2.7. Биркгоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976.
2.8. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров : Пер. с англ. М.: Наука, 1968.
2.9. Курош А.Г. Курс высшей алгебры. М.: Физматгиз, 1963.
2.10. Кемени Дж., Снелл Дж., Томпсон Дж. Введение в конечную математику. М.: ИИЛ, 1963.
2.11. Теория кодирования : Пер. с англ. Сборник работ в области математической теории кодирования. М.: Мир, 1964.
2.12. Теория информации и её приложения : Пер. с англ. Сборник переводов под ред. А.А. Харкевича. М.: ГИФМЛ, 1959.
2.13. Панин В.В. Основы теории информации. Ч.1. М.: МИФИ, 2001.
2.14. Говорухин В.Н., Цибулин В.Г. Введение в Maple. Математический пакет для всех. М.: Мир, 1997.
2.15. Дьяконов В.П. Математическая система MAPLE V R3/R4/R5. М.: «СОЛОН», 1998.
2.16. Херхагер М., Партолль Х. Mathcad 2000. Полное руководство. : Перевод с немец. под ред. К.Ю. Королькова. Киев: «Ирина», BHV, 2000.
2.17. Кондрашов В.Е., Королёв С.Б. MATLAB как система программирования научно технических расчётов. М.: Мир, 2002.
2.18. Дьяконов В.П., Абраменкова И.В. МАТЛАБ 5.0/5.3. Система символьной математики. М.: «Нолидж», 1999.
2.19. Яглом А.М., Яглом И.М. Вероятность и информация. М.: Наука, 1973.
2.20. Аршинов М.Н., Садовский Л.Е. Коды и математика. Серия: библиотечка «Квант». М.: Наука, 1983.

III. ЦИКЛИЧЕСКИЕ КОДЫ

Циклические коды являются подклассом класса групповых (n, k)-кодов с проверкой на чётность [3.1, 3.8].

Циклические коды обладают следующими преимуществами по сравнению с групповыми (n, k)-кодами с проверкой на чётность, не являющимися циклическими:

описание циклического кода в принципе может быть проще;

реально используемые циклические коды позволяют исправлять многократные ошибки;

математическая структура циклических кодов допускает использование более простых алгоритмов декодирования;

реализация операции кодирования циклических кодов проще.

Первым изучил циклические коды Прейндж (Prange E., 1957).

Мы приведём в качестве обоснования важности изучения циклических кодов, естественно с необходимостью учёта временного фактора, лишь нескольких цитат из отдельных литературных источников.

«Коды Боуза (Bose R. C.), Чоудхури (Ray-Chaudhuri D. K.) и Хоквингема (Hocquenghem A.) – БЧХ-коды, открытые Хоквингемом (1959) и независимо от него Боузе и Чоудхури (1960), представляют собой класс циклических кодов, которые обладают весьма мощной способностью исправлять ошибки и одновременно допускают простые алгоритмы декодирования. Наиболее простым примером БЧХ-кодов являются *двоичные* коды, но совершенно аналогично можно в качестве алфавита выбирать элементы произвольного поля Галуа $GF(p)$, где p – простое число. Порождающий многочлен для этих кодов определяется в терминах некоторого расширения $GF(p^m)$ поля $GF(p)$.» [3.1, с. 256].

«Эффективность БЧХ-кодов с обнаружением ошибок можно продемонстрировать на следующем примере. В европейских системах передачи данных широко используется двоичный (255, 231)-код. Он построен над $GF(2)$ с помощью примитивного элемента α из $GF(2^8)$ мультипликативного порядка $(2^8 - 1) = 255$. Степень кодирующего многочлена равна 24. Его корнями являются также α, α^2, α^3, α^4, α^5, и α^6, что обеспечивает минимальное расстояние 7 и обнаружение до шести ошибок. Разумеется, будут обнаружены многие другие комбинации ошибок. Поскольку в общем числе слов длины 255 доля кодовых слов составляет $2^{-24} \approx 1/(16\times10^6)$, то при вводе случайных слов лишь примерно одно из шестнадцати миллионов оказалось бы кодовым. В течение многих лет эксплуатации европейских систем связи не было случая, чтобы ошибка передачи прошла незамеченной при декодировании.» [3.8, с. 343].

В основе теории циклических кодов лежит *теория Галуа* (Galois, 26.10.1811 – 30.05.1832, французский математик и революционер), устанавливающая описание расширений полей в терминах *групп* [3.7].

3.1. КОЛЬЦО КЛАССОВ ВЫЧЕТОВ Z_m И ЕГО СВОЙСТВА

Пусть целое число $m \geq 1$. Рассмотрим кольцо классов вычетов Z_m (см. приложение 3.18).

Так как операции сложения и умножения над классами вычетов определены через соответствующие операции над целыми числами – элементами этих классов, то, очевидно, что для операции сложения и операции умножения над классами вычетов выполняются законы замкнутости, ассоциативности и коммутативности, а для операций сложения и умножения выполняется закон дистрибутивности.

Роль нулевого элемента при сложении выполняет класс $\bar{0}$, а роль единичного элемента при умножении – класс $\bar{1}$. Обратным элементом для класса вычетов $\bar{r} \neq \bar{0}$ при сложении в Z_m является класс вычетов $\overline{m - r}$; действительно, согласно определению операции сложения классов вычетов

$$\bar{r} + \overline{m - r} = \bar{0}. \qquad (3\text{-}1)$$

Таким образом, множество m элементов Z_m относительно операции сложения является аддитивной абелевой группой порядка m, называемой *аддитивной группой кольца*.

Рассмотрим теперь *свойства множества* m элементов Z_m относительно операции умножения и ответим на вопрос, могут ли быть свойства этого множества такими, чтобы Z_m являлось *полем*?

Коммутативное кольцо Z_m является полем, если оно имеет единицу по умножению и каждый его ненулевой элемент имеет обратный элемент по умножению.

Очевидно, что в любом кольце нуль по сложению $\bar{0}$ не имеет обратного элемента по умножению $\bar{r}$:

$$\bar{0} \cdot \bar{r} = \bar{0} \neq \bar{1} \qquad (3\text{-}2)$$

при любом возможном $\bar{r}$.

Можно показать, что имеет место также отсутствие обратных элементов по умножению у ненулевых элементов, произведение которых равно нулю и которые называются *делителями нуля*. Действительно, допустив противное, придём к противоречию: $\bar{0}$ имеет обратный элемент по умножению (см. также теорему 3.4). Поэтому, если в Z_m имеются ненулевые делители нуля $\bar{0}$, то Z_m полем не является. Это положение иллюстрируют табл. 3.4, 3.6, 3.8, 3.9 и 3.10.

ПРИМЕР 3.1. Рассмотрим в качестве примера содержимое табл. 3.1 – 3.10. В ячейках таблиц приведены через запятую

результаты выполнения операции сложения и операции умножения над парами элементов колец классов вычетов по модулю m Z_m для $m = 1, 2, \ldots, 10$. В этих таблицах ради упрощения их создания применён широко используемый в теории кодирования приём: там, где это не приводит к путанице, в обозначении класса вычетов $\bar{r}$ опущена чёрточка и класс вычетов изображается, следовательно, как натуральное число r.

Кольцо Z_1 состоит лишь из одного нулевого элемента $\bar{0}$ и, следовательно, полем не является.

Кольца Z_m, приведенные в табл. 3.2, 3.3, 3.5 и 3.7, являются *конечными полями*, называемыми (простыми) полями Галуа (Galois Fields – поля Галуа; [3.7]) и обозначаемыми как $GF(m)$; m – число элементов поля. В этих примерах *колец* классов вычетов Z_m, являющихся одновременно *полями* классов вычетов, значения m есть ***простые числа***: 2, 3, 5, 7.

Z_1 (Кольцо, но не поле) Таблица 3.1

+, ·	0
0	0, 0

Z_2 ($GF(2)$) Таблица 3.2

+, ·	0	1
0	0, 0	1, 0
1	1, 0	0, 1

Z_3 ($GF(3)$) Таблица 3.3

+, ·	0	1	2
0	0, 0	1, 0	2, 0
1	1, 0	2, 1	0, 2
2	2, 0	0, 2	1, 1

Z_4 (Кольцо, но не поле) Таблица 3.4

+, ·	0	1	2	3
0	0, 0	1, 0	2, 0	3, 0
1	1, 0	2, 1	3, 2	0, 3
2	2, 0	3, 2	0, 0	1, 2
3	3, 0	0, 3	1, 2	2, 1

Делитель $\bar{0}$: $\bar{2}$.

Z_5 ($GF(5)$) Таблица 3.5

+, ·	0	1	2	3	4
0	0, 0	1, 0	2, 0	3, 0	4, 0
1	1, 0	2, 1	3, 2	4, 3	0, 4
2	2, 0	3, 2	4, 4	0, 1	1, 3
3	3, 0	4, 3	0, 1	1, 4	2, 2
4	4, 0	0, 4	1, 3	2, 2	3, 1

Z_6 (Кольцо, но не поле) Таблица 3.6

+, ·	0	1	2	3	4	5
0	0, 0	1, 0	2, 0	3, 0	4, 0	5, 0
1	1, 0	2, 1	3, 2	4, 3	5, 4	0, 5
2	2, 0	3, 2	4, 4	5, 0	0, 2	1, 4
3	3, 0	4, 3	5, 0	0, 3	1, 0	2, 3
4	4, 0	5, 4	0, 2	1, 0	2, 4	3, 2
5	5, 0	0, 5	1, 4	2, 3	3, 2	4, 1

Делители $\bar{0}$: $\bar{2}$, $\bar{3}$ и $\bar{4}$.

Z_7 ($GF(7)$) Таблица 3.7

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

Z_8 (Кольцо, но не поле) Таблица 3.8

+, ·	0	1	2	3	4	5	6	7
0	0, 0	1, 0	2, 0	3, 0	4, 0	5, 0	6, 0	7, 0
1	1, 0	2, 1	3, 2	4, 3	5, 4	6, 5	7, 6	0, 7
2	2, 0	3, 2	4, 4	5, 6	6, 0	7, 2	0, 4	1, 6
3	3, 0	4, 3	5, 6	6, 1	7, 4	0, 7	1, 2	2, 5
4	4, 0	5, 4	6, 0	7, 4	0, 0	1, 4	2, 0	3, 4
5	5, 0	6, 5	7, 2	0, 7	1, 4	2, 1	3, 6	4, 3
6	6, 0	7, 6	0, 4	1, 2	2, 0	3, 6	4, 4	5, 2
7	7, 0	0, 7	1, 6	2, 5	3, 4	4, 3	5, 2	6, 1

Делители $\bar{0}$: $\bar{2}$, $\bar{4}$ и $\bar{6}$.

Z_9 (Кольцо, но не поле) Таблица 3.9

+, ·	0	1	2	3	4	5	6	7	8
0	0, 0	1, 0	2, 0	3, 0	4, 0	5, 0	6, 0	7, 0	8, 0
1	1, 0	2, 1	3, 2	4, 3	5, 4	6, 5	7, 6	8, 7	0, 8
2	2, 0	3, 2	4, 4	5, 6	6, 8	7, 1	8, 3	0, 5	1, 7
3	3, 0	4, 3	5, 6	6, 0	7, 3	8, 6	0, 0	1, 3	2, 6
4	4, 0	5, 4	6, 8	7, 3	8, 7	0, 2	1, 6	2, 1	3, 5
5	5, 0	6, 5	7, 1	8, 6	0, 2	1, 7	2, 3	3, 8	4, 4
6	6, 0	7, 6	8, 3	0, 0	1, 6	2, 3	3, 0	4, 6	5, 3
7	7, 0	8, 7	0, 5	1, 3	2, 1	3, 8	4, 6	5, 4	6, 2
8	8, 0	0, 8	1, 7	2, 6	3, 5	4, 4	5, 3	6, 2	7, 1

Делители $\bar{0}$: $\bar{3}$, $\bar{6}$.

Z_{10} (Кольцо, но не поле) Таблица 3.10

+, ·	0	1	2	3	4	5	6	7	8	9
0	0, 0	1, 0	2, 0	3, 0	4, 0	5, 0	6, 0	7, 0	8, 0	9, 0
1	1, 0	2, 1	3, 2	4, 3	5, 4	6, 5	7, 6	8, 7	9, 8	0, 9
2	2, 0	3, 2	4, 4	5, 6	6, 8	7, 0	8, 2	9, 4	0, 6	1, 8
3	3, 0	4, 3	5, 6	6, 9	7, 2	8, 5	9, 8	0, 1	1, 4	2, 7
4	4, 0	5, 4	6, 8	7, 2	8, 6	9, 0	0, 4	1, 8	2, 2	3, 6
5	5, 0	6, 5	7, 0	8, 5	9, 0	0, 5	1, 0	2, 5	3, 0	4, 5
6	6, 0	7, 6	8, 2	9, 8	0, 4	1, 0	2, 6	3, 2	4, 8	5, 4
7	7, 0	8, 7	9, 4	0, 1	1, 8	2, 5	3, 2	4, 9	5, 6	6, 3
8	8, 0	9, 8	0, 6	1, 4	2, 2	3, 0	4, 8	5, 6	6, 4	7, 2
9	9, 0	0, 9	1, 8	2, 7	3, 6	4, 5	5, 4	6, 3	7, 2	8, 1

Делители $\bar{0}$: $\bar{2}$, $\bar{4}$, $\bar{5}$, $\bar{6}$, и $\bar{8}$.

END

Если Z_m является полем, то *множество его ненулевых элементов* относительно умножения согласно определению поля образует коммутативную группу – *мультипликативную группу поля*.

Очевидно, что мультипликативная группа поля Галуа $GF(m)$ является циклической группой порядка m - 1.

3.2. ИДЕАЛ И НЕКОТОРЫЕ ЕГО СВОЙСТВА

В теории групп важную роль играет понятие коммутативной подгруппы, являющейся *нормальным делителем*. Подобную же роль играет понятие *двустороннего идеала* в теории колец.

ОПРЕДЕЛЕНИЕ 3.1. *Подмножество элементов кольца R называется (двусторонним) идеалом I, если оно обладает следующими двумя свойствами:*

1) *I само является кольцом относительно операций в R,*

2) *для любого элемента $a \in I$ и любого элемента $b \in R$ произведения ab и ba принадлежат I.*

END

Например, в кольце целых чисел множество всех целых чисел, кратных некоторому фиксированному целому числу, является идеалом.

Из приведенного определения идеала следует, что идеал I является *подгруппой* аддитивной группы кольца R. Поэтому аддитивная группа кольца может быть разложена по этой подгруппе и могут быть образованы *смежные классы*, называемые в рассматриваемом случае *классами вычетов*. Естественно, что все рассмотренные выше свойства смежных классов разложения группы по подгруппе имеют место и для классов вычетов.

Так как групповая операция сложения является коммутативной, то идеал является нормальным делителем и может быть определена операция сложения классов вычетов. Может быть определена также операция умножения классов вычетов. Так как определённые операции над классами вычетов (как и в случае разложения группы на смежные классы по подгруппе) введены на основе использования операций сложения и умножения элементов группы, то справедливы ассоциативный и дистрибутивный законы. Таким образом, имеет место следующая теорема.

ТЕОРЕМА 3.1. *Классы вычетов по идеалу I в некотором кольце R образуют* ***кольцо классов вычетов***.

END

ПРИМЕР 3.2. Разобьём бесконечное множество элементов кольца целых чисел {x} на два класса: класс чётных чисел {0} и класс нечётных чисел {1}:

$$x\begin{cases} \in \{0\} \mid x \equiv 0 \pmod 2, \\ \in \{1\} \mid x \equiv 1 \pmod 2. \end{cases}$$

В этом случае имеются два класса вычетов по модулю 2: {0} и {1}, которые образуют *кольцо классов вычетов* относительно операций их сложения и умножения.

Очевидно, что кольцо классов вычетов по модулю два имеет конечный порядок, равный 2, и содержит элементы {0} и {1}.

Таблица 3.11

+, ·	{0}	{1}
{0}	{0}, {0}	{1}, {0}
{1}	{1}, {0}	{0}, {1}

Из табл. 3.11 следует, что класс вычетов {0} является идеалом в кольце классов вычетов по модулю два и, следовательно, в кольце целых чисел подмножество чётных чисел образует идеал.

END

3.3. ИДЕАЛЫ И КЛАССЫ ВЫЧЕТОВ ЦЕЛЫХ ЧИСЕЛ

С помощью алгоритма деления Евклида (приложение 3.18) можно доказать, что НОД d двух целых чисел r и s всегда может быть представлен в виде:

$$d = ar + bs, \qquad (3\text{-}3)$$

где a и b – целые числа [3.2, с. 168].

ПРИМЕР 3.3. При определении с помощью алгоритма Евклида НОД и НОК чисел n =13172 и m =257 в примере 3.29 выполнялись следующие вычисления:

$$13172 = 51 \cdot 257 \cdot + 65,$$

$$257 \cdot = 3 \cdot 65 + 62,$$

$$65 = 1\cdot62 + 3,$$

$$62 = 20\cdot3 + 2,$$

$$3 = 1\cdot2 + 1,$$

$$2 = 2\cdot1 + 0;$$

Производя последовательность вычислений в обратном порядке, найдём:

$$d = 1 = 3 - 1\cdot2 = 3 - 1\cdot(62 - 20\cdot3) = -62 + 21\,3 =$$

$$= -62 + 21\cdot(65 - 1\cdot62) = -62 + 21\cdot(65 - 62) =$$

$$= 21\cdot65 - 22\,62 = 21\cdot65 - 22\cdot(257 - 3\cdot65) =$$

$$= 87\cdot65 - 22\cdot257 = 87\cdot(13172 - 51\cdot257) - 22\cdot257 =$$

$$= 87\cdot13172 - (87\cdot51 + 22)\cdot257 = 87\cdot13172 - 4459\cdot257 = 1.$$

Таким образом, мы получили:

$$d = an + bm,$$

где $a = 87$ и $b = -4459$.

END

Докажем следующую теорему.

ТЕОРЕМА 3.2. *Совокупность целых чисел образует идеал тогда и только тогда, когда она состоит из всех чисел,* ***кратных некоторому целому числу***.

ДОКАЗАТЕЛЬСТВО

НЕОБХОДИМОСТЬ. Предположим, что совокупность целых чисел, о которой идёт речь в теореме, является идеалом.

Покажем, что в этом случае эта совокупность состоит из всех чисел, кратных некоторому целому числу.

Пусть r – наименьшее целое положительное число, принадлежащее идеалу, а s – любое другое целое число, также принадлежащее идеалу. Тогда НОД d этих чисел согласно (3-3) также принадлежит идеалу. Так как r – наименьшее целое положительное число в идеале, то $r \le d$. Поскольку r делится на d, то $d \le r$. Поэтому $r = d$ и s делится на r; т.е. на r делится *любое целое число* s, принадлежащее идеалу.

ДОСТАТОЧНОСТЬ. Пусть любое целое число s, принадлежащее совокупности целых чисел, о которой идёт речь в теореме, кратно r. Требуется доказать, что в этом случае эта совокупность целых чисел является идеалом.

При оговоренных условиях любое число, кратное r, по определению (см. определение 3.1) принадлежит идеалу и, следовательно, вся эта совокупность целых чисел – подмножество некоторого кольца целых чисел – является идеалом.

ЧТД

! В качестве иллюстрации теоремы 3.2 и некоторых последующих теорем и утверждений приведём рассмотрение некоторых свойств идеала I_m кольца Z – множества целых чисел, являющегося коммутативным кольцом с единицей.

Пусть I_m – некоторый идеал кольца Z, $I_m \subset Z$ и пусть $m = 5$ – *минимальное целое положительное число* из I_5.

Любой элемент $s \in I_5$ должен согласно теореме 3.2 иметь вид:

$$s = 5q,$$

где q – произвольное число из Z. Таким образом, в рассматриваемом случае в I_5 входят только целые числа: 0, ±5, ±10, ±15, ±20, …; при этом идеалу I_5 принадлежит 0 и не принадлежит 1. I_5 является аддитивной абелевой группой бесконеч-

ного порядка и, следовательно, является подгруппой аддитивной абелевой группы кольца Z.

⌟

Идеал, состоящий из всех элементов, кратных одному из элементов кольца, называется *главным идеалом*. Кольцо, в котором каждый идеал является главным, называется *кольцом главных идеалов*.

Например, кольцо всех целых чисел, согласно теореме 3.2, является кольцом главных идеалов.

Идеал, состоящий из всех целых чисел, кратных положительному целому числу m, обозначается через (m). Кольцо классов вычетов, образованное классами вычетов по идеалу (m), называется *кольцом целых чисел по модулю m* [3.2, с. 168–170; 3.3, с. 70-72].

! I_5 состоит из всех целых чисел, кратных 5 – элементу кольца Z, и, следовательно, является главным идеалом. Согласно сказанному в предыдущем абзаце I_5 = (5). Кольцо *классов вычетов*, образованное по идеалу (5), называется кольцом целых чисел по модулю 5.

⌟

ТЕОРЕМА 3.3. *Каждый класс вычетов по модулю m содержит либо* 0, *либо целое положительное число, меньшее m. Нуль является элементом идеала* {0}, *а все остальные целые положительные числа, меньшие m, принадлежат различным классам вычетов, отличным от* {0}.

ДОКАЗАТЕЛЬСТВО.

Предположим, что произвольное целое число s принадлежит некоторому классу вычетов; представим этот элемент в виде

$$s = mq + r, \qquad (3\text{-}4)$$

где r принадлежит *тому же самому классу вычетов*, $0 \le r < m$; q – целое число. Так как s и r принадлежат одному и тому же классу вычетов, то

$$r - s \equiv 0 \pmod{m}. \qquad (3\text{-}5)$$

Так как r может принимать значения из множества $\{0, 1, \ldots, m - 1\}$, то каждое значение r из этого множества значений определяет один из классов вычетов, которому принадлежит это r; причём нуль является элементом идеала (как элемент подгруппы аддитивной группы).

ЧТД

В теореме 3.3 речь шла о классах вычетов $\{0\}, \{1\}, \ldots, \{m - 1\}$; там, где это не вызывает недоразумений, мы будем обозначать классы вычетов так же, как: $0, 1, \ldots, m - 1$; т.е. будем обозначать их как числа.

! Кольцо классов вычетов по модулю 5 имеет классы вычетов {0}, {1}, {2}, {3}, {4}, или короче, – классы вычетов 0, 1, 2, 3, 4.

⌟

ТЕОРЕМА 3.4. *Кольцо классов вычетов по модулю m является* ***полем*** *тогда и только тогда, когда m –* ***простое число***.

ДОКАЗАТЕЛЬСТВО

НЕОБХОДИМОСТЬ. Пусть кольцо классов вычетов по модулю m является полем. Покажем, что в этом случае m – простое число.

Предположим противное: пусть $m = rs$, где r и s – некоторые целые числа, не кратные m. Поэтому будет иметь место соотношение

$$\{r\}\{s\} = \{m\} = \{0\}; \qquad (3\text{-}6)$$

если при этом класс $\{r\}$ обладает обратным элементом $\{r\}^{-1}$, то

$$\{r\}^{-1}\{r\}\{s\} = \{s\} = \{r\}^{-1}\{0\} = \{0\}, \qquad (3\text{-}7)$$

что противоречит предположению о том, что r и s – некоторые целые числа, не кратные m. Поэтому класс вычетов $\{r\}$ *не может иметь обратного элемента* и кольцо классов вычетов *не является полем.*

ДОСТАТОЧНОСТЬ. Предположим, что дано кольцо классов вычетов по модулю m, которое является *простым числом.* Покажем, что в этом случае кольцо классов вычетов является полем.

Для этого нам достаточно показать, что *для* ***каждого*** *класса вычетов*, исключая идеал $\{0\}$, существует обратный по умножению элемент. Каждый такой ***ненулевой*** класс вычетов содержит целое число s, которое удовлетворяет неравенствам: $0 < s < m$.

Поскольку $\{1\}^{-1}\{1\} = \{1\}$, то можно предполагать, что $s > 1$. Так как согласно предположению m – простое число и $s < m$, то НОД s и m равен 1. Но тогда согласно соотношению (3-3)

$$1 = am + bs, \qquad (3\text{-}8)$$

и, следовательно, $\{b\}\{s\} = \{1\}$; откуда найдём:

$$\{s\}^{-1} = \{b\}. \qquad (3\text{-}9)$$

ЧТД

Поле, о котором шла речь в теореме 3.4, называется *простым полем Галуа* или *полем Галуа из p элементов GF(p)* ***характеристики*** p (см. [3.3, с. 76-77]); p – простое число.

! Кольцо целых чисел по модулю простого числа $m = 5$ согласно теореме 3.4 является полем $Z_5 = GF(5) = GF(p)$, характеристики $p = m = 5$ (см. табл. 3.5).

↵

Доказано *существование конечных полей*, называемых *расширенными* полями Галуа $GF(q)$ характеристики p, порядок которых $q = p^s$, где p – простое число, а s – любое целое положительное число [3.3, с. 76; 3.7].

3.4. МНОГОЧЛЕНЫ

Выражение

$$f(X) = f_n X^n + f_{n-1} X^{n-1} + \ \ldots\ + f_1 X + f_0 X^0, \qquad (3\text{-}10)$$

определяет *многочлен* $f(X)$ *степени* n ***над полем*** F_0, если коэффициенты $f_n, f_{n-1}, \ldots f_1, f_0$ являются элементами поля F_0 и если коэффициент f_n не равен нулю; при этом будем считать, что коэффициенты f_i определены для всех $i \geq 0$ и $f_i = 0$ для $i > n$. Символ X в многочлене $f(X)$ называется *неопределённым* [3.1, 3.2].

При таком определении многочлен над полем F_0 можно рассматривать как способ представления бесконечной последовательности элементов поля $f_0, f_1, \ldots$, когда лишь конечное число членов этой последовательности отлично от нуля. Степенью полинома при этом считается наибольшее целое положительное число n, для которого $f_n \neq 0$.

При этом полагается, что $X^0 = 1$, где 1 – единичный элемент поля F_0. С учётом этого соглашения выражение (3-10) может быть переписано в виде:

$$f(X) = f_n X^n + f_{n-1} X^{n-1} + \ \ldots\ + f_1 X + f_0, \qquad (3\text{-}10\text{a})$$

В частном случае *нулевого многочлена* или 0-*многочлена* для всех $n \geq 0$ $f_n = 0$. Полагают, что 0-многочлен имеет степень $n = 0$:

$$f(X) = f_n = f_0 = 0 \cdot X^0 = 0 \cdot 1 = 0; \qquad (3\text{-}11)$$

однако некоторые авторы считают степень 0-многочлена *неопределённой* [3.3, с. 83].

Два многочлена называются *равными*, если каждый из них соответствует одной и той же последовательности коэффициентов.

Многочлен называется *нормированным*, если коэффициент при наивысшей степени X равен единице:

$$f_n = 1. \qquad (3\text{-}12)$$

Суммой двух многочленов $f(X)$ и $g(X)$ над данным полем называется многочлен над этим же полем, определяемый соотношением:

$$f(X) + g(X) = \sum_{i=0}^{\infty} (f_i + g_i) X^i \qquad (3\text{-}13)$$

Степень полинома-суммы $f(X) + g(X)$ равна тому максимальному n, для которого $f_n + g_n \neq 0$ и, следовательно, не превосходит максимальной из степеней $f(X)$ и $g(X)$.

Произведением двух многочленов $f(X)$ и $g(X)$ над данным полем называется многочлен над этим же полем, определяемый соотношением:

$$f(X)\, g(X) = \sum_{i} \Big(\sum_{j=0}^{i} f_j g_{i-j} \Big) X^i \qquad (3\text{-}14)$$

[3.3, с. 83].

Если степень полинома $f(X)$ равна n, $f_n \neq 0$, а степень полинома $g(X)$ равна m, $g_m \neq 0$, то первое, отличное от нуля, слагаемое этого многочлена равно $f_n g_m X^{n+m}$.

Очевидно, что если $g(X) = 0$, то для любых многочленов $f(X)$

$$f(X)g(X) = 0, \qquad (3\text{-}15)$$

и, если $f(X) \neq 0$ и $g(X) \neq 0$, то

$$f(X)g(X) \neq 0. \qquad (3\text{-}16)$$

Единичным многочленом называется *нормированный многочлен* нулевой степени:

$$f(X) = f_n = f_0 = 1 \cdot X^0 = 1 \cdot 1 = 1; \qquad (3\text{-}17)$$

Умножение многочлена $f(X)$ над некоторым полем на некоторый элемент α этого поля согласно (3-14) определяется соотношением:

$$\alpha f(X) = \sum_{i} (\alpha f_i) X^i. \qquad (3\text{-}18)$$

Отрицательный многочлен для данного многочлена $f(X)$ определяется соотношением:

$$-f(X) = \sum_{i} (-f_i) X^i. \qquad (3\text{-}19)$$

Очевидно, что рассматриваемое множество многочленов с определёнными над ними операциями образует аддитивную абелеву группу. Очевидно также, что для операции умножения многочленов справедливы ассоциативный и коммутативный законы; а для операций сложения и умножения выполняется дистрибутивный закон:

$$[f(X) + g(X)]\, h(X) = f(X)h(X) + g(X)h(X), \qquad (3\text{-}20)$$

где $h(X)$ – некоторый полином из рассматриваемого множества полиномов.

Однако в рассматриваемом множестве многочленов с операциями их сложения и умножения, за исключением случая единичного многочлена, *отсутствуют обратные по умножению элементы*, и, следовательно, *оно является* ***кольцом*** бесконечного порядка, *но не является* ***полем***.

Укажем ещё некоторые легко устанавливаемые свойства многочленов, которые потребуются нам в дальнейшем:

$$-[f(X)g(X)] = [-f(X)]g(X) = f(X)[-g(X)], \qquad (3\text{-}21)$$

$$f(X)g(X) = f(X)h(X) \Rightarrow g(X) = h(X) \text{ при } f(X) \neq 0 \ . \quad (3\text{-}22)$$

ПРИМЕР 3.4. Рассмотрим многочлены с коэффициентами из $F_0 = Z_2 = \{0, 1\}$ – т.е. двоичные многочлены: $g(X) = 1+X$, $0 = 0 \cdot X^0$ и $1 = 1 \cdot X^0$ из кольца многочленов бесконечного порядка. Определим результаты выполнения следующих операций:

$$g(X) \cdot 0 = 0 \cdot g(X) = (1+X) \cdot 0 = 0 \cdot (1+X) = 0 \cdot 1 + 0 \cdot X = 0,$$

$$g(X) \cdot 1 = 1 \cdot g(X) = (1+X) \cdot 1 = 1 \cdot (1+X) = 1+X = g(X),$$

$$g(X)+1 = 1+ g(X) = 1+X+1 = 1+1+X = 0+X = X,$$

$$g(X)+0 = 0+g(X) = 1+X+0 = 0+1+X = 1+X = g(X).$$

END

ПРИМЕР 3.5. 1) Определить число всех различных многочленов степени n и ниже над полем F_0 порядка $|F_0| = p$.

ОТВЕТ

Искомое число различных многочленов равно $|F_0|^{n+1} = p^{n+1}$.

2) Привести все многочлены над полем $F_0 = GF(2)$ степени 2 и ниже.

ОТВЕТ

В рассматриваемом случае порядок поля F_0 $|F_0| = p = 2$, а *максимально* возможная степень рассматриваемых многочленов $n = 2$. Поэтому общее число рассматриваемых многочленов

$$|F_0|^{n+1} = p^{n+1} = 2^3 = 8.$$

Табл. 3.12 содержит 8 всех различных многочленов, степень которых не превосходит двух.

Таблица 3.12

Степень многочленов	Многочлены
0	$0 = 0 \cdot X^0$, $1 = 1 \cdot X^0$
1	X, $1+X$
2	X^2, $1+X^2$, $X+X^2$, $1+X+X^2$

3) Вычислить значения двух многочленов, представленных в табл. 3.12: $1+X$ и $1+X^2$ для всех значений X из поля Z_2.

ОТВЕТ

Вычисленные значения многочленов $1+X$ и $1+X^2$ приведены в табл. 3.13.

Таблица 3.13

Значения X из поля Z_2	Значения многочлена $1+X$	Значения многочлена $1+X^2$
0	1	1
1	0	0

Несмотря на то, что *значения* биномов $1+X$ и $1+X^2$ для $X = 0$ и для $X = 1$ совпадают, рассматриваемые *как двоичные многочлены* биномы $1+X$ и $1+X^2$ *различны*.

END

Обозначим ***множество всех многочленов над полем*** $F_0 = GF(p)$, где p – простое число, как $F_0[X]$, а множество всех многочленов степени n и менее – как $F_0^{(n)}[X]$.

Степень многочлена $f(X)$ будем обозначать как $\deg f$.

3.5. ИДЕАЛЫ МНОГОЧЛЕНОВ И КЛАССЫ ВЫЧЕТОВ

Ниже будет изложен материал, подобный сведениям, приведенным в разд. 3.2. Поэтому часто будут приводиться теоремы без доказательств (которые можно найти в [3.1, 3.2,

3.3]), поскольку они будут близки к теоремам, доказанным в разд. 3.2 и на которые будут делаться ссылки.

Если многочлены $r(X)$, $s(X)$ и $t(X)$ связаны соотношением $r(X)s(X) = t(X)$, то говорят, что $t(X)$ *делится* на $r(X)$ и на $s(X)$, или что $r(X)$ и $s(X)$ *являются делителями* $t(X)$ или являются *множителями* для $t(X)$.

Многочлен $p(X)$ степени n, который не делится ни на какой многочлен степени, меньшей, чем n, но большей 0, называется *неприводимым*.

ПРИМЕР 3.6. Доказать, что двоичные многочлены, приведенные в табл. 3.14, исчерпывают множество всех неприводимых многочленов над полем $Z_2 = GF(2)$ степени четыре и ниже.

Многочлены первой степени. Многочлены X и $(X+1)$ неприводимы *по определению*.

Многочлены второй степени. Многочлен второй степени $f(X) = X^2+aX+b$, $a, b \in \{0, 1\}$, неприводим в том и только в том случае, если он не делится ни на X, ни на X-1 (X-1 = X+1), что эквивалентно выполнению соотношений: $f(0) = b \neq 0$ и $f(1) = =1+a+b \neq 0$ или соотношений: $b = 1$ и $a = 1$. Следовательно, лишь единственный многочлен $f(X) = X^2+X+1$ является неприводимым.

Многочлены третьей степени. Многочлен третьей степени $f(X) = X^3+aX^2+bX+c$, $a, b, c \in \{0, 1\}$, неприводим в том и только в том случае, если он не делится ни на X, ни на $X+1$, что эквивалентно выполнению соотношений: $f(0) = c \neq 0$ и $f(1) = 1+a+b + c \neq 0$ или соотношений: $c = 1$ и $a+b = 1$. Следовательно, имеются лишь два неприводимых многочлена третьей степени X^3+X^2+1 и X^3+X+1.

Таблица 3.14

Степень многочленов	Неприводимые многочлены
1	X, $(X+1)$
2	X^2+X+1
3	(X^3+X^2+1), (X^3+X+1)
4	$(X^4+X^3+X^2+X+1)$, (X^4+X^3+1), (X^4+X+1)

Многочлены четвёртой степени. Многочлен четвёртой степени $f(X) = X^4+aX^3+bX^2+cX + d$, $a, b, c, d \in \{0, 1\}$, неприводим в том и только в том случае, если он не делится ни на один из неприводимых многочленов первой или второй степени.

Так как имеется только один неприводимый многочлен второй степени, то все не являющиеся неприводимыми многочлены четвёртой степени, кроме многочлена $X^4+X^2+1 = =(X^2+X+1)^2$, должны делиться на один из многочленов первой степени.

Следовательно, для всех неприводимых многочленов четвёртой степени должны выполняться соотношения: $f(0) = d \neq 0$ и $f(1) = 1+a+b+c+d \neq 0$ или соотношения: $d = 1$ и $a+b+c \neq 0$. Очевидно, что этим условиям удовлетворяют следующие многочлены четвёртой степени: $(X^4+X^3+X^2+X+1)$, (X^4+X^3+1), (X^4+X^2+1), (X^4+X+1), однако многочлен X^4+X^2+1 не является неприводимым.

END

! Вместо неприводимого многочлена $X^4+X^3+X^2+X+1$ в [3.3] на с. 87 фигурирует многочлен $X^4+X^3+X^2+1=(X+1)(X^3+X+1)$.

↵

В Приложении 5.2 приведены разложения биномов $X^n + 1$, $1 \leq n \leq 31$, на неприводимые сомножители над полем

$GF(2)$, полученные с помощью компьютерного математического пакета Maple V R5 (см. Приложение 5.3).

НОД двух многочленов называется *нормированный многочлен наибольшей степени*, являющийся *делителем* обоих многочленов. Если НОД двух многочленов равен 1, то говорят, что эти два многочлена являются *взаимно простыми*.

Степень произведения двух многочленов равна сумме степеней многочленов-сомножителей. Ненулевой многочлен *нулевой степени* (т.е. $1 \cdot X^0 = 1$) является элементом поля $GF(p)$ и, следовательно, имеет обратный элемент по умножению ($1^{-1}=1$); однако для многочленов степени $n > 0$ обратных элементов *не существует*.

Алгоритм Евклида – «алгоритм деления с остатком» применим и в случае многочленов: для любой пары многочленов над $F_0=GF(p)$ $s(X)$-делимое и $d(X)$-делитель, $d(X) \neq 0$, существует *единственная* пара многочленов над полем F_0 $q(X)$-частное и $r(X)$-остаток, таких, что

$$s(X) = d(X)\, q(X) + r(X), \qquad (3\text{-}23)$$

причём *степень* $r(X)$ *меньше степени* $d(X)$ [3.1, с. 233; 3.2, с. 171; 3.3, с. 84; 3.7].

ПРИМЕР 3.7. Показать, что двоичный многочлен $s(X) = X^5+X^2+1$ является *неприводимым* многочленом.

Очевидно, что данный многочлен не делится на X. Проверим, будет ли его делителем многочлен $X+1$:

$$\begin{array}{l} X^5 \qquad\quad +X^2+1 \\ \underline{X^5+X^4} \\ \quad X^4 \qquad +X^2+1 \\ \quad \underline{X^4+X^3} \\ \qquad X^3+X^2+1 \\ \qquad \underline{X^3+X^2} \\ \qquad\quad 1 \end{array} \qquad \left| \begin{array}{l} X+1 \\ \hline X^4+X^3+X^2 \end{array} \right. \qquad (3\text{-}24)$$

Так как остаток $r(X) = 1 \neq 0$, то $X+1$ не является делителем $s(X)$. Мы исчерпали все линейные делители; проверим квадратные. Легко установить, что не являются делителями $s(X)$ следующие квадратные многочлены: X^2, $X^2+X=X(X+1)$ и $X^2+1=X^2+2X+1=(X+1)^2$. Остаётся проверить ещё один многочлен: X^2+X+1:

$$\begin{array}{l} X^5 \qquad\quad +X^2+1 \\ \underline{X^5+X^4+X^3} \\ \qquad X^4+X^3+X^2+1 \\ \qquad \underline{X^4+X^3+X^2} \\ \qquad\quad 1 \end{array} \qquad \left| \begin{array}{l} X^2+X+1 \\ \hline X^3+X^2 \end{array} \right. \qquad (3\text{-}24a)$$

Таким образом, многочлены второй степени не являются делителями $s(X)$. Следовательно, возможные делители следует искать среди полиномов степени ≥ 3, однако все произведения таких многочленов имеют степень ≥ 6. Следовательно, двоичный многочлен $s(X)$ *неприводим*.

END

Аналогично сравнению целых чисел по модулю m можно определить сравнение для многочленов над полем $GF(p)$ *по модулю некоторого заданного многочлена*.

Сравнение многочленов $a(X)$, $b(X)$ *по модулю многочлена* $f(X)$

$$a(X) \equiv b(X) \pmod{f(X)} \qquad (3\text{-}25)$$

по определению эквивалентно равенству

$$a(X) - b(X) = q(X)\, f(X) \qquad (3\text{-}26)$$

для некоторого многочлена-частного $q(X)$.

Все операции в сравнении (3-25) выполняются по mod p [3.24, с. 10].

Все многочлены $a(X)$ над полем $GF(p)$, такие, что