CHAPTER 1

Semigroups

This chapter introduces, in Section 1, the first basic concept of our theory – semigroups – and gives a few examples. In Section 2, we define the most important basic algebraic notions on semigroups – subsemigroups, idempotent elements, and homomorphisms resp. isomorphisms – and state some simple properties.

There are plenty of examples of semigroups having no idempotent elements. The main result of Section 4, however, is that every compact right topological semigroup has idempotent elements. This theorem will be applied repeatedly in later chapters to the Stone-Čech compactification βS of a discrete semigroup S, and it is the fact responsible for many combinatorial resp. dynamical applications of the theory.

In Section 3, we present a less obvious example of semigroups, the free ones, enjoying a particular universal property. A reader not interested in the somewhat abstract arguments of this section may skip it it for now and return to it when reading Chapter 7.

1. Examples of semigroups

1.1. Definition A *semigroup* is a pair $(S, \cdot)$ in which S is a non-empty set and $\cdot$ is a binary associative operation on S. I.e. the equation $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ holds for all $x, y, z \in S$.

As long as not otherwise stated, we write the semigroup operation as multiplication. And we mostly omit it typographically, i.e. we write S instead of $(S, \cdot)$, xy instead of $x \cdot y$, $x(yz)$ instead of $x \cdot (y \cdot z)$, and so on.

Two particularly popular and simple semigroups are given in part (a) of the following definition; they are also the most important ones.

1.2. Example (a) The set $\omega = \{0, 1, 2, \dots\}$ of all natural numbers (including 0) forms a semigroup $(\omega, +)$, under the usual addition of natural numbers. Similarly, the set $\mathbb{N} = \{1, 2, 3, \dots\}$ of all positive natural numbers (excluding 0) gives the semigroup $(\mathbb{N}, +)$, under addition.
(b) Both ω and $\mathbb{N}$ are also semigroups under multiplication: $(\omega, \cdot)$ and $(\mathbb{N}, \cdot)$.

1.3. Example Let S be a non-empty set. There are two extremely simple semigroup structures on S: with the multiplication given by $x \cdot y = x$, for $x, y \in S$, $(S, \cdot)$ is called the *left zero semigroup* over S.
Also, fixing an element a of S and putting $x * y = a$, for all $x, y \in S$, gives a semigroup structure on S.

1.4. Example Let X be any set and denote by $\mathcal{P}_f(X)$ the set of all finite non-empty subsets of X. Clearly, $\mathcal{P}_f(X)$ is a semigroup under the operation of taking the union of two sets. And so is the set $\mathcal{P}(X)$ consisting of all subsets of X.

1.5. Definition A semigroup S is *commutative* if the equation $xy = yx$ holds for all $x, y \in S$.

All semigroups considered above are commutative, except the left zero semigroup in Example 1.3. But the following one is highly non-commutative.

1.6. Example For an arbitrary set X, we write ${}^X X$ for the set of all mappings from X to X. The set ${}^X X$ is a semigroup under the composition $\circ$ of mappings as multiplication. Unless the preceding examples, it is not commutative if X has at least two elements.

1.7. Example Let $(G, \cdot, e, ^{-1})$ be a group; here $e \in G$ is the identity of G and x^{-1} is the inverse of an element x. Then $(G, \cdot)$ is a semigroup, the semigroup arising from G. Groups enjoy additional properties which do not hold for arbitrary semigroups. E.g. they satisfy the cancellation rules: $xa = ya$ resp. $ax = ay$ imply that $x = y$.

2. Special maps, elements, and subsets of semigroups

In this section, we define some algebraic notions from the theory of semigroups – homomorphisms, subsemigroups, idempotent resp. zero elements – and state some very simple facts about them. The notions and their properties are used over and over again; we thus prefer to collect them here to be able to quote them later, when needed.
A reader experienced in algebraic reasoning will be familiar with this material and just have a sketchy view; other readers may prefer to read it only when it is applied.

The semigroups $(\omega, +)$ and $(\mathbb{N}, +)$, respectively $(\omega, \cdot)$ and $(\mathbb{N}, \cdot)$, look quite similar, but differ in some algebraic aspect, i.e. they are non-isomorphic. More precisely, isomorphic semigroups may differ by their underlying sets but have otherwise exactly the same algebraic behaviour, non-isomorphic ones are considered as essentially different. This is made precise by the following definitions.

1.8. Definition Assume S and T, more exactly $(S, \cdot)$ and $(T, \cdot)$, are semigroups.
(a) A map $h : S \to T$ from S to T is a *homomorphism* if it commutes with the semigroup operations of S respectively T, i.e. if $h(x \cdot y) = h(x) \cdot h(y)$ holds for all $x, y \in S$.
(b) A homomorphism $h : S \to T$ is called an *embedding* or a *monomorphism* if it is one-one, an *epimorphism* if it is onto, and an *isomorphism* from S onto T if it is bijective.
(c) S and T are said to be *isomorphic* if there is an isomorphism from S onto T.

For example, the set $P = \{2, 4, 8, \dots\} \subseteq \mathbb{N}$ of all powers of 2 is a semigroup under multiplication, and mapping $n \in \mathbb{N}$ to $2^n \in P$ defines an isomorphism from $(\mathbb{N}, +)$ onto $(P, \cdot)$.

1.9. Definition and Remark More generally, for any multiplicative semigroup $(S, \cdot)$ and any $a \in S$, we write a^n for the product $a_1 \cdot \dots \cdot a_n$ where $a_i = a$ for

$1 \leq i \leq n$.
And mapping n to a^n gives a homomorphism from $(\mathbb{N}, +)$ into $(S, \cdot)$.

How do we show that two given semigroups are non-isomorphic? E.g. like this: every isomorphism $h : S \to T$ between semigroups $(S, \cdot)$ and $(T, \cdot)$ preserves commutativity, since if S is commutative, then $h(x)h(y) = h(xy) = h(yx) = h(y)h(x)$ holds for arbitrary $x, y \in S$. In other words, a commutative semigroup is certainly not isomorphic to a non-commutative one.
We begin to consider elements with special properties in semigroups; in particular, idempotent elements will play a prominent role throughout the text.

1.10. Definition Assume $(S, \cdot)$ is a semigroup.
(a) An element e of S is *idempotent* if $e \cdot e = e$.
(b) $z \in S$ is a *zero* of S if $x \cdot z = z \cdot x = z$ holds for all $x \in S$.
(c) An element n of S is an *identity* of S if $n \cdot x = x \cdot n = x$ holds for all $x \in S$.

We can now argue that the semigroups $(\omega, +)$ and $(\mathbb{N}, +)$ from 1.2 are non-isomorphic: every homomorphism $h : S \to T$ maps idempotent elements e of S to idempotents in T, because $h(e) \cdot h(e) = h(e \cdot e) = h(e)$. But $(\omega, +)$ has 0 as its unique idempotent element and $(\mathbb{N}, +)$ has no idempotent element. Similarly, $(\omega, \cdot)$ and $(\mathbb{N}, \cdot)$ are non-somorphic: $(\omega, \cdot)$ has two distinct idempotent elements (0 and 1), $(\mathbb{N}, \cdot)$ only one (1). We will often work with the semigroups $(\omega, +)$ and $(\mathbb{N}, +)$; it will depend of the situation which of them works better.
In the semigroup $\mathcal{P}_f(X)$ from Example 1.4, all elements are idempotent.

1.11. Notation Assume $(S, \cdot)$ is a semigroup, $a \in S$ and $M, N \subseteq S$. We define the subsets aM, Ma, MN of S by

$$a \cdot M = aM = \{am : m \in M\},$$
$$M \cdot a = Ma = \{ma : m \in M\},$$
$$M \cdot N = MN = \{mn : m \in M, n \in N\}.$$

1.12. Definition A *subsemigroup* of $(S, \cdot)$ is a non-empty subset T of S which is closed under the multiplication of S, i.e. it satisfies $T \cdot T \subseteq T$. In other words, T is a semigroup under the multiplication of S restricted to T.

For example, $(\mathbb{N}, +)$ is a subsemigroup of $(\omega, +)$. And for every idempotent e of a semigroup S, $\{e\}$ is a subsemigroup of S.

1.13. Definition Let M be a non-empty subset of a semigroup $(S, \cdot)$. There is a least subsemigroup of S including M, namely the set

$$\langle M \rangle = \{a_1 \cdot \cdots \cdot a_n : n \in \mathbb{N} \text{ and } a_1, \ldots, a_n \in M\}$$

of all finite non-empty products of elements of M. It is called *the subsemigroup* of S *generated by* M.
For T a subsemigroup of S, M is said to be a *set of generators of* T if $\langle M \rangle = T$.

E.g. in the additive semigroup of natural numbers, the subsemigroup $T = \{2, 3, 4, \ldots\}$ is generated by the set $M = \{2, 3\}$. Let us note that in this example, the representation of an element of T as a finite sum of elements of M is not unique, e.g. $6 = 2 + 2 + 2 = 3 + 3$.

We note some simple connections between homomorphisms, subsemigroups, and generating sets.

1.14. Lemma *(a) Assume $h : S \to T$ is a semigroup homomorphism. Then for any subsemigroup P of S, the image $h[P] = \{h(x) : x \in P\}$ of P under h is a subsemigroup of T. Similarly, for any subsemigroup Q of T, the preimage $h^{-1}[Q] = \{x \in S : h(x) \in Q\}$ of Q under h is a subsemigroup of S, if non-empty.*
(b) For $h : S \to T$ a homomorphism and $M \subseteq S$, h maps the subsemigroup of S generated by M onto the subsemigroup of T generated by $h[M]$.
(c) Assume M is a set of generators of S. Then two homomorphisms g and h from S to T coincide iff they coincide on M, i.e. iff $g(x) = h(x)$ holds for all $x \in M$.

Proof. By straigtforward calculations. In (c), consider the set $P = \{x \in S : g(x) = h(x)\}$. It is a subsemigroup of S and includes M; hence $S = \langle M \rangle \subseteq P$. $\square$

3. Free semigroups

In this section, we define a very special example of semigroups, the free ones. They are easily understood by their very construction in 1.15 and, on the other hand, quite important for the theory of semigroups because of their characteristic universal property stated in 1.16 and 1.18.

1.15. Construction Assume that L is an arbitrary non-empty set. In the context of this section, the set L is called an *alphabet*; the elements of L are the *letters* of L.
(a) We denote by L^* the set of all ordered sequences of finite length greater than 0. I.e. a typical element of L^* has the form

$$w = (b_1, \dots, b_n)$$

where $n \in \mathbb{N}$ and $b_1, \dots, b_n$ are any elements of L. We usually omit the brackets and the periods in the notation of w, thus abbreviating

$$w = b_1 \dots b_n.$$

The elements of L^* are called *words* (of finite length) over the alphabet L. More exactly, the word $w = b_1 \dots b_n$ has length $n \in \mathbb{N}$. Two words $v = a_1 \dots a_m$ and $w = b_1 \dots b_n$ from L^* coincide iff their lenghs m and n are the same and $a_i = b_i$ holds for all $i \in \{1, \dots, n\}$. E.g., if a, b are two different letters fron L, then $v = abaa$ and $w = aaba$ are different words both of length four.
(b) Under the conventions from (a), we write the one-letter words (b), for $b \in L$, simply by as b and thus consider L to be a subset of L^*.
(c) The set L^* is made into a semigroup, the *free semigroup over* L, under the operation of concatenation: for $v = a_1 \dots a_m$ and $w = b_1 \dots b_n$ in L^*, put

$$vw = a_1 \dots a_m b_1 \dots b_n,$$

the word of length $m + n$ which arises by writing w directly after v. E.g. for $v = abaa$ and $w = aaba$, we obtain $vw = abaaaaba$ and $wv = aabaabaa$.

We can now prove the universal property of free semigroups.

1.16. Theorem *Assume that L^* is the free semigroup over L, S is an arbitrary semigroup, and $f : L \to S$ is an arbitrary map from L into S. Then there is a unique semigroup homomorphism $\bar{f} : L^* \to S$ extending f.*

Proof. Assume that $(S,\cdot)$ is a semigroup. Every word $w = b_1 \dots b_n$ over L is the concatenation of its one-letter subwords $b_1, \dots, b_n$. It follows that for a homomorphism $g : L^* \to S$ extending f, we must have $g(w) = f(b_1) \cdot \ \dots \ \cdot f(b_n)$, which proves the uniqueness statement.
On the other hand, the map $\bar{f} : L^* \to S$ given by

$$\bar{f}(b_1 \dots b_n) = f(b_1) \cdot \ \dots \ \cdot f(b_n)$$

is obviously a homomorphism from L^* into S which extends f. □

Theorem 1.16 is the reason for calling the semigroup L^* *free* over L: the elements of $L \subseteq L^*$ do not satisfy any equations, except those which hold in all semigroups. This is because an equation satisfied by elements of L in L^* is preserved under homomorphisms and would thus hold for arbitrary elements of arbitrary semigroups. For example, the law $xy = yx$ of commutativity does not hold in arbitrary semigroups, as we know fom Example 1.6, and it does not hold in the free semigroup over an at least two-letter alphabet – see 1.15(c).

1.17. Remark The free semigroup over a one-letter alphabet $L = \{a\}$ is isomorphic to $(\mathbb{N}, +)$, the additive semigroup of positive natural numbers: the words over L have the form $w = a^n$ where $n \in \mathbb{N}$ and a^n is the sequence of length n with all entries equal to a. Mapping $n \in \mathbb{N}$ to a^n, we obtain an isomorphism from $\mathbb{N}$ onto L^*.

The following corollary is the reason for an effect we will meet later: in many situations, combinatorial principles valid for free semigroups carry over to arbitrary semigroups.

1.18. Corollary *Every semigroup is the homomorphic image of a free one.*

Proof. Let S be an arbitrary semigroup; we fix an alphabet L of size at least $|S|$ and a map f from L onto S. The homomorphic extension $\bar{f} : L^* \to S$ of f, given by Theorem 1.16, maps L^* onto S. □

4. Compact right topological semigroups and idempotents

The examples above, e.g. $(\mathbb{N}, +)$ or any free semigroup, show that semigroups do not necessarily have idempotent elements. In this section, however, we prove that semigroups from a very special class, the compact right topological ones, do have idempotents. This fact will first be used in Chapter 5 to prove a highly non-trivial combinatorial fact, Hindman's theorem.

1.19. Definition (a) In a semigroup $(S,\cdot)$, we define for any $s \in S$ the *right translation* map $\rho_s : S \to S$ with respect to s by $\rho_s(x) = x \cdot s$. Similarly, the *left translation* $\lambda_s : S \to S$ with respect to s is defined by $\lambda_s(x) = s \cdot x$.
(b) A *compact right topological semigroup* is a triple $(S, \cdot, \mathcal{O})$ where $(S, \cdot)$ is a semigroup, $\mathcal{O}$ is a topology on S, the space $(S, \mathcal{O})$ is compact and Hausdorff, and for every $s \in S$, the right translation map ρ_s is continuous with respect to $\mathcal{O}$. By abuse of notation, we will simply say that S is a compact right topological semigroup.

Note that, in a compact right topological semigroup S, we do not require that the left translations λ_s are continuous. In particular, the multiplication $\cdot : S \times S \to S$

on S is not required to be jointly continuous. In fact, in the principal example of a compact right topological semigroup to be considered later, the Stone-Čech compactification βS of a discrete semigroup S, left translations will usually not be continuous.

1.20. Example We give some simple examples of semigroups with a compact Hausdorff topology on them. They are, in fact, topological semigroups, in the sense that their multiplication is jointly continuous.
(a) The unit circle in the complex plain

$$C = \{z \in \mathbb{C} : |z| = 1\}$$

is a compact subset of $\mathbb{C}$ and closed under complex multiplication, thus a topological semigroup. More precisely, it is a topological group, i.e. both its multiplication and the operation of taking inverses are continuous.
(b) The unit disk in $\mathbb{C}$, i.e.

$$D = \{z \in \mathbb{C} : |z| \leq 1\}$$

is a compact topological semigroup, under complex multiplication.
(c) Every finite semigroup, equipped with the discrete topology, is a compact topological semigroup.

Unless semigroups in general, compact right topological semigroups do have idempotents.

1.21. Theorem *Every compact right topological semigroup has an idempotent element.*

This is a direct consequence of the two subsequent lemmas. By a closed subset of S, we understand, of course, a *topologically* closed subset.

1.22. Lemma *Every compact right topological semigroup has a minimal closed subsemigroup.*

Proof. A standard application of Zorn's Lemma: let S be a compact right topological semigroup. The system $\mathcal{T}$ of closed subsemigroups of S is partially ordered by reverse inclusion and non-empty because $S \in \mathcal{T}$. Every chain $\mathcal{C}$ in the partial order $(\mathcal{T}, \supseteq)$ has a least upper bound, namely $\bigcap_{T \in \mathcal{C}} T$ – note that this intersection is non-empty, because S is compact and $\mathcal{C}$ has the finite intersection property. Thus by Zorn's lemma, $\mathcal{T}$ has a maximal element M. This means that M is a minimal closed subsemigroup of S. □

1.23. Lemma *Let S be a compact right topological semigroup, M a minimal closed subsemigroup of S, and $e \in M$. Then e is idempotent (and $M = \{e\}$, by minimality).*

Proof. We proceed in two steps.
Claim 1. $Me = M$. – To see this, we note that Me is a non-empty subset of M (because $e \in M$ and M is closed under multiplication). It is also a subsemigroup of M, as is easily checked. Moreover, it is compact, being the image of the compact subset M of S under the continuous right multiplication ρ_e with respect to e. The claim follows by minimality of M.
Claim 2. The set $N = \{x \in M : xe = e\}$ of M coincides with M. – This follows

from the fact that N is a closed subsemigroup of M: N is a subset of M which is obviously closed under multiplication. To see that it is non-empty, write, by Claim 1, the element e of $M = Me$ in the form $e = xe$ for some $x \in M$; then $x \in N$. And N is closed, being the intersection of the closed subsets M and $\rho_e^{-1}[\{e\}]$ (the preimage of e under the continuous map ρ_e) of S.

By Claim 2, we see that $e \in N$ and thus that $e \cdot e = e$. □

We can conclude from Theorem 1.21 that every finite semigroup has an idempotent element. There is, of course, an elementary proof of this fact, and the reader is encouraged to find it for herself.

Exercises

(1) A semigroup S is called *simply generated* if there is an element a of S such that $\{a\}$ is a set of generators of S. Thus S is the set $\{a^n : n \in \mathbb{N}\}$, consisting of all powers of a. Describe all simply generated semigroups, up to isomorphism.

(2) Give an elementary proof for the fact that every finite semigroup has an idempotent element.

(3) Assume that $(S, \cdot)$ is a semigroup.
(a) Prove that the *algebraic center* $CS = \{s \in S : xs = sx$ holds for all $x \in S\}$ of S is a subsemigroup of S, if non-empty.
(b) Assume that, in addition, a topology is given on S; prove that the *topological center* $LS = \{s \in S : \lambda_s$ is continuous$\}$ of S is a subsemigroup of S, if non-empty.
(c) For every right topological semigroup S, the algebraic center is contained in the topological one.

(4) Assume v and w are two elements of a free semigroup, i.e. two words over an alphabet L, and that $vw = wv$. Prove that there is a word u over L such that v and w are both powers of u.

(5) This exercise provides a slightly more general, and also more abstract, approach to free semigroups than given in Section 2 above. Given any set L, we call a pair (F, e) a free (semigroup) extension of L if F is a semigroup, $e : L \to F$ is a map, and for every map $f : L \to S$ from L into an arbitrary semigroup S, there is a unique semigroup homomorphism $\bar{f} : F \to S$ such that $f = \bar{f} \circ e$. Thus the semigroup L^* constructed in 1.15, with the inclusion map from L to L^*, is a concrete example of a free extension of L.
(a) Prove that any two free extensions (F, e) and (G, ε) of L are isomorphic over L, i.e. there is a unique isomorphism $h : F \to G$ satisfying $h \circ e = \varepsilon$.
(b) Conclude that in a free extension (F, e) of L, the map e is one-one and the image $e[L]$ of L under e generates F. We will therefore assume, in the rest of the exercises, that in a free extension (F, e) of L, L is a subset of F, e is the inclusion map from L to F, and F is generated by L. We say that F is free over its subset L.
(c) Prove that, for a semigroup $F \supseteq L$, F is free over L iff every $x \in F$ can be written, in a unique way, as the product

$$x = a_1 \cdot \ \ldots \ \cdot a_n$$

where $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in L$.

(6) (a) We define, on the real unit interval $X = [0, 1]$, two functions t_0 and t_1 by $t_0(x) = x/2$, $t_1(x) = (x + 1)/2$. Prove that the semigroup S of $({}^X X, \circ)$

generated by t_0, t_1 is free over $\{t_0, t_1\}$, in the sense of the preceding exercise.
(b) Try to generalize this statement as follows: for $k \in \mathbb{N}$, there are functions $f_0, \ldots, f_k$ from $X = [0, 1]$ into itself generating a free subsemigroup.
(c) More generally, assume that L is a set of functions from an arbitrary set X to itself, and any two distinct elements of L have disjoint ranges. Prove that the subsemigroup of $({}^X X, \circ)$ generated by L is free over L.