Mathematics for Cryptography I: Notation and Groups

Distributed Lab

July 18, 2024

ZKDL Camp

Plan

Some words about the course

About ZKDL

- ZKDL is an intensive course on low-level zero-knowledge cryptography.
- We will learn zero-knowledge proving systems **from total scratch**.
- This means that the material is **hard**. We want commitment and attention from your side.
- We, in turn, provide you structured explanation of the material, practical examples and exercises.

Note

This course is beneficial for everyone: even lecturers do not know all the material and content is subject to change. Please, feel free to ask questions and provide feedback, and we will adjust the material accordingly.

Why ZKDL?

- Better Mathematics understanding.
- Skill of reading academic papers and writing your own ones.
- Public speech skills for lecturers on complex topics.
- Our knowledge structurization condensed in one course.
- Importance of ZK is quite obvious.
- And, of course, cryptography is fun!

Note

We are R&D experts in Cryptography, so we need to boost our skills in academic writing, lecturing, and understanding very advanced topics.

Format

1. We will gather every Thursday at 7PM.
2. Lecturer will be different based on the topic.
3. We will send you the lecture notes beforehand. Highly recommended to read it before the lecture.
4. We also attach exercises, which are highly recommended. You might ask questions about them during the lecture.
5. *Optionally*, we will conduct workshops on a separate day. We will discuss this later.

Contents

Notation

Sets

Definition

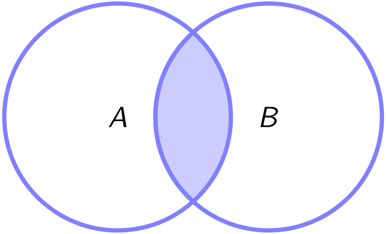
Set is a collection of *distinct* objects, considered as an object in its own right.

Example

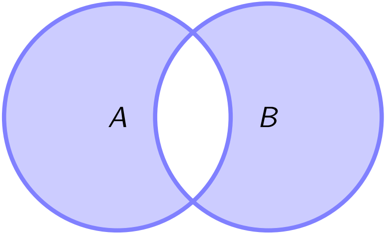
- $\mathbb{N}$ is a set of natural numbers.
- $\mathbb{Z}$ is a set of integers.
- $\mathbb{R}$ is a set of real numbers.
- $\mathbb{R}_{>0}$ is a set of positive real numbers.
- $\{1, 2, 5, 10\}$ is a set of four elements.
- $\{1, 2, 2, 3\} = \{1, 2, 3\}$ – we do not count duplicates.
- $\{1, 2, 3\} = \{2, 1, 3\}$ – order does not matter.
- $\{\{1, 2\}, \{3, 4\}, \{\sqrt{5}\}\}$ is a valid set – elements can be sets themselves.

Operations on sets

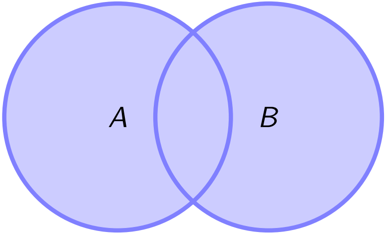
$A \cap B$



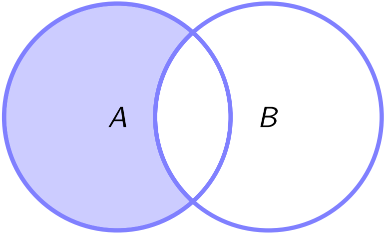
$\overline{A \cap B}$



$A \cup B$



$A \setminus B$



Operations on sets: Examples

Example

What does $\mathbb{Z} \setminus \{0, 1\}$ mean?

Example

How to simplify $\mathbb{Q} \cap \mathbb{Z}$?

Example

What is the result of $\{1, 2, 3\} \cup \{3, 4, 5\}$?

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 $x^3 = 1$.
- $\{x \in \mathbb{N} : x \text{ is prime}\} \setminus \{2\}$ – a set of odd prime numbers.

Question #1

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

Question #2(*)

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

Cartesian Product

Definition

Cartesian product of two sets A and B is a set of all possible ordered pairs (a, b) where $a \in A$ and $b \in B$. We denote it as $A \times B$.

Definition

Cartesian power of a set A is a set of all possible ordered tuples $(a_1, a_2, \cdots, a_n)$ where $a_i \in A$. We denote it as A^n.

Example

Consider sets $A = \{1, 2\}$ and $B = \{3, 4\}$. Then, $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$.

Example

$\mathbb{R}^2$ is a set of all possible points in the Cartesian plane.

Cartesian Product Questions

Question #1

What does $\{0,1\}^5$ mean?

Question #2

How to interpret the set $\{(x,y) \in \mathbb{N}^2 : x = y\}$.

Question #3(*)

How to interpret the set $\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$

Basic Logic

- $\forall$ means "for all".
- $\exists$ means "there exists", $\exists!$ means "there exists the only".
- $\wedge$ 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 $x \xleftarrow{R} \{\text{heads}, \text{tails}\}$.

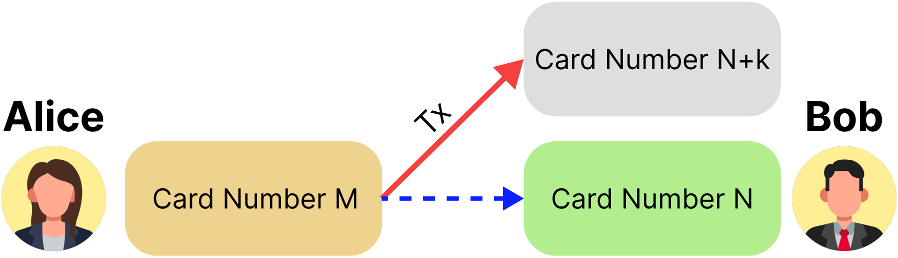
Notation

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:

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

Rhetorical 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.

Questions

Question #1

Does any group have at least one subgroup?

Answer. Yes, take $\mathbb{H} = \{e\} \leq \mathbb{G}$.

Question #2*

Let $\mathrm{GL}(\mathbb{R}, 2)$ be a mutliplicative group of invertable matrices, while $\mathrm{SL}(\mathbb{R}, 2)$ be a multiplicative group of matrices with determinant 1. Is $\mathrm{SL}(\mathbb{R}, 2) \leq \mathrm{GL}(\mathbb{R}, 2)$?

Answer. Yes. For $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(\mathbb{R}, 2)$ the inverse is $A^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Also, $\det(AB) = \det A \cdot \det B$, so the product of two matrices with determinant 1 has determinant 1, so the operation in closed.

Cyclic Subgroup.

Definition

Given a group $\mathbb{G}$ and $g \in \mathbb{G}$ the cyclic subgroup generated by g is

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = \{\dots, g^{-3}, g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\}.$$

Example

Consider the group of integers modulo 12, denoted by $\mathbb{Z}_{12}$. Consider $2 \in \mathbb{Z}_{12}$, the subgroup generated by 2 is then

$$\langle 2 \rangle = \{2, 4, 6, 8, 10, 0\}$$

Definition

We say that a group $\mathbb{G}$ is **cyclic** if there exists an element $g \in \mathbb{G}$ such that $\mathbb{G}$ is generated by g, that is, $\mathbb{G} = \langle g \rangle$.

Cyclic Subgroup Examples.

Example

Take $\mathbb{Q}^\times$. One of the possible cyclic subgroups is $\mathbb{H} = \{2^n : n \in \mathbb{Z}\}$.

Question

What is the generator of $\mathbb{H}$ in the example above?

Question

What is the generator of
$7\mathbb{Z} = \{7k : k \in \mathbb{Z}\} = \{\dots, -14, -7, 0, 7, 14, \dots\}$?

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.,

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

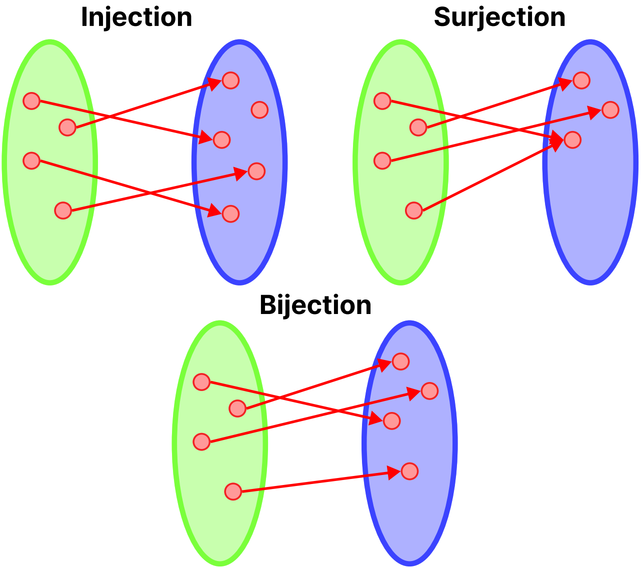
Example

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



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 ϕ an isomorphism?

Field

Informal Definition

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

Definition

A **field** is a set $\mathbb{F}$ with two operations $\oplus$ and $\odot$ such that:

1. $(\mathbb{F}, \oplus)$ is an abelian group with identity $e_\oplus$.
2. $(\mathbb{F} \setminus \{e_\oplus\}, \odot)$ is an abelian group.
3. The **distributive law** holds:
   $\forall a, b, c \in \mathbb{F} : a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

Field Examples

Example

The set of real numbers $(\mathbb{R}, +, \times)$ is obviously a field. So is $(\mathbb{Q}, +, \times)$.

Definition

Finite Field is the set $\{0, \dots, p-1\}$ equipped with operations modulo p is a field if p is a prime number.

Example

The set $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ with operations modulo 5 is a field. Operation examples:

- $3 + 4 = 2$.
- $3 \times 2 = 1$.
- $4^{-1} = 4$ since $4 \times 4 = 1$.

Thanks for your attention!