The Cayley type theorem for semigroups

Presentation · October 2018

CITATIONS
0

READS
10,109

1 author:

Jens Fehlau
Universität Potsdam
1 PUBLICATION **0** CITATIONS

SEE PROFILE

University of Potsdam
Department of Mathematics and Science

Institute of Mathematics

Bachelor's thesis

The Cayley type theorem for semigroups

By:	Jens Fehlau
Date of birth:	18.06.1994
Supervisors:	PD Dr. Jörg Koppitz
	Dr. Andreas Braunß
Published:	09.10.2018

This page intentionally left blank

ABSTRACT

This paper mainly deals with the basics of semigroup theory. The foundation of this thesis is the first chapter of Tero Harju's lecture notes on semigroup theory, dating back to 1996. Constructing a number system, working through examples to make abstract concepts tangable, and proving the "Cayley type theorem for semigroups" is this paper's main goal. All the main definitions which are not part of Harju's notes are taken out of Joachim Gräter's 2018 "Algebra and Arithmetik" script, whereas the historical excursion has been inspired by Christopher Holling's article on the early developements of semigroup theory.

PREFACE

The term "semigroup" was first introduced in 1904 to describe a system that extends results of finite groups to infinite ones.
The definition of those "semigroups" slighty differs from our understanding nowadays. The modern, now used definiton of semigroups got more and more common in the early years of the twentieth century without a real name (for example in the representation-theoretic work of Frobenius and Schur (1906) where it was first observed that a group's inverses were unnecessary for the problem at hand). Although used by many at the time, one cannot really talk about semigroup theory because if used, they were nothing but byproducts of the work at hand.
The first proper use of semigroup theory can be attributed to Anton Kazimirovich Suschkewitsch and his work in the early 1920. His usage of (algebraic) semigroup theory before the rest of the world is what granted us many different results we now take for granted.
Suschkewitschs textbook *The Theory of Generalised Groups* (1937) and his other work (which mostly remainded unknown for many many years) together with many papers appearing in and after the 1930s laid a broad foundation of the theory, peaking in an outburst of papers in 1940 and 1941 wich can be condensed into three different, highly influential papers: Rees (1940), Clifford (1941) and Dubreil (1941). Rees' paper contained semigroup theory's first great structure theorem (which is appropriately know nowadays as Rees' Theorem), while Cliffords paper with his structure theorem, which has no analogues in either group or ring theory, can be marked as the beginning of an independent theory of semigroups.
Starting with the 1950s it was apparent that semigroup theory could stand on its own. The theory had been advanced further and further, especially in the USSR. But due to a lack of communication at that time between countries, it so happened that a lot of results were derived simultaneously in different parts of the world resulting in a lot of duplicates.
One problem that came with quite similar derivations, was that everyone was using different notation, definitions and terminology. To tackle this specific problem, Clifford and Preston's classic book *The Algebraic Theory of Semigroups* has been published starting 1961, which is still considered the norm up to this date when it comes to notation and the sorts. This standardisation was one of the reasons why semigroup theory became a worldwide established and still researched branch of mathematics.

Contents

1 The Set of Natural Numbers

Before we can begin to go into detail about semigroup theory, we have to make some preparations beforehand. We start off by introducing the so-called *Peano Axioms*, which allow us to construct the number system that we usually call *the set of natural numbers* or *positive integers*.

Definition. **The Peano Axioms:**

Let there exists a non-empty set $\mathbb{N}$ such that

P1: $0 \in \mathbb{N}$.
P2: For all $n \in \mathbb{N}$ there exists a unique $\text{succ}(n) \in \mathbb{N}$, called the successor of n.
P3: For all $n \in \mathbb{N}$ holds $\text{succ}(n) \neq 0$.
P4: If $m, n \in \mathbb{N}$ and $\text{succ}(m) = \text{succ}(n)$, then $m = n$.
P5: For any $S \subseteq \mathbb{N}$ satisfying

(i) $0 \in S$
(ii) $s \in S \Rightarrow \text{succ}(s) \in S$

,we have $S = \mathbb{N}$.

This newly constructed set will allow us to perform basic arithmetic using two operations that we call *addition* and *multiplication* on $\mathbb{N}$.

Definition. **The usual addition:**

Let for all $n, m \in \mathbb{N}$, $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(n, m) \mapsto n + m$ be given by:

(i) $n + 0 = n$
(ii) $n + \text{succ}(m) = \text{succ}(n + m)$,whenever $n + m$ is defined.

Definition. **The usual multiplication:**

Let for all $n, m \in \mathbb{N}$, $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(n, m) \mapsto n \cdot m$ be given by:

(iii) $n \cdot 0 = 0$
(iv) $n \cdot \text{succ}(m) = n \cdot m + n$,whenever $n \cdot m$ is defined.

Now that we have established those operations, it is time to introduce the main tool for proving statements regarding the natural numbers:

Theorem. **The principle of mathematical induction:**

Let $\mathcal{P}(n)$ be a certain proposition. $\mathcal{P}(n)$ is said to be true for all $n \in \mathbb{N}$ under the condition, that $\mathcal{P}(k = 0)$ (the base step) is true and, for every $k \in \mathbb{N}$, $\mathcal{P}(k)$ (the induction hypothesis) is true implies $\mathcal{P}(\text{succ}(k))$ is true.

What this theorem basically states, is, that we assume a certain statement about $n \in \mathbb{N}$ to be true, and show, that this hypothesis ensures our statement to still hold for the successor of n. Let us now establish a few rules about the natural numbers that we are going to use at a later point of time.

Proposition. **$\mathbf{P}_1$:** We have $n + \text{succ}(0) = \text{succ}(n)$ for all $n \in \mathbb{N}$

Proof. Let $n \in \mathbb{N}$ be any arbitrary natural number, then:

$$\begin{aligned} n + \text{succ}(0) &\overset{(ii)}{=} \text{succ}(n + 0) \\ &\overset{(i)}{=} \text{succ}(n) \end{aligned}$$

Thus the proposition $\mathbf{P}_1$ has been successfully established.

We usually denote succ(0) as the element $1 \in \mathbb{N}$.

□

Proposition. **$\mathbf{P}_2$:** For all $n \in \mathbb{N}$ we have $n \cdot 0 = 0 = 0 \cdot n$.

Proof. We are going to make use of the principle of mathematical induction. Let $\mathcal{P}(n)$: $n \cdot 0 = 0 = 0 \cdot n$ for all $n \in \mathbb{N}$. Consider the base step $\mathcal{P}(0)$:

$$0 \cdot 0 \overset{(iii)}{=} 0 \overset{(iii)}{=} 0 \cdot 0$$

which is true. Let us now assume that for some $k \in \mathbb{N}$ $\mathcal{P}(k)$ is true. Let us now confirm that this induction hypothesis ensures $\mathcal{P}(\text{succ}(k))$ being true.

$$\Rightarrow 0 \cdot \text{succ}(k) \overset{(iv)}{=} 0 \cdot k + 0 \overset{\mathcal{P}(k)}{=} k \cdot 0 + 0 \overset{(iii)}{=} 0 + 0 \overset{(i)}{=} 0 \overset{(iii)}{=} \text{succ}(k) \cdot 0$$

□

Proposition. **$\mathbf{P}_3$:** We have $n \cdot 1 = n \cdot \text{succ}(0) = n = \text{succ}(0) \cdot n = 1 \cdot n$ for all $n \in \mathbb{N}$.

Proof. We proceed by induction. Let $\mathcal{P}(n)$: $\quad n \cdot \text{succ}(0) = n = \text{succ}(0) \cdot n$ for all $n \in \mathbb{N}$. The base step $\mathcal{P}(0)$:

$$0 \cdot \text{succ}(0) \overset{\mathbf{P}_2}{=} \text{succ}(0) \cdot 0 \overset{(iii)}{=} 0$$

is clearly true, following from our multiplication's definition and the fact that 0 commutes. Now let us assume that $\mathcal{P}(k)$ is true for some $k \in \mathbb{N}$. Then it follows for $\mathcal{P}(\text{succ}(k))$:

$$\text{succ}(k) \cdot \text{succ}(0) \overset{(iv)}{=} \text{succ}(k) \cdot 0 + \text{succ}(k) \overset{(iii)}{=} \text{succ}(k)$$

and

$$\text{succ}(0) \cdot \text{succ}(k) = \text{succ}(0) \cdot k + \text{succ}(0) \overset{\mathcal{P}(k)}{=} k + \text{succ}(0) = \text{succ}(k)$$

□

2 Basic Definitions and Examples

Now that we have established the first few rules about $\mathbb{N}$ using the principle of mathematical induction, we can finally start with introducing the most basic algebraic pair, the *magma.*

2.1 *Definition.* **Magma:**

Let M be a non-empty set. An **algebraic structure** $(M,\circ)$, $\circ : M\times M \to M$ is called a **magma** or **groupoid** if it is closed under the operation $\circ$, i.e.

$$\text{for all } a, b \in M\text{: } a \circ b \in M \ .$$

Such operations are called **binary** with the property that they map all ordered pairs $(a, b) \in M \times M$ to an element $\circ(a, b) \in M$. In a more mathematical notation, we have $(a, b) \mapsto \circ(a, b)$. The mapping $\circ$ is usually called a product of $(M,\circ)$ and can also be denoted as $a \circ b$ or simply ab instead of $\circ(a, b)$.

Same goes for our magma. We are sometimes going to denote an algebraic pair as just M instead of $(M, \circ)$ if it is clear from the context what we actually mean. Note, that whenever I refer to something in this paper as just a **pair** or an algebraic structure, we are going to assume this pair to be **at least** a magma and that the operation acting on the set is binary.

Example. (1) The pair $(\mathbb{N}, +)$, $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ forms a magma under addition.

Proof. We proceed by induction. Let $n \in \mathbb{N}$ be a fixed but arbitrary natural number and let

$$\mathcal{P}(m)\text{: } \ n + m \in \mathbb{N} \text{ for all } m \in \mathbb{N} \ .$$

As the base step we would like to consider $\mathcal{P}(0)$. This is indeed true, since $n + 0 \in \mathbb{N}$ by the addition's definition. Now we want to suppose that for some $k \in \mathbb{N}$ $\mathcal{P}(k)$ is true. Thus it follows that $\mathcal{P}(\text{succ}(k))$: $n + \text{succ}(k) \in \mathbb{N}$ is true, since $n + \text{succ}(k) = \text{succ}(n + k)$ by the second part of our addition's definition. It immediately follows by **P2** that $\text{succ}(n + k) \in \mathbb{N}$, whenever $n + k \in \mathbb{N}$. By the principle of mathematical induction we can conclude that the proposition $\mathcal{P}(m)$ is true for all $m \in \mathbb{N}$ and thus $\mathbb{N}$ is closed under addition. By definition $(\mathbb{N}, +)$ is a magma.

□

2.2 *Definition.* **Submagma:**

For every algebraic structure we can define a substructure. Let $(M, \circ)$ be a Magma and $M_S \subseteq M$ a non-empty subset of M. A pair $(M_S, \circ)$, $\circ : M_S \times M_S \to M_S$ is called a **submagma** or **subgroupoid** of M if it is closed under the operation $\circ$, which we then denote as $M_S \leq M$.

Example. (2) An example of such a submagma is the fact, that every magma is a submagma of itself. Let $(M, \circ)$ be a magma, meaning that M is closed under the operation $\circ : M\times M \to M$. Since every set is a subset of itself, meaning $M \subseteq M$, it follows that $(M, \circ) \subseteq (M, \circ)$ is indeed a submagma of itself.

□

After laying the foundations of abstract algebra, we can move on to introducing the semigroup theory's main actor, namely *the semigroup* itself.

2.3 *Definition.* **Semigroups:**

Let us now consider a magma $(S, \circ)$ where our operation $\circ : S \times S \to S$ is **associative**, meaning that the order of carrying out the binary operation is not relevant. In mathematical notation we can define associativity as:

$$\forall a, b, c \in S\colon\ a \circ (b \circ c) = (a \circ b) \circ c\ .$$

If this property indeed holds for said $(S, \circ)$, then we usually call this pair a **semigroup**. Also, just because the order of carrying out the operation is irrelevant does not imply that we can change the order of our elements on which the operation is carried out. If our S only consists of finitely many elements we call it a **finite semigroup**.

It may now be apparent that we can start off with a simple algebraic structure and add more and more properties to it until we get a new one which underlies new rules and has more advanced characteristics.

2.4 *Definition.* **Commutative algebraic structures**:

Let $(S, \circ)$ be an algebraic structure. We call S **commutative** or **abelian** if for all $x, y \in S$ we have

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

Example. (3) $(\mathbb{N}, +)$ is an abelian semigroup. Let $(\mathbb{N}, +)$ be the pair of positive integers and the corresponding addition. We have already proven $(\mathbb{N}, +)$ to be a magma. To show that $(\mathbb{N}, +)$ also forms a semigroup we just need to show, that for all $m, n, p \in \mathbb{N}$ we have $m + (n + p) = (m + n) + p$.

Proof. Let $m, n \in \mathbb{N}$ be fixed but arbitrary natural numbers and let

$$\mathcal{P}(p)\colon \quad m + (n + p) = (m + n) + p \text{ for all } p \in \mathbb{N}$$

Consider $\mathcal{P}(0)$ as the base step. By (i) we can confirm that

$$m + (n + 0) \overset{(i)}{=} m + n \overset{(i)}{=} (m + n) + 0$$

indeed holds. Now we want to suppose, that for some $k \in \mathbb{N}$ $\mathcal{P}(k)$ is true. We need to show that $\mathcal{P}(k)$ ensures $\mathcal{P}(\text{succ}(k))$ is true. It follows by our addition's property (ii), that for $\mathcal{P}(\text{succ}(k))$ we have:

$$m + (n + \text{succ}(k)) \overset{(ii)}{=} m + \text{succ}(n + k) \overset{(ii)}{=} \text{succ}(m + (n + k))$$

and

$$(m + n) + \text{succ}(k) \overset{(ii)}{=} \text{succ}((m + n) + k)\ .$$

This immediately implies, that whenever $\mathcal{P}(k)$ is true

$$m + (n + \text{succ}(k)) = \text{succ}(m + (n + k)) \overset{\mathcal{P}(k)}{=} \text{succ}((m + n) + k) = (m + n) + \text{succ}(k)$$

and thus $\mathcal{P}(\text{succ}(k))$ is true. By the principle of mathematical induction $\mathcal{P}(p)$ is true for all $p \in \mathbb{N}$ and we can conclude that the operation is associative and that $(\mathbb{N}, +)$ is indeed a semigroup. We denote the associative law as **A**.

Next we need to confirm that $0 \in \mathbb{N}$ commutes with every element of the natural numbers. As always, we proceed by using the principle of mathematical induction. Let for all $n \in \mathbb{N}$

$$\mathcal{P}(n)\text{: } n + 0 = n = 0 + n$$

be our proposition. Obviously, we can confirm that our base step

$$\mathcal{P}(0) : 0 + 0 \overset{(i)}{=} 0 \overset{(i)}{=} 0 + 0$$

is indeed a true statement. Next we would like to suppose, that for some arbitrary natural number $k \in \mathbb{N}$ P(k) is true.

$$\Rightarrow 0 + \text{succ}(k) \overset{(ii)}{=} \text{succ}(0 + k) \overset{\mathcal{P}(k)}{=} \text{succ}(k + 0) \overset{(i)}{=} \text{succ}(k) \overset{(i)}{=} \text{succ}(k) + 0$$

By induction we have shown that $0 \in \mathbb{N}$ commutes with all $n \in \mathbb{N}$. This step was necessary for generalizing the commutation argument to all $n, m \in \mathbb{N}$.

Let us now fix some $n \in \mathbb{N}$ and define for all $m \in \mathbb{N}$

$$\mathcal{P}(m)\text{:} \qquad n + m = m + n \ .$$

The base step $\mathcal{P}(0)$ follows directly from the previous observation. Now we want to suppose that $\mathcal{P}(k)$ is true and we want to see if this induction hypothesis ensures $\mathcal{P}(\text{succ}(k))$ being true.

$$\Rightarrow \text{succ}(k) + n \overset{\mathbf{P}_1}{=} (k + \text{succ}(0)) + n \overset{\mathbf{A}}{=} k + (\text{succ}(0) + n) \overset{\mathcal{P}(k)}{=} k + (n + \text{succ}(0)) \overset{\mathbf{P}_1}{=} k + \text{succ}(n) \overset{(ii)}{=}$$
$$\text{succ}(k + n) \overset{\mathcal{P}(k)}{=} \text{succ}(n + k) \overset{(ii)}{=} n + \text{succ}(k)$$

Hence we have confirmed the commutative law **C** and the proof is complete. □

Example. (4) An example of a pair **not** being a semigroup is $(\mathbb{N}_o, +)$, where $\mathbb{N}_o = \{1, 3, 5, ...\} \subset \mathbb{N}$ is the set of all odd positive integers and $+$ the natural number's addition. Note that an odd number $n \in \mathbb{N}_o$ has the property, that it can be written as $n = k \cdot 2 + 1$, where $k \in \mathbb{N}$ and $2 = \text{succ}(1)$.

Proof. Before we can begin with the main proof, let us establish the closure of $\mathbb{N}$ under multiplication and the so called distributive law **D**.

Let $n \in \mathbb{N}$ be a fixed but arbitrary natural number and let

$$\mathcal{P}(m)\text{:} \qquad n \cdot m \in \mathbb{N} \text{ for all } m \in \mathbb{N}$$

The base step $\mathcal{P}(0)$ being true follows immediately from (iii). Now we want to suppose that for some $k \in \mathbb{N}$ $\mathcal{P}(k)$ is true. Let us confirm, that our induction hypothesis ensures, that $\mathcal{P}(\text{succ}(k))$ is true.

$$\Rightarrow n \cdot \text{succ}(k) \overset{(iv)}{=} n \cdot k + n$$

By $\mathcal{P}(k)$ we can confirm, that $n \cdot k \in \mathbb{N}$ and we also know that the natural numbers are closed under addition, implying that $n \cdot k + n \in \mathbb{N}$. Hence the closure under multiplication has been established. □

Next we would like to show, that $(n+m)\cdot p = n\cdot p + m\cdot p$ for all $n,m,p \in \mathbb{N}$. Let $n,m \in \mathbb{N}$ be fixed but arbitrary and let

$$\mathcal{P}(p): \qquad (n+m)\cdot p = n\cdot p + m\cdot p \text{ for all } p \in \mathbb{N}\ .$$

Our base step $\mathcal{P}(0)$ is clearly true, since $(n+m)\cdot 0 \overset{(iii)}{=} 0 \overset{(i)}{=} 0+0 \overset{(iii)}{=} n\cdot 0 + m\cdot 0$. We now want to consider $\mathcal{P}(k)$ to be true. Then it follows that $\mathcal{P}(\text{succ}(k))$:

$$(n+m)\cdot \text{succ}(k) \overset{(iv)}{=} (n+m)\cdot k + (n+m) \overset{\mathcal{P}(k)}{=} n\cdot k + m\cdot k + (n+m) \overset{\mathbf{A}}{=} n\cdot k + (m\cdot k + n) + m \overset{\mathbf{C}}{=} n\cdot k + (n + m\cdot k) + m \overset{\mathbf{A}}{=} (n\cdot k + n) + (m\cdot k + m) \overset{(iv)}{=} n\cdot \text{succ}(k) + m\cdot \text{succ}(k)$$

is true by the induction hypothesis and other already established laws. Thus the distributive law **D** has been proven to be true.

□

Let $n,m \in \mathbb{N}_o$, and thus $n = k\cdot 2+1$ and $m = l\cdot 2+1$, where $k,l \in \mathbb{N}$:

$$\begin{aligned} n+m &= k\cdot 2+1+l\cdot 2+1 \\ &\overset{\mathbf{C}}{=} k\cdot 2+l\cdot 2+1+1 \\ &\overset{\mathbf{A}}{=} k\cdot 2+l\cdot 2+(1+1) \\ &\overset{\mathbf{P}_3}{=} k\cdot 2+l\cdot 2+(1\cdot 1+1) \\ &\overset{(iv)}{=} k\cdot 2+l\cdot 2+1\cdot \text{succ}(1) \\ &= k\cdot 2+l\cdot 2+1\cdot 2 \\ &\overset{\mathbf{D}}{=} (k+l+1)\cdot 2 \end{aligned}$$

By our closure laws we know, that $(k+l+1) \in \mathbb{N}$ and hence $(k+l+1)\cdot 2 \in \mathbb{N}$. But this result is not element of $\mathbb{N}_o$ since it takes the form of $n+m = a\cdot 2$, $a \in \mathbb{N}$, i.e. an even positive integer. Thus $(\mathbb{N}_o, +)$ is not closed under the operation and fails to even be a magma. Thus it is no semigroup.

Note, that we have just shown that our claim holds for all arbitrary odd positive integers. Generalization is always good, but sometimes there are ways to simplify such proofs further. We would have also shown that the pair does not form a magma, if we would have come up with a good counterexample. Let us now consider the element $1 \in \mathbb{N}_o$. Then:

$$1+1 = 1+\text{succ}(0) \overset{\mathbf{P}_1}{=} \text{succ}(1) = 2 \overset{\mathbf{P}_3}{=} 1\cdot 2$$

Which takes the form of an even positive integer by our previous observation. That also means that the closure already fails for two distinct examples and so it does for the general case in conclusion.

□

Example. (5) Let $\mathcal{T}_X$ be the set of all functions $\alpha : X \to X$. Then $(\mathcal{T}_X, \circ)$ is a semigroup, where $\circ$ represents function composition $(\beta\circ\alpha)(x) = \beta(\alpha(x))$ for all $x \in X$ and $\alpha,\beta \in \mathcal{T}_X$.

Proof. Let us first verify the closure under the function composition. Let α and β be two functions of $\mathcal{T}_X$, then:

$$(\beta \circ \alpha)(x) = \beta(\alpha(x)) \in \mathcal{T}_X \ ,$$

since $\beta : X \to X$ and $\alpha : X \to X$ implies, that $\beta \circ \alpha : X \to X$. Now for the associativity. Let $\alpha, \beta, \gamma \in \mathcal{T}_X$, then:

$$[\alpha \circ (\beta \circ \gamma)](x) = \alpha((\beta \circ \gamma)(x)) = \alpha(\beta(\gamma(x)) = (\alpha \circ \beta)(\gamma(x)) = [(\alpha \circ \beta) \circ \gamma](x)$$

We have successfully introduced the **semigroup of transfomations**.

□

Those were already a lot of examples, but in order for us to understand the theory of semigroups, we have to understand semigroups in itself first and how to prove simple statements regarding them. The next few sites will consist of the longest proof of the paper.

Example. (6) Let ($\mathbb{N}$,$\star$) be defined by $\star : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, where the binary operation is defined as

$$n \star m = \max\{n, m\} = \begin{cases} n & , n \geq m \\ m & , \text{otherwise} \end{cases}$$

Our goal is it to show, that this pair forms indeed a semigroup. Before we can actually show it, we have to prove, that one element can be less or equal to another element. So let us show, that the natural numbers are a **totally ordered** set. Let us at first recall a few little facts about binary relations.

Definition. **Relation:** A binary relation $\mathcal{R} \subseteq S \times S$ on a set S is called:

- Reflexive, if $a\mathcal{R}a$ holds for all $a \in S$
- Symmetric, if whenever $a\mathcal{R}b$ then $b\mathcal{R}a$ for all $a, b \in S$
- Transitive, if whenever $a\mathcal{R}b$ and $b\mathcal{R}c$ then $a\mathcal{R}c$ for all $a, b, c \in S$

Definition. **Strict order relation on** $\mathbb{N}$:

For each $n, m \in \mathbb{N}$ we define $< \subseteq \mathbb{N} \times \mathbb{N}$ by:

$$n < m \text{ iff there exists some } p \in \mathbb{N}\backslash\{0\}, \text{ such that } p + n = m$$

Analogously, we define $> \subseteq \mathbb{N} \times \mathbb{N}$ by:

$$n > m \Leftrightarrow m < n$$

Definition. **Order relation:**

Let S be a non-empty set. For each $a, b \in S$ we define $\leq \subseteq S \times S$ by

$$a \leq b \text{ if either } a < b \textbf{ or } a = b \ .$$

Also, for each $a, b \in S$ we define $\geq \subseteq S \times S$ by

$$a \geq b \Leftrightarrow b \leq a \ .$$

We can show that $\mathbb{N}$ is totally ordered if our order relation holds for all positive integers and if $a \leq b$ **or** $b \leq a$ for all $a, b \in \mathbb{N}$ (*connex property*). In the next steps we are going to establish a few facts about the **strict order relation** by which our order relation is basically defined and the so-called **trichotomy law**.

Proposition. **$\mathbf{P}_4$:** For all $n \in \mathbb{N}$ and $m \in \mathbb{N}\backslash\{0\}$ we have $m + n \neq n$.

Proof. Let $m \in \mathbb{N}\backslash\{0\}$ be fixed but arbitrary. Let us consider the proposition

$$\mathcal{P}(n): \qquad m + n \neq n \text{ for all } n \in \mathbb{N}$$

The base step $\mathcal{P}(0)$: $m + 0 \overset{(i)}{=} m \neq 0$ is true, since $m \in \mathbb{N}\backslash\{0\}$. Now let us assume that $\mathcal{P}(k)$ is true for some $k \in \mathbb{N}$ and see if this ensures $\mathcal{P}(\text{succ}(k))$ to be true. Suppose $\mathcal{P}(\text{succ}(k))$ is false, then by **P4** we know, that $m + \text{succ}(k) \overset{(iii)}{=} \text{succ}(m + k) = \text{succ}(k)$ implies $m + k = k$. This equation can only hold if $m = 0$ but this in itself is a contradiction, since $m \in \mathbb{N}\backslash\{0\}$ and so the implication could not hold. Hence, $m + k \neq k$ which was our induction hypothesis. Thus $\mathcal{P}(\text{succ}(k))$ is true and the proposition has been established.

□

Lemma. **$\mathbf{L}_1$:** $< \subseteq \mathbb{N} \times \mathbb{N}$ is transitive, but neither reflexive nor symmetric. If this holds, we call $<$ an **order**.

Proof. Let $m, n, p \in \mathbb{N}$ and without loss of generality let us set $m < n$ and $n < p$. By the definition of our order relation there exists some $k, r \in \mathbb{N}\backslash\{0\}$, such that $k + m = n$ and $r + n = p$.

Then we have $r + n = r + (k + m) \overset{\mathbf{A}}{=} (r + k) + m = p$. This deals with the transitivity, since there exists some $(r + k) = s \in \mathbb{N}$ such that $s + m = p$. And this is equivalent to saying, that $m < p$.

Now let us consider $n \in \mathbb{N}$. Now $n < n$ is false, since if it were true, there would exist some $k \in \mathbb{N}\backslash\{0\}$, such that $k + n = n$. But this is not possible due to our above proposition. We can now conclude that our order relation is not reflexive.

Lastly, let $n, m \in \mathbb{N}$ and let us assume that $n < m$ **and** $m < n$. But we have shown that our relation is transitive, which immediately implies, that $n < n$, which is false due to $< \subseteq \mathbb{N} \times \mathbb{N}$ not being reflexive. Thus, our relation is not symmetric and we have proven $\mathbb{N}$ to be an ordered set.

□

Just like announced, we are now going to prove the *trichotomy law*. It is quite a powerful statement which deals with the connex property and our order relation at the same time. It basically gives us the certainty that only one of the three relations between two positive integers can be true at the same time. Note that this proof has been inspired by Schaum's Outlines of Abstract Algebra [Second edition, page 43] and that the basic outline is identical.

Theorem. **The trichotomy law:**

For any $n, m \in \mathbb{N}$ one **and only** one of the following is true:

$$\bullet\ n = m \qquad \bullet\ n < m \qquad \bullet\ n > m$$

Proof. Let $n \in \mathbb{N}$ be any arbitrary positive integer and let $\mathcal{N}_1 = \{m\} \subset \mathbb{N}$, $\mathcal{N}_2 = \{p \mid p \in \mathbb{N},\ p < m\} \subset \mathbb{N}$ and $\mathcal{N}_3 = \{p \mid p \in \mathbb{N}, p > m\} \subset \mathbb{N}$. In the following process, we are going to prove that $\{\mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3\}$ is a partition relative to $\{=, <, >\}$.

Let us introduce some $m \in \mathbb{N}$. At first, let us suppose that $m = 0$, hence $\mathcal{N}_1 = \{0\}$, $\mathcal{N}_2 = \{\}$ (since no element of the natural numbers can be less than 0 by **P3**) and $\mathcal{N}_3 = \{p \mid p \in \mathbb{N}, p > 0\}$. Obviously we now have $\mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3 = \mathbb{N}$. Next we want to set $m \neq 0$. Since $0 \in \mathcal{N}_2$, it follows that $0 \in \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$. Now we want to choose any $n \neq 0 \in \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$.

Case I: $n \in \mathcal{N}_1 \Rightarrow n = m$ and so is $\text{succ}(n) \in \mathcal{N}_3$

Case II : $n \in \mathcal{N}_2$, such that $n + k = m$ for some $k \in \mathbb{N}$. If $k = 0$, then it follows that $n = m \in \mathcal{N}_1$. On the other hand, if $k \neq 0$ such that $k = \text{succ}(0) + q$ for some $q \in \mathbb{N}$, then:

$$n + \text{succ}(0) + q \overset{\mathbf{P}_1}{=} \text{succ}(n) + q = m, \text{ and so } \text{succ}(n) \in \mathcal{N}_3.$$

Case III : $n \in \mathcal{N}_3 \Rightarrow \text{succ}(n) > n > m \Rightarrow \text{succ}(n) \in \mathcal{N}_3$

Thus, for all $n \in \mathbb{N}$ we have $n \in \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$ implying that $\text{succ}(n) \in \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$. Since $0 \in \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$ we can conclude, that $\mathbb{N} = \mathcal{N}_1 \cup \mathcal{N}_2 \cup \mathcal{N}_3$.

Now $n \in \mathcal{N}_2$, since $m \not< m$, hence $\mathcal{N}_1 \cap \mathcal{N}_2 = \{\}$. Analogous, $m \not> m$ and so $\mathcal{N}_1 \cap \mathcal{N}_3 = \{\}$. Lastly, let us suppose that there is some $k \in \mathbb{N}$ satisfying $p \in \mathcal{N}_2 \cap \mathcal{N}_3$. It then follows, that $p < m$ **and** $p > m$, which is equivalent to saying, that $p < m$ **and** $m < p$. But this in itself is a contradiction because the transitivity of $<$ now ensures $p < p$ which is clearly false. Thus, $\mathcal{N}_2 \cap \mathcal{N}_3 = \{\}$.

This very important law deals with the connex property which is key to having a totally ordered set.

□

Now that we have shown that $\mathbb{N}$ is totally ordered, we can finally start to show, that $(\mathbb{N}, \star)$ is a semigroup. First we need to show, that the pair is closed under its binary operation, meaning that for all $n, m \in \mathbb{N} : n \star m \in \mathbb{N}$.

Proof. We have to consider two main cases.

Case 1: $n \geq m \Rightarrow n \star m = \max\{n, m\} = n \in \mathbb{N}$

Case 2: $m \geq n \Rightarrow n \star m = \max\{n, m\} = m \in \mathbb{N}$

Thus, the closure has been shown. The next part is going to consist of a lot of casework. We now have to show, that for all $n, m, k \in \mathbb{N}$ we have $n \star (m \star k) = (n \star m) \star k$.

Case 1: $n \geq m \geq k$, then:

$n \star (m \star k) = \max\{n, \max\{m, k\}\} = \max\{n, m\} = n = \max\{n, k\} = \max\{\max\{n, m\}, k\} = (n \star m) \star k$

Case 2: $n \geq k \geq m$, and so:

$$n \star (m \star k) = \max\{n, \max\{m, k\}\} = \max\{n, k\} = \max\{\max\{n, m\}, k\} = (n \star m) \star k$$

Case 3: If $m \geq n \geq k$ we have:

$n \star (m \star k) = \max\{n, \max\{m, k\}\} = \max\{n, m\} = m = \max\{m, k\} = \max\{\max\{n, m\}, k\} = (n \star m) \star k$

Case 4: For $m \geq k \geq n$ we get:

$n \star (m \star k) = \max\{n, \max\{m, k\}\} = \max\{n, m\} = m = \max\{m, k\} = \max\{\max\{n, m\}, k\} = (n \star m) \star k$

Case 5: $k \geq n \geq m$:

$$n \star (m \star k) = \max\{n, \max\{m, k\}\} = \max\{n, k\} = \max\{\max\{n, m\}, k\} = (n \star m) \star k$$

Case 6: And finally, when $k \geq m \geq n$:

$n \star (m \star k) = \max\{n, \max\{m, k\}\} = \max\{n, k\} = k = \max\{m, k\} = \max\{\max\{n, m\}, k\} = (n \star m) \star k$

Thus, we have shown that $(\mathbb{N}, \star)$ is associative and closed under its operation, making it a semigroup.

□

This was a lot of work! Now that we have understood how to prove a pair to be a semigroup, we can continue by adding new properties to algebraic structures.

2.5 *Definition.* **Monoids and groups:**

Let $(S, \circ)$ be a semigroup. We call an element $e \in S$ a **left identity**, if for all $x \in S$:

$$e \circ x = x$$

Analogously, we call $e \in S$ a **right identity**, if for all $x \in S$:

$$x \circ e = x$$

If both properties hold for one element $e \in S$, we usually call it an **identity** of S. If said semigroup $(S, \circ)$ has such an identity, we call it a **monoid**.

Lemma. **L_2:** A semigroup S can have at most one identity. Such an identity is in fact unique, meaning if S has a left identity $e \in S$ and a right identity $\tilde{e} \in S$, then $e = \tilde{e}$.

Proof. Since e is a left identity and $\tilde{e}$ a right one: $e = e \circ \tilde{e} = \tilde{e}$

□

We usually denote the identity of a monoid S as 1_S or just 1. But depending on the monoid, we are going to make use of the identity's established notation.

Example. (7) Let us consider the pair $(\mathbb{N}, +)$. The natural number's identity with respect to the binary operation $+$ is $0 \in \mathbb{N}$.

Proof. $0 + n \overset{\mathbf{C}}{=} n + 0 \overset{\mathbf{(i)}}{=} n$, for all $n \in \mathbb{N}$

Hence, the pair $(\mathbb{N}, +)$ forms a monoid.

□

Example. (8) Let us consider the pair $(\mathbb{N}, \cdot)$. The natural number's identity with respect to the binary operation $\cdot$ is $1 \in \mathbb{N}$. The proof of this fact follows immediately from $\mathbf{P}_3$.

If a given semigroup S does not have an identity element we can make a monoid S^1 out of it, by adjoining an identity to S:

$$S^1 = \begin{cases} S & \text{, if S is a monoid} \\ S \cup \{1\} & \text{, if S is not a monoid} \end{cases}$$

A monoid $(G, \circ)$ is called a **group**, if for every element $x \in G$ there exists a $x^{-1} \in G$, such that

$$x \circ x^{-1} = 1 = x^{-1} \circ x$$

2.6 *Definition.* **Zeros and idempotents**

An element $x \in S$ is called a **left zero**, if for all $y \in S$ we have

$$x \circ y = x.$$

Analogously, an element $x \in S$ having the property, that for all $y \in S$ we have

$$y \circ x = x$$

is called a **right zero** of S. If an element $x \in S$ has both properties, then it is called a **zero**.

Lemma. $\mathbf{L}_3$**:** A semigroup $(S, \circ)$ can have at most one zero, meaning that it is unique.

Proof. Let $0, \widetilde{0} \in S$ be two zeros of S. Then

$$0 = 0 \circ \widetilde{0} = \widetilde{0}$$

since 0 and $\widetilde{0}$ are both left **and** right zeros.

□

An element $e \in S$ is called an **idempotent**, if $e \circ e = e^2 = e$ holds, where e^2 is the product of e with itself two times. We refer to the **set of all idempotents** of S by $E_s = \{e \in S \mid e^2 = e\}$.

Example. (9) The pair $(\mathbb{N}, \cdot)$ has $0 \in \mathbb{N}$ and $1 \in \mathbb{N}$ as idempotents.

Proof. $0 \cdot 0 \overset{(iii)}{=} 0$ and $1 \cdot 1 = 1 \cdot \text{succ}(0) \overset{(iv)}{=} 1 \cdot 0 + 1 \overset{(iii)}{=} 0 + 1 \overset{\mathbf{C}}{=} 1 + 0 \overset{(i)}{=} 1$

□

Example. (10) Let S be a set, and let $\bullet : S \times S \to S$ be defined as

$$a \bullet b = a \qquad \text{for all } a, b \in S \ .$$

$(S, \bullet)$ forms a semigroup, where each $a \in S$ is a left zero **and** a right identity at the same time. Also, all elements are idempotents, meaning that $S = E_S$.

Proof. At first let us confirm that $(S, \bullet)$ is indeed a semigroup. Let $a, b, c \in S$, then:

$$a \bullet (b \bullet c) = a \bullet b = (a \bullet b) \bullet c$$

Moreover, $a \bullet b = a \in S$ by definition. The left zero and right identity property is trivial. Let $e \in S$, then:

$$e \bullet e = e \text{ for all } e \in S \ .$$

Thus, every element is an idempotent, implying that $S = E_S$

□

Lemma. $\mathbf{L_4}$**:** If $(G, \circ)$ is a group, then $E_G = \{e\}$, where $e \in G$ is the groups identity.

Proof. Let $g \in G$ be any idempotent of G. Since G is a group there exists a $g^{-1} \in G$ for all $g \in G$, such that $g \circ g^{-1} = g^{-1} \circ g = e$.

$$\begin{aligned} &\Rightarrow g \circ g = g \\ &\Leftrightarrow g \circ g \circ g^{-1} = g \circ g^{-1} \\ &\Leftrightarrow g \circ e = g = e \end{aligned}$$

Since $g \in G$ was by definition any idempotent, we now have confirmed that $g = e$, meaning that $E_S = \{e\}$.

□

Example. (11) Let $(S, \cdot)$ be a semigroup. For any two subsets $A, B \subseteq S$ we define their product by

$$A \cdot B = \{a \cdot b \mid a \in A,\ b \in B\}$$

This newly obtained operation is associative, since we use the semigroups operation (which ensures associativity) on our new set's elements. Hence, the subsets of S form the so-called **global semigroup** of S. We denote it by 2^S. For some subset $A \subseteq S$, we let $A^2 = A \cdot A$ as usual.

2.7 *Definition.* **Cancellation semigroups**

A semigroup S is called **left cancellative**, if for all $x, y, z \in S$ we have:

$$z \circ x = z \circ y \Rightarrow x = y$$

By the same arguments, we call S **right cancellative**, if

$$x \circ z = y \circ z \Rightarrow x = y$$

If a semigroup $(S, \circ)$ satisfies both properties, we call it **cancellative**.

Example. (12) $(\mathbb{N}, +)$ is a cancellative monoid.

Proof. We have already proven $(\mathbb{N}, +)$ to be a monoid. Let $n, m \in \mathbb{N}$ be fixed but arbitrary positive integers. Let us consider the proposition

$$\mathcal{P}(p): \qquad n + p = m + p \Rightarrow n = m \text{ , for all } p \in \mathbb{N}.$$

The base step $\mathcal{P}(0)$ is true, since

$$n \overset{(i)}{=} n + 0 = m + 0 \overset{(i)}{=} m \Leftrightarrow n = m.$$

Let us assume $\mathcal{P}(k)$ to be true for all $k \in \mathbb{N}$. Then it follows for $\mathcal{P}(\text{succ}(k))$:

$$n + \text{succ}(k) \overset{(ii)}{=} \text{succ}(n + k) \overset{\mathcal{P}(k)}{=} \text{succ}(m + k) \overset{(ii)}{=} m + \text{succ}(k)$$

By **P4** and $\mathcal{P}(k)$ we can conclude that:

$$\text{succ}(n + k) = \text{succ}(m + k) \Rightarrow n + k = m + k \overset{\mathcal{P}(k)}{\Longrightarrow} n = m$$

By the principle of mathematical induction we have confirmed $(\mathbb{N}, +)$ to be right cancellative. Now all that is left to do, is to show that the pair is also left cancellative. This fact follows immediately from $(\mathbb{N}, +)$ being abelian. So for all $n, m, p \in \mathbb{N}$ we have:

$$p + n = p + m \overset{\mathbf{C}}{\Longleftrightarrow} n + p = m + p \Rightarrow n = m$$

□

3 Subsemigroups and Direct Products

3.1 *Definition.* **Subsemigroups**:

Let $(S, \circ)$ be a semigroup and $S_S \neq \{\}$ a non-empty subset of S. We say that $(S_S, \circ)$ is a **subsemigroup** of S, being denoted by $S_S \leq S$, if S_S is closed under the operation of S:

$$\text{for all } x, y \in S_S: \qquad x \circ y \in S_S \text{ ,}$$

that is,

$$S_S \leq S \Leftrightarrow S_S^2 \subseteq S_S \text{ .}$$

This definition is analogous to the one on submagmas. A subsemigroup makes use of the mother semigroup's operation. This also means, that the associative property is induced on S_S which also implies, that S_S forms a semigroup in its own right.

Example. (13) Consider $(\mathbb{N}_e, +)$, where $\mathbb{N}_e$ denotes the set of even positive integers $\mathbb{N}_e = \{n = k \cdot 2,\, k \in \mathbb{N}\} \subset \mathbb{N}$. This pair forms a subsemigroup of $(\mathbb{N}, +)$. On the other hand, $(\mathbb{N}_e, \cdot)$ does not, because the multiplication is not the operation of $(\mathbb{N}, +)$.

Proof. All we need to prove is $(\mathbb{N}_e, +)$ being a semigroup. Since all elements of this pair can be constructed in terms of positive integers, the associativity gets induced by the mother semigroup. Now let $n, m \in \mathbb{N}_e$,where $n = k \cdot 2$ and $m = p \cdot 2$. Then:

$$\begin{aligned} n + m &= k \cdot 2 + p \cdot 2 \\ &\overset{\mathbf{D}}{=} (k + p) \cdot 2 \end{aligned}$$

Since $(k + p) = s \in \mathbb{N}$ we also know that $(k + p) \cdot 2$ is of the form $s \cdot 2 \in \mathbb{N}_e$. Hence, the pair is closed under addition and we can conclude that $(\mathbb{N}_e, +) \leq (\mathbb{N}, +)$

□

Lemma. **$\mathbf{L_5}$:** Let $A_i \leq S$ be subsemigroups of S for all $i \in I$. If their intersection is non-empty, then

$$\bigcap_{i \in I} A_i \leq S.$$

Proof. Suppose that the intersection is non-empty. If $x, y \in A = \bigcap_{i \in I} A_i$, then for each $i \in I$ we have $x, y \in A$. Then $x \circ y \in A$, just as required.

□

For some non-empty subset $X \subseteq S$ we denote

$$[X]_S = \bigcap \{A \mid X \subseteq A,\, A \leq S\} \ .$$

Then, by $\mathbf{L_5}$ $[X]_S$ is a subsemigroup of S, which we usually call the **subsemigroup generated by X**. It is the smallest subsemigroup of S which contains X. Sometimes $[X]_S$ will be denoted simply as $[X]$, if S is clear from the context.

When $X = \{x\}$, called a **singleton**, then we write $[x]_S$ instead of $[\{x\}]_S$. In general, we rather write $[x_1, x_2, ...]_S$ instead of $[\{x_1, x_2, ...\}]_S$ no matter if $X = \{x_1, x_2, ...\}$ is finite or not.

Theorem. Let $X \neq \{\}$, $X \subseteq S$ for a semigroup $(S, \circ)$, then

$$[X]_S = \bigcup_{n=1}^{\infty} X^n = \{x_1 \circ x_2 \circ ... \circ x_n \mid n \geq 1,\, x_i \in X\} \ .$$

Proof. Let $A = \bigcup_{n=1}^{\infty} X^n$ and $a, b \in A$. Then a and b are finite products of elements of X. This also means, that $a \circ b$ is a finite product of elements of X and are thus in A. The associative property gets induced by S on A, making $A \leq S$. Also, $X^n \subseteq [X]_S$ for all $n \geq 1$, since $[X]_S \leq S$, and hence the claim follows. We denote this new result as $\mathbf{T_1}$ because we are going to need it at a later time.

□

Let M be a monoid. We say that a $X \subseteq M$ **generates** M as a monoid, if $[X]_M = M$ or $[X]_M = M \backslash \{1_M\}$. Hence in a monoid the identity element is always taken into consideration, meaning a generator set does not need to produce it.

3.2 *Definition.* **Direct products:**

Let $(S, \circ)$ and $(T, \bullet)$ be two algebraic structures. The **direct product** $S \times T$ is defined as follows:

$$\text{for all } x_i \in S \text{ and } y_i \in T \text{ we have:} \qquad (x_1, y_1) \cdot (x_2, y_2) = (x_1 \circ x_2, y_1 \bullet y_2) \ .$$

We define $S_1 \times S_2 \times ... \times S_n$ as the finite direct product of the semigroups S_i and one can observe that the direct product on semigroups in itself forms a semigroup.

Proof. Let $(S, \circ)$ and $(T, \bullet)$ be semigroups with $s_1, s_2 \in S$ and $t_1, t_2 \in T$. For the closure we obtain:

$$S \times T = (s_1, t_1) \cdot (s_2, t_2) = (s_1 \circ s_2, t_1 \bullet t_2) \in \{(s, t) \mid s \in S,\, t \in T\} \ .$$

Since S and T are semigroups, we know that the product of their elements are elements of the semigroups respectively. Thus we have verified the closure. Showing the associativity is quite some work. Let us define at first, what it means for us to take the direct product of three semigroups. Let S and T be like above and $(P, \star)$ be a third semigroup, then

$$(S \times T) \times P = \{((s, t), p) \mid s \in S,\, t \in T \text{ and } p \in P\} \ .$$

With this out of the way we can get started. Let $s_1, s_2, s_3 \in S$, $t_1, t_2, t_3 \in T$ and $p_1, p_2, p_3 \in P$, then:

$$\begin{aligned}
(S \times T) \times P &= [((s_1, t_1), p_1) \cdot ((s_2, t_2), p_2)] \cdot ((s_3, t_3), p_3) \\
&= (((s_1, t_1) \cdot (s_2, t_2)), p_1 \star p_2) \cdot ((s_3, t_3), p_3) \\
&= ((s_1 \circ s_2, t_1 \bullet t_2), p_1 \star p_2) \cdot ((s_3, t_3), p_3) \\
&= (((s_1 \circ s_2, t_1 \bullet t_2) \cdot (s_3, t_3)), (p_1 \star p_2) \star p_3) \\
&= (((s_1 \circ s_2) \circ s_3, (t_1 \bullet t_2) \bullet t_3), (p_1 \star p_2) \star p_3) \\
&\overset{(*)}{=} ((s_1 \circ (s_2 \circ s_3), t_1 \bullet (t_2 \bullet t_3)), p_1 \star (p_2 \star p_3)) \\
&= (((s_1, t_1) \cdot (s_2 \circ s_3, t_2 \bullet t_3)), p_1 \star (p_2 \star p_3)) \\
&= ((s_1, t_1), p_1) \cdot ((s_2 \circ s_3, t_2 \bullet t_3), p_2 \star p_3) \\
&= ((s_1, t_1), p_1) \cdot (((s_2, t_2) \cdot (s_3, t_3)), p_2 \star p_3) \\
&= ((s_1, t_1), p_1) \cdot [((s_2, t_2), p_2) \cdot ((s_3, t_3), p_3)] = S \times (T \times P) \ ,
\end{aligned}$$

where $(*)$ follows from the fact, that S, T and P are semigroups and their operations associative. Thus we have shown, that the direct product of semigroups indeed forms a semigroup itself.

□

Example. (14) Let $(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$ be two pairs. Then the direct product of $(\mathbb{N}, +) \times (\mathbb{N}, \cdot)$ for all $n_i, m_i \in \mathbb{N}$ is:

$$(n_1, m_1) \cdot (n_2, m_2) = (n_1 + n_2, m_1 \cdot m_2) \ .$$

The operations are valid, since $\mathbb{N}$ is closed under multiplication and addition.

The direct product is one way to easily combine two semigroup operations of S and T. This new semigroup $S \times T$ gets induced by the properties of both S and T.

We call the mappings $\pi_1 : S \times T \to S$ and $\pi_2 : S \times T \to T$ such that $\pi_1(x, y) = x$ and $\pi_2(x, y) = y$ **projections** of $S \times T$. In general we can also observe, that the direct product is not an abelian action, meaning $S \times T \neq T \times S$.

4 Homomorphisms and Transformations

This new chapter is going to deal with one of the tools which will allow us to state and prove the paper's main theorem in question. *Homomorphisms*, or just *morphisms*, are quite an important concept in linear and abstract algebra and many other fields of mathematics.

4.1 *Definition.* **Homomorphism:**

Let $(S, \circ)$ and $(T, \star)$ be two algebraic structures with corresponding **binary** operations. A mapping $\varphi : S \to T$ is called a **homomorphism**, if for all $x, y \in S$ we have

$$\varphi(x \circ y) = \varphi(x) \star \varphi(y) \ .$$

Hence, a homomorphism respects the product of one algebraic structure while transferring elements to some other structure. A homomorphism can also be used to **identify** elements, meaning $\varphi(x) = \varphi(y)$.

Example. (15) Let us define some $\varphi : S \to T$, with $S = (\mathbb{N}, +)$ and $T = (\mathbb{N}^{2x2}, +)$ where the latter pair represents all the two by two matrices with positive integer entries under the regular matrix addition.

Now consider

$$\varphi(n) = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \text{ for all } n \in \mathbb{N}.$$

This mapping is indeed a homomorphism, since we have for all $n, m \in S$:

$$\varphi(n+m) = \begin{pmatrix} n+m & 0 \\ 0 & n+m \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} + \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} = \varphi(n) + \varphi(m).$$

This φ indeed satisfies the homomorphism property.

□

Example. (16) Let $\varphi : S \to T$, where $S = (\mathbb{N}, \cdot)$ and $T = (\mathbb{N}, +)$. Now consider for all $n \in \mathbb{N}$ $\varphi(n) = n$. This is an example of a mapping **not** being a homomorphism. To prove this statement, we just need to find one counterexample. Let $n = 17$ for example, then

$$17 = \varphi(17) \overset{\mathbf{P_3}}{=} \varphi(17 \cdot 1) \neq \varphi(17) + \varphi(1) = 17 + 1 \overset{\mathbf{P_1}}{=} \text{succ}(17),$$

which can clearly not be the case, since by $\mathbf{P_4}$ and $\mathbf{C}$ we know that $m + n = n + m \neq n$ for all $m \in \mathbb{N}\backslash\{0\}$.

□

Lemma. $\mathbf{L_7}$: Let $(S, \circ)$ and $(T, \star)$ be given pairs and $\varphi : S \to T$ a homomorphism. If $X \subseteq S$, then $\varphi([X]_S) = [\varphi(X)]_T$.

Proof. If $x \in [X]_S$, then by $\mathbf{T_1}$ there exists some $x_i \in X$ such that $x = x_1 \circ ... \circ x_n$. Since φ is a homomorphism,

$$\varphi(x) = \varphi(x_1 \circ ... \circ x_n) = \varphi(x_1) \star ... \star \varphi(x_n)$$

and thus $\varphi([X]_S) \subseteq [\varphi(X)]_T$. Considering the other direction, if $y \in [\varphi(X)]_T$, then once again by $\mathbf{T_1}$ we have $y = \varphi(x_1) \star ... \star \varphi(x_n)$ for some $\varphi(x_i) \in \varphi(X)$, where $x_i \in X$. Just like before, since φ is a homomorphism, we have $y = \varphi(x_1 \circ ... \circ x_n)$ for $x_1 \circ ... \circ x_n \in [X]_S$.

□

Lemma. $\mathbf{L_8}$: Let $(S, \cdot)$, $(T, \bullet)$ and $(P, \star)$ be given pairs. If $\varphi_1 : S \to T$ and $\varphi_2 : T \to P$ are homomorphisms, then so is $\varphi_2 \circ \varphi_1 : S \to P$, where $\circ$ denotes function composition.

Proof. We have for all $x, y \in S$:

$$(\varphi_2 \circ \varphi_1)(x \cdot y) = \varphi_2(\varphi_1(x \cdot y)) = \varphi_2(\varphi_1(x) \bullet \varphi_1(y)) = \varphi_2(\varphi_1(x)) \star \varphi_2(\varphi_1(y)) = (\varphi_2 \circ \varphi_1)(x) \star (\varphi_2 \circ \varphi_1)(y)$$

since φ_1 and φ_2 are homomorphisms by definition.

□

For a mapping $\varphi : S \to T$ we denote the **restriction** of φ to the subset $X \subseteq S$ by $\varphi\restriction X$. We define $\varphi\restriction X : X \to T$ for all $x \in X$ by

$$(\varphi\restriction X)(x) = \varphi(x).$$

This result states, that two homomorphisms are the same if they map the generators in the same way.

Theorem. Let $(S, \cdot)$ and $(T, \bullet)$ be two pairs, $X \subseteq S$ and $\varphi_1, \varphi_2 : S \to T$ be two homomorphisms, then

$$\varphi_1 \restriction X = \varphi_2 \restriction X \Leftrightarrow \varphi_1 \restriction [X]_S = \varphi_2 \restriction [X]_S$$

Proof. The implication from right to left is obvious. Since our mappings are equal on $[X]_S$, they are also equal on X because it is just a subset of $[X]_S$.

For the other direction of the equivalence consider some $r = x_1 \cdot ... \cdot x_n \in [X]_S$. Then by $\mathbf{T_1}$ and since φ_1 and φ_2 are homomorphisms, we have for $x_i \in X$:

$$\varphi_1(r) = \varphi_1(x_1 \cdot ... \cdot x_n) = \varphi_1(x_1) \bullet ... \bullet \varphi_1(x_n) = \varphi_2(x_1) \bullet ... \bullet \varphi_2(x_n) = \varphi_2(x_1 \cdot ... \cdot x_n) = \varphi_2(r)$$

□

4.2 *Definitions.* **Embeddings and isomorphisms:**

A homomorphism $\varphi : S \to T$ is called

- an **embedding** or **monomorphism**, denoted $\varphi : S \hookrightarrow T$, if $\varphi(x) = \varphi(y)$ implies $x = y$. This special property is called **injectivity**.

- an **epimorphism**, denoted $\varphi : S \twoheadrightarrow T$, if for all $y \in T$ there exists some $x \in S$ with $\varphi(x) = y$. This is called **surjectivity**.

- an **isomorphism**, denoted $\varphi : S \rightarrowtail T$, if it is an embedding **and** an epimorphism, meaning it is injective **and** surjective. If this is the case, we call the mapping φ a **bijection**.

- an **endomorphism**, if $S = T$.

- an **automorphism**, if it is both an isomorphism **and** an endomorphism.

Lemma. $\mathbf{L_9}$: Let us denote the **identity mapping** of some pair $(S, \cdot)$ by $id_S : S \to S$, where $id_s(x) = x$ for all $x \in S$. This mapping forms an automorphism.

Proof. Obviously our domain is the same as our codomain, namely S. So we nearly have id_S being an endomorphism if we can prove it to be a homomorphism. Let us now confirm id_S being one:

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

This statement has been proven to be correct. Now we need to show, that we are dealing with a bijection. Let us confirm the injectivity first:

$$id_S(x) = id_S(y) \Leftrightarrow x = y \ .$$

On the other hand, for the surjectivity we have:

$$id_S(x) \overset{(\star)}{=} id_S(y) = y \ ,$$

where $(\star)$ follows directly from id_S being injective. Thus our lemma has been established.

□

Lemma. **L_{10}**: Let $(S, \cdot)$ be a pair. For all $\varphi : S \to S$ we have $\varphi \circ id_S = \varphi = id_S \circ \varphi$ under function composition.

Proof. $(\varphi \circ id_S)(x) = \varphi(id_S(x)) = \varphi(x) = id_S(\varphi(x)) = (id_S \circ \varphi)(x)$

□

Proposition. **P_5**: Let $f : S \to T$ and $g : T \to P$ be two bijections. Then their composition $g \circ f : S \to P$ is also a bijection.

Proof. For the injectivity we have:

$$\begin{aligned}&(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y)\\ &\Leftrightarrow f(x) = f(y)\\ &\Leftrightarrow x = y,\end{aligned}$$

where all the equivalences follow from the fact, that f and g are bijections and thus injections. For the surjection property we need to take a closer look at f and g which are also surjections in itself:

$$\text{for all } p \in P \text{ there exists some } t \in T \text{ with } g(t) = p$$

$$\text{and}$$

$$\text{for all } t \in T \text{ there exists some } s \in S \text{ with } f(s) = t$$

Then,

$$(g \circ f)(s) = g(f(s)) = g(t) = p\ ,$$

meaning there exists some $s \in S$ for every $p \in P$ with $(g \circ f)(s) = p$ which is the definition of the composition being surjective.

Hence the composition is injective and surjective, making it a bijection.

□

Proposition. **P_6**: $\varphi : S \to T$ is bijective iff φ has an inverse $\varphi^{-1} : T \to S$.

Proof. Let φ be bijective and let us suppose there exists some φ^{-1}. Since φ is bijective, it is also surjective, meaning there exists some $s \in S$ for all $t \in T$ with $\varphi(s) = t$. Now let $\varphi^{-1}(t) = s$. We know that our φ is injective and thus s is unique, making φ^{-1} well defined.

The property of an inverse is that if we compose it with the original function we are going to be left with the identity mapping. Let us confirm this statement from both directions of the composition. Let $s \in S$ and $\varphi(s) = t$, then we also have $\varphi^{-1}(t) = s$. Then:

$$(\varphi^{-1} \circ \varphi)(s) = \varphi^{-1}(\varphi(s)) = \varphi^{-1}(t) = s = id_S(s)$$

and

$$(\varphi \circ \varphi^{-1})(t) = \varphi(\varphi^{-1}(t)) = \varphi(s) = t = id_T(t) \ .$$

This finishes the first implication of the equivalence. Let us now have an inverse $\varphi^{-1} : T \to S$ of φ. We have to show, that $\varphi : S \to T$ is bijective. Let $t \in T$ and $\varphi^{-1}(t) = s$, then

$$\varphi(s) = \varphi(\varphi^{-1}(t)) = (\varphi \circ \varphi^{-1})(t) = id_T(t) = t \ .$$

This finishes the surjectivity, since we have found some $s \in S$ for all $t \in T$ with $\varphi(s) = t$. Lastly we have to take care of the injectivity. Let $s_1, s_2 \in S$, such that $\varphi(s_1) = \varphi(s_2)$. Now let $\varphi(s_1) = t$. Since we have an inverse function, we also have $\varphi^{-1}(t) = s_1$. Thus we obtain:

$$s_1 = id_S(s_1) = (\varphi^{-1} \circ \varphi)(s_1) = \varphi^{-1}(\varphi(s_1)) = \varphi^{-1}(\varphi(s_2)) = (\varphi^{-1} \circ \varphi)(s_2) = id_S(s_2) = s_2$$

Thus we have shown, if $\varphi(s_1) = \varphi(s_2)$, then $s_1 = s_2$ which is the definition of injectivity. By this new proposition, we can also immediately derive a new statement for the inverse function itself. Consider φ, which is nothing but the inverse function's inverse function, meaning $\varphi = (\varphi^{-1})^{-1}$. By our equivalence we know, that since an inverse function now exists to our inverse function, it is equivalent to saying that our inverse function φ^{-1} is bijective.

□

Lemma. **$\mathbf{L_{11}}$**: Let $(S, \cdot)$ and $(T, \bullet)$ be two pairs. If $\varphi : S \to T$ is an isomorphism, then the **inverse map** $\varphi^{-1} : T \to S$ is also an isomorphism.

Proof. At first we have to confirm that an inverse mapping exists. By **$\mathbf{P_6}$** this is indeed the case, since φ is bijective. Furthermore, we have $\varphi \circ \varphi^{-1} = id_S$, where $id_s : S \to S$ is the identity function, with $id_S(x) = x$. Those facts also follow immediately from **$\mathbf{P_6}$**. And hence, because φ is a homomorphism we have for all $x, y \in S$:

$$\varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) \bullet \varphi(\varphi^{-1}(y)) = x \bullet y$$

and so $\varphi^{-1}(x) \cdot \varphi^{-1}(y) = \varphi^{-1}(x \bullet y)$.

□

An algebraic structure S is **embeddable** in another structure T, if there exists some $\varphi : S \hookrightarrow T$. A structure S is **isomorphic** to T, being denoted by $S \cong T$, if there exists an isomorphism $\varphi : S \rightarrowtail T$. Two isomorphic structures share their **algebraic** properties.

The endomorphisms of some S are closed under composition, that is, if $\varphi_1, \varphi_2 : S \to S$ are endomorphisms, then so is $\varphi_2 \circ \varphi_1$. The same statement holds true for automorphisms.

Theorem. The endomorphisms of a semigroup S form a monoid.

Proof. At first let us ensure the closure. Let $(\mathrm{End}(S), \circ)$ be our pair, where we have the set of endomorphisms of $(S, \cdot)$ under function composition. Now let $f, g \in \mathrm{End}(S) = \{\varphi : S \to S\}$. For the composition of f and g to be closed under composition, we just have to show, that $g \circ f$ is once again a homomorphism. Since f and g are homomorphisms themselves, it then follows, that

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

for all $x, y \in S$. This result is nothing new though, since we have verified its correctness already in $\mathbf{L_8}$. This deals with the closure. The associativity follows immediately for all $f, g, h \in \mathrm{End}(S)$:

$$[f \circ (g \circ h)](x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = [(f \circ g) \circ h](x) \ .$$

Last but not least we have to make sure that there is some $id_S \in \mathrm{End}(S)$ such that $f \circ id_S = f = id_S \circ f$ for all $f \in \mathrm{End}(S)$. This is indeed the case, and by $\mathbf{L_9}$ and $\mathbf{L_{10}}$ the claim follows.

□

Theorem. The automorphisms of a semigroup S form a group.

Proof. Let $(\mathrm{Aut}(S), \circ)$ be a pair, and let $f, g \in \mathrm{Aut}(S) = \{\varphi : S \to S \mid \varphi \text{ is a bijection}\}$. Since an automorphism is nothing but an endomorphism **and** a bijection, we nearly get $(\mathrm{Aut}(S), \circ)$ being a monoid from the previous theorem. All that is left to show, is that the composition of f and g is also a bijection. This follows immediately from $\mathbf{P_5}$.

Thus, all that we now need, is that for all $f \in \mathrm{Aut}(S)$ there exists some $f^{-1} \in \mathrm{Aut}(S)$ such that $f \circ f^{-1} = id_S = f^{-1} \circ f$. Since f is a bijection, there indeed exists a bijective inverse function f^{-1} of f by $\mathbf{P_6}$. The fact that f^{-1} is a homomorphism follows immediately from $\mathbf{L_{11}}$. Thus $\mathrm{Aut}(S)$ is indeed a group under function composition.

□

4.3 *Definition.* **The full transformation semigroup:**

Let X be a set, and let $\mathcal{T}_X$ be the set introduced back in (5). This set forms the so-called **full transformation semigroup** on X under function composition.

Example. (17) Let $X = \{1, 2\}$. Altogether we have $2 \cdot 2 = 4$ functions in $\mathcal{T}_X$. A mapping $\varphi : X \to X$, which is defined by $\varphi(1) = 2$ and $\varphi(2) = 2$ can be represent mainly in two ways:

$$\varphi = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \qquad \text{or} \qquad 1 \overset{\varphi}{\to} 2$$

Now we let

$$\zeta = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix},$$

and $S = [\varphi, \zeta]_S$ the semigroup of $\mathcal{T}_X$ generated by φ and ζ. Then we have:

$$\varphi^2 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \varphi \qquad \zeta^2 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = id_X \qquad \varphi \circ \zeta = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \varphi$$

$$\zeta \circ \varphi = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \qquad \varphi \circ \zeta^2 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \varphi$$

Those combinations and ζ itself actually cover all the elements of this semigroup. Thus, $S = \{\varphi, \zeta, \zeta \circ \varphi, \zeta^2\}$ has all in all 4 elements. This also means, that $S = \mathcal{T}_X$ since it covers all possible combinations of $\mathcal{T}_X$.

5 Representations and the Cayley type Theorem

5.1 *Definition.* **Representations:**

We call a homomorphism $\varphi : S \to \mathcal{T}_X$ a **representation** of a structure S. The mapping φ is called a **faithful representation**, if $\varphi : S \hookrightarrow \mathcal{T}_X$, namely an embedding.

The following theorem is the climax of this paper. It states that every semigroup can be realized as a transformation semigroup of some set. In other words we can say, that for each semigroup S there exists some set X, such that $S \cong P \leq \mathcal{T}_X$ for a semigroup P of transformations.

5.2 *Theorem.* **The Cayley theorem for semigroups:**

Every semigroup S has a faithful representation.

Proof. We can equivalently rephrase the theorem into:

$$\text{Each semigroup is embedded in some } \mathcal{T}_X \ .$$

This basically means that we need to show, that there exists some $\varphi : S \to \mathcal{T}_X$, such that φ is injective **and** a homomorphism.

Let $(S, \cdot)$ be some semigroup. Now consider $X = S^1$, meaning that we have adjoined an identity 1 to S in case S is not a monoid. Now let $\mathcal{T}_X = \{\rho \mid \rho : X \to X\}$ be the full transformation semigroup.

For every $s \in S$ we let $\rho_s \in \mathcal{T}_X$ be the **left translation** $\rho_s(x) = s \cdot x$ for all $x \in X$. Now consider $\varphi(s) = \rho_s$.

Let us verify the injectivity of φ first. That means we have to show, that for all $s, t \in S$:

$$\varphi(s) = \varphi(t) \Rightarrow s = t.$$

Then, $\varphi(s) = \varphi(t)$ is equivalent to saying $\rho_s = \rho_t$, and so we have $\rho_s(x) = \rho_t(x)$ for all $x \in X$. In particular, by using our adjoined identity element $1 \in X$, we have

$$\rho_s(1) = \rho_t(1) \Leftrightarrow s \cdot 1 = t \cdot 1 \Leftrightarrow s = t.$$

Thus, $\varphi : S \to \mathcal{T}_X$ is injective. What is left to show, is φ being a homomorphism. Let s and t be like above, then we have for all $x \in X$:

$$(\rho_s \circ \rho_t)(x) = \rho_s(\rho_t(x)) = \rho_s(t \cdot x) = s \cdot (t \cdot x) \overset{(\star)}{=} (s \cdot t) \cdot x = \rho_{st}(x),$$

where $(\star)$ is justified, by $(S, \cdot)$ being a semigroup, and thus associative. With this new observation we can finally conclude, that for all $s, t \in S$:

$$\varphi(s \cdot t) = \rho_{st} = \rho_s \circ \rho_t = \varphi(s) \circ \varphi(t) \ .$$

This clearly shows, that $\varphi : S \to \mathcal{T}_X$ is indeed a homomorphism and an injection making it an embedding in the process. Thus $\varphi : S \hookrightarrow \mathcal{T}_X$ and the theorem has been proven.

□

Note that the identity element 1 is needed in the proof, in order for us to verify the injectivity of φ. It is of need, because there exists some semigroup S, one without an identity element, which hast two left identities $x \neq y$. If this is the case, then $xz = yz$ for all $z \in S$.

Hence, in a loosely speaking manner, we can, by Cayley's theorem for semigroups, conclude, that the theory of semigroups can be taught as the theory of transformations.

REFERENCES

Tero Harju: *Lecture Notes on Semigroups*. Department of Mathematics, University of Turku, Finland, 1996.

Prof. Dr. J. Gräter: *Algebra und Arithmetik*. Department of Mathematics, University of Potsdam, Germany, 2018.

Frank Ayres, Lloyd R. Jaisingh: *Schaum's Outline of Abstract Algebra, Second Edition*. The McGraw-Hill Companies, 2004.

Christopher Hollings: *The Early Development of the Algebraic Theory of Semigroups*. Archive for History of Exact Sciences 63(5):497-536, September 2009.