Mathematics for Cryptography: Number Theory, Groups, Polynomials

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.

About ZKDL

- ZKDL is an intensive course on low-level zero-knowledge cryptography.
- We will learn zero-knowledge proving systems **from total scratch**.

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.

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.

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.

Format

1. We will gather every Thursday at 7PM.
2. Lecturer will be different based on the topic.

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.

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 optional but highly recommended. You might ask questions about them during the lecture.

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 optional but 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

1. Mathematics Preliminaries: group and number theory, finite fields, polynomials, elliptic curves etc.
2. Building SNARKs from scratch.
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.

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.

Sets

Definition

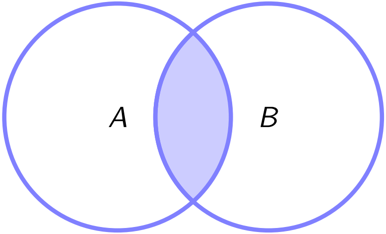
Set is a collection of *distinct* objects, considered as an object in its own right.

Example

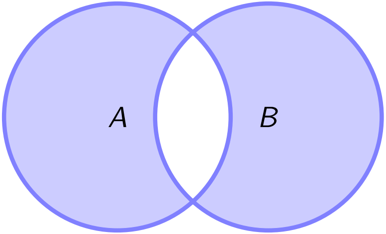
- $\mathbb{N}$ is a set of natural numbers.
- $\mathbb{Z}$ is a set of integers.
- $\mathbb{R}$ is a set of real numbers.
- $\mathbb{R}_{>0}$ is a set of positive real numbers.
- $\{1, 2, 5, 10\}$ is a set of four elements.
- $\{1, 2, 2, 3\} = \{1, 2, 3\}$ – we do not count duplicates.
- $\{1, 2, 3\}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

Operations on sets

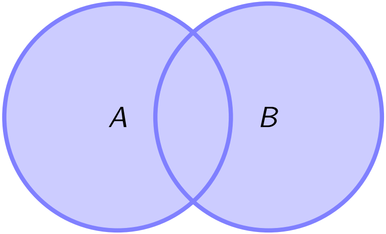
$A \cap B$



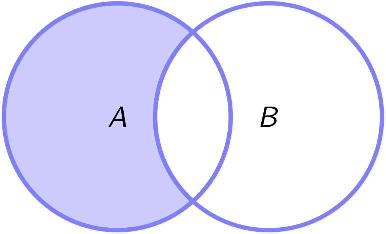
$\overline{A \cap B}$



$A \cup B$



$A \setminus B$



Defining sets

Example

- $\{x \in \mathbb{R} : x^2 = 1\}$ – a set of real numbers that satisfy the equation $x^2 = 1$.

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.

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 $x^3 = 1$.

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.

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 $\{x \in \mathbb{N} : x^2 = 2\}$?

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 $\{\sin \pi k : k \in \mathbb{Z}\}$?

Basic Logic

- $\forall$ means "for all".
- $\exists$ means "there exists", $\exists!$ means "there exists the only".
- $\wedge$ means "and".
- $\vee$ means "or".

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 $(\forall x \in \mathbb{N}) : \{x > 0\}$?

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

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 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 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 $x \xleftarrow{R} \{\text{heads}, \text{tails}\}$.

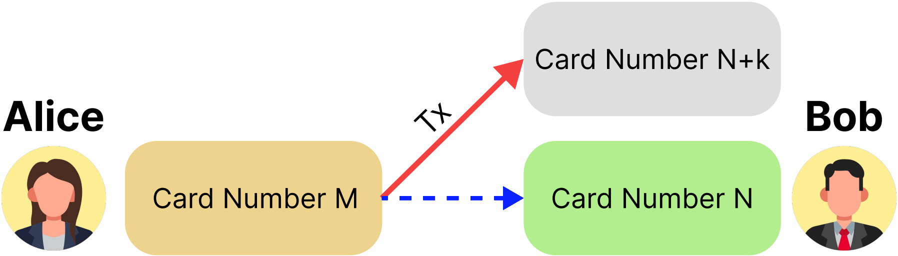
Notation

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.

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:

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

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:

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

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 $\forall a, b \in \mathbb{G} : a \oplus b \in \mathbb{G}$.

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:** $\forall a, b, c \in \mathbb{G} : (a \oplus b) \oplus c = a \oplus (b \oplus c)$.

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 $\forall a \in \mathbb{G} : e \oplus a = a \oplus e = a$.

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 $(\ominus a)$.

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.

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.

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?

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.

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.

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?

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?

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?

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 $\mathbb{H} \leq \mathbb{G}$.

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.

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?

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 $\mathrm{SL}(\mathbb{R}, 2) \leq \mathrm{GL}(\mathbb{R}, 2)$?

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.

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.,

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

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.,

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

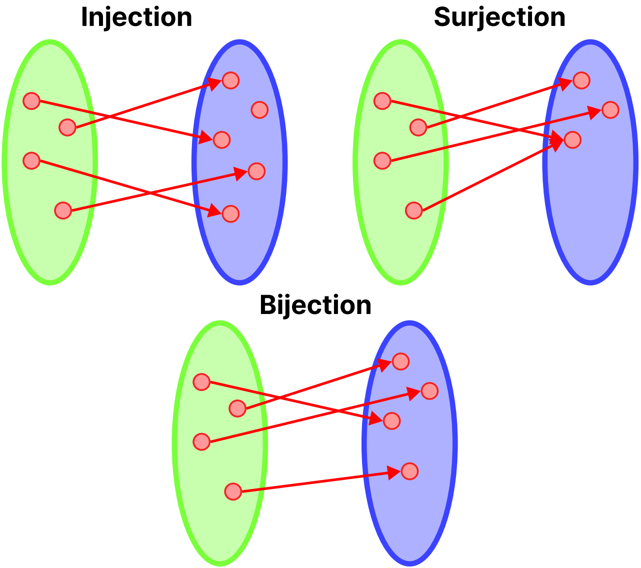
Example

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.

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 $\mathbb{G} \cong \mathbb{H}$.

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 $2^x = 3 \in \mathbb{R}_{>0}$.

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.

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 $(\mathbb{Q}, +, \times)$.

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 $\{0, \ldots, p-1\}$ equipped with operations modulo p is a field if p is a prime number.

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 $4 \times 4 = 1$.

Polynomials

Definition

Definition

A **polynomial** $f(x)$ is a function of the form

$$p(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n = \sum_{k=0}^{n} c_k x^k,$$

where $c_0, c_1, \ldots, c_n$ are coefficients of the polynomial.

Definition

Definition

A **polynomial** $f(x)$ is a function of the form

$$p(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n = \sum_{k=0}^{n} c_k x^k,$$

where $c_0, c_1, \ldots, c_n$ are coefficients of the polynomial.

Definition

A set of polynomials depending on x with coefficients in a field $\mathbb{F}$ is denoted as $\mathbb{F}[x]$, that is

$$\mathbb{F}[x] = \left\{ p(x) = \sum_{k=0}^{n} c_k x^k : c_k \in \mathbb{F},\ k = 0, \ldots, n \right\}.$$

Example

Consider the finite field $\mathbb{F}_3$. Then, some examples of polynomials from $\mathbb{F}_3[x]$ are listed below:

1. $p(x) = 1 + x + 2x^2$.
2. $q(x) = 1 + x^2 + x^3$.
3. $r(x) = 2x^3$.

Examples of Polynomials

Example

Consider the finite field $\mathbb{F}_3$. Then, some examples of polynomials from $\mathbb{F}_3[x]$ are listed below:

1. $p(x) = 1 + x + 2x^2$.
2. $q(x) = 1 + x^2 + x^3$.
3. $r(x) = 2x^3$.

If we were to evaluate these polynomials at $1 \in \mathbb{F}_3$, we would get:

1. $p(1) = 1 + 1 + 2 \cdot 1 \bmod 3 = 1$.
2. $q(1) = 1 + 1 + 1 \bmod 3 = 0$.
3. $r(1) = 2 \cdot 1 = 2$.

More about polynomials

Definition

The **degree** of a polynomial $p(x) = c_0 + c_1x + c_2x^2 + \dots$ is the largest $k \in \mathbb{Z}_{\geq 0}$ such that $c_k \neq 0$. We denote the degree of a polynomial as $\deg p$. We also denote by $\mathbb{F}^{(\leq m)}[x]$ a set of polynomials of degree at most m.

More about polynomials

Definition

The **degree** of a polynomial $p(x) = c_0 + c_1 x + c_2 x^2 + \dots$ is the largest $k \in \mathbb{Z}_{\geq 0}$ such that $c_k \neq 0$. We denote the degree of a polynomial as $\deg p$. We also denote by $\mathbb{F}^{(\leq m)}[x]$ a set of polynomials of degree at most m.

Example

The degree of the polynomial $p(x) = 1 + 2x + 3x^2$ is 2, so $p(x) \in \mathbb{F}_3^{(\leq 2)}[x]$.

More about polynomials

Definition

The **degree** of a polynomial $p(x) = c_0 + c_1 x + c_2 x^2 + \dots$ is the largest $k \in \mathbb{Z}_{\geq 0}$ such that $c_k \neq 0$. We denote the degree of a polynomial as $\deg p$. We also denote by $\mathbb{F}^{(\leq m)}[x]$ a set of polynomials of degree at most m.

Example

The degree of the polynomial $p(x) = 1 + 2x + 3x^2$ is 2, so $p(x) \in \mathbb{F}_3^{(\leq 2)}[x]$.

Theorem

For any two polynomials $p, q \in \mathbb{F}[x]$ and $n = \deg p, m = \deg q$, the following two statements are true:

1. $\deg(pq) = n + m$.
2. $\deg(p+q) = \max\{n, m\}$ *if* $n \neq m$ *and* $\deg(p+q) \leq m$ *for* $m = n$.

Roots of Polynomials

Definition

Let $p(x) \in \mathbb{F}[x]$ be a polynomial of degree $\deg p \geq 1$. A field element $x_0 \in \mathbb{F}$ is called a root of $p(x)$ if $p(x_0) = 0$.

Roots of Polynomials

Definition

Let $p(x) \in \mathbb{F}[x]$ be a polynomial of degree $\deg p \geq 1$. A field element $x_0 \in \mathbb{F}$ is called a root of $p(x)$ if $p(x_0) = 0$.

Example

Consider the polynomial $p(x) = 1 + x + x^2 \in \mathbb{F}_3[x]$. Then, $x_0 = 1$ is a root of $p(x)$ since $p(x_0) = 1 + 1 + 1 \bmod 3 = 0$.

Roots of Polynomials

Definition

Let $p(x) \in \mathbb{F}[x]$ be a polynomial of degree $\deg p \geq 1$. A field element $x_0 \in \mathbb{F}$ is called a root of $p(x)$ if $p(x_0) = 0$.

Example

Consider the polynomial $p(x) = 1 + x + x^2 \in \mathbb{F}_3[x]$. Then, $x_0 = 1$ is a root of $p(x)$ since $p(x_0) = 1 + 1 + 1 \bmod 3 = 0$.

Theorem

Let $p(x) \in \mathbb{F}[x], \deg p \geq 1$. Then, $x_0 \in \mathbb{F}$ is a root of $p(x)$ if and only if there exists a polynomial $q(x)$ (with $\deg q = n - 1$) such that

$$p(x) = (x - x_0)q(x)$$

Polynomial Division

Theorem

Given $f, g \in \mathbb{F}[x]$ *with* $g \neq 0$*, there are unique polynomials* $p, q \in \mathbb{F}[x]$ *such that*

$$f = q \cdot g + r,\ 0 \leq \deg r < \deg g$$

Polynomial Division

Theorem

Given $f, g \in \mathbb{F}[x]$ with $g \neq 0$, there are unique polynomials $p, q \in \mathbb{F}[x]$ such that

$$f = q \cdot g + r, \; 0 \leq \deg r < \deg g$$

Example

Consider $f(x) = x^3 + 2$ and $g(x) = x + 1$ over $\mathbb{R}$. Then, we can write $f(x) = (x^2 - x + 1)g(x) + 1$, so the remainder of the division is $r \equiv 1$. Typically, we denote this as:

$$f \operatorname{div} g = x^2 - x + 1, \quad f \bmod g = 1.$$

The notation is pretty similar to one used in integer division.

Polynomial Divisibility

Definition

A polynomial $f(x) \in \mathbb{F}[x]$ is called **divisible** by $g(x) \in \mathbb{F}[x]$ (or, g **divides** f, written as $g \mid f$) if there exists a polynomial $h(x) \in \mathbb{F}[x]$ such that $f = gh$.

Polynomial Divisibility

Definition

A polynomial $f(x) \in \mathbb{F}[x]$ is called **divisible** by $g(x) \in \mathbb{F}[x]$ (or, g **divides** f, written as $g \mid f$) if there exists a polynomial $h(x) \in \mathbb{F}[x]$ such that $f = gh$.

Theorem

If $x_0 \in \mathbb{F}$ is a root of $p(x) \in \mathbb{F}[x]$, then $(x - x_0) \mid p(x)$.

Polynomial Divisibility

Definition

A polynomial $f(x) \in \mathbb{F}[x]$ is called **divisible** by $g(x) \in \mathbb{F}[x]$ (or, g **divides** f, written as $g \mid f$) if there exists a polynomial $h(x) \in \mathbb{F}[x]$ such that $f = gh$.

Theorem

If $x_0 \in \mathbb{F}$ is a root of $p(x) \in \mathbb{F}[x]$, then $(x - x_0) \mid p(x)$.

Definition

A polynomial $f(x) \in \mathbb{F}[x]$ is said to be **irreducible** in $\mathbb{F}$ if there are no polynomials $g, h \in \mathbb{F}[x]$ both of degree more than 1 such that $f = gh$.

Polynomial Divisibility

Example

A polynomial $f(x) = x^2 + 16$ is irreducible in $\mathbb{R}$. Also $f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$, yet it is reducible over $\mathbb{R}$: $f(x) = (x - \sqrt{2})(x + \sqrt{2})$.

Polynomial Divisibility

Example

A polynomial $f(x) = x^2 + 16$ is irreducible in $\mathbb{R}$. Also $f(x) = x^2 - 2$ is irreducible over $\mathbb{Q}$, yet it is reducible over $\mathbb{R}$: $f(x) = (x - \sqrt{2})(x + \sqrt{2})$.

Example

There are no polynomials over complex numbers $\mathbb{C}$ with degree more than 2 that are irreducible. This follows from the *fundamental theorem of algebra*. For example, $x^2 + 16 = (x - 4i)(x + 4i)$.

Interpolation

Question

How can we define the polynomial?

The most obvious way is to specify coefficients $(c_0, c_1, \ldots, c_n)$. Can we do it in a different way?

Interpolation

Question

How can we define the polynomial?

The most obvious way is to specify coefficients $(c_0, c_1, \ldots, c_n)$. Can we do it in a different way?

Theorem

Given $n+1$ distinct points $(x_0, y_0), \ldots, (x_n, y_n)$, there exists a unique polynomial $p(x)$ of degree at most n such that $p(x_i) = y_i$ for all $i = 0, \ldots, n$.

Illustration with two points

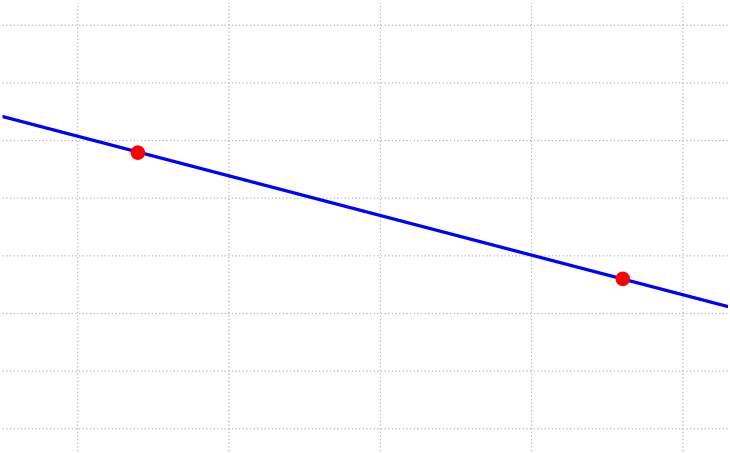


Figure: 2 points on the plane uniquely define the polynomial of degree 1 (linear function).

Illustration with five points

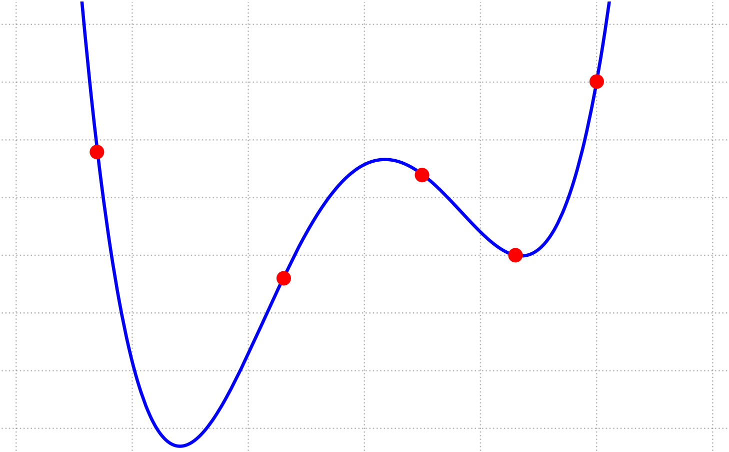


Figure: 5 points on the plane uniquely define the polynomial of degree 4.

Illustration with three points

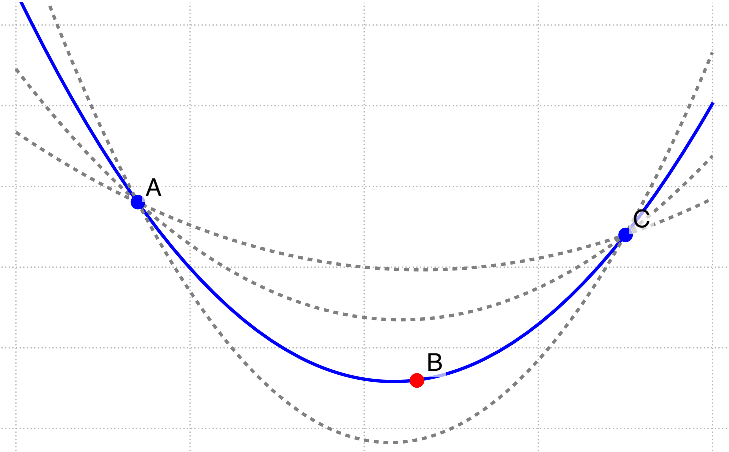


Figure: 2 points are not enough to define the quadratic polynomial $(c_2x^2 + c_1x + c_0)$.

One of the ways to interpolate the polynomial is to use the Lagrange interpolation.

Theorem

Given $n+1$ *distinct points* $(x_0, y_0), \ldots, (x_n, y_n)$, *the polynomial* $p(x)$ *that passes through these points is given by*

$$p(x) = \sum_{i=0}^{n} y_i \ell_i(x), \quad \ell_i(x) = \prod_{i=0, j \neq i}^{n} \frac{x - x_j}{x_i - x_j}.$$

Application: Shamir Secret Sharing

Motivation

How to share a secret α among n people in such a way that any t of them can reconstruct the secret, but any $t-1$ cannot?

Application: Shamir Secret Sharing

Motivation

How to share a secret α among n people in such a way that any t of them can reconstruct the secret, but any $t-1$ cannot?

Definition

Secret Sharing scheme is a pair of efficient algorithms $(\mathsf{Gen}, \mathsf{Comb})$ which work as follows:

- $\mathsf{Gen}(\alpha, t, n)$: probabilistic sharing algorithm that yields n shards $(\alpha_1, \dots, \alpha_t)$ for which t shards are needed to reconstruct the secret α.

Application: Shamir Secret Sharing

Motivation

How to share a secret α among n people in such a way that any t of them can reconstruct the secret, but any $t-1$ cannot?

Definition

Secret Sharing scheme is a pair of efficient algorithms $(\text{Gen}, \text{Comb})$ which work as follows:

- $\text{Gen}(\alpha, t, n)$: probabilistic sharing algorithm that yields n shards $(\alpha_1, \dots, \alpha_t)$ for which t shards are needed to reconstruct the secret α.
- $\text{Comb}(\mathcal{I}, \{\alpha_i\}_{i \in \mathcal{I}})$: deterministic reconstruction algorithm that reconstructs the secret α from the shards $\mathcal{I} \subset \{1, \dots, n\}$ of size t.

Shamir's Protocol

Note

Here, we require the **correctness**: for every $\alpha \in F$, for every possible output $(\alpha_1, \ldots, \alpha_n) \leftarrow \mathsf{Gen}(\alpha, t, n)$, and any t-size subset $\mathcal{I}$ of $\{1, \ldots, n\}$ we have

$$\mathsf{Comb}(\mathcal{I}, \{\alpha_i\}_{i \in \mathcal{I}}) = \alpha. \tag{1}$$

Shamir's Protocol

Note

Here, we require the **correctness**: for every $\alpha \in F$, for every possible output $(\alpha_1, \dots, \alpha_n) \leftarrow \mathsf{Gen}(\alpha, t, n)$, and any t-size subset $\mathcal{I}$ of $\{1, \dots, n\}$ we have

$$\mathsf{Comb}(\mathcal{I}, \{\alpha_i\}_{i \in \mathcal{I}}) = \alpha. \tag{1}$$

Definition

Now, **Shamir's protocol** works as follows: $F = \mathbb{F}_q$ and

- $\mathsf{Gen}(\alpha, k, n)$: choose random $k_1, \dots, k_{t-1} \xleftarrow{R} \mathbb{F}_q$ and define the polynomial

  $$\omega(x) := \alpha + k_1 x + k_2 x^2 + \cdots + k_{t-1} x^{t-1} \in \mathbb{F}_q^{\leq (t-1)}[x], \tag{2}$$

  and then compute $\alpha_i \leftarrow \omega(i) \in \mathbb{F}_q,\ i = 1, \dots, n$.

Shamir's Protocol

Definition

- $\text{Comb}(\mathcal{I}, \{\alpha_i\}_{i \in \mathcal{I}})$: interpolate the polynomial $\omega(x)$ using the Lagrange interpolation and output $\omega(0) = \alpha$.

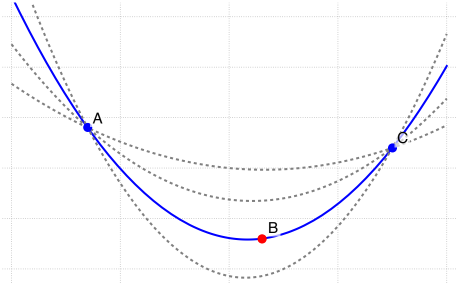


Figure: There are infinitely many quadratic polynomials passing through two blue points (gray dashed lines). However, knowing the red point allows us to uniquely determine the polynomial and thus get its value at 0.

Thanks for your attention!