university of groningen

faculty of mathematics and natural sciences

Maximal ideals of rings in models of set theory

Bachelor Project Mathematics

January 2017

Student: P. Glas

First supervisor: Prof.dr. J. Top

Second supervisor: Prof.dr. L. C. Verbrugge

Abstract

In this thesis we investigate a method used in set theory, namely Paul Cohen's forcing technique. The forcing technique allows one to obtain models of Zermelo-Fraenkel set theory such that the Axiom of Choice (AC) fails. These models are called symmetric extensions. Properties of algebraic structures that crucially depend on AC do not hold in a symmetric extension. An example of this follows from a theorem proved by Wilfred Hodges in 1973. This theorem states that if every commutative ring with 1 has a maximal ideal, than AC holds. Thus any symmetric extension contains a commutative ring with 1 that has no maximal ideal. A natural question is whether it is possible to find explicitly a commutative ring with 1 that has no maximal ideal in a particular symmetric extension. In this thesis we show that this is the case for a particular symmetric extension known as the Basic Cohen model. First, we study Hodges' proof in detail. After that we introduce the forcing method and study a particular symmetric extension. In this extension we describe a commutative ring with 1 that has no maximal ideal, by using a ring which is essential in Hodges' proof.

Contents

1 Introduction **4**

2 Preliminaries **6**
2.1 Set Theory 6
2.2 Transfinite Induction and Recursion 11
2.3 Axiom of Choice 12
2.4 Model Theory 14

3 Algebra and Choice **17**
3.1 Rings and Trees 17
3.2 Construction of $\mathbb{Q}[T]$ 19
3.3 Properties of $\mathbb{Q}[T]$ 20
3.4 Maximal Ideals and Choice 21
3.5 Additional results 27

4 Forcing **28**
4.1 Motivation and Outline 28
4.2 Generic Extensions 28
4.3 Symmetric Extensions 35
4.4 Construction of a Symmetric Model 39
4.5 Properties of the Symmetric Model 40

5 Discussion **46**

A Vector Space without Basis **47**

1 Introduction

In this bachelor's thesis we will be concerned with a technique used in set theory called *forcing*, which was invented by Paul Cohen[1]. To understand this notion, we first need some historical background.
George Cantor, who founded set theory as an independent branch of mathematics at the end of the 19th century, introduced the notion of a cardinal number for infinite sets. Informally speaking, a cardinal number of a set corresponds to the size of that set. Cantor showed that the set of natural numbers and the set of real numbers have different cardinal numbers. He also conjectured that there is no cardinal number between the cardinal number of the natural numbers and the cardinal number of the continuum. This conjecture became known as the Continuum Hypothesis (CH).[2]
Cantor's approach to sets was non-axiomatic. In 1908, Zermelo and Fraenkel proposed a set of axioms for sets, denoted by ZF. Some time after that Zermelo and Fraenkel also included the Axiom of Choice (AC), which gives the theory ZFC. This theory was accepted by most of the mathematical community as an appropriate foundation of mathematics. However, it took about 30 more years before some real progress was made with respect to CH. In 1940 Kurt Gödel showed that CH is consistent with respect to ZFC[3]. This means that if we assume that no contradiction can be derived from the axioms of ZFC, then this is also the case for the axioms of ZFC with CH included. This gave mathematicians who hoped that it was possible to derive CH from ZFC more confidence in their search for such a proof. However, in 1963 Paul Cohen showed that the negation of CH is also consistent with respect to ZFC[1]. This result together with Gödel's work showed that CH is independent of ZFC: neither CH nor its negation are derivable from ZFC. Moreover, Cohen showed that the same holds for AC with respect to ZF.
The method which Cohen used to establish his results is called forcing. The relative consistency of a statement with respect to a collection of axioms is established by constructing a *model* for the axioms together with the statement. Informally, a model for a set of axioms in set theory is a set in which all the axioms are true. In this thesis we investigate Cohen's forcing technique, applied to models of ZF in which AC fails. We will focus our attention on results in the field of algebra that are related to AC. It has been shown that every commutative ring with 1 has a maximal ideal if and only if AC holds. Thus any model of ZF+$\neg$AC[1] contains a commutative ring with 1 that has no a maximal ideal. The question then arises whether it is possible to construct a model of ZF in which we can explicitly find such a ring. As far as we know, this question has not been addressed in the literature. In this thesis we show how to find a commutative ring with 1 that has no maximal ideal in one of Cohen's models of ZF+$\neg$AC.

[1]By this we mean any model in which all axioms of ZF are true and AC fails

The structure of this thesis is as follows. Chapter 2 contains the necessary preliminaries from set theory. In Chapter 3 we discuss several results in algebra which are related to AC. Our main focus will be on Wilfred Hodges' result from 1973 that if every commutative ring with 1 has a maximal ideal, then AC holds[4]. We present his proof in this thesis, and provide additional details and some examples of the constructions that Hodges introduces in his proof. In Chapter 4 we turn to a particular model of ZF in which AC fails. We will provide many details of the construction, since the method is quite technical. We show that in one of Cohen's models where the Axiom of Choice fails, we can explicitly find a commutative ring with 1 that has no maximal ideal in the model. Additionally, in one of the appendices we show how to adapt this model in order to obtain a vector space without basis.
We assume that the reader has some basic knowledge of the language of first-order logic and set theory, and we assume familiarity with algebraic structures such as groups, rings and fields on the level of a second year undergraduate course in rings and fields.
I would like to thank Professor Top for the help and guidance that he offered during this project. One thing which I learned from him is to appreciate examples, which can really help you understand definitions or proofs. The meetings with Professor Top were always a pleasure. I also would like to thank Professor Verbrugge for her willingness to go beyond her obligations as a second supervisor by providing me with additional feedback. Finally, I would like to thank my two good friends Annelies en Roos, with whom I studied together for almost every day during the past six months. This made studying at the university even more pleasant.

2 Preliminaries

In this chapter we introduce the reader to the concepts from set theory and model theory that we will use in chapter 3 and 4. We follow the presentation as given in [5] and [6].

2.1 Set Theory

In set theory we study the properties of sets. The reader is probably familiar with the use of sets in mathematics. We will therefore not bother you with introducing the basic set-theoretical operations such as intersection, union, etc. We use the following convention with respect to the relations $\subseteq$ and $\subset$: $\subseteq$ indicates the subset-relation, possibly with equality, while $\subset$ indicates the *proper* subset-relation.
As in most fields of mathematics, we start with a list of axioms. In this thesis we will be concerned with ZF, the theory consisting of the axioms formulated by Zermelo and Fraenkel. These axioms either assert the existence of particular sets, or tell us how to find new sets from given sets. For future reference I will list the axioms here, accompanied with a short explanation.

1. *Extensionality.* two sets are equal if they contain the same elements. Formally,
$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

2. *Foundation.* Every nonempty set contains an element which is disjoint from itself:
$$\forall x (\exists y (y \in x) \rightarrow \exists y (y \in x \wedge \neg \exists z (z \in x \wedge z \in y)))$$
As a consequence of Foundation, $x \in x$ cannot occur. Also, there does not exist an infinite sequence $... \in x \in y \in z$.

3. *Restricted Comprehension Scheme.* For every set z, every subcollection y defined by a formula φ is also a set. Formally, for every formula φ with free variables among x, z, w_1,..., w_n,
$$\forall z \forall w_1, ..., w_n \exists y \forall x (x \in y \leftrightarrow (x \in z \wedge \varphi)).$$
For instance, if x and y are sets then it follows from Comprehensions that $x \cap y = \{z \in x : z \in y\}$ is a set.

4. *Pairing.* For any two sets x, y there exists a set z containing exactly those two sets, $\{x, y\}$ (uniqueness follows by Extensionality):

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

5. *Union.* The union of a set x, denoted by $y := \bigcup x$ is also a set:

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

   It is common practice to write $x \cup y$ for $\bigcup \{x, y\}$. Thus, $\bigcup x$ is the set containing precisely those elements of the sets which are elements of x.

6. *Power Set.* For every set x there exists a set which contains precisely those sets as elements which are subsets of x. We call this set the power set of x, and denote it $\mathcal{P}x$.

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

   Note that $x \in \mathcal{P}x$, since every set is a subset of itself.

7. *Replacement Scheme.* The image of a set under a function is also a set. Formally, for every formula φ with free variables z, w,

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

8. *Infinity.* There exists a set containing infinitely many elements:

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

The first seven axioms tell us how to obtain sets from given sets. Infinity is the only axiom which postulates unconditionally the existence of a set. Let us call this set $\mathbb{N}$. We can use this set to show that there exist other sets, such as an empty set: $\emptyset = \{x \in \mathbb{N} : x \neq x\}$. That $\emptyset$ is the only empty set follows from Extensionality. Also note that there are actually infinitely many axioms, since Replacement and Restricted Comprehension are axiom schemes: we have an axiom for any formula φ.
We can represent mathematical objects such as numbers, ordered pairs and functions by sets. For instance, $0 := \emptyset$, $1 := \{\emptyset\}$. Note that 1 as defined here is a set because we can apply Pairing with $x = y = 0$, and the observation that $\{x\} = \{x, x\}$ (apply Extensionality). If we use Pairing again with $\{x\}$ and $\{x, y\}$, we obtain the ordered pair $(x, y) := \{\{x\}, \{x, y\}\}$. Finally, a function is a set of ordered pairs $f = \{(x, y) : \forall x \forall y_1 \forall y_2 (((x, y_1), (x, y_2) \in f) \rightarrow y_1 = y_2)\}$. Note that '$(x, y_1), (x, y_2) \in f$' is an abbreviation of the

formula '$(x, y_1) \in f \wedge (x, y_1) \in f$'. To enhance the readability of this text we will sometimes use abbreviations when the intended formula is clear. Given a function f, we will denote the domain of f by $dom(f)$, the range of f by $ran(f)$ and the image of f by $im(f)$.
We need the notions 'universe' and 'class' from set theory. First we need a place where all our set theory takes place, a so-called universe. This is the universe of all sets, which we will denote by V. This universe is an example of what is called a *proper class*: a collection which is not a set from the viewpoint of ZF. We need to introduce classes because if we assume that every specifiable collection is a set, called Unrestricted Comprehension, we run into contradictions such as Russell's paradox.

Example 2.1. Consider $R = \{x : x \notin x\}$, and suppose that R is a set. Then $R \in R$ if and only if $R \notin R$, a contradiction. However, R as defined here is not necessarily a set in ZF since we are only allowed to consider specifiable subcollections of already existing sets by Restricted Comprehension Scheme. It follows from Foundation that there is no set which is an element of itself, for if x is a set with $x \in x$ then $\{x\}$ does not have an element disjoint from itself. Now we are assured that R is not a set, since for all sets x we have $x \notin x$, thus R would be the set of all sets. But that implies $R \in R$, a contradiction with Foundation.

In the remaining part of this thesis, we denote Restricted Comprehension Scheme by 'Comprehension'. We now proceed with orderings on sets. Given a set P, we can use the Cartesian product $P \times P = \{(p, q) : p, q \in P\}$ to define the notion of a partial order $\leq$, a subset of $P \times P$. Note that we are not using Unrestricted Comprehension here, since $(p, q) \in \mathcal{P}(\mathcal{P}(P))$. We use the conventional notation $p \leq q$ for the statement $(p, q) \in \ \leq$.

Definition 2.2. A *partially ordered set*, or a *poset*, is an ordered pair $\mathbb{P} = (P, \leq)$ with P a set and a subset $\leq \ \subseteq P \times P$ such that the following properties are satisfied for all $p, q \in P$:

1. $p \leq p$.

2. $p \leq q$ and $q \leq p$ imply $p = q$.

3. $p \leq q$ and $q \leq q$ imply $p \leq q$.

These properties are usually called *reflexivity*, *anti-symmetry* and *transitivity*. Two elements in $p, q \in P$ are called *comparable* if $p \leq q$ or $q \leq p$ holds. $\mathbb{P}$ is called *linearly ordered* if all elements in P are comparable. In such a case we call $\leq$ a *linear order*.

In the remaining part of this thesis, we will denote the poset $\mathbb{P}$ by P.

Example 2.3. Take an arbitrary set P, and order $\mathcal{P}(P)$ by saying that for any $A, B \subseteq P$, $A \leq B$ if and only if $A \subseteq B$. It is easily verified that $(\mathcal{P}(P), \subseteq)$ is a partially ordered set. Alternatively, we could reverse the order and still obtain a partial order: $A \leq B$ iff $B \subseteq A$.

An element p of a poset P is called *maximal* if for all $q \in P$, $p \leq q$ implies $p = q$. Similarly, An element p of a poset P is called *minimal* if for all $q \in P$, $q \leq p$ implies $p = q$. Finally, if $Q \subseteq P$, then $p \in P$ is called an *upper bound* for Q if $q \leq p$ for all $q \in Q$. A poset can have many maximal or minimal elements, since not all elements might be comparable. A linearly ordered set $(L, \leq)$ is called *well-ordered* if any subset $S \subseteq L$ has a minimal element. In this case we say that $\leq$ is a *well-order*.
We will now introduce ordinals. First we need to define a *strict* linear order. Given a set O, a relation $< \ \subseteq O \times O$ is called a *strict linear order* if $<$ satisfies transitivity, irreflexivity and a property called *trichotomy*, defined as follows. For all $x, y \in O$ we have exactly one of the following three properties: $x < y$, $y < x$ or $x = y$. The set $(O, <)$ is said to be *strictly linearly ordered*. A *strict well-order* is a strict linear order $<$ with the same additional property that defines a well-order $\leq$. We call $(O, <)$ a *strictly well-ordered* set in such a case. We note that from a strict linear order $<$ we can obtain a linear order $\leq$ as follows. If $(O, <)$ is a strictly linearly ordered set, then we obtain a linearly ordered set $(O, \leq)$ if we put

$$\leq \ = \ < \cup \{(x, y) \in O \times O : x = y\}.$$

Similarly, given a linearly ordered set $(O, \leq)$ we obtain a strictly linearly ordered set $(O, <)$ if we put

$$< \ = \ \leq \ \setminus \{(x, y) \leq : x = y\}.$$

When we consider a partial ordered set $(P, \leq)$ and for $p, q \in P$ we write $p < q$, this must be understood as an abbreviation of $p \leq q \wedge p \neq q$.

Definition 2.4. A set A is called *transitive* if for all $x \in A$ and all y, $y \in x$ implies $y \in A$.

Note that $(O, \in)$ is not a partially ordered set, since that implies $x \in x$ for every $x \in O$, which is not allowed by Foundation. However, $(O, \in)$ is a strictly well-ordered set if we let for all $x, y \in O$, $x < y$ if and only if $x \in y$.

Definition 2.5. A set α is an ordinal if α is transitive and $(\alpha, \in)$ is a strictly well-ordered set.

Let $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, and continue in this way such that n is the set containing $0, .., n - 1$. These sets are the finite ordinals. We can

also define the first infinite ordinal, $\omega = \{0, 1, 2, ...\}$, containing all finite ordinals. We can continue in this way by letting $\omega + 1 = \omega \cup \{\omega\}$. So we can keep counting into the infinite.
We need to make a distinction between *successor* ordinals and *limit* ordinals. For any ordinal α, let $S(\alpha) = \alpha \cup \{\alpha\}$.

Definition 2.6. Let α be any ordinal. Then

- α is called a *successor ordinal* if there exists some ordinal β such that $\alpha = S(\beta)$.
- α is called a *limit ordinal* if $\alpha \neq 0$ and α is not a successor ordinal.

Example 2.7. Any finite ordinal is a successor ordinal. ω is a limit ordinal.

Ordinals enable us to extend recursive definitions and induction beyond the natural numbers, called transfinite recursion/induction respectively. Details are given in the next section. The proof of the next theorem can be found in [6], chapter 4.

Theorem 2.8. *Every well-ordered set is isomorphic (with respect to the ordering) to a unique ordinal.*

Besides ordinals we also need the notion of a cardinal. The cardinality of a finite set with n elements is n. Infinite cardinals correspond to certain limit ordinals. We denote them by $\aleph_0, \aleph_1, ...$ The cardinality of a set S is defined as the cardinal for which there exists a bijection onto S. Often, the cardinality of a set is called its size. $\aleph_0$ is the cardinality of the set of natural numbers. A set S is called *countable* if it has the same cardinality as some subset of the natural numbers. A set S is called *uncountable* if it is not countable. When we say that a set is countable we shall always mean countable and infinite (see Definition 2.18).
The remaining part of this chapter introduces some more terminology.

Definition 2.9. A filter $G \subseteq P$ of a poset P is a set satisfying

1. if $p \in G$ and $p \leq q \in P$, then $q \in G$.
2. For all $p, q \in G$ there exists a $r \in G$ such that $r \leq p$ and $r \leq q$.

Example 2.10. Consider the set $\mathbb{N}$ with the usual ordering. This is a well-ordered set. Now consider $\mathbb{Z}$. This set is totally ordered but not well-ordered, since $\mathbb{Z}$ has several subsets without minimal element, for instance $\mathbb{Z}$ itself. A filter on $\mathbb{Z}$ is given by $\{m \in \mathbb{Z} : n \leq m\}$ for a particular n.

Example 2.11. Consider the set E of even positive integers, a subset of $\mathbb{N}$. Order E by saying $p \geq q$ iff $p|q$, i.e. p divides q. This gives a partial order on E. Moreover, E has a unique maximal element 2. A filter on E is given by $\{n \in E : n = 2^m \text{ for some } m \in \mathbb{N}_{>0}\}$.

Definition 2.12. A set $D \subseteq P$ of a poset P is called *dense* iff for all $p \in P$ there exists a $q \in D$ with $q \leq p$.

Example 2.13. Consider E as in Example 2.11. A trivial example of a dense set in E is E. Another example is the set $D = \{n \in E : n = 2^m \text{ for some } m = 2k, k \in \mathbb{N}_{>0}\}$.

2.2 Transfinite Induction and Recursion

In this section, we will discuss the extension of induction and recursion to (and beyond) the ordinals. Suppose C is a class contained in ON, the class of all ordinal numbers. ON is not a set in ZF. First we prove the Transfinite Induction theorem.

Theorem 2.14. *Suppose $C \subseteq ON$ such that $C \neq \emptyset$. Then C has a least element with respect to $\in$.*

Proof. Recall that ordinals are transitive and strictly well-ordered by $\in$. If x, y are ordinals, we have exactly one of the following: $x \in y$, $y \in x$ or $x = y$. Thus to find a least element of C we have to show that there is some $x \in C$ such that $x \cap C = \emptyset$. Take arbitrary $y \in C$. If $y \cap C \neq \emptyset$ then since y is an ordinal there exists an $\in$-least element $x \in y \cap C$. Suppose $z \cap C \neq \emptyset$. Then there is some ordinal $z \in x \cap C$, which implies $z \in y \cap C$. This is a contradiction, since x was the least element with this property. □

How is this theorem used in practice, i.e. how does one prove a property by transfinite induction for all ordinals α? This is done similarly as in a proof by induction on the natural numbers: for a property φ we show that if φ holds for all $\beta < \alpha$, then φ holds for α. This establishes φ for all ordinals, because if not, then there exists by Theorem 2.14. a least ordinal for which φ does not hold, which gives a contradiction.
However, the version of induction that we will use throughout the text is a generalization of Theorem 2.14. We can also have induction on well-founded, set-like relations. The definition of well-foundedness is not important since all sets which we consider are well-founded by Regularity. A relation is set-like if it resembles the $\in$-relation. We will use induction on $\in$, which is obviously set-like.

Recall that for natural numbers, a function is defined recursively on $\mathbb{N}$ when for given n, $f(n)$ is defined in terms of $m < n$ with $m, n \in \mathbb{N}$. We can do so similarly for ordinals, but we need to show that such functions are well-defined. This is the transfinite Recursion Theorem. A proof can be found in [5]. A *class function* is a function such that the domain and range form a class.

Theorem 2.15. *Suppose we have a class function $F : V \to V$. Then there is a unique class function $G : ON \to V$ such that for all ordinals α,*

$$G(\alpha) = F(\{G(\beta) : \beta \in \alpha\}).$$

Thus given any ordinal α, we can define G on α by considering how G is defined on all ordinals $\beta \in \alpha$. Transfinite induction and recursion will be used several times in Chapter 4. As with transfinite induction, well-founded set-like relations also support definitions by transfinite recursion. In the next section, we formulate and discuss the Axiom of Choice.

2.3 Axiom of Choice

The original formulation of AC is as follows.

Axiom of Choice. For every collection X of nonempty sets there exists a function such that the image of every set $a \in X$, $f(a)$, is in a. Formally;

$$\forall X(\emptyset \notin X \to \exists f(f : X \to \bigcup X) \wedge \forall a \in X(f(a) \in a)).$$

Here the expression '$f : X \to \bigcup X$' is an abbreviation for a formula of ZF. The function f, which is not necessarily unique, is often called a choice function: given a collection of nonempty sets we can choose an element of each set simultaneously. In many cases we do not need AC to do this, because such a function can be found explicitly.

Example 2.16. Consider the set $X = \{\{0, 1\}, \{1, 2\}\}$. Define f by putting $f(\{0, 1\}) = 0$, $f(\{1, 2\}) = 2$. Then f is a choice function.

Example 2.17. Let X be the set consisting of all nonempty finite subsets of $\mathbb{Z}$. Since any finite subset a of $\mathbb{Z}$ has a least element with respect to the standard linear ordering on $\mathbb{Z}$, we can define $f(a) = min(a)$, which gives the minimal element in a. Clearly f is a choice function.

The power of AC consists in the fact that it asserts the existence of such a function for any collection. Note that AC is not constructive: it does not

give us a recipe how to find such a function for an arbitrary collection, it only asserts that such a function exists.
ZF together with AC (ZF+AC), denoted by ZFC, is by most mathematicians viewed as an appropriate foundation for all of mainstream mathematics. There are several theorems in mainstream mathematics which cannot be proven without AC. For instance, AC has important consequences in the fields of algebra and topology.[7] The proofs of those theorems often require statements which are logically equivalent to AC.[2] We state two well-known equivalent statements here. Proofs can be found in [6], Chapter 1. We will encounter other equivalent statements later.

Zorn's Lemma. If P is a poset with the property that every linearly ordered subset of P has an upper bound in P, then P has a maximal element.

Well-ordering Theorem. Every set can be well-ordered.

Let us look at some consequences. The well-ordering theorem implies that the set of real numbers $\mathbb{R}$ can be well-ordered. However, the 'theorem' does not tell us how to construct such a well-ordering. Another consequence, which is counter-intuitive, is the Banach-Tarski paradox: If we take a solid sphere in 3-space, we can decompose it into finitely many pieces which we can put back together to form two identical copies of the original sphere.[8] Finally, we state two definitions of finiteness which are equivalent if AC holds. The proof can be found in [6], Chapter 1. The first definition is the standard definitions of finiteness.

Definition 2.18. A set S is called *finite* if there exists a bijection $f : n \to S$ for some $n \in \mathbb{N}$. S is called *infinite* if S is not finite.

Definition 2.19. A set S is called *Dedekind-*, or *D-infinite* if there exists an injection $f : \mathbb{N} \to S$. S is called *D-finite* if there does not exist such an injection.

Note that if S is finite, then S is D-finite. But if S is D-finite and AC does not hold, then it is not always true that S is finite, as we will see in chapter 4.

[2] When we say that a statement is equivalent to AC, we always mean 'equivalent with respect to ZF'. Thus, if we say that a statement φ is equivalent to AC, it means that in ZFC we can prove φ, and in ZF+φ we can prove AC.

2.4 Model Theory

In Chapter 4 we will be considering models of ZF and ZFC. In the Introduction we made the informal statement that a model in set theory is a set satisfying a collection of axioms. In this section we will make precise what that means. We follow the presentation given in [6], chapter 2.

Definition 2.20. A *language* $\mathcal{L}$ is a triple $(con(\mathcal{L}), fun(\mathcal{L}), rel(\mathcal{L}))$ where the sets $con(\mathcal{L})$ is a set of constants, $fun(\mathcal{L})$ is a set of function symbols and $rel(\mathcal{L})$ is a set of relation symbols. Each function symbol and relation symbol has a specified *arity*, which is the number of arguments.

With a language we can inductively build terms and formulas, using auxiliary symbols such as the equality symbol, the propositional connectives, quantifiers, variables and brackets. The definition of terms and formulas of a language can be found in most logic texts, for example in Chapter 18.2 of [9].

Definition 2.21. A *structure* for the language $\mathcal{L}$, also called an $\mathcal{L}$-structure, is a pair $\mathfrak{M} = (M, (\cdot)^{\mathfrak{M}})$ where M is a nonempty set and $(\cdot)^{\mathfrak{M}}$ is a function defined on the symbols of $\mathcal{L}$ with the following properties:

1. For every constant c in $\mathcal{L}$, $(c)^{\mathfrak{M}}$ is an element of A.
2. For every n-place predicate R in $\mathcal{L}$, $(R)^{\mathfrak{M}}$ is a subset of A^n.
3. For every n-ary function symbol f in $\mathcal{L}$, $(f)^{\mathfrak{M}}$ is a function with domain A^n and range A.

Given an $\mathcal{L}$-structure $\mathfrak{M}$, consider the language $\mathcal{L}_{\mathfrak{M}}$, which is the language $\mathcal{L}$ together with, for each element $m \in \mathfrak{M}$, an extra constant m.

The structure $\mathfrak{M}$ is called the *interpretation* of the language $\mathcal{L}_{\mathfrak{M}}$. Using the way in which formulas and terms are constructed, we can now define what it means for a formula φ to be true in $\mathfrak{M}$, which we write symbolically as $\mathfrak{M} \models \varphi$. We just give an example here: for any terms t_1, t_2 we define $\mathfrak{M} \models t_1 = t_2$ iff $(t_1)^{\mathfrak{M}} = (t_2)^{\mathfrak{M}}$.
We can now say what it means when we are considering a model of a set of sentences such as ZFC. Formally, as shown in the first section, the axioms of ZFC are written in the language of first-order logic with the 2-ary relation symbol $\in$. Call this language $\mathcal{L}^{\in}$. ZFC is called an $\mathcal{L}^{\in}$-*theory*. The symbols that we use which are not officially part of our language, such as $\cup$ and $\subseteq$, may be regarded as abbreviations.

Definition 2.22. Consider an $\mathcal{L}^{\in}$-theory T. An $\mathcal{L}^{\in}$-structure $\mathfrak{M}$ is called a *model* of T if every sentence φ in T is true in $\mathfrak{M}$. In symbolic notation,

$$\mathfrak{M} \models \varphi$$

for every $\varphi \in T$.

We use the following abbreviation. When T is the theory under consideration and $\mathfrak{M}$ the corresponding model with set M, we will write $M \models T$. Thus, we write $M \models \text{ZFC}$ if all axioms of ZFC are true in M.

Definition 2.23. Let T be a theory. We say that T is *consistent* if T has a model.[3]

Although the notation is quite cumbersome, the idea of the above definitions is that we have a 'world' which makes particular sentences true. The model under consideration is usually called a 'universe' in the context of set theory. We have now defined the notion of a model specifically for set theory, but the definition can be made more general for arbitrary mathematical structures. For instance, the list of axioms of a group constitutes a theory, for which a particular group such as $(\mathbb{Z}, +, 0)$ is a model.

Definition 2.24. Let M and N be $\mathcal{L}$-structures. We say that N is a *substructure* of M if $N \subseteq M$ and the following conditions are satisfied:

1. $(c)^N = (c)^M$ for every constant c of $\mathcal{L}$.
2. f^N is the restriction of f^M to N^n for every n-ary function symbol of $\mathcal{L}$.
3. $R^N = R^M \cap N^n$ for every n-ary relation symbol R of $\mathcal{L}$.

When N and M are also models for $\mathcal{L}$, we say that N is a *submodel* of M.

We are now able to state a theorem known as the Downward Löwenheim-Skolem theorem.

Theorem 2.25. *Let V be an infinite model of a theory T with countable language $\mathcal{L}$, and let $C \subseteq V$ be a countable subset. Then there is a submodel M of V which is also countable.*

This theorem, together with the Reflection Principle which we will not

[3]Officially, this is not a definition of consistency for a theory. Consistency is defined as a provability-property of a theory: a theory is set to be consistent if it is not possible to derive a contradiction from the theory in first-order logic. If a theory T is consistent in this sense, then it follows from Gödel's Completeness Theorem that T has a model[5].

state here, imply that if we have a model of ZFC, then we can also find a countable model which satisfies any finite list of axioms of ZFC. Unfortunately, it follows from Gödel's Second Incompleteness Theorem that we cannot prove within ZFC that there exists a model satisfying all axioms of ZFC. This poses no real problem since we can always include the axioms that we need. In the rest of this thesis, when we are talking about a countable model of ZFC we actually mean a model satisfying a suitable finite number of axioms.

The countable models that we consider in Chapter 4 must satisfy an additional property: they should be transitive. Why this is the case will become clear later. Note that the Löwenheim-Skolem theorem provides us with a countable submodel V. It can be shown that this model will be isomorphic to a countable transitive model M. For the interested reader: this is done using the Mostowski Collapse, another result which we will not state here. Both the Reflection Principle and the Mostowski Collapse are discussed in [5].

The existence of countable models of ZFC might seem counterintuitive. It can be proved in ZFC that there are uncountable sets, such as the set of real numbers. If M is a countable model of ZFC, then this statement is also true in M. But M is countable, so at first sight it seems as if we have a contradiction. This is known as Skolem's Paradox. However, the paradox is resolved once we look more carefully at what happens. There is a difference between a statement being true in M (Definition 2.22) and a statement being true outside this model. From the viewpoint of M, a bijection between M and $\mathbb{N}$ does not exist. However, outside M we can find such a bijection. Hence, the notion of 'uncountable' should be used with care, since it depends on the context.

The Downwards Löwenheim-Skolem theorem provides us with a model of ZFC which is the starting point of Cohen's forcing method, which we will study in Chapter 4. Before that, we first investigate the relationship between AC and the existence of maximal ideals in commutative rings with 1.

3 Algebra and Choice

In this chapter we show that AC is equivalent to the statement that every commutative ring with 1 has a maximal ideal. The left-to right direction is well known, and follows from a straightforward application of Zorn's Lemma. The right-to left direction is far from straightforward and we will need quite some definitions and lemmas before we can prove this result, which is due to Hodges [4]. This is the content of sections 3.1, 3.3 and 3.4. Although we follow Hodges' proof closely, we have added some examples in order to illustrate his method. Moreover, we prove a few statements which Hodges left for the reader to check. In Section 3.5 we briefly mention the relation between AC and other results in algebra. In Section 3.2 we have a little detour when we take a careful look at the construction of a particular ring, set-theoretically.

3.1 Rings and Trees

The essential concept in Hodges' proof is a tree. He defines a tree as follows.

Definition 3.1. Let T be a poset. T is called a *tree* if for all $t \in T$, the set $\hat{t} = \{r \in T : r \leq t\}$ is linearly ordered. A maximal totally ordered subset of T is called a *branch*.[4]

Example 3.2. Consider the set T of finite sequences of 0's and 1's: $T = \{(a_1, ..., a_n) : n \in \mathbb{N} \text{ and } a_i \in \{0, 1\}\}$. For any two sequences $t_1, t_2 \in T$, put $t_1 \leq t_2$ if and only if t_2 extends t_1 as a sequence: for $t_1 = (a_1, ..., a_n)$, $t_2 = (b_1, ..., b_m)$, $n \leq m$ and $a_i = b_i$ for all $i \in \{1, ..., n\}$. Then $(T, \leq)$ is a tree. T has infinitely many branches: any branch contains comparable sequences of any length. For example, the set consisting of the sequences of 0's of any length is a branch.

Trees will be important in this thesis: they will be the key in proving that AC holds if and only if every commutative ring with 1 has a maximal ideal.

Lemma 3.3. *AC holds if and only if every tree has a branch.*

Proof. '⇒': Let T be tree. Let L be the set of linearly ordered subsets of T, and order L by inclusion. This gives a partial order on L. Any totally

[4]This definition of a tree is a bit uncommon. In most texts it is required that for every $t \in T$, $\hat{t} = \{r \in T : r \leq t\}$ is well-ordered, see for instance Kunen's book.[5] Although it does not make a real difference in the proof, we will use Hodges' definition to stay as close to his original proof as possible.

ordered subset S of L has an upper bound in L, namely the union of all elements in S. Hence from Zorn's lemma it follows that L has a maximal element, which is a branch of T.
'$\Leftarrow$': Assume that every tree has a branch. We show that every set can be well-ordered, which implies AC. Suppose A is any set, with T the collection of injective maps $f : \alpha \to A$ with α an ordinal. It is not obvious that T is a set since the collection of all ordinals ON is not a set (see appendix A), so we are going to prove this. We show that the collection O of all ordinals α such that there is an injective function $f : \alpha \to A$ is a set. Then it follows by Separation that T is a set, since

$$T = \{f \in \mathcal{P}(O \times A) : f \text{ is an injective function}\}.$$

Consider the set

$$W = \{(y, <) : y \subseteq A \text{ and } < \text{ gives a well-order on } y\}.$$

It follows from Separation that W is a set, since W is a subset of $\mathcal{P}(A \times A \times A)$, where '$<$ is a well-order on y' is a formula in the language of ZF. By Theorem 2.8, every y is order-isomorphic to a unique ordinal. Thus there exists a function

$$F : W \to ON.$$

Then $F(W)$ is a set by Replacement. But any $\alpha \in O$ well-orders a subset $y \subseteq A$, so

$$O \subseteq F(W).$$

It follows from Comprehension that O is a set. Now order T as follows: put $f \leq g$ if and only if g extends f as a function. That is, if and only if $dom(g) \subseteq dom(f)$ and the restriction of f to $dom(g)$ equals g. Then T is a poset. Moreover, T is also a tree. Let $f, g, h \in T$ with $g, h \leq f$. There are ordinals α_1 and α_2 with $dom(g) = \alpha_1$, $dom(h) = \alpha_2$. Since one of these ordinals is a subset of the other we see that g and h are comparable. Thus T is a tree, which has by assumption a branch B. Now take the union $\bigcup B$. This is an injective map $h : \beta \to A$ for some ordinal α. We also see that h is surjective, otherwise we can extend h within T which contradicts the maximality of B. □

Now we combine the notions tree and ring. Take an arbitrary tree T, the field $\mathbb{Q}$ and take the polynomial ring $\mathbb{Q}[T]$, with $t \in T$ as variables. Any polynomial in this ring is a finite sum of monomials multiplied by some nonzero $q \in \mathbb{Q}$. Recall that a monomial m in a polynomial ring containing variables $t \in T$ is a finite product of powers of variables, i.e. $m = t_1^{j_1} ... t_n^{j_n}$ with $j_1, .., j_n \in \mathbb{N}_{>0}$ and $t_i \in T$ for $i = 1, .., n$. If $f = q_1 m_1 + ... + q_n m_n \in \mathbb{Q}[T]$, we call the m_i a monomial of f for $i = 1, ..., n$, or an f-monomial.

In the next section we show how to construct $\mathbb{Q}[T]$ carefully from a set-theoretical point of view. As will become clear later, it is important that this can be done without using AC. The reader who is not interested in the set-theoretical construction of $\mathbb{Q}[T]$ may feel assured that this construction is possible in ZF and skip section 3.2.

3.2 Construction of $\mathbb{Q}[T]$

Usually, a ring is defined as a 5-tuple $(S, +, 0, \cdot, 1)$, where S is a set, $+, \cdot \subseteq S \times S \times S$ are maps satisfying the ring axioms with 0 and 1 the neutral elements for addition and multiplication respectively. First we define the underlying set. Any monomial $m = t_1^{j_1}...t_n^{j_n}$ can be identified with a function $m : T \to \mathbb{N}$ with finite support, i.e. $m(t_i) = j_i$ for $i = 1, .., n$ and zero elsewhere. Then put

$$M = \{m \in \mathcal{P}(T \times \mathbb{N}) : m \text{ is a function with finite support}\}.$$

Since F and f are sets, M is a set by Separation. We can now find the underlying set for $\mathbb{Q}[T]$, by noting that any polynomial corresponds to a finite sum of monomials and some $q \in \mathbb{Q}$. Thus any monomial corresponds to a function $p : M \to \mathbb{Q}$ with finite support, i.e.

$$\mathbb{Q}[T] = \{p \in \mathcal{P}(M \times \mathbb{Q}) : p \text{ is a function with finite support }\}.$$

To see that $\mathbb{Q}[T]$ 'contains' $\mathbb{Q}$, note that M contains the zero function $\mathbf{0}$, i.e. $\mathbf{0}(t) = 0$ for all $t \in T$. The constant term $q \in \mathbb{Q}$ of a polynomial corresponds to the ordered pair $(\mathbf{0}, q)$. Thus, the set $\mathbb{Q}[T]$ contains a set which whe can identify with $\mathbb{Q}$, namely $\{\mathbf{0}\} \times \mathbb{Q}$.

We still need to define addition and multiplication on the set $\mathbb{Q}[T]$. The sum of two polynomials p_1, p_2, which we denote as $p_1 + p_2$, is defined pointwise on all $m \in M$ by

$$(p_1 + p_2)(m) = p_1(m) +_{\mathbb{Q}} p_2(m).$$

Clearly, this gives a function with finite support since there are at most finitely many $t \in T$ such that $p_1(t) \neq 0$ or $p_2(t) \neq 0$. Note that addition is a map

$$+ : \mathbb{Q}[T] \times \mathbb{Q}[T] \to \mathbb{Q}[T]$$

which is surjective.
In order to define multiplication of polynomials, we first need to define how to multiply monomials. This is done as follows: the product of two monomials is another monomial denoted as $m_1 * m_2$, which satisfies

$$(m_1 * m_2)(t) = m_1(t) +_{\mathbb{Q}} m_2(t).$$

The product of two polynomials p_1, p_2 which we denote as $p_1 \times p_2$, is now defined pointwise on all $m \in M$ by

$$(p_1 \times p_2)(m) = \sum_{m_i * m_j = m} p_1(m_i) \cdot_{\mathbb{Q}} p_2(m_j),$$

where the summation of the right-hand side is done in $\mathbb{Q}$. In the remaining part of this chapter we always abbreviate $p_1 \times p_2$ with $p_1 p_2$.
Addition and multiplication of polynomials as defined in this section satisfy the ring-axioms because we defined these operations by using the operations in $\mathbb{Q}$.

3.3 Properties of $\mathbb{Q}[T]$

We now prove two lemmas for the ring $\mathbb{Q}[T]$ which will be used later. The proofs are basic.

Lemma 3.4. *The ring $\mathbb{Q}[T]$ is a unique factorization domain (UFD).*

Proof. First we verify that $\mathbb{Q}[T]$ is an integral domain. For any $f, g \in \mathbb{Q}[T]$ we can find some finite subset $F \subseteq T$ such that $f, g \in \mathbb{Q}[F]$. Since $\mathbb{Q}[F]$ is an integral domain, it follows that $\mathbb{Q}[T]$ is also an integral domain.
The unique factorization is verified similarly: take $f \in \mathbb{Q}[T]$. Then $f \in \mathbb{Q}[F]$ for some finite subset $F \subseteq T$. Suppose $g|f$. Then $g \in \mathbb{Q}[F]$, since $\mathbb{Q}$ has no zero divisors: if t is a variable appearing in g and $f = gh$ with $h \neq 0$, then $deg_t(f) \geq deg_t(g)$. Since $\mathbb{Q}[F]$ is a UFD which contains all divisors of f, we see that $\mathbb{Q}[T]$ is a UFD. □

The proof of the previous lemma shows that although T may be infinite, the ring $\mathbb{Q}[T]$ behaves as a polynomial ring in a finite number of variables. Let $G \subseteq T$. Denote by (G) the ideal in $\mathbb{Q}[T]$ finitely generated by G; any $f \in (G)$ can be written as $f_1 t_1 + ... + f_n t_n$ with $t_1, ..., t_n \in G$, $f_1, ..., f_n \in \mathbb{Q}[T]$.

Lemma 3.5. *The set $I = (G)$ is a prime ideal of $\mathbb{Q}[T]$.*

Proof. It is obvious that I is an ideal. Moreover, I is a proper ideal since it does not contain any $q \in \mathbb{Q}$. To see that I is prime, let $fg \in I$. Then $f \cdot g = g_1 t_1 + ... + g_n t_n$ with variables $t_1, ..., t_n \in G$. If $f, g \notin I$, then the product fg would contain a term without a variable in G since $\mathbb{Q}[T]$ is a domain. Hence $f \in I$ or $g \in I$ and I is a prime ideal. □

Let R be an integral domain with $S \subseteq R$ a *multiplicatively closed subset*: if $1 \in S$ and $ab \in S$ for all $a, b \in S$. Suppose also that $0 \notin S$. Consider the

equivalence relation which is used to construct the field of fractions of R, and apply this to $R \times S$: for $(r, s), (r', s') \in R \times S$, define $(r, s) \sim (r', s')$ if and only if $rs' - r's = 0$. Denote the equivalence class corresponding to an element $(r, s) \in R \times S$ by $\frac{r}{s}$. Define the *localization of R at S* as

$$S^{-1}R := \{\frac{r}{s} : r \in R, s \in S\}.$$

It is straightforward to verify that $S^{-1}R$ is a ring. As with the construction of the field of fractions, we are adding inverses to R. However, in this case we only add inverses for the elements in S.
This construction will be used in the next section to prove the main theorem of this chapter. We will be able to relate maximal ideals of the ring $S^{-1}R$, for suitable S, to branches of a tree T when $R = \mathbb{Q}[T]$.

3.4 Maximal Ideals and Choice

In this section we will show that every commutative ring with 1 has a maximal ideal if and only if AC holds. First we show the right-to left direction. The proof as presented here can be found in most undergraduate texts and syllabi on rings and fields, for instance in [10].

Theorem 3.6. *If AC holds, then every commutative ring with 1 has a maximal ideal.*

Proof. Assume that AC holds, and let R be a commutative ring with 1. We use Zorn's lemma (which is equivalent to Choice) to show that it has a maximal ideal. Consider the set J consisting of all proper ideals of R, which we partially order by inclusion. Let C be a chain in J. Take the union $U = \bigcup_{I \in C} I$. It is easy to verify that U is a proper ideal of R in J, because 1 is not in any ideal of C. Clearly U is also an upper bound of C. Hence we can apply Zorn's lemma and conclude that J has a maximal element. This is a maximal ideal of R. □

For the converse direction, it is possible to weaken our assumption. We will be able to derive AC from the assumption that every UFD has a maximal ideal. In the remaining part of this chapter we follow again Hodges' proof, see [4]. We are going to show that if every UFD has a maximal ideal, then every tree has a branch. By Lemma 3.3, this implies that every set can be well-ordered, hence AC holds.
Consider again the ring $\mathbb{Q}[T]$, with T an arbitrary non-empty tree (the empty tree just gives us the field $\mathbb{Q}$). Let L be the set of totally ordered subsets of

T, and let

$$S = \mathbb{Q}[T] - \bigcup_{G \in L} (G).$$

Then S is multiplicatively closed because S is the complement of a union of prime ideals: none of these ideals contains 1, and if $a, b \in S$ then $a, b \notin \bigcup_{G \in L}(G)$. Hence it follows from the definition of a prime ideal that ab is not in any of the prime ideals, which implies $ab \in S$. Finally, we have $0 \notin S$ since any ideal contains 0. Therefore

$$R := S^{-1}\mathbb{Q}[T] \tag{1}$$

is a ring. R is not a field since for any tree the set L is nonempty, hence there are elements $f \in \mathbb{Q}[T]$ such that $f \notin S$. In R we want to relate maximal ideals of R with branches of T. We illustrate this idea in the following example.

Example 3.7. Consider the tree $T = \{e, e_0, e_1\}$ with $e \leq e_0$, $e \leq e_1$ and e_0 and e_1 incomparable. Then $f \in S$ if f is of the form

$$f = q_0 e_0^k + q_1 e_1^l + g$$

with $k, l \geq 1$ and $q_0, q_1 \in \mathbb{Q} \setminus \{0\}$ where g is such that the first two terms do not vanish. The only other option for $f \in S$ is that f has a constant term. T has two branches, namely $\{e, e_0\}$ and $\{e, e_1\}$. We can verify that both (e, e_0) and (e, e_1) are maximal ideals in R. For take $f \notin (e, e_0)$ and consider the ideal (e, e_0, f). Then there is an f-monomial which is either constant or of the form e_1^k with $k \geq 1$. But that implies that either $f \in S$, or we can find a $g \in (e, e_0)$ such that $g + f \in S$. Hence $(e, e_0, f) = R$, so (e, e_0) is maximal. The same argument applies for (e, e_1).
We will show that we have found all maximal ideals of R, by proving that any maximal ideal is generated by a branch in T. First we show that any maximal ideal is contained in an ideal generated by a branch. Suppose that this is not the case for some maximal ideal M. Then there are $f, h \in M$ such that

1. $f \in (e, e_0)$ and $f \notin (e, e_1)$
2. $h \notin (e, e_0)$ and $h \in (e, e_1)$.

If we now take $e_1^j \in R$ with $g = f + e_1^j h$ such that no f-monomial equals any $e_1^j h$-monomial, then g is not generated by a linearly ordered set, so g is a unit in R. To see this, assume $g \in (e, e_0)$ and write $f = ek + e_0 k_0$, and $g = el + el_0$, with $l, k, l_0, k_0 \in R$. Then

$$e_1^j h = e(l - k) + e_0(l_0 - k_0)$$

which gives a contradiction with property 2. The case $g \in (e, e_1)$ leads to a similar argument, therefore $g \in (e, e_1)$ is also not possible. So g is a unit but

also an element of M, a contradiction. Thus all polynomials of a maximal ideal are generated by a particular branch of T. But then we see that e and either e_0 or e_1 (but not both) are also contained in M, since we have assumed that M is a maximal ideal.
Since any maximal ideal is generated by a branch, and every branch generates a maximal ideal, we conclude that R has precisely two maximal ideals.

We will now verify a few useful properties of the ring R as defined in (1). We have a criterion for units (invertible elements) of R, which is also a UFD.

Lemma 3.8. *An element $r = \frac{f}{s} \in R$ is invertible if and only if for all $t \in T$, $f \notin (\hat{t})$.*

Proof. Recall from Definition 3.1 that for any $t \in T$, $\hat{t}$ is the linearly ordered set $\{t_0 \in T : t_0 \leq t\}$. Suppose $r \in R$ is invertible and consider any $t \in T$. Then $f \notin (\hat{t})$, because otherwise f is generated by a linearly ordered set which implies $f \notin S$.
For the other direction, suppose that for all $t \in T$, $f \notin (\hat{t})$. We want to show that $f \in S$. Suppose that this is not the case: then there exists a finite linearly ordered $G \subseteq T$ with $f \in G$. Take $t = max(G)$. Then $f \in (\hat{g})$, a contradiction. Thus $f \in S$. □

If $r = \frac{f}{s}$ and common factors are cancelled, then f and s are unique up to units in $\mathbb{Q}$. We are able to cancel common factors, because if $f = \frac{fs}{hs}$, then $s \in S$. To see this, assume $s \notin S$. Then s is in some prime ideal (G). But then this is also the case for hs, so by definition of S we have $hs \notin S$.

Lemma 3.9. *The ring R is a UFD.*

Proof. R is an integral domain because $\mathbb{Q}[T]$ is an integral domain. Take $r = \frac{f}{s}$ such that r is not invertible, and f and s have no common factors. Suppose we have the factorizations $\frac{f}{s} = \frac{p_1}{r_1}..\frac{p_m}{r_m}$ and $\frac{f}{s} = \frac{p'_1}{k_1}..\frac{p'_n}{k_n}$. Then we have $p_1...p_m = f = p'_1...p'_n$ and $r_1...r_m = s = k_1...k_n$. Since $\mathbb{Q}[T]$ is a UFD, it follows that the factorization is unique up to units, hence R is a UFD. □

Now let M be a maximal ideal of R. We will define a subset $D \subseteq T$ such that $M = (D)$. Moreover, we will show that D is a branch of T, which means that every maximal ideal of R is generated by a branch of T. We already saw a particular case in Example 3.7. However, we will have to do some work before we can prove the general case.

Suppose $r = \frac{f}{s} \in M$ with $f \neq 0$ such that common factors are cancelled. Such an r exists because R is not a field. Write $f = q_1 m_1 + ... + q_n m_n$, with $m_1, ..., m_n$ distinct monomials over T and $q_1, ..., q_n \in \mathbb{Q}$. Since any proper ideal does not contain units, there exists by Lemma 3.8 a $t \in T$ such that $f \in (\hat{t})$. Hence each m_i has a factor in $(\hat{t})$ for $i = 1, ..., n$. Since there are finitely many f-monomials, there is some finite $A \subseteq (\hat{t})$ such that A contains precisely those factors and A is linearly ordered. A is not necessarily unique, but there are finitely many such sets since f has finitely many monomials, where each monomial has finitely many factors. Let $A_1, ..., A_k$ be all the sets with the required properties. Let $M(r)$ be the set containing the maximal element of each A_i. That is, $M(r) = \{max(A_i) : 1 \leq i \leq k\}$. We can verify the following properties, which we will use several times in this chapter:

1. If $t \in M(r)$, then $r \in (\hat{t})$.

2. If $r = \frac{f}{s} \neq 0$, and $r' = \frac{f'}{s'} \in M$ is such that every monomial of f is also a monomial of f', then for every $t' \in M(r')$ there is a $t \in M(r)$ such that $t \leq t'$.

Now we consider the following set:

$$D = \{t \in T : \forall r \in M \exists t' \in M(r) \text{ such that } (t' \leq t \text{ or } t \leq t'))\}.$$

Thus $t \in D$ if and only if every element of M has a factor of some monomial to which t is comparable. First, let us check that D is nonempty.

Lemma 3.10. *The set D is nonempty.*

Proof. Suppose $D = \emptyset$. Then for every $r_1 = \frac{f_1}{s_1} \in M$ with $t \in M(r_1)$ there exists some $r_2 = \frac{f_2}{s_2} \in M$ such that for all $t' \in M(r_2)$, t and t' are incomparable. Since M is an ideal, $f_1, f_2 \in M$ and therefore also $g = q_1 f_1 + q_2 f_2 \in M$ for any $q_1, q_2 \in \mathbb{Q}$. Note that common monomials of f_1 and f_2 are not cancelled if we choose q_1, q_2 appropriately. Now we can use property 2 to conclude that there are $t_1 \in M(r_1), t_2 \in M(r_2)$ such that $t_1, t_2 \leq t$ for some $t \in M(g)$. Hence $t_1, t_2 \in \hat{t}$ which is linearly ordered, a contradiction. □

We note that the statement that D is nonempty is trivial when T has a *root*: an element t_0 which is minimal in T, and comparable with all $t \in T$.

Lemma 3.11. *D is contained in the maximal ideal M.*

Proof. Take any $t \in D$, and suppose $t \notin M$. Then by maximality of M there are elements $r_1, r_2 \in R$, $r_0 \in M$ such that $tr_1 + r_0 r_2 = 1$. By definition

of D there is an $t' \in M(r_0)$ which is comparable with t. From property 1 it follows that $r_0 \in (\hat{t'})$. There are now two cases to consider.

1. If $t' \leq t$, then $t, t' \in (\hat{t})$, hence $1 \in (\hat{t})$.

2. If $t \leq t'$, then $t, t' \in (\hat{t'})$, hence $1 \in (\hat{t'})$.

Both cases are impossible since $(\hat{t'}), (\hat{t})$ are proper ideals in R. □

An immediate consequence of Lemma 3.11 is that $(D) \subseteq M$.

Lemma 3.12. *If $t \in D$ and $t_0 \leq t$, then $t_0 \in D$.*

Proof. Let $r \in M$ be nonzero. By definition of D there exists a $t' \in M(r)$ which is comparable with t. Again we have two cases.

1. If $t \leq t'$, then $t_0 \leq t'$.

2. If $t' \leq t$, then t' and t_0 are comparable since $(\hat{t})$ is linearly ordered.

Since r was chosen arbitrarily, we see that $t_0 \in D$.

□

Lemma 3.13. *The maximal ideal M is contained in (D).*

Proof. Let $r = \frac{f}{s} \in M \setminus (D)$. By property 1 and Lemma 3.12 it follows that if $t \in D$, then $t \notin M(r)$. Let $M(r) = \{t_1, ..., t_n\}$. Then $t_i \notin D$ for $i = 1, ..., n$. Hence by definition of D, for any t_i we can find a $r_i = \frac{f_i}{s_i} \in M$ such that for all $t' \in M(r_i)$, t_i and t' are incomparable. As in the proof of Lemma 3.10, find appropriate $q_1, ..., q_n \in \mathbb{Q}$ such that in the sum

$$g = f + q_1 f_1 + ... + q_n f_n$$

no f-monomials and any f_i-monomials for $i = 1, ..., n$ vanish. Because $f, f_1, ..., f_n \in M$, also $g \in M$. Take any $t_0 \in M(g)$. From property 2 it follows that there are $t_j \in M(f)$, $t \in M(f_j)$ such that $t_j, t \leq t_0$. But $\hat{t_0}$ is linearly ordered, hence t_j and t are comparable, a contradiction with the choice of the r_j. □

Lemma 3.11 and 3.13 together imply $(D) = M$. We now prove the main theorem of this chapter.

Theorem 3.14. *If every UFD has a maximal ideal, then AC holds.*

Proof. We will show that if every UFD has a maximal ideal, then every tree has a branch. Let T be a tree. Take the ring $R = S^{-1}\mathbb{Q}[T]$ as constructed above. Assume that R has a maximal ideal M. The argument preceding the present proof shows $(D) = M$ for some $D \subseteq T$. We claim that D is a branch in T. If not, there exists a totally ordered subset $E \subseteq T$ with $D \subseteq E$. Hence, there must exist a $t \in E$ such that $t' \leq t$ and $t' \neq t$ for all $t' \in D$. Hence $D \subset \hat{t}$. Now consider the proper ideal $(\hat{t})$. For this ideal we now have $M = (D) \subset (\hat{t})$, contradicting the maximality of M. Therefore D is a branch of T. Using Lemma 3.3 we conclude that AC holds. □

We end this section by strengthening the relationship between maximal ideals in $R = S^{-1}\mathbb{Q}[T]$ with T is a tree, and branches in T. Hodges' proof shows that every maximal ideal in R is generated by a branch in T. We now establish the converse, namely that every branch in T generates a maximal ideal in R. This result is not relevant for our discussion of AC, but the ring that Hodges used in his proof is interesting in its own right. By the following proposition and Theorem 3.14, we are able to determine for a particular ring R the exact amount of maximal ideals, if the number of branches in the corresponding tree T is known.

Proposition 3.15. *Let $R = S^{-1}\mathbb{Q}[T]$ be the ring with corresponding tree T. Suppose that $B \subseteq T$ is a branch in T. Then (B) is a maximal ideal in R.*

Proof. Take $f \notin (B)$, and consider the ideal (B, f). Without loss of generality we can assume that no f-monomial m has a factor in B, because any monomial with a factor in B is already in the ideal (B). Hence for every $b \in B$ and every t which is a factor of some f-monomial, either b and t are incomparable or $b \in \hat{t}$. There are no other cases, since $t \in \hat{b}$ implies (Lemma 3.13) that $t \in B$, which contradicts the assumption that no f-monomial is generated by B. We want to find a $b \in B$ such that b is incomparable with every factor of every f-monomial. Such a b gives us an $f + b \in (B, f)$ which is not generated by any linearly ordered set, hence $f + b \in S$ which implies $(B, f) = R$.
In order to find such a b, fix $b_1 \in B$. If b_1 is incomparable to every factor of every f-monomial, we are done. If not, then there exists a t_1 which is a factor of some f-monomial, such that $b_1 \in \hat{t_1}$. There are now two cases:

1. $b_1 = t_1$
2. $b_1 < t_1$

We see that case 1 is not possible, since by assumption no f-monomial has a factor in B. Therefore we have $b_1 < t_1$. But then there exists a $b_2 \in B$ such

that $b_1 < b_2$, with b_2 and t_1 incomparable. Because if not, $B \subset \hat{t_1}$ which contradicts the maximality of B.
If b_2 is incomparable to every factor of every f-monomial, we are done. If not, we can again find some t_2 which is a factor of some f-monomial with $b_2 \in \hat{t_2}$. Similarly to the case of b_1 and t_1 we have two cases, and we can use the same argument to conclude that there must exist a $b_3 \in B$ with $b_2 < b_3$ and with b_3 and t_2 incomparable. Note that b_3 and t_1 are also incomparable. Continuing this argument, we find every time some b_i which is incomparable to $t_1, ..., t_{i-1}$, with $b_j < b_i$ for $j = 1, ..., i-1$. At some point we run out of factors of f-monomials, of which there are only finitely many. So we will end up with some $b_n \in B$ which is incomparable to every factor of every f-monomial. This gives $f + b_n \in S$, which implies that $(B, f) = R$. Since f was chosen arbitrarily, we conclude that (B) is a maximal ideal in R. □

Example 3.16. Let T be the set of finite sequences of binary digits as in Example 3.2, and let $R = S^{-1}\mathbb{Q}[T]$. Since T has infinitely many branches we can conclude from Theorem 3.14 and Proposition 3.15 that R has infinitely many maximal ideals.

3.5 Additional results

Besides the results from the previous section, there are several theorems in the field of algebra that depend on AC, for instance in field theory and linear algebra. The standard proof of the next result uses Zorn's lemma.[10]

Theorem 3.17. *(ZFC) Every field K has a unique algebraic closure.*

Another example of the application of AC is found in linear algebra.

Theorem 3.18. *(ZFC) Given a vector space V and a linearly independent subset $L \subseteq V$, there exists a basis B for V with $L \subseteq B$.*

A proof of this theorem can be found in [10], in which again Zorn's Lemma is used. As it turns out, the reverse is also true: if every vector space has a basis, then AC is true. A proof can be found in [11].
This concludes our discussion of the relation between AC and theorems in algebra. We turn now to Cohen's method of forcing.

4 Forcing

In this chapter we will discuss Cohen's forcing method. For the original proof, see [1]. We follow the presentation of Kenneth Kunen as given in [5], Chapter 7. We will start with introducing the idea behind forcing. After that we study the general method, which we will apply to find several specific forcing extensions.

4.1 Motivation and Outline

The idea of forcing is the following: Start with a countable transitive model M of ZFC provided by the Downwards Löwenheim-Skolem theorem (Theorem 2.25). We are going to extend M to a model $M[G]$ of ZFC with $M \subset M[G]$. This can be achieved by taking a poset $P \in M$ and a subset $G \subset P$ such that $G \notin M$. The idea is somewhat similar to extensions in field theory. There one starts with a field K which is extended by adjoining one or more $a \notin K$ to K. Such an extension should be a field and thus be closed under field operations. The same holds for models of set theory: $M[G]$ should be closed under set-theoretical operations. The elements of P are called *forcing conditions*. Choosing G will force particular statements to hold in $M[G]$ and others not. The method is so powerful because the resulting extension is highly sensitive to the used poset P and the filter G, for which there are many possibilities.
Forcing as studied in Section 4.2 provides only models where at least ZFC holds, and we want to find a model where AC fails. This is done by restricting the model $M[G]$ to a model N such that $M \subset N \subset M[G]$, which is the content of Section 4.3. In Section 4.4 and 4.5 we apply the methods to obtain particular models $M[G]$ and N with $M \subset N \subset M[G]$.

4.2 Generic Extensions

As stated in the previous section, we start with a countable transitive model M of ZFC. We are now going to extend M by adjoining an element $G \notin M$ to M. The resulting model will be denoted by $M[G]$. G will be a filter with the following property.

Definition 4.1. Let M be set with a poset $P \in M$. A filter G is called *P-generic over M* if for all dense sets $D \subset P$ with $D \in M$, $G \cap D \neq \emptyset$. When the intended set M and poset P are clear from the context, we will just say that G is generic.

It is possible that $G \in M$, which would result in a trivial extension $M = M[G]$. However, most generic filters will not be in M, as shown in Lemma 4.3. In the remaining part of this chapter, we let P be a poset with a maximal element denoted by 1, G be a P-generic filter over M and M a countable transitive model of ZFC.

Definition 4.2. Let $p, q \in P$. p and q are said to be *incompatible*, notation $p \perp q$, if there does not exist an $r \in P$ with $r \leq p$ and $r \leq q$.

This definition allows us to formulate a condition on a generic filter G which prevents $G \in M$.

Lemma 4.3. *Suppose that $P \in M$ satisfies*

$$\forall p \in P \exists q, r \in P (q \leq p \wedge r \leq p \wedge q \perp r), \tag{2}$$

and G is generic, then $G \notin M$.

Proof. Suppose $G \in M$, and take the complement $D = P \setminus G$. Then $D \in M$ by Replacement. Moreover, D is dense: Take $p \in P$. If $p, q, r \in P$ are as in (1), then q and r cannot both be in G (this follows from the second property in the definition of a filter). Hence either $q \in D$ or $r \in D$. Since G is generic, $G \cap D \neq \emptyset$. This contradicts $D = P \setminus G$. □

The idea of forcing is as follows. Although $M \subset M[G]$, the construction is such that all elements of $M[G]$ have *names* in M. This means that although from the viewpoint of the universe M, a particular set S might not exist, we can still talk about a universe containing S and determine properties of S. Take for instance the generic filter G. Although in most cases $G \notin M$ by Lemma 4.3, we will still be able to determine particular properties of G from the viewpoint of M. We will illustrate this idea later with an example, when we have defined the universe $M[G]$. First, we define which sets in M will be names.

Definition 4.4. A *P-name* is a collection of ordered pairs $< \sigma, p >$ where σ is a P-name and $p \in P$. Formally, for ordinals α, β, let

1. $\{\emptyset\} = V_0^P$
2. $V_{\alpha+1}^P = \mathcal{P}(V_\alpha^P \times P)$
3. $V_\alpha^P = \bigcup_{\beta<\alpha} V_\beta^P$ when α is a limit ordinal.

Now we define the class of P-names as $V^P = \bigcup \{V_\alpha^P : \alpha \text{ is an ordinal}\}$.

Although the informal definition looks circular, the formal definition of a P-name shows that the definition is by transfinite recursion as discussed in Chapter 2.

Example 4.5. A trivial example is that $\emptyset$ is a P-name. Suppose that $p, q \in P$. Then the following sets are P-names:

1. $\{(\emptyset, p), (\emptyset, q)\}$ is a P-name because $\emptyset$ is a P-name.

2. $\{(\{(\emptyset, p), (\emptyset, q)\}, p), (\emptyset, q)\}$ is a P-name because the set from the previous example is a P-name.

The class of P-names in M is given by $M^P = V^P \cap M$. Every P-name will correspond to the following set in $M[G]$.

Definition 4.6. Given a P-name τ, define $\tau[G] = \{\sigma[G] : (\exists p \in G)(\sigma, p) \in \tau\}$.

Note that this definition is again by transfinite recursion. One important property which we want $M[G]$ to satisfy is that $M \subset M[G]$, which means that we need to find P-names for every $x \in M$. We define the *canonical* name of $x \in M$ as $\check{x} = \{(\check{y}, 1) : y \in x\}$.

Definition 4.7. Define $M[G] = \{\tau[G] : \tau \text{ is a P-name}\}$.

Lemma 4.8. *M is contained in $M[G]$, i.e. $M \subseteq M[G]$.*

Proof. The proof is by induction on the relation $\in$. First we see that $\check{\emptyset}[G] = \emptyset \in M[G]$. Next, suppose that for for all $y \in x$, $y \in M[G]$. Then using the fact that every filter contains 1 and the induction hypothesis,

$$\check{x}[G] = \{\check{y}[G] : y \in x\} = \{y : y \in x\} = x.$$

□

For the proof that $M[G]$ is a model of ZFC, we need to define the notion of forcing. First, we will give an example of a set which is not in M if $G \notin M$. This example is also intended as a motivation of the definition of forcing. This example can also be found in [5].

Example 4.9. Take the following partially ordered set: Let P be the set of all finite partial functions from $\mathbb{N}$ to $\{0, 1\}$. For any $p, q \in P$, put

$$p \leq q \Leftrightarrow q \subseteq p.$$

As in Chapter 3, p is said to *extend* q. For example, if $p = \{(0,0),(1,0),(2,0)\}$, $q = \{(0,0),(1,0)\}$, $r = \{(0,0),(1,1)\}$. Then p extends q, but p does not extend r since $p(1) \neq r(1)$.
Let G be a generic filter in P. Then

$$f_G := \bigcup G : \mathbb{N} \to \{0,1\}$$

is a function, because G does not contain incompatible elements. Now consider the P-name

$$\varphi = \{((n,\check{m}),p) : p \in P \wedge n \in dom(p) \wedge p(n) = m\}.$$

Now we can verify that φ is the name of the function f_G:

$$\begin{aligned} \varphi[G] &= \{((n,\check{m})[G],p) : p \in G \wedge n \in dom(p) \wedge p(n) = m\} && (3)\\ &= \{((n,m),p) : p \in G \wedge n \in dom(p) \wedge p(n) = m\}. && (4) \end{aligned}$$

Note that (2) follows from two applications of Definition 4.6. (3) follows from Lemma 4.8. Thus by Definition 4.7 it follows that $f_G \in M[G]$.

For the particular poset P used in the example there can be many different generic filters G. The specific properties of f_G depend on G. However, the fact that f_G is a function in $M[G]$ is true no matter what particular generic filter G is. Thus f_G is forced to be a function in $M[G]$. we will generalize the idea of the previous example in the following definition.

Definition 4.10. Let $\varphi(\tau_1,..,\tau_n)$ be a sentence, $p \in P$, $\tau_1,..,\tau_n$ P-names. We say that p forces $\varphi(\tau_1,..,\tau_n)$, which we write as $p \Vdash \varphi(\tau_1,..,\tau_n)$, if for all generic G with $p \in G$, $M[G] \models \varphi(\tau_1[G],..,\tau_n[G])$.

We give some comment on this definition of forcing. First, notice that a particular statement is forced to be true by $p \in P$ only if it does not matter which generic filter G we choose, as long as $p \in G$ holds, as illustrated in Example 4.9. Second, Kunen's definition of forcing deviates from Cohen's approach. Cohen defines the forcing relation by recursion on the complexity of formulas, without refering to a generic filter G.[1] As a consequence of Cohen's definition, it may be decided within M if a particular forcing statement holds. Kunen shows that his approach is equivalent, by defining another forcing relation $\Vdash^*$ which does not refer to objects outside M, and shows that $\Vdash$ and $\Vdash *$ are equivalent. We show the definition of $\Vdash^*$ here. The equivalence with $\Vdash$ is stated in Theorem 4.13.

Definition 4.11. Let $p \in P$. We say that a set $D \subset P$ is dense below p if for all $q \leq p$ with $q \in P$ there exists an $r \in D$ with $r \leq q$.

Definition 4.12. Let $\varphi(x_1, ..., x_n)$ be a formula with all free variables shown, $p \in P$ and $t_1, ..., t_n \in M^P$. Then we say:

1. $p \Vdash^* \tau_1 = \tau_2$ and only if the two following clauses hold:

   - for all $(\pi_1, s_1) \in \tau_1$, the set

     $$\{q \leq p : q \leq s_1 \rightarrow \exists(\pi_2, s_2) \in \tau_2(q \leq s_2 \wedge q \Vdash^* \pi_1 = \pi_2)\}$$

     is dense below p.

   - for all $(\pi_2, s_2) \in \tau_2$, the set

     $$\{q \leq p : q \leq s_2 \rightarrow \exists(\pi_1, s_1) \in \tau_1(q \leq s_1 \wedge q \Vdash^* \pi_1 = \pi_2)\}$$

     is dense below p.

2. $p \Vdash^* \tau_1 \in \tau_2$ if and only if the set

   $$\{q : \exists(\pi, s) \in \tau_2(q \leq s \wedge q \Vdash^* \pi = \tau_1)\}$$

   is dense below p.

3. $p \Vdash^* (\varphi(\tau_1, .., \tau_n) \wedge \theta(\tau_1, .., \tau_n))$ if and only if

   $$p \Vdash^* \varphi(\tau_1, .., \tau_n) \text{ and } p \Vdash^* \theta(\tau_1, .., \tau_n).$$

4. $p \Vdash^* \neg\varphi(t_1, ..., t_n)$ if and only if there is no $q \leq p$ with $q \Vdash^* \varphi(t_1, ..., t_n)$.

5. $p \Vdash^* \exists x\varphi(x, t_1, ..., t_n)$ if and only if the set

   $$\{r : \exists\sigma \in M^P(r \Vdash^* \varphi(\sigma, t_1, ..., t_n)\}$$

   is dense below p.

This definition does the required job. It means exactly the same in V as it does in M since we only refer to sets and names in M. We have not defined the forcing relation for all connectives, and we also did not mention $\forall$. This is not a problem, since we can define the other connectives in terms of the connectives for which the forcing relation is defined. Similarly, '$\forall x\varphi$' is equivalent to '$\neg\exists x\neg\varphi$'. The equivalence $\Vdash$ and $\Vdash *$ is shown in part 1 of the next theorem. In part 2 we find an important relation between $\Vdash$ and $\models$. The proof of this theorem is not very difficult, but it is quite long and technical. Hence we omit the proof. The reader can find the proof in chapter 7.3 of [5].

Theorem 4.13. *Let $\varphi(\tau_1, ..., \tau_n)$ be a sentence with P-names $\tau_1, ..., \tau_n$. Then we have the following:*

1. *For all $p \in P$,*

$$p \Vdash \varphi(\tau_1, .., \tau_n) \Leftrightarrow p \Vdash^* \varphi(\tau_1, .., \tau_n)$$

2. *For any generic filter G,*

$$M[G] \models \varphi(\tau_1[G], .., \tau_n[G]) \Leftrightarrow (\exists p \in G) p \Vdash \varphi(\tau_1, .., \tau_n)$$

To see how the definitions work, we prove a few lemmas which will be used later in this chapter.

Lemma 4.14. *Let $p \in P$, and $\varphi(\tau_1, ..., \tau_n)$ be a sentence with P-names $\tau_1, ..., \tau_n$ such that $p \Vdash \varphi(\tau_1, ..., \tau_n)$. Then for all $q \in P$ with $q \leq p$, $q \Vdash \varphi(\tau_1, ..., \tau_n)$.*

Proof. Take p, q as above. Let G be a generic filter with $q \in G$. By the definition of a filter we also have $p \in G$. Hence $M[G] \models \varphi(\tau_1[G], .., \tau_n[G])$. Therefore by definition 4.8, $p \Vdash \varphi(\tau_1, ..., \tau_n)$. □

Lemma 4.15. *With notation as before, the set $A = \{p \in P : p \Vdash \varphi(\tau_1, .., \tau_n) \vee p \Vdash \neg\varphi(\tau_1, .., \tau_n)\}$ is dense in M.*

Proof. Suppose A is not dense. For the moment, write φ for $\varphi(\tau_1, ..., \tau_n)$. Then by Definition 2.10 there exists a $p \in P$ such that for all $q \in P$ with $q \leq p$, $q \notin A$. Hence for all $q \leq p$, not $q \Vdash \neg\varphi$, which by Theorem 4.13.1 is equivalent to not $q \Vdash^* \neg\varphi$. But then it follows from Definition 4.12.3 that $p \Vdash^* \varphi$. Applying Theorem 4.13.1 again we see that $p \Vdash \varphi$. But then by the previous lemma it follows that for all $q \leq p$, $q \Vdash \varphi$, hence $q \in A$ which is a contradiction. □

Lemma 4.13 deserves some comment. Since A is dense, $G \cap A \neq \emptyset$ which means by Theorem 4.11.2 that for any sentence $\varphi(\tau_1, ..., \tau_n)$ and sets $\tau_1[G], ..., \tau_n[G]$ in $M[G]$ either $\varphi(\tau_1[G], ..., \tau_n[G])$ or its negation is true. So for any property there exists a $p \in G$ such that for any sets in $M[G]$, p forces the property or its negation to be true in $M[G]$.
We are now ready to state and prove the main theorem of this section.

Theorem 4.16. *With notation as above, $M[G]$ is transitive and countable with $G \in M[G]$, and $M[G] \models ZFC$.*

Proof. For transitivity, let $y \in x$ with $x \in M[G]$. By Definition 4.5 and 4.6 there are $p, q \in G$ and P-names $(\sigma, p), (\tau, q)$ with $(\sigma, p) \in \tau$, $\tau[G] = x$ and $\sigma[G] = y$. Thus by definition of $M[G]$ we have that $y \in M[G]$.
To see that $M[G]$ is countable, we note that there is a surjection from class of P-names M^P onto $M[G]$. But $M^P \subset M$, and M is countable. $M[G]$ is not finite, since $M \subset M[G]$. Hence $M[G]$ is countable.
By transitivity it follows that $p \in P$ implies $p \in M$, so every $p \in P$ has a canonical name $\check{p}$. Now consider the name $g = \{(\check{p}, p) : p \in P\}$. Then

$$g[G] = G,$$

hence $G \in M[G]$. Now we verify some axioms of ZFC for $M[G]$.
Extensionality follows by transitivity: assume that for all $x, y, z \in M[G]$ that $z \in x$ if and only if $z \in y$, and suppose $z \in x$. We have to show that $z \in y$. This is true because $z \in M[G]$. Similarly, when $z \in y$ we see that $z \in x$.
Pairing holds because for $x, y \in M[G]$ with names τ, σ, $\{(\tau, 1), (\sigma, 1)\}$ is a name for $\{x, y\}$.
For Power Set we need forcing. Fix $\tau[G] \in M[G]$. We need to find a name σ such that for all $\mu[G] \subset \tau[G]$, $\mu[G] \in \sigma[G]$. Then, once we know that Separation is true, it follows that $\mathcal{P}(\tau[G]) = \{x \in \sigma[G] : x \subset \tau[G]\} \in M[G]$. Take the name

$$\sigma = \{(\mu, 1) : \forall (\psi, p) \in \mu \exists q \in P((\psi, q) \in \tau)\}.$$

Now fix any name ζ such that $\zeta[G] \subset \tau[G]$. Take the name

$$\epsilon = \{(\pi, p) : \exists q \in P((\pi, q) \in \tau) \text{ and } p \Vdash \pi \in \zeta\}.$$

Then for all $(\pi, p) \in \epsilon$ there is a $q \in P$ with $(\pi, q) \in \tau$, hence $(\epsilon, 1) \in \sigma$ which implies $\epsilon[G] \in \sigma[G]$. Therefore we are done when we show that $\epsilon[G] = \zeta[G]$. Take $x \in \epsilon[G]$. Then $x = \pi[G]$ for some $(\pi, p) \in \epsilon$ with $p \in G$. Since $p \Vdash \pi \in \zeta$ it follows by Theorem 4.11.2 that $\pi[G] \in \zeta[G]$.
For the other direction, take $x = \pi[G] \in \zeta[G]$. Then by Theorem 4.11.2 there exists a $p \in G$ such that $p \Vdash \pi \in \zeta$. Since there exists a $q \in P$ with $(\pi, q) \in \tau$, by definition of ϵ we see that $(\pi, p) \in \epsilon$, hence $\pi[G] \in \epsilon[G]$.

The verification of the other axioms proceeds in a similar way: one must find a name τ such that $\tau[G]$ corresponds to the set which is needed to verify a particular axiom, using Theorem 4.11.2. For details we refer to [5], Chapter 7.4. □

4.3 Symmetric Extensions

In the previous section we obtained an extension $M \subset M[G]$, where both M and $M[G]$ are models of ZFC. The aim of this section is to obtain a model N of ZF + $\neg$AC such that $M \subset N \subset M[G]$ holds. N will be called a *symmetric* extension.
The idea of symmetric extensions originated with Fraenkel, who constructed permutation models of ZFA, which is a theory that also permits the existence of *atoms*, objects without elements that are not sets. For these atoms, Extensionality is no longer true. Cohen was able to modify the construction of symmetric extensions such that it fits into his method of forcing. In order to construct such a model, we need some definitions. We will follow [8], Chapter 5.

Definition 4.17. Let P be a poset. An *automorphism* of P, also called a P-automorphism, is a bijection $\pi : P \to P$ such that $\pi(1) = 1$, and for all $p, q \in P$,

$$p \leq q \Leftrightarrow \pi(p) \leq \pi(q)$$

Automorphisms of posets are thus structure-preserving bijections with respect to the order $\leq$. The next step is to extend automorphisms to P-names.

Definition 4.18. Let M be a model of ZFC, P be a poset, π an automorphism of P and $\tau \in M^P$. The extension of π to M^P, which we denote as π^P, is obtained by defining

- $\pi^P(\check{\emptyset}) = \check{\emptyset}$;
- $\pi^P(\tau) = \{(\pi^P(\sigma), \pi(p)) : (\sigma, p) \in \tau\}$.

We call π^P an M^P-automorphism.

The name M^P-automorphism is justified since we have by definition $(\sigma, p) \in \tau$ if and only if $(\pi^P(\sigma), \pi(p)) \in \pi^P(\tau)$. For M^P-automorphisms, we will need to prove some lemmas. But first we give an example to show how the definition works.

Example 4.19. Consider the name $\{(\check{\emptyset}, 1), (\{(\check{\emptyset}, 1)\}, 1)\}$. Then for any automorpism π,

$$\begin{aligned}
\pi^P(\{(\check{\emptyset}, 1), (\{(\check{\emptyset}, 1)\}, 1)\}) &= \{(\pi^P(\check{\emptyset}), \pi(1)), (\pi^P(\{(\check{\emptyset}, 1)\}), 1)\} \\
&= \{(\check{\emptyset}, 1), (\{(\pi^P(\check{\emptyset}), \pi(1))\}, \pi(1))\} \\
&= \{(\check{\emptyset}, 1), (\{(\check{\emptyset}, 1)\}, 1)\}
\end{aligned}$$

The following lemma is needed to show that M is contained in the model N which we are going to construct.

Lemma 4.20. *For all $x \in M$ and any P-automorphism π, $\pi^P(\check{x}) = \check{x}$.*

Proof. The proof is by induction on $\in$. For $\emptyset$ the property is true by definition. Now suppose that for all $(\check{y}, 1) \in \check{x}$, $\pi^P(\check{y}) = \check{y}$. Then from the induction hypothesis and Definition 4.17 it follows that

$$\pi^P(\check{x}) = \{(\pi^P(\check{y}), \pi(1)) : y \in x\} = \{(\check{y}, 1) : y \in x\} = \check{x}$$

Thus, by induction the result follows. □

The third statement of the following lemma will be usefull when we study a particular symmetric extension. The first and the second statement are needed to establish the third. The proofs are again basic applications of the definitions of a generic filter, an automorphism and forcing, and we invite the reader to try and find a proof for himself.

Lemma 4.21. *Suppose that $\pi : P \to P$ is an automorphism. Then the following are true:*

1. *$\pi^{-1}(G)$ is a generic filter, with $\tau[\pi^{-1}(G)] = \pi^P(\tau)[G]$ for any name τ.*
2. *$M[\pi^{-1}(G)] = M[G]$.*
3. *If for $p \in P$ we have $p \Vdash \varphi(\tau_1, .., \tau_n)$, then $\pi(p) \Vdash \varphi(\pi^P(\tau_1), .., \pi^P(\tau_n))$.*

Proof. 1. First we show that $\pi^{-1}(G)$ is a filter, which means that we need to verify the two properties in the definition of a filter. For property 1, take $x \in \pi^{-1}(G)$ and $y \in P$ such that $x \leq y$. Then $\pi(x) \leq \pi(y)$, with $\pi(x) \in G$. Since G is a filter this means $\pi(y) \in G$, hence $y \in \pi^{-1}(G)$. Property 2 is verified similarly.
Now we show that G is generic. First we show that if D is dense, then $D^{-1} = \pi^{-1}(D)$ is also dense. Take any $p \in P$, and take $q \in P$ with $\pi(p) = q$. Since D is dense we can find an $r \in D$ with $r \leq q$. That gives us

$$\pi^{-1}(r) \leq \pi^{-1}(q) = \pi^{-1}(\pi(p)) = p,$$

with $\pi^{-1}(r) \in D^{-1}$.
Now take D an arbitrary dense set. Then there exists some $z \in D^{-1} \cap G$, which gives $\pi^{-1}(z) \in D \cap \pi^{-1}(G)$.
The statement that $\tau[\pi^{-1}(G)] = \pi^P(\tau)[G]$ for any name τ is proved

by induction on $\in$. The proof is similar to the proofs by induction shown in Lemma 4.8 and Lemma 4.20.

2. This follows by the previous statement and the definition of $M[G]$.

3. Take G a generic filter with $\pi(p) \in G$, and assume that $p \Vdash \varphi(\tau_1, .., \tau_n)$. Then $p \in \pi^{-1}(G)$, and

$$M[\pi^{-1}(G)] \models \varphi(\tau_1[\pi^{-1}(G)], ..., \tau_n[\pi^{-1}(G)]$$

by the definition of forcing and the fact that $\pi^{-1}(G)$ is a generic filter. Now we can use statements 1 and 2 of this lemma to conclude that

$$M[G] \models \varphi(\pi^P(\tau_1)[G], ..., \pi^P(\tau_n)[G])$$

which gives us the forcing relation we are looking for,

$$\pi(p) \Vdash \varphi(\pi^P(\tau_1), ..., \pi^P(\tau_n)),$$

since G was any generic filter containing $\pi(p)$.

□

Lemma 4.19.3 can also be proved using the definition of $\Vdash^*$, with induction on the complexity of φ[8]. However, the given proof is quite short and shows the usefulness of Definition 4.8.
Now suppose that we have a certain collection of automorphisms of a poset P. This set admits a group-structure, using composition as group-law. This is straightforward to verify and we leave it to the reader. The following definition is completely general for groups, but will be used later with respect to groups of P-automorphisms.

Definition 4.22. Let $\mathcal{G}$ be a group. A *normal filter* on $\mathcal{G}$ is a nonempty set $\mathcal{F}$ of subgroups such that

1. if $H \in \mathcal{F}$ and $K \supseteq H$ is a subgroup of $\mathcal{G}$, then $K \in \mathcal{F}$.

2. $K \in \mathcal{F}$ and $H \in \mathcal{F}$ implies $K \cap H \in \mathcal{F}$.

3. $\pi \in \mathcal{G}$ and $H \in \mathcal{F}$ implies $\pi H \pi^{-1} \in \mathcal{F}$.

We have the following trivial example of a filter on a group $\mathcal{G}$: if e is the neutral element of $\mathcal{G}$, then every filter containing the subgroup $\{e\}$ contains all subgroups of $\mathcal{G}$.

Definition 4.23. Let τ be a P-name, $\mathcal{G}$ be a group of P-automorphisms and $\mathcal{F}$ a normal filter on $\mathcal{G}$. We define the following notions:

- $sym_{\mathcal{G}}(\tau) := \{\pi \in \mathcal{G} : \pi^P(\tau) = \tau\}$.
- τ is said to be *symmetric* if $sym_{\mathcal{G}}(\tau) \in \mathcal{F}$.
- If τ is symmetric, then τ is *hereditarily symmetric* if σ is hereditarily symmetric for all $< \sigma, p > \in \tau$.

Note that $sym_{\mathcal{G}}(\tau)$ is a subgroup of $\mathcal{G}$; this is again straightforward to verify. Thus the definition of a symmetric name makes sense. Also, not that the definition of hereditarily symmetric name is by transfinite recursion, as discussed in Section 2.2. We can now obtain a model of ZF by defining

$$N := \{\tau[G] : \tau \text{ is hereditarily symmetric}\},$$

as stated in the next theorem. Note that when we use the trivial filter, $N = M[G]$ and AC therefore also holds.

Theorem 4.24. *Let N be as defined above, namely the set of sets in $M[G]$ which have a hereditarily symmetric name. Then N is countable and transitive with $M \subseteq N \subseteq M[G]$ and $N \models ZF$.*

Proof. The relation $M \subseteq N \subseteq M[G]$ is clear from the definition of N and Lemma 4.18. Therefore we also have that N is countable, using that M and $M[G]$ are countable. It follows immediately from Definition 4.21 that N is transitive, since for any hereditarily symmetric name τ with $(\sigma, p) \in \tau$ it is necessary that σ is hereditarily symmetric.
Let $\mathcal{F}$ be the normal filter and $\mathcal{G}$ the group of automorphisms.
For Pairing, take $\tau[G], \sigma[G] \in N$. Then $sym_{\mathcal{G}}(\tau), sym_{\mathcal{G}}(\sigma) \in \mathcal{F}$. Since $\mathcal{F}$ is a normal filter we also have $sym_{\mathcal{G}}(\tau) \cap sym_{\mathcal{G}}(\sigma) \in \mathcal{F}$. Now consider $\{\tau[G], \sigma[G]\}$ which has the name $\theta = \{(\tau, 1), (\sigma, 1)\}$. Now we note that $sym_{\mathcal{G}}(\theta) \supset sym_{\mathcal{G}}(\tau) \cap sym_{\mathcal{G}}(\sigma)$, hence again by the definition of a normal filter we have that θ is symmetric. Since τ and σ are by assumption hereditarily symmetric, $\theta \in N$. □

The complete proof can be found in [8]. We note that Jech's approach differs from Kunen's: it can be shown that a transitive set is a model of ZF when it is *almost universal* and *closed under Gödel operations*. The definitions and proof can be found Chapter 3 of the same book. Jech constructs a model and shows that it satisfies the mentioned two properties.
The extension N is called a *symmetric* extension of M. In the next section we will show how to construct a particular N such that AC fails in N.

4.4 Construction of a Symmetric Model

We will now construct a model N of ZF in which AC fails. The previous sections shows that N depends on four parameters: a poset P, a generic filter G, a group $\mathcal{G}$ of P-automorphisms and a normal filter $\mathcal{F}$ on $\mathcal{G}$. Let us first fix these parameters. We start with a countable transitive model M of ZFC.

Poset. Let P be the set of partial finite functions $p : \mathbb{N} \times \mathbb{N} \to \{0, 1\}$. That is, p is a function with finite $dom(p) \subset \mathbb{N} \times \mathbb{N}$. Order this set by reverse inclusion as in Example 4.9:

$$f \leq g \Leftrightarrow g \subset f \tag{5}$$

The maximal element of P is the function with empty domain, which equals $\emptyset$.

Generic Filter. Since M is countable, we can enumerate all dense subsets of P in M as D_0, D_1, D_2,.... We can also write $P = \{p_0, p_1, p_2, ...\}$, because $P \in M$ implies that P is countable. Take $p^0 \in D_0$ and define $p^n \in P$ recursively: Let $P_n = \{p_i \in D_n : p_i \leq p^{n-1}\}$, which is nonempty since D_n is dense. Let p^n be the $p_i \in P_n$ with lowest index i. Now we can define our generic filter: let

$$G = \{p \in P : \exists p^n \leq p\}.$$

By definition, G intersects all dense subsets in P. It is straightforward to verify that G is a filter. Also, it follows from the construction of G that G is generic.

Group of P-automorphisms. Suppose π is a permutation of $\mathbb{N}$. We can extend π to an automorphism π^* of P as follows: for any $p \in P$ and $(x, y) \in dom(p)$, put

$$\pi^*(p)(\pi(x), y) = p(x, y).$$

Thus we have

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

That π^* is an automorphism of P is not difficult to check. The automomorphisms π^* can be extended to P-names, as indicated in the previous section. Hence, any permutation of $\mathbb{N}$ induces an automorphism of P. Now we let $\mathcal{G}$ be the group of automorphisms of P induced by permutations of $\mathbb{N}$.

Filter on Group. For finite $E \subset \mathbb{N}$, let

$$\mathit{fix}_{\mathcal{G}}(E) = \{\pi^* \in \mathcal{G} : (\forall e \in E)\pi(e) = e\}$$

Then $\mathit{fix}_{\mathcal{G}}(E)$ is a subgroup of $\mathcal{G}$. Now define

$$\mathcal{F} = \{H : H \text{ is a subgroup of } \mathcal{G} \text{ and } (\exists E \subset \mathbb{N})\mathit{fix}_{\mathcal{G}}(E) \subset H\}.$$

If $\mathit{fix}_{\mathcal{G}}(E) \subset \mathit{sym}_{\mathcal{G}}(\tau)$ for a name τ, then we call E the *support* of τ. In the next Lemma we show that $\mathcal{F}$ is a normal filter.

Lemma 4.25. *The set $\mathcal{F}$ is a normal filter on $\mathcal{G}$.*

Proof. First, we note that $\mathcal{F}$ is nonempty since $\mathit{fix}_{\mathcal{G}}(\emptyset) \subset \mathcal{G}$, therefore $\emptyset \in \mathcal{F}$. Next, we verify the three conditions given in the definition.

1. Let $H \in \mathcal{F}$. Then there is some finite $E \subset \mathbb{N}$ such that $\mathit{fix}_{\mathcal{G}}(E) \subset H$. If $H \subset K$, then also $K \in \mathcal{F}$ since $\mathit{fix}_{\mathcal{G}}(E) \subset H \subset K$.

2. Let $H, K \in \mathcal{F}$, with $E_H, E_K \subset \mathbb{N}$ such that $\mathit{fix}_{\mathcal{G}}(E_H) \subset H$ and $\mathit{fix}_{\mathcal{G}}(E_K) \subset K$. Then $\mathit{fix}_{\mathcal{G}}(E_H \cap E_K) \subset H \cap K$.

3. Suppose that $H \in \mathcal{F}$, with E such that $\mathit{fix}_{\mathcal{G}}(E) \subset H$. Take any $\pi^* \in \mathcal{G}$, and consider the finite set $\pi(E) = \{\pi(e) : e \in E\}$. Take $\psi \in \mathit{fix}_{\mathcal{G}}(\pi(E))$. For any $e \in E$ it is the case that $\pi^{-1}\psi\pi(e) = e$. Therefore $\pi^{-1}\psi\pi \in \mathit{fix}_{\mathcal{G}} \subset H$, or equivalently, $\psi \in \pi H \pi^{-1}$. Therefore $\pi H \pi^{-1} \in \mathcal{F}$.

□

We have now defined all the parameters which we need in order to construct a symmetric extension N of M. We can define $M[G]$, since we have a partially ordered set P with a generic filter G. We also have defined the notion of symmetry with respect to P-names by constructing a normal filter $\mathcal{F}$ for a specified group of automorphisms $\mathcal{G}$. Thus, let N be the symmetric extension obtained from the hereditarily symmetric names. In the next section we investigate the properties of N.

4.5 Properties of the Symmetric Model

In this section we will show that $N \models \neg\text{AC}$, by finding a set A which cannot be well-ordered in N. The model that we consider was constructed by Cohen[1]. We will follow the presentation given in [8]. The fact that we find a set which cannot be well-ordered has some pleasant consequences

for our purposes. If we return to Chapter 3, we may observe that Hodges' proof provides us with a recipe for finding a ring without a maximal ideal. We have to combine the tree which was used in the proof of Lemma 3.3 with the ring of Theorem 3.14. If we have a set which does not admit a well-ordering, by our discussion it follows that we also can find in N a tree without a branch, and therefore specify a commutative ring with 1 that does not have a maximal ideal. This connection has not been noticed in the literature, as far as we know.
Other models in which algebraic structures with 'strange' properties are constructed can be found in the literature. For instance, models have been constructed in which a field without algebraic closure is found or a vector space without basis. These results can be found in [8], based on [12] and [13]. However, those models are permutation models. In the Appendix we include a description of a similar model as described in this section, where we find a vector space without a basis. The argument is based on the permutation model described by [13]. We discuss this model because it is closely related to the model which we describe in this section.
First we need to find the set A. In $M[G]$ we have the following sets:

- $a_n = \{k \in \mathbb{N} : \exists p \in G(p(n,k) = 1)\}$
- $A = \{a_n : n \in \mathbb{N}\}$

These sets have names

- $\tau_n = \{(\check{k}, p) : k \in \mathbb{N} \wedge p \in P \wedge p(n,k) = 1\}$,
- $\mathcal{A} = \{(\tau_n, 1) : n \in \mathbb{N}\}$

respectively. First we need to show that these sets are in N.

Lemma 4.26. *The sets A and a_n are in N for all $n \in \mathbb{N}$.*

Proof. Take any permutation π of $\mathbb{N}$. Then $\pi(n) = m$ for some $m \in \mathbb{N}$. If we consider the induced automorphism π^P we see that

$$\begin{aligned}\pi^P(\tau_n) &= \pi^P(\{(\check{k}, p) : k \in \mathbb{N} \wedge p \in P \wedge p(n,k) = 1\}) \\ &= \{(\pi^P(\check{k}), \pi^*(p)) : k \in \mathbb{N} \wedge p \in P \wedge p(n,k) = 1\} \\ &= \{(\check{k}, \pi^*(p)) : k \in \mathbb{N} \wedge p \in P \wedge \pi^* p(\pi(n), k) = 1\} \\ &= \tau_m.\end{aligned}$$

Hence it follows from Definition 4.23 and the definition of $fix_{\mathcal{G}}(\{n\})$ in Section 4.4 that $fix_{\mathcal{G}}(\{n\}) \subset sym_{\mathcal{G}}(\tau_n)$. From this calculation it follows that for any permutation of $\mathbb{N}$, π^P permutes $\mathcal{A}$. Therefore $fix_{\mathcal{G}}(\emptyset) \subset sym_{\mathcal{G}}(\mathcal{A})$.

Now we need to show that $\mathcal{A}$ and τ_n are hereditarily symmetric. But this follows from the fact that canonical names are hereditarily symmetric, hence τ_n is hereditarily symmetric for each n. Thus it also follows that $\mathcal{A}$ is hereditarily symmetric. □

Lemma 4.27. *If $n \neq m$, $N \models a_n \neq a_m$.*

Proof. Take $n, m \in \mathbb{N}$ such that $n \neq m$ and $N \models a_n = a_m$. Then by Theorem 4.11.2 there is some $p \in G$ with $p \Vdash \tau_n = \tau_m$. Take $(n,k), (m,k) \notin dom(p)$. Define a partial function q by setting $q(x,y) = p(x,y)$ for all $(x,y) \in dom(p)$, $q(n,k) = 1$, $q(m,k) = 0$. Then $q \leq p$ which implies $q \in G$, and $q \Vdash \check{k} \in \tau_n$ since by definition of a_n, for all generic G with $q \in G$ we have $N \models k \in a_n$. But also $q \Vdash \check{k} \notin \tau_m$, since $r \leq q$ implies $r(m,k) = 0$. However, from $q \leq p$ and Lemma 4.13 it follows that $q \Vdash \tau_n = \tau_m$, a contradiction. □

Theorem 4.28. *The set A cannot be well-ordered in N.*

Proof. Suppose A can be well-ordered. Then A is $\in$-isomorphic to some ordinal by Theorem 2.8. From the previous lemma it follows that A is infinite. Since for any infinite ordinal α, $\omega \subset \alpha$, there exists an injective function $f : \omega \to A$ in N with corresponding P-name σ. Let E be a finite support of σ, and $p \in P$ such that $p \Vdash (\sigma$ is an injective function of $\mathcal{A}$ into $\check{\omega})$. Since E is finite, there exist $k \in \omega$, $q \leq p$ and $n \notin E$ such that $q \Vdash \sigma(\check{k}) = \tau_n$.
Take $m \in \mathbb{N}$ such that $m \notin E$ and $(m,i) \notin dom(p)$ for any $i \in \mathbb{N}$. Let $\pi : \mathbb{N} \to \mathbb{N}$ be the transposition which interchanges n and m. Then we have the following:

1. $\pi^*(p)$ and p are compatible;
2. $\pi^* \in fix_{\mathcal{G}}(E)$;
3. $\pi(n) \neq n$.

Now, (1) is true since it follows from the definition of π that $\pi^*(p) = p$. (2) and (3) are also true by definition. From (2) it follows that $\pi^P(\sigma) = \sigma$. Since any induced automorphism fixes canonical names, we have $\pi^P(\check{k}) = \check{k}$, hence $\pi^P(\sigma(\check{k})) = \sigma(\check{k})$. Now it follows from our considerations and Lemma 4.18 that

$$\pi(p) \Vdash \pi^P(\sigma(\check{k})) = \pi^P(\tau_n)$$

reduces to

$$p \Vdash \sigma(\check{k}) = \tau_{\pi(n)}.$$

But this is a contradiction since f is a function and by the definition of π and Lemma 4.27, in N we have $a_{\pi(n)} \neq a_n$. Hence in N there exists no injection of ω into A, hence in N we cannot well-order A. □

If we take a look back at Definition 2.17, we have the following immediate consequence from Lemma 4.27 and the proof of Theorem 4.28.

Corollary 4.28.1. *A is infinite and D-finite in N*

We are almost ready to prove the main theorem of this thesis. We use the set A to construct a tree as follows. As in Chapter 3, we consider the set T' of all injective functions from an ordinal to A. We showed that T' is a set without using AC, hence we already know that this set T' also exists in N. But we can also find such a set T in $M[G]$. Now T and T' are not the same, since in $M[G]$ the set A is countable, and as we just showed A is not countable in N. However, we can construct T' as a subset of T. It is not necessary to do so, since we already know that T' must exist in N, but it further illustrates the forcing method. The reader who does not wish to be bothered with more technical details can safely skip the material up to the next lemma.

For $f, g \in T$ put $f \leq g$ if and only if g extends f as a function. Then T is a tree with respect to $\leq$. We are going to find the name of T. T is a set of sets of ordered pairs. Suppose $x, y \in M[G]$ have names σ, τ respectively. Since $(x, y) = \{\{x\}, \{x, y\}\}$, the set

$$a := \{(\{(\sigma, 1)\}, 1), (\{(\sigma, 1), (\tau, 1)\}, 1)\}$$

is a name for (x, y). We will abbreviate a with (σ, τ) to avoid unreadable expressions. Suppose $\mathcal{O}$ is a name for the set O in $M[G]$, consisting of all ordinals α for which there is an injective function into A. Take a function f in T with $\mathrm{dom}(f) = \alpha$ and write $f = \{(\beta, a_n) : \beta \in \alpha \text{ and } a_n \in A\}$. Consider the following names:

- $\psi = \{(\check{\beta}, \tau_n) : (\beta, a_n) \in f\}$
- $\mathcal{T} = \{(\psi, 1) : f \in T\}$

Then ψ is a name for f, $\mathcal{T}$ is a name for T. Suppose m is a finite ordinal. Then for $\{1, ..., k = m - 1\}$ we have the following:

- $\psi = \{(\check{1}, \tau_{n_1}), ..., (\check{k}, \tau_{n_k})\}$
- $fix_{\mathcal{G}}(\{n_1, ..., n_k\}) \subset sym_{\mathcal{G}}(\psi)$

Hence f is in N, because we already established that canonical names and all τ_n are hereditarily symmetric. However, by Theorem 4.28 it follows that if $g : \alpha \to A$ is an injective function with $\omega \leq \alpha$, then g is not in N. Thus it follows that T is not in N. However, we have in N some set T' consisting

of all injective functions $f : m \to A$ with m a finite ordinal.
Consider the set $T^{<\omega} \subset T$, the set containing all $f : n \to A \in T$ such that n is a finite ordinal. This set has the name

$$\mathcal{T}^{<\omega} = \{(\psi, 1) : f \in T^{<\omega}\}.$$

Let π be a permutation of $\mathbb{N}$. Then $\pi^P(\psi) \in \mathcal{T}^{<\omega}$, since $\pi^P(\psi)$ corresponds to a finite injective function and for any permutation π, π^P fixes canonical names. Moreover, since π permutes $\mathbb{N}$ we can find for any ψ with $(\psi, 1) \in \mathcal{T}^{<\omega}$ a $\theta \in \mathcal{T}^{<\omega}$ such that $\pi^P(\theta) = \psi$. Hence

$$\pi^P(\mathcal{T}^{<\omega}) = \mathcal{T}^{<\omega},$$

so $fix_{\mathcal{G}}(\emptyset) \subset sym_{\mathcal{G}}(\mathcal{T}^{<\omega})$ and $\mathcal{T}^{<\omega}$ is in N. In N, $\mathcal{T}^{<\omega}$ is the set containing all injective functions $f : n \to A$ where n is a finite ordinal.

To see that the partial order is also in N, consider the set

$$\leq^{<\omega} = \{(f, g) \in \ \leq : f, g \in \mathcal{T}^{<\omega}\}$$

with name $\preceq^{<\omega} = \{(\psi_f, \psi_g) : (f, g) \in \ \leq^{<\omega}\}$. Then for any permutation π,

$$\pi^P(\preceq^{<\omega}) = \preceq^{<\omega}$$

since ψ_g extends ψ_f if and only if $\pi^P(\psi_g)$ extends $\pi^P(\psi_g)$.
From the properties of $\leq^{<\omega}$ we see that $T^{<\omega}$ is a tree in N.

Lemma 4.29. *The tree $T^{<\omega}$ has no branch in N.*

Proof. Suppose that $T^{<\omega}$ has a branch in N. Then it follows from the proof of Lemma 3.3 that we can well-order A. However, that gives a contradiction with Theorem 4.28. □

Now consider the ring $\mathbb{Q}[T^{<\omega}]$. This ring is also in N, since we can construct it explicitly using the axioms of ZF. Take

$$R = S^{-1}\mathbb{Q}[T^{<\omega}],$$

with S as defined in chapter 3. We showed that R is a UFD. We can now state and prove the main theorem of this thesis. The proof is easy, since all the work has already been done.

Theorem 4.30. *The ring R has no maximal ideal in N.*

Proof. Suppose R has a maximal ideal in N. Then it follows from the proof of Theorem 3.14 that $T^{<\omega}$ has a branch. But that is not possible, as we showed in Lemma 4.29. Therefore, R has no maximal ideal in N. □

Before we move to the conclusion, we note that it is possible to provide other proofs which show that if every commutative ring with 1 has a maximal ideal, then AC holds. For instance, Bernhard Banaschewski has given a more direct proof of this implication: from the assumption that every commutative ring with 1 has a maximal ideal, he shows for every partition of a given set there exists a choice function[14]. Cohen has constructed another symmetric model in which he find a countable set of pairs which has no choice function. An accessible discussion of this construction can be found in Chapter 5.4 of [8], where this model is called the Second Cohen model. Thus it follows from similar reasoning as in Theorem 4.30 that we can also find a commutative ring with 1 that has no maximal ideal in the Second Cohen model.

5 Discussion

In this thesis we have given a detailed description of Cohen's forcing method. We showed how we can use the forcing technique to obtain for some model M of ZFC, an extended model $M[G]$ with $G \in M[G]$ and $G \notin M$.
We also investigated the relationship between AC and several results in algebra. More specifically, we investigated Hodges' proof of the relationship between maximal ideals in commutative rings with 1 and AC: every such a ring has a maximal ideal if and only if AC holds.
Hodges' theorem implies that models of ZF+$\neg$AC should contain a ring without a maximal ideal. His proof also suggests a way how to find such a ring, given that we have a model N of ZF: we should find a set which cannot be well-ordered in N. Paul Cohen already showed how to do this, and we discussed his construction. We were able to show, using Cohen's technique of creating a symmetric extension N of M such that N is a model of ZF, that it is indeed possible to find an explicit example of such a ring in a particular symmetric extension. Additionally, we showed how to find a vector space without basis in a slightly adapted symmetric extension.
Our search for a commutative ring with 1 without maximal ideal was not methodical, in the sense that we found a commutative ring with 1 without maximal ideal by using the specific properties of Cohen's model. As such, our approach does not indicate whether it is possible to find some ring with the required properties in an arbitrary model of ZF+$\neg$AC. Maybe it is possible to develop a method such that in any given model of ZF+$\neg$AC, possibly satisfying additional conditions, some commutative ring with 1 that has no maximal ideal can be found.
Hodges' proof is interesting in its own right, since a strong relationship is established between maximal ideals of the ring R with corresponding tree T, and branches in T. Recall that in the proof that every maximal ideal of R with corresponding tree T is generated by a branch in T, essential use was made of the fact that $\mathbb{Q}$ is an infinite field. An interesting question is whether it is possible to modify the proof such that it suffices to consider some finite field instead of $\mathbb{Q}$. We note that the proof in [14], which has a lot of similarities with Hodges' proof, can be made to work with a finite field. There is however a lower bound on the size of this field.

A Vector Space without Basis

The subject of this thesis was inspired by the bachelor thesis of Frank Roumen, who described a symmetric model in which he tried to obtain a vector space without basis[15]. However, he was unable to show that there exists such a vector space in his model. Here we construct a different symmetric model, where we are able to find such a vector space. This symmetric model is related to the permutation model of Theorem 10.2 in [8]; we need only to adjust the argumentation slightly.
We consider a modified version of the Basic Cohen model: the forcing poset and the generic filter are the same. Consider in $M[G]$ again the following sets:

- $a_n = \{k \in \mathbb{N} : \exists p \in G(p(n,k) = 1)\}$
- $A = \{a_n : n \in \mathbb{N}\}$

These sets have names

- $\tau_n = \{(\check{k}, p) : k \in \mathbb{N} \wedge p \in P \wedge p(n,k) = 1\}$,
- $\mathcal{A} = \{(\tau_n, 1) : n \in \mathbb{N}\}$

Since in $M[G]$ the set A is countable, we can endow A with a vector space structure borrowed from a countable infinite-dimensional vector space such as $\mathbb{F}_2[x]$, the polynomials over $\mathbb{F}_2$ in the variable x.
Now, instead of taking as the group $\mathcal{G}$ all the automorphisms induced by permutations of $\mathbb{N}$ we only take those permutations which also induce an automorphism of the linear structure of A. The proof of Lemma 4.26 shows that any permutation of $\mathbb{N}$ induces a permutation of $\mathcal{A}$. These permutations preserve the linear structure (which is essentially only $+$ since the field is $\mathbb{F}_2$) when they preserve the structure of the name of $+$, $\check{+}$.
Take $\mathcal{G}$ is prescribed above, and take the normal filter $\mathcal{F}$ as in chapter 4. In this way we obtain a symmetric extension N, in which A is still an infinite-dimensional vector space since all automorphisms preserve the linear structure. Now consider any linearly independent subset $B \subset A$ in N with hereditarily symmetric name β. We want to show that B is finite. Suppose otherwise. Since B is in N there is some finite $E \subset \mathbb{N}$ such that $fix_{\mathcal{G}}(E) \subset sym_{\mathcal{G}}(\beta)$. Let $[E]$ be the finite-dimensional subspace of A generated by the set $x_E = \{x_n : n \in E\}$. This subspace is in N since E is a finite support for the name of x_E.

Lemma A.1. *There exists a support E' of β such that x_E is a linearly independent set.*

Proof. Suppose that $x_i \in x_E$ is linearly dependent with respect to x_E. Then

$$x_i = x_1 + ... + x_n$$

for $x_1, ..., x_n \in x_E$, all distinct from x_i. For any $\psi \in \mathit{fix}_{\mathcal{G}}(E \setminus \{x_i\})$ we also see that $\psi \in \mathit{fix}_{\mathcal{G}}(E)$ since ψ induces an automorphism of the linear structure: ψ fixes $1, .., n$ and therefore also i. Moreover, since $E \setminus \{x_i\} \subset E$ we automatically have

$$\mathit{fix}_{\mathcal{G}}(E) \subset \mathit{fix}_{\mathcal{G}}(E \setminus \{x_i\}),$$

so $\mathit{fix}_{\mathcal{G}}(E \setminus \{x_i\})$ is nonempty. Therefore $E \setminus \{x_i\}$ is also a support for β. Hence we may continue removing linearly dependent elements until we have a set E' which is a linearly independent set. E' is still a support for β. □

Since B is infinite, there exist $x_n, x_m \in B$ such that $x_n, x_m \notin [E]$. Write $x_n + x_m = x_k$, with $x_k \notin B$ since B is a linearly independent set.
Now let π be the transposition (nk) of the set $E^* = E' \cup \{n, k\}$.

Lemma A.2. *The transposition π induces an automorphism π^P of $\mathcal{A}$.*

Proof. The set E^* gives a linearly independent set x_{E^*}. According to Theorem 3.18 we can extend E^* to a basis of A in $M[G]$. Extend π to a permutation of the names of the elements in this basis as follows: if $\tau_{n_1}, \tau_{n_2}, ...$ are the names of the basis $x_{n_1}, x_{n_2}, ...$ with $n_i = k$, $n_j = n$ for some i, j, then π acts as a transposition on n, k and leaves the remaining part of the basis fixed. Now all we need to do is to define π linearly on any $\tau_n \in \mathcal{A}$. Thus if in $M[G]$

$$x_k = x_{n_1} + ... + x_{n_m},$$

then put $\pi k = j$ with j such that in $M[G]$,

$$x_j = x_{\pi n_1} + ... + x_{\pi n_m}.$$

This gives us a permutation of $\mathbb{N}$ which we denote again by π. If fully extended to P-names as usual, π induces a map π^P which is an automorphism of $\mathcal{A}$. □

Now we have a contradiction: We have $\pi^* \in \mathit{fix}_{\mathcal{G}}(E) \subset \mathit{sym}_{\mathcal{G}}(\beta)$, however we also have $\pi^P(\tau_n) = \tau_k \notin \beta$. Thus, A has no infinite linearly independent subsets in N, and therefore A has no basis in N since A has infinite dimension.
A last remark: AC is not a necessary tool for the proof of Lemma A.2, since A as a vector space is isomorphic to $\mathbb{F}_2[x]$, which is generated by the countable basis $\{1, x, x^2, ...\}$. It can be shown without using AC that a vector space with this property has a basis. See also [15], Theorem 2.4.

References

[1] P. J. Cohen. *Set Theory and the Continuum Hypothesis*. W.A. Benjamin, Inc., 1966.

[2] S. Abott. *Understanding Analysis*. Springer, 2001.

[3] K. Gödel. *The consistency of the Axiom of Choice and of the Generalized Continuum Hypothesis with the Axioms of Set Theory*. Princeton University Press, 1940.

[4] W. Hodges. Krull implies Zorn. *J. London Math. Soc.*, 19(2):285–287, 1979.

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

[6] I. Moerdijk and J. van Oosten. Sets, models and proofs. `https://www.staff.science.uu.nl/~ooste110/syllabi/setsproofs09.pdf`, 2011.

[7] H. Rubin and J. Rubin. *Equivalents of the Axiom of Choice*. North-Holland Publishing Company, 1963.

[8] T. J. Jech. *The Axiom of Choice*. Dover, 1973.

[9] J. Barwise and J. Etchemendy. *Language, Proof and Logic*. CSLI Publications, 2008.

[10] D. J. H. Garling. *A Course in Galois Theory*. Cambridge University Press, 1986.

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

[12] 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.

[13] H. Läuchli. Auswahlaxiom in der Algebra. *Commentarii Mathematici Helvetici*, 37:1–18, 1963.

[14] B. Banaschewski. A new proof that "Krull implies Zorn". *Mathematical Logic Quarterly*, 40:478–480, 1994.

[15] F. A. Roumen. Bases for vector spaces in different models of set theory. `http://scripties.fwn.eldoc.ub.rug.nl/scripties/Wiskunde/Bachelor/2010/Roumen.F.A./`, 2010.