КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Практическая работа 5

Математические основы криптографии: исследование алгебраических структур

Данный материал демонстрирует разбор задания, посвященного исследованию абстрактных алгебраических структур.

Будем говорить, что на множестве X задана алгебраическая операция $*$, если любой упорядоченной паре элементов $x, y \in X$ поставлен в соответствие однозначно определенный элемент $z \in X$, который обозначается $z = x * y$. Множество X с заданной на нем алгебраической операцией $*$ будем называть алгебраической структурой и обозначать $(X; *)$.

Выполнение задания включает исследование пяти свойств, которыми может обладать алгебраическая структура:

- свойство ассоциативности;
- существование нейтрального элемента;
- существование обратимых элементов;
- свойство коммутативности;
- свойство квазигруппы.

В каждом случае необходимо привести доказательство выполнения свойства либо опровергнуть его с помощью контрпримера.

Пример 1.

Изучить все свойства алгебраической структуры $(\mathbb{R};*)$, где $a * b = 3a - 2b$, $\forall a, b \in \mathbb{R}$. Установить, является ли данная структура группой.

Решение.

Сначала проверим, действительно ли операция $*$, заданная на множестве $\mathbb{R}$, является алгебраической. Для этого необходимо установить наличие трех признаков алгебраической операции: всюдуопределенности, однозначности и замкнутости. Отметим, что операция $*$ построена на основе известных нам операций умножения и вычитания, определенных на множестве $\mathbb{R}$. Соответственно, при исследовании операции $*$ необходимо исходить из свойств операций умножения и вычитания.

Итак, очевидно, что для любой упорядоченной пары $a, b \in \mathbb{R}$ можно выполнить следующую последовательность действий:

(1) умножить первый элемент пары на число 3, получив новое число $a' \in \mathbb{R}$;

(2) умножить второй элемент пары на число 2, получив новое число $b' \in \mathbb{R}$;

(3) вычесть из числа a' число b', получив новое число $c \in \mathbb{R}$.

Не существует таких значений $a, b \in \mathbb{R}$, для которых перечисленная последовательность действий была бы невозможна. Следовательно, всюдуопределенность имеет место.

Выполнение действий (1)–(3) для данной пары $a, b \in \mathbb{R}$ приведет к получению однозначно определенного значения $c \in \mathbb{R}$. Выполнив перечисленные действия дважды для данной пары $a, b \in \mathbb{R}$, невозможно получить значения $c_1 \in \mathbb{R}$ и $c_2 \in \mathbb{R}$, такие, что $c_1 \neq c_2$. Это следует из свойств операций умножения и вычитания, определенных на множестве $\mathbb{R}$. Значит, операция $*$ обладает признаком однозначности.

Наконец, для любой пары действительных чисел a и b, число $c = a * b$ всегда будет действительным. Следовательно признак замкнутости также имеет место.

Таким образом, операция $*$, определенная на множестве $\mathbb{R}$, является алгебраической, и множество $\mathbb{R}$ является алгебраической структурой относительно операции $*$.

Теперь последовательно проверим, обладает ли данная алгебраическая операция известными нам свойствами.

Начнем со свойства *ассоциативности*. Алгебраическая операция $*$, заданная на множестве $\mathbb{R}$, является ассоциативной, если для любой тройки элементов $x, y, z \in \mathbb{R}$ выполняется соотношение $x * (y * z) = (x * y) * z$.

Чтобы проверить, выполняется ли приведенное соотношение в нашем примере, раскроем левую его часть для данной операции $*$, затем — правую часть и сопоставим результат. Если полученные выражения будет тождественно равны, то свойство ассоциативности выполняется. В противном случае приведем контрпример, опровергающий данное свойство.

$x * (y * z) = x * (3y - 2z) = 3x - 2(3y - 2z) = 3x - 6y + 4z.$

$(x * y) * z = (3x - 2y) * z = 3(3x - 2y) - 2z = 9x - 6y - 2z.$

Очевидно, что полученные выражения не тождественны друг другу. Приведем контрпример для свойства ассоциативности.

Пусть $x = 1, y = 2, z = -1.$

Тогда

$x * (y * z) = 3 \cdot 1 - 6 \cdot 2 + 4 \cdot (-1) = -13,$

$(x * y) * z = 9 \cdot 1 - 6 \cdot 2 - 2 \cdot (-1) = -1.$

Таким образом, существует как минимум одна тройка элементов $x, y, z \in \mathbb{R}$ для которой соотношение $x * (y * z) = (x * y) * z$ не выполняется. Следовательно, операция $*$ не является ассоциативной.

Теперь проверим наличие в алгебраической структуре $(\mathbb{R}; *)$ нейтрального элемента. Предположим, что существует число $e \in \mathbb{R}$, такое, что $x * e = e * x = x \ \forall x \in \mathbb{R}$. Причем элемент, обладающий указанным свойством, должен быть единственным. Раскроем левую данного выражения: $x * e = x,\ 3x - 2e = x,\ e = x$. Очевидно, что для разных значений $x \in \mathbb{R}$ будут получены разные значения e. Это свидетельствует о том, что нейтрального элемента в алгебраической структуре $(\mathbb{R}; *)$ не существует. И раскрывать правую часть соотношения, определяющего свойство существования нейтрального элемента, уже нет необходимости.

Поскольку алгебраическая структура $(\mathbb{R}; *)$ не содержит нейтрального элемента, то и обратимых элементов в ней нет, так как само понятие обратимости элементов алгебраической структуры определяется через понятие нейтрального элемента.

Осталось проверить два свойства.

Алгебраическая операция $*$ на множестве $\mathbb{R}$ называется коммутативной, если для любых элементов $x, y \in \mathbb{R}$ справедливо равенство $x * y = y * x$. Очевидно, что необходимо раскрыть обе части данного равенства и сопоставить их друг с другом:

$x * y = 3x - 2y$,

$x * y = 3y - 2x$.

Полученные выражения не тождественны друг другу. Поэтому подберем контрпример, опровергающий коммутативность операции $*$.

Пусть $x = 3, y = 5$.

Тогда

$x * y = 3 \cdot 3 - 2 \cdot 5 = -1$,

$x * y = 3 \cdot 5 - 2 \cdot 3 = 9$.

Таким образом, существует как минимум одна пара элементов $x, y \in \mathbb{R}$ для которой соотношение $x * y = y * x$ не выполняется. Следовательно, операция $*$ не является коммутативной.

Теперь проверим последнее свойство.

Алгебраическая структура $(\mathbb{R}; *)$ называется квазигруппой, если для любых $a, b \in \mathbb{R}$ однозначно разрешимы уравнения $a * x = b$ и $y * a = b$.

Проверим однозначную разрешимость этих уравнений для данной операции $*$.

Начнем с первого уравнения. Раскроем его, после чего выразим неизвестное x: $a * x = b$, $3a - 2x = b$, $x = \frac{3a-b}{2}$. Очевидно, что выражение $x = \frac{3a-b}{2}$ имеет смысл для любой пары действительных чисел $a, b \in \mathbb{R}$ и, кроме того, определено вполне однозначно. Таким образом, первое уравнение является однозначно разрешимым для любых $a, b \in \mathbb{R}$.

Аналогичным образом поступим со вторым уравнением: $y * a = b$, $3y - 2a = b$, $y = \frac{2a+b}{3}$. Полученное выражение имеет смысл для любой пары действительных чисел и не несет в себе неоднозначности.

Таким образом, алгебраическая структура $(\mathbb{R}; *)$ является квазигруппой.

Наконец, ответим на последний вопрос задания: является ли алгебраическая структура $(\mathbb{R}; *)$ группой? Группа — это алгебраическая структура, которая одновременно является полугруппой и квазигруппой. $(\mathbb{R}; *)$ является квазигруппой, но не является полугруппой, так как операция $*$ не обладает свойством ассоциативности. Следовательно, алгебраическая структура $(\mathbb{R}; *)$ группой не является.

Пример 2. На некотором, пока не определенном, числовом множестве введем нестандартное умножение $x \otimes y = x+y-x-y$. Выяснить свойства операции $\otimes$.

Решение. Если множество замкнуто относительно стандартных операций + и •, оно замкнуто и относительно $\otimes$.

Коммутативность операции очевидна.

Проверим **ассоциативность**. Для произвольных x,y,z запишем гипотетическое равенство (которое надо проверить): $(x \otimes y) \otimes z = x \otimes (y \otimes z)$ и в два шага развернем его левую и правую часть в соответствии с определением операции.

$(x \otimes y) \otimes z = (x+y-x \cdot y) \otimes z = (x+y-x \cdot y)+z-(x+y-x \cdot y) \cdot z = x+y+z-(x \cdot y+x \cdot z+y \cdot z)+x \cdot y \cdot z.$

$x \otimes (y \otimes z) = x \otimes (y+z-y \cdot z) = x+(y+z-y \cdot z)-x \cdot (y+z-y \cdot z) = x+y+z-(x \cdot y+x \cdot z+y \cdot z)+x \cdot y \cdot z.$

Видим, что операция $\otimes$ **ассоциативна**.

Для **нейтрального элемента e** должно при любом x быть

$x \otimes e = x+e-x \cdot e = x,$

откуда $e \cdot (1-x)=0$. Так как x - любое число, получаем, что e=0.

Для симметричного элемента $\bar{x}$ должно при любом x выполняться условие:

$$x \otimes \bar{x} = x + \bar{x} - x \cdot \bar{x} = e = 0$$

Откуда $\bar{x} \cdot (1-x)+x=0$

следовательно, $\bar{x}=\frac{x}{x-1}$.

Заключаем, что для существования симметричных элементов в базовом множестве должно быть выполнимо деление (т.е. это, как минимум, множество рациональных чисел Q), причем из этого множества надо исключить число 1 (а не 0, как в обычной арифметике).

ДОМАШНЕЕ ЗАДАНИЕ

1. Изучить все свойства алгебраической структуры $(\mathbb{R}; *)$, является ли группой алгебраическая структура $(\mathbb{R}; *)$, где операция

$x*y=x+y-x\cdot y$?

2. Изучить все свойства алгебраической структуры $(\mathbb{R}; *)$, является ли группой алгебраическая структура $(\mathbb{R}; *)$, где операция

$a*b=2a-3b+1$?

3. Нестандартное сложение чисел задается формулой $x \oplus y = x + y - 1$. Выясните свойства операции $\oplus$. Установить, является ли данная структура группой.