Mathematics for Informatics

Algebra: Discrete logarithm, rings and fields (lecture 7 of 12)

Francesco Dolce

dolcefra@fit.cvut.cz

Czech Technical University in Prague

B231 - Winter 2023/2024

created: September 12, 2023, 14:48

Discrete logarithm problem

The standard logarithm (in base α) of the number β is the solution of the equation

$$\alpha^x = \beta \quad \text{in the group } (\mathbb{R}, \cdot).$$

Definition (Discrete logarithm problem in $\mathbb{Z}_p^\times$)

Let us consider the group $\mathbb{Z}_p^\times$, α one of its generator and β one of its element. To solve the discrete logarithm problem means to find the integer $1 \leq x \leq p-1$ such that

$$\alpha^x \equiv \beta \ (mod\ p)$$

The discrete logarithm?

No reasonably fast algorithm solving the discrete logarithm problem is known. But rising to the power in $\mathbb{Z}_p^\times$ can be done effectively.

The speed of the best known algorithms is roughly proportional to $\sqrt{p}$, i.e., for p having its binary representation 1024 bits long, such algorithm makes approximately 2^{512} operations.

Thus we obtain a one-way function that can be used for **asymmetric cipher**:

- Find $\beta \equiv \alpha^x \pmod{p}$ is easy, knowing x, α and p;
- Find x, knowing β, α and p is very difficult

In **RSA** (**R**ivest-**S**hamir-**A**dleman) cryptosystem, the one way function "multiplying of primes" is used:

- Multiplication of primes is easy and fast, while prime factorization of the result is very difficult.

RSA

Alice

Initialization: she finds two large prime numbers p and q,
she computes $n = p \cdot q$ and $\psi(n) = (p-1)(q-1)$,
she chooses $e \in \{1, 2, \ldots, \psi(n) - 1\}$ so that $\gcd(e, \psi(n)) = 1$,
she computes the private key d so that $d \cdot e = 1 \mod \psi(n)$.

She sends the public key $k_{pub} = (n, e)$ to Bob.

Bob

Bob wants to send the message x.
He encrypts the message $y = x^e \mod n$ and sends y to Alice.

Alice

Alice decrypts the message by $x = y^d \mod n$.

Diffie-Hellman Key Exchange

Initialization: Alice finds some large prime number p and some generator α of the group $\mathbb{Z}_p^\times$.
She publishes p and α. (Finding a large prime and a generator are not easy tasks!)

Alice	**Bob**
chooses private key $a \in \{2, \ldots, p-2\}$	chooses private key $b \in \{2, \ldots, p-2\}$
computes public key $A \equiv \alpha^a \bmod p$	computes public key $B \equiv \alpha^b \bmod p$

exchange of public keys A and B $\longleftrightarrow$

computes $k_{AB} \equiv B^a \bmod p$	computes $k_{AB} \equiv A^b \bmod p$

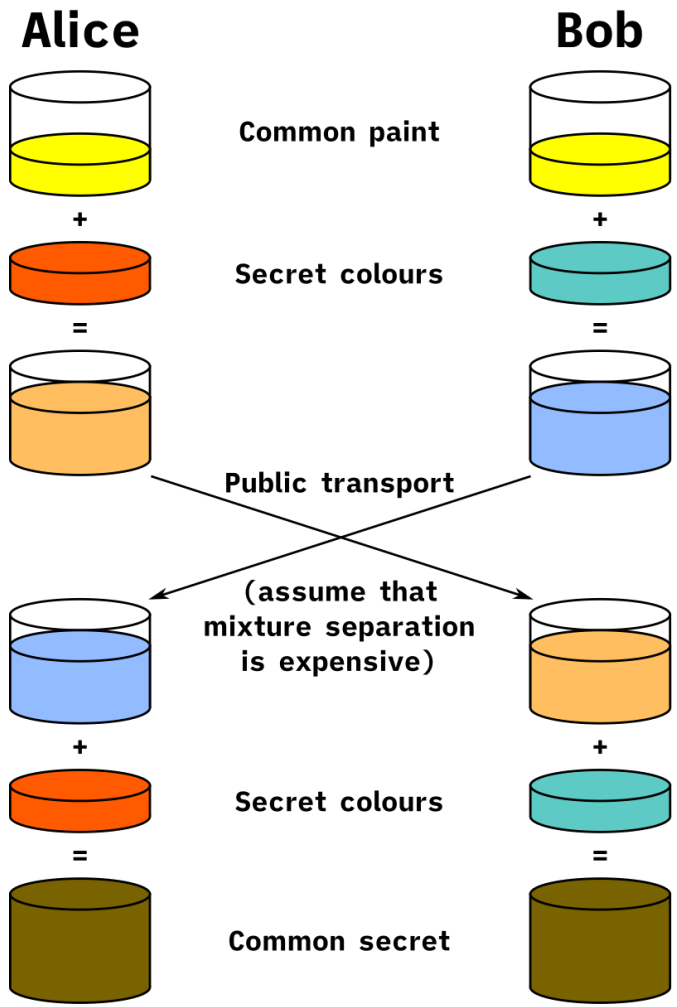
Principle

Diffie-Hellman Key Exchange is built on the following facts:

- Rising to the power in $\mathbb{Z}_p^\times$ is commutative, and so the value of k_{AB} is the same for both Alice and Bob:

$$k_{AB} \equiv (\alpha^b)^a \equiv \alpha^{ab} \mod p$$
$$k_{AB} \equiv (\alpha^a)^b \equiv \alpha^{ab} \mod p.$$

- Rising to the power is not computationally complex (square & multiply algorithm).
- The inverse operation to rising to the power (the discrete logarithm) is computationally exhausting.



Discrete logarithm in general

The discrete logarithm problem can be defined in an arbitrary cyclic group.

Definition (problem of discrete logarithm in group $G = (M, \cdot)$)

Let $G = (M, \cdot)$ be a cyclic group of order n, α one of its generators and β one of its an element.
To solve the discrete logarithm problem means to find the integer $1 \leq x \leq n$ s.t.

$$\alpha^x = \beta.$$

Discrete logarithm in general

The discrete logarithm problem can be defined in an arbitrary cyclic group.

Definition (problem of discrete logarithm in group $G = (M, \cdot)$)

Let $G = (M, \cdot)$ be a cyclic group of order n, α one of its generators and β one of its an element.
To solve the discrete logarithm problem means to find the integer $1 \leq x \leq n$ s.t.

$$\alpha^x = \beta.$$

If we use additive notation:

Definition (problem of discrete logarithm in group $G = (M, +)$)

Let $G = (M, +)$ be a cyclic group of order n, α one of its generators and β one of its element.
To solve the discrete logarithm problem means to find the integer $1 \leq k \leq n$ s.t.

$$k \times \alpha = \beta.$$

The discrete logarithm is not always complicated

Consider the group $\mathbb{Z}_p^+$.
It is a cyclic group of prime order p, and each positive $\alpha < p - 1$ is its generator.
The problem of discrete logarithm in this group has the form of the equation

$$k\alpha \equiv \beta \pmod{p}.$$

We can solve it easily: we find the inverse of α in the group $\mathbb{Z}_p^\times$ (for instance by polynomial EEA), and the solution is $k = \beta\alpha^{-1} \pmod{p}$.

The discrete logarithm is not always complicated

Consider the group $\mathbb{Z}_p^+$.
It is a cyclic group of prime order p, and each positive $\alpha < p - 1$ is its generator.
The problem of discrete logarithm in this group has the form of the equation

$$k\alpha \equiv \beta \pmod{p}.$$

We can solve it easily: we find the inverse of α in the group $\mathbb{Z}_p^\times$ (for instance by polynomial EEA), and the solution is $k = \beta\alpha^{-1} \pmod{p}$.

Example

Let $p = 11$, $\alpha = 3$ and $\beta = 5$. We want to find k such that $k \cdot 3 \equiv 5 \pmod{11}$.

The discrete logarithm is not always complicated

Consider the group $\mathbb{Z}_p^+$.
It is a cyclic group of prime order p, and each positive $\alpha < p-1$ is its generator.
The problem of discrete logarithm in this group has the form of the equation

$$k\alpha \equiv \beta \pmod{p}.$$

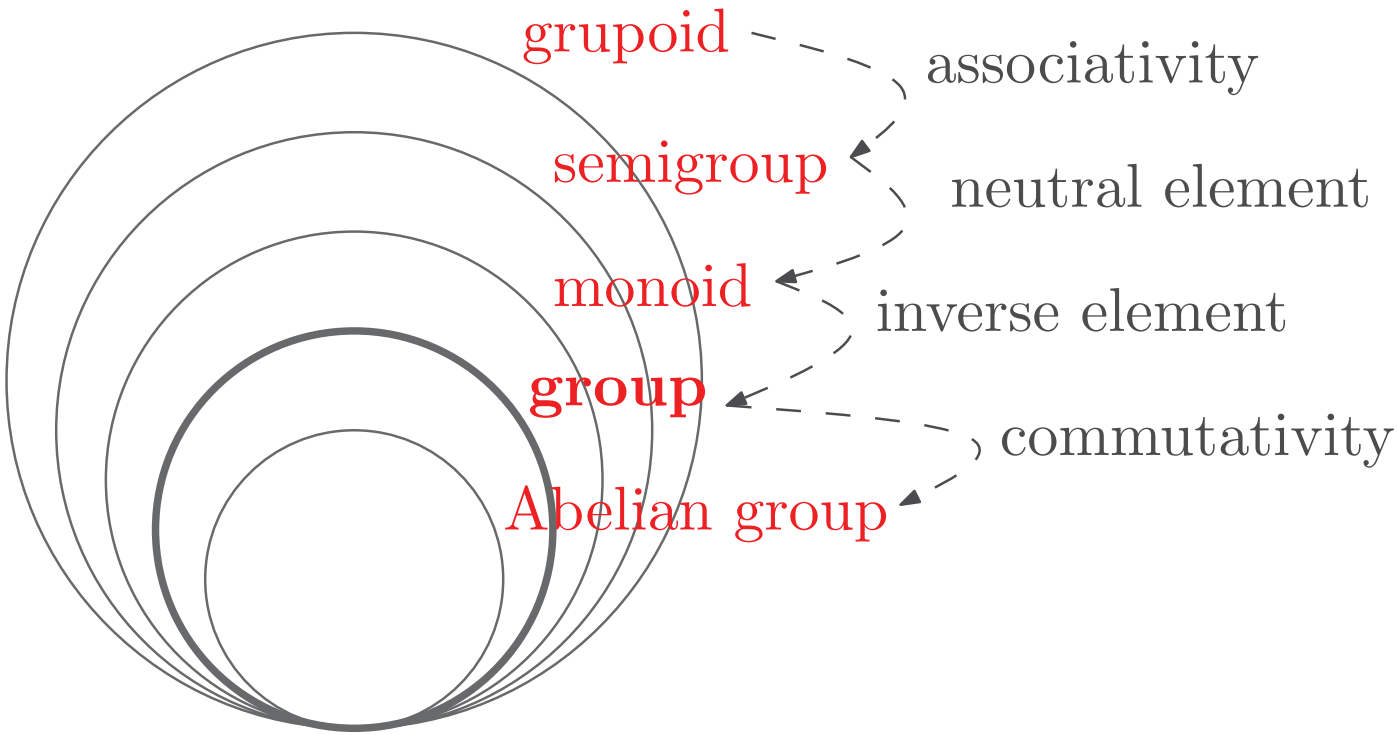
We can solve it easily: we find the inverse of α in the group $\mathbb{Z}_p^\times$ (for instance by polynomial EEA), and the solution is $k = \beta\alpha^{-1} \pmod{p}$.

Example

Let $p = 11$, $\alpha = 3$ and $\beta = 5$. We want to find k such that $k \cdot 3 \equiv 5 \pmod{11}$.
We easily verify that in $\mathbb{Z}_{11}^\times$ we have $3^{-1} = 4$, and thus $k = 5 \cdot 4 \pmod{11} = 9$.

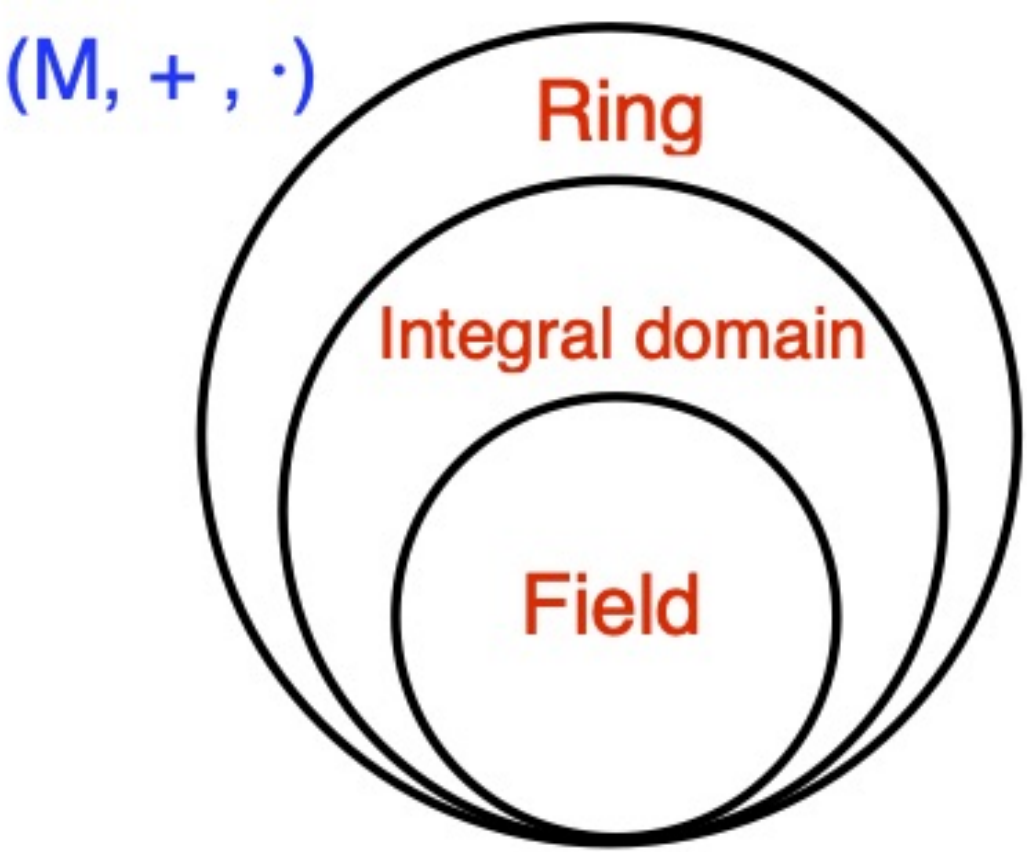
Sets with one binary operation

A nonempty set M with a binary operation $\cdot$ (resp. $+$ for the additive notation).



Sets with two binary operations

For more sophisticated arithmetical operations with numbers we need **both** addition and multiplication.



Definition of a ring

Definition (Ring)

Let M be a nonempty set, and $+$ and $\cdot$ two binary operations. We say that $R = (M, +, \cdot)$ is a ring if the following holds:

- $(M, +)$ *is an* ***Abelian group***,
- $(M, \cdot)$ *is a* ***monoid***,
- *both left and right* ***distributive law*** *hold:*

$$\forall\, a, b, c \in M \text{ we have: } \quad a(b + c) = ab + ac \quad \wedge \quad (a + b)c = ac + bc.$$

We respect the standard convention that the multiplication has a higher priority than the addition (and use the concatenation, instead of $\cdot$, when it is clear from the context).

Definition of a ring

Definition (Ring)

Let M be a nonempty set, and $+$ and $\cdot$ two binary operations. We say that $R = (M, +, \cdot)$ is a ring if the following holds:

- $(M, +)$ *is an* ***Abelian group***,
- $(M, \cdot)$ *is a* ***monoid***,
- *both left and right* ***distributive law*** *hold:*

$$\forall\, a, b, c \in M \text{ we have: } \quad a(b+c) = ab + ac \quad \wedge \quad (a+b)c = ac + bc.$$

We respect the standard convention that the multiplication has a higher priority than the addition (and use the concatenation, instead of $\cdot$, when it is clear from the context).
Sometimes, $(M, \cdot)$ is required to be only a semigroup (or even a groupoid).

Terminology

Let $R = (M, +, \cdot)$ be a ring.

- If $\cdot$ is associative, R is an associative ring (always true when $(M, \cdot)$ is a monoid)
- If $\cdot$ is commutative, R is a commutative ring.

Terminology

Let $R = (M, +, \cdot)$ be a ring.

- If $\cdot$ is associative, R is an associative ring (always true when $(M, \cdot)$ is a monoid)
- If $\cdot$ is commutative, R is a commutative ring.
- $(M, +)$ is called the additive group of the ring R.
- $(M, \cdot)$ is called the multiplicative groupoid/semigroup/monoid of the ring R.

Terminology

Let $R = (M, +, \cdot)$ be a ring.

- If $\cdot$ is associative, R is an associative ring (always true when $(M, \cdot)$ is a monoid)
- If $\cdot$ is commutative, R is a commutative ring.
- $(M, +)$ is called the additive group of the ring R.
- $(M, \cdot)$ is called the multiplicative groupoid/semigroup/monoid of the ring R.
- The neutral element of the group $(M, +)$ is called the zero element and is denoted by 0; the inverse element to $a \in M$ is denoted as $-a$.

Terminology

Let $R = (M, +, \cdot)$ be a ring.

- If $\cdot$ is associative, R is an associative ring (always true when $(M, \cdot)$ is a monoid)
- If $\cdot$ is commutative, R is a commutative ring.
- $(M, +)$ is called the additive group of the ring R.
- $(M, \cdot)$ is called the multiplicative groupoid/semigroup/monoid of the ring R.
- The neutral element of the group $(M, +)$ is called the zero element and is denoted by 0; the inverse element to $a \in M$ is denoted as $-a$.
- Inside the ring **we can define the operation subtraction** by

$$a - b := a + (-b).$$

Examples

- $(\mathbb{N}, +, \cdot)$ is not a ring, because $(\mathbb{N}, +)$ is not a group.

Examples

- $(\mathbb{N}, +, \cdot)$ is not a ring, because $(\mathbb{N}, +)$ is not a group.
- $(\mathbb{Z}, +, \cdot)$ is a ring.

Examples

- $(\mathbb{N}, +, \cdot)$ is not a ring, because $(\mathbb{N}, +)$ is not a group.
- $(\mathbb{Z}, +, \cdot)$ is a ring.
- The trivial ring is $(\{0\}, +, \cdot)$ (if it holds that $0 \cdot 0 = 0$).

Examples

- $(\mathbb{N}, +, \cdot)$ is not a ring, because $(\mathbb{N}, +)$ is not a group.
- $(\mathbb{Z}, +, \cdot)$ is a ring.
- The trivial ring is $(\{0\}, +, \cdot)$ (if it holds that $0 \cdot 0 = 0$).
- The set $(\mathbb{R}^{n,n}, +, \cdot)$ of square real matrices with the usual addition and multiplication is a ring; the zero element is the zero matrix.

Examples

- $(\mathbb{N}, +, \cdot)$ is not a ring, because $(\mathbb{N}, +)$ is not a group.
- $(\mathbb{Z}, +, \cdot)$ is a ring.
- The trivial ring is $(\{0\}, +, \cdot)$ (if it holds that $0 \cdot 0 = 0$).
- The set $(\mathbb{R}^{n,n}, +, \cdot)$ of square real matrices with the usual addition and multiplication is a ring; the zero element is the zero matrix.
- The set of all polynomials (with complex / real / integer coefficients) is a ring; the zero element is the zero polynomial $p(x) = 0$.

Basic properties of rings

In an arbitrary ring $(M, +, \cdot)$, the following holds.

- Left and right distributive law for subtracting, i.e.,

$$a(b - c) = ab - ac.$$

Indeed:

Basic properties of rings

In an arbitrary ring $(M, +, \cdot)$, the following holds.

- Left and right distributive law for subtracting, i.e.,

$$a(b-c) = ab - ac.$$

Indeed:

$$ac + a(b-c) = a(c+b-c) = ab \quad \Longrightarrow \quad a(b-c) = ab - ac.$$

□

Basic properties of rings

In an arbitrary ring $(M, +, \cdot)$, the following holds.

- Left and right distributive law for subtracting, i.e.,

$$a(b-c) = ab - ac.$$

Indeed:

$$ac + a(b-c) = a(c+b-c) = ab \quad \Longrightarrow \quad a(b-c) = ab - ac.$$

□

- Multiplying by the zero element returns the zero element, i.e.,

$$\forall a \in M \qquad a \cdot 0 = 0 \quad \wedge \quad 0 \cdot a = 0.$$

Indeed:

Basic properties of rings

In an arbitrary ring $(M, +, \cdot)$, the following holds.

- Left and right distributive law for subtracting, i.e.,

$$a(b-c) = ab - ac.$$

Indeed:

$$ac + a(b-c) = a(c+b-c) = ab \quad \Longrightarrow \quad a(b-c) = ab - ac.$$

□

- Multiplying by the zero element returns the zero element, i.e.,

$$\forall a \in M \qquad a \cdot 0 = 0 \quad \wedge \quad 0 \cdot a = 0.$$

Indeed:

$$a \cdot 0 = a(a-a) = aa - aa = 0.$$

□

Integral domain

Definition (zero divisors)

*Let $R = (M, +, \cdot)$ be a ring. Two **nonzero** elements $a, b \in M$ such that*

$$a \cdot b = 0$$

are called zero divisors.

Definition (integral domain)

*A commutative ring **without** zero divisors is called an integral domain.*

Examples of integral domains

- $(\mathbb{Z}, +, \cdot)$ is an integral domain.

Examples of integral domains

- $(\mathbb{Z}, +, \cdot)$ is an integral domain.
- Each number ring $(M, +, \cdot)$, where $M \subset \mathbb{C}$ and $+$ and $\cdot$ are classical, is an integral domain.

Examples of integral domains

- $(\mathbb{Z}, +, \cdot)$ is an integral domain.
- Each number ring $(M, +, \cdot)$, where $M \subset \mathbb{C}$ and $+$ and $\cdot$ are classical, is an integral domain.
- The ring $(\mathbb{R}^{n,n}, +, \cdot)$ is **not** an integral domain for $n \geq 2$, because it is not commutative; moreover, it has zero divisors:

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Definition of field

Definition (field)

A ring $T = (M, +, \cdot)$ is a field if $(M \setminus \{0\}, \cdot)$ is an Abelian group. This group is called the multiplicative group of the field T.

Definition of field

Definition (field)

A ring $T = (M, +, \cdot)$ is a field if $(M \setminus \{0\}, \cdot)$ is an Abelian group. This group is called the multiplicative group of the field T.

Why do we have to remove the zero element?

Because the zero has no inverse (with respect to the multiplication), i.e., it is not possible to divide by zero: $0^{-1} =?!$.

We can divide by all other elements of the field!

$$\text{dividing} := \text{multiplying by the inverse element}$$

$$\frac{a}{b} := a \cdot b^{-1} \quad \text{for } b \neq 0.$$

Examples of fields

- The ring of integers $(\mathbb{Z}, +, \cdot)$ is **not** a field, because $(\mathbb{Z} \setminus \{0\}, \cdot)$ misses some inverse elements.

Examples of fields

- The ring of integers $(\mathbb{Z}, +, \cdot)$ is **not** a field, because $(\mathbb{Z} \setminus \{0\}, \cdot)$ misses some inverse elements.

- The ring of rational numbers $(\mathbb{Q}, +, \cdot)$ is a field. Moreover, it is the smallest number field (with the common arithmetical operations).

Examples of fields

- The ring of integers $(\mathbb{Z}, +, \cdot)$ is **not** a field, because $(\mathbb{Z} \setminus \{0\}, \cdot)$ misses some inverse elements.

- The ring of rational numbers $(\mathbb{Q}, +, \cdot)$ is a field. Moreover, it is the smallest number field (with the common arithmetical operations).

- The smallest field is the so-called trivial field $(\{0, 1\}, +, \cdot)$, with operations given by the following tables:

$+$	0	1
0	0	1
1	1	0

and

$\cdot$	0	1
0	0	0
1	0	1

The first table corresponds to the bit operation `XOR` and the latter to `AND`, or, alternatively, to the addition and multiplication modulo 2.

Some properties

In each field all usual arithmetical operations are defined:

addition, *subtraction*, *multiplication*, *division*, and all operations derived from them such as *rising to the power*, *root extractions*, *logaritm*, ...

Using the trivial field we have all these operations over one bit. Later we will show how to extend them to any number of bits.

Some properties

In each field all usual arithmetical operations are defined:

addition, *subtraction*, *multiplication*, *division*, and all operations derived from them such as *rising to the power*, *root extractions*, *logaritm*, ...

Using the trivial field we have all these operations over one bit. Later we will show how to extend them to any number of bits.

Theorem

Each field is an integral domain.

Some properties

In each field all usual arithmetical operations are defined:

addition, *subtraction*, *multiplication*, *division*, and all operations derived from them such as *rising to the power*, *root extractions*, *logaritm*, ...

Using the trivial field we have all these operations over one bit. Later we will show how to extend them to any number of bits.

Theorem

Each field is an integral domain.

Proof.

Since the multiplicative group of the field $(M \setminus \{0\}, \cdot)$ is closed under multiplication, for all nonzero a, b it holds that their product $a \cdot b \in M \setminus \{0\}$ is again nonzero. □

Homomorphism and isomorphism

Definition

A mapping f from the ring (resp. field) R_1 to the ring (resp. field) R_2 is a homomorphism if f is a homomorphism of the corresponding additive and multiplicative groupoids (resp. groups).
If, moreover, f is bijective (injective and surjective), it is an isomorphism.

Finite fields

A field with finite number of elements is called finite.
The number of elements is said to be the order of the field.

Finite fields

A field with finite number of elements is called finite.
The number of elements is said to be the order of the field.

An example of finite field is the set (of residue classes modulo p)

$$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$$

with operations modulo a **prime** p (see previous lectures).

E.g., for $p = 5$ we obtain the field with following operations:

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

and

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Additive group $(\mathbb{Z}_p, +_p)$

- The order of the group $\mathbb{Z}_p^+ = (\mathbb{Z}_p, +_p)$ is the prime number p.
- Each nonzero element is a generator (this holds for all groups with prime order).
- $\mathbb{Z}_p^+ = (\mathbb{Z}_p, +_p)$ is a group even when p is not prime.

Multiplicative group $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$

- The order of the group $\mathbb{Z}_p^\times = (\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ is $p-1$ and this is never a prime number for $p \neq 3$!
- $\mathbb{Z}_p^\times$ is cyclic (i.e., there exists a generator).
- The number of generators depends on $p-1$, and is equal to the number of numbers coprime to $p-1$, i.e., $\varphi(p-1)$.
- If k with $k < p$ divides $p-1$, then there exists a subgroup in $\mathbb{Z}_p^\times$ of order k and it contains just the elements for which $a^k = 1$.

Orders of fields?

We have shown a construction of a finite field of order p with p prime.
Are there fields of any arbitrary order?

Orders of fields?

We have shown a construction of a finite field of order p with p prime.
Are there fields of any arbitrary order?

Theorem

Any finite field has ***order*** $\mathbf{p^n}$*, where* p *is a prime number and* n *is a positive natural number.*
(The prime number p *is called the characteristic of the field.)*
Furthermore, all fields of order p^n *are isomorphic.*
Additionally, the multiplicative group of a finite field is cyclic.

Orders of fields?

We have shown a construction of a finite field of order p with p prime.
Are there fields of any arbitrary order?

Theorem

Any finite field has ***order*** $\mathbf{p^n}$*, where* p *is a prime number and* n *is a positive natural number.*
(The prime number p *is called the characteristic of the field.)*
Furthermore, all fields of order p^n *are isomorphic.*
Additionally, the multiplicative group of a finite field is cyclic.

Consequence: There are no fields of order 6, 10, 12, 14, ...

If we chose $p = 2$ and $n = 8$, we obtain the field providing us with arithmetic on 1 byte (8 bits)!

Symmetric cryptography

Secure exchange of longer text performed by asymmetric ciphers (RSA, Diffie-Hellman and others) is not effective.

That is why the **symmetric ciphers** are used: symmetric ciphers assume that (and take advantage of) Alice and Bob share some secret key.
Asymmetric ciphers are used only for exchanging this private key.

A very common method is the block cipher called **A**dvanced **E**ncryption **S**tandard (AES).
Here we get acquainted with the mathematics underlying this method.

AES block cipher

The text we want to securely transfer is divided into (e.g.) blocks having 8 bits. Then, these blocks are encoded using the shared key so that the decoding can be easily made using the same key.

This cipher AES is based on the fact that arithmetic operations with $n = 8$ bits can be understood as operations in a finite field with 2^n elements for $n = 8$. The fields with 2^n elements are called binary fields and are denoted $GF(2^n)$ (as *Galois Fields*).

We now explain how to define addition and multiplication in these fields.

The wrong way

Consider a field $GF(2^8)$. Each element can be represented as an 8 bit string, e.g., 11010110, 01100011, etc.

Addition: Addition can be defined component-wise modulo 2. i.e.

$$11010110 + 01100011 = (1 +_2 0)(1 +_2 1) \cdots (0 +_2 1) = 10110101.$$

The wrong way

Consider a field $GF(2^8)$. Each element can be represented as an 8 bit string, e.g., 11010110, 01100011, etc.

Addition: Addition can be defined component-wise modulo 2. i.e.

$$11010110 + 01100011 = (1 +_2 0)(1 +_2 1) \cdots (0 +_2 1) = 10110101.$$

The neutral (zero) element is 00000000, and each element is inverse to itself. We have an additive group.

The wrong way

Consider a field $GF(2^8)$. Each element can be represented as an 8 bit string, e.g., 11010110, 01100011, etc.

Addition: Addition can be defined component-wise modulo 2. i.e.

$$11010110 + 01100011 = (1 +_2 0)(1 +_2 1) \cdots (0 +_2 1) = 10110101.$$

The neutral (zero) element is 00000000, and each element is inverse to itself. We have an additive group.

Multiplication: Multiplication cannot be defined component-wise: The neutral element would be 11111111 and the inverse to (e.g.) 11111110 would not exist.

The wrong way

Consider a field $GF(2^8)$. Each element can be represented as an 8 bit string, e.g., 11010110, 01100011, etc.

Addition: Addition can be defined component-wise modulo 2. i.e.

$$11010110 + 01100011 = (1 +_2 0)(1 +_2 1) \cdots (0 +_2 1) = 10110101.$$

The neutral (zero) element is 00000000, and each element is inverse to itself. We have an additive group.

Multiplication: Multiplication cannot be defined component-wise: The neutral element would be 11111111 and the inverse to (e.g.) 11111110 would not exist.

Multiplication must be defined in a different way!

Rings of polynomials over a ring / field

In order to be able to add, subtract, and multiply a polynomial of the form $\sum_i a_i x^i$, we only need to know how to add, subtract, and multiply the coefficients.

In general, we can construct a ring of polynomials over an arbitrary ring or field similar to the one we know from real or complex numbers.

Rings of polynomials over a ring / field

In order to be able to add, subtract, and multiply a polynomial of the form $\sum_i a_i x^i$, we only need to know how to add, subtract, and multiply the coefficients.

In general, we can construct a ring of polynomials over an arbitrary ring or field similar to the one we know from real or complex numbers.

Definition

Let K be a ring. The commutative ring of polynomials over K, denoted $K[x]$, is the set of polynomials with coefficients in K together with operations of addition and multiplication defined as:

$$\left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{n} (a_i + b_i) x^i;$$

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{i=0}^{n+m} \left(\sum_{j+k=i} a_j b_k\right) x^i.$$

Irreducible polynomial

Definition

Let K be a field and $P(x) \in K[x]$ be of degree at least 1.
We say that $P(x)$ is irreducible over K if, for any two polynomials $A(x)$ and $B(x)$ from $K[x]$, it holds that

$$A(x) \cdot B(x) = P(x) \quad \Rightarrow \quad \big(\text{degree of } A(x) = 0 \quad \vee \quad \text{degree of } B(x) = 0\big).$$

Irreducible polynomial

Definition

Let K be a field and $P(x) \in K[x]$ be of degree at least 1.
We say that $P(x)$ is irreducible over K if, for any two polynomials $A(x)$ and $B(x)$ from $K[x]$, it holds that

$$A(x) \cdot B(x) = P(x) \quad \Rightarrow \quad \big(\text{degree of } A(x) = 0 \quad \vee \quad \text{degree of } B(x) = 0\big).$$

Irreducible polynomials are primes among polynomials!
Their definition is analogous as well as their properties.

Example: Whereas $x^2 + 1$ is irreducible over the field $\mathbb{Q}$, the polynomial $x^2 - 1 = (x + 1)(x - 1)$ is not.

Irreducible polynomial

Definition

Let K be a field and $P(x) \in K[x]$ be of degree at least 1.
We say that $P(x)$ is irreducible over K if, for any two polynomials $A(x)$ and $B(x)$ from $K[x]$, it holds that

$$A(x) \cdot B(x) = P(x) \quad \Rightarrow \quad \big(\text{degree of } A(x) = 0 \quad \vee \quad \text{degree of } B(x) = 0\big).$$

Irreducible polynomials are primes among polynomials!
Their definition is analogous as well as their properties.

Example: Whereas $x^2 + 1$ is irreducible over the field $\mathbb{Q}$, the polynomial $x^2 - 1 = (x + 1)(x - 1)$ is not.

Remark: $x^2 + 1$ is irreducible over the field $\mathbb{Q}$, but not over the field $\mathbb{Z}_2$, where the coefficients are added and multiplied modulo 2:

$$x^2 + 1 = (x + 1)(x + 1) = x^2 + 2x + 1.$$

Irreducible polynomial as a modulus

We define modulo polynomial as:

$$A(x) \pmod{P(x)} := \text{the remainder of the division of } A(x) \text{ by } P(x).$$

The result is always a polynomial of degree less than the degree of $P(x)$.

Irreducible polynomial as a modulus

We define modulo polynomial as:

$$A(x) \pmod{P(x)} := \text{ the remainder of the division of } A(x) \text{ by } P(x).$$

The result is always a polynomial of degree less than the degree of $P(x)$.

Example: for $A(x) = x^3$ and $P(x) = x^2 + 1$ we have $A(x) = x(x^2 + 1) + (-x)$ and thus

$$x^3 \equiv -x \pmod{x^2 + 1}.$$

If $P(x)$ is irreducible (with respect to the field from which the coefficients are taken), the remainders after division by $P(x)$ form a group (if we again remove the zero polynomial).

Field $GF(2^4)$

The elements $GF(2^4)$ are represented as polynomials of order at most 3 with coefficients h_i from the field $\mathbb{Z}_2$:

$$h_3x^3 + h_2x^2 + h_1x + h_0 \approx (h_3h_2h_1h_0)_2.$$

Thus, the 16 elements of $GF(2^4)$ are:

$$0,\ 1,\ x,\ x+1,\ \ldots,\ x^3+x^2+x+1$$

or

$$0000,\ 0001,\ 0010,\ 0011,\ \ldots,\ 1111.$$

Field $GF(2^4)$

The elements $GF(2^4)$ are represented as polynomials of order at most 3 with coefficients h_i from the field $\mathbb{Z}_2$:

$$h_3x^3 + h_2x^2 + h_1x + h_0 \approx (h_3h_2h_1h_0)_2.$$

Thus, the 16 elements of $GF(2^4)$ are:

$$0,\ 1,\ x,\ x+1,\ \ldots,\ x^3+x^2+x+1$$

or

$$0000,\ 0001,\ 0010,\ 0011,\ \ldots,\ 1111.$$

Addition component-wise modulo 2:

$$(x^3+x+1)+(x^2+x+1) = x^3+x^2.$$

Field $GF(2^4)$ – multiplication

Multiplication modulo a chosen irreducible polynomial, e.g., $x^4 + x + 1$.

Example: multiplication $A(x) \cdot B(x)$ for $A(x) = x^3 + x^2 + 1 \approx 1101$ and $B(x) = x^2 + x \approx 0110$.

Field $GF(2^4)$ – multiplication

Multiplication modulo a chosen irreducible polynomial, e.g., $x^4 + x + 1$.

Example: multiplication $A(x) \cdot B(x)$ for $A(x) = x^3 + x^2 + 1 \approx 1101$ and $B(x) = x^2 + x \approx 0110$.

1. Multiply $A(x) \cdot B(x)$ classically and rewrite coefficients mod 2:

$$A(x) \cdot B(x) = x^5 + 2x^4 + x^3 + x^2 + x = x^5 + x^3 + x^2 + x.$$

Field $GF(2^4)$ – multiplication

Multiplication modulo a chosen irreducible polynomial, e.g., $x^4 + x + 1$.

Example: multiplication $A(x) \cdot B(x)$ for $A(x) = x^3 + x^2 + 1 \approx 1101$ and $B(x) = x^2 + x \approx 0110$.

1. Multiply $A(x) \cdot B(x)$ classically and rewrite coefficients mod 2:

$$A(x) \cdot B(x) = x^5 + 2x^4 + x^3 + x^2 + x = x^5 + x^3 + x^2 + x.$$

2. Find the remainder after division by $P(x)$. Since

$$x^5 = x(x^4 + x + 1) + (x^2 + x), \quad \text{it holds} \quad x^5 \equiv x^2 + x \pmod{x^4 + x + 1},$$

and we have

$$x^5 + x^3 + x^2 + x \equiv (x^2 + x) + (x^3 + x^2 + x) \equiv \mathbf{x^3} \pmod{x^4 + x + 1}.$$

Field $GF(2^4)$ – multiplication

Multiplication modulo a chosen irreducible polynomial, e.g., $x^4 + x + 1$.

Example: multiplication $A(x) \cdot B(x)$ for $A(x) = x^3 + x^2 + 1 \approx 1101$ and $B(x) = x^2 + x \approx 0110$.

1. Multiply $A(x) \cdot B(x)$ classically and rewrite coefficients mod 2:

$$A(x) \cdot B(x) = x^5 + 2x^4 + x^3 + x^2 + x = x^5 + x^3 + x^2 + x.$$

2. Find the remainder after division by $P(x)$. Since

$$x^5 = x(x^4 + x + 1) + (x^2 + x), \quad \text{it holds} \quad x^5 \equiv x^2 + x \pmod{x^4 + x + 1},$$

and we have

$$x^5 + x^3 + x^2 + x \equiv (x^2 + x) + (x^3 + x^2 + x) \equiv \mathbf{x^3} \pmod{x^4 + x + 1}.$$

Hence we get that $1101 \cdot 0110 = 1000 \pmod{x^4 + x + 1}$.

AES in field $GF(2^8)$

According to the specification of AES, the multiplication is done modulo

$$x^8 + x^4 + x^3 + x + 1.$$

Construction of a finite field

In general, we construct a finite field $GF(p^k)$ using polynomials as follows.

Let $m(x) \in \mathbb{Z}_p[x]$ be an irreducible polynomial of degree k.

$$GF(p^k) = \Big(\{q(x) \in \mathbb{Z}_p[x] \colon \deg(q) < k\}, \quad +, \quad \cdot \bmod m(x) \Big).$$