

# Mathematics for Cryptographers. Preliminaries.

ZKDL Camp

July 18, 2024



# Plan

- 1 Some words about the course
- 2 Notation
  - Sets
  - Logic
- 3 Basic Group Theory
  - Reasoning behind Groups
  - Group Definition and Examples
- 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 Dive 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

## Definition

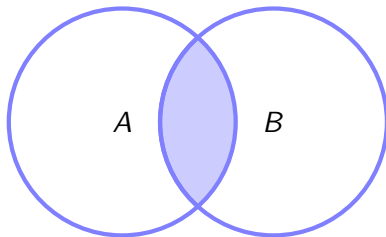
**Set** is a collection of distinct objects, considered as an object in its own right.

## Example

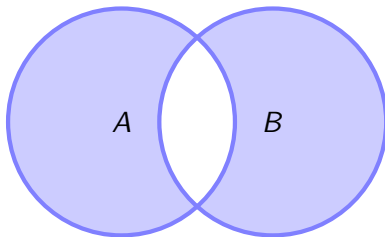
- $\mathbb{N}$  is a set of natural numbers.
- $\mathbb{Z}$  is a set of integers.
- $\mathbb{R}$  is a set of real numbers.
- $\mathbb{C}$  is a set of complex numbers.
- $\{1, 2, 5, 10\}$  is a set of four elements.
- $\{1, 2, 2, 3\}$  simply equals to  $\{1, 2, 3\}$  – we do not count duplicates.

# Operations on sets

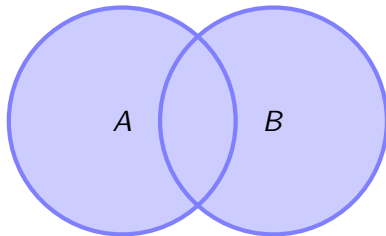
$$A \cap B$$



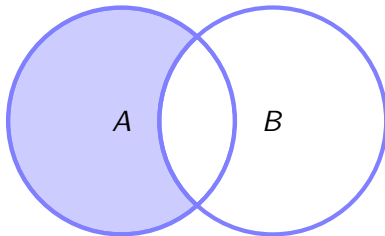
$$\overline{A \cap B}$$



$$A \cup B$$



$$A \setminus B$$





# 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

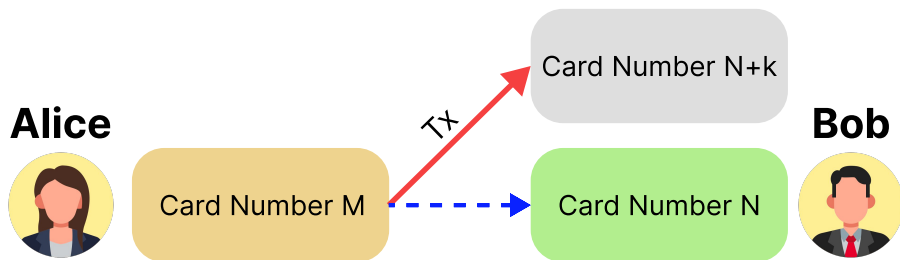
Is it true that  $(\forall x \in \mathbb{Z}) (\exists y \in \mathbb{N}) : \{y > x\}$ ?

# 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:

$$\text{Dmytro} \oplus \text{Dan} = \text{Friendship}$$

$$\text{Dan} \oplus \text{Friendship} = \text{Dmytro}$$

$$\text{Friendship} \oplus \text{Dmytro} = \text{Dan}$$

## 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

```
1  /// Trait that represents a group.
2  pub trait Group: Sized {
3      /// Checks whether the two elements are equal.
4      fn eq(&self, other: &Self) → bool;
5      /// Returns the identity element of the group.
6      fn identity() → Self;
7      /// Adds two elements of the group.
8      fn add(&self, a: &Self) → Self;
9      /// Returns the negative of the element.
10     fn negate(&self) → Self;
11     /// Subtracts two elements of the group.
12     fn sub(&self, a: &Self) → Self {
13         self.add(&a.negate())
14     }
15 }
```

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  $(\mathbb{R}_{>0}, \cdot)$  is a group for similar reasons.

## Question #1

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

## Question #2

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



# 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.

# Polynomials

## 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.

## 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).

*Thanks for your attention!*