rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

Bases for vector spaces in different models of set theory

Bachelorondersoek Wiskunde

Juli 2010

Student: F.A. Roumen

Eerste Begeleider: prof. dr. J. Top

Tweede Begeleider: dr. J. Terlouw

Summary

In this thesis, we will consider two models of set theory and look at consequences of these models in linear algebra. The first model satisfies the Axiom of Choice; we will show that this is equivalent to existence of bases for all vector spaces. We will also prove that countability of a vector space is sufficient for proving existence of bases without the Axiom of Choice. The second model will be constructed using the forcing technique. It contains an infinite-dimensional vector space having only finite-dimensional subspaces, which implies that this vector space has no basis.

Contents

Introduction

Infinite-dimensional vector spaces usually behave differently than finite-dimensional vector spaces. For example, finite-dimensional spaces always have bases, which makes their structure easy to understand and to reason about. One might ask which parts of the theory of finite-dimensional spaces can be transferred to the infinite-dimensional case. It turns out that this depends on the particular model of set theory in which one is working. In this thesis, we will consider two different models of set theory and study linear algebra in both models. In particular, we will generalize the definition of 'basis' to infinite-dimensional cases and ask whether every vector space has a basis in the model. It turns out that a crucial axiom determining the structure of vector spaces is the Axiom of Choice. Accepting this axiom implies that every vector space has a basis, but rejecting the axiom it is possible to construct a vector space that has no basis. We will show how to construct such a space and prove many of its counter-intuitive properties, for instance that it has no infinite-dimensional proper subspaces despite being infinite-dimensional itself. We will also give conditions which guarantee the existence of bases, even in the absence of Choice.

Chapter 1 contains some preliminary material about set theory and partially ordered sets, which will frequently be used throughout the thesis.

In Chapter 2 we will use a model of set theory in which the Axiom of Choice holds and consider consequences in linear algebra. We give a generalized definition of a basis, prove that all vector spaces have bases in this model and provide a condition under which a vector space has a basis when the Axiom of Choice is rejected. Finally we will show that the theorem "Each vector space has a basis" cannot be proven without using Choice.

Chapter 3 introduces a technique called 'forcing' that is often applied to create models of set theory and prove properties of these models. We will use this method to construct a model containing a vector space without a basis and prove other properties of this space, for instance that it has only finite-dimensional proper subspaces despite being infinite-dimensional itself. The construction in this chapter differs from the method used in the literature: in this thesis we will explicitly define the model, while in the literature only the existence of the model is proven using the Jech–Sochor embedding theorem. The method used in the literature is sketched in Appendix B.

Chapter 1

Sets and order

This chapter contains some preliminaries for the rest of this thesis. In Sections 1.1 and 1.2 we discuss some set theory, especially the concept of models and equivalents of the Axiom of Choice. Section 1.3 contains an introduction to order theory. The main reference for Section 1.1 is [2]. Section 1.2 is based on [5] and the order theory in Section 1.3 comes from [4, 8].

1.1 Axioms and models

Set theory can be used to represent all mathematical objects, like numbers and functions, as certain sets. Therefore set theorists consider no objects other than sets: everything in the set-theoretical universe is a set, and all members of a set are sets themselves.

The development of set theory starts from a list of intuitively obvious axioms. The axioms can be stated in a natural language like English, or in a formal language consisting of only mathematical symbols. English-language sentences have the advantage of being easier to understand, but formal expressions are usually more precise.

There are multiple versions of the axiom system for set theory. In this text we will work in the Zermelo–Fraenkel system, denoted ZF. A few examples of axioms of ZF are the following.

Axiom of Extensionality. *Two sets are equal if they contain the same elements. Formally,*

$$\forall x \forall y \left(\forall z \left(z \in x \leftrightarrow z \in y \right) \rightarrow x = y \right).$$

The reverse implication is always true, so this axiom could also be stated as "Two sets are equal if and only if they contain the same elements".

Axiom of Pairing. *If x and y are sets, then there exists a set containing x and y and nothing else. This set is denoted $\{x, y\}$. The formal version of this axiom is*

$$\forall x \forall y \exists z \forall w \left(w \in z \leftrightarrow (w = x \vee w = y) \right).$$

For a full list see Appendix A.

A *model* for an axiomatic system is a mathematical structure satisfying all axioms. To give a simple example, consider the theory of vector spaces. The axioms of this theory include $x + y = y + x$, $x + 0 = x$ et cetera. A model of this system is a structure that satisfies all axioms, so a model is simply a vector space. Similarly, a model of set theory is a collection of objects, called sets, that satisfy all ZF axioms. A more precise definition of models will be given in Section 3.1.

Finding models of set theory is much more difficult than finding examples of vector spaces, because the axioms for set theory are more complicated. Instead of finding examples, we will present a property that well-behaved models should have. Suppose that M is a model of ZF and $y \in M$. As said before, all elements of a set should be sets themselves. Hence, since y should be interpreted as a set, all elements of y must be in M as well.

Definition 1.1. A set M is called *transitive* if $x \in M$ whenever $x \in y$ and $y \in M$.

There exist non-transitive models of ZF, but as transitive models are easier to work with, we will require our models to be transitive.

1.2 Axiom of Choice

One important axiom of set theory is known as the Axiom of Choice. It is the following statement.

Axiom of Choice. *If X is a collection of non-empty sets, then there exists a function $f : X \to \bigcup X$ such that $f(x) \in x$ for all $x \in X$.*

The function f is called a *choice function*. Intuitively the axiom states that, given a collection of non-empty sets, it is possible to choose one element of every set in the collection. The function f assigns to every set an element of that set. To give a very simple example, let

$$X = \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}.$$

This is a collection of non-empty sets. A choice function for X is

$$\begin{array}{rrcl} f: & \{1\} & \mapsto & 1 \\ & \{1,2\} & \mapsto & 2 \\ & \{1,2,3\} & \mapsto & 1 \end{array}$$

Of course, there are also other possible choice functions. The Axiom of Choice is actually not necessary in this special case, as the existence of f can be derived from the other axioms. More generally, if X is finite, then there exists a choice function for X which can be constructed without using Choice. The Axiom of Choice is only indispensable for some infinite sets.

The Axiom of Choice seems intuitively obvious. Nonetheless some mathematicians have objections against the axiom because of its non-constructive nature and bizarre consequences. The axiom is non-constructive, because it asserts the existence of a choice function without providing explicit means to construct such a function. This is a reason why the Axiom of Choice differs in

nature from the other axioms of ZF. Besides being non-constructive, the consequences of the Axiom of Choice can be quite strange. For instance, Choice implies that it is possible to decompose a sphere into four pieces, which can be translated and rotated to form two copies of the original sphere. This decomposition is known as the Banach–Tarski paradox.

Accepting the Axiom of Choice yields paradoxical results, but it has many desirable consequences as well. In this thesis, we will first look at consequences of accepting Choice, and thereafter we look at what might happen upon rejection. In other words, we will look at models of ZF with and without the Axiom of Choice. The theory consisting of all axioms of ZF together with Choice is denoted as ZFC.

In its original formulation, the Axiom of Choice can be difficult to apply. We will therefore state some equivalent formulations of the Axiom of Choice. The proofs can be found in [5]. The first equivalent statement is the Axiom of Multiple Choice. The standard Axiom of Choice asserts that it is possible to select a single element of each set in a collection, or, equivalently, a one-element subset of each set. In the Axiom of Multiple Choice, this one-element subset is replaced by a finite subset.

Axiom of Multiple Choice. *If $\{X_i \mid i \in I\}$ is a family of non-empty sets, then there exists a family $\{F_i \mid i \in I\}$ of non-empty finite sets $F_i \subseteq X_i$.*

Trivially the Axiom of Choice implies the Axiom of Multiple Choice, but both axioms are in fact equivalent.

Many equivalents of the Axiom of Choice are phrased in the language of partial orders. Furthermore, the technique of forcing discussed in Chapter 3 also heavily relies on the notion of order. Therefore we will give a short introduction to partially ordered sets in the next section, before discussing other equivalents of the Axiom of Choice.

1.3 Partial orders

Ordered structures are ubiquitous in mathematics. For instance, the natural numbers can be ordered by the standard $\leq$ relation, and inclusion orders the sets. These are examples of the general notion of a partial order.

Definition 1.2. A *partially ordered set* is a set P together with a relation $\leq$ on P satisfying

1. (Reflexivity) $x \leq x$ for all $x \in P$.
2. (Anti-symmetry) $x \leq y$ and $y \leq x$ imply $x = y$.
3. (Transitivity) $x \leq y$ and $y \leq z$ imply $x \leq z$.

If, moreover, the relation satisfies

4. (Totality) $x \leq y$ or $y \leq x$ for all $x, y \in P$

then P is called a *totally ordered set* or a *chain*.

An element $1 \in P$ is called *maximal* if there is no element larger than 1, i.e. $1 \leq x$ implies $1 = x$. Minimal elements are defined analagously. The relation $\leq$ is called a *well-order* if it is a total order and every non-empty subset of P contains a minimal element. In that case P is called *well-ordered*.

If Q is a subset of P and $x \in P$, then x is an *upper bound* for Q if $q \leq x$ for all $q \in Q$. Of course we can also define lower bounds. Not all subsets of a partially ordered set have upper bounds, and even if an upper bound exists, it need not be an element of the subset.

This terminology enables us to state two more equivalents of the Axiom of Choice.

Well-order Theorem. *Every set can be well-ordered.*

Zorn's Lemma. *If every chain in the partially ordered set P has an upper bound, then P possesses a maximal element.*

Especially the well-order theorem is usually regarded as counter-intuitive. For example, it is unclear how to exhibit a well-order on the set $\mathbb{R}$ of real numbers. This is again a non-constructive aspect of the Axiom of Choice or the well-order theorem: it claims the existence of a well-order on $\mathbb{R}$ but fails to provide a method to construct the order.

For the discussion of forcing in Chapter 3, we need some additional definitions of special subsets in a partially ordered set.

Definition 1.3. A *filter* is a non-empty subset F of a partially ordered set P satisfying

1. If $x \in F$ and $x \leq y \in P$, then $y \in F$.
2. If $x, y \in F$, then F contains a lower bound for $\{x, y\}$. Explicitly, for all $x, y \in F$ there exists $z \in F$ such that $z \leq x$ and $z \leq y$.

A filter can alternatively be characterized as a subset of P that is closed under "moving upwards" and under taking lower bounds. The first condition in the definition can be expressed more conveniently with the following notations. For an arbitrary subset $S \subseteq P$, define the filter

$$\uparrow S = \{x \in P \mid (\exists y \in S) y \leq x\}.$$

So $\uparrow S$ is the set of all elements in P above some element in S, and is called the filter *generated by* S. For $y \in P$ we define

$$\uparrow y = \uparrow \{y\} = \{x \in P \mid y \leq x\}.$$

Condition 1 in the definition of a filter is equivalent to "If $x \in F$, then $\uparrow x \subseteq F$".

Definition 1.4. A subset D of a partially ordered set P is said to be *dense* if $\uparrow D = P$.

This is a very compact way of writing "D is dense if for every $x \in P$ there exists $y \in D$ such that $y \leq x$". Informally a set is dense if every element in P can be obtained by going upwards from some element in the dense set.

We will finish with a number of examples of partial orders and the above definitions.

Examples.

1. Let X be an arbitrary set and let $\mathcal{P}X = \{S \mid S \subseteq X\}$ be the power set of X, i.e. the set of all subsets of X. Then X can be ordered by inclusion. $\mathcal{P}X$ is totally ordered if and only if X is empty or X is a singleton. The only maximal element is X. As an example of a partial order with multiple maximal elements, consider $\mathcal{P}X \setminus \{X\}$ ordered by inclusion. For this set, $X \setminus \{x\}$ is maximal for each $x \in X$.

   If $\mathcal{S}$ is a subset of $\mathcal{P}X$, that is, $\mathcal{S}$ is a set of subsets of X, then the union $\bigcup \mathcal{S}$ is an upper bound for $\mathcal{S}$. This shows that all subsets of $\mathcal{P}X$ have an upper bound, but this upper bound might be outside the subset, for instance if $\mathcal{S} = \{\{x\}, \{y\}\}$ where $x \neq y$. In the partially ordered set $\mathcal{P}X \setminus \{X\}$, not all subsets have an upper bound, since the union might equal the entire set X.

   Suppose that X is infinite. Then the set of infinite subsets of X with a finite complement forms a non-trivial filter in $\mathcal{P}X$. A subset of $\mathcal{P}X$ is dense if and only if it contains the empty set. Notice that this happens for all partial orders with a minimal element.

2. We will look at number sets. $\mathbb{N}$ ordered by the standard $\leq$ relation is an example of a well-order. $\mathbb{Z}$ is totally ordered, but not well-ordered by $\leq$, since for example the subset $\mathbb{Z}$ itself has no minimal element. All filters in $\mathbb{Z}$ are of the form $\{n \in \mathbb{Z} \mid n \geq m\}$ for a certain $m \in \mathbb{Z}$. Every dense set must be an infinite decreasing sequence, for instance $\{0, -2, -4, -6, \dots\}$.

3. Let P be the set of partial functions from X to Y, where X and Y are arbitrary sets. A partial function from X to Y is a function f with $\mathrm{dom}(f) \subseteq X$ and $\mathrm{im}(f) \subseteq Y$, so f need not be defined on the entire domain X. An interesting order is reverse inclusion:

   $$f \leq g \Leftrightarrow \mathrm{dom}(f) \supseteq \mathrm{dom}(g) \text{ and } (\forall x \in \mathrm{dom}(g)) f(x) = g(x),$$

   or, equivalently,

   $$f \leq g \Leftrightarrow \mathrm{graph}(f) \supseteq \mathrm{graph}(g).$$

   The maximal element of this P is the empty function: the function whose domain is the empty set. The minimal elements are the total functions.

   A slight variation on this example will be important later on. Consider the set P of finite partial functions, which are partial functions with a finite domain. This set contains no minimal elements. If $x \in X$, then the set $D_x = \{f \in P \mid x \in \mathrm{dom}(f)\}$ is dense in P, since every function can be extended to a function with x in its domain.

Chapter 2

Linear algebra in ZFC

The set of true facts depends on the particular model in which one is working. Throughout this chapter, we will work in a model of set theory that satisfies the Axiom of Choice and look at the consequences in linear algebra. In particular, we will define the concept of vector space basis for infinite-dimensional vector spaces and prove that every vector space has a basis assuming the Axiom of Choice. Furthermore it can be useful to know when this axiom can be avoided in the proof. If this is the case, then the theorem might be true in other models of set theory as well. We will show that Choice cannot be avoided in general, but also provide a condition under which vector spaces still have bases.

The material in Section 2.1 is well-known, see for example [3]. Section 2.2 is taken from [5].

2.1 Existence of bases

Many easily provable results from the theory of finite-dimensional vector spaces are less obvious or false in infinite-dimensional spaces. We shall prove some infinite-dimensional versions of several theorems in linear algebra. Analysis of vector spaces usually becomes easier if one has a basis for the vector space. The infinite-dimensional analogue of a basis for a finite-dimensional vector space is called a Hamel basis.

Definition 2.1. A subset B of a vector space V over a field K is called a *Hamel basis* if the following conditions hold:

1. Every finite subset of B is linearly independent.

2. Every vector $v \in V$ can be written as

$$v = v_1 b_1 + \cdots + v_n b_n$$

for certain $n \in \mathbb{N}$, $v_i \in K$, $b_i \in B$.

Note that both conditions in this definition involve a finiteness constraint: only finite linear combinations are allowed. This is necessary because it is impossible to speak about infinite sums in vector spaces without additional structure.

As an example of a Hamel basis, consider the vector space

$$V = \{(x_1, x_2, \dots) \mid x_i \in \mathbb{R}, \text{ only a finite number of } x_i \text{ is nonzero}\}.$$

All finite subsets of the set $B = \{(1,0,0,\dots),(0,1,0,\dots),(0,0,1,\dots)\}$ are linearly independent and every element $v \in V$ can be written as a finite linear combination of vectors in B, since the number of nonzero entries in v is finite. Hence B is a Hamel basis for V. The restriction on the number of nonzero entries is crucial, since B does not form a basis for $\mathbb{R}^\omega = \{(x_1, x_2, \dots) \mid x_i \in \mathbb{R}\}$: the vector $(1,1,1,\dots)$, for example, cannot be written as a finite linear combination of vectors in B. It is not obvious whether this vector space has a Hamel basis at all. However, the following theorem shows that it does.

Theorem 2.2. *Every vector space over every field has a Hamel basis.*

Proof. Let V be a vector space over a field K, and let P be the collection of all subsets of V satisfying condition 1 in the definition of a Hamel basis. P is non-empty since $\varnothing \in P$. We will use Zorn's Lemma to show that P, ordered by inclusion, contains a maximal element. This element will turn out to be a basis for V.

Let $\mathcal{C}$ be an arbitrary chain in P. Define $X = \bigcup \mathcal{C}$, then clearly X is an upper bound for $\mathcal{C}$. In order to show that $X \in P$, let $\{x_1, \dots, x_n\}$ be a finite subset of X. For all i, $x_i \in C_i$ for some $C_i \in \mathcal{C}$, since $X = \bigcup \mathcal{C}$. Because $\mathcal{C}$ is a chain, all C_i are contained in $C \in \mathcal{C}$, where C is the maximum of $C_1, \dots, C_n$ under the inclusion order. Hence $x_i \in C$. Since C satisfies condition 1, the set $\{x_1, \dots, x_n\}$ is linearly independent, so $X \in P$, as desired. Every chain in P has an upper bound in P, so by Zorn's Lemma P possesses a maximal element B.

We will show that B is a Hamel basis by checking both criteria. The first one is obvious, since $B \in P$. Suppose that there is a vector $v \in V$ that cannot be written as a linear combination of vectors in B. We will derive a contradiction by showing that every finite subset of $B \cup \{v\}$ is linearly independent. Let $B' \subseteq B \cup \{v\}$ be finite. If $v \notin B'$, then $B' \subseteq B$, which implies that B' is linearly independent. If $v \in B'$, then B' is also linearly independent, since v is no linear combination of vectors in B. Therefore $B \cup \{v\} \in P$, contradicting the maximality of B. □

This proof is non-constructive, since it uses Zorn's Lemma. For example, the proof does not allow us to write down an explicit basis for $\mathbb{R}^\omega$, even though we know it exists.

Other well-known theorems can easily be derived once the existence of bases is established. One example is the following.

Corollary 2.3. *Let V be a vector space over K. Then each subspace S of V has a linear complement, i.e. there is a subspace T of V such that $S \cap T = \{0\}$ and $S + T = V$.*

Proof. Let B be a basis for S. This basis can be extended to a basis $B' \supseteq B$ for V. This follows from application of Zorn's Lemma to the set of linearly independent subsets of V containing B'; the details are very similar to the proof of Theorem 2.2, but with P consisting only of the linearly independent subsets S of V for which $B \subseteq S$. Then $\mathrm{Span}(B' \setminus B)$ is the linear complement of S. □

In some cases, it is possible to prove the existence of bases without invoking Zorn's Lemma.

Theorem 2.4. *Every vector space generated by a countable number of elements has a Hamel basis.*

Proof. Of course, this theorem is implied by Theorem 2.2, but here it will be shown without the use of Zorn's Lemma. Consider a vector space V that is generated by a countable number of elements: $V = \mathrm{Span}\{v_1, v_2, \ldots\}$. Let $B_0 = \varnothing$ and define B_n recursively as follows: let $S_n \subseteq \{v_1, v_2, \ldots\}$ be the set of vectors linearly independent from B_{n-1}. If $S_n = \varnothing$, then define $B_n = B_{n-1}$. Otherwise choose the $v_i \in S_n$ with lowest index i, and define $B_n = B_{n-1} \cup \{v_i\}$. Thus we obtain a chain of linearly independent sets $B_0 \subseteq B_1 \subseteq B_2 \subseteq \cdots$. Now set

$$B = \bigcup_{n \in \mathbb{N}} B_n.$$

We claim that B is a Hamel basis for V.

1. If $B' \subseteq B$ is finite, then every element of B' is contained in some B_n, since $B = \bigcup B_n$ and $\{B_n \,|\, n \in \mathbb{N}\}$ is a chain. Therefore B' is linearly independent.

2. Since V is generated by v_1, v_2, …, it suffices to prove that each v_i can be written as a linear combination of vectors in B. Suppose that this does not hold for v_i, then $B \cup \{v_i\} = \bigcup B_n \cup \{v_i\}$ is linearly independent, hence $v_i \in S_n$ for all n. But from the definition of S_n it follows that $v_i \notin S_{i+1}$, because the linear independent vector with lowest index is removed from S_n in every iteration. Therefore any vector can be written as a linear combination of elements in B. □

This proof works in every model of ZF, so countably generated vector spaces have a basis in every model. Moreover, this basis is constructible by the method in the above proof. The theorem can be generalized by substituting an arbitrary well-ordered set for the countable set of generators, since the recursion can be performed over any well-ordered set.

2.2 Necessity of the Axiom of Choice

One might wonder whether the proof of Theorem 2.4 can be generalized to uncountable generating sets. Unfortunately, this is not true. In this section it will be shown that some form of the Axiom of Choice is necessary to prove the existence of bases for all vector spaces.

We will start by introducing some definitions. In the following, I will denote an index set, X_i for $i \in I$ a non-empty set of variables for which $X_i \cap X_j = \varnothing$ whenever $i \neq j$, and $X = \bigcup_{i \in I} X_i$. Furthermore, k is an arbitrary field, and $k(X)$ denotes the field of rational functions with coefficients in k and variables in X.

Definition 2.5. Let $f \in k(X)$, $f \neq 0$ be a monomial, written as $f = \alpha x_1^{n_1} x_2^{n_2} \cdot \ldots \cdot x_m^{n_m}$ for $x_j \in X$. Then the *i-degree* of f is $d_i(f) = \sum_j n_j$ where the sum is taken over all j for which $x_j \in X_i$.

Example 2.6. Take the sets of variables $X_1 = \{x_1, x_2\}$ and $X_2 = \{y_1, y_2, y_3\}$, and let $f = 3x_1x_2^5y_1^2y_3$. Then $d_1(f) = 6$ and $d_2(f) = 3$.

Every rational function in $k(X)$ can be written in the form

$$\frac{f_1 + f_2 + \cdots + f_n}{g_1 + g_2 + \cdots + g_m}$$

for certain monomials $f_1, f_2, \ldots, f_n$ and $g_1, g_2, \ldots, g_m$. In the proof that existence of bases implies the Axiom of Choice, we will use a field consisting of rational functions of this form where all f_k and g_k have the same i-degree for all i. The next definition will simplify the terminology a little.

Definition 2.7. A rational function

$$\frac{f_1 + f_2 + \cdots + f_n}{g_1 + g_2 + \cdots + g_m} \in k(X)$$

is called *i-homogeneous of degree 0* if all f_k and g_k have the same i-degree.

Example 2.8. Let X_1 and X_2 be as in Example 2.6. The function

$$\frac{3x_1x_2^5y_1^2y_3 - x_1^6}{x_2^6y_1^3 + x_1^3x_2^3y_1y_2y_3 - 5x_1x_2^5y_2^3}$$

is 1-homogeneous of degree 0, since all monomials it consists of have 1-degree 6. However, it is not 2-homogeneous of degree 0.

In order to show that the Axiom of Choice is necessary to prove Theorem 2.2, we will first prove that existence of bases implies the Axiom of Multiple Choice. Since this axiom is equivalent to Choice, this shows that Choice is a necessary condition for existence of bases. This proof is a slight adaptation of the one found in [1, 5].

Theorem 2.9. *If every vector space over each field has a basis, then the Axiom of Choice holds.*

Proof. Let k be a field. The choice of k is immaterial, but for definiteness take $k = \mathbb{F}_2$. Let $\{X_i \mid i \in I\}$ be an arbitrary family of non-empty sets and set $X = \bigcup_{i \in I} X_i$. By the remarks preceding this theorem, it suffices to find a family F_i of finite non-empty subsets of X_i. Define

$$K = \{f \in k(X) \mid f \text{ is } i\text{-homogeneous of degree 0 for all } i \in I\}.$$

Then K is a subfield of $k(X)$, which implies that $k(X)$ can be viewed as a vector space over K. By hypothesis, the vector space $k(X)$ over K has a basis B.

Fix $i \in I$. Since B is a basis, any monomial $x \in X_i$ can be expressed as a linear combination

$$x = x_1b_1 + x_2b_2 + \cdots + x_nb_n$$

where $x_j \in K$, $b_j \in B$. Now we will show that x_j/x does not depend on the choice of the monomial x, i.e. $x, y \in X_i$ implies $x_j/x = y_j/y$.

Let $x, y \in X_i$ and write

$$x = x_1b_1 + x_2b_2 + \cdots + x_nb_n;$$

$$y = y_1c_1 + y_2c_2 + \cdots + y_mc_m.$$

We can rewrite y as

$$y = \frac{y}{x}x = \frac{y}{x}\left(x_1b_1 + x_2b_2 + \cdots + x_nb_n\right).$$

Since expressions in terms of basis vectors are unique and $\frac{y}{x} \in K$, it follows that $n = m$, $b_j = c_j$, and $y_j = \frac{y}{x}x_j$ for each $j \in \{1, \ldots, n\}$. Thus $x_j/x = y_j/y$. Since x_j/x depends only on i and j, we can call it α_{ij}.

Since $x_j \in K$, the rational function x_j is by definition i-homogeneous of degree 0 for all i. Therefore, for all $j \in \{1, \ldots, n\}$ the denominator of α_{ij} must contain at least one variable in X_i. Define F_i to be the set of variables in the denominator of α_{ij} for some $j \in \{1, \ldots, n\}$. Then each F_i is finite and $\varnothing \neq F_i \subseteq X_i$, so the Axiom of Multiple Choice holds, whence the Axiom of Choice is true. □

Chapter 3

Forcing

In the previous chapter we looked at the consequences of the Axiom of Choice in linear algebra. Because the Axiom of Choice is controversial, it is interesting to see what remains if the axiom is rejected. In this chapter, it will be shown that rejection of the axiom yields very unexpected results. From Theorem 2.2 and Theorem 2.9 it follows that the existence of bases is equivalent with the Axiom of Choice. It is therefore not surprising that there exist vector spaces without bases if the axiom is rejected. But even worse things can happen: there might exist an infinite-dimensional vector space with only finite-dimensional proper subspaces. The phrase "there might exist" should be read as "there is a model of ZF in which it exists". Because models of set theory are difficult to construct, this chapter will only contain a sketch of the construction.

The construction technique used in this chapter is called *forcing*, and was invented by Paul Cohen (1934–2007). The material on generic extensions is mainly based on [2, 8]. For the symmetric extensions we will follow [7], but we use partially ordered sets instead of Boolean-valued models. Theorem 3.28 comes from [9].

3.1 Relativization

Distinct models of set theory may have different properties. If M is any model of ZF, then of course all axioms of ZF are true in M, as well as all consequences of these axioms. But as there are propositions not implied by the axioms, the choice of M influences the set of true formulas in M. First we will take a closer look at what it means for a formula to be true in a model. For each formula in terms of the symbols of set theory, there is a corresponding formula expressing properties of the model.

Definition 3.1. If φ is a formula and M is any set, then the *relativization* of φ to M, written as φ^M, is obtained by replacing each occurrence of $\forall x \psi$ in ϕ by $\forall x(x \in M \to \psi)$ and each occurrence of $\exists x \psi$ by $\exists x(x \in M \wedge \psi)$.

The expression $\forall x(x \in M \to \psi)$ is usually written as $(\forall x \in M)\psi$ and the expression $\exists x(x \in M \wedge \psi)$ is usually written as $(\exists x \in M)\psi$. Note that the definition does not require M to be a model. The relativization is defined for any set, although the notion is most useful in the case where M is a model.

Intuitively, the relativization φ^M is the formula φ with a new interpretation of the quantifiers: in φ, the sequence of symbols '$\forall x\psi$' is interpreted as "ψ holds for all sets x", while in φ^M, this sequence is interpreted as "ψ holds for all sets x in M". Similar remarks hold for '$\exists x\psi$'. The universe of discourse in φ^M is restricted to M.

The truth or falsehood of a formula φ does not always yield information about the truth of φ^M.

Example 3.2. Let $M = \{\varnothing, \{\varnothing\}\}$. Consider the statement φ:

$$\exists x \exists y \exists z \, (y \in x \wedge z \in x \wedge y \neq z) \, .$$

This is a formal way of expressing that a set containing at least two elements exists, so φ is true. φ^M can be written as

$$(\exists x \in M)(\exists y \in M)(\exists z \in M) \, (y \in x \wedge z \in x \wedge y \neq z) \, .$$

This means, informally, that M contains a set consisting of at least two elements. But since all sets in M contain at most one element, φ^M is false.

Now let ψ be the statement

$$\exists x \forall y \, (y \notin x) \, .$$

Then both ψ, asserting the existence of an empty set, and ψ^M, claiming that M contains a set possessing no elements of M, are true.

If M is a model of ZF, then determining the truth of a relativized proposition is less troublesome: the truth value of φ^M equals the truth value of φ whenever φ has a truth value in ZF. If φ is independent from the axioms, then it might be either true or false in M.

Definition 3.3. Let M be a set and φ a sentence. We write $M \models \varphi$, and say "φ is true in M" or "M is a model for φ", if φ^M is true.

This definition can be extended to sets S of sentences: if $M \models \varphi$ for all sentences $\varphi \in S$, then this will be written as $M \models S$. As an example, note that the phrase "M is a model for ZF" can now be expressed formally as $M \models \mathrm{ZF}$.

3.2 Idea of the construction

We wish to construct a model of ZF with an additional property: the model should contain an infinite-dimensional vector space V for which every proper subspace is finite-dimensional. The axioms of ZF fail to guarantee the existence of V, since there are models in which all infinite-dimensional vector spaces contain infinite-dimensional subspaces. This holds for example if every vector space has a basis, so the Axiom of Choice prevents us from finding V. We will need to create a model violating the Axiom of Choice.

The idea of the construction is as follows. According to the Löwenheim–Skolem Theorem, there exists a countable transitive model, henceforth c.t.m., M of ZFC. At first sight it might seem contradictory that such a countable model exists: it can be proven in ZFC that for instance the uncountable $\mathbb{R}$ exists, so $\mathbb{R} \in M$. But by transitivity it follows that M contains all elements

of $\mathbb{R}$ and hence M is not countable. What in fact happens here is that the set $\mathbb{R}$ in M is different from the "real" $\mathbb{R}$. To avoid ambiguity and confusion, we will employ the symbols $\mathbb{R}$ and $\mathbb{R}^M$. Because M is countable, $\mathbb{R}^M$ must also be countable, i.e. there exists a bijection $f : \mathbb{N} \to \mathbb{R}^M$. But this bijection f is not an element of M, since $M \models (\mathbb{R}^M$ is uncountable). In other words, $\mathbb{R}^M$ is countable when considered as a set in the entire universe, but uncountable when considered as a set in M.

After the resolution of this apparent paradox, the actual construction can begin. If M already satisfies the desired properties, there is no need to continue, so suppose that this is not the case. Then we seek for a set $G \notin M$ and extend M to a larger model $M[G]$ containing G. Unfortunately, this model will satisfy the Axiom of Choice and consequently cannot contain V. We will proceed by removing some sets from $M[G]$, obtaining a new model N for which $M \subseteq N \subseteq M[G]$. Among the removed sets will be many choice functions, well orders and infinite-dimensional subspaces of vector spaces, so when carried out correctly N will be the right model.

The construction involves a number of parameters, among which is the set G. The choice of parameters will influence the true propositions in the models $M[G]$ and N. We will first describe how to construct $M[G]$ and N in general. Thereafter a strategic choice of parameters will yield the desired model.

3.3 Generic extensions

In this section, M will always be a c.t.m. of ZFC. To find a set G, we let $P \in M$ be a partially ordered set with maximal element 1. To be able to control $M[G]$, we let G be a generic filter in P, which means the following.

Definition 3.4. A filter G in P is called *P-generic* over M if $G \cap D \neq \varnothing$ for all dense subsets $D \subseteq P$ with $D \in M$.

We would like $M[G]$ to have the properties $M \subseteq M[G]$, $G \in M[G]$ and, most importantly, $M[G] \models$ ZFC. Roughly speaking, this is achieved by adjoining G to M and taking the closure under set-theoretical operations.

Definition 3.5. A *P-name* is a collection of ordered pairs $< \sigma, p >$ where σ is a P-name and $p \in P$.

This definition appears to be circular, but it is in fact a recursive definition of the class of P-names, as the following example shows.

Example 3.6. $\varnothing$ is vacuously a P-name. It follows that $\{< \varnothing, p >\}$ and $\{< \varnothing, p >, < \varnothing, q >\}$ for $p, q \in P$ are P-names, as well as

$$\{< \{< \varnothing, p >\}, q >, < \{< \varnothing, p >, < \varnothing, q >\}, p >\}$$

et cetera.

Definition 3.7. Given a P-name τ and a subset $G \subseteq P$, define

$$\mathrm{val}(\tau, G) = \{\mathrm{val}(\sigma, G) \mid (\exists p \in G) < \sigma, p > \in \tau\}.$$

This is again a recursive definition. Note that G need not be a generic filter in this definition.

Example 3.8. Always $\mathrm{val}(\varnothing, G) = \varnothing$. If $p \in G$, then $\mathrm{val}(\{< \varnothing, p >\}, G) = \{\varnothing\}$, while if $p \notin G$, then $\mathrm{val}(\{< \varnothing, p >\}, G) = \varnothing$.

Using this terminology we can define a new model that extends M.

Definition 3.9. Let G be a subset of P, then

$$M[G] = \{\mathrm{val}(\tau, G) \mid \tau \in M \text{ is a } P\text{-name}\}.$$

The set $M[G]$ is usually called a *generic extension* of M. We should verify that $M[G]$ satisfies all properties stated earlier. For this, a definition and a lemma might come in handy. Recall that 1 is the maximal element of P.

Definition 3.10. The *canonical name* of $x \in M$ is $\check{x} = \{< \check{y}, 1 > \mid y \in x\}$.

Lemma 3.11. *Let $x \in M$ and let $G \subseteq P$ be a filter, then* $\mathrm{val}(\check{x}, G) = x$.

Proof. By induction on x. If $x = \varnothing$, then by definition $\check{x} = \varnothing$, so $\mathrm{val}(\check{x}, G) = \mathrm{val}(\varnothing, G) = \varnothing = x$. Suppose that $\mathrm{val}(\check{y}, G) = y$ for all $y \in x$. Then, since G is a filter, $1 \in G$, hence

$$\mathrm{val}(\check{x}, G) = \{\mathrm{val}(\check{y}, G) \mid y \in x\} = \{y \mid y \in x\} = x. \qquad \square$$

This lemma shows that every element of M has a name in $M[G]$.

Theorem 3.12. *If $G \subseteq P$ is a filter, then $M[G]$ is a c.t.m. of ZFC for which $M \subseteq M[G]$ and $G \in M[G]$.*

Proof. If $x \in M$, then by Lemma 3.11 $x = \mathrm{val}(\check{x}, G) \in M[G]$ since $\check{x}$ is a P-name, hence $M \subseteq M[G]$.

To see that $G \in M[G]$, note that

$$\mathrm{val}(\{< \check{p}, p > \mid p \in P\}, G) = \{\mathrm{val}(\check{p}, G) \mid p \in G\} = \{p \mid p \in G\} = G.$$

For transitivity, take $x \in y \in M[G]$, then $y = \mathrm{val}(\tau, G)$ for some P-name $\tau \in M$. Because $x \in y = \mathrm{val}(\tau, G)$, there is a P-name σ such that $x = \mathrm{val}(\sigma, G)$, thus $x \in M[G]$.

Next consider the cardinality of $M[G]$. As proven before, $M \subseteq M[G]$, which implies $|M| \leq |M[G]|$. On the other hand,

$$|M[G]| = |\{\mathrm{val}(\tau, G) \mid \tau \in M \text{ is a } P\text{-name}\}| \leq |\{\mathrm{val}(\tau, G) \mid \tau \in M\}| \leq |M|.$$

From the countability of M it follows that $M[G]$ is countable.

It remains to be proven that all axioms of ZF are true in $M[G]$. This proof is long, although the idea is simple: it amounts to checking all axioms one by one. Here we will prove Extensionality and Pairing and refer to [8] for the other axioms.

Extensionality relativized to $M[G]$ becomes

$$(\forall x, y \in M[G])\,[x = y \leftrightarrow (\forall z \in M[G])\,(z \in x \leftrightarrow z \in y)]\,.$$

The 'only if' part of this statement is trivial; the 'if' part follows from transitivity of $M[G]$: if $w \in x \in M[G]$, then $w \in M[G]$, hence $w \in y$. Similarly $w \in y$ implies $w \in x$, thus $x = y$.

To show that Pairing holds, let x and y be sets in $M[G]$ corresponding to the names τ and σ, respectively. Then

$$\mathrm{val}(\{< \tau, 1 >, < \sigma, 1 >\}, G) = \{\mathrm{val}(\tau, G), \mathrm{val}(\sigma, G)\} = \{x, y\}.$$

This shows that $M[G]$ contains a name for the pair $\{x, y\}$. $\square$

3.4 Symmetric extensions

The model $M[G]$ satisfies all axioms of ZF, but it also satisfies the Axiom of Choice. It is therefore impossible that it contains an infinite-dimensional vector space with only finite-dimensional subspaces: if the Axiom of Choice holds, then all vector spaces have a basis, so by removing one element from the basis of an infinite-dimensional vector space we obtain a proper infinite-dimensional subspace. We shall create a restriction of $M[G]$ to obtain a new model.

Definition 3.13. An *automorphism* of P is a bijective map $\pi : P \to P$ for which $x \leq y \Leftrightarrow \pi(x) \leq \pi(y)$ and $\pi(1) = 1$.

Thus an automorphism of a partially ordered set is a bijection onto itself preserving all structure. Every automorphism of P induces a bijection of the set of P-names in the following way.

Definition 3.14. Let π be an automorphism of P, and τ a P-name. Then

$$\pi^P(\tau) = \{< \pi^P(\sigma), \pi(p) > \mid < \sigma, p > \in \tau\}$$

Stated more simply, π^P applies π to all elements of P in its argument, while leaving everything else unchanged. Although the definition looks complicated, the next example might clarify how to use it in practice.

Example 3.15. $\pi^P(\varnothing) = \varnothing$, and

$$\pi^P\left(\{< \{< \varnothing, p >\}, q >, < \{< \varnothing, p >, < \varnothing, q >\}, p >\}\right)$$
$$= \{< \{< \varnothing, \pi(p) >\}, \pi(q) >, < \{< \varnothing, \pi(p) >, < \varnothing, \pi(q) >\}, \pi(p)\}.$$

Lemma 3.16. *For any automorphism π of P, the map π^P preserves canonical names. That is, $\pi^P(\check{x}) = \check{x}$ for each $x \in M$.*

Proof. By induction on x. Trivially $\pi^P(\varnothing) = \varnothing$. Suppose that $\pi^P(\check{y}) = \check{y}$ for all $y \in x$, then

$$\pi^P(\check{x}) = \pi^P(\{< \check{y}, 1 > \mid y \in x\}) = \{< \pi^P(\check{y}), \pi(1) >\} = \{< \check{y}, 1 > \mid y \in x\} = \check{x}.$$

□

Let $\mathcal{G}$ be a group of automorphisms of P. The definition of the model constructed in this section will be relative to the group $\mathcal{G}$ and a certain collection of subgroups of $\mathcal{G}$.

Definition 3.17. A *normal filter* is a nonempty set $\mathcal{F}$ of subgroups of $\mathcal{G}$ for which

1. If $H \in \mathcal{F}$ and $K \supseteq H$ is a subgroup of $\mathcal{G}$, then $K \in \mathcal{F}$.
2. $H \in \mathcal{F}$ and $K \in \mathcal{F}$ imply $H \cap K \in \mathcal{F}$.
3. $\pi \in \mathcal{G}$ and $H \in \mathcal{F}$ imply $\pi H \pi^{-1} \in \mathcal{F}$.

Actually this definition has nothing to do with automorphism groups; normal filters can be defined for a general group as well.

Definition 3.18. Let τ be a P-name.

- $\mathrm{sym}_{\mathcal{G}}(\tau) = \{\pi \in \mathcal{G} \mid \pi^P(\tau) = \tau\}$
- The name τ is said to be *symmetric* (with respect to $\mathcal{G}$ and $\mathcal{F}$) if $\mathrm{sym}_{\mathcal{G}}(\tau) \in \mathcal{F}$.
- If τ is symmetric, then it is *heriditarily symmetric* if σ is heriditarily symmetric for all $<\sigma, p> \in \tau$.

The class of heriditarily symmetric P-names forms a subclass of the class of all P-names. We will use the heriditarily symmetric names to define the model N. The definition of N is almost equal to the definition of $M[G]$, except that it uses only the heriditarily symmetric names, instead of all P-names.

Definition 3.19. Let G be a subset of P, then

$$N = \{\mathrm{val}(\tau, G) \mid \tau \in M \text{ is heriditarily symmetric}\}.$$

The model N is called a *symmetric extension* of M. It depends on the parameters P, G, $\mathcal{G}$ and $\mathcal{F}$, so it should be referred to as $N(P, G, \mathcal{G}, \mathcal{F})$ if one wants to be precise. However, the parameters are usually understood from context, so it suffices to write N.

Theorem 3.20. *Let a partially ordered set P with maximal element 1, a generic filter $G \subseteq P$, a group $\mathcal{G}$ of automorphisms of P and a normal filter $\mathcal{F}$ on $\mathcal{G}$ be given. Then N is a c.t.m. of ZF for which $M \subseteq N \subseteq M[G]$.*

Proof. Again we will only sketch the proof and refer to [7] for the details.

For the inclusion $M \subseteq N$, if $x \in M$, then $\mathrm{val}(\check{x}, G) = x$. From Lemma 3.16 it follows that $\check{x}$ is heriditarily symmetric, thus $x \in N$. The inclusion $N \subseteq M[G]$ follows from the fact that every heriditarily symmetric name is a P-name.

Countability of N follows from the inclusions $M \subseteq N \subseteq M[G]$ and Theorem 3.12.

If $x \in y \in N$, then $y = \mathrm{val}(\tau, G)$ for some heriditarily symmetric P-name τ. It follows that there is a P-name σ for which $x = \mathrm{val}(\sigma, G)$. σ is the first component of some ordered pair in τ, so σ is heriditarily symmetric, hence $x \in N$. This establishes transitivity.

Transitivity implies that N satisfies the Axiom of Extensionality. To show that Pairing holds, let τ and σ be heriditarily symmetric P-names, so $\{\pi \in \mathcal{G} \mid \pi^P(\tau) = \tau\} \in \mathcal{F}$ and $\{\pi \in \mathcal{G} \mid \pi^P(\sigma) = \sigma\} \in \mathcal{F}$. Since $\mathcal{F}$ is a normal filter,

$$\{\pi \in \mathcal{G} \mid \pi^P(\tau) = \tau \text{ and } \pi^P(\sigma) = \sigma\} \in \mathcal{F}.$$

Hence $\{<\tau, 1>, <\sigma, 1>\}$ is a heriditarily symmetric P-name. We omit the proofs of the other axioms. □

3.5 The forcing relation

We would like to have a method for deciding whether a given proposition is true in the model N. The notion of forcing is useful for this purpose.

Definition 3.21. Let $p \in P$ and let $\varphi(\tau_1, \dots \tau_n)$ be a formula whose variables are P-names. We say that p *forces* $\varphi(\tau_1, \dots, \tau_n)$, and write $p \Vdash \varphi(\tau_1, \dots, \tau_n)$, if for all generic $G \subseteq P$ with $p \in G$, we have

$$N(P, G, \mathcal{G}, \mathcal{F}) \models \varphi(\mathrm{val}(\tau_1, G), \dots, \mathrm{val}(\tau_n, G)).$$

In the formal expression $p \Vdash \varphi(\tau_1, \dots, \tau_n)$, the sentence $\varphi(\tau_1, \dots, \tau_n)$ is a statement in the so-called *forcing language*: the language with P-names as variables. Sentences in the forcing language can be expressed in the model M, since all P-names are in M. The sentences should be regarded as purely formal expressions without an interpretation in M, because $\mathrm{val}(\tau, G)$ need not be a member of M. The forcing relation enables us to make assertions about N using sentences expressible entirely in M.

The following Lemma states a direct consequence of the definition of forcing.

Lemma 3.22. *Let $p, q \in P$ with $q \leq p$ and let $\varphi(\tau_1, \dots, \tau_n)$ be a formula in the forcing language for which $p \Vdash \varphi(\tau_1, \dots, \tau_n)$. Then $q \Vdash \varphi(\tau_1, \dots, \tau_n)$.*

Proof. Let $G \subseteq P$ be a generic filter with $q \in G$. Then also $p \in G$, so $N \models \varphi(\mathrm{val}(\tau_1, G), \dots, \mathrm{val}(\tau_n, G))$ since $p \Vdash \varphi(\tau_1, \dots, \tau_n)$. Therefore $q \Vdash \varphi(\tau_1, \dots, \tau_n)$. □

The next result is one of the main theorems of the theory of forcing. It expresses an easy relationship between the forcing relation and truth and is often used to switch back and forth between $\models$ and $\Vdash$. The proof can be found in [8].

Theorem 3.23. *Let φ be a formula, G a generic filter and N the corresponding symmetric model. Then*

$$N \models \varphi(\mathrm{val}(\tau_1, G), \dots, \mathrm{val}(\tau_n, G)) \Leftrightarrow (\exists p \in G) p \Vdash \varphi(\tau_1, \dots, \tau_n)$$

Because symmetric models are based on automorphisms, it is sometimes useful to know the relationship between $\Vdash$ and an automorphism. This is the content of the last part of the following Lemma.

Lemma 3.24. *Let $G \subseteq P$ be a generic filter and $\pi : P \to P$ an automorphism.*

1. *$\pi^{-1}(G)$ is a generic filter.*
2. *$\mathrm{val}(\tau, \pi^{-1}(G)) = \mathrm{val}(\pi^P(\tau), G)$ for every P-name τ.*
3. *$M[\pi^{-1}(G)] = M[G]$*
4. *$N(P, \pi^{-1}(G), \mathcal{G}, \mathcal{F}) = N(P, G, \mathcal{G}, \mathcal{F})$*
5. *If $p \Vdash \varphi(\tau_1, \dots, \tau_n)$, then $\pi(p) \Vdash \varphi(\pi^P(\tau_1), \dots, \pi^P(\tau_n))$.*

Proof.

1. This follows because π is an automorphism and G is a generic filter.

2. By induction on τ. Clearly the assertion holds for $\tau = \varnothing$. Suppose that $\mathrm{val}(\sigma, \pi^{-1}(G)) = \mathrm{val}(\pi^P(\sigma), G)$ for each $< \sigma, p > \in \tau$. Then

$$\begin{aligned}\mathrm{val}(\tau, \pi^{-1}(G)) &= \{\mathrm{val}(\sigma, \pi^{-1}(G)) \mid (\exists p \in \pi^{-1}(G)) < \sigma, p > \in \tau\} \\ &= \{\mathrm{val}(\pi^P(\sigma), G) \mid (\exists p \in \pi^{-1}(G)) < \sigma, p > \in \tau\} \\ &= \{\mathrm{val}(\pi^P(\sigma), G) \mid (\exists \pi(p) \in G) < \pi^P(\sigma), \pi(p) > \in \pi^P(\tau)\} \\ &= \mathrm{val}(\pi^P(\tau), G)\end{aligned}$$

3. We prove the inclusion $M[\pi^{-1}(G)] \subseteq M[G]$, the reverse inclusion then holds because π is an automorphism. Take $x \in M[\pi^{-1}(G)]$ with name τ. Then $x = \mathrm{val}(\tau, \pi^{-1}(G)) = \mathrm{val}(\pi^P(\tau), G)$ by 2, so $x \in M[G]$.

4. Follows from 3, since equal generic models yield equal symmetric submodels.

5. Assume that $p \Vdash \varphi(\tau_1, \ldots, \tau_n)$ and let G be a generic filter with $\pi(p) \in G$. Then $p \in \pi^{-1}(G)$, so

$$N(P, \pi^{-1}(G), \mathcal{G}, \mathcal{F}) \models \varphi(\mathrm{val}(\tau_1, \pi^{-1}(G)), \ldots, \mathrm{val}(\tau_n, \pi^{-1}(G)))$$

By 2 and 4,

$$N(P, G, \mathcal{G}, \mathcal{F}) \models \varphi(\mathrm{val}(\pi^P(\tau_1), G), \ldots, \mathrm{val}(\pi^P(\tau_n), G))$$

Therefore

$$\pi(p) \Vdash \varphi(\mathrm{val}(\pi^P(\tau_1), G), \ldots, \mathrm{val}(\pi^P(\tau_n), G)) \qquad \square$$

3.6 Choice of parameters

The construction of the model N involves the parameters P, G, $\mathcal{G}$ and $\mathcal{F}$. We are ready to choose these parameters appropriately in order to obtain a model containing an infinite-dimensional vector space with only finite-dimensional subspaces.

Partially ordered set. Let P be the set of all finite partial functions from $\mathbb{N} \times \mathcal{P}\mathbb{N} \times \mathcal{P}\mathbb{N}$ to $\{0, 1\}$. That is, a function f is in P if its domain $\mathrm{dom}(f)$ is finite, $\mathrm{dom}(f) \subseteq \mathbb{N} \times \mathcal{P}\mathbb{N} \times \mathcal{P}\mathbb{N}$ and $\mathrm{im}(f) \subseteq \{0, 1\}$. Order this set by reverse inclusion, i.e.

$$f \leq g \Leftrightarrow \mathrm{dom}(f) \supseteq \mathrm{dom}(g) \text{ and } (\forall x \in \mathrm{dom}(g)) f(x) = g(x).$$

The maximal element of this P is the empty function: the function whose domain is the empty set.

Generic filter. We will use countability of M to construct a generic filter. The construction carefully avoids the Axiom of Choice by imitating the proof of Theorem 2.4.

Since M is countable, we can enumerate all dense subsets of P in M as $D_0, D_1, D_2, \ldots$. We can also write $P = \{p_0, p_1, p_2, \ldots\}$ because $P \in M$. Take $p^0 \in D_0$ and define $p^n \in P$ recursively as follows: let $P_n = \{p_i \in D_n \mid p_i \leq$

$p^{n-1}\}$, which is non-empty since D_n is dense. Let p^n be the $p_i \in P_n$ with lowest index i. Thus we obtain a chain $p^0 \geq p^1 \geq p^2 \geq \cdots$. Now set

$$G = \uparrow\{p^n \mid n \in \mathbb{N}\}.$$

Then G is a filter and the intersection $G \cap D_n$ is non-empty for every $n \in \mathbb{N}$ since $p_n \in G$, hence G is P-generic over M.

Automorphism group. If π is any permutation of $\mathbb{N} \times \mathcal{P}\mathbb{N}$, then π can be extended to an automorphism π^* of P. For any $p \in P$, the partial function $\pi^* p$ is defined by

$$\operatorname{dom}(\pi^* p) = \{(\pi(x), y) \mid (x, y) \in \operatorname{dom}(p)\},$$
$$(\pi^* p)(\pi(x), y) = p(x, y).$$

We let $\mathcal{G}$ be the group of automorphisms of P induced by permutations of $\mathbb{N} \times \mathcal{P}\mathbb{N}$.

Note that each π^* induces an automorphism of the set of P-names, which is necessary to define the notion of symmetry. This induced automorphism should be denoted as $(\pi^*)^P$, but to avoid cumbersome notation we will write π^P.

Normal filter. First define for each $E \subseteq \mathbb{N} \times \mathcal{P}\mathbb{N}$ the set

$$\operatorname{fix}_{\mathcal{G}}(E) = \{\pi^* \in \mathcal{G} \mid (\forall e \in E)\pi(e) = e\}.$$

Then let

$$\mathcal{F} = \{H \text{ subgroup of } \mathcal{G} \mid (\exists \text{ finite } E \subseteq \mathbb{N} \times \mathcal{P}\mathbb{N})\, \operatorname{fix}_{\mathcal{G}}(E) \subseteq H\},$$

in other words,

$$\mathcal{F} = \uparrow\{\operatorname{fix}_{\mathcal{G}}(E) \mid E \subseteq \mathbb{N} \times \mathcal{P}\mathbb{N} \text{ is finite}\}$$

where $\uparrow$ is taken with respect to the set of subgroups of $\mathcal{G}$ ordered by inclusion.

Lemma 3.25. *$\mathcal{F}$ is a normal filter on $\mathcal{G}$.*

Proof. $\mathcal{F}$ is non-empty, since $\mathcal{G} \in \mathcal{F}$. We check the properties in the definition of a normal filter.

1. Let $K \supseteq H \in \mathcal{F}$, then there exists a finite E such that $\operatorname{fix}_{\mathcal{G}}(E) \subseteq H \subseteq K$, hence $K \in \mathcal{F}$.

2. If $H, K \in \mathcal{F}$, then there are finite E_1, E_2 for which $\operatorname{fix}_{\mathcal{G}}(E_1) \subseteq H$ and $\operatorname{fix}_{\mathcal{G}}(E_2) \subseteq K$. But as $\operatorname{fix}_{\mathcal{G}}(E_1 \cap E_2) = \operatorname{fix}_{\mathcal{G}}(E_1) \cap \operatorname{fix}_{\mathcal{G}}(E_2)$, we get $\operatorname{fix}(E_1 \cap E_2) \subseteq H \cap K$ and therefore $H \cap K \in \mathcal{F}$.

3. Take $H \in \mathcal{F}$ and $\pi^* \in \mathcal{G}$ and let E be a finite set for which $\operatorname{fix}_{\mathcal{G}}(E) \subseteq H$. We will show that $\operatorname{fix}_{\mathcal{G}}(\pi[E]) \subseteq \pi H \pi^{-1}$. Take $\rho \in \operatorname{fix}_{\mathcal{G}}(\pi[E])$, then $\rho\pi(e) = \pi(e)$ for all $e \in E$. It follows that $\pi^{-1}\rho\pi(e) = e$, so $\pi^{-1}\rho\pi \in \operatorname{fix}_{\mathcal{G}}(E)$, hence $\pi^{-1}\rho\pi \in H$, thus $\rho \in \pi H \pi^{-1}$. Because $\operatorname{fix}_{\mathcal{G}}(\pi[E]) \subseteq \pi H \pi^{-1}$ and $\pi[E]$ is finite, we conclude that $\pi H \pi^{-1} \in \mathcal{F}$. □

These ingredients yield a model N as defined in Definition 3.19. For this specific choice of parameters, a necessary and sufficient condition for $x \in N$ is that there exists a finite $E \subseteq \mathbb{N} \times \mathcal{P}\mathbb{N}$ such that

$$\operatorname{fix}_{\mathcal{G}}(E) \subseteq \operatorname{sym}_{\mathcal{G}}(\tau)$$

where τ is a name for x. Next we shall explore the properties of the model N.

3.7 Linear algebra in N

A number of sets in N will play an important role in the construction. For each $n \in \mathbb{N}$, $S \in \mathcal{P}\mathbb{N}$ define the set

$$x_{nS} = \{T \in \mathcal{P}\mathbb{N} \mid (\exists p \in G) p(n, S, T) = 1\}.$$

Furthermore, let

$$A = \{\{x_{nS} \mid S \in \mathcal{P}\mathbb{N}\} \mid n \in \mathbb{N}\}.$$

These sets have names

$$\xi_{nS} = \{< \check{T}, p > \mid p(n, S, T) = 1\}; \quad \text{val}(\xi_{nS}, G) = x_{nS};$$

$$\alpha = \{< \{< \xi_{nS}, 1 > \mid S \in \mathcal{P}\mathbb{N}\}, 1 > \mid n \in \mathbb{N}\}; \quad \text{val}(\alpha, G) = A.$$

We shall prove in two steps that a vector space over $\mathbb{F}_2$ with underlying set A satisfies many unusual properties.

Definition 3.26. A set S is called *amorphous* if S is infinite and every infinite subset of S has a finite complement.

The first step will be to prove that A is amorphous in N. This already shows that the model is quite strange, as the existence of amorphous sets seems counter-intuitive. This is a consequence of the construction of N: this model contains the set A but not the bijection between $\mathbb{N}$ and A, given by $n \mapsto \{x_{nS} \mid S \in \mathcal{P}\mathbb{N}\}$. The following theorem is therefore true in N, but not in the entire universe; it is even false in $M[G]$.

Theorem 3.27. *$N \models A$ is amorphous*

Proof. Suppose that A is not amorphous; this means that A has an infinite subset $B \in N$ for which $A \setminus B$ is also infinite. Since $B \in N$, the set B has a name β satisfying

$$\text{fix}_{\mathcal{G}}(E) \subseteq \text{sym}_{\mathcal{G}}(\beta)$$

for some finite $E \subseteq \mathbb{N} \times \mathcal{P}\mathbb{N}$.

The set

$$\{p \in P \mid (\forall n \in \mathbb{N})(p \Vdash \{\xi_{nS} \mid S \in \mathcal{P}\mathbb{N}\} \in \beta \text{ or } p \Vdash \{\xi_{nS} \mid S \in \mathcal{P}\mathbb{N}\} \in \alpha \setminus \beta)\}$$

is dense, so by genericity of G there exists $p \in G$ such that for all $n \in \mathbb{N}$

$$p \Vdash \{\xi_{nS} \mid S \in \mathcal{P}\mathbb{N}\} \in \beta \text{ or } p \Vdash \{\xi_{nS} \mid S \in \mathcal{P}\mathbb{N}\} \in \alpha \setminus \beta.$$

Let

$$S_0 = \{n \in \mathbb{N} \mid p \Vdash \{\xi_{nS} \mid S \in \mathcal{P}\mathbb{N}\} \in \beta\}$$

and choose $n, m \in \mathbb{N}$ such that

1. $(n, S), (m, S) \notin E$ for all $S \in \mathcal{P}\mathbb{N}$;
2. $(n, S, T), (m, S, T) \notin \text{dom}(p)$ for all $S, T \in \mathcal{P}\mathbb{N}$;
3. $n \in S_0$;
4. $m \in \mathbb{N} \setminus S_0$.

It is always possible to find such m and n, because E and $\mathrm{dom}(p)$ are finite whilst S_0 and $\mathbb{N} \setminus S_0$ are infinite.

Define a permutation $\pi : \mathbb{N} \times \mathcal{P}\mathbb{N} \to \mathbb{N} \times \mathcal{P}\mathbb{N}$ by $\pi(n, S) = (m, S)$, $\pi(m, S) = (n, S)$ and $\pi(k, S) = (k, S)$ for all $S \in \mathcal{P}\mathbb{N}$, $k \neq n, m$. This permutation is an element of $\mathrm{fix}_{\mathcal{G}}(E) \subseteq \mathrm{sym}_{\mathcal{G}}(\beta)$, so $\pi^P(\beta) = \beta$. We claim that $\pi^P(\xi_{nS}) = \xi_{mS}$. This follows from the next calculation.

$$\begin{aligned} \pi^P(\xi_{nS}) &= \pi^P(\{< \check{T}, q > \mid q(n, S, T) = 1\}) \\ &= \{< \check{T}, \pi^* q > \mid q(n, S, T) = 1\} \\ &= \{< \check{T}, \pi^* q > \mid (\pi^* q)(m, S, T) = 1\} \\ &= \xi_{mS} \end{aligned}$$

From 3 it follows that

$$p \Vdash \{\xi_{nS} \mid S \in \mathcal{P}\mathbb{N}\} \in \beta.$$

According to part 5 of Lemma 3.24,

$$\pi^* p \Vdash \pi^P(\{\xi_{nS} \mid S \in \mathcal{P}\mathbb{N}\}) \in \pi^P(\beta).$$

Therefore

$$\pi^* p \Vdash \{\xi_{mS} \mid S \in \mathcal{P}\mathbb{N}\} \in \beta.$$

By definition of π, we have $\mathrm{dom}(p) = \mathrm{dom}(\pi^* p)$, so 2 implies $p = \pi^* p$. Hence

$$N \models \{x_{mS} \mid S \in \mathcal{P}\mathbb{N}\} \in B,$$

contradicting 4. □

In similar constructions presented in [6, 7, 9], it is asserted that A can be made into a vector space over $\mathbb{F}_2$ by defining operations $+$ and $\cdot$ on A. This could be achieved by taking a countable vector space over $\mathbb{F}_2$, like $\mathbb{F}_2[X]$, and using the fact that A is also countable to transfer the linear structure to A. A problem with this attempt is that it is unclear that the resulting operations exist in the model N. Here we have not been able to solve the problem. Assume for practical reasons that it is possible to define addition and multiplication on A.

The second step will be to show that this vector space satisfies a number of counter-intuitive properties. The proof does not use any details of the construction of the model N, except for the existence of an amorphous set. The same proof would work for any model satisfying this property.

Theorem 3.28. *Let X be a vector space over $\mathbb{F}_2$ with an amorphous underlying set. Then:*

1. *X is infinite-dimensional.*
2. *Every proper linear subspace of X is finite-dimensional.*
3. *X has no basis.*
4. *The only subspaces of X that have a linear complement are $\{0\}$ and X itself.*

5. *The dual space X^* consists of only the zero function.*

Proof.

1. X is infinite but the field of X is finite, so X must be infinite-dimensional.
2. Let Y be a proper subspace of X, and take $v \in Y \setminus X$. If Y would be infinite, then $v + Y$ would be infinite as well, but as Y and $v + Y$ are disjoint, this contradicts the fact that X is amorphous. Thus Y is finite and hence finite-dimensional.
3. Suppose that B is a basis for X. By 1, B is infinite, so for any $b \in B$ the set $B \setminus \{b\}$ is infinite as well. But then the subspace of X spanned by $B \setminus \{b\}$ is infinite-dimensional, contradicting 2.
4. At least one of the subspaces of a complemented pair must be infinite-dimensional, so by 2, one of them must be X.
5. Let $\theta : X \to \mathbb{F}_2$ be a non-trivial linear functional. Then $\ker(\theta)$ is finite-dimensional, so $X/\ker(\theta) \cong \mathrm{im}(\theta) = \mathbb{F}_2$ is infinite-dimensional, which is impossible. □

Conclusion

In this thesis, we have defined the concept of a model of set theory and did linear algebra in several models. The Axiom of Choice played an important role in deciding which statements are true. If this axiom is satisfied by the model, every vector space has a Hamel basis. Furthermore, if we assume that all vector spaces have a basis, then this implies the Axiom of Choice, which shows that Choice is necessary in the proof that every vector space has a basis. In the special case of a countable vector space one can prove the existence of bases in ZF.

It is possible to construct a model of set theory that fails the Axiom of Choice by choosing a suitable partially ordered set P, a generic filter G on P, a group $\mathcal{G}$ of automorphisms of P and a normal filter $\mathcal{F}$ on $\mathcal{G}$ and forming the corresponding symmetric extension N. This model contains an amorphous set and hence an infinite-dimensional vector space whose proper subspaces are all finite-dimensional. Using this fact it can easily be shown that this vector space has no basis and that it enjoys several counter-intuitive properties.

We saw a problem in the construction of the amorphous vector space: although it is possible to define the operations of addition and multiplication, we did not show that these are in the model N. It is unclear to us how to solve this problem, nor whether it is essential for proving existence of a vector space without a basis.

Appendix A

Axioms of ZF

Here we will present an overview of the axioms of ZF, mainly taken from [8]. In Section 1.1 we already saw an axiom about equality of sets.

Axiom of Extensionality. *Two sets are equal if they contain the same elements. Formally,*

$$\forall x \forall y \left(\forall z \left(z \in x \leftrightarrow z \in y \right) \rightarrow x = y \right).$$

The following axioms can be applied to construct new sets from old ones.

Axiom of Pairing. *If x and y are sets, then there exists a set containing x and y and nothing else. This set is denoted $\{x, y\}$. The formal version of this axiom is*

$$\forall x \forall y \exists z \forall w \left(w \in z \leftrightarrow (w = x \vee w = y) \right).$$

Axiom of Union. *The set-theoretical universe is closed under arbitrary unions.*

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists w (z \in w \wedge w \in x))$$

The set y in this axiom is called the union *of x and is unique by Extensionality.*

Axiom of Power Sets. *Each set x has a power set denoted by $\mathcal{P}x$. This set consists of all subsets of x. Uniqueness follows from Extentionality.*

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$$

Next we have two axioms that are actually axiom schemata. This means that they represent an infinite number of axioms, one axiom for each possible formula φ.

Axiom of Comprehension. *Given a set x, it is possible to form the subset of x consisting of all z satisfying $\varphi(z)$.*

$$\forall x \exists y \forall z (z \in y \leftrightarrow (z \in x \wedge \varphi(z)))$$

The set y can be written as $\{z \in y \mid \varphi(z)\}$.

Axiom of Replacement. *The image of a set under a function is again a set. $\varphi(w, z)$ should be a formula with two free variables, where the first one represents points in the domain and the second one points in the range.*

$$(\forall w \exists! z \varphi(w, z)) \rightarrow \forall x \exists y \forall z (z \in y \leftrightarrow \exists w (w \in x \wedge \varphi(w, z)))$$

Until now, we have provided a number of ways to construct new sets given certain sets, but we have not yet established the existence of even a single set. The next axiom postulates the existence of an infinite set, thus showing that the set-theoretical universe is non-empty.

Axiom of Infinity. *There exists a set containing the empty set and containing* $x \cup \{x\}$ *whenever it contains* x*.*

$$\exists x((\forall y(\forall z(z \notin y)) \to y \in x) \wedge \forall y(y \in x \to y \cup \{y\} \in x))$$

This is a rather difficult existence axiom. Together with the Axiom of Comprehension, it can be used to prove the existence of an empty set, which is an easier statement. Let ω be a set satisfying the condition of the Axiom of Infinity and construct, by Comprehension, the subset $\varnothing = \{x \in \omega \,|\, x \neq x\}$. This set satisfies $\forall x(x \notin \varnothing)$. Moreover, it is unique by Extensionality.

The last axiom is rarely used in the development ordinary mathematics, but it proves for example that there is no set x for which $x \in x$.

Axiom of Regularity. *Every set* x *contains a set disjoint from* x*.*

$$\forall x \exists y(y \in x \wedge x \cap y = \varnothing)$$

Appendix B

The basic Fraenkel model

In Chapter 3 we constructed a symmetric model containing an amorphous set and consequently a vector space with many peculiar properties. In the literature, for example in [6, 7, 9], this is achieved using a different method: first, a model of ZF set theory with atoms is constructed. This theory differs from the ordinary ZF set theory in that not every object under consideration is a set. This theory also contains atoms, which are objects that are not sets and do not contain elements. A set is something that can contain atoms and other sets. The model of ZF with atoms is constructed in such a way that it contains an amorphous set. Second, the Jech–Sochor embedding theorem is applied. This theorem transfers a fragment of the theory with atoms to the theory without atoms. This appendix will sketch the method used in the literature.

We shall construct a model of ZF with atoms. Let A be a countable set of atoms, and let $\mathcal{G}$ be the group of all permutations of A. Every $\pi \in \mathcal{G}$ can be extended to an automorphism of the set-theoretical universe, denoted π^V, defined by

$$\pi^V(x) = \begin{cases} \pi(x) & \text{if } x \in A \\ \{\pi^V(y) \,|\, y \in x\} & \text{if } x \notin A \end{cases}$$

To obtain a normal filter, first define for each $E \subseteq A$

$$\operatorname{fix}_{\mathcal{G}}(E) = \{\pi \in \mathcal{G} \,|\, (\forall e \in E)\pi(e) = e\}.$$

Then let

$$\mathcal{F} = \{H \text{ subgroup of } \mathcal{G} \,|\, (\exists \text{ finite } E \subseteq A) \operatorname{fix}_{\mathcal{G}}(E) \subseteq H\}.$$

The proof that $\mathcal{F}$ is a normal filter is similar to the proof of Lemma 3.25. Define for each x

$$\operatorname{sym}_{\mathcal{G}}(x) = \{\pi \in \mathcal{G} \,|\, \pi^V(x) = x\}.$$

We call x *symmetric* if $\operatorname{sym}_{\mathcal{G}}(x) \in \mathcal{F}$, which holds if and only if there exists a finite $E \subseteq A$ such that $\operatorname{fix}_{\mathcal{G}}(E) \subseteq \operatorname{sym}_{\mathcal{G}}(x)$.

We will consider the model

$$V = \{x \,|\, x \text{ is symmetric and } x \subseteq V\}.$$

This model is called the basic Fraenkel model. In general, models of ZF with atoms constructed using a group of permutations of the atoms are called permutation models.

Theorem B.1. *$V \models A$ is amorphous.*

Proof. Suppose that A is not amorphous, then there is a $B \subseteq A$ such that both B and $A \setminus B$ are infinite. V is a model of ZFA, $A \in V$ and $B \subseteq A$, hence $B \in V$. It follows that there is a finite subset $E \subseteq A$ for which $\mathrm{fix}_{\mathcal{G}}(E) \subseteq \mathrm{sym}_{\mathcal{G}}(B)$. Take $x \in B \setminus E$ and $y \in (A \setminus B) \setminus E$, which is possible because B and $A \setminus B$ are infinite, while E is finite. Let $\pi \in \mathcal{G}$ be a permutation for which $\pi \in \mathrm{fix}_{\mathcal{G}}(E)$, $\pi(x) = y$ and $\pi(y) = x$. Such π exists since $x, y \notin E$ and π is indeed a permutation of A because $x, y \in A$ and $E \subseteq A$. Since $\pi \in \mathrm{fix}_{\mathcal{G}}(E) \subseteq \mathrm{sym}(B)$, we get $\pi^V(B) = B$. This means that π permutes the set B, so $\pi(x) \in B$, which is a contradiction. □

The Jech–Sochor embedding theorem enables us to obtain a symmetric model with similar properties. The general formulation is as follows.

Theorem B.2. *Let V be a permutation model with set of atoms A. Then there exists a symmetric model N, a set $A^N \in N$ and a bijection $F : V' \to N'$ for certain $V' \subseteq V$ and $N' \subseteq N$ such that $F(A) = A^N$ and*

$$x \in y \Rightarrow F(x) \in F(y).$$

This theorem states that a subset of V has the same structure as a subset of N. It is not possible to embed the full structure of V in N, because ZF without and with atoms are different theories. However, it is always possible to get V' and N' "sufficiently large" such that N contains an amorphous set. For details and a proof of the embedding theorem see [7].

Bibliography

[1] A. Blass. Existence of bases implies the axiom of choice. *Contemporary Mathematics*, 31:31–33, 1984.

[2] K. Easwaran. A cheerful introduction to forcing and the continuum hypothesis. *ArXiv e-prints 0712.2279*, 2007.

[3] S.H. Friedberg, A.J. Insel, and L.E. Spence. *Linear Algebra*. Prentice Hall, 2003.

[4] P.R. Halmos. *Naive Set Theory*. D. Van Nostrand Company, 1960.

[5] H. Herrlich. *Axiom of Choice*. Springer, 2006.

[6] J.L. Hickman. The construction of groups in models of set theory that fail the axiom of choice. *Bull. Austral. Math. Soc.*, 14:199–232, 1976.

[7] T.J. Jech. *The Axiom of Choice*. North-Holland Publishing Company, 1973.

[8] K. Kunen. *Set Theory, An Introduction to Independence Proofs*. North-Holland Publishing Company, 1980.

[9] H. Laeuchli. Auswahlaxiom in der algebra. *Commentarii Mathematici Helvetici*, 37:1–18, 1963.