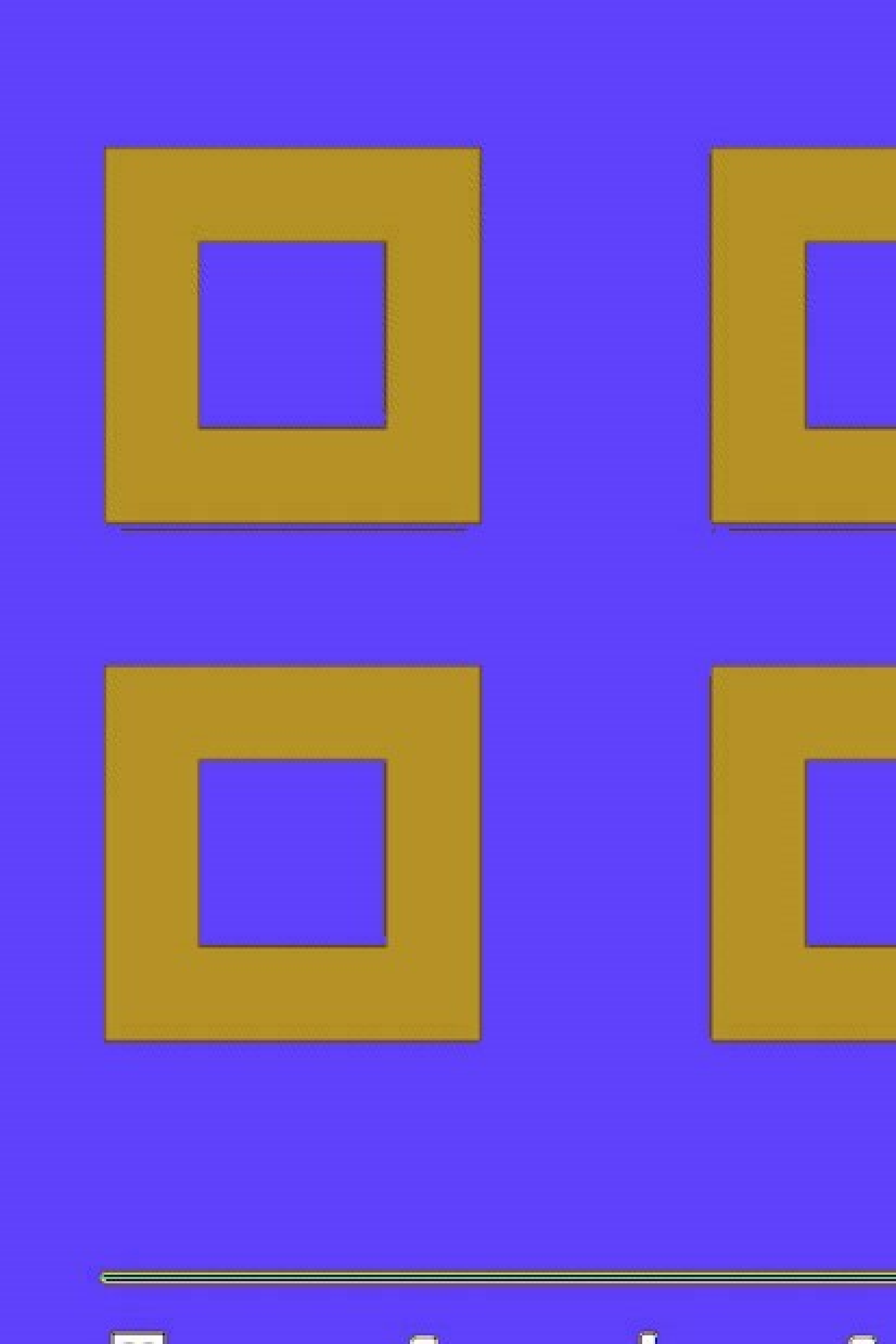

ATLANTIS STUDIES IN MATHEMATICS
VOLUME 1

SERIES EDITOR: **J. VAN MILL**

Atlantis Studies in Mathematics

Series Editor:

J. van Mill, VU University Amsterdam, the Netherlands

(ISSN: 1875-7634)

Aims and scope of the series

The series 'Atlantis Studies in Mathematics' (ASM) publishes monographs of high quality in all areas of mathematics. Both research monographs and books of an expository nature are welcome.

All books in this series are co-published with World Scientific.

For more information on this series and our other book series, please visit our website at:

www.atlantis-press.com/publications/books

ATLANTIS PRESS

AMSTERDAM – PARIS

World Scientific

Topological Groups and Related Structures

Alexander Arhangel'skii,
Ohio University, Athens, Ohio, U.S.A.

Mikhail Tkachenko,
Universidad Autónoma Metropolitana, Mexico City, Mexico

ATLANTIS PRESS
AMSTERDAM – PARIS

World Scientific

Atlantis Press
29 avenue Laumière
75019 Paris, France

For information on all Atlantis Press publications, visit our website at: www.atlantis-press.com.

ISBN: 978-90-78677-06-2 e-ISBN: 978-94-91216-35-0
ISSN: 1875-7634

Foreword

Algebra and topology, the two fundamental domains of mathematics, play complementary roles. Topology studies continuity and convergence and provides a general framework to study the concept of a limit. Much of topology is devoted to handling infinite sets and infinity itself; the methods developed are qualitative and, in a certain sense, irrational. Algebra studies all kinds of operations and provides a basis for algorithms and calculations. Very often, the methods here are finitistic in nature.

Because of this difference in nature, algebra and topology have a strong tendency to develop independently, not in direct contact with each other. However, in applications, in higher level domains of mathematics, such as functional analysis, dynamical systems, representation theory, and others, topology and algebra come in contact most naturally. Many of the most important objects of mathematics represent a blend of algebraic and of topological structures. Topological function spaces and linear topological spaces in general, topological groups and topological fields, transformation groups, topological lattices are objects of this kind. Very often an algebraic structure and a topology come naturally together; this is the case when they are both determined by the nature of the elements of the set considered (a group of transformations is a typical example). The rules that describe the relationship between a topology and an algebraic operation are almost always transparent and natural — the operation has to be continuous, jointly or separately. However, the methods of study developed in algebra and in topology do not blend so easily, and that is why at present there are very few systematic books on topological algebra, probably, none which can be qualified as a reasonably complete textbook for graduate students and a source of references for experts. The need for such a book is all the greater since the last half of the twentieth century has witnessed vigorous research on many topics in topological algebra. Especially strong progress has been made in the theory of topological groups, going well beyond the limits of the class of locally compact groups. The excellent book [**236**] by E. Hewitt and K. A. Ross just sketches some lines of investigation in this direction in a short introductory chapter dedicated to topological groups.

In the 20th century and during the last seven years many topologists and algebraists have contributed to Topological Algebra. Some outstanding mathematicians were involved, among them J. Dieudonné, L. S. Pontryagin, A. Weil, and H. Weyl. The ideas, concepts, and constructions that arise when topology and algebra come into contact are so rich, so versatile, that it has been impossible to include all of them in a single book; we have made our choice. What we have covered here well may be called “topological aspects of topological algebra”. This domain can be characterized as the study of connections between topological properties in the presence of an algebraic structure properly related to the topology.

A. D. Alexandroff, N. Bourbaki, M. I. Graev, S. Kakutani, E. van Kampen, A. N. Kolmogorov, A. A. Markov, and L. S. Pontryagin were among the first contributors to the theory of topological groups. Among those who contributed greatly to this field are W. W. Comfort, M. M. Choban, E. van Douwen, V. I. Malykhin, J. van Mill, and B. A. Pasynkov. These mathematicians have also contributed greatly to other aspects of topological algebra and of general topology.

Though the theory of topological groups is a core subject of topological algebra, a considerable attention has been given to the development of the theory of universal topological algebras, where topology and most general algebraic operations are blended together. This subject started to gain momentum with the works of A. I. Mal'tsev and in later years, some aspects of Mal'tsev's work especially close to general topology were developed by M. M. Choban and V. V. Uspenskij.

The fundamental topic of various types of continuity of algebraic operations was developed in the works of A. Bouziad, R. Ellis, D. Montgomery, I. Namioka, J. Troallic, and L. Zippin. The recent excellent book [**241**] of N. Hindman and D. Strauss contains a wealth of material on algebraic operations on compacta satisfying weak continuity requirements.

One of the leading topics in the general theory of topological groups was that of free topological groups of Tychonoff spaces. It is well represented in our book. A. A. Markov, S. Kakutani, T. Nakayama, and M. I. Graev were at the origins of this chapter. In later years S. A. Morris, P. Nickolas, O. G. Okunev, V. G. Pestov, O. Sipacheva, K. Yamada, and some other mathematicians have worked very successfully in this field.

Our book also contains a very brief introduction to topological dynamics. Among the first who worked in this field were W. Gottshalk, V. V. Niemytzki, and R. Ellis. J. de Vries, one of the later contributors to the subject, wrote the basic monograph [**530**] which gave a strong impuls to its further development. Some recent successes in the field are connected with the names of S. A. Antonyan, V. G. Pestov, S. Glasner, M. Megrelishvili, and V. V. Uspenskij. Well-written, very informative surveys [**379, 378**] by Pestov will orient the reader on this topic.

In this book we refer also to the works of many other excellent mathematicians, among them O. Alas, T. Banakh, L. G. Brown, R. Z. Buzyakova, D. Dikranjan, S. García-Ferreira, P. Gartside, I. I. Guran, K. P. Hart, S. Hernández, G. Itzkowitz, P. Kenderov, K. Kunen, W. B. Moors, P. Nyikos, E. Martín-Peinador, I. Prodanov, I. V. Protasov, D. A. Raĭkov, E. A. Reznichenko, D. Robbie, M. Sanchis, D. B. Shakhmatov, A. Shibakov, L. Stoyanov, A. Tomita, F. J. Trigos-Arrieta, N. Ya. Vilenkin, S. Watson, and E. Zelenyuk. We should also mention that the development of topological algebra was strongly influenced by survey papers [**109, 110, 113**] of W. W. Comfort (and coauthors), and by the books [**410**], [**249**] of W. Roelke and S. Dierolf and of T. Hussain, respectively.

We do not mention here the names of those who have worked recently in the theory of locally compact topological groups. This vast subject is mostly beyond the scope of this book, we have provided only a brief introduction to it.

This book is devoted to that area of topological algebra which studies the influence of algebraic structures on topologies that properly fit the structures. This domain could be called *"Topological invariants under algebraic boundary conditions"*. The book is by no means complete, since this area of mathematics is now rapidly developing in many directions. The central theme in the book is that of general (not necessarily locally compact) topological groups. However, we do not restrict ourselves to this main topic; on the contrary, we try to use it as a starting point in the investigation of more general objects, such as semitopological groups or paratopological groups, for example.

While not striving for completeness, we have made an attempt to provide a representative sample of some old and of some relatively recent results on general topological groups, not restricting ourselves just to two or three topics. The areas covered to a lesser or greater extent are cardinal invariants in topological algebra, separate and joint continuity of group operations, extremally disconnected and related topologies on groups, free topological groups, the Raĭkov completion of topological groups, Bohr topologies, and duality theory for compact Abelian groups.

One of the generic questions in topological algebra is how the relationship between topological properties depends on the underlying algebraic structure. Clearly, the answer to this should strongly depend on the way the algebraic structure is related to the topology. The weaker the restrictions on the connection between topology and algebraic structure are, the larger is the class of objects entering the theory. Because of that, even when our main interest is in topological groups, it is natural to consider more general objects with a less rigid connection between topology and algebra. Examples we encounter in such a theory help us to better understand and appreciate the fruits of the theory of topological groups.

Chapter 1 is of course, of an introductory nature. We define, apart from topological groups, the main objects of topological algebra such as semitopological groups, quasitopological groups, paratopological groups, and present the most elementary and natural examples and the most general facts. Some of these facts are non-trivial, even though they are easy to prove. For example, we establish that every open subgroup of a topological group is closed, and that every discrete subgroup of a pseudocompact group is finite. It is proved in this chapter that every infinite Abelian group admits a non-discrete Hausdorff topological group topology. Quotients, products, and Σ-products are also discussed in Chapter 1, as well as the natural uniformities on topological groups and their quotients.

In the course of the book, we introduce and study several important classes of topological groups. In particular, in Chapter 3 we study systematically ω-narrow topological groups which can be characterized as topological subgroups of arbitrary topological products of second-countable topological groups. An elementary introduction to the theory of locally compact groups is also given in Chapter 3. Then this topic is developed in Chapter 9, where an introduction into the theory of characters of compact and locally compact Abelian groups is to be found. Since there are several good sources covering this subject (such as [**236**], [**243**], and [**327**] just to mention a few), we do not pursue this topic very far. However, elements of the Pontryagin–van Kampen duality theory are presented, and the exposition is elementary and practically self-contained.

The celebrated theorem of Ivanovskij and Kuz'minov on the dyadicity of compact groups is proved in Chapter 4. Again, the proof is elementary (though not simple), polished, and self-contained. We apply Pontryagin–van Kampen duality theory to continue the study of the algebraic and topological structures of compact Abelian groups in Chapter 9. The book [**243**] by K.-H. Hofmann and S. A. Morris provides those readers who are interested in the duality theory with considerably more advanced material in this direction.

In Chapter 4 we consider the class of extremally disconnected groups, the class of Čech-complete groups, as well as the classes of feathered groups and P-groups. For each of these classes of groups we prove original and delicate theorems and then establish non-trivial relations between them. Feathered topological groups (called also p-groups) present a natural generalization of locally compact groups and of metrizable groups, that makes them especially interesting.

One of the unifying themes of this book is that of completions and completeness. One can look at completeness in topological algebra either from a purely topological point of view or from the point of view of the theory of uniform spaces; this latter takes into account the algebraic structure much better than the purely topological one. The basic construction of the Raĭkov completion of an arbitrary topological group is presented in Chapter 3; later on, it has many applications. Čech-completeness of topological groups is studied in Chapter 4, and the relationship of Dieudonné completion of a topological group with the group structure is a subject of a rather deep investigation in Chapter 6. In particular, we learn in Chapter 6 that under very general assumptions it is possible to extend continuously the group operations from a topological group to its Dieudonné completion. We also establish that this is not always possible. The class of Moscow groups is instrumental in the theory developed in Chapter 6. The class of $\mathbb{R}$-factorizable groups is studied in Chapter 8. This class serves as a bridge from general topological groups to second-countable groups via continuous real-valued functions. It also turns out to be important in the study of completions of topological groups.

Chapter 5 is devoted to cardinal invariants of topological groups. Invariants of this kind (which associate with topological spaces cardinal numbers "measuring" the space under consideration in one sense or another), play an especially important role in general topology; probably, this happens because the techniques they provide fit best the set-theoretic nature of general topology. So one may expect that in the study of non-compact topological groups cardinal invariants should occupy a prominent place. The following phenomenon makes the situation even more interesting: The structure of topological groups turns out to be much more sensitive to restrictions in terms of cardinal invariants than the structure of general topological spaces. For example, metrizability of a topological group depends only on whether the group is first-countable or not (Birkhoff–Kakutani's theorem). For paratopological groups the statement is no longer true (the Sorgenfrey line witnesses this); however, a weaker theorem holds: every first-countable paratopological group has a G_δ-diagonal. How delicate problems involving cardinal invariants of compact groups can be, is shown by the following simple result: It is not possible either to prove, or to disprove in ZFC that every compact group of cardinality not greater than $\mathfrak{c} = 2^\omega$ is metrizable.

In Chapter 7, a very powerful and delicate construction is presented — that of a free topological group over a Tychonoff space. Under this construction, any Tychonoff space X can be represented as a closed subspace of a topological group $F(X)$ in such a way that every continuous mapping of a space X into a space Y can be uniquely extended to a continuous homomorphism of $F(X)$ to $F(Y)$. The set X, of course, serves as an algebraic basis of $F(X)$. However, the relationship between the topology of X and that of $F(X)$ is the most intriguing; there are many unexpected and subtle results on free topological groups and quite a few unsolved problems. One of the most important theorems here states that the cellularity of the free topological group $F(X)$ of an arbitrary compact Hausdorff space X is countable. Curiously, one can demonstrate that this happens not because of the existence of a regular measure on $F(X)$ (in contrast with the case of compact groups). In fact, such a measure on $F(X)$ exists if and only if X is discrete.

Yet another major topic in the book is that of transformation groups, and the closely associated concepts of homogeneous spaces and of groups of homeomorphisms. A section is devoted to these matters in Chapter 3, where it is established that the group of isometries of a metric space is a topological group, when endowed with the topology of pointwise convergence. It is proved in this connection that every topological group is topologically isomorphic to a subgroup of the group of isometries of some metric space. This provides an important technical tool for some arguments.

Frequently, results on topological groups are followed by a discussion of other structures of topological algebra, such as semitopological and paratopological groups. This is done in almost every chapter. However, we have also devoted the whole of Chapter 2 to basic facts regarding such objects. A *paratopological group* is a group G with a topology such that the multiplication mapping of $G \times G$ to G is jointly continuous. A *semitopological group* G is a group G with a topology such that the multiplication mapping of $G \times G$ to G is separately continuous. A *quasitopological group* G is a group G with a topology such that the multiplication mapping of $G \times G$ to G is separately continuous and the inverse mapping of G onto itself is continuous. A natural example of a paratopological group is obtained by taking the group of homeomorphisms of a dense-in-itself locally compact zero-dimensional non-compact space, with the compact-open topology. The Sorgenfrey line under the usual addition is a paratopological group which is hereditarily separable, hereditarily Lindelöf and has the Baire property.

In 1936, D. Montgomery proved that every semitopological group metrizable by a complete metric is, in fact, a paratopological group. In 1957, R. Ellis showed that every locally compact semitopological group is a topological group. In 1960, W. Zelazko established that each completely metrizable semitopological group is a topological group. Later, in 1982, N. Brand proved that every Čech-complete paratopological group is a topological group. Recently A. Bouziad made a decisive contribution to this topic. He proved that every Čech-complete semitopological group is a topological group. This theorem naturally covers and unifies both principal cases, those of locally compact semitopological groups and of completely metrizable semitopological groups.

Since each Čech-complete topological group is paracompact, Bouziad's theorem implies that every Čech-complete semitopological group is paracompact. These and related results, with applications, are presented in Chapter 2. In this same chapter we construct an operation of a rather general nature on the Čech–Stone compactification βG of an arbitrary discrete group G. With this operation, the compact space βG becomes a right topological group. This structure has interesting applications; we mention some of them in problem sections. The reader who wants to learn more on this subject is advised to study the recent book [**241**] by N. Hindman and D. Strauss.

We formulate and discuss quite a few open problems, many of them are new. Each section is followed by a list of exercises and problems, including open problems. However, we should warn the reader that some of the new open problems might turn out not to be difficult after all. That does not necessarily mean that they should have been discarded. The main interest of many of the new questions we have posed lies in the fact that they delineate a new direction of research. On many occasions exercises and problems are provided with hints, references, and comments. In this way, many additional directions and topics are introduced. Here are two outstanding examples of old unsolved questions. Is it possible to construct in ZFC a non-discrete extremally disconnected topological group? Is it possible to construct in ZFC a countable non-metrizable topological group G such that G is a Fréchet–Urysohn space?

We would be grateful for the information on the progress of open problems posed in this book.

We hope that this book will achieve several goals. First, we believe that it can be used as a reasonably complete introduction to the theory of general topological groups beyond the limits of the class of locally compact groups. Second, we expect that it may lead advanced students to the very boundaries of modern topological algebra, providing them with goals and with powerful techniques (and maybe, with inspiration!). The exercise and problem sections can be especially useful in that respect. One can use this book in a research seminar on topological algebra (with an eye to unsolved problems) and also in advanced courses — at least four special courses can be arranged on the basis of this book. Fourth, we expect that the book will serve quite effectively as a reference, and will be helpful to mathematicians working in other domains of mathematics.

The standard reference book for general topology is R. Engelking's book *General Topology* [**165**]. We expect that the reader either knows the basic facts from general topology that we need, or that he/she will not find it too difficult to extract the corresponding information from [**165**].

We wish to express our deep gratitude to the second author's former students Constancio Hernández García and Yolanda Torres Falcón for their continued help in our work on this book over many years. We are also indebted to Richard G. Wilson whose comments enabled us to improve the text.

A. V. ARHANGEL'SKII, *M. G. TKACHENKO*
arhangel@math.ohiou.edu mich@xanum.uam.mx

February 21, 2008

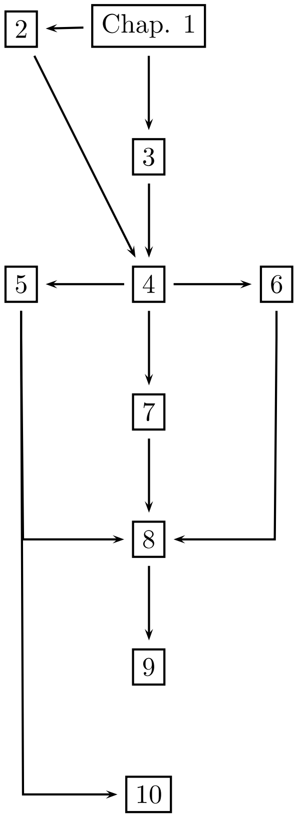

FIGURE 1. Logical dependence of chapters.

Contents

Chapter 1

Introduction to Topological Groups and Semigroups

Notation. We write $\mathbb{N}$ for the set of positive integers, ω for the set of non-negative integers, and $\mathbb{P}$ for the set of prime numbers. The set of all integers is denoted by $\mathbb{Z}$, the set of all real numbers is $\mathbb{R}$, and $\mathbb{Q}$ stands for the set of all rational numbers.

The symbols τ, λ, κ are used to denote infinite cardinal numbers. A cardinal number τ is also interpreted as the smallest ordinal number of cardinality τ. Each ordinal is the set of all smaller ordinals. Thus, ω is both the smallest infinite ordinal number and the smallest infinite cardinal number.

All topologies considered below are assumed to satisfy T_1-separation axiom, that is, we declare all one-point sets to be closed. The closed unit interval $[0, 1]$ of the real line $\mathbb{R}$, with its usual topology, is denoted by I, and Sq stands for the convergent sequence $\{1/n : n \in \mathbb{N}\} \cup \{0\}$ with its limit point 0, also taken with the usual topology. We use the symbol $\mathbb{C}$ to denote the complex plane with the usual sum and product operations, while $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ is the unit circle with center at the origin of $\mathbb{C}$.

1.1. Some algebraic concepts

In this section we establish the terminology and notation that will be used throughout the book.

In dealing with groups, we will adhere to the multiplicative notation for the binary group operation. In discussions involving a multiplicative group G, the symbol e will be reserved for the identity element of G.

We are very much concerned with groups in this course. For many purposes, however, it is natural and convenient considering semigroups. A *semigroup* is a non-void set S together with a mapping $(x, y) \to xy$ of $S \times S$ to S such that $x(yz) = (xy)z$ for all x, y, z in S. That is, a semigroup is a non-void set with an associative multiplication. Given an element x of a semigroup S, one inductively defines

$$x^2 = xx,\ x^3 = xx^2,\ \ldots,\ x^{n+1} = xx^n,$$

for every $n \in \mathbb{N}$. The associativity of multiplication in S implies the equality $x^n x^m = x^{n+m}$ for all $x \in S$ and $n, m \in \mathbb{N}$.

An element e of a semigroup S is called an *identity* for S if $ex = x = xe$ for every $x \in S$. Not every semigroup has an identity (see items 4) and 6) of Example 1.1.1). However, if a semigroup S has an identity, then it is easy to see that this identity is unique. Whenever

A. Arhangel'skii and M. Tkachenko, *Topological Groups and Related Structures*, Atlantis Studies in Mathematics 1, DOI 10.2991/978-94-91216-35-0_1, © 2008 Atlantis Press/World Scientific

we use the symbol e without explanation, it always stands for the identity of the semigroup under consideration.

A semigroup with identity is called *monoid*. An element a of a monoid M is said to be *invertible* if there exists an element b of M such that $ab = e = ba$. Note that if a is an invertible element of a monoid M, then the element $b \in M$ such that $ab = e = ba$ is unique. Indeed, suppose that $ab = e$, $ba = e$, $ac = e$, and $ca = e$. Then we have

$$c = ec = (ba)c = b(ac) = be = b.$$

This fact enables us to use notation a^{-1} for such an element b of M. We also say that b is the *inverse* of a. It is clear that $(a^{-1})^{-1} = a$ for each invertible element $a \in M$. Further, one can define negative powers of an invertible element $a \in M$ by the rule $a^{-n} = (a^{-1})^n$, for each $n \in \mathbb{N}$. It is a common convention to put $a^0 = e$. We leave to the reader a simple verification of the equality $a^n a^m = a^{n+m}$ which holds for all $n, m \in \mathbb{Z}$.

If every element a of a monoid M is invertible, then M is called a *group*.

Let S be a semigroup. For a fixed element $a \in S$, the mappings $x \mapsto ax$ and $x \mapsto xa$ of S to itself are called the *left* and *right actions* of a on S, and are denoted by λ_a and ϱ_a, respectively.

If G is a group, the mapping $x \mapsto x^{-1}$ of G onto itself is called *inversion*. Left and right actions of every element $a \in G$ on G are, in this case, bijections. They are called *left* and *right translations* of G by a.

EXAMPLE 1.1.1. Each of the following is a semigroup but not a group.

1) The set $\mathbb{Z}$ of all integers with the usual multiplication.
2) The set $\mathbb{Q}$ of all rational numbers with the usual multiplication.
3) The set $\mathbb{R}$ of all real numbers with the usual multiplication.
4) The set of all positive real numbers with the usual addition in the role of the product operation.
5) The set $\mathbb{N}$, in which the product of x and y is defined as $\max\{x, y\}$.
6) The set $\mathbb{N}$, in which the product of x and y is defined as $\min\{x, y\}$.
7) Any set S with $|S| > 1$, where the product xy is defined as y.
8) Any set S with $|S| > 1$, where the product xy is defined as x.
9) The set $S(X, X)$ of all mappings of a set X to itself with the composition of mappings in the role of multiplication, where $|X| > 1$. $\square$

In items 4) and 6) of the above example, the corresponding semigroups have no identity. The semigroups in 1)–3), 5), and 9) are monoids.

Now we present a few standard examples of groups.

EXAMPLE 1.1.2. Each of the following is a group:

1) The set $\mathbb{Z}$ of all integers with the usual addition in the role of multiplication.
2) The set $\mathbb{Q} \setminus \{0\}$ of all non-zero rational numbers with the usual multiplication.
3) The set $\mathbb{R} \setminus \{0\}$ of all non-zero real numbers with the usual multiplication.
4) The set of all positive real numbers with the usual multiplication.
5) The set $\{0, 1\}$ with the binary operation defined as follows:

$$0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 1 + 1 = 0.$$

This group is denoted by $\mathbb{Z}(2)$ or by D; it is called the *cyclic group* of two elements, or the *two-element group*. More generally, for an integer $n > 1$, let $\mathbb{Z}(n) = \{0, 1, \ldots, n-1\}$

be the set of all non-negative residues modulo n with addition modulo n. For example, $2 + (n - 1) = 1$ in $\mathbb{Z}(n)$; of course, n must be greater than or equal to 3 in order for 2 to be an element of $\mathbb{Z}(n)$. An easy verification shows that $\mathbb{Z}(n)$ with the addition just defined is a commutative group. It is called the *cyclic group of order* n.

6) The set $\mathbb{T}$ of all complex numbers z such that $|z| = 1$ with respect to the usual multiplication of complex numbers ($|z|$ denotes here the modulus of z).
7) The set of all n by n matrices, where the coefficients are real numbers, with non-zero determinant, and with the usual matrix multiplication. This group is called the *general linear group* of degree n over $\mathbb{R}$.
8) If X is any non-void set, then the set of all one-to-one mappings of X onto X forms a group $\mathcal{S}_X$ under the operation of composition. This group is called the *permutation group* on X. If X is finite and has n elements, then $\mathcal{S}_X$ is denoted by $\mathcal{S}_n$ and is called the *symmetric group* of degree n. □

A semigroup (monoid, group) S is called *Abelian* or *commutative* if $xy = yx$, for all $x, y \in S$. Clearly, the semigroups in items 7), 8), 9) of Example 1.1.1 and the groups in 7) of Example 1.1.2 (with $n \geq 2$ and $|X| \geq 3$, respectively) are not Abelian.

Let A and B be subsets of a semigroup G. Then AB denotes the set $\{ab : a \in A, b \in B\}$, and, if G is a group, A^{-1} denotes the set $\{a^{-1} : a \in A\}$. A subset A of a group G is called *symmetric* if $A^{-1} = A$.

We write aB for $\{a\}B$ and Ba for $B\{a\}$. We abbreviate AA as A^2, AAA as A^3, *etc.* Similarly, A^{-2} is a substitute for $A^{-1}A^{-1}$, *etc.*

A non-empty subset H of a semigroup S is called a *subsemigroup* of S if $xy \in H$, for all x, y in H. A non-empty subset H of a group G is called a *subgroup* of G if $xy^{-1} \in H$, for all x, y in H.

Clearly, a subset H of a group G is a subgroup of G if and only if for each $x, y \in H$, $xy \in H$ and $x^{-1} \in H$. Every group contains at least two subgroups — the whole group G and the subgroup consisting of the identity only. These subgroups are called *trivial*. Note that the empty set is not a group and, therefore, is not a subgroup of any group. Obviously, for any subgroup H of a group G we have $H^2 = HH = H$. However, in general, the same is not true for subsemigroups of semigroups.

In any group G, if $a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$. If H is any subgroup of G then, for any $a \in G$, $a^{-1}Ha$ is also a subgroup of G. If H is a subgroup of a group G such that $a^{-1}Ha = H$ for each $a \in G$, then H is said to be an *invariant* or *normal* subgroup of G. Since in Topology "normal" refers to a separation property of spaces, we will use the term "invariant" to denote this property of subgroups. Of course, in any Abelian group, every subgroup is invariant.

If H is a subgroup of a group G and $a \in G$, then the sets aH and Ha are called *left* and *right cosets* of H in G, respectively. The element a is a *representative* of both cosets.

For any two right cosets Ha and Hb, either they are disjoint or coincide. Furthermore, $Ha = Hb$ if and only if $ab^{-1} \in H$. Indeed, $ab^{-1} \in H$ implies that $Hab^{-1} \subset H^2 = H$. Hence, $Ha \subset Hb$. Similarly, since $(ab^{-1})^{-1} = ba^{-1} \in H$, it follows that $Hb \subset Ha$. Therefore, $Ha = Hb$. Conversely, if $Ha = Hb$, then $h_1a = h_2b$ for some $h_1, h_2 \in H$, whence $ab^{-1} = h_1^{-1}h_2 \in H$.

Let H be an invariant subgroup of a group G. Then $aH = Ha$ for each $a \in G$. In other words, the left cosets of H are the same as the right cosets of H. On the set of all cosets of

H we define multiplication by the rule $aHbH = abH$. It is easy to see that our definition of multiplication of cosets is correct. Indeed, suppose that $aH = a_1H$ and $bH = b_1H$ for some $a, a_1 \in G$ and $b, b_1 \in G$. Then $aa_1^{-1} \in H$ and $bb_1^{-1} \in H$ whence it follows, by the invariance of H in G, that

$$ab(a_1b_1)^{-1} = abb_1^{-1}a_1^{-1} \in aHa_1^{-1} = (aHa^{-1})aa_1^{-1} = Haa_1^{-1} = H.$$

Therefore, $aHbH = abH = a_1b_1H = a_1Hb_1H$, thus showing that the result of multiplication of two cosets does not depend on the choice of representatives in these cosets.

For each aH, we have that $(aH)H = (aH)(eH) = aH$ and $(a^{-1}H)(aH) = (a^{-1}a)H = eH = H$. This shows that H plays the role of the identity in the set of all cosets, and $a^{-1}H$ is the inverse of aH. Hence, the set of all cosets of H is a group with respect to the multiplication defined above. This group is called the *quotient group* of G and denoted by G/H. Note that if G is an Abelian group, then the quotient group G/H is defined for each subgroup H of G.

If G is a semigroup and H is a subsemigroup of S, then it may happen that, for some a and b in S, the sets aS and bS do not coincide and, nonetheless, are not disjoint.

We can also think of subgroups of semigroups. Let S be a semigroup. We will call G a *subgroup* of S if $G \subset S$ and G is a group under the restriction of the product operation in S to G.

Let S be a semigroup. An element x of S is called an *idempotent* if $xx = x$. The set of all idempotents of S is denoted by $E(S)$. Every idempotent of a group G coincides with the identity e of G. Indeed, if $x^2 = x$ for some $x \in G$, then $x^2x^{-1} = xx^{-1} = e$, that is, $x = e$.

EXAMPLE 1.1.3. Let X be a non-empty set. Then the idempotents of the semigroup $S(X, X)$ of all mappings of X to itself are precisely the mappings $f \colon X \to X$ satisfying the condition $f(x) = x$ for every $x \in f(X)$. □

Now we give several definitions and present some special results on groups which will be used in the sequel.

A *homomorphism* of a semigroup (monoid, group) G to a semigroup (monoid, group) F is a mapping $f \colon G \to F$ such that $f(ab) = f(a)f(b)$ for all $a, b \in G$. Given a homomorphism of monoids $f \colon G \to H$, the set $\{x \in G : f(x) = e_H\}$ is called the *kernel* of f and denoted by $\ker f$. It follows immediately from the definition that $\ker f$ is a subsemigroup of G.

A homomorphism of a semigroup (monoid, group) G onto a semigroup (monoid, group) F which is a one-to-one mapping is called an *isomorphism*.

If G and H are monoids with respective identities e_G and e_H and $f \colon G \to H$ is a homomorphism onto H, then $f(e_G) = e_H$. Indeed, put $h = f(e_G)$ and for an arbitrary element $b \in H$, take $a \in G$ with $f(a) = b$. Then $bh = f(ae_G) = f(a) = b$ and $hb = f(e_Ga) = f(a) = b$. Since the identity of a monoid is unique, we infer that $h = e_H$.

If G and H are groups, then the equality $f(e_G) = e_H$ holds for every homomorphism f of G to H. Indeed, the above argument gives the equality $bh = b$ for an arbitrary element $b \in f(G)$, where $h = f(e_G)$. Since H is a group, we have that $b^{-1}bh = b^{-1}b = e_H$ and, hence, $h = e_Hh = e_H$.

Furthermore, the kernel of f is a subgroup of the group G. For every $a \in \ker f$, we have that $e_H = f(e_G) = f(aa^{-1}) = f(a)f(a^{-1}) = f(a^{-1})$, whence it follows that $a^{-1} \in \ker f$. Since $\ker f$ is a subsemigroup of G, it must be a subgroup of G.

An isomorphism of a group G onto itself is called an *automorphism* of G.

EXAMPLE 1.1.4. Let $Aut(G)$ be the set of all automorphisms of a group G with the operation of composition, $(g \circ f)(x) = g(f(x))$ for all $f, g \in Aut(G)$ and $x \in G$. Evidently, $Aut(G)$ is a group. The group $Aut(G)$ need not be commutative, even if G is commutative.

There exists a natural homomorphism φ of G onto a subgroup of $Aut(G)$ defined as follows. For arbitrary $a, x \in G$, put $\varphi_a(x) = axa^{-1}$. It is clear that

$$\varphi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y)$$

for all $x, y \in G$, so φ_a is a homomorphism of G to G. For an element $y \in G$, put $x = a^{-1}ya$. Then $\varphi_a(x) = y$ and, therefore, $\varphi_a(G) = G$. One easily verifies that the mapping φ_a is one-to-one, so it is an automorphism of G. The correspondence $a \mapsto \varphi_a$ is the homomorphism φ of G to $Aut(G)$ we are looking for. Indeed,

$$(\varphi_a \circ \varphi_b)(x) = \varphi_a(\varphi_b(x)) = \varphi_a(bxb^{-1}) = abxb^{-1}a^{-1} = \varphi_{ab}(x)$$

for all $a, b, x \in G$. Therefore, $\varphi_a \circ \varphi_b = \varphi_{ab}$ or, equivalently, $\varphi(ab) = \varphi(a) \circ \varphi(b)$.

The automorphisms φ_a of G, with $a \in G$, are called *inner automorphisms.* If the group G is Abelian, then φ_a is the identity mapping of G for each $a \in G$. In other words, $\ker \varphi$ coincides with the group G in this case. In general, the kernel of φ coincides with the *center* $Z(G)$ of G defined by $Z(G) = \{a \in G : ax = xa \text{ for all } x \in G\}$. $\square$

Given a subgroup H of a group G with identity e, we say that H is a *central subgroup* of G if $H \subset Z(G)$, that is, $hx = xh$ for all $h \in H$ and $x \in G$. An element a of G is said to be an element *of finite order* or, equivalently, a *torsion element* if $a^n = e$, for some $n \in \mathbb{N}$. If this is the case, then the smallest $n \in \mathbb{N}$ for which $a^n = e$ is called the *order* of a and is denoted by $o(a)$. If all elements of G have finite orders, we say that G is a *torsion group*. If the group G has no elements of finite order, except for e, then it is called *torsion-free.*

The *cyclic subgroup* of G generated by an element $a \in G$ is the set $\{a^k : k \in \mathbb{Z}\}$. This subgroup is also denoted by $\langle a \rangle$. Every cyclic group is evidently commutative. If $a \in G$ is a torsion element and $o(a) = n$, then the cyclic subgroup $\langle a \rangle$ has exactly n elements or, more precisely, $\langle a \rangle = \{a^k : 1 \le k \le n\}$. The set of all elements $a \in G$ of finite order is called the *torsion part* of G and is denoted by $tor(G)$. If the group G is commutative, the torsion part $tor(G)$ is a subgroup of G. Indeed, if $x, y \in tor(G)$, there exist integers $m, n \in \mathbb{N}$ such that $x^m = e$ and $y^n = e$. Set $N = mn$. Since G is commutative, it follows that $(xy)^N = x^N y^N = (x^m)^n (y^n)^m = e^n e^m = e$, whence $xy \in tor(G)$. Similarly, $(x^{-1})^m = (x^m)^{-1} = e^{-1} = e$. If G is commutative, we will call $tor(G)$ the *torsion subgroup* of G.

Suppose that A is a non-empty subset of a semigroup S. Then $\langle A \rangle$ denotes the smallest subsemigroup of S which contains the set A. It is clear that every element $b \in \langle A \rangle$ has the form $b = a_1 \dots a_n$, where $a_1, \dots, a_n$ are arbitrary elements of A. If A is a non-empty subset of a group G, we use the same symbol $\langle A \rangle$ to denote the smallest subgroup of G that contains A. Similarly, every element $g \in \langle A \rangle$ has the form $g = a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n}$ for some $a_1, \dots, a_n \in A$ and $\varepsilon_1, \dots, \varepsilon_n = \pm 1$, where n is an arbitrary positive integer. Therefore, the cyclic subgroup $\langle a \rangle$ of G is generated by the one-point set $\{a\}$.

In the next lemma we give a necessary and sufficient condition for a homomorphism defined on a subgroup of an Abelian group to admit an extension over a bigger subgroup.

LEMMA 1.1.5. *Let H be a subgroup of an Abelian group G, f a homomorphism of H to an Abelian group F, and let $x \in G$ and $y \in F$. Define a number $m \in \mathbb{N}^* = \mathbb{N} \cup \{\infty\}$ by $m = \min\{n \in \mathbb{N}^* : nx \in H\}$ (thus, $m = \infty$ if $nx \notin H$ for each $n \in \mathbb{N}$). Then f admits an extension to a homomorphism $h\colon \langle H \cup \{x\}\rangle \to F$ satisfying $h(x) = y$ if and only if either $m = \infty$ or $m \in \mathbb{N}$ and $my = f(mx)$.*

PROOF. Necessity is evident, so we only prove sufficiency. Let $H_0 = \langle H \cup \{x\}\rangle$. It suffices to consider the following two cases.

Case 1. $m = \infty$. Then kx is not in H for each $k \in \mathbb{N}$, so every element $z \in H_0$ has a unique representation in the form $z = kx + a$ with $k \in \mathbb{Z}$ and $a \in H$. Put $h(kx + a) = ky + f(a)$ for all $k \in \mathbb{Z}$ and $a \in H$. This defines a mapping $h\colon H_0 \to F$. If $z_1 = kx + a$ and $z_2 = lx + b$ are two elements of H_0, then $h(z_1 + z_2) = (k + l)y + f(a + b) = h(z_1) + h(z_2)$, so h is a homomorphism.

Case 2. $m \in \mathbb{N}$. Then $mx \in H$, by the definition of m. Put $h(x) = y$ and, more generally, $h(kx + a) = ky + f(a)$ for all $k \in \mathbb{Z}$ and $a \in H$. Let us verify that the mapping $h\colon H_0 \to F$ is correctly defined. Indeed, suppose that $kx + a = lx + b$ for some $k, l \in \mathbb{Z}$ and $a, b \in H$. Then $(k - l)x = b - a \in H$, so m divides $k - l$ by our choice of m. Hence $k - l = mp$, for some $p \in \mathbb{Z}$. It follows that

$$(ky + f(a)) - (ly + f(b)) = (k - l)y - f(b - a) = mpy - f(mpx) = 0,$$

or, in other words, $h(kx + a) = h(ly + b)$. Thus, the value $h(kx + a)$ does not depend on the choice of $k \in \mathbb{Z}$ and $a \in H$.

One easily verifies that, in either case, h is a homomorphism of H_0 to F that extends f. □

A group G is said to be *divisible* if $G^n = G$ for each $n \in \mathbb{N}$. In other words, given $x \in G$ and $n \in \mathbb{N}$, there is an element $y \in G$ such that $y^n = x$. The group $\mathbb{T}$ of complex numbers $z \in \mathbb{C}$ with $|z| = 1$ is, obviously, divisible. The additive group of real numbers is also a divisible group. On the other hand, the group $\mathbb{Z}(2) = \{0, 1\}$ is not divisible. A fundamental property of divisible groups is the following one.

THEOREM 1.1.6. *Let H be a subgroup of an Abelian group G. Then every homomorphism f of H to any divisible group F can be extended to a homomorphism of G to F.*

PROOF. We argue with the aim to use Zorn's lemma. Denote by $\mathcal{P}$ the family of the pairs (K, g) such that K is a subgroup of G containing H and $g\colon K \to F$ a homomorphism such that the restriction of g to H coincides with f. Given two elements (K, g) and (K_1, g_1) in $\mathcal{P}$, we put $(K, g) \le (K_1, g_1)$ if $K \subset K_1$ and g_1 extends g. This gives us a partially ordered set $(\mathcal{P}, \le)$. Suppose that $\mathcal{C} \subset \mathcal{P}$ is a *chain* in $\mathcal{P}$, that is, a subset of $\mathcal{P}$ linearly ordered by the order $\le$ of $\mathcal{P}$. Put

$$P^* = \bigcup\{P : (P, g) \in \mathcal{C} \text{ for some homomorphism } g\colon P \to F\}$$

and define a mapping $g^*\colon P^* \to F$ by the rule $g^*(x) = g(x)$, where $x \in P$ and $(P, g) \in \mathcal{C}$. Since $\mathcal{C}$ is a chain in $(\mathcal{P}, \le)$, it follows that P^* is a subgroup of G, $H \subset P^*$, and g^* is a homomorphism of P^* to F. If follows from the definition of (P^*, g^*) that $(P, g) \le (P^*, g^*)$ for each $(P, g) \in \mathcal{C}$. We have proved that every chain in $(\mathcal{P}, \le)$ has an upper bound in $(\mathcal{P}, \le)$.

Therefore, by Zorn's lemma, the partially ordered set $(\mathcal{P}, \leq)$ has a maximal element (K, h). It remains to verify that $K = G$. Suppose to the contrary that $K \neq G$ and choose an element $a \in G \setminus K$. Since F is divisible, Lemma 1.1.5 guarantees the existence of a homomorphism $h_0 \colon K_0 \to F$ extending h, where $K_0 = \langle K \cup \{a\} \rangle$. It is clear that $(K, h) < (K_0, h_0)$ and that $(K_0, h_0) \in \mathcal{P}$. This contradicts the maximality of (K, h) and finishes the proof. $\square$

PROPOSITION 1.1.7. *Let G be any group, and b any element of G distinct from the identity e of G. Then there exists a cyclic subgroup H of G containing b and isomorphic to a subgroup of the circle group $\mathbb{T}$.*

PROOF. Let us consider two cases.

Case 1. b is of finite order. Let p be the order of b. Put $\varphi = 2\pi/p$, and $a = \cos\varphi + i \sin\varphi$. Then $a \in \mathbb{T}$, and the order of a in the group $\mathbb{T}$ is p. Put $H = \langle b \rangle$, $K = \langle a \rangle$, and $g(b^n) = a^n$, for each $n = 1, \ldots, p$. Then H is a subgroup of G containing b, K is a subgroup of $\mathbb{T}$, and g is an isomorphism of H onto K.

Case 2. b is not of finite order. There exists φ such that $0 < \varphi < \pi$ and for any pair $(n, k) \in \mathbb{N} \times \mathbb{N}$, $n\varphi$ is not equal to $2k\pi$. Put $a = \cos\varphi + i \sin\varphi$ and $g(b^n) = a^n$, for each $n \in \mathbb{Z}$. Then g is an isomorphism of the subgroup $H = \langle b \rangle$ of G onto the subgroup $K = \langle a \rangle$ of $\mathbb{T}$, and $b \in H$. $\square$

From Theorem 1.1.6 and Proposition 1.1.7 we obtain:

COROLLARY 1.1.8. *For any Abelian group G, and any element a of G distinct from the identity e of G, there exists a homomorphism g of G to the circle group $\mathbb{T}$ such that $g(a) \neq 1$.*

PROOF. By Proposition 1.1.7, there exists a subgroup H of G which contains a and is isomorphic to a subgroup K of $\mathbb{T}$. Fix an isomorphism f of H onto K. Clearly, $f(a) \neq 1$. It remains to apply Theorem 1.1.6. $\square$

To finish this section we present two interesting and important examples of groups the first of which is called the *group of quaternions* and the second one is the group of *r-adic numbers*. In fact, the group of quaternions has a richer structure. Here are the necessary definitions.

A non-empty set S with two binary operations $+$ and $\cdot$ called *addition* and *multiplication*, respectively, is said to be a *ring* if the following conditions are satisfied:

(R1) $(S, +)$ is a commutative group;
(R2) $(S, \cdot)$ is a monoid;
(R3) $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$ for all $x, y, z \in S$.

Condition (R3) expresses the distributive law that relates addition and multiplication in S. It is common practice to abbreviate $(S, +, \cdot)$ simply as S when there is no confusion with the operations in S. Let 0 and 1 be neutral elements of the group $(S, +)$ and monoid $(S, \cdot)$, respectively. We leave to the reader the simple verification of the equality $0 \cdot x = x \cdot 0 = 0$, which holds for each $x \in S$. Notice that if $0 = 1$, then S contains only the element 0.

If the multiplication in a ring S is commutative, then the ring is called *commutative.* A ring S in which $0 \neq 1$ and every non-zero element $x \in S$ is invertible with respect to multiplication is called a *skew field.* A commutative skew field is a *field.*

Clearly, $\mathbb{R}$ and $\mathbb{C}$ are fields when considered with their usual addition and multiplication. The set $M(n,\mathbb{R})$ of all n by n matrices with real entries and the usual matrix addition and multiplication is a non-commutative ring, for each $n > 1$. The set $P[x_1,\dots,x_n]$ of all polynomials of mutually commuting variables $x_1,\dots,x_n$ with real coefficients and the usual sum and multiplication is an example of a commutative ring. For every integer $r > 1$, the set $\mathbb{Z}(r)$ of non-negative residues modulo r with addition and multiplication modulo r is another example of a commutative ring (we noted in item 5) of Example 1.1.2 that $\mathbb{Z}(r)$ is a commutative group with respect to addition). It is well known (and easy to verify) that $\mathbb{Z}(r)$ is a field if and only if the number r is prime. Yet another example of a commutative ring is the set $\mathbb{R}^X$ of all real-valued functions on a non-empty set X, with the pointwise operations of addition and multiplication of functions.

A non-trivial example of a skew field is presented below.

EXAMPLE 1.1.9. Denote by $\mathbf{Q}$ the set of all linear combinations $q = a + \mathbf{i}b + \mathbf{j}c + \mathbf{k}d$, where a, b, c, d are real numbers and $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are special symbols satisfying the equalities $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$, $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$, $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$. We introduce the usual coordinatewise addition in $\mathbf{Q}$ by the rule

$$[a + \mathbf{i}b + \mathbf{j}c + \mathbf{k}d] + [a' + \mathbf{i}b' + \mathbf{j}c' + \mathbf{k}d'] = (a + a') + \mathbf{i}(b + b') + \mathbf{j}(c + c') + \mathbf{k}(d + d').$$

With this addition, $\mathbf{Q}$ is a commutative group called the *additive group of quaternions*.

The product of two quaternions $q = a + \mathbf{i}b + \mathbf{j}c + \mathbf{k}d$ and $q' = a' + \mathbf{i}b' + \mathbf{j}c' + \mathbf{k}d'$ is formed by multiplying out the formal linear polynomials and applying the above equalities and the commutativity rules $x\mathbf{i} = \mathbf{i}x$, $x\mathbf{j} = \mathbf{j}x$, $x\mathbf{k} = \mathbf{k}x$ for each $x \in \mathbb{R}$:

$$\begin{aligned}(a + \mathbf{i}b + \mathbf{j}c + \mathbf{k}d)(a' + \mathbf{i}b' + \mathbf{j}c' + \mathbf{k}d') = {} & (aa' - bb' - cc' - dd') \\ & + \mathbf{i}(ab' + ba' + cd' - dc') \\ & + \mathbf{j}(ac' - bd' + ca' + db') \\ & + \mathbf{k}(ad' + bc' - cb' + da').\end{aligned}$$

We leave to the reader the routine verification of the fact that the multiplication in $\mathbf{Q}$ is associative. It is clear that $\mathbf{Q}$ has the neutral element $\mathbf{1} = 1 + \mathbf{i}0 + \mathbf{j}0 + \mathbf{k}0$ with respect to multiplication, so $(\mathbf{Q}, \cdot)$ is a non-commutative monoid. In addition, the sum and multiplication in $\mathbf{Q}$ satisfy the distributive law, whence it follows that $\mathbf{Q}$ is a non-commutative ring.

Let $\mathbf{Q}^* = \mathbf{Q} \setminus \{\mathbf{0}\}$, where $\mathbf{0} = 0 + \mathbf{i}0 + \mathbf{j}0 + \mathbf{k}0$ is the *zero element* of $\mathbf{Q}$. It turns out that every non-zero element $q \in \mathbf{Q}$ is invertible. Indeed, for $q = a + \mathbf{i}b + \mathbf{j}c + \mathbf{k}d$, put $\bar{q} = a - \mathbf{i}b - \mathbf{j}c - \mathbf{k}d$. An easy calculation shows that $q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2$. Therefore, if $q \neq \mathbf{0}$, then $r = \bar{q}\alpha$ is an inverse of q, where $\alpha = 1/(a^2 + b^2 + c^2 + d^2)$. Since $\mathbf{Q}$ is a monoid, the inverse of q is unique, and $\mathbf{Q}^*$ is a multiplicative group. It follows that $\mathbf{Q}$ is a skew field. Sometimes $\mathbf{Q}^*$ is called the *multiplicative group of quaternions*. Notice that $U = \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ is a subgroup of $\mathbf{Q}^*$ called the *group of quaternion units*. □

In the following example we construct, for every integer $r > 1$, the additive group Ω_r of r-adic numbers. Later on, we shall define multiplication in Ω_r, thus making the group Ω_r into a commutative ring (see Example 3.1.31).

EXAMPLE 1.1.10. Let r be an integer with $r > 1$. Denote by A the set $\{0, 1, \dots, r-1\}$ and consider the Cartesian product $P = A^{\mathbb{Z}}$ of infinitely many copies of the set A enumerated by the integers. In other words, P consists of the sequences $\mathbf{x} = (\dots, x_{n-1}, x_n, x_{n+1}, \dots)$ infinite in both sides, where $x_n \in A$ for each $n \in \mathbb{Z}$. Let Ω_r be the subset of P formed by all sequences $\mathbf{x}$ such that $x_n = 0$ for all $n < k$, where k is an integer depending upon $\mathbf{x}$.

Our aim is to define addition in Ω_r which, in a sense, mimics the decomposition of a natural number M into powers of r. More precisely, every $M \in \mathbb{N}$ can be represented in the polynomial form

$$M = x_0 + x_1 r + x_2 r^2 + \cdots + x_m r^m, \tag{1.1}$$

where $x_0, x_1, x_2, \dots, x_m \in A$, $x_m \neq 0$ and $m \in \omega$. It is easy to verify that such a representation of M is unique. This gives us a bijection between $\mathbb{N}$ and all finite sequences $\mathbf{x} = (x_0, x_1, x_2, \dots, x_m)$ such that $x_i \in A$ for each $i \le m$ and $x_m \neq 0$.

Suppose that for a positive integer N, we have a decomposition

$$N = y_0 + y_1 r + y_2 r^2 + \cdots + y_n r^n \tag{1.2}$$

similar to (1.1). Then the number $M + N$ can also be decomposed into powers of r, and the coefficients of the corresponding decomposition admit an explicit expression in terms of x_i and y_i. Indeed, let

$$M + N = z_0 + z_1 r + z_2 r^2 + \cdots + z_k r^k, \tag{1.3}$$

where $z_0, z_1, \dots, z_k \in A$, $z_k \neq 0$ and $k \in \omega$. It follows from (1.1), (1.2) and (1.3) that $x_0 + y_0 = z_0 + t_0 r$, where t_0 is either 0 or 1. Clearly, $t_0 = 1$ iff $x_0 + y_0 \ge r$, so that z_0 is the least non-negative residue of $x_0 + y_0$ modulo r. Again, we apply (1.1)–(1.3) and the above equality $x_0 + y_0 = z_0 + t_0 r$ to deduce that $z_1 r + r^2 P = (x_1 + y_1 + t_0) r + r^2 Q$ for some non-negative integers P and Q. Therefore, $x_1 + y_1 + t_0 = z_1 + t_1 r$, where $t_1 = P - Q$. Since $0 \le x_1 + y_1 + t_0 \le 2(r-1) + 1 < 2r$ and $z_1 \ge 0$, it follows that t_1 is either 0 or 1, and that z_1 is the least non-negative residue of $x_1 + y_1 + t_0$ modulo r.

Suppose that we have defined $z_0, z_1, \dots, z_s \in A$ and $t_0, t_1, \dots, t_s \in \{0, 1\}$ for some integer $s \ge 1$ such that the equality $z_i + t_i r = x_i + y_i + t_{i-1}$ holds for each $i = 0, 1, \dots, s$ (where $t_{-1} = 0$). Taking the sum of (1.1) and (1.2) compared with (1.3) and using the above equalities with $i = 0, 1, \dots, s$, we obtain that

$$x_{s+1} + y_{s+1} + t_s = z_{s+1} + t_{s+1} r, \tag{1.4}$$

where $z_{s+1} \in A$ and t_{s+1} is either 0 or 1. It is clear that the integer k in the equality (1.3) that determines the expansion of $M + N$ satisfies $k \le \max\{m, n\} + 1$. Summing up, the equalities (1.4), together with $x_0 + y_0 = z_0 + t_0 r$, enable us to define inductively the numbers $z_0, z_1, \dots, z_k \in A$ satisfying (1.3) in terms of x_i and y_i.

We are now in position to give a formal definition of the addition in Ω_r which is based on the equalities (1.4). Denote by $\mathbf{0}$ the zero sequence in Ω_r each element of which is zero. First, we set $\mathbf{x} + \mathbf{0} = \mathbf{x}$ and $\mathbf{0} + \mathbf{x} = \mathbf{x}$ for each $\mathbf{x} \in \Omega_r$. Let $\mathbf{x} = (x_n)$ and $\mathbf{y} = (y_n)$ be arbitrary elements of Ω_r, both distinct from $\mathbf{0}$. Choose integers m_0 and n_0 such that $x_{m_0} \neq 0$ and $x_n = 0$ if $n < m_0$ and, similarly, $y_{n_0} \neq 0$ and $y_n = 0$ if $n < n_0$. Set $k_0 = \min\{m_0, n_0\}$. We define a sequence $\mathbf{z} = (z_n) \in \Omega_r$ as follows. First, we choose $z_{k_0} \in A$ and $t_{k_0} \in \{0, 1\}$ satisfying $x_{k_0} + y_{k_0} = z_{k_0} + t_{k_0} r$. Clearly, the numbers z_{k_0} and t_{k_0} are uniquely defined by this equality and the restrictions on them. Suppose that $z_{k_0}, z_{k_0+1}, \dots, z_k$ and $t_{k_0}, t_{k_0+1}, \dots, t_k$ have been defined for some integer $k \ge k_0$. Then we choose $z_{k+1} \in A$ and $t_{k+1} \in \{0, 1\}$ satisfying $x_{k+1} + y_{k+1} + t_k = z_{k+1} + t_{k+1} r$. Again, such a choice is always possible and is unique. This inductive procedure defines a sequence $\mathbf{z} = (z_n) \in \Omega_r$, where $z_n = 0$ if $n < k_0$. It remains to put $\mathbf{x} + \mathbf{y} = \mathbf{z}$. This finishes our definition of addition in Ω_r.

It turns out that the set Ω_r with the addition just defined is a commutative group called the *group of r-adic numbers.* Indeed, it is clear from the above definition and the commutativity of the addition in $\mathbb{Z}$ that $\mathbf{x}+\mathbf{y} = \mathbf{y}+\mathbf{x}$ and that $\mathbf{x}+\mathbf{0} = \mathbf{x}$ for all $\mathbf{x}, \mathbf{y} \in \Omega_r$. Given an arbitrary non-zero element $\mathbf{x} = (x_n)$ in Ω_r, we define an element $\mathbf{y} \in \Omega_r$ as follows. Suppose that $x_m \neq 0$ and $x_n = 0$ for each $n < m$. Set $y_n = 0$ if $n < m$, $y_m = r - x_m$, and $y_n = r - x_n - 1$ if $n > m$. Then the element $\mathbf{y} = (y_n) \in \Omega_r$ satisfies $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x} = \mathbf{0}$.

It remains to verify that the addition in Ω_r is an associative operation. Let $\mathbf{x}, \mathbf{y}, \mathbf{z}$ be arbitrary elements of Ω_r and suppose that at least one of them is different from $\mathbf{0}$. Take the least integer m such that one of the values x_m, y_m, z_m is distinct from zero. Then $x_n = y_n = z_n = 0$ for each $n < m$ and it is clear that the values of $(\mathbf{x}+\mathbf{y})+\mathbf{z}$ and $\mathbf{x}+(\mathbf{y}+\mathbf{z})$ at the index n are equal to zero, for each $n < m$. To show that the values of the two elements coincide at every index $n \geq m$, we argue as follows. Let Σ_m be the set of all elements $\mathbf{t} \in \Omega_r$ such that $t_n = 0$ if $n < m$ and only finitely many values t_n with $n \geq m$ are distinct from zero. Consider the mapping φ of Σ_m to the set of non-negative integers defined by the rule

$$\varphi(\mathbf{t}) = t_m + t_{m+1} r + t_{m+2} r^2 + \cdots .$$

Since $\mathbf{t}$ is in Σ_m, the above sum is finite. It follows from our definition of the addition in Ω_r that φ has the property $\varphi(\mathbf{x} + \mathbf{y}) = \varphi(\mathbf{x}) + \varphi(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \Sigma_m$. Informally speaking, φ preserves addition or, equivalently, φ is a homomorphism of Σ_m onto the additive semigroup of non-negative integers. It is also clear that $\varphi(\mathbf{t}) = 0$ iff $\mathbf{t} = \mathbf{0}$. It follows that φ is a bijection preserving operation. Since addition of integers is associative, the same is true for addition in Σ_m. Finally, we return back to the elements $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \Omega_r$ considered above. For any index $k \geq m$, consider the "truncated" elements $\mathbf{x}', \mathbf{y}', \mathbf{z}'$ coinciding with $\mathbf{x}, \mathbf{y}, \mathbf{z}$, respectively, at every index $n \leq k$, and whose values are equal to zero for each index $n > k$. Then $\mathbf{x}', \mathbf{y}', \mathbf{z}'$ are elements of Σ_m, whence it follows that $(\mathbf{x}' + \mathbf{y}') + \mathbf{z}' = \mathbf{x}' + (\mathbf{y}' + \mathbf{z}')$. Evidently, the values of the elements $(\mathbf{x}' + \mathbf{y}') + \mathbf{z}'$ and $(\mathbf{x} + \mathbf{y}) + \mathbf{z}$ at the index k coincide, and the same is valid for the elements $\mathbf{x}' + (\mathbf{y}' + \mathbf{z}')$ and $\mathbf{x} + (\mathbf{y} + \mathbf{z})$. Since $k \geq m$ is arbitrary, we conclude that $(\mathbf{x} + \mathbf{y}) + \mathbf{z} = \mathbf{x} + (\mathbf{y} + \mathbf{z})$. Therefore, the addition in Ω_r is associative and Ω_r is a commutative group with neutral element $\mathbf{0}$.

Denote by $\mathbb{Z}_r$ the set of all elements $\mathbf{x} \in \Omega_r$ such that $x_n = 0$ for each $n < 0$. Omitting the values of $\mathbf{x}$ at negative indices, we may rewrite every element $\mathbf{x} \in \mathbb{Z}_r$ as $\mathbf{x} = (x_0, x_1, x_2, \ldots)$, thus identifying $\mathbb{Z}_r$ with the corresponding subset of A^ω. We leave to the reader a simple verification of the fact that $\mathbb{Z}_r$ is a subgroup of the additive group Ω_r. We will call $\mathbb{Z}_r$ the *group of r-adic integers.* $\square$

Exercises

1.1.a. Prove that if H is a subgroup of a group G, then, for any $a \in G$, $a^{-1}Ha$ is also a subgroup of G.

1.1.b. Verify that for every Abelian group G and every $n \in \mathbb{N}$, the set $G[n] = \{x \in G : nx = 0_G\}$ is a subgroup of G.

1.1.c. Let H be a subgroup of a group G such that $G = H \cup aH$, for some $a \in G$. Show that H is an invariant subgroup of G.

1.1.d. Let $r > 1$ be an integer and G a torsion group such that for every element $x \in G$, the order $o(x)$ of x and the number r are mutually prime. Prove that the mapping $\varphi_r \colon G \to G$ defined by $\varphi_r(x) = x^r$ is a bijection of G onto G. Show that φ_r is a homomorphism if the group G is commutative.

1.1.e. Let G be an Abelian torsion group. Verify that every finite subset A of G generates a finite subgroup $\langle A\rangle$ of G. Show that the conclusion is no longer valid for non-commutative groups.

1.1.f. Give an example of an infinite Abelian group all proper subgroups of which are finite.

1.1.g. Give an example of a semigroup G and a subsemigroup S of G such that, for some a and b in G, the sets aS and bS do not coincide and are not disjoint.

1.1.h. Does Theorem 1.1.6 remain valid if we drop the assumption that the group G is Abelian?

1.1.i. Give an example of a semigroup G such that $\varnothing = \bigcap_{n=1}^{\infty} G^n$.

1.1.j. For every quaternion $q = a+\mathbf{i}b+\mathbf{j}c+\mathbf{k}d$ (see Example 1.1.9), put $|q| = \sqrt{a^2 + b^2 + c^2 + d^2}$. Show that the set $\{q \in \mathbf{Q} : |q| = 1\}$ is a subgroup of $\mathbf{Q}^*$.

1.1.k. Let Ω_r be the group of r-adic numbers defined in Example 1.1.10, where $r > 1$.

(a) Verify that the "multiplication" of a non-zero element $\mathbf{x} \in \Omega_r$ by r moves every value x_k of $\mathbf{x}$ to the next position on the right. In other words, if m is the least integer such that $x_m \neq 0$, then the values y_n of the element $\mathbf{y} = r\mathbf{x}$ satisfy $y_n = 0$ for each $n \leq m$ and $y_{n+1} = x_n$ for $n \geq m$. Deduce that the mapping φ_r of Ω_r to Ω_r defined by $\varphi_r(\mathbf{x}) = r\mathbf{x}$ is an isomorphism of Ω_r onto itself.

(b) Use a) to solve the equation $2x = \mathbf{a}$ in the group Ω_6, where $\mathbf{a} = (\dots, 0, \dots, 0, 1, 1, 1, \dots)$ is an element of the subgroup $\mathbb{Z}_6$ of Ω_6 with $a_0 = 1$.

Problems

1.1.A. Show that the solutions of the equation $X^2 = E_2$ in the multiplicative group $GL(2, \mathbb{R})$ of all invertible 2 by 2 matrices with real entries do not form a subgroup of the group $GL(2, \mathbb{R})$, where E_2 is the identity matrix (i.e., the neutral element of $GL(2, \mathbb{R})$). Deduce that the conclusion in Exercise 1.1.b is no longer valid in the non-Abelian case.

1.1.B. Let $\mathbf{Q}^*$ be the multiplicative group of non-zero quaternions.

(a) Verify that the solutions of the equation $q^2 = \mathbf{1}$ in $\mathbf{Q}$ form a two-element subgroup of $\mathbf{Q}^*$.

(b) Show that the solutions of the equation $q^2 = -\mathbf{1}$ in $\mathbf{Q}$ can be naturally identified with the points of the unit sphere in $\mathbb{R}^3$.

(c) How many solutions does the equation $q^3 = \mathbf{1}$ have in $\mathbf{Q}$? Does the set of solutions form a submonoid of $\mathbf{Q}$?

1.1.C. If G is a group and $a, b \in G$, then the element $[a, b] = aba^{-1}b^{-1}$ of G is called the *commutator* of a and b. Is the set $\{[x, y] : x, y \in G\}$ a subgroup (submonoid) of G?

1.1.D. How many subgroups does the symmetric group S_4 contain (see item 8) of Example 1.1.2)? How many of them are invariant in S_4?

1.1.E. Let H be an invariant subgroup of a group G and K an invariant subgroup of H. Is K then invariant in G?

1.1.F. Let r and k be mutually prime natural numbers, where $r > 1$. Prove that for every element $\mathbf{a}$ of the group $\mathbb{Z}_r$ of r-adic integers defined in Example 1.1.10, the equation $k\mathbf{x} = \mathbf{a}$ has a solution in $\mathbb{Z}_r$. Deduce that the group Ω_r is divisible, for each r.

Hint. To prove the first assertion, take any $\mathbf{a} = (a_n)_{n\in\omega}$ in $\mathbb{Z}_r$, and define by induction on $n \in \omega$ an element $\mathbf{x} = (x_n)_{n\in\omega}$ in $\mathbb{Z}_r$ and a function $t \colon \omega \to \{0, 1\}$ such that $kx_0 \equiv a_0 \pmod r$ and $kx_{n+1} + t(n) \equiv a_{n+1} \pmod r$ for each $n \geq 0$. To guarantee the existence of solutions $x_0, x_1, \dots$ of the congruences, apply the conclusion of Example 1.1.d to the cyclic group $\mathbb{Z}(r)$. The second assertion of the problem follows from the first one if one applies Exercise 1.1.k.

1.1.G. The construction of the group Ω_r of r-adic numbers described in Example 1.1.10 admits a natural generalization as follows. First, we fix an element $\mathbf{a} = (\ldots, a_{-1}, a_0, a_1, \ldots)$ of $\mathbb{N}^{\mathbb{Z}}$ such that $a_n \geq 2$, for each $n \in \mathbb{Z}$. For every $n \in \mathbb{Z}$, put $A_n = \{0, 1, \ldots, a_n - 1\}$, and consider the product $\Pi = \prod_{n\in\mathbb{Z}} A_n$. Denote by $\Omega_{\mathbf{a}}$ the set of all elements $\mathbf{x} = (\ldots, x_{-1}, x_0, x_1, \ldots)$ of Π such that $x_n = 0$ for each $n < n_0$, where $n_0 \in \mathbb{Z}$ depends on $\mathbf{x}$. Given two elements $\mathbf{x} = (x_n)$ and $\mathbf{y} = (y_n)$ of $\Omega_{\mathbf{a}}$, we define by induction an element $\mathbf{x} + \mathbf{y} = \mathbf{z} = (z_n) \in \Omega_{\mathbf{a}}$ as follows. If $\mathbf{x}$ (or $\mathbf{y}$) contains only zero entries, put $\mathbf{z} = \mathbf{y}$ ($\mathbf{z} = \mathbf{x}$, respectively). Otherwise put $z_n = 0$ and $t_n = 0$ for each $n < m_0$, where m_0 is the maximal integer with the property that $x_n = 0 = y_n$ for all $n < m_0$. Choose $z_{m_0} \in A_{m_0}$ and an integer $t_{m_0} \geq 0$ such that $x_{m_0} + y_{m_0} = z_{m_0} + t_{m_0} a_{m_0}$. If we have defined z_k and t_k for all $k < n$, where $m_0 < n$, then there exist $z_n \in A_n$ and a non-negative integer t_n such that $x_n + y_n + t_{n-1} = z_n + t_n a_n$ (note that the numbers z_n and t_n are uniquely determined by these conditions). Each element of $\Omega_{\mathbf{a}}$ is called an $\mathbf{a}$-*adic number*.

a) Verify that $\Omega_{\mathbf{a}}$ is an Abelian group (called the *group of* $\mathbf{a}$-*adic numbers*).
b) Show that, for certain $\mathbf{a}$, the group $\Omega_{\mathbf{a}}$ can have elements of finite order distinct from the neutral element of the group.
c) Characterize the sequences $\mathbf{a}$ such that the corresponding group $\Omega_{\mathbf{a}}$ is torsion-free.
d) Verify that the set of $\mathbf{x} \in \Omega_{\mathbf{a}}$ with $x_n = 0$, for each $n < 0$, is a subgroup of $\Omega_{\mathbf{a}}$; this group is called the *group of* $\mathbf{a}$-*adic integers* and is denoted by $\mathbb{Z}_{\mathbf{a}}$.
e) Prove that the group $\mathbb{Z}_{\mathbf{a}}$, for $\mathbf{a} = (2, 3, 4, \ldots)$, is divisible and torsion-free (notice that in the case of $\mathbb{Z}_{\mathbf{a}}$, we do not have to specify the entries a_n of $\mathbf{a}$ with $n < 0$).

1.2. Groups and semigroups with topologies

A *right topological semigroup* consists of a semigroup S and a topology $\mathcal{T}$ on S such that for all $a \in S$, the right action ϱ_a of a on S is a continuous mapping of the space S to itself.

A *left topological semigroup* consists of a semigroup S and a topology $\mathcal{T}$ on the set S such that for all $a \in S$, the left action λ_a of a on S is a continuous mapping of the space S to itself.

A *semitopological semigroup* is a right topological semigroup which is also a left topological semigroup.

A *topological semigroup* consists of a semigroup S and a topology $\mathcal{T}$ on S such that the multiplication in S, as a mapping of $S \times S$ to S, is continuous when $S \times S$ is endowed with the product topology.

A *right topological monoid* is a right topological semigroup with identity. Similarly, a *topological monoid* is a topological semigroup with identity, and a *semitopological monoid* is a semitopological semigroup with identity.

A *left (right) topological group* is a left (right) topological semigroup whose underlying semigroup is a group, and a *semitopological group* is a left topological group which is also a right topological group.

A *paratopological group* G is a group G with a topology on the set G that makes the multiplication mapping $G \times G \to G$ continuous, when $G \times G$ is given the product topology.

For a group G, the inverse mapping $In\colon G \to G$ is defined by the rule $In(x) = x^{-1}$, for each $x \in G$. A semitopological group with continuous inverse is called a *quasitopological group*.

A *topological group* G is a paratopological group G such that the inverse mapping $In\colon G \to G$ is continuous. An easy verification shows that G is a topological group if and only if the mapping $(x, y) \mapsto xy^{-1}$ of $G \times G$ to G is continuous.

It is evident that every topological group is a topological semigroup, every topological semigroup is a semitopological semigroup, and every semitopological semigroup is both a left and right topological semigroup.

EXAMPLE 1.2.1. Let $\mathcal{T}$ be the topology on $\mathbb{R}$ with the base $\mathcal{B}$ consisting of the sets $[a, b) = \{x \in \mathbb{R} : a \le x < b\}$, where $a, b \in \mathbb{R}$ and $a < b$. With this topology, and the natural addition in the role of multiplication, $\mathbb{R}$ is a paratopological group and, therefore, a topological semigroup. However, $(\mathbb{R}, \mathcal{T})$ is not a topological group since the inverse operation $x \mapsto -x$ is discontinuous. This paratopological group is called the *Sorgenfrey line*. □

EXAMPLE 1.2.2. Let $S = \mathbb{R} \cup \{\alpha\}$ be the one-point compactification of the usual space $\mathbb{R}$ of real numbers. Define multiplication on S by the rule $xy = x + y$ if x and y are in $\mathbb{R}$, and $xy = \alpha$, otherwise. With this operation, S is a semitopological semigroup. However, S is not a topological semigroup, since the multiplication mapping of $S \times S \to S$ is not (jointly) continuous at the point (α, α). □

Note that every group (semigroup) can be turned into a topological group (semigroup) by providing it with the discrete topology. However, the problem of existence of non-discrete Hausdorff topologies on infinite groups which would make them into topological groups is a delicate one. We will discuss it for Abelian groups in Section 1.4.

A useful series of right topological semigroups comes when considering semigroups of the form $S(X, X)$ with weak topologies.

For a topological space X, let $S_p(X, X)$ be the semigroup $S(X, X)$ of all mappings of the set X to X, taken with the topology of pointwise convergence. This topology has the standard base $\mathcal{B}$ which consists of the sets

$$O(x_1, \dots, x_n, U_1, \dots, U_n) = \{f \in S(X, X) : f(x_i) \in U_i \text{ for } i = 1, \dots, n\},$$

where $x_1, \dots, x_n$ are pairwise distinct points of X and $U_1, \dots, U_n$ are non-empty open sets in X, for some $n \in \mathbb{N}$.

THEOREM 1.2.3. *For any topological space X, $S_p(X, X)$ is a right topological semigroup. Further, for any $f \in S(X, X)$, the left action λ_f of f on $S_p(X, X)$ is continuous if and only if the mapping $f\colon X \to X$ is continuous.*

PROOF. Take any $f, g \in S(X, X)$ and a finite subset K of X. Put $L = f(K)$. For each $x \in K$ take an open neighbourhood O_x of $gf(x)$ in X. Let V be the set of all $h \in S(X, X)$ such that $h(x) \in O_x$ for each $x \in K$, and let U be the set of all $g' \in S(X, X)$ such that $g'f(x) \in O_x$ for each $f(x) \in L = f(K)$. Then, clearly, V is a standard open neighbourhood of gf in $S_p(X, X)$, and U is an open neighbourhood of g in $S_p(X, X)$ such that $\varrho_f(U) \subset V$ (that is, $Uf \subset V$). Therefore, $S_p(X, X)$ is a right topological semigroup.

To deduce the last statement of the theorem, we consider the left action λ_f for some $f \in S(X, X)$. Take an arbitrary point $a \in X$ and a non-empty open set V in X. It is easy to see that

$$\lambda_f^{-1}[O(a, V)] = \{g \in S(X, X) : f(g(a)) \in V\} = \{g \in S(X, X) : g(a) \in f^{-1}(V)\}.$$

Therefore, if the mapping $f\colon X \to X$ is continuous, the set $\lambda_f^{-1}[O(a, V)]$ is open in $S_p(X, X)$. Since the sets of the form $O(a, V)$ constitute a subbase for the topology of $S_p(X, X)$, we conclude that the left action λ_f is continuous.

Conversely, suppose that the mapping f is discontinuous. Then we can find a point $a \in X$ and an open neighbourhood V_0 of $b = f(a)$ in X such that $f(U) \setminus V_0 \neq \varnothing$ for each neighbourhood U of a. Let 1_X be the identity mapping of X onto itself. Evidently, $f = \lambda_f(1_X)$ is in $O(a, V_0)$. Take an arbitrary basic neighbourhood $O = O(x_1, \ldots, x_n, U_1, \ldots, U_n)$ of 1_X in $S_p(X, X)$, where the points $x_1, \ldots, x_n$ are pairwise distinct. Then $x_i \in U_i$ for each $i \leq n$. We claim that the image $\lambda_f(O)$ is not a subset of $O(a, V_0)$, so that λ_f is discontinuous at 1_X.

Indeed, if $a \in \{x_1, \ldots, x_n\}$, we can assume that $a = x_1$. Then $W = U_1 \setminus \{x_2, \ldots, x_n\}$ is an open neighbourhood of a in X and, hence, $f(W) \setminus V_0 \neq \varnothing$. Choose a point $y_0 \in W$ such that $f(y_0) \notin V_0$ and take an arbitrary $g \in S(X, X)$ such that $g(x_1) = y_0$ and $g(x_i) = x_i$ for each i with $1 < i \leq n$. Then $g \in O$, and $\lambda_f(g) = f \circ g \in \lambda_f(O) \setminus O(a, V_0)$ since $f(g(a)) = f(y_0) \notin V_0$. Similarly, if $a \notin \{x_1, \ldots, x_n\}$, we can choose a point $y_0 \in W = X \setminus \{x_1, \ldots, x_n\}$ such that $f(y_0) \notin V_0$ and take a mapping $g\colon X \to X$ with $g(a) = y_0$ and $g(x_i) = x_i$ for each $i \leq n$. Then again $g \in O$ and $f \circ g = \lambda_f(g) \in \lambda_f(O) \setminus O(a, V_0)$.

Thus, the left action λ_f of f on $S_p(X, X)$ is discontinuous for every discontinuous mapping f. $\square$

COROLLARY 1.2.4. *Let X be a topological space. The following statements are equivalent:*

1) *$S_p(X, X)$ is a topological semigroup.*
2) *$S_p(X, X)$ is a semitopological semigroup.*
3) *The space X is discrete.*

PROOF. If X is discrete, then every mapping f of X to X is continuous, so the left action λ_f is continuous by Theorem 1.2.3, and $S_p(X, X)$ is a semitopological semigroup by the same theorem. Hence, 3) implies 2). Conversely, if $S_p(X, X)$ is a semitopological semigroup then all left actions λ_f are continuous, which implies, by Theorem 1.2.3, that all mappings $f\colon X \to X$ are continuous. Since the one-point sets in X are closed, the space X must be discrete. Therefore, 2) and 3) are equivalent.

Clearly, 1) implies 2). We leave it to the reader to verify that 3) implies 1). $\square$

Some more examples are in order.

EXAMPLE 1.2.5. We present here several types of topologies on groups (semigroups).

a) Let G be an arbitrary group (semigroup), and let $\mathcal{T}$ be the family of all subsets of G, i.e., the discrete topology of G. With this topology, G is a topological group (semigroup). We shall often refer to such a G as a *discrete group.*
b) Let G be an arbitrary infinite group and let $\mathcal{T}$ consist of G and the subsets of G having finite complements. Then G is not a paratopological group. However, G is a semitopological group with continuous inverse, that is, a quasitopological group. Note that G with this topology is a T_1-space but not Hausdorff.
c) The additive group $\mathbb{R}$ of all real numbers with its usual topology is a locally compact, non-compact Abelian group.

d) The multiplicative circle group $\mathbb{T}$ with the topology inherited from the complex number field $\mathbb{C}$ is a compact Abelian group.
e) Let G be the group $GL(n, \mathbb{R})$ of all invertible n by n matrices with real entries (see also item 7) of Example 1.1.2). We endow G with the topology of a subspace of the n^2-dimensional Euclidean space. Then G is a topological group. Indeed, the formula for multiplying two matrices and the formula for inverting a matrix employ only continuous functions of the entries of the matrices. This group is called the *general linear group* of degree n over $\mathbb{R}$. Similarly, the general linear group $GL(n, \mathbb{C})$ over the field $\mathbb{C}$ of complex numbers, with the matrix multiplication and the topology induced from $\mathbb{C}^{n^2}$ is again a topological group.
f) Let $\mathbf{Q}$ be the additive group of quaternions (see Example 1.1.9). Consider the natural mapping $f: \mathbf{Q} \to \mathbb{R}^4$ defined by the rule $f(q) = (x, y, z, t)$, for each $q = x + \mathbf{i}y + \mathbf{j}z + \mathbf{k}t \in \mathbf{Q}$. Clearly, f is a bijection of $\mathbf{Q}$ onto $\mathbb{R}^4$. We topologize $\mathbf{Q}$ by declaring the mapping f to be a homeomorphism. In other words, a subset U of $\mathbf{Q}$ is open if and only if the image $f(U)$ is open in $\mathbb{R}^4$. This agreement makes $\mathbf{Q}$ into a locally compact, second-countable Hausdorff topological group. Clearly, the restriction of f to $\mathbf{Q}^* = \mathbf{Q} \setminus \{\mathbf{0}\}$ fails to be a homomorphism of the multiplicative group $\mathbf{Q}^*$ to the additive group $\mathbb{R}^4$. However, $\mathbf{Q}^*$ with this topology (called Euclidean) turns out to be a topological group. This fact follows easily from the definition of the multiplication and the procedure of inversion in $\mathbf{Q}^*$ given in Example 1.1.9. Therefore, the multiplicative group of quaternions $\mathbf{Q}^*$ with the Euclidean topology is a locally compact Hausdorff topological group. □

EXAMPLE 1.2.6. Let G and H be right topological semigroups, and $G \times H$ their product. For each $x \in G$, the set $\{x\} \times H$ is called a *vertical fiber* of $G \times H$. For each $y \in H$, the set $G \times \{y\}$ is called a *horizontal fiber* of $G \times H$. Every vertical fiber can be considered as a copy of the right topological semigroup H. Similarly, every horizontal fiber can be interpreted as a copy of the right topological semigroup G. Therefore, we can treat every fiber as a topological space.

Now we will define two new topologies on $G \times H$, each of which contains the product topology on $G \times H$.

The first one is the *cross* topology. A subset W of $G \times H$ belongs to it if and only if the intersection of W with every fiber of $G \times H$ (horizontal and vertical) is open in the fiber. It is easy to verify that the semigroup $G \times H$ with the usual (coordinatewise) multiplication and with the cross topology is again a right topological semigroup.

The second new topology on $G \times H$ is defined as follows. Take the family $SC(G \times H)$ of all real-valued functions f on $G \times H$ such that the restriction of f to each fiber is a continuous function on this fiber. It is well known that the functions in $SC(G \times H)$ need not be continuous on the space $G \times H$. Now let σ be the smallest topology on $G \times H$ which makes all functions $f \in SC(G \times H)$ continuous.

It is easy to see that if G and H are Tychonoff spaces, then the topology σ on $G \times H$ contains the usual topology of $G \times H$ and also is Tychonoff. However, the cross topology on $G \times H$ need not be regular, even if G and H are second-countable spaces. □

The usual product topology on products of finitely many factors can be used to obtain many interesting examples of topological groups and semigroups. Especially, if we combine the product operation with the operation of taking a topological subgroup (subsemigroup)