# 2.A BINARY OPERATIONS ---
## Semigroups, Monoids and Groups

In algebra one mainly study sets with an "algebraic structure" i.e. sets in which one can "compute" with elements. The characteristic of such a "computation-operation" or "binary operation" is: for every pair of elements in the given set an another element of this set is assigned which in general depends on the order of the starting pair of elements. This is introduced in the following:

**2.A.1 Definition** Let $A$ be a set. A binary operation on $A$ is a map $\top : A \times A \longrightarrow A$. A set $A$ together with a binary operation $\top$ is called a binary operation-structure and is usually denoted by $(A, \top)$ or simply by $A$, with keeping in mind the given (fixed) binary operation on $A$. The image $\top(a, b)$ of the pair under the binary-operation $\top$ is usually denoted by $a \top b$. There are several commonly used notations for binary operations, e.g. $a * b$, $a \sqcap b$, $a \sqcup b$, $a \square b$, $a \Delta b$, $a \circ b$, $a + b$, $a \cdot b$ or just $ab$.
We generally use the multiplicative notation $ab$ and refer to $ab$ as the product of $a$ and $b$. Sometimes we also use the additive notation $a+b$ and refer to $a+b$ as the sum of $a$ and $b$.
A set may have several binary operations defined

on it. For example, on the sets $\mathbb{N} = \{0,1,2,\cdots\}$, $\mathbb{Z} = \{0,\pm1,\pm2,\cdots\}$, $\mathbb{Q} = \{a/b \mid a,b\in\mathbb{Z}, b\neq 0\}$, $\mathbb{R}$ and $\mathbb{C}$, of natural numbers, integers, rational numbers, real numbers, complex numbers, respectively, the usual addition $+$ and the usual multiplication $\cdot$ are binary operations.

**2.A.2 Examples** Let $X$ be any set. On the power set $\mathfrak{P}(X)$ of $X$, the union $\cup$, the intersection $\cap$ and the symmetric difference $\Delta$ are binary operations. On the sets $X^X = \text{Maps}(X,X)$ of maps from $X$ into itself or $\mathfrak{S}(X) = \{f\in X^X \mid f \text{ is bijective}\}$ of permutations on $X$, the composition of maps $\circ$ is a binary operation.

For the acquaintance with binary operations, we first describe particular computation-rules which are valid for many examples of binary operations.

**2.A.3 Definitions** Let $\top$ be a binary operation on a set $A$.

(1) $\top$ is said to be associative if for all $a,b,c\in A$, we have $(a\top b)\top c = a\top(b\top c)$.

It is not difficult to prove the following general associative-law (by induction on $n$):

General-Parentheses-rule : The product of an arbitrary sequence $a_1, \dots, a_n$ of elements in $A$, $n \geq 1$, is independent of the parentheses[1].

---

[1] The longer expressions $(\cdots((a_1 a_2) a_3) a_4 \cdots) a_n$ (standard parentheses) are not ambiguous. Parentheses may be inserted in any fashion for purpose and convenience of computations, the final result of two (or more) of such computations will be the same.

For $n \in \mathbb{N}^*$, let $\alpha_n$ denote the number of possible parentheses for a product of $n$ factors $a_1, \dots, a_n$. Then $\alpha_1 = 1$, $\alpha_n = \sum_{i=1}^{n-1} \alpha_i \alpha_{n-i}$, $n \geq 2$ and $\alpha_n = (2n-2)!/n!(n-1)!$, $n \in \mathbb{N}^*$.

-- One can think of binary operations and elements for which all these parentheses give distinct elements!

(2) T is said to be <u>commutative</u> if for all $a, b \in A$, we have $aTb = bTa$.

A binary-operation structure $(A, T)$ with the associative binary operation $T$ is called a <u>semi-group</u>. If in addition $T$ is commutative then it is called a <u>commutative semigroup</u>.

Let $A$ be a set with an associative and commutative binary operation (multiplicatively written). Then the product of a sequence of elements $a_1, \cdots, a_n$ in $A$ is not only independent of the parentheses but also of the order of the terms of the sequence: (General commutative law) For every permutation $\sigma$ of $\{1, 2, \cdots, n\}$, $a_{\sigma(1)} \cdots a_{\sigma(n)} = a_1 \cdots a_n$.
Proof is by induction on $n$ and is left to a reader.
In the additive notation the general commutative law is: $a_{\sigma(1)} + \cdots + a_{\sigma(n)} = a_1 + \cdots + a_n$. We also write shortly $\sum_{i=1}^{n} a_{\sigma(i)} = \sum_{i=1}^{n} a_i$.

Now we are interested in the properties of special elements in a binary-operation structure

(3) Let $A$ be a binary operation structure (multiplicatively written) and let $e \in A$. We say that $e$ is <u>left-neutral</u> in $A$ if for all $a \in A$, we have $ea = a$; $e$ is <u>right-neutral</u> in $A$ if for all $a \in A$, we have $ae = a$; $e$ is <u>neutral</u> in $A$ if $e$ is left-neutral and right-neutral in $A$, i.e. $ea = ae = a$ for all $a \in A$.

Neutral elements are unique; more generally, Let $e$ be a left-neutral element and let $e'$ be a right-neutral element in the semigroup $A$. Then $e = e'$. In particular, if neutral element exists, then it is unique (and hence write the neutral elem)

Proof Since $e$ is left-neutral, $ee' = e'$ and since $e'$ is right-neutral, $ee' = e$. Therefore $e' = e$.

(3) A semigroup which has a neutral element is called a monoid.

If a multiplicatively written binary operation structure $A$ has a neutral element, then it is often called the unity and is denoted by $1_A$. In an additively written binary operation structure the neutral element is called the zero-element and is denoted by $0_A$. This language had originated from the usual addition $+$ and the usual multiplication on the sets $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{N}$; The usual zero $0$ (resp. usual one $1$) is the neutral element in $(\mathbb{Q},+)$, $(\mathbb{Z},+)$, $(\mathbb{N},+)$ (resp. in $(\mathbb{Q},\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{N},\cdot)$). For the usual addition on $\mathbb{N}^*$, there is no neutral element.

(4) Let $M$ be a monoid (multiplicatively written) with the neutral element $e = e_M$. An element $a \in M$ is called invertible (or unit) in $M$ if there exists $a' \in M$ such that $aa' = a'a = e$. Further, such an element $a' \in M$ is called an inverse of $a$ in $M$.

Let $M$ be a semigroup and $M' \subseteq M$ be a subset of $M$. If $M'$ is closed under the binary operation of $M$, i.e. if $a', b' \in M'$, then $a'b' \in M'$, then $M'$ is called a subsemigroup of $M$. In this case the binary operation of $M$ induces a binary operation on $M'$ and with this $M'$ is a semigroup. Moreover, if $M$ is a monoid and if the neutral element $e$ of $M$ belongs to $M'$, then $e$ is also the neutral element of $M'$ and in this case $M'$ is called a submonoid of $M$.

For example, $(\mathbb{N}, +)$ is a submonoid of the monoids $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$; $(\mathbb{N}^*, +)$ is a subsemigroup of $(\mathbb{N}, +)$. The set $\mathfrak{S}(X)$ of permutations on a set $X$ is a submonoid of the monoid $(X^X, \circ)$ of the set of maps from $X$ into $X$ under composition $\circ$ of maps.

The intersection of a family of subsemigroups (resp. submonoids) of a semigroup (resp. monoid) $M$ is again a subsemigroup (resp. submonoid) of $M$. It follows that: for every family $a_i, i \in I$, of elements in a semigroup (resp. a monoid) $M$, there exists a smallest subsemigroup (resp. submonoid) $N$ containing all $a_i, i \in I$. This subsemigroup (resp. submonoid) $N$ is called the subsemigroup (resp. submonoid) generated by the family $a_i, i \in I$ and the family $a_i, i \in I$, is called a generating system of $N$.

For example, $2\cdot\mathbb{N} := \{2n \mid n \in \mathbb{N}\}$, $3\cdot\mathbb{N} := \{3n \mid n \in \mathbb{N}\}$, and $N := \{0, 2, 3, 4, 5, 6, \cdots\} = \mathbb{N} \setminus \{1\}$ are submonoids of $(\mathbb{N}, +)$ generated by $\{2\}$, $\{3\}$ and $\{2, 3\}$, resp.

If the element $a$ in a monoid $M$ has inverse in $M$, then it is unique (if $a'$ and $a''$ are both inverses of $a$, then $a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''$.)

If the element $a \in M$ in a multiplicatively written (resp. additively written) monoid $M$ has an inverse then its inverse is often denoted by $a^{-1}$ (resp. $-a$ also called the negative of $a$).

The set of invertible elements in a monoid $M$ is denoted by $M^{\times}$, i.e.

$$M^{\times} := \{ a \in M \mid a \text{ is invertible in } M \}.$$

In the monoids $(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$ every element is invertible, i.e. $(\mathbb{Q}, +)^{\times} = \mathbb{Q}$ and $(\mathbb{Z}, +)^{\times} = \mathbb{Z}$. But in the monoid $(\mathbb{N}, +)$ the element $0$ is the only invertible element, i.e. $(\mathbb{N}, +)^{\times} = \{0\}$. For the multiplicative monoids $(\mathbb{Q}, \cdot)$, $(\mathbb{Z}, \cdot)$ and $(\mathbb{N}, \cdot)$ we have: $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$,

$\mathbb{Z}^{\times} = \{1, -1\}$ and $\mathbb{N}^{\times} = \{1\}$.

In the monoid $(X^X, \circ)$ of the maps from $X$ into $X$ under composition $\circ$, an element $\varphi \in X^X$ is invertible if and only if there exists $\varphi' \in X^X$ such that $\varphi \circ \varphi' = \varphi' \circ \varphi = id_X$. This is precisely the case if and only if $\varphi$ is bijective; in this case $\varphi' = \varphi^{-1}$ (the inverse map of $\varphi$). Therefore $(X^X, \circ)^{\times} = \mathfrak{S}(X) =$ the set of permutations on $X$.

We note the following computation-rules for invertible elements:

**2.A.4**
Computation-rules for invertible elements: Let $M$ be a monoid (multiplicative) with the identity element $e = e_M$. Then:

(1) $e$ is invertible and $e^{-1} = e$

(2) If $a \in M$ is invertible, then $a^{-1}$ is also invertible and $(a^{-1})^{-1} = a$.

(3) If $a_1, \cdots, a_n \in M$ are invertible, then the product $a_1 \cdots a_n$ is also invertible and
$$(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}.$$
In particular, if $a, b \in M$ are invertible, then the product $ab$ is also invertible and
$$(ab)^{-1} = b^{-1}a^{-1}.$$

Proof (1) and (2) are obvious. (3) is proved by induction on $n$. It is therefore enough to prove for $n=2$. Since $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$ and $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$, the assertion is clear.

**2.A.5 Corollary** In a monoid $M$ the set $M^{\times}$ of invertible elements is a submonoid in which every element is invertible.

In the additive commutative monoid $M$, the computation-rules for invertible elements $a, b \in M$ are:
(1) $-0_M = 0_M$. (2) $-(-a) = a$. (3) $-(a+b) = (-a)+(-b) = -a-b$.

Let $M$ be a semigroup, $a \in M$ and $n \in \mathbb{N}^*$. The $n$-fold product (a....a ($n$-times)) of $a$ with itself is called the $n$-th power of $a$ and is denoted by $a^n$. In particular, $a^1 = a$.
If $M$ has the neutral element $e$, then we put $a^0 := e$. Moreover, if $a$ is invertible in $M$, then $a^n$ for $n \in \mathbb{Z}$, $n < 0$, is defined by $a^n := (a^{-1})^{-n}$. By 2A.4 (3) we have $a^n = (a^{-1})^{-n} = (a^{-n})^{-1}$.

**2.A.6 Computation-rules for powers.** Let $M$ be a semigroup and let $a, b \in M$ be commuting elements of $M$, i.e. $ab = ba$. Then for all $m, n \in \mathbb{N}^*$, we have:

(1) $a^m a^n = a^{m+n}$. (2) $(a^m)^n = a^{mn}$.

(3) $a^m b^n = b^n a^m$. (4) $(ab)^m = a^m b^m$.

If $M$ has the neutral element $e$, then the rules (1) – (4) hold for all $m, n \in \mathbb{N}$. Moreover, if $a$ and $b$ are invertible or one of them is invertible, then the rules (1) – (4) also hold for all those $m, n \in \mathbb{Z}$ for which these rules make sense.

Proof: For exponents $m, n \in \mathbb{N}$, the rules (1) and (2) are trivial, the rules (3) and (4) are special cases of the general commutative law. For the cases of negative exponents with the help of the definition of the powers with negative exponents, we reduce to prove these rules for exponents in $\mathbb{N}$ by replacing $a, b$ either by $a^{-1}, b$ or by $a^{-1}, b^{-1}$. But then we need to note that: if $a$ and $b$ commute, then $a^{-1}, b$ and $a^{-1}, b^{-1}$ also commute; this is clear from $b = a^{-1}(ab) = a^{-1}(ba) = (a^{-1}b)a$ and hence $ba^{-1} = (a^{-1}b)(aa^{-1}) = a^{-1}b$. Finally, $a^{-1}b^{-1} = (ba)^{-1} = (ab)^{-1} = b^{-1}a^{-1}$. Further, details are left to a reader.

If the binary operation in a monoid $M$ is written additively, then the $n$-th powers of $a \in M$ are called <u>$n$-folds</u> and denoted by $na$, $n \in \mathbb{N}$ (resp. $n \in \mathbb{Z}$ if $a \in M^\times$). (In particular, $1\,a = a$ and $0 \cdot a = 0_M$.) The $n$-folds of $a$ are also called, generally, the <u>natural</u> (resp. <u>integral</u>) <u>multiple</u> of $a$. The computation-rules in 2.A.6 are then written as:

(1) $ma + na = (m+n)a$ (2) $n(ma) = (mn)a = (nm)a$.

(3) $ma + nb = nb + ma$ (4) $m(a+b) = ma + mb$.

We now come to the concept of divisibility in monoids:

**2.A.7 Definition** Let $M$ be a commutative monoid. An element $a \in M$ is called a <u>divisor</u> of $b \in M$, (resp. $b \in M$ is a <u>multiple</u> of $a \in M$), if there exists $c \in M$ such that $ac = b$; we often write this as $a \mid b$ and read "<u>a divides b</u>"

If $a$ is a divisor of $b$ and if $ac = b$, then the element $c$ is in general not uniquely determined by $a$ and $b$. However, if the semigroup $M$ is regular, then this quotient $c$ is uniquely determined.

**2.A.8 Definition** Let $M$ be a semigroup (not necessarily commutative) and let $a \in M$. We say that $a$ is *left-regular* (resp. *right-regular*) in $M$ if for all $x, y \in M$, from $ax = ay$ (resp. $xa = ya$) it follows that $x = y$; $a$ is called *regular* if it is both left-regular and right-regular.

We note some computation-rules:

**2.A.9 Lemma** Let $M$ be a monoid with the neutral element $e$. Then

(1) $e$ is regular

(2) If $a \in M$ is invertible, then $a$ is regular.

(3) If $a, b \in M$ are regular, then the product $ab$ is also regular.

*Proof* (1) is trivial. (2) From $ax = ay$ it follows that $a^{-1}(ax) = a^{-1}(ay)$, i.e. $ex = ey$ or $x = y$. Similarly, from $xa = ya$, we get $x = y$.

(3) From $(ab)x = (ab)y$, we get $a(bx) = a(by)$ and hence $bx = by$, since $a$ is regular and then $x = y$, since $b$ is regular. Similarly, prove the right-regularity of $ab$.

For an element $a \in M$ in a semigroup $M$, the map $\lambda_a : M \to M$, $x \mapsto ax$, is called the *left-multiplication* by $a$ and the map $\rho_a : M \to M$, $y \mapsto ya$

is called the <u>right multiplication</u> by a. An element a is left-regular (resp. right regular) if and only if $\lambda_a$ (resp. $\rho_a$) is injective. In particular, a is regular if and only if $\lambda_a$ and $\rho_a$ are injective. The set $M^* := \{a \in M \mid a \text{ is regular in } M\}$ of regular elements is a subsemigroup of M by 2.A.9. Moreover, if M is a monoid, then $M^*$ is a submonoid of M. Further, for any monoid M, by 2.A.9 $M \subseteq M^* \subseteq M$. We say that a semigroup M is regular if every element of M is regular, i.e. $M^* = M$.

**2.A.10 Definition** A <u>group</u>[1] is a monoid in which every element is invertible. Therefore a group is a set with an associative binary operation (multiplicatively written) with an element $e \in G$ such that the following conditions are satisfied:

(1) e is a neutral element in G, i.e. $ea = ae = a$ for all $a \in G$.

(2) For every $a \in G$, there is an inverse element, i.e. an element $a' \in G$ with $aa' = a'a = e$.

If in addition the binary operation of G is commutative, then we say that G is a <u>commutative</u> or <u>abelian</u>[2] group.

---

[1] The use of the word "Group" goes back to <u>Évariste Galois</u> (1811–1832).

2 Named after Niels-Henrik Abel (1802–1829).

**2.A.11 Remark** The requirements in the definition 2.A.10 of a group can be weakened. Often the following assertion is used:
Let $G$ be a semigroup with an element $e \in G$ with properties:
(1') $e$ is right-neutral, i.e. $ae = a$ for all $a \in G$.
(2') For every element $a \in G$, there is a right inverse, i.e. an element $a' \in G$ with $aa' = e$.
Then $G$ is a group with neutral element $e$.
For a proof first we shall show that $e$ is the neutral element in $G$. Let $a \in G$ be arbitrary. Then there exist $a', a'' \in G$ with $aa' = e$ and $a'a'' = e$. Therefore $a = ae = a(a'a'') = (aa')a'' = ea''$; further $ea'' = (ee)a'' = e(ea'')$ and hence putting $ea'' = a$, we get $a = ea$ as required. Finally we need not only to show $aa' = e$, but also to show $a'a = e$. This is clear, since $a = a''$ proved just above.
- Naturally, the above assertion remain true if we replace "right-neutral" by "left-neutral" and at the same time "right-inverse" by "left-inverse"

**2.A.12 Example** Let $G$ be a group (written multiplicatively). Then the binary operation on $G$ defined by $G \times G \longrightarrow G$, $(a,b) \longmapsto ab^{-1}$ is not associative if there is at least one $b \in G$ with $b \neq b^{-1}$. To check this, put $a * b := ab^{-1}$. Then $a*(b*c) = a(b*c)^{-1} = a(bc^{-1})^{-1} = acb^{-1}$, on the other hand $(a*b)*c = (ab^{-1})c^{-1} = ab^{-1}c^{-1}$ and $acb^{-1} \neq ab^{-1}c^{-1}$ for arbitrary $a \in G$, $b = e$ and an element $c$ with $c^{-1} \neq c$.

**2.A.13 Examples** On a singleton set $\{x\}$, there is a unique binary operation, namely $(x,x) \mapsto x$. With this binary operation $\{x\}$ is clearly a group. This group is called the trivial group. — In the additive notation it is called the zero-group.

The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ with the usual addition are groups, but $(\mathbb{N},+)$ is not a group. Moreover, $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$ and $\mathbb{C}\setminus\{0\}$ with the usual multiplication are groups, but $(\mathbb{Z}\setminus\{0\},\cdot)$ is not a group. All these are commutative groups.

If $M$ is a monoid, then the subset $M^\times$ of invertible elements of $M$ is a group (under the same binary operation of $M$) by 2.A.5. This group is called the unit group of the monoid $M$.

The groups are distinguished non-empty semigroups in which certain equations have solutions. Let $G$ be a semigroup and let $a, b \in G$. We say that the equation $ax=b$ (resp. $ya=b$) have solution in $G$ or is solvable in $G$, if there exists $x_0 \in G$ (resp. $y_0 \in G$) such that $ax_0=b$ (resp. $y_0a=b$). Further, we say that these equations have unique solutions in $G$ if $x_0$ (resp. $y_0$) are uniquely determined by $a$ and $b$. In regular semigroups solvable equations always have unique solutions (by definition).

**2A.14 Theorem** Let $G$ be a non-empty semi-group. Then the following statements are equivalent:

(1) $G$ is a group.

(2) For arbitrary $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions in $G$.

(3) For arbitrary $a, b \in G$, the equations $ax = b$ and $ya = b$ have solutions in $G$.

Proof (1) $\Rightarrow$ (2): Since $a(a^{-1}b) = (aa^{-1})b = eb = b$, $a^{-1}b$ is a solution of $ax = b$ in $G$. Analogously, $ba^{-1}$ is a solution of $ya = b$ in $G$. Conversely, if $x_0, y_0 \in G$ are solutions of $ax = b$ and $ya = b$, respectively, i.e. $ax_0 = b$ and $y_0 a = b$. ultiplying these equations on the left (resp. right) by $a^{-1}$, we get $x_0 = a^{-1}b$ and $y_0 = ba^{-1}$. This proves the uniqueness of solutions.

The statement (3) is weaker than (2) and hence clearly (2) $\Rightarrow$ (3).

(3) $\Rightarrow$ (1): Since $G \neq \phi$, there is an element $e \in G$. By (3) the equation $yb = b$ has a solution $b \in G$, i.e. $eb = b$. We shall show that for an arbitrary element $a \in G$, $ea = a$. For this let $c \in G$ be a solution of the equation $bx = a$, i.e. $bc = a$. Then $ea = e(bc) = (eb)c = bc = a$. Therefore $e$ is a left-neutral element in $G$. Further, every element $a \in G$ has a left-inverse $a'$ in $G$, since the equation $ya = e$ has a solution, say $a'$ in $G$. Therefore by the Remark 2.A.11 $G$ is a group.

**2.A.15 Corollary** Let $G$ be a non-empty semigroup. Then the following statements are equivalent:

(1) $G$ is a group.

(2) For every $a \in G$, the left-translation $\lambda_a : G \longrightarrow G$, $x \longmapsto ax$ and the right-translation $\rho_a : G \longrightarrow G$, $y \longmapsto ya$ are bijective.

(3) For every $a \in G$, the left-translation $\lambda_a : G \longrightarrow G$, $x \longmapsto ax$ and the right-translation $\rho_a : G \longrightarrow G$, $y \longmapsto ya$ are surjective

Proof The assertions (2) and (3) of this corollary are equivalent with the assertions (2) and (3) of 2.A.14, respectively.

**2.A.16 Corollary** A non-empty finite semigroup $G$ is a group if and only if $G$ is regular.

Proof If $G$ is a group, then clearly $G$ is a regular semigroup. Conversely, if $G$ is regular, then both $\lambda_a : G \longrightarrow G$, $x \longmapsto ax$ and $\rho_a : G \longrightarrow G$, $y \longmapsto ya$ are injective and hence also surjective, since $G$ is finite. Now the assertion follows from 2.A.15.

Non-empty semigroups of groups need not be again groups, for example $\mathbb{N} (\subseteq \mathbb{Z})$ with usual addition is not a group, But $\mathbb{N}$ is regular. From 2.A.16 we still have:

**2.A.17 Corollary** Non-empty finite subsemigroups of groups are again groups.

<u>2.A.18 Example</u> On the set $\mathbb{N}$ of natural numbers consider the binary operations $T_1, T_2, T_3$ defined by:

$mT_1n := m^n$ , $mT_2n := m^2+n^2$ , $mT_3n := m$.

The binary operation $T_1$ is neither associative nor commutative; $T_2$ is commutative, but not associative and $T_3$ is associative, but not commutative. In $(\mathbb{N}, T_3)$ every element is right-neutral, but no element is left-neutral. Moreover, all equations of the form $y T_3 a = b$ has unique solution in $(\mathbb{N}, T_3)$, but the equations of the form $a T_3 x = b$ has a solution only in the case $a=b$. Naturally $(\mathbb{N}, T_3)$ is not a group.

<u>2.A.19 Example</u> On the power set $\mathfrak{P}(X)$ of a set both the binary operations "$\cap$" and "$\cup$" are commutative and associative. Further, $X$ is the neutral element with respect to $\cap$ and $\phi$ is the neutral element with respect to $\cup$. Nevertheless, in the case $X \neq \phi$, neither $(\mathfrak{P}(X), \cap)$ nor $(\mathfrak{P}(X), \cup)$ is a group, since in both the examples, the neutral element is the only invertible element; this is also the only regular element.

<u>2.A.20 Example</u> On the set $X^X = \mathrm{Maps}(X, X)$ of all the maps from $X$ into itself, the composition of maps $\circ$ is an associative binary operation, i.e. $(X^X, \circ)$ is a semigroup with the identity map

$id_X$ as the neutral element. If $X$ has at least two elements $a, b$ with $a \neq b$, then this semi-group is not commutative. Namely, if $f$ and $g \in X^X$ are the constant maps $X \longrightarrow X$, $x \longmapsto a$ and $X \longrightarrow X$, $x \longmapsto b$, respectively, then $f \circ g$ is the constant map $x \longmapsto a$ and $g \circ f$ is the constant map $x \longmapsto b$ and hence $f \circ g \neq g \circ f$.
In the monoid $(X^X, \circ)$, the bijective maps are precisely the invertible elements, i.e. the unit group of the monoid $(X^X, \circ)$ is the group of permutations on $X$. Further, the injective maps are precisely the left-regular elements and the surjective maps are precisely the right-regular elements. In particular, in this example, invertible elements are precisely regular elements.

**2.A.21 Example** (Permutation group on $X$)
The set $\mathfrak{S}(X)$ of all bijective maps from $X$ onto $X$ with the composition of maps $\circ$ is a group. The identity map $id_X$ is the neutral element in $(\mathfrak{S}(X), \circ)$ and for $f \in \mathfrak{S}(X)$ is the inverse map $f^{-1} \in \mathfrak{S}(X)$ of $f$ is the inverse of $f$ in $(\mathfrak{S}(X), \circ)$. This group $(\mathfrak{S}(X), \circ)$ is called the permutation group on $X$. If $X$ has at least elements, then $\mathfrak{S}(X)$ is not commutative:

Moregenerally, on the set of all relations $\mathcal{R}(X)$ $(= \mathfrak{P}(X \times X))$ on $X$, define the binary operation $\circ$ by:

$$R \circ S := \{(x,y) \in X \times X \mid \text{there exists } z \in X \text{ such that } (x,z) \in S \text{ and } (z,y) \in R\}$$

Then $(\mathcal{R}(X), \circ)$ is a monoid and $(X^X, \circ)$ is a submonoid. Moreover, the set of invertible elements in $(\mathcal{R}(X), \circ)$ is precisely $\mathfrak{S}(X)$.

**2.A.22 Example** (Binary operation table)
A binary operation $\top$ on a finite set $A = \{a_1, \cdots, a_n\}$ of $n$ elements is more often notified in the form of a binary operation-table:

| $\top$ | $a_1$ | $\cdots$ | $a_j$ | $\cdots$ | $a_n$ | |
|---|---|---|---|---|---|---|
| $a_1$ | $a_1 \top a_1$ | $\cdots$ | $a_1 \top a_j$ | $\cdots$ | $a_1 \top a_n$ | |
| | $\vdots$ | $\ddots$ | $\vdots$ | | $\vdots$ | |
| $a_i$ | $a_i \top a_1$ | $\cdots$ | $a_i \top a_j$ | $\cdots$ | $a_i \top a_n$ | $\longrightarrow$ $i$-th row |
| | $\vdots$ | | $\vdots$ | $\ddots$ | $\vdots$ | |
| $a_n$ | $a_n \top a_1$ | $\cdots$ | $a_n \top a_j$ | $\cdots$ | $a_n \top a_n$ | |
| | | | $\uparrow$ $j$-th column | | | |

In the $(i,j)$-th position (in the $i$-th row and $j$-th column) there is the element $a_i \top a_j$.

Clearly the binary operation $\top$ is commutative if and only if the binary-operation table is symmetric with respect to the reflection along the main diagonal.

The element $a_i$ is the neutral element w.r.to $\top$ if and only if the $i$-th row and $j$-th column is equal to the given-row $a_1, \cdots, a_n$ respectively the given column ${}^t(a_1, a_2, \cdots, a_n)$.

The element $a_i$ is regular if and only if in the i-th row and in the j-th column every element of A appear at most - (and hence by the finiteness of A also exactly) once. This means that all equations $a_i T x = b$ and $y T a_i = b$ have unique solutions in A. Therefore if T is associative, then $(A, T)$ is a group if and only if in every row and column of the binary-operation table of T every element of A (exactly once) appear. In the case when $(A, T)$ is a group, the binary operation table is called the group-table of $(A, T)$

As an example, consider the semigroup $(X^X, \circ)$ for the set $X = \{1, 2\}$; this has exactly four elements, namely, $id_X$, $f$, $g$ and $h$, where $f(1) = f(2) = 1$; $g(1) = g(2) = 2$ and $h(1) = 2$, $h(2) = 1$. Then the binary-operation table of $(X^X, \circ)$ is:

| $\circ$ | id | f | g | h |
|---|---|---|---|---|
| id | id | f | g | h |
| f | f | f | f | f |
| g | g | g | g | g |
| h | h | g | f | id |

Once again this table confirms that $(X^X, \circ)$ is neither commutative nor a group.

**2.A.23 Example** Let $\sigma_1$ and $\sigma_2$ denote the mirror reflections of the coordinate-axes in $\mathbb{R}^2$, i.e. $\sigma_1 : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, $(x,y) \longmapsto (x,-y)$ and $\sigma_2 : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, $(x,y) \longmapsto (-x,y)$. Let $\delta : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be the rotation by $\pi$ at the origin, i.e. $\delta(x,y) = (-x,-y)$. Consider the set $M = \{id_{\mathbb{R}^2}, \sigma_1, \sigma_2, \delta\}$

Then: $\sigma_1 \circ \sigma_1 = id_{\mathbb{R}^2}$, $\sigma_2 \circ \sigma_2 = id_{\mathbb{R}^2}$, $\sigma_1 \circ \sigma_2 = \delta$,

$\sigma_2 \circ \sigma_1 = \delta$, $\delta \circ \sigma_1 = \sigma_2 = \sigma_1 \circ \delta$, $\delta \circ \sigma_2 = \sigma_1 = \sigma_2 \circ \delta$

and $\delta \circ \delta = id_{\mathbb{R}^2}$. Therefore the composition $\circ$ of maps is a binary operation on $M$ with the binary-operation table:

| $\circ$ | $id_{\mathbb{R}}$ | $\sigma_1$ | $\sigma_2$ | $\delta$ |
|---|---|---|---|---|
| $id_{\mathbb{R}}$ | $id_{\mathbb{R}^2}$ | $\sigma_1$ | $\sigma_2$ | $\delta$ |
| $\sigma_1$ | $\sigma_1$ | $id_{\mathbb{R}^2}$ | $\delta$ | $\sigma_2$ |
| $\sigma_2$ | $\sigma_2$ | $\delta$ | $id_{\mathbb{R}^2}$ | $\sigma_1$ |
| $\delta$ | $\delta$ | $\sigma_2$ | $\sigma_1$ | $id_{\mathbb{R}^2}$ |

Moreover, the composition $\circ$ is associative and $(M, \circ)$ is a commutative group.

**2.A.24 Example** (Direct product) Let $M_1$, $M_2$ be sets with binary operations $T_1$, $T_2$, resp. Then on the cartesian product $M_1 \times M_2$ the component-wise binary operation is defined by $(a_1, a_2) \top (b_1, b_2) := (a_1 T_1 b_1, a_2 T_2 b_2)$. Moreover, all computation-rules which hold for both $T_1$ and $T_2$ also hold for $T$. In particular, if $(M_1, T_1)$ and $(M_2, T_2)$ are semigroups, then $(M_1 \times M_2, T)$ is also a semigroup; if $e_1 \in M_1$ and $e_2 \in M_2$ are neutral elements, then $(e_1, e_2)$ is the neutral element in $(M_1 \times M_2, T)$; an element $(a_1, a_2) \in M_1 \times M_2$ is invertible if and only if $a_1$ is invertible in $M_1$ and $a_2$ is invertible in $M_2$; if $(M_1, T_1)$ and $(M_2, T_2)$ are groups, then $(M_1 \times M_2, T)$ is also a group. $(M_1 \times M_2, T)$ is called the direct product of $(M_1, T_1)$ and $(M_2, T_2)$.

More generally, let $M_i$, $i \in I$, be a family of sets with (multiplicatively written) binary operations. Then on the product $\prod_{i \in I} M_i$ the component wise binary operation is defined by

$$\left((a_i)_{i\in I}, (b_i)_{i \in I}\right) \longmapsto (a_i b_i)_{i \in I}$$

This binary operation is called the product of binary operations of $M_i$, $i \in I$ and the product set $\prod_{i \in I} M_i$ with this product binary operation is called the direct product of $M_i$, $i \in I$.

Moreover, all the computation-rules which hold for all $M_i$, $i\in I$, also hold for $\prod_{i\in I} M_i$. In particular, if $M_i$, $i\in I$, are all semigroups, then $\prod_{i\in I} M_i$ is also a semigroup. -- Called the direct product of the semigroups $M_i$, $i\in I$; if all $M_i$, $i\in I$, are monoids with neutral elements $e_i\in M_i$, $i\in I$, then $\prod_{i\in I} M_i$ is also monoid with the neutral element $(e_i)_{i\in I}$; an element $(a_i)_{i\in I} \in \prod_{i\in I} M_i$ is invertible if and only if each $a_i$, $i\in I$, is invertible in $M_i$, $i\in I$, i.e. $\left(\prod_{i\in I} M_i\right)^{\times} = \prod_{i\in I} M_i^{\times}$; therefore the direct product monoid $\prod_{i\in I} M_i$ of monoids $M_i$, $i\in I$, is a group if and only if each $M_i$, $i\in I$, is a group, this group is called the direct product of the groups $M_i$, $i\in I$.

In the special case when $M_i = M$ for all $i\in I$ and with the same binary operation on $M$. One can interpret $I$-tuples $(a_i)_{i\in I} \in \prod_{i\in I} M$ as maps from $I$ into $M$, i.e. as elements in $M^I = \mathrm{Maps}(I, M)$.

Then the above componentwise binary operation corresponds to the binary-operation on $M^I$:

$(fg)(i) := f(i)\,g(i)$, $f, g\in M^I$, $i\in I$

(in the additive notation on $M$:

$(f+g)(i) := f(i) + g(i)$, $f, g \in M^I$, $i\in I$.) With this binary operation $M^I$ is called the I-fold direct product of $M$.

If $M$ is a semi-group (resp. monoid, group), then $M^I$ is also a semi-group (resp. monoid, group). Further, if $M$ is a monoid, then the unit group of the monoid $M^I$ is the $I$-fold direct product of the unit group $M^\times$ of $M$, i.e. $(M^I)^\times = (M^\times)^I$

## 2.A Exercises

1. Let $s$ and $t$ be integers. Then $\top : \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$, $(a,b)\longmapsto a\top b := sa+tb$, is a binary operation on $\mathbb{Z}$. For which $s, t \in \mathbb{Z}$, this binary operation is associative (resp. commutative)?

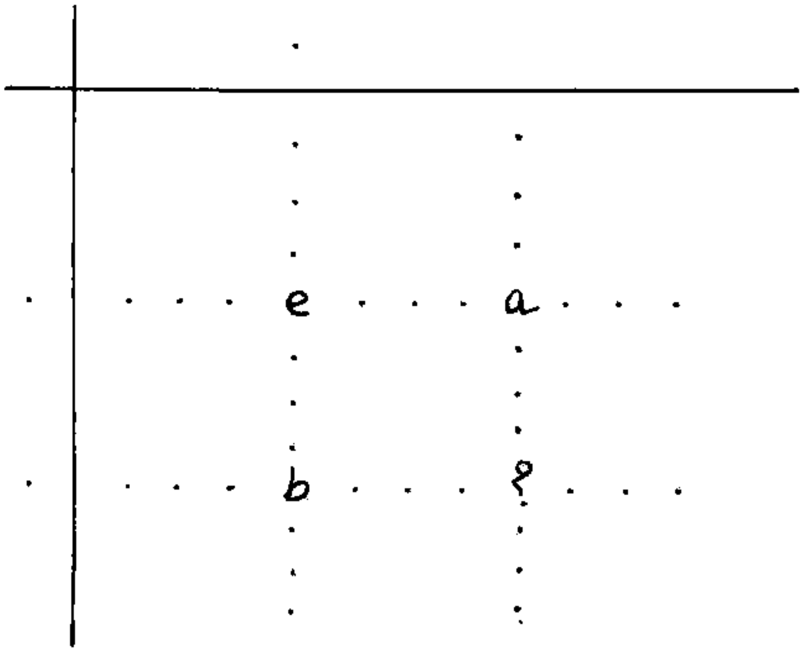
2. On the set $\mathbb{R}\setminus\{1\}$ define the binary operation $\top$ by: $a\top b := a+b-ab$. Show that $(\mathbb{R}\setminus\{1\},\top)$ is a commutative group.

3. Let $M$ be a monoid and $x\in M$. Show that $x^2=e$ if and only if $x$ is invertible in $M$ with $x^{-1}=x$.

4. Reconstruct the group-table from the following table by filling-up missing places. (The solution is unique!)

| | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ |
|---|---|---|---|---|---|
| $a_1$ | . | . | . | $a_4$ | . |
| $a_2$ | . | $a_3$ | $a_4$ | . | . |
| $a_3$ | . | . | . | . | . |
| $a_4$ | . | . | . | . | . |
| $a_5$ | . | . | . | . | . |

5. In the following group-table of a (finite) group with neutral element $e$, which element of $G$ must be there at the position marked by ?:



6. In every row and every column of the following binary-operation table every element appears exactly once. However, it is not a group-table why?

| | e | a | b | c | d |
|---|---|---|---|---|---|
| e | e | a | b | c | d |
| a | a | e | c | d | b |
| b | b | d | e | a | c |
| c | c | b | d | e | a |
| d | d | c | a | b | e |

7. For an element $a$ in a monoid $M$, the following statements equivalent:

(1) $a$ is invertible in $M$, i.e. $a \in M^{\times}$.

(2) The left translation $\lambda_a : M \longrightarrow M$ is bijective.

(3) The right-translation $\rho_a : M \longrightarrow M$ is bijective.

8. Let $a$ be an element in a monoid $M$ with neutral element $e$. We say that $a$ has a left-inverse if there exists $a' \in M$ such that $a'a = e$ and has a right-inverse if there exists $a'' \in M$ such that $aa'' = e$. Show that if $a \in M$ has a $\underbrace{\text{left-inverse}}_{a' \in M}$ and $\underbrace{\text{right inverse}}_{a'' \in M}$, then $a$ is invertible and $\bar{a}^{1} = a' = a''$. Deduce that if $a \in M$ has more than one right inverse (resp. left inverse), then $a$ has no left-inverse (resp. right inverse).

9. In the monoid $\mathbb{N}^{\mathbb{N}}$ (under composition $\circ$), let $\varphi \in \mathbb{N}^{\mathbb{N}}$ be defined by $\varphi(0) := 0$, $\varphi(n) = n-1$ if $n \geq 1$ and $\psi \in \mathbb{N}^{\mathbb{N}}$ be defined by $\psi(n) = n+1$. Then $\varphi\psi = id_{\mathbb{N}}$ and the element $\psi \in \mathbb{N}^{\mathbb{N}}$ has infinitely many left-inverses and hence in particular, not invertible in $\mathbb{N}^{\mathbb{N}}$

10. Let $M$ be a monoid, in which every equation of the form $ax = b$ with $a, b \in M$ has a solution in $M$. Show that $M$ is a group.

11. Let $M$ be a monoid and let $x \in M$ with $x^d = e$ for some $d \in \mathbb{N}^*$. Show that $x \in M^*$ and for all $m, n \in \mathbb{Z}$, $x^m = x^n$ if $m \equiv n \pmod d$.

12. Let $M$ be a monoid and let $a_1, \cdots, a_n \in M$ be such that the product $a_1 \cdots a_n$ is invertible in $M$. Then in the following cases, show that all $a_1, \cdots, a_n$ are also invertible in $M$:

(1) $a_1, \cdots, a_n$ are pairwise commutative, i.e. $a_i a_j = a_j a_i$ for all $1 \leq i, j \leq n$.

(2) $M$ is finite, i.e. $M$ has only finitely many elements

(3) $M$ is regular

13. Let $M$ be a lattice, i.e. an ordered set, in which every two elements has infimum and supremum. We put: for $a, b \in M$,
$a \sqcup b := \operatorname{Sup}\{a,b\}$ and $a \sqcap b := \operatorname{Inf}\{a,b\}$.
Show that the binary operations $\sqcup$ and $\sqcap$ on $M$ are associative, commutative and satisfy the so-called fusion-rules: for all $a, b \in M$,
$$a \sqcup (a \sqcap b) = a \text{ and } a \sqcap (a \sqcup b) = a.$$
Conversely, suppose that $M$ is a set with two associative and commutative binary operations $\sqcup$ and $\sqcap$, in which the above fusion-rules hold. Then define a relation $\leq$ on $M$ by:
$a \leq b$ for $a, b \in M$ if $a \sqcap b = a$. Then show that $\leq$ is an order on $M$ and $a \sqcup b = \operatorname{Sup}\{a,b\}$ and $a \sqcap b = \operatorname{Inf}\{a,b\}$ for all $a, b \in M$.

14. a) Let $M = \{a, b\}$ be a set with two distinct elements $a$ and $b$. There are exact 16 binary-operations on $M$. How many of these binary operations on $M$ are associative, commutative and have neutral element?

b) From a binary operation $*$ on an arbitrary set $M$, using many-fold product maps, we can define new binary operations on $M$, for example, $(x,y) \longmapsto (x*x)*(y*y)$, $(x,y) \mapsto x*(y*x)$, and so on... . Show that on the two element set $M = \{t, f\}$ using the binary-operation given by the table:

| $\mid$ | $t$ | $f$ |
|---|---|---|
| $t$ | $f$ | $t$ |
| $f$ | $t$ | $t$ |

, we can get all binary operations on $M = \{t, f\}$ by the above process. (Remark If the elements $t$ and $f$ of $M$ are both truth-values "True" and "False" resp., then the above given binary operation $\mid$ on $M$ is called the Sheffer stroke. The stroke $\mid$ is named after Henry M. Sheffer (American logician, 1882-1964; Polish Jew born in Ukraine who migrated to USA. In 1913 Sheffer provided an axiomatization of Boolean algebras using the stroke $\mid$, a logical operation equivalent to the negation of the conjunction operation $\wedge$, i.e. $p \mid q \equiv \neg(p \wedge q)$; in ordinary language "not both".)

15. Let $M$ be a semigroup with the following two properties: (1) For all $a \in M$, the left-translations $\lambda_a : M \to M$, $x \mapsto ax$, are surjective. (2) There exists at least one $b \in M$ such that the right translation $\rho_b : M \to M$, $y \mapsto yb$ is surjective. Show that $M$ is a group.

16. Construct a semigroup $M$ which is not a group, but there is an element $e \in M$ satisfying the following properties: (1) $ea = a$ for all $a \in M$. (2) For every $a \in M$, there exists $a' \in M$ such that $aa' = e$.

17 Let $G$ be a finite group with $n$ elements and let $(a_1, \cdots, a_n) \in G^n = G \times G \times \cdots \times G$ ($n$-times). Show that there exists indices $r, s$ with $0 \leq r < s \leq n$ such that $a_{r+1} \cdots a_s = e_G$.
(Hint: The products $a_1 \cdots a_s$, $s = 0, \cdots, n$ cannot be pairwise distinct.)