**2.3.11 RSA Cryptosystem** Alice and Bob want to exchange messages – numbers.

Alice chooses two big prime numbers $p$ and $q$ and their product $N = p \cdot q$. Further, she chooses a number $e_A$ coprime to $\varphi(N) = (p-1)(q-1)$. Finally, she computes $e_A$ for which

$$d_A \cdot e_A \equiv 1 \,(\mathrm{mod}\, \varphi(N)).$$

Alice publishes: $N$, and $d_A$.

Secret: $p$, $q$, $\varphi(N)$, and $e_A$.

Bob wants to send a message $x$, a number $0 < x < N$. He computes $y$, $0 < y < N$ such that

$$x^{d_A} \equiv y \,(\mathrm{mod}\, N),$$

and sends $y$ to Alice.

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

$$y^{e_A} \equiv z \,(\mathrm{mod}\, N).$$

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

**2.3.12 Proof of the fact that $x = z$.** We know that

$$z = \left(x^{d_A}\right)^{e_A} = x^{d_A \cdot e_A}.$$

Moreover,

$$d_A \cdot e_A = 1 + k\,(p-1)\,(q-1).$$

First, we shall prove that $x^{d_A\, e_A} \equiv x \,(\mathrm{mod}\, p)$. We know that $x^{d_A\, e_A} = x^{1+k(p-1)(q-1)}$. Hence it suffices to show that

$$x^{1+m(p-1)} \equiv x \,(\mathrm{mod}\, p).$$

And this is an easy induction based on the following fact (which uses that $p$ is a prime and therefore $x^p \equiv x \,(\mathrm{mod}\, p)$.

$$x^{1+m(p-1)} = x^{1+p-1+(m-1)(p-1)} = x^p \cdot x^{(m-1)(p-1)} \equiv x \cdot x^{(m-1)(p-1)} = x^{1+(m-1)(p-1)}.$$

Similarly, it can be shown that

$$x^{d_A\, e_A} \equiv x \,(\mathrm{mod}\, q).$$

To finish the proof, it suffices to show that: If $z \equiv x \,(\mathrm{mod}\, p)$ and $z \equiv x \,(\mathrm{mod}\, q)$ for $p, q$ coprime, then $z \equiv x \,(\mathrm{mod}\, p \cdot q)$.

We have $z \equiv x \,(\mathrm{mod}\, p)$ means $z - x = k \cdot p$, $z \equiv x \,(\mathrm{mod}\, q)$ means $z - x = l \cdot q$. Hence, $k \cdot p = l \cdot q$. Since $p$ and $q$ are coprime and $p$ divides $l \cdot q$, $p$ must divide $l$. Hence $l = s \cdot p$ and $z - x = s \cdot p \cdot q$ which means that $x \equiv z\ (N)$, Because $0 \leq x, z < N$ necessarily $x = z$.

# Chapter 3

# Binary Operations

In the last lecture, we introduced the residue classes $\mathbb{Z}_n$ together with their addition and multiplication. We have also shown some properties that these two operations have. Today, we will study sets together with one operation in general and try to derive some properties that can be used regardless how an operation is defined and what elements a set has. We will define item-by-item groupids (the most general case), semigroups (groupoids that satisfy the associativity law), monoids (semigroups with a neutral element), and groups (monoids where every element is invertible).

## 3.1 Groupoids, Semigroups, Monoids

**3.1.1 Groupoids.** The most general notion of this section is the notion of a groupoid.

**Definition.** 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 called a *groupoid*. □

Note that the only condition for a binary operation on $S$ is that **for every** pair of elements of $S$ their result must be defined and must be an element in $S$.

A binary operation is usually denoted by $\cdot$, or $+$, $\circ$, $\star$ etc. (A binary operation $\circ$ assigns to elements $x, y$ the element $x \circ y$.)

**Examples of groupoids.** The following are groupoids.

1) $(\mathbb{R}, +)$ where $+$ is addition on the set of all real numbers.
2) $(\mathbb{Z}, +)$ where $+$ is addition on the set of all integers.
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.
5) $(\mathbb{Z}, \cdot)$ where $\cdot$ is multiplication on the set of all integers.
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.

**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.

**3.1.2 Semigroups.** General groupoids are structures where it is rather difficult to "calculate". Indeed, if we want to "multiply" four elements we must know in which order to do it. It means whether it is $a \circ ((b \circ c) \circ d)$, or $a \circ ((b \circ c) \circ d)$, or one of the other two possibilities. First, we will be interested in groupoids where we do not need to use brackets, these will be groupoids where the associative law holds.

**Definition.** Given a groupoid $(S, \circ)$. If for every $x, y, z \in S$ we have

$$x \circ (y \circ z) = (x \circ y) \circ z \tag{3.1}$$

$(S, \circ)$ is called a *semigroup*. □

The property 3.1 is called the *associative law*.

**Examples of semigroups.** The following groupoids are 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 $f\colon X \to X$ 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 nonzero real numbers together with the division :. Indeed, $4 : (2 : 4) = 8$, but $(4 : 2) : 4 = \frac{1}{2}$.

**3.1.3 Neutral (Identity) Element.** A groupoid $(S, \circ)$ may or may not have an element that "does not change" anything if it is used. The precise definition is given bellow.

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

$$e \circ x = x = x \circ e \quad \text{for every } x \in S. \tag{3.2}$$

□

If the operation is denoted by $\cdot$ then we usually use the term "identity element" instead of a neutral element.

**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.

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

**3.1.4 Uniqueness of the Neutral Element.** The following proposition shows that if a groupoid $(S, \circ)$ has its neutral element then it is unique.

**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 $(S, \circ)$. □

*Justification.* Consider the product $e \circ f$. From the property of $e$ we have $e \circ f = f$ (indeed, take $x = f$); from the property of $f$ we have $e \circ f = e$ (indeed, take $x = e$). Hence $e = f$, and in this case $e$ is the neutral element. □

**3.1.5 Monoids.** We will be mainly interested in semigroups which have the neutral element; they will be called monoids.

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

In the paragraph above, we gave couple of examples of monoids and also an example of a semigroup which is not a monoid.

**Convention.** In the following text, the fact that $(S, \circ)$ is a monoid with the neutral element $e$ will be shortened to $(S, \circ, e)$.

**3.1.6 Powers in a Monoid.** Similarly as powers are defined in $(\mathbb{R}, \circ, 1)$ we can introduce powers in an arbitrary monoid.

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

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

□

Note that if the operation is $+$ with neutral element 0 then we write $0\,a = 0$ instead of $a^0$ and $k\,a$ instead of $a^k$.

**3.1.7 Invertible Elements.** In many examples given above, we can somehow "reverse" the operation. For instance, in $(\mathbb{R}, +, 0)$ we can subtract; in $(\mathbb{R}, \cdot, 1)$ we can divide by any nonzero number; in $(M_n, \cdot, E)$ where $M_n$ is the set of all square matrices of order $n$, and $E$ is the identity matrix, we can cancel all the regular matrices (this means multiplying by the inverse matrix to a given regular one). In this paragraph, roughly speaking, we characterize those elements of a monoid that not only permit "cancellation" but "help solving equations". More precisely:

**Definition.** Given a monoid $(S, \circ, e)$. We say that an element $a \in S$ is *invertible* if there exists an element $y \in S$ such that

$$a \circ y = e = y \circ a. \tag{3.3}$$

□

Let us show that if $y$ from 3.3 exists then it is unique.

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

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

then $x = y$. □

*Justification.* Consider the product $x \circ a \circ y$. Since we are in a semigroup it holds that

$$y = e \circ y = (x \circ a) \circ y = x \circ (a \circ y) = x \circ e = x.$$

□

**3.1.8 The Inverse Element.** Since $y$ from 3.3 is unique we can define:

**Definition.** 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 called the *inverse element to* $a$ and is denoted by $a^{-1}$. □

**Remark.** If a binary operation is denoted by $+$ we speak about the *opposite* element (instead of the inverse element) and denote it by $-a$ (instead of $a^{-1}$). The reason is that we sometimes have two different binary operations defined on the same set, (indeed, on the set $\mathbb{R}$ we have both $+$ and $\cdot$), hence it is convenient to distinguish between "inverses" with respect to $+$ and with respect to $\cdot$.

**3.1.9** We know that not every element of a general monoid is invertible. Indeed, consider for example the set of all square matrices together with multiplication and the identity matrix. Then only regular matrices are invertible, and moreover for any regular matrix $A$ it holds that $(A^{-1})^{-1} = A$. The next proposition shows that properties of invertible elements and their inverses are the same in any monoid.

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

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

□

*Justification.*

1. It suffices to notice that $e \circ e = e$, this immediately means that $e^{-1} = e$.

2. Assume that $a$ is invertible. Then we have $a \circ a^{-1} = e = a^{-1} \circ a$. If we look at the last identities we see that $a$ is the element such that if we multiply by it the element $a^{-1}$ we get $e$. Hence $a = (a^{-1})^{-1}$.

3. Assume that $a^{-1}$ and $b^{-1}$ exist. Then

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ e \circ a^{-1} = a \circ a^{-1} = e.$$

Similarly, we get that $(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$. We have shown that $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$. □

**Remark.** Note that **it is not** always the case that $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$. This holds when the operation $\circ$ is commutative, i.e. $x \circ y = y \circ x$ for every $x$ and $y$.