НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

Модуль 1. Математические основы помехоустойчивого кодирования

Основные сведения из теории чисел, групп, колец, полей.

Иванов Ф. И.
к.ф.-м.н., доцент

Национальный исследовательский университет
«Высшая школа экономики»

12 июня 2020 г.

Операции на множестве

Рассмотрим произвольное множество M и бинарную операцию $*$, заданную на M.

Определение

Если $\forall a,b \in M$ выполняется $a * b \in M$ и $b * a \in M$, то говорят, что множество M замкнуто относительно операции $*$.

Определение

Говорят, что для операции $*$, заданной в M, существует обратная операция, если при любых $a \in M$ и $b \in M$ каждое из уравнений

$$a * x = b, x * a = b$$

имеет решение в M и при том единственное.

Без ограничения общности опустим знак операции $*$, перейдя, таким образом, к употреблению операции, которую будем называть умножением.

Определение группы - I

Определение

Непустое множество G называется группой, если выполняются следующие условия:

- *Множество замкнуто относительно некоторой операции.*
- *Операция ассоциативна: $(ab)c = a(bc)$.*
- *В G выполняется обратная операция.*

Группа называется коммутативной/абелевой, если всегда

$$ab = ba.$$

Пример некоммутативной группы

Группа $\mathbb{S}_n$ - симметрическая группа перестановок длины n с операцией суперпозиции. Всего перестановок $n!$. Суперпозиция двух перестановок π, ξ: $\eta = \pi \cdot \xi$ определяется как:

$$\eta = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi_1 & \pi_2 & \pi_3 & \dots & \pi_n \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \xi_1 & \xi_2 & \xi_3 & \dots & \xi_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \xi(\pi_1) & \xi(\pi_2) & \xi(\pi_3) & \dots & \xi(\pi_n) \end{pmatrix}$$

Операция суперпозиции некоммунтативна:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$

а

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

Определение группы - II

Определение

Непустое множество G называется группой, если выполняются следующие условия:

1. *Множество G замкнуто относительно некоторой операции.*
2. *Операция ассоциативна*
3. *Для каждого $a \in G$ существует нейтральный элемент $e \in G$: $ae = ea = a$ т.е. такой элемент, который оставляет элемент a неизменным.*
4. *Для каждого $a \in G$ существует обратный элемент $a^{-1} \in G$: $a^{-1}a = aa^{-1} = e$.*

Вместо записи $aa \dots a$ будем писать a^n. Вместо e будем писать 0 или 1 в зависимости от контекста.

Порядок элемента, порядок группы

Определение

Число элементов конечной группы G называется порядком группы, обозначение $o(G)$.

Определение

Пусть G - конечная группа и $a \in G$, тогда найдется такое $n > 0$, что $a^n = 1$. Наименьшее среди таких n назовем порядком элемента a.

Теорема

Если элемент a имеет порядок n, то:

1. *Все элементы $1, a, a^2, \ldots, a^{n-1}$ различны.*
2. *Всякая другая степень элемента a, положительная или отрицательная, равна одному из этих элементов.*

Примеры групп

1. Аддитивная группа целых чисел $\mathbb{Z}$.
2. Аддитивная группа всех рациональных чисел $\mathbb{Q}$.
3. Аддитивная группа действительных чисел $\mathbb{R}$.
4. Аддитивная группа всех четных чисел.
5. Все отличные от нуля рациональные числа образуют группу по умножению: мультипликативную группу рациональных чисел.
6. Мультипликативная группа классов вычетов приведенной системы по модулю m.
7. Группа всех p^n векторов длины n с основанием p и операцией поразрядного сложения по модулю p.

Подгруппы

Определение

Подмножество H группы G называется подгруппой этой группы, если оно само является группой относительно операции, определенной в группе G.

Для установления факта, является ли подмножество H элементов группы G подгруппой группы G, достаточно проверить:

1. Замкнутость множества H относительно данной операции.
2. Содержится ли в H вместе с a также и a^{-1} (автоматом для конечных подгрупп)

Подгруппы циклической группы

Определение

Группа G называется циклической, если существует такой элемент $a \in G$, что любой $b \in G$ имеет вид $b = a^i$, $i \in \mathbb{N} \cup \{0\}$.

Теорема

Подгруппа циклической группы сама циклическая. Она состоит либо из единицы группы, либо из всех степеней элемента a^l, имеющего наименьший возможный положительный показатель l, (где a — элемент, порождающий всю исходную группу G.)

Теорема

Числа l такие, что $n = pl$ и только они являются порождающими элементами циклических подгрупп H циклической группы G.

Порождающие элементы циклической группы

Определение

Элемент a называется порождающим или первообразным элементом группы G.

Теорема

Вместе с элементом a порождающими элементами группы будут все такие степени a^m, что $(m, n) = 1$, т. е. циклическая группа имеет $\phi(n)$ порождающих элементов, где $\phi(x)$ — функция Эйлера.

Пример циклической группы

Пусть группа G есть циклическая группа порядка $n = 63$, и пусть β — её порождающий (первообразный, образующий) элемент. Числа 3, 7, 9, 21 — суть делители порядка группы G. Подгруппа $H_3 \subset G$ порождается элементом β^3. Имеем

$$H_3 = \{\beta^3, \beta^6, \beta^9, \beta^{12}, \beta^{15}, \beta^{18}, \beta^{21}, \beta^{24}, \beta^{27}, \beta^{30},$$

$$\beta^{33}, \beta^{36}, \beta^{39}, \beta^{42}, \beta^{45}, \beta^{48}, \beta^{51}, \beta^{54}, \beta^{57}, \beta^{60}, \beta^{63} = 1\}.$$

В свою очередь

$$H_{21} \subset H_3,\ H_9 \subset H_3, \text{ где } H_9 = \{\beta^9, \beta^{18}, \beta^{27}, \beta^{36}, \beta^{45}, \beta^{54}, \beta^{63} = 1\},$$

$$H_{21} = \{\beta^{21}, \beta^{42}, \beta^{63} = 1, \}.$$

Далее

$$H_{21} \subset H_7 \subset G,\ H_7 = \{\beta^7, \beta^{14}, \beta^{21}, \beta^{28}, \beta^{35}, \beta^{42}, \beta^{49}, \beta^{56}, \beta^{63} = 1\}.$$

В четырёх подгруппах содержится 27 различных элементов. Так как $\varphi(63) = 36$, то остальные 36 элементов являются порождающими (первообразными, образующими) элементами группы G, и потому никакой истинной подгруппе принадлежать не могут.

Смежные классы. Разложение группы по подгруппе

Пусть $H = h_1, h_2, ..., h_i, ...$ подгруппа группы G, и $a \in G$.

Определение

Множество $aH = \{ah_1, ah_2, ..., ah_i, ...\}$ *называется левосторонним (левым) смежным классом группы* G*, по подгруппе* H*. Множество* Ha *называется правосторонним, (правым) смежным классом группы* G*, по подгруппе* H*.*

Рассмотрим последовательность:

$$a_0H, a_1H, a_2H, ..., a_jH, ...,$$

где $a_0 \in H, a_i \notin H, i \geq 1$

Теорема

Всякий смежный класс определяется любым своим элементом.

Смежные классы. Разложение группы по подгруппе

Теорема

Утверждения о смежных классах:

- *Смежные классы либо не пересекаются, либо совпадают. Это значит, что при заданной подгруппе $H \subset G$ каждый элемент $a \in G$ принадлежит в точности одному смежному классу.*
- *Все смежные классы равномощны*
- *Два элемента a и b принадлежат одному и тому же смежному классу тогда и только тогда, когда $a^{-1}b \in H$.*
- *За исключением самой подгруппы H смежные классы по ней не являются группами.*

Вся группа G распадается на непересекающиеся смежные классы по подгруппе H.

$$G = a_0H \cup a_1H \cup a_2H \cup ... \cup a_jH \cup ...,$$

Теорема Лагранжа

Определение

Число различных смежных классов в разложении группы G по подгруппе H называется индексом подгруппы H в группе G. Обозначение: $[G : H]$.

Теорема

$o(G) = o(H) * [G : H]$

Следствие

- *Порядок подгруппы конечной группы есть делитель порядка группы.*
- *Порядок элемента конечной группы есть делитель порядка группы.*
- *Группа, порядок которой есть простое число, является циклической.*

Кольцо

Определение

Кольцом называется такая система элементов K с определёнными в ней сложением $a+b$ и умножением $a \cdot b$, что:

1. $(K,+)$ - *абелева группа*
2. *Умножение ассоциативно*
3. *Сложение и умножение связаны законами дистрибутивности:*

$$a(b+c) = ac + bc, (b+c)a = ba + ca$$

Следствие

1. *Дистрибутивность вычитания:* $a(b-c) = ab - ac$
2. *Умножение на* 0*:* $a * 0 = a(b-b) = ab - ab = 0$

Делители нуля

Известно, что $a * 0 = 0$, однако в общем случае можно выбрать $a,b \neq 0$, $a,b \in K$: $ab = 0$. Такие a,b называют делителями нуля.

Пример

Пусть $m = ab$, $a,b > 1$. Рассмотрим кольцо классов вычетов по модулю m. Выберем два элемента: $m_1 = a + mT_1$, $m_2 = b + mT_2$, тогда

$$ab = (a + mT_1)(b + mT_2) = mT_3 \equiv 0 \mod m$$

Определение

Кольцо без делителей нуля называется областью целостности.

Поле

Определение

Если отличные от нуля элементы коммутативного кольца образуют группу по умножению, то это кольцо называется полем.

Теорема

Поле не имеет делителей нуля.

Теорема

Конечная область целостности есть поле.

Теорема

Кольцо классов вычетов по модулю m будет полем тогда и только тогда, когда m простое число.

Примеры полей

1. Поле вещественных чисел $\mathbb{R}$, поле рациональных чисел $\mathbb{Q}$, поле комплексных чисел $\mathbb{C}$.
2. Поле классов вычетов по простому модулю p будем обозначать символом $GF(p)$. Иначе говоря, полем $GF(p)$ является полная система неотрицательных вычетов по модулю p, и операции сложения и умножения чисел $0, 1, 2, ..., p-1$ выполняются по модулю p.

Линейное векторное пространство

Определение

Линейным векторным пространством над полем F называется множество V векторов, удовлетворяющее условиям:

- *Множество V является аддитивной абелевой группой.*
- *Для любых $c \in F$ и $v \in V$ имеет место $cv \in V$.*
- *Выполняются дистрибутивные законы, т.е. если $c \in F; u,v \in V$, то $c(u+v) = cu + cv$, и если $c,d \in F; v \in V$, то $(c+d)v = cv + dv$.*
- *Умножение ассоциативно, т.е. $(cd)v = c(dv)$.*

Определение

Подмножество векторов A пространства V называется подпространством, если в нем выполняются условия определения пространства.

Базис и размерность линейного пространства

Пусть $A \subset V$ есть подпространство пространства V.
Векторы $v_1, v_2, ..., v_k \in A$ называются линейно зависимыми над полем F, если найдутся такие не все равные нулю элементы $a_1, a_2, ..., a_k \in F$, что

$$a_1 v_1 + a_2 v_2 + ... + a_k v_k = 0.$$

В противном случае векторы $v_1, v_2, ..., v_k \in A$ называются линейно независимыми. Максимальное число k линейно независимых векторов подпространства A называется его размерностью, а сама совокупность этих векторов называется базисом подпространства.