Louisiana State University
LSU Digital Commons

LSU Doctoral Dissertations | Graduate School

2014

Constructive aspects of Kochen's theorem on p-adic closures

Evan Michael Eakins
Louisiana State University and Agricultural and Mechanical College, evan.eakins@gmail.com

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_dissertations

 Part of the Applied Mathematics Commons

Recommended Citation
Eakins, Evan Michael, "Constructive aspects of Kochen's theorem on p-adic closures" (2014). *LSU Doctoral Dissertations*. 1936.
https://digitalcommons.lsu.edu/gradschool_dissertations/1936

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Doctoral Dissertations by an authorized graduate school editor of LSU Digital Commons. For more information, please contactgradetd@lsu.edu.

CONSTRUCTIVE ASPECTS OF KOCHEN'S THEOREM ON P-ADIC CLOSURES

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Evan Eakins
B.A., Cornell College, 2007
M.S., Louisiana State University, 2013
May 2014

Acknowledgments

This dissertation would not have been possible without several contributions. It is a pleasure to thank Alexander Prestel and Philip Scowcroft for their answers to certain questions.

This work was motivated by work by Georg Kreisel in [14] brought to my attention by Prof. Delzell. It was further motivated by other work of Kreisel and others on unwinding. The specific subject is based on the work by Simon Kochen in [12].

It is a pleasure also to thank LSU for providing me with a pleasant working environment. A special thanks to Dr. Charles N. Delzell for his aid in this research.

This dissertation is dedicated to my family for their support and encouragement.

Table of Contents

Abstract

In this work we begin with a brief survey of set theory and arithmetic to provide background for a logical procedure to 'cleanse' the Axiom of Choice from a proof of a theorem of Kochen's. We accomplish this in the following chapters. We then discuss certain theorems involving definable Skolem functions. These theorems are used in Chapter 5 to give a construction of a p-adic closure of a p-valued field. Certain further considerations and open questions are addressed in the final chapter.

Chapter 1
Set Theory

This chapter begins with a concise coverage of the set theory I will utilize throughout this thesis; those who feel they have a good grasp of axiomatic set theory are encouraged to skim or skip. I largely follow Cohen [1].

Set theory was developed from ideas of Georg Cantor in the late 19th century. Largely due to paradoxes arising from Gottlob Frege's Axiom of Comprehension ($\exists y \forall x(x \in y \leftrightarrow \phi(x))$, most famously Bertrand Russell's Antinomy (use $x \notin x$ as $\phi(x)$, commonly called the barber paradox), it began to be axiomatised in the early years of the 20th century by such mathematicians as Zermelo, Fraenkel and Skolem. The most common system is attributed to Zermelo and Fraenkel and called ZF. We will use the standard set of logical symbols for "not", "or", "and", "equals", parentheses and both lower and upper case letters to represent sets:

$$\{\forall, \exists, \neg, \vee, \wedge, \rightarrow, \leftrightarrow, =, (,), x, y, z, \ldots, X, Y, Z, \ldots\}.$$

It is technically possible to decrease the number of logical connectives and quantifiers. For example, with $\neg$ and $\vee$ one can recreate all the other logical connectives (sometimes called Boolean operators) with suitable, though necessarily longer, formulas. In fact, as computer scientists well know, either one of the operators for "nor" or "nand" could be used to generate all the others if we made up symbols for them. Sparser symbol sets, of course, almost always have extensive shorthand added to them and, while I will adhere to that for the non-logical symbols, it would require excessive exposition here for tangential points. In addition to these logical symbols, the ZF system uses one non-logical symbol in what is called the *language*

of set theory, $\mathcal{L}_S = \{\in\}$. Here, $\in$ is a binary relation symbol which is understood to mean set membership. This is a very sparse language in which to represent all of mathematics; we will liberally define new symbols as shorthand. To start:

Definition 1.1. $x \subseteq y \leftrightarrow \forall z(z \in x \to z \in y)$
$x \subset y \leftrightarrow (x \subseteq y \wedge \neg(x = y))$.

The axioms of ZFC are as follows:

($S1$) Axiom of Extensionality:

$$\forall x\, \forall y(\forall z(z \in x \leftrightarrow z \in y) \to x = y).$$

($S2$) Axiom of the Null Set:

$$\exists x\, \forall y(\neg(y \in x)).$$

($S3$) Axiom of Unordered Pairs:

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

($S4$) Axiom of Union:

$$\forall x\, \exists y\, \forall z(z \in y \leftrightarrow \exists t(z \in t \wedge t \in x)).$$

($S5$) Axiom of Infinity:[1]

$$\exists x(\varnothing \in x \wedge \forall y(y \in x \to (y \cup \{y\} \in x))).$$

($S6_n$) Axiom Schema of Replacement:

$\forall t_1, \ldots, t_k(\forall x\, \exists! y(A_n(x, y; t_1, \ldots, t_k) \to \forall u\, \exists v B(u, v)))$,

where $B(u, v) \leftrightarrow \forall r(r \in v \leftrightarrow \exists s(s \in u \wedge A_n(s, r; t_1, \ldots, t_k)))$,

and $A_n(x, y; t_1, \ldots, t_k), n = 1, 2, \ldots$, is an enumeration of all the countably many formulas in our system with at least two free variables, where $k = k_n \geq 0$ depends on n.

[1] We will define the nullset symbol, $\varnothing$, in the discussion below.

($S7$) Axiom of the Power Set:

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

($S8$) Axiom of Foundation (or Regularity):

$\forall x \, \exists y (x = \varnothing \vee (y \in x \wedge \forall z (z \in x \rightarrow \neg (z \in y))))$.

($S9$) Axiom of Choice:

If a function h is defined carrying $\alpha \mapsto A_\alpha, A_\alpha \neq \varnothing$ for all $\alpha \in x$, then there exists another function f, called a choice function, such that for all $\alpha \in x, f(\alpha) \in A_\alpha$.

The purpose of Axiom S1 is to exclude atoms, or any non-sets, from the models. All sets are defined by their members and built up from the empty set. Axiom S2 asserts the existence of an empty set. In combination with Axiom S1, the set x whose existence Axiom S2 guarantees is unique and therefore can be denoted by a symbol $x := \varnothing$. Some prefer to have $\varnothing$ as a constant symbol believing systems like ours are sparse to the point of ridiculousness; while not following them I sometimes feel pangs of sympathy. For Axiom S3 we write the unordered pair $z = \{x, y\}$. We also define $\{x\} = \{x, x\}$ and $\langle x, y \rangle = \{\{x\}, \{x, y\}\}$, the latter called the ordered pair of x and y. By Axiom S1 the ordered pair of x and y is unique. From this we define functions as follows:

Definition 1.2. A *function* is a set f of ordered pairs such that $(\langle x, y \rangle \in f) \wedge (\langle x, z \rangle \in f) \rightarrow y = z$. We call the set of all x such that $\langle x, y \rangle \in f$ for some y the *domain* and the set of all y such that $\langle x, y \rangle \in f$ for some x the *range*.

It is important to note for Axiom S4 that it states that y is the union of all the members of x. We denote this with the unary operator $\bigcup x$. We can also define:

$$z = x \cup y \leftrightarrow \forall t (t \in z \leftrightarrow (t \in x \ \vee \ t \in y)).$$

This is what we more commonly think of as the union of two (or more) sets. We denote the interated binary operator by $\bigcup_{n=1}^{k} x_n$. The similarity in notation is unfortunate but generally quite clear in context. Axiom S5 guarantees the existence of an infinite set; we will show later how this can be used to define $\mathbb{N}$, the set of natural numbers.

The Axiom of Replacement, Axiom S6, is a very strong axiom that allows us to build new sets from old sets by means of formulas with two or more free variables. This axiom is presented in this way so as to (hopefully) avoid contradictions (most notably Russell's Antimony). The reason for this is that the properties A_n define functions φ so that for each u, the range of φ on u is a set v, and v cannot have cardinality greater than u. This axiom is, for practical purposes, frequently weakened to the Axiom of Separation (S6*):

$$\forall t_1, \ldots, t_k \, \forall x \, \exists y \, \forall z (z \in y \leftrightarrow z \in x \wedge A_n(z; t_1, \ldots, t_k))$$

where $A_n(z; t_1, \ldots, t_k)$ for $n = 0, 1, 2, \ldots$ ranges over formulas with at least one free variable. This is strictly weaker than Replacement and an easy consequence of it. It allows us to create new sets by separating out all elements with a 'property' A_n.

The power set of a set x is, like the empty set, unique by Axiom S1 and can be denoted by the unary operator $\mathcal{P}$. It is the set of all subsets of x and can be written $y = \mathcal{P}(x)$. This cannot be defined using Replacement, for the cardinality of y can be shown to be greater than that of x (a result of Cantor). This allows us to construct sets of cardinality greater than that of the natural numbers.

Axiom S8 guarantees what is called well-foundedness, hence the name. What it does is prevent infinite descending chains in $\in$; so for example, $x \in x$ is prohibited.

This along with Axioms S1 and S2 guarantee that all of our sets are built up from $\varnothing$.

The Axiom of Choice is abbreviated AC and is the most controversial of the ZF axioms, so much so that we tend to call the first eight ZF and the whole set of nine ZFC. One reason for this is the exceptionally non-constructive nature of the axiom and several of its consequences. As an example, ZFC proves that there exists a well-ordering of the real numbers, but it is impossible to write a formula $\phi(x, y)$ in $\mathcal{L}_S$ to define it. Other reasons include the sufficiency of ZF for many theoretical purposes and the interest in investigating certain consequences that are contradicted by AC [15].

The last important point about ZF (and ZFC) is that it is an infinite axiom system due to the Axiom Schema of Replacement. There is an alternative system called GB (Gödel-Bernays; von Neumann also worked on it) that uses only finitely many axioms, but to do so it is forced to introduce the idea of a proper class and a new set of objects in addition to sets, namely classes. Since the purpose of this exposition is not to present set theory per se we will not go deeper into it (though we will use the idea of a class to discuss the class of ordinals; in general we do not require it).

Next we need to introduce the concept of ordinals. One way to generate the ordinals is to begin with the natural numbers and generalize the concept to infinite sets. The other route to building the ordinals is to begin with well-ordered sets and either take canonical representives of equivalence classes or deal directly with the classes themselves. Since clarity and simplicity is what we are after in this case, we will build the canonical representives briefly. To begin, we need to define orders and well-orders.

Definition 1.3. A *(strict) ordering* on a set X is a set R of ordered pairs of members of X such that:

1) for all $x, y \in X$ one and only one of the following hold: $x = y$, $\langle x, y\rangle \in R$, $\langle y, x\rangle \in R$. It is customary to write $x < y$ in place of $\langle x, y\rangle \in R$; and

2) $x < y$ and $y < z$ imply $x < z$.

A *well-ordering* on X is an ordering such that if $Y \subseteq X$ and $Y \neq \varnothing$ then $\exists x(x \in Y \wedge \forall y \in Y \rightarrow \neg(y < x))$. This means that any non-empty subset Y of X has a least element.

In these cases we say that X is *ordered* (or *well-ordered*) by $<$.

To define equivalence classes on well-ordered sets we first need an order that allows us to compare them; this requires the idea of initial segments:

Definition 1.4. Let X be well-ordered by $<$. We call $Y \subseteq X$ an *initial segment* of X if $\forall x, y \in X((x \in Y \wedge y < x) \rightarrow y \in Y)$.

It can be shown that for any two well-ordered sets there must be a unique order-preserving map from one onto an initial segment of the other. Note it is quite possible for there to be such maps going both ways; if so, they are inverses of each other. We define the non-strict ordering on well-ordered sets to be $\overline{X} \leq \overline{Y}$ if there is an order-preserving map from X onto an intial segment of Y. If this map is not onto Y then $\overline{X} < \overline{Y}$; if it is onto Y then $\overline{X} = \overline{Y}$ (the bars are to distinguish between this last case and set equality). Now is where we could either define the ordinals to be the equivalence classes for this relation or build canonical representives of said equivalence classes. To build the latter we need to define transitive sets:

Definition 1.5. A set x is called *transitive* if $(y \in x \wedge z \in y) \rightarrow z \in x$.

Then we use this definition to define ordinal numbers:

Definition 1.6. An *ordinal* is a set which is well-ordered by $\in$ and is transitive. We typically denote the ordinal $\varnothing$ as 0. Lower-case Greek letters will be used to denote ordinals.

This definition then requires a theorem to show that any well-ordered set has an order-preserving map onto some ordinal α. This is not any great difficulty nor very important to our purpose. As a corollary we can show that for two ordinals α and β, if $\overline{\alpha} = \overline{\beta}$ then $\alpha = \beta$, and if $\overline{\alpha} < \overline{\beta}$ then $\alpha \in \beta$. The latter is simply the definition of the ordering we gave above; the former says that, for ordinals, isomorphism implies equality. There are two classes of ordinals: an ordinal α is called a *successor ordinal* if $\exists\beta(\alpha = \beta \cup \{\beta\})$; we usually denote $\alpha = \beta \cup \{\beta\}$ as $\alpha = \beta + 1$. If $\alpha \neq 0$ and α is not a successor ordinal, we call it a *limit ordinal*. The *natural numbers* can now be defined to be 0 and those successor ordinals α such that $\beta < \alpha \rightarrow (\beta$ is a successor or $\beta = 0)$. It is easy to see that the Axiom of Infinity could be replaced by the statement that a limit ordinal exists. We denote the least limit ordinal by ω, and it is simple to see that this is the set of all natural numbers (usually denoted by $\mathbb{N}$).[2] The proper class of all ordinals (in the GB sense) is customarily denoted by On. The ordinals will allow us to extend the usual idea of mathematical induction on the natural numbers to all ordinals. We call this transfinite induction.

Transfinite induction will begin similarly to the ordinary sort. Let $\Phi(\alpha)$ be a formula in $\mathcal{L}_S$ with a free variable α ranging over the ordinals; we begin by proving the initial condition $\Phi(0)$. Then we proceed to check that for successor ordinals $\alpha+1$, $\Phi(\alpha+1)$ holds if $\Phi(\alpha)$ holds. Thus far it is mostly identical to the usual sort of induction; the new step is to deal with limit ordinals. If α is a limit ordinal, we

[2] I.e., $\omega = \mathbb{N}$.

show that $\Phi(\alpha)$ holds if $\Phi(\beta)$ holds for all $\beta < \alpha$. At this point, as with standard induction on $\mathbb{N}$, we conclude that $\Phi(\alpha)$ is true for all ordinals α.

One of the reasons we introduced set theory and transfinite induction on the ordinals is to look at a method of Kreisel [13], using Gödel's constructible universe, for cleansing AC from proofs. We want to apply this to a result in p-adic fields, namely Kochen's analog to Hilbert's 17th problem. This method, it should be pointed out, is equally applicable to cleansing the generalized continuum hypothesis (GCH) from certain proofs; though in our case this will not be needed. The core idea has to do with Gödel's concept of the *constructible universe*, L, versus the usual *universe of sets*, V. Following Solovay's summary [20], V can be defined as all sets belonging to some level of the *cumulative hierarchy*. It is composed of the sets $R(\alpha)$ defined for all ordinals α by transfinite recursion, as follows:

1) $R(0) = \varnothing$.

2) If $\alpha = \beta + 1$, then $R(\alpha) = \mathcal{P}(R(\beta))$ where $\mathcal{P}$ is, as above, the power set operator.

3) If α is a limit ordinal, then $R(\alpha) = \bigcup_{\gamma<\alpha} R(\gamma)$.

Thus $V = \bigcup_{\alpha\in \mathrm{On}} R(\alpha)$. The statement that all sets belong to some $R(\alpha)$ is equivalent to the Axiom of Foundation.

The constructible universe is very similar. However, before proceeding, let us define the restriction of a formula A.

Definition 1.7. The *restriction* of a formula A to a set (or class) X, denoted by A_X, is the formula A where all bound variables $\forall x$ or $\exists y$ are replaced by $\forall x \in X$ or $\exists y \in X$.

L is composed of the sets $L(\alpha)$ defined for all ordinals α by transfinite recursion, as follows:

1) $L(0) = \varnothing$.

2) If $\alpha = \beta + 1$, then $L(\alpha)$ consists of the union of $L(\beta)$ and all subsets x of $L(\beta)$ that are definable in set theory when the bound variables are restricted to range over $L(\beta)$, possibly with parameters (free variables) in $L(\beta)$. This means that there is a formula $A(z, y_1, \ldots, y_n)$ of $\mathcal{L}_S$ with free variables $z, y_1, \ldots, y_n$, and there are elements $t_1, \ldots, t_n \in L(\beta)$ such that $x = \{z \in L(\beta) \mid A_{L(\beta)}(z, t_1, \ldots, t_n)\}$.

3) If α is a limit ordinal, then $L(\alpha) = \bigcup_{\gamma<\alpha} L(\gamma)$.

Thus $L = \bigcup_{\alpha \in \mathrm{On}} L(\alpha)$. A set x is called *constructible* if and only if it appears in some $L(\alpha)$ (i.e., $\exists\alpha(x \in L(\alpha))$). This hierarchy is seemingly much more limited than the cumulative hierarchy (and is considered to be so by most mathematicians). At any rate, L is certainly a subclass of V. However, utilizing the hypothesis that $V = L$, which is not seriously believed by anyone, we can sometimes deduce results that would be more difficult without it, and in certain cases the assumption can then be shown to have been unnecessary.

Before we continue we need to take a brief run through a formalization of arithmetic. First, we usually prefer to discuss arithmetic in a language other than that of set theory ($\mathcal{L}_S$). After all, we prefer to work with binary operators like $+$ and $\cdot$ and frequently with an exponential operator (binary), a successor operator (unary), or a binary relation $<$, as well. This leads to the idea of *interpretations*, which is central to the idea that all of mathematics can be expressed in set theory. In fact, that is almost exactly the idea; that we can define each of the necessary operations and relations for a particular field of mathematics by means of the language and axioms of set theory, and so analyze that field of mathematics in set thoery. In model theory this process of working with one language and axiom system and interpreting it in another is called, fittingly enough, an *interpretation*. It requires us,

firstly, to define the non-logical symbols of the first language in terms of those of the second and then, secondly, to apply this to interpreting the non-logical axioms. We will use this to interpret arithmetic in set theory.

There are many possible languages for arithmetic, but $\mathcal{L}_A = \{S, +, \cdot, 0\}$ will do for example. Here S is a unary function symbol designating the successor, $+$ and $\cdot$ are the binary addition and multiplication function symbols, and 0 is the obvious constant symbol. We want to interpret this in set theory, whose language has, please recall, one and only one binary relation symbol $\in$, though we shall, of course, utilize the shorthand we have defined previously. We interpret 0 to be $\varnothing$ and $S(0)$ to be $\varnothing \cup \{\varnothing\}$ (recall that for ordinals this was called $0+1$), which we also denote as 1. A natural number n is interpreted as the nth ordinal number x; thus a set x is the interpretation of a natural number if and only if $x \in \omega$. It remains to interpret addition and multiplication of natural numbers as suitable set-theoretic operations on members of ω.

For this we will need the notion of a cardinal number. We first define a new order relation:

Definition 1.8. If A and B are sets, then $\overline{\overline{A}} \leq \overline{\overline{B}}$ if there is an injection of A into B. $\overline{\overline{A}} = \overline{\overline{B}}$ if there is a one-to-one correspondence between A and B. $\overline{\overline{A}} < \overline{\overline{B}}$ if there is an injection of A into B but there is not an injection of B into A (the double bar is to distinguish from the order relation on ordinals).

Definition 1.9. A *cardinal* is an ordinal α such that if $\overline{\beta} < \overline{\alpha}$ then $\overline{\overline{\beta}} < \overline{\overline{\alpha}}$.

We note that every finite ordinal number is a finite cardinal number and conversely, so the finite cardinals are precisely the interpretations of the natural numbers. Now we can interpret addition on natural numbers. For (finite) cardinals α, β, and γ, let $\alpha + \beta = \gamma$ if and only if $\overline{\overline{(\alpha \times \{0\}) \cup (\beta \times \{1\})}} = \overline{\overline{\gamma}}$. The Cartesian

products are to ensure that the union is of disjoint sets, so it is 'counting' the full number of elements. Multiplication of natural numbers is interpreted by $\alpha \cdot \beta = \gamma$ if and only if $\overline{\overline{\alpha \times \beta}} = \overline{\overline{\gamma}}$ [15].

Thus we have interpreted the language of arithmetic in set theory. For the axioms of arithmetic, Peano's are standard; they can now be translated into the language of set theory by appropriate application of the interpretations we have just given. What we mean by an arithmetic formula is now defined as any formula in $\mathcal{L}_S$ that is the translation of a formula in $\mathcal{L}_A$ [6] [16].

Before continuing, we need to define a sentence in logic. A *sentence* is a formula with no free variables. This implies that it is either true or false once the formula is interpreted in a structure. This is unlike formulas with free variables, whose truth or falsehood is dependent on the values input for the free variables. As an example, think of the formula $x + 4 = 2$ in $\mathcal{L}_A$;[3] this could be true or false depending on what value one assigns to the free variable x. However, if one instead thinks of the formulas $\forall x(x + 4 = 2)$ or $\exists x(x + 4 = 2)$, both in $\mathbb{Z}$, then it is easily seen that the first is false while the second is true. It is also important to point out that sentences true in one structure need not be true in another. For example, $\exists x(x + 4 = 2)$ is not true in $\mathbb{N}$.

Returning now to our use of the constructible universe, we need to discuss the idea called *absoluteness*. Absoluteness is a logical idea that looks at sentences which are true in one model if and only if they are true in another model, usually a submodel. In our case we wish to compare V, the universe of all sets, and L, Gödel's constructible universe. In this context, a sentence will be said to be absolute if it is true in V if and only if it is true in L. Note that On is a subclass of L which is

[3] $4 = S(S(S(S(0)))),\ 2 = S(S(0))$.

a subclass of V; so all ordinals, in particular ω, are in both L and V. This tells us that every arithmetic sentence is absolute in this sense, because the interpretation of the natural numbers as ω is identical in V and L (e.g., a quantifier $\forall x \in \omega$ has the same effect as $\forall x \in L \cap \omega$, since $L \cap \omega = \omega$).

For our application we would like to introduce certain additional ideas on cardinals and the Continuum Hypothesis (CH). We write

$$\aleph_0 (= \omega) < \aleph_1 < \cdots < \aleph_\omega < \aleph_{\omega+1} < \cdots < \aleph_\alpha < \cdots$$

for the sequence of infinite (well-ordered) cardinal numbers. The Continuum Hypothesis asserts that $2^{\aleph_0} = \aleph_1$ (where $2^{\aleph_0}$ is the cardinality of $\mathcal{P}(\aleph_0)$). We write GCH for the Generalized Continuum Hypothesis, which asserts that for every ordinal α, $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

Finally, suppose ϕ is an absolute sentence in $\mathcal{L}_S$ (for example, ϕ could be any arithmetic sentence, as above).

Theorem 1.10. *Any proof of ϕ from ZF + AC + GCH can be transformed into a proof of ϕ from ZF alone.*

To see this, let $\lambda(x)$ be $\exists \alpha (x \in L(\alpha))$, a formula in $\mathcal{L}_S$ defining L; recall, for all $x \in V$, $(x \in L \leftrightarrow \lambda(x))$. Now we relativize every line of the given proof of ϕ to L; i.e., in every formula in the proof,

$$\text{we replace any universal quantifiers } \forall x \cdots \text{ with } \forall x (\lambda(x) \rightarrow \cdots),$$
$$\text{and any existential quantifiers } \exists x \cdots \text{ with } \exists x (\lambda(x) \wedge \cdots).$$

The resulting sequence of formulas is no longer quite a proof, but it can be completed to a proof by inserting small pieces of proof in appropriate places.

As an example, one commonly used rule of inference is the generalization rule, which allows us to write $\forall x \, \phi$ on line i of a proof if there exists a $j < i$ such that

ϕ is the formula on line j. This rule does not allow us to pass from ϕ_L to $(\forall x \phi)_L$, since the latter is $\forall x(\lambda(x) \rightarrow \phi_L)$, which is not of the required form (namely, $\forall x\,(\phi_L)$). However, since ϕ_L is an earlier line in the proof, we can infer $\lambda(x) \rightarrow \phi_L$ tautologically from ϕ_L. Then we may deduce the desired formula $\forall x(\lambda(x) \rightarrow \phi_L)$ by the generalization rule. All the other common rules of inference can be handled in a similar and fairly straightforward fashion.

Next, Gödel proved that the relativizations AC_L and GCH_L of AC and GCH, respectively, to L, can be proved from ZF. So in the relativized proof of ϕ, we can replace any line AC_L or GCH_L occurring there with Gödel's ZF-proofs of AC_L and GCH_L, respectively. Thus, the relativized proof of ϕ may mention AC_L or GCH_L, but it does not invoke AC or GCH as axioms. Finally, since ϕ, the end-formula of this proof, is absolute, its relativization ϕ_L is equivalent to ϕ. We thus have a proof of ϕ from ZF alone.

The idea of using Gödel's proofs of AC_L and GCH_L from ZF to "automatically" cleanse proofs of arithmetic sentences of any use of AC or GCH, is due to Kreisel [12]. Gödel's original motivation for proving AC_L and GCH_L from ZF was to show that AC and GCH are consistent with ZF [9].[4]

[4]Later, Paul Cohen showed that ¬AC and ¬GCH are also consistent with ZF [1]. Gödel's and Cohen's results, together, imply that AC and GCH can neither be proved nor disproved in ZF, partially solving the first problem in Hilbert's famous, 1900 list of 23 unsolved problems: to prove or disprove CH. (Curiously, Hilbert published an incorrect proof of CH in 1926.)

Chapter 2
Formally p-adic Fields

The first result we would like to present in this thesis is a formal 'cleansing' of the Axiom of Choice from Kochen's proof of his p-adic analog of Artin's solution to Hilbert's 17th problem (which involved real closed fields) along the lines discussed in the previous chapter. First, we give a brief overview of the 17th problem and more details on Kochen's p-adic analog thereof.

Definition 2.1. Let R be a real closed field (e.g., $\mathbb{R}$). A function $f \in R(X_1, \ldots, X_n)$ is called *positive semi-definite* if for all $\vec{x} = (x_1, \ldots, x_n) \in R^n$ either $f(\vec{x})$ is undefined or $f(\vec{x}) \geq 0$.

The 17th problem was to prove that any positive semi-definite function over a real closed field could be written as a sum of squares of rational functions in $R(X_1, \ldots, X_n)$ [2]. Kochen's analog was to look at functions which are integral definite over a p-adically closed field and show that they could be written as elements integral over a special ring that would be analogous to the sums of squares in the real case. To begin we look at valued fields:

Definition 2.2. A function v from a field K to $\Gamma \cup \{\infty\}$, where Γ is an additive, ordered, Abelian group (the *value group*), is a *valuation* if $\forall x, y \in K$:

(1) $v(x) = \infty \leftrightarrow x = 0$,

(2) $v(xy) = v(x) + v(y)$,

(3) $v(x + y) \geq \min(v(x), v(y))$.

We call a field K along with a valuation v a *valued field*. The ring formed by all elements whose value is greater than or equal to 0 is called the *valuation ring*, and is denoted by $\mathcal{O}_K$ (the K will often be suppressed where no confusion would occur). The maximal ideal of this ring, which is the ring of all elements of strictly positive value, is denoted by $\mathcal{M}_K$. The *residue class field* of (K, v) is defined to be $\mathcal{O}/\mathcal{M}$, it is often denoted by $\overline{K}$.

Definition 2.3. Let K be a valued field. Then $r(X_1, \ldots, X_n) \in K(X_1, \ldots, X_n)$ is *integral definite* in K if for every $\vec{x} = (x_1, \ldots, x_n) \in K^n$, either $r(\vec{x})$ is not defined or $r(\vec{x}) \in \mathcal{O}_K$.

For a fixed prime number p we can define a further specialization of a valuation:

Definition 2.4. A valuation, v, of a field K of characteristic 0 is a *p-valuation* if:

(1) the value group has $v(p)$ as its smallest positive element; and

(2) the residue class field $\overline{K} \cong \mathbb{Z}/p\mathbb{Z}$.

As an example consider the p-adic valuation on $\mathbb{Q}$. If you take $\frac{m}{n} \in \mathbb{Q}$, you can write it as $\frac{m}{n} = p^q \frac{a}{b}$ with a, b relatively prime and not divisible by p in a unique way. The p-adic valuation on $\mathbb{Q}$ is $v(\frac{m}{n}) = q$.

We will also require an operator that will take the place of the square operator in the 17th problem, Kochen's γ-operator:

$$\gamma(x) = \frac{x^p - x}{p((x^p - x)^2 - 1)} \qquad \left(= \frac{1}{p\big((x^p - x) - (x^p - x)^{-1}\big)} \right), \tag{2.1}$$

for $x \in K$.

We can now define the three classes of fields that are needed for Kochen's Theorem:

Definition 2.5. A field K is called *p-valued* if it is equipped with a p-valuation.

Definition 2.6. A field L is *formally p-adic over a p-valued subfield* K if $1/p \notin \mathcal{O}_K[\gamma(L)]$. K is *formally p-adic* if it is formally p-adic over $\mathbb{Q}$ equipped with the p-adic valutation.

Definition 2.7. A field is *p-adically closed* if it is formally p-adic and no proper algebraic extension is formally p-adic.

The main example of a p-adically closed field is $\mathbb{Q}_p$, the field of p-adic numbers. For an example of the development of the p-adic numbers and their arithmetic, see [11, Chapter 1].

A significant piece of what we are doing will revolve around equivalences with these ideas; for instance, a field is formally p-adic if and only if it admits a p-valuation. The following definitions are needed for a theorem on properties of p-adically closed fields:

Definition 2.8. An ordered abelian group, G, is a $\mathbb{Z}$*-group* if there is a smallest positive element in G and $|G/nG| = n$ for all positive integers n.

Definition 2.9 (Hensel's Lemma)**.** We say that a valued field K *satisfies Hensel's Lemma*, or is *Henselian*, if for each $f \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ with $v(f(a)) > 0$ and $v(f'(a)) = 0$, there exists an $\alpha \in \mathcal{O}$ with $f(\alpha) = 0$ and $v(\alpha - a) > 0$.

Theorem 2.10. *A p-valued field K is p-adically closed if and only if K is Henselian and the value group is a* $\mathbb{Z}$*-group.*

A proof of this theorem can be found in [18]. This second formulation of p-adically closed is important because our first definition was not first-order definable in the language of valued fields (either $\mathcal{L}_M$ or $\mathcal{L}_W$; see below), because it would require quantifying over all extension fields of a given field. This second definition

is first-order definable and helps explain why the axioms for p-adically closed fields are chosen as they are.

There are two standard languages and axiom systems for p-adically closed fields; Weispfenning showed in [21] that they are equivalent, so we can use either. The first is MacIntyre's language: $\mathcal{L}_M = \{+, -, \cdot, ^{-1}, 0, 1, V, P_n\}$, for $n = 2, 3, \ldots$; V and P_n are unary predicates. MacIntyre's axioms are the universal axioms for commutative rings with 1 (these may be looked up in any graduate algebra text) as well as new axioms specific to p-adically closed fields, as follows. Note that the symbols n and p are not in the formal language. We shall often write n as an abbreviation of the term $(\cdots(1+1)+\cdots+1)$ with n summands. We shall do the same for p.

$(M1)_n$ $\underbrace{1+\ldots+1}_{n \text{ times}} \neq 0$ for $n \geq 1$

$(M2)$ $0^{-1} = 0 \wedge (x \neq 0 \rightarrow xx^{-1} = 1)$

$(M3)$ $V(0) \wedge V(1) \wedge \neg V(p^{-1}) \wedge ((V(x) \wedge V(y)) \rightarrow (V(x-y) \wedge V(xy)))$

$(M4)$ $\neg V(x) \rightarrow (V(x^{-1}) \wedge V((px)^{-1}))$

$(M5)$ $V(x) \rightarrow \bigvee_{0 \leq i < p} V(p^{-1}(x-i))$

$(M6)_n$ $\exists w \left(\left(\left(\bigwedge_{i=0}^{n} V(x_i) \right) \wedge V(y) \wedge V\left(p^{-1} \sum_{i=0}^{n} x_i y^i \right) \wedge \neg V\left(p^{-1} \sum_{i=1}^{n} i x_i y^{i-1} \right) \right) \rightarrow \left(V(w) \wedge V(p^{-1}(y-w)) \wedge \sum_{i=0}^{n} x_i w^i = 0 \right) \right)$ for $n \geq 1$
(this is Hensel's lemma)

$(M7)_n$ $\exists z((y^n = x \rightarrow P_n(x)) \wedge (P_n(x) \rightarrow z^n = x))$ for $n \geq 2$

$(M8)_n$ $\bigvee_{r=0}^{n-1} \bigvee_{\substack{1 \leq a < p^{2v(n)+1} \\ p \nmid a}} P_n(x(ap^r)^{-1})$ for $n \geq 2$

Notice that for Axiom schema 8 we need to define the actual valuation function v on $\mathbb{Q}$. This is done as usual: write $n = p^i \cdot \frac{a}{b}$ for $n \in \mathbb{Q}$ and $a, b, i \in \mathbb{Z}$, with a and b (relatively prime and) not divisible by p; then let $v(n) = i$.

Weispfenning's language, $\mathcal{L}_W$, is a 2-sorted language consisting of an F-sort: $\{+, -, \cdot, 0, 1\}$; a Γ-sort: $\{<, +_\Gamma, -_\Gamma, 0_\Gamma, \infty, 1_\Gamma, \equiv_n\}$; and two functions $\pi : \Gamma \to F$, $\pi(n) = p^n$, a cross-section, and $v : F \to \Gamma$ the valuation.[1] The axioms are those for commutative rings with 1 (F-sort), those for ordered Abelian groups with 0_Γ and 1_Γ (Γ-sort), and the following ($x, y, z, \ldots$ will be used for F-variables, $\xi, \eta, \zeta, \gamma, \ldots$ will be used for Γ-variables, n and p are F-abbreviations as they were in $\mathcal{L}_M$ above):

$(W1)_n$ $\underbrace{1 + \ldots + 1}_{n \text{ times}} \neq 0 \qquad$ for $n \geq 1$

$(W2)$ $\exists y(x \neq 0 \to xy = 1)$

$(W3)$ $(v(x) = \infty \leftrightarrow x = 0) \wedge (v(xy) = v(x) +_\Gamma v(y)) \wedge$
$((v(x) \leq v(y)) \to (v(x) \leq v(x + y)))$

$(W4)$ $(\xi \neq 0 \to (\xi +_\Gamma (-_\Gamma \xi) = 0_\Gamma)) \wedge (\xi +_\Gamma \infty = \infty) \wedge (-_\Gamma \infty = \infty) \wedge (1_\Gamma \neq \infty) \wedge$
$(\xi \neq \infty \to \xi < \infty)$

$(W5)$ $(v(\pi(\xi)) = \xi) \wedge (\pi(\xi +_\Gamma \eta) = \pi(\xi)\pi(\eta)) \wedge (\pi(1_\Gamma) = p)$

$(W6)_n$ $\xi \neq 0 \to \bigvee_{0 \leq r < n} \xi \equiv_n r \qquad$ for $n \geq 2$

$(W7)_n$ $\exists \zeta((\xi \equiv_n \eta \to \underbrace{\zeta +_\Gamma \cdots +_\Gamma \zeta}_{n \text{ times}} +_\Gamma \xi = \eta) \wedge (\underbrace{\gamma +_\Gamma \cdots +_\Gamma \gamma}_{n \text{ times}} +_\Gamma \xi = \eta \to \xi \equiv_n \eta))$
for $n \geq 2$

$(W8)$ $v(x) = 0_\Gamma \to \bigvee_{0 \leq i < p} 0_\Gamma < v(x - i)$

[1] Weispfenning introduced another language without 1_Γ or $\equiv_n$. We do not use it here.

$$(W9)_n\ \exists z\left(\left(\left(\bigwedge_{i=0}^{n} 0_\Gamma \leq v(x_i)\right) \wedge (0_\Gamma \leq v(y)) \wedge \left(0_\Gamma < v\left(\sum_{i=0}^{n} x_i y^i\right)\right) \wedge \right.\right.$$
$$\left.\left.\left(0_\Gamma = v\left(\sum_{i=1}^{n} i x_i y^{i-1}\right)\right)\right) \rightarrow \left((0_\Gamma < v(z-y)) \wedge \left(\sum_{i=0}^{n} x_i z^i = 0\right)\right)\right)$$
for $n \geq 1$ (Hensel's lemma)

As noted above, Weispfenning's language and axioms are a little more complex, but their equivalence with MacIntyre's is written out in Weispfenning's paper [21].

Now let us formally state Kochen's theorem in customary terms (we shall write $\vec{X} = (X_1, \ldots, X_n)$ where the X_i's are indeterminates):

Theorem 2.11 (Kochen's Theorem)**.** *Let K be a p-adically closed field. Then $f(\vec{X}) \in K(\vec{X})$ is integral definite in K if and only if $f(\vec{X})$ is integral over the ring $\mathcal{O}_K[\gamma(K(\vec{X}))]_T$.*

Here localizing at T is understood to be localizing at all elements of the form $1 + pv$, where $v \in \mathcal{O}_K[\gamma(K(\vec{X}))]$. $f(\vec{X})$ being integral, of course, means, for some $m \in \mathbb{N}$, there exists an identity

$$f^m + \frac{w_{m-1}}{1 + pv_{m-1}} f^{m-1} + \cdots + \frac{w_0}{1 + pv_0} = 0$$

for some $w_i, v_i \in \mathcal{O}_K[\gamma(K(\vec{X}))]$.

In fact, we will instead use a strengthening of this theorem due to Roquette [18]:

Theorem 2.12. *Let K be a p-adically closed field. $f(\vec{X})$ is integral definite if and only if there exist $g, h \in \mathcal{O}_K[\gamma(K(\vec{X}))]$ such that $f = \dfrac{g}{1 + ph}$.*

We now give a brief overview of Kochen's proof (Roquette's proof uses places and algebraic geometry and so is not as applicable to our goals). Firstly, if K is p-valued, then for all $x \in K$, $\gamma(x) \in \mathcal{O}$ or $\gamma(x)$ is undefined. (This is an analog of the fact that $x^2 \geq 0$ for all x in an ordered field.) From this, the 'if' directions in 2.11 and 2.12 follow easily. It can then be shown, using Zorn's lemma (which

is equivalent to the Axiom of Choice), that, up to isomorphism, there is a unique p-adically closed extension to any p-valued field K whose value group is a $\mathbb{Z}$-group (this actually uses Zorn's lemma twice). Then using the model completeness of p-adically closed fields (like most model-theoretic results, this is not particularly constructive) and analysis of how integral definiteness interacts with the properties of p-adically closed fields, Kochen arrives at the conclusion of Theorem 2.11 [12].

Chapter 3
Cleansing the Axiom of Choice from Kochen's Proof

The goal of this chapter is to prove the following theorem:

Theorem 3.1. *The uses of Zorn's Lemma in any proof of Theorem 2.12 can be eliminated. Thus, Theorem 2.12 follows from ZF alone.*

In order to formally cleanse Kochen's proof of the Axiom of Choice it will suffice, by Theorem 1.10, to formulate Theorem 2.12 as an arithmetic sentence.

Before doing that, however, let us discuss how exactly this process will work. Gödel, as part of the work leading to his incompleteness theorems, created an arithmetization of logical syntax. This system assigned natural numbers (called *Gödel numbers*) to all of the logical and non-logical symbols in the language, which allowed the rules for well-formed formulas and proofs to be phrased in arithmetic terms as statements about natural numbers.[1] As an example of the usefulness of this idea, let us look at the first incompleteness theorem. It states that for any consistent, recursive axiom system of arithmetic, there are sentences in $\mathcal{L}_A$ that are true in $\mathbb{N}$ but cannot be proven from those axioms. In proving the first incompleteness theorem, Gödel supposed that there exists an $\mathcal{L}_A$-formula $\beta(x)$ such that $\beta(n)$ is true if and only if n is the Gödel number of a sentence true in $\mathbb{N}$. Then he let n_0 be the Gödel number of $\neg\beta$ and used it to construct a sentence in $\mathcal{L}_A$ that is either true and not in the set that $\beta(x)$ defines, or false and in that set. In either case it is clear that $\beta(x)$ cannot define the set of sentences true in $\mathbb{N}$.

[1] A development aimed specifically at number theory is in [6]. One aimed more generally at any formal system is in [10].

Our application of Gödel numbers is to form a sentence with quantifiers ranging only over the natural numbers that says 'there exists an s that is the Gödel number of a proof of Kochen's theorem'. This, since it is entirely arithmetic (we only quantify over natural numbers), can be relativised to L where we can eliminate the Axiom of Choice. This leaves us with a proof, which does not rely on AC, that Kochen's theorem can be proven in whatever system is adopted for p-adically closed fields (discussed in Chapter 2). So we need to construct an arithmetic statement that is equivalent to the informal statement that Kochen's theorem can be proven.

Before doing that, however, let us look at how to arithmetize the syntax of MacIntyre's language. First we want to break the symbols up into two classes: the logical symbols ($\forall, \exists, \neg, \vee, \wedge, \rightarrow, \leftrightarrow, =, (,)$, and the variables v_1, v_2, etc.) and the non-logical symbols ($\mathcal{L}_M$). Then we create a function h that assigns odd numbers to the logical symbols and even numbers to the non-logical symbols. So for example $h(\forall) = 1$, $h(v_1) = 21$, $h(+) = 0$, $h(0) = 8$ and $h(P_2) = 14$. For expressions in the formal language we assign the appropriate number to each symbol in order and then let the Gödel number of the expression equal the product of the primes raised to the number of the symbol plus one. So, for example, $V(0) \wedge V(1)$ is formalized as $V0 \wedge V1$ in $\mathcal{L}_M$, so the symbols' numbers would be $12, 8, 9, 12, 10$ and the Gödel number of the expression would be $2^{13} \cdot 3^9 \cdot 5^{10} \cdot 7^{13} \cdot 11^{11}$. We can then show that the basic ideas of the metamathematics (such as well-formed formulas and deductions) can be represented in arithmetic. This follows a customary and familiar process as in [6] or [10].

Now we can pursue the goal of this chapter, which is to show that the use of AC in the form of Zorn's lemma can be formally eliminated as claimed in Theorem 3.1. In the formal language (Kochen, of course, used the informal ZFC-based system of ordinary mathematics; that does not work for what we are doing here), we are

proving the conclusion of Theorem 2.12 from the axioms of p-adically closed fields, which we designate as Π_p. As stated above either one of our two axiom systems for p-adically closed fields can be used as Π_p.

So, fix n and d in $\mathbb{N}$. Let

$$\begin{aligned}
\vec{X} &= (X_1, \ldots, X_n) \qquad \text{(as before)}, \\
\vec{A} &= (A_1, \ldots, A_{\binom{n+d}{n}}), \quad \text{and} \\
\vec{B} &= (B_1, \ldots, B_{\binom{n+d}{n}})
\end{aligned}$$

be indeterminates. Let

$$\begin{aligned}
\alpha &= (\alpha_1 \ldots, \alpha_n) \in \mathbb{N}^n \text{ be a multi-index}, \\
\vec{X}^\alpha &= X_1^{\alpha_1} \cdots X_n^{\alpha_n}, \text{ and} \\
|\alpha| &= \alpha_1 + \cdots + \alpha_n.
\end{aligned}$$

(Note that the number of $\alpha \in \mathbb{N}^n$ with $|\alpha| \leq d$ is $\binom{n+d}{n}$.) Finally, let $f_{n,d} \in \mathbb{Q}(\vec{A}, \vec{B}; \vec{X})$ be the general rational function of degree d in $\vec{X}$:

$$f_{n,d}(\vec{A}, \vec{B}; \vec{X}) = \frac{\sum_{|\alpha| \leq d} A_{\sigma(\alpha)} \vec{X}^\alpha}{\sum_{|\alpha| \leq d} B_{\sigma(\alpha)} \vec{X}^\alpha},$$

where

$$\sigma : \{\, \alpha \in \mathbb{N}^n \mid |\alpha| \leq d \,\} \to \left\{ 1, 2, \ldots, \binom{n+d}{n} \right\}$$

is some bijection. (As usual, we define the degree of a rational function to be the maximum of the degrees of its numerator and denominator.)

Kochen's Theorem says that if p is prime, K is p-adically closed, $\vec{a}, \vec{b} \in K^{\binom{n+d}{n}}$, and $f_{n,d}(\vec{a}, \vec{b}; \vec{X})$ is integral definite in $\vec{X}$ over K, then there exist g, h such that

$f = \dfrac{g}{1+ph}$, where

$$g = \sum_{i=1}^{m} k_i \prod_{j=1}^{o} \gamma(l_{ij}), \text{ for some } k_i \in \mathcal{O} \text{ and } l_{ij} \in K(\vec{X}), \text{ and}$$
$$h = \sum_{i=1}^{m} k'_i \prod_{j=1}^{o} \gamma(l'_{ij}), \text{ for some } k'_i \in \mathcal{O} \text{ and } l'_{ij} \in K(\vec{X}).$$

Note that we can use the same m for both g and h, for if g, say, has more summands than h, we may add some extra summands to h with the corresponding extra coefficients $k'_i = 0$. Similarly, we can use the same o for each summand in g and in h, because we can choose some extra l_{ij} or l'_{ij} such that $\gamma(l_{ij}) = 1$ or $\gamma(l'_{ij}) = 1$, by a simple application of Hensel's Lemma. In fact, we can even arrange for $m = o$, by replacing the smaller of m and o with the larger of the two numbers. So we shall drop the letter o, and replace it with m from now on. Furthermore, we may increase this new m so as to ensure that for all i, j, $\deg l_{ij} \leq m$ and $\deg l'_{ij} \leq m$. Thus, we now have

$$\begin{aligned} g &= \sum_{i=1}^{m} k_i \prod_{j=1}^{m} \gamma(l_{ij}), \text{ for some } k_i \in \mathcal{O} \text{ and } l_{ij} \in K(\vec{X}) \text{ with } \deg l_{ij} \leq m, \text{ and} \\ h &= \sum_{i=1}^{m} k'_i \prod_{j=1}^{m} \gamma(l'_{ij}), \text{ for some } k'_i \in \mathcal{O} \text{ and } l'_{ij} \in K(\vec{X}) \text{ with } \deg l'_{ij} \leq m. \end{aligned} \tag{3.1}$$

Lemma 3.2. *The upper bound m in* (3.1) *can be chosen independently of $\vec{a}$ and $\vec{b}$; i.e., m need depend only on n, d, and p.*

Proof. This is a consequence of a "compactness" argument, as follows.

Let $\vec{y} := (y_1, \ldots, y_{\binom{n+d}{n}})$ and $\vec{z} := (z_1, \ldots, z_{\binom{n+d}{n}})$ be variables, and let $\phi_{n,d,p}(\vec{y}, \vec{z})$ be an $\mathcal{L}_M$-formula expressing the condition that $f_{n,d}(\vec{y}, \vec{z}; \vec{X})$ is integral definite in

$\vec{X}$. Let $\psi_{n,d,p,m}(\vec{y},\vec{z})$ be an $\mathcal{L}_M$-formula expressing the condition that there exist

$$\vec{s}_{ij} = (s_{i,j,1},\ldots,s_{i,j,\binom{n+m}{n}}),$$

$$\vec{t}_{ij} = (t_{i,j,1},\ldots,t_{i,j,\binom{n+m}{n}}),$$

$$\vec{s}'_{ij} = (s'_{i,j,1},\ldots,s'_{i,j,\binom{n+m}{n}}),$$

$$\vec{t}'_{ij} = (t'_{i,j,1},\ldots,t'_{i,j,\binom{n+m}{n}}),$$

$$k_1,\ldots,k_m, \text{ and}$$

$$k'_1,\ldots,k'_m$$

such that $V(k_i)$, $V(k'_i)$, and $f = \dfrac{g}{1+ph}$, where g,h are as in (3.1), and the $\vec{s}_{ij},\vec{t}_{ij}$ are the $\vec{X}$-coefficients of the numerator and denominator of l_{ij} in (3.1), respectively, and the $\vec{s}'_{ij},\vec{t}'_{ij}$ are the $\vec{X}$-coefficients of the numerator and denominator of l'_{ij}. As before, write Π_p for Macintyre's axioms. The contrapositive of Theorem 2.12 can now be expressed as: For every model K of Π_p and every $\vec{a},\vec{b} \in K^{\binom{n+d}{n}}$, if

$$\neg\psi_{n,d,p,1}(\vec{a},\vec{b}), \neg\psi_{n,d,p,2}(\vec{a},\vec{b}),\ldots$$

all hold in K, then $\neg\phi_{n,d,p}(\vec{a},\vec{b})$ holds in K. By Gödel's completeness theorem, there is a proof in $\mathcal{L}_M$ from the axiom system

$$\Pi_p \cup \{\neg\psi_{n,d,p,1}(\vec{y},\vec{z}), \neg\psi_{n,d,p,2}(\vec{y},\vec{z}),\ldots\} \tag{3.2}$$

of the formula $\neg\phi_{n,d,p}(\vec{y},\vec{z})$. Since any proof has finite length, only finitely many of the axioms in (3.2) are actually used. Thus, there is some $m \in \mathbb{N}$ such that from

$$\Pi_p \cup \{\neg\psi_{n,d,p,1}(\vec{y},\vec{z}),\ldots,\neg\psi_{n,d,p,m}(\vec{y},\vec{z})\}$$

we can prove $\neg\phi_{n,d,p}(\vec{y},\vec{z})$. So from $\Pi_p \cup \{\phi_{n,d,p}(\vec{y},\vec{z})\}$ we can prove

$$\psi_{n,d,p,1}(\vec{y},\vec{z}) \vee \cdots \vee \psi_{n,d,p,m}(\vec{y},\vec{z}),$$

which, in turn, implies, more simply, $\psi_{n,d,p,m}(\vec{y},\vec{z})$. Thus by the Deduction Theorem [6, pp. 118], for this m we have a proof from Π_p alone of

$$\phi_{n,d,p}(\vec{y},\vec{z}) \to \psi_{n,d,p,m}(\vec{y},\vec{z});$$

and by the generalization rule,

$$\forall \vec{y},\vec{z}(\phi_{n,d,p}(\vec{y},\vec{z}) \to \psi_{n,d,p,m}(\vec{y},\vec{z})), \tag{3.3}$$

proving the lemma. □

The above proof of (3.3) from Π_p takes place in $\mathcal{L}_M$; it depends on n, d, p, and m (where m is sufficiently large, depending on n, d, and p). Let $s_{n,d,p,m}$ be the Gödel code of this proof. Let η be the $\mathcal{L}_A$-formula

$$\forall n,d,p\ \exists m,s\ (s = \text{the Gödel code of a proof in } \mathcal{L}_M \text{ of (3.3) from } \Pi_p).$$

We have thus proved η, using Theorem 2.12 (which was proved in ZFC). If we interpret η in $\mathcal{L}_S$ (as in Chapter 1), we see that η is an arithmetic sentence that has been proved from ZFC. By Theorem 1.10, this proof can be transformed into a proof of η from ZF alone, as claimed in Theorem 3.1.

A consequence of this 'cleansing' is that something akin to Kreisel's 'unwinding' of Artin's Theorem for real closed fields (Hilbert's 17th problem) may be possible with its p-adic analog, Kochen's Theorem. This 'unwinding' is what Kreisel called the process of extracting constructive content from seemingly non-constructive proofs; a thorough overview is in [2] and [8]. Some ideas on how it may be accomplished in this case appear in Chapter 6.

Chapter 4
Definable Skolem Functions for $\mathbb{Q}_p$

Our task now is to illuminate certain ideas that will be needed for our construction of a p-adic closure of a p-valued field. Fundamentally this will revolve around two processes to deal with *Skolem functions*. Introducing Skolem functions is a method in logic to eliminate the use of existential quantifiers, which are the primary way that non-constructive content is introduced. In order to use them in a way that does not itself introduce constructively questionable content, we will have to show that certain conditions hold and that the Skolem functions we are introducing are definable in the original language. What follows is mainly a summary of Philip Scowcroft's work on this subject [19].

Definition 4.1. A theory $\mathcal{T}$ *admits definable Skolem functions* if for every formula $\phi(\vec{x}, y)$ such that $\mathcal{T}$ proves $\exists y\, \phi(\vec{x}, y)$, there is a definable function f such that $\mathcal{T}$ proves $\phi(\vec{x}, f(\vec{x}))$.

The fact that the theory of p-adically closed fields admits definable Skolem functions was originally due to van den Dries [5]. He used criteria from model theory that did not provide a direct, constructive proof; this was provided by Scowcroft [19]. A key element is:

Theorem 4.2. *Let $\mathcal{T}$ be a model-complete $\mathcal{L}$-theory and A a set of prenex Π_2 sentences (i.e., sentences of the form $\forall \vec{x}\, \exists \vec{y}\, \phi(\vec{x}, \vec{y})$ where ϕ is quantifier-free) which axiomatizes $\mathcal{T}$. Assume that $\mathcal{T}$ Skolemizes A: that is, for every $\forall \vec{x}\, \exists \vec{y}\, \phi(\vec{x}, \vec{y})$ in A there is a definable function f for which*

$$\mathcal{T} \vdash \forall \vec{x}\, \phi(\vec{x}, f(\vec{x})).$$

Then $\mathcal{T}$ admits definable Skolem functions.

This theorem shows how to obtain definable Skolem functions in a primitive recursive manner dependent on Weispfenning's quantifier elimination (in [21]; see Theorem 5.2 below for its statement). Specifically this depends on the fact that Weispfenning's quantifier elimination procedure is primitive recursive; Weispfenning performed this in both his language $\mathcal{L}_W$ and MacIntyre's, $\mathcal{L}_M$. The idea is that instead of using existential quantifiers, we extend the language to introduce new functions that will replace the need for them. As an example, look at the axiom schema $(M7)_n$ for $\mathcal{L}_M$:

$$\exists z\,((y^n = x \to P_n(x)) \wedge (P_n(x) \to z^n = x)).$$

The pertinent part can be written $\exists z\,(P_n(x) \to z^n = x)$. What we do is replace the quantifier by a function $f_n(x)$ so that the axiom becomes $P_n(x) \to f_n(x)^n = x$. Provided that we can define the function f_n in the original language, this will allow us to replace all the existential quantifiers that the use of this axiom schema introduces into our proof of Kochen's Theorem. To demonstrate this we first need a lemma of Denef's [4, Lemma 7.1].

Lemma 4.3. *Let S be a definable subset of $\mathbb{Q}_p^{m+q}$. For $\vec{x} \in \mathbb{Q}_p^m$, let*

$$S_x = \{\vec{y} \in \mathbb{Q}_p^q \mid (\vec{x}, \vec{y}) \in S\}.$$

Let $\alpha \in \mathbb{N}, \alpha \geq 1$. Suppose, for all $\vec{x} \in \mathbb{Q}_p^m$, that S_x is nonempty and that Card $S_x \leq \alpha$, *where* Card *denotes the cardinality. Then there exist definable functions $f_1(\vec{x}), \ldots, f_q(\vec{x})$ from $\mathbb{Q}_p^m$ to $\mathbb{Q}_p$ such that $(\vec{x}, f_1(\vec{x}), \ldots, f_q(\vec{x})) \in S$ for all $\vec{x} \in \mathbb{Q}_p^m$.*

This lemma provides a method to select one particular nth root of x. To see that one of the nth roots can be singled out by this lemma, first note that there are at

most n of them; so letting $\alpha = n$, the cardinality can be bounded as required. We next define kth-power residues. This definition requires an alternate, equivalent form of Hensel's lemma often called the Hensel-Rychlik lemma (see [7, pps. 87-88] for a proof of equivalence):

Lemma 4.4. *A valued field K is Henselian if and only if for each $f \in \mathcal{O}[X]$ and $a \in \mathcal{O}$ with $v(f(a)) > 2v(f'(a))$, there exists $\alpha \in \mathcal{O}$ with $f(\alpha) = 0$ and $v(a - \alpha) > v(f'(a))$. Here, $\mathcal{O}$ is the valuation ring and $v(x)$ is the valuation.*

Consider the multiplicative group $K^\times$. This lemma can used to prove that for any $k \in \mathbb{N}, k \geq 2$, the index (i.e. $[K^\times : K^{\times k}]$) of the subgroup $K^{\times k}$ of kth-powers in $K^\times$ is finite, and that we can choose natural numbers as representatives for the cosets in the quotient group $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times k}$.

Definition 4.5. The *kth-power residue* of an element $x \in K^\times$ is the coset $xK^{\times k}$.

By means of an easy induction on q, the proof of Lemma 4.3 reduces to the case where $q = 1$. For $q = 1$ the proof breaks up into three cases:

1) Card $S_x = 1$,

2) The elements of S_x do not all have the same value, or

3) The elements of S_x do not all have the same kth-power residue for an arbitrary $k \in \mathbb{N}, k \geq 2$.

What we are going to do is to repeatedly replace S_x by a smaller subset S'_x in order to reduce the cardinality of S_x (eventually) to 1. In case 1) there is no further work to do. So assume Card $S_x \geq 2$. We then choose for membership in S'_x those element(s) of S_x that have the lowest value. Then, if multiple elements have the same value we can distinguish them by their kth-power residues. This builds on work done by MacIntyre in [17].

It should now be clear that the proof of case 3) above is the key to Denef's lemma. Denef's proof was rather light on details, so I give a more detailed account here. First, we want to adjust S_x so that the mean, $\overline{y}$, of its elements is 0. This is easily achieved by replacing the elements y_i in S_x with $y_i - \overline{y}$. So we can assume $S_x = \{y_1, y_2, \ldots, y_m\}$ with $\overline{y} = 0$ and $m = \operatorname{Card} S_x \leq n$. Furthermore assume $m > 1$ and $v(y_1) = v(y_2) = \cdots = v(y_m)$. Write $y_i = p^{v(y_i)} y_i'$; then $v(y_i') = 0$, and the mean of the y_i''s is still 0.

Let $\kappa = \max\limits_{j=1,\ldots,m} v(j)$ and choose $k = \phi(p^{\kappa+1})$, where ϕ is Euler's totient function. This means $v(k) = v(\phi(p^{\kappa+1})) = v((p-1)p^{\kappa}) = \kappa$. Now, consider the finite set R of positive integers of the form

$$b_0 + b_1 p + \cdots + b_{2v(k)} p^{2v(k)},$$

where every b_i belongs to $\{0, \ldots, p-1\}$ and b_0 is not 0. If $v(x) = 0$ for some $x \in \mathbb{Q}_p$, then there is a unique r from R with $x = r + p^{1+2v(k)} z$, where $v(z)$ is nonnegative. This means

$$\frac{x}{r} = 1 + p^{1+2v(k)} \frac{z}{r}$$

with $v\left(\dfrac{z}{r}\right) = v(z) \geq 0$. Lemma 4.4 can be used to show that $\dfrac{x}{r}$ is a kth-power in $\mathbb{Q}_p$. Then $x \in r\mathbb{Q}_p^{\times k}$.

Returning to the y_i''s, since we are assuming that the y_i''s all have the same kth-power residue, and since the y_i''s are of value 0 by construction, there is an integer $r \in R$,

$$r = b_0 + b_1 p + \cdots + b_{2\kappa} p^{2\kappa},$$

such that each y_i' belongs to the coset of r. Thus each y_i' is r times the kth-power of an element e_i. Both r and e_i must have value 0, and, since $k = (p-1)p^{\kappa}$, $e_i^k = 1 + p^{\kappa+1} z_i$, where z_i has nonnegative value. To see this we utilize induction on κ. For $\kappa = 0$, we have $k = p - 1$, and $e_i^{p-1} = 1 + p z_i$ by Fermat's Little Theorem,

as required. For $\kappa > 0$, suppose we have found z_i such that $e_i^k = 1 + p^{\kappa+1}z_i$. We must find w with nonnegative value such that $e_i^{kp} = 1 + p^{\kappa+2}w$. To do this, note that $e_i^{kp} = (e_i^k)^p = (1 + p^{\kappa+1})^p z_i$ by the inductive hypothesis. This equals

$$1 + \binom{p}{1}p^{\kappa+1}z_i + \binom{p}{2}(p^{\kappa+1}z_i)^2 + \cdots + \binom{p}{p-1}(p^{\kappa+1}z_i)^{p-1} + \binom{p}{p}(p^{\kappa+1}z_i)^p.$$

The second term has $p^{\kappa+2}$ as a factor. For the third term, $p^{2\kappa+3}$ is a factor; for the penultimate term, $p^{(p-1)\kappa+p}$ is a factor. Since the last term has $p^{p\kappa+p}$ as a factor, all the terms but the first have $p^{\kappa+2}$ as a factor. This causes $e_i^{kp} = 1 + p^{\kappa+2}w$ for some w with nonnegative value.[1]

To continue, we now have each $y_i' = r(1+p^{\kappa+1}z_i)$, and since the elements y_i' have sum 0 (since $\overline{y_i}$ is 0), $0 = r\Big(m + \sum_i p^{\kappa+1}z_i\Big)$. Since r has value 0, $m = p^{\kappa+1}\Big(-\sum_i z_i\Big)$ and so $\kappa+1 \leq v(m)$, contrary to the choice of κ (recall $\kappa = \max_{j=1,\ldots,m} v(j)$ so $v(m) \leq \kappa$) and case 3). Therewith Lemma 4.3 is proven.[2]

This can now be combined with Scowcroft's work in [19] and Weispfenning's quantifier elimination in [21] to construct the defining formula $\phi(x, y)$ in $\mathcal{L}_M$ of a Skolem function for the nth root of x. Defining the Skolem function for Hensel's Lemma in a primitive recursive manner can be handled entirely with Scowcroft and Weispfenning's work. This means that we do not really need to extend the language with additional symbols for the Skolem functions; we can define the new symbols as shorthand, as we did with the new symbols we introduced in Chapter 1. So the definable Skolem functions allow us to replace the existential quantifiers that occur in our axioms with terms. We will use this in our construction of p-adic closures in Chapter 5.

[1] My thanks to R. Perlis for his aide with this induction argument.

[2] This elucidation of Denef's proof relies heavily on correspondence from P. Scowcroft.

Chapter 5
A Construction of a P-adic Closure

Definition 5.1. A field L is called a *p-adic closure* of a p-valued field K if L is a maximal p-valued extension field of K that is algebraic over K. Equivalently, L is a p-adically closed algebraic extension of K whose unique p-valuation extends the valuation on K.

In this section we want to present a finitary construction of the p-adic closure of a p-valued field. In order to do this we first have to set some limitations. One fact that we should recognize is that the p-adic closure of a p-valued field is not in general unique, in contrast to the fact that the real closure of an ordered field is always unique. The reason for this, however, is that the value group can be extended in different ways. If we simply choose an appropriate extension of the value group, or alternatively require that the value group begins as a $\mathbb{Z}$-group, then the p-adic closure will be unique. Therefore if we wish our p-adic closure to be unique, we would need, as a preliminary step, to ensure that the value group is a $\mathbb{Z}$-group.

Next, whether the p-adic closure of the given p-valued field is unique or not, we must obviously assume that the field operations in K $(+, -, \cdot, ^{-1})$ are computable and the predicates in K $(V, P_2, P_3, \ldots)$ decidable in order to effectively construct a p-adic closure.

For this section we will write PCF for the first-order formal system in the language of valued fields $(\mathcal{L}_M)$ based on an appropriate set of logical axioms and rules of inference for the classical, first-order predicate calculus with equality (e.g., see

[10]), together with the non-logical axioms for MacIntyre's language $(M1)$-$(M8)$ which we hope the reader will recall from Chapter 2.

Let K be a p-valued field. We will denote by $\mathrm{PCF}(K)$ the formal system whose language, $\mathcal{L}_M(K)$, is $\mathcal{L}_M$ supplemented by constant symbols c_k for each $k \in K$, and whose axioms are $(M1)$-$(M8)$ supplemented by the diagram of K. The latter is defined to be the set of those atomic $\mathcal{L}_M(K)$-sentences and negated atomic $\mathcal{L}_M(K)$-sentences that hold in K. We will also make use of Weispfenning's quantifier elimination for p-valued fields (see [21]):

Theorem 5.2. *To any formula ϕ in the language $\mathcal{L}_M$ of valued fields, we can, in a primitive recursive way, associate two objects:*

(1) a quantifier-free *formula ψ in $\mathcal{L}_M$ and*

(2) a proof *in PCF of the equivalence $\phi \leftrightarrow \psi$.*

The notation $\mathrm{PCF}(K) \vdash \theta$ will mean there is a proof of θ in $\mathrm{PCF}(K)$.

Corollary 5.3. *PCF(K) is logically complete; i.e., for every sentence ϕ in $\mathcal{L}_M(K)$, either $\mathrm{PCF}(K) \vdash \phi$ or $\mathrm{PCF}(K) \vdash \neg\phi$ (and we can decide which if K is computable).*

If for a formula $\phi(x)$ in $\mathcal{L}_M(K)$ with no free variables other than x,

$$\mathrm{PCF}(K) \vdash \exists x \, \forall y \, (\phi(x) \wedge (\phi(y) \rightarrow x = y)),$$

then we call $\phi(x)$ *uniquely satisfiable*. We call uniquely satisfiable $\mathcal{L}_M(K)$-formulas $\phi(x)$ and $\psi(x)$ *equivalent* if

$$\mathrm{PCF}(K) \vdash \exists x \, (\phi(x) \wedge \psi(x)).$$

We shall define the elements of our p-adic closure, P, to be the equivalence classes $[\phi(x)]$ of uniquely satisfiable $\mathcal{L}_M(K)$-formulas $\phi(x)$.

We then have to define all the field operations on P. Define $[\phi(x)] +_P [\psi(y)]$ to be $[\theta(z)]$, where $\theta(z)$ is:

$$\exists x\, \exists y\, (\phi(x) \wedge \psi(y) \wedge z = x + y).$$

We define $\cdot_P$ similarly. We define $-_P[\phi(x)]$ as $[\psi(y)]$, where $\psi(y)$ is $\exists x\, (\phi(x) \wedge y = -x)$. We define $[\phi(x)]_P^{-1}$ as $[\psi(y)]$, where $\psi(y)$ is $\exists x\, (\phi(x) \wedge (y = x^{-1})$. We define 0_P and 1_P as $[x = 0]$ and $[x = 1]$, respectively.

Next we verify that the field axioms hold for these definitions. For commutativity of addition we need that for uniquely satisfiable ϕ and ψ,

$$[\phi(x)] +_P [\psi(y)] = [\psi(y)] +_P [\phi(x)],$$

which simplifies to:

$$PCF(K) \vdash \exists x\, \exists y\, (\phi(x) \wedge \psi(y) \wedge x + y = y + x).$$

This is established by the field axioms and the unique satisfiability of ϕ and ψ. To see that P satisfies $(M2)$ we need to break it into two cases; the first case is where $[\phi(x)] = [x = 0]$ and the second case is where $[\phi(x)] \neq [x = 0]$. For the first case we need to show $[x = 0]^{-1} = [x = 0]$, which means

$$\mathrm{PCF}(K) \vdash \exists y\, (\exists x\, (x = 0 \wedge y = x^{-1}) \wedge y = 0).$$

This is true since $0^{-1} = 0$, which follows from $\mathrm{PCF}(K)$, by $(M2)$. In the second case we need to show $[\phi(x)] \cdot_P [\exists x\, (\phi(x) \wedge y = x^{-1})] = [x = 1]$. This follows from $xx^{-1} = 1$, which in turn follows from $\mathrm{PCF}(K)$ in this case.

The other field axioms can be handled similarly, except for $0_P \neq 1_P$. Since $0_P \neq 1_P$ means

$$\mathrm{PCF}(K) \nvdash \exists x\, (x = 0 \wedge x = 1),$$

or equivalently, $\mathrm{PCF}(K) \nvdash 0 = 1$, this is equivalent to the consistency of $\mathrm{PCF}(K)$ (since $\mathrm{PCF}(K) \vdash 0 \neq 1$). This consistency must be proved by finitary, syntactic means and not in the usual way by appealing to the existence of a model of $\mathrm{PCF}(K)$, which is precisely what we are trying to construct. A finitary consistency proof could be extracted from an unwinding process on the proof of Kochen's Theorem; further thoughts on this are included in Chapter 6.

Consistency can also be used to show that P has characteristic 0. To show this we need to show that

$$[x = 1] +_P \cdots +_P [x = 1] \neq [x = 0]$$

for any number of summands n, $n \geq 1$. This means

$$\mathrm{PCF}(K) \nvdash \exists z \Big(\exists x_1, \ldots, x_n (x_1 = 1 \wedge \cdots \wedge x_n = 1 \wedge z = x_1 + \cdots + x_n) \wedge z = 0 \Big)$$

This is equivalent to $\mathrm{PCF}(K) \nvdash 1{+}1{+}\cdots{+}1 = 0$. Assuming $\mathrm{PCF}(K)$ is consistent, this follows from $(M1)_n$.

Next we need to define a valuation ring $\mathcal{O}$ in P: $[\phi(x)] \in \mathcal{O}$ iff

$$\mathrm{PCF}(K) \vdash \exists x (\phi(x) \wedge V(x)).$$

Similarly, we define $\mathfrak{P}_n$ in P: $[\phi(x)] \in \mathfrak{P}_n$ iff

$$\mathrm{PCF}(K) \vdash \exists x \, \exists z (\phi(x) \wedge z^n = x).$$

To show P satisfies $(M3)$ we need to show

$$\begin{aligned} \mathrm{PCF}(K) \vdash \exists x \, (x = 0 \wedge V(x)) \wedge \exists y \, (y = 1 \wedge V(y)) \wedge \neg \exists z \, (z = p^{-1} \wedge V(z)) \\ \wedge \Big(\big(\exists x (\phi(x) \wedge V(x)) \wedge \exists y (\psi(y) \wedge V(y)) \big) \rightarrow \\ \big(\exists z (z = x - y \wedge V(z)) \wedge \exists w (w = xy \wedge V(w)) \big) \Big). \end{aligned}$$

This simplifies to

$$\mathrm{PCF}(K) \vdash \Big(V(0) \wedge V(1) \wedge \neg V(p^{-1}) \wedge ((V(x) \wedge V(y)) \to (V(x-y) \wedge V(xy)))\Big).$$

This is precisely $(M3)$. That P satisfies $(M4)$ and $(M5)$ follows similarly. For $(M8)_n$ we need to show that

$$\mathrm{PCF}(K) \vdash \bigvee_{r=0}^{n-1} \bigvee_{\substack{1 \le a < p^{2v(n)+1} \\ p \nmid a}} \exists x \, \exists z_{ra}(\phi(x) \wedge z_{ra}^n = x(ap^r)^{-1}).$$

This follows from the fact that $(M8)_n$ is an axiom in PCF.

Next we will use Scowcroft's Theorem 4.2 as applied to p-adically closed fields to produce a uniquely satisfiable formula for both of the axiom schemata that involve existential quantifiers ($(M6)_n$, $(M7)_n$) [19]. Using these functions we can define the w whose existence axiom schema $(M6)_n$ asserts and the z whose existence axiom schema $(M7)_n$ asserts to be the equivalence classes of the uniquely satisfiable formulas that define the appropriate Skolem functions (as described in Chapter 4). Thus, P satisfies all of MacIntyre's axioms, and so it is p-adically closed.

Next, K can be embedded as a valued subfield of P by the mapping $k \mapsto [x = c_k]$ ($k \in K$), which one can easily check to be a value-preserving embedding since $\mathrm{PCF}(K)$ contains the diagram of K.

What is left is to show that every element $[\phi(x)]$ of P is algebraic over K. By Theorem 5.2 we can represent $[\phi(x)]$ by a quantifier-free formula $\psi(x)$ containing no variables other than x. Now, we can organize $\psi(x)$ into disjunctive normal form:

$$\bigvee_i \Big(\bigwedge_j p_{ij} = 0 \wedge \bigwedge_j q_{ij} \neq 0 \wedge \bigwedge_j V(r_{ij}) \wedge \bigwedge_{n=2}^{k} \Big(\bigwedge_j P_n(s_{nij}) \Big) \wedge \bigwedge_{n=2}^{k} \Big(\bigwedge_j \neg P_n(u_{nij}) \Big) \Big),$$

where p_{ij}, q_{ij}, r_{ij}, s_{nij} and u_{nij} are terms in $\mathcal{L}_M(K)$ (built up from $x, 0, 1$, and finitely many c_k by the field operations $+, -, \cdot, ^{-1}$). We did not include negated atomic formulas $\neg V(r_{ij})$ in our disjunctive normal form above, because $\neg V(x) \leftrightarrow$

$V((px)^{-1})$. The terms p_{ij}, q_{ij}, r_{ij}, s_{nij} and u_{nij} can be viewed as rational functions in x with coefficients in K. Now, for some i there exists an x satisfying the ith disjunct, since $\phi(x)$ was (uniquely) satisfiable; fix that i. The subset of P defined by

$$\bigwedge_j q_{ij} \neq 0 \wedge \bigwedge_j V(r_{ij}) \wedge \bigwedge_{n=2}^{k} \Big(\bigwedge_j P_n(s_{nij}) \Big) \wedge \bigwedge_{n=2}^{k} \Big(\bigwedge_j \neg P_n(u_{nij}) \Big)$$

can be shown to be either empty or infinite. Therefore, since $\phi(x)$ is uniquely satisfiable, at least one of the p_{ij} is non-constant when viewed as a function of x. It follows that $[\phi(x)]$ is algebraic over K. Thus, P is a p-adic closure of K, as claimed.

Chapter 6
Further Considerations

The full 'unwinding' process for the proof of Kochen's Theorem would revolve primarily on two processes which are analagous to processes used in the real closed case of 'unwinding' the proof of Artin's Theorem [2] [14]. In the real closed case these are to address the squares and odd-degree polynomials. Kreisel showed how this could be done in [14]. In the p-adic case analagous processes would need to be found for the nth-powers and for 'Hensel'-polynomials of the form

$$x^n + x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0 \in \mathcal{O}[x], a_i \in \mathcal{M}.$$

Recall, $\mathcal{M}$ is the maximal ideal of the valuation ring $\mathcal{O}$. In addition to these two cases it is also important to build tools to more deeply analyze the functioning of the γ-operator (2.1).

In the case of the nth-roots we can use Denef's Lemma 4.3 to mimic Kreisel's work on finding square roots. It will require more cases, and consequently more complicated formulas but presents no ultimate challenge.

The difficulty lies with finding a way to reduce a 'Hensel'-polynomial to another 'Hensel'-polynomial with a common root but lower degree. This could potentially be tackled by converting to other forms of Hensel's lemma, but thus far despite extensive efforts I have yet to succeed and it remains an open problem.

The γ-operator has also proven difficult to work with. One result that could help open this portion of the 'unwinding' process would be to find a way to write any element of the field K in the form

$$\sum\prod\gamma(x_{ij}) + \frac{1}{p}\Big(\sum\prod\gamma(y_{ij})\Big)$$

. This would be analagous to the fact that in a field of characteristic not 2 any element r can be written as

$$r = \left(\frac{1+r}{2}\right)^2 + (-1)\left(\frac{1-r}{2}\right)^2.$$

Unfortunately the nature of the γ-operator has made this an extremely difficult process to construct.

References

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

[2] C.N. Delzell, *Kreisel's Unwinding of Artin's Proof*, Kreiseliana, A.K.Peters Wellesley, Massachusetts, (1996), pp. 113-246.

[3] C.N. Delzell *A New Simpler finitary construction of the Real Closure of a computable ordered field* Preprint, 2008.

[4] J. Denef, *The Rationality of the Poincaré Series to the p-adic Points on a Variety*, Inventiones Mathematicae Vol. 77, (1984), pp. 1-23 (Lemma 7.1 on pp. 14-15)

[5] L. v.d.Dries, *Algebraic Theories with Definable Skolem Functions*, Journal of Symbolic Logic Vol.49, No.2 June 1984, pp. 625-629.

[6] H. Enderton, *A Mathematical Introduction to Logic*, Harcourt/Academic Press San Diego 2001.

[7] A.J. Engler and A. Prestel, *Valued Fields*, Springer Monographs in Mathematics, Springer-Verlag, 2005.

[8] S. Feferman, *Kreisel's Unwinding Program*, Kreiseliana, A.K.Peters Wellesley, Massachusetts, (1996), pp. 247-274

[9] K. Gödel, *The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory*, Kurt Gödel Collected Works Vol. II, Oxford University Press, 1990.

[10] S. Kleene, *Introduction to Metamathematics*, D. Van Nostrand Company, Inc. New York, 1952.

[11] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics Vol. 58, Springer-Verlag, New York, 1977.

[12] S. Kochen, *Integer Valued Rational Functions over the p-adic Numbers: A p-adic Analogue of the Theory of Real Fields*, Proceedings of Symposia in Pure Mathematics Vol. XII, American Mathematical Society, 1969.

[13] G. Kreisel, *Some Uses of Metamathematics*, British Journal for the Philosophy of Science Vol. VII No. 26, August 1956, pp. 161-173.

[14] G. Kreisel, *Sums of Squares*, Summaries of Talks Given at the Summer Institute for Symbolic Logic, 1957, Cornell University Institute of Defense Analyses, Princeton, (1960), pp. 313-20.

[15] A. Levy, *Basic Set Theory* Dover Books on Mathematics, 1979.

[16] D. Marker, *Model Theory: An Introduction*, Graduate Texts in Mathematics Vol. 217, Springer, New York 2002.

[17] A. MacIntyre, *On Definable Subsets of p-adic Fields*, Journal of Symbolic Logic Vol.41, No.3 September 1976, pp. 605-610.

[18] A. Prestel and P. Roquette, *Formally p-adic Fields*, Lecture Notes in Mathematics 1050, Springer-Verlag, 1984.

[19] P. Scowcroft, *A Note on Definable Skolem Functions*, The Journal of Symbolic Logic Vol. 53, No. 3 Sept. 1988, pp. 905-911.

[20] R. Solovay, *Introductory Note to Gödel 1938, 1939, 1939a, and 1940*, Kurt Gödel Collected Works Vol. II, Oxford University Press, 1990.

[21] V. Weispfenning, *Quantifier elimination and decision procedures for valued fields* Models and sets (proceedings of Logic Colloquium '83), Lecture Notes in Mathematics, Vol. 1103, Springer-Verlag. Berlin, (1984), pp. 419-472.

Vita

Evan Eakins was born in 1984, in Redmond, Washington. He finished his undergraduate studies at Cornell College in May 2007. He earned a master of science degree in mathematics from Louisiana State University in May 2013. In August 2007 he came to Louisiana State University to pursue graduate studies in mathematics. He is currently a candidate for the degree of Doctor of Philosophy in mathematics for the spring of 2014.