MODEL THEORY OF FIELDS

DECIDABILITY, AND BOUNDS FOR POLYNOMIAL IDEALS

L.P.D. VAN DEN DRIES

MODEL THEORY OF FIELDS

Decidability, and bounds for polynomial ideals

PROEFSCHRIFT

ter verkrijging van de graad van doctor in de Wiskunde en Natuurwetenschappen aan de Rijksuniversiteit te Utrecht, op gezag van de Rector Magnificus Prof. Dr. A. Verhoeff, volgens besluit van het College van Decanen in het openbaar te verdedigen op woensdag 21 juni 1978 des namiddags te 4.15 uur

door

LAURENTIUS PETRUS DIGNUS

VAN DEN DRIES

geboren op 26 mei 1951

te Ens

Promotor: **DR. D. VAN DALEN**

ACKNOWLEDGEMENTS

To my promotor, *D. van Dalen*, I am especially grateful for his stimulation, and careful checking of the manuscript. I am also indebted to *Ju. Eršov*, *M. Jarden*, *A. Macintyre*, *A. Prestel*, *P. Ribenboim*, *J. Strooker* and *J. Treur* for inspiring discussions on certain points of this thesis.

The excellent typing of the manuscript is due to *Sophie van Sterkenburg*. I thank her also, and *D. van Dalen*, *J. Zucker* and *H. Barendregt* for useful hints concerning presentation and the English text.

I zou ook mijn ouders, en mijn huisgenoten, willen danken voor de wijze waarop zij bijgedragen hebben aan het tot stand komen van dit proefschrift.

CONTENTS

PREFACE

This thesis treats two, somewhat different topics: in Chapters II and III the main goal is to prove decidability results for certain classes of fields, in Chapter IV we derive bounds for polynomial ideals using model theory, while the Appendix contains both types of results.

One is advised to read the introductions in Chapter I and in Chapter IV, and also the '*Samenvatting*' if possible, because these give the motivation, summarize the main new results, and can be understood without knowing the model theoretic terminology required in the other parts. This terminology and some basic theorems are found in sections 2 and 3 of Chapter I. This Chapter contains some propositions of which it may not be clear to the reader whether or not they are new. Concerning this: (*1.1*), (*1.2*), part of the theorem of (*3.3*), the proposition of (*3.5*) and the theorem of (*3.6*), all of Chapter I, do not seem to occur in the literature.

During completion of the manuscript it turned out that most of (*2.3*) and (*2.4*) of Chapter I is also treated -somewhat differently- in §2 of "*Model-complete theories of pseudo-algebraically closed fields*", a preprint of W. Wheeler.

I would like to thank W. Baur for a helpful communication connected with (*A.3*) of the Appendix.

By personal communication I learned further that the proof in (*3.5*) of Chapter IV was also found by D. Lascar and that the result in (*A.9*) of the Appendix has been proved before by D. Lascar and by L. Lipshitz.

NOTATIONS

$\mathbb{N}$	=	$\{0,1,2,3,\ldots\}$
$\mathbb{Z}$	=	ring of integers
$\mathbb{Q}$	=	field of rational numbers
$\mathbb{R}$	=	field of real numbers
$\mathbb{Q}_p$	=	field of p-adic numbers
$\mathbb{Z}_p$	=	ring of integers of $\mathbb{Q}_p$
$\mathbb{F}_p$	=	finite field of p elements
$\mathbb{A}$	=	ring of adèles = $\{x \in \mathbb{R} \times \prod_{p\,\mathrm{prime}} \mathbb{Q}_p \mid x_p \notin \mathbb{Z}_p$ for at most finitely many $p\}$

Further notations and conventions are introduced in Chapter I, *(2.1)*, *(2.2)*, *(3.4)* and *(3.5)*.

A restricted use is also made of nonstandard methods and ultraproducts. For this one may consult [Rob. & Roq., §2] and [Ch. & Ke., 4.1.].

"The virtue of model theory is its ability to organize succinctly the sort of tiresome algebraic details associated with elimination theory".

G. Sacks

CHAPTER I *Preparations*

§1. *Introduction*

It is undisputed that in and before the last century algebra was largely the study of systems of equations of various kinds: the art of solving them, giving conditions for their solvability and clarifying the structure of their solution set.

In the course of the 20^{th} century this practice seems to have changed. So much that modern algebra often seems to be a study of all kinds of axiomatically defined structures, such as groups and rings, with emphasis on their substructures, quotient structures, sheaf representations, etc. In category theory this has even gone so far, that the 'elements' (i.e. the numbers and quantities, used by classical algebraists to carry out their operations and computations) have disappeared all together, their role as basic entities taken over by morphisms. However, this change is perhaps more one of methods, than of goals. The basic difference is that the classical methods for treating algebraic problems were extremely algorithmic and constructive compared with the methods fashionable today. A good example is the theory of linear equations, one of the basic results of which goes back (at least in Europe) to the 18^{th} century, and is called Cramer's rule:

a system of linear equations (with coefficients in a given field)

$$\begin{aligned} a_{11}x_1 + \dots + a_{1n}x_n &= b_1 \\ &\vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n &= b_m \end{aligned}$$

has a solution in that field iff the rank of the matrix (a_{ij}) equals the rank of the augmented matrix (a_{ij}, b_i), where the rank of a matrix was defined as the size of its largest non vanishing minor; moreover, if there is a solution, it can be given by certain rational expressions in the coefficients a_{ij}, b_i.
All this was proved by carrying out rather complicated computations with the coefficients.

Now in the modern theory of linear algebra -of which the theory of linear equations is a small part- the basic notions are linear space, linear map, dimension, etc. and computations are almost absent. I think however nobody would consider such a theory satisfactory if the above result wouldn't follow from it. Fortunately it does follow and the proof reduces to only one small computational fact: that a matrix is invertible iff its determinant is nonzero. So the modern theory of linear equations 'substitutes ideas for computations', but solving linear equations explicitly remains important.
Of course there is a second reason for the success of modern methods: many problems can be stated in an invariant way, i.e. without reference to a coordinate system; while the old theory could only be used after a choice of coordinates to carry out its many computations, modern linear algebra can attack its problems directly, without much computation.

On a more advanced level, namely in algebraic geometry, similar elimination methods were developed. Let me quote from Abhyankar's paper [Ab, p. 418]:

"Elimination theory. This encompasses the explicit algorithmic procedures of solving several simultaneous polynomial equations in several variables. Here some of the prominent names are: Sylvester (1840), Kronecker (1882), Mertens (1886), König (1903), Hurwitz (1913), and Macauley (1916).

It is a vast theory. There used to be a belief, substantially justified, that elimination theory is capable of handling most problems of algebraic geometry in a rigorous and constructive manner. This is of course not surprising, after all, what is algebraic geometry but another name for systems of polynomial equations!

What is surprising is that under Bourbaki's influence it somehow became fashionable to bring elimination theory into disrepute. To quote from page 31 of Weil (1946, Foundations of algebraic geometry): "The device that follows, which, it may be hoped, finally eliminates from algebraic geometry the last traces of elimination theory, is borrowed from C. Chevalley's Princeton Lectures".
It seems to me, what Bourbaki achieved was trading in constructive proofs for mere existence proofs".

Elimination theory begins with the introduction of the resultant of two polynomials: let

$$f(X) = a_0 X^n + a_1 X^{n-1} + \dots + a_n \qquad (a_0 \neq 0)$$

$$g(X) = b_0 X^m + b_1 X^{m-1} + \dots + b_m \qquad (b_0 \neq 0).$$

Then f(X) and g(X) have a common root iff its resultant:

$$\begin{vmatrix} a_0 & a_1 \dots a_n & & & \\ & a_0 & a_1 \dots a_n & & \\ & & \dots\dots\dots & & \\ & & & a_0 & a_1 \dots a_n \\ b_0 & b_1 \dots b_m & & & \\ & b_0 & b_1 \dots b_m & & \\ & & \dots\dots\dots & & \\ & & & b_0 & b_1 \dots b_m \end{vmatrix}$$

equals zero; it is understood here that the coefficients $a_0, \dots, b_m$ and the common root lie in a fixed <u>algebraically</u> <u>closed</u> field.
An important point is that this gives us an <u>effective</u> necessary and sufficient condition on the coefficients for the two polynomials to

have a common root. This can be generalized to an arbitrary finite set of polynomial equations in any number of variables: certain equalities and inequalities between polynomial expressions in the coefficients are necessary and sufficient conditions for the system to have a solution.

The following quotation from Hilbert [Hi, p.414] gives a good explanation why these elimination methods fell into disrepute. Hilbert discusses as an example the problem how many connected components ('von einander getrennten Mänteln') a surface in $\mathbb{P}_3(\mathbb{R})$ of order 4 can have. He first gives a topological argument that this number is finite, then says that arguments on intersection multiplicities imply that it can be at most 12, and goes on as follows with an elimination argument:

"Da eine quaternäre Form 4. Ordnung 35 homogene Koeffizienten besitzt, so können wir uns eine bestimmte Fläche 4. Ordnung durch einen Punkt im 34-dimensionalen Raume veranschaulichen. Die Diskriminante der quaternären Form 4. Ordnung ist vom Grade 108 in den Koeffizienten derselben; gleich Null gesetzt, stellt sie demnach im 34-dimensionalen Raume eine Fläche 108. Ordnung dar. Da die Koeffizienten der Diskriminante selbst bestimmte ganze Zahlen sind, so lässt sich der topologische Charakter der Diskriminantenflache nach den Regeln, die uns für den 2- und 3-dimensionalen Raum geläufig sind, genau feststellen, so dass wir über die Natur und Bedeutung der einzelnen Teilgebiete, in die die Diskriminantenfläche den 34-dimensionalen Raum zerlegt, genaue Auskunft erhalten können. Nun besitzen die durch Punkte des nämlichen Teilgebietes dargestellten Flächen 4. Ordnung gewiss alle die gleiche Mäntelzahl, und es ist daher möglich, durch eine endliche,wenn auch sehr mühsame und langwierige

Rechnung, festzustellen, ob eine Fläche 4. Ordnung mit $n \leqq 12$ Mänteln vorhanden ist oder nicht.

Die eben angestellte geometrische Betrachtung ist also ein dritter Weg zur Behandlung unserer Frage nach der Höchstzahl der Mäntel einer Fläche 4. Ordnung. Sie beweist die Entscheidbarkeit dieser Frage durch eine endliche Anzahl von Operationen. Prinzipiell ist damit eine bedeutende Förderung unseres Problems erreicht: dasselbe ist zurückgeführt auf ein Problem von dem Range etwa der Aufgabe, die $10^{(10^{10})}$-te Ziffer der Dezimalbruchentwicklung von π zu ermitteln - einer Aufgabe, deren Lösbarkeit offenbar ist, deren Lösung aber unbekannt bleibt.

Vielmehr bedurfte es einer von ROHN ausgeführten tiefgehenden schwierigen algebraisch-geometrischen Untersuchung, um einzusehen, dass bei einer Fläche 4. Ordnung 11 Mäntel nicht möglich sind; 10 Mäntel dagegen kommen wirklich vor. Erst diese vierte Methode bringt somit die völlige Lösung des Problems.

Diese speziellen Ausführungen zeigen, wie verschiedenartige Beweismethoden auf dasselbe Problem anwendbar sind, und sollen nahelegen, wie notwendig es ist, das Wesen des mathematischen Beweises an sich zu studieren, wenn man solche Fragen, wie die nach der Entscheidbarkeit durch endlich viele Operationen mit Erfolg aufklären will.

At the end of this discussion there is already the suggestion that metamathematics might be useful, at least in theory, in answering concrete mathematical questions. One might even guess from it that such decision methods in a non-trivial area led Hilbert into believing that also in number theory there are hidden elimination methods to decide every question. We now know that this extrapolation is false, by the famous negative results of Gödel and Church, even strengthened by J. Robinson, H. Putnam, M. Davis and J. Matyasevic to lead to the negative solution of Hilbert's 10^{th} problem.

From Hilbert's discussion one can learn that elimination theory can in principle answer many questions, but that the sheer amount of computation to be done often prevents its application.
Another reason why it fell into disrepute is that for most purposes certain consequences of elimination theory suffice, and that these could also be proved with other means: Hilbert's Nullstellensatz, Chevalley's Constructibility Theorem and the completeness of projective varieties could be mentioned in this context.

At the same time that elimination theory was hoped to be eliminated' once and for all from algebraic geometry, a new interest in it arose, this time coming from workers in mathematical logic. In particular A. Robinson introduced some fascinating new ideas of which the importance only gradually became clear.(This in contrast with his later invention, nonstandard analysis, which was picked up immediately by many mathematicians.)
It all started when Tarski developed an elimination theory for real closed fields, i.e. ordered fields in which polynomials which change sign have a root; $\mathbb{R}$ is an example of such a field. This means that for any general system of polynomial equations and inequalities -using '$=$', '$\neq$', '$<$', '$\leqslant$'- he could give necessary and sufficient conditions on the coefficients -in the form of certain polynomial equations and inequalities in these coefficients- for the solvability of the system; the coefficients and the solution are understood to lie in a real closed field, and the conditions do not depend on the real closed field considered. A well-known illustration of this is the following:

$$aX^2 + bX + c = 0 \quad (a,b,c \in \mathbb{R}) \text{ has a real solution}$$
$$\text{iff } (a \neq 0 \text{ and } b^2 \geqslant 4ac) \text{ or } (a = 0 \text{ and } b \neq 0) \text{ or } (a = 0 \text{ and } b = 0 \text{ and } c = 0).$$

Actually, Tarski was inspired by a metamathematical problem, namely the decidability problem for the elementary theory of the reals, and hence his result was formulated in the terminology of mathematical logic. The proof however was entirely in the style of the 19th century, involving many computations and case distinctions. Yet it clearly was a great step forward, if only because it showed that a whole class of problems could be solved simply by patient labour. But of course there are several mathematically meaningful applications.

It requires some concepts from logic, to make the above vague formulation of Tarski's result precise.

Consider a fixed infinite sequence of variables $v_1, v_2, \ldots$.

Define an atomic formula as one of the form '$p(y_1,\ldots,y_n) = q(y_1,\ldots,y_n)$', or '$p(y_1,\ldots,y_n) < q(y_1,\ldots,y_n)$' with $y_1,\ldots,y_n$ among the variables, and $p,q \in \mathbb{Z}[y_1,\ldots,y_n]$.

New formulas are formed from old by the rules

(*i*) if ϕ,ψ are formulas, then also $(\neg\phi),(\phi\vee\psi),(\phi\wedge\psi)$;

(*ii*) if ϕ is a formula, then also $(\exists v_i\ \phi)$ and $(\forall v_i\ \phi)$.

A bound occurrence of a variable y in a formula is an occurrence in a subformula $(\exists y\ \phi)$ or $(\forall y\ \phi)$. If an occurrence is not bound it is said to be free. We write $\phi(y_1,\ldots,y_n)$ for a formula ϕ all of whose free variables are among $y_1,\ldots,y_n$.

The basic notion is that of satisfaction: if R is a commutative ring with unity, $<$ any binary relation on R (e.g. an ordering),

$\phi = \phi(y_1,\dots,y_n)$ a formula and $r_1,\dots,r_n \in R$, then $\phi(r_1,\dots,r_n)$ is the result of substituting $r_1,\dots,r_n$ for the free occurrences of $y_1,\dots,y_n$ in ϕ.
To say that $\phi(r_1,\dots,r_n)$ holds in $(R,<)$, or $(R,<)$ satisfies $\phi(r_1,\dots,r_n)$, has the obvious meaning if the logical symbols are interpreted as usual; notation: $(R,<) \models \phi(r_1,\dots,r_n)$.
Two formulas $\phi(y_1,\dots,y_n)$ and $\psi(y_1,\dots,y_n)$ are called equivalent for $(R,<)$ if for all $(r_1,\dots,r_n) \in R^n$: $(R,<) \models \phi(r_1,\dots,r_n)$ iff $(R,<) \models \psi(r_1,\dots,r_n)$.

Tarski's Theorem can now be stated as follows:

For each formula $\phi = \phi(y_1,\dots,y_n)$ there is a formula $\psi = \psi(y_1,\dots,y_n)$ in which no quantifiers $\exists v_i$ or $\forall v_i$ occur, which is equivalent with ϕ for each real closed field $(R,<)$; moreover ψ can be constructed effectively from ϕ.

For instance, in the above illustration on the preceding page

ϕ is $(\exists v_4\ v_1 v_4^2 + v_2 v_4 + v_3 = 0)$

and ψ is $(v_1 \neq 0 \wedge v_2^2 \geqslant 4v_1 v_3) \vee (v_1 = 0 \wedge v_2 \neq 0) \vee$
$(v_1 = 0 \wedge v_2 = 0 \wedge v_3 = 0)$.

By a theorem of logic it actually suffices to prove Tarski's result for formulas ϕ of the form $\exists z \phi'(z,y_1,\dots,y_n)$ with ϕ' open (i.e. without quantifiers); these are the formulas expressing the solvability of a system of equations and inequalities in one variable; but we should keep in mind that Tarski's Theorem applies to arbitrary formulas, not only those which state the solvability of systems of equations and inequalities. In particular, if a formula ϕ has no free variables

- a so called sentence - it expresses an elementary statement about real closed fields; by Tarski's result one may suppose ϕ to have no quantifiers, and so its truth in a real closed field can be computed, and turns out to be independent of the real closed field considered! Two typical applications of this are:

(1) Milnor and Bott showed topologically that for $n \neq 1,2,4,8$ there are no division algebras of rank n over $\mathbb{R}$. Given $n \in \mathbb{N}$, it is easy to construct a sentence ϕ_n such that a real closed field R satisfies ϕ_n iff there are no division algebras of rank n over R. If $\mathbb{R} \models \phi_n$, also $R \models \phi_n$, hence Milnor & Bott's result holds for any real closed field; more interesting is that through applying Tarski's reduction steps to ϕ_n one gets a purely algebraic proof, for given n.

(2) Krull and Neukirch determined in [K.&N.] the absolute Galois group of $\mathbb{R}(t)$, using topological properties of Riemann surfaces. In [v.d.D.&R.] it is shown that their results are essentially of algebraic nature and generalize to any real closed field.

In the fifties A. Robinson discovered a new class of arguments which were at the same time powerful, general, and simple, and which allowed him to prove elimination theorems, not only for algebraically closed and real closed fields, but for many other classes of algebraic structures as well.
Also, he gave surprising new applications. The best known is the application to Hilbert's 17^{th} problem. As a matter of fact the theory of real closed fields was created by Artin and Schreier to solve this problem [Ar.&S.].
However, Artin still needed some fairly complicated arguments to derive

the positive solution of the 17^{th} problem (cf. [Ar]). Robinson, in a sense, trivialized all this, and considerably strengthened Artin's results (cf. [Rob 1]).

To get an idea of his methods, let us consider again linear equations: let $\mathcal{R}$ be a class of commutative rings with identity. We define:

$\mathcal{R}$ admits linear elimination if for each formula

$$\phi_{mn}(a_{11},..,a_{mn},b_1,..,b_m) \overset{\text{def}}{=} \exists x_1 ..\exists x_n \begin{bmatrix} a_{11}x_1 + .. + a_{1n}x_n = b_1 & \wedge \\ a_{21}x_1 + .. + a_{2n}x_n = b_2 & \wedge \\ & \vdots \\ \cdot \qquad \cdot \quad \cdot & \wedge \\ a_{m1}x_1 + .. + a_{mn}x_n = b_m & \end{bmatrix}$$

there is an open formula $\psi_{mn}(a_{11},..,a_{mn},b_1,..,b_m)$ which is equivalent with ϕ_{mn} for each ring $R \in \mathcal{R}$ (here the 'atoms' of ψ_{mn} are of the form $p = q$, where p and q are polynomials in the a's and b's over $\mathbb{Z}$.
So by Cramer's rule the class of fields admits linear elimination.

Definition

(*a*) $\mathcal{R}$ is called an elementary class if $\mathcal{R}$ is the class of all rings (commutative with unity) satisfying a fixed set of sentences (called axioms for $\mathcal{R}$).

(*b*) $\mathcal{R}$ has PEP (= the prime extension property) if each subring R of any ring in $\mathcal{R}$ has a prime extension R' in $\mathcal{R}$, i.e. $R \subset R' \in \mathcal{R}$, and R' can be embedded over R in each R-extension in $\mathcal{R}$.

(*1.1*) *Theorem*

If $\mathcal{R}$ is an elementary class with PEP such that $R_1 \subset R_2$ $(R_1, R_2 \in \mathcal{R})$

<u>implies that R_2 is a faithfully flat R_1-module</u>, <u>then $\mathcal{R}$ admits linear elimination.</u>

<u>*Proof*</u> *(sketch):* from the faithful flatness one needs only the consequence that solvability of a system of linear equations is preserved downward. See Ch. IV (2.6).
Of course solvability is also preserved upward. Now a general model theoretic fact is that any 'elementary property' which is preserved upward and downward among the structures of an elementary class with PEP, can be expressed (for all the structures simultaneously) by an open formula. See (2.12) for details. □

<u>*Remarks*</u>

(a) Fields are those commutative rings with identity $\neq 0$ whose nonzero elements are invertible, so the class of fields is elementary. If $K \subset L$ with K and L fields, then L is a free K-module, so certainly faithfully flat. Finally, if R is a subring of a field, then clearly the quotient field of R is a prime extension of R with respect to the class of fields; so the class of fields has PEP. Hence we have a new proof that the class of fields admits linear elimination.

(b) Another class satisfying the hypothesis - and hence the conclusion - of the theorem is the class of boolean rings.

(c) General considerations from logic tell us that (roughly): "linear elimination for $\mathcal{R}$ is recursive in any set of axioms for $\mathcal{R}$". This means that the theorem is not as inconstructive as one might think.

The following result suggests that structures must be sufficiently 'large', to admit elimination.

(1.2) *Theorem*

Let D be an integral domain such that {D} admits linear elimination. Then D is a field.

Proof

D may be assumed infinite because finite integral domains are fields. By assumption there is an open formula $\operatorname{div}(v_1,v_2)$ equivalent with $\exists v_3\ v_1 v_3 = v_2$ for D. $\operatorname{div}(v_1,v_2)$ may be brought in disjunctive normal form, and using $a \neq 0 \wedge b \neq 0 \Leftrightarrow ab \neq 0$ (holding in D) each disjunct may be brought in the form:

$$p_1(v_1,v_2) = \ldots = p_k(v_1,v_2) = 0 \wedge q(v_1,v_2) \neq 0,\ (k \geqslant 0)$$

with $p_1,\ldots,p_k,\ q \in \mathbb{F}[v_1,v_2]\setminus\{0\}$, $\mathbb{F}$ the primering of D (formally the polynomials have integer coefficients, but these are naturally interpreted by their images in D).

Suppose that $k > 0$ for each disjunct. This leads to a contradiction: form a product $P(v_1,v_2)$ by taking from each disjunct $p_1(v_1,v_2)$ as a factor; then:

$$P(a,b) = 0, \text{ for all } a,b \in D \text{ with } a|b \text{ in } D,$$

so in particular the non-zero polynomial $P(X,XY) \in \mathbb{F}[X,Y]$ vanishes on $D\times D$, which is impossible, because D is infinite.

So some disjunct is simply of the form $q(v_1,v_2) \neq 0$ with $q \in \mathbb{F}[v_1,v_2]\setminus\{0\}$. Let $0 \neq a \in D$; then $q(aXY,Y) \in D[X,Y]\setminus\{0\}$, hence there are $x,y \in D\setminus\{0\}$ with $q(axy,y) \neq 0$, which implies $axy|y$ in D, so $ax|1$, and a is invertible in D. $\square$

Remark

This result and its proof are along the lines of some recent theorems, which can be found in [M.,M. & v.d.D.].

I will now discuss two contributions of Robinson in more detail which have been the starting point of a considerable amount of research.

A. *Differential fields*

These are pairs (F,d) with F a field and $d: F \to F$ a derivation; expressions, built up from variables and elements of F using the ring-operations and the symbol d, are called differential polynomials over F, and they lead to algebraic differential equations.
The study of these with algebraic methods is called differential algebra (Ritt, Kolchin).

In the fifties Seidenberg gave an elimination theory for systems of algebraic differential equations in char. 0, but there was a difference with, say, elimination theory for algebraically closed fields:

given a general system of algebraic differential equations:

$$p_1(a,x) = \ldots = p_k(a,x) = 0$$

(a and x stand for the vector of coefficients and the sequence of variables respectively),
Seidenberg constructed an 'open' condition R(a) such that for any a from a differential field (F,d) of char. 0:

$$(F,d) \models R(a)$$

iff the system has a solution in an <u>extension differential field</u> of (F,d).

So the analogue of 'algebraically closed field' was missing. Robinson showed on the basis of general principles that a certain elementary class of differential fields of char. 0 deserved to be called the class of differentially closed fields, and proved that all differentially closed fields are elementarily equivalent, i.e. satisfy the same sentences. However, he did not reprove with his own methods Seidenberg's result. This was done quite simply by L. Blum in 1968, and she could also characterize the differentially closed fields as the differential fields (F,d) of char. 0 with F algebraically closed and such that for f(X) and g(X) differential polynomials in one variable over (F,d) with order(g) $<$ order(f), f(X) = 0, g(X) $\neq$ 0 has a solution in (F,d).

Robinson had also asked whether a differential field(F,d) of char. 0 has a differential closure, i.e. a differentially closed extension of (F,d) which can be embedded over (F,d) into any differentially closed extension of (F,d).
This turned out to be a surprisingly difficult question. It is fair to say that the model theory needed for applications in algebra is in general rather simple and can be learnt quickly by any algebraist, but this question required some of the deeper theorems of two model theorists pur sang: M. Morley and S. Shelah.
From their results Blum derived the existence and uniqueness of the differential closure.
Later it turned out that -in contrast with the algebraic and real closure - the differential closure is in general not minimal: the differential closure of $\mathbb{Q}$ contains properly an isomorphic copy of itself (proved independently by E. Kolchin, M. Rosenlicht, S. Shelah).
A readable account on this subject -containing the references omitted here - is given by C. Wood in [Wo].

B. *Valued fields*

Here, finally, a kind of breakthrough was accomplished: using his typical techniques, Robinson could prove (around 1955) that the class of

non-trivially valued algebraically closed fields has an elimination theory, before this was proved by more orthodox methods.
From then on this became the usual procedure: first a certain class of algebraic structures was proved to admit elimination by model theory, and later this elimination was given explicitly.
The precise result, referred to above, is the same as the one for real closed fields, except that in the definition of atomic formula '$p(y_1,\dots,y_n) < q(y_1,\dots,y_n)$', is replaced by '$p(y_1,\dots,y_n)$ div $q(y_1,\dots,y_n)$', where 'a div b' is interpreted for a valued field (K,v) as '$v(a) \leq v(b)$', $v:K \to \Gamma\cup\{\infty\}$ being the (Krull) valuation on K.
A corollary is: two non-trivially valued algebraically closed fields are elementarily equivalent iff they, as well as their residue fields, have the same characteristic.

But most important was that it led some mathematicians to look for new applications of model theoretic methods in algebra and number theory.
So finally with the work of Ax & Kochen, and Eršov (1965-1966) on p-adic fields and other valued fields, model theory became connected with number theory: an asymptotic form of a conjecture of E. Artin could be proved; later it turned out that the full form was not valid (Terjanian).
It is true that Ax & Kochen originally used other model theoretic tools - ultra products - but in their last joint paper [Ax & Ko] they showed how some of their strongest results could most elegantly be developed in the framework set up by Robinson; Eršov seems to have done this from the beginning.

Let us consider the p-adic fields $\mathbb{Q}_p$ more closely. The p-adic field $\mathbb{Q}_p$ (p a prime) was invented by K. Hensel in 1897 as a kind of approximation to the field of rational numbers $\mathbb{Q}$, having 'better' properties than $\mathbb{Q}$. Just as $\mathbb{Q}$ it has a subring of 'integers' $\mathbb{Z}_p$, and $\mathbb{Q} \subset \mathbb{Q}_p$, $\mathbb{Z} \subset \mathbb{Z}_p$. Given any polynomial equation with coefficients in $\mathbb{Z}$, the equation has a solution in $\mathbb{Z}_p$ iff it has modulo p^n a solution in $\mathbb{Z}$ for each $n \in \mathbb{N}$.

Now, the properties that $\mathbb{Q}_p$ made so convenient for number theorists are, strangely enough, its excellent topological properties, like local compactness; in fact $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to a certain field topology on $\mathbb{Q}$.

But this tends to obscure another fundamental and desirable fact: that one can decide effectively elementary questions about $\mathbb{Q}_p$, and this is indeed one of the Ax-Kochen-Eršov results; more precisely, $\mathbb{Q}_p$ endowed with some extra structure has an elimination theory.

Later P.J. Cohen gave an explicit description of this elimination procedure in [C]; his work was extended and completed by V. Weispfenning [We].

Important is that Cohen's procedure shows certain uniformities with respect to the residue rings involved, and using this fact he could give more effective versions of several results of Ax & Kochen.

For instance, Ax & Kochen proved:

given an elementary statement A about valued fields, then for all but finitely many primes p one has:

A holds in $\mathbb{Q}_p$ iff A holds in the field of formal Laurentseries $\mathbb{F}_p((t))$.

By Cohen's method one can construct a primitive recursive function of the argument A giving an upperbound for the exceptional primes.

Another important development was initiated by Ax'decision methods for the class of finite fields and the class of finite prime fields ([Ax], 1968), which can also be put in the form of an elimination theory, see [Ki].
Here the number theory required (Weil's result on curves over finite fields, Cebotarev's Density Theorem) becomes rather heavy for the ordinary model theorist!
Ax'work has interesting consequences, for instance, given any system of polynomial equations with integer coefficients, the set of primes p such that the system has a solution modulo p has an effectively computable rational Dirichlet density, which moreover is >0 if the set is infinite.
In 1976 Fried & Sacerdote in [F.&S.] published an explicit description of the algorithms whose existence had been proved model-theoretically by Ax.
It should be mentioned that Ax'results have been completed and generalized in several directions by M. Jarden who discovered in relation to this interesting connections between Dirichlet density and Haar measure (on certain infinite Galois groups), see [J1].

But let us return to the original idea behind p-adic fields, i.e. the isolation of those properties of $\mathbb{Q}$ which have to do with the behaviour of only one prime p. This idea is very successful, in the sense that elementary statements on valued fields can be decided effectively for $\mathbb{Q}_p$.
But for $\mathbb{Q}$ this does not imply much: for instance, one can decide effectively whether a system of polynomial equations with coefficients in $\mathbb{Z}$ has for each $n \in \mathbb{N}$ a solution modulo p^n. Combining Cohen's and Ax' results one can even decide effectively whether such a system has for each $0 < m \in \mathbb{N}$ a solution modulo m.

But of course one really wants to decide whether such a system has a solution in $\mathbb{Z}^k$, if k is the number of variables. In that case the above decision method suffices only for those equation systems for which the local-global (or Hasse) principle works: a <u>necessary condition</u> for a system of equations over $\mathbb{Z}$ to have a solution in $\mathbb{Z}^k$ (k being the number of unknowns) is of course to have a solution in $\mathbb{Z}_p^k$ for all primes p, and a solution in $\mathbb{R}^k$. The <u>Hasse principle</u> is said to apply to the equation system if this condition is also <u>sufficient</u>. An example is provided by the famous theorem of Hasse-Minkowski saying that the Hasse principle applies to equations $f = 0$, f being a quadratic form over $\mathbb{Z}$, and where only zeros $\neq(0,\ldots,0)$ are counted as solutions.

Let me now explain roughly what is done in Chapters II and III of this thesis. Recall that Tarski, Robinson, Ax, Kochen and Eršov proved that certain classes of ordered resp. valued fields (i.e. fields endowed with <u>one</u> distinguished ordering, resp. valuation) admit an elimination theory. In ch. II and III certain classes of fields endowed with <u>several</u> distinguished orderings and valuations are shown to have an elimination theory and to admit effective decision of elementary statements.

As an example consider finitely many primes $p_1,\ldots,p_k$, let $v_{p_i}:\mathbb{Q}\to\mathbb{Z}\cup\{\infty\}$ be the p_i-adic valuation on $\mathbb{Q}$, and consider all structures $(F,v_1,\ldots,v_k,<)$ with F a field of char. 0, $v_i:F\to\mathbb{Z}\cup\{\infty\}$ a valuation on F extending v_{p_i} with residue field $\mathbb{F}_{p_i}$ (in other words (F,v_i) is an <u>immediate</u> extension of $(\mathbb{Q},v_{p_i})$), and $<$ an archimedean ordering on F. Among these structures some are 'large'. The main result is that, given an elementary statement on such structures, one can decide effectively whether it holds in all the 'large' structures simultaneously.

It may be instructive to see what this means for some special cases:

for k = 0, the 'large' structures are simply the archimedean real closed fields (among these is $\mathbb{R}$); for k = 1, and supposing that the ordering is omitted from the structure, the henselian subfields of $\mathbb{Q}_p$ are the 'large' ones; in both cases the result reduces to those of Tarski, etc. In the general case the 'large' structures are certain 'intersections' $F_1 \cap \ldots \cap F_k \cap R$ with F_i a henselian subfield of $\mathbb{Q}_{p_i}$ and R a real closed subfield of $\mathbb{R}$.
One of the reasons for considering these 'semi-local' fields is to approximate the arithmetic properties of $\mathbb{Q}$ better than is done by the local fields $\mathbb{Q}_p$, $\mathbb{R}$, and at the same time to preserve that elementary statements can be decided. This leads to effective necessary conditions on an equation over $\mathbb{Z}$ to have a solution in integers, which are perhaps stronger than those provided by the local fields $\mathbb{Q}_p$ and $\mathbb{R}$. Whether they are really stronger, is for me, through lack of number theoretic experience, as yet a matter of speculation.
Another important question is how the absolute Galois group of a 'semi-local' field depends on the absolute Galois groups of the corresponding local fields, and whether in some sense the absolute Galois group of $\mathbb{Q}$ can be approximated by the absolute Galois groups of the 'semi-local' fields. There is an interesting conjecture by Eršov with respect to the first problem. For details see (3.13) Ch. II and (3.7) Ch. III.

Coming to the end of this preview I should remark that I mentioned only a small part of interesting and relevant work in this area. I have concentrated here on fields.
There are many similar results for other kinds of structures: graphs, ordered abelian groups, boolean algebras, to mention only a few.
At least I should say a few words about a new development, started in

1969 by A. Robinson, which was originally inspired by P.J. Cohen's forcing method.

Many model theorists took part in this development and several useful new notions and instruments were created (some of these can be found in §2).

Applied in algebra the notion of forcing clarified the fundamental model theoretic differences between the class of skew fields and the class of fields, and similarly between the class of groups and the class of abelian groups; in particular, for groups and skew fields there is a connection with word problems (A. Macintyre and B.H. Neumann).

Also it promoted a better understanding and elegant formulation of many of the older results of Robinson and others.

For a more detailed description of the applications of Robinson's methods, one may consult Macintyre, [M2].

§2. Relevant model theory and algebra

(2.1) Preliminaries

The model theoretic terminology used here is a mixture of that in Shoenfield [Sh] and Sacks [Sa].

Algebraic notions, especially from field theory, are taken from Lang [L1] and [L3].

Let me lay down some conventions.

A 'language' (called 'similarity type' by Sacks) is always first-order with equality, and is formally the set of its non-logical symbols (function symbols, predicate symbols and constants).

There is a fixed sequence of variables $v_1, v_2, ..$ used for all languages.

In the following, let $\mathcal{L}$ be a language.

An open $\mathcal{L}$-formula is an $\mathcal{L}$-formula without quantifiers; an existential $\mathcal{L}$-formula is an $\mathcal{L}$-formula of the form $\exists x_1 \ldots \exists x_m \phi(x_1,..,x_m,y_1,..,y_n)$ with ϕ open; here, and in the following, I will write $\psi(z_1,..,z_k)$ for a formula ψ whose free variables are among $z_1,..,z_k$.

Similarly a universal $\mathcal{L}$-formula is an $\mathcal{L}$-formula of the form $\forall x_1 .. \forall x_m \phi(x_1,..,x_m,y_1,..,y_n)$ with ϕ open, and a $\forall\exists$-formula is a formula of the form $\forall x_1 .. \forall x_n \exists y_1 .. \exists y_m \phi(x,y,z)$ with ϕ open.

An $\mathcal{L}$-theory or a theory in $\mathcal{L}$ is a set of $\mathcal{L}$-sentences; where possible without ambiguity, two equivalent $\mathcal{L}$-theories will be identified.

If A is an $\mathcal{L}$-structure, then $|A|$ is its universe and $\mathcal{L}(A)$, or $\mathcal{L}(|A|)$, is the language $\mathcal{L}$, augmented by a new constant for each element a of $|A|$, called its name.

In general $a \in |A|$ is identified with its name; an $\mathcal{L}(A)$-formula is also called an A-formula.

For a structure A, Diag(A), the diagram of A, is the set of all atomic and negated atomic A-sentences which are true in A, and $\text{Diag}^+(A)$, the positive diagram of A, is the set of all atomic A-sentences true in A.

By abuse of language a model of Diag(A) will be considered as an extension of A, and similarly a model B of $\mathrm{Diag}^+(A)$ as a structure B together with a morphism $A \to B$.

'$A \subset B$' stands for: 'A is a substructure of B' (or equivalently, 'B is an extension of A'); and it will be understood in this case that A and B are structures for the same language.

If T is an $\mathcal{L}$-theory, then Mod(T) is the class of its models, i.e. the class of $\mathcal{L}$-structures satisfying all sentences in T.

A class of $\mathcal{L}$-structures is called an elementary class if it is of the form Mod(T) for some $\mathcal{L}$-theory T.

In the model theoretic treatment of elimination theories the notion of 'existentially closed' has turned out to be useful, cf. [M2].

(2.2) *Definition*

Let $A \subset B$. Then A is called existentially closed in B if each existential A-sentence true in B is also true in A.

As an example consider commutative rings with identity. Because only such rings will be considered in the following, let us make the

CONVENTION 'ring' will from now on mean 'commutative ring with identity';

a ring is considered as a structure of type $(R,+,\cdot,-,0,1)$, i.e. the language of rings is $\{+,\cdot,-,0,1\}$.

A field is a ring with $1 \neq 0$, whose nonzero elements are units; a domain is a subring of a field; if D is a domain, Q(D) is its quotient field.

Now one easily checks the following:

If R,S are rings with $R \subset S$, then R is existentially closed in S iff

<u>each system of polynomial equations and inequations</u>

$$f_1(X_1,\dots,X_n) = 0,\dots,f_k(X_1,\dots,X_n) = 0 \quad (f_i \in R[X_1,\dots,X_n])$$
$$g_1(X_1,\dots,X_n) \neq 0,\dots,g_\ell(X_1,\dots,X_n) \neq 0 \quad (g_j \in R[X_1,\dots,X_n])$$

<u>with a solution in S^n has also a solution in R^n.</u>

The reader not familiar with model theoretic terminology can take this as a definition in the case of rings. Some rather fundamental theorems state that one ring is existentially closed in another, for instance Hilbert's Nullstellensatz (see (2.5)(a)) and Artin's Approximation Theorem (see Appendix to Ch. IV).

(2.3) *Proposition*

(a) Let K and L be fields, $K \subset L$ and K existentially closed in L. Then the field extension $L|K$ is regular.

(b) Let D and E be domains, $D \subset E$ and D existentially closed in E. Then $Q(D)$ is existentially closed in $Q(E)$.

Proof

(a) for the notion of regular field extension see [L1, Ch. III, §1]. K is clearly algebraically closed in L, so it suffices to show that $L|K$ is separable, and hence we may suppose $\mathrm{char}(K) = p > 0$. Let $a_1,\dots,a_n \in K$ be such that $a_1^{\frac{1}{p}},\dots,a_n^{\frac{1}{p}}$ are linearly independent over K. It suffices to show that this implies their linear independence over L. If $\Sigma\lambda_i a_i^{\frac{1}{p}} = 0$ with $\lambda_i \in L$ and say $\lambda_1 \neq 0$, then $\Sigma\lambda_i^p a_i = 0$. So $\Sigma a_i X_i^p = 0$, $X_1 \neq 0$ has a solution in L^n, and then by assumption also a solution in K^n, which contradicts the K-linear independence of $a_1^{\frac{1}{p}},\dots,a_n^{\frac{1}{p}}$.

(b) Consider for simplicity the case of one equation $f(X_1,\dots,X_n) = 0$ having a solution $(x_1,\dots,x_n) \in (Q(E))^n$, where $f \in D[X_1,\dots,X_n]$.
Let $f(Y_1/Z,\dots,Y_n/Z) = F(Y_1,\dots,Y_n,Z)/Z^k$ with
$F(Y_1,\dots,Y_n,Z) \in D[Y_1,\dots,Y_n,Z]$, $k \in \mathbb{N}$.
Let $x_i = y_i/z$ $(y_i, 0 \neq z \in E)$. Then the system $F(Y_1,\dots,Y_n,Z) = 0$, $Z \neq 0$ has the solution $(y_1,\dots,y_n,z) \in E^{n+1}$, so it has a solution $(y_1',\dots,y_n',z') \in D^{n+1}$.
Then putting $x_i' = y_i'/z'$, $(x_1',\dots,x_n') \in (Q(D))^n$ is a solution of $f(X_1,\dots,X_n) = 0$. $\square$

(2.4) Let me illustrate a typical trick in proving existential closedness.

Let two fields K and L be given with $K \subset L$ and $L|K$ separable (this last assumption should certainly be verified if one wants to prove that K is existentially closed in L, by (2.3)).
Let a system *(1)* of polynomial equations and inequations with a solution in L^n be given:

(1) $f_1(X_1,\dots,X_n) = \dots = f_k(X_1,\dots,X_n) = 0$, $(f_i \in K[X_1,\dots,X_n])$
$g_1(X_1,\dots,X_n) \neq 0,\dots,g_\ell(X_1,\dots,X_n) \neq 0$ $(g_j \in K[X_1,\dots,X_n])$.

Now I will indicate much simpler systems of equations and inequations (solvable in L) whose solvability in K implies the solvability of *(1)* in K.
Let $(x_1,\dots,x_n) \in L^n$ be a solution of *(1)*. Take a separating transcendence base $y_1,\dots,y_t$ of $K(x_1,\dots,x_n)$ over K and $z \in L$ separable algebraic over $K(y_1,\dots,y_t)$ such that $K(x_1,\dots,x_n) = K(y_1,\dots,y_t,z)$.
After multiplying z by a suitable nonzero element of $K(y_1,\dots,y_t)$ the minimal polynomial of z over $K(y_1,\dots,y_t)$ may be assumed to be $p(y_1,\dots,y_t,Z)$ for some $p = p(Y_1,\dots,Y_t,Z) \in K[Y_1,\dots,Y_t,Z]$, which is monic and separable in Z.

Consider now for $0 \neq q \in K[Y_1,\dots,Y_t]$ the system:

(2_q) $p(Y_1,\dots,Y_t,Z) = 0$, $q(Y_1,\dots,Y_t) \neq 0$.

This system has the solution $(y_1,\dots,y_t,z) \in L^{t+1}$.

Claim

Suppose each system (2_q) has a solution in K^{t+1}. Then (1) has a solution in K^n.

It may be instructive to see two proofs.

Proof by model theory:

Let σ be the K-sentence

$$\exists v_1 \dots \exists v_n \left(\bigwedge_{i=1}^{k} f_i(v_1,\dots,v_n) = 0 \wedge \bigwedge_{j=1}^{\ell} g_j(v_1,\dots,v_n) \neq 0 \right).$$

We have to prove $K \models \sigma$. Let FL be the theory of fields, let $\underline{c}_1,\dots,\underline{c}_t,\underline{d}$ be new constants and put

$\Gamma = \mathrm{FL} \cup \mathrm{Diag}\, K \cup \{p(\underline{c}_1,\dots,\underline{c}_t,\underline{d}) = 0\} \cup \{q(\underline{c}_1,\dots,\underline{c}_t) \neq 0 \mid 0 \neq q \in K[Y_1,\dots,Y_t]\}$.

Then each model of Γ contains an isomorphic copy of

$$K(y_1,\dots,y_t,z) = K(x_1,\dots,x_n), \text{ so } \Gamma \models \sigma.$$

Then by the Compactness Theorem there is $0 \neq q \in K[Y_1,\dots,Y_t]$ with

$$\Gamma_q \overset{\mathrm{def}}{=} \mathrm{FL} \cup \mathrm{Diag}\, K \cup \{p(\underline{c}_1,\dots,\underline{c}_t,\underline{d}) = 0,\ q(\underline{c}_1,\dots,\underline{c}_t) \neq 0\} \models \sigma.$$

But by the assumption in the claim, K (together with a suitable interpretation of $\underline{c}_1,\dots,\underline{c}_m,\underline{d}$ in K) is a model of Γ_q, so $K \models \sigma$.

Proof by manipulation:

Write $x_i = r_i(y_1,\dots,y_t,z)/q(y_1,\dots,y_t)$ and

$g_j(x_1,\dots,x_n)^{-1} = s_j(y_1,\dots,y_t,z)/q(y_1,\dots,y_t)$, $1 \leq i \leq k$, $1 \leq j \leq \ell$,

for suitable $r_i, s_j \in K[Y_1,\dots,Y_t,Z]$, $0 \neq q \in K[Y_1,\dots,Y_t]$.

Then we have:

$$(3)\quad \begin{cases} f_i(r_1/q,..,r_n/q) = F_i/q^{d_i} \text{ with } F_i \in K[Y_1,..,Y_t,Z],\ d_i \in \mathbb{N}. \\ (g_j(r_1/q,..,r_n/q)\cdot s_j/q)-1 = G_j/q^{e_j} \text{ with } G_j \in K[Y_1,..,Y_t,Z],\ e_j \in \mathbb{N}. \end{cases}$$

Then $f_i(x_1,..,x_n) = F_i(y_1,..,y_t,z)/q^{d_i}(y_1,..,y_t) = 0$,

so $F_i(y_1,..,y_t,z) = 0$ and

$g_j(x_1,..,x_n)\cdot g_j(x_1,..,x_n)-1 = G_j(y_1,..,y_t,z)/q^{e_i}(y_1,..,y_t) = 0$,

so $G_j(y_1,..,y_t,z) = 0$.

Hence by the irreducibility of p we get:

(4) $\quad p|F_i$ and $p|G_j$ in $K[Y_1,..,Y_t,Z]$.

Now let $(y_1',..,y_t',z') \in K^{t+1}$ be a solution of (2_q) and put

$$x_i' = r_i(y_1',..,y_t',z')/q(y_1',..,y_t').$$

Then by (3) and (4) $(x_1',..,x_n') \in K^n$ is a solution of (1).

Remark

Variants of this reduction procedure appear in Ch. II (1.19), Ch. II (1.14) and (2.6). In all 3 cases the model theoretic argument is really the guiding principle, while the proof by 'algebraic manipulation' is in the first two cases simply too complicated to write down.

(2.5) *Applications*

(a) Let me first show how it follows that an algebraically closed field K is existentially closed in each extension field L (this is one of the forms of Hilbert's Nullstellensatz):
L|K is separable, so by the claim it certainly suffices to prove that for any two polynomials $p \in K[Y_1,..,Y_t,Z]$ and $0 \neq q \in K[Y_1,..,Y_t]$ with p monic and of positive degree in Z there is a solution in K^{t+1} of the system

$$p(Y_1,..,Y_t,Z) = 0,\ q(Y_1,..,Y_t) \neq 0.$$

Well, take any $(y_1,..,y_t) \in K^t$ with $q(y_1,..,y_t) \neq 0$.
Then $p(y_1,..,y_t,Z)$ has a root z in K, so $(y_1,..,y_t,z)$ is a solution as desired.

(b) A special case of a result on p. 71 in [L1] is:
if $f(Z_1,..,Z_n) \in K[Z_1,..,Z_n]$ is irreducible (K a field), then f is absolutely irreducible iff $Q(K[Z_1,..,Z_n]/(f))$ is a regular extension of K.
Combining this with the reduction in (2.4) gives the following.

Theorem

Let L be an extension field of the field K.
Then the following are equivalent:

(i) K is existentially closed in L.

(ii) $L|K$ is regular, and for each two polynomials $p = p(Y_1,..,Y_t,Z) \in K[Y_1,..,Y_t,Z]$, $0 \neq q = q(Y_1,..,Y_t) \in K[Y_1,..,Y_t]$ such that p is monic in Z and absolutely irreducible, the system

$$p(Y_1,..,Y_t,Z) = 0,\ q(Y_1,..,Y_t) \neq 0$$

has a solution in K^{t+1} if it has one in L^{t+1}.

Proof

(i) $\Rightarrow$ *(ii)* is trivial, using the definitions and (2.3).
(ii) $\Rightarrow$ *(i)*. In order to prove that K is existentially closed in L, it suffices by (2.4) to consider the following situation: a point $(y_1,..,y_t,z) \in L^{t+1}$ is 'generic' zero of an irreducible polynomial $p(Y_1,..,Y_t,Z) \in K[Y_1,..,Y_t,Z]$, monic in Z, which means

$$K(y_1,..,y_t,z) \simeq_K Q(K[Y_1,..,Y_t,Z]/(p)).$$

We have then only to show that for $0 \neq q \in K[Y_1,..,Y_t]$

$$p(Y_1,..,Y_t,Z) = 0,\ q(Y_1,..,Y_t) \neq 0$$

has a solution in K^{t+1}. Note that $(y_1,..,y_t,z) \in L^{t+1}$ is a solution. Now $L|K$ is regular, so $Q(K[Y_1,..,Y_t,Z]/(p))|K$ is regular, so by the result in [L1] mentioned above, p is absolutely irreducible, hence *(ii)* gives the desired solution in K^{t+1}. □

(2.6) Given a class K of $\mathcal{L}$-structures, a structure $A \in K$ is called K-existentially closed if A is existentially closed in each of its extensions in K.

K is called inductive if the union of each chain of structures in K (ordered by the substructure relation) also belongs to K.

The proof of the following proposition gives in embryonal form a very useful construction. To make it as accessible as possible, only the case that K is a class of rings will be treated in the proof.

(2.7) ***Proposition***

Let K be an inductive class.

Then each $A \in K$ has a K-existentially closed extension.

Proof

Let R be a ring in K. Let $(\Sigma_\alpha)_{1\leqslant\alpha<\kappa}$ be an enumeration of all (finite) systems of polynomial equations and inequalities with coefficients in R (κ is a cardinal, α ranges over ordinals). Then an ascending chain $(R_\alpha)_{\alpha<\kappa}$ in K is formed inductively as follows:

$R_0 = R$,

for $\alpha+1<\kappa$ $R_{\alpha+1}$ is some extension of R_α in K in which $\Sigma_{\alpha+1}$ has a solution, if such an extension exists; otherwise $R_{\alpha+1} = R_\alpha$;

for a limit ordinal $\lambda \neq 0$ less than κ, put $R_\lambda = \cup\{R_\alpha|\alpha<\lambda\}$.

Now by construction $R^1 \overset{\text{def.}}{=} \cup\{R_\alpha|\alpha<\kappa\}$ has for each α the property: if Σ_α has a solution in an extension of R^1 in K, then Σ_α has already

a solution in R^1.
However new systems of equations and inequalities over R^1 can arise. This difficulty is remedied as follows:
in the same way R^1 was constructed from $R^0 \overset{\text{def.}}{=} R$, one constructs R^2 from R^1, and with induction R^{n+1} from R^n ($n \in \mathbb{N}$). Then $R^* = \cup\{R^n | n \in \mathbb{N}\}$ is a K-existentially closed extension of R: this is because each finite system of equations and inequalities with coefficients in R^* has actually all its coefficients in R^n for some $n \in \mathbb{N}$, and so has a solution in R^{n+1} if it has a solution in a K-extension of R^*. □

(2.8) One usually considers classes which are elementary. Therefore we define a theory T to be inductive if Mod(T) is inductive, i.e. the union of each chain of models of T is a model of T.

Then for a theory T the following are equivalent ([Sh, p.77]):

(1) T is inductive.

(2) For each ascending chain $(A_n)_{n\in\mathbb{N}}$ of models of T its union $\cup\{A_n | n \in \mathbb{N}\}$ is a model of T.

(3) T has a $\forall\exists$-axiomatization.

If T is a theory, then we use the terminology 'T-existentially closed' instead of 'Mod(T)-existentially closed', or even 'existentially closed', if T is clear from context.
E_T is by definition the <u>class of T-existentially closed models of T.</u>
The proposition of (2.7) implies that each model of an inductive theory can be embedded in a member of E_T.
For instance, in the case that T is the theory of domains or the theory of fields, E_T is the class of algebraically closed fields, by (2.5)(a).

(2.9) *Definition*

A class K of $\mathcal{L}$-structures is said to <u>have an elimination theory</u>, or to <u>admit elimination</u> if each existential $\mathcal{L}$-formula is equivalent with an open $\mathcal{L}$-formula for all structures in K simultaneously; or equivalently: each $\mathcal{L}$-formula is equivalent with an open $\mathcal{L}$-formula, for all structures in K simultaneously.

Clearly, if K admits elimination, then the smallest elementary class of $\mathcal{L}$-structures containing K also admits elimination. Therefore we can restrict our attention to elementary classes in discussing the matter of elimination.
So, for a theory T, we say that T admits elimination if Mod(T) admits elimination.

Now, the goal is to deduce a model theoretic criterion for a theory to admit elimination, similar to the criterion given in (1.1) for linear elimination. Existential closedness replaces in this context faithful flatness. We also need a condition on the substructures of models of the theory. So let us discuss substructures.

(2.10) *Definition*

If T is an $\mathcal{L}$-theory, then $T_\forall$ is the set of all universal $\mathcal{L}$-sentences which follow from T. A straightforward diagram argument shows that an $\mathcal{L}$-structure is a model of $T_\forall$ iff it is a substructure of a model of T.

Example

If T is the theory of algebraically closed fields, then $T_\forall$ is the theory of domains.

If T has an axiomatization consisting of universal sentences, then T is called a universal theory.

By the above T is universal iff each substructure A of a model of T is a model of T (Łoś-Tarski).

Definition

Let T be a theory, $B \models T$ and $A \subset B$. Then B is called a prime extension of A (w.r.t. T) if B can be embedded over A in any model of T extending A. T is said to have PEP (= the prime extension property) if each substructure of a model of T has a prime extension.

Example

ACF, the theory of algebraically closed fields, has PEP: the prime extension of a domain is the algebraic closure of its quotient field.

The obvious analogue of the theorem in §1 is:

(2.11) *Theorem*

If T is a theory with PEP and each model of T is existentially closed, then T admits elimination.

Example

It was already verified that ACF satisfies the hypothesis of (2.11), so ACF admits elimination.

Most theories, which have been proved to admit elimination, indeed satisfy the hypothesis of (2.11). However, PEP is certainly not a necessary condition for admitting elimination, see for example Ch. II (3.8).

The concept of 'amalgamation' provides us with a necessary and sufficient condition.

(2.12) *Definition*

A theory T has AP (= the amalgamation property) if for any two models $\mathcal{B}, \mathcal{C}$ of T which extend a common model A of T there is a model $\mathcal{D}$ and embeddings $\mathcal{B} \to \mathcal{D}$, $\mathcal{C} \to \mathcal{D}$ such that the diagram

$$\begin{tikzcd}
 & \mathcal{B} \arrow[dr] & \\
A \arrow[ur, hook] \arrow[dr, hook] & & \mathcal{D} \\
 & \mathcal{C} \arrow[ur] &
\end{tikzcd}$$

commutes.

Proposition

Let T be an $\mathcal{L}$-theory such that either T has PEP or $T_\forall$ has AP, and let $\phi(y_1,..,y_n)$ be an $\mathcal{L}$-formula. Then the following are equivalent:

(*i*) ϕ is equivalent (w.r.t. T) with an open $\mathcal{L}$-formula

(*ii*) for any two models $A,\mathcal{B}$ of T with $A \subset \mathcal{B}$, and all $a_1,..,a_n \in |A|$: $A \models \phi(a_1,..,a_n) \Leftrightarrow \mathcal{B} \models \phi(a_1,..,a_n)$.

Proof

(*i*) $\Rightarrow$ (*ii*) is trivial.

(*ii*) $\Rightarrow$ (*i*): by an application of the theorem on constants [Sh, p.33], we reduce (*i*) to the case $n = 0$, i.e. ϕ is a sentence. Also, without loss of generality, we may assume that $\mathcal{L}$ has a constant.

Let $\Gamma = \{\theta \mid \theta$ is an open $\mathcal{L}$-sentence with $T \vdash \phi \to \theta\}$. Then it suffices to prove that $T \cup \Gamma \vdash \phi$. Suppose this is not the case. Then there is $A \models T \cup \Gamma \cup \{\neg\phi\}$.

Let $\mathcal{B}$ be the substructure of A generated by the empty set. Then the hypothesis on T clearly imply that $T \cup \mathrm{Diag}(\mathcal{B}) \vdash \neg\phi$. But every element of $|\mathcal{B}|$ is the interpretation of a variable free $\mathcal{L}$-term, hence there is open $\mathcal{L}$-sentence ψ with $T \vdash \psi \to \neg\phi$ and $B \models \psi$; but then $\neg\psi \in \Gamma$ and $A \models \psi$. Contradiction. $\square$

Note that this makes precise an argument in the proof of the result on linear elimination in §1.
The proposition also implies (2.11), because under the hypothesis of (2.11) existential formulas have property (ii) of the proposition.

By the same argument, the proposition implies one half of the following theorem.

(2.13) *Theorem*

The following are equivalent for a theory T:

(*i*) T admits elimination;

(*ii*) all models of T are existentially closed and $T_\forall$ has AP.

Proof

By the remark preceding (2.13) only (*i*) ⇒ (*ii*) has to be proved. That all models of T are existentially closed is trivial. Let A be a substructure of a model of T, and let B, C be two extensions of A, $B \subset B' \models T$ and $C \subset C' \models T$. Then the assumption that each $\mathcal{L}$-formula is equivalent with an open $\mathcal{L}$-formula, clearly implies:

$$(B',a)_{a\in|A|} \equiv (C',a)_{a\in|A|}.$$

Now an easy diagram argument implies that any two elementarily equivalent structures have a common elementary extension. Applying this to the preceding two structures gives that $T_\forall$ has AP. $\square$

(2.14) *Remarks*

(*a*) (2.13) will be used to prove the elimination results in Ch. II and III.

(b) Using (2.13) a second proof that ACF admits elimination can be given: if suffices to prove that the theory of domains has AP, and this will follow if the theory of fields has AP. So let L and M be two extension fields of a field K. Then $L \otimes_K M$ modulo any of its maximal ideals is a common K-extension of L and M.

(c) Actually in theorems (2.11) and (2.13) 'existentially closed' can be replaced by a weaker condition:
if A and B are $\mathcal{L}$-structures with $A \subset B$, we define A to be n-existentially closed in B ($n \in \mathbb{N}$) if each $\mathcal{L}(A)$-sentence $\exists x_1 .. \exists x_n \phi(x_1,..,x_n)$ with ϕ open, true in B, is also true in A.

If A and B are rings this means that every finite system of polynomial equations and inequalities in n variables over A which has a solution in B^n, also has a solution in A^n.
If T is a theory then an n-existentially closed model of T is a model of T which is n-existentially closed in each extension which is a model of T.

Claim

In (2.11) and (2.13) "existentially closed" can be replaced by "1-existentially closed".

This rests on the following trivial observation:
if each $\mathcal{L}$-formula $\exists x \phi(x,y_1,..,y_n)$ (ϕ open) is equivalent with an open $\mathcal{L}$-formula, then each existential $\mathcal{L}$-formula is equivalent with an open $\mathcal{L}$-formula (all this with respect to a certain $\mathcal{L}$-theory T).

Combining the claim with the fundamental theorem of Algebra one can give a simple proof of Tarski's Theorem, see [Rob2, p.44].

(2.15) Elimination is rather sensitive as to the language used. For instance, the theory of real closed fields can also be formulated in the language of rings: in the axioms for real closed fields every instance of an atomic formula "$t \leqslant d$" can be replaced by a formula "$\exists x(t+x^2 = d)$" (x a variable not occurring in t,d). But in the language of rings the theory of real closed fields does not admit elimination: the quantifier '$\exists x$' in '$\exists x(y = x^2)$' cannot be eliminated within the language of rings.
One can even prove the following (an analogue of theorem (1.2) of §1): if D is a domain such that $\{D\}$ admits elimination, then D is a finite or an algebraically closed field. For an easy proof, see [M., M.& v.d.D.].
A concept which is less language dependent, and often serves as a substitute for elimination, is <u>model completeness.</u>

(2.16) <u>*Definition*</u>
An $\mathcal{L}$-theory T is called <u>model complete</u> if for any two models A,B of T with $A \subset B$ and for each $\mathcal{L}$-formula $\phi(x_1,..,x_n)$ and all $(a_1,..,a_n) \in |A|^n$:

$$A \models \phi(a_1,..,a_n) \Leftrightarrow B \models \phi(a_1,..,a_n).$$

(if two structures A,B with $A \subset B$ have the above property, we write $A \prec B$, and say that <u>B is an elementary extension of A</u>, or <u>A an elementary substructure of B).</u>

Clearly, a theory admitting elimination is model complete, and a model complete theory is inductive by Tarski's Lemma, see [Sh, p.77].

The basic tool in establishing model completeness is

(2.17) *Robinson's Test.* <u>A theory T is model complete iff each model of T is existentially closed.</u>

Lemma

Let $A \subset B$. Then A is existentially closed in B iff B can be embedded over A in an elementary extension of A.

Proof

Let A be existentially closed in B. Then by the compactness theorem $\mathrm{Th}((A,a)_{a\in|A|}) \cup \mathrm{Diag}(B)$ has a model C and so $A \prec C$, $B \subset C$.
The other direction is trivial. □

Proof of Robinson's Test

Suppose each model of T is existentially closed and let A, B be models of T with $A \subset B$. Then, using the lemma, chains (A_n) and (B_n) of models of T are formed as indicated, with induction on n:

$$\begin{tikzcd}
A_0 = A \arrow[rr, "\prec"] \arrow[dr] & & A_1 \arrow[rr, "\prec"] \arrow[dr] \arrow[d, phantom, "\otimes"] & & A_2 \arrow[dr] \arrow[d, phantom, "\otimes"] & & {} \\
& B_0 = B \arrow[ur] \arrow[rr] \arrow[u, phantom, "\otimes"] & & B_1 \arrow[ur] \arrow[rr] \arrow[u, phantom, "\otimes"] & & B_2 \arrow[ur] &
\end{tikzcd}$$

Here the arrows indicate embeddings, the horizontal ones elementary embeddings. Now, by Tarski's Lemma (cf. [Sh, p.77])

$$\bigcup_{n=0}^{\infty} A_n = \bigcup_{n=0}^{\infty} B_n$$

is an elementary extension of A as well as of B, hence $A \prec B$.
The other direction is trivial. □

To appreciate the strength of the test, one cannot do better than read Robinson's beautiful paper [Rob3].

(2.18) There are two reasons for studying models of a theory admitting elimination.

First of all, because they may be important in themselves, like $\mathbb{C}$, and $\mathbb{R}$, and the elimination theory makes them more easily accessible.
But also - as in the case of p-adic fields - they reflect properties of more basic structures - like $\mathbb{Q}$ - , and one hopes to be able to prove results for these more basic, but very complicated structures, by studying extensions which are models of a theory admitting elimination, or at least models of a model complete theory.
This idea has been formalized in the concept of model companion.

(2.20) *Definition*

Let T be an inductive $\mathcal{L}$-theory.
Then an $\mathcal{L}$-theory $\tilde{T}$ is called a model companion of T if

(*i*) each model of $\tilde{T}$ is a model of T;

(*ii*) each model of T can be embedded in a model of T;

(*iii*) $\tilde{T}$ is model complete.

If also

(*iv*) T has AP

holds, then $\tilde{T}$ is called model completion of T.

The canonical example is, of course, ACF which is model completion of the theory of domains (as well as of the theory of fields).
Note that (2.13) can be reformulated as:
T admits elimination iff T is a model completion of a universal theory.
The basic result on model companions is

(2.21) Theorem

Let T be an inductive theory. Then T has at most one model companion. It has one iff E_T is an elementary class. In that case $\tilde{T}$ with $E_T = \mathrm{Mod}(\tilde{T})$ is the model companion of T.

Proof

Suppose that $\tilde{T}$ is model companion of T. Then it is easily seen that each model of $\tilde{T}$ belongs to E_T.
If $A \in E_T$, then $A \subset B \models \tilde{T}$ for some B. As A is existentially closed in B, A satisfies all $\forall\exists$-sentences which are true in B.
But $\tilde{T}$, as an inductive theory, has a $\forall\exists$-axiomatization; hence $A \models \tilde{T}$.
So $E_T = \mathrm{Mod}(\tilde{T})$.
On the other hand, suppose $E_T = \mathrm{Mod}(\tilde{T})$ for a theory $\tilde{T}$. Then by (2.7) and Robinson's Test $\tilde{T}$ is model companion of T. $\square$

Remark

The results and concepts mentioned in this section find their origin in ideas of Robinson, dating from the fifties. Some of the people who introduced more recent notions, such as AP and model companion, collaborated under the name of Eli Bers, see for instance [Ek.&Sab.]. Some other useful criteria for a theory to admit elimination were given by L. Blum and J. Shoenfield, see [Sa, p.89] and [Ki].
Instead of 'T admits elimination' some authors use the terminology 'T admits quantifier elimination' of 'T is substructure complete'.

§3. *Examples*

A number of (mostly wellknown) results on concrete theories will be listed, which are used in Ch. II and III. We will also make some terminological conventions.

(3.1) *Domains and fields* (References: [L3], [Rob2]).
The theories D and FL of domains and fields are formulated in the language of rings. Both have as their model completion the theory ACF of algebraically closed fields.
ACF admits elimination.

(3.2) *Ordered domains* (References: [Ar.&S.], [Rob2]).
For technical reasons (see §1 of Ch. III) an ordered domain is most conveniently defined as a structure (D,P) with D a domain, P a subset of D such that:

(*i*) $P+P \subset P$,

(*ii*) $P \cdot P \subset P$,

(*iii*) $P \cap (-P) = \{0\}$,

(*iv*) $P \cup (-P) = D$.

Associated with such a P (called an ordering) is a linear order $\leqslant_P$ on D:

$$x \leqslant_P y \overset{\text{def.}}{\Leftrightarrow} y-x \in P.$$

We use '$\leqslant$' instead of '$\leqslant_P$' if P is clear from context. We also write '$x < y$' for '$x \leqslant y$ and $x \neq y$'; '$x \geqslant y$' for '$y \leqslant x$', and '$x > y$' for '$x \geqslant y$ and $x \neq y$'.
So the language of ordered domains is the language of rings augmented by one unary predicate symbol P. The theory of ordered domains is called 'OD'. An ordering P on a domain D is uniquely extendable to an

ordering, called Q(P), on the quotient field Q(D); and if $\mathcal{D}$ = (D,P) $\models$ OD , we write Q($\mathcal{D}$) for (Q(D),Q(P)). The theory of ordered fields is OF. If (D,P) is an ordered domain, then a function f:A $\to$ D (A any set) is said to change sign (for the ordering P) if $\exists$a,b $\in$ A f(a) < 0 and f(b) > 0.

A real closed field is an ordered field such that every sign changing polynomial function in one variable (with coefficients in the field) has a root in the field.

In a real closed field the ordering is identical to the set of squares.

The theory of real closed fields is called RCF.

Fact: RCF admits elimination and is the model completion of OD and of OF.

Although it will not be needed, let me mention a recent theorem [M.,M.& v.d.D.]: RCF is the only theory in the language of OD and extending OD which admits elimination.

(3.3) *Valued fields* (References: [Ri1], [Rob2]).

A valued field is a field K together with a surjective map $v:K \to \Gamma \cup \{\infty\}$ with Γ an ordered abelian group s.t.

$v(a) = \infty \Leftrightarrow a = 0,$

$v(ab) = va + vb$,

$v(a+b) \geqslant \min(va,vb)$ (convention: $g+\infty = \infty$, $g \leqslant \infty$).

v is then called a (Krull) valuation on K, and is non-trivial if $\Gamma \neq \{0\}$.

Associated with v are: its valuation ring $V_v = \{k \in K | v(k) \geqslant 0\}$, the maximal ideal $M_v = \{k \in K | v(k) > 0\}$ of V_v, and its residue field $K_v = V_v/M_v$; $\Gamma = \Gamma_v$ is called its value group.

One notion especially is important:

Definition

A valued field (K,v) is called henselian if each polynomial $f(X) \in V_v[X]$, such that $\bar{f}(X) \in K_v[X]$ has a simple root $\alpha \in K_v$, has a root $a \in V_v$ with $\bar{a} = \alpha$.

An embedding $(K,v) \to (L,w)$ of valued fields is an embedding $K \to L$ together with an embedding $\Gamma_v \to \Gamma_w$ such that the diagram

$$\begin{tikzcd} K^\bullet \arrow[r] \arrow[d] & L^\bullet \arrow[d] \\ \Gamma_v \arrow[r] & \Gamma_w \end{tikzcd} \quad \text{commutes.}$$

Such an embedding induces embeddings $V_v \to V_w$ and $K_v \to L_w$. The embedding is called immediate if it induces isomorphisms $\Gamma_v \simeq \Gamma_w$ and $K_v \simeq L_w$.

Each valued field (K,v) has a henselization , i.e. a henselian field (K^h,v^h) together with an embedding $(K,v) \to (K^h,v^h)$ such that for each embedding $(K,v) \to (L,w)$ with (L,w) henselian there is a unique embedding $(K^h,v^h) \to (L,w)$ making

$$\begin{tikzcd} (K,v) \arrow[r] \arrow[d] & (K^h,v^h) \arrow[dl] \\ (L,w) & \end{tikzcd} \quad \text{commutative.}$$

$(K,v) \to (K^h,v^h)$ is immediate and $K^h|K$ is a separable algebraic extension.

For our purpose (see for example Ch. III) a valuation is best seen as defining a divisibility relation on the field. This point of view also generalizes to domains:

Definition

Let D be a domain. Then a linear divisibility relation (l.d. relation) on D is a binary relation div on D such that for all $a,b,c \in D$:

(i) (a div b and b div c) $\Rightarrow$ (a div c);

(ii) a div b or b div a;

(iii) (a div b and a div c) $\Rightarrow$ a div(b+c);

(iv) if $c \neq 0$, then (a div b $\Leftrightarrow$ ac div bc);

(v) not 0 div 1.

An l.d. relation div on the domain D induces a valuation ring V_{div} of the quotient field Q(D):

$$V_{div} = \{\tfrac{a}{b} \mid a,b \in D,\ b \neq 0,\ b \text{ div } a\},$$

and for the corresponding valuation v_{div} on Q(D) one has

$$v_{div}(a) \leqslant v_{div}(b) \Leftrightarrow a \text{ div } b \quad (\forall a,b \in D).$$

div $\mapsto V_{div}$ is easily seen to be a bijection of the set of l.d. relations on D onto the set of valuation rings of Q(D); its inverse is given by

$$V \mapsto \text{div}_V = \{(a,b) \in D\times D \mid v(a) \leqslant v(b)\},$$

where v is the valuation on Q(D) associated with V.

Clearly with an l.d. relation div on D a unique l.d. relation Q(div) on Q(D) corresponds, such that

$$(D,\text{div}) \subset (Q(D),Q(\text{div})).$$

So let us redefine a valued field as a field with an l.d. relation on it, and define a valued domain as a substructure of a valued field, i.e. as a domain with an l.d. relation.

It is easily seen that the model theoretic notion of embedding for valued fields corresponds with the algebraic one given above.
If (K,div) is a valued field, then v_K, Γ_K, V_K, M_K and $\bar{K}$ will denote the corresponding valuation, value group, valuation ring, its maximal ideal, and the residue field.
The theories of valued domains and valued fields are denoted by D_{val} and F_{val} (the language being the language of rings with an extra symbol div).

Let ACF_{val} be the theory of algebraically closed non-trivially valued fields.

Theorem

ACF_{val} admits elimination, hence is model completion of D_{val} and of F_{val}.

Proof

In §1 this was mentioned as a result of Robinson. But he actually only proved ACF_{val} to be model complete (this was all he needed to derive the decidability of ACF_{val}, and to classify its models up to elementary equivalence, see [Rob2]).
To get elimination, it will, by (2.11) and (2.17), suffice to prove:

ACF_{val} has PEP.

Let $K = (K, div_K)$ be a valued field; if div_K is non-trivial, then $(\tilde{K}, \widetilde{div})$ ($\tilde{K}$ = alg. closure of K, and $\widetilde{div}$ = any extension of div_K to $\tilde{K}$) is a prime extension of (K,div); this is due to the well-known fact that any two extensions of the valuation on K to valuations on a normal extension of K are conjugate over K; similarly, if div_K is trivial, then $(\widetilde{K(X)}, \widetilde{div})$ is a prime extension, X being trancendental and div an arbitrary extension of div_K to $K(X)$. □

In [M.,M.& v.d.D.] it is proved that ACF_{val} is the only theory in the language of valued domains, which extends the theory of non-trivially valued domains and admits elimination.

(3.4) *Prime extensions*

Before discussing the next examples, some more information has to be given on prime extensions.

Definition

Let T be a theory.

(a) T has PEP_{unique} (= 'the unique prime extension property') if T has PEP and any two prime extensions of a structure $A \models T_\forall$ are isomorphic over A.

(b) T has $PEP_{minimal}$ (= 'the minimal prime extension property') if T has PEP and each $A \models T_\forall$ has a prime extension which does not properly contain any other prime extension of A (a so called minimal prime extension).

(c) T has $PEP_{universal}$ if each $A \models T_\forall$ has an extension $\bar{A} \models T$ which can be embedded uniquely over A in each extension $B \models T$ of A. Such an $\bar{A}$ is clearly defined up to isomorphism over A, and is a prime extension of A; $\bar{A}$ is called the universal prime extension of A.

Examples

(1) The theories FL, RCF, and the theory of henselian valued fields have $PEP_{universal}$.

For FL the universal prime extension of $D \models FL_\forall$ is the quotient field Q(D); for RCF the universal prime extension of an ordered domain $\mathcal{D}$ is the real closure of $Q(\mathcal{D})$; for the theory of henselian valued fields (note that the class of henselian valued fields is elementary) the universal prime extension of (D,div) is the henselization of (Q(D),Q(div)) .

(2) ACF <u>and</u> ACF_{val} <u>have</u> $PEP_{minimal}$ <u>but not</u> $PEP_{universal}$.
The minimal prime extension of a domain D (with respect to ACF) is of course the algebraic closure of Q(D), and in general this algebraic closure has non-trivial D-automorphisms, so cannot be a universal prime extension of D.
For ACF_{val}, see the proof of the theorem in (3.3).

(3) <u>The theory of differentially closed fields of char. 0 and the theory of atomless boolean algebras both have</u> PEP_{unique} <u>but not</u> $PEP_{minimal}$.

(4) There are also examples known of theories (even admitting elimination), which have PEP but not PEP_{unique}.

Clearly: $\underline{PEP_{universal} \Rightarrow PEP_{minimal} \Rightarrow PEP_{unique} \Rightarrow PEP}$, and the examples show that no arrow can be reversed, not even for theories admitting elimination.
Also the following is easy:
if the theory T has $PEP_{minimal}$ and $\tilde{A}$ is prime extension of $A \models T_\forall$, then $\tilde{A}$ does not contain properly any extension of A which is a model of T.

(3.5) *Algebraic elements*

The reader will have noted that in some cases a prime extension can be obtained by adjoining 'algebraic' elements. Model theoretic notions of 'algebraic' have been defined by A. Robinson (1951), B. Jónsson

(1962), M. Morley (1965) and others. Their notions have been compared by P. Bacsich in [Bac]. From his paper I take the following definitions.

First some notation and terminology: "$\exists^{\leq n} x\phi$" is shorthand for the formula expressing that for at most n x's ϕ holds.
A <u>primitive</u> formula is an existential formula of the form $\exists x_1 .. \exists x_n \phi$ with ϕ a conjunction of atoms and negations of atoms.

Definition

Let T be a theory and $A \subset B \models T$, $n \in \mathbb{N}$;

(*i*) an A-formula $\phi(x)$ is called <u>algebraic of degree</u> $\leq n$ over A, if $\phi(x)$ is primitive and $T \cup \mathrm{Diag}(A) \vdash \exists^{\leq n} x\phi(x)$;
note that the latter means: for each extension $C \models T$ of A $C \models \exists^{\leq n} x\phi(x)$,

(*ii*) $b \in |B|$ is called <u>Robinson-algebraic of degree</u> $\leq n$ over A in B, if $B \models \phi(b)$ for some A-formula $\phi(x)$ which is algebraic of degree $\leq n$ over A,

(*iii*) B is <u>Robinson-algebraic over A</u>, if each $b \in |B|$ is Robinson-algebraic over A in B,

(*iv*) A is <u>Robinson-algebraically closed</u> if there is no extension $C \models T$ of A with $c \in |C| \setminus |A|$ which is Robinson-algebraic over A in C,

(*v*) $b \in |B|$ is called <u>n-potent</u> over A in B if for each extension $C \models T$ of A there are at most n elements of $|C|$ which are the image of b under an A-embedding of B into C.

The proofs given in [Bac] imply:

Theorem

Let T be an $\mathcal{L}$-theory, $A \subset B \models T$, $b \in |B|$, $n \in \mathbb{N}$.

Then the following are equivalent:

(a) b is Robinson-algebraic of degree $\leqslant n$ over A in B.

(b) b is n-potent over A in B.

(c) There is a primitive $\mathcal{L}$-formula $\Theta(x, z_1, \ldots, z_k)$ such that $T \vdash \forall z_1 \ldots z_k \exists^{\leqslant n} x \Theta(x, z_1, \ldots, z_k)$ and there is $\bar{a} \in |A|^k$ with $B \models \Theta(b, \bar{a})$.

Moreover, the set of all $b \in |B|$ which are Robinson-algebraic over A in B is the universe of a substructure of B.
If B is T-existentially closed, then B is Robinson-algebraically closed.

One of the connections with prime extensions is:

Proposition

Let T be a theory admitting elimination and suppose each $A \models T_\forall$ has an extension $\tilde{A} \models T$ which is Robinson-algebraic over A. Then T has $PEP_{minimal}$ and $\tilde{A}$ as above is the prime extension of A.
If moreover $\tilde{A}$ as above does not have a non-trivial A-automorphism, for all $A \models T_\forall$, then T has $PEP_{universal}$.

Proof

Let $A \subset B \models T$. First note that because B is T-existentially closed, B is also Robinson-algebraically closed by the preceding theorem.
Because $T_\forall$ has AP by (2.13), there is $C \models T$ with $B \subset C$ and an embedding $f: \tilde{A} \to C$ such that the diagram

$$\begin{tikzcd} & B \arrow[dr, hook] & \\ A \arrow[ur, hook] \arrow[dr, hook] & & C \\ & \widetilde{A} \arrow[ur, hook, "f"'] & \end{tikzcd}$$ commutes.

Then $a \in |\widetilde{A}|$ is Robinson-algebraic over A in $\widetilde{A}$, and so $f(a) \in |C|$ is Robinson-algebraic over A in C, so $f(a)$ is Robinson-algebraic over B in C, hence $f(a) \in |B|$.

As $f(|\widetilde{A}|) \subset |B|$, this shows that $\widetilde{A}$ is a prime extension of A.

If $A \subset B \subset \widetilde{A}$ and $B \models T$, then as above each $a \in |\widetilde{A}|$ is Robinson-algebraic over B in $\widetilde{A}$, hence belongs to $|B|$, so $B = \widetilde{A}$. So T has $PEP_{minimal}$.

The last part is proved as follows: let $A \subset B \models T$ and suppose f,g are two A-embeddings of $\widetilde{A}$ into B. Then, if $c \in |\widetilde{A}|$, $g(c)$ is, as above, Robinson-algebraic over A, hence over $f(\widetilde{A})$, in B. Because $f(\widetilde{A}) \models T$, this implies $g(c) \in |f(\widetilde{A})|$. So $g(\widetilde{A}) \subset f(\widetilde{A})$, and by symmetry $g(\widetilde{A}) = f(\widetilde{A})$. But then $g^{-1} \circ f$ is an A-automorphism of $\widetilde{A}$, which by assumption implies $g = f$. $\square$

Remark

If a theory T has $PEP_{universal}$, then the prime extension $\widetilde{A}$ of any $A \models T_\forall$ is indeed Robinson-algebraic over A. This is because each $b \in |\widetilde{A}|$ is clearly 1-potent over A in $\widetilde{A}$.

(3.6) *p-adic fields* (References: [Ax&Ko], [Ko], [M1]).

Let p be a prime number. A p-valued field is a valued field of char. 0 with residue field $\mathbb{F}_p$ and $v(p) = 1$ (by notation) as the smallest positive element of the value group. So $\mathbb{Q}$ with its p-adic valuation is a p-valued field.

A p-adically closed field is a p-valued field without any proper

algebraic (valued) extension which is also p-valued, or equivalently it is a henselian p-valued field, whose value group Γ satisfies $\#(\Gamma/_{n\Gamma}) = n$, for all $1 \leqslant n \in \mathbb{N}$.
So $\mathbb{Q}_p$, and its valued subfield of algebraic numbers (= the henselization of $\mathbb{Q}$ with its p-adic valuation) are p-adically closed.
Since the work of Ax-Kochen and Eršov it was known that the theory of p-adically closed fields is complete and model complete. Later a special study of these valued fields was made by Kochen in [Ko] (and also by P. Roquette), who found many similarities with ordered and real closed fields.
However, the theory of p-adically closed fields does not admit elimination in the language of valued fields.
Also a p-valued field has in general no prime extension (with respect to the theory of p-adically closed fields), although it has one - namely its henselization- if $\#(\Gamma/_{n\Gamma}) = n$ for all $n \in \mathbb{N}$, $n \geqslant 1$, where Γ is its value group.

A natural remedy to the first defect was given by A. Macintyre in [M1]: define for each p-adically closed field $K = (K,\mathrm{div})$ and for each $n \in \mathbb{N}$ with $2 \leqslant n$ a unary predicate P_n^K by:

$$P_n^K(a) \text{ iff } a \in K^n = \{k^n | k \in K\}.$$

Let pCF be the theory of p-adically closed fields formulated in the language of valued fields augmented by new unary predicate symbols $\underline{P}_n$ $(2 \leqslant n \in \mathbb{N})$, with the obvious defining axioms

$$\forall x(\underline{P}_n(x) \leftrightarrow \exists y(y^n = x)),$$

added to the theory. Macintyre proved: pCF admits elimination.

Macintyre did not treat the question of prime extensions for pCF in [M1].

Theorem

pCF has $PEP_{universal}$.

Proof

Let $A = (D, div, P_2, P_3, ..) \models (pCF)_\forall$. Note first (for later use) that $Q(D)$ can be uniquely expanded to a model $Q(A) = (Q(D), Q(div), ...)$ of $(pCF)_\forall$, with $A \subset Q(A)$.

Let $A \subset B \models$ pCF and define $\tilde{A}$ as the substructure of B whose universe is the set of all $b \in |B|$ which are algebraic over $Q(D)$.

Claim $\tilde{A} \models$ pCF.

As the underlying field of $\tilde{A}$ is algebraically closed in the underlying field of B, $\tilde{A}$ is clearly henselian as a valued field; let now $0 \neq b \in |\tilde{A}|$ and $2 \leqslant n \in \mathbb{N}$. Then, because $0, 1, 2.1, ..., (n-1).1$ are a complete set of representatives of Γ mod $n\Gamma$, where Γ = value group of B, there is $0 \leqslant i < n$ with $v(bp^i) \in n\Gamma$ (v the valuation of B), so for some $0 \neq u \in |B|$ $v(bp^i u^n) = 0$, hence by Fact 1 in [M1] $bp^i u^n k^{-1} \in P_n^B$ for some $0 \neq k \in \mathbb{N}$, so $bp^i k^{-1} \in P_n^B$, so $bp^i k^{-1}$ is also an n^{th} power in $\tilde{A}$, which implies $v(b) \equiv j.1 \bmod n\Delta$ for some $0 \leqslant j < n$, Δ being the value group of $\tilde{A}$, hence $\#(\Delta/_{n\Delta}) = n$.

That $P_n^{\tilde{A}}$ is the set of n^{th} powers in $\tilde{A}$ follows because $\tilde{A}$ is algebraically closed in B.

So the claim is proved.

Now $\tilde{A}$ is clearly Robinson-algebraic over A. Then by the proposition of (3.5) the proof reduces to showing: $\tilde{A}$ has no non-trivial A-automorphism.

Suppose σ is such a non-trivial A-automorphism of $\tilde{A}$.

Take a maximal substructure

$$K = (K, div_K, P_2^K, P_3^K) \text{ of } \tilde{A} = (L, div_L, P_2^L, P_3^L, ...)$$

on which σ is the identity.

Then for all $n \in \mathbb{N}$, $n \geqslant 2$: $P_n^K = K^n$. Suppose $a \in P_n^K \setminus K^n$, and let $b \in |\widetilde{A}|$ be an n^{th} root of a. Then, because $b \notin K$, $\sigma(b) \neq b$ and $\sigma(b)\cdot b^{-1} = \rho \neq 1$ is an n^{th} root of unity. Then by Fact 2 in [M1] $\rho \notin L^m$ for some $2 \leqslant m \in \mathbb{N}$. But as in the proof of the claim above one finds rational $q \neq 0$ with $qb \in L^m = P_m$, so $\sigma(qb) \in L^m$ and $\sigma(qb)(qb)^{-1} = \rho \in L^m$, contradiction.

Also (K,div_K) is clearly a henselian valued field, by the universal property of the henselization and the definition of K.

Finally, using $P_n^K = K^n$, one shows just as in the proof of the claim above, that $\#(\Gamma_K/n\Gamma_K) = n$, for all $n \in \mathbb{N}$, $n \geqslant 2$.

So $K \models \mathrm{pCF}$, and because $\widetilde{A}$ is minimal prime extension of A, one has $K = \widetilde{A}$, contradicting $\sigma \neq 1$. □

Concluding remarks

(*a*) Some extra notation: pFL denotes the theory of models of PCF whose underlying domain is a field.

From the proof of the theorem one obtains also:

(*b*) Each p-adically closed field (K,div_K) has a unique expansion -namely $(K,\mathrm{div}_K,K^2,K^3,\dots)$- to a model of pFL.

(*c*) From (*b*) one gets that $\mathbb{Q}$ has a unique expansion to a model of pFL, namely that expansion which makes it a substructure of $(K,\mathrm{div}_K,K^2,K^3,\dots)$ where (K,div_K) is the henselization of $\mathbb{Q}$ endowed with its p-adic valuation.

(*d*) As far as I know there is not yet an explicit description of the elimination theory of pCF.

(3.7) *π-valued fields* (References: [Ax&Ko]).

Let π be a symbol, and define a π-valued field as a structure (K,div_K,π) with (K,div_K) a valued field with residue field of char. 0

and $\pi \in K$ such that $v(\pi) = 1$ (by convention) is the smallest positive element of the value group.

Define a $\underline{\pi}$-adically closed field as a $\underline{\pi}$-valued field which has no proper algebraic ($\underline{\pi}$-valued) extension.

Equivalently, a $\underline{\pi}$-adically closed field is a $\underline{\pi}$-valued field which is henselian, whose value group Γ satisfies $\#(\Gamma/_{n\Gamma}) = n$, $(1 \leqslant n \in \mathbb{N})$, and whose residue field is algebraically closed.

So $(\mathbb{C}((\pi)), \mathrm{div}, \pi)$, where div belongs to the valuation ring $\mathbb{C}[\![\pi]\!]$, is a $\underline{\pi}$-adically closed field.

By the results of Ax-Kochen and Eršov the theory of $\underline{\pi}$-adically closed fields is complete and model complete.

But again this theory has the same defects as the theory of p-adically closed fields formulated in the language of valued fields.

So define for each $\underline{\pi}$-adically closed field $\mathcal{K} = (K,\dots)$ the predicates $P_n^{\mathcal{K}} (2 \leqslant n \in \mathbb{N})$ by $P_n^{\mathcal{K}} = K^n$, and extend the language of valued fields by adding a constant $\underline{\pi}$ and the unary predicate symbols $\underline{P}_n (2 \leqslant n \in \mathbb{N})$.

Let $\underline{\pi}$CF be the theory of $\underline{\pi}$-adically closed fields formulated in this language, with the obvious defining axioms for $\underline{P}_n$. Then one can show along the lines of Macintyre's proof of Theorem 1 in [M1]:

$\underline{\pi}$CF admits elimination

(Elsewhere I will give a more elementary proof of this result, than the one obtained by following Macintyre's method.)

The same reasoning as in the proof of the claim in the theorem of (3.6), augmented by an easy argument on the residue field, shows:

$\underline{\pi}$CF has $\mathrm{PEP}_{\mathrm{minimal}}$.

Of course $\underline{\pi}$CF does not have $\mathrm{PEP}_{\mathrm{universal}}$:

$(\mathbb{C}((\pi)), \mathrm{div}, \pi, \mathbb{C}((\pi))^2 \dots)$

has a non-trivial automorphism over its substructure

$(\mathbb{R}((\pi)), \mathrm{div}', \pi, P_2, \dots)$.

Concluding remarks

(a) By Hensel's lemma it is clear that
$P_n = K^n = \{x \in K \mid v(x) \in n \cdot \Gamma_K \cup \{\infty\}\}$ $(2 \leqslant n \in \mathbb{N})$ for each $(K, \mathrm{div}_K, P_2, \ldots) \models \underline{\pi}\mathrm{CF}$.

(b) $\underline{\pi}$FL is by definition the theory of models of $(\underline{\pi}\mathrm{CF})_\forall$ whose underlying domain is a field.

(c) Each $\underline{\pi}$-adically closed field has a unique expansion to a model of $\underline{\pi}$FL.

CHAPTER II *Fields with n orderings*

In this chapter the model theory of fields, or rather domains, with a given number of orderings will be treated.
Not so much for its own sake, as well in order to demonstrate techniques and to use results which also play an important role in Ch. III.

§1. *The model companion*

(1.1) *Definition*

Let $n \in \mathbb{N}$. An n-ordered domain is a structure $\mathcal{D} = (D, P_1, .., P_n)$ with D a domain and P_i an ordering on D.
OD_n is the theory of n-ordered domains.
Similarly an n-ordered field is defined, and OF_n is the theory of n-ordered fields. See Ch. I (3.2) for the notion of ordered domain as used here.

The main result of this section is:

(1.2) *Theorem*

OD_n *has a model companion* $\overline{OD}_n$, *whose models are the models* $(K, P_1, .., P_n)$ *of* OF_n *satisfying:*

(α) P_i *and* P_j *induce different (interval) topologies on K, for all* $1 \leq i < j \leq n$.

(β) *For each irreducible* $f(T,X) \in K[T,X]$ *and* $a \in K$ *such that* $f(a,X)$ *changes sign on K with respect to each of the orderings* P_i, *there exists* $(c,d) \in K \times K$ *with* $f(c,d) = 0$.

So the (universal) axioms of OD_n, together with the field axiom

$\forall x \neq 0\ \exists y(xy=1)$, and (α),(β) give us an axiomatization of $\overline{OD}_n$.
That (α) can be formulated in the language of OD_n is seen as follows. A basis of neighbourhoods of 0 in an ordered field (K,P) is given by the sets $(-\varepsilon,\varepsilon)$ with $0 < \varepsilon \in K$. So we can express in the language of OD_n that some neighbourhood of 0 in the P_i-topology is not a neighbourhood of 0 in the P_j-topology, or conversely.
Orderings inducing different topologies are also called independent orderings.

(1.3) To prove the theorem it suffices by Ch. I (2.21) to show:

A Each existentially closed model of OD_n is an n-ordered field satisfying (α) and (β) of (1.2).

B Each model of OF_n satisfying (α) and (β) of (1.2) is existentially closed.

If $n = 0$ (1.2) is evidently true, as (α) becomes vacuous and (β) only says that K is an algebraically closed field. So for $n = 0$ we get the old result that ACF is the model companion of the theory of domains. Therefore we shall assume $n \geqslant 1$ in the following (although the case $n = 1$ gives nothing new too: $OD_1 = OD$, so $\overline{OD}_1 = RCF$).

The next three lemmas together imply part *A*.

(1.4) *Lemma*

Each n-ordered domain can be embedded in an n-ordered field.

Proof

If $(D,P_1,..,P_n)$ is an n-ordered domain, then

$$(D,P_1,..,P_n) \subset (Q(D),Q(P_1),..,Q(P_n)) \models OF_n. \quad \square$$

(1.5) In order to motivate the next lemma, it is useful to have an equivalent formulation of (α) of (1.2). This formulation is provided by the following fact: two orderings P and Q on a field K are independent iff each neighbourhood of 0 in the P-topology and each neighbourhood of 1 in the Q-topology have non-empty intersection. This follows from an approximation theorem ((1.7)) which we will use very often. The following notion is due to I. Kaplansky, see [Ka].

(1.6) *Definition*

Let K be a field. A V-topology on K is a Hausdorff ring topology on K, such that if any two subsets A and B of K are bounded away from 0 (i.e. disjoint with a 0-neighbourhood) then also AB is bounded away from 0.

A theorem, proved independently by I. Fleischer and Kowalsky-Dürbaum says that a topology on a field K is a V-topology iff it is the topology induced by an absolute value function $K \to \mathbb{R}$, or the valuation topology induced by a (Krull) valuation on K. Of course an interval topology induced by an ordering is also a V-topology. Note that V-topologies are field topologies. For a very short proof of the next theorem, see [P.&Z.].

(1.7) *Approximation Theorem for V-topologies* (A.S. Stone).
Let K be a field and $\tau_1,\ldots,\tau_m$ be different V-topologies on K, and let for each $1 \leqslant i \leqslant m$ U_i be a non-empty τ_i-open subset of K. Then $U_1 \cap\ldots\cap U_m \neq \emptyset$.

In the following, if an n-ordered domain $(D,P_1,\ldots,P_n)$ is given, I will write $\leqslant_i, <_i$, etc. to refer to the linear order on D defined by

P_i $(1 \leqslant i \leqslant n)$.

(1.8) *Lemma*

Let $K = (K, P_1, .., P_n) \models OF_n$ and let $1 \leqslant i < j \leqslant n$ and $0 <_i \varepsilon_1 \in K$ and $0 <_j \varepsilon_2 \in K$. Then K can be embedded into some $\mathcal{L} = (L, Q_1, .., Q_n) \models OF_n$ with an $x \in L$ satisfying:

$$-\varepsilon_1 <_i x <_i \varepsilon_1 \text{ and } 1-\varepsilon_2 <_j x <_j 1+\varepsilon_2 .$$

Proof

We put $L = K(X)$ and $x = X$ and extend $P_1, .., P_n$ to orderings $Q_1, .., Q_n$ on L such that X is positive in the Q_i-ordering and infinitesimal with respect to (K, P_i), i.e. $0 <_i X <_i \varepsilon$ for all $0 <_i \varepsilon \in K$, and $X-1$ is infinitesimal in the Q_j-ordering with respect to (K, P_j). □

(1.9) For the next lemma (and also for later developments) recall that, given an ordered field (K, P) and an algebraic extension $K(\alpha)$ of K with $f(X) \in K[X]$ as minimum polynomial of α, P can be extended in precisely r ways to an ordering on $K(\alpha)$, where r is the number of roots of $f(X)$ in the real closure $(\overline{K}, \overline{P})$ of (K, P): if $\alpha_1 < \ldots < \alpha_r$ are these roots, then $\alpha \mapsto \alpha_k$ gives a K-embedding of $K(\alpha)$ into $\overline{K}$ which induces an ordering P_k on $K(\alpha)$, and $P_1, .., P_r$ are exactly the r different extensions of P to $K(\alpha)$.

(1.10) *Lemma*

Let $K = (K, P_1, .., P_n) \models OF_n$ and $f(T, X) \in K[T, X]$ be irreducible and $a \in K$ such that $f(a, X)$ changes sign on K w.r.t. P_i, for each $1 \leqslant i \leqslant n$. Then K can be embedded in an $\mathcal{L} = (L, Q_1, .., Q_n) \models OF_n$ with $(c, d) \in L \times L$ such that $f(c, d) = 0$.

Proof

Let t be transcendental over K and extend the ordering P_i to an ordering P_i' on K(t) such that t-a is infinitesimal with respect to (K,P_i), and do this for $1 \leqslant i \leqslant n$. Then the polynomial f(t,X) $f(t,X) \in K(t)[X]$ changes sign on K(t) w.r.t. each ordering P_i', so f(t,X) has a root in the real closure of $(K(t),P_i')$, $1 \leqslant i \leqslant n$. But as $f(t,X) \in K(t)[X]$ is irreducible, this implies that P_i' can be extended to an ordering Q_i on the field $K(t)[X]/_{(f(t,X))}$. Put $L = K(t)[X]/_{(f(t,X))}$ and $c = t$, $d = X \bmod f(t,X)$, and we have $f(c,d) = 0$ as required. □

Using the definition of existential closedness (Ch. I (2.2) and (2.6)) we see that (1.4), (1.8) and (1.10) imply part *A* of (1.3). For part *B* we need some more lemmas.

(1.11) Lemma

Let $\mathcal{K} = (K,P_1,\ldots,P_n) \models OF_n$ satisfy (β) of (1.2). Then each $f(X) \in K[X]$ of odd degree has a root in K, and $P_1 \cap \ldots \cap P_n = K^2$.

Proof

Replacing f by a suitable irreducible factor, we may assume f to be irreducible. Then use (β) and the fact that an odd degree polynomial over an ordered field changes sign with respect to the ordering. If $a \in (P_1 \cap \ldots \cap P_n) \setminus K^2$, then $X^2 - a \in K[X]$ is irreducible and changes sign w.r.t. P_i, for each $1 \leqslant i \leqslant n$. So it has a root in K by (β), contradiction. □

(1.12) Lemma

Let K be a field in which every odd degree polynomial of K[X] has a root. Then there is for each finite separable extension L of K a chain of fields:

$$K = L_0 \subset L_1 \subset \ldots \subset L_m = L \text{ with } [L_{i+1} : L_i] = 2, \ (0 \leqslant i < m).$$

Proof (from [Ri2, p.153]):
Let M be a finite Galois extension of K containing L. Suppose $[M : K]$ has an odd factor >1. Then any 2-Sylow subgroup H of $Gal(M|K)$ is a proper subgroup of odd index. Hence the fixed field of H is a proper odd degree extension of K, so there is an irreducible $f \in K[X]$ of odd degree >1, contradicting the hypothesis of the lemma.
Hence $Gal(M|K)$ is a 2-group and $Gal(M|L) \subset Gal(M|K)$.
By [Ri2, p.53] there exists a chain of subgroups

$Gal(M|L) = G_m \subset G_{m-1} \subset \ldots \subset G_0 = Gal(M|K)$ with $(G_i : G_{i+1}) = 2$, $0 \leqslant i < m$, giving rise, by the fundamental theorem of Galois theory to a chain of subfields as described. □

(1.13) Lemma
Let (K,P) be an ordered field such that each $f(X) \in K[X]$ of odd degree has a root in K. Then: K is dense in $\overline{K}$ (where $(\overline{K},\overline{P})$ is the real closure of (K,P)), iff K^2 is dense in $P = \{x \in K | x \geqslant 0\}$.

Proof
(⇒): Let $0 < a \in K$ and $0 < \varepsilon \in K$. Then we have to prove that $(a,a+\varepsilon) \cap K^2 \neq \emptyset$. By assumption we can find $0 < \delta \in K$ with $2\delta\sqrt{a}+\delta^2 < \varepsilon$ and $b \in K$ with $\sqrt{a} < b < \sqrt{a}+\delta$ (where the positive square root is taken). Then $b^2 \in (a,a+\varepsilon)$.
(⇐): By lemma (1.12) it suffices to show that for any quadratic extension $K(\sqrt{a}) \subset \overline{K}$ of K, K is dense in $K(\sqrt{a})$ and that $K(\sqrt{a})$ inherits the properties that each odd degree polynomial over it has a root in it, and that its set of squares is dense in its set of nonnegative

elements.

Each odd degree polynomial over $K(\sqrt{a})$ has an irreducible factor of odd degree, which is necessarily of degree 1: otherwise $K(\sqrt{a})$ has an extension of odd degree >1, hence K has a finite extension of degree not a power of 2, contradicting (1.12).

If K is dense in $K(\sqrt{a})$, then the density of K^2 in P implies easily the density of $(K(\sqrt{a}))^2$ in $\tilde{P} \cap K(\sqrt{a})$.

Finally, to prove that K is dense in $K(\sqrt{a})$ it suffices, by the cofinality of K in $K(\sqrt{a})$, to show that $(\sqrt{a}-\varepsilon,\sqrt{a}+\varepsilon) \cap K \neq \emptyset$ for each $0 < \varepsilon \in K$. Choose $0 < x,y \in K$ with $0 < \frac{1}{2}a < x^2 < a < y^2$ and $y^2-x^2 < \varepsilon\sqrt{a}$. Then $0 < x < \sqrt{a} < y$ and $y-x = (y^2-x^2)/(y+x) < \varepsilon\sqrt{a}/y+x < \varepsilon$, hence $x,y \in (\sqrt{a}-\varepsilon,\sqrt{a}+\varepsilon)$. □

Remark

Prof. A. Prestel indicated to me an easy topological proof of (1.13): if K^2 is dense in P and each odd degree polynomial over K has a root in K, then also the <u>completion</u> $(\hat{K},\hat{P})$ of (K,P) satisfies these properties, and this implies that $(\hat{K},\hat{P})$ is real closed, and as K is dense in $\hat{K}$, K is dense in the real closure of (K,P). However, to make this reasoning precise, one needs a few properties of complete V-topological fields, see Ch. III, (1.18).

(1.14) *Corollary*

<u>Let</u> $\mathcal{K} = (K,P_1,..,P_n) \models OF_n$ <u>satisfy (α) and (β) of (1.2). Then</u> (K,P_i) <u>is dense in its real closure, for all</u> $1 \leqslant i \leqslant n$.

Proof

By (1.11) and (1.13) it suffices to show that $P_1 \cap ... \cap P_n$ is dense in the set P_i, with respect to the P_i-topology on K. So let $0 <_i a <_i b$, $a,b \in K$; then by (α) and the Approximation Theorem (1.7)

there is $x \in K$ with $a <_i x <_i b$ and $0 <_j x$ for all $j \neq i$.
Hence $x \in P_1 \cap \ldots \cap P_n$. □

In the next lemma (α) of (1.2) is generalized to polynomials in more than 2 variables. The essential tool is Hilbert's irreducibility theorem as exposed in [Roq], see also [L2, Ch.VIII].

(1.15) *Definition*

Let K be a field and $f = f(T, X_1, .., X_k) \in K(T)[X_1, .., X_k]$ be irreducible ($k \geqslant 1$). The basic Hilbert set over K associated to f is defined as the set of all $t \in K$ for which $f(t, X_1, .., X_k) \in K[X_1, .., X_k]$ is defined and irreducible.
A Hilbert set over K is the intersection of a finite number of basic Hilbert sets over K.
Hilbert's irreducibility theorem is said to hold for K, or K is a Hilbertian field, if each Hilbert set over K is non-empty.

No two sources in the literature seem to agree over the definition of Hilbert set. Anyway, the Hilbertian fields as defined above are the same as those of [Roq] and [L2, Ch. VIII], as is easily checked.
An elegant and useful nonstandard interpretation of Hilbert's irreducibility theorem is given in [Roq]: let K be a field, $^*K$ its nonstandard extension in an enlargement of a suitable structure containing K, and define an element $t \in {}^*K$ to be a Hilbert element over K if $t \notin K$ and $K(t)$ is algebraically closed in $^*K$. Then it is proved in [Roq] that K is Hilbertian iff there exists a Hilbert element over K.

Examples

$\mathbb{Q}$ is a Hilbertian field; each rational function field $F(Z)$ is Hilbertian; a finitely generated field extension of a Hilbertian field is Hilbertian; a field having a non-trivial Henselian valuation is not Hilbertian.

The following result, which may be interesting in itself, is needed in §3.

(1.16) *Theorem*

Let $\tau_1,\ldots,\tau_n$ be different non-discrete V-topologies on a Hilbertian field K and let for each $1 \leqslant i \leqslant n$ U_i be a non-empty open subset of K and let H be a Hilbert set over K. Then $U_1 \cap \ldots \cap U_n \cap H \neq \emptyset$.

Proof

I will freely use concepts and results from [Roq] and [P.&Z.].
The above theorem states that a certain conjunction of local sentences holds for $(K,\tau_1,\ldots,\tau_n)$, so we may assume that $(K,\tau_1,\ldots,\tau_n)$ is ω-complete. Hence τ_i is the topology induced by a non-trivial valuation $v_i : K^{\cdot} \to G_i$, G_i an ordered abelian group. Let t be a Hilbert element over K and take $x \in K$ with $v_i(x) \geqslant 0$ if $v_i(t) < 0$, while $v_i(x) < 0$ if $v_i(t) \geqslant 0$. Then $u = (t+x)^{-1}$ is also a Hilbert element, and satisfies $v_i(u) > 0$ for all $1 \leqslant i \leqslant n$.
Take for each $1 \leqslant i \leqslant n$ $a_i \in U_i$ and $g_i \in G_i$ with $\{y \in K \mid v_i(y-a_i) \geqslant g_i\} \subset U_i$, and choose $y \in K$ such that for all $1 \leqslant i \leqslant n$ $v_i(y-a_i) \geqslant g_i$, and $0 \neq z \in K$ such that for all $1 \leqslant i \leqslant n$ $v_i(z) \geqslant g_i$.
Then $w = y+zu$ is a Hilbert element with $v_i(w-a_i) \geqslant g_i$ for all $1 \leqslant i \leqslant n$, so $w \in U_1 \cap \ldots \cap U_n$. Apply now the generalized Gilmore-Robinson theorem in [Roq]. $\square$

(1.17) Lemma

Let $(K,P_1,..,P_n) \models OF_n$ satisfy (α) and (β) of (1.2), and let $f = f(T_1,..,T_m,X) \in K[T_1,..,T_m,X]$ $(m \geqslant 1)$ be irreducible and $(a_1,..,a_m) \in K^m$ be such that $f(a_1,..,a_m,X)$ changes sign on K for each ordering P_i.
Then f has a zero $(c_1,..,c_m,d) \in K^{m+1}$.

Proof

With induction to m. Suppose the statement is true for $m \geqslant 1$, and let $f = f(T_1,..,T_m,T_{m+1},X) \in K[T_1,..,T_{m+1},X]$ be irreducible and $(a_1,..,a_{m+1}) \in K^{m+1}$ be such that $f(a_1,..,a_{m+1},X)$ changes sign on K for each P_i.
Take for each $1 \leqslant i \leqslant n$ a sufficiently small P_i-neighbourhood U_i of a_{m+1} such that for all $a_{m+1}' \in U_i$ $f(a_1,..,a_m,a_{m+1}',X)$ still changes sign on K for the ordering P_i.
Next choose infinite subsets A and B of K such that for all $t_0 \in A$, $t_1 \in B$ $t_0+t_1a_1 \in U_1 \cap ... \cap U_n$ (such subsets exist by (1.7)). Then, by the standard interpretation of [Roq , Theorem 3.4.], there are $t_0 \in A$ and $t_1 \in B$ such that $t_0+t_1T_1$ is in the basic Hilbert set over $K(T_1,..,T_m)$ associated to f considered as an irreducible element of $K(T_1,..,T_m)(T_{m+1})[X]$. Put $g(T_1,..,T_m,X) = f(T_1,..,T_m,t_0+t_1T_1,X)$.
Then $g \in K[T_1,..,T_m,X]$ is irreducible as an element of $K(T_1,..,T_m)[X]$ and $g(a_1,..,a_m,X)$ changes sign on K, for each ordering P_i.
By Gauss' lemma: $g = c.\ G$, with $c \in K[T_1,..,T_m]$ and irreducible $G \in K[T_1,..,T_m,X]$. By slightly changing $(a_1,..,a_m)$, if necessary, we may assume $c(a_1,..,a_m) \neq 0$, and so the induction hypothesis can be applied to G, and gives a zero of G, hence one of f. □

To finish the proof of part *B* a more precise version of (1.17) is needed, namely:

(1.18) Lemma

Let $(K,P_1,..,P_n) \models OF_n$ satisfy (α) and (β) of (1.2) and let $R(T_1,..,T_m,X) \in K[T_1,..,T_m,X]$ be of degree $d > 0$ in X and monic in X and irreducible, and let for each $1 \leqslant i \leqslant n$ k_i be a natural number with $1 \leqslant k_i \leqslant d$, and let $(a_{i_1},..,a_{i_m}),(b_{i_1},..,b_{i_m})$ be m-tuples in K with $a_{ij} <_i b_{ij}$, for all $1 \leqslant j \leqslant m$, such that for each m-tuple $(c_{i_1},..,c_{i_m})$ in K with $a_{ij} <_i c_{ij} <_i b_{ij}$ $(j = 1,2,..,m)$ $R(c_{i_1},..,c_{i_m},X)$ has at least k_i roots in the real closure of (K,P_i). Then there is $(c_1,..,c_m,d) \in K^{m+1}$ with $R(c_1,..,c_m,d) = 0$, such that for each $i, 1 \leqslant i \leqslant n$: $a_{ij} <_i c_j <_i b_{ij}$ $(j = 1,2,..,m)$, and d is the $k_i{}^{th}$ root of $R(c_1,..,c_m,X)$ in the real closure of (K,P_i) (where the roots are numbered in increasing order).

Remark

It may be useful to look first at the proof in (1.19) to see how the problem is reduced to the rather technical lemma (1.18).

Proof

Let us first consider the case that for some w in the algebraic closure $\tilde{K}$ of K the set $\{t = (t_1,..,t_m) \in K^m | R(t,w) = 0\}$ is dense in K^m with respect to the Zariski topology on K^m (whose closed sets are by definition the zero sets in K^m of sets of polynomials in $K[T_1,..,T_m]$).

As K is infinite, it is wellknown that K^m is dense in $\tilde{K}^m$ and that the Zariski topology of $\tilde{K}^m$ induces on K^m the Zariski topology of K^m. So $\{t \in K^m | R(t,w) = 0\}$ is also dense in $\tilde{K}^m$, hence $\forall t \in \tilde{K}^m$ $R(t,w) = 0$, which implies:

$$R(T_1,..,T_m,w) = 0.$$

Then no T_j can appear in R. For if some T_j does, write

$$R = \Sigma c_{i_1,\ldots,i_m}(X) T_1^{i_1} \times \ldots \times T_m^{i_m} \quad \text{with} \quad c_{i_1,\ldots,i_m}(X) \in K[X].$$

Then $c_{i_1,\ldots,i_m}(w) = 0$, so the $c_{i_1,\ldots,i_m}(X)$ have a common factor in $K[X]$, contradicting the irreducibility of R. This in turn implies that $R \in K[X]$ is linear. (Otherwise K has a proper algebraic extension to which each ordering P_i can be extended, and by (1.12) this extension may assumed to be of the form $K(\sqrt{a}), a \in K\setminus K^2$. But this contradicts (1.11) as $a = (\sqrt{a})^2$ is in $P_1 \cap \ldots \cap P_n$.)
The linearity of $R \in K[X]$ makes the lemma trivial.
So in the following we will assume:

(a) <u>For each $w \in \tilde{K}$ the set</u> $\{t \in K^m | R(t,w) = 0\}$ <u>is not dense in K^m w.r.t. the Zariski topology on K^m;</u> in particular $R \notin K[X]$.

Next we may assume:

(b) $a_{1j} = a_{2j} = \ldots = a_{nj} = a_j$, $b_{1j} = b_{2j} = \ldots = b_{nj} = b_j$ $(j = 1,\ldots,m)$.

Namely, given $1 \leqslant j \leqslant m$, choose $\varepsilon_{ij} <_i 0$ such that $a_{ij}+\varepsilon_{ij} <_i b_{ij}-\varepsilon_{ij}$ and replace all a_{ij} by an element g_j of $\bigcap_{i=1}^{n}(a_{ij}, a_{ij}+\varepsilon_{ij})_i$ and all b_{ij} by an element b_j of $\bigcap_{i=1}^{n}(b_{ij}-\varepsilon_{ij}, b_{ij})_i$, which is possible by (1.7).
Let $D = D(T_1,\ldots,T_m)$ be the discriminant of R considered as a polynomial in X. Then $D \neq 0$, because R is irreducible and char(K) = 0.
So, after making the intervals $(a_j, b_j)_i$ smaller, if necessary, we may also assume that $D(t_1,\ldots,t_m) \neq 0$ for all $(t_1,\ldots,t_m) \in K^m$ with $t_j \in \bigcap_{i=1}^{n}(a_j,b_j)_i$ $(j = 1,\ldots,m)$, i.e. for all such $(t_1,\ldots,t_m)$ $R(t_1,\ldots,t_m,X)$ has no multiple roots.
Then the implicit function theorem for polynomials over real closed fields implies that, after making the imtervals $(a_j,b_j)_i$ smaller if necessary, the k_i^{th} root of $R(t_1,\ldots,t_m,X)$ is a continuous function

of $(t_1,..,t_m)$ (for those $(t_1,..,t_m)$ such that for all $1 \leq j \leq m$: $t_j \in (a_j,b_j)_i$, where these intervals are taken in the real closure of (K,P_i)), for each $1 \leq i \leq n$; and similarly for the other roots. Hence, making the intervals $(a_j,b_j)_i$ again smaller if necessary, and using (1.7) and (1.14), one can get the following situation:

(c) There exist $\alpha,\beta \in K$, $\alpha <_i \beta$, $(i = 1,..,n)$, such that for each $1 \leq i \leq n$: if $(t_1,..,t_m) \in K^m$ satisfies $t_j \in (a_j,b_j)_i$ for all $j = 1,..,m$, then $R(t_1,..,t_m,X)$ has a unique root in the interval $(\alpha,\beta)_i$ of the real closure of (K,P_i). This root even is in the smaller interval $(\alpha,\alpha+\frac{1}{2}(\beta-\alpha))_i$, is a simple root, and is the k_ith root of $R(t_1,..,t_m,X)$ in the real closure of (K,P_i).

Put $\gamma = (\beta-\alpha)^{-1}$, so $\gamma >_i 0$ for all $i = 1,..,n$. By a result of W.D. Geyer, in this form used by M. Jarden in [J2, p.297], it follows that

$$R(T_1,..,T_m,\alpha+(Z^2+U^2+V^2+\gamma)^{-1}) \in K(Z,U,V)[T_1,..,T_m]$$

is irreducible.

By the standard interpretation of [Roq , Th. 3.4.] there are $u,v \in K$ such that

$$R(T_1,..,T_m,\alpha+(Z^2+U^2+(u+vZ)^2+\gamma)^{-1}) \in K(Z,U)[T_1,..,T_m]$$

is irreducible.

Applying this trick once again we get $r,s \in K$ such that:

(d) $R(T_1,..,T_m,\alpha+(Z^2+(r+sZ)^2+(u+vZ)^2+\gamma)^{-1}) \in K(Z)[T_1,..,T_m]$ is irreducible.

Let $q(Z) = Z^2+(r+sZ)^2+(u+vZ)^2+\gamma \in K[Z]$. [Roq , Th. 3.4.] and (1.7) also imply that r and u can be taken arbitrarily close to 0 in each P_i-topology on K, so we may assume that for each $1 \leq i \leq n$:

(e) the function $z \mapsto \alpha+(q(z))^{-1}$, defined on the real closure of (K,P_i), includes in its image the interval $(\alpha,\alpha+\frac{1}{2}(\beta-\alpha))_i$ of this real closure.

Write $R(T_1,..,T_m,\alpha+(q(Z))^{-1}) = S(T_1,..,T_m,Z)\cdot p(Z)\cdot(q(Z))^{-k}$ with $p(Z) \in K[Z], k \geqslant 0$, $S = S(T_1,..,T_m,Z) \in K[T_1,..,T_m,Z]$ such that the coefficients of S, considered as a polynomial in $(T_1,..,T_m)$, have no common factor in $K[Z]$. Then by (d) and Gauss' Lemma:

(*f*) S is irreducible in $K[T_1,..,T_m,Z]$.

By (a) there is a nonempty Zariski-open set U in K^m such that for all $t \in U$: $R(t,X)$ and $p(Z)$ have no common root in $\tilde{K}$. Hence, after making the intervals $(a_j,b_j)_i$ smaller if necessary, and using (1.7), we may also assume:

(*g*) For all $t = (t_1,..,t_m) \in K^m$ with $t_j \in \bigcap_{i=1}^{n}(a_j,b_j)_i$, $(j = 1,..,m)$, $R(t,X)$ and $p(Z)$ have no common root in K.

Hence, by the definition of S, combining (c), (e), (g) and (1.14):

(*h*) For each $t = (t_1,..,t_m) \in K^m$ with $t_j \in \bigcap_{i=1}^{n}(a_j,b_j)_i$, $(j = 1,..,m)$, and each $1 \leqslant i \leqslant m$: $S(t_1,..,t_m,Z)$ changes sign on K for the ordering P_i, and if z is any root of $S(t_1,..,t_m,Z)$ in the real closure of (K,P_i), then $\alpha+(q(z))^{-1}$ is the k_ith root of $R(t,X)$ in this real closure.

Applying the same trick of Jarden to S and the variables T_j we get that

$$F(Y,Z) = F(Y_{11},Y_{12},Y_{13},..,Y_{m1},Y_{m2},Y_{m3},Z) \overset{\text{def}}{=}$$
$$S(a_1+(b_1-a_1)(Y_{11}^2+Y_{12}^2+Y_{13}^2+2)^{-1},..,a_m+(b_m-a_m)(Y_{m1}^2+Y_{m2}^2+Y_{m3}^2+2)^{-1},Z)$$

is irreducible in $K(Y)[Z]$.

Write $F(Y,Z) = f(Y,Z)\cdot r(Y)$ with irreducible $f \in K[Y,Z]$ and $r(Y) \in K(Y)$. The denominator of r is a product of factors $Y_{j1}^2+Y_{j2}^2+Y_{j3}^2+2$, so r is defined on each $y \in K^{3m}$.

Take any $y \in K^{3m}$. Then $a_j+(b_j-a_j)(y_{j1}^2+y_{j2}^2+y_{j3}^2+2)^{-1} \in \bigcap_{i=1}^{n}(a_j,b_j)_i$, $(1 \leqslant j \leqslant m)$, so by (h) we get:

$F(y,Z)$ changes sign on K for each ordering P_i,

so $f(y,Z)$ changes sign on K for each ordering P_i.
Hence by lemma (1.17) f has a zero in K^{3m+1}, and this is also a zero of F. 'Par abus de langage' , let this zero be (y,z), and put $c_j = a_j+(b_j-a_j)(y_{j1}^2+y_{j2}^2+y_{j3}^2+2)^{-1}$ $(1 \leqslant j \leqslant m)$ and $d = \alpha+(q(z))^{-1}$, Then by (h) and (b): $(c_1,..,c_m,d) \in K^{m+1}$ satisfies the conclusion of (1.17). $\square$

(1.19) The proof of part $\mathcal{B}$, (1.3), can now be finished by model theory as follows:

<u>Let $\mathcal{K} = (K,P_1,..,P_n) \models OF_n$ satisfy (α) and (β) and let $\mathcal{K} \subset \mathcal{L} \models OD_n$ and suppose ρ is a $\mathcal{K}$-existential sentence true in $\mathcal{L}$. It remains to show: ρ is true in $\mathcal{K}$.</u>

Let $\mathcal{L} = (L,Q_1,..,Q_n)$. By (1.4) and the assumption that ρ is existential we may assume that L is a finitely generated field extension of K. Because char. $K = 0$, we can then write $L = K(t_1,..,t_m)[\alpha]$ with $t = (t_1,..,t_m)$ a transcendence base of L over K and such that α has minimum polynomial $R(t_1,..,t_m,X)$ over $K(t_1,..,t_m)$, with $R = (T_1,..,T_m,X)$ an irreducible polynomial of $K[T_1,..,T_m,X]$ (see Ch. I, (2.4) for a similar argument). R is monic and of positive degree, say $d > 0$, in X. Let for each $1 \leqslant i \leqslant n$ α be the k_i^{th} root of $R(t,X)$ in the real closure of the ordered field $(K(t),Q_i \cap K(t))$, so $1 \leqslant k_i \leqslant d$.

Consider the following sets of sentences in the language of OD_n, augmented by names for the elements of K and new constants $\underline{c}_1,..,\underline{c}_m,\underline{d}$:

$\Gamma_1 = OF_n \cup \mathrm{Diag}(\mathcal{K})$.

For each $1 \leqslant i \leqslant n$, let $\Gamma_{2,i}$ be the set of all sentences $S(\underline{c}_1,..,\underline{c}_m) >_i 0$, such that $S(T_1,..,T_m) \in K[T_1,..,T_m]$ and $S(t) >_i 0$.
Put $\Gamma_2 = \Gamma_{2,1} \cup ... \cup \Gamma_{2,n}$.

Let for each $1 \leqslant i \leqslant n$ $\Theta_i(\underline{c}_1,..,\underline{c}_m,\underline{d})$ be an open sentence (not containing the predicates $\underline{P}_1,..,\underline{P}_{i-1},\underline{P}_{i+1},..,\underline{P}_n$), such that for any ordered field extension (M,P) of (K,P_i) and all $c_1,..,c_m,d \in M$: $(M,P) \models \Theta_i(\underline{c}_1,..,\underline{c}_m,\underline{d})$ iff d is the k_i^{th} root of $R(t_1,..,c_m,X)$ in the real closure of (M,P) (such Θ_i exists by Tarski's Theorem mentioned in Ch. I, §1, or by Sturm's Theorem, see [L3, p.276]).
Let $\Gamma_3 = \{\Theta_1(\underline{c},\underline{d}),..,\Theta_n(\underline{c},\underline{d})\}$ $(\underline{c} = (\underline{c}_1,..,\underline{c}_m))$.
Note that $(\mathcal{L},t_1,..,t_m,\alpha) \models \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ and that (using the remarks in (1.9)) $(\mathcal{L},t_1,..,t_m,\alpha)$ can be embedded over K in each model of $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ (where as usual models of Γ_1 are considered as OF_n-extensions of K).
So $\mathcal{L} \models \rho$ implies $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \models \rho$. Hence, by the compactness theorem, there are finite subsets $\Delta_1,..,\Delta_n$ of $\Gamma_{2,1},..,\Gamma_{2,n}$ respectively, such that, putting $\Delta = \Delta_1 \cup ... \cup \Delta_n$:

(a) $\Gamma_1 \cup \Delta \cup \Gamma_3 \vdash \rho$.

Let for each $1 \leqslant i \leqslant n$ $\psi_i(\underline{c}_1,..,\underline{c}_m)$ be an open sentence (not containing the constant $\underline{d}$ or the predicates $\underline{P}_1,..,\underline{P}_{i-1},\underline{P}_{i+1},..,\underline{P}_n$), such that for each ordered field extension (M,P) of (K,P_i) and all $c_1,..,c_m \in M$: $(M,P) \models \psi_i(\underline{c}_1,..,\underline{c}_m)$ iff $R(c_1,..,c_m,X)$ has at least k_i roots in the real closure of (M,P) (such ψ_i exists, again by Tarski's Theorem).
Note that
$(K(t),Q_1 \cap K(t),..,Q_n \cap K(t),t_1,..,t_m) \models \Gamma_4 \overset{\text{def.}}{=} \{\psi_1(\underline{c}),..,\psi_n(\underline{c})\}$
and that $(K(t),Q_1 \cap K(t),..,Q_n \cap K(t),t_1,..,t_m)$ can be embedded over K into each model of $\Gamma_1 \cup \Gamma_2$, so each model of $\Gamma_1 \cup \Gamma_2$ satisfies Γ_4.
Hence by the compactness theorem there is a finite subset of Γ_2, which (after enlarging Δ) we may assume to be Δ, such that

(b) $\Gamma_1 \cup \Delta \vdash \Gamma_4$.

Let $1 \leqslant i \leqslant n$. $\Gamma_1 \cup \Delta_i$ is consistent, so there are elements $a_{i1}, b_{i1}, \ldots, a_{im}, b_{im}$ in the real closure of (K, P_i) with $a_{ij} <_i b_{ij}$, such that for all $c_{i1}, \ldots, c_{im}$ in this real closure with $a_{ij} <_i c_{ij} <_i b_{ij}$ $(j = 1, \ldots, m)$, Δ_i is true if $\underline{c}_1, \ldots, \underline{c}_m$ are interpreted as $c_{i1}, \ldots, c_{im}$ respectively.
Because of (1.14) we may assume all a_{ij}, b_{ij} to be in K. Now *(b)* implies that all assumptions of lemma (1.18) are satisfied. Then the conclusion of (1.18) says that there are $c_1', \ldots, c_m', d'$ in K such that $\Delta \cup \Gamma_3$ is satisfied in K if $\underline{c}_1, \ldots, \underline{c}_m, \underline{d}$ are interpreted as $c_1', \ldots, c_m', d'$ respectively. Then *(a)* and the definition of Γ_1 imply that $K \models \rho$. □

Comment

The proof of Theorem (1.2) will become perhaps more perspicuous by the following remarks.
The model theoretic argument above is the key to the existence of the model companion. Namely, it shows that the n-ordered fields for which the hypotheses of (1.18) minus (α) and (β) imply its conclusion, are existentially closed. Conversely, it is easily shown that (1.18) remains valid if (α) and (β) are replaced by the requirement that the n-ordered field is existentially closed. Hence the existentially closed n-ordered fields are exactly those for which "(1.18) with (α) and (β) omitted from the hypothesis" holds. But this shows that the class of existentially closed n-ordered fields is elementary!, so OF_n has a model companion, and it is then only a matter of applying a lot of reduction steps to reach the simple axiomatization given by (α) and (β) of (1.2).

Note that $\overline{OD}_1$ equals necessarily RCF (by Ch. I, (2.21)), so $\overline{OD}_1$, is a complete theory, and is the model completion of OD_1. Contrasting with this is the following result.

(1.20) *Proposition*

Let $n \geq 2$. Then $\overline{OD}_n$ has $2^{\aleph_0}$ different complete extensions, and it is not the model completion of OD_n or OF_n.

Proof

Let us suppose $n = 2$ for simplicity, and let $(p_k)_{k \in \mathbb{N}}$ be a 1-1 enumeration of the set of primes, and define $L = \mathbb{Q}(\sqrt{p_k} \mid k \in \mathbb{N})$. By easy valuation theory one proves that $\sqrt{p_k} \notin \mathbb{Q}(\sqrt{p_\ell} \mid \ell < k)$. Hence, given any $S : \mathbb{N} \to \{0,1\}$, there are ordering $P_{s,1}$ and $P_{s,2}$ on L such that for all $k \in \mathbb{N}$ $\sqrt{p_k}$ has the same sign with respect to $P_{s,1}$ and $P_{s,2}$ if $s(k) = 0$, and different signs, if $s(k) = 1$.
Let for each $s : \mathbb{N} \to \{0,1\}$ K_s be an existentially closed extension of $(L, P_{s,1}, P_{s,2})$. Then we have for $s \neq t$ $(s,t : \mathbb{N} \to \{0,1\})$:

$$K_s \not\equiv K_t.$$

Suppose namely that $s(k) = 0$ and $t(k) = 1$. Then in K_s each of the two square roots of p_k has the same sign with respect to the first and the second ordering of K_s, while in K_t they have different signs.
So $(K_s)_{s : \mathbb{N} \to \{0,1\}}$ is a family of $2^{\aleph_0}$ pairwise non elementary equivalent models of $\overline{OD}_2$, and this implies the first statement of the proposition.
That $\overline{OD}_2$ is not the model completion of OF_2, follows (by Ch. I, (2.20)) from the fact that OF_2 does not have AP: $\mathbb{Q}$ has exactly one OF_2-structure, and $\mathbb{Q}(\sqrt{2})$ exactly 4, and $4 > 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$, and we apply then the following lemma, which often can be used to show that a certain theory of fields does not have AP. $\square$

(1.21) <u>*Lemma*</u>

Let L be any language extending the language of rings, and let T be an L-theory extending FL such that T has AP.

Then the following holds:

if $\mathcal{K} \models T$ and K is the underlying field of $\mathcal{K}$, and $L = K(\alpha)$, with α algebraic of degree n over K, then L has at most n expansions to a model $\mathcal{L}$ of T with $\mathcal{K} \subset \mathcal{L}$.

<u>*Proof*</u>

Suppose $(\mathcal{L}_i)_{1 \leqslant i \leqslant n+1}$ is a family of expansions of L as described.
By AP there is a model $\mathcal{A} \supset \mathcal{K}$ of T, and there are $\mathcal{K}$-embeddings $\varphi_i : \mathcal{L}_i \to \mathcal{A}$. The minimum polynomial $f \in K[X]$ of α has at most n roots, say $\alpha_1, .., \alpha_k, k \leqslant n$, in $\mathcal{A}$, hence $\varphi_i(\alpha)$ can assume at most k different values in $\mathcal{A}$, and if $\varphi_i(\alpha) = \varphi_j(\alpha)$, then necessarily $\varphi_i = \varphi_j$, so $\mathcal{L}_i = \mathcal{L}_j$. □

Let me finish this section showing that the finiteness of n seems essential. Let κ be an <u>infinite</u> cardinal and let OD_κ be the theory of structures $(D, P_\lambda | \lambda < \kappa)$ with (D, P_λ) an ordered domain for each $\lambda < \kappa$.

(1.22) <u>*Proposition*</u>

<u>OD_κ has no model companion.</u>

<u>*Proof*</u>

Let $K = (K, P_\lambda | \lambda < \kappa)$ be an existentially closed model of OD_κ. It is routine to show that this implies $K^2 = \cap \{P_\lambda | \lambda < \kappa\}$.
Using a simple chain argument one can reach the situation that for each $\lambda < \kappa$ there is $x_\lambda \in K$ with $x_\lambda <_\lambda 0$ but $x_\lambda >_\mu 0$ for all $\mu < \kappa, \mu \neq \lambda$. Let D be a free ultrafilter on $\kappa = \{\lambda | \lambda < \kappa\}$.

Then the sequence $(x_\lambda)_{\lambda<\kappa}$ gives rise to an element x in the universe K^κ/D of K^κ/D, which is positive for each of the κ distinguished orderings of K^κ/D, by Łoś' Theorem. But this theorem also implies that x is not a square in K^κ/D, so K^κ/D is not existentially closed. We have shown that the class of existentially closed models of OD_κ is not an elementary class, so OD_κ has no model companion by Ch. I (2.21). □

Remark

There is however another way to consider infinitely many orderings on a field. A preordering on a field K is a subset Q of K with

$$K^2 \subset Q, Q+Q \subset Q, Q \cdot Q \subset Q,$$

or equivalently, it is an intersection of orderings on the field. So one can consider a preordering on a field as describing the space of orderings which contain the preordering, and this space is compact with respect to a certain topology on it. The use of compactness instead of the finiteness of $n \in \mathbb{N}$ might lead to a proof that the theory of preordered fields has a model companion.

§2. *Decidability and elimination*

The main result of this section is

(2.1) *Theorem*

The model companion $\overline{OD}_n$ of OD_n is decidable.

This will be proved in (2.11) as an easy consequence of the following classification (2.2) of complete extensions of $\overline{OD}_n$.

For each field K we put

$\mathrm{alg}(K) = \{\alpha \in K \mid \alpha \text{ is algebraic over the prime field of } K\}$.

(2.2) *Theorem*

Let $(K,P_1,\ldots,P_n)$ and $(L,Q_1,\ldots,Q_n)$ be models of $\overline{OD}_n$.

Then: $(K,P_1,\ldots,P_n) \equiv (L,Q_1,\ldots,Q_n) \quad \Leftrightarrow$

$(\mathrm{alg}(K),P_1 \cap \mathrm{alg}(K),\ldots,P_n \cap \mathrm{alg}(K)) \simeq (\mathrm{alg}(L),Q_1 \cap \mathrm{alg}(L),\ldots,Q_n \cap \mathrm{alg}(L))$.

The proof is given in (2.8).

(2.3) We will now indicate an extension by definitions $\widetilde{OD}_n$ of $\overline{OD}_n$ which admits elimination.

Let natural numbers d and k with $d \geqslant 2$ and $1 \leqslant k \leqslant d$ be given; then there is an open formula $R_{d,k}(\underline{P},z,x_1,\ldots,x_d)$ in the language of ordered fields, such that for any ordered field (K,P) and all $b,a_1,\ldots,a_d \in K$: $(K,P) \models R_{d,k}(\underline{P},b,a_1,\ldots,a_d)$ if and only if b is the k^{th} root of $Z^d+a_1Z^{d-1} + \ldots + a_d$ in the real closure of (K,P).

Using Tarski's elimination theory, or Sturm's Theorem, one can effectively construct such a formula $R_{d,k}$ from (d,k).

For reasons which will become clear now I made explicit the appearance of the predicate symbol $\underline{P}$ in $R_{d,k}$.

Extend the theory $\overline{OD}_n$ to the theory $\widetilde{OD}_n$ by introducing new predicate symbols $\underline{W}_{d,k_1,\ldots,k_n}$ $(d \geq 2,\ 1 \leq k_i \leq d)$ and by adding as defining axioms the universal closures of:

$$W_{d,k_1,\ldots,k_n}(x_1,\ldots,x_d) \leftrightarrow \exists z\left(\bigwedge_{i=1}^{n} R_{d,k_i}(\underline{P}_i, z, x_1,\ldots,x_d)\right)$$

(2.4) *Theorem*

$\widetilde{OD}_n$ <u>admits elimination.</u>

This will be proved in (2.14).

The following lemma is the key to all above results.

(2.5) *Lemma*

Let

$$\begin{tikzcd} & L_1 \arrow[dr, hook] & \\ K \arrow[ur, hook] \arrow[dr, hook] & & M \\ & L_2 \arrow[ur, hook] & \end{tikzcd}$$

be a (commutative) diagram of field inclusions with L_1 and L_2 linearly disjoint over K.

Let P_1 and P_2 be orderings on L_1, L_2 resp. with $P_1 \cap K = P_2 \cap K$. Then P_1 and P_2 have a common extension to an ordering on L_1L_2.

Proof

By [L3 , Prop. 1, page 262] and Zorn's Lemma the problem can be reduced to the case that $L_1 = K(\alpha)$ and $L_2 = K(\beta)$ for certain $\alpha, \beta \in M$.

There are two subcases:

(*a*) one of α,β, say α, is algebraic over K;

(*b*) α and β are transcendental over K.

Suppose (*a*) holds. Then $L_1L_2 = L_2[\alpha]$ and so the canonical map

$$L_1 \otimes_K L_2 \to L_1L_2$$

is an isomorphism.

Further, by the amalgamation property for ordered fields, there is an ordered field (N,Q) and there are ordered field embeddings such that the diagram

$$\begin{tikzcd} & (L_1,P_1) \arrow[dr] & \\ (K,P) \arrow[ur, hook] \arrow[dr, hook] & & (N,Q) \\ & (L_2,P_2) \arrow[ur] & \end{tikzcd}$$

$P=P_1 \cap K$ commutes.

We may assume that N is generated by the images of L_1 and L_2, so the induced K-algebra morphism $L_1 \otimes_K L_2 \to N$ is onto, and as $L_1 \otimes_K L_2$ is a field, this morphism is even an isomorphism. Hence it induces an isomorphism $N \to L_1L_2$, and the image of Q under this map is a common extension of P_1 and P_2 to an ordering on L_1L_2.

Suppose that *(b)* holds. Then α and β are algebraically independent over K. Let $\underline{a},\underline{b}$ be new constants and consider the set of sentences

$\Gamma = OF \cup \mathrm{Diag}(K,P) \cup \{p(\underline{a}) > 0 \mid p \in K[X], p(\alpha) > 0 \text{ in } (L_1,P_1)\} \cup$

$\{q(\underline{b}) > 0 \mid q \in K[Y], q(\beta) > 0 \text{ in } (L_2,P_2)\} \cup \{r(\underline{a},\underline{b}) \neq 0 \mid 0 \neq r \in K[X,Y]\}$.

It is clear that if Γ is consistent, then an ordering on $K(\alpha,\beta)$ as required exist. So by the compactness theorem it suffices to prove: let $p_1,\dots,p_k \in K[X]$ and $q_1,\dots,q_\ell \in K[Y]$ be such that $p_i(\alpha) > 0$ in (L_1,P_1) and $q_j(\beta) > 0$ in (L_2,P_2) $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant \ell)$, and $0 \neq r \in K[X,Y]$; then in the real closure of (K,P) there are a,b such that $p_i(a) > 0, q_j(b) > 0, r(a,b) \neq 0$ $(1 \leqslant i \leqslant k, 1 \leqslant j \leqslant \ell)$.

Now, $OF \cup \mathrm{Diag}(K,P) \cup \{p_i(\underline{a}) > 0 \mid 1 \leqslant i \leqslant k\}$ and

$OF \cup \mathrm{Diag}(K,P) \cup \{q_j(\underline{b}) > 0 \mid 1 \leqslant j \leqslant \ell\}$ are consistent theories, so in the real closure of (K,P) there are non-empty open subsets A and B such that for all $a \in A$: $p_i(a) > 0$ $(1 \leqslant i \leqslant k)$ and for all $b \in B$: $q_j(b) > 0$ $(1 \leqslant j \leqslant \ell)$; because A and B are infinite, there are $a \in A, b \in B$ with $r(a,b) \neq 0$. $\square$

(2.6) *Lemma*

Let $K = (K,P_1,..,P_n) \models OF_n$. Then the following properties are equivalent.

(a) There is no proper algebraic extension L of K such that $P_1,..,P_n$ can be extended to orderings on L.

(b) K is algebraically closed in L for each extension $\mathcal{L} = (L,Q_1,..,Q_n) \models OF_n$ of K.

(c) There is an extension $\mathcal{L} = (L,Q_1,..,Q_n) \models \overline{OD}_n$ of K such that K is algebraically closed in L.

(d) $P_1 \cap ... \cap P_n = K^2$ and each odd degree polynomial in K[X] has a root in K.

Proof

(a) ⇒ (b) ⇒ (c) ⇒ (d) are clear by (1.11) and (1.2).

(d) ⇒ (a): suppose $L|K$ is proper algebraic such that $P_1,..,P_n$ can be extended to L. Then by (1.12) we may assume $L = K(\sqrt{a}), a \in K\setminus K^2$. But then $a = (\sqrt{a})^2$ would be in $P_1 \cap ... \cap P_n$, so in K^2, contradiction. □

Definition

Let $OF_{n,alg}$ be the theory of the class of structures $K \models OF_n$ which satisfy the equivalent conditions (a),(b),(c),(d) of (2.6).

So an axiomatization of $OF_{n,alg}$ is given by the axioms for OF_n and (d) of (2.6). I do not know whether

$\overline{OD}_n = OF_{n,alg} \cup \{\text{axiom } (\alpha) \text{ of } (1.2)\}$.

(I would be surprised if it was.)

(2.7) *Corollary*

$OF_{n,alg}$ has AP.

Proof

Let embeddings $K \to \mathcal{L}_1, K \to \mathcal{L}_2$ be given with $K \models OF_{n,alg}$, $\mathcal{L}_1, \mathcal{L}_2 \models OF_n$. Let $K = (K, P_1, .., P_n)$, $\mathcal{L}_1 = (L_1, Q\ , .., Q_n)$, $\mathcal{L}_2 = (L_2, R_1, .., R_n)$. K is identified with a subfield of L_1, and L_2 resp. via the above embeddings. Because K is algebraically closed in L_1 and char(K) = 0, $L_1 | K$ is a regular field extension (see [L1, p.56]), which implies that L_1 and L_2 can be embedded in a common extension field M in such a way that L_1 and L_2 are linearly disjoint over K. Then, by (2.5), for each $1 \leqslant i \leqslant n$ the orderings Q_i and R_i have a common extension to an ordering S_i on $L_1 L_2 \subset M$. Then the following diagram of embeddings commutes:

$$\begin{tikzcd} & \mathcal{L}_1 \arrow[dr] & \\ K \arrow[ur, hook] \arrow[dr, hook] & & (L_1 L_2, S_1, .., S_n). \quad \square \\ & \mathcal{L}_2 \arrow[ur] & \end{tikzcd}$$

(2.8) *Proof of (2.2)*

Let us write K for $(K, P_1, .., P_n)$ and alg(K) for (alg(K), $P_1 \cap$ alg(K), ..., $P_n \cap$ alg(K)), and similarly introduce $\mathcal{L}$ and alg($\mathcal{L}$). Suppose alg(K) $\simeq$ alg($\mathcal{L}$). Let us identify alg(K) and alg($\mathcal{L}$). alg(K) is a model of $OF_{n,alg}$, by (2.6) (c), so (2.7) implies that there is a commutative diagram of embeddings:

$$\begin{tikzcd} & K \arrow[dr] & \\ \mathrm{alg}(K) \arrow[ur, hook] \arrow[dr, hook] & & M \\ & \mathcal{L} \arrow[ur] & \end{tikzcd}$$

Extending M if necessary, we may assume $M \models \overline{OD}_n$. Then $K \prec M$ and $\mathcal{L} \prec M$, so $K \equiv \mathcal{L}$. Conversely, let $K \equiv \mathcal{L}$. Then, by compactness, $\overline{OD}_n \cup \mathrm{Diag}(K) \cup \mathrm{Diag}(\mathcal{L})$ has a model M, and we may identify K and $\mathcal{L}$

with substructures of M.

Then, because $K \prec M$ and $\mathcal{L} \prec M$, we get that

$\mathrm{alg}(K) = \mathrm{alg}(M)$ and $\mathrm{alg}(\mathcal{L}) = \mathrm{alg}(M)$, so $\mathrm{alg}(K) \simeq \mathrm{alg}(\mathcal{L})$. □

(2.9) *Definition*

For each monic irreducible $f = f(X) \in \mathbb{Q}[X]$, let K_f be the field $\mathbb{Q}[X]/_{(f)}$ and let α_f be the residue class of X : $\alpha_f = X+(f)$.
So $K_f = \mathbb{Q}(\alpha_f)$ and $f(X)$ is the minimum polynomial of α_f over $\mathbb{Q}$. Let r_f be the number of roots of $f(X)$ in the real closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$, and let $\alpha_1 <\ldots< \alpha_{r_f}$ be these roots. Then for $1 \leqslant k \leqslant r_f$
$P_{f,k}$ is by definition the ordering on K_f induced by the embedding $\alpha_f \to \alpha_k$ of K_f into $\bar{\mathbb{Q}}$.
In other words: $P_{f,k}$ is the unique ordering on K_f such that $(K_f,P_{f,k}) \models R_{d,k}(\underline{P},\alpha_f,a_1,\ldots,a_d)$, if $f(X) = X^d+a_1X^{d-1}+\ldots+a_d$, $d \geqslant 2$.
(See (2.3) for definition of $R_{d,k}$.)

The decidability of $\overline{\mathrm{OD}}_n$ will be seen (in (2.11)) to rest on the following facts:

(2.10) *Fact 1*

There is an algorithm which, given $f = f(X) \in \mathbb{Q}[X]\setminus\mathbb{Q}$, determines whether f is irreducible.

Fact 2

There is an algorithm which, given irreducible and monic $f = f(X) \in \mathbb{Q}[X]$, computes r_f.

Concerning fact 1: by Gauss' lemma it suffices to have a factorization algorithm for $\mathbb{Z}[X]$. Such an algorithm, due to Kronecker, is given in [v.d.W., p. 79].

Fact 2 is a consequence of Sturm's Theorem [L3, p.276].

(2.11) *Proof of (2.1)*

Theorem (1.2) clearly implies that the set of logical consequences of $\overline{OD}_n$ is recursively enumerable. So it suffices to prove that the complement of this set is also recursively enumerable.

Let $\overline{OD}_n \nvdash \sigma$, σ a sentence in the language of OD_n.

Then there is a model $K = (K,P_1,..,P_n)$ of $\overline{OD}_n \cup \{\neg\sigma\}$.

Let, as in (2.8), alg(K) be the substructure of K with universe alg(K). Then (2.3) and (2.6) imply:

$$\overline{OD}_n \cup \mathrm{Diag}(\mathrm{alg}(K)) \vdash \neg\sigma.$$

The compactness theorem then shows that there is a subfield L of alg(K) with $[L : \mathbb{Q}] < \infty$, such that:

$$\overline{OD}_n \cup \mathrm{Diag}(L,P_1\cap L,..,P_n\cap L) \vdash \neg\sigma.$$

But $(L,P_1\cap L,..,P_n\cap L) \simeq (K_f,P_{f,k_1},..,P_{f,k_n})$ for some irreducible monic $f \in \mathbb{Q}[X]$, and numbers $k_1,..,k_n$ satisfying $1 \leqslant k_1 \leqslant r_f,..,1 \leqslant k_n \leqslant r_f$.

So $\quad \overline{OD}_n \cup \mathrm{Diag}(K_f,P_{f,k_1},..,P_{f,k_n}) \vdash \neg\sigma.$

Let $f = X^d+a_1X^{d-1}+...+a_d$. If $d = 1$, then clearly $\overline{OD}_n \vdash \neg\sigma$.

Suppose $d \geqslant 2$. Then a model of $\overline{OD}_n \cup \mathrm{Diag}(K_f,P_{f,k_1},..,P_{f,k_n})$ is essentially the same as a model of

$$\overline{OD}_n \cup \{\exists z\,(\bigwedge_{i=1}^{n} R_{d,k_i}(\underline{P}_i,z,a_1,..,a_d))\}\text{ , as is clear}$$

from the remarks in (2.9), so

$$\overline{OD}_n \cup \{\exists z\,(\bigwedge_{i=1}^{n} R_{d,k_i}(\underline{P}_i,z,a_1,..,a_d))\} \vdash \neg\sigma.$$

We have now proved one half of the following equivalence:

A sentence σ is not derivable from $\overline{OD}_n$ if and only if either $\overline{OD}_n \vdash \neg\sigma$, or there is irreducible $f = f(X) = X^d+a_1X^{d-1}+..+a_d \in \mathbb{Q}[X]$, $d \geqslant 2$, and numbers $k_1,..,k_n$ with $1 \leqslant k_i \leqslant r_f$ $(i = 1,..,n)$, such that

$$\overline{OD}_n \cup \{\exists z\,(\bigwedge_{i=1}^{n} R_{d,k_i}(\underline{P}_i,z,a_1,..,a_d))\} \vdash \neg\sigma.$$

The other half of the equivalence follows by noting that any existentially closed extension of $(K_f, P_{f,k_1}, \ldots, P_{f,k_n})$ is a model of $\overline{OD}_n \cup \{\neg\sigma\}$.
From the equivalence, and using facts 1. and 2. in (2.10), we get the recursive enumerability of

$\{\sigma \mid \overline{OD}_n \not\vdash \sigma\}$. □

(2.12) *Definition*

$$\widetilde{OD}_{n,alg} \overset{\text{def.}}{=} OF_{n,alg} \cup (\widetilde{OD}_n)_\forall .$$

(see (2.3) for the meaning of $\widetilde{OD}_n$).

So the models of $\widetilde{OD}_{n,alg}$ are the substructures $(K, P_1, \ldots, P_n, \ldots)$ of models of $\widetilde{OD}_n$ with $(K, P_1, \ldots, P_n) \models OF_{n,alg}$.
Clearly $(\widetilde{OD}_{n,alg})_\forall = (\widetilde{OD}_n)_\forall$.

(2.13) *Lemma*

(1) Each model of $OF_{n,alg}$ has a unique expansion to a model of $\widetilde{OD}_{n,alg}$.

(2) $\widetilde{OD}_{n,alg}$ has $PEP_{universal}$ (cf. Ch. I, (3.4)).

Proof

(1) Let $(K, P_1, \ldots, P_n, W_{d,k_1,\ldots,k_n} \mid 2 \leqslant d,\ 1 \leqslant k_i \leqslant n)$ be an expansion of a model $(K, P_1, \ldots, P_n)$ of $OF_{n,alg}$ to a substructure of a model of $\widetilde{OD}_n$.
Then (2.6) implies easily: if $2 \leqslant d$, $1 \leqslant k_i \leqslant d$ $(i = 1, \ldots, n)$ and $a_1, \ldots, a_d \in K$, then $W_{d,k_1,\ldots,k_n}(a_1, \ldots, a_d)$ holds iff $Z^d + a_1 Z^{d-1} + \ldots + a_d$ has a root in K which is, for each $1 \leqslant i \leqslant n$, the k_ith root in the real closure of (K, P_i).
In other words: the defining axioms for the extra <u>W</u>-predicates (cf. (2.3)) hold in the expansion. So there is only one choice for the expansion.

(2) Let $\mathcal{D} = (D,P_1,..,P_n,..) \models (\widetilde{OD}_n)_\forall$. Take any extension of $\mathcal{D}$ to a model of $\widetilde{OD}_n$ and let $\bar{\mathcal{D}} = (\bar{D},\bar{P}_1,..,\bar{P}_n,..)$ be the substructure of this extension whose universe $\bar{D}$ consists of the elements which are algebraic over $Q(D)$. So clearly $\bar{\mathcal{D}} \models \widetilde{OD}_{n,alg}$.
We will prove that $\bar{\mathcal{D}}$ is the universal prime extension of $\mathcal{D}$ to a model of $\widetilde{OD}_{n,alg}$.
So let $\mathcal{L} = (L,Q_1,..,Q_n,..)$ be any extension of $\mathcal{D}$ with $\mathcal{L} \models \widetilde{OD}_{n,alg}$.
Let $Q(D) \subset K \subset \bar{D}$, with K a finite extension of $Q(D)$.
We will prove that $(K,\bar{P}_1\cap K,..,\bar{P}_n\cap K)$ can be embedded uniquely over $(D,P_1,..,P_n)$ into $(L,Q_1,..,Q_n)$. This is clear if $K = Q(D)$. So let $[K : Q(D)] = d > 1$. Then we can write: $K = Q(D)[a]$ where the minimum polynomial $f(X)$ of a over $Q(D)$ has coefficients in D:
$f(X) = X^d+a_1X^{d-1}+..+a_d \in D[X]$. Then $\mathcal{D} \models \underline{W}_{d,k_1,..,k_n}(a_1,..,a_d)$, where for each $1 \leq i \leq n$ a is the k_i th root of $f(X)$ in the real closure of $(K,\bar{P}_i\cap K)$ (which is naturally identified with the real closure of $(Q(D),Q(P_i)))$.
Because $\mathcal{D} \subset \mathcal{L}$, also $\mathcal{L} \models \underline{W}_{d,k_1,..,k_n}(a_1,..,a_d)$.
As in the proof of (1) this implies there is $b \in L$ such that, for each $1 \leq i \leq n$, b is the k_i th root of $f(X)$ in real closure of (L,Q_i), hence also the k_i th root of $f(X)$ in the real closure of $(Q(D),Q(P_i))$, considered as a subfield of the real closure of (L,Q_i).
So there is an embedding of $(K,\bar{P}_1\cap K,..,\bar{P}_n\cap K)$ over $(D,P_1,..,P_n)$ into $(L,Q_1,..,Q_n)$ given by $a \mapsto b$, and this is clearly the only $(D,P_1,..,P_n)$-embedding of $(K,\bar{P}_1\cap K,..,\bar{P}_n\cap K)$ into $(L,Q_1,..,Q_n)$.
If we put all these embeddings together, we obtain: there is a unique $(D,P_1,..,P_n)$-embedding of $(\bar{D},\bar{P}_1,..,\bar{P}_n)$ into $(L,Q_1,..,Q_n)$.
Because the defining axioms for the W-predicates (cf. (2.3)) hold in $\bar{\mathcal{D}}$ and in $\mathcal{L}$, this embedding is even an embedding of $\bar{\mathcal{D}}$ into $\mathcal{L}$. $\square$

(2.14) *Proof of (2.4)*

$\widetilde{OD}_n$ is, as an extension by definitions of $\overline{OD}_n$, a model complete theory, so by Ch. I, (2.13), it suffices to show that $(\widetilde{OD}_n)_\forall$ has AP. So let A,B,C be models of $(\widetilde{OD}_n)_\forall$ and let embeddings $A \to B$ and $A \to C$ be given. This induces embeddings $\bar{A} \to \bar{B}$ and $\bar{A} \to \bar{C}$ of their prime extensions w.r.t. $\widetilde{OD}_{n,alg}$. But $\widetilde{OD}_{n,alg}$ has AP, as follows easily from (2.7) and (2.13) (1).
So we can embed $\bar{B}$ and $\bar{C}$ over $\bar{A}$ in a model $\mathcal{D}$ of $\widetilde{OD}_n$, giving us also embeddings of B and C over A in $\mathcal{D}$. □

(2.15) *Remark*

The theory $\overline{OD}_n$ shows many model theoretic similarities with the theory of pseudo-finite fields introduced by Ax in [Ax].
(A pseudo-finite field F is an infinite field of the form $(\prod_{i\in I} F_i)/\underline{m}$, each F_i being a finite field, or equivalently, it is a perfect field with for each $n \geq 1$ precisely one extension of degree n and such that each absolutely irreducible $p \in F[X,Y]$ has infinitely many zeros in $F\times F$.)
Kiefe defines in [Ki] the d-ary predicate $\underline{W}_d$ $(d \geq 2)$ for each pseudo-finite field F as follows:
$\underline{W}_d(a_1,..,a_d)$ holds in F iff $X^d+a_1X^{d-1}+..+a_d$ has a root in F, and she shows that the corresponding extension by definitions of the theory of pseudo-finite fields admits elimination.

For the theories $\overline{OD}_n (n \geq 3)$ however, this procedure does not work, as is shown in the following example.

(2.16) *Example*

Let (K,P_1,P_2) be maximal among the algebraic OF_2-extensions of $(\mathbb{Q}(\sqrt{2}),Q_1,Q_2)$, Q_1 and Q_2 being the two orderings on $\mathbb{Q}(\sqrt{2})$.

Take models A and B of $\overline{OD_3}$ with $(K,P_1,P_1,P_2) \subset A$ and $(K,P_1,P_2,P_2) \subset B$. Note that by (2.6) K is algebraically closed in the underlying fields of A and B. Because $P_1 \neq P_2$ there is a non-constant polynomial with integral coefficients which has a root $a \in K$ such that $a >_{P_1} 0$ and $a <_{P_2} 0$, so $A \not\equiv B$. Let A' and B' be the expansions of A and B obtained by defining for A and B the predicates $\underline{W}_d$ $(d \geqslant 2)$ just as Kiefe did for pseudo-finite fields. Then A' and B' satisfy the same open sentences in the language of OD_3 extended by the predicates $\underline{W}_d$, but $A' \not\equiv B'$.

Hence $\overline{OD_3}$ extended by the defining axioms for $\underline{W}_d$, $d \geqslant 2$, is a theory not admitting elimination.

§3. *Extension problems and algebraic properties of existentially closed n-ordered fields*

Each ordered field has a real closed algebraic extension, i.e. its real closure. For $n > 1$, things are not so nice: if P is the unique ordering on $\mathbb{R}$, then $(\mathbb{R},P,P)$ has of course no extension $(K,P_1,P_2) \models \overline{OD}_2$ with $K|\mathbb{R}$ algebraic, not even such an extension with (K,P_1) archimedean over $(\mathbb{R},P)$.
So it is desirable to have some conditions on $\mathcal{K} = (K,P_1,..,P_n) \models OF_n$ which imply that $\mathcal{K}$ has an extension $\mathcal{L} = (L,Q_1,..,Q_n) \models \overline{OD}_n$ with $L|K$ algebraic, or (L,Q_i) archimedean over (K,P_i) for each $1 \leqslant i \leqslant n$.
Concerning this I found the following.

(3.1) *Theorem*

Let $\mathcal{K} = (K,P_1,..,P_n) \models OF_n$ and suppose K is a countable Hilbertian field and $P_1,..,P_n$ are independent.
Then $\mathcal{K}$ has an extension $(L,Q_1,..,Q_n) \models \overline{OD}_n$ with $L|K$ algebraic.

Before proving this: finitely generated extension fields of $\mathbb{Q}$ are countable and Hilbertian, and different archimedean orderings on a field are independent. Hence the assumptions in the theorem hold in a number of interesting cases.

(3.2) *Proposition*

Let $P_1,..,P_n$ be non-archimedean orderings on the field K. Then $(K,P_1,..,P_n)$ has an extension $(L,Q_1,..,Q_n) \models \overline{OD}_n$ with (L,Q_i) archimedean over (K,P_i), for all $1 \leqslant i \leqslant n$.

(3.3) *Proposition*

Let $P_1,..,P_n$ be archimedean orderings on the countable field K. Then $(K,P_1,..,P_n)$ has an extension $(L,Q_1,..,Q_n) \models \overline{OD}_n$ with (K,P_i) dense in (L,Q_i), for each $1 \leqslant i \leqslant n$.

For later purposes the proof of (3.1) is placed in a general model-theoretic framework by the following lemma.

(3.4) *Lemma*

Let a theory T in a language L have an axiomatization $\{\forall \bar{x}_k \exists \bar{y}_k \tau_k(\bar{x}_k,\bar{y}_k) \mid k \in \mathbb{N}\}$, with $\bar{x}_k,\bar{y}_k$ sequences of distinct variables $(x_1,..,x_{p(k)}),(y_1,..,y_{q(k)})$ respectively, and $\tau_k(\bar{x}_k,\bar{y}_k)$ an open L-formula ($k \in \mathbb{N}$).

Suppose a class $\underline{C}$ of countable L-structures is given such that for each $A \in \underline{C}$, $k \in \mathbb{N}$, and $a_1,..,a_{p(k)} \in |A|$ there is $B \in \underline{C}$ with $A \subset B$ and with $B \models \exists \bar{y}_k \, \tau_k(a_1,..,a_{p(k)},\bar{y}_k)$.

Then for each $A \in \underline{C}$ there is an ascending chain $A = B_0 \subset B_1 \subset ... \subset B_n \subset B_{n+1}...$ of structures in $\underline{C}$ with

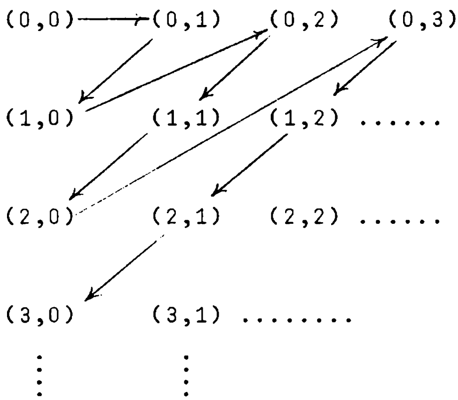
$$\bigcup_{n \in \mathbb{N}} B_n \models T.$$

Proof

Let $A \in \underline{C}$ be given. Fix for each $B \in \underline{C}$ an enumeration $(\bar{a}_B(n))_{n \in \mathbb{N}}$ of all pairs $((a_1,..,a_{p(k)}),k)$ with $a_1,..,a_{p(k)} \in |B|$ and $k \in \mathbb{N}$.

Let further $\pi: \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be the following bijection:

$\pi(0) = (0,0)$, $\pi(1) = (0,1)$, $\pi(2) = (1,0)$, $\pi(3) = (0,2)$, $\pi(4) = (1,1)$, $\pi(5) = (2,0)$, $\pi(6) = (0,3)$, etc. In the following picture one sees how $\mathbb{N} \times \mathbb{N}$ is enumerated by π:



Note that the first coordinate of $\pi(k)$ is always $\leqslant k$.

Take $\mathcal{B}_0 = \mathcal{A}$, and suppose $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_n \in \underline{C}$ have already been constructed with $\mathcal{B}_0 \subset \mathcal{B}_1 \subset \ldots \subset \mathcal{B}_n$. Let $\pi(n) = (i,j)$, so $i \leqslant n$. Then $\bar{a}_{\mathcal{B}_i}(j)$ is some pair $((a_1,\ldots,a_{p(k)}),k)$ with $(a_1,\ldots,a_{p(k)}) \in |\mathcal{B}_i|$.
Hence $a_1,\ldots,a_{p(k)} \in |\mathcal{B}_n|$; then choose for $\mathcal{B}_{n+1}$ an extension of $\mathcal{B}_n$ in $\underline{C}$ with $\mathcal{B}_{n+1} \models \exists \bar{y}_k \tau_k(a_1,\ldots,a_{p(k)},\bar{y}_k)$.
Let $\mathcal{B} = \bigcup_{n\in\mathbb{N}} \mathcal{B}_n$. Then $\mathcal{B} \models T$: let $k \in \mathbb{N}$ and $a_1,\ldots,a_{p(k)} \in |\mathcal{B}|$.
Choose $i \in \mathbb{N}$ with $a_1,\ldots,a_{p(k)} \in |\mathcal{B}_i|$ and $j \in \mathbb{N}$ with $((a_1,\ldots,a_{p(k)}),k) = \bar{a}_{\mathcal{B}_i}(j)$ and let n be such that $\pi(n) = (i,j)$; then $\mathcal{B}_{n+1} \models \exists \bar{y}_k \tau_k(a_1,\ldots,a_{p(k)},\bar{y}_k)$ by construction, so $\mathcal{B} \models \forall \bar{x}_k \exists \bar{y}_k \tau_k(\bar{x}_k,\bar{y}_k)$.
$\square$

(3.5) *Proof of (3.1)*

Let T be the theory $\mathrm{Diag}(K) \cup \overline{\mathrm{OD}}_n$, and take for $\underline{C}$ the class of all structures $(L,Q_1,\ldots,Q_n,a|a \in K)$ with $L|K$ a finite extension, and $(L,Q_1,\ldots,Q_n) \models \mathrm{OF}_n$ an extension of K.
Note that for $(L,Q_1,\ldots,Q_n,a|a \in K) \in \underline{C}$ and $1 \leqslant i < j \leqslant n$, Q_i and Q_j are independent. This is because they induce on the subfield K of L the P_i-topology, resp., the P_j-topology, which are different.
It is easy to express the axiomatization of T given by $\mathrm{Diag}(K)$ and

$(\alpha),(\beta)$ of (1.2) in the form required in (3.4), for instance (β) may be rephrased as follows:

For each $f(T,X) \in K[T,X]$, each $a \in K$ and all $r_1, s_1, \ldots, r_n, s_n \in K$ such that $f(a,r_i) <_i 0$, $f(a,s_i) >_i 0$ $(1 \leqslant i \leqslant n)$, either f is reducible in $K[T,X]$, or $\exists c,d \in K$ $f(c,d) = 0$.

Note finally that for $(L,Q_1,\ldots,Q_n,a|a \in K) \in \underline{C}$, L is also Hilbertian. Hence, in order to apply (3.4) in this situation, it suffices to prove: let M be a Hilbertian field and $R_1,\ldots,R_n$ independent orderings on M and let $f(T,X) \in M[T,X]$ be irreducible and $a \in M$ with $f(a,X)$ changing sign on M for each R_i; then there is a finite extension N of M such that $R_1,\ldots,R_n$ can be extended to orderings on N and $\exists c,d \in N$ $f(c,d) = 0$.

To prove this, choose for each $1 \leqslant i \leqslant n$ an R_i-neighbourhood U_i of a such that for each $t \in U_i$ $f(t,X)$ still changes sign in K with respect to R_i. By (1.16) there is $t \in U_1 \cap \ldots \cap U_n$ with $f(t,X) \in K[X]$ irreducible. Now the proof of (1.10) can be followed (with $K, K(t), P_i, P_i'$ replaced by M, M, R_i, R_i'). □

(3.6) *Lemma*

Let (K,P) be an ordered field such that P is either non-archimedean, or P is archimedean and K is countable. Then for each $0 < \varepsilon \in K$, $a \in K$, there exists an ordered extension $(K(X),Q)$ which is archimedean over (K,P) with $a-\varepsilon < X < a+\varepsilon$.

Proof

Replacing (K,P) by its real closure, if necessary, we may assume (K,P) real closed. The case that P is archimedean and K countable is trivial: embed (K,P) in $\mathbb{R}$, and identify X with some real number in $(a-\varepsilon,a+\varepsilon)$ which is transcendental over K.

Suppose now that P is non-archimedean. Then put $D = \{x \in K \mid \forall k \in \mathbb{N}\setminus\{0\} \quad x < a + \frac{1}{k}\varepsilon\}$ and $S = K\setminus D$. Then (D,S) is a Dedekind cut on K, and D has no largest nor has S a smallest element: if $b \in D$, then also $b+\delta\varepsilon \in D$, where $\delta \in K$ is such that $0 < \delta < \frac{1}{k}$, $\forall k \in \mathbb{N}\setminus\{0\}$.

Then by [Baer, Lemma 1.1] an ordered extension as stated exists. □

(3.7) *Proofs of (3.2) and (3.3)*

Note first that an archimedean ordered field is dense in each archimedean extension.

Hence the following statements, together with an obvious chain construction, imply (3.2) and (3.3).

Let $\mathcal{K} = (K,P_1,..,P_n) \models OF_n$ and $P_1,..,P_n$ be either all non-archimedean, or all archimedean and K countable. Then the following holds:

(1) If $1 \leqslant i < j \leqslant n$ and $0 <_i \varepsilon_1 \in K$, $0 <_j \varepsilon_2 \in K$, then $\mathcal{K}$ can be embedded into some $\mathcal{L} = (L,Q_1,..,Q_n) \models OF_n$ with an $x \in L$ satisfying $-\varepsilon_1 <_i x <_i \varepsilon_1$ and $1-\varepsilon_2 <_j x <_j 1+\varepsilon_2$ and with (L,Q_k) archimedean over (K,P_k), for all $1 \leqslant k \leqslant n$.

(2) If $f(T,X) \in K[T,X]$ is irreducible and $a \in K$ is such that $f(a,X)$ changes sign on K for each P_i, then there is an extension $\mathcal{L} = (L,Q_1,..,Q_n)$ of $\mathcal{K}$ with $(c,d) \in L\times L$ such that $f(c,d) = 0$, and with (L,Q_i) archimedean over (K,P_i), $(1 \leqslant i \leqslant n)$.

(1) and (2) are easily proved along the lines of (1.8) and (1.10), using (3.6). Note also that L in (1) and (2) can be taken to have the same cardinality as K has. This is essential for the chain construction. □

(3.8) Remark

(3.1) provides an example of a model of $(\widetilde{OD}_n)_\forall$ which has no prime extension to a model of $\widetilde{OD}_n$, for each $n > 1$: let $\overline{\mathbb{Q}}$ be the real closure of $\mathbb{Q}$, P its unique ordering, $\widetilde{K}$ the unique expansion of $K = (\mathbb{Q},P,..,P) \models OF_{n,alg}$ to a model of $(\widetilde{OD}_n)_\forall$. Let $Q_1,..,Q_n$ be different archimedean orderings on $\overline{\mathbb{Q}}(X)$, and R a non-archimedean ordering on $\overline{\mathbb{Q}}(X)$. Then $\overline{\mathbb{Q}}(X)$ is a countable Hilbertian field, and $Q_1,..,Q_n$ are independent, as well as $Q_1,..,Q_{n-1},R$.
Let $\mathcal{L}_1,\mathcal{L}_2$ be algebraic extensions of $(\overline{\mathbb{Q}}(X),Q_1,..,Q_n)$, $(\mathbb{Q}(X),Q_1,..,Q_{n-1},R)$ respectively, with $\mathcal{L}_1,\mathcal{L}_2 \models \overline{OD}_n$, and let $\widetilde{\mathcal{L}}_1,\widetilde{\mathcal{L}}_2$ be the unique expansions of $\mathcal{L}_1,\mathcal{L}_2$ to models of $\widetilde{OD}_n$.
Then $\widetilde{\mathcal{L}}_1,\widetilde{\mathcal{L}}_2$ are clearly minimal extensions of $\widetilde{K}$ to models of $\widetilde{OD}_n$, but they are not isomorphic. Hence $\widetilde{K}$ does not have a prime extension to a model of $\widetilde{OD}_n$.
Concluding this section I will indicate some of the interesting algebraic properties of model of $\overline{OD}_n$.

(3.9) Lemma

Let $P_1,..,P_n$ be independent orderings on a field K. Then $P_1,..,P_n$ are the only orderings on K containing $P_1 \cap ... \cap P_n$.

Proof

Suppose Q is another ordering on K containing $P_1 \cap ... \cap P_n$. Let m with $1 \leq m \leq n$ be minimal with $Q \supset P_1 \cap ... \cap P_m$. Then $m > 1$ and $P_1 \cap ... \cap P_{m-1} \cap Q$ is strictly included in $P_1 \cap ... \cap P_{m-1}$. But $[K^\bullet : P_1^\bullet \cap ... \cap P_{m-1}^\bullet] = 2^{m-1}$, because the canonical map

$$K^\bullet/_{P_1^\bullet \cap ... \cap P_{m-1}^\bullet} \to K^\bullet/_{P_1^\bullet} \times ... \times K^\bullet/_{P_{m-1}^\bullet}$$

is an isomorphism of groups, by (1.7), and similarly $[K^\bullet : P_1^\bullet \cap .. \cap P_m^\bullet] = 2^m$, and $P_1 \cap ... \cap P_{m-1} \supsetneqq P_1 \cap ... \cap P_{m-1} \cap Q \supset P_1 \cap ... \cap P_m$, so necessarily

$P_1 \cap\ldots\cap P_{m-1} \cap Q = P_1 \cap\ldots\cap P_m$.

Choose $q \in Q\setminus P_m$; adding, if necessary, to q an element of $P_1 \cap\ldots\cap P_n$ which is sufficiently close to 0 with respect to P_m, and sufficiently large with respect to $P_1,\ldots,P_{m-1}$, we get:

$$q \in P_1 \cap\ldots\cap P_{m-1} \cap Q = P_1 \cap\ldots\cap P_m,$$

so $q \in P_m$, contradiction. □

(3.10) Recall that associated with a real field K is the non-empty boolean space $\mathcal{O}(K)$ of all its orderings. A subbasis for the topology is given by the sets $W_K(a) = \{P \in \mathcal{O}(K) | a \text{ is negative for } P\}$. This is called the Harrison subbasis. That it defines a boolean, i.e. compact and totally disconnected, topology follows easily from an obvious 1-1 correspondence of $\mathcal{O}(K)$ with the set of ultra filters on the boolean algebra of open sentences in the language of OF ∪ Diag(K), modulo equivalence with respect to the theory OF ∪ Diag(K). Typically, algebraists prove the same fact using a 1-1 correspondence with the set of minimal prime ideals of the Wittring of K.

Definition

An SAP-field (Knebusch) is a real field K such that the Harrison subbasis is a basis of $\mathcal{O}(K)$.

(3.11) *Proposition*

If $(K,P_1,\ldots,P_n) \models \overline{OD}_n$, then $P_1,\ldots,P_n$ are the only orderings on K, and K is an SAP-field.

Proof

That $P_1,\ldots,P_n$ are the only orderings on K follows from (3.9) and $P_1 \cap\ldots\cap P_n = K^2$. Take for each $1 \leq i \leq n$ $a_i \in K$ such that a_i is negative with respect to P_i and positive with respect to the other orderings on K.

Then $W_k(a_i) = \{P_i\}$. So K is an SAP-field. $\square$

(3.12) The absolute Galoisgroup of existentially closed n-ordered fields is completely known as the following theorem shows.

Let $(K,P_1,..,P_n) \models OF_{n,alg}$. Take for each $1 \leqslant k \leqslant n$ a real closure R_k of (K,P_k) within a fixed algebraic closure $\tilde{K}$ of K, and let $\sigma_k \in Gal(\tilde{K}|K)$ be the conjugation over R_k, i.e. $\sigma_k(i) = -i$ and $\sigma_k|R_k = id(R_k)$. Clearly

$$K = R_1 \cap ... \cap R_n = \text{fixed field of } \{\sigma_1,..,\sigma_n\}.$$

Hence by the main theorem of infinite Galois theory, $Gal(\tilde{K}|K)$ is topologically generated by $\{\sigma_1,..,\sigma_n\}$.

(3.13) *Theorem*

If under the above assumptions, either $P_1,..,P_n$ are independent or $n = 2$ and $P_1 \neq P_2$, then $Gal(\tilde{K}|K)$ is the free product within the category of profinite 2-groups of its subgroups $\{1,\sigma_1\},...,\{1,\sigma_n\}$.

For $n = 2$ and $P_1 \neq P_2$ this is proved in [Br., Er.,& Ka.].
The authors even construct explicitly R_1 and R_2 in this case: if $x \in K$ is such that $x >_1 0$ and $x <_2 0$, then R_1 can be chosen as

$$K(\sqrt[2^n]{x} \mid n \in \mathbb{N}),$$

and R_2 as

$$K(\varepsilon_{n+1}\sqrt[2^n]{x} \mid n \in \mathbb{N}),$$

where of course

$$(\sqrt[2^{n+1}]{x})^2 = \sqrt[2^n]{x},\ \sqrt[1]{x} = x,$$

and (ε_{n+1}) is any sequence of roots of unity with $\varepsilon_1 = 1$, $\varepsilon_2 = -1$, $(\varepsilon_{n+1})^2 = \varepsilon_n$ for all $n \geqslant 1$.

It is stated in [Er, p.428] that Kal'nei has generalized this to the case that $n > 2$ and the orderings are independent (unpublished as far as I know).

CHAPTER III *Model theory of fields with several orderings and valuations*

§1. *The model companion*

The situation of Ch. II is generalized so as to cover also (Krull) valuations of certain types on a field of characteristic 0 (prime characteristic causes some technical difficulties and is not considered in order to show the main idea as clearly as possible). Alas, some new terminology is indispensable.

(1.1) *Definition*

A t-language ('t' for 'topology') is a language extending the language of rings with extra constants and predicate symbols (but no extra function symbols of rank >0).

(1.2) *Definition*

A t-theory is a universal theory T in a t-language, together with a distinguished open formula $B_T(v_1,..,v_k,v_{k+1})$ such that the following conditions are satisfied:

(a) T extends the theory of domains.

(b) If $\mathcal{D}_1,\mathcal{D}_2$ are models of T with the same underlying domain D such that for each constant $\underline{c}$ and each (say p-ary) predicate symbol $\underline{R}$: $\underline{c}^{\mathcal{D}_1} = \underline{c}^{\mathcal{D}_2}$ and $\underline{R}^{\mathcal{D}_1} \cap (D^\cdot)^p = \underline{R}^{\mathcal{D}_2} \cap (D^\cdot)^p$ ($D^\cdot = D\setminus\{0\}$), then $\mathcal{D}_1 = \mathcal{D}_2$.

(c) Each model $\mathcal{D}$ of T with underlying domain D has a unique extension to a model K with underlying domain Q(D); this model K will be denoted by $Q(\mathcal{D})$.

(d) For each model K of T $\cup$ FL with underlying field K the family of all sets $\{b \in K | K \models B_T(a_1,..,a_k,b)\}$ $((a_1,..,a_k) \in K^k)$ is a

basis of neighbourhoods of 0 for a (necessarily unique) Hausdorff ring topology on K;
this topology will be denoted by τ_K.

(e) For each model K of $T \cup FL$ with underlying field K and each (say p-ary) predicate symbol $\underline{R}$ $\underline{R}^K \cap (K^{\cdot})^p$ is a clopen subset of $(K^{\cdot})^p$, where $(K^{\cdot})^p$ is endowed with the product topology induced by τ_K.

(1.3) *Examples*

(1) OD (cf. Ch.I, (3.2)) is a t-theory with distinguished formula

$$B_{OD}(v_1, v_2, v_3) := (v_1 < v_3 < v_2) \wedge (v_1 < 0 < v_2).$$

(This expression is of course shorthand for a formula using only the unary predicate symbol '$\underline{P}$' in stead of '<'.)

(a), *(b)* and *(c)* are trivial. It is also wellknown that $B_{OD}(v_1, v_2, v_3)$ induces the interval topology defined by the ordering of an ordered field; so *(d)* follows. *(e)* means that for an ordering on the field K the set $\{a \in K | a > 0\}$ is a clopen subset of $K^{\cdot}$ with respect to the interval topology. (It is certainly not a clopen subset of K.)

(2) D_{val} (cf. Ch.I, (3.3)) is a t-theory with distinguished formula $B_{val}(v_1, v_2) := \underline{div}(v_1, v_2) \wedge v_1 \neq 0$.

(a), *(b)* and *(c)* are again trivial.

(d) is also easy: given a field K with valuation $v : K \to \Gamma \cup \{\infty\}$, the family of all sets $\{b \in K | v(b) \geq g\}$ $(g \in \Gamma)$ defines a basis of (clopen) neighbourhoods of 0 for the, so called, valuation topology on K induced by v.

Just as an interval topology, it is a V-topology (cf. Ch.II (1,6)).

(e) is easily checked.

(3) $(pCF)_\forall$ and $(\underline{\pi}CF)_\forall$ (cf. Ch.I, (3.6) and (3.7)) are t-theories

with same distinguished formula $B_{val}(v_1, v_2)$ as above.
Again the required conditions are easily checked, except perhaps (e) for the predicates $\underline{P}_n$ $(n \geq 2)$.
Let $K = (K, \mathrm{div}_K, P_2, P_3, ..) \models$ pFL. If $a \in K$ and $v_K(a) > 2.v_K(n)$, then $v_K((1+\frac{1}{n}a)^n - (1+a)) > 2.v_K(n)$, which implies by a strong form of Hensel's lemma (cf. Appendix, (A.2)) that $1+a$ is an n^{th} power in the prime extension of K, so $1+a \in P_n$.
But then $P_n \setminus \{0\}$ is an open subgroup of $K^{\cdot}$, hence also a closed subgroup.
The argument for $(\underline{\pi}CF)_\forall$ is similar, but easier and is left to the reader.

(1.4) *Definition*

Let $n \geq 1$ and $T_1, .., T_n$ be t-theories.
The theory $(T_1, .., T_n)$ is then defined as the theory whose models are the structures $(D, \mathcal{P}_1, .., \mathcal{P}_n)$ with D a domain and $(D, \mathcal{P}_i) \models T_i$, $i = 1, .., n$.

Remark

If the language $L(T_i)$ of T_i and $L(T_j)$ of T_j have for all i,j with $1 \leq i < j \leq n$ only the ring operation symbols in common, then formally: $L(T_1, .., T_n) = L(T_1) \cup ... \cup L(T_n)$ and $(T_1, .., T_n) \models T_1 \cup ... \cup T_n$.
However, in cases like $T_1 = ... = T_n = OD$, the procedure is to make $L(T_1), ..., L(T_n)$ first disjoint, except for the ring operation symbols, by an obvious indexing and then defining $(T_1, .., T_n)$ formally as above.
So if $T_1 = ... = T_n = OD$, we get $(T_1, .., T_n) = OD_n$ (cf. Ch.II).

(1.5) *Basic conventions for the rest of this chapter*

n is a fixed integer ≥ 1. $T_1, .., T_n$ are fixed t-theories, such that for

<u>each</u> $1 \leqslant i \leqslant n$:

T_i <u>has a model completion</u> $\bar{T}_i$ <u>and for each model</u>
$K = (K,\ldots) \models \bar{T}_i$: $\mathrm{char}(K) = 0$ <u>and</u> τ_K <u>is not discrete.</u>
(note that by condition (c) of (1.2) K is indeed a field).

Remark

If each T_i is chosen from among OD, $D_{val,0}$, $(pCF)_V$(p prime), $(\underline{\pi}CF)_V$, then these assumptions on T_i are satisfied.
($D_{val,0}$ is D_{val} + axioms expressing characteristic 0.)

Now the theorem corresponding to (1.2) of Ch. II is:

(1.6) *Theorem*

$(T_1,\ldots,T_n)$ <u>has a model companion.</u>

The proof is given in (1.12), (1.13) and (1.14).
First some preparations.

(1.7) *Lemma*

Let (G,τ) be a topological group with τ Hausdorff and not discrete.
Then each non-empty open subset of G is infinite.

Proof

Clear. $\square$

(1.8) *Lemma*

Let T be a t-theory and $\Theta(v_1,\ldots,v_k)$ be an open L(T)-formula. Then there is an open L(T)-formula $\Theta'(v_1,\ldots,v_k,v_{k+1},\ldots,v_{2k})$ such that for each $\mathcal{D} \models T$ and $a_1,\ldots,a_k \in |\mathcal{D}|$, $b_1,\ldots,b_k \in |\mathcal{D}|\setminus\{0\}$:

$$Q(\mathcal{D}) \models \Theta(a_1 b_1^{-1},\ldots,a_k b_k^{-1}) \Leftrightarrow \mathcal{D} \models \Theta'(a_1,\ldots,a_k,b_1,\ldots,b_k)$$

Proof

Let $\underline{a}_1,..,\underline{a}_k,\underline{b}_1,..,\underline{b}_k$ be new constants and consider the set Γ of all open sentences $\psi(\underline{a}_1,..,\underline{a}_k,\underline{b}_1,..,\underline{b}_k)$ with

$$T \vdash \forall z_1..\forall z_k((\theta(z_1,..,z_k) \wedge \bigwedge_{i=1}^{k} \underline{b}_i z_i = \underline{a}_i \wedge \underline{b}_i \neq 0) \rightarrow \psi(\underline{a}_1,..,\underline{a}_k,\underline{b}_1,..,\underline{b}_k)).$$

Let us write $\underline{a}$; $\underline{b}$; $\underline{z}$; $\forall z$ etc. for $\underline{a}_1,..,\underline{a}_k$; $\underline{b}_1,..,\underline{b}_k$; $z_1,..,z_k$; $\forall z_1..\forall z_k$. It clearly suffices to prove the following:

Claim

$$T \cup \Gamma \vdash \forall z((\bigwedge_{i=1}^{k} \underline{b}_i z_i = \underline{a}_i \wedge \underline{b}_i \neq 0) \rightarrow \theta(z)).$$

Take any model $K' = (K,a,b)$ of $T \cup \Gamma$ with $b_i \neq 0$ $(1 \leqslant i \leqslant k)$ and suppose there are $c_1,..,c_k \in |K|$ with $b_i c_i = a_i$ $(1 \leqslant i \leqslant k)$ and $K' \models \neg\theta(c)$ (such K' exists if the claim would not be true).
Because $c_i = a_i b_i^{-1}$ and $\Gamma \cup \{\theta\}$ consists of open formulas, one may assume without loss of generality that $K = Q(\mathcal{D})$, where $\mathcal{D}$ is generated by $\{a_1,..,a_k,b_1,..,b_k\}$.
Let $\mathcal{D}' = (\mathcal{D},a,b)$. Then from condition (c) of (1.2) we get:

$$T \cup \mathrm{Diag}(\mathcal{D}') \vdash \forall z((\bigwedge_{i=1}^{k} \underline{b}_i z_i = \underline{a}_i) \rightarrow \neg\theta(z)).$$

Hence, by the compactness theorem, there is an open formula $\phi(v_1,..,v_{2k})$ with

$$\mathcal{D}' \models \phi(\underline{a},\underline{b}) \text{ and } T \vdash \phi(\underline{a},\underline{b}) \rightarrow \forall z((\bigwedge_{i=1}^{k} \underline{b}_i z_i = \underline{a}_i) \rightarrow \neg\theta(z)),$$

implying:

$$T \vdash \forall z((\theta(z) \wedge \bigwedge_{i=1}^{k} (\underline{b}_i z_i = \underline{a}_i \wedge \underline{b}_i \neq 0)) \rightarrow \neg\theta(\underline{a},\underline{b})),$$

so $\neg\phi(\underline{a},\underline{b}) \in \Gamma$, which contradicts $\mathcal{D}' \models \Gamma \cup \{\phi(\underline{a},\underline{b})\}$. $\square$

Remark

If T is given, say T = OD, then this model theoretic proof can be avoided, and Θ' can be easily constructed from Θ. Note that conditions *(b)*, *(d)* and *(e)* of (1.2) on T were not needed in the proof of the lemma.

(1.9) Let in the following $u_1,..,u_\ell,x_1,..,x_m,y$ denote distinct variables, and let u,x denote the sequences $u_1,..,u_\ell$ and $x_1,..,x_m$ respectively.
It is also desirable to use these variables in polynomials but to distinguish this use I will write in that case capital letters $U_1,..,U_\ell,X_1,..,X_m,Y$ and U,X.
It will be clear that, for instance, '$\exists x$' is used as shorthand for '$\exists x_1 .. \exists x_m$'.

Definition

Let T be a t-theory.
A t-basic T-formula in (u,x) is a formula in the language of T of one of the following forms:

(i) $\underline{R}(S_1(u,x),..,S_p(u,x)) \wedge \bigwedge_{i=1}^{p} S_i(u,x) \neq 0$

(ii) $\neg\underline{R}(S_1(u,x),..,S_p(u,x)) \wedge \bigwedge_{i=1}^{p} S_i(u,x) \neq 0$

where $\underline{R}$ is a p-ary predicate symbol and

$S_1,..,S_p \in \mathbb{Z}[U,X]$.

Lemma

Let T be a t-theory and $\phi(u,x)$ be a conjunction of t-basic T-formulas in (u,x) and suppose $K = (K,\mathcal{P}) \models T \cup FL$ and $a \in K^\ell = K \times ... \times K$ (cartesian product).
Then $\{b \in K^m | K \models \phi(a,b)\}$ is an open subset of K^m.

Proof

Clearly it suffices to consider the case that $\phi(u,x)$ is t-basic. Then the conclusion of the lemma is an easy consequence of the continuity of polynomial functions, condition *(e)* of (1.2), and the definition of t-basic formula. □

(1.10) *Definition*

Let $\ell, m \in \mathbb{N}$. An (ℓ,m)-condition is a sequence

$$\langle \sigma_1(u),..,\sigma_n(u),\phi_1(u,x),..,\phi_n(u,x),\Theta_1(u,x,y),..,\Theta_n(u,x,y),F(u,x,y)\rangle$$

with $u = (u_1,..,u_\ell)$, $x = (x_1,..,x_m)$ such that for each $1 \leqslant i \leqslant n$:

(1) $\sigma_i(u)$ is an open $L(T_i)$-formula.

(2) $\phi_i(u,x)$ is a conjunction of t-basic T_i-formulas in (u,x).

(3) $\Theta_i(u,x,y)$ is an open $L(T_i)$-formula.

(4) $F(U,X,Y)$ is a polynomial in $\mathbb{Z}[U,X,Y]$, monic and of positive degree in Y.

(5) $\overline{T}_i \vdash \forall u(\sigma_i(u) \to \exists x\phi_i(u,x))$, and
$\overline{T}_i \vdash \forall u\forall x\{(\sigma_i(u) \wedge \phi_i(u,x)) \to \exists y(F(u,x,y) = 0 \wedge \Theta_i(u,x,y))\}$

(1.11) *Definition*

$\overline{(T_1,..,T_n)}$ is the theory whose models are those

$$K = (K,\mathcal{P}_1,..,\mathcal{P}_n) \models (T_1,..,T_n)$$

such that:

(i) K is a field

(ii) for each (ℓ,m)-condition as in (1.10) and each $a \in K^\ell$, such that $F(a,X_1,..,X_m,Y) \in K[X_1,..,X_m,Y]$ is irreducible and $K \models \bigwedge_{i=n}^{n} \sigma_i(a)$, the following holds:

$$K \models \exists x\exists y\{F(a,x,y) = 0 \wedge \bigwedge_{i=1}^{n} (\phi_i(a,x) \wedge \Theta_i(a,x,y))\}.$$

Note that *(i)* and *(ii)* actually say that K satisfies certain sentences, so (1.11) defines indeed a theory.

Now (1.6) can be made more explicit as follows:

(1.12) $\overline{(T_1,..,T_n)}$ <u>is model companion of</u> $(T_1,..,T_n)$.

Using (2.21) of Ch. I we split the proof of (1.12) in two parts:

A. Each existentially closed model of $(T_1,..,T_n)$ is a model of $\overline{(T_1,..,T_n)}$.

B. Each model of $\overline{(T_1,..,T_n)}$ is an existentially closed model of $(T_1,..,T_n)$.

(1.13) *Proof of (1.12), part A.*

Let $K = (K,\mathcal{O}_1,..,\mathcal{O}_n)$ be an existentially closed model of $(T_1,..,T_n)$.
Let $K_i = (K,\mathcal{O}_i)$ and note that $K_i \models T_i$.
That K is a field follows immediately from condition (c) of (1.2) which holds for each T_i.

Let now an (ℓ,m)-condition be given as in (1.10) (the notation used in (1.10) is preserved here), and let $a \in K^\ell$ be such that $F(a,X_1,..,X_m,Y) \in K[X_1,..,X_m,Y]$ is irreducible and for all $1 \leqslant i \leqslant n$:

$$K_i \models \sigma_i(a).$$

Let for each $1 \leqslant i \leqslant n$ $F_i = (F_i,..)$ be a $(\# K)^+$-saturated extension of K_i with $F_i \models \overline{T}_i$.
Then, by (5) of (1.10), we get: $F_i \models \exists x \phi_i(a,x)$.
So the set $\{b \in F_i^m | F_i \models \phi_i(a,b)\}$ is non-empty, and open by the lemma in (1.9), hence by (1.7) and the fact that τ_{F_i} is not discrete, this set contains a cartesian product $B_1 x ... x B_m$ with B_j an infinite subset of F_i.
Because F_i is $(\# K)^+$-saturated, this implies that there is

$(b_1^i,..,b_m^i) \in F_i^m$ with $\mathcal{F}_i \models \phi_i(a,b_1^i,..,b_m^i)$ and $b_1^i,..,b_m^i$ <u>algebraically independent over K.</u>

Then, by (5) of (1.10), there is $c^i \in F_i$ with $F(a,b_1^i,..,b_m^i,c^i) = 0$ and $\mathcal{F}_i \models \Theta_i(a,b_1^i,..,b_m^i,c^i)$.

Because $F(a,X_1,..,X_m,Y)$ is irreducible, the fields $K(b_1^i,..,b_m^i,c^i)$ and $K(b_1^j,..,b_m^j,c^j)$ are for any i and j in $\{1,..,n\}$ isomorphic over K via an isomorphism sending b_r^i to b_r^j and c^i to c^j. These isomorphisms permit us to construct an extension

$$\mathcal{L} = (K(b_1,..,b_m,c),\mathcal{R}_1,..,\mathcal{R}_n) \models (T_1,..,T_n)$$

of $\mathcal{K}$ such that for each $1 \leqslant i \leqslant n$ $(K(b_1,..,b_m,c),\mathcal{R}_i)$ embeds into $\mathcal{F}_i$ over K via $b_r \mapsto b_r^i, c \mapsto c^i$, $1 \leqslant r \leqslant m$.

Hence

$$\mathcal{L} \models F(a,b_1,..,b_m,c) = 0 \wedge \bigwedge_{i=1}^{n} (\phi_i(a,b_1,..,b_m) \wedge \Theta_i(a,b_1,..,b_m,c)).$$

Because $\mathcal{K}$ is existentially closed, this implies

$$\mathcal{K} \models \exists x \exists y\ F(a,x,y) = 0 \wedge \bigwedge_{i=1}^{n} (\phi_i(a,x) \wedge \Theta_i(a,x,y)). \quad \square$$

(1.14) <u>*Proof of (1.12), part B*</u> (compare with Ch. II (1.19)).

Let $\mathcal{K} = (K,\mathcal{P}_1,..,\mathcal{P}_n)$ be a model of $\overline{(T_1,..,T_n)}$, and let $\mathcal{K}_i = (K,\mathcal{P}_i) \models T_i$. Suppose ρ is an existential $\mathcal{K}$-sentence true in an extension $\mathcal{L} = (L,\mathcal{R}_1,..,\mathcal{R}_n) \models (T_1,..,T_n)$ of $\mathcal{K}$.

<u>To prove</u>: <u>ρ is true in $\mathcal{K}$.</u>

Without loss of generality we assume L to be a finitely generated field extension of K. Because char(K) = 0 by the assumption of (1.5), this implies that $L = K(b_1,..,b_m,c)$ with $(b_1,..,b_m)$ a transcendence base of $L|K$ and such that for a certain irreducible $F(X_1,..,X_m,Y) \in K[X_1,..,X_m,Y]$ $F(b_1,..,b_m,Y)$ is the minimum polynomial of c over $K(b_1,..,b_m)$ (in particular $F(X,Y)$ is monic and of positive degree in Y).

In the following 'b' will be written as shorthand for the sequence $b_1,\dots,b_m$. Let $K_i(b)$ be the substructure of $(L,\mathcal{R}_i)$ with underlying domain $K(b)$, and similarly $K(b)$ is the substructure of $\mathcal{L}$ with underlying domain $K(b)$.

Consider the following sets of sentences in the language of $(T_1,\dots,T_n)$ augmented by names for the elements of K and new constants $\underline{b}_1,\dots,\underline{b}_m,\underline{c}$ (with '$\underline{b}$' written for the sequence $\underline{b}_1,\dots,\underline{b}_m$):

$\Gamma_{1,i} = T_i \cup FL \cup \mathrm{Diag}(K_i)$ for each $1 \leqslant i \leqslant n$;

$\Gamma_1 = \Gamma_{1,1} \cup \Gamma_{1,2} \cup\dots\cup \Gamma_{1,n} = (T_1,\dots,T_n) \cup \mathrm{Diag}(K) \cup FL$;

for each $1 \leqslant i \leqslant n$:

$\Gamma_{2,i}$ is the set of all sentences $\phi(a,\underline{b})$ where for some $\ell \in \mathbb{N}$ and $a \in K^\ell$ $\phi(u,x)$ $(u = (u_1,\dots,u_\ell),\ x = (x_1,\dots,x_m))$ is a t-basic T_i-formula in (u,x) such that $K_i(b) \models \phi(a,\underline{b})$ (where $\underline{b}_i$ is interpreted as b_i);

$\Gamma_2 = \Gamma_{2,1} \cup\dots\cup \Gamma_{2,n}$.

It is easily shown that conditions (*b*) and (*c*) of (1.2) imply for each $1 \leqslant i \leqslant n$ that $(K_i(b),b) \models \Gamma_{1,i} \cup \Gamma_{2,i}$ and that $(K_i(b),b)$ can be embedded (uniquely) over K_i into each model of $\Gamma_{1,i} \cup \Gamma_{2,i}$. Hence:

(*1*) $(K(b),b) \models \Gamma_1 \cup \Gamma_2$ and $(K(b),b)$ can be embedded uniquely over K into each model of $\Gamma_1 \cup \Gamma_2$.

Let $0 < d = \deg_Y F(X,Y)$.

The $K_i(b)$-formula '$F(\underline{b},y) = 0$' in the free variable y is algebraic of degree $\leqslant d$ over $K_i(b)$ with respect to the theory T_i (see Ch. I (3.5) for the definition of algebraic formula used here).

c realizes the formula in $(L,\mathcal{R}_i)$ and T_i is universal and has AP by the assumptions made in (1.5) on T_i.

Hence Th. 4.1. of [Bac] can be applied, and gives:

the open type of c over $K_i(b)$ is principal (this can of course also be seen directly by an easy argument).

We may assume this open type to be generated by a formula '$F(b,y) = 0 \wedge \Theta_i(y)$' where Θ_i is an <u>open</u> $K_i(b)$-formula.

By lemma (1.8) we may assume (par abus de langage):

$\Theta_i(y) = \Theta_i(\underline{b},y)$, with $\Theta_i(x,y)$ an open K_i-formula.

Put $\Gamma_3 = \{F(\underline{b},\underline{c}) = 0,\ \Theta_1(b,c),..,\Theta_n(\underline{b},\underline{c})\}$.

Then, by (1) above and the properties of the Θ_i's, we get:

$(\mathcal{L},b,c) \models \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ and $\mathcal{L}(b,c)$ can be embedded over K in each model of $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$.

This implies that the existential K-sentence ρ is true in each model of $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$, so by the compactness theorem there are finite subsets $\Delta_1,..,\Delta_n$ of $\Gamma_{2,1},..,\Gamma_{2,n}$ respectively such that:

(2) $\quad \Gamma_1 \cup \Delta \cup \Gamma_3 \vdash \rho \quad$ (with $\Delta = \Delta_1 \cup\ldots\cup \Delta_n$).

<u>Now we come to the essential point of the proof:</u>

because T_i has <u>model completion</u> $\overline{T}_i$, there is (for each $1 \leqslant i \leqslant n$) an open K_i-formula $\psi_i(x)$ such that:

(3) $\quad \overline{T}_i \cup \mathrm{Diag}(K_i) \vdash \psi_i(x) \leftrightarrow \exists y(F(x,y) = 0 \wedge \Theta_i(x,y))$.

Then $(K_i(b),b) \models \psi_i(\underline{b})$, so by the remark preceding (1):

$\Gamma_{1,i} \cup \Gamma_{2,i} \vdash \psi_i(\underline{b})$. So by the compactness theorem there is a finite subset of $\Gamma_{2,i}$ which together with $\Gamma_{1,i}$ has $\psi_i(\underline{b})$ as logical consequence.

Without loss of generality we may suppose this finite subset to be Δ_i. Hence $\Gamma_{1,i} \cup \Delta_i \vdash \psi_i(\underline{b})$. Together with (3) this gives for each $1 \leqslant i \leqslant n$:

(4) $\quad \overline{T}_i \cup \mathrm{Diag}(K_i) \cup \Delta_i \vdash \exists y(F(\underline{b},y) = 0 \wedge \Theta_i(\underline{b},y))$.

Let $\phi_i(\underline{b})$ be the conjunction of the sentences in Δ_i.
Then, because $K_i \subset K_i(b) \models \phi_i(\underline{b})$, we get also:

(5) $\quad \overline{T}_i \cup \mathrm{Diag}(K_i) \vdash \exists x \phi_i(x)$.

By the compactness theorem we can strengthen (2), (4) and (5) as follows: there is for each $1 \leqslant i \leqslant n$ an open K_i-sentence σ_i with $K_i \models \sigma_i$ such that:

(6) $\quad (T_1,..,T_n) \cup FL \cup \{\sigma\ ,..,\sigma_n,\phi_1(\underline{b}),..,\phi_n(\underline{b})\} \cup \Gamma_3 \vdash \rho$.

(7) $\quad \overline{T}_i \cup \{\sigma_i,\phi_i(\underline{b})\} \vdash \exists y(F(\underline{b},y) = 0 \wedge \Theta_i(\underline{b},y)) \quad (1 \leqslant i \leqslant n)$.

(8) $\quad \overline{T}_i \cup \{\sigma_i\} \vdash \exists x \phi_i(x) \quad (1 \leqslant i \leqslant n)$.

It is now necessary to display also the elements of K occurring in the various formulas: we can choose $\ell \in \mathbb{N}$ and $a \in K^\ell$ such that (by abuse of language):

(9) $\quad \Theta_i(x,y) = \Theta_i(a,x,y)$ for a certain open $L(T_i)$-formula
$\Theta_i(u,x,y) \quad (u = (u_1,..,u_\ell)) \quad (1 \leqslant i \leqslant n)$.

(10) $\quad F(X,Y) = F(a,X,Y)$ for a certain $F(U,X,Y) \in \mathbb{Z}[U,X,Y]$.

(11) $\phi_i(\underline{b}) = \phi_i(a,\underline{b})$ for a certain conjunction $\phi_i(u,x)$ of t-basic T_i-formulas in (u,x) $(1 \leqslant i \leqslant n)$.

(12) $\sigma_i = \sigma_i(a)$ for a certain open $L(T_i)$-formula $\sigma_i(u)$ $(1 \leqslant i \leqslant n)$.

Then (7) - (12) imply that
$\langle \sigma_1(u),..,\sigma_n(u),\phi_1(u,x),..,\phi_n(u,x),\Theta_1(u,x,y),..,\Theta_n(u,x,y),F(u,x,y)\rangle$
is an (ℓ,m)-condition (see (1.10)).
Then $K \models \overline{(T_1,..,T_n)}$ implies, by *(ii)* of (1.11), that there are elements $\underline{b}_1',..,\underline{b}_m',\underline{c}'$ in K such that, if $\underline{b}_1,..,\underline{b}_m,\underline{c}$ are interpreted as $b_1',..,b_m',c'$, then:

$$(K,b_1',..,b_m',c') \models F(a,\underline{b},\underline{c}) = 0 \wedge \bigwedge_{i=1}^{n} \phi_i(a,\underline{b}) \wedge \Theta_i(a,\underline{b},\underline{c}),$$

which, by (6), implies: $K \models \rho$. □

In §2 it will be shown that the axiomatization of $\overline{(T_1,..,T_n)}$ given by *(i)* and *(ii)* of (1.11) can be simplified considerably.
But first some properties of models of $\overline{(T_1,..,T_n)}$

(1.15) *Definition*

If $\tau_1,..,\tau_n$ are topologies on a set R, then $\tau_1 \vee ... \vee \tau_n$ is by definition the least upper bound of $\{\tau_1,..,\tau_n\}$ in the set of topologies on R (which is ordered by inclusion).
It is easily checked that if R is a ring and $\tau_1,..,\tau_n$ are ring topologies, then $\tau_1 \vee ... \vee \tau_n$ is a ring topology on R and a basis of 0-neighbourhoods is given by the sets $U_1 \cap ... \cap U_n$ with U_i a τ_i-neighbourhood of 0, for all $1 \leqslant i \leqslant n$.

(1.16) *Proposition*

Let $K = (K,P_1,..P_n)$ be an existentially closed model of $(T_1,..,T_n)$,

$K_i = (K, P_i) \models T_i \quad (1 \leqslant i \leqslant n)$. Then:

(i) $\tau_{K_1} \vee \ldots \vee \tau_{K_n}$ is not discrete and no τ_{K_i} is discrete.

(ii) If for each $1 \leqslant i \leqslant n$ U_i is a non-empty τ_{K_i}-open subset of K, then $U_1 \cap \ldots \cap U_n \neq \emptyset$ (and hence is infinite by *(i)* and (1.7)).

Proof

T_i has as distinguished formula $B_{T_i}(v_1, \ldots, v_k, v_{k+1})$ and without loss of generality we may assume $k \in \mathbb{N}$ to be the same for all $1 \leqslant i \leqslant n$. A typical $\tau_{K_1} \vee \ldots \vee \tau_{K_n}$ neighbourhood of $0 \in K$ is

$$\bigcap_{i=1}^{n} \{b \in K \mid K_i \models B_{T_i}(a_i, b)\} \quad (a_1, \ldots, a_n \text{ elements of } K^k),$$

and it suffices to prove that such a neighbourhood contains an element $\neq 0$. Let, as in (1.13), $F_i = (F_i, \ldots)$ be a $(\# K)^+$-saturated extension of K_i with $F_i \models \overline{T}_i$. Then $\{b \in |F_i| : F_i \models B_{T_i}(a_i, b)\}$ is infinite by (1.7), so by saturatedness contains an element transcendental over. K, which implies that K_i has an extension $(K(X), \mathcal{R}_i) = T_i \cup \{B_{T_i}(a_i, X)\}$. Then

$$\mathcal{L} = (K(X), \mathcal{R}_1, \ldots, \mathcal{R}_n) \models (T_1, \ldots, T_n) \cup \{\exists x \neq 0 \ \bigwedge_{i=1}^{n} B_{T_i}(a_i, x)\},$$

hence, because K is existentially closed, the above mentioned set contains an element $\neq 0$, and *(i)* is proved.

(ii) can be proved similarly. □

(1.17) In Ch. II, (1.14) we proved that, roughly speaking, an existentially closed model of OD_n is dense in each of its n real closures. It is not clear to me whether the analogue in our general situation holds. However, the next proposition gives important cases in which it is valid.

First a lemma.

(1.18) Lemma

Let (K,P) be an ordered, respectively (K,v) a valued field. Then:

(1) K is dense in the real closure of (K,P) $\Leftrightarrow$
for each polynomial $f(Y) \in K[Y]$ and all $a,b,\varepsilon \in K$ with $a < b, 0 < \varepsilon$ and $f(a) < 0 < f(b)$ there is c with $a < c < b$ and $|f(c)| < \varepsilon$.

(2) K is dense in the henselization of (K,v) $\Leftrightarrow$
for each polynomial $f \in V_v[Y]$ and $a \in V_v$ such that $f(a) \in M_v$, and $f'(a) \notin M_v$, the set $\{v(f(a+m)) \mid m \in M_v\}$ has no upper bound in Γ_v.

Proof

It is clear that the first half of (1), resp. (2) implies the second half.

Suppose now that the second half of (1), resp. (2) holds. Then this half clearly remains valid if (K,P) resp. (K,v) is replaced by its completion $(\hat{K},\hat{P})$, resp. $(\hat{K},\hat{v})$.

But a result of Kaplansky, [Ka], says that in a complete V-topological field F polynomial maps $F \to F$ are closed maps; this implies in our case that $(\hat{K},\hat{P})$ is real closed, resp. $(\hat{K},\hat{v})$ is henselian.

So the real closure $(\overline{K},\overline{P})$ of (K,P) embeds over (K,P) into $(\hat{K},\hat{P})$, and because K is dense in $\hat{K}$, K is also dense in $\overline{K}$. The valued field case is treated similarly. □

Remark

For an algebraic proof of (1) and a nice application, see McKenna, [McK].

(1.19) Proposition

Let $\mathcal{K} = (K,\mathcal{P}_1,\ldots,\mathcal{P}_n)$ be an existentially closed model of $(T_1,\ldots,T_n)$, $\mathcal{K}_i \models T_i$ for all $1 \leq i \leq n$. Suppose T_1 is one of the theories OD,

$(pCF)_\forall$ (p a prime), $(\underline{\pi}CF)_\forall$.
Then K is dense in L where $\mathcal{L}_1 = (L, \mathcal{R}_1)$ is the prime extension of $\mathcal{K}_1$ (with respect to $\overline{T}_1$).

Proof

Suppose first $T_1 = OD$ and $(K,\mathcal{P}_1) = (K,P)$. Let $a,b,\varepsilon \in K, f(Y) \in K[Y]$ be given with $a < b, 0 < \varepsilon$ and $f(a) < 0 < f(b)$. By the lemma, we have only to prove that there is $c \in K$ with $a < c < b$ and $|f(c)| < \varepsilon$. Clearly f has a zero c' in the real closure of (K,P) with $a < c' < b$, and the ordering on $K[c']$ (induced by this real closure) can be extended to an ordering on $K(c',T)$ with T infinitely close to c' with respect to the ordering on K (i.e. $0 < |T-c'| < \delta$ for each $0 < \delta \in K$). Then $a < T < b$ and $|f(T)| < \varepsilon$. Let P' be the ordering on $K(T)$ induced by the ordering of $K(c',T)$. Extend $\mathcal{P}_2,..,\mathcal{P}_n$ to $\mathcal{P}_2',..,\mathcal{P}_n'$ such that $(K,\mathcal{P}_i) \subset (K(T),\mathcal{P}_i') \models T_i$ $(2 \leqslant i \leqslant n)$ (this is possible because T is transcendental over K).
Then $\mathcal{K} \subset (K(T),P',\mathcal{P}_2,..,\mathcal{P}_n) \models \exists t(a < t < b \wedge |f(t)| < \varepsilon)$, and because $\mathcal{K}$ is existentially closed, this implies there is $c \in K$ with $a < c < b$ and $|f(c)| < \varepsilon$.
Suppose now $T_1 = (pCF)_\forall$. Let $\mathcal{K}_1 = (K,\mathcal{P}_1) = (K,div,P_2,P_3,..)$ and let $0 \neq a \in P_m, 2 \leqslant m \in \mathbb{N}$.

Claim 1

$v(a) \in m\Gamma$, where v is the valuation and Γ the value group associated with (K,div).
Let b be one of the m^{th} roots of a in the prime extension of $\mathcal{K}_1$ and extend the $(pCF)_\forall$-structure of $\mathcal{R}_1(b)$ to a $(pCF)_\forall$-structure on $K(b,X)$ such that the value of X is >0 and let $T = b(1+X)$. Then the $(pCF)_\forall$-structure of $K(b,X)$ induces on $K(T)$ a $(pCF)_\forall$-structure.

$(K(T),\mathcal{P}_1) = (K(T),\text{div}',P_2',P_3',..)$, say with valuation v' and value group Γ'. Then $v'(a) = v'(a(1+X)^m) = v'(T^m) \in m\Gamma'$.

Because T is transcendental over K, $\mathcal{P}_2,..,\mathcal{P}_n$ can be extended to $\mathcal{P}_2',..,\mathcal{P}_n'$ on K(T), such that

$$K \subset \mathcal{L} = (K(T),\mathcal{P}_1',..,\mathcal{P}_n') \models (T_1,..,T_n).$$

Now $\mathcal{L} \models \exists t(t^m \underline{\text{div}}\ a \wedge a\ \underline{\text{div}}\ t^m)$, so, because K is existentially closed, $v(a) \in m\Gamma$.

Claim 2

$\#(\Gamma/_{m\Gamma}) = m$ for all $1 \leq m \in \mathbb{N}$.

For let $g \in \Gamma$ and take $0 \neq b \in K$ with $v(b) = g$. As is shown in the proof of the theorem in (3.6), Ch. I, there is $0 \neq q \in \mathbb{Q}$ with $K = \underline{P}_m(qb)$. By claim 1 this implies $v(qb) \in m$, so $g = v(b) \equiv -v(q) \equiv i \pmod{m\Gamma}$ for some i, $0 \leq i < m$. Hence claim 2 is proved.

Let $\overline{K}_1 = (\overline{K},\overline{\text{div}},\overline{P}_1,..)$ be the prime extension of K_1. Because of Claim 2 $(\overline{K},\overline{\text{div}})$ is the henselization of (K,div), and just as for T_1 = OD one can prove that K is dense in $\overline{K}$ (endowed with the topology $\tau_{\overline{K}_1}$).

The case $T_1 = \underline{\pi}$CF is left to the reader.

(Only one new difficulty occurs compared with pCF, namely the residue field may not be algebraically closed, and this is treated once again by the trick of carefully adjoining a transcendental to the field.) □

(1.20) Let me finish this section with discussing a possible generalisation of the main theorem (1.6). P. Winkler treats in [Wi] some general constructions on model complete theories giving, under certain conditions, new model complete theories. For instance, he proves that the disjoint union of two theories each having an algebraically bounded model companion has a model companion. Now in

our case not a <u>disjoint</u> union of theories is considered, but what one might call, an amalgamated union, with the theory of domains as common part. It seems to me that something like algebraic boundedness is really behind the proof of (1.6). All this suggests a common generalization of Winkler's and my results.
To substantiate the above a bit, let us show that algebraic boundedness holds in our situation.

Definition

A theory T is called algebraically bounded if the infinitary quantifier $\exists^{\infty}$: 'there are infinitely many' can be eliminated, i.e. if every "formula" built up using $\exists^{\infty}$ is equivalent, with respect to T, to a formula not involving $\exists^{\infty}$.

(1.21) *Proposition*

Let T be a t-theory with a model completion $\overline{T}$, such that $K \models \overline{T}$ implies that τ_K is not discrete.
Then $\overline{T}$ is algebraically bounded.

Proof

T admits elimination, so it suffices to show that $\exists^{\infty} x\ \Theta(u_1, .., u_k, x)$ is equivalent with an L(T)-formula, for each open formula Θ.

Claim

Each open formula $\Theta(u_1, .., u_k, x)$ is equivalent, with respect to $\overline{T}$, to a disjunction of formulas

$$\bigwedge_{i=1}^{p} f_i(u,x) = 0 \wedge \bigwedge_{j=1}^{q} \Theta_i(u,x),$$

with $f_i \in \mathbb{Z}[U,X]$, and each Θ_i a t-basic formula in (u,x).

The proof of the claim is by a diagram-compactness argument, using mainly condition (b) of (1.2), and is left to the interested reader. By the claim it suffices to consider the case that $\Theta(u,x)$ is a conjunction as displayed in the claim. Let $(c_j(U))_{j\in J}$ be the finite set of non-zero coefficients of the f_j's, considered as polynomials in X.

Then, by (1.7) and the lemma in (1.9), $\exists^{\infty}x\ \Theta(u,x)$ is easily seen to be equivalent to

$$\bigwedge_{j\in J} c_j(u) = 0 \wedge \exists x \bigwedge_{j=1}^{q} \Theta_i(u,x). \quad \square$$

§2. *A criterion for elementary equivalence, and simplification of the axioms for* $\overline{(T_1,..,T_n)}$

Define for each model K of $(T_1,..,T_n)$ alg(K) as the substructure of K whose universe is the set of algebraic numbers in K.
The following result is the analogue of (2.2), Ch. II, and its proof is indicated in (2.5).

(2.1) *Theorem*

Let K and $\mathcal{L}$ be models of $\overline{(T_1,..,T_n)}$.

Then: $K \equiv \mathcal{L} \Leftrightarrow \mathrm{alg}(K) \simeq \mathrm{alg}(\mathcal{L})$.

The simplification stated in the next proposition is that only $(\ell,1)$-conditions have to be considered, in stead of (ℓ,m)-conditions for all $(\ell,m) \in \mathbb{N} \times \mathbb{N}$ (cf. (1.11)).

(2.2) *Proposition*

Let $n > 1$, $K = (K,\mathcal{P}_1,..,\mathcal{P}_n) \models (T_1,..,T_n)$.

Then: $K \models \overline{(T_1,..,T_n)} \Leftrightarrow$

(*i*) K is a field, and

(*ii*) for each $(\ell,1)$-condition as given in (1.10) and each $a \in K^\ell$, such that $F(a,X,Y) \in K[X,Y]$ is irreducible and
$K \models \bigwedge_{1\leqslant i\leqslant n} \sigma_i(a)$,
the following holds:
$K \models \exists x\exists y(F(a,x,y) = 0 \wedge \bigwedge_{1\leqslant i\leqslant n} \phi_i(a,x) \wedge \Theta_i(a,x,y))$.

Just as (1.17) of Ch. II this can be shown by applying Hilbert's irreducibility theorem for function fields. But there is also a more model theoretic proof which might be useful in other situations. This

proof, given in (2.7), is based on a general lemma (2.6).
The following lemma is the analogue of (2.5) of Ch. II.

(2.3) *Lemma*

Let T be a t-theory with model completion $\overline{T}$ such that $\mathcal{K} \models \overline{T}$ implies that $\tau_{\mathcal{K}}$ is not discrete.

Let

$$\begin{tikzcd} & L_1 \arrow[dr] & \\ K \arrow[ur] \arrow[dr] & & M \\ & L_2 \arrow[ur] & \end{tikzcd}$$

be a commutative diagram of field inclusions with L_1 and L_2 linearly disjoint over K and let $\mathcal{K}, \mathcal{L}_1, \mathcal{L}_2$ be expansions of K, L_1, L_2 respectively, to models of T with $\mathcal{K} \subset \mathcal{L}_1, \mathcal{K} \subset \mathcal{L}_2$.

Then $L_1L_2 (\subset M)$ has an expansions $\mathcal{L} \models T$ with $\mathcal{L}_1 \subset \mathcal{L}, \mathcal{L}_2 \subset \mathcal{L}$.

Proof

Similar to that of lemma (2.5) of Ch. II.
Note that in stead of formulas '$p(\underline{a}) > 0$' one considers formulas $\phi(\underline{a})$ where $\phi(x) = \phi(c_1,..,c_\ell,x)$ and $\phi(u,x)$ is a t-basic formula in (u,x). In stead of a real closure one may take any existentially closed extension. □

The analogues of (2.6) and (2.7), Ch. II, in our general situation are given by:

(2.4) *Proposition*

The class of models $\mathcal{K} = (K, \mathcal{P}_1,..,\mathcal{P}_n) \models (T_1,..,T_n)$, such that K is a field which is algebraically closed in L for some extension $(L, \mathcal{R}_1,..,\mathcal{R}_n) \models \overline{(T_1,..,T_n)}$ of $\mathcal{K}$, is an elementary class. Define

$(T_1,..,T_n)_{alg}$ as the theory such that $\mathrm{Mod}((T_1,..,T_n)_{alg})$ is the class mentioned above.

Then:

(i) $(K,..) \models (T_1,..,T_n)_{alg}$ and $(K,..) \subset (L,..) \models (T_1,..,T_n)$ imply that K is algebraically closed in L.

(ii) $(T_1,..,T_n)_{alg}$ has AP.

Proof

The class mentioned is clearly closed under ultraproducts and its complement within $\mathrm{Mod}(T_1,..,T_n)$ is closed under ultrapowersm hence the class is elementary (cf. [Ch.& Ke.,p.322]).

Let now $K = (K,..) \models (T_1,..,T_n)_{alg}$ and $K \subset \mathcal{L} = (L,..) \models (T_1,..,T_n)$.

For *(i)* we have to show that K is algebraically closed in L.

Without loss of generality we may assume L a field. Now K has by definition an extension $\mathcal{L}' = (L',..) \models \overline{(T_1,..,T_n)}$ such that K is algebraically closed in L'. Because char. K = 0, the field extension $L'|K$ is regular. By the same reasoning as in the proof of (2.7), Ch. II we may conclude that there is a commutative diagram of embeddings:

$$\begin{tikzcd}
 & \mathcal{L}' \arrow[dr] & \\
K \arrow[ur] \arrow[dr] & & M = (M,..) \models (T_1,..,T_n) \\
 & \mathcal{L} \arrow[ur] &
\end{tikzcd}$$

Because $\mathcal{L}'$ is existentially closed, L' is algebraically closed in M, hence K is algebraically closed in M, so also in L.

The same argument proves *(ii)*. □

(2.5) *Proof*

Proof of (2.1): one simply repeats the proof given in (2.8), Ch. II, using (2.4). □

(2.6) *Lemma*

Let T be universal theory in a t-language with the following properties:

(*i*) Conditions (*a*) and (*c*) of (1.2) hold and the underlying domains are of characteristic 0.

(*ii*) T has an extension T_{alg} whose models are exactly those $\mathcal{K} = (K,..) \models T$ with an underlying field K which is algebraically closed in L for some existentially closed extension $\mathcal{L} = (L,..)$ of $\mathcal{K}$.

(*iii*) T_{alg} has AP.

(*iv*) The 2-existentially closed models of T form an elementary class $\mathrm{Mod}(T^2)$, $T \subset T^2$.

Then T^2 is model companion of T.

Proof

Let $\mathcal{K} = (K,..) \models T^2$. We have to show that $\mathcal{K}$ is m-existentially closed for each $m \in \mathbb{N}$. This is proved by induction on m, m = 2 being trivial. For simplicity of notation we treat only m = 3. So let $\Theta(x)$, $x = (x_1, x_2, x_3)$, be an open $\mathcal{K}$-formula and suppose $\mathcal{K} \subset \mathcal{L} = (L,..) \models T \cup \{\exists x\, \Theta(x)\}$.

We have to show that $\mathcal{K} \models \exists x\, \Theta(x)$.

Without loss of generality we may assume $\mathcal{L}$ is existentially closed. Let $b = (b_1, b_2, b_3)$ such that $\mathcal{L} \models \Theta(b)$. Let M be the algebraic closure of $K(b_1)$ in L, and let $\mathcal{M}$ have underlying domain M and $\mathcal{K} \subset \mathcal{M} \subset \mathcal{L}$. So $\mathcal{M} \models T_{alg}$.

Claim

$T^2 \cup \mathrm{Diag}(\mathcal{M}) \vdash \exists x_2 \exists x_3\, \Theta(b_1, x_2, x_3)$.

For let $\mathcal{C} \models T_2 \cup \mathrm{Diag}(\mathcal{M})$. Make a commutative diagram of embeddings

$$\begin{tikzcd}
 & \mathcal{L} \arrow[dr] & \\
\mathcal{M} \arrow[ur, hook] \arrow[dr, hook, dashed] & & \mathcal{D} \models T \\
 & \mathcal{C} \arrow[ur] &
\end{tikzcd}$$

which is possible by *(iii)*. Then $\mathcal{D} \models \exists x_2 \exists x_3 \Theta(b_1, x_2, x_3)$, and because $\mathcal{C}$ is 2-existentially closed, this implies $\mathcal{C} \models \exists x_2 \exists x_3 \Theta(b_1, x_2, x_3)$, and the claim is proved.

We assume now also that $b_1 \notin K$ (if $b_1 \in K$, then we should have taken b_2, or b_3 in stead of b_1). Then b_1 is transcendental over K, so each <u>finitely</u> generated field extension N of K with $K(b_1) \subset N \subset M$ is, because $\mathrm{tr.\,deg}_K M = 1$, of the form $K(b_1, \alpha)$. By the claim there is finite $\Delta \subset \mathrm{Diag}(\mathcal{M})$ with $T^2 \cup \Delta \vdash \exists x_2 \exists x_3 \Theta(b_1, x_2, x_3)$. The observation above on subextensions of $M|K$ implies that Δ is equivalent (with respect to $T^2 \cup \mathrm{Diag}\,\mathcal{K}$) to an open sentence $\psi(\underline{b}_1, \underline{\alpha})$ which involves, besides names for the elements of $\mathcal{K}$, only the name $\underline{b}_1$ for b_1 and at most one other name $\underline{\alpha}$. But $\mathcal{K}$ is 2-existentially closed, so $\mathcal{K} \models \exists x_1 \exists v \psi(x_1, v)$, which by $\mathcal{K} \models T^2 \cup \mathrm{Diag}(\mathcal{K})$ implies: $\mathcal{K} \models \exists x \Theta(x)$. $\square$

(2.7) *Proof of (2.2)*

We will actually show that a model $\mathcal{K}$ of $(T_1, .., T_n)$ satisfies the axioms *(i)* and *(ii)* of (2.2) iff it is 2-existentially closed. Then (2.2) will follow from lemma (2.6) because all the properties required hold for $(T_1, .., T_n)$, by (2.4).

That each existentially closed model of $(T_1, .., T_n)$ satisfies the axioms *(i)* and *(ii)* of (2.2) is proved as in (1.13) (replace 'existentially closed' by '2-existentially closed', etc.).

Conversely, suppose $\mathcal{K} = (K, ..) \models (T_1, .., T_n)$ satisfies *(i)* and *(ii)* of (2.2). We have to prove:

<u>K is existentially closed.</u>

Let $\rho = \exists v_1 \exists v_2 \mu(v_1, v_2)$, μ an open K-formula, and let $\mathcal{L} = (L, ..) \models (T_1, .., T_n)$ be an extension of K with $\mathcal{L} \models \rho$.

We have to show that $K \models \rho$; let $e, f \in L$ with $\mathcal{L} \models \mu(e,f)$.

Without loss of generality one may assume $L = K(e,f)$. There are 3 cases:

(α) $\text{tr. deg}_K L = 0$

(β) $\text{tr. deg}_K L = 1$

(γ) $\text{tr. deg}_K L = 2$

Case (α) is trivial because (a degenerated case of) axiom (*ii*) implies $K \models (T_1, .., T_n)_{alg}$, so $K = \mathcal{L}$ in case (α).

For case (β) one can almost literally copy the proof in (1.14), taking $m = 1$, and using at the end axiom (*ii*).

Case (γ) is reduced to case (β) with the same trick as used in the proof of (2.6): take an existentially closed extension of $\mathcal{L}$, let M be the subextension whose underlying domain is the algebraic closure M of K(e) in this existentially closed extension. Let T' be $(T_1, .., T_n) \cup \{$axiom (*i*), axioms (*ii*) of (2.2)$\}$. Then $T' \cup \text{Diag}(M) \vdash \exists v_2 \mu(e, v_2)$, (use that $M \models (T_1, .., T_n)_{alg}$, that $(T_1, .., T_n)_{alg}$ has AP, and that by the preceding the models of T' are at least 1-existentially closed). Now $\text{tr. deg}_K M = 1$, and we have reduced to case (β). $\square$

§3. *Decidability, and a conjecture of Eršov.*

The 'raison d'être' of the preceding two sections lies in the following theorem.

(3.1) *Theorem*

Suppose that for each $i \in \{1,..,n\}$ T_i is either OD or $(pCF)_\forall$ for some prime p. Then $(\overline{T_1,..,T_n})$ is decidable.

The proof is in the style of §2 of Ch. II, see (3.6). The first thing we need is an analogue for p-adically closed fields of "the k^{th} root of a polynomial of degree d $(1 \leqslant k \leqslant d)$".
It may be an interesting fact in itself that such a notion indeed exists:

(3.2) *Proposition*

Let T be a model complete theory having $PEP_{universal}$. Suppose $\phi(x_1,..,x_m,y)$ is a formula with $T \vdash \forall x \exists^{\leqslant d} y\ \phi(x,y)$ $(1 \leqslant d \in \mathbb{N})$. Then there are open formulas $\phi_1(x,y),...,\phi_d(x,y)$ such that:

(i) $T \vdash \phi(x,y) \leftrightarrow (\phi_1(x,y) \vee ... \vee \phi_d(x,y))$,

(ii) $T \vdash \forall x \exists^{\leqslant 1} y\ \phi_i(x,y)$, for all $1 \leqslant i \leqslant d$,

(iii) $T \vdash \neg\exists x \exists y(\phi_i(x,y) \wedge \phi_j(x,y))$, for all $1 \leqslant i < j \leqslant d$.

Proof

T admits elimination by (2.11 and (2.17) , ch. I, so without loss of generality we may assume $\phi(x,y)$ open. Adding m new constants $\underline{c}_1,..,\underline{c}_m$ to the language and replacing $\phi(x,y)$, $\forall x \exists^{\leqslant d} y\ \phi(x,y)$ etc. by $\phi(\underline{c}_1,..,\underline{c}_m,y)$, $\exists^{\leqslant d} y\ \phi(\underline{c}_1,..,\underline{c}_m,y)$, etc. preserves the hypothesis, so by the theorem on constants, [Sh, p.33], we may suppose m = 0.

Moreover we may assume that the language contains a constant.

Claim

If $A \subset B \models T_\forall$ and $B \models \phi(b), b \in |B|$, then the open type realized by b over A (with respect to the theory $T_\forall$) has a generator $\psi(y)$ such that $T_\forall \cup \mathrm{Diag}(A) \vdash \exists^{\leq 1} y\ \psi(y)$ (cf. [Bac, §4] for the terminology).

Proof of the claim

Let D be the prime extension of $A(b)$ and let C be the prime extension of A. $C|A$ may be realized as a subextension of $D|A$.
Then by model completeness C and D contain the same (finite) number of elements satisfying $\phi(y)$, hence b belongs to $|C|$. Now each element of $|C|$ is 1-potent over A (see (3.5), Ch.I), hence the open type of b over A, which is principal by [Bac, Th.4.1.], has a generator $\psi(y)$, with the stated property, and the claim is proved.
Let $\underline{b}$ be a new constant and define:
$\Gamma = \{\neg\Theta(\underline{b}) | \Theta(y) \text{ is open formula}, T \vdash \exists^{\leq 1} y\ \Theta(y), T \vdash \Theta(y) \rightarrow \phi(y)\}$.
Suppose there is a model (B,b) of $T_\forall \cup \Gamma \cup \{\phi(\underline{b})\}$.
Let A be the smallest substructure of B. Then by the claim above there is an open A-formula $\psi(y)$ with $(B,b) \models \psi(\underline{b})$, $T_\forall \cup \mathrm{Diag}(A) \vdash \exists^{\leq 1} y\ \psi(y)$ and $T_\forall \cup \mathrm{Diag}(A) \vdash \psi(y) \rightarrow \phi(y)$.
Applying compactness to $T_\forall \cup \mathrm{Diag}\ A$, we get an open sentence σ in the language of T with $T_\forall \vdash \sigma \rightarrow \exists^{\leq 1} y\ \psi(y)$ and $T_\forall \vdash \sigma \rightarrow (\psi(y) \rightarrow \phi(y))$ and $A \models \sigma$. We put $\Theta(y) := \sigma \wedge \psi(y)$ and get: $T \vdash \exists^{\leq 1} y\ \Theta(y)$, $T \vdash \Theta(y) \rightarrow \psi(y)$, implying that $\neg\Theta(\underline{b}) \in \Gamma$, which contradicts $(B,b) \models \Gamma \cup \Theta(\underline{b})$.
So the theory $T_\forall \cup \Gamma \cup \{\phi(\underline{b})\}$ is inconsistent. Using compactness we get open formulas $\Theta_1(y),..,\Theta_p(y)$ such that $T \vdash \exists^{\leq 1} y\ \Theta_i(y)$ $(1 \leq i \leq p)$ and $T \vdash \phi(y) \leftrightarrow (\Theta_1(y) \vee ... \vee \Theta_p(y))$.
After replacing $\Theta_1,..,\Theta_p$ by $\Theta_1, \Theta_2 \wedge \neg\Theta_1, .., \Theta_p \wedge (\neg\Theta_1 \wedge \neg\Theta_2 ...)$ if

necessary, we may assume also $T \vdash \neg\exists y(\Theta_i(y) \wedge \Theta_j(y))$, $1 \leq i < j \leq p$. Finally, we choose for $\phi_k(y)$ $(1 \leq k \leq d)$ an open formula, which is (w.r.t. T) equivalent to:

$$\bigvee_{\substack{I \subset \{1,..,p\} \\ \#(I) = k}} (\Theta_{\max(I)}(y) \wedge (\bigwedge_{i \in I} \exists y \Theta_i(y)) \wedge (\bigwedge_{\substack{1 \leq j \leq \max(I) \\ j \notin I}} \neg\exists y \Theta_j(y))).$$

Roughly speaking, $\phi_k(b)$ holds iff $\Theta_\ell(b)$ holds where ℓ is the k^{th} number i in the sequence 1,2,..,p for which there exists an y with $\Theta_i(y)$. Note that we need d formulas to cover all possibilities. Then clearly $\phi_1(y),..,\phi_d(y)$ are the required formulas. $\square$

(3.3) Let us apply (3.2) to T := pCF (p a prime) and

$\phi(x_1,..,x_d,y) := y^d+x_1y^{d-1}+...+ x_d = 0 \quad (2 \leq d \in \mathbb{N})$.

We obtain, as in (2.2) of Ch. II, open formulas $R^T_{d,k}(y,x_1,..,x_d)$ in the language of pCF, such that

$pCF \vdash \forall x \exists^{\leq 1} y\, R^T_{d,k}(y,x)$ for each $1 \leq k \leq d$,

$pCF \vdash y^d+x_1y^{d-1}+...+ x_d = 0 \leftrightarrow \bigvee_{1 \leq k \leq d} R^T_{d,k}(y,x_1,..,x_d)$,

$pCF \vdash \neg\exists x \exists y(R_{d,k}(y,x) \wedge R_{d,\ell}(y,x))$ for all $1 \leq k < \ell \leq d$.

Because pCF has a recursive axiomatization, one can effectively construct such $R^T_{d,k}(y,x)$.

(3.4) Suppose that for each $1 \leq i \leq n$ T_i is either OD or $(pCF)_\forall$ for some prime p.

Then the theory $\overline{(T_1,..,T_n)}$ is extended to the theory $\widetilde{(T_1,..,T_n)}$ by introducing new predicate symbols $\underline{W}_{d,k_1,..,k_n}$ $(2 \leq d,\ 1 \leq k_i \leq d)$, and by adding as defining axioms the universal closures of:

$$\underline{W}_{d,k_1,..,k_n}(x_1,..,x_d) \leftrightarrow \exists y(\bigwedge_{1 \leq i \leq n} R^{\bar{T}_i}_{d,k_i}(y,x_1,..,x_d))$$

(3.5) *Theorem*

Suppose that for each $i \in \{1,..,n\}$ T_i is either OD or $(pCF)_\forall$ for some prime p. Then $\widetilde{(T_1,..,T_n)}$ admits elimination.

(3.6) *Proofs of (3.1) and (3.5)*

We simply copy the proofs of (2.1) and (2.4) of Ch. II, except for replacing OD_n, $\overline{OD}_n$, $OF_{n,alg}$, $\widetilde{OD}_n$, etc. by $(T_1,..,T_n)$, $\overline{(T_1,..,T_n)}$, $(T_1,..,T_n)_{alg}$, $\widetilde{(T_1,..,T_n)}$.

One should also keep in mind that the roles of (2.5), (2.6), (2.7), (2.9) of Ch. II are taken over by (2.3), (2.4), (2.4), (3.2) of Ch. III.

Finally the obvious generalizations of (2,10), (2,12) and (2.13) of Ch. II are left to the reader. □

(3.7) Eršov considers in [Er] fields K which have for each $i \in \{1,..,n\}$ a Krull valuation v_i such that $v_1,..,v_n$ induce different topologies on K and there is no proper algebraic extension L of K to which each v_i has an immediate extension.

(If $\mathcal{K} = (K,...) \models (T_1,..,T_n)$ and each T_i is a $(pCF)_\forall$ or $(\underline{\pi}CF)_\forall$, then K with the n valuations induced by the $(T_1,..,T_n)$-structure of $\mathcal{K}$, clearly has this property.

Let for each $i \in \{1,..,n\}$ K_i be a henselization of (K,v_i) within a fixed algebraic closure $\widetilde{K}$ of K, (cf. Ch. I (3.3)). Then clearly $K_1 \cap ... \cap K_n = K$, so $Gal(\widetilde{K}|K)$ is generated by its subgroups $Gal(\widetilde{K}|K\ ),...,Gal(\widetilde{K}|K_n)$. Eršov conjectures: $Gal(\widetilde{K}|K)$ is the free product (within the category of profinite groups) of its subgroups $Gal(\widetilde{K},K_1),...,Gal(\widetilde{K},K_n)$.

For a special case he proves a 'p-analogue' of this conjecture, for each prime p.

CHAPTER IV *Bounds in the theory of polynomial ideals*

§1. *Introduction*

The title of this chapter indicates a topic to which A. Robinson returned again and again. There are a lot of results in this subject. We mention a few of them (with $X = (X_1,..,X_n)$):

(1.1) Given natural numbers n and d, there is $A = A(n,d) \in \mathbb{N}$ such that for each field K and all $f_1,..,f_m,g \in K[X]$ of degree $\leq d$:
$g \in (f_1,..,f_m) \Leftrightarrow g = \Sigma h_i f_i$ for certain $h_i \in K[X]$ of degree $\leq A$.

(1.2) Given natural numbers n and d, there is $B = B(n,d) \in \mathbb{N}$ such that for each field K and all $f_1,..,f_m,g \in K[X]$ of degree $\leq d$:
$g \in \sqrt{(f_1,..,f_m)} \Leftrightarrow g^B = \Sigma h_i f_i$ for certain $h_i \in K[X]$ of degree $\leq B$.

(1.3) Given natural numbers n and d, there is $C = C(n,d) \in \mathbb{N}$ such that for each field K and any two ideals I and J of K[X] generated by polynomials of degree $\leq d$ the following holds:
$I \cap J$ and $I:J$ are generated by polynomials of degree $\leq C$.

(1.4) Given natural numbers n and d, there is $D = D(n,d) \in \mathbb{N}$ such that for each field K and every proper ideal I of K[X] generated by polynomials of degree $\leq d$ the following holds:
I is prime $\Leftrightarrow$ for all $f,g \in K[X]$ of degree $\leq D$, if $fg \in I$ then $f \in I$ or $g \in I$.

(1.5) Given natural numbers n and d there is $E = E(n,d) \in \mathbb{N}$, such that for each field K and each ideal I of K[X] generated by

polynomials of degree $\leqslant d$ the following holds:
each of the minimal prime ideals of I is generated by polynomials of degree $\leqslant E$, and there are at most E minimal prime ideals of I.

The oldest proofs of these results are constructive -see [He], where ideas of Kronecker, M. Noether, J. König, Macauley and Hentzelt are used- and give extra information: for instance concerning (1.3) it is shown how to construct generators for $I \cap J$ and $I:J$ if generators for I and J are given, and this permits us also to give explicit recursion formulas for the functions A and C. A recent treatment in this style, free from the mistakes occurring in [He], is [Se].

In the fifties A. Robinson showed how (1.2) trivially follows from Hilbert's Nullstellensatz by a model theoretic argument. This quickly became a kind of paradigma. Later he also proved (1.1) by combining a non-standard trick with well-known facts on primary decomposition, see [Ek] for a review of this and related work.

One might ask for the significance of such model theoretic proofs. This seems to me to lie in their simplicity, compared with the many complicated constructions needed in the older proofs, and also in certain new interpretations, which model theory permits. For instance, in §2 I will show that (1.1), (1.3) and many similar results can be explained by the faithful flatness of certain 'internal' polynomial rings over their subring of ordinary polynomials.
In §3 I will prove (1.4) by combining a model theoretic compactness argument with a somewhat elaborated version of: "an irreducible variety is birationally equivalent with a hypersurface". (1.5) is then almost immediate, by well-known model theoretic arguments.

Another reason for giving model theoretic proofs is given by A. Robinson in his list of problems [Rob4].

In the third problem "On effective procedures in differential algebra" he indicates that analogues of (1.1), (1.3) and (1.4) for differential polynomials are still open, even for n = 1 and that the famous Ritt problem is of this nature. If this is due to extreme complications which an orthodox, constructive proof would probably involve, then one might hope model theory to be useful in this area. But first one should of course give systematic model theoretic proofs of (1.1) - (1.5), etc., to learn what kind of arguments are involved. Robinson explicitly mentions the bound D in (1.4) as one, which 'does not follow from any known model theoretic arguments', [Rob4, p.503]).
Such arguments will be given in sections 2 and 3. (Actually we will prove more precise statements than (1.1) - (1.5).)

§2. *"The concept of flatness is a riddle that comes out of algebra, but which technically is the answer to many prayers"*

D. Mumford

(1.1) and *(1.3)* are actually consequences, as in [He], of the following two stronger results:

(2.1) *Theorem*

Given $n,d,k \in \mathbb{N}$ there is $\alpha = \alpha(n,d,k) \in \mathbb{N}$, such that for each field K and each system of homogeneous linear equations

$$(A)\quad \begin{cases} f_{11}Y_1 + \dots + f_{1\ell}Y_\ell = 0 \\ \quad\vdots \\ f_{k1}Y_1 + \dots + f_{k\ell}Y_\ell = 0 \end{cases}$$

with all $f_{ij} \in K[X]$ of degree $\leqslant d$, the solution set in $K[X]^\ell$ is generated as $K[X]$-module by solutions $g = (g_1,\dots,g_\ell)$ with $\deg(g) \leqslant \alpha$ (i.e. $\deg(g_i) \leqslant \alpha$ for $1 \leqslant i \leqslant \ell$).

(2.2) *Theorem*

Given $n,d,k \in \mathbb{N}$ there is $\beta = \beta(n,d,k) \in \mathbb{N}$, such that for each field K and each system of linear equations

$$(B)\quad \begin{cases} f_{11}Y_1 + \dots + f_{1\ell}Y_\ell = f_1 \\ \quad\vdots \\ f_{k1}Y_1 + \dots + f_{k\ell}Y_\ell = f_k \end{cases}$$

with all $f_{ij}, f_i \in K[X]$ of degree $\leqslant d$, there is a solution $g \in (K[X])^\ell$ with $\deg(g) \leqslant \beta$, if there is a solution in $(K[X])^\ell$ at all.

Remark

The numbers α and β do not depend on the number ℓ of unknowns. This is so because for given n,d,k the K-linear space of column vectors

f in $K[X]^k$ with $\deg f \leq d$ has finite dimension, say ℓ (only depending on n,d,k) and if bounds α,β hold for this special value of ℓ, it clearly holds also for all other values. This type of argument will in the following tacitly be left to the reader, and in such cases ℓ will be considered as bounded in terms n,d and k.

For the proof of (2.1) we have to recall a result on flatness.

(2.3) *Fact 1*

Let R,S be rings and $R \subset S$. Then the following are equivalent:

(*i*) S is a flat R-module.

(*ii*) For each homogeneous linear equation $f_1Y_1+\ldots+f_\ell Y_\ell = 0$ ($f_i \in R$) the solutions in S^ℓ are S-linear combinations of solutions in R^ℓ.

(*iii*) For each system of homogeneous linear equations

$$\begin{cases} f_{11}Y_1 + \ldots + f_{1\ell}Y_\ell = 0 \\ \\ f_{k1}Y_1 + \ldots + f_{k\ell}Y_\ell = 0 \end{cases} \qquad (f_{ij} \in R)$$

the solutions in S^ℓ are S-linear combinations of solutions in R^ℓ.

For the proof see [Bo2, Ch.1, §2, n° 11], where (i) $\Rightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) is shown.

(2.4) *Proof of (2.1)*

Suppose n,d,k given and α does not exist. So for each $m \in \mathbb{N}$ there is a field K_m and a system of type (A) over K_m and a solution in $(K_m[X])^\ell$ which is not generated by solutions of degree $\leq m$. Consider a structure containing all fields K_m, polynomial rings $K_m[X]$, $\mathbb{N}$, etc. and take an enlargement of this structure. By the saturatedness of enlargements

there is an internal field K in this enlargement and an infinite natural number ω such that the following holds:
there are $f_{ij}(i=1,..,k;\ j=1,..,\ell)$ in the (internal) nonstandard polynomial ring $K^*[X]$ over K, all of degree $\leqslant d$ giving rise to a system (A) having a solution in $(K^*[X])^\ell$ which is not a $K^*[X]$-linear combination of solutions of degree $\leqslant\omega$, so in particular not a linear combination of solutions in $(K[X])^\ell$. Here $K[X]$ is considered as naturally embedded in $K^*[X]$.

Claim

$K^*[X]$ is a flat $K[X]$-module.

If this claim holds, then one gets a contradiction using (i) $\Leftrightarrow$ (iii) of Fact 1, noting that all f_{ij} are in $K[X]$.
Let us now prove the claim with induction to n, using (i) $\Leftrightarrow$ (ii) of Fact 1: let $f_1,..,f_\ell \in K[X]$ be given and consider a solution $g = (g_1,..,g_\ell) \in (K^*[X])^\ell$ of $f_1Y_1+...+f_\ell Y_\ell = 0$; we have to show that g is generated by solutions in $(K[X])^\ell$. Assume $n > 0$.
We may of course suppose $f_1 \neq 0$ and also (after carrying out a linear transformation on the variables X) that f_1 is monic, say of degree p, in X_n.
$(-f_2,f_1,0,...,0),(-f_3,0,f_1,...,0),...,(-f_\ell,0,0,...,f_1)$ are also solutions in $(K[X])^\ell$ of $f_1Y_1+...+f_\ell Y_\ell = 0$, and by subtracting suitable multiples of these solutions from $(g_1,..,g_\ell)$ one obtains a solution $(g_1',..,g_\ell')$ with $g_2',..,g_\ell'$ all of degree $<p$ in X_n, so $(g_1',..,g_\ell')$ has components in $(K^*[X_1,..,X_{n-1}])[X_n]$. By the induction hypothesis $K^*[X_1,..,X_{n-1}]$ is a flat $K[X_1,..,X_{n-1}]$-module, so $(K^*[X_1,..,X_{n-1}])[X_n]$ is a flat $K[X]$-module. (This last conclusion is a consequence of the preservation of flatness under extension by scalars, see [Bo2, Ch.1, §2,7].)

Hence $(g_1',\dots,g_\ell')$ is generated by solutions in $(K[X])^\ell$, by (i) $\Leftrightarrow$ (ii) of Fact 1. □

(2.5) *Remarks*

(a) The claim in the proof should be considered as the nonstandard form of Theorem (2.1).

(b) Let us show how (1.3) follows: if $I = (f_1,\dots,f_k)$, $J = (g_1,\dots,g_\ell)$ with all f_i, g_i of degree $\leq d$, then generators for $I \cap J$ can be obtained by first giving generators in $(K[X])^{k+\ell}$ for the solutions of $Y_1 f_1 + \dots + Y_k f_k = Z_1 g_1 + \dots + Z_\ell g_\ell$, and then taking for each of these generators $(y_1,\dots,y_k,z_1,\dots,z_\ell)$ the element $y_1 f_1 + \dots y_k f_k$ as a generator for $I \cap J$.
Similarly, generators for $I:J$ are obtained by giving generators in $(K[X])^{1+k\ell}$ for the solutions of

$$\begin{cases} g_1 Y = f_1 Z_{11} + \dots + f_k Z_{1k} \\ g_\ell Y = f_1 Z_{\ell 1} + \dots + f_k Z_{\ell k} \end{cases}$$

and taking the first components of these generators.

For the proof of (2.2) we need the concept of faithfully flatness.

(2.6) *Fact 2*

Let R,S be rings and $R \subset S$. Then the following are equivalent:

(i) S is a faithfully flat R-module.

(ii) S is a flat R-module and $\underline{m}S \neq S$ for each maximal ideal $\underline{m}$ of R.

(iii) S is a flat R-module and each system of linear equations.

$$\begin{cases} f_{11} Y_1 + \dots + f_{1\ell} Y_\ell = f_1 \\ \vdots \\ f_{k1} Y_1 + \dots + f_{k\ell} Y_\ell = f_\ell \end{cases} \qquad (f_{ij}, f_i \in R)$$

with a solution in S^ℓ has also a solution in R^ℓ.

See [Bo2, §3] for the proof.

Just as in the proof of (2.1) one shows easily that the nonstandard equivalent of (2.2), in conjunction with (2.1), is the following:

(2.7) <u>If $K^*[X]$ is the internal polynomial ring in</u> $X = (X_1,\ldots,X_n)$, <u>$n \in \mathbb{N}$, over a field K, then $K^*[X]$ is a faithfully flat $K[X]$-module.</u>

(Here K is supposed to be an internal field of an enlargement, in order that $K^*[X]$ makes sense.)

<u>*Proof of (2.7)*</u>

Let $\underline{m}$ be a maximal ideal of $K[X]$. By (i) $\Leftrightarrow$ (ii) of (2.6) we have to show only that $\underline{m}\cdot K^*[X] \neq K^*[X]$.
By Hilbert's Nullstellensatz $\underline{m}$ has a zero x in L^n, where L is the *algebraic closure of K, so the internal K-algebra morphism $K^*[X] \to L$ given by $X \mapsto x$ contains $\underline{m}\cdot K^*[X]$ in its kernel, hence $\underline{m}\cdot K^*[X] \neq K^*[X]$. $\square$

<u>*Remark*</u>

(1.1) <u>is an immediate consequence of (2.2).</u>

§3. *Prime ideals in* $K[X]$.

For simplicity we consider first the case of perfect K. Then the algebraic fact underlying our proof of (1.4) is the following lemma, which is nothing more then an elaborated version of:
an irreducible K-variety is birationally equivalent over K with a hyper surface.

(3.1) *Lemma*

Let K be a perfect field, $f_1,..,f_m \in K[X]$ of degree $\leqslant d$ and put $I = (f_1,..,f_m)$. Then the following are equivalent:

(i) I is a prime ideal.

(ii) There exist t, $0 \leqslant t \leqslant n$, and irreducible $P \in K[Y_1,..,Y_t,Z]$ of degree >0 in Z and $h_1,..,h_n \in K[Y_1,..,Y_t,Z]$, $h \in K[Y_1,..,Y_t]\setminus\{0\}$ and $g_1,..,g_t,g \in K[X]$ such that

(a) $h^d f_i(h_1/h,..,h_n/h) \in P.K[Y_1,..,Y_t,Z]$, $1 \leqslant i \leqslant m$,

(b) $P(g_1,..,g_t,g) \in I$,

(c) $I : (h(g_1,..,g_t)) = I$ and $I \neq K[X]$,

(d) $h(g_1,..,g_t)X_j - h_j(g_1,..,g_t,g) \in I$, $1 \leqslant j \leqslant n$.

Proof

(i) ⇒ (ii). Let $x_j = X_j+I \in K[X]_{/I}$ for $1 \leqslant j \leqslant n$. Then $K(x_1,..,x_n)|K$ is separable, so has a separating transcendence base $y_1,..,y_t$ over K with $\{y_1,..,y_t\} \subset \{x_1,..,x_n\}$ (see [L3, p.266]).
The proof of the primitive element theorem in [L3, p.185] shows that there is $z \in K[x_1,..,x_n]$ ($= K[X]_{/I}$) with $K(y_1,..,y_t,z) = K(x_1,..,x_n)$. Let us introduce new indeterminates $Y_1,..,Y_t,Z$ and write Y for $(Y_1,..,Y_t)$, y for $(y_1,..,y_t)$ and x for $(x_1,..,x_n)$.
Let $P = P(Y,Z) \in K[Y,Z]$ be the irreducible polynomial such that

$P(y,z) = 0$. Further choose $g_1,..,g_t,g \in K[X]$ with $y_i = g_i(x)$, $1 \leq i \leq t$, and $z = g(x)$, and choose $h_1,..,h_n \in K[Y,Z]$ and $h \in K[Y]\setminus\{0\}$ with $x_j = h_j(y,z)/h(y)$.

Then *(a)*, *(b)*, *(c)*, *(d)* follow easily from:

I is the kernel of $K[X] \to K(x)$, and $P\cdot K[Y,Z]$ is the kernel of $K[Y,Z] \to K(y,z)$.

(ii) $\Rightarrow$ (i): We put $x_j = X_j+I$ and $y_i = Y_i+P\cdot K[Y_1,..,Y_t,Z]$ and use the notations Y, y and x from above.

Let $\Theta : K[X] \to K[Y,Z]_h$ be the K-algebra morphism with $\Theta(X_j) = h_j/h$. Because $h \notin P.K[Y,Z]$ we have $h(y) \neq 0$, so we can extend the evaluation map $K[Y,Z]_h \to K[y,z]_{h(y)}$.

By *(a)* we get $\Theta(f_i)(y,z) = f_i(h_1(y,z)/h(y),...,h_n(y,z)/h(y))$, so Θ induces $\bar{\Theta}$ such that the following diagram of K-algebra morphisms commutes:

$$\begin{array}{ccc} K[X] & \xrightarrow{\Theta} & K[Y,Z]_h \\ \downarrow & & \downarrow \\ K[x] & \xrightarrow{\bar{\Theta}} & K[y,z]_{h(y)} \\ \| & & \\ K[X]/(f_1,..,f_m) & & \end{array} \qquad (\alpha)$$

We define the K-algebra morphism $\mu : K[Y,Z] \to K[X]$ by $\mu(Y_i) = g_i(X)$ and $\mu(Z) = g(X)$. Then $\mu(P)(x) = P(g_1,..,g_t,g)(x) = 0$ by *(b)*, so μ induces $\bar{\mu}$ such that the following diagram of K-algebra morphisms commutes:

$$\begin{array}{ccc} K[Y,Z] & \xrightarrow{\mu} & K[X] \\ \downarrow & & \downarrow \\ K[y,z] & \xrightarrow{\bar{\mu}} & K[x] \end{array} \qquad (\beta)$$

Now these 4 morphism can be extended uniquely to K-algebra morphisms such that the following diagram commutes

$$\begin{array}{ccc} K[X,Z]_h & \xrightarrow{\mu} & K[X]_{\mu(h)} \\ \downarrow & & \downarrow \\ K[y,z]_{h(y)} & \xrightarrow{\bar{\mu}} & K[x]_{\mu(h)(x)} \end{array} \qquad (\gamma)$$

(The extensions of μ and $\bar{\mu}$ are denoted by the same letters).

That the morphisms in (γ) are indeed <u>extensions</u> of those in (β) is seen as follows: $h \neq 0$, and $h(y) \neq 0$ since $h \notin P.K[Y,Z]$, so $K[Y,Z] \subset K[Y,Z]_h$ and $K[y,z] \subset K[y,z]_{h(y)}$; $\mu(h)(x) = h(g_1,..,g_t)(x)$ is not a zero divisor of $K[x] \neq \{0\}$ by (c), so $\mu(h) \neq 0$ and $K[X] \subset K[X]_{\mu(h)}$ and $K[x] \subset K[x]_{\mu(h)(x)}$.

From (α) and (γ) we get the commutive diagram:

$$\begin{array}{ccc} K[X] & \xrightarrow{\mu\circ\Theta} & K[X]_{\mu(h)} \\ \downarrow & & \downarrow \\ K[x] & \xrightarrow{\bar{\mu}\circ\bar{\Theta}} & K[x]_{\mu(h)(x)} \end{array} \qquad (\delta)$$

(d) means that $\mu(h)X_j - \mu(h_j) \in I$, so we get

$$x_j = \mu(h_j)(x)/\mu(h)(x) \qquad (\varepsilon).$$

Similarly $(\mu\circ\Theta)(X_j) = \mu(h_j)/\mu(h)$, so

$$(\bar{\mu}\circ\bar{\Theta})(x_j) = \mu(h_j)(x)/\mu(h)(x) \qquad (\zeta).$$

From (ε) and (ζ) it follows that $\bar{\mu}\circ\bar{\Theta} : K[x] \to K[x]_{\mu(h)(x)}$ is the inclusion map, hence $\bar{\Theta}$ is 1-1, so is an embedding of the ring $K[x]$ in the domain $K[y,z]_{h(y)}$. This implies that $K[x]$ is a domain, i.e. I is prime. □

The model theoretic fact underlying our proof of (1.4) is:

(3.2) Lemma

Let T be an L-theory, and let Γ and Δ be sets of L-sentences such that $T \models \bigwedge\Gamma \leftrightarrow \bigvee\Delta$.

Then there are finite subsets Γ_0 of Γ and Δ_0 of Δ such that $T \vdash \bigwedge\Gamma_0 \rightarrow \bigvee\Delta_0$. For such Γ_0 and Δ_0 we have: $T \vdash \bigwedge\Gamma \leftrightarrow \bigwedge\Gamma_0$.

Proof

$\bigvee\Delta$ is true in each model of $T \cup \Gamma$, so by the compactness theorem there is a finite subset Δ_0 of Δ with $T \cup \Gamma \vdash \bigvee\Delta_0$. A second application of the compactness theorem gives a finite subset Γ_0 of Γ with $T \vdash \bigwedge\Gamma_0 \rightarrow \bigvee\Delta_0$. The second statement of the lemma is trivial. $\square$

(3.3) Let now $f_1(C,X),\ldots,f_m(C,X)$ be given polynomials in $\mathbb{Z}[C,X]$, C denoting a sequence of variables $C_1,\ldots,C_k$.

Using *(1.1)* we see that for each each $r \in \mathbb{N}$ there is a formula $\overline{\text{prime}}_r(C)$ (in the language of rings) such that for each field K and $c \in K^k$:

$K \models \overline{\text{prime}}_r(c) \Leftrightarrow$ for all $g,h \in K[X]$ of degree $\leqslant r$, if

$gh \in (f_1(c,X),\ldots,f_m(c,X))$, then

$g \in (f_1(c,X),\ldots,f_m(c,X))$ or $h \in (f_1(c,X),\ldots,f_m(c,X))$.

Hence it is clear that for each field K and $c \in K^k$:

$K \models \bigwedge\{\overline{\text{prime}}_r(c) \mid r \in \mathbb{N}\} \Leftrightarrow (f_1(c,X),\ldots,f_m(c,X))$ is prime.

Similarly, by *(1.1)* and *(1.3)* there is for each $r \in \mathbb{N}$ a formula $\underline{\text{prime}}_r(C)$ such that for each perfect field K and $c \in K^k$:

$K \models \underline{\text{prime}}_r(c) \Leftrightarrow$ there is $0 \leqslant t \leqslant n$ and there are irreducible $P \in K[Y_1,\ldots,Y_t,Z]$ of positive degree in Z and $h_1,\ldots,h_n \in K[Y_1,\ldots,Y_t,Z]$, $h \in K[Y_1,\ldots,Y_t]\setminus\{0\}$, and $g_1,\ldots,g_t,g \in K[X]$, all of degree $\leqslant r$, such that *(a)*, *(b)*, *(c)* and *(d)* of (3.1) hold with $f_i = f_i(c,X)$.

Lemma (3.1) tells us that the ideal $(f_1(c,X),\ldots,f_m(c,X)) \in K[X]$, for K a perfect field and $c \in K^k$, is prime iff

$K \models \bigvee\{\underline{\text{prime}}_r(c) \mid r \in \mathbb{N}\}$.

Let now $(1.4)_p$ be the statement (1.4), with 'for each field K' changed to 'for each perfect field K'.

(3.4) Proof of $(1.4)_p$

Take for $f_1(C,X),\ldots,f_m(C,X)$ the m general polynomials in $X = (X_1,\ldots,X_n)$ of degree d, i.e. their coefficients are the $k = m.\binom{d+n}{n}$ variables $(C_1,\ldots,C_k) = C$ ($\binom{d+n}{n}$ = number of monomials $X_1^{i_1}\ldots X_n^{i_n}$ with $i_1+\ldots+i_n \leqslant d$). Let now pFL be the theory of perfect fields. Then by (3.3)

$pFL \models \bigwedge\{\overline{\text{prime}}_r(C) \mid r \in \mathbb{N}\} \leftrightarrow \bigvee\{\underline{\text{prime}}_r(C) \mid r \in \mathbb{N}\}$, $C_1,\ldots,C_k$ being considered as new constants.

An application of (3.2) finishes the proof. □

(3.5) Let me make some remarks how to use the model theoretic lemma (3.2) which does not seem to be noticed before. In the above the infinite conjunction was the trivial part and to find an equivalent disjunction required the algebraic lemma (3.1).

Also in Ritt's problem an infinite conjunction is easy to find, so that a positive solution of the problem 'only' requires an equivalent infinite disjunction.

I'll now indicate an example where the infinite disjunction is trivial, while the conjunction requires a non-trivial result.

Let $g(C,X), f_1(C,X),\ldots,f_m(C,X) \in \mathbb{Z}[C,X]$ be the m+1 general polynomials of degree d in X ($C = (C_1,\ldots,C_k)$, $k = (m+1)\cdot\binom{d+n}{n}$). Then one easily constructs for each $r \in \mathbb{N}$ a formula $\phi_r(C)$ (in the language of rings) such that for each field K and $c \in K^k$:

$K \models \phi_r(c) \Leftrightarrow g(c,X) = \Sigma h_i(X)\cdot f_i(c,X)$ for certain $h_i(X) \in K[X]$ of degree $\leqslant r$ $(i = 1,\dots,m)$.

Similarly one can construct for each $r \in \mathbb{N}$ a formula $\psi_r(C)$ such that for each field K and $c \in K^k$:

$K \models \psi_r(c) \Leftrightarrow g(c,x) = 0$ for each ring $K[x]$, $x = (x_1,\dots,x_n)$, such that $\dim_K K[x] \leqslant r$ and $f_1(c,x) = \dots = f_m(c,x) = 0$.

Let K be any field, I an ideal of $K[X]$, and $g \in K[X]$. Then, using $I = \cap\{I+\underline{m}^n \mid \underline{m}$ is a maximal ideal of $K[X]$, $n \in \mathbb{N}\}$, we obtain:

$g \in I$ iff $g(x) = 0$ for each ring $K[x]$ of finite K-dimension, such that x is a zero of I.

Combining the above three remarks, we get:

$$FL \models \vee\{\phi_r(C) \mid r \in \mathbb{N}\} \leftrightarrow \wedge\{\psi_r(C) \mid r \in \mathbb{N}\}.$$

Using a recursive enumeration of all proofs from FL, we will find $A(n,d)$ with $FL \vdash \vee\{\phi_r(C) \mid 0 \leqslant r \leqslant A(n,d)\} \leftrightarrow \wedge\{\psi_r(C) \mid 0 \leqslant r \leqslant R\}$ for some $R \in \mathbb{N}$. This gives a new proof of *(1.1)* with the extra result that we can take for A a recursive function.

(3.6) A problem related to (1.4) is:

Let a computable field K be given (i.e. the elements of K are numbered in such a way that the ring operations on K correspond with recursive functions, see [Ra, p. 352] for details). Is there an algorithm to determine whether an ideal of $K[X]$ given by a finite set of generators is prime?

A necessary condition is that there is an algorithm to determine whether a polynomial in one variable over K is irreducible. It will be shown in (3.7) that for perfect K this is also sufficient. However, the result can be stated without any reference to computability of the field by extending the language of rings as follows:

add for each $k \in \mathbb{N}$, $k \geqslant 2$ $2k$ (Skolem) function symbols A_{k_i}, B_{k_i} $(1 \leqslant i \leqslant k)$

and the unary function symbol $^{-1}$ to the language of rings.
Similarly we extend the theory of perfect fields pFL to the theory

pFL* by adding axioms saying for a model K^* of

pFL* (with underlying perfect field K) the following:

each polynomial $T^k+a_1T^{k-1} + \ldots + a_k \in K[T]$ $(k \geqslant 2)$ is either irreducible, or factors as

$(A_{k1}(a_1,\ldots,a_k)T^{k-1} + \ldots + A_{kk}(a_1,\ldots,a_k)) \cdot (B_{k1}(a_1,\ldots,a_k)T^{k-1} + \ldots$
$\ldots + B_{kk}(a_1,\ldots,a_k))$ and for each $a \in K$: $a = 0$ or $a \cdot a^{-1} = 1$.

pFL* might be called the theory of perfect fields endowed with a process for factoring polynomials in one variable.

Note that pFL* has a <u>universal</u> and <u>recursive</u> axiom system. For instance, perfectness can be expressed by saying that if characteristic $= p > 0$, then for each a $T^p - a$ is reducible.

We can also for a polynomial $f = f(C,X) \in \mathbb{Z}[C,X]$ find an <u>open</u> formula $Irr_f(C)$ in the language of pFL* such that for each model K^* of pFL* and all $c \in K^k$:

$$K^* \models Irr_f(c) \Leftrightarrow f(c,X) \in K[X] \text{ is irreducible.}$$

$n = 1$: this case is easy using the new function symbols.

$n > 1$: the Kronecker trick ([L2, p.150]) can be used to reduce to $n = 1$.

(3.7) *Theorem*

<u>There is an open formula</u> prime (C) <u>in the augmented language such that for each</u> $K^* \models$ pFL* <u>and each</u> $c \in K^k$:

$K^* \models$ prime $(c) \Leftrightarrow (f_1(c,X),\ldots,f_m(c,X)) \subset K[X]$ <u>is prime</u>.

<u>Moreover the formula</u> prime (C) <u>can be determined effectively from</u> $f_1(C,X),\ldots,f_m(C,X) \in \mathbb{Z}[C,X]$.

Remark

For the last statement of (3.7) we need the fact that we can take

recursive functions for A and C in (1.1) and (1.3).
For A this was proved in (3.5). An explicit formula for C can be found on p. 296 in [Se].

Proof

For all models K^* and L^* of pFL^* with $K^* \subset L^*$ and all $c \in K^k, c \in \mathbb{N}$ we have:

$$K^* \models \underline{\text{prime}}_r(C) \Rightarrow L^* \models \underline{\text{prime}}_r(c),$$
$$L^* \models \overline{\text{prime}}_r(c) \Rightarrow K^* \models \overline{\text{prime}}_r(c).$$

This is clear from the meaning of the formulas, except perhaps for the first implication which rests also on the following:
if K and L are fields with $K \subset L$, I an ideal of $K[X]$, $g \in K[X]$ and $I : (g) = I$, then $I \cdot L[X] : (g \cdot L[X]) = I \cdot L[X]$. It is left to the reader to verify that this follows from the flatness of L as a K-module.
The last part of (3.4) shows that there exist $r,s \in \mathbb{N}$ with

$$pFL^* \vdash \overline{\text{prime}}_r(C) \leftrightarrow \underline{\text{prime}}_s(C).$$

pFL^* is a universal theory, hence by Ch. I (2.12) and the 2 implications above $\overline{\text{prime}}_r(C)$ is equivalent to an open formula prime (C). This formula satisfies the requirements.
<u>Because</u> A and C are recursive, the formulas $\underline{\text{prime}}_d(C)$ and $\overline{\text{prime}}_d(C)$ can be constructed effectively from $d \in \mathbb{N}$.
So r and s and an open formula prime (C) as above are found by going systematically through the proofs of pFL^*. □

(3.8) Let us now prove statement (1.5) of §1 for perfect K. In fact we will state in (3.10) a somewhat stronger result which has also the following corollary:

(*) <u>Let K be a perfect computable field with an algorithm to test irreducibility of polynomials in one variable over K.</u>

Then there is an algorithm which computes for every ideal I of $K[X]$, given by a finite set of generators, the finitely many minimal primes of I.

Recall that for an ideal I of $K[X]$ the set of minimal primes of I can be characterized as the unique finite set $\{P_1,\ldots,P_r\}$ of primes in $K[X]$ such that $P_i \not\subset P_j$ for $i \neq j$ and for each $x \in \tilde{K}^r$ ($\tilde{K}$ = alg. closure of K): x is a zero of I iff x is a zero of some P_i.
Let C and $f_1(C,X),\ldots,f_m(C,X)$ be as before. A pFL^*-term $\tau(C,X)$ will be called polynomial in X if it is of the form

$$\Sigma\alpha_{i_1\ldots i_n}(C)X_1^{i_1}\ldots X_n^{i_n}.$$

Let $T(C,X)$ with or without subscript denote in the following a finite set of pFL^*-terms in the k+n-variables C,X which are polynomial in X. If K^* is a model of pFL^* and $c \in K^k$ we let $(T(c,X)_K)$ be the ideal of $K[X]$ generated by all $\tau(c,X)$ with $\tau(C,X) \in T(C,X)$.

(3.9) *Lemma*

Given an r-tuple $T = (T_1(C,X),\ldots,T_r(C,X))$ ($r \in \mathbb{N}$), there is an open pFL^*-formula minimal $\text{primes}_T(C)$ such that for each $K \models pFL^*$ and each $c \in K^k$:

$K^* \models$ minimal $\text{primes}_T(c) \Leftrightarrow \{(T_1(c,X)_K),\ldots,(T_r(c,X)_K)\}$ is the set of minimal primes of $(f_1(c,X),\ldots,f_m(c,X)) \subset K[X]$.

Proof

This is an easy consequence of the above characterization of the set of minimal primes and the fact that ACF admits elimination. □

(3.10) *Corollary*

There exist $T_1,\ldots,T_M$, each T_i being an r-tuple $(T_{i_1}(C,X),\ldots,T_{i_r}(C,X))$

for some $r \in \mathbb{N}$, such that

$$pFL^* \vdash \forall C\big(\bigvee_{1\leq i\leq M} \text{minimal primes}_{T_i}(C)\big).$$

Proof

Let $(T_\lambda)_{\lambda\in\Lambda}$ be an enumeration of all tuples $(T_1(C,X),\ldots,T_r(C,X))$, $r \in \mathbb{N}$. Then the infinite disjunction $\bigvee_{\lambda\in\Lambda}$ minimal $\text{primes}_{T_\lambda}(c)$ is true in every structure (K^*,c) with $K^* \models pFL^*$ and $c \in K^k$. The compactness theorem allows one to replace the infinite disjunction by a finite subdisjunction. □

Remark

The same arguments as at the end of (3.7) show that $T_1,\ldots,T_M$ can be found effectively. Hence the statement made in (3.8) follows.

I will now indicate how everything generalizes to arbitrary fields K. We use the function α introduced in (2.1).

(3.11) *Lemma*

For all $m,n,d \in \mathbb{N}$ and each field extension $L|K$ with $[L : K] = m$ and each ideal I of $L[X]$ which is generated by polynomials of degree $\leq d$ we have:

$I \cap K[X]$ is generated by polynomials of degree $\leq \alpha(n,d,m)$.

Proof

Let m,n,d,K,L and I be as indicated and let $I = (f_1,\ldots,f_\ell)$, $\deg f_i \leq d$. Take a K-linear basis $\alpha_1 = 1,\alpha_2,\ldots,\alpha_m$ of L and write:

(*) $\quad \alpha_i\alpha_j = \sum_k c_{ijk}\alpha_k \qquad (c_{ijk} \in K)$,

(**) $\quad f_i = \sum_k f_{ik}\cdot\alpha_k \qquad (f_{ik} \in K[X],\ \deg f_{ik} \leq d)$.

Using (*) and (**) the equation $\sum_{i=1}^{\ell}(\sum_{j=1}^{m} Y_{ij}\alpha_j)f_i = Z$ (the unknowns

Y_{ij}, Z ranging over $K[X]$) is equivalent to:

$$\begin{cases} \Sigma d_{ij1} Y_{ij} = Z \\ \cdots\cdots = 0 \\ \qquad\cdot \qquad\quad \cdot \\ \Sigma d_{ijm} Y_{ij} = 0 \end{cases} \qquad (d_{ijk} \in K[X] \text{ of degree } \leq d).$$

By construction the last components z of the solutions $(y_{11},..,y_{\ell m},z)$ of the system form the ideal $I \cap K[X]$, and, by (2.1), this ideal is generated by polynomials of degree $\leq \alpha(m,n,d)$. □

(3.12) *Definition*

An ideal I of $K[X]$ is said to be a separable prime ideal if I is a prime ideal such that the extension $Q(K[X]_{/I})|K$ is separable.

Note that (3.1) remains true with the following changes: omit 'perfect' in the hypothesis, replace (i) by: 'I is a separable prime ideal', and augment (ii) by requiring P to be separable in Z.

(3.13) *Lemma*

Let I be an ideal of $K[X]$. Then we have:

I is prime $\Leftrightarrow$ there exists a purely inseparable finite extension $L|K$ and a separable prime ideal J of $L[X]$ with $J \cap K[X] = I$.

Proof

$\Leftarrow$ is trivial. $\Rightarrow$: let $x_i = X_i + I$, so $Q(K[X]_{/I}) = K(x_1,..,x_n)$. It suffices to consider the case char. $K = p > 0$. $K^{p^{-\infty}}(x_1,..,x_n)|K^{p^{-\infty}}$ is separable, hence has a separating transcendence base $S \subset \{x_1,..,x_n\}$, so each x_i is root of a polynomial $\sum_j f_{ij}(S)T^j$, separable in $T, f_{ij}(S) \in K^{p^{-\infty}}[S]$. Let $L|K$ be any subextension of $K^{p^{-\infty}}|K$ containing the coefficients of all $f_{ij}(S)$, and let J be the ideal of all $g \in L[X]$ with $g(x_1,..,x_n) = 0$. Then J is clearly an ideal as required.

(3.14) It is useful to have some information on purely inseparable extensions: for $r \in \mathbb{N}$ we define a field $L|K$ to be of <u>type r</u> if either $L = K$, or $L = K(c_1^{p^{-r}},..,c_k^{p^{-r}})$ where $0 < \text{char } K = p \leqslant r$ and $\{c_1,..,c_k\}$ is a p-independent subset of K with k elements and $k \leqslant r$. See [Bo1, p. 133] for the definition of p-independence, and its consequences, among which is the following:
each purely inseparable extension of finite degree of K is a subextension of an extension of type r, for some $r \in \mathbb{N}$.
Let us also define an ideal I of $K[X]$ to be <u>prime of type</u> r if there is an extension $L|K$ of type r and an ideal J of $L[X]$ with $J \cap K[X] = I$, this ideal J satisfying the following: $J = (f_1,..,f_m)$ for certain $f_i \in L[X]$ of degree $\leqslant r$, and there is $0 \leqslant t \leqslant n$ and there are irreducible $P \in L[Y_1,..,Y_t,Z]$, separable and of positive degree in Z, and $h_1,..,h_n \in L[Y_1,..,Y_t,Z]$, $h \in L[Y_1,..,Y_t]\setminus\{0\}$ and $g_1,..,g_t, g \in L[X]$ such that *(a)*, *(b)*, *(c)* and *(d)* of (3.1) hold, with K, d, I changed to L, r, J.

(3.15) Finally we can prove *(1.4)* for arbitrary K: by (3.11) we can construct for each $r \in \mathbb{N}$ a formula <u>prime type</u>$_r(C)$ such that for each field K and $c \in K^k$:
$K \models$ <u>prime type</u> $_r(c) \Leftrightarrow (f_1(c,X),...,f_m(c,X)) \subset K[X]$ is prime of type r.
By (3.13) and the remark in (3.12) we get that for each field K and each $c \in K^k$ $(f_1(c,X),...,f_m(c,X)) \subset K[X]$ is prime iff
$K \models \bigvee\{$<u>prime type</u>$_r(c)$ $r \in \mathbb{N}\}$.
The rest of the argument is similar to the proof in (3.4), with '<u>prime type</u>$_r(C)$' taking over the role of the formula '<u>prime</u>$_r(C)$'. □

(3.16) Let us also generalize (3.7) and (3.10). We first extend the language of rings by adding, as in (3.6), the function symbols A_{ki} and B_{ki} $(1 \leqslant i \leqslant k \geqslant 2)$ and $^{-1}$, and also adding new (Skolem) function symbols C_{kip} $(1 \leqslant i \leqslant k \geqslant 2$, p a prime) of rank k. Then we extend the theory FL of fields to the theory FL^* in the new language by adding the same defining axioms for A_{ki}, B_{ki} and $^{-1}$ as in (3.6), and by adding defining axioms for the C_{kip} saying for a model K^* of FL^* (with underlying field K) and $c = (c_1, .., c_k) \in K^k$:
$(C_{k1p}(c), \dots, C_{kkp}(c))$ is a non-trivial solution in K^k of the equation $c_1 \cdot Y_1^p + \dots + c_k \cdot Y_k^p = 0$, if there is such a solution and char. $K = p > 0$.

FL^* might be called the theory of fields endowed with procedures for factoring polynomials, and solving linear dependence relations over the subfield of p^{th} powers, in case of characteristic $p > 0$.

Now (3.7), (3.8), (3.9) and (3.10) remain valid if we replace 'pFL^*' by 'FL^*', omit everywhere 'perfect', and add in the hypothesis of statement (*) of (3.8) that there is an algorithm to test whether a finite set is linearly independent over the subfield of p^{th} powers, in case of characteristic $p > 0$.

The proofs carry over.

APPENDIX

The two theorems in this appendix may be described as providing bounds for certain polynomial ideals and at the same time as giving information on the solvability of certain systems of equations. The novelty does not lie so much in these results, as well as in their proofs. See [Be., De., Li.& v.d.D.] for related results and proofs.

(A.1) *Definition*

A local ring $(R,\underline{m})$ ($\underline{m}$ = the maximal ideal of R) is called henselian if for each $f(T) \in R[T]$ and each simple root $\alpha \in \bar{R} = R/\underline{m}$ of $\bar{f}(T) \in \bar{R}[T]$ there is $a \in R$ with $f(a) = 0$ and $\bar{a} = \alpha$.

So a valued field (K,v) is henselian (Ch.I, (3.3)) iff its valuation ring is henselian. We will need the (wellknown) equivalence of 'Hensel's Lemma' with a strong form of it , sometimes called after Hensel-Rychlik.

(A.2) *Proposition*

For a local ring $(R,\underline{m})$ the following are equivalent:

(*i*) $(R,\underline{m})$ is henselian.

(*ii*) For each $f(T) \in R[T]$, $a \in R$, $c \in \underline{m}$ such that $f(a) = c\cdot(f'(a))^2$, there is $b \in R$ with $f(b) = 0$ and $a-b \in cf'(a)R$.

Proof

(*i*) $\Rightarrow$ (*ii*): write $f(a+T) = f(a) + f'(a)\cdot T + \sum_{i\geq 2} b_i T^i =$ $c\cdot(f'(a))^2 + f'(a)\cdot T + \sum_{i\geq 2} b_i T^i$, for certain $b_i \in R$.

Substitution of $cf'(a)Z$ for T gives:

$$f(a+cf'(a)Z) = c(f'(a))^2 \quad (1+Z+\sum_{i\geq 2} cd_i Z^i)$$

for certain $d_i \in R$.

$1+Z+\Sigma cd_i Z^i$ has a root z in R, so $b = a+cf'(a)z$ is a root of $f(T)$ as required.

(i) is a special case of *(ii)*, so *(ii)* $\Rightarrow$ *(i)* is trivial. □

(A.3) ***Lemma***

Let a commutative diagram of rings and ring morphisms be given

$$\begin{tikzcd} D \arrow[rr] \arrow[dr, hook] & & V \arrow[d, "\pi"] \\ & R \arrow[ur, dashed, "\lambda"] \arrow[r, "g"'] & C \end{tikzcd}$$

such that

(i) V is a henselian valuation ring,

(ii) π is onto, g is 1-1, and C is a domain,

(iii) R is finitely generated over its subring D and $Q(R)|Q(D)$ is separable.

Then R can be lifted, i.e. there is a morphism λ as indicated which makes the two subdiagrams commutative.

Proof

Because $D \to V$ and $R \to C$ are 1-1 we consider D as a subring of V and R as a subring of C.

By induction on the number of generators of R over D it suffices to consider the case that $R = D[r]$ and either

(a) r is transcendental over D, or

(b) r is separable algebraic over $Q(D)$.

In case *(a)*, choose any $b \in V$ with $\pi(b) = r$ and define λ by putting $\lambda(r) = b$.

Suppose *(b)* holds. Let $f(T) \in D[T]$ be such that f is irreducible in $Q(D)[T]$ and $f(r) = 0$. Choose any $b \in V$ with $\pi(b) = r$. Then $f(b) \in \mathrm{Ker}(\pi)$ and $f'(b) \notin \mathrm{Ker}(\pi)$ (because $f(r) = 0$, $f'(r) \neq 0$). As V is a valuation ring, this implies that $f(b) = c\cdot(f'(b))^2$ with $c \in \mathrm{Ker}(\pi)$ (for if $c \notin V$ we get a contradiction applying π to $\frac{1}{c}\cdot f(b) = (f'(b))^2$, and $c \in V\setminus\mathrm{Ker}(\pi)$ similarly gives a contradiction). Then, by *(A.2)*, there is $b' \in V$ with $f(b') = 0$ and $b-b' \in \mathrm{Ker}(\pi)$, i.e. $\pi(b') = r$. Then $\lambda(r) = b'$ defines a morphism as required. □

In the following theorem, we write $v(a_1,\ldots,a_k)$ for $\min(va_1,\ldots,va_k)$ (v a valuation).

(A.4) ***Theorem***

Let D be a domain of characteristic 0 and $f = (f_1(X),\ldots,f_m(X))$, $f_i(X) \in D[X]$, $X = (X_1,\ldots,X_n)$.

Then there is an integer $c \geqslant 1$ and a nonzero $d \in D$ with the following property:

for each henselian valuation ring $V \supset D$, with associated valuation $v : Q(V)^{\cdot} \to \Gamma_v$, each $g \in \Gamma_v, g > 0$, and each $x \in V^n$ such that $v(fx) > c.g + v(d)$, there is $y \in V^n$ with $f(y) = 0$ and $v(y-x) > g$.

Remark

With D noetherian and the rings $V \supset D$ restricted to discrete valuation rings, this is [Gr, Theorem on p.143].

***Proof of** (A.4)*

Suppose this is not true. Then for each $c \in \mathbb{N}\setminus\{0\}$ and $d \in D\setminus\{0\}$ there is a triple $(V_{c,d}, g_{c,d}, x_{c,d})$ with a henselian valuation ring $V_{c,d} \supset V$, $0 < g_{c,d} \in$ value group associated to $V_{c,d}$ and $x_{c,d} \in (V_{c,d})^n$

such that $v_{c,d}(f(x_{c,d})) > c.g_{c,d} + v_{c,d}(d)$ and there is no $y \in (V_{c,d})^n$ with $fy = 0$ and $v_{c,d}(y-x) > g_{c,d}$.

(*) Note that for $c_1,..,c_k \in \mathbb{N}\setminus\{0\}$ and $d_1,..,d_k \in D\setminus\{0\}, k > 0$, the triple $(V_{c,d}, g_{c,d}, x_{c,d})$, with $c = \Sigma c_i$, $d = \Pi d_i$, has simultaneously the properties required for each $(V_{c_i,d_i}, g_{c_i,d_i}, x_{c_i,d_i})$ $(i=1,...,k)$.

The statement (*) implies by an obvious compactness argument that there is even a triple $({}^*V, {}^*g, {}^*x)$ with ${}^*V$ a henselian valuation ring, ${}^*V \supset D$, $0 < {}^*g \in$ value group of ${}^*V$, and ${}^*x \in ({}^*V)^n$ such that for <u>all</u> $c \in \mathbb{N}\setminus\{0\}, d \in D\setminus\{0\}$:

${}^*v(f({}^*x)) > c.{}^*g + {}^*v(d)$, and there is no $y \in ({}^*V)^n$ with $f(y) = 0$ and ${}^*v(y-{}^*x) > {}^*g$ (${}^*v$ = valuation associated to ${}^*V$).

Put $I = \{a \in {}^*V \mid {}^*v(a) > c.g + {}^*v(d)$ for all $c \in \mathbb{N}\setminus\{0\}$ and $d \in D\setminus\{0\}\}$.

It is clearly a prime ideal of ${}^*V$. Putting $C = {}^*V/I$ and letting $\pi : {}^*V \to C$ be the canonical map, we obtain a commutative diagram:

$$\begin{tikzcd} D \arrow[r, hook] \arrow[dr] & {}^*V \arrow[d, "\pi"] \\ & C \end{tikzcd}$$

$D \to C$ is 1-1: if $0 \neq d \in D$, then clearly $d \notin I$, so $\pi(d) \neq 0$.

Now $\pi({}^*x) \in C^n$ is a solution of $f(X) = 0$, because $f({}^*x) \in I$.

Because $Q(D[\pi({}^*x)])|Q(D)$ is separable, (A.3) implies that $\pi{}^*x$ can be 'lifted' to a solution $y \in ({}^*V)^n$ of $f(X) = 0$, so ${}^*v(y-{}^*x) > {}^*g$ (because $\pi(y) = \pi({}^*x)$), contradiction. □

In the following, let $X = (X_1,..,X_n)$, let K be a field, and define $K[X]^\sim = \{f \in K[\![X]\!] \mid f$ is algebraic over $K(X)\}$.

A special case of a theorem of M. Artin, [Art, (1.10)], reads:

(A.5) <u>Let</u> $f(Y) = (f_1(Y),...,f_m(Y)), f_i(Y) \in K[X,Y], Y = (Y_1,..,Y_N)$.

<u>If</u> $f(Y) = 0$ <u>has a solution in</u> $K[\![X]\!]$, <u>then it has a solution in</u> $K[X]^\sim$.

Remark

Using the terminology introduced in Ch. I, (2.2), this is equivalent to saying that the ring $K[X]^{\sim}$ is existentially closed in $K[\![X]\!]$. With a variant of the reduction described in Ch. I, (2.4), one can indeed streamline Artin's proof at some points, but this will not be done here. Artin uses an elaborate analysis of his proof to derive a seemingly much stronger result, namely (A.6) below, cf. [Art, (6.1)]. We will show that (A.6) is a simple model theoretic consequence of (A.5).

(A.6) *Theorem*

Let $m,n,N,d,\alpha \in \mathbb{N}$ be given. Then there is $\beta = \beta(m,n,N,d,\alpha) \in \mathbb{N}$ such that for each field K and $f(Y) = (f_1(Y),\dots,f_m(Y)) \in (K[X,Y])^m$ ($X = (X_1,\dots,X_n)$, $Y = (Y_1,\dots,Y_N)$), with all $f_i(Y)$ of total degree $\leqslant d$ in (X,Y), and each $\bar{y} \in K[X]^N$ with $f(\bar{y}) \equiv 0(\mathrm{mod}(X)^{\beta})$ there is $y \in (k[X]^{\sim})^N$ with $f(y) = 0$ and $\bar{y} \equiv y(\mathrm{mod}(X)^{\alpha})$.

(A.7) *Lemma*

Let k be a field, $f(Y) = (f_1(Y),\dots,f_m(Y))$, $f_i(Y) \in k[X,Y]$. $X = (X_1,\dots,X_n)$, $Y = (Y_1,\dots,Y_N)$ and $\alpha \in \mathbb{N}$. Then there is $\beta \in \mathbb{N}$ such that for each $\bar{y} \in k[X]^N$ with $f(\bar{y}) \equiv 0(\mathrm{mod}(X)^{\beta})$ there is $y \in (k[X]^{\sim})^N$ with $f(y) = 0$ and $y \equiv \bar{y}(\mathrm{mod}(X)^{\alpha})$.

Proof

Suppose this is not true. Then for each $b \in \mathbb{N}$ there is $y_b \in k[X]^N$ with $f(y_b) \equiv 0(\mathrm{mod}(X)^b)$ but such that for no $y \in (k[X]^{\sim})^N$: $f(y) = 0$ and $y \equiv y_b(\mathrm{mod}(X)^{\alpha})$.

Let M be a structure containing all relevant objects.

In an enlargement $^*M$ of M the objects $k, k[X]$, etc. have nonstandard extensions $^*k, ^*(k[X])$, etc., and the sequence $(y_b)_{b\in\mathbb{N}}$ extends to a *sequence $(y_b)_{b\in {}^*\mathbb{N}}$.

Let $\omega \in {}^*\mathbb{N}\setminus\mathbb{N}$. Then $f(y_\omega) \equiv 0(\bmod (X)^\omega)$ (in the ring $^*(k[X])$, and there is no $y \in ({}^*(k[X]^\sim))^N$ with $f(y) = 0$ and $y \equiv y_\omega(\bmod (X)^\alpha)$.

The map $\pi : {}^*(k[X]) \to {}^*k[\![X]\!]$, given by

$$\pi(\sum_{i\in({}^*\mathbb{N})^n} a_i X^i) = \sum_{i\in\mathbb{N}^n} a_i X^i$$

is clearly a $^*k[X]$-morphism, and $f(\pi y_\omega) = 0$ in $^*k[\![X]\!]$, hence by (A.5) there is $y' \in ({}^*k[X]^\sim)^N$ with $f(y') = 0$ and $y' \equiv \pi y_\omega(\bmod (X)^\alpha)$.

The henselian local ring $({}^*k[X])^\sim,(X){}^*(k[X])^\sim)$ extends the local ring $({}^*k[X]_{(X)},(X){}^*k[X]_{(X)})$, so there is a $^*k[X]_{(X)}$-morphism Θ of $({}^*k[X])^\sim$ into $^*(k[X]^\sim)$ (cf. [La, Th. 4]). Let $y = \Theta(y')$. Then $f(y) = 0$.

Write $y_\omega = u+v$ with $u \in ({}^*k[X])^N$ and $v \equiv 0(\bmod (X)^\alpha)$ (in $^*(k[X])$).

Then it is straightforward to check that $y_\omega, \pi y_\omega, y'$ and y are all congruent to u modulo $(X)^\alpha$, (in the ring $^*(k[X]^\sim)$), so $y_\omega \equiv y(\bmod (X)^\alpha)$, contradiction! □

(A.8) Proof of (A.6)

Let $F_1(C,X,Y),\ldots,F_m(C,X,Y) \in \mathbb{Z}[C,X,Y]$ be the m general polynomials of degree d in (X,Y) (so $C = (C_1,\ldots,C_M)$ with $M = m.\binom{d+n+N}{n+N}$).

Consider the elementary class Mod(T), whose models are the structures $\mathcal{R} = (R,\underline{m},K,X_1,\ldots,X_n,d_1,\ldots,d_M) = (R,\underline{m},K,X,d)$ such that:

$(R,\underline{m})$ is a henselian local ring, K a subfield of R, $X_1,\ldots,X_n$ are elements of $\underline{m}$ which are algebraically independent over K, and $d_1,\ldots,d_M \in K$.

(*) For each field K and $c \in K^M$ $(K[X]^\sim,(X)K[X]^\sim,K,X,c)$ is a model of T which can embedded over K into each model $(R,\underline{m},K,X,d)$ of T (cf. [La, Th. 4]).

For each $b \in \mathbb{N}$ one easily constructs a sentence σ_b such that for each model $\mathcal{R} = (R,\underline{m},K,X,d)$ of T:

$\mathcal{R} \models \sigma_b \Leftrightarrow$ for each $\bar{y} \in (K[X])^N$ with $F_i(a,X,\bar{y}) \equiv 0(\mathrm{mod}(X)^b),(i=1,..,m)$, there is $y \in R^N$ with $F_1(d,X,y) = \ldots = F_m(d,X,y) = 0$, and $y \equiv \bar{y}(\mathrm{mod}\ \underline{m}^b)$. (It clearly suffices in the right hand side to consider only $\bar{y}$ all of whose components are of degree $\leqslant b$.)

Using (*) and the lemma this implies:

$$T \models \vee\{\sigma_b | b \in \mathbb{N}\}.$$

By compactness there is then $\beta \in \mathbb{N}$ such that $T \vdash \sigma_\beta$.

This β clearly satisfies the requirements. □

(A.9) ***Remark***

One can effectively write down a list of axioms for the theory T introduced in *(A.8)*, so given m,n,N,d,α in $\mathbb{N}$ we can effectively find a $\beta \in \mathbb{N}$ satisfying *(A.6)*, by generating all theorems of T.

This has the following obvious but interesting consequence:

Let a field K be given and suppose there is an algorithm to decide whether a given finite system of polynomial equations with coefficients in $\mathbb{F}$ ($\mathbb{F}$ the prime field of K, or even any computable subfield of K) has a solution in K.

(Examples of such fields are the finite, algebraically closed, real closed and p-adic fields.)

Then there is also an algorithm to decide whether a given finite system of polynomial equations with coefficients in $\mathbb{F}[X_1,..,X_n]$ has a solution in $K[\![X_1,..,X]\!]$.

REFERENCES

[Ab] S.S. Abhyankar, *Historical ramblings in algebraic geometry*, Am. Math. Monthly 83 (1976), 409-448.

[Ar] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, Hamb. Abh. 5 (1927), 100-115.

[Ar. & S.] E. Artin and O. Schreier, *Algebraïsche Konstruktion reeller Körper*, Hamb. Abh. 5 (1926), 85-99.

[Art] M. Artin, *Algebraic approximation of structures over complete local rings*, Publ. Math. I.H.E.S. 36 (1969), 23-58.

[Ax] J. Ax, *The elementary theory of finite fields*, Ann. of Math. 88 (1968), 239-271.

[Ax & Ko] J. Ax and S. Kochen, *Diophantine problems over local fields III*: Ann. of Math. 83 (1966), 437-456.

[Bac] P. Bacsich, *Defining algebraic elements*, J.S.L. 38 (1973), 93-101.

[Baer] R. Baer, *Dichte, Archimedizität und Starrheit geordneter Körper*, Math. Ann. 188 (1970), 165-205.

[Be., De., Li. & v.d.D.] J. Becker, J. Denef, L. Lipshitz and L. van den Dries, *Ultraproducts and approximation in local rings*, Preprint, 28 pages.

[Bo1] N. Bourbaki, *Algèbre, Chapitres 4 et 5.* Hermann, Paris (1959).

[Bo2] N. Bourbaki, *Algèbre Commutative, Chapitres 1 et 2.* Hermann, Paris (1961).

[Br., Er. & Ka.] S. Bredikhin, Yu. Eršov and V. Kal'nei, *Fields with two linear orderings*, Matem. Zam, 7 (1970), 525-536 = Math. Notes 7 (1970), 319-325.

[C] P.J. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure & Appl. Math. 22 (1969), 131-153.

[Ch. & Ke.] C. Chang and H. Keisler, *Model Theory.* North-Holland, Amsterdam (1973).

[v.d.D. & Ri] L. van den Dries and P. Ribenboim, *A Lefschetz' principle in Galois theory*, Preprint, 8 pages.

[Ek] P. Eklof, *Ultraproducts for Algebraists*, in [HML], 105-137.

[Ek. & Sab.] P. Eklof and G. Sabbagh, *Model completions and modules*, Ann. of Math. Logic 2 (1971), 251-295.

[Er] Yu. Eršov, *Semilocal fields*, Soviet Math. Dokl. 15 (1974), 424-428.

[F. & S.] M. Fried and G. Sacerdote, *Solving diophantine problems over all residue class fields of a number field and all finite fields*, Ann. of Math. 194 (1976), 203-233.

[Gr] M. Greenberg, *Strictly local solutions of diophantine equations*, Pac. J. of Math. 51 (1974), 143-153.

[He] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. 95 (1926), 736-788.

[Hi] D. Hilbert, *Axiomatisches Denken*, Math. Ann. 78 (1918), 405-415.

[HML] *Handbook of Mathematical Logic*, ed. Barwise, North-Holland, Amsterdam (1977).

[J1] M. Jarden, *Elementary statements over large algebraic fields*, Trans. AMS 164 (1972), 67-91.

[J2] M. Jarden, *Algebraic extensions of hilbertian fields of finite corank*, Israel J. of Math. 18 (1974), 279-307.

[Ka] I. Kaplansky, *Polynomials in topological fields*, Bull. AMS 54 (1948), 909-916.

[Ki] C. Kiefe, *Sets definable over finite fields : their zeta-functions*, Trans. AMS 223 (1976), 45-59.

[Ko] S. Kochen, *Integer valued rational functions over the p-adic* *numbers*: a p-adic analogue of the theory of real fields, in *Proceedings of Symposia in Pure Mathematics XII*, *Number Theory*, ed. Leveque-Strauss, AMS (1969), 57-73.

[K. & N.] W. Krull and J. Neukirch, *Die Struktur der absoluten Galoisgruppe über dem Körper* $\mathbb{R}(t)$, Math. Ann. 193 (1971), 197-209.

[La] J.-P. Lafon, *Anneaux Henséliens*, Bull. Soc. math. France 91 (1963), 77-107.

[L1] S. Lang, *Introduction to Algebraic Geometry*, Interscience, New York, (1958).

[L2] S. Lang, *Diophantine Geometry*, Interscience, New York, (1961).

[L3] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., (1965).

[M1] A. Macintyre, *On definable subsets of p-adic fields*, J.S.L. 41 (1976), 605-610.

[M2] A. Macintyre, *Model completeness*, in [HML], 139-180.

[M., M. & v.d.D.] A. Macintyre, K. McKenna and L. van den Dries, *Quantifier elimination in algebraic structures*, Preprint.

[McK] K. McKenna, *New facts about Hilbert's 17th problem*, in [MA], 220-230.

[MA] *Model Theory and Algebra*. *A memorial Tribute to Abraham Robinson*, ed. Saracino & Weispfenning, Lecture Notes 498, Springer-Verlag, Berlin, (1975).

[P] A. Prestel, *Lectures on formally real fields*, Monografias de Matemática, IMPA, Rio de Janeiro, (1975).

[P. & Z.] A. Prestel and M. Ziegler, *Model theoretic methods in the theory of topological fields*, to appear.

[Ra] M. Rabin, *Computable algebra: general theory and theory of computable fields*, Trans. AMS 95 (1960), 341-360.

[Ri1] P. Ribenboim, *Théorie des Valuations*, Publ. du Dépt. de Math., Univ. de Montréal (1967).

[Ri2] P. Ribenboim, *L'Arithmétique des corps*, Hermann, Paris (1972).

[Rob1] A. Robinson, *On ordered fields and definite functions*, Math. Ann. 130 (1955), 257-271.

[Rob2] A. Robinson, *Complete Theories*, North-Holland, Amsterdam (1956).

[Rob3] A. Robinson, *Solution of a problem of Tarski*, Fund. Math. 47 (1959), 179-204.

[Rob4] A. Robinson, *Metamathematical problems*, J.S.L. 38 (1973), 500-516.

[Rob. & Roq.] A. Robinson and P. Roquette, *On the Finiteness Theorem of Siegel and Mahler concerning Diophantine Equations*, J. of Number Theory 7 (1975), 121-176.

[Roq] P. Roquette, *Nonstandard aspects of Hilbert's Irreducibility Theorem*, in [MA], 231-275.

[Sa] G. Sacks, *Saturated Model Theory*, Benjamin, New York, 1972.

[Se] A. Seidenberg, *Constructions in Algebra*, Trans. AMS 197 (1974), 273-313.

[Sh] J. Shoenfield, *Mathematical Logic*, Addison-Wesley, Reading, Mass., 1967.

[v.d.W.] B. van der Waerden, *Moderne Algebra I*, Springer-Verlag, Berlin, (1930).

[We] V. Weispfenning, *On the elementary theory of Hensel fields*, Ann. of Math. Logic 10 (1976), 59-93.

[Wi] P. Winkler, *Model-completeness and Skolem expansions*, in [MA], 408-463.

[Wo] C. Wood, *The model theory of differential fields revisited*, Israel J. of Math. 25 (1976), 331-352.

SAMENVATTING

Een favoriete bezigheid van wiskundigen is altijd geweest het oplossen van vergelijkingen, dit 'oplossen' op te vatten in ruime zin.
Tot in de 20e eeuw lag hierbij de nadruk op het vinden van directe, algoritmische methoden, die overigens altijd van het grootste belang zullen zijn.
Beschouw nu bijvoorbeeld een vergelijking
(*) $f(x_1,..,x_n) = 0$ (f een veelterm met rationale coëfficiënten), waarbij de oplossingen in rationale getallen gevraagd worden, een zgn. *Diophantische vergelijking*.
Voor zelfs vrij eenvoudige Diophantische vergelijkingen bleken algoritmische oplossingsmethoden niet beschikbaar te komen, of weinig inzicht te verschaffen. Om nu toch de gewenste informatie over de oplossingen te verkrijgen, ging men bijvoorbeeld de oplossingen van (*) in de p-adische lichamen $\mathbb{Q}_p$ en in het lichaam $\mathbb{R}$ der reëele getallen bestuderen. Dit procédé, genaamd *lokaliseren* en *completeren*, blijkt erg nuttig, vooral ook op het verwante gebied der algebraïsche meetkunde (zie b.v. de *'Introduction'* van [Bo2]).
Men kan zelfs met voordeel het oplossen in alle $\mathbb{Q}_p$ en in $\mathbb{R}$ vervangen door het oplossen in één ring, de ring $\mathbb{A}$ der adèles, die $\mathbb{Q}$ als deelring heeft. Nu is $\mathbb{A}$ voor arithmetische doeleinden zo bijzonder geschikt gebleken vanwege zijn topologische eigenschappen. Deze geschiktheid is onlangs nog eens bevestigd door zijn modeltheoretische eigenschappen: er is een effectieve methode om van een gegeven 'elementaire' uitspraak over ringen na te gaan of deze waar is voor $\mathbb{A}$, i.h.b. kan men van een vergelijking (*) bepalen of er oplossingen in $\mathbb{A}$ zijn, of er oneindig veel zijn, enz. Dit resultaat (Weispfenning, nog ongepubliceerd) kan men beschouwen als een samenvatting van eerder werk door A. Tarski,

A. Robinson, J. Ax, S. Kochen, Ju. Eršov en P.J. Cohen.

Nu is het belang van $\mathbb{A}$ voor Diophantische vergelijkingen sterk afhankelijk van: welke eigenschappen van $\mathbb{Q}$ worden in $\mathbb{A}$ weerspiegeld? Men kan b.v. zeggen dat sommige 'kwadratische' eigenschappen van $\mathbb{Q}$ in $\mathbb{A}$ goed teruggevonden kunnen worden (Hasse-Minkowski). Maar $\mathbb{Q}$ heeft geen nuldelers en $\mathbb{A}$ wel. O.a. deze overwegingen hebben mij er toe gebracht om de modeltheoretische aspecten te bestuderen van de lichamen die in de hoofdstukken II en III aan de orde komen.
Typisch voorbeeld: beschouw de objecten $(K,<,v_1,v_2)$ met K een lichaam, $<$ een lineaire ordening op K, $v_1 : K^\cdot \to \mathbb{Z}$ een p-adische waardering, d.w.z. $v_1(p) = 1$ en $K_{v_1} = \mathbb{F}_p$, en $v_2 : K^\cdot \to \mathbb{Z}$ een q-adische waardering (p en q gegeven priemgetallen).
Voor de 'existentieel afgesloten' objecten in deze categorie blijkt inderdaad een resultaat te gelden als boven voor $\mathbb{A}$ beschreven is (zie Ch. III, (3.1)). Mijn hoop is dat deze existentieel afgesloten objecten de structuur van $\mathbb{Q}$ beter behouden dan de ring $\mathbb{R}\times\mathbb{Q}_p\times\mathbb{Q}_q$.

Hoofdstuk IV is van een ander karakter: hierin worden enkele problemen opgelost die door A. Robinson zijn gesuggereerd, zie [Rob4, problem 3].

CURRICULUM VITAE

Zoals al uit het titelblad blijkt werd de schrijver van dit proefschrift geboren op *26 mei 1951* te Ens (N.O.P.).
In *1969* behaalde hij het diploma gymnasium-β aan het Prof. ter Veen lyceum (Emmeloord) en ging in hetzelfde jaar wiskunde studeren aan de Rijksuniversiteit Utrecht (bijvakken aanvankelijk natuur- en sterrenkunde, later wijsbegeerte van de wiskunde). In *1973* legde hij het kandidaatsexamen af, en op *1 juli 1974* het doctoraal examen, met als hoofdrichting grondslagen van de wiskunde.
Vanaf *1 februari 1975* is hij aangesteld als tijdelijk wetenschappelijk medewerker aan het Mathematisch Instituut te Utrecht om onderzoek te doen op het gebied van de grondslagen der wiskunde, te assisteren bij het onderwijs hierin, en bij het wiskunde onderwijs aan voorkandidaten.

Van belang voor het tot stand komen van dit proefschrift is geweest o.a.:
het volgen van lezingen door *Prof. S. Kochen* over 'The Model Theory of Local Fields' (Kiel, 1974), een verblijf in Kingston (Canada) en de samenwerking aldaar met *Prof. P. Ribenboim* (september - december '75), maar bovenal de inspiratie uitgaande van de werken van *Abraham Robinson* (1918-1974).