# Mathematics for Cryptographers. Preliminaries.

ZKDL Camp

July 18, 2024

# Plan

1. Some words about the course
2. Notation
   - Sets
   - Logic
   - Randomness and Sequences
3. Basic Group Theory
   - Reasoning behind Groups
   - Group Definition and Examples
   - Subgroup
   - Homomorphism and Isomorphism
4. Polynomials

# Some words about the course

# About ZKDL

- ZKDL Camp is a series of lectures and workshops on zero-knowledge proofs and cryptography.
- Here, we will learn state-of-the-art zero-knowledge systems: what are SNARKs, how they work under the hood from total scratch.
- If possible, we will conduct workshops, where we will show practical implementations of the theoretical material.
- Primary audience: cryptographers, R&D Engineers, ZK developers, and everyone wanting to boost their understanding of cryptography.

**Note**

This is not a regular course: we require a lot of commitment and the material is fairly complex. However, we will try to make it as simple as possible.

# Approximate Camp Structure

1. Mathematics Preliminaries (3-4 lectures): group and number theory, finite fields, polynomials, elliptic curves etc.
2. Deep Delve into SNARKs: General definition, arithmetic circuits, commitment schemes, encryption etc.
3. Analysis of modern zero-knowledge proving systems: Groth16, Plonk, BulletProofs, STARK etc.
4. Specialization topics: low-level optimizations, advanced protocols such as folding schemes, Nova etc.

# Notation

# Sets

## Definition

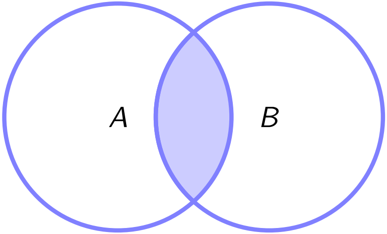
**Set** is a collection of distinct objects, considered as an object in its own right.

## Example

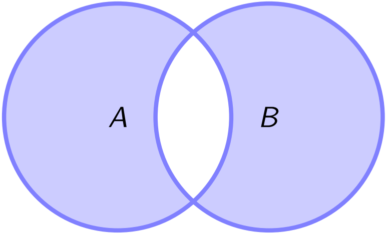
- $\mathbb{N}$ is a set of natural numbers.
- $\mathbb{Z}$ is a set of integers.
- $\mathbb{R}$ is a set of real numbers.
- $\mathbb{C}$ is a set of complex numbers.
- $\{1, 2, 5, 10\}$ is a set of four elements.
- $\{1, 2, 2, 3\}$ simply equals to $\{1, 2, 3\}$ – we do not count duplicates.

# Operations on sets

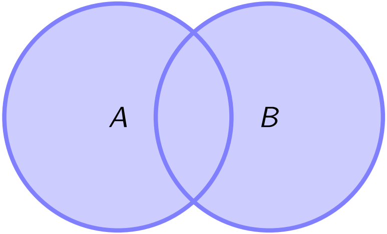
$A \cap B$



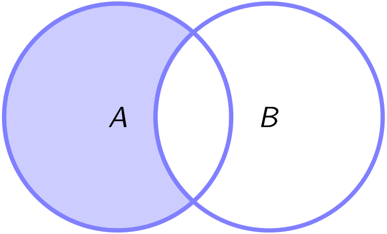
$\overline{A \cap B}$



$A \cup B$



$A \setminus B$



# Defining sets

### Example

- $\{x \in \mathbb{R} : x^2 = 1\}$ – a set of real numbers that satisfy the equation $x^2 = 1$.
- $\{x \in \mathbb{Z} : x \text{ is even}\}$ – a set of even integers.
- $\{x^2 : x \in \mathbb{R}, x^3 = 1\}$ – a set of squares of real numbers that satisfy the equation $x^3 = 1$.
- $\{x \in \mathbb{N} : x \text{ is prime}\}$ – a set of prime natural numbers.

### Question #1

How to simplify the set $\{x \in \mathbb{N} : x^2 = 2\}$?

### Question #2(*)

How to simplify the set $\{\sin \pi k : k \in \mathbb{Z}\}$?

# Basic Logic

- $\forall$ means "for all".
- $\exists$ means "there exists".
- $\wedge$ means "and".
- $\vee$ means "or".

**Question #1**

Is it true that $(\forall x \in \mathbb{N}) : \{x > 0\}$?

**Question #2**

Is it true that $(\exists x \in \mathbb{N}) : \{x \geq 0 \wedge x < 1\}$?

**Question #3**

Is it true that $(\forall x \in \mathbb{Z})\,(\exists y \in \mathbb{N}) : \{y > x\}$?

# Randomness and Sequences

## Notation

To denote probability of event $E$, we use notation $\Pr[E]$. For example,

$$\Pr[\text{It will be cold tomorrow}] = 0$$

## Notation

To denote that we take an element from a set $S$ uniformly at random, we use notation $x \xleftarrow{R} S$.
For example, when throwing a coin, we can write $x \xleftarrow{R} \{\text{heads}, \text{tails}\}$.

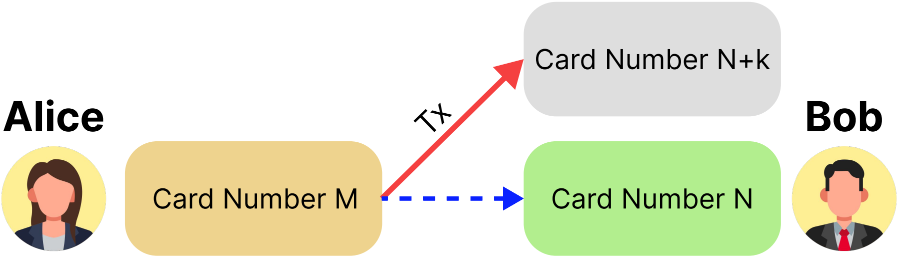
## Notation

To denote an infinite sequence $x_1, x_2, \cdots$, we use $\{x_i\}_{i \in \mathbb{N}}$. To denote a finite sequence $x_1, x_2, \cdots, x_n$, we use $\{x_i\}_{i=1}^n$. To enumerate through a list of indeces $\mathcal{I} \subset \mathbb{N}$, we use notation $\{x_i\}_{i \in \mathcal{I}}$.

# Basic Group Theory

# Why Groups?!

Well, first of all, we want to work with integers...
Imagine that Alice pays to Bob with a card number $N$, but instead of paying to a number $N$, the system pays to another card number $N + k, k \ll N$, which is only by 0.001% different. Bob would not be 99.999% happy...



# Why Groups?!

But integers on their own are not enough. We need to define a structure that allows us to perform operations on them.
This is very similar to interfaces: we abstract from the implementation, just merely stating we have "some" addition/multiplication.

### Example

Consider set $\mathbb{G} := \{\text{Dmytro}, \text{Dan}, \text{Friendship}\}$. We can safely define an operation $\oplus$ as:

$$\begin{aligned}\text{Dmytro} \oplus \text{Dan} &= \text{Friendship}\\ \text{Dan} \oplus \text{Friendship} &= \text{Dmytro}\\ \text{Friendship} \oplus \text{Dmytro} &= \text{Dan}\end{aligned}$$

### Rethorical question

What makes $(\mathbb{G}, \oplus)$ a group?

# Group Definition

## Definition

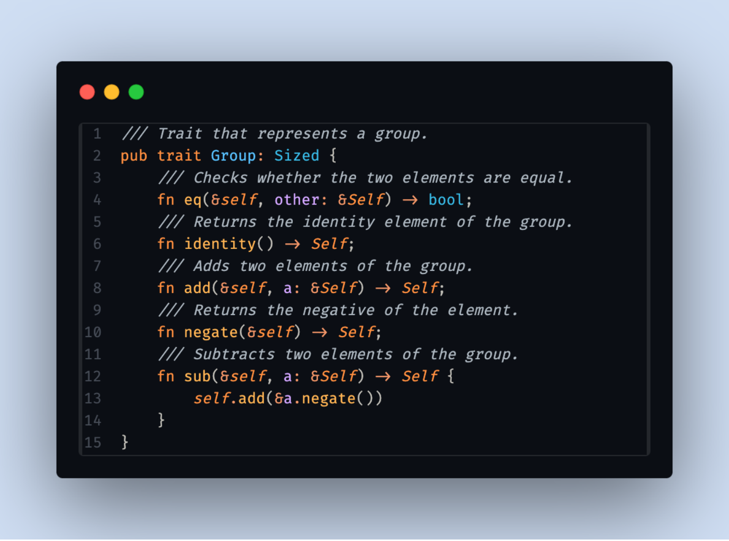
**Group** $(\mathbb{G}, \oplus)$, is a set with a binary operation $\oplus$ with following rules:

1. **Closure:** Binary operations always outputs an element from $\mathbb{G}$, that is $\forall a, b \in \mathbb{G} : a \oplus b \in \mathbb{G}$.
2. **Associativity:** $\forall a, b, c \in \mathbb{G} : (a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. **Identity element:** There exists a so-called identity element $e \in \mathbb{G}$ such that $\forall a \in \mathbb{G} : e \oplus a = a \oplus e = a$.
4. **Inverse element:** $\forall a \in \mathbb{G}\ \exists b \in \mathbb{G} : a \oplus b = b \oplus a = e$. We commonly denote the inverse element as $(\ominus a)$.

## Definition

A group is called **abelian** if it satisfies the additional rule called **commutativity**: $\forall a, b \in \mathbb{G} : a \oplus b = b \oplus a$.

# Explanation for Developers: Trait



```rust
/// Trait that represents a group.
pub trait Group: Sized {
    /// Checks whether the two elements are equal.
    fn eq(&self, other: &Self) -> bool;
    /// Returns the identity element of the group.
    fn identity() -> Self;
    /// Adds two elements of the group.
    fn add(&self, a: &Self) -> Self;
    /// Returns the negative of the element.
    fn negate(&self) -> Self;
    /// Subtracts two elements of the group.
    fn sub(&self, a: &Self) -> Self {
        self.add(&a.negate())
    }
}
```

More on that: `https://github.com/ZKDL-Camp/lecture-1-math`.

# Group Examples

### Example

A group of integers with the regular addition $(\mathbb{Z}, +)$ (also called the *additive* group of integers) is a group.

### Example

The multiplicative group of positive real numbers $(\mathbb{R}_{>0}, \times)$ is a group for similar reasons.

### Question #1

Is $(\mathbb{R}, \times)$ a group? If no, what is missing?

### Question #2

Is $(\mathbb{Z}, \times)$ a group? If no, what is missing?

# Small Note on Notation

### Additive group

We say that a group is *additive* if the operation is denoted as $+$, and the identity element is denoted as $0$.

### Multiplicative group

We say that a group is *multiplicative* if the operation is denoted as $\times$, and the identity element is denoted as $1$.

### Rule of thumb

We use additive notation when we imply that the group $\mathbb{G}$ is the set of points on the elliptic curve, while multiplicative is typically used in the rest of the cases.

# Abelian Groups Examples and Non-Examples

### Question #3

Is $(\mathbb{R}, -)$ a group? If no, what is missing?

### Question #4

Set $V$ is a set of tuples $(v_1, v_2, v_3)$ where each $v_i \in \mathbb{R} \setminus \{0\}$. Define the operation $\odot$ as

$$(v_1, v_2, v_3) \odot (u_1, u_2, u_3) = (v_1 u_1, v_2 u_2, v_3 u_3)$$

Is $(V, \odot)$ a group? If no, what is missing?

### Conclusion

Group is just a fancy name for a set with a binary operation that behaves nicely.

# Subgroup

## Question

Suppose $(\mathbb{G}, \oplus)$ is a group. Is any subset $\mathbb{H} \subset \mathbb{G}$ a group?

## Definition

A **subgroup** is a subset $\mathbb{H} \subset \mathbb{G}$ that is a group with the same operation $\oplus$. We denote it as $\mathbb{H} \leq \mathbb{G}$.

## Example

Consider $(\mathbb{Z}, +)$. Then, although $\mathbb{N} \subset \mathbb{Z}$, it is not a subgroup, as it does not have inverses.

## Example

Consider $(\mathbb{Z}, +)$. Then, $3\mathbb{Z} = \{3k : k \in \mathbb{Z}\} \subset \mathbb{Z}$ is a subgroup.

# Tiny question

Question

Does any group have at least one subgroup?

Yeah, $\mathbb{H} = \{e_{\mathbb{G}}\} \leq \mathbb{G}$.

# Homomorphism

### Definition

A **homomorphism** is a function $\phi : \mathbb{G} \to \mathbb{H}$ between two groups $(\mathbb{G}, \oplus)$ and $(\mathbb{H}, \odot)$ that preserves the group structure, i.e.,

$$\forall a, b \in \mathbb{G} : \phi(a \oplus b) = \phi(a) \odot \phi(b)$$

### Example

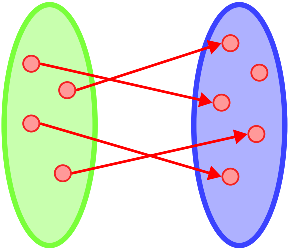
Consider $(\mathbb{Z}, +)$ and $(\mathbb{R}_{>0}, \times)$. Then, the function $\phi : \mathbb{Z} \to \mathbb{R}_{>0}$ defined as $\phi(k) = 2^k$ is a homomorphism.

**Proof**. Take any $n, m \in \mathbb{Z}$ and consider $\phi(n + m)$:

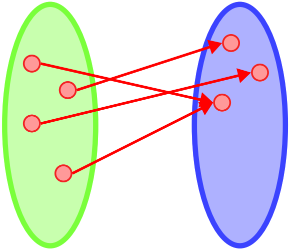
$$\phi(n + m) = 2^{n+m} = 2^n \times 2^m = \phi(n) \times \phi(m)$$

# Mapping types

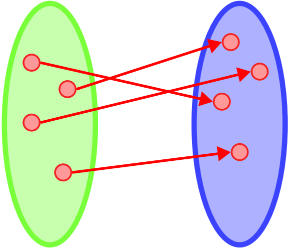
Injection



Surjection



Bijection



# Homomorphism

## Definition

**Isomorphism** is a bijective homomorphism.

## Definition

Two groups $\mathbb{G}$ and $\mathbb{H}$ are **isomorphic** if there exists an isomorphism between them. We denote it as $\mathbb{G} \cong \mathbb{H}$.

## Example

$\phi : k \mapsto 2^k$ from the previous example is a homomorphism between $(\mathbb{Z}, +)$ and $(\mathbb{R}_{>0}, \times)$, but not an isomorphism. Indeed, there is no $x \in \mathbb{Z}$ such that $2^x = 3 \in \mathbb{R}_{>0}$.

## Question

What can we do to make $\phi$ an isomorphism?

# Field

### Definition

**Field** $K$ is a set equipped with appropriate **addition** and **multiplication** operations with the corresponding well-defined inverses, where you can perform the basic arithmetic.

# Field

## Definition

**Field** $K$ is a set equipped with appropriate **addition** and **multiplication** operations with the corresponding well-defined inverses, where you can perform the basic arithmetic.

- $\mathbb{R}$ (real numbers) is a field.
- $\mathbb{Q}$ (rational numbers) is a field.
- $\mathbb{C}$ (complex numbers) is a field.
- $\mathbb{N}$ (natural numbers) is not a field: there is no additive inverse for 2 ($-2$ is not in $\mathbb{N}$).
- $\mathbb{Z}$ (integers) is not a field: additive inverse is defined, but the multiplicative is not ($2^{-1}$ is not defined).

# Polynomials

*Thanks for your attention!*