Perspectives in Mathematics
Anniversary of Oberwolfach 1984
© Birkhäuser Verlag, Basel

Some Tendencies in Contemporary Algebra

PETER ROQUETTE

Mathematisches Institut, Im Neuenheimer Feld 288,
D-6900 Heidelberg (FRG)

Dem Andenken an ***Wilhelm Süss*** *gewidmet, den Gründer und spiritus rector des Mathematischen Instituts in Oberwolfach*

1 Introduction

Mathematics is, on the one hand, a *cumulative science.* Once a mathematical theorem has been proved to be true then it remains true forever; it is added to the stock of mathematical discoveries which has piled up through the centuries and it can be used to proceed still further in our pursuit of knowledge.

On the other hand, the mere proof of validity of a theorem is in general not satisfactory to mathematicians. We also want to know "why" the theorem is true, we strive to gain a better understanding of the situation than was possible for previous generations. Consequently, although a mathematical theorem never changes its content, we can observe a continuous change of the *form of presentation*, in the course of history of our science. Sometimes a result seems to be better understood if it is generalized, or if it is looked at from a different point of view, or if it is embedded into a general theory which opens analogies to other fields of mathematics. Also, in order to make further progress possible it is often convenient and sometimes necessary to develop a framework, conceptual and notational, in which the known results become trivial and almost self-evident at least from a formalistic point of view. So when we look at the history of mathematics we indeed observe a change, not in the nature of mathematical truth but in *the attitude of mathematicians* towards it. It may well be that sometimes a new theory is but the response to a current fashion, and sometimes it may be mere fun to derive a theorem by unconventional means. But mostly the changes in attitude reflect a serious effort towards a better understanding of the mathematical universe.

It is fascinating to observe such trends in the past and see how they have led to the picture of today's mathematics. But likewise it is not without interest to search for trends in *contemporary* mathematics since they will shape the future of our science.

In this article we shall restrict our discussion to *algebra.* But even in algebra the reader cannot expect a full account of all the many recognizable threads of development. Some of these are quite obvious to the attentive observer: for instance the tendency towards *geometrization of algebra*, which means adopting the language of geometry and its way of arguing. This has had striking successes, the most recent one being the proof of Mordell's conjecture by Faltings, and it has found its due recognition by the contemporary mathematical public. Another obvious trend in present-day algebra is its *algorithmization*, i. e. the desire to supplement every existence proof and actually all arguments, by an effective algorithm if this is possible at all. Again, this is not exactly new and algorithms have been pursued throughout the history of algebra. But during this century it often seemed, or it was at least proclaimed that the *structural viewpoint* is to be dominating, and that in this framework computational or algorithmical considerations are at most of secondary interest. Today, since the structural viewpoint has become firmly inserted in contemporary mathematical thinking it is realized again that algorithms are essential, not only for computers but also theoretically, as part of our understanding of mathematics.

In this article we propose to discuss some other tendency of contemporary algebra, not yet quite as auspicious as the ones mentioned above and not even known to many, but nevertheless somewhat remarkable. This is the *intrusion of model theoretic notions and arguments into algebra*. Here, "model theory" is used in the sense of mathematical logic. The field of mathematical logic was formerly regarded as pertaining mainly to the foundations of mathematics only, giving the mathematician a (hopefully) solid base for his work but otherwise not influencing actual mathematical research activity. Some mathematicians had even voiced their opinion that mathematical logic does not properly belong to mathematics but should be considered as part of philosophy. This has completely changed, in the meantime. Model theoretic notions and results have intruded heavily into mathematics and in particular into algebra. Model theory provides the algebraist with a new way of reasoning which was not available before. This is possible if he (the algebraist) remains conscious of *the formal language with which algebraic structures are described.* Perhaps a good illustration will be the discussion of the model theoretic notion of *elementary equivalence* which is much more adapted to the investigation of algebraic structures than the notion of *isomorphism*, contrary to what is claimed in many textbooks of algebra. The notion of isomorphism is of set-theoretical nature and introduces set-theoretical difficulties into algebra which are not inherent in the algebraic problem itself. Whereas the notion of elementary equivalence permits to deduce the same consequences as from isomorphism, but it also allows to change sets without disturbing algebraic properties.

The idea to make use of model theory in this way is originally due to *Abraham Robinson.*

When I first planned to write this article I meant to give a review about all applications of model theory in algebra, or at least about the most important ones. But soon it turned out that this task would have required more space than available here, and more time for preparation. Also, in view of the large amount of literature is has become doubtful whether a comprehensive report about model theory in algebra would be of much value today. As said above, model theory provides us with a new method, a new way of mathematical reasoning. In order to explain this method it is perhaps sufficient to discuss particular examples where it has been applied.

Accordingly this article will be restricted to certain parts of algebra. The examples selected for our discussion come from field theory; they are all connected with the work of the algebra group in Heidelberg.*) Although we realize that this selection is somewhat arbitrary we hope that it will be sufficient for our purpose: to acquaint the reader with some of the *basic principles* of model theoretic methods in algebra.

2 Elementary Equivalence

Let us discuss the model theoretic notion of *elementary equivalence* in relation to the classical algebraic notion of *isomorphism*. Modern algebra deals with *algebraic structures* as its basic objects. Examples of algebraic structures are groups, rings, fields, ordered fields etc. Along with the notion of structure there comes the notion of *isomorphism* between structures of the same kind: group isomorphism, ring isomorphism etc. If we have established that two algebraic structures K and L, say fields, are isomorphic then we know that *every algebraic property of K is shared by L, and vice versa*. This is precisely the reason why isomorphism theorems are of fundamental importance in algebra.

But is isomorphism between K and L really necessary to draw the above conclusion? *Are there non-isomorphic algebraic structures which do have the same algebraic properties*?

In order to discuss this question it is necessary to specify what is meant by "algebraic property" of a given algebraic structure. As a rule, an algebraist does not bother to make this precise because in concrete situations it always seems to be evident which properties are admissible as "algebraic properties" in the above sense. For instance, if we consider rings then the property of being commutative is certainly admissible: if a ring K is commutative then every isomorphic copy of K is commutative too. What is the general description of "algebraic properties" which are admissible in this context?

We consider algebraic structures of a given type, say fields or groups. These structures are defined by *axioms*. The axioms contain references to certain functions and relations which are defined on structures of the type considered. For instance, the group axioms refer to a 2-variable function $x \cdot y$ which denotes the group operation. The field axioms refer to two 2-variable functions $x + y$ and

*) We have *excluded* the work with *nonstandard methods* in algebra and number theory. For this we refer to our report [Rq3].

$x \cdot y$, denoting addition and multiplication in the field, etc. Now an "algebraic statement" with respect to the given type of structure must be expressible *solely* in terms of these functions and relations which appear in the axioms.

We envisage the axioms written in a *formal language* $\mathscr{L}$ whose vocabulary is adapted to the structure type considered; thus the vocabulary contains the appropriate function symbols and relation symbols (including constant symbols). It is always understood that $\mathscr{L}$ is an *elementary* (or first order) language. This means that the variables in $\mathscr{L}$ denote individuals only; there are no set variables or function variables. Accordingly, quantification ($\forall$ or $\exists$) is permitted with respect to individuals only. Historical experience shows that for most of the relevant algebraic structures, the axioms can indeed be stated in an elementary language. (This has led some authors to *define* algebraic structures as being those whose axioms can be stated in an elementary language.)

We now can give the definition of an admissible "algebraic property" of a structure: *such property should be expressible by a sentence φ in the language $\mathscr{L}$.* In other words: a structure K has this property if and only if φ holds in K. For instance in ring theory, the property of a ring K to be commutative means that the following sentence holds in K:

$$(\forall x)\,(\forall y)\,(xy = yx).$$

The precise definition of the notion of *sentence* in a formal language $\mathscr{L}$ can be found in any introductory treatise on mathematical logic [Po], [Bar], [CK].

Now let us review the situation: We have a formal (elementary) *language* $\mathscr{L}$, with a vocabulary consisting of certain function symbols and/or relation symbols (including perhaps some constant symbols, e.g. 0 and 1 in case of field theory). We consider *structures of type* $\mathscr{L}$, which means that the function symbols and relation symbols in $\mathscr{L}$ should have an interpretation by means of functions resp. relations in the structure. Any set of sentences of $\mathscr{L}$ defines a *theory*; the defining sentences are called *axioms* of that theory. An $\mathscr{L}$-structure K is called a *model* of the theory if all the axioms hold in K. If φ is any sentence in $\mathscr{L}$, and if φ holds in all models then φ is said to be a *theorem* of the theory. In general, if φ is an arbitrary sentence then φ may hold in some models but perhaps not in all models of the theory. If φ holds in K then it is customary to write $K \models \varphi$. We then say that φ defines an "algebraic property" of K or that K has the property φ.

Definition: Two models K and L are said to be *elementary equivalent* if every algebraic property of K is shared by L, and vice versa. In other words: $K \models \varphi$ iff $L \models \varphi$. If this is so then we write $K \equiv L$.

If K and L are isomorphic then we write $K \approx L$. Clearly, isomorphic models are elementary equivalent. Now our above question can be formulated, more precisely, as follows:

Do there exist non-isomorphic models which are elementary equivalent?

Model theory provides the answer to this question: Yes, *to every infinite* *model K there exists a non-isomorphic, elementary equivalent model L.* Indeed, for every sufficiently large cardinal number α there exists a model $L \equiv K$ such that $|L| = \alpha$. "Sufficiently large" means that α should be infinite and greater or equal to the cardinality of the vocabulary of the language $\mathscr{L}$. This is the theorem of Löwenheim-Skolem-Tarski. If we are dealing with group theory, or ring theory, or field theory etc. then there are only finitely many function symbols and relation symbols in the vocabulary and hence we can find a model $L \equiv K$ in *every* infinite cardinality α; in particular L can be countable.

In case of a *finite* model K it is easily seen that every elementary equivalent model $L \equiv K$ is isomorphic: $L \approx K$.

We conclude that, for the investigation of properties of algebraic structures, *the notion of isomorphism* is adequate in the case of finite structures, but it is *inadequate for infinite structures.* The adequate notion is that of elementary equivalence. If we want to know whether an algebraic structure K has a certain property φ then it suffices to find a structure $L \equiv K$ for which the validity of φ can be checked; L need not be isomorphic to K.

Hence a *new way of mathematical reasoning is introduced into classical algebra, with the notion of isomorphism being replaced by elementary equivalence.* The success of this new method depends on how one is able to handle, algebraically, the notion of elementary equivalence. Let us look at some examples, classical ones and some that are more recent.

3 Algebraically Closed Fields

We refer to the celebrated paper of *E. Steinitz* [St] which appeared in volume 137 of *Crelle's Journal* (1910). This paper contains the first systematic study of fields from the "algebraic" point of view, i.e. solely as models of the field axioms. Today we are so used to this kind of viewpoint that we can hardly imagine the impact and the source of inspiration which Steinitz' paper generated for the mathematicians of his time. It became a "classic" and, because of its fundamental importance it was reprinted in book form some twenty years after its first appearance (and later again in one of the post-war Chelsea editions). Steinitz' program was to give a constructive description of all fields, up to isomorphisms. For our purpose his results on *algebraically closed* fields are relevant. Steinitz showed that an algebraically closed field K is completely determined, up to isomorphisms, by two invariants: its *characteristic* $p = \operatorname{char}(K)$ which is either 0 or a prime number, and its *transcendence degree* $t = \operatorname{tr}(K)$ which is a cardinal number. Both p and t can be arbitrarily prescribed: there exists an algebraically closed field with given characteristic and given transcendence degree.

If $\operatorname{tr}(K)$ is finite then the algebraically closed field is denumerable, $|K| = \aleph_0$. If $\operatorname{tr}(K)$ is infinite then $|K| = \operatorname{tr}(K)$. Consequently, if $|K| > \aleph_0$ then $|K| = \operatorname{tr}(K)$; in this case Steinitz' theorem says that for fixed characteristic

$p \geqq 0$, K is *uniquely determined* (up to isomorphisms) *by its cardinality*. This fact is expressed by saying that *the theory of algebraically closed fields of characteristic p is categorical in every uncountable cardinality.*

Now there is a general theorem of model theory, called *Łos-Vaught test*, to the following effect: For any theory T, if T is categorical in but one infinite cardinality greater or equal to the cardinality of the vocabulary of the language, then all infinite models of T are elementary equivalent [Bar]. We conclude that *all algebraically closed fields of characteristic p are elementary equivalent.* Thus if we want to know whether an algebraically closed field K has a certain algebraic property φ then the transcendence degree $\operatorname{tr}(K)$ is of no importance; if φ holds in any other algebraically closed field of the same characteristic then φ also holds in K. In characteristic zero this fact is commonly known as the *Lefschetz principle.* Historically, this name is not exactly correct since Lefschetz in his book on Algebraic Geometry [Le] stated a somewhat different principle, related but not quite identical to the above. To explain this we need the notion of *elementary extension.*

Quite generally let T be an arbitrary theory, formulated in an elementary language $\mathscr{L}$, and let K, L be models of T. We suppose that $K \subset L$, which means that L should be an extension of K. The notion of elementary equivalence $K \equiv L$ has been defined above already: every sentence φ of $\mathscr{L}$ which holds in K, should also hold in L. Now let us consider formulas $\varphi(x_1, \ldots, x_n)$ depending on free parameters $x_1, \ldots, x_n$. Let $c_1, \ldots, c_n \in K$. Then $\varphi(c_1, \ldots, c_n)$ repesents a property of K in whose formulation the elements $c_1, \ldots, c_n \in K$ are involved, besides of the other constants, functions and relations which are defined in K as an $\mathscr{L}$-structure. More precisely, $\varphi(c_1, \ldots, c_n)$ is a sentence in the extended language $\mathscr{L}_K$ whose vocabulary contains constants to denote the individual elements $c \in K$, besides of the constant symbols, function symbols and relation symbols in the vocabulary of $\mathscr{L}$. Now if every sentence $\varphi(c_1, \ldots, c_n) \in \mathscr{L}_K$ which holds in K does also hold in L (and vice versa), then *L is said to be an elementary extension of K.* Notation: $K \prec L$. Clearly, $K \prec L$ implies $K \equiv L$. (But not conversely.)

In the theory of algebraically closed fields, it is immediate from Steinitz' work (this time applying the Łos-Vaught test to $\mathscr{L}_K$):

Every extension of algebraically closed fields is an elementary extension.

This is the "Lefschetz principle" as stated by Lefschetz in his book. Indeed, he considers an algebraically closed field K of characteristic zero. Let V denote an irreducible variety, defined in n-dimensional affine space by a system of polynomial equations

$$\text{(E)} \qquad f_1(x_1, \ldots, x_n) = 0, \ldots, f_n(x_1, \ldots, x_n) = 0.$$

Let K_0 be an algebraically closed subfield of K, containing all the finitely many coefficients $c_1, \ldots, c_r$ of $f_1, \ldots, f_m$, and such that K_0 is of finite transcendence degree. Then K_0 may be isomorphically embedded into the complex number field; let us identify K_0 with its isomorphic image: $K_0 \subset \mathbb{C}$. Then the equations

(E) define also a complex variety V^* in n-dimensional affine space over $\mathbb{C}$. Now the important fact, Lefschetz continues, is that *in the passage from V to V^* all the strictly algebraic properties of V are preserved.* Lefschetz does not explain what is meant by "strictly algebraic properties of V". If we interpret this as those properties which can be expressed by sentences of the form $\varphi(c_1,\ldots,c_r)$ in the elementary language $\mathscr{L}_{K_0}$ then indeed, they are preserved because $K_0 \prec K$ and $K_0 \prec \mathbb{C}$. (It is conceivable, though, that the Lefschetz principle applies also to other "strictly algebraic properties" which can be expressed in a higher order language only. See [Ek] and the literature cited there.)

In model theory the following terminology is used: A theory T is called *complete* if all models of T are elementary equivalent. T is called *model-complete* if every extension of models of T is an elementary extension. Thus the result of our above discussion can be briefly stated as follows:

The theory of algebraically closed fields of fixed characteristic $p \geqq 0$ is complete, and it is also model-complete.

Before proceeding to the next example, let us briefly indicate how this fact may be used as a tool in various arguments of geometric nature.

Consider a system of polynomial equations of the form (E) where the $f_1,\ldots,f_m$ are polynomials over an algebraically closed field K. The *Hilbert Nullstellensatz* gives a necessary and sufficient condition for the existence of a solution $x_1,\ldots,x_n \in K$ of the equation (E). Namely, the ideal generated by $f_1,\ldots,f_m$ in the polynomial ring $K[X_1,\ldots,X_n]$ should not be trivial; it should be a *proper* ideal. Clearly, this condition is necessary. Conversely, if the condition is satisfied let P be a maximal ideal of $K[X_1,\ldots,X_n]$ containing $f_1,\ldots,f_m$ and consider the residue class ring $K[X_1,\ldots,X_n]/P = R$. This is an integral domain containing K, and the residue classes $x_i = X_i \bmod P$ satisfy (E). Now R can be embedded into its field of quotients which in turn can be embedded into an algebraically closed field L, by the work of Steinitz. By construction, the statement

$$(\exists x_1)(\exists x_2)\ldots(\exists x_n)(f_1(x_1,\ldots,x_n)=0 \wedge \ldots \wedge f_m(x_1,\ldots,x_n)=0)$$

holds in L. Note that this statement is expressible by a sentence in $\mathscr{L}_K$, the constant parameters being the coefficients $c_1,\ldots,c_r \in K$ of the polynomials $f_1,\ldots,f_m$. Since $K \prec L$ we conclude that the above statement holds in K too, which is to say that there exist $x_1,\ldots,x_n \in K$ satisfying (E).

Thus we see that the Hilbert Nullstellensatz is *almost trivial* in view of the model-completeness of the theory of algebraically closed fields.

A less direct example of an application of model-completeness for algebraically closed fields is the following. Let K be an algebraically closed field of characteristic 0 and $K(t)$ the rational function field of one variable over K. Given any finite subset $S \subset K \cup \{\infty\}$, consider the maximal algebraic field extension F_S of $K(t)$ which is unramified outside of S. Then F_S is a Galois extension of $K(t)$. What is the structure of its Galois group G_S? The answer is that G_S is generated, as a profinite group, by $s=|S|$ elements $\sigma_1,\ldots,\sigma_s$ with the *defining relation* $\prod_{1\leqq i\leqq s}\sigma_i=1$. *Hence G_S is a free profinite group in $s-1$ generators.* In the case $K=\mathbb{C}$ a proof of this assertion is well known from the analytic theory of holomorphic functions, using the Riemann existence theorem. By means of model-completeness we would like to deduce that the above assertion holds for an arbitrary algebraically closed field of characteristic 0. In trying to apply model-completeness we try to express the above assertion by a sentence $\varphi\in\mathscr{L}_S$, the language of fields extended by s constant symbols to denote the elements of S. However, such sentence φ does not exist. But it is possible to find a sequence $\varphi_1,\varphi_2,\ldots$ of sentences in $\mathscr{L}_S$ such that the above assertion is equivalent to that all φ_n hold ($n=1,2,3,\ldots$). Each φ_n describes the factor groups of G_S of order n. For details of the construction of φ_n we refer to the literature [DrR2]. By model-completeness we can now deduce that each φ_n holds in every algebraically closed field K of characteristic 0 with a prescribed finite set $S\subset K\cup\{\infty\}$. Hence indeed, G_s is free profinite on $s-1$ generators.

No algebraic proof, without the use of analysis and topology, has been found for this structure theorem for G_S. However it follows from model theoretic fundamentals that such an algebraic proof exists, i.e. each φ_n can be deduced within $\mathscr{L}_S$ from the axioms of algebraically closed fields of characteristic 0.

If K is an algebraically closed field of characteristic $p>0$ then the structure of G_S as a profinite group is still unknown.

Let us close this section with the following remark. While talking about the "theory of algebraically closed fields" we have envisaged that theory as given by certain axioms. The reader should keep in mind, however, that these axioms are not finite in number. Indeed, to the finitely many axioms of field theory there is to be added for each $n=1,2,3,\ldots$ an axiom which says that every polynomial of degree n has a root. It is not possible to find finitely many axioms in $\mathscr{L}$ for the theory of algebraically closed fields.

Similarly, the axioms expressing the property of characteristic 0 are not finite in number: for each $n=1,2,3,\ldots$ one has the axiom that 1 added n times to itself does not give 0. It is not possible to find finitely many axioms in $\mathscr{L}$ which imply characteristic zero.

4 Real Closed Fields

The algebraic theory of real fields was originated by E. Artin and O. Schreier [AS] with their three papers in volume 5 of the *Hamburger Abhandlungen* (1926). It is noteworthy that Artin and Schreier start by mentioning the paper of Steinitz. They point out its importance for the development of "abstract" algebra and then they put forward a program how to include real algebra into the abstract framework of Steinitz. A closer look at the Artin-Schreier program reveals that one problem is left out and not mentioned at all, namely the classification problem for real closed fields, up to isomorphisms. This would be the analog of Steinitz' classification for algebraically closed fields as discussed above. Later authors have tried to fill this gap and to arrive at a classification for real closed fields; partial results were obtained [EGH] but no general satisfactory solution of the problem is known today. The transcendence degree (resp. cardinality) of the real closed field is *not* sufficient for classification up to isomorphism; one has to add more subtle invariants, as e.g. the order type of the field with respect to its (unique) ordering. But the order type is not sufficient either [Ro3]. The problem seems to be difficult.

In any case, if the classification problem were important then it should have been at least mentioned in the general program of Artin-Schreier, even though the solution could not be given. Why are Artin and Schreier silent on this problem? The answer is easily perceived: because the classification up to isomorphism is *not* important; it is of little significance with respect to algebraic problems. Instead, the *classification up to elementary equivalence* is the proper problem to be considered.

This broader classification problem is indeed mentioned, and also solved, in the Artin-Schreier papers. It follows from their work that *all real closed fields are elementary equivalent.* In other words: *The theory of real closed fields is complete.*

To be sure, the completeness theorem is not formally considered in the Artin-Schreier papers; this was done later by Tarski [TM]. But all the essential ingredients of the completeness proof can be found in the Artin-Schreier papers. The authors recognized quite clearly the significance of their work for the elementary-equivalence classification problem. This can be inferred from the statement, to be found in their paper, that "*the theorems of real algebra hold in any real closed field*". Properly interpreted, this means for every sentence φ in the language $\mathscr{L}$ of fields, if φ holds in the ordinary real number field $\mathbb{R}$ then φ holds in every real closed field. Indeed: this means completeness.

In addition to completeness, Artin-Schreier also tacitly proved *model-completeness* for the theory of real closed fields; again this was later formally verified by Tarski [TM]. Today this is known as the *Tarski principle* for real closed fields, and it is the real analog to the Lefschetz principle for algebraically closed fields.

The main motivation for the introduction and study of real closed fields was Artin's solution of the 17th Hilbert problem. Artin's theorem says that every positive definite rational function $f(X_1,\ldots,X_n)\in\mathbb{R}(X_1,\ldots,X_n)$ is a sum of squares of rational functions.*) In other words: if f is not a sum of squares in $\mathbb{R}(X_1,\ldots,X_n)$ then f is not positive definite, i.e. there exist $a_1,\ldots,a_n\in\mathbb{R}$ such

*) Strictly speaking, Hilbert formulated this problem over $\mathbb{Q}$ instead of $\mathbb{R}$. But today it has become customary to speak of Hilbert's 17th problem with reference to $\mathbb{R}$ (or to any real closed base field). From this the corresponding problem for $\mathbb{Q}$ can be deduced by simple density arguments.

that $f(a_1,\dots,a_n)$ is defined and $f(a_1,\dots,a_n)<0$. As A. Robinson [Ro2] has observed, this theorem is an *almost trivial* consequence of model-completeness for real closed fields. The argument is as follows.

Since f is not a sum of squares in $\mathbb{R}(X_1,\dots,X_n)$ it follows from Artin's theory [AS] that there exists an ordering of the field $\mathbb{R}(X_1,\dots,X_n)$ such that $f < 0$. Let L denote the real closure of $\mathbb{R}(X_1,\dots,X_n)$ with respect to this ordering. Then $\mathbb{R} \subset L$ and hence, by model-completeness, L is an *elementary* extension of $\mathbb{R}$. Consequently, if the sentence

$$(\exists x_1)\dots(\exists x_n): f(x_1,\dots,x_n)<0 \tag{S}$$

holds in L then it also holds in $\mathbb{R}$. But in L this sentence holds by construction; one may take $x_i = X_i (1 \leqq i \leqq n)$. Thus the above sentence holds in $\mathbb{R}$ which means that there exist $a_1,\dots,a_n \in \mathbb{R}$ such that $f(a_1,\dots,a_n)<0$. Q.E.D.

The beauty and simplicity of this (A. Robinson's) proof for Artin's theorem is apparent.

Note that in the sentence (S) above, an inequality sign is used which *a priori* does not belong to the vocabulary of the language of fields. The use of this inequality sign can be avoided since the ordering relation in a real closed field is uniquely determined: the positive elements are precisely the non-zero squares. Consequently, the above sentence (S) can be replaced by the following sentence in the language of fields:

$$(\exists z)(\exists x_1)\dots(\exists x_n)\left(z \neq 0 \wedge f(x_1,\dots,x_n) = -z^2\right). \tag{S'}$$

However, for the validity of A. Robinson's argument it does not matter whether we use (S) or (S'). For the model-completeness theorem or real closed fields holds in either case: with respect to the language of fields, and with respect to the language of ordered fields.

As to the proof of model-completeness, we have said above already that all its essential ingredients are to be found in the Artin-Schreier papers. However, by using basic fundamentals of model theory the proof can be considerably simplified, and in particular Artin's specialization arguments can be avoided, i.e. replaced by embedding arguments. Since this is perhaps not yet widely known among algebraists, let us briefly sketch this proof:

Let $K \subset L$ be an extension of real closed fields. We have to show that L is an *elementary* extension of K. By general model theoretic principles it suffices to show that L can be K-isomorphically embedded into a sufficiently saturated non-standard model (or ultrapower) K^* of K. More precisely, K^* should be α-saturated for some cardinal number $\alpha > |L|$. By general induction (Zorn's lemma) the problem is reduced to the case where $L|K$ is of transcendence degree 1. Let $x \in L$ be transcendental over K; then L is the real closure of the ordered field $K(x)$. By the functorial property of the real closure, every order-preserving K-embedding $K(x) \hookrightarrow K^*$ extends (uniquely) to an embedding $L \hookrightarrow K^*$ (note that K^* is real closed too). Hence it suffices to construct an order-preserving K-embedding $K(x) \hookrightarrow K^*$. Now the ordering of $K(x)$ is uniquely determined by the *Dedekind cut* which x determines in K. The cut consists of the two disjoint sets $C_x, D_x \subset K$:

$$C_x = \{c \in K : c < x\}$$
$$D_x = \{d \in K : d > x\}.$$

The saturation property of K^* guarantees the existence of $\xi \in K^*$ which determines the same cut:

$$C_\xi = C_x, \quad D_\xi = D_x.$$

Then the substitution $x \mapsto \xi$ yields the required order-preserving K-embedding $K(x) \approx K(\xi) \subset K^*$.

We have given this proof because the same typical pattern of argument applies also to other situations, yielding model-completeness results for other classes of fields. See below for various classes of valued fields. In all those cases the problem is reduced to an embedding problem for a purely transcendental extension $K(x)$ into a saturated model K^* of K, the embedding preserving certain additional structure which is connected with the class of fields considered. By the way, in the case of algebraically closed fields as discussed in section 3, the proof of model completeness can also be made to follow the same pattern. In this case there is no additional structure given, and thus we are faced with the K-embedding of $K(x)$, where K is algebraically closed, into a saturated ultrapower K^*. But this is trivially achieved by the substitution $x \mapsto \xi$ where $\xi \in K^*$ is an arbitrary transcendental over K.

Hilbert's 17th problem yields but one example for the application of the model-completeness theorem for real closed fields. There are many other examples: for instance, the *real Nullstellensatz* [Kri], [Du], giving conditions for a variety to have *real* points. It is also possible to generalize the Krull-Neukirch theorem [KrN] about the structure of the absolute Galois group of $\mathbb{R}(t)$, to arbitrary real closed base fields K instead of $\mathbb{R}$ [DrR1]. Various other applications have been given: e.g. to real algebraic function theory or to real algebraic geometry [DK]. A very interesting development concerning sums of $2n$-th powers (instead of sums of squares as in Hilbert's 17th problem) has recently been started by E. Becker; see [BeJ], [Pr].

Perhaps it is not superfluous to state explicitly the *axioms for real closed fields:*

(1) the field axioms;

(2) every sum of two squares is a square;

(3) if a is not a square then $-a$ is a square;

$(4)_n$ every polynomial of odd degree $2n+1$ has a root.

Note that $(4)_n$ is an infinite set of axioms, one axiom each for $n=1,2,3,\ldots$ It is not possible to find finitely many axioms for the theory of real closed fields.

The completeness result of Tarski says that these axioms describe the algebraic theory of $\mathbb{R}$. In other words: If φ is a sentence in the language of fields then *φ holds in $\mathbb{R}$ if and only if φ can be derived from the above axioms.*

5 *p*-adically Closed Fields

In the foregoing section we have discussed the algebraic theory of $\mathbb{R}$. It seems natural to ask, analogously, for the algebraic theory of the Hensel field $\mathbb{Q}_p$. Here and in the following, p denotes a prime number and $\mathbb{Q}_p$ is the completion of the rational number field $\mathbb{Q}$ with respect to the p-adic valuation.

Hensel's book [He] containing his discovery of the fields $\mathbb{Q}_p$ had appeared in 1908, two years before the Steinitz' paper. Steinitz informs us that it was mainly Hensel's discovery which induced him to write his article. It seems that in those times, the Hensel fields were somehow regarded to be strangers in the mathematical world; they had never been encountered before, at least not explicitly. Hence there was a desire for a general, axiomatic, abstract field theory into which the p-adic fields would fit naturally. According to Steinitz, his article was to be regarded as a first step in this direction containing the *foundations* only of a general field theory. He announced further investigations including, he said, applications to geometry, number theory and analytic theory of functions. It is not quite clear what he had in mind because none of those announced applications were ever published. His reference to *geometry* might perhaps indicate that he had envisaged an abstract theory of *real fields*, of the kind which Artin and Schreier presented 16 years later. When he mentions *number theory* then we may assume that he included an abstract theory of *p-adic fields;* this seems quite probable since he knew about Hensel's discovery and explicitly mentions it as a source of inspiration for his work.

In any case, Steinitz did never return to his announced applications, and his work was continued by Artin-Schreier [AS] in the case of real fields. It is natural to expect that soon after the appearance of the Artin-Schreier papers, the analogous theory for the p-adic fields would have been developed. Strangely enough, this was not the case. The algebraic theory of p-adic fields was given only recently by Kochen [Ko1,2]. This delay is surprising because during the twenties and thirties, the use of p-adic fields in number theory had led to striking results: for quadratic forms, for simple algebras, in class field theory etc. These successes created an atmosphere quite favorable for the so-called p-adic methods; the Hensel fields $\mathbb{Q}_p$ were now accepted, not only by the specialists, as belonging to the fundamentally important mathematical structures, similar in importance to the field $\mathbb{R}$. What, then, were the historical reasons that

Artin-Schreier's real algebra was not immediately matched by an analogous p-adic algebra?

Perhaps one of the reasons may be seen in the fact that the notion of *elementary equivalence* had *not yet been recognized* in its fundamental importance for algebra and number theory. If it would have been, then the search for the fields elementary equivalent to $\mathbb{Q}_p$ would probably have started, or at least have been mentioned as being desirable. But this was not the case and it seems that the Artin-Schreier theory was considered to be of singular nature, not being transferable to the p-adics.

In some cases, though, elementary equivalence for $\mathbb{Q}_p$ was tacitly mentioned and used. For instance, it was observed that the field $\mathbb{Q}_p^{(0)}$, of algebraic numbers within $\mathbb{Q}_p$, has for all practical purposes the same algebraic properties as $\mathbb{Q}_p$ itself. For instance, the absolute Galois group over $\mathbb{Q}_p^{(0)}$ is the same as the Galois group over $\mathbb{Q}_p$, and local class field theory also holds over $\mathbb{Q}_p^{(0)}$, etc. Later, it was observed that *every* subfield $K \subset \mathbb{Q}_p$ which is algebraically closed within $\mathbb{Q}_p$, can be used equally well as a base field for p-adic algebraic geometry [La2]. These arguments were in fact of the nature of elementary equivalence arguments, without however being explicitly stated that way.

A second reason for the delay in the systematic development of p-adic algebra was perhaps the lack of suitable prominent problems. We remember that one of the driving forces for the Artin-Schreier theory was the solution of Hilbert's 17th problem. This was concerned with *positive definite* functions. The notion of positive definite function involves the ordering relation $<$ and hence belongs to *real* algebra. But Hilbert did not state a corresponding problem belonging to p-adic algebra.

What, then, would be the p-adic analog to Hilbert's 17th problem?

Instead of positive definite functions it seems natural to consider, in the p-adic case, the *p-integral definite functions*. Let $\mathbb{Z}_p$ denote the ring of p-integers in $\mathbb{Q}_p$; it can also be described as the p-adic completion of $\mathbb{Z}$. A rational function

$$f(X_1, \ldots, X_n) \in \mathbb{Q}_p(X_1, \ldots, X_n)$$

is called *p-integral definite* if

$$f(a_1, \ldots, a_n) \in \mathbb{Z}_p$$

for all $a_1, \ldots, a_n \in \mathbb{Q}_p$, provided $f(a_1, \ldots, a_n)$ is defined which means that $a_1, \ldots, a_n$ is not a zero of the denominator of f. (By continuity, it suffices that $f(a_1, \ldots, a_n) \in \mathbb{Z}_p$ on some Zariski-open subset of $\mathbb{Q}_p^n$.)

Problem: To describe all p-integral definite rational functions $f \in \mathbb{Q}_p(X_1, \ldots, X_n)$. Let us call this the Problem $(17)_{\mathrm{p}}$*—it is the p-adic analog to Hilbert's* 17th *problem.*

In the real case, positive definite functions are sums of squares. In the p-adic case, the square operator x^2 has to be replaced by some other operator $\gamma_p(x)$

which is adapted to p-adic theory. Kochen [Ko1] has found such an operator, which in p-adic algebra plays a similar role as does the square operator in real algebra:

$$\gamma_p(x) = \frac{1}{p}\left(\wp(x) - \frac{1}{\wp(x)}\right)^{-1}$$

with $\wp(x) = x^p - x$ the Artin-Schreier operator. This operator looks somewhat complicated; no wonder that the development of p-adic algebra was delayed. Merckel in his thesis [Me] gave a detailed study of those rational functions $\eta(x) \in \mathbb{Q}_p(x)$ which may serve, in p-adic algebra, in the same way as does $\gamma_p(x)$. It is clear that $\eta(x)$ cannot be a polynomial because polynomials have a p-adic pole (at infinity) and hence cannot be p-integral definite. Merckel has found certain admissible functions $\eta(x)$ of smaller denominator degree than $\gamma_p(x)$, but it seems that $\gamma_p(x)$ is the most "natural" operator. In the following we write $\gamma(x)$ instead of $\gamma_p(x)$, since p remains fixed in the discussion. $\gamma(x)$ is called the *p-adic Kochen operator.*

It is easily verified that $\gamma(x)$ is p-integral definite, i.e. $\gamma(a) \in \mathbb{Z}_p$ for every $a \in \mathbb{Q}_p$. Consequently, for arbitrary

$$g = g(X_1, \ldots, X_n) \in \mathbb{Q}_p(X_1, \ldots, X_n)$$

the function

$$\gamma(g) \in \mathbb{Q}_p(X_1, \ldots, X_n)$$

is p-integral definite too. Hence so is every expression of the form

$$\Phi(\gamma(g_1), \ldots, \gamma(g_r))$$

where $\Phi(Y_1, \ldots, Y_r)$ is a polynomial over $\mathbb{Z}$ and

$$g_1, \ldots, g_r \in \mathbb{Q}_p(X_1, \ldots, X_n).$$

Note that

$$1 + p \cdot \Phi(\gamma(g_1), \ldots, \gamma(g_r))$$

assumes values in $1 + p\mathbb{Z}_p$; these values are *units* in $\mathbb{Z}_p$. It follows that every rational function of the form

$$f = \frac{\Psi(\gamma(g_1), \ldots, \gamma(g_r))}{1 + p\Phi(\gamma(g_1), \ldots, \gamma(g_r))} \tag{F}$$

is p-integral definite, Φ and Ψ being arbitrary polynomials in $\mathbb{Z}[Y_1,\ldots,Y_r]$ (for some $r\in\mathbb{N}$) and $g_1,\ldots,g_r\in\mathbb{Q}_p(X_1,\ldots,X_n)$.

As said above, γ is the p-adic analog of the square operator. The expressions of the form (F) are the p-adic analogs of the "sum of squares" in the real theory.

Now Kochen [Ko1] and the author [Rq1] have proved that *every p-integral definite rational function can be put into the form* (F). This result can be viewed as the p-adic analog of Artin's theorem in the real case.

Its proof is a mere copy of A. Robinson's proof as given in the preceding section, *once* the proper notions and facts of p-adic algebra are established. These are as follows (for the proofs we refer e.g. to [PRq]).

Let K be a field. K is called *p-adic* if $\frac{1}{p}$ cannot be written in the form (F) with $g_1,\ldots,g_r\in K$. (This is the analog of the definition of *real* field: there, -1 cannot be written as a sum of squares). Every p-adic field K admits a maximal algebraic p-adic extension field L; the latter is called a *p-adic closure* of K. If $K=L$ then K is called *p-adically closed*. In a p-adically closed field K the elements of the form $\gamma(g)$ with $g\in K$ form a ring $\mathcal{O}_K$ which is in fact a valuation ring of the field K. The maximal ideal of $\mathcal{O}_K$ is generated by p, and the residue class field $\mathcal{O}_K/p$ is of order p. In general, for arbitrary field K, valuation rings with these two properties are called *p-valuation rings*. K admits a p-valuation ring if and only if K is a p-adic field. (Thus in p-adic theory, the p-valuations are the analogs of the ordering relations in the real theory.) Given any p-valuation ring $\mathcal{O}$ of K there exists a p-adic closure L of K whose canonical p-valuation ring $\mathcal{O}_L=\gamma(L)$ lies above $\mathcal{O}$, i.e. $\mathcal{O}_L\cap K=\mathcal{O}$. If an element $f\in K$ is contained in all p-valuation rings of K then f is called *totally p-integral*. This is the case if and only if f is of the form (F) as explained above. (The last statement is not quite straightforward to prove. It is easy to see that every totally p-integral $f\in K$ is a root of a monic polynomial whose coefficients are of the form (F). In order to show that f itself is actually of the form (F), one has to rely more heavily on commutative algebra; see [Rq1].)

All the above mentioned facts from p-adic algebra are quite analogous to the corresponding facts in real algebra. So is the following

Model Completeness Theorem: Every extension $K\subset L$ of p-adically closed fields is an elementary extension, i.e. the theory of p-adically closed fields is model-complete.

This is the Lefschetz-Tarski principle for p-adically closed fields. Based on this principle, the solution of "Hilbert's problem $(17)_p$" (i.e. the proof of the above mentioned Kochen-Roquette theorem) can be given straightforward, copying A. Robinson's proof of Artin's theorem. This will be left to the reader.

As to the proof of the p-adic model-completeness theorem, it is obtained by a similar pattern as described above in the real case. Firstly, general model theoretic considerations permit the reduction to the following embedding problem: Let $K(x)$ be a rational function field over a p-adically closed field K, and suppose that $K(x)$ is equipped with a p-valuation ring $\mathcal{O}$, i.e. $K(x)$ is

p-valued. *Then $K(x)$ admits a K-isomorphic, valuation-preserving embedding into every sufficiently saturated non-standard model K^* of K.*

Secondly, in order to solve this embedding problem one has to give a description of the possible p-valuations of $K(x)$. It turns out that only two cases are possible:

(1) *Either* $K(x)$ is *ramified* over K, i.e. the value group of $K(x)$ is a proper extension of the value group of K. In this case, after suitable change of the generator x, the value group $v(K(x))$ is generated by $v(x)$ over $v(K)$. (We use v to denote the p-valuation of $K(x)$.) $v(x)$ is of infinite order modulo $v(K)$ and *the given p-valuation of $K(x)$ is uniquely determined by the cut which $v(x)$ determines in the (totally ordered) value group $v(K)$.* Using saturation property, we find $\xi \in K^*$ such that $v(\xi)$ determines the same cut in $v(K)$; hence the substitution $x \mapsto \xi$ yields the desired embedding $K(x) \approx K(\xi) \subset K^*$.

(2) *Or* $K(x)$ is an *immediate* extension of K, i.e. $K(x)$ and K have the same value groups and the same residue fields. In this case we consider the *neighborhood filter* which x determines on K, as follows. For each $c \in K$ consider the distance $v(x-c)$ from c to x; let U_c denote the set of those $a \in K$ which lie in the disc around x with radius $v(x-c)$. These sets U_c then form the neighborhood filter of x on K. It turns out that *the p-valuation of $K(x)$ is uniquely determined by this neighborhood filter.* Using saturation property we can find $\xi \in K^*$ which determines the same neighborhood filter on K; hence the substitution $x \mapsto \xi$ yields the desired embedding $K(x) \approx K(\xi) \subset K^*$.

Let us add some more words about the problem $(17)_p$. Its solution, as stated above, says that every p-integral definite function is representable in the form (F). A glance at (F) will convince the reader that this kind of representation looks much more involved than the corresponding "sum of squares"-representation in the real case. Hence one would like to have more information about (F). There is an effective bound for the number r of g_i's and for the degrees of their numerators and denominators, the bound depending on the degrees of numerator and denominator of f (and of course on the number n of variables). The existence of such effective bound follows from general principles of model theory. No explicit form for this bound has yet been obtained; probably it would be of no great value for use in computations. In the real case Pfister [Pf] has shown that for n variables, any sum of squares is already the sum of 2^n squares. Is there a corresponding result for the p-adics, giving a bound for r in terms of the number of variables only? This is not known. While in the real case the theory of quadratic forms is available for the study of "sums of squares", no equivalent in the p-adics is known to investigate the structure of the Kochen operator. The only structure theorem known in this direction is the *principal ideal theorem* [Rq2] which says that the ring of elements of the form (F) is in fact a *Bezout ring*: every finitely generated ideal is principal. We have already mentioned Merckel's thesis [Me] searching for simpler operators $\eta(x)$ which can replace $\gamma(x)$. Perhaps this search should be extended to operators $\eta(x_1, \ldots, x_s)$ of several variables, and also to finite or infinite systems $\eta_1, \eta_2, \ldots$ which simultaneously can replace

$\gamma(x)$. We also mention the thesis by J. Unruh [Un] who investigated systematically whether the g_i in (F) can be restricted to a proper subset $E \subset \mathbb{Q}_p(X_1, \ldots, X_n)$, such that the validity of the main theorem is preserved. Such a set E must necessarily be infinite. More precisely, there must be infinitely many irreducible polynomials appearing in the numerator of elements of E, or likewise in the denominators of elements in E (if $n \geqq 2$). Many similar results in [Un] show that such admissible E is fairly big; nevertheless it is possible to construct admissible E which are considerably smaller than the whole $K(X_1, \ldots, X_n)$. Here again, the situation is not yet fully clear.

Perhaps it is more suitable to investigate the problem from the *multiplicative* point of view; this would amount to the study of the *unit group* of the Kochen ring. (For quadratic forms, the multiplicative theory had led to Pfister's result mentioned above.) The above remarks have been inserted to point out that the p-adic Kochen operator is not yet fully understood and that more research in this direction would be desirable.

We have arranged the above discussion of p-adic algebra such as to match the foregoing discussion of real algebra. In particular, our discussion was focused around the proof of "Hilbert's problem $(17)_p$", the p-adic analog of the Hilbert problem 17 in the proper sense. We should mention, however, that historically the "problem $(17)_p$" did not play any role in the development of p-adic algebra. This problem $(17)_p$ was stated by Kochen [Ko1] only *after* p-adic algebra had been properly formulated. Independent of special problems to be solved, the formulation of p-adic algebra was given in full recognition of the fact that real algebra should have a counterpart in the p-adics. This recognition came about as a fall out from the work of Ax-Kochen on another prominent problem, namely Artin's conjecture about the C_2-property of $\mathbb{Q}_p$. (See also section 7.)

The model completeness theorem has been used for various other applications. For instance: the p-adic *Nullstellensatz*, the question about p-adic rational points in algebraic geometry, p-adic places and holomorphy rings in p-adic function fields etc. For details we refer e.g. to [PRq].

Let us explicitly state the *axioms for p-adically closed fields:*

(1) the field axioms;

(2) the elements of the form $\gamma_p(a)$ form a p-valuation ring $\mathcal{O}$ of the field;

$(3)_n$ Hensel's lemma with respect to $\mathcal{O}$, for polynomials of degree n.

Note that $(3)_n$ are infinitely many axioms; one for each $n = 1, 2, 3, \ldots$ Axioms $(3)_n$ express the fact that a p-adically closed field K is *Henselian* with respect to its canonical valuation. But the Henselian property does *not* yet suffice to characterize p-adically closed fields. There is another set of axioms which express the fact that the value group $v(K)$ is a $\mathbb{Z}$-group. Recall that a totally ordered abelian group Γ is called a $\mathbb{Z}$-group if it is elementary equivalent to $\mathbb{Z}$. This means that Γ contains a smallest positive element ε and for each n, the factor group Γ/n has exactly n cosets, represented by $0, \varepsilon, 2\varepsilon, \ldots, (n-1)\varepsilon$. In the case of a p-valued field K with valuation ring $\mathcal{O}$, the value group is isomorphic to the multiplicative group $K^{\times}$ modulo the units $\mathcal{O}^{\times}$. Its smallest positive element is the value of p. This gives rise to the following set of axioms:

$(4)_n$ Every field element a can be written in the form

$$a = p^i b^n u$$

for some $i = 0, 1, \ldots, n-1$, where b is a field element and u is a unit in the valuation ring $\mathcal{O}$.

A field is p-adically closed if and only if it satisfies the above axioms. The theory of p-adically closed fields is complete [PRq], and hence *the above axioms describe the algebraic theory of the Hensel field* $\mathbb{Q}_p$.

So again the situation is quite analogous to the situation in case of real algebra.

In number theory, not only the fields $\mathbb{Q}_p$ are of interest but also their finite extensions. These can be dealt with in the same way; the results are quite similar, the differences to the case of $\mathbb{Q}_p$ are of technical nature only. See [PRq].

6 Elimination of Quantifiers

Let T be a theory and $\varphi(x_1, \ldots, x_n)$ a formula in the language of T, where $x_1, \ldots, x_n$ are free parameters in $\mathcal{L}$. Given a model K of T and $a_1, \ldots, a_n \in K$ we want to know whether $\varphi(a_1, \ldots, a_n)$ holds in K. Usually a mathematician will ask for a necessary and sufficient criterion $\psi(x_1, \ldots, x_n)$, i.e. $\varphi(a_1, \ldots, a_n)$ holds in K if and only if $\psi(a_1, \ldots, a_n)$ does. $\psi(x_1, \ldots, x_n)$ should also be a formula in $\mathcal{L}$ and it should be independent of K, i.e. the criterion should hold in every model of T. If the criterion is to be of interest then $\psi(x_1, \ldots, x_n)$ should be somehow "simpler" than $\varphi(x_1, \ldots, x_n)$. If possible then $\psi(x_1, \ldots, x_n)$ *should be free of quantifiers*, so that $\psi(a_1, \ldots, a_n)$ can be checked directly by looking at $a_1, \ldots, a_n$ and the algebraic relations between them, without referring to the whole structure K.

The classical example of such problem is *elimination theory* in the theory of algebraically closed fields, formulated within the language of fields. In its simplest case, we are given two homogeneous forms $f(X, Y)$, $g(X, Y)$ in two variables. The resultant $R(f, g)$ is a certain polynomial in the coefficients of f and g. The vanishing of the resultant: $R(f, g) = 0$, is a quantifier-free criterion for the existence of a non-trivial common zero in an algebraically closed field. The parameters of the general set-up are here the coefficients of $f(X, Y)$ and $g(X, Y)$.

An arbitrary theory T is said to admit *quantifier elimination* in the language $\mathcal{L}$, if every formula $\varphi(x_1, \ldots, x_n)$ in $\mathcal{L}$ is T-equivalent, in the sense as explained above, to a quantifier-free formula $\psi(x_1, \ldots, x_n)$ in $\mathcal{L}$.

General model theory provides us with a very useful condition for the existence of quantifier elimination. Namely, a theory T admits elimination of quantifiers in the language $\mathscr{L}$ if and only if *every two models L_1, L_2 of T are substructure equivalent* in the following sense: If K is a common substructure, $K \subset L_1$ and $K \subset L_2$, then L_1 and L_2 should be elementary equivalent over K. This means that L_1 and L_2 satisfy the same sentences in $\mathscr{L}_K$, the language $\mathscr{L}$ augmented by constants to denote the elements of K. Note that in this condition, K need not be a model of T; the axioms of T need not be satisfied in K. The only requirement is that K is a substructure of L_1 and of L_2 with respect to all the relations and functions belonging to the vocabulary of the language $\mathscr{L}$.

For instance, consider the theory of algebraically closed fields within the language of fields. To check the above condition, consider two algebraically closed fields L_1 and L_2 which contain a common subfield*) K, not necessarily algebraically closed. But then L_1, L_2 each contain an algebraic closure $\tilde{K}_1$ resp. $\tilde{K}_2$ of K. By Steinitz' theory it follows that any two algebraic closures of K are K-isomorphic: $\tilde{K}_1 \underset{K}{\approx} \tilde{K}_2$. After identifying $\tilde{K}_1 = \tilde{K}_2 = \tilde{K}$, both L_1 and L_2 now appear as extensions of the algebraically closed field $\tilde{K}$. By model completeness: $\tilde{K} \prec L_1$, $\tilde{K} \prec L_2$, hence L_1 and L_2 are elementary equivalent over $\tilde{K}$ and *a fortiori* over K. *We conclude that the theory of algebraically closed fields admits elimination of quantifiers.*

This has been first proved by Tarski [TM], and today it constitutes one of the prominent class-room examples for quantifier elimination. It explains why one has to expect a condition of the type of the resultant: $R(f, g) = 0$, for the existence of common non-trivial zeros of f and g. But of course the explicit form of the resultant as given in algebra textbooks will *not* come out of such general considerations. In each special case, the explicit form of the quantifier-free ψ equivalent to φ is to be the object of detailed investigation.

The theory of real closed fields admits elimination of quantifiers in the language of ordered fields. The ordinary language of fields does not suffice in this case. This is clearly seen by testing the above criterion of substructure equivalence: L_1 and L_2 are now real closed fields, containing the subfield K. Hence they contain real closures $\tilde{K}_1, \tilde{K}_2$ respectively, of K. Now if we work in the language of ordered fields then K is an *ordered* subfield of L_1 and L_2; this means that L_1 and L_2 induce the same ordering in K. It follows that $\tilde{K}_1$ and $\tilde{K}_2$ are real closures *with respect to the same ordering* of K. Hence by Artin-Schreier [AS] they are K-isomorphic. The rest of proof can proceed in the same way as in the case of algebraically closed fields, this time using model-completeness for the theory of real closed fields. On the other hand, if we work in the language of fields then K is just a subfield of L_1 and of L_2. The orderings of K induced by L_1, L_2 may be

*) A substructure of a field is an integral domain (provided the vocabulary of field theory is taken to be the same as for ring theory, with no specific symbol for division). Now if a field L contains an integral domain D then L contains, canonically, the quotient field K of D.

distinct and, in that case, $\tilde{K}_1$ and $\tilde{K}_2$ are *not* K-isomorphic. The proof breaks down and, in fact, we have counterexamples showing that there are models of the theory which are *not* substructure-equivalent.

The most prominent example for elimination of quantifiers in real algebra is given by *Sturm's theorem*. For given n, consider monic polynomials $f(X)$ of degree n. Sturm's theorem gives a quantifier free criterion for $f(X)$ to admit a root ϑ in a given interval $a \leqq \vartheta \leqq b$. (The parameters in this problem are the coefficients of f and the end points of the interval.) The Sturm criterion is formulated in the language of *ordered* fields; it is *not* possible to formulate it without quantifiers in the theory of fields only, in the absence of the relation symbol $\leqq$. (Of course, every inequality $x \leqq y$ may be replaced in real closed fields by $(\exists z)(y - x = z^2)$. But the latter formula contains an existential quantifier.)

According to Tarski, the elimination of quantifiers for the algebraic theory of $\mathbb{R}$ implies elimination of quantifiers for Euclidean geometry. Was this what Steinitz had in mind when he announced applications of his algebra to geometry? Most probably we shall never know.

Now let us discuss elimination of quantifiers in p-adic algebra. Due to our experience in real algebra, we work p-adically in the *language of valued fields*, not just in the language of fields. But even in the language of valued fields, elimination of quantifiers does *not* hold for the theory of p-adically closed fields. For if we try to verify the condition of substructure equivalence in the same manner as in the above two cases, then we arrive at the following problem: Let K be a p-valued field and consider the p-adic closures $\tilde{K}$ whose canonical p-valuation induces the given valuation in K. Are all such p-adic closures K-isomorphic? (As it is the case in the corresponding problem for real closures.) The answer is: *No*, there are counterexamples. This implies that quantifier elimination fails.

In view of this situation there arises the problem of classification of the various p-adic closures $\tilde{K}$ of a p-valued field K. It is no restriction to assume K to be Henselian, for in any case, the Henselization K^h of K is contained in $\tilde{K}$. Now the classification problem for $\tilde{K}$ leads to certain invariants of cohomological nature which, as it turns out, can be explicitly identified. There are infinitely many, in fact uncountably many non-isomorphic p-adic closures $\tilde{K}$ of K (except in the trivial case when K itself is already p-adically closed). In any case, it can be proved that *every p-adic closure $\tilde{K}$ can be obtained from K by the adjunction of radicals* [PRq]. (An n-th radical ϑ over K is the form $\vartheta = \sqrt[n]{a}$ with $a \in K$; in other words, ϑ is the root of the binomial $X^n - a$.) As a consequence, *it can be shown* [PRq] *that two p-adic closures $\tilde{K}_1$, $\tilde{K}_2$ of a p-valued field K are isomorphic if and only if*

$$\tilde{K}_1^n \cap K = \tilde{K}_2^n \cap K$$

for each $n = 1, 2, \ldots$ Here, $\tilde{K}_1^n$ denotes the set of n-th powers of elements in $\tilde{K}_1$;

hence $\tilde{K}_1^n \cap K$ is the set of those elements $a \in K$ which admit n-th radicals $\sqrt[n]{a}$ in $\tilde{K}_1$. (Similarly for $\tilde{K}_2^n \cap K$.)

The above results imply that elimination of quantifiers can be achieved, also in the p-adic case, in a certain extended language. Let us extend the language of valued fields by adjoining predicate symbols $P_1, P_2, P_3, \ldots$ In p-adically closed fields $P_n(x)$ it to be interpreted as x being an n-th power. Now if L is p-adically closed and K is a *substructure of L with respect to this extended language*, then:

(1) K is a subfield of L,

(2) K carries a valuation ring $\mathcal{O}$ which is induced by the canonical valuation ring $\mathcal{O}_L$, i.e. $\mathcal{O} = K \cap \mathcal{O}_L$.

(3) For each n, K carries a certain distinguished subset $P_n(K)$ which is induced by the set of n-th powers of L, i.e. $P_n(K) = K \cap L^n$.

Consequently, if K is a substructure (in the extended sense) of two p-adically closed fields L_1 and L_2 then $K \cap L_1^n = K \cap L_2^n$. If $L_1 = \tilde{K}_1$ and $L_2 = \tilde{K}_2$ are p-adic closures of K we conclude from the above theorem that $\tilde{K}_1$ and $\tilde{K}_2$ are isomorphic. Consequently, if we work in the extended language then we can argue in the same way as in the real closed case or in the algebraically closed case. Hence, any two p-adically closed fields are substructure equivalent with respect to the extended language. Hence, *the theory of p-adically closed fields admits quantifier elimination in the extended language.*

According to our above definition, the "extended language" is obtained from the language of valued fields by adjunction of the new predicate symbols $P_1, P_2, \ldots$ It can be shown that *the above result remains valid if we start from the language of fields, not valued fields.*

It would be interesting to know explicitly *the p-adic analog of Sturm's theorem*, giving a criterion for a monic polynomials $f(X)$ to have a p-integral root. This criterion should be quantifier-free in the extended language. In other words: the criterion should be expressible in the language $\mathcal{L}$ of fields, with quantifiers permitted in the form $(\exists y)(x = y^n)$ only, where x is a term. No such p-adic analog of Sturm's theorem is known, except in special cases when the polynomial satisfies in addition the conditions of Hensel's lemma (or of related lemmas).

Elimination of quantifiers in the extended language has been discovered by Macintyre [Ma]. As a consequence he proved that every infinite, definable subset of $\mathbb{Q}_p^n$ (the n-dimensional vector space over $\mathbb{Q}_p$) has a non-empty interior. For real closed fields, this was known before, in view of Tarski's elimination of quantifier theorem.

Another interesting application of elimination of quantifiers in the algebraic theory of $\mathbb{Q}_p$, has recently been given by J. Denef [Den]. The problem was to prove the rationality of the Poincaré series associated to the p-adic points of a variety, and of related series. In the course of proof a certain integral has to be evaluated over a certain subset D of $\mathbb{Z}_p^n$; this subset is definable and can be shown (by quantifier elimination) to be a Boolean combination of rather simple sets, for which the corresponding integral can indeed be evaluated, giving the desired information.

Quantifier elimination in the extended language can be carried over *mutatis mutandis* to finite extensions of $\mathbb{Q}_p$. See [PRq].

7 Diophantine Problems and Valued Fields

We have seen above that the theory of p-adically closed fields is complete, and that it admits a recursive set of axioms. Consequently, it follows that the theory is *decidable*. That is, there exists an effective procedure to determine for each sentence φ in the language of valued fields, whether φ does or does not hold in all p-adically closed fields. By completeness, this is equivalent to saying that φ holds (resp. does not hold) in $\mathbb{Q}_p$.

Now let V be an affine variety in n-space, given by polynomial equations of the form

$$f_1(x_1,\ldots,x_n)=0,\ldots,f_r(x_1,\ldots,x_n)=0. \tag{D}$$

We assume that the coefficients of these polynomials are integers in $\mathbb{Z}$. The *Diophantine problem* in $\mathbb{Z}$ asks whether (D) has a solution in integers $x_1,\ldots,x_n\in\mathbb{Z}$, i.e. whether V as a $\mathbb{Z}$-rational point. The corresponding problem for $x_1,\ldots,x_n\in\mathbb{Z}_p$ is *decidable*, by what we have said above. It has been shown by Weispfenning [We1] that the decision procedure can be made to be *uniform* in p, in a certain sense. This implies that *it is decidable whether the Diophantine problem* (*D*) *has a solution everywhere locally* or, in other words, whether there is a solution $x_1,\ldots,x_n$ whose coordinates are contained in the adele ring $A(\mathbb{Z}) = \prod_p \mathbb{Z}_p$ (direct product).

Now if we knew that the variety V satisfies Hasse's *local-global principle* (for integer points) then we could conclude that the original Diophantine problem (D) over $\mathbb{Z}$ is decidable. However, varieties with local-global principle are very rare. It has been shown by Julia Robinson and Matijasevic [DMR] that the *general* Diophantine problem (D) over $\mathbb{Z}$ is in fact *not* decidable. There does *not* exist an effective algorithm which permits for every system of equations of the form (D), to decide whether there is a solution $x_1,\ldots,x_n\in\mathbb{Z}$.

The situation does not improve if we replace $\mathbb{Q}$ by an algebraic number field K of finite degree and, accordingly, $\mathbb{Z}$ by the ring of algebraic integers of K. But we may go to the limit, arriving at the algebraic closure $\mathbb{Q}^a$ of $\mathbb{Q}$, the field of all algebraic numbers, and correspondingly at the integral closure $\mathbb{Z}^a$ of $\mathbb{Z}$, the ring of all algebraic integers. Does there exist a decision procedure for solutions of (D) with $x_1, \ldots, x_n \in \mathbb{Z}^a$? In other words: can Hilbert's 10th problem be positively solved for $\mathbb{Z}^a$ instead of $\mathbb{Z}$?

The conjecture that this may perhaps be the case had been voiced by Skolem [Sk]. He said that by general mathematical experience, many algebraic problems become decidable if one considers structures satisfying *closure properties* which are connected with the particular problem. This rather vague heuristic principle can be made precise, as we have seen, with respect to *algebraic closure*, *real closure*, *p-adic closure*. These closure properties render the respective theories decidable. Skolem's question is whether the algebraic theory of $\mathbb{Q}^a$, with distinguished subring $\mathbb{Z}^a$, is decidable? The proper language for this theory would be the theory of fields augmented by one predicate symbol to identify the elements in $\mathbb{Z}^a$.

The answer to the above general Skolem question is not yet known. However one may restrict this question and ask for the decidability at least of the Diophantine problems of the form (D), with solutions $x_1, \ldots, x_n \in \mathbb{Z}^a$.

This restricted question has recently been answered affirmatively by Rumely in a yet unpublished paper [Ru], based on former work by D. Cantor and the author [CRq]. The main point is *the local-global principle for Diophantine problems of the form* (D). This means the following: let $\mathbb{Q}_p^a$ denote the algebraic closure of $\mathbb{Q}_p$ and $\mathbb{Z}_p^a$ the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p^a$. Then $\mathbb{Z}_p^a$ is called the ring of algebraic p-adic integers. Now the local-global principle can be stated as follows: *If for each p, the Diophantine problem* (D) *admits a solution in* $\mathbb{Z}_p^a$ *then* (D) *admits solution* $x_1, \ldots, x_n \in \mathbb{Z}^a$.

In [CRq] this has been proved in the case when the variety V is unirational, i.e. parametrizable via rational functions. (More precisely, [CRq] covers the problem for *simple* points on unirational varieties.) The generalization to arbitrary varieties has been announced by Rumely, based on a detailed study of local heights on algebraic curves of higher genus.

In the course of proof of this local-global principle it turns out that for given V, only *finitely many* prime numbers are critical, in the sense that for the other primes the existence of a local solution in $\mathbb{Z}_p^a$ can easily be ascertained by general theorems. Consequently, the decision problem for global solutions is reduced to the local decision problem for a finite set of primes given in advance; by induction this is reduced to one single prime.

Now we recall that $\mathbb{Q}_p^a$ is an *algebraically closed field*, and $\mathbb{Z}_p^a$ is a *valuation ring* of $\mathbb{Q}_p^a$. We see that in the local case, we are studying *algebraically closed valued fields*. In this situation there is an old theorem of A. Robinson, saying that *the theory of algebraically closed valued fields is model-complete*, with respect to the language of valued fields. (It is understood that the valuation is non-trivial.) This, together with the fact that the axioms of algebraically closed fields are recursively enumerable, shows that *the algebraic theory of* $\mathbb{Q}_p^a$, *valued by* $\mathbb{Z}_p^a$, *is decidable*. In this respect we have for $\mathbb{Q}_p^a$, $\mathbb{Z}_p^a$ the same situation as described above for $\mathbb{Q}_p$, $\mathbb{Z}_p$.

In particular we see that, indeed, Diophantine problems (D) over $\mathbb{Z}^a$ are decidable.

Besides of its application to Diophantine problems over $\mathbb{Z}^a$, the theorem of A. Robinson is of importance also on its own. It admits a *classification of algebraically closed valued fields, up to elementary equivalence*, by two invariants: the characteristic p_1 of the field and the characteristic p_2 of the residue field.

For given invariants p_1, p_2 there exists a *prime model*, i.e. an algebraically closed valued field with invariants p_1, p_2 which is isomorphically contained in *every* algebraically closed valued field with the same invariants. If $p_1 = 0, p_2 = p > 0$ then the prime model is $\mathbb{Q}^a$, the field of algebraic numbers, equipped with a valuation extending the p-adic valuation of $\mathbb{Q}$. (It does not matter which extension is chosen because all such extensions are conjugate over $\mathbb{Q}$.) If $p_1 = p_2 = 0$ then the prime model is $\mathbb{Q}(x)^a$, the field of algebraic functions, equipped with any valuation over $\mathbb{Q}$ (it does not matter which). Similarly, if $p_1 = p_2 = p > 0$ then the prime model is $\mathbb{F}_p(x)^a$ with any valuation ($\mathbb{F}_p$ denoting the field with p elements). By general model theory, the existence of prime models together with model-completeness implies completeness. Hence the theory of algebraically closed valued fields with given invariants (p_1, p_2) is complete.

By the way, the theory of algebraically closed valued fields admits *elimination of quantifiers*, because any two models are substructure-equivalent. Indeed, if K is a valued field contained in two algebraically closed valued fields L_1 and L_2 then the algebraic closure K^a, as a field, is isomorphically contained in both L_1 and L_2. The valuations of K^a induced by L_1 and by L_2 are both extensions of the given valuation of K. Hence they are *conjugate* over K. Hence after applying a suitable K-isomorphism we may assume that both L_1 and L_2 induce in K^a the same valuation. By model-completeness, L_1 and L_2 are now elementary equivalent over K^a, hence a priori over K. So the argument is completely analogous to the corresponding argument in the case of p-adically closed fields, or real closed fields, or algebraically closed fields. Model theory provides the proper framework for questions of this kind.

A. Robinson published his theorem about algebraically closed valued fields already in the year 1956 [Ro 1]. But it seems that it did not become widely known among algebraists, at least not as much as it would deserve in view of its importance. This is somewhat curious because algebraic geometry over *valued* fields has been quite well recognized as an important object of study, via Hensel's p-adic theory.

There have been several generalizations of Robinson's above theorem, concerning valued fields which are not algebraically closed. The first motivation came from the work of Ersov [Er 1], Ax and Kochen [AK] about Artin's conjecture on the C_2-property of $\mathbb{Q}_p$. Let us briefly discuss the model theoretic framework of the problem, without going into the detail about the content of the C_2-property.

Let φ be a sentence in the language of valued fields, and suppose we want to know whether φ holds in the fields $\mathbb{Q}_p$. If the problem is difficult then we may first try the power series fields $\mathbb{F}_p((x))$ in one variable x over the finite field $\mathbb{F}_p$ with p elements. $\mathbb{F}_p((x))$ is a complete valued field with the same residue field as $\mathbb{Q}_p$ (viz. $\mathbb{F}_p$) and the same value group (viz. $\mathbb{Z}$). Mathematical experience shows that often (though not always) the field $\mathbb{F}_p((x))$ is easier to investigate than $\mathbb{Q}_p$. Suppose then that we have found that φ holds in $\mathbb{F}_p((x))$, for all prime numbers p. Can we infer from this that φ holds in every $\mathbb{Q}_p$?

Consider the ultraproduct $K = \prod\limits_p \mathbb{F}_p((x))/\mathscr{D}$ of the fields $\mathbb{F}_p((x))$ *modulo a non-principal ultrafilter* $\mathscr{D}$ *on the set of all prime numbers p.* This ultraproduct is a valued field, and the algebraic properties of K are precisely those which hold in $\mathscr{D}$-almost all factors $\mathbb{F}_p((x))$. (That is, there should exist a set D of the ultrafilter such that the property holds in $\mathbb{F}_p((x))$ for all $p \in D$.) In particular, φ holds in K. We now compare K with the corresponding ultraproduct of p-adic fields: $K' = \prod\limits_p \mathbb{Q}_p/\mathscr{D}$. We note that K, K' both have the same residue field, namely $\prod\limits_p \mathbb{F}_p/\mathscr{D}$, which is of characteristic zero. Also, they have the same value group, namely $\prod\limits_p \mathbb{Z}/\mathscr{D}$; this is an ultrapower of $\mathbb{Z}$ and hence elementary equivalent to $\mathbb{Z}$. Both K and K' are Henselian. This is because the Henselian property can be described by (infinitely many) sentences in the language of valued fields; since each factor $\mathbb{F}_p((x))$ resp. $\mathbb{Q}_p$ is Henselian it follows that K and K' are indeed Henselian. From the above it follows that K, K' are elementary equivalent via the following

Theorem of Ersov [Er1]. *Consider two Henselian valued fields K, K' whose residue fields are of characteristic* 0. *If the residue fields of K and K' are elementary equivalent in the language of ordered groups, then K and K' are elementary equivalent in the language of valued fields.*

It follows that φ holds in K', hence φ holds for $\mathbb{Q}_p$ if p belongs to a certain set D of the ultrafilter $\mathscr{D}$. Since $\mathscr{D}$ is an *arbitrary* non-principal ultrafilter on the set of primes we conclude: φ holds in almost all $\mathbb{Q}_p$ (i.e. all but for a finite number of primes p). Consequently, by means of Ersov's theorem we have obtained the following important *transfer principle: If φ holds in almost all power series fields $\mathbb{F}_p((x))$ then φ holds in almost all $\mathbb{Q}^p$, and vice versa.*

This transfer principle applies to all sentences φ in the language of valued fields, not just to those sentences which make up the C_2-property.

Note that Ersov's theorem contains Robinson's completeness theorem in case of residue characteristic 0. For if K, K' are algebraically closed valued fields then their residue field $\bar{K}, \overline{K'}$ are algebraically closed too; by the Lefschetz principle it follows that $\bar{K}, \overline{K'}$ are elementary equivalent. Moreover, their value groups $v(K)$ and $v(K')$ are *divisible*. It is known that all divisible, totally ordered abelian groups are elementary equivalent. Thus indeed, Ersov's theorem shows that K, K' are elementary equivalent. Hence Robinson's completeness theorem.

There arises the question whether Ersov's theorem can be generalized to the case of residue characteristic $p > 0$. This is true if the following additional condition is satisfied: K is of characteristic 0 and is absolutely unramified, i.e. the value $v(p)$ is the smallest positive element in the value group. In addition, the residue field is to be perfect. It is clear that this result includes e.g. the completeness theorem for p-adically closed fields.

If K too is of characteristic $p > 0$ then the Henselian property of K is not sufficient in this context. Itn seems natural to replace it by the property of K to be *immediately closed* This means that K (as a valued field) should not admit any proper algebraic immediate extension. Every immediately closed field is Henselian, but not conversely.

Ersov's theorem now holds for $\operatorname{char}(K) = p > 0$, if K is *immediately closed* and, moreover, K satisfies the so-called Kaplansky hypothesis (A). This means, firstly, that the residue field $\bar{K}$ does not admit any algebraic extension of finite degree divisible by p; equivalently, every additive polynomial with coefficients in $\bar{K}$ should have a root in $\bar{K}$. Secondly, the value group $v(K)$ should not admit, in its divisible hull, any extension of finite degree divisible by p; equivalently, every equation $p\xi = \alpha$ with $\alpha \in v(K)$ should have a solution $\xi \in v(K)$. See [Ka], [Wh].

The above generalizations of what we called Ersov's theorem have also been proved by Ersov himself [Er1], and independently by Ax-Kochen [AK].

Kaplansky's hypothesis (A) does not seem unnatural in this context, but many fields appearing in mathematical nature do *not* satisfy it. Some effort has been spent to investigate other cases where hypothesis (A) does not apply. See e.g. Delon [Del]. Pank [Pa] has studied the Galois theoretic interpretation of hypothesis (A). Kuhlmann [Ku] has studied Hensel fields where hypothesis (A) is *not* satisfied. But the results obtained so far are not yet conclusive.

There have been generalizations of the theorems of Ersov and Ax-Kochen. An extensive literature is centered around it. A thorough and quite general study has been made by Basarab [Bas]. See also Transier [Tr].

8 Concluding Remarks

As pointed out already, our report is not meant to be comprehensive. There are many more instances where the intrusion of model theoretic concepts and methods into algebra could have been demonstrated. The reader may consult the papers of our list of references, or the literature cited in those papers. Here it was our purpose to get the reader interested in this new kind of algebraic reasoning. But perhaps we should avoid the word "new" in this context because as we have seen the roots of model theory can be traced right back to the beginning of "Modern Algebra" (in the sense of van der Waerden's book [vdW]). In fact, *model theory is naturally and inherently an offspring of the axiomatic viewpoint of contemporary mathematics*. So when today we observe model theory playing an important role in algebra, then this is not surprising and not exactly new. But now mathematicians are becoming more and more conscious about the *close connection between mathematical structures and the formal language $\mathscr{L}$ which is used to describe those structures.*

Of course there is no inherent reason why to restrict the language to be elementary (or first order), as we did in this article. For even when the axioms can be stated in an elementary language (as is the case for most algebraic theories) then one may be interested in properties which are of higher order. For instance in ring theory, the property of a ring to be *Noetherian* cannot be expressed in the elementary language of ring theory. In the theory of valued fields, *topological properties* are in general not of elementary nature. Hence if one wants to include such properties into the investigation then one has to work with higher order languages, adapted to the specific purpose.

A beautiful example in this direction is the work of Prestel and Ziegler [PrZ] about the so-called *local theory of topological fields*. In this theory, the language $\mathscr{L}$ contains (besides of the ordinary vocabulary of field theory) a set of additional variables U to denote neighborhoods of 0. Accordingly, the language contains a relation symbol $t \in U$ to denote that t belongs to U; here t may be any term in the language of fields. A sentence φ in this language is called *local* if, for every topological field K in which φ holds, φ remains true if the range of the set variables is restricted to a *basis* of neighborhoods around 0. Similarly if φ does not hold in K then it is required that φ remains false if the range of the set variables is restricted to a *basis* around 0. For instance the Hausdorff axiom is local in this sense: it requires that for $a \neq b$ there exist neighborhoods U, V such that $(a+U) \cap (b+V) = \emptyset$; clearly this can be expressed in the above language $\mathscr{L}$ and, if it holds in K then it also holds if U, V are restricted to a basis, and conversely. By inspection one verifies that all the axioms of topological fields, if stated in terms of neighborhoods around 0, are local.

The above definition of local sentences is semantic; they can also be defined syntactically: see [PrZ].

Two topological fields are called *locally equivalent if they satisfy the same local sentences.*

Now it is shown in [PrZ] that *the complex number field $\mathbb{C}$ is locally equivalent to each $\mathbb{Q}_p^a$, the algebraic closure of the p-adic Hensel field $\mathbb{Q}_p$.* In fact: all algebraically closed topological fields of characteristic 0 are locally equivalent, provided the topology is Hausdorff and non-discrete. This is a "*Lefschetz principle*" *for topological algebraically closed fields.* It seems remarkable that the field $\mathbb{C}$ with the ordinary archimedean absolute value, and the fields $\mathbb{Q}_p^a$ with their non-archimedean valuations referring to different primes p, are all equivalent with respect to their local topological properties. In a way this corresponds to the experience gained in developing p-adic analysis. Although the fields $\mathbb{C}$ and $\mathbb{Q}_p^a$ are essentially different as valued fields, experience has shown that they show a similar behavior with respect to *local algebro-topological properties.* Perhaps it will be possible to extend the Prestel-Ziegler result also to local *analytic* properties, if the $\mathbb{Q}_p^a$ are replaced by their completions.

As to the fields $\mathbb{R}$ and $\mathbb{Q}_p$, they are *not* locally equivalent because they are not even elementary equivalent in the language of fields. On the other hand, these fields do share certain local properties, for instance the following: For every n, the monic polynomials in $K[X]$ of degree n which have a *simple* zero in K form an *open set*, in the space of all monic polynomials of degree n. It is shown [PrZ] that this is equivalent to the validity of the *Implicit Function Theorem* (for polynomials) to hold in the field. Every such field is locally equivalent to a topological field L which admits a basis of neighborhoods around 0 consisting of *Henselian valuation ideals* (i. e. maximal ideals of Henselian valuation rings of L). The nice thing about this is, that e. g. the Implicit Function Theorem for $\mathbb{R}$ (resp. for $\mathbb{Q}_p$) can be reduced to the ordinary Hensel's Lemma in such field L. Since the original work by Hensel [He], Rychlik [Ry] and Ostrowski [Os] it has become common knowledge that there is a great similarity between Hensel's lemma and the classical analytic theorem for implicit functions (or continuity of roots etc.). Here too, model theory provides the proper framework to give this experience a precise meaning and, moreover, model theory gives us new ways of mathematical reasoning: e. g. to *deduce* analytic theorems for $\mathbb{R}$ or $\mathbb{C}$ from properties of non-archimedean valued fields.

It is to be hoped that further investigations can provide us with even more detailed information about the similarities in local analytic behavior of the fields $\mathbb{R}$ and $\mathbb{Q}_p$.

References

[AS] Artin, E., O. Schreier, *Algebraische Konstruktion reeller Körper. Über die Zerlegung definiter Funktionen in Quadrate. Eine Kennzeichnung der reell abgeschlossenen Körper.* Hamburger Abhandlungen **5** (1926), 85—231.

[AK] Ax, J., S. Kochen, *Diophantine problems over local fields*, I, II. Amer. J. Math. **87** (1965), 605—648. III. Annals of Math. **83** (1966), 437—456.

[Bar] Barwise, J. (ed.), *Handbook of Mathematical Logic*. North Holland (1978).

[Bas] Basarab, S., *A model theoretic transfer theorem for henselian valued fields*. Crelle's Journal 311/312 (1979), 1—30.

[BeJ] Becker, E., B. Jacob, *Rational points on algebraic varieties over a generalized real closed field*. A model theoretic approach. To appear in Crelle's Journal (1984).

[CRq] Cantor, D., P. Roquette, *On diophantine equations over the ring of all algebraic integers*. Journ. Number Theory **18** (1984), 1—26.

[CK] Chang, C., J. Keisler, *Model Theory*. North Holland (1973).

[Ch] Cherlin, G., *Model theoretic algebra*. Selected topics. Springer Lecture Notes **521** (1976).

[DMR] Davis, M., Yu. Matijasevic, J. Robinson, *Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution*. Proc. Symp. Pure Math. **28** (1976), 223—378.

[Del] Delon, F., *Quelques proprietés des corps values en théorie des modèles*.Thèse, Paris (1981).

[Den] Denef, J., *The rationality of the Poincaré series associated to the p-adic points on a variety* (Second version). Preprint (1983).

[DK] Delfs, H., M. Knebusch, *On the homology of algebraic varieties over real closed fields.* Crelle's Journal **335** (1982), 122—163.

[Dr1] van den Dries, L., *Model theory of fields.* Thesis, Utrecht (1978).

[Dr2] van den Dries, L., *Reducing to prime characteristic, by means of Artin approximation and constructible properties, and applied to Hochster algebras.* Comm. Math. Inst. Utrecht **16** (1983).

[DrR1] van den Dries, L., P. Ribenboim, *Lefschetz principle in Galois theory.* Queen's Math. preprint **5** (1976).

[DrR2] van den Dries, L., P. Ribenboim, *Application de la théorie des modèles aux groupes de Galois de corps de fonctions.* C. R. Acad. Sciences Paris **288** (1979), série A, 789—792.

[Du] Dubois, D., *A Nullstellensatz for ordered fields.* Ark. Math. **8** (1969), 111—114.

[Ek] Eklof, P., *Lefschetz's principle and local functors.* Proc. AMS **37** (1973), 333—339.

[EGH] Erdös, P., L. Gillman, M. Hendrikson, *An isomorphism theorem for real closed fields.* Annals of Math. **61** (1955), 542—554.

[Er1] Ersov, Yu., *On the elementary theory of maximal valued fields* (russian). Algebra i Logika I: **4** (1965), 31—69. II: **5** (1966), 8—40. III: **6** (1967), 31—73.

[Er2] Ersov, Yu., *Decision problems in constructible models* (russian). Moscow (1980) (translation to appear in Springer Verlag).

[He] Hensel, K., *Theorie der Algebraischen Zahlen I.* Teubner Leipzig (1908).

[Ka] Kaplansky, I., *Maximal fields with valuations.* Duke Math. J. **9** (1942), 303—321.

[Ko1] Kochen, S., *Integer valued rational functions over the p-adic numbers.* In: Number Theory, Proc. Symp. Pure Math. XII. Houston (1967), 57—73

[Ko2] Kochen, S., *The model theory of local fields.* In: Logic Conference Kiel (1974), Springer Lecture Notes **499**.

[Kri] Krivine, J. L., *Anneaux préordonnés.* Journ. d'Analyse Math. **12** (1964), 307—326.

[KrN] Krull, W., J. Neukirch, *Die Struktur der absoluten Galoisgruppe über dem Körper $R(t)$.* Math. Annalen **193** (1971), 197—209.

[Ku] Kuhlmann, F. V. (to appear).

[La1] Lang, S., *On quasi algebraic closure.* Annals of Math. **55** (1952), 373—390.

[La2] Lang, S., *The theory of real places.* Annals of Math. **57** (1953), 378—391.

[La3] Lang, S., *Some applications of the local uniformization theorem.* Amer. Journ. Math. **76** (1954), 362—374.

[Le] Lefschetz, S., *Algebraic Geometry.* Princeton (1953).

[Ma] Macintyre, A., *On definable sets of p-adic numbers.* J. Symb. Logic **41** (1976), 605—610.

[MaMD] Macintyre, A., K. McKenna, L. van den Dries, *Elimination of quantifiers in algebraic structures.* Advances in Math. **47** (1983), 74—87.

[Me] Merckel, M., *Darstellung des Ringes der total-p-adisch ganzen Elemente eines formal p-adischen Körpers als ganze Hülle von Quotientenringen von Wertbereichen geeigneter Funktionen.* Dissertation Heidelberg (1978).

[Os] Ostrowski, A., *Untersuchungen zur arithmetischen Theorie der Körper.* Math. Z. **39** (1935), 269—404.

[Pa] Pank, M., *Beiträge zur reinen und angewandten Bewertungstheorie.* Dissertation Heidelberg (1976).

[Pf] Pfister, A., *Zur Darstellung definiter Funktionen als Summe von Quadraten.* Inventiones math. **4** (1967), 229—237.

[Po] Potthoff, K., *Einführung in die Modelltheorie und ihre Anwendungen.* Wiss. Buchges. Darmstadt (1981).

[Pr] Prestel, A., *Model theory of fields. An application to positive definite polynomials over* $\mathbb{R}$. To appear: Mémoirs de la Societé Mathématique de France.

[PRq] Prestel, A., P. Roquette, *Formally p-adic fields.* Springer Lecture Notes 1050 (1984).

[PrZ] Prestel, A., M. Ziegler, *Model theoretic methods in the theory of topological fields.* Crelle's Journal 299/300 (1978), 318—341.

[Ro1] Robinson, A., *Complete theories*. North Holland (1956).

[Ro2] Robinson, A., *On ordered fields and definite functions*. Math. Ann. **130** (1955), 257—271.

[Ro3] Robinson, A., *Solution of a problem by Erdös-Gillman-Henrikson*. Proc. Amer. Math. Soc. **7** (1956), 908—909.

[Ro4] Robinson, A., *Introduction to model theory and the metamathematics of algebra*. North Holland (1963).

[RoG] Robinson, A., P. C. Gilmore, *Metamathematical considerations and the relative irreducibility of polynomials*. Canad. Journ. Math. **7** (1955), 483—489.

[RoRq] Robinson, A., P. Roquette, *On the finiteness theorem of Siegel and Mahler concerning diophantine equations*. Journ. Number Theory **7** (1975), 121—176.

[Rq1] Roquette, P., *Bemerkungen zur Theorie der formal p-adischen Körper*. Beitr. Algebra Geometrie **1** (1971), 177—193.

[Rq2] Roquette, P., *Principal ideal theorems for holomorphy rings in fields*. Crelle's Journal 262/263 (1973), 361—374.

[Rq3] Roquette, P., *p-adische und saturierte Körper*. Neue Variationen zu einem alten Thema von Hasse. Mitteilungen Math. Gesellschaft Hamburg **11,** Heft 1 (1982), 25—45.

[Ru] Rumely, R., *Capacity theory on algebraic curves and canonical heights*. Manuscript (Sept. 8, 1982).

[Ry] Rychlik, K., *Zur Bewertungstheorie der algebraischen Körper*. Crelle's Journal 153 (1924), 94—107.

[Sk] Skolem, Th., *Lösung gewisser Gleichungen in ganzen algebraischen Zahlen, insbesondere in Einheiten*. Skrifter Norske Videnskap-Akad. Oslo I. Mat. Nat. Kl. No. 10 (1934).

[St] Steinitz, E., *Algebraische Theorie der Körper*. Crelle's Journal 137 (1910), 167—309.

[TM] Tarski, A., J. McKinsey, *A decision method for elementary algebra and geometry*. Univ. California Press Berkeley (1951).

[Tr] Transier, R., *Verallgemeinerte formal p-adische Körper*. Archiv d. Math. **32** (1979), 572—584.

[Un] Unruh, J., Dissertation Heidelberg (1984).

[vdW] van der Waerden, B., *Moderne Algebra* (Erster Teil). Springer Verlag (1. Aufl. 1936).

[We1] Weispfenning, V., *Die Entscheidbarkeit des Adelringes eines algebraischen Zahlkörpers*. Manuskript (1976). Vgl. auch Habilitationsschrift Heidelberg (1978).

[We2] Weispfenning, V., *Nullstellensätze — A model theoretic framework*. Zeitschrift f. math. Logik und Grundlagen d. Math. **23** (1977), 539—545.

[We3] Weispfenning, V., *Aspects of quantifier elimination in algebra*. Preprint (revised Nov. 1983).

[Wh] Whaples, G., *Galois cohomology of additive polynomial and n-th power mappings of fields*. Duke Math. Journ. **24** (1957), 143—150