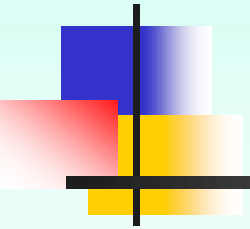
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек. 11 2022 КІБ-19

АБСТРАКТНАЯ АЛГЕБРА

Раздел математики, изучающий алгебраические системы (алгебраические структуры), такие как:

- группы,
- кольца,
- поля,

модули, решётки, а также отображения между такими структурами.

Группа

G Множество *S*, Операция ●

1. Замкнутость
2. Ассоциативность
3. Существование нейтрального элемента
4. Существование инверсии

АБЕЛЕВА *5. Коммутативность*

Бинарная операция

Бинарная операция $\circ$ – это некоторая функция

f: $S \circ S \to S$

Здесь S - некоторое множество.

$$S = \mathbb{R} \to f1(x, y) = x + y; f2(x, y) = x * y$$

Просто пишем z $= x + y; z = x * y$

$$S = \mathbb{Z}_n \to f1(x, y) = (x + y) mod\ n$$
$$S = \mathbb{Z}_n \to f2(x, y) = (x * y) mod\ n$$

Просто пишем z $= x + y; z = x * y$

Символы операций ***произвольны, можно использовать любой! НО ТАК ПРИНЯТО!***

Аддитивная бинарная операция

Бинарная операция $+$, Множество S .

Если удовлетворяет свойствам:

1. Замкнутости

$$\forall\, a, b \in S, :\ (a + b) \in S$$

2. Ассоциативности

$$\forall\, a, b, c\ \in S :\quad a + (b + c) = (a + b) + c$$

3. **Существования нейтрального элемента 0**

$$e = 0:\ \ a + 0 = 0 + a = a$$

4. **Существование инверсии**

$$\forall\, a \in S, : \exists b \in S :\ a + b = e, \qquad b = -a$$

– обратный (противоположенный) элемент.

5. **Коммутативности**

$$\forall\, a, b \in S:\ \ (a + b) = (b + a)$$

То это аддитивная бинарная операция.

Мультипликативная бинарная операция

Бинарная операция $\times$. Множество S .

Если удовлетворяет свойствам:

1. Замкнутости

$$\forall\, a, b \in S, :\ (a \times b) \in S$$

2. Ассоциативности

$$\forall\, a, b, c\ \in S :\quad a \times (b \times c) = (a \times b) \times c$$

3. **Существования нейтрального элемента 1**

$$e = 1:\ \ a \times 1 = 1 \times a = a$$

4. **Существование инверсии**

$$\forall\, a \in S, : \exists b \in S :\ a \times b = e, \qquad b = a^{-1}$$

– обратный (противоположенный) элемент.

5. **Коммутативности**

$$\forall\, a, b \in S:\ \ (a \times b) = (b \times a)$$

То - мультипликативная бинарная операция.

Операция возведения в степень

Множество S . Операция $\circ$ - **ассоциативна!**

Возведение в степень

$$a \in S, : (a \circ a \circ a \circ a \circ \cdots \circ a) \in S$$

n раз !!

Аддитивная операция

$$(a + a + a + a + \cdots + a) = n\,a$$

Мультипликативная операция

$$(a \times a \times a \times a \times \cdots \times a) = a^n$$

Свойства

$$a^n \circ a^m = a^{n+m} \qquad a^{n^m} = a^{n*m}$$

Группа

Группа G есть пара $\langle S, \circ \rangle$, состоящая из множества S (элементов группы) и $\circ$ - бинарной операции, удовлетворяющая условиям

1. Замкнутость

$$\forall\, a, b \in S, : \ (a \circ b) \in S$$

2. Ассоциативность

$$\forall\, a, b, c \ \in S : \quad a \circ (b \circ c) = (a \circ b) \circ c$$

3. **Существование нейтрального элемента (обладает единицей, единичный элемент)**

$$\exists e \in S \ : \ \forall\, a \in S : \quad a \circ e = e \circ a = a$$

4. **Существование инверсии**

$$\forall\, a \in S, : \exists a^{-1} \in S : \ a \circ a^{-1} = e$$

5. **Коммутативность (абелева группа)**

$$\forall\, a, b \in S: \ (a \circ b) = (b \circ a)$$

Группа

Группа G называется **конечной**, если множество S состоит из конечного числа элементов. В противном случае группа G называется бесконечной.

Порядок конечной группы G - количество элементов S. Обозначается $|G|$.

Аддитивная группа $\langle S, + \rangle$.
Мультипликативная группа $\langle S, \times \rangle$.
Группа с операцией $\otimes$ $\langle S, \otimes \rangle$.
Группа с некоторой операцией $\therefore$ $\langle S, \therefore \rangle$.

Группа. Пример

$G = \langle \mathbb{Z}, + \rangle$. Это группа?

$\mathbb{Z} = \{\dots -2, -1, 0, 1, 2, \dots\}$. Пусть $x, y, z \in \mathbb{Z}$.

1. Замкнутость

$$(x + y) \in \mathbb{Z}$$

2. Ассоциативность

$$[x + (y + z)] = [(x + y) + z]$$

3. Существование нейтрального элемента

$$e = 0 \in S, \qquad x + 0 = 0 + x = x$$

4. Существование инверсии (аддитивная!)

$$x + (-x) = e = 0$$

5. Коммутативность

$$(x + y) = (y + x)$$

Аддитивная бесконечная абелева группа!

Группа. Пример

$G = \langle \mathbb{Z}_n, + \rangle$. Это группа?

$\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$. Пусть $x, y, z \in \mathbb{Z}_n$.

1. Замкнутость

$$(x + y) mod\ n \in \mathbb{Z}_n$$

2. Ассоциативность

$$[x + (y + z)] mod\ n = [(x + y) + z] mod\ n,$$

3. Существование нейтрального элемента

$$e = 0 \in S, \qquad x + 0 = 0 + x = x$$

4. Существование инверсии (аддитивная!)

$$x + (-x) = e = 0$$

5. Коммутативность

$$(x + y) mod\ n = (y + x) mod\ n$$

Аддитивная конечная абелева группа, $|G|=n$

Группа. Пример

$G = \langle \mathbb{Z}_n, \times \rangle$. А это группа?

$\mathbb{Z}_n = \{0, 1, 2, \dots, (n-1)\}$. Пусть $x, y, z \in \mathbb{Z}_n$.

1. Замкнутость

$$(x \times y) mod\ n \in \mathbb{Z}_n$$

2. Ассоциативность

$$[x \times (y \times z)] mod\ n = [(x \times y) \times z] mod\ n,$$

3. Существование нейтрального элемента

$e = 0 \in S$, $x \times 0 = 0 \times x = x$!! НЕТ

$e = 1 \in S$, $x \times 1 = 1 \times x = x$!! ДА

4. Существование инверсии (мультипликативной)

$x \times (x^{-1}) = e = 1$!!!! не для всех n

5. Коммутативность

$$(x \times y) mod\ n = (y \times x) mod\ n$$

Мультипликативная конечная абелева группа, только когда n - простое число!!!

Группа. Пример

Пусть $\boldsymbol{S = \{F, T\}}$. Группа $\boldsymbol{B = \langle \{F, T\}, \oplus \rangle}$.
Операция $\oplus$ задана как

	F	T
F	F	T
T	T	F

Это группа ??? Какая?

1. Замкнутость

$$(x \oplus y) \in S$$

2. Ассоциативность

$$[x \oplus (y \oplus z)] = [(x \oplus y) \oplus z]$$

3. Существование нейтрального элемента

$$e = F \in S, \qquad x \oplus F = F \oplus x = x$$

4. Существование инверсии

$$x = F, x^{-1} = T, \qquad x = T, x^{-1} = F$$

5. Коммутативность

$$(x \oplus y) = (y \oplus x)$$

Конечная абелева группа!

Группа. Пример

Пусть $S = \{F, T\}$. Группа $B = \langle \{F, T\}, \oplus \rangle$.
Операция $\oplus$ задана как

	F	T
F	F	T
T	T	F

ТАБЛИЦА КЭЛИ

Операция «ИСКЛЮЧАЮЩАЯ ИЛИ»

1. Замкнутость

$$(x \oplus y) \in S$$

2. Ассоциативность

$$[x \oplus (y \oplus z)] = [(x \oplus y) \oplus z]$$

3. Существование нейтрального элемента

$$e = F \in S, \qquad x \oplus F = F \oplus x = x$$

4. Существование инверсии

$$x = F, x^{-1} = T, \qquad x = T, x^{-1} = F$$

5. Коммутативность

$$(x \oplus y) = (y \oplus x)$$

Конечная абелева группа!

Группа. Пример

Пусть $S = \{A, B, C, D\}$
Операция $\circ$ задана как

	A	B	C	D
A	A	B	C	D
B	B	C	D	A
C	C	D	A	B
D	D	A	B	C

Это группа ???

Группа. Пример

Пусть $S = \{A, B, C, D\}$

Операция $\circ$ задана как

	A	B	C	D
A	A	B	C	D
B	B	C	D	A
C	C	D	A	B
D	D	A	B	C

1. Замкнутость

$$(x \circ y) \in S$$

2. Ассоциативность

$$[A \circ (B \circ C)] = [(A \circ B) \circ C], \ldots.$$

3. Существование нейтрального элемента

$$e = A \in S, \qquad x \oplus A = A \oplus x = x$$

4. Существование инверсии

$$x = A, \ x^{-1} = A, \qquad x = B, x^{-1} = D, \ x = C, x^{-1} = C$$

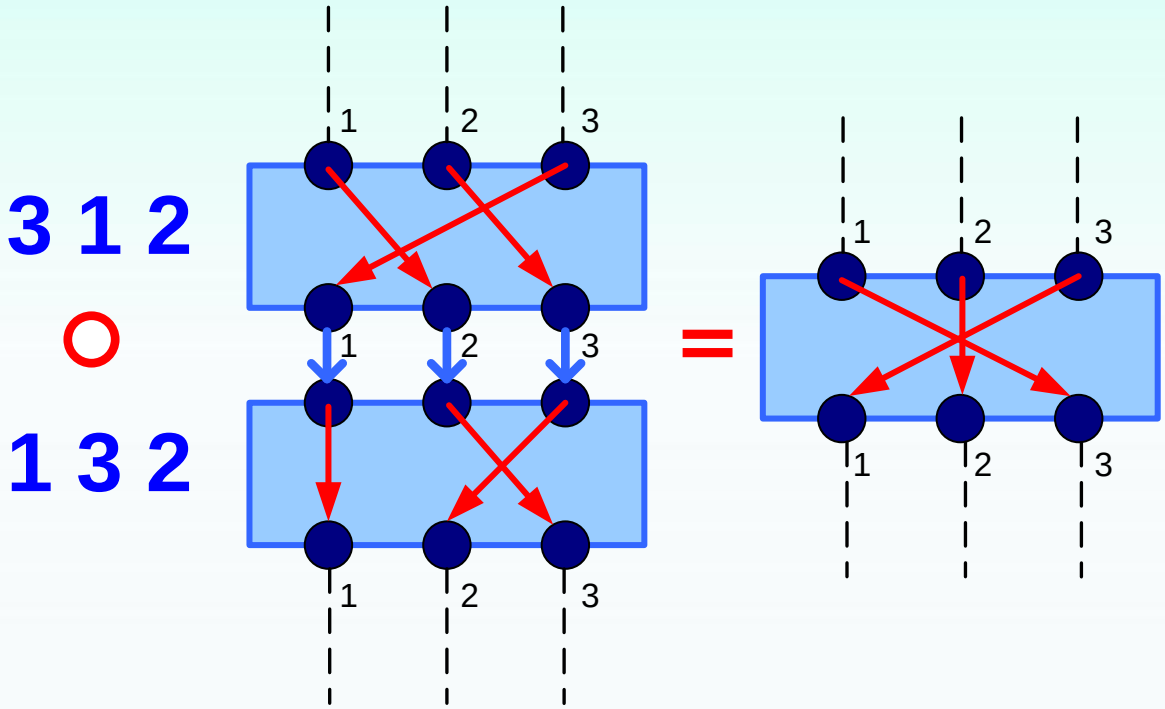
5. Коммутативность

$$(x \oplus y) = (y \oplus x)$$

Конечная абелева группа!

Группа перестановок. Пример

Пусть $S =$
$\{[1\ 2\ 3], [1\ 3\ 2], [\ 2\ 1\ 3], [2\ 3\ 1], [3\ 1\ 2\ ], [3\ 2\ 1]\}$
Элементы множества есть **перестановки.**
Операция $\circ$ есть « ***композиция*** ». Например



Группа перестановок

Пусть $S =$
$\{[1\ 2\ 3], [1\ 3\ 2], [\ 2\ 1\ 3], [2\ 3\ 1], [3\ 1\ 2\ ], [3\ 2\ 1], \}$
Операция $\circ$ задана как:

Первая перестановка

	1 2 3	1 3 2	2 1 3	2 3 1	3 1 2	3 2 1
1 2 3	1 2 3	1 3 2	2 1 3	2 3 1	3 1 2	3 2 1
1 3 2	1 3 2	1 2 3	2 3 1	2 1 3	3 2 1	3 1 2
2 1 3	2 1 3	3 1 2	1 2 3	3 2 1	1 3 2	2 3 1
2 3 1	2 3 1	3 2 1	1 3 2	3 1 2	1 2 3	2 1 3
3 1 2	3 1 2	2 1 3	3 2 1	1 2 3	2 3 1	1 3 2
3 2 1	3 2 1	2 3 1	3 1 2	1 3 2	2 1 3	1 2 3

Вторая перестановка

Результат операции композиции

Это группа?

Порядок Группы

Порядок $\mathbf{Ord(G)}$ группы $G = \langle S, \circ \rangle$ – мощность множества S группы. То есть $\mathbf{Ord}(G) = \|S\|$. Для конечного S порядок группы есть количество элементов множества S: $\mathbf{Ord}(G) = |S|$.

Порядок Элемента

Порядок $ord\,(a)$ элемента a в группе G - наименьшее целое положительное число $n > 0$, такое что $a^n = e$, если такое существует. Тогда $ord\,(a) = n$.
Если такое n не существует $ord\,(a) = \infty$.

Порядок элемента → характеризует «***расстояние***» элемента от нейтрального элемента.

Порядок элемента

Пример $G = \langle \mathbb{Z}_n, + \rangle$. $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$.

$Ord(G) = 6$

a=0: $0^0 mod\ 6 = 0 \rightarrow H_0 = \langle \{0\}, + \rangle$

a=1: $1^0 mod\ 6 = 0$, $1^1 mod\ 6 = 1$, $1^2 mod\ 6 = 2$, $1^3 mod\ 6 = 3$, $1^4 mod\ 6 = 4$, $1^5 mod\ 6 = 5 \rightarrow H_1 = \langle \{0,1,2,3,4,5\}, + \rangle = G$

a=2: $2^0 mod\ 6 = 0$, $2^1 mod\ 6 = 2$, $2^2 mod\ 6 = 2$

$\rightarrow H_2 = \langle \{0,2,4\}, + \rangle$

a=3: $3^0 mod\ 6 = 0$, $3^1 mod\ 6 = 3 \rightarrow H_3 = \langle \{0,3\}, + \rangle$

a=4: $4^0 mod\ 6 = 0$, $4^1 mod\ 6 = 4$, $4^2 mod\ 6 = 2 \rightarrow H_4 = \langle \{0,2,4\}, + \rangle$

a=5: $5^0 mod\ 6 = 0$, $5^1 mod\ 6 = 5$, $5^2 mod\ 4 = 2$, $5^3 mod\ 6 = 3$, $5^4 mod\ 6 = 2$, $5^5 mod\ 6 = 1 \rightarrow H_4 = \langle \{0,1,2,3,4,5\}, + \rangle$

$ord(0) = 1, ord(1) = 6, ord(2) = 3$

$ord(3) = 2, ord(4) = 3, ord(5) = 6$

Порядок элемента суть порядок группы, которую он генерирует.

Кольцо

Кольцо R есть тройка $\langle S, \circ, \therefore \rangle$, состоящая из множества S (элементов группы) и ДВУХ операций:

$\circ$ - бинарная, удовлетворяющая условиям замкнутости, ассоциативности, существования нейтрального элемента, существования инверсии, коммутативности (относительно $\circ$ - абелева группа). Нейтральный элемент относительно $\circ \rightarrow \mathbf{0}$.

$\therefore$ - бинарная, удовлетворяющая условиям замкнутости, ассоциативности, коммутативности. Нейтральный элемент относительно $\therefore \rightarrow \mathbf{1}$, причем **1 не есть 0** .

Существование инверсии **не требуется!**

Кольцо

Кроме того:

3. Коммутативность

$$\forall\, a, b \in S\colon\ (a \therefore b) = (b \therefore a)$$

4. Дистрибутивность

$$\forall\, a, b, c \in S\colon\ (a \therefore (b \circ c)) = (a \therefore b) \circ (a \therefore c)$$

Такие кольца называются **коммутативными.**

Кольцо. Пример

Пусть $S = \{F, T\}$. Кольцо $B = \langle \{F, T\}, \oplus, \otimes \rangle$.

Операция $\oplus$:

	F	T
F	F	T
T	T	F

Операция $\otimes$:

	F	T
F	F	F
T	F	T

Это Кольцо ???

1. Замкнутость

$$(x \otimes y) \in S$$

2. Ассоциативность

$$[x \otimes (y \otimes z)] = [(x \otimes y) \otimes z]$$

3. Существование нейтрального элемента

$$1 = T \in S, \qquad x \otimes T = T \otimes x = x$$

4. Существование инверсии

5. Коммутативность

$$(x \otimes y) = (y \otimes x)$$

6. Дистрибутивность

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$$

Кольцо!

Поле

Поле *F* это коммутативное кольцо *R* если ненулевые элементы кольца образуют группу относительно операции $\therefore$.

Или – вторя операция удовлетворяет всем 5 свойствам, определенным для первой операции, за исключением того, что нейтральный элемент первой операции не имеет инверсии относительно второй операции.

Сравнение структур

Алгебраическая структура	Операции	Наборы целых
Группа	$(+ \ -)$ или $(\times \ \div)$	$\mathbb{Z}_n$ или $\mathbb{Z}_n^*$
Кольцо	$(+ \ -)$ и $(\times)$	$\mathbb{Z}$
Поле	$(+ \ -)$ и $(\times \ \div)$	$\mathbb{Z}_p$

Поле Галуа

В криптографии:

поле Галуа $GF(p^n)$

- конечное поле с p^n элементами, где p - простое число, $n \in \mathbb{Z}_n \backslash 0$.

ЛИТЕРАТУРА

Нечаев В.И. Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.:, ВШ., 1999.- 109 с.

Введение в криптографию. **Под общ. ред. В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012 – 348 с. ISBN 978-5-4439-0026-1

ЛИТЕРАТУРА

Венбо Мао. Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7 (рус.)

Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. – Москва: Вильямс, 2016. 1024 с.

ЛИТЕРАТУРА

Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.

Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.

A. Menezes, P. van Oorschot, S. Vanstone.

Handbook of Applied Cryptography.- CRC Press, 1996.

END # 11