Teaching Mathematics and Statistics in Sciences - IPA HU-SRB/0901/221/088
Interesting Mathematical Problems in Sciences and Everyday Life - 2011

How to use algebraic structures

Branimir Šešelja
Department of Mathematics and Informatics, Faculty of Sciences
University of Novi Sad
Trg D. Obradovića 4, Novi Sad, Serbia
seselja@dmi.uns.ac.rs
http://www.dmi.uns.ac.rs/Faculty/seseljab

Mathematical branches are based on relational and operational structures. These arose in mathematics through orderings, measures, classification, counting and basic operations with numbers. Among relational structures we advance partially ordered sets (posets), lattices and Boolean algebras, the latter satisfying all important ordering properties. These ordered structures appear in nature, and can be visually represented by particular (Hasse) diagrams, in which it is possible to identify relevant properties. There are many examples of posets, lattices and Boolean algebras in the nature, as well as in scientific methods by which the nature is being investigated. In digital technology Boolean functions are applied and used, and in the present context we point out their applications and minimization methods. Operational structures originate in the structures of numbers, which are main examples of groups, rings and fields. Groups of symmetries were investigated in crystallography, quotient groups in coding and error correcting, and finite fields, similarly to Boolean algebras, are applied in defining and investigating performances of semi-conductors and chips.

1. Introduction

The best known and the most important link of mathematics to everyday life are numbers. It is the reason why numbers were the core and the basic source for the creation and development of mathematical topics like e.g., calculus, equations, orderings, functions. Throughout history, usually some basic and frequently used properties of relations and operations with numbers have been investigated: finding solutions of equations, understanding divisibility and distribution of prim numbers, investigating properties of operations like associativity, commutativity and others. General properties of these leaded to development of abstract structures carrying main properties of relations and operations on numbers: partially ordered sets (posets), lattices, Boolean algebras - all connected to relations, and groups, rings, fields - dealing with binary operations originating from addition and multiplication. In this abstract framework, algebra has gone even further, defining and investigating universal algebras and algebraic systems. These are nonempty sets equipped with arbitrary operations and relations, fulfilling identities and first order formulas, including as particular cases all aforementioned structures.

Our aim here is to present basic properties of relational and operational structures which arise in connection with numbers. In one hand these are relational, mostly dealing with equivalence and ordering relations, and in the other we analyze operational structures, represented by groups and rings. For each of these we start with a motivating, usually well known, properties arising in connection with numbers. Then we present abstract and general definitions of a structure we are dealing with, and we derive relevant properties. Finally we switch to examples, dealing again with the most important ones, with structures of numbers. When abstract properties are applied in this context, they can be better understood, obtaining particular meaning in the real word environment.

2. Relational structures

In this section we present two main relational structures which are used in modeling numerous situations in real life and in mathematics. They are based on equivalence relations and on orderings.

Binary relations on a nonempty set are subsets of its square. Hence if A is a nonempty set, universe, then $\rho \subseteq A^2$ is a **binary relation** on A. The ordered pair (A, ρ) is a particular **relational structure**.

If we consider all binary relations on a nonempty set A, then we deal with the power set $P(A^2)$ of all subsets of the square of A. In this collection we can use set-theoretic operations (intersection, union, complementation), but also for a relation ρ we have the **inverse relation**:

$$\rho^{-1} = \{(x, y) \mid (y, x) \in \rho\}.$$

The **diagonal relation** on A consists of ordered pairs with equal components:

$$\Delta = \{(x, x,) \mid x \in A\}.$$

The square A^2 is a **full relation** on A. Apart from intersection and union, there is one more binary operation among relations on A, the **composition of relations**: for $\rho, \theta \subseteq A^2$,

$$\rho \circ \theta = \{(x, y) \mid (\exists z)((x, z) \in \rho \wedge (z, y) \in \theta)\}.$$

The composition of relations is not commutative in general, but it is associative.

2.1. Equivalence relation

Classifying objects according to some property is a frequent procedure in many fields. Grouping individuals in a company so that people in each group are of the same age, or sorting fruits (e.g., apples) in separate boxes so that each contains items of the same size, are some examples; ”being of the same age” or ”having the same size” are equivalence relations, and the classification gives the corresponding quotient set. In mathematics, equality of fractions is obtained by grouping ordered pairs of integers according to the property of having equal cross–products.

Relation ρ on a set A is **reflexive** if it fulfills the following:

$(\forall x)(x, x) \in \rho.$ (r)

This definition implies that *the relation ρ on A is reflexive if and only if $\Delta \subseteq \rho$.*

The relation ρ on A is **symmetric** if for all $x, y \in A$

$(x, y) \in \rho \Rightarrow (y, x) \in \rho.$ (s)

Equivalently, *ρ is symmetric if and only if $\rho \subseteq \rho^{-1}$.*

The relation ρ on A is **transitive** if for all $x, y, z \in A$

$(x, y) \in \rho \wedge (y, z) \in \rho \Rightarrow (x, z) \in \rho.$ (t)

By the definition of composition of relations, *ρ is transitive if and only if $\rho \circ \rho \subseteq \rho$.*

Example 1 a) Relations $=$, $\leqslant$, $\geqslant$, $\mid$ on $\mathbb{N}$ are all reflexive and transitive.

b) Relation of parallelism for lines in a plain:

$p \| q \quad \overset{\text{def}}{\longleftrightarrow}$ *p and q do not intersect or they coincide*

is reflexive, symmetric and transitive, while the orthogonality relation

$p \perp q \ \overset{\text{def}}{\longleftrightarrow}\ p$ *and* q *are perpendicular i.e., form a right angle*

is only symmetric.

c) The relation $\rho = \{(1,1),(1,2),(2,2)\}$ is reflexive on the set $\{1,2\}$, but not on the set $\{1,2,3\}$, since it does not contain the diagonal of the latter.

d) The relation $\rho = \{(x,y) \mid |x-y| < 1\}$ on the set $\mathbb{R}$ of real numbers is reflexive and symmetric, but it is not transitive.

A reflexive, symmetric and transitive relation ρ on A is an **equivalence relation**, **equivalence** on this set.

Example 2 a) Relation of parallelism for lines in a plain (Example 1 b)), parallelism for lines in a space, these are examples of equivalence relations on the corresponding sets of lines.

b) The relation $\equiv_3$ on the set $\mathbb{N}_0 = \{0,1,2,\dots\}$, defined by

$m \equiv_3 n \quad \longleftrightarrow m$ *and* n *have the same reminder when divided by* 3

is an equivalence relation. Number 3 can be replaced by any other positive integer; another equivalence relation on $\mathbb{N}_0$ is obtained.

c) Equality, i.e., diagonal Δ is an equivalence relation on any nonempty set A. It is the smallest (under inclusion) equivalence relation on A: it is included in each equivalence on A, while no proper subset of Δ is reflexive on A, hence it is not an equivalence on this set.

One could prove that neither of the properties (r), (s) and (t) is a consequence of the other two. Hence these properties are *independent*.

Let ρ be an equivalence relation on a set A and for $a \in A$, let

$[a]_\rho := \{x \mid a\rho x\}$ – **equivalence class of** a.

Next, let

$A/\rho := \{[x]_\rho \mid x \in A\}$. – **quotient set**.

Hence, the quotient set A/ρ is a collection of special subsets of A identified by its elements, the subsets being called classes. Each class $[a]_\rho$ contains members of A related (under ρ) to the given element a.

Next we prove that these classes are nonempty, pairwise disjoint and that their union is A.

Theorem 3 *Let* ρ *be an equivalence relation on a set* A *and* $x, y \in A$*. Then*

a) $[x]_\rho \neq \emptyset$*;*

b) $[x]_\rho \cap [y]_\rho \neq \emptyset \ \Rightarrow\ [x]_\rho = [y]_\rho$*;*

c) $\bigcup\{[x]_\rho \mid x \in A\} = A$*.*

Proof. a) For every x in A, due to reflexivity, we have $x\rho x$. Hence at least $x \in [x]_\rho$ and $[x]_\rho$ is nonempty.

b) Suppose $z \in [x]_\rho \cap [y]_\rho$. Hence $x\rho z$ and $y\rho z$. Using this and properties of equivalence relation, we prove that the classes $[x]_\rho$ and $[y]_\rho$ coincide:

$u \in [x]_\rho \Rightarrow x\rho u$, i.e., $u\rho x$; since $x\rho z$, it follows $u\rho z$, and by $z\rho y$ we have $u\rho y$, hence $y\rho u$; therefore $u \in [y]_\rho$, i.e., $[x]_\rho \subseteq [y]_\rho$; analogously one can prove the reverse inclusion, therefore the classes coincide.

c) Every $x \in A$ belongs to $[x]_\rho$; hence A is a subset of the union of classes; the converse is obvious, which completes the proof ■

Observe that an *equivalence class can be represented by each of its elements*: if $y \in [x]_\rho$, then the classes $[y]_\rho$ and $[x]_\rho$ are not disjoint, therefore they are equal; hence, for every $y \in [x]_\rho$, we have $[x]_\rho = [y]_\rho$.

In Set theory there is a special name for the collections bearing properties of quotient sets.

A collection of nonempty, pairwise disjoint subsets of a set A, union of which is A, is called a **partition** of the set A. Sets in partition are its **classes** or **blocks**.

A quotient set A/ρ is thus a partition of A.

Example 4 $a)$ Equivalence classes of the relation $\equiv_3$ (Example 2 b)) are collections of numbers with the same reminder under division by 3:

$\{1, 4, 7, \dots\}$; $\{2, 5, 8, \dots\}$; $\{0, 3, 6, 9, \dots\}$.

This is a partition of the set $\mathbb{N}_0$.

$b)$ The diagonal relation Δ on an arbitrary set A has one-element classes: each element is related only to itself.

$c)$ The relation of parallelism split the collection of all lines in a plain into *directions*: each class consists of mutually parallel lines.

Not only that equivalence classes under an equivalence relation form a partition of the underlying set, but also the converse hold: *a partition on set A determines an equivalence relation on A.* Indeed, it is straightforward to prove that the required equivalence is obtained by relating elements which belong to the same class of the partition.

We come to the final example, showing a typical use of equivalence relations and quotient sets in mathematics.

Example 5 (i) When defining rational numbers as fractions, we start with the ring $(\mathbb{Z}, +, \cdot)$ of integers and we construct the direct product $\mathbb{Z}_1 \times \mathbb{Z}$, where $\mathbb{Z}_1 = \{x \in \mathbb{Z} \mid x \neq 0\}$. Then, on this product we define the relation $\sim$:

$$(a, b) \sim (c, d) \quad \text{if and only if} \quad a \cdot d = b \cdot c.$$

Obviously, $\sim$ is an equivalence relation on the product. Each class represents a fraction denoted by any of its members, and e.g.,

$$\frac{3}{5} = \frac{21}{35}$$

simply means that the corresponding ordered pairs $(5, 3)$ and $(35, 21)$ have equal cross-products: $3 \cdot 35 = 5 \cdot 21$.

(ii) In order to define vectors in an Euclidean plain, we start with ordered pairs of points in this plain. Then we group pairs lying on parallel lines, having the same direction and equal length of the corresponding line segments. This is an equivalence relation on the set of ordered pairs, and each equivalence class is a vector, represented by any of its members.

2.2. Ordering relation

We start with several diagrams of relational structures. They originate in different fields and all of them represent orderings.

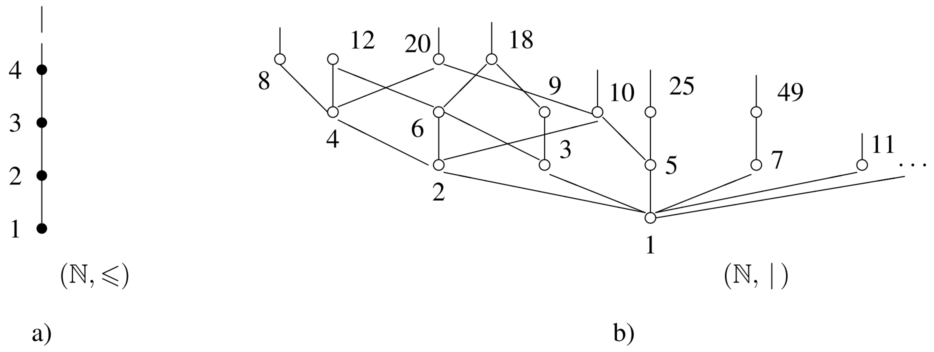


Figure 1

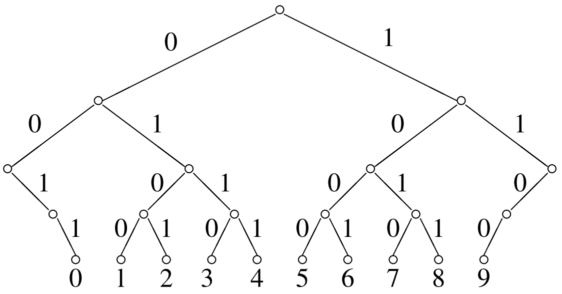
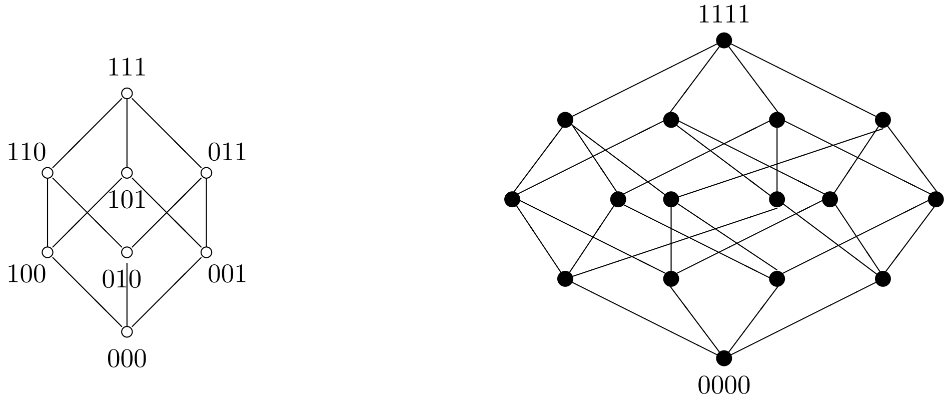


Figure 2



a)

b)

Figure 3

A relation ρ na A is **antisymmetric** if the following holds:

if $x \neq y$ and $x\rho y$, then it is not $y\rho x$. (a)

The implication (a) is tautologically equivalent with the formula

$x\rho y \wedge y\rho x \;\Rightarrow\; x = y.$ (a')

The latter (a') is the second way to formulate the antisymmetry. Finally, the antisymmetry of a relation ρ on a set A is equivalent with the formula: $\rho \cap \rho^{-1} \subseteq \Delta$.

Example 6 a) The relations $<$, $\leqslant$, $>$, $\geqslant$, $|$ on $\mathbb{N}$ are all antisymmetric.

b) On the power set $\mathcal{P}(A)$, the set inclusion $\subseteq$, as well as the strong inclusion $\subset$ are antisymmetric relations.

c) The diagonal Δ of a set A is antisymmetric. It is also symmetric; the diagonal and its nonempty subsets are the only relations which are both, symmetric and antisymmetric.

A relation ρ na A is an **ordering relation**, **order**, or equivalently a **partial order** if it is reflexive, antisymmetric and transitive.

Example 7 a) Basic ordering relations on $\mathbb{N}$ are $\leqslant$ and $|$.

Analogously defined, the relation $\leqslant$ is an order also on the other sets of numbers: $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$.

b) On the power set $\mathcal{P}(A)$ of an arbitrary set A, inclusion $\subseteq$ is an ordering relation.

If ρ is an ordering relation on A, then we say that A is **ordered** by ρ. The relational structure (A, ρ) is said to be an **ordered set**, or equivalently a **partially** ordered set, a **poset**.

If ρ is an order on A, then the inverse relation ρ^{-1} is an ordering on A as well. For the reflexivity and transitivity this is almost straightforward, and the antisymmetry of ρ^{-1} follows from the formula $\rho \cap \rho^{-1} \subseteq \Delta$. The relation ρ^{-1} is the **dual order** for ρ.

An ordering ρ on A is **linear** or **total** if it fulfills additional property:

for all $x, y \in A, \quad x\rho y \vee y\rho x. \qquad (\ell)$

Example 8 The well known posets on numbers are $(\mathbb{N}, \leqslant)$, $(\mathbb{N}, |)$, $(\mathbb{Z}, \leqslant)$, $(\mathbb{R}, \leqslant\ )$.

Also $(\mathcal{P}(A), \subseteq)$ is a poset, A being an arbitrary set.

Apart from the latter and the poset $(\mathbb{N}, |)$, all others in this example are linearly ordered.

For most of the listed posets, well known are also the dually ordered ones: $(\mathbb{N}, \geqslant)$, $(\mathbb{R}, \geqslant)$, $(\mathcal{P}(A), \supseteq)$ etc.

Finite posets can be represented by Hasse **diagrams**. Elements of the underlying set are represented by points in a plain and $x\rho y$ is denoted by the edge from x to y, with x being lower than y. There is no edge from x to x, neither there is an edge connecting x and z, if there are edges for $x\rho y$ and $y\rho z$.

Example 9 In Figure 4 some posets are represented by diagrams. The one in $a)$ is the poset $(\{1, 2, 3, 4\}, \leqslant)$ which is linearly ordered. $b)$ represents some subsets of the set $\{a, b, c, d\}$ ordered by inclusion. Diagram $c)$ is the set $\{1, 2, 3, 4, 5, 6\}$ ordered by $\ |\ $ (divisibility), and $d)$ is the power set of a two-element set under inclusion.

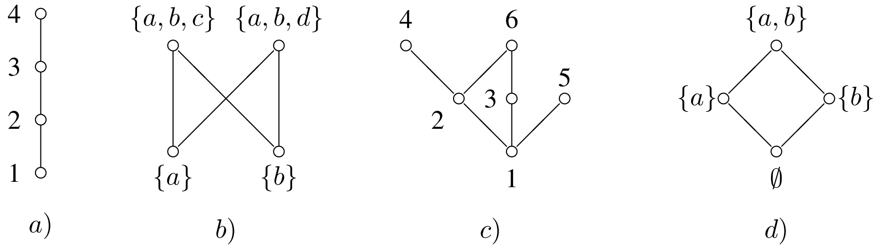


Figure 4

Linearly ordered set is also called a **chain**.

If (A, ρ) is a poset and $B \subseteq A$, then also B is ordered by the relation $\ \rho\ $ inherited from A. If in such a case B is linearly ordered, it is a chain in A.

An element $a \in A$ is **minimal** if there is no $x \in A$ so that $x \neq a$ and $x\rho a$.

An element $a \in A$ is **maximal** if there is no $x \in A$ so that $x \neq a$ and $a\rho x$.

An element a is the **smallest**, **least** in A if for all $x \in A$, $a\rho x$.

An element a is the **greatest** in A if for all $x \in A$, $x\rho a$.

Example 10 In the poset $(\mathbb{N}, |)$ a chain is e.g., $\{1, 2, 2^2, 2^3, \dots\}$.

In $(\mathbb{N}, \leqslant)$ number 1 is the smallest and minimal, the same holds in $(\mathbb{N}, |)$. In $(\mathbb{Z}, \leqslant)$ there is no elements from the above list.

U $(\mathcal{P}(A), \subseteq)$ the empty set is minimal and the smallest, the set A is maximal and the greatest.

The poset in Figure 4 b) has two minimal and to maximal elements, the smallest and the greatest do not exist.

The poset in Figure 4 c) possesses three maximal elements ($4, 5$ and 6) and one minimal (1) which is the smallest as well.

If it exists in a poset, *the smallest (greatest) element is unique.* Indeed, if m_1 and m_2 are two smallest elements in (A, ρ), then $m_1 \rho m_2$, since m_1 is the smallest, and analogously $m_2 \rho m_1$, because m_2 is the smallest. Due to antisymmetry of ρ we get $m_1 = m_2$.

Theorem 11 *In a finite poset (A, ρ) there is at least one minimal (maximal) element.*

Proof. Indeed, if an element a is minimal in (A, ρ), then we are done. Otherwise there is an element smaller than a. Repeating the above procedure we get an ascending chain which, in a finite poset should end, obviously by a minimal element. Analogously we get maximal elements. ■

If B is a nonempty subset of a poset (A, ρ), then a **lower bound** of B is an element a in A satisfying: $a \rho x$, for all $x \in B$.

An **upper bound** of a subset B in (A, ρ) is an element $b \in A$ such that: $x \rho b$, for all $x \in B$.

Let (A, ρ) be a poset and$B$ its nonempty subset. Denote by B^ℓ the set of all lower bounds, and by B^u the set of all upper bounds of B:

$B^\ell := \{x \in A \mid x \rho b, \text{ for all } b \in B\}$;

$B^u := \{x \in A \mid b \rho x, \text{ for all } b \in B\}$.

If B^ℓ is not empty and contains the greatest element m, then m is **infimum**, the **greatest lower bound** of B in (A, ρ): $m = \inf B$

Analogously, if B^u is not empty and contains the smallest element n, then n is **supremum**, the **least upper bound** of B in (A, ρ): $n = \sup B$

Being the greatest and the smallest elements of the corresponding sets, infimum and supremum are unique, if they exist.

Example 12 a) In the poset $(\mathbb{N}, \leqslant)$ for each finite subset there is supremum, which is the greatest element of this subset. Again in $(\mathbb{N}, \leqslant)$, infimum of any subset is its smallest element.

b) In the poset $(\mathbb{N}, |)$ infimum of the finite subset is the *greatest common divisor* (gcd), and supremum is the *least common multiple* (lcm).

c) In the poset represented by diagram in Figure 4 b), there is no infimum for the set $\{\{a\}, \{b\}\}$ nema infimum, since there are no lower bounds; neither there is supremum, since the set of upper bounds $\{\{a, b, c\}, \{a, b, d\}\}$ does not have the smallest element.

d) In any power set ordered by inclusion, infimum of a collection of subsets is their set intersection, and supremum is union.

2.3. Lattice

A poset in which infimum and supremum exist for every two-element subset is called a **lattice**. A lattice is usually denoted by $(L, \leqslant)$.

Example 13 All numbers, from naturals to reals are lattices under the corresponding order $\leqslant$. Indeed, this order is linear, hence infimum of a two-element set is greater, and supremum smaller of these elements:

$\inf\{a, b\} = \min\{a, b\}; \quad \sup\{a, b\} = \max\{a, b\}.$

More general, every linearly ordered set is a lattice.

b) The poset $(\mathbb{N}, |)$ is a lattice, since for any two naturals m, n,

$\inf\{m, n\} = \text{gcd}(m, n); \quad \sup\{m, n\} = \text{lcm}(m, n).$

c) A power set under inclusion is a lattice in which infimum and supremum are set intersection and union, respectively.

d) The poset in Figure 2 (an example of a *tree*) is not a lattice: infima are missing. In Figure 4, lattices are posets in a) and d), the other two are not. In Figure 3, both posets are lattices.

Since infimum and supremum are unique if they exist, it is obvious that *in any lattice L it is possible to define two binary operations* denoted by $\wedge$ – **meet** and $\vee$ – **join**, as follows: for $x, y \in L$

$x \wedge y := \inf\{x, y\}; \quad x \vee y := \sup\{x, y\}.$

The following identities involving meet and join in a lattice are direct consequences of set-theoretic properties of infimum and supremum.

Theorem 14 *In any lattice L, the following identities are fulfilled.*

$$\begin{aligned} &x \wedge y = y \wedge x \\ &x \vee y = y \vee x \end{aligned} \qquad (\textit{commutativity})$$

$$\begin{aligned} &x \wedge (y \wedge z) = (x \wedge y) \wedge z \\ &x \vee (y \vee z) = (x \vee y) \vee z \end{aligned} \qquad (\textit{associativity})$$

$$\begin{aligned} &x \wedge (x \vee y) = x \\ &x \vee (x \wedge y) = x \end{aligned} \qquad (\textit{absorption})$$

$$\begin{aligned} &x \wedge x = x \\ &x \vee x = x \end{aligned} \qquad (\textit{idempotency}).$$

Operations meet and join and the order in a lattice are connected in the following obvious way:

$x \leqslant y$ *if and only if* $x \wedge y = x$ *if and only if* $x \vee y = y$.

Observe that due to associativity of both operations, *infimum and supremum exist for every finite subset of a lattice.* A consequence is that *every finite lattice possesses the smallest and the greatest element.* These are usually denoted by 0 – the smallest element, the **bottom**, and by 1 – the greatest element, the **top** of the lattice.

Some additional properties, fulfilled by particular lattices are as follows.

A lattice $(L, \leqslant)$ is said to be **distributive** if it satisfies the following two identities

$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$

Example 15 All posets which are lattices in Figures 1 – 4 are distributive. Two nondistributive lattices are presented in Figure 5.

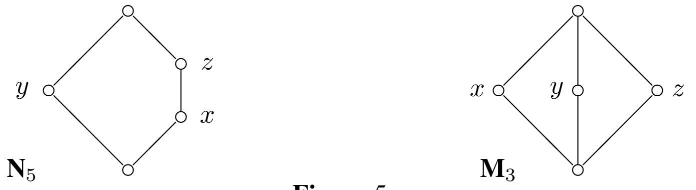


Figure 5

If a lattice L has the bottom (0) and the top (1), then we say that it is **bounded** and we can talk about complements of elements in L: an element x has a **complement** x' if

$x \wedge x' = 0 \qquad \text{and} \qquad x \vee x' = 1.$

An element in a bounded lattice can have no complements, it can possess exactly one complement, but also more of them. Elements 0 and 1 are complements each to other.

Example 16 In the lattice $\mathbf{N}_5$ (Figure 5), y has two complements, both x and z precisely one. In the lattice $\mathbf{M}_3$, every denoted element has two complements.

The lattice of divisors of 12 (Figure 6) under divisibility is distributive, and apart of the bottom and the top, complements each to other are only 3 and 4.

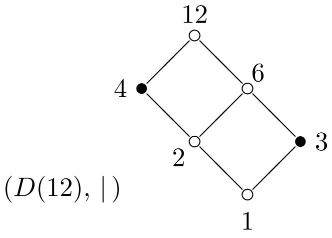


Figure 6

Theorem 17 *In a bounded distributive lattice an elements can have at most one complement.*

Proof. If x' and x'' are complements in a distributive lattice, then

$x \wedge x' = 0$ and $x \vee x' = 1$, and also $x \wedge x'' = 0$ and $x \vee x'' = 1$.

Now, by the property of the top and by distributive equalities

$x' = x' \wedge 1 = x' \wedge (x \vee x'') = (x' \wedge x) \vee (x' \wedge x'') = (x'' \wedge x) \vee (x' \wedge x'') = x'' \wedge (x \vee x') = x'' \wedge 1 = x''.$ ■

A lattice L is **complemented** if each element in L has a complement. L is **uniquely complemented** if each element has precisely one complement. By Theorem 17, *distributive complemented lattice is uniquely complemented.*

A distributive complemented lattice is called a **Boolean lattice**.

Example 18 Every power set is a Boolean lattice under inclusion. Complements coincide with set-complements.

All divisors of a square-free natural number n (the one which is a product of distinct primes) is a Boolean lattice under divisibility. The complement of a divisor x is n/x.

Lattices in Figure 3 and the one in Figure 4 d) are Boolean.

Boolean lattices have many important applications in mathematics and informatics.

3. Operational structures

Dealing with numbers is usually connected with some usage of main operations on them: addition and multiplication. Therefore we talk about structures like $(\mathbb{N}, +, \cdot\,)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, +, \cdot\,)$, $(\mathbb{R}, +)$, $(\mathbb{R}, +, \cdot\,)$ and others.

In a general settings, a nonempty set equipped with a collection of operations is an **operational structure**. Here we describe the most important abstractly defined structures, motivated by numbers and operations on them. After deriving basic properties of particular algebraic structures with one and two binary operations, we apply them back to structures of numbers. General notions become concrete objects, and properties of abstract operations obtain meanings related to addition and multiplication.

We also describe some relations on these structures, introducing the notion of a congruence relation and further a linear order compatible with the operations. In this framework we describe integers with respect to division. Concerning order, we get ordered integral domains and finally a complete ordered field representing real numbers.

3.1. Groupoids

An ordered pair $(G, *)$, where G is a nonempty set and $*$ is a binary operation on G is a **groupoid**. Hence, a groupoid is an operational structure with one binary operation and is sometimes denoted by the underlying set G.

Example 19 Groupoid on sets of numbers are e.g., $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{R}^+, \cdot)$ etc.

Each table of a binary operation in propositional logic, given in the sequel, determines a groupoid on the set $\{\top, \bot\}$ of truth values.

$\wedge$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

$\vee$	$\top$	$\bot$
$\top$	$\top$	$\top$
$\bot$	$\top$	$\bot$

$\Rightarrow$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\top$	$\top$

$\Leftrightarrow$	$\top$	$\bot$
$\top$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

A groupoid G is **commutative** if for all $x, y \in G$

$x * y = y * x.$

A groupoid G is **associative** if for all $x, y, z \in G$

$x * (y * z) = (x * y) * z.$

An associative groupoid is called a **semigroup**.

An element e of a groupoid G is said to be a **neutral element** of G, if for all $x \in G$

$e * x = x \quad \text{and} \quad x * e = x.$

A neutral element of a groupoid is also called a **unit**.

A semigroup with a unit is said to be a **monoid**.

Example 20 a) Above mentioned groupoids on sets of numbers are commutative: $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$ etc. The following ones are not commutative: $(\mathbb{Z}, -)$ and $(\mathbb{R} \setminus \{0\}, :)$, and the implication table on $\{\top, \bot\}$ in Example 19.

b) The table of a finite commutative groupoid is symmetric with respect to the main diagonal. The first of the following two groupoids is commutative, and the second is not.

$*$	a	b	c
a	a	b	b
b	b	c	a
c	b	a	a

$\cdot$	x	y	z
x	y	x	x
y	x	y	y
z	z	z	z

c) Examples of associative groupoids, semigroups, are e.g., $(\mathbb{N}, +)$ and $(\mathcal{P}(A), \cap)$, while the groupoid $(\mathbb{Z}, -)$ is not associative.

d) A groupoid with a unit is e.g., $(\mathbb{R}^+, \cdot)$ (positive reals under multiplication); the unit is number 1. $(\mathbb{Z}, +)$ is also a groupoid with a unit, neutral element, which is in this case number 0. Both are monoids.

e) In the groupoid $(\{p, n\}, \oplus)$, defined by the table below, the neutral element is p.

$\oplus$	p	n
p	p	n ,
n	n	p

Theorem 21 *If there is a neutral element in a groupoid, then this element is unique.*

Proof. If e_1 and e_2 are both neutral elements in a groupoid $(G, *)$, then $e_1 = e_1 * e_2$, since e_2 is a neutral element; $e_2 = e_1 * e_2$, since e_1 is a neutral element. Hence $e_1 = e_2$. ■

In a monoid $(G,*)$ i.e., in a semigrup with the unit e, an element $b \in G$ is an **inverse** of $a \in G$, if $a*b = b*a = e$.

Theorem 22 *An element of a monoid can have at most one inverse.*

Proof. Let e be the unit in a monoid $(G,*)$ and let $a \in G$. If b and c are inverses of a, then: $a * b = b * a = e$ and $a * c = c * a = e$.

Now we have $b = b * e = b * (a * c) = (b * a) * c = e * c = c$. ■

Let $(G,*)$ be a groupoid and G_1 a nonempty subset of G. Then the structure $(G_1, *_1)$ is a **subgroupoid** of $(G,*)$ if $(G_1, *_1)$ itself is a groupoid and $*_1$ is the restriction of $*$ to $G_1 \times G_1$. In other words, a nonempty subset of a groupoid which is closed under the groupoid operation is its subgroupoid.

Usually, the operations in both,a groupoid and in its subgroupoid are denoted in the same way: $(G,*)$ and $(G_1,*)$.

Example 23 a) $(\mathbb{N},+)$ is a subgroupoid of $(\mathbb{Z},+)$.

$*$	a	b	c	d
a	a	b	b	b
b	b	c	a	d
c	b	a	a	d
d	d	a	a	c

b) Subgroupoids of the groupoid given by the above table are $\{a\}$ and $\{a,b,c\}$. The latter is denoted in the table.

Theorem 24 *Let $(G_1,*)$ be a subgroupoid of a groupoid $(G,*)$.*

(a) *If G commutative, then also G_1 is commutative.*

(b) *If G is associative, then also G_1 is associative.*

Proof. (a) Values of $x * y$ and $y * x$ for a valuation from G_1 are also values for these terms in G. Since G is commutative, these values are equal, hence also, G_1 is commutative.

(b) Analogously as in (a). ■

Obviously, the analogue theorem is valid for any identity in the language of groupoids.

3.2. Groups

A grupoid $(G,\cdot)$ is a **group**, if there is an element $e \in G$ so that the following hold:

(1) For all $x, y, z \in G$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

(2) For every $x \in G$

$$x \cdot e = e \cdot x = x.$$

(3) For every $x \in G$ there is $y \in G$, such that

$$x \cdot y = y \cdot x = e.$$

In (3), y denote the **inverse element** for $x \in G$. Hence, a group is a *monoid in which for every element there is an inverse.*

Example 25 a) Among semigroups of numbers, groups are $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{Q}^+,\cdot)$, $(\mathbb{R}^+,\cdot)$. Where the operation is addition, the neutral element is number 0, and the inverse for a number a is $-a$: in groups under multiplication, the neutral element is number 1, and the inverse for a is $\frac{1}{a}$. Number 0 is removed in $(\mathbb{Q}\setminus\{0\},\cdot)$ and $(\mathbb{R}\setminus\{0\},\cdot)$, since it does not possesses an inverse under multiplication.

The semigroups $(\mathbb{N},+)$, $(\mathbb{N}_0,+)$, $(\mathbb{N},\cdot)$, $(\mathbb{Z}\setminus\{0\},\cdot)$ are not groups, due to the lack of inverses, while $(\mathbb{N},+)$ does not have the neutral element.

b) One-element, **trivial** group $(\{a\},*)$ has the obvious operation: $a\cdot a=a$, and a two-element group is e.g., the set $\{-1,1\}$ under arbitrary multiplication.

c) All bijections (permutations) $A\longrightarrow A$, where A is e.g., a three-element set $\{a,b,c\}$, form a group under the composition of functions:

$$e=\begin{pmatrix} a & b & c\\ a & b & c\end{pmatrix},\quad f=\begin{pmatrix} a & b & c\\ a & c & b\end{pmatrix},\quad g=\begin{pmatrix} a & b & c\\ b & a & c\end{pmatrix},$$
$$h=\begin{pmatrix} a & b & c\\ b & c & a\end{pmatrix},\quad j=\begin{pmatrix} a & b & c\\ c & a & b\end{pmatrix},\quad k=\begin{pmatrix} a & b & c\\ c & b & a\end{pmatrix}.$$

The operation (composition) $\circ$ on $\{e,f,g,h,j,k\}$ is given by the table:

$\circ$	e	f	g	h	j	k
e	e	f	g	h	j	k
f	f	e	h	g	k	j
g	g	j	e	k	f	h
h	h	k	f	j	e	g
j	j	g	k	e	h	f
k	k	h	j	f	g	e .

This permutation group on a three-element set is usually denoted by S_3 and it is called the **symmetric group** S_3.

The **order** of a finite group is the number of its elements. The group which is not finite is said to be **of infinite order**.

If the operation in a group is commutative, then also the group is said to be **commutative**, or **Abelian**.

In Example 25, all groups are Abelian, except S_3.

By Theorem 21, a neutral element in a group is unique, and by Theorem 22, each element in a group has the unique inverse. Usually, the inverse element of $a\in G$ is denoted by a^{-1}. In additive notation (the operation in a group is $+$), the neutral element is denoted by 0, and inverse of a by $-a$.

Theorem 26 *If $(G,\cdot)$ is a group and $a,b\in G$, then equations*

$a\cdot x=b$ *and* $y\cdot a=b$

have unique solutions over x and y.

Proof. One solution c of the equation $a\cdot x=b$ is $c=a^{-1}\cdot b$. Suppose that also $d\in G$ is a solution, i.e., that $a\cdot d=b$. Then $d=e\cdot d=(a^{-1}\cdot a)\cdot d=a^{-1}\cdot(a\cdot d)=a^{-1}\cdot b=c$.

Analogously we prove the second part. ■

For a finite group this uniqueness of equational solutions has an impact on the operation table: *in every row and column, each element appears exactly ones.*

Other straightforward consequences of Theorem 26 are the following **cancelation properties**.

Theorem 27 *If a, b and c are arbitrary elements of a group $(G, \cdot)$, then:*

$a \cdot c = b \cdot c$ *implies* $a = b$; $c \cdot a = c \cdot b$ *implies* $a = b$.

The neutral element of a groupoid is *idempotent*: $e \cdot e = e$. In a group also the converse holds.

Theorem 28 *In any group $(G, \cdot)$, $x \cdot x = x$, implies $x = e$.*

Proof. Let $x \in G$ and $x \cdot x = x$. Then $x = x \cdot e = x \cdot (x \cdot x^{-1}) = (x \cdot x) \cdot x^{-1} = x \cdot x^{-1} = e$. ■

A subgroupoid $(H, \cdot)$ of a group $(G, \cdot)$ is its **subgroup** if it is a group itself.

It is easy to prove that *the unit of a subgroup coincides with the unit of a group, and that also the inverse of an element in a subgroup is the same as the inverse of this element in the whole group.*

Theorem 29 *A nonempty subset H of a group $(G, \cdot)$ is its subgroup if and only if the following two conditions hold:*

(1) *If $a, b \in H$, then $a \cdot b \in H$.*

(2) *If $a \in H$, then $a^{-1} \in H$.*

Proof. If H is a subgroup of G, then (1) holds since the operation in a subgroup is the restriction of the group operation; (2) follows by the above comment about inverses in a subgroup.

Conversely, suppose (1) and (2) hold. Then by (1) the operation in H is a restriction of the operation in G to H. Next, there is an $a \in H$, since $H \neq \emptyset$, hence by (2), $a^{-1} \in H$, and by (1), $a \cdot a^{-1} = e \in H$. Associativity holds, thus $(H, \cdot)$ is a group. ■

The following can be proved similarly.

Theorem 30 *A nonempty subset H of a group $(G, \cdot)$ is its subgroup if and only if* $a, b \in H$ *implies* $a \cdot b^{-1} \in H$.

In each group $(G, \cdot)$, $\{e\}$ and G are **trivial** subgroups. Other subgroups are **proper** or nontrivial.

Example 31 a) In the group $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$ is a proper subgroup.

In the group $(\mathbb{R} \setminus \{0\}, \cdot)$ a proper subgroup is $(\mathbb{R}^+, \cdot)$.

b) The group $(\{a, b, c\}, *)$, given by the table below, has no proper subgroups.

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

c) In the symmetric group S_3 (Example 25 c)), permutations e, h, j form a subgroup. There are also three two-element subgroups: $\{e, f\}$, $\{e, g\}$ and $\{e, k\}$.

d) Nontrivial subgroups of the group $(\mathbb{Z}, +)$ are sets of numbers all divisible by a fixed $n \in \mathbb{N}$, $n \geqslant 2$.

Theorem 32 *If H and K are subgroups of group G, then also $H \cap K$ is a subgroup of G.*

Proof. Straightforward, since the set intersection of two groups contains e (hence it is nonempty) and is closed under the group operation as well as under taking inverses. ■

Analogously one can show that *the set intersection of an arbitrary family of subgroups of a group is its subgroup.*

For $n \in \mathbb{N}$, let $a^n = a \cdot \ldots \cdot a$, where a appears n times. Next,

$$a^0 := e; \quad \text{and} \quad a^{-n} := (a^{-1})^n, \quad n \in \mathbb{N}.$$

In additive notation $na := a + a + \cdots + a$, $0a := O$ and $-na := n(-a)$, $n \in \mathbb{N}$.

By obvious properties of the above exponentiation, we have the following.

Theorem 33 *If G is a group and $a \in G$, then the set $\langle a \rangle$, defined by $\langle a \rangle := \{a^p \mid p \in \mathbb{Z}\}$ is a subgroup of G.*

For $a \in G$, $\langle a \rangle$ is a **cyclic subgroup** of G, **generated** by a.

If $G = \langle a \rangle$ for some a, a group G is said to be **cyclic**.

Example 34 a) In the group $(\mathbb{R} \setminus \{0\}, \cdot)$, number 2 generates the cyclic subgroup $\langle 2 \rangle = \{2^p \mid p \in \mathbb{Z}\}$.

b) The group $(\mathbb{Z}, +)$ is cyclic, generated by number 1.

Each subgroup of $(\mathbb{Z}, +)$ (Example 31) is cyclic, generated by the number whose multiples are its elements.

c) The group $(\{a, b, c\}, *)$ from Example 31 b) is cyclic. It is generated by b, but also by c.

Next we show that any subgroup is a class of the particular partition of the group. Moreover, in a finite case all classes of this partition have equal number of elements.

If H is a subgroup of a group G and $a \in G$, then the set

$$H \cdot a := \{h \cdot a \mid h \in H\}$$

is called the **right coset** of G over H, or $a \in G$; it is also denoted by $Ha = \{ha \mid h \in H\}$.

The following connects subgroups and particular relations on a group. The proof is straightforward.

Theorem 35 *If H is a subgroup of a group G, then the relation δ_H on G, defined by*

$$a \delta_H b \ \text{ if and only if } \ ab^{-1} \in H$$

is an equivalence relation.

Theorem 36 *If H is a subgroup of a group G and $a \in G$, then for every $x \in G$*

$$x \in Ha \ \text{ if and only if } \ x \delta_H a.$$

Proof. If $x \in Ha$, then $x = ha$ for some $h \in H$, hence $xa^{-1} = (ha)a^{-1} = h(aa^{-1}) = he = h$, i.e., $xa^{-1} = h \in H$, and thus $x\delta_H a$. Conversely, if $x\delta_H a$, then $xa^{-1} \in H$, and $xa^{-1} = h$ for some $h \in H$,i.e., $xa^{-1}a = ha$ or $x = ha$, which finally gives $x \in Ha$. ■

Example 37 Consider the subgroup $H = \{e, f\}$ of S_3 (Example 25 c)). We have:

$H \circ e = \{e \circ e, f \circ e\} = \{e, f\} = H$ and similarly $H \circ f = \{e \circ f, f \circ f\} = \{f, e\} = H$;

$H \circ g = \{e \circ g, f \circ g\} = \{g, h\}$; $H \circ h = \{e \circ h, f \circ h\} = \{h, g\}$;

$H \circ j = \{e \circ j, f \circ j\} = \{j, k\}$; $H \circ k = \{e \circ k, f \circ k\} = \{k, j\}$.

Hence, right cosets of S_3 over $H = \{e, f\}$ are $\{e, f\}$, $\{g, h\}$ and $\{k, j\}$.

By Theorem 36, Ha is the equivalence class of $a \in G$ under δ_H, hence *right cosets over H form a partition $\{Ha \mid a \in G\}$ of G.*

Theorem 38 *If H is a subgroup of G and $a \in G$, then the mapping $\sigma_a : h \mapsto ha$ is a bijection of H onto Ha.*

Proof. If $h_1, h_2 \in H$ and $a \in G$, then $h_1 a = h_2 a$ implies $h_1 = h_2$, by cancelation law. Hence σ_a is an injection. For $ha \in Ha$ it is clear that $\sigma_a(h) = ha$, i.e., σ_a is also a surjection. ■

As an obvious consequence of Theorem 38, we get the following so called **Lagrange theorem** for finite groups.

Theorem 39 *The order of a finite group is divisible by the order of its subgroup.*

Analogously to a right coset of a group G with respect to its subgroup H, we have a **left coset** aH for $a \in G$:

$$aH := \{ah \mid h \in H\},$$

and the corresponding equivalence relation λ_H on G:

$$a\lambda_H b \text{ if and only if } a^{-1}b \in H.$$

Here analogously, we have that aH is the equivalence class of $a \in G$ under λ_H.

In additive notation right and left cosets are denoted by $H + a$ and $a + H$, respectively.

Example 40 In S_3 (Example 37), left cosets under $H = \{e, f\}$ are $\{e, f\}$, $\{g, j\}$ and $\{h, k\}$ and they do not coincide with the right ones with respect to the same subgroup.

So, in general $Ha \neq aH$.

A subgroup H of a group G is **normal**, if for every $a \in G$, $Ha = aH$.

The fact that H is a normal subgroup of a group G is denoted by $H \lhd G$.

Obviously, if $H \lhd G$, then $\delta_H = \lambda_H$.

Example 41 a) In every group G, trivial subgroups $\{e\}$ and G are normal.

b) If a group is Abelian, then every subgroup is normal.

c) In S_3 (Example 25 c)) the subgroup $\{e, h, j\}$ is normal.

An equivalence relation ρ on a group $(G, \cdot)$ is a **congruence relation** on this group if it is compatible with the operation $\cdot$, i.e., if

$x\rho y$ and $u\rho v$ imply $(x \cdot u)\rho(y \cdot v)$.

If ρ is a congruence on G, then it is straightforward that also $x\rho y$ implies $x^{-1}\rho y^{-1}$

Theorem 42 *If $H \lhd G$, then the relation δ_H is a congruence relation on G.*

Proof. Let $x\,\delta_H y$ and $u\,\delta_H v$. Then $xy^{-1} = h_1 \in H$ and $uv^{-1} = h_2 \in H$. Hence $x = h_1 y$ and $u = h_2 v$, therefore $xu = h_1 y h_2 v$. Since $H \lhd G$, we have $yH = Hy$. Since $yh_2 \in yH$, it follows $yh_2 \in Hy$, i.e., there is $h_3 \in H$, such that $yh_2 = h_3 y$. It follows that $xu = h_1 h_3 yv = hyv$, where $h = h_1 h_3 \in H$. Thus, $xu \in Hyv$, and this holds if and only if $xu\,\delta_H yv$. ■

The converse also holds, i.e., *for any congruence on a group G, its class containing the neutral element is a normal subgroup of G.*

If $H \lhd G$ and $G/H = \{aH \mid a \in G\}$, then we define a binary operation $*$ on G/H: $aH * bH := abH$.

This operation is well defined: if $a_1 \in aH, b_1 \in bH$, then $a_1 = ah_1, b_1 = bh_2$, for some $h_1, h_2 \in H$. Hence, since $H \lhd G$, $a_1 b_1 = ah_1 bh_2 = abh_3 h_2 = abh$, for some $h_3 \in H$ and $h = h_3 h_2$. Therefore, $a_1 b_1 \in abH$.

If $(G_1, \cdot\,)$ and $(G_2, \circ\,)$ are groups, then the mapping $f : G_1 \to G_2$ is a **homomorphism** if for all $x, y \in G_1$,

$f(x \cdot y) = f(x) \circ f(y)$.

Theorem 43 *If G is a group and H its normal subgroup, then the structure $(G/H, *)$ is group, the* ***quotient group*** *of G over H, and the mapping $h : x \mapsto xH$ is a homomorphism from G onto G/H.*

Proof. The fact that $(G/H, *)$ follows directly by the definition of the operation $*$. Further, for $x, y \in G$, $h(x \cdot y) = xyH = xHyH = h(x) * h(y)$. ■

The operation in the quotient group G/H is usually denoted by the same symbol as the operations in G and H.

Example 44 Consider the group $(\mathbb{Z}, +)$, and its subgroup $(\mathbb{Z}_3, +)$ of all numbers divisible by 3. This subgroup is normal (all subgroups are normal, since $(\mathbb{Z}, +)$ is Abelian) and thus we can construct the quotient group $(\mathbb{Z}/\mathbb{Z}_3, +)$, which consists of three **residue classes**: $\mathbb{Z}_3 = \{0, -3, 3, -6, 6, \ldots\}$, $1 + \mathbb{Z}_3 = \{1, -2, 4, -5, 7, \ldots\}$ and $2 + \mathbb{Z}_3 = \{2, -1, 5, -4, 8, \ldots\}$. If we denote these classes respectively by $\overline{0}, \overline{1}$ and $\overline{2}$, then we get the following table of the corresponding group operation:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

3.3. Rings

Numbers are equipped with two basic binary operations, and we usually represent them as the corresponding operational structures: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and so on. These are our main examples for the following general definition.

A **ring** is an operational structure $(R, +, \cdot)$ with two binary operations, fulfilling:

(i) $(R, +)$ is an Abelian group;

(ii) $(R, \cdot)$ is asemigroup;

(iii) the following distributive laws are fulfilled: for all $x, y, z \in R$

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad \text{and} \quad (x + y) \cdot z = (x \cdot z) + (y \cdot z).$$

According to this notation, $(R, +)$ is the *additive group* of a ring, hence its neutral element is denoted by 0, and the inverse of x by $-x$. $(R, \cdot)$ is the *multiplicative semigroup* of a ring. In addition, $+$ is said to be the *first*, and $\cdot$ the *second* operation. It is usual to omit brackets for products, as for numbers; the order of applying operations is hence $(\cdot)$ before $(+)$.

Example 45 a) The main example of a ring is the structure $(\mathbb{Z}, +, \cdot\,)$ of integers with respect to addition and multiplication.

Also rational numbers, then reals and complex numbers, all these form rings under addition and multiplication.

In particular, one element ring contains only the element 0; the structure $(\{0\}, +, \cdot)$ is a **zero ring**, where $0 + 0 = 0 \cdot 0 = 0$.

b) If $(G, +)$ is an arbitrary Abelian group and the operation "$\cdot$" is defined so that for all x, y, $x \cdot y = 0$, then the structure $(G, +, \cdot)$ is a ring.

c) The set $\{f \mid f : \mathbb{R} \to \mathbb{R}\}$ of all functions with one variable on the set of real numbers is a ring with respect to the operations $+$ and $\cdot$ defined by:

$(f + g)(x) := f(x) + g(x)$ and $(f \cdot g)(x) := f(x) \cdot g(x)$.

The zero element is the function $O(x) = 0$, for all x.

d) Even integers form a ring under addition and multiplication.

e) An example of a four-element ring is here given by its operations.

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

$\cdot$	0	a	b	c
0	0	0	0	0
a	0	a	0	a
b	0	b	0	b
c	0	c	0	c

A ring is said to be a **ring with a unit** if there is a neutral element, usually denoted by 1, with respect to the second operation.

A ring is **commutative** if the second operation, multiplication is commutative.

In the above example, all rings of numbers are commutative and have a unit element, as well as the ring of real functions, in which the unit is the constant function $e(x) = 1$. The ring of even integers is commutative, but without a unit, and the finite one (Example 45 e)) is not commutative neither with a unit.

The last ring has the following property. There are non-zero elements (a and b) whose product is zero.

In general, an element $a \neq 0$ of a ring R is a **zero divisor** if there is $b \neq 0$, so that $a \cdot b = 0$ or $b \cdot a = 0$.

Accordingly, a ring is said to be a ring **without zero divisors** if for all $x, y \in R$

$x \cdot y = 0$ implies $x = 0$ or $y = 0$.

Example 46 In the ring of real functions (Example 45 c)) let

$$f(x) = \begin{cases} x & \text{if } x \leqslant 0 \\ 0 & \text{if } x > 0 \end{cases} \quad \text{and} \quad g(x) = \begin{cases} 0 & \text{if } x \leqslant 0 \\ x & \text{if } x > 0 \end{cases} .$$

Functions f and g are zero divisors, since $f \neq O$, $g \neq O$, while $f \cdot g(x) = O(x) = 0$, for every x, i.e., $f \cdot g = O$.

Next we present some properties of rings.

Theorem 47 *In a ring R the following hold for any x, y:*

(a) $x \cdot 0 = 0 \cdot x = 0$;

(b) $(-x)\cdot y = x\cdot(-y) = -(x\cdot y)$;

(c) $(-x)\cdot(-y) = x\cdot y$.

Proof. (a) $x\cdot 0 = x\cdot(0+0) = x\cdot 0 + x\cdot 0$. Since 0 is the only idempotent element in the group $(R,+)$ (Theorem 28), we have $x\cdot 0 = 0$. The rest can be proved analogously. ■

Theorem 48 *Let R be a ring with a unit 1. Then:*

(a) *A unit in a ring is unique;*

(b) *if R has at least two element, then $1 \neq 0$.*

Proof. (a) follows by the uniqueness of a neutral element in a groupoid (Theorem 21).

(b) $1 = 0$ implies $x = x\cdot 1 = x\cdot 0 = 0$, for every x in R, hence a ring has one element only. ■

A subset P of a ring $(R,+,\cdot)$ is its **subring**, if P is itself a ring with respect to the restrictions of ring operations.

Example 49 a) $\{0\}$ and R are **trivial** subrings of any ring R.

b) Even numbers form a subring of the ring of integers.

c) Integers form a subring of the ring of rational numbers, and both are subrings of the ring of reals.

Due to Theorem 30 in additive notation, and by the fact that closedness under operations preserves identities, we have the following criterium.

Theorem 50 *A nonempty subset P of a ring R is its subring if the following holds for all $x, y \in P$:*

1) $x + (-y) \in P$ *and* 2) $x\cdot y \in P$.

Motivated by the role of normal subgroups, we define special subrings.

A subring I of a ring R is an **ideal** if:

(a) for all $a \in I$ and $x \in R$, $ax \in I$ and $xa \in I$.

Equivalently (by Theorem 30), a nonempty subset I of a ring R is its ideal, if and only if (a) holds, and also

(b) for $x, y \in I$ $x - y \in I$.

By (b), $(I,+)$ is a subgroup of $(R,+)$, and due to (a), the restriction of $\cdot$ to I is an operation on I.

Example 51 a) In the ring $(\mathbb{Z},+,\cdot)$, for an arbitrary $a \in \mathbb{Z}$, the set $\{ax \mid x \in \mathbb{Z}\}$ is an ideal. E.g., if $a = 3$, then this ideal is the set $\{0,-3,3,-6,6,-9,9,\dots\}$.

b) $\{0\}$ is an ideal in any ring.

As for groups and other operational structures, an equivalence relation ρ on a ring $(R,+,\cdot)$ is a **congruence relation** on R if it is compatible with both operations, i.e., if

$x\rho y$ and $u\rho v$ imply $(x+u)\rho(y+v)$ and also $x\rho y$ and $u\rho v$ imply $(x\cdot u)\rho(y\cdot v)$.

Theorem 52 *If ρ congruence relation on a ring R, then the class $[0]_\rho$ in R/ρ is an ideal u R.*

Conversely, if I is an ideal in a ring R, then there is a congruence ρ on R, such that $I = [0]_\rho$.

Proof. If ρ is a congruence on a ring R and $a \in [0]_\rho, x \in R$, then $a\rho\, 0$, and since $x\rho x$ it follows that $ax\,\rho\, 0x$, i.e., $ax\,\rho\, 0$ and $ax \in [0]_\rho$. Similarly $xa \in [0]_\rho$, and (a) holds. (b) also holds, since $[0]_\rho$ is a subgroup in $(R, +)$.

Conversely, let I be an ideal in a ring R. Then I is a normal subgroup in $(R, +)$, hence there is a congruence ρ_I on $(R, +)$: $x\rho_I y$ if and only if $x + I = y + I$. ρ_I is also compatible with the second operation in R. Indeed, let $x\rho_I y$ and $u\rho_I v$, i.e., let $[x]_\rho = x + I = y + I = [y]_\rho$ and similarly, $u + I = v + I$. Then, $y \in x + I$ and $v \in u + I$. We prove that $yv \in xu + I$. Indeed, $y = x + i, v = u + j$, for some $i, j \in I$. Hence $yv = (x + i)(u + j) = xu + xj + iu + ij = xu + k$, where $k = xj + iu + ij \in I$, since I is an ideal. Therefore, $yv \in xu + I$, and $xu + I = yv + I$.

Finally, $[0]_{\rho_I} = I$. Since $[0]_{\rho_I} = \{x \in R \mid 0\rho_I x\}$, we have $x \in [0]_{\rho_I}$ if and only if $0\rho_I x$, which is equivalent with $0 + I = x + I$, i.e., with $I = x + I$. The latter holds if and only if $x \in I$. ■

As in the case of groups, starting with an ideal I or the corresponding congruence ρ on a ring $(R, +, \cdot)$, we can construct the quotient ring $(R/I, +, \cdot)$, where the operations are:

$(a + I){+}(b + I) = (a + b) + I, \quad$ and $\quad (a + I){\cdot}(b + I) = ab + I.$

The proof that these operations are well defined is similar to the one for groups.

Again similarly as in the group case, if I is an ideal on a ring R, then the mapping $h : R \to R/I$, given by $h(x) = x + I$, is a **homomorphism**, i.e., it is compatible with the operations: for any $x, y \in R$

$h(x + y) = h(x) + h(y)$ and $h(x \cdot y) = h(x) \cdot h(y)$.

Example 53 The ideal $I = \{0, -3, 3, -6, 6, -9, 9, \dots\}$ of the ring $\mathbb{Z}$ (Example 44) corresponds to the congruence relation ρ_I:

$$x\rho_I y \text{ if and only if } 3 \mid (x - y).$$

$\mathbb{Z}/I$ consists of three residue classes:

$I,\ 1 + I = \{1, -2, 4, -5, 7, -8, 10, \dots\},\ 2 + I = \{2, -1, 5, -4, 8, -7, \dots\}$. The operation tables are

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

.

Commutative ring with a unit without zero divisors is an **integral domain**.

Example 54 a) $(\mathbb{Z}, +, \cdot)$ is an integral domain, while e.g., the ring of even integers is not (it does not possesses a unit).

b) The set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain with respect to ordinary addition and multiplication.

A **field** is a commutative ring $(P, +, \cdot)$ with a unit, in which $(P \setminus \{0\}, \cdot)$ is a group.

Example 55 a) Real numbers form a field $(\mathbb{R}, +, \cdot)$, rational numbers $(\mathbb{Q}, +, \cdot)$ also. The ring $(\mathbb{Z}, +, \cdot)$ of integers is not a field.

b) A ring given by the tables below is, up to the isomorphism, a unique two-element field.

$+$	0	1
0	0	1
1	1	0

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

The reason for removing zero with respect to the second operations is the following. For every x in a ring we have $0 \cdot x = 0$, and since in a ring with a unit $0 \neq 1$, 0 does not have an inverse under multiplication.

Theorem 56 *A field is an integral domain.*

Proof. If for $a, b \in P$, $ab = 0$ and $a \neq 0$, then $a^{-1}ab = a^{-1} \cdot 0 = 0$, i.e., $b = 0$ and similarly if $b \neq 0$. Therefore, there are no zero divisors in P, hence it is an integral domain. ■

The converse holds for finite integral domains.

Theorem 57 *A finite integral domain is a field.*

Proof. We have to show the existence of inverses for non-zero elements in a finite integral domain. If $a \neq 0$, then among a, a^2, $a^3, \dots, a^n, \dots$, there are equal elements, since the structure is finite. Let $a^p = a^q$, $p < q$. Then $a^p = a^p \cdot a^{q-p}$, where $q - p > 0$. Hence $a^p \cdot (e - a^{q-p}) = 0$. Now, $a \neq 0$ implies $a^p \neq 0$ (no zero divisors) .Further, $a^p \neq 0$ implies $e - a^{q-p} = 0$, i.e., $a^{q-p} = e$. Hence $a \cdot a^{q-p-1} = e$, where $q - p - 1 \geqslant 0$. Therefore, a^{q-p-1} is the inverse element for a. ■

3.4. Integers

Here we apply the above properties of rings to the structure $(\mathbb{Z}, +, \cdot\,)$ of integers, for which we already know that it is an integral domain.

In a commutative ring R with a unit, for $a \in R$, the set

$$\langle a \rangle := \{xa \in R \mid x \in R\}$$

is an ideal, which is straightforward to prove. It is called a **principal ideal** generated by a. This is the smallest ideal containing a.

In the ring of integers these ideals are sets containing all multiples of a fixed natural numbers:

$\{\dots, -4, -2, 0, 2, 4, 6, \dots\}$, $\{\dots, -6, -3, 0, 3, 6, 9, \dots\}$ and so on. We prove that these are the only ideals in this ring.

Theorem 58 *Every ideal in the ring $\mathbb{Z}$ is principal.*

Proof. Let I be an ideal in $\mathbb{Z}$. If it is $\{0\}$, then this ideal is principal. If there is a non-zero $x \in I$, then since $-x \in I$, there are positive integers in I and let a be the smallest one. For $x \in I$, there are $q, r \in \mathbb{Z}$, with $0 \leqslant r < a$, such that $x = aq + r$. Hence $r = x - aq$, and $x, aq \in I$ implies $r \in I$. Since a is the smallest positive number in I, it follows that $r = 0$. Thus $x = aq$, i.e., $x \in \langle a \rangle$. Because $\langle a \rangle$ is the smallest ideal containing a, it follows that $I = \langle a \rangle$. ■

Hence, every non-zero ideal in $\mathbb{Z}$ consists of all multiples of its smallest positive member n; this is the set

$\langle n \rangle = \{0, -n, n, -2n, 2n, -3n, 3n, \dots\}$.

Conversely, for every natural number n, the set $\langle n \rangle$ is an ideal u $\mathbb{Z}$.

Therefore, for each ideal $\langle n \rangle$ in $\mathbb{Z}$, the quotient ring $\mathbb{Z}/\langle n \rangle$ consists of *residue classes*, i.e., of the sets $\langle n \rangle$, $1 + \langle n \rangle$, $2 + \langle n \rangle$, $\dots$, $(n-1) + \langle n \rangle$.

The function $x \mapsto x + \langle n \rangle$ is a homomorphism from the ring $\mathbb{Z}$ onto $\mathbb{Z}/\langle n \rangle$.

Example 59 a) The ideal in $\mathbb{Z}$ generated by number 6 is

$\langle 6 \rangle = \{0, -6, 6, -12, 12, -18, 18, \dots\}$.

The other five residue classes are $1 + \langle 6\rangle, \ldots, 5 + \langle 6\rangle$. They are respectively denoted by $\overline{0}, \overline{1}, \ldots, \overline{5}$, and the operations in $\mathbb{Z}/\langle 6\rangle$ are given by the following tables.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

The ring $\mathbb{Z}/\langle 6\rangle$ is commutative, it has the unit element, but also it possesses the zero divisors: e.g., $\overline{2} \cdot \overline{3} = \overline{0}$.

b) For the ideal $\langle 3\rangle = \{0, -3, 3, -6, 6, \ldots\} = \overline{0}$, we get the ring from Example 53. This one is an integral domain, and being finite, it is a field.

It is obvious that for every natural number n, the ring $(\mathbb{Z}/\langle n\rangle, +, \cdot)$ is commutative and it has the unit element.

Theorem 60 *The ring $(\mathbb{Z}/\langle n\rangle, +, \cdot)$ is an integral domain if and only if n is a prime number.*

Proof. Let n be a prime number. Suppose that for two non-zero classes $\overline{p}$ and $\overline{q}$ we have $\overline{p}\overline{q} = \overline{0}$. Then, since $\overline{p}\overline{q} = \overline{pq}$, it follows $pq \in \langle n\rangle$, and $n \mid pq$. The number n is prime, hence either $n \mid p$ or $n \mid q$, whence $p \in \langle n\rangle$ or $q \in \langle n\rangle$, i.e., $\overline{p} = \overline{0}$ or $\overline{q} = \overline{0}$. $\mathbb{Z}/\langle n\rangle$ is thus an integral domain.

Conversely, let $\mathbb{Z}/\langle n\rangle$ be an integral domain . If $n = pq$, then $p \leqslant n$ and $q \leqslant n$. Further, $n = pq$ implies $\overline{0} = \langle n\rangle = \overline{pq} = \overline{p}\overline{q}$. Since there are no zero divisors, either $\overline{p} = \overline{0}$, or $\overline{q} = \overline{0}$. In the first case $p \in \langle n\rangle$, pa $n \mid p$, whence $n \leqslant p$, and since $p \leqslant n$, it follows that $n = p$. In the second case analogously we get $n = q$. Therefore, n is a prime number. ■

.

The following is an obvious consequence of the fact that a finite integral domain is a field.

Theorem 61 *The ring $(\mathbb{Z}/\langle n\rangle, +, \cdot)$ is a field if and only if n is a prime number.* ■

As we know, each ideal I in a ring R corresponds to a congruence ρ_I:

$x \,\rho_I\, y$ if and only if $x + I = y + I$ if and only if $x - y \in I$.

Conversely, if ρ is a congruence relation on a ring R, then the class $[0]_\rho$ is an ideal.

Every non-zero ideal in the ring $\mathbb{Z}$ is principal, of the form $\langle n\rangle$, and n is a divisor of every element in this ideal. The corresponding congruence is denoted by $\equiv$ (mod n), hence we have:

$x \equiv y(\text{mod } n)$ if and only if $n \mid (x - y)$.

If $a \equiv b(\text{mod } n)$, we say that *$a$ and b are congruent modulo n.*

4. Conclusion

Our aim with this text is to present a methodological approach to some basic mathematical topics (mostly numbers), investigating abstract relational and operational structures and their properties. It seems reasonable to start with well known notions and their properties, like concrete sets, relations and operations (natural numbers, integers, $\leq$, $\mid$, addition, multiplication,...) and list their properties. Then these can be abstractly investigated in the framework of posets, lattices, groups, rings and others. Coming back to numbers, we apply these properties and formulate them in the known language, so that they improve the readers understanding and knowledge of this basic mathematical notions.

References

[1] M. Božić i drugi, *Brojevi*, Školska knjiga, Zagreb, 1985.

[2] R.A. Dean, *Elements of abstract algebra*, John Wiley and Sons, Inc., 1966.

[3] V. Devidé, *Zadaci iz apstraktne algebre*, Naučna knjiga, Beograd, 1979.

[4] M.Z. Grulović, *Osnovi teorije grupa*, Univerzitet u Novom Sadu, 1997.

[5] S. Milić, *Elementi algebre*, Institut za matematiku, Novi Sad, 1984.

[6] Z. Stojaković, Dj. Paunić, *Zadaci iz algebre - grupe, prsteni polja*, Univerzitet u Novom Sadu, Novi Sad, 1998.

[7] B. Šešelja, A. Tepavčević, *Algebra 1*, Symbol, Novi Sad, 2010.

[8] B. Šešelja, A. Tepavčević, *Algebra 2*, Symbol, Novi Sad, 2011.

[9] A. Tepavčević, B. Šešelja, *Matematičke osnove informatike*, Stylos, Novi Sad, 1995.