# Zero Knowledge Bootcamp

## #2. Algebraic Structures

RareSkills

# Algebraic structures

An algebraic structure is a set together with a number of operations obeying some rules

- Semi-groups
- Monoids
- Groups
- Rings
- Fields
- Algebras

# Groups

A group G is a set together with an operation $\oplus$ that obeys the following properties:

**closure** – if $a \in G$ and $b \in G \rightarrow a \oplus b \in G$

**associativity** – $(a \oplus b) \oplus c = a \oplus (b \oplus c)$

**neutral element** – $\exists\, e \in G$ s.t. $\forall a \in G, a \oplus e = e \oplus a = a$

**inverse element** – $\forall a \in G \,\exists\, a^{-1} \in G$ s.t. $a \oplus a^{-1} = a^{-1} \oplus a = e$

Do the integers under multiplication form a group?

Do the positive integers under addition form a group?

Do the 2x2 matrices over the reals under matrix multiplication form a group?

# Rings

A ring with unity $R$ is a set together with two operations $\oplus$ and $\otimes$ that obeys the following properties:

**closure** – if $a \in R$ and $b \in R \rightarrow a \oplus b \in R$ and $a \otimes b \in R$

**commutativity** – $a \oplus b = b \oplus a$

**associativity** – $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ and $(a \otimes b) \otimes c = a \otimes (b \otimes c)$

**additive identity** – $\exists 0 \in R$ s.t. $\forall a \in R,\ a \oplus 0 = 0 \oplus a = a$

**additive inverse** – $\forall a \in R,\ \exists -a \in R$ s.t. $a \oplus -a = -a \oplus a = 0$

**multiplicative identity** – $\exists 1 \in R$ s.t. $\forall a \in R,\ a \otimes 1 = 1 \otimes a = a$

**distributivity** – $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Do the set of polynomials of degree d form a rings under polynomial addition and multiplication?

Do the set of polynomials of any degree form a rings under polynomial addition and multiplication?

RareSkills

# Fields

A field F is a ring with one more property

**multiplicative inverse** $- \forall a \neq 0 \in F \, \exists \, a^{-1} \in F \, \text{s.t.} \; a \oplus a^{-1} = a^{-1} \oplus a = 1$

Do the integers form a field?

Do the integers module p form a field?

# Characteristic of the field

The characteristic of a field is the number of times you add the multiplicative identity element to itself until you get the additive identity element. If you never reach it, the characteristic of the field is zero.

$$1 \cdot p = 0$$

# Finite groups

A group is said to be finite if it has a finite number of elements. The number of elements in a finite group is said to be the order of the group.

$$(\mathbb{Z}_p, +) = \{0, 1, 2, 3, ..., p-1\} \text{ what is its order?}$$

$$(\mathbb{Z}_p^*, \cdot) = \{1, 2, 3, ..., p-1\} \text{ what is its order?}$$

# Homomorphism

Given two grupos A and B, there exists a homomorphism between A and B if $\exists\phi : A \to B, \phi(a) = b$, where $a \in A$ and $b \in B$, s.t. $\phi(a_1 \oplus a_2) = \phi(a_1) \cdot \phi(a_2)$ $\forall a_1, a_2 \in A$.

RareSkills

# Example 1.

A: All integers with addition
B: All integers powers of two under multiplication

$$\phi(q) = 2^q$$

$$\phi(p+q) = 2^{p+q} = 2^p \cdot 2^q = \phi(p) \cdot \phi(q)$$

# Homomorphic encryption

Let's say I want to prove that I know two numbers whose sum is 15, that is, x+y=15, without revealing the numbers.

# Discrete log problem for modules

Let $a^q = b \text{ (mod p)}$

find q is a hard problem