Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

617

Keith J. Devlin

The Axiom of Constructibility:

A Guide for the Mathematician

Springer-Verlag
Berlin Heidelberg New York

Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

617

Keith J. Devlin

The Axiom of Constructibility:

A Guide for the Mathematician

Springer-Verlag
Berlin Heidelberg New York 1977

Author
Keith J. Devlin
Department of Mathematics
University of Lancaster
Lancaster/England

Library of Congress Cataloging in Publication Data

Devlin, Keith J
The axiom of constructibility.

(Lecture notes in mathematics ; 617)
Bibliography: p.
Includes index.
1. Axiom of constructibility. I. Title. II. Series: Lecture notes in mathematics (Berlin) ; 617.
QA3.L28 no. 617 [QA248] 510'.8s [511'.3] 77-17119

AMS Subject Classifications (1970): 02K15, 02K25, 02K05, 04-01, 04A30, 20A10, 20K35, 54D15

ISBN 3-540-08520-3 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-08520-3 Springer-Verlag New York Heidelberg Berlin

Printed in Germany

Printing and binding: Beltz Offsetdruck, Hemsbach/Bergstr.
2140/3140-543210

PREFACE

Consider the following four theorems of pure mathematics.

The Hahn-Banach Theorem of Analysis: If F is a bounded linear functional defined on a subspace $\underset{\sim}{M}$ of a Banach space $\underset{\sim}{B}$, there is an extension of F to a linear functional G on $\underset{\sim}{B}$ such that $\|G\| = \|F\|$.

The Nielsen-Schreier Theorem of Group Theory: If $\underset{\sim}{G}$ is a free group and $\underset{\sim}{H}$ is a subgroup of $\underset{\sim}{G}$, then $\underset{\sim}{H}$ is a free group.

The Tychonoff Product Theorem of General Topology: The product of any family of compact topological spaces is compact.

The Zermelo Well-Ordering Theorem of Set Theory: Every set can be well-ordered.

The above theorems have two things in common. Firstly they are all fundamental results in contemporary mathematics. Secondly, none of them can be proved without the aid of some powerful set theoretical assumption: in this case the Axiom of Choice.

Now, there is nothing wrong about assuming the Axiom of Choice. But let us be sure about one thing: we are making an assumption here. We are saying, in effect, that when we speak of "set theory", the Axiom of Choice is one of the basic properties of sets which we intend to use. This is a perfectly reasonable assumption to make, as most pure mathematicians would agree. Moreover (and here we are at a distinct advantage over those who first advocated the use of the Axiom of Choice), we know for sure that assuming the Axiom of Choice does not lead to a contradiction with our other (more fundamental) assumptions about sets.

In Chapter I of this book we describe four classic open problems of mathematics, as above one from Analysis, one from Algebra, one from General Topology, and one from Set Theory. Since we call these "problems" rather than "theorems", however, it should be obvious that they are not quite the same as our four statements above. Indeed, it can be shown that assuming the axiom of choice does not lead to a solution of any of these problems. But by making a further assumption about sets, we are able to solve each of these problems (and many more problems known to be unsolvable without such an assumption). This assumption is the Axiom of Constructibility.

The Axiom of Constructibility is an axiom of set theory. It is a natural axiom, closely bound up with what we mean by "set". It implies the axiom of choice. It is known not to contradict the more basic assumptions about sets. And as we have already indicated, its assumption leads to the solution of many problems known to be unsolvable from the Axiom of Choice alone. Time alone will tell whether or not this axiom is eventually accepted as a basic assumption in mathematics. Currently, the situation is not unlike that involving the Axiom of Choice some sixty years ago. The axiom is being applied more and more, and what is more it tends to decide problems in the "correct" direction. And one can provide persuasive arguments which justify the adoption of the axiom. (Again as with the Axiom of Choice in the past, there are also arguments against its adoption.) However, since the axiom is being applied in different areas of pure mathematics, it is a proposition of interest to the mathematician at large regardless of the final outcome concerning its "validity".

Until recently the notion of a constructible set was studied extensively only by the mathematical logician. Indeed, any kind of in-depth study requires a considerable acquaintance with the ideas and methods of mathematical logic — in particular, the notions of formal languages, satisfaction, model theory, and a good deal of pure set theory. But with the growing use of the Axiom of Constructibility in areas outside of set theory, the axiom has become of interest to mathematicians who do not possess all of these prerequisites from logic. It is for this audience that we have written this short account. Our basic premise in writing has been that, whilst it would be very nice if everyone had at least a basic knowledge of elementary mathematical logic, this is almost certainly not the case. We therefore assume no prior knowledge of mathematical logic. (The one exception is Chapter V, but the book is designed so that this chapter can be totally ignored without affecting anything else.) Since it would clearly be far too great a task to develop this material to a level adequate for anything approaching a comprehensive treatment of constructibility, we choose instead to cut some corners and arrive at the required definitions very quickly. In other words, we present here a description of set theory and the Axiom of Constructibility, not the theory itself. Admittedly this approach may prove annoying to logicians — but they do not need to read this account, being well equipped to consult a more mathematical account.

The book is divided up as follows. In Chapter I we discuss some well known problems of pure mathematics. Since each of these problems is unsolvable on the basis of the current system of set theory, but can be solved if one assumes the Axiom of Constructibility, they provide both a motivation for considering the axiom, as well as illustrations of its application. In Chapter II we give a brief account of set theory. This forms the basis of our description of constructibility in Chapter III. Chapter IV applies the Axiom of Constructibility in order to solve the problems considered in Chapter I. Chapter V is different from the rest of this book in that some knowledge of logic is assumed.(At least, for a full appreciation of our discussion a prior knowledge of logic is required. The reader may be able to gain some idea of what is going on without such knowledge. We certainly try to keep things as simple as possible.) In Chapter V we try to explain just how it is that the Axiom of Constructibility enables one to answer questions of mathematics of the kind considered in the previous chapters. In order to illustrate our description we present a further application of the axiom, this time in Measure Theory. (We thereby provide some consolation for measure theorists who may have felt left out by our choice of problems in Chapter I.) The book is structured on the assumption that many readers will not wish to go into the subject matter of Chapter V very thoroughly, if at all.

It is to be hoped that mathematicians may wish to use the Axiom of Constructibility. For this reason the proofs in Chapter IV are given in some detail, except that in each case we state without proof a very general combinatorial principle which is a consequence of the Axiom of Constructibility, and then use this principle in order to prove the desired result. The advantage of this approach is that the reader may use the proof as a model for other proofs, without having to spend a great deal of time investigating the Axiom of Constructibility itself.

Finally a word about our use of the phrase "pure mathematics". In writing this book it has been convenient to restrict the meaning of this phrase to "pure mathematics other than set theory". A similar remark applies to our use of the word "mathematician" in our title.

CONTENTS

FOUR FAMOUS PROBLEMS

In order both to motivate the consideration of the Axiom of Constructibility, and to illustrate its use, we give here a brief account of four well known problems of pure mathematics, one from analysis, one from algebra, one from general topology, and one from set theory. These problems all have one thing in common: they cannot be solved on the basis of the usual set theoretical assumptions (axioms), but they are solvable if we assume the Axiom of Constructibility.

1. A Problem in Real Analysis[1]

Let X be an infinite set, $<$ a linear ordering of X. We may define a topology on X by taking as an open basis all intervals $(a,b) = \{ x \in X \mid a < x < b \}$ for $a,b \in X$ with $a < b$. A classic theorem of Cantor says that if X has no largest member and no smallest member, and if the above topology on X is both connected and separable, then X is (considered as an ordered topological space) homeomorphic to the real line, $\mathbb{R}$, (considered as an ordered topological space). The basic idea behind the proof is to take a countable dense subset of X (by separability), prove that this set is isomorphic to the rationals, $\mathbb{Q}$, and then show that X must be isomorphic to the Dedekind completion of the dense subset, and hence isomorphic to $\mathbb{R}$, the Dedekind completion of $\mathbb{Q}$. Use is made of the fact that the connectedness of X is equivalent to the two facts (a) that for each pair a,b of elements of X with $a < b$ there is a third element, c, of X with $a < c < b$, and (b) that every subset of X which is bounded above/below in X has a least upper bound/ greatest lower bound in X.

It is not unnatural to ask if the above characterisation of the real line is the best possible. Can we, for instance, weaken any of the conditions on X (and $<$) and still obtain the conclusion that such an X will be isomorphic to $\mathbb{R}$? From this standpoint, the following question is quite natural. Let us say that a linearly

1. Strictly speaking, this is not a problem of real analysis itself. But it is clearly of interest to any real analyst. (We make no apology for any ambiguity in this last sentence.)

ordered set X satisfies the <u>countable chain condition</u> (c.c.c.) if every collection of pairwise disjoint open intervals is countable. (The reader should not worry about where "chains" get into the act. There are good historical reasons for using the word "chain" here, as well as some, not so overwhelming, mathematical reasons.) Clearly, if X is separable, then X will satisfy the c.c.c. So it is not unreasonable to pose the following question:

Let X be an infinite set, $<$ a linear ordering of X. Suppose that under the ordering $<$, X has no largest member and no smallest member. Regard X as a topological space as above. If X is connected and satisfies the c.c.c., does it follow that $X \cong \mathbb{R}$?

This question was first raised by <u>M. Souslin</u> in 1920. It soon became known as <u>The Souslin Problem</u>. Curiously enough, although the question is so basic and so very simple to pose, it resisted numerous attempts at solution over the next forty years. Of course (?), in view of the important role played by the fact that the reals have a countable dense subset, one would expect the Souslin Problem to have a negative answer. But no counterexample was forthcoming. We shall see why in the ensuing chapters.

2. <u>A Problem in Algebra</u>

We consider now a famous problem of group theory. As a first step, let us establish the convention that "group" will always mean "abelian group".

Let G, A, B be groups. We say that G is an <u>extension of</u> A <u>by</u> B iff A is a subgroup of G (written $A \lhd G$) and $G/A \cong B$. (Thus B describes, in a sense, the <u>manner</u> in which G <u>extends</u> A.)

Given groups G and A with G an extension of A, there is a unique (up to isomorphism) group B such that G is an extension of A by B: namely the group G/A. The <u>extension problem</u> (for abelian groups) asks the following converse question. Given groups A and B, determine the extensions of A by B. There is always at least one such: namely, the direct sum $A \oplus B$. But there may be more than one. For instance, let $\mathbb{Z}$ be the group of integers, $2\mathbb{Z}$ the subgroup of the even integers, and $\underset{\sim}{2}$ the unique group of order 2. Now, $\mathbb{Z}/2\mathbb{Z} \cong \underset{\sim}{2}$, so $\mathbb{Z}$ is an extension of $2\mathbb{Z}$ by $\underset{\sim}{2}$. But $\mathbb{Z} \not\cong 2\mathbb{Z} \oplus \underset{\sim}{2}$ since $\mathbb{Z}$ is torsion free and $2\mathbb{Z} \oplus \underset{\sim}{2}$ has torsion. The following solution to the extension problem is due to <u>Baer</u>.

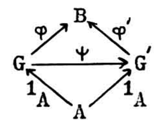
Let G, G$'$ be extensions of A by B. Thus $G/A \cong B$, $G'/A \cong B$. Let

$$G \xrightarrow{\varphi} B \qquad \text{and} \qquad G' \xrightarrow{\varphi'} B$$

be the canonical projections. We write $G \sim G'$ iff there is an isomorphism

$$G \xrightarrow{\psi} G'$$

which makes the following diagram commute:



(As usual, 1_A denotes the identity morphism on A into whatever extension of A is being considered.)

It is easily seen that $\sim$ is an equivalence relation on the set of all extensions of A by B. The relation $G \sim G'$ is stronger than isomorphism, and is clearly the correct notion of "sameness" when we are considering extensions of A by B.

R. Baer proved, in 1949, that the set of equivalence classes of extensions of A by B under the above equivalence relation itself forms a group. We denote this group by Ext(B,A). It is the group of extensions of A by B. It is outside the scope of this book to describe the group operation involved in Ext(B,A), and indeed we shall not need to know it. What we do need to know is that the identity element of the group Ext(B,A) is the equivalence class of the direct sum $A \oplus B$.

We should also mention that as a result of work by Schreier it is possible to give a description of the members of Ext(B,A) in terms of A and B.

Let us recall now that a group G will be free iff there is a set $\{g_i \mid i \in I\}$ of elements of G such that every non-zero element of G has a unique representation of the form

$$n_1 g_{i_1} + \cdots + n_k g_{i_k} ,$$

where $i_1, \ldots, i_k$ are distinct members of I and $n_1, \ldots, n_k$ are non-zero integers.

We then say $\{g_i \mid i \in I\}$ is a basis for G. A basis is thus the same as a linearly independent generating set. We relate the notion of a free group to the extension problem as follows.

2.1 Theorem

Let $H \lhd G$. If G/H is free, then $G = H \oplus N$ for some $N \lhd G$, $N \cong G/H$.

Proof: Let $\{H + k \mid k \in K\}$ be a basis for G/H , where $K \subseteq G$. Let $N = \langle K \rangle_G$, the subgroup of G generated by K. It is easily checked that $G = H \oplus N$. □

2.2 Corollary

If B is free, then $\mathrm{Ext}(B,A) = 0$.

Proof: Let $A \lhd G$, $G/A \cong B$. Since G/A is free, 2.1 gives $G \cong A \oplus B$. (More precisely, the proof of 2.1 shows that $G \sim A \oplus B$ in the sense defined above.) □

The above result has a converse. In order to obtain the converse, we recall the following standard theorem.

2.3 Theorem (Nielsen-Schreier)

If G is free and $H \lhd G$, then H is free. □

2.4 Lemma

Let B be a given group. If $\mathrm{Ext}(B,A) = 0$ for all groups A, then B is free.

Proof: Let F be the free group on B (i.e. the unique group which is freely generated by the set B). Let

$$F \xrightarrow{\varphi} B$$

extend the identity function on B. Set $A = \mathrm{Ker}(\varphi)$. Then F is an extension of A by B, so by hypothesis, $F \cong A \oplus B$. Hence there is an embedding

$$B \longrightarrow F.$$

So by 2.3, B is free. □

Now , by 2.2, if G is free, then $\mathrm{Ext}(G,\mathbb{Z}) = 0$. J. H. C. Whitehead asked, in 1951, if this statement has a valid converse. In other words, does the property that $\mathrm{Ext}(G,\mathbb{Z}) = 0$ characterise the free groups G ? Defining a W-group to be any group G for which $\mathrm{Ext}(G,\mathbb{Z}) = 0$, this reduces to showing that every W-group is free. Until recently, the only result of note on this problem was the following, proved in 1951:

2.5 Theorem (Stein)

Every countable W-group is free. □

We shall return to the Whitehead Problem in later chapters.

3. A Problem in General Topology

Let $(X,\mathcal{T})$ be a topological space. The following separation properties which X may satisfy are well known.

X is T_0 if, whenever $x,y \in X$ and $x \neq y$ there is an open set U which contains exactly one of x, y.

X is T_1 if, whenever $x,y \in X$ and $x \neq y$ there are open sets U, V such that $x \in U$, $y \notin U$ and $x \notin V$, $y \in V$.

X is T_2 (Hausdorff) if, whenever $x,y \in X$ and $x \neq y$ there are disjoint open sets U, V such that $x \in U$ and $y \in V$.

X is regular if, whenever $x \in X$ and $A \subseteq X$ is closed and $x \notin A$, there are disjoint open sets U, V such that $x \in U$ and $A \subseteq V$. X is T_3 if it is regular and T_1.

X is normal if, whenever A, B are disjoint closed subsets of X there are disjoint open sets U, V such that $A \subseteq U$ and $B \subseteq V$. X is T_4 if it is normal and T_1.

It is immediate that $T_4 \to T_3 \to T_2 \to T_1 \to T_0$. None of these implications is reversible.

The following generalisation of the Hausdorff property occurs in the literature. We say a subset Y of X is discrete if every point of X has a neighborhood which contains at most one point of Y. (Thus if X is T_1, a subset Y of X will be discrete iff Y has no limit points in X, which says that the elements of Y are spaced well apart from each other.) A space is collectionwise Hausdorff if, whenever Y is a discrete set, there is a family $\{U_y \mid y \in Y\}$ of pairwise disjoint open sets such that $y \in U_y$ for all $y \in Y$. (We call such a family a separation of Y.)

Now, it is not hard to show that the Hausdorff property does not in general imply the collectionwise Hausdorff property. Indeed, there are T_4 spaces which are not collectionwise Hausdorff. So we ask what extra conditions on a space are required in order to yield the conclusion that it be collectionwise Hausdorff ? Considerations outside of our present scope lead to the following precise question (which is fairly close to the best possible). Recall that a space is said to satisfy the first axiom of countability if for each point x the neighborhood system of x has a countable basis. The question now is: Is every first countable T_4 space collectionwise Hausdorff? We investigate this problem in IV.4. Let us finish by mentioning that this question first arose out of research on a very famous problem of General Topology — the normal Moore space problem (which is still open). This problem deals with the metrization problem (i.e. which topological spaces are metric spaces ?). Roughly speaking, what the normal Moore space problem asks is whether every first countable T_4 space is collectionwise normal.

4. A Problem in Set Theory

The oldest of our four problems — the continuum problem — dates back to Cantor. The question raised here is: How many real numbers are there ? In order to make this precise we require some elementary notions from set theory.

Fundamental in mathematics is the notion of counting. And it is to be expected that our reader is familiar with (at least some of!) the natural numbers 0,1,2,... . Using the natural numbers we may "count" the "number" of elements in any finite set. But what about infinite sets ? Well, why not extend the natural number system into the transfinite ? Why not indeed! By doing this we obtain the ordinal number system, which commences with the natural numbers, and which is adequate to "count" the elements of any set. What are the ordinal numbers ? We answer this question by first answering the question: What are the natural numbers ?

The number 0 we define to be the empty set, $\emptyset$. The number 1 we define to be the set $\{0\}$ (i.e. the set with precisely one element, that element being the natural number 0). The number 2 we define to be the set $\{0,1\}$. Proceeding inductively, we define the number n+1 to be the set $\{0,1, . . . ,n\}$. Notice that the number n is always a set with exactly n elements, those elements being precisely the numbers smaller than n. To obtain the ordinal numbers we continue the definition into the transfinite. The first infinite ordinal, denoted by ω , is the set

$$\{0,1, . . . ,n, . . . \quad . . . . . . \}$$

of all natural numbers. The second infinite ordinal, $\omega+1$, is the set

$$\{0,1, . . . ,n, . . . \quad . . . . . . ,\omega\} .$$

In general, the next ordinal number after α will be the set $\alpha \cup \{\alpha\}$. And when we have defined the sequence of ordinals

$$0,1, . . . ,n, . . . ,\omega,\omega+1, . . . ,\alpha, . . . \quad ,$$

this sequence having no last member, the "next" ordinal number will be the set

$$\{0,1, . . . ,n, . . . ,\omega,\omega+1, . . . ,\alpha, . . . \}$$

of all ordinals constructed so far.

In general we use lower case Greek letters to denote ordinal numbers. Notice that by our definition of ordinal number, if α , β are ordinal numbers, α will precede β (i.e. be smaller than β), written $\alpha < \beta$, just in case $\alpha \in \beta$. Thus the ordinal numbers are totally ordered by $\in$. Indeed they are well-ordered by $\in$. Moreover, regarded as the set of all smaller ordinal numbers, each ordinal number is itself well-ordered by $\in$.

Now, each ordinal number has associated with it a canonical well-ordering : namely $\in$. It can be shown that every well-ordered set P can be put into an orderpreserving, one-one correspondence with a unique ordinal, called the order-type of P, written otp(P). In this way the ordinal numbers can be used to "count" the number of elements in any well-ordered set (otp(P) being the answer for the well-ordered set P). But by Zermelo's Well-Ordering Theorem (which is a consequence of the Axiom of Choice), every set can be well-ordered. Hence we may use the ordinal numbers to "count" the elements of any set. The problem here is that the result of our counting depends upon the well-ordering chosen. Now in the case of finite sets we are used to the fact that it does not matter in which order we count the elements of that set ; the answer will always be the same. But for infinite sets this is no longer the case. Different well-orderings of the same set can lead to different results to the process of counting the elements of that set. For example, consider the set, ω, of natural numbers. Under the usual well-ordering, this set, ω, has order-type ω . But we can also well-order the set ω as follows:

$$\{0,2,4, \ldots \ldots, 1,3,5, \ldots \ldots\} .$$

Under this well-ordering the order-type of the same set ω is the ordinal number $\omega+\omega$, which is the second ordinal constructed by taking the set of all previous ordinals when that set has no largest member. Thus, although we can use the ordinal numbers for "counting" infinite sets, they are really only suited for measuring the size of well-ordered sets. Fortunately, however, using the ordinal numbers we may obtain a number system which is able to "count" the elements of an arbitrary set. We make use of the fact that the ordinal numbers are themselves well-ordered by $\in$.

Given a set X, we define its cardinality to be the least ordinal number α which may be put into one-one correspondence with X. Equivalently, the cardinality of X is the least order-type of all well-orderings of X. The cardinality of X is usually denoted by $|X|$. Any ordinal number which equals $|X|$ for some set X is called a cardinal number. It is immediate from this definition that an ordinal number α will be a cardinal number iff it cannot be put into one-one correspondence with any smaller ordinal number. Clearly, $0,1,2, \ldots, n, \ldots$ are all cardinal numbers. So too is ω . But $\omega+1$, $\omega+2$, etc. are not cardinal numbers, since each may be put into one-one correspondence with ω . The first cardinal after ω is denoted by ω_1,