетов по модулю $f(X)$ конечного порядка только в том случае, если $f(X)$ – ***неприводимый*** многочлен над $F_0 = GF(p)$; при этом элемент $\{0\}$ – нуль по сложению и элемент $\{1\}$ – единица по умножению.

Взяв от каждого класса вычетов по одному вычету, получим *полную систему вычетов*. Следовательно, полная система вычетов является совокупностью многочленов степени не выше n - 1, т.е. многочленов вида (3-28).

Несложно убедиться в том, что *полная система вычетов* по модулю *неприводимого* над $F_0 = GF(p)$ многочлена

$f(X)$, где p – простое число, с определёнными выше операциями сложения и умножения элементов этой системы удовлетворяет всем *законам поля* (см. теоремы 3.4 и 3.13).

Таким образом, *полная система вычетов по модулю неприводимого* многочлена $f(X)$ над полем F_0 с операциями сложения и умножения её элементов является конечным *полем*, содержащим p^n элементов – многочленов степени не выше n - 1 – представителей всех классов вычетов.

Множество всех классов вычетов по модулю неприводимого над F_0 многочлена $f(X)$ с определёнными над ними бинарными операциями сложения и умножения обозначают как $F_0[f] = F = GF(p^n)$ (n – любое целое положительное число) и называют *расширенным полем* или *расширением степени n основного поля* $F_0 = GF(p)$.

Так как операции над элементами в $F_0 = GF(2)$ являются теми же самыми, что и операции над элементами в F, то 0 и 1 также принадлежащие F, образуют поле F_0, содержащееся в F.

Таким образом, новое, расширенное поле $F = F_0[f]$ порядка p^n состоит из классов вычетов, среди которых содержатся элементы основного поля F_0, и поэтому говорят, что новое поле содержит в себе исходное – основное поле [3.3; 3.7].

ОПРЕДЕЛЕНИЕ 3.2. *Если подмножество F_0 элементов поля F ($F_0 \subseteq F$) само является полем, то F_0 называется* ***подполем*** *поля F, а F –* ***расширением*** *F_0.*

END

Там, где это не вызывает путаницы, для краткости, мы будем в тексте вместо слов «класс вычетов по модулю $f(X)$» писать просто «многочлен», имея в виду некоторый многочлен из полной системы вычетов по модулю $f(X)$, являющийся представителем класса вычетов, о котором идёт речь.

Подчеркнём дополнительно, что в отличие от случая *простого поля* $F_0 = GF(p)$, когда элементами поля являются

целые числа, в случае *расширенного поля* $F = GF(p^n)$, элементами поля являются *многочлены с коэффициентами из* $GF(p)$ *степени не выше n* - 1. В частности, при $p = 2$, $F_0 = GF(2) = \{0, 1\}$; при этом *числа* 0 и 1 – элементы поля $F_0 = GF(2)$ принадлежат также полю $F = GF(2^n)$ и рассматриваются в нём как *нулевой и единичный многочлен* соответственно.

Таким образом, мы показали, что если $f(X)$ – *неприводимый многочлен* из $F_0[X]$ степени n, то можно построить *новое расширенное поле* $F_0[f] = F = GF(p^n)$ порядка p^n, элементами которого являются классы вычетов по модулю $f(X)$.

Элемент α *из расширенного поля* $F_0[f]$ *называется корнем многочлена* $f(X)$ *над полем* F_0, *если* $f(\alpha) = 0$.

Исходя из практики использования циклических кодов, мы ограничимся ниже лишь рассмотрением случаев однократных корней.

Согласно алгоритму Евклида имеем:

$$f(X) = (X - \alpha)h(X) + r(X). \qquad (3\text{-}33)$$

Так как степень многочлена $(X - \alpha)$ равна 1, то степень $r(X)$ должна быть равна 0 и, следовательно, $r(X)$ является элементом поля r_0; степень же $h(X)$ равна n - 1. Подставляя в (3-33) α вместо X, получим: $f(\alpha) = r_0$.

ТЕОРЕМА 3.5. *Элемент* α, *принадлежащий полю, является корнем ненулевого многочлена* $f(X)$ *над этим полем тогда и только тогда, когда* $(X - \alpha)$ *является делителем* $f(X)$. *Кроме того, если* $f(X)$ *имеет степень n, то число элементов поля, являющихся корнями* $f(X)$, *не превосходит n.*

ДОКАЗАТЕЛЬСТВО

НЕОБХОДИМОСТЬ. Если $f(\alpha) = 0$, то $r_0 = 0$ и, следовательно, $(X - \alpha)$ является делителем $f(X)$.

ДОСТАТОЧНОСТЬ. Если $(X - \alpha)$ является делителем $f(X)$, то $f(X) = (X - \alpha)h(X)$ и, следовательно, $f(\alpha) = 0$.

Теперь представим $f(X)$ в виде произведения элемента поля и неприводимых множителей степени не меньше 1. Так как степень $f(X)$ равна сумме степеней его множителей, то существует не более n множителей. Так как это разложение является *единственным* [3.1, с. 235], то, следовательно, $f(X)$ имеет не более n корней.

ЧТД

Далее, если $f(X)$ имеет в поле $F_0[f]$ ν различных однократных корней, то существует такой многочлен $h(X) \in F_0^{n-\nu}[X]$ степени n - ν, что $f(X) = (X-\alpha_1), \ldots, (X-\alpha_\nu)\, h(X)$.

Можно показать, что многочлен $X^n - 1$ не имеет кратных корней, если n и p взаимно просты [3.2, с. 237].

ПРИМЕР 3.8. Привести состав *простого* поля Галуа - $GF(2)$ и *расширенных* полей Галуа: $GF(2^2)$ и $GF(2^3)$.

Таблица 3.15

Поле	Состав полей
$GF(2)$	0, 1
$GF(2^2)$	0, 1, X, X+1
$GF(2^3)$	0, 1, X, X+1, X^2, X^2+1, X^2+X, X^2+X+1

Табл. 3.15 содержит состав полей $GF(2)$, $GF(2^2)$ и $GF(2^3)$.

END

Наибольший общий делитель $d(X)$ двух многочленов $r(X)$ и $s(X)$ всегда может быть представлен в виде

$$d(X) = a(X)r(X) + b(X)s(X), \qquad (3\text{-}34)$$

где $a(X)$ и $b(X)$ – многочлены (см. (3-3)).

ПРИМЕР 3.9. Даны двоичные многочлены $r(X) = (1+X)(1+X^2)$ и $s(X) = (1+X)^2$.

Требуется определить НОД $d(X)$ данных многочленов $r(X)$ и $s(X)$, представить его согласно (3-34) и определить $a(X)$ и $b(X)$.

Заметим, что $s(X) = (1+X)^2 = (1+2X+X^2) = (1+X^2)$. Очевидно, что $r(X)$ делится на $s(X)$ и, следовательно, НОД $d(X) = s(X) = (1+X^2)$.

Кроме того, $r(X) = (1+X)(1+X^2) = (1+X^2) + X(1+X^2)$. Откуда находим: $r(X) = d(X) + Xs(X)$ и, следовательно,

$$d(X) = 1 \cdot r(X) + Xs(X) = (1+X)(1+X^2) + X(1+X^2) = (1+X^2);$$

$$a(X) = 1, \quad b(X) = X.$$

END

ПРИМЕР 3.10. Даны неприводимые многочлены:

$$g_1(X) = X^3+X+1, \qquad g_2(X) = X^3+X^2+1.$$

Построить поле порядка 2^3, используя:

а) неприводимый многочлен $g_1(X)$ и определить корни многочленов $g_1(X)$ и $g_2(X)$ в этом поле;

b) неприводимый многочлен $g_2(X)$ и определить корни многочленов $g_1(X)$ и $g_2(X)$ в этом поле.

РЕШЕНИЕ

Пункт а). Рассмотрим классы вычетов многочленов по модулю X^3+X+1: {0}, {1}, {X}, {X+1}, {X^2}, {X^2+1}, {X^2+X}, {X^2+X+1}.

Согласно (3-31) и (3-32) сложение и умножение этих классов вычетов определяются правилами:

$$\{f_1(X)\} + \{f_2(X)\} = \{f_1(X)+f_2(X)\}, \qquad (3\text{-}35)$$

$$\{f_1(X)\}\{f_2(X)\} = R_{g(X)}[f_1(X)f_2(X)], \qquad (3\text{-}36)$$

где $R_{g(X)}[f_1(X)\cdot f_2(X)]$ – остаток от деления $f_1(X)\cdot f_2(X)$ на неприводимый многочлен $g(X)$ ($g_1(X)$ или $g_2(X)$), с помощью кото-

рого создаётся поле; $f_1(X)$ и $f_2(X)$ – представители классов вычетов.

Мы не приводим здесь таблицы для сложения элементов поля $GF(2^3)$ в соответствии с выражением (3-35), а приводим лишь таблицу умножения элементов этого поля в соответствии с выражением (3-36) – табл. 3.16, построенную с помощью пакета Maple V R5.

Таблица 3.16

•	1	α	α+1	α^2	α^2+1	α^2+α	α^2+α+1
1	1	α	α+1	α^2	α^2+1	α^2+α	α^2+α+1
α	α	α^2	α^2+α	α+1	1	α^2+α+1	α^2+1
α+1	α+1	α^2+α	α^2+1	α^2+α+1	α^2	1	α
α^2	α^2	α+1	α^2+α+1	α^2+α	α	α^2+1	1
α^2+1	α^2+1	1	α^2	α	α^2+α+1	α+1	α^2+α
α^2+α	α^2+α	α^2+α+1	1	α^2+1	α+1	α	α^2
α^2+α+1	α^2+α+1	α^2+1	α	1	α^2+α	α^2	α+1

Утомительную процедуру построения таблиц, подобных приведенной табл. 3.16, можно существенно упростить, если использовать свойства $GF(2^3)$ как циклической группы: ненулевые элементы $GF(2^3)$ всегда могут быть представлены как степени некоторого одного элемента этого поля.

Поле $F_0[g_1] = GF(2^m)$, $m = 3$, в рассматриваемом случае образуется как поле классов вычетов – многочленов над $GF(2)$ по модулю X^3+X+1.

Обозначим класс вычетов, содержащий X, как α; в этом случае α является *корнем многочлена* X^3+X+1 и *примитивным* элементом поля $GF(2^3)$.

Таким образом, все *ненулевые элементы поля* оказались представленными последовательностью степеней ненулевого элемента поля α, называемого примитивным элементом: α^i, $i = 0, 1, 2, \ldots, 6$.

В этом случае произведение двух элементов поля, представленных в форме α^i и α^j, может быть выполнено следующим образом:

$$\alpha^i \cdot \alpha^j = \alpha^{R_7(i+j)}, \qquad (3\text{-}37)$$

где $R_7(i+j)$ – остаток от деления $i+j$ на 7.

Табл. 3.17 содержит представление всех ненулевых элементов созданного поля $F_0[g_1]$ и значения полиномов $g_1(X)$ и $g_2(X)$ для каждого ненулевого элемента поля α^i, $i = 0, 1, 2, \ldots, 6$.

Таблица 3.17

Степенное представление	Многочленное представление	Векторное представление	$g_1(\alpha^i)$	$g_2(\alpha^i)$
$\alpha^0 = 1$	1	(0 0 1)	1	1
α	α	(0 1 0)	0	$\alpha^2 + \alpha$
α^2	α^2	(1 0 0)	0	α
α^3	$\alpha + 1$	(0 1 1)	$\alpha^2 + \alpha$	0
α^4	$\alpha^2 + \alpha$	(1 1 0)	0	α^2
α^5	$\alpha^2 + \alpha + 1$	(1 1 1)	α^2	0
α^6	$\alpha^2 + 1$	(1 0 1)	α	0
$\alpha^7 = 1$	1	(0 0 1)	1	1

Из рассмотрения четвёртого столбца табл. 3.17 следует, что в поле $F_0[g_1] = GF(2^m)$, $m = 3$, созданном с помощью неприводимого многочлена $g_1(X)$, корни $g_1(X)$ даются последовательностью степеней примитивного элемента α: α^i, $i = 1, 2, 4$, а из рассмотрения пятого столбца табл. 3.17 следует, что

в поле $F_0[g_1] = GF(2^3)$ корни $g_2(X)$ даются последовательностью степеней примитивного элемента α: α^i, $i = 3, 5, 6$.

Заметим, что

$$g_1(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^4)=X^3+(\alpha+\alpha^2+\alpha^4)X^2+$$

$$+(\alpha^3+\alpha^5+\alpha^6)X+\alpha^7 = X^3+X+1, \qquad (3\text{-}38)$$

так как

$(\alpha+\alpha^2+\alpha^4) \equiv 0$, $(\alpha^3+\alpha^5+\alpha^6) \equiv 1$ и $\alpha^7 \equiv 1 \pmod{(\alpha^3+\alpha+1)}$;

и

$$g_2(X) = (X-\alpha^3)(X-\alpha^5)(X-\alpha^6)=X^3+(\alpha^3+\alpha^5+\alpha^6)X^2+$$

$$+(\alpha^8+\alpha^9+\alpha^{11})X+\alpha^{14} = X^3+X^2+1, \qquad (3\text{-}39)$$

так как

$(\alpha^3+\alpha^5+\alpha^6) \equiv 1$, $(\alpha^8+\alpha^9+\alpha^{11}) \equiv 0$ и $\alpha^{14} \equiv 1 \pmod{(\alpha^3+\alpha+1)}$.

Иначе говоря, мы доказали, что

$$\prod_{i=0}^{6}(X-\alpha^i) = (X-1)(X^3+X+1)(X^3+X^2+1) = X^7-1 \qquad (3\text{-}39a)$$

(см. Приложение 5.2).

Отметим также, что $7 = (2^m-1) = (2^3-1)$.

Пункт b). Решим ту же задачу построения поля $F_0[g_2] = GF(2^3)$ с помощью неприводимого многочлена $g_2(X) = X^3+X^2+1$, используя свойства $GF(2^3)$ как циклической группы.

Рассмотрим классы вычетов многочленов по модулю X^3+X^2+1: $\{0\}$, $\{1\}$, $\{X\}$, $\{X+1\}$, $\{X^2\}$, $\{X^2+1\}$, $\{X^2+X\}$, $\{X^2+X+1\}$.

Поле $F_0[g_2] = GF(2^3)$ в рассматриваемом случае образуется как поле классов вычетов – многочленов над $GF(2)$ по модулю X^3+X^2+1.

Обозначим класс вычетов, содержащий X, как α; в этом случае α является *корнем многочлена* X^3+X^2+1 и *примитивным* элементом этого поля $GF(2^3)$.

Табл. 3.18 содержит представление всех ненулевых элементов созданного поля и значения полиномов $g_1(X)$ и $g_2(X)$ для каждого ненулевого элемента поля α^i, $i = 0, 1, 2, \ldots, 6$.

Таблица 3.18

Степенное представление	Многочленное представление	Векторное представление	$g_1(\alpha^i)$	$g_2(\alpha^i)$
$\alpha^0 = 1$	1	(0 0 1)	1	1
α	α	(0 1 0)	$\alpha^2 + \alpha$	0
α^2	α^2	(1 0 0)	$\alpha + 1$	0
α^3	$\alpha^2 + 1$	(1 0 1)	0	$\alpha + 1$
α^4	$\alpha^2 + \alpha + 1$	(1 1 1)	$\alpha^2 + 1$	0
α^5	$\alpha + 1$	(0 1 1)	0	α^2
α^6	$\alpha^2 + \alpha$	(1 1 0)	0	α
$\alpha^7 = 1$	1	(0 0 1)	1	1

Из рассмотрения четвёртого столбца табл. 3.18 следует, что в поле $F_0[g_2] = GF(2^3)$, созданном с помощью неприводимого многочлена $g_2(X)$, корни $g_1(X)$ даются последовательностью степеней примитивного элемента α: α^i, $i = 3, 5, 6$, а из рассмотрения пятого столбца табл. 3.18 следует, что в поле $F_0[g_2]$ корни $g_2(X)$ даются последовательностью степеней примитивного элемента α: α^i, $i = 1, 2, 4$.

Заметим, что

$$g_1(X) = (X-\alpha^3)(X-\alpha^5)(X-\alpha^6)=X^3+(\alpha^3+\alpha^5+\alpha^6)X^2+$$

$$+(\alpha^8+\alpha^9+\alpha^{11})X+\alpha^{14} = X^3+X+1, \qquad (3\text{-}40)$$

так как

$(\alpha^3+\alpha^5+\alpha^6) \equiv 0$, $(\alpha^8+\alpha^9+\alpha^{11}) \equiv 1$ и $\alpha^{14} \equiv 1 \pmod{(\alpha^3+\alpha^2+1)}$;

и

$$g_2(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^4)=X^3+(\alpha+\alpha^2+\alpha^4)X^2+$$

$$+(\alpha^3+\alpha^5+\alpha^6)X+\alpha^7 = X^3+X^2+1, \qquad (3\text{-}41)$$

так как

$(\alpha+\alpha^2+\alpha^4) \equiv 1$, $(\alpha^3+\alpha^5+\alpha^6) \equiv 0$ и $\alpha^7 \equiv 1 \pmod{(\alpha^3+\alpha^2+1)}$.

Табл. 3.17 и 3.18 построены также с помощью пакета Maple V R5.

END

Отметим, что рассмотренные в пунктах a) и b) примера 3.10 различные конечные поля с одним и тем же числом элементов, созданные с помощью двух различных неприводимых многочленов $g_1(X)$ и $g_2(X)$, *изоморфны*, т.е. они различаются только обозначениями их элементов [3.3, с. 58, 74, 101].

Из рассмотренного примера 3.10 следует, что неприводимый многочлен $g(X)$ степени m однозначно определяется последовательностью степеней примитивного элемента заданного поля $GF(2^m)$, определяющих последовательность всех его m различных корней (см. выражения (3-38), (3-39), (3-40), (3-41)).

Таким образом, многочлен $g_1(X)g_2(X)$ имеет в поле $F_0[g_1] = GF(2^m)$, $m = 3$, шесть корней, определяемых последовательностями степеней примитивного элемента α: $i = 1, 2, 4$ и $i = 3, 5, 6$.

Бином $X^7-1=(X-1)g_1(X)g_2(X)$ имеет в этом же поле семь корней, определяемых последовательностями степеней примитивного элемента α: $i = 0, 1, \ldots, 6$.

В Приложении 5.4 приведена таблица, содержащая разложение бинома X^n+1, $7 \le n \le 147$ (255, 511), на *неприводимые сомножители* над полем $GF(2)$ [3.10].

Для каждого из неприводимых сомножителей бинома $X^n+1 = X^n-1$ указана его степень m и последовательность степеней примитивного элемента поля, определяющая m различных корней неприводимого сомножителя. Сомножитель $X-1$, входящий в разложение бинома X^n-1 при любом n, в этом приложении не приводится.

Неприводимые многочлены – сомножители бинома X^n+1 для краткости даны в восьмеричном представлении (см. табл. 3.19).

Таблица 3.19

Octal	0	1	2	3	4	5	6	7
Binary	000	001	010	011	100	101	110	111

ПРИМЕР 3.11. Табл. 3.20 является фрагментом табл. 5.4 (Приложение 5.4).

В соответствии со сказанным выше, данные этого фрагмента таблицы позволяют определить следующие два неразложимых сомножителя одной и той же степени m=3 (см. табл. 3.19).

Первый сомножитель $g_1(X)$ определяется восьмеричным представлением 13, чему соответствует двоичное представление $001011 \Leftrightarrow X^3+X+1$.

Таблица 3.20

Степень бинома	Последовательности степеней корней неприводимых многочленов	Неприводимые сомножители	m
1	2	3	4
7	1 2 4 3 6 5	13 15	3 3

Кроме того, указана последовательность степеней примитивного элемента поля: 1 2 4; следовательно, согласно (3-38), $g_1(X) = X^3+X+1$; $\alpha^1=\alpha$ (примитивный элемент поля $GF(2^3)$ является корнем многочлена $g_1(X)$ и, следовательно, *расширенным полем является поле* $F_0[g_1] = GF(2^m)$, $m = 3$).

Второй сомножитель $g_2(X)$ определяется восьмеричным представлением 15, чему соответствует двоичное представление $001101 \Leftrightarrow X^3+X^2+1$.

Кроме того указана последовательность степеней примитивного элемента поля: 3 6 5; следовательно, согласно (3-39), $g_2(X) = X^3+X^2+1$; $\alpha^1=\alpha$ (примитивный элемент поля $GF(2^3)$ не является корнем многочлена $g_2(X)$).

Наличие третьего сомножителя $(X\text{-}1)$ бинома $X^7\text{-}1$ подразумевается по умолчанию. Таким образом, окончательно имеем:

$$X^7\text{-}1 = (X\text{-}1)(X^3+X+1)(X^3+X^2+1).$$

END

Пусть $g(X)$ – *неприводимый* многочлен степени m над полем $F_0 = GF(p) = GF(2)$. Это означает, что уравнение $g(X)= = 0$ ***не имеет*** решений в поле F_0. Однако в выше рассмотренных примерах было показано, что уравнение $g(X) = 0$ ***имеет решения*** *в расширенном поле* $F_0[g] = GF(p^m) = GF(2^m)$.

Алгебра многочленов (см. далее подраздел 3.6) *по модулю* $g(X)$ – ***неприводимого*** *многочлена степени* m над полем $F_0 = GF(2)$ *является* ***расширением поля*** F_0 – полем $F_0[g] = =GF(2^m)$.

Обозначим класс вычетов ***по модулю*** $g(X)$ $\{X\}$, содержащий многочлен X, как α. Пусть $g(X) = \sum_{i=0}^{m} g_i X^i$. Тогда

$$g(\alpha) = g_0+g_1\alpha+\ldots+g_m\alpha^m = g_0+g_1\{X\}+\ldots+g_m\{X^m\} =$$

$$= \{g_0+g_1X+\ldots+g_mX^m\} = \{g(X)\} = \{0\}. \qquad (3\text{-}41a)$$

А это и означает, что многочлен $g(X)$ имеет корень α в поле $F_0[g]$.

Каждый элемент β поля $F_0[g]$ может быть представлен двумя способами [3.3, с. 93-94].

1) *Многочленное представление*:

$\beta = a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0, \quad a_{m-i} \in F_0, \quad 1 \le i \le m.$

2) *Векторное представление*. Выбрав в качестве *базиса* $\alpha^{m-1}, \alpha^{m-2}, \ldots, a_0$ – *элементы поля* $F_0[g]$, каждый элемент β поля $F_0[g]$ можно представить в виде последовательности символов из F_0 : $(a_{m-1}, a_{m-2}, \ldots, a_0)$ (см. табл. 3.17 и табл. 3.18).

ТЕОРЕМА 3.6. (*Совокупность многочленов образует идеал тогда и только тогда, когда все входящие в неё многочлены кратны некоторому фиксированному многочлену.*

END

Эта теорема является аналогом теоремы 3.2. Из теоремы 3.6 следует, что кольцо многочленов есть кольцо главных идеалов.

Идеал, состоящий из всех многочленов, кратных многочлену $f(X)$, обозначается как $(f(X))$.

В теории групп с помощью подгрупп – нормальных делителей строятся фактор-группы. В теории колец роль нормальных делителей играют идеалы.

Кольцо классов вычетов, образованных по идеалу $(f(X))$, называется кольцом многочленов по модулю $f(X)$.

ПРИМЕР 3.12. Предположим, что дано множество многочленов (с коэффициентами из некоторого поля) с определёнными над ними операциями сложения и умножения. Подмножество всех многочленов этого множества, кратных многочлену $g(X)$, является идеалом.

END

ТЕОРЕМА 3.7. *Каждый класс вычетов по модулю многочлена* $f(X)$ *степени* n *содержит либо* 0, *либо ненулевой многочлен степени меньшей* n. *Нуль является элементом идеала, а различные ненулевые многочлены степеней, меньших* n, *принадлежат различным классам вычетов.*

END

В следующей теореме используется понятие коммутативной *линейной алгебры* (см. приложение 2.9).

ТЕОРЕМА 3.8. *Классы вычетов многочленов по модулю многочлена $f(X)$ степени n с введёнными над ними операциями образуют коммутативную линейную алгебру размерности n над полем коэффициентов.*

ДОКАЗАТЕЛЬСТВО. Умножение класса вычетов на скаляр $c \in P_0$ определяется соотношением: $c\{r(X)\} = \{cr(X)\}$. Легко проверить, что при этом выполняются все аксиомы *векторного пространства* и *линейной алгебры*. Следовательно, классы вычетов по модулю многочлена степени n действительно образуют линейную коммутативную алгебру над полем коэффициентов.

Если многочлены интерпретировать как векторы, то можно утверждать, что векторное пространство имеет размерность n, так как существует n классов вычетов $\{1\}$, $\{X\}$, $\{X^2\}$, …, $\{X^{n-1}\}$, порождающих всё векторное пространство:

$$\{a_0 + a_1X + \ldots + a_{n-1}X^{n-1}\} =$$

$$= a_0\{1\} + a_1\{X\} + \ldots + a_{n-1}\{X^{n-1}\}. \qquad (3\text{-}42)$$

Эти n классов вычетов линейно независимы, так как левая часть выражения (3-42) может обращается в нуль только в следующих случаях:

если многочлен $\{a_0 + a_1X + \ldots + a_{n-1}X^{n-1}\}$ делится на многочлен $f(X)$ степени n, что невозможно,
или

если все коэффициенты a_i, $i = 0, 1, \ldots, n-1$, этого многочлены равны нулю;

в то время как правая часть выражения (3-42) является ***произвольной*** *линейной комбинацией* классов вычетов $\{1\}$, $\{X\}$, $\{X^2\}$, …, $\{X^{n-1}\}$ [3.2, с. 173].

ЧТД

ТЕОРЕМА 3.9. *Пусть I – идеал в алгебре многочленов по модулю $f(X)$, а $g(X)$ – отличный от нуля многочлен наименьшей степени, такой, что класс вычетов $\{g(X)\}$ принадлежит I. При этом класс вычетов $\{s(X)\}$ принадлежит I тогда и только тогда, когда оба многочлена $s(X)$ и $f(X)$ делятся на $g(X)$.*

END

ТЕОРЕМА 3.10. *Для любого идеала I в алгебре многочленов по модулю $f(X)$ существует единственный нормированный многочлен $g(X)$ минимальной степени, такой, что класс вычетов $\{g(X)\}$ принадлежит идеалу I. И наоборот, каждый нормированный многочлен $g(X)$, являющийся делителем $f(X)$, порождает некоторый идеал I, в котором $g(X)$ является нормированным многочленом минимальной степени.*

END

ТЕОРЕМА 3.11. *Пусть $f(X) = g(X)h(X)$, где $f(X)$ – многочлен степени n, а $h(X)$ – многочлен степени k. Тогда идеал, порожденный классом вычетов $\{g(X)\}$ в алгебре многочленов по модулю $f(X)$, имеет размерность k.*

END

ОПРЕДЕЛЕНИЕ 3. 3. *Нормированный многочлен минимальной степени $g(X)$, такой, что его класс вычетов $\{g(X)\}$ принадлежит идеалу, называется* ***порождающим многочленом этого идеала***.

END

ТЕОРЕМА 3.12. *Пусть в алгебре многочленов по модулю $f(X)$ $g(X)h(X) = f(X)$, где $f(X)$, $g(X)$ и $h(X)$ – нормированные многочлены. Тогда класс вычетов $\{a(X)\}$ принадлежит нулевому пространству идеала, порождённого многочленом $h(X)$, то-*

ода и только тогда, когда он принадлежит идеалу, порождённому многочленом $g(X)$.

ДОКАЗАТЕЛЬСТВО

ДОСТАТОЧНОСТЬ. Предположим, что $\{a(X)\}$ принадлежит идеалу, порождённому многочленом $g(X)$, а $\{b(X)\}$ – любой класс вычетов из идеала, порождённого многочленом $h(X)$.

В этом случае $a(X)$ кратен $g(X)$, $b(X)$ кратен $h(X)$ и, следовательно, произведение $a(X)b(X)$ кратно $f(X)$. Поэтому $\{a(X)\}\{b(X)\} = \{a(X)b(X)\} = 0$. Следовательно, $\{a(X)\}$ принадлежит нулевому пространству идеала, порождённого $h(X)$.

НЕОБХОДИМОСТЬ. Предположим, что $\{a(X)\}$ принадлежит нулевому пространству идеала, порождённого $h(X)$. Требуется доказать, что $\{a(X)\}$ принадлежит идеалу, порождённому $g(X)$.

Согласно предположению $\{a(X)\}\{h(X)\} = 0$ и, следовательно, произведение $a(X)h(X)$ должно быть кратно $f(X)$; это означает, что многочлен $a(X)$ должен быть кратен многочлену $g(X)$ и, следовательно, $\{a(X)\}$ принадлежит идеалу, порождённому $g(X)$.

ЧТД

Эта теорема лежит в основе процедур декодирования циклических кодов.

3.7. ПОЛЯ ГАЛУА

Пусть $g(X)$ – неприводимый многочлен степени m над полем $F_0 = G(p)$, где p – простое число, а $F_0[g] = F = GF(p^m)$ – поле, образованное классами вычетов по модулю неприводимого многочлена $g(X)$. В этом случае исходное поле F_0 называется *основным*, а новое поле $F = GF(p^m)$, элементами которого являются классы вычетов по модулю $g(X)$, – *расширением степени* m основного поля F_0. В необходимых случаях мы будем обозначать новое поле как $GF(q)$, где $q = p^m$.

ТЕОРЕМА 3.13. *Пусть* $g(X)$ *– многочлен с коэффициентами из поля* F_0. *Алгебра многочленов над полем* F_0 *по модулю* $g(X)$ *является* ***полем*** *тогда и только тогда, когда многочлен* $g(X)$ ***неприводим*** *над полем* F_0, *т.е. если* $g(X)$ *нельзя представить в виде произведения многочленов с коэффициентами из* F_0.

END

Доказательство аналогично доказательству теоремы 3.4.

Как уже говорилось, если класс вычетов $\{X\}$ обозначен как α и если $g(\alpha) = 0$, то α – корень многочлена $g(X)$.

Доказано, что кольцо многочленов над $GF(2)$ содержит, по крайней мере, один *неприводимый многочлен любой степени* $k \geq 1$ [3.4, с. 80, 93].

ТЕОРЕМА 3.14. *В поле характеристики* p *имеет место равенство* $(a + b)^p = a^p + b^p$.

END

Рассмотрим теперь основное поле F_0 и некоторое его расширение. Пусть β – *любой* элемент расширения.

ОПРЕДЕЛЕНИЕ 3.4. *Нормированный многочлен наименьшей степени* $m(X)$ *над основным полем* F_0, *такой, что* $m(\beta) = 0$, *называется* ***минимальным многочленом*** *или* ***минимальной функцией для*** β.

END

ТЕОРЕМА 3.15. *Минимальная функция* $m(X)$ *для любого элемента* β *является* ***неприводимым многочленом***.

ДОКАЗАТЕЛЬСТВО. Предположим противное: $m(X) = m_1(X)m_2(X)$, где $m_1(X)$ и $m_2(X)$ – многочлены степени выше нулевой. Тогда $m_1(\beta)m_2(\beta) = m(\beta) = 0$ и, следовательно, по крайней мере, один из сомножителей $m_1(\beta)$ или $m_2(\beta)$ должен быть равен нулю. Но это противоречит предположению о том, что $m(X)$ – минимальный многочлен.

ЧТД

ТЕОРЕМА 3.16. *Если $f(X)$ – многочлен над полем F_0 и если $f(\beta)=0$, то многочлен $f(X)$ делится на $m(X)$ –* ***минимальный многочлен для*** β.

END

Из этой теоремы вытекает:

1) минимальная функция для β *единственна*;

2) если $g(X)$ – нормированный неприводимый многочлен и $g(\beta) = 0$, то $g(X) = m(X)$, где $m(X)$ – минимальный многочлен для β.

ТЕОРЕМА 3.17. *Для каждого элемента из расширения степени m основного поля F_0 существует минимальная функция для этого элемента степени m или меньше.*

END

ТЕОРЕМА 3.18. *Совокупность корней многочлена X^{q-1} - 1 является совокупностью всех q - 1 ненулевых элементов расширения $GF(q) = GF(p^m)$.*

END

ТЕОРЕМА 3.19. *Многочлен X^n - 1 делится на многочлен X^m-1 тогда и только тогда, когда n делится на m.*

END

Из теоремы 3.19, в частности, следует, что X^n-1 всегда делится на X-1.

ОПРЕДЕЛЕНИЕ. 3.5. *Пусть $g(X)\in F_0[X]$ и n –* ***минимальное целое число****, такое, что $g(X)|(X^n-1)$; в этом случае n называется* ***показателем многочлена*** $g(X)$ [3.3, с. 97].

END

УТВЕРЖДЕНИЕ 3.1. *Пусть $F_0 = GF(p)$, $g(X)$ – нормированный неприводимый многочлен* ***степени*** *m, $g(X) \in F_0[X]$, и n –* ***показатель*** *$g(X)$. Тогда m –* ***минимальное целое число****, такое, что $n|(p^m - 1)$. В частности, если $n = p^m - 1$, то $g(X)$ называется* ***примитивным многочленом*** [3.2, с. 185; 3.3, с. 98].

END

ТЕОРЕМА 3.20. *В поле $GF(q) = GF(p^m)$ существует* ***примитивный элемент*** α, *т.е. элемент порядка q-1. Каждый ненулевой элемент поля $GF(q)$ может быть представлен как некоторая степень α, т.е. мультипликативная группа поля Галуа $GF(q)$ является* ***циклической****.*

END

ЛЕММА 3.1. *Все конечные группы, порядок которых есть простое число, являются циклическими.*

ДОКАЗАТЕЛЬСТВО. Пусть G – конечная мультипликативная группа порядка m (m – простое число). Рассмотрим в G совокупность элементов, образованную некоторым элементом $\alpha \neq 1$ и всеми его степенями: $\alpha\alpha = \alpha^2$, $\alpha\alpha^2 = \alpha^3$ и т.д. Число таких элементов не превышает m и, следовательно, конечно; поэтому где-то должно начаться повторение, т.е. $\alpha^i = \alpha^j$ для некоторых i и j. Следовательно, некоторая степень элемента α равна 1. Пусть s – наименьшее целое положительное число, такое, что $\alpha^s = 1$; *число s называется* ***порядком элемента*** α. Элементы 1, α, α^2, …, α^{s-1} образуют подгруппу группы G, так как произведение любых двух элементов из этой совокупности есть элемент этой совокупности, а элементом обратным α^l является α^{s-l}.

Порядок подгруппы s должен быть делителем простого числа m. Следовательно, $s = m$ и группа G является циклической.

ЧТД

ЛЕММА 3.2. *Пусть s – порядок циклической группы, порождённой элементом α. Тогда порядок элемента α^i равен* $\frac{s}{<<s,\ i>>}$, *где $<<s, i>>$ – НОД чисел s и i.*

ДОКАЗАТЕЛЬСТВО. Пусть l – порядок элемента α^i. По определению порядка элемента l является минимальным целым числом, таким, что $(\alpha^i)^l = \alpha^{il} = 1$. Отсюда и из того, что порядок элемента α равен порядку циклической группы s, следует,

что l – минимальное целое число, такое, что $s|il$. Это означает, что $l = \frac{s}{<< s, i >>}$ [3.3, с. 66].

ЧТД

ТЕОРЕМА 3.21. *Если $f(X)$ – многочлен с коэффициентами из основного поля $GF(p)$ и β – корень $f(X)$ в расширении этого поля $GF(p)$, то β^p также является корнем $f(X)$.*

END

ТЕОРЕМА 3.22. *Каждый многочлен $g(X)$ степени m, неприводимый над основным полем $GF(p)$, является делителем многочлена $X^{p^m} - X$.*

END

ТЕОРЕМА 3.22а. *Любой элемент конечного поля порядка p^m является корнем многочлена $X^{p^m} - X$* [3.3, с. 96].

END

В связи с теоремами 3.22 и 3.22а см. также теорему 3.18.

ТЕОРЕМА 3.22б. *Для любого простого числа p и любого целого положительного m* ***существует*** *конечное поле порядка p^m* [3.3, с. 100].

END

ТЕОРЕМА 3.23. *Пусть $g(X)$ – многочлен степени m с коэффициентами из поля $GF(p)$, который неприводим в этом поле, и пусть β – корень многочлена $g(X)$ в расширении поля. Тогда $\beta, \beta^p, \ldots, \beta^{p^{m-1}}$ образуют совокупность всех корней многочлена $g(X)$.*

END

ТЕОРЕМА 3.24. *Пусть $GF(p^m)$ – поле, являющееся расширением поля $GF(p)$ и пусть $\beta \in GF(p^m) - \{0\}$. Тогда* ***показатель*** *минимального многочлена $m_\beta(X)$ для элемента β равен* ***порядку*** *ν элемента β. Степень r многочлена $m_\beta(X)$ является минимальным целым положительным числом, таким, что $\nu | (p^r - 1)$; при этом $r|m$. Корнями уравнения $m_\beta(X) = 0$ являются следующие r различных элементов: $\beta, \beta^p, \ldots, \beta^{p^{r-1}}$* [3.3, с. 101].

END

Согласно теореме 3.24, если $g(X)$ – неприводимый многочлен степени m из $F_0[X]$, то он не имеет корней в F_0, однако $g(X)$ имеет m корней в расширенном поле $F_0[g] = GF(p^m)$ [3.3, с. 101 – 102].

3.8. ЦИКЛИЧЕСКИЕ КОДЫ

В этом подразделе и далее рассматриваются *двоичные* циклические коды, т.е. коды, которым соответствуют многочлены от неопределённой переменной X с коэффициентами из $GF(2)$.

ОПРЕДЕЛЕНИЕ 3.6. *Подпространство векторов $\{\mathbf{v}\}$ длины n V называется* ***циклическим подпространством*** *или* ***циклическим кодом****, если для любого вектора $\mathbf{v} = (a_{n-1}, a_{n-2}, \ldots, a_0) \in V$ вектор $\mathbf{v}' = (a_0, a_{n-1}, a_{n-2}, \ldots, a_1)$, получаемый в результате циклического сдвига компонент вектора $\mathbf{v}$ на единицу вправо, также принадлежит V.*

END

Далее мы будем рассматривать вектор $\mathbf{v}$ или соответствующую ему кодовую комбинацию длины n $(a_{n-1}, a_{n-2}, \ldots, a_0)$ как элементы алгебры многочленов по модулю $X^n - 1$, которую обозначим как A_n.

Каждой комбинации $(a_{n-1}, a_{n-2}, \ldots, a_0)$ длины n соответствует многочлен $a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_0$ степени меньшей n с коэффициентами из $GF(2)$, которому в A_n соответствует класс вычетов $\{a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_0\}$.

Элементами алгебры многочленов A_n по модулю $X^n - 1$ являются классы вычетов многочленов, которые обозначаются как $\{r(X)\}$, $r(X) \in F_0^{(n-1)}[X]$, при этом ненулевой много-

член $r(X)$ является многочленом *наименьшей степени* в классе вычетов.

Таким образом, классу вычетов соответствует определённый вектор, о котором мы можем одновременно говорить как о многочлене от X с коэффициентами из $GF(2)$.

Следующая теорема описывает свойства циклического кода как идеала и как циклического подпространства в алгебре многочленов A_n.

ТЕОРЕМА 3.25. *В алгебре многочленов по модулю X^n-1 подпространство является циклическим подпространством в том и только в том случае, если оно является идеалом.*

ДОКАЗАТЕЛЬСТВО

ДОСТАТОЧНОСТЬ. Пусть вектор $\boldsymbol{v}$ принадлежит подпространству V, которое является идеалом. Покажем, что V – циклическое подпространство.

Умножение на X эквивалентно циклическому сдвигу компонент вектора:

$$X(a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_0) =$$

$$= a_{n-1}(X^n - 1) + a_{n-2}X^{n-1} + \ldots + a_0X + a_{n-1} =$$

$$= a_{n-2}X^{n-1} + \ldots + a_0X + a_{n-1}, \qquad (3\text{-}43)$$

и, следовательно,

$$\{X\}\{a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_0\} =$$

$$= \{a_{n-2}X^{n-1} + \ldots + a_0X + a_{n-1}\}. \qquad (3\text{-}44)$$

Так как по условию V – идеал и $\boldsymbol{v}$ принадлежит V, то $\{X\}\boldsymbol{v}$ также (по определению идеала) принадлежит V. А так как $\{X\}\boldsymbol{v}$ – новый вектор, полученный в результате циклического сдвига координат $\boldsymbol{v}$, то V – циклическое подпространство (по определению циклического подпространства).

НЕОБХОДИМОСТЬ. Предположим, что вектор $\boldsymbol{v}$ принадлежит циклическому подпространству V. Покажем, что V – идеал.

В этом случае для любого вектора $\boldsymbol{v}$ из V произведение $\{X\}\boldsymbol{v}$ принадлежит V, а следовательно, при любом j произведение $\{X\}^j\boldsymbol{v} = \{X^j\}\boldsymbol{v}$ также принадлежит V. Так как V – подпространство, то любая линейная комбинация

$$c_{n-1}\{X^{n-1}\}\boldsymbol{v} + c_{n-2}\{X^{n-2}\}\boldsymbol{v} + \ldots + c_0\boldsymbol{v} =$$
$$= \{c_{n-1}X^{n-1} + c_{n-2}X^{n-2} + \ldots + c_0\}\boldsymbol{v}$$

принадлежит V.

Таким образом, мы имеем: произведение любого вектора $\boldsymbol{v}$ – элемента V на $\{c_{n-1}X^{n-1} + c_{n-2}X^{n-2} + \ldots + c_0X\}$ – произвольный элемент алгебры A_n принадлежит V; и, следовательно, V – идеал.

ЧТД

Следует понять, чем обусловлено *направление* (вправо или влево) циклического сдвига при умножении многочлена $(a_{n-1}X^{n-1}+a_{n-2}X^{n-2} + \ldots + a_0)$ на X в (3-43).

Из приведенных выше сведений о структуре алгебры A_n по модулю многочлена X^n - 1 вытекает следующее.

Если $g(X)$ – нормированный многочлен наименьшей степени, определяющий класс вычетов $\{g(X)\}$, принадлежащий идеалу I алгебры многочленов A_n, и $f(X)$ – многочлен степени меньшей, чем n, который делится на $g(X)$, то класс вычетов $\{f(X)\}$ также принадлежит идеалу I, и наоборот;

если $\{f(X)\}$ принадлежит идеалу I, то многочлен $f(X)$ делится на $g(X)$;

многочлен $g(X)$ – *многочлен, порождающий идеал I*;

кроме того, бином X^n-1 делится на $g(X)$, и любой нормированный многочлен, на который делится бином X^n-1, порождает свой идеал в алгебре A_n.

Таким образом, многочлен $g(X)$, на который делится бином X^n-1, полностью определяет циклический код C_g. Этот