Week 7
Binary Operations
Discrete Math

Marie Demlová
http://math.fel.cvut.cz/en/people/demlova

March 31, 2022

Residue Classes Modulo n

Properties of $\oplus$.

- $\oplus$ is associative, i.e. for any three integers i, j, k we have:

$$([i]_n \oplus [j]_n) \oplus [k]_n = [i]_n \oplus ([j]_n \oplus [k]_n).$$

- $\oplus$ is commutative, i.e. for any two integers i, j we have:

$$[i]_n \oplus [j]_n = [j]_n \oplus [i]_n.$$

- The class $[0]_n$ plays the role of "zero", more precisely, for any integer i we have:

$$[0]_n \oplus [i]_n = [i]_n.$$

- We can "subtract", more precisely for any integer $[i]_n$ there exists class $-[i]_n$ such that

$$[i]_n \oplus (-[i]_n) = [0]_n.$$

Residue Classes Modulo n

Properties of the Operation $\odot$.

- $\odot$ is associative, i.e for any three integers i, j, k we have:

$$([i]_n \odot [j]_n) \odot [k]_n = [i]_n \odot ([j]_n \odot [k]_n).$$

- $\odot$ is commutative, i.e. for any two integers i, j we have:

$$[i]_n \odot [j]_n = [j]_n \odot [i]_n.$$

- The class $[1]_n$ plays the role of "identity", More precisely, for any integer i we have:

$$[1]_n \odot [i]_n = [i]_n.$$

For a residue class $[i]_n$ there is a residue class $[x]_n$ such that

$$[i]_n \odot [x]_n = [1]_n$$

iff the numbers i and n are relatively prime.

Residue Classes Modulo n

Convention.

Later on we will write $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ instead of $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ and the operations $\oplus$, $\odot$ will be denoted by an "ordinary signs", i.e. simply by $+$ and $\cdot$.

Note that we can write that in $\mathbb{Z}_n$ for every $i, j \in \mathbb{Z}_n$

$$i + j = k, \quad \text{where } k \text{ is the remainder when } i + j \text{ is divided by } n;$$

$$i \cdot j = l, \quad \text{where } l \text{ is the remainder when } i\,j \text{ is divided by } n.$$

RSA cryptosystem

Alice and Bob want to exchange messages – numbers.

Alice:

- chooses two big prime numbers p and q and their product $N = p \cdot q$;
- chooses a number e_A coprime to $\phi(N) = (p-1)(q-1)$;
- computes d_A for which
$$d_A \cdot e_A \equiv 1 \pmod{\phi(N)}.$$
- makes public: N, and e_A.
- Secret: p, q, $\phi(N)$, and d_A.

RSA cryptosystem

Bob:

- wants to send a message x, a number $0 < x < N$.
- He computes y, $0 < y < N$ such that
$$x^{e_A} \equiv y \pmod{N},$$
- sends y to Alice.

Alice receives y, computes z, $0 < z < N$ for which

$$y^{d_A} \equiv z \pmod{N}.$$

Fact.

It holds that $z = x$. is the message went by Bob.

Groupoids, Semigroups, Monoids

A binary operation on a set S is any mapping from the set of all pairs $S \times S$ into the set S.

A pair $(S, \circ)$ where S is a set and $\circ$ is a binary operation on S is a groupoid.

Examples of groupoids.

1) $(\mathbb{R}, +)$ where $+$ is addition on the set of all real numbers.
3) $(\mathbb{N}, +)$ where $+$ is addition on the set of all natural numbers.
4) $(\mathbb{R}, \cdot)$ where $\cdot$ is multiplication on the set of all real numbers.
6) $(M_n, \cdot)$ where M_n is the set of all square matrices of order n, and $\cdot$ is multiplication of matrices.
7) $(\mathbb{Z}_n, \oplus)$ for any $n > 1$.
8) $(\mathbb{Z}_n, \odot)$ for any $n > 1$.
9) $(\mathbb{Z}, -)$, where $-$ is subtraction on the set of all integers.

Groupoids, Semigroups, Monoids

Examples which are not groupoids.

- $(\mathbb{N}, -)$ is not a groupoid because subtraction is not a binary operation on $\mathbb{N}$. Indeed, $3 - 4$ is not a natural number.
- $(\mathbb{Q}, :)$, where $:$ is the division, because $1 : 0$ is not defined.

Semigroups.

A groupoid $(S, \circ)$ is a semigroup if for every $x, y, z \in S$ we have

$$x \circ (y \circ z) = (x \circ y) \circ z$$

The above law is called associative law.

The associative law allows to write $a_1 \circ a_2 \circ a_3$ for $(a_1 \circ a_2) \circ a_3$ or $a_1 \circ (a_2 \circ a_3)$.

Similarly, we write

$$a_1 \circ a_2 \circ \ldots \circ a_n$$

independently on the brackets.

Groupoids, Semigroups, Monoids

Examples of semigroups.

1) $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{N}, +)$.
2) $(\mathbb{R}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{N}, \cdot)$.
3) $(\mathbb{Z}_n, \oplus)$, $(\mathbb{Z}_n, \odot)$.
4) $(M_n, +)$, $(M_n, \cdot)$, where M_n is the set of square real matrices of order n and $+$ and $\cdot$ is addition and multiplication, respectively, of matrices.
5) $(A, \circ)$ where A is the set of all mappings $f : X \to X$ for a set X, and $\circ$ is the composition of mappings.

Examples of groupoids which are not semigroups.

- $(\mathbb{Z}, -)$, i.e. the set of all integers with subtraction. Indeed, $2 - (3 - 4) = 3$ but $(2 - 3) - 4 = -5$.
- $(\mathbb{R} \setminus \{0\}, :)$, i.e. the set of non-zero real numbers together with the division $:$. Indeed, $4 : (2 : 4) = 8$, but $(4 : 2) : 4 = \frac{1}{2}$.

Groupoids, Semigroups, Monoids

Neutral element. Given a groupoid $(S, \circ)$. An element $e \in S$ is a neutral (also *identity*) element if

$$e \circ x = x = x \circ e \quad \text{for every } x \in S.$$

Examples of neutral elements.

1) For $(\mathbb{R}, +)$ the number 0 is its neutral element, the same holds for $(\mathbb{Z}, +)$.
2) For $(\mathbb{R}, \cdot)$ the number 1 is its neutral (identity) element, the same holds for $(\mathbb{Z}, \cdot)$, and $(\mathbb{N}, \cdot)$.
3) For $(M_n, \cdot)$ where $\cdot$ is the multiplication of square matrices of order n the identity matrix is its neutral (identity) element.
4) $(\mathbb{Z}_n, \oplus)$ has the class $[0]_n$ as its neutral element.
5) $(\mathbb{Z}_n, \odot)$ has the class $[1]_n$ as its neutral (identity) element.

Groupoids, Semigroups, Monoids

Example of a groupoid that does not have a neutral element. The groupoid $(\mathbb{N} \setminus \{0\}, +)$. Indeed, there is not a positive number e for which $n + e = n = e + n$ for every positive $n \in \mathbb{N}$

Proposition. Given a groupoid $(S, \circ)$. If there exist elements e and f such that for every $x \in S$ we have $e \circ x = x$ and $x \circ f = x$, then $e = f$ is the neutral element of $(S, \circ)$.

Groupoids, Semigroups, Monoids

Monoid. If in a semigroup $(S, \circ)$ there exists a neutral element then we call $(S, \circ)$ a monoid.

The fact that $(S, \circ)$ is a monoid with the neutral element e is shortened to $(S, \circ, e)$.

Powers in a monoid. Given a monoid $(S, \circ, e)$ and its element $a \in S$. The powers of a are defined by:

$$a^0 = e, \quad a^{i+1} = a^i \circ a \text{ for every } i \geq 0.$$

Invertible element. Given a monoid $(S, \circ, e)$. An element $a \in S$ is invertible if there exists an element $y \in S$ such that

$$a \circ y = e = y \circ a.$$

Groupoids, Semigroups, Monoids

Proposition. Given a monoid $(S, \circ, e)$. If there are elements $a, x, y \in S$ such that

$$x \circ a = e \text{ and } a \circ y = e,$$

then $x = y$.

Inverse element. Let $(S, \circ, e)$ be a monoid, and $a \in S$ an invertible element. Let $y \in S$ satisfy

$$a \circ y = e = y \circ a.$$

Then y is the inverse element to a and is denoted by a^{-1}.

Groupoids, Semigroups, Monoids

Proposition.

Let $(S, \circ, e)$ be a monoid. Then

- e is invertible and $e^{-1} = e$.
- If a is invertible then so is a^{-1}, and we have $(a^{-1})^{-1} = a$.
- If a and b are invertible elements then so is $a \circ b$, and we have $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Cancellation by an inverse element.

Let $(S, \circ, e)$ be a monoid, and let $a \in S$ is its invertible element. Then

$$a \circ b = a \circ c, \quad \text{or} \quad b \circ a = c \circ a \quad \text{implies} \quad b = c.$$

Groups

Groups. A monoid $(S, \circ, e)$ in which every element is invertible is called a group.

Examples of groups.

- The monoid $(\mathbb{R}, +, 0)$. Indeed, for every $x \in \mathbb{R}$ there exists $-x$ for which $x + (-x) = 0 = (-x) + x$.
- The monoid $(\mathbb{Z}, +, 0)$. Indeed, for each integer x there exists an integer $-x$ for which $x + (-x) = 0 = (-x) + x$.
- The monoid $(\mathbb{R}^+, \cdot, 1)$, where $\mathbb{R}^+$ is the set of all positive real numbers. Indeed, for every positive real number x there exists a positive real number $\frac{1}{x}$ for which $x \cdot \frac{1}{x} = 1 = \frac{1}{x} \cdot x$.
- The monoid $(\mathbb{Z}_n, \oplus, [0]_n)$. Indeed, for a class $[i]_n$ there exists a class $[n-i]_n$ for which $[i]_n \oplus [n-i]_n = [0]_n = [n-i]_n \oplus [i]_n$.

Groups

Examples.

- The monoid $(\mathbb{Z}, \cdot, 1)$ is not a group. Indeed, for example 2 is not invertible.
- The monoid $(\mathbb{Z}_n, \odot, [1]_n)$ is not a group. Indeed, the class $[0]_n$ is not invertible because for any $[i]_n$ we have $[0]_n \odot [i]_n = [0]_n \neq [1]_n$.
- Let A be the set of all permutation of $\{1, 2, \ldots, n\}$, and let $\circ$ be the composition. Then $(A, \circ)$ is a group. Indeed, it is a monoid with the neutral element id; moreover, every permutation ϕ has its inverse permutation ϕ^{-1}.
- Let B be the set of all mappings from the set $\{1, 2, \ldots, n\}$ into itself, where $n > 1$. Let $\circ$ be the composition. Then $(B, \circ, id)$ is not a group; indeed, it is a monoid but any mapping that is not one-to-one is not invertible.

Groups

Proposition. Given a group $(S, \circ)$ with its neutral element e. Then for every two elements $a, b \in S$ there exist unique $x, y \in S$ such that

$$a \circ x = b, \qquad y \circ a = b.$$

Theorem.

A semigroup $(S, \circ)$ is a group if and only if every equation of the form $a \circ x = b$ and every equation of the form $y \circ a = b$ has at least one solution.

More precisely: A semigroup $(S, \circ)$ is a group if and only if for every two elements $a, b \in S$ there exist $x, y \in S$ such that $a \circ x = b$ and $y \circ a = b$.

Groups

Commutative semigroups, monoids, groups.

A semigroup $(S, \circ)$ (monoid, group) is called commutative if it satisfies the *commutative law*, i.e. for every two elements $x, y \in S$

$$x \circ y = y \circ x.$$