**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

**Федеральное государственное образовательное бюджетное учреждение высшего профессионального образования «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ им. проф. М. А. БОНЧ-БРУЕВИЧА»**

---

**С. С. Владимиров**

# МАТЕМАТИЧЕСКИЕ ОСНОВЫ ТЕОРИИ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

**Курс лекций**

СПб ГУТ)))

**Санкт-Петербург**
**2014**

# 2. Математические основы помехоустойчивого кодирования

Помехоустойчивое кодирование базируется на широком математическом аппарате, включающем в себя двоичную алгебру, матричное исчисление, операции с полиномами, комбинаторику, алгебру конечных полей и теорию графов.

Далее кратко рассмотрим те отдельные элементы этих разделов математики, которые могут быть применены при изучении алгоритмов и принципов помехоустойчивого кодирования.

## 2.1. Элементы двоичной алгебры

Позиционная система счисления с основанием 2 называется *двоичной системой счисления* [3].

Для записи чисел в двоичной системе используются две цифры: 0 и 1. Основание системы 2 записывается как $10_2$ [3].

Каждая цифра двоичного числа соответствует степени двойки, равной номеру позиции цифры слева. В табл. 2.1 приведены значения первых степеней.

*Таблица 2.1*

*Степенной ряд двойки (до 12-й степени включительно)*

| **Показатель степени** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Значение** | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 |

### *2.1.1. Перевод двоичного числа в десятичное*

Перевод двоичного числа в десятичное производится по классической схеме сложения степеней двойки с коэффициентами, которыми являются соответствующие цифры этого двоичного числа.

Процесс перевода двоичного числа в десятичное рассмотрим на примере двоичного числа

$$100111001011_2.$$

Для простоты распишем показатели степени

$$\begin{matrix}11&10&9&8&7&6&5&4&3&2&1&0\\1&0&0&1&1&1&0&0&1&0&1&1\end{matrix}_2.$$

Таким образом, можно написать

$$1\cdot2^{11}+0\cdot2^{10}+0\cdot2^9+1\cdot2^8+1\cdot2^7+1\cdot2^6+0\cdot2^5+0\cdot2^4+1\cdot2^3+0\cdot2^2+1\cdot2^1+1\cdot2^0.$$

Убрав степени с коэффициентом 0, получим

$$1\cdot2^{11}+1\cdot2^8+1\cdot2^7+1\cdot2^6+1\cdot2^3+1\cdot2^1+1\cdot2^0.$$

Уберем коэффициенты и раскроем степени

$$2^{11}+2^8+2^7+2^6+2^3+2^1+2^0 = 2048+256+128+64+8+2+1 = 2507.$$

Таким образом

$$100111001011_2 = 2507_{10}.$$

### *2.1.2. Перевод десятичного числа в двоичное*

Для перевода десятичного числа в двоичное используется процедура последовательного деления десятичного числа на два с накоплением остатка.

Для примера рассмотрим обратный перевод числа $2507_{10}$, полученного в примере, приведенном в предыдущем подразделе.

| | | |
|---|---|---|
| 2507 | 2 | |
| 1 | 1253 | 2 |
| 1 | 626 | 2 |
| 0 | 313 | 2 |
| 1 | 156 | 2 |
| 0 | 78 | 2 |
| 0 | 39 | 2 |
| 1 | 19 | 2 |
| 1 | 9 | 2 |
| 1 | 4 | 2 |
| 0 | 2 | 2 |
| 0 | 1 | |

Результат записывается, начиная с конца. Таким образом

$$2507_{10} = 100111001011_2.$$

При переводе небольших десятичных чисел иногда удобнее использовать разложение в ряд степеней двойки (см. табл. 2.1), обратно рассмотренной в подразделе 2.1.1 процедуре.

Например, число $292_{10}$ можно представить как

$$292_{10} = 256+32+4 = 2^8+2^5+2^2 = 100100100_2.$$

### 2.1.3. Операции над двоичными числами

В табл. 2.2 приведены таблицы сложения и умножения двоичных чисел.

*Таблица 2.2*

*Таблицы сложения (а) и умножения (б) двоичных чисел*

Двоичное сложение (а)

| $+$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 10 |

Двоичное умножение (б)

| $\times$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

В табл. 2.3 приведены таблицы логического сложения (дизъюнкция, «ИЛИ», OR) и умножения (конъюнкция, «И», AND) двоичных чисел.

*Таблица 2.3*

*Таблицы логического сложения (а) и умножения (б) двоичных чисел*

Логическое сложение (а)

| OR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

Логическое умножение (б)

| AND | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

С точки зрения помехоустойчивого кодирования наиболее важной является операция сложения по модулю 2, показанная в табл. 2.4. Ей соответствует логическая операция «исключающее-ИЛИ» (XOR).

*Таблица 2.4*

*Таблица сложения двоичных чисел по модулю 2*

| $\oplus$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

## 2.2. Матрицы и действия над ними

### 2.2.1. Понятие матрицы

*Матрицей* называется прямоугольная таблица чисел из некоторого числового поля, имеющая $m$ строк и $n$ столбцов [4, 5].

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

В общем случае такая матрица называется *прямоугольной* размера $m \times n$ или $m \times n$-матрицей. Если $m = n$, то матрица называется *квадратной порядка* $n$. Числа, составляющие матрицу, называются ее *элементами*. При двухиндексном обозначении элементов первый индекс всегда указывает номер строки, а

второй индекс — номер столбца, на пересечении которых стоит данный элемент [4, 5].

Каждой $m \times n$-матрице $A$ с элементами $a_{ij}$ соответствует $n \times m$-матрица с элементами $a_{ji}$. Она называется *транспонированной* к $A$ и обозначается через $A'$. $(A')' = A$. Строки матрицы $A$ становятся столбцами в $A'$ и столбцы матрицы $A$ становятся строками в $A'$ [5].

$$A = \begin{bmatrix} 1 & 3 & 5 & -3 \\ 3 & 5 & 12 & 6 \\ 7 & -4 & -8 & 2 \end{bmatrix} \quad \longrightarrow \quad A' = \begin{bmatrix} 1 & 3 & 7 \\ 3 & 5 & -4 \\ 5 & 12 & -8 \\ -3 & 6 & 2 \end{bmatrix}$$

Прямоугольная матрица размера $m \times 1$, т. е. состоящая из одного столбца, называется *вектор-столбцом* или *столбцевой матрицей*. Прямоугольная матрица размера $1 \times n$, т. е. состоящая из одной стороки, называется *вектор-строкой* или *строчной матрицей* [4, 5].

Квадратную матрицу, у которой все элементы, расположенные вне главной диагонали, равны нулю, называют *диагональной* [4, 5].

$$\begin{bmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & d_n \end{bmatrix}$$

Диагональная матрица, в которой все элементы главной диагонали равны 1, называется *единичной* [5].

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

### *2.2.2. Операции с матрицами*

**Сложение матриц.** Складываются только матрицы одного размера. Сложение производится поэлементно.

$$\begin{bmatrix} 1 & 3 & 5 & -3 \\ 3 & 5 & 12 & 6 \\ 7 & -4 & -8 & 2 \end{bmatrix} + \begin{bmatrix} 4 & -2 & 3 & 1 \\ 8 & -6 & 1 & 4 \\ 2 & 4 & 13 & 5 \end{bmatrix} = \begin{bmatrix} 5 & 1 & 8 & -2 \\ 11 & -1 & 13 & 10 \\ 9 & 0 & 5 & 7 \end{bmatrix}$$

**Умножение матрицы на число.** Каждый элемент матрицы умножается на это число.

$$3 \times \begin{bmatrix} 1 & 3 & 5 & -3 \\ 3 & 5 & 12 & 6 \\ 7 & -4 & -8 & 2 \end{bmatrix} = \begin{bmatrix} 3 & 9 & 15 & -9 \\ 9 & 15 & 36 & 18 \\ 21 & -12 & -24 & 6 \end{bmatrix}$$

**Умножение матриц.** Матрицы умножаются по правилу «строка-на-столбец». Для того, чтобы матрицу $A$ можно было умножить на матрицу $B$, Количество столбцов в $A$ должно быть равно количеству строк в $B$. Таким образом, результатом произведения $m \times l$-матрицы $A$ на $l \times n$-матрицу $B$ будет $m \times n$-матрица $C$ [5].

$$\begin{bmatrix} 1 & 3 & 5 & -3 \\ 3 & 5 & 12 & 6 \\ 7 & -4 & -8 & 2 \end{bmatrix} \times \begin{bmatrix} 4 & -2 & 3 & 1 \\ 8 & -6 & 1 & 4 \\ 2 & 4 & 13 & 5 \\ 4 & 1 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 26 & -3 & 71 & 32 \\ 100 & 18 & 170 & 95 \\ -12 & -20 & -87 & -45 \end{bmatrix}$$

Для примера рассмотрим умножение первой строки матрицы $A$ на первый столбец матрицы $B$.

$$(1 \cdot 4) + (2 \cdot 8) + (5 \cdot 2) + (-3 \cdot 4) = 26.$$

## 2.3. Элементы комбинаторики

Любая совокупность элементов произвольного рода образует *множество*. Множество, состоящее из конечного числа элементов, называется *конечным множеством* [6].

Если существует два множества $A$ и $B$, и при этом каждый элемент множества $B$ принадлежит множеству $A$, то $B$ называется *подмножеством* множества $A$. Произвольное $k$-элементное подмножество $n$-элементного множества называется *сочетанием* из $n$ элементов по $k$ ($C_n^k$). Порядок элементов в подмножестве не имеет значения. Иногда вместо слова «сочетание» употребляется термин — *комбинация* из $n$ элементов по $k$ [6].

$$C_n^k = \frac{n!}{k!(n-k)!}.$$

Множество называется *упорядоченным*, если каждому элементу этого множества поставлено в соответствие некоторое число (номер элемента) от 1 до $n$, где $n$ — число элементов множества, так что различным элементам соответствуют различные числа. Упорядоченные множества считаются различными, если они отличаются либо своими элементами, либо их порядком. Различные упорядоченные множества, которые отличаются лишь порядком элементов (т. е. могут быть получены из того же самого множества), называются *перестановками* $P_n$ этого множества [6].

$$P_n = n!.$$

Упорядоченные $k$-элементные подмножества множества из $n$ элементов называются *размещениями* из $n$ элементов по $k$ ($A_n^k$). Различные размещения

из $n$ по $k$ отличаются количеством элементов либо их порядком [6]. Число различных размещений из $n$ по $k$ равно

$$A_n^k = k! \cdot C_n^k = \frac{n!}{(n-k)!} = n(n-1)\ldots(n-k+1).$$

## 2.4. Операции с полиномами

При изучении помехоустойчивых кодов под *полиномом (многочленом)* будем понимать многочлен от одной переменной, т. е. конечную сумму вида

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

где $a_k$ — *коэффициент* многочлена $f(x)$ при $x^k$ [7]. Каждый из элементов многочлена вида $a_k x^k$ называется *одночленом* степени $k$.

Многочлен, все коэффициенты которого равны нулю, называется *нулевым многочленом*. Если многочлен не является нулевым, то наибольшее из таким чисел $k$, что $a_k \neq 0$, называется *степенью* этого многочлена [7].

При изучении помехоустойчивого кодирования мы в основном будем сталкиваться с полиномами трех видов:

1. Полином с десятичными коэффициентами.
2. Полином с коэффициентами 0 или 1 (простое поле $\mathrm{GF}(2)$).
3. Полином с коэффициентами, принадлежащими конечному полю $\mathrm{GF}(2^p)$.

В этом разделе рассмотрим операции с полиномами первых двух видов. Полиномы с коэффициентами, принадлежащими конечному полю $\mathrm{GF}(2^p)$, затронем при рассмотрении математики конечных полей Галуа.

Полиномы можно записывать в виде вектор-строки коэффициентов. Например, полином

$$f(x) = 2 + 4x + 5x^2 + 3x^4 + 2x^6$$

можно записать как

$$f(x) = [2030542]$$

или

$$f(x) = [2450302],$$

в зависимости от того, записывать его по возрастанию или по убыванию степеней. Часто такая форма записи применяется для полиномов с коэффициентами, принадлежащими простому полю $\mathrm{GF}(2)$. Такая запись внешне совпадает с записью двоичного числа. Также при работе с литературой необходимо уточнять используется запись по убыванию или по возрастанию степеней. Полином

$$f(x) = x^4 + x + 1$$

может быть записан как

$$f(x) = 1\overleftarrow{0011}$$

или

$$f(x) = 11\overrightarrow{001}.$$

**Сумма полиномов.** При суммировании полиномов складываются коэффициенты одночленов одной степени.

$$\begin{aligned}
&f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n,\\
&g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m,\\
&m > n,\\
&h(x) = f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots +\\
&+(a_n + b_n)x^n + \ldots + (a_m + b_m)x^m.
\end{aligned}$$

При рассмотрении полиномов с коэффициентами 0 и 1, принадлежащими простому полю $\mathrm{GF}(2)$ необходимо учитывать, что сложение в этом случае производится по модулю 2. Таким образом, при сложении двух одночленов одной степени с коэффициентом 1, результирующий одночлен будет иметь коэффициент 0.

$$(1 + x + x^2 + x^4) + (x + x^3 + x^4 + x^5) = 1 + x^2 + x^3 + x^5.$$

То есть, происходит сокращение одночленов одной степени.

**Произведение полиномов.** Умножение полиномов выполняется по следующему принципу

$$\begin{aligned}
&f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n,\\
&g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m,\\
&h(x) = f(x)g(x) = f(x)b_0 + f(x)b_1x + f(x)b_2x^2 + \ldots + f(x)b_mx^m =\\
&= (b_0a_0 + b_0a_1x + \ldots + b_0a_nx^n) + (b_1a_0x + b_1a_1x^2 + \ldots + b_1a_nx^{n+1}) + \ldots +\\
&+(b_ma_0x^m + b_ma_1x^{1+m} + \ldots + b_ma_nx^{n+m}).
\end{aligned}$$

Далее полученные полиномы складываются по обычному правилу. Таким образом, в результате произведения полинома степени $n$ на полином степени $m$ получается полином степени $n+m$.

Умножение полиномов с коэффициентами из простого поля $\mathrm{GF}(2)$ производится аналогично с учетом того, что операция сложения осуществляется по модулю 2.

**Деление полиномов.** Для деления полиномов можно использовать процедуру деления в столбик, подобно рассмотренному ранее делению двоичных чисел.

$$\begin{array}{r|l} 4x^3+10x^2+6x+1 & 2x^2+4x+1 \\ \underline{-\,4x^3+\ 8x^2+\ 2x\ \ \ \ } & \underline{\ \ 2x+1\ \ \ \ } \\ \ \ \ \ \ 2x^2+\ 4x+1 & \\ \underline{\ \ \ \ \ \ \ \ \ \ \ \ } & \\ \ \ \ \ \ \ \ \ \ \ 0 & \end{array}$$

Таким образом

$$\frac{4x^3+10x^2+6x+1}{2x^2+4x+1} = 2x+1.$$

Аналогично производится деление полиномов с коэффициентами из простого поля $\mathrm{GF}(2)$. Вместо операции вычитания используется сложение по модулю 2.

$$\begin{array}{r|l} \oplus\, x^5+x^4+x^3+x+1 & x^2+1 \\ \underline{\ \ x^5+x^3\ \ \ \ \ \ \ \ \ \ } & \underline{\ \ x^3+x^2+1\ \ \ \ } \\ \ \ \ \oplus\, x^4+\ x+1 & \\ \ \ \ \underline{\ \ x^4+x^2\ \ \ \ \ \ } & \\ \ \ \ \ \ \ x^2+x+1 & \\ \ \ \ \ \ \oplus\, x^2+1 & \\ \ \ \ \ \ \underline{\ \ \ \ \ \ \ \ } & \\ \ \ \ \ \ \ \ \ \ \ x & \end{array}$$

Таким образом

$$\frac{x^5+x^4+x^3+x+1}{x^2+1} = (x^3+x^2+1)+\frac{x}{x^2+1}.$$

## 2.5. Понятие группы, кольца и поля

### *2.5.1. Группа*

*Группой* называется множество элементов, для которых определена некоторая операция «$\bullet$» (сложение или умножение) и выполняется ряд приведенных ниже аксиом [8, 9].

**Аксиома G.1.** Операция «$\bullet$» может быть применена к любым двум элементам группы, в результате чего получается третий элемент группы.

$$\text{Если} \quad a \in G \quad \text{и} \quad b \in G, \quad \text{то} \quad a \bullet b \in G.$$

Аксиома G.1 определяет *замкнутость операции в группе*. Как правило операции над элементами называют *сложением* («+») или *умножением* («$\cdot$»/«$\times$»), даже если они не являются обычными сложением и умножением. В соответствии с двумя записями операций различают *аддитивную* и *мультипликативную* группы [8, 9].

**Аксиома G.2.** *Свойство ассоциативности.* Для любых трех элементов $a$, $b$ и $c$ из группы $G$ верно

$$a \bullet (b \bullet c) = (a \bullet b) \bullet c.$$

То есть порядок выполнения операций несущественен.

**Аксиома G.3.** В $G$ всегда существует единичный элемент $e$, такой, что

$$a \bullet e = e \bullet a = a \quad \text{для любого} \quad a \in G.$$

Для аддитивной группы единичный элемент называют нулем, обозначают 0 и определяют из уравнения

$$a + 0 = 0 + a = a.$$

Для мультипликативной группы единичный элемент называют единицей и определяют из уравнения

$$a \cdot 1 = 1 \cdot a = a.$$

**Аксиома G.4.** Для любого элемента $a \in G$ существует обратный элемент $a^{-1}$ такой, что

$$a \bullet a^{-1} = a^{-1} \bullet a = e.$$

Для аддитивной группы обратный к $a$ элемент обозначается $-a$ и находится из уравнения

$$a + (-a) = (-a) + a = 0.$$

Для мультипликативной группы обратный к $a$ элемент обозначается $a^{-1}$ и находится из уравнения

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Кроме того, для любого элемента $a \in G$ и любого целого положительного $n$

$$(a^n)^{-1} = (a^{-1})^n.$$

Можно ввести степени элемента $a$ с целыми отрицательными показателями так что $a^{-n} = (a^n)^{-1}$ [10, 11]. Также можно обозначить

$$a^0 = e.$$

Все обычные правила действий со степенями остаются справедливыми в любой группе [10, 11].

Рассмотрим всевозможные степени произвольного элемента $g$ группы $G$

$$\ldots, g^{-2}, g^{-1}, g^0 = e, g^1 = g, g^2, \ldots.$$

Если все эти степени различны, то элемент $g$ называется *элементом бесконечного порядка*; иначе он называется *элементом конечного порядка*.

Для любого элемента конечного порядка существуют такие числа $N$, что $g^N = e$[1]. Наименьшее из этих чисел называется порядком $n$ элемента $g$ [10, 11].

Также верно утверждение, что для любого элемента $g$ порядка $n$ равенство $g^m = e$ имеет место тогда и только тогда, когда $m$ делится на $n$[2] [10, 11].

В группе $G$ порядок 1 имеет только единичный элемент $e$ [10, 11].

Соответственно, выделяют *конечные* группы, состоящие из конечного числа элементов, и *бесконечные*. Количество элементов в конечной группе, называется ее *порядком* [10].

Если кроме аксиом G.1–G.4 выполняется *аксиома коммутативности G.5*, то группа называется *коммутативной* или *абелевой* [8, 9, 10].

**Аксиома G.5.** *Аксиома коммутативности.* Для двух произвольных элементов $a$ и $b$ из $G$ справедливо[9, 10, 11]

$$a \bullet b = b \bullet a.$$

В качестве примера аддитивной группы можно привести совокупность действительных чисел. Единичным элементом при этом является ноль. Множество всех действительных чисел без нуля образует мультипликативную группу. Единичным элементом является 1, а обратным $\frac{1}{a}$ [9].

Другим примером группы является совокупность двоичных $n$-символьных комбинаций, которая образует группу из $2^n$ элементов вокруг операции сложения по модулю 2. Единичным является элемент, состоящий из нулей (например, 0000), а обратный элемент равен самому элементу ($0101 \oplus 0101 = 0000$) [9].

### *2.5.2. Подгруппы и смежные классы*

Подмножество элементов группы $G$ называется *подгруппой* $H$, если оно удовлетворяет всем аксиомам группы. Для того чтобы определить, является ли $H$ подгруппой $G$, надо проверить только замкнутость операции (G.1) и наличие обратных элементов (G.4). Например, множество целых чисел является подгруппой группы из множества действительных чисел [9, 10, 11].

Таким образом, любая подгруппа автоматически является группой [10].

Подмножество группы $G$, состоящее из ее единицы $e$, а также сама группа $G$ тоже являются подгруппами. Они получили название *тривиальных подгрупп* [10].

[1] Поиск доказательства студентам на дом

[2] Поиск доказательства студентам на дом

Важным классом подгрупп являются *циклические подгруппы* [12]. *Циклической подгруппой* группы $G$ называется подгруппа $H$ порядка $m$, состоящая из элементов $(h, h^2, h^3, \ldots, h^{m-1}, h^m = e) = (e, h, h^2, h^3, \ldots, h^{m-1})$ [9].

Для произвольной группы $G$ и ее подгруппы $H$ подмножество группы $G$, состоящее из всех элементов вида $h \bullet g$ ($g \bullet h$), где $h$ — прозвольный элемент подгруппы $H$, а $g$ — некоторый фиксированный элемент группы $G$, называется *смежным классом* элемента $g$ по подгруппе $H$ и обозначается через $Hg$ ($gH$) [10].

Смежные классы, образованные операцией $h \bullet g$, получили название *правых смежных классов* ($Hg$), а классы, образованные операцией $g \bullet h$ — *левых смежных классов* ($gH$) [9]. Для абелевых групп правые и левые смежные классы совпадают [9, 12].

Отдельный элемент $g \in gH$ называется *представителем смежного класса* $gH$ [12].

Для смежных классов верен ряд теорем[3] [10].

1. *Смежный класс $Hg'$ любого элемента $g'$ из смежного класса $Hg$ совпадает с классом $Hg$. То есть, если два смежных класса пересекаются, то они совпадают.*
2. *Два элемента $g_1$ и $g_2$ группы $G$ тогда и только тогда принадлежат одному смежному классу по подгруппе $H$, когда $g_1 \bullet g_2^{-1} \in H$.*
3. *Смежный класс $Hg$ тогда и только тогда совпадает с подгруппой $H$, когда $g \in H$.*

Для подгруппы $H$ конечной группы $G$ верна *теорема Лагранжа. Порядок конечной группы делится на порядок любой ее подгруппы. Соответствующее частное равно индексу подгруппы.* При этом, под индексом подгруппы понимается число смежных классов по подгруппе $H$ [10].

Подгруппа $H$ группы $G$ называется *нормальным делителем*, если для любого элемента $h \in H$ и любого элемента $g \in G$ элемент $g \bullet h \bullet g^{-1}$ принадлежит $H$. Любая подгруппа абелевой группы является конечным делителем [10].

### 2.5.3. Кольцо

*Кольцом $R$* называется множество элементов, на котором определены две операции — сложение и умножение, и выполняется ряд аксиом [9, 12].

**Аксиома R.1.** Множество $R$ является *аддитивной абелевой группой*.

**Аксиома R.2.** *Замкнутость операции умножения.* Для любых двух элементов $a, b \in R$ определено их произведение

$$a \cdot b = c \in R.$$

[3] Поиск доказательства студентам на дом

**Аксиома R.3.** Для любых трех элементов $a, b, c \in R$ выполняется *ассоциативный закон*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \qquad a + (b + c) = (a + b) + c.$$

**Аксиома R.4.** Для любых трех элементов $a, b, c \in R$ выполняется *дистрибутивный закон*

$$a \cdot (b + c) = a \cdot b + a \cdot c, \qquad (b + c) \cdot a = b \cdot a + c \cdot a.$$

**Аксиома R.5.** В кольце существует элемент $e$, называемый *единицей кольца*, который является нейтральным элементом относительно умножения, т. е. $e \cdot a = a \cdot e = a$ для любого $a \in R$ [12].

Элемент $a \neq 0$ кольца $R$ называется *делителем нуля*, если в $R$ существует такой элемент $b \neq 0$, что $a \cdot b = 0$ [12].

В кольце для операции умножения аксиомы G.3, G.4 и G.5 (см. раздел 2.5.1) могут не выполняться. Если же операция умножения коммутативна в кольце, то такое кольцо называется *коммутативным*. Если в кольце существует единичный элемент относительно операции умножения (выполняется аксиома G.3), то это кольцо называется *кольцом с единицей* [9].

В качестве примера кольца можно предложить все целые положительные и отрицательные числа и нуль, образующие коммутативное кольцо с единицей относительно обычных операций сложения и умножения [9].

### *2.5.4. Поле*

*Полем F* называют коммутативное кольцо с единицей, в котором каждый ненулевой элемент имеет мультипликативный обратный элемент (т. е. обратный по умножению) [9, 12].

Другими словами, полем называют множество, которое является аддитивной абелевой группой; ненулевые же элементы этого множества образуют мультипликативную абелевую группу, и выполняется закон дистрибутивности [9].

По аналогии с группами число элементов поля называется *порядком* поля. Поля, порядки которых конечны, называются *конечными полями* или *полями Галуа*. Конечные поля имеют наибольшее значение в теории кодирования [9]. Подробнее поля Галуа рассмотрены в разделе 3

Поле имеет ряд свойств, вытекающих из его определения [9].

**F.1.** Для любого элемента поля $a \cdot 0 = 0 \cdot a = 0$.
**F.2.** Для элементов $a, b \in F$, не равных нулю, $a \cdot b \neq 0$.
**F.3.** Для любых элементов $a, b \in F$ $a + b \neq 0$.
**F.4.** Если $a \cdot b = a \cdot c$ и $a \neq 0$, то $b = c$.

Примером поля является множество чисел $(0, 1, 2, \ldots, p-1$, где $p$ — простое число, образует конечное поле, в котором сложение и умножение производятся по модулю $p$ [9].