WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com

Foundational Mathematics for Web3 Builders

Implemented in RUST

Lecture 36

July 24, 2024

Algebraic Structures

11.1 Introduction

1. Modern cryptography relies heavily on algebraic structures, which serve as the mathematical foundation for a variety of cryptographic protocols and methods.
2. This chapter introduces some common algebraic structures such as groups, rings, and fields.
3. Understanding these structures and their features is critical for developing secure cryptographic systems and furthering the discipline of cryptography, particularly in the post-quantum age.

(1) Groups: Groups are algebraic structures made up of a set with a single binary operation that has four properties: closure, associativity, identity, and invertibility.

Definition 9

Let G be a nonempty set together with a binary operation $\circ : G \times G \to G$. The system $(G, \circ)$ is a group if it satisfies the following axioms:

$11 \equiv 0 + (1+2)$

$3 = 3$

$a \times b = 1$

a) For each $x \in G$ and $y \in G$, $x \circ y$ is an element of G. (Closure axiom);

$+1 = 1 \in \mathbb{Z}$

$-2, 2$

b) For all $x, y, z \in G$, $(x \circ y) \circ z = x \circ (y \circ z)$ (Associativity axiom);

$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ $\quad 4 \times a \neq 1$

$2, \frac{1}{2}$

$2 \times \frac{1}{2} = 1$

c) There is an identity element $e \in G$ such that for all $g \in G$, $e \circ g = g \circ e = g$ (Identity axiom);

$3 \times \frac{1}{3} = 1$

$\frac{1}{4} \times 4 = 1$

d) For each $a \in G$ there exists an element $b \in G$ such that $a \circ b = b \circ a = e$ (Existence of inverse axiom);

$2 \times a = 1$

$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, \dots\}$

The number of elements of a group G denoted by $|G|$ is called the order of the group. For instance, if G is a group containing n elements then we write $|G| = n$.

$|\mathbb{Z}|$

Definition 10

A group G is said to be infinite or of infinite order if it has an infinite number of elements, otherwise the group is finite or of finite order.

Definition 11

A group G is called Abelian or Commutative if it satisfies the additional property:

e) For all $g, h \in G$, $g \circ h = h \circ g$ (Commutativity axiom)

$g \times h =$

Groups not satisfying this property are said to be noncommutative or nonabelian.

$$\begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix} \times \begin{pmatrix} 1 & 4 \\ 8 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 8 & 2 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 1 & 3 \end{pmatrix}$$

25 12 10 16

- If the group's defined operation is addition, the group can support both addition and subtraction because subtraction is the additive inverse of addition.
- This is true for both multiplication and division. A group can support either addition/subtraction or multiplication/division operations, but not both at the same time.

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}$

Example 44

The set of integers $\mathbb{Z}$ under addition forms an abelian group, with 0 being the identity and $-a$ representing the inverse of $a \in \mathbb{Z}$.

$-3 + -2 = -2 + -3 = -5$ Commutative

Example 45

The set $n\mathbb{Z} = \{nz : n, z \in \mathbb{Z}\}$ under addition forms an abelian group, with 0 as the identity and $n(-z)$ as the inverse of nz.

$2\mathbb{Z} = \{\dots, -6, -4, -2, 0, 2, 4, \dots\}$

$N = \{0, 1, 2, 3, \cdots\}$

Example 46

The set of non-negative integers under addition is not an abelian group since there are no additive inverses for positive integers.

a group

Example 47

Let $B = \{\cdots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$.. Does B form a group under addition on $\mathbb{Z}$?

$4 + 3 = 7 \notin B$

$4 + 5 = 9 \notin B$

Not closed – Not a group

Solution

B does not form a group under addition since it is not closed under addition. For instance, $4 + 5 = 9 \notin B$. Notice that the rest of the group axioms are satisfied. That is, it has the identity element 0, every element has an inverse and associativity is satisfied.

$2 \times a = 1$

$-3 \times x = 1$

$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, \cdots\}$

Example 48

The set of integers under multiplication is not an abelian group as there are no inverses for any numbers other than ± 1.

Not a group

$A = \{-1, 1\}$ $\quad -1 \times 1 = -1 \in A$

Example 49

The set $\{-1, 1\}$ under multiplication is an abelian group, with 1 as the identity and -1 as its inverse.

Example 50

The set of rational numbers $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ under addition forms an abelian group, with 0 as the identity and $-\frac{a}{b}$ as the inverse of $\frac{a}{b}$.

$\frac{a}{b}$ A fraction number

$\frac{1}{2}, \frac{1}{3}, \frac{7}{1}, \frac{8}{1}$

$\mathbb{Z} =$

Example 51

The set of non-zero rational numbers $\mathbb{Q}^*$ under multiplication forms an abelian group, with 1 as the identity and $\frac{b}{a}$ as its inverse.

Example 52

The group of units in $M(\mathbb{R})$ is

$$GL(2, \mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$$

and is referred to as the general linear group of degree 2 over $\mathbb{R}$. It is an infinite non abelian group.

Example 53

Let $G = \{A, B, C, D\}$ where A, B, C and D are 2×2 matrices given by:

Cayley

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

and $D = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

$\times$	A	B	C	D
A				
B				
C				
D				

Does G form a group under multiplication?

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = B$$

$$BC = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = D$$

$-1+0 \quad 0+0 \quad 0+0$

Solution

We draw a Cayley table to check most of the axioms.

A is identity

$\times$	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

Table 1

From table 1, closure is satisfied since multiplication of any two elements of set G gives an element of the set. Here, A is the identity element. Each element has an inverse for instance $A^{-1} = A$, $B^{-1} = B$, $C^{-1} = C$ and $D^{-1} = D$. Associativity is not checked by the Cayley table but it is known that matrix multiplication is associative. Thus, the set of above matrices forms a group.

$a \times b = 1$

$B^{-1} = B$

$A^{-1} = A$

$C^{-1} = C$

$D^{-1} = D$

$BC = CB$

$2+i$ $\quad$ $3+4i$

Example 54

has $a+bi$, where i is Imaginary

$i^2=-1$

The set of complex numbers $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$ under addition forms an abelian group, with 0 as the identity.

Example 55

3, 2, -1, 0, 1

$\mathbb{C}^*$ $\mathbb{Z}^*$

The set of non-zero complex numbers $\mathbb{C}^*$ under multiplication forms an abelian group, with 1 as the identity.

Example 56

$3+0i$ $-$ $2+0i$

$2+0i$ 7 -3

Let H be a set of complex numbers given by $H = \{i, -i, 1, -1\}$. Is $(H, \times)$ a group?

$(H, \times)$ a group

×	i	$-i$	1	-1
i	-1	1	i	$-i$
$-i$	1	-1		
1				
-1				

$i \times -i = -(i^2)$

$i^2=-1$

$-i \times i$ $i \times i$

$a \times b = 1$

Solution

$i^{-1} = -i$ ✓

$\times$	i	-i	~~1~~	-1
i	-1	1	i	-i
-i	1	-1	-i	i
~~1~~	i	-i	1	-1
-1	-i	i	-1	1

Table 2

From table 2, closure is satisfied since each entry is an element of the set H. Element 1 is the identity element. Each element has an inverse for instance i is the inverse of $-i$ while $-i$ is the inverse of i. Each of 1 and -1 is its own inverse. It is known that multiplication in H is associative. Thus $(H, \times)$ is a group.

$0, 1, 2, \cdots, n-1$ residues

Example 57

The set $\mathbb{Z}_n$ of residue classes $[a]_n$ with the addition operator forms an abelian group, where $[0]_n$ is the identity and $[-a]_n$ is the inverse of $[a]_n$.

$\mathbb{Z}_3 = \{\cancel{0}, 1, 2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Example 58

The set $\mathbb{Z}_n^*$ of residue classes $[a]_n$ with $\gcd(a, n) = 1$ under multiplication forms an abelian group. The identity is $[1]_n$, and if b is a multiplicative inverse of a modulo n, then $[b]_n$ is the inverse of $[a]_n$.

$4/3 = 1$

Let us study the following addition and multiplication Cayley tables of $\mathbb{Z}_5$ and $\mathbb{Z}_5^*$.

$\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_n$ order

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ Relatively prime

$\mathbb{Z}_5=\{0,1,2,3,4\}$

$\mathbb{Z}_5^*=\{1,2,3,4\}$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

a: Addition table for $\mathbb{Z}_5$

6 mod 5

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

b: Multiplication table for $\mathbb{Z}_5^*$

8 mod 3

12 mod 5

$2^{-1}=3$
$3^{-1}=2$
$4^{-1}=4$

$2+a=0$
$-2=3$

$4+1=0$

Table 3

$\mathbb{Z}_5^*$

From table 3a, it is clear that $(\mathbb{Z}_5,+)$ is a group. Indeed, $+$ is a binary operation on $\mathbb{Z}_5$. Element 0 is the identity element. $\mathbb{Z}_5$ is associative for instance $(4+3)+1=4+(3+1)=3$. Every element has an inverse for instance 4 and 1 are inverses of each other while 2 and 3 are inverses of each other. Table 3b shows that $(\mathbb{Z}_5^*,\times)$ is a group.

Note that all elements have inverses for example $1^{-1} = 1,\ 2^2 = 3,\ 3^{-1} = 2,\ 4^{-1} = 4$. Note also that the identity is 1, closure and associativity are satisfied. Here, $\mathbb{Z}_n^*$ is a group of nonzero integers in $\mathbb{Z}_n$ less than n but relatively prime to n.

Study the following Cayley table for $\mathbb{Z}_{15}^*$ for emphasize.

$\mathbb{Z}_{15}^* = \{ \}$

22 mod 15

$\cdot$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Table 4: Multiplication table for $\mathbb{Z}_{15}^*$