# Введение в теорию кодирования

Гурген Г. Аракелов

12 октября 2014 г.

# Оглавление

# Глава 1

# Группы

## 1.1 Алгебра, полугруппа, моноид

**Определение 1.1.1.** *Бинарной алгеброй называется непустое множество $S$ произвольной природы, с заданной на нем бинарной операцией $\beta : S^2 \to S$.*

Если операция $\beta$ ассоциативна то бинарная алгебра называется **полугруппой**. Для удобства будем вместо $\beta(a, b)$ писать просто $ab$. Левым единичным элементом $e$, или просто леовой единицей, называется элемент удовлетворяющий следующему свойству:

$$\boxed{\forall(a \in S)\ ea = a}$$

Аналогично вводится понятие правой единицы - элемента удовлетворяющего свойству:

$$\boxed{\forall(a \in S)\ ae = a}$$

Заметим, что если в полугруппе имеется и левая $e_l$ и правая единица $e_r$, то они совпадают.

$$e_r = e_l e_r = e_l$$

**Определение 1.1.2.** ***Моноидом*** *называется полугруппа с левой и правой единицей.*

Более точно, моноид это пара, состоящая из некоторого непустого множество произвольной природы $S$ и заданной на нем бинарной операцией $\beta, \beta(x, y) = xy$, для которой справедливы следующие свойства:

M1: $x(yz) = (xy)z$; **ассоциативность**;
M2: $(\exists e \in S) : (\forall x \in S) ex = xe = x$; **наличие единицы.**

## 1.2 Понятие группы

**Определение 1.2.1.** *Непустое множество произвольной природы $\mathfrak{B}$ (например чисел, отображений, матриц) называется **группой**, если выполняются следующие условия:*

***1. Задан закон композиции,** который каждой паре элементов $(a, b)$ из $\mathfrak{B}$ ставит в соответствие третий элемент $c$ из того же множества, как правило называемый произведением элементов $a$ и $b$, и обозначаемый как $ab$ или $a \cdot b$.*

***2. Закон ассоцитивности.** Для любых элементов $a, b, c$ из $\mathfrak{B}$*

$$\boxed{a(bc) = (ab)c.}$$

***3.** В $\mathfrak{B}$, отностительно заданного закона композиции, существует (левая)единица, т.е. элемент удовлетворяющий свойству*

$$\boxed{ea = a, \text{ для всех } a \text{ из } G.}$$

***4.** Для каждого элемента $a$ из $\mathfrak{B}$, отностительно заданного закона композиции, существует хотя бы один(левый) $a^{-1}$ обратный элемент, определяемый свойством:*

$$\boxed{a^{-1} \cdot a = e}$$

Стоит заметить, что произведение элементов в группе может зависеть от порядка следования сомножителей, и не всегда $a \cdot b = b \cdot a$. Группа называется конечной, если ее множество содержит конечное число элементов, иначе будем говорить, что имеем дело с бесконечной группой.

**Примеры**

*1. Возьмем в качестве множества элементов целые числа $Z$. В качестве закона композиции будем рассматривать простое умножение. Проверим будет ли являться группой пара $[Z, \cdot^2]$*

Условия 1 и 2 выполняются, так как умножение целых чисел является ассоциативной операцией. Условие 3 и 4 в данном случае выполняться не будут, так как не существует единичного элемента относительно умножения в множестве $Z$. Таким образом $[Z, \cdot^2]$- группой не является.

Если в качестве множества мы рассмотрим целые числа без нуля $Z/0$, то тогда в качестве единичного элемента можно взять 1 и условие 3 будет выполняться. Однако даже при таком подходе мы не получим группу, так как отноститльно умножения для всех элементов кроме 1 не будет существовать обратного.

*2. Возьмем в качестве множества опять целые числа $Z$, а качестве операции - сложение чисел.*
В этом случае условия 1 и 2 опять же выполненны. В качестве единичного элемента возьмем 0, т.е. условие 3 тоже выполненно. В качестве обратного элемента для любого элемента $a$ досточно взять элемент $-a$, т.к. $a + (-a) = 0$. Мы получили выполнение всех 4-х условий, поэтому пара $[Z, \cdot^2]$ является группой.

*3. Если в качестве множества взять множество состоящее только из единицы, а в качестве закона композиции рассматривать обычное умножение, то мы опять получим группу* $[\{1\}, \cdot^2]$.

В первых двух примерах мы имеем дело с бесконечными группами. В примере 3, построенная группа является конечной.

**Определение 1.2.2.** *Группа называется **абелевой**, если в ней выполняется закон коммутативности: $ab = ba$ для всех $a$ и $b$ из заданного множества.*

Докажем несколько простых лемм, которые понадобяться нам в дальнейшем.

**Теорема 1.2.1.** *В каждой группе, для любого элемента $a$, его правый обратный и левый обратный совпадают.*

*Доказательство.*
$$a^{-1}aa^{-1} = ea^{-1} = a^{-1}$$
Домножим левую и правую части на элемент обратный к $a^{-1}$.Получим:
$$aa^{-1} = e$$
Из последнего следует доказательство леммы. □

**Лемма 1.** *Для элемента $a^{-1}$ обратным элементом является $a$.*

*Доказательство.* Пусть $x$ обратный элемент к $a^{-1}$. Тогда имеем:
$$a^{-1}x = e$$
Домножим левую и правую части уравнения на $a$ и получим:
$$ex = ae$$
$$x = a$$
□

**Лемма 2.** *Каждая левая и правая единицы совпадают.*

*Доказательство.*

$$ae = aa^{-1}a = ea = a$$

□

Заметим, что уравнения $ax = b$ и $ya = b$ разрешимы. А именно для первого случая $x = a^{-1}b$, а для второго $y = ba^{-1}$. Так как:

$$a(a^{-1}b) = (aa^{-1})b = b$$

$$(ba^{-1})a = b(aa^{-1}) = b$$

**Лемма 3.** *Обратным элементом к произведению* $(ab)$*, является* $b^{-1}a^{-1}$*, т.е.* $(ab)^{-1} = b^{-1}a^{-1}$

*Доказательство.* Пусть $x$ обратный элемент к $(ab)$. Докажем что $x = b^{-1}a^{-1}$.
По условию:

$$(ab)x = e$$

Умножим левую и правую части на $b^{-1}a^{-1}$, получим:

$$b^{-1}a^{-1}abx = b^{-1}a^{-1}e$$

$$b^{-1}bx = b^{-1}a^{-1}$$

$$x = b^{-1}a^{-1}$$

□

### 1.2.1 Аддитивные группы

В определение группы, использование в качестве операции-умножения, не является обязательным. Вместо умножения $\cdot^2$, в качестве операции, может использоваться простое сложение $+^2$. В этом случае , обычно, единичный элемент обозначается как 0, а сама группа называется аддитивной или модулем.

В аддитивных группах, обычно пологают что сложение коммутативная операция, т.е.

$$a + b = b + a.$$

Обратный к $a$ элемент в аддитивных группах обозначается как $-a$, и вместо $a + (-b)$ обычно пишут $a - b$.

**Примеры**

*1. Примером аддитивной группы служит множество целых чисел со сложением и нулем в качестве единичного элемента.*

*2. Аддитивной группой также является множество n-мерных векторов, с введенным на нем операцией покоординатного сложения.*

### 1.2.2 Подстановки

### 1.2.3 Подгруппы

Понятие подгруппы широко используется в теории групп. Многие прикладные задачи, построенны на свойстваъ подгрупп. В этом разделе мы рассмотрим понятие подгруппы и основные свойства, которыми обладают подгруппы группы.

Формально, пусть у нас имеется некторая группа $\mathfrak{B}$. Подгруппой в данной группе будет группа, множество элементов которого является подмножеством группы $\mathfrak{B}$. Определим понятие подгруппы более строго.

**Определение 1.2.3.** *Подмножество* $\mathfrak{b}$*группы* $\mathfrak{B}$ *называется подгруппой если выполняются следующие условия:*

*1.* $\forall x \in \mathfrak{b}, \forall y \in \mathfrak{b}, xy \in \mathfrak{b}$

*2.* $\forall x \in \mathfrak{B}, x^{-1} \in \mathfrak{B}$.

Первое свойство требует, чтобы вместе с любыми двумя элементами $x, y$ в подгруппе содержалось и их произведение. Второе свойство требует, чтобы для каждого жлемента подгруппа содержала и обратный к нему элемент.

При выполнении данных двух свойств, подгруппа $\mathfrak{b}$ будет сново являться группой. Это очевидно, так как если аксиомы группы 1-2 выполняются в группе $\mathfrak{B}$, то они выполняются и в подгруппе $\mathfrak{b}$. Выполнение акиомы группы 4 следует из свойства 2, т.к. $aa^{-1} = e \in \mathfrak{b}$.

Пусть $a, b, c, ...$ элементы некторой группы $\mathfrak{B}$ $\mathfrak{B}$ могут сущестать подгруппы, содержащие данные элементы. В этом случае пересечение подгрупп снова явялется подгруппой в данной группе. Сформулируем более сильную теорему.

**Лемма 4.** *Пересечение, любого количества подгупп, группы* $\mathfrak{B}$ *снова является подгруппой в* $\mathfrak{B}$.

*Доказательство.* Пусть у нас имееется любое количество подгрупп $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}...$ группы $\mathfrak{B}$. И пусть их пересечение $\mathfrak{d}$ содержит элементы $a, b, c, ....$ Докажем что $\mathfrak{b}$ снова является подгруппой.

Рассмотрим произведение любых двух элементов $ab$. т.к. $a \in \mathfrak{a}$ отсюда следует, что $ab \in \mathfrak{a}$. Но $a, b$ также входят и $\mathfrak{b}$ и в остальные подгруппы. Отсюда следует, что и $ab\mathfrak{b}, ab \in \mathfrak{c}$.... Это означает что, $ab \in d$. То есть, этим доказывается выполнение условия 1 подгруппы. Аналогично доказывается, тот факт, что вместе с каждым элементов, множество $\mathfrak{d}$ содержит и обратный к нему. Это означает, что в множестве $\mathfrak{d}$ выполняются условия подгруппы, а это означает, что $\mathfrak{d}$- подгруппа. □

# 1.3 Кольца, тела, поля

## 1.3.1 Кольца

Алгебра и арифметика оперируют элементами различной природы. Это могут быть числа, матрицы, перестановки, отображения и т.д. В этой главе мы рассмотрим еще одну абстрактную структуру.

Под системой с двойной композицией, подразумевается произвольное множество элементов $a, b, c, d, ...$, для которых однозначно определенны две операции, обычно называемые сложением $+$ и умножением $*$.

# Глава 2

# Элементы теории чисел

## 2.1 Делимость и делители

Одним из ключевых понятий в тоерии чисел является понятие деления одного числа на другое. Пока, мы будем считать что находимся в поле целых чисел, и если понадобится, то будем расширять данное поле. Основные теоремы и свойства, которые мы покажем для целых чисел, легко обобщаются на многие расширения поля целых чисел. Мы будем говорить что $a$ делит $b$, если для нектороге $k$ выполняется соотношение $ka = b$. Факт деления $b$ на $a$ будем обозначать следующим образом: $a|b$. Заметим, что для любого числа $a$ существуют, так называемые, тривиальные делители: $a, 1$.

## 2.2 Простые и составные числа

Целые числа, среди делителей которых только тривиальные делители, называются простыми. Простые числа обладают многими замечательными свойствами и играют важнейшую роль в прикладной алгебре и в теории чисел. Многие криптографичесие системы основанны именно на свойствах таких чисел. Приведем пример простых чисел:

$$\ldots -5, -3, -1, 1, 2, 3, 5, 7, 11, 13, 17, 23, 29\ldots$$

Ученные-математики издавно заметили красивые особенности таких чисел. Большинство существующих шифровальных алгоритмов основанно на том, что не существует быстрого способа, который по некторому числу, смог определить является оно простым или нет с **абсолютной точностью**. Здесь подчеркивается, абсолютная точность, потому, что существуют различные вероятностные алгоритмы проверки на простоту.

Это такие алгоритмы, которые получая на вход некторое число $n$ могут с некторой вероятностью $P$ утверждать, что $n-$ простое. почти всегда, вероятность напрямую зависит от времени работы и от количества проделанных итераций алгоритма. Обычно чем больше итераций мы проведем, тем с большей вероятностью можем утверждать что данное число простое. Мы рассмотрим такие алгоритмы в следующих главах.

**Лемма 5.** *Простых чисел бесконечно много.*

*Доказательство.* Докажем от противного.

Допустим, что множество простых чисел-конечно. Тогда существует наибольшее из них. Обозначим его $n$.

Рассмотрим число следующего вида:

$$p = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot n = n!$$

Число $p$ - это произведение всех чисел от 1 до $n$. Докажем что $p+1$-простое. Так как, $2 \mid p \to 2 \nmid (p+1)$. Аналогично можно доказать, что $p+1$ не делится ни на какое другое число от 2 до $p$, из чего мы можем сделать вывод о том, что $p+1$- простое число. Простота $p+1$ противоречит нашему предположению, поэтому простых чисел бесконечно много. □

## 2.3 Деление и остатки

Относительно заданного числа $n$ все целые числа можно разбить на две группы- те которые кратны $n$, т.е. делятся на $n$, и те которые не делятся на $n$ без остатка. Большая часть теории чисел основанная на разделении последней группы на классы эквивалентности, в зависимости от того, что получается в остатке при делении на $n$.

Данное разбиение основанно на следующей теореме.

**Лемма 6** (О делении)**.** *Для любого целого числа $a$ и любого положительного целого $n$, существует единственная пара целых чисел $q$ и $r$, таких, что $0 \leq r < n$ и $a = qn + r$.*

Доказательство данной теоремы довольно тривиально, поэтому здесь она приведенная без него. Величина $q = \lfloor a/n \rfloor$ называется **частным** деления. Величина $r = a \ mod\ n$ называется **остатком от деления**. Таким образом, $n|a$, тогда и только тогда когда $a \ mod\ n = 0$.

В зависимости от того, чтому равны остатки чисел от деления на $n$ (*модули по n*), их можно разбить на $n$ классов эквивалентности. Класс эквивалентности по модулю **n**, в котором содержится целое число $a$ имеет следующий вид:

$$[a]_n = \{a + kn : k \in Z\}$$

Запись $a \in [b]_n$ означает, что $a \equiv b \ (mod\ n)$ Множество всех таких классво эквивалентности имеет вид:

$$\mathbf{Z}_n = [a]_n : 0 \leq a \leq n - 1$$

## 2.4 Общие делители и наибольшие общие делители

Число $c$ называется общим делителем чисел $a, b$, если $c$ делит одновременно и $a$, и $b$. Для любых двух чисел 1 является их общим делителем. Например для чисел 15 и 6 общими делителями служат $1, 3$. Важное свойство общих делителй заключается в том, что для всех целых чисел:

$$\textit{из } d \mid a \textit{ и } d \mid b \textit{ следует, что } \ d \mid (ax + by) \tag{2.1}$$

Максимальное из общих делителей двух чисел называется - их наибольим общим делителем. Мы будем обозначать его $gcd(a, b)$. В приведенном выше примере $gcd(15, 6) = 3$. Понятие наибольшего общего делителя является одним из основных в теории чисел и многие вещи основанны на свойствах наибольшего общего делителя. Приведем некоторые свйоства наибольшего общего делителя двух чисел.

$$gcd(a, b) = gcd(b, a) \tag{2.2}$$

$$gcd(a, b) = gcd(-a, b) \tag{2.3}$$

$$gcd(a, b) = gcd(|a|, |b|) \tag{2.4}$$

$$gcd(a, b) = |a| \tag{2.5}$$

$$gcd(a, ka) = a \forall k \in \mathbf{Z} \tag{2.6}$$

Сформулированная ниже теорема является довольно полезной и мы будем часто на нее ссылаться.

**Теорема 2.4.1.** *Если $a$ и $b$ произвольные целые числа, отличные от нуля, то величина $gcd(a, b)$ равна наименьшему положительному элементу множества $\{ax + by : x, y \in \boldsymbol{Z}\}$*

*Доказательство.* Обозначим через $s$ наименьшую положительную линейную комбинацию чисел $a$ и $b$, т.е. $s = ax + by$ для некоторых $x, y \in \mathbf{Z}$. Пусть $q = \lfloor a/s \rfloor$. Тогда имеем:

$$a \bmod s = a - qs = a - q(ax + by) = a(1 - qx) + b(-qy),$$

поэтому величина $a \bmod s$ также является линейной комбинацией чисел $a, b$. Имеет место соотношение

$$0 \leq a \bmod s \leq s.$$

Но поскольку, $s$-наименьшая из таких комбинаций, отсюда следует что $a \bmod s = 0$. Это означает, что $s|a$. Аналогично можно доказать и для $b$. Тем самым, мы показали что $s$ является общим делителем $a$ и $b$, т.е. $s|a$ и $s|b$. Справедливо равенство

$$gcd(a, b) \geq s.$$

Из (2.1) следует что

$$gcd(a, b)|s,$$

так как, $s$ линейная комбинация $a, b$. Из последнего следует, что

$$gcd(a, b) \leq s$$

Объединяя два соотнощения

$$gcd(a, b) \leq sugcd(a, b) \geq s$$

делаем вывод, что

$$s = gcd(a, b).$$

□

**Следствие 2.4.1.** *Для любых целых чисел $a$ и $b$ и произвольного неотрицательного числа $n$ справедливо соотношение:*

$$gcd(an, bn) = ngcd(a, b)$$

$$d|gcd(a, b)$$

**Следствие 2.4.2.** *Для всех положительных чисел $a, b, n$, из условия что $n|ab$ $gcd(a, n) = 1$ следует соотношение $n|b$.*

**Следствие 2.4.3.** *Для любых целых чисел $a$ и $b$ из соотношение $d|a$ и $d|b$ следует, что*

$$d|gcd(a, b)$$

Докажем еще одну важнейшую теорему, сформулированную в XVII веке Пьером Ферма и играющую одну из ключевых роле в теории чисел.

**Теорема 2.4.2** (Малая теорема **П.Ферма**). *Пусть $a, p$ - произвольные взаимно простые числа. Тогда, если $p$ - простое, то справедливо сравнение:*

$$a^{p-1} \equiv 1 \pmod p \tag{2.7}$$

*Доказательство.* Существуют разные подходы к доказательству данной теоремы. Мы рассмотри наиболее изящное и простое доказательство, основанное на теории групп и на теореме **Лагранжа**.

Пусть $\mathfrak{G}$ - конечная группа порядка $n$. Тогда По теореме **Лагранжа**, из того что порядок элемента $g \in \mathfrak{G}$ делит порядок группы, следует что $g^n = e$. Рассмотрим группу вычетов по модулю $p - Z_p$. Порядок данной группы - $p$. Ненулевые элементы $Z_p$ образуют группу по умножению-${Z_p}^*$. Порядок ${Z_p}^*$ очевидно, равен $p-1$. В данной групее порядок любого элемента, является делителем порядка группы, т.е. $p-1$. В итоге получаем что для всех элементов $k \in {Z_p}^*$, $k^{p-1} = e$. Из последнего вытекает доказательство теоремы.

$\square$

# Глава 3

# Теория кодирования

## Введение

В данной главе мы рассмотрим некоторые проблемы из теории передачи информации, а именно двоичное кодирование и декодирование сигналов, передаваемых по некоторому каналу с шумом. Типичная ситуация следующая: у нас есть последовательность символов, конечной длины, из некторого алфавита. Мы хотим передать данную последовательность по некоторому каналу с шумом и с ненулевой вероятностью $q$, каждый передаваемый символ будет принят ошибочно. Допустим, что мы передаем последовательность длины 10000знаков и $q = 0.01\%$. Даже при, такой, относительно небольшой вероятности ошибки, вероятность $P_0$ того, что наша последовательность, при прямой передачи символа за символом, будет передана абсолютно правильно будет следующей:

$$P_0 = (1 - 0.01)^{10000} \simeq 10^{-4.4} < 0.004\%$$

Данный результат вытекает из классической формулы Бернули, которую можно найти в любом учебнике по теории вероятностей. В дальнейшем, в целях удобства, мы будем пердполагать, что наш алфавит двоичный и состоит из двух символов

$$\Sigma = \{0, 1\}$$

. Все изложенное далее можно обобщить и на любой другой алфавит, содержащий произвольной количество элементов.

## 3.1 Кодирование

Во многих системах передачи информации, за ошибку даже в одном бите приходится дорого платить. Поэтому одной из главных задач, теории передачи информации является уменьшение вероятности искажения передаваемых данных. В этой главе мы рассмотрим эффективные методы увеличения надежности передачи информации, с помощью систематических кодов разного типа. Большая их часть принадлежит к классу *групповых* кодов, и основывается на теореме *Лагранжа.*

Идея, положенная в основу всех систематических кодов следующая: последовательности, подлежащие передачи, кодируются последовательностями большей длины. Приемник, на основе дополнительной информации, способен распознавать или исправлять ошибки, вызванные шумом. Принятая последовательность декодируется по определенной схеме в изначальную последовательность символов до кодирования.

**Определение 3.1.1.** *Двоичным* $(m, n)$*-кодом, называется пара, состоящая из схемы кодирования:*

$$E : 2^m \to 2^n,$$

*и схемы декодирования:*

$$D : 2^n \to 2^m,$$

*где* $2^n$*-это множество всех двоичных последовательностей длины* $n$*.*

Функции $E$è$D$ выбираются так, чтобы функция $H = E \diamond H \diamond D$, где $H$-функция ошибок, с вероятностью близкой к единице была тождественной.

Все коды можно разделить на два класса:
**Коды с обнаружением ошибок** и **Коды с исправлением ошибок.**

**Пример.** Простая схема кодирования основанна на проверки четности. Схема кодирования $E$ определяется следующим образом:

$$E : a_1 a_2 ... a_m \to b_1 b_2 ... b_m b_{m+1},$$

где,

$$b_i = a_i \text{ при } i \leq m,$$
$$b_{m+1} = 1 \text{ если } \sum_{i=1}^{m} a_i \text{-нечетная},$$
$$b_{m+1} = 0 \text{ иначе}.$$