MODEL-COMPLETENESS

by

Philip Kelenson

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements for the degree of Master of Arts.

Department of Mathematics,
McGill University,
Montreal.

August 1961

I am grateful

to Professor Lambek

for his encouragement and assistance.

Contents

Introduction

A sentence X in the lower predicate calculus L is said to be defined in a set K of sentences in L if all the extralogical symbols of X occur in K. K is said to be complete if every sentence X in L which is defined in K and which is consistent with K, is deducible from K. Semantically, the completeness of a set K asserts that any two models of K satisfy the same "axioms" (sentences) which can be formulated in L using only the extralogical symbols that appear in K. Thus from the fact that the set K* of axioms for the concept of an algebraically closed field of specified characteristic is complete, it follows that a sentence X in L which is satisfied by the field of complex numbers is satisfied also by all fields of characteristic zero. Again, the completeness of the "theory" of real closed fields implies that any sentence in L which is satisfied by the field of real numbers can be deduced from the set K_R of axioms for the concept of a real closed field.

The completeness of the theories of real closed fields and of algebraically closed fields of specified characteristic was first established by A. Tarski (see Tarski [1] p.p. 54-55) as a corollary to the construction of a decision procedure for real closed fields. Tarski makes use of a generalization of Sturm's theorem and of an effective method of elimination of quantifiers. These results were obtained independently of a detailed procedure of elimination, by A. Robinson, using a modified notion of completeness, called "model-completeness." Other interesting results on the completeness of algebraic theories were also obtained (see Robinson [3]).

Briefly, we define a set K of sentences in L to be model-complete if, for any model M of K, any two extensions of M which are models of K satisfy the same elementary "axioms" which can be formulated in terms of the relations, operations and elements of M. Many interesting applications of the concept of model -completeness to problems of a metamathematical and purely mathematical (algebraic) nature have also been given by Robinson in a series of recent publications. (See especially Robinson [3], [8], [9], [10]). The purpose of this thesis is to assemble these results. More specifically, we shall develop the general theory of model-completeness in detail, and give examples of its application to questions of completeness of algebraic theories on the one hand, and to "concrete" algebraic problems on the other.

A central theme of this paper is to establish the model-completeness of the elementary theories of real closed and algebraically closed fields. Using the model completeness of the theory of real closed fields we shall present a generalized solution of Hilbert's 17th problem - "The Expression of Definite Forms by Squares"- which was originally solved by E. Artin. Moreover, we shall strengthen Artin's result by proving the existence of upper bounds for the number of squares required and for the degrees of the summands involved.

It will be shown that the concept of model-completeness is closely connected with the notions of "persistent" and "invariant" predicates in the lower predicate calculus L. It then follows that a generalized version of model-completeness, called relative model-completeness, can be successfully applied to certain problems of definability in L. Further concrete results in field theory are then obtained.

All the results of this paper were obtained by Robinson using a formal la guage L_0 which does not include function symbols. Since every function of n places may be regarded as an n+1-ary relation it follows that every formula including function symbols is "translatable" or "interpretable" in L_0. We have included function symbols in our language L to facilitate the formalization of algebraic theories and the proof of the "extended completeness theorem". This theorem and its corollaries which are proved in chapter 3 are of fundamental importance in all subsequent chapters of the text.

Chapter 0. Mathematical preliminaries.

(0.0) Let A be a set of objects and let $\emptyset$ be a set of n-ary functions or operations (n = 0,1,2,...) such that the set of 0-ary functions of $\emptyset$ is to be identified with A. We say that A is closed with respect to $\emptyset$ if for any m-tuple $a_1, \ldots a_m$ of elements of A ($m \geq 0$) and any m-ary function $G(x_1, \ldots x_m)$ in $\emptyset$ we have $G(a_1, \ldots a_m) \in A$ whenever each $a_i \in A$, i = 1,2,...m.

(0.1) By a (mathematical) system M we shall understand an ordered triple $M = (A, \emptyset, \mathcal{R})$ where

(1) A is a non-empty set of objects called the constants of M.

(2) $\emptyset$ is a set of n-ary functions or operations (n=0,1,2,...) such that A is closed with respect to $\emptyset$. The set of n-ary functions where $n \geq 1$ may be empty.

(3) $\mathcal{R}$ is a non-empty set of n-ary relations (n = 1,2,...) such that every relation $R \in \mathcal{R}$ is well defined on the entire set A of constants of M, that is, for every m-tuple $a_1, \ldots a_m$ of constants of M it is definite (although not necessarily decidable) whether or not $R(a_1, \ldots a_m)$ holds in M.

We shall use the familiar notation $a \in M$, $G(x_1, \ldots x_m) \in M$ $R(x_1, \ldots x_m) \in M$ rather then the more correct notation $a \in A, G \in \emptyset$, $R \in \mathcal{R}$ to indicate that certain constants, functions or relations belong to the sets A, $\emptyset$, $\mathcal{R}$ respectively of the system M.

(0.2) Two systems $M = (A, \emptyset, \mathcal{R})$ and $M' = (A', \emptyset', \mathcal{R}')$ are said to be isomorphic (in symbols $M \simeq M'$) if there exist one-one mappings, $A \leftrightarrow A'$, $\emptyset \leftrightarrow \emptyset'$ and $\mathcal{R} \leftrightarrow \mathcal{R}'$ such that

(1) $G \in \emptyset \leftrightarrow G' \in \emptyset'$ only if G and G' are both n-ary functions, for some $n \geq 0$.

(2) $R \in \mathcal{R} \leftrightarrow R' \in \mathcal{R}'$ only if R and R' are both m-ary relations for some $m \geq 1$.

(3) If $G \in \emptyset \leftrightarrow G' \in \emptyset'$ where G and G' are both n-ary functions, $n \geq 1$ and $a_i \in A \leftrightarrow a_i' \in A'$ i=1,2,...n then $G(a_1, \ldots a_n) \leftrightarrow G'(a_1', \ldots a_n')$.

(4) $R(a_1, \ldots a_m)$ holds in M if and only if $R'(a_1', \ldots a_m')$ holds in M' where R and R' are any corresponding relations of M and M' respectively $(m \geq 1)$ and $a_i \in A \leftrightarrow a_i' \in A'$, $i=1,2,\ldots m$.

(0.3) Let $M_1=(A_1, \emptyset_1, \mathcal{R}_1)$ be a system. A system $M_2=(A_2, \emptyset_2, \mathcal{R}_2)$ is said to be an extension of M_1 if there exist subsets $A_1' \subseteq A_2$, $\emptyset_1' \subseteq \emptyset_2$, $\mathcal{R}_1' \subseteq \mathcal{R}_2$ such that:

(1) $M_1' = (A_1', \emptyset_1', \mathcal{R}_1')$ is a system.

(2) $M_1' \simeq M_1$

(3) For any m-ary relation $R' \in \mathcal{R}_1'$ and for any m-tuple $a_1' \ldots a_m' \in A_1'$, $R'(a_1', \ldots a_m')$ holds in M_1', if and only if it holds in M_2.

We shall employ the familiar notation $M_1 \subseteq M_2$ to indicate that M_2 is an extension of M_1. If, in addition, A_1' is a proper subset of A_2, then M_2 is called a proper extension of M_1 and we write $M_1 \subset M_2$. We also say that M_1 is a sub-system (proper subsystem) of M_2.

Of special importance are those mathematical systems in which a relation of equality is defined. With this in mind we say that:

(0.4) A system M is algebraic if it contains a binary relation $\equiv$ called a relation of equality in M such that, for arbitrary $a, b, c, a_1, a_2, \ldots a_n, b_1, b_2, \ldots b_n$, we have:

(1) $a \equiv a$ holds in M.

(2) $a \equiv b$ holds in M only if $b \equiv a$ holds in M.

(3) If $a \equiv b$ and $b \equiv c$ both hold in M then so does $a \equiv c$.

(4) If $a_1 \equiv b_1, \ldots a_n \equiv b_n$ all hold in M then $\zeta(a_1, \ldots a_n) \equiv \zeta(b_1, \ldots b_n)$ holds in M, for every n-ary function $\zeta \in M$, $n \geq 0$.

(5) If $a_1 \equiv b_1, \ldots a_n \equiv b_n$ all hold in M then $R(a_1, \ldots a_n)$ holds in M only if $R(b_1, \ldots b_n)$ holds in M where R is any n-ary relation of M, $n \geq 1$.

The relation $\equiv$ of an algebraic system M divides the set A of constants of M into equivalence classes $\overline{A}$ in the usual way

and these in turn, define an algebraic system $\overline{M}$, homomorphic with M with the relation $\overline{=}$ replaced by the relation = of ordinary mathematical equality. When discussing a concrete algebraic system such as a group, field, or (totally) ordered set, we shall refer to $\overline{M}$ rather then M and thus replace the relation $\overline{=}$ by =. By the cardinality of M we shall understand the cardinal number of the set $\overline{A}$ of constants of $\overline{M}$.

(0.5) We define a Boolean Algebra to be an algebraic system $B = (A, \cup, \cap, *)$ where $\cup$, $\cap$ are binary operations of B, $*$ is a unary operation of B, satisfying the postulates:

(1) $a \cup b = b \cup a$

(2) $(a \cup b) \cup c = a \cup (b \cup c)$

(3) $a \cap b = (a^* \cup b^*)^*$

(4) $a \cup b = a$ if and only if $a \cup b^* = c \cup c^*$

for arbitrary $a, b, c \in A$.

Let $B = (A, \cup, \cap, *)$ be a Boolean algebra.

(0.6) A non empty subset J of A is called an ideal in B if the conditions:

(1) $a \in J$ and $b \in J$ only if $a \cap b \in J$.

(2) $a \in J$ only if $a \cup b \in J$.

are satisfied for arbitrary $a, b \in A$. An ideal J in B is maximal if $J \neq A$ and if the only ideal in B of which J is a proper subset, is A itself.

(0.7) We shall require the following results which are proved in some detail in Robinson [1]:

(a) Every ideal $J \neq A$ is included in a maximal ideal Jo. (This follows by a direct application of Zorn's lemma.)

(b) A maximal ideal Jo in B is characterized by the fact that for any $a \in A$ precisely one of the two elements a and a^* belongs to Jo.

It follows that:

(c) If Jo is a maximal ideal of B then $a \cup b \in Jo$ if and only if either $a \in Jo$ or $b \in Jo$ (or both).

Chapter 1 The Propositional Calculus C

The propositional calculus C to which we refer below is that of Whitehead and Russel (in Principia Mathematica) as modified by Bernays. Its properties are discussed fully in Hilbert and Ackerman [1] ; also in Robinson [1] where a detailed proof of the extended completeness theorem is developed. We shall outline this proof below.

Following Robinson [1] we admit a set $P = \{p,q,r,\ldots\}$ of propositional variables of arbitrary transfinite cardinal number. It is assumed that the reader is familiar with the concepts of (well-formed) formula, theorem, truth function, tautology, disjuctive (conjunctive) normal form, and with the deductive properties of C.

(1.o) The connectives $\vee$ and $\sim$ are regarded as primary and denote disjunction and negation respectively. The connectives $\supset, \wedge, \equiv$, denote implication, conjunction, and equivalence respectively; and are to be regarded as abbreviations. Thus:

$(p \supset q) = \sim p \vee q$; $(p \wedge q) = \sim(\sim p \vee \sim q)$; $(p \equiv q) = (p \supset q) \wedge (q \supset p)$.

In what follows K shall denote an arbitrary subset (possibly empty) of the set F of all formulae of C, and R_K shall denote the set of all propositional variables which appear in (some of the formulae of) K.

(1.1) A truth function f(p), $p \in R$ which assigns truth values to the elements of R , that is, which maps R into the two element set $V = \{0,1\}$ is called a valuation of R .

(1.2) The inductive definitions:

(1) $f(\sim X) = 0$ if $f(X) = 1$

(2) $f(\sim X) = 1$ if $f(X) = 0$

(3) $f(X \vee Y) = 0$ if $f(X) = 0$ and $f(Y) = 0$

(4) $f(X \vee Y) = 1$, otherwise,

extend the domain of f to F_R where F_R is the set of all formulae generated by (that is, containing only) variables of R_K .

(1.3) A valuation f of R_K is said to be admissible (for given K)

if the extension (1.2) yields $f(X) = 1$ for all X in K

(1.4) A formula X is said to be deducible from K if there exist formulae $X_1, \ldots X_k \in K, k \geq 0$ such that the formula $Y = \left((X_1 \wedge \ldots \wedge X_k) \supset X\right)$ is provable in (is a theorem of) C. We stipulate that $Y = X$ for $k = 0$.

The following properties follow readily for arbitrary formulae X and Y:

(1.5) (a) If X belongs to K then X is deducible from K.

(b) X and Y are both deducible from K if and only if $(X \wedge Y)$ is deducible from K.

(c) If X is deducible from K then so is $(X \vee Y)$.

(1.6) A set K is said to be contradictory if every formula is deducible from K. An equivalent condition is that for some formula X the formula $(X \wedge \sim X)$ is deducible from K. Otherwise, K is consistent. We have:

(1.7) The set $K \cup \{X_1, \ldots X_u\}$ is contradictory if and only if the formula $\sim(X_1 \wedge \ldots \wedge X_u)$ is deducible from K. In particular for $X_1 = X$, it follows that the formula $\sim X$ is deducible from K if and only if the set $K \cup \{X\}$ is contradictory.

We define a relation $X \approx Y$ in F by the condition that $(X \equiv Y)$ be provable in C. We then have:

(1.8) The relation $\approx$ is an equivalence in F. Moreover, the relation $\approx$ is substitutive with respect to the application of the connectives $\sim$ and $\vee$. That is, if $X \approx X'$ and $Y \approx Y'$ then $\sim X \approx \sim X'$ and $(X \vee Y) \approx (X' \vee Y')$. We are now in a position to prove the "extended completeness theorem of C".

(1.9) Theorem. If a set K of formulae in C is consistent then there exists an admissible valuation for the variables R_K of K.

Proof: Let F_R be the set of formulae generated by the variables R_K, and let A be the set of equivalence classes of F_R modulo the relation $\approx$. On A we introduce the operations $\cup, \cap, *$ by the definitions:

$a \cup b = c$ if $X \vee Y \approx Z$

$a^* = b$ if $\sim X \approx Y$

$a \cap b = c$ if $X \wedge Y \approx Z$

for some (and hence for all) formulae $X \in a$, $Y \in b$, $Z \in c$. That these operations do indeed yield unique results follows from (1.8). It is also easily verified that the system $B = (A, \vee, \wedge, *)$ is a Boolean algebra.

By properties (b) and (c) of (1.5) it follows that those constants of B (equivalence classes of F_R) that contain formulae of F_R which are deducible from K constitute an ideal J_K of B. Now $J_K \neq A$, as K is consistent, by assumption. Hence by (0.7) -(a), J_K is contained in a maximal ideal Jo. Now Jo consists likewise of equivalence classes of F_R . Let Ko be the set theoretical union of all formulae which belong to these classes. Then, by property (a) of (1.5), we have $K \subseteq Ko$. We now assign the truth value 1 to all propositional variables which appear in Ko. It can be shown (by mathematical induction on the length of X, using properties (b) and (c) of (0.7) for Jo) that this valuation yields the truth value 1 for all X in Ko and the truth value 0 for all remaining formulae of F . As $K \subseteq Ko$, we have an admissible valuation for the variables R_K of K, as required.

We mention at this point that (1.9) in conjunction with (1.7) implies that every tautology in C is provable, that is C is complete in Gödel's sense. Since the axioms and rules of inference of C are chosen with the result that every theorem of C is a tautology, we have an effective method for determining the theorems (tautologies) of C.

Chapter 2. The language L (Lower predicate calculus with functors)

(2.0) Our object language L is constructed as follows:

Atomic Symbols:

(a) Individual variables x,y,z...constituting a countable set.

(b) Relation symbols of n places n=1,2,...

These consist of Roman Capitals followed by round brackets in which n empty argument places are indicated by means of commas. Thus R (, ,) is a ternary relation symbol. The number of relation symbols available for each n is supposed to be transfinite.

(c) Functors(function or operation symbols) of n places: n=0,1,...

These shall be denoted by Greek letters σ, π, φ...followed by round brackets as in (b). Functors of 0 places are called individual constants. These constitute a set of arbitrary transfinite cardinal number.

(d) Propositional Connectives: $\sim, \vee, \supset, \wedge, \equiv$

These are interpreted in accordance with (1.0).

(e) Quantifiers: ( ) ; (E)

These denote the universal and existential quantifiers respectively.

The expression (x) is to be read "For all x"

while (Ex) is to be read "There exists an x"

(f) Square brackets:

These are to be used for grouping the parts of a formula in the usual way. They shall often be omitted whenever no ambiguity results.

We shall refer to relation symbols and functors as the extralogical-symbols of L.

We define a set $\mathfrak{T}$ of terms of L inductively as follows:-

(2.1) (1) An individual variable is a term.

(11) An individual constant is a term.

(111) If $t_1,..t_n$ are terms and σ is a functor of n places n=1,2,.... then $\sigma(t_1,..t_n)$ is a term.

A term in which no individual variables appear is called a constant. Constants will be denoted by small Roman letters --a,b,c,....

(2.2) A relation symbol whose places have been filled by terms is called an Atomic formula. Thus, if R is a binary relation, G is a binary functor, τ is a unary functor, then R (G(τ(x),a),c) is an atomic formula.

We define a set of (well-formed) formulae of L inductively as follows:

(2.3) (a) (Bracketed) Atomic formulae are formulae.

(b) If X and Y are formulae then so are $\sim$X and X$\vee$Y, provided that X and Y do not contain identical variables of which only one is quantified.

(c) If X is a formula then (y) X and (Ey) X are formulae provided X does not already contain the variable y in a quantifier.

Thus the expression $(Ez)\, R(\varphi z) \vee Q(G(x,y), a)$ is a formula.

(2.4)Let (y) X and (Ey)X be formulae.
Whenever the variable y appears in X it is said to be within the scope of the quantifier ( ) or (E).

A variable y which occurs in a formula X is said to be free in X, if it is not within the scope of any quantifier.

A formula X which contains the n free variables $y_1,..y_n$ ($n \geq o$) and no other free variables will be called a predicate of order n or briefly an n-ary predicate. It will be denoted by X ($y_1,... y_n$). Predicates of order zero are called sentences. If X (y y) is a given predicate of order $n > o$ then X ($t_1,..t_n$) shall denote the formula obtained by substituting the terms $t_1,... t_n$ for the variables $y_1,..y_n$ respectively at all occurrences of $y_1,..y_n$ in X.

In particular X($a_1,.. a_n$) shall denote the sentence obtained by substituting the constants $a_1,.. a_n$ for $y_1,... y_n$ as above. We observe that X($a_1,.. a_n$) may contain other constants as well. Thus we shall also make use of the notation X ($a_1,... a_n$) to indicate simply that

the constants $a_1, \ldots a_\mu$ appear in the formula X. Then $X(y_1, \ldots y_\mu)$ shall indicate the predicate obtained by replacing $a_1, \ldots a_\mu$ by $y_1, \ldots y_\mu$ respectively.

We shall assume that the reader is familiar with the general deductive theory of the lower predicate calculus. Most of the results to follow shall be stated without proof. Following Robinson [1] and 2 we choose axioms and primitive rules of inference which prove to be most basic in the general theory. They also suffice to establish all the "required" semantic properties of L.

We define a subset T of the set S of sentences of L which we call the theorems or provable sentences of L inductively as follows:

(2.5) (a) Any sentence $f(X_1 \ldots X_\mu)$ which is obtained from a tautology (theorem) $f(p_1, \ldots p_\mu)$ of the propositional calculus C by substituting arbitrary sentences $X_1, \ldots X_\mu$ for the propositional variables $p_1, \ldots p_\mu$ of C respectively (and by inserting square brackets) is a theorem of L.

(b) If two sentences of the form X and $X \supset Y$ are theorems then Y is also a theorem.

(c) Any sentence of the form $[(x)\ F(x)] \supset F(a)$ or of the form $F(a) \supset [(Ex)\ F(x)]$ is a theorem where F(x) is a predicate of order one and a is any constant of L.

(d) A sentence is a theorem if it is obtained from a theorem by substituting one variable for another provided the result is a formula in the sense of (2.3).

(e) If a sentence of the form $X \supset F(a)$ is a theorem where F is a unary predicate and a is an individual constant which does not occur in the sentence X or in the predicate F then so is the sentence $X \supset [(y)\ F(y)]$ provided that it is a formula.

(f) If the sentence $F(a) \supset X$ is a theorem where F and a are defined as in (e) then so is the sentence $[(Ey)\ F(y)] \supset X$ provided that it is a formula.

(g) If $[(x_1)\ldots(x_m)F(x_1,\ldots x_m, \varphi(x_1,\ldots x_m)] \supset X$ is a theorem where F is an m + 1-ary predicate; φ is a functor of m places, and X is any sentence in which φ does not appear then th. sentence $[(x_1)\ldots(x_m)(Ez)\ F\ (x_1,\ldots x_m, z)] \supset X$ is a theorem provided that it is a formula.

We observe that by virtue of (a) and (b) of (2.5) all rules of inference which are valid in the propositional calculus C are likewise valid in L provided that we replace "formulae in C" by "sentences in L." Thus we may introduce the concepts of deducibility, consistency etc. in L in accordance with (1.4) and(1.6).

We note that every theorem of L is deducible from an arbitrary set K of sentences while a sentence X is deducible from the empty set of sentences if and only if X is provable.

In addition to properties (a), (b), (c) of (1.5) the following can be derived:

(2.6) (a) Let K, $\overline{K}$ be sets of sentences in L. Then the sentence X is deducible from $K \cup \overline{K}$ if and only if there exist sentences $\overline{Y}_1,\ldots\overline{Y}_n$ $(n \geq o)$ such that the sentence $[\overline{Y}_1 \wedge \ldots \wedge \overline{Y}_n] \supset X$ is deducible from K alone. (It is possible that n = o if $\overline{K}$ is empty or if X is deducible from K alone).

(b) If the sentences X and $X \supset Y$ are both deducible from a set K then so is Y.

(c) If a sentence $(x_1)\ldots(x_n)F(x_1,\ldots x_n)$, where F is a predicate of order $n \geq 1$ is deducible from a set K then so is the sentence $F\ (a_1,\ldots a_n)$ for arbitrary constants $a_1,\ldots a_n$.

(d) If a sentence of the form $F\ (a_1\ldots a_n)$ is deducible from a set K where F is a predicate of order $n \geq 1$ then so is the sentence $(Ex_1)\ldots(Ex_n)\ F\ (x_1,\ldots x_n)$.

(e) If the sentence $F(a_1,\ldots a_n)$ is deducible from K where F is a predicate of order $n \geq 1$ and $a_1,\ldots a_n$ are individual constants which do not appear in the sentences of K or in the predicate F then so is the sentence $(x_1)\ \ldots(x_n)\ F\ (x_1,\ldots x_n)$.

(f) If the sentence $X \supset F(a_1, \ldots a_u)$ is deducible from K where F is a predicate of order $n \geq 1$ and $a_1, \ldots a_u$ are individual constants which do not appear in X or in the sentences of K or in the predicate F then so is the sentence $X \supset [(x_1) \ldots (x_u) F(x_1 \ldots x_u)]$.

(g) If the sentence $F(a_1, \ldots a_u) \supset X$, where F and $a_1, \ldots a_u$ are defined as in (f), is deducible from K then so is the sentence $[(Ex_1) \ldots (Ex_u) F(x_1, \ldots x_u)] \supset X$.

Again, in addition to (1.7), we have:

(2.7) A set K of sentences is contradictory if and only if some (finite) subset of K is contradictory, or equivalently, a set K is consistent if and only if every (finite) subset of K is consistent.

Let K be an arbitrary set (possibly empty) of formulae.

(2.8) A formula Q is said to be <u>defined in K</u> if all the extralogical symbols that occur in Q also occur in (some of the formulae of) K. Q is said to be <u>partially-defined</u> in K if all relation symbols and functors of $n \geq 1$ places that occur in Q also occur in K. (We note that Q may still contain constants which do not appear in K.)

(2.9) Two predicates Q_1 and Q_2 of order $m \geq 0$ are said to be <u>K-equivalent</u> if the sentence $(x_1) \ldots (x_m) [Q_1(x_1, \ldots x_m) \equiv Q_2(x_1, \ldots x_m)]$ is deducible from K. In particular, two sentences X and Y are K-equivalent if the sentence $X \equiv Y$ is deducible from K.

We shall require the following result:

(2.10) If two predicates Q and Q* are K-equivalent then the sentence

$$(q_1)(q_2) \ldots (q_n) Q(x_1, \ldots x_n) \equiv (q_1)(q_2) \ldots (q_n) Q^*(x_1, \ldots x_n)$$

is deducible from K where n is the order of Q and $q_1, q_2, \ldots q_n$ is any sequence of quantifiers such that q_i contains the variable x_i, $i = 1, 2, \ldots n$.

<u>Proof</u>: Let $a_1, \ldots a_u$ be any individual constants which do not occur in either Q or Q* or in K. Then by (2.6)-(c), (1.5)-(b) and our hypothesis the sentence $Q(a_1, \ldots a_n) \supset Q^*(a_1, \ldots a_u)$ is deducible from K. Suppose first that $(q_u) = (x_u)$ then by (2.6) -(e) the sentence $(x_u) [Q(a_1 \ldots a_{u-1}, x_u) \supset Q^*(a_1, \ldots a_{u-1}, x_u)]$ is deducible from K and hence so is the sentence $[(x_u) Q(a_1, \ldots a_{u-1}, x_u)] \supset [(x_u) Q^*(a_1, \ldots a_{u-1}, x_u)]$

by the rules of deduction of the lower predicate calculus. Using (2.6)-(d) a similar argument yields the deducibility of the sentence $[(Ex_u)Q(a_1,\ldots a_{u-1},x_u)] \supset [(Ex_u)Q^*(a_1,\ldots a_{u-1},x_u)]$ from K. Thus in any case, the sentence $[(q_u)Q(a_1,\ldots a_{u-1},x_u)] \supset [(q_u)Q^*(a_1,\ldots a_{u-1},x_u)]$ is deducible from K. It follows by a simple induction argument that the sentence $[(q_1)\ldots(q_u)Q(x_1,\ldots x_u)] \supset [(q_1)\ldots(q_u)Q^*(x_1,\ldots x_u)]$ is deducible from K. The conclusion of (2.10) now follows from the hypothesis by interchanging Q and Q* in the above and by using (1.5)-(b).

(2.11) Two predicates (sentences) Y_1 and Y_2 are said to be <u>equivalent</u> if they are ϕ - equivalent where ϕ denotes the empty set. (We note that if two predicates Y_1 and Y_2 are equivalent then they are K-equivalent for any set K. We write $Y_1 \simeq Y_2$.

(2.12) It is known that the relation of equivalence may be regarded as an "equality" on the set of predicates of L in so far as it is substitutive with respect to the propositional connectives and quantifiers of L (regarded as operators).

In fact let X be a predicate which contains the predicate R of order $n \geq 0$ at least once. Let us indicate the dependence of X on R by writing X = X(R). We shall denote by X(Y) the result of substituting in X for R the predicate Y of order n; and the following "rule of replacement" is valid in L:

If Y_1 and Y_2 are equivalent predicates of order n then for any predicate X = X(R) in L where R is a predicate of order n (as above) we have $X(Y_1) \simeq X(Y_2)$.

We note that if R occurs more than once in X then the replacement of R by Y and Y need not take place everywhere provided only that it is carried out at the same places of X for both Y and Y .

(2.13) By a <u>syntactical transform</u> T we shall understand a correspondence which associates with each element X of a certain class of predicates another predicate $X' = T(X)$ by a definite or effective formal rule.

We define a syntactical transform N on the set of all predicates of L, inductively, as follows:

$N(X) = \sim X$ if X is atomic

$N(\sim X) = X$

$N(X \vee Y) = N(X) \wedge (Y)$; $N(X \wedge Y) = N(X) \vee N(Y)$.

$N\left([(Ez)X]\right) = (z)N(X)$

$N\left([(z)X]\right) = (Ez)N(X)$

Thus $N(X)$ is the predicate obtained from X (where X contains only the connectives $\vee, \wedge, \sim$) by interchanging the connectives $\vee$ and $\wedge$, then interchanging universal and existential quantifiers, and finally replacing all atomic formulae in X by their negations. We shall call $N(X)$ the negation of X. In fact, the following result is well known:

(2.14) For every predicate X we have $N(X) \simeq [\sim X]$

A predicate X in L is said to be in prenex normal form if it is of the form $X = (q_1)\ldots(q_n)[Z]$ where $n \geq 0$, the q_j are quantifiers with respect to different variables, Z is a predicate that is free of quantifiers, and the scope of each quantifier is the entire part of the formula which follows it. Thus, the sentence $(Ey)\ (x)[F(x) \vee Q(y)]$ is in prenex normal form, while the sentence $(Ey)\ [(x)F(x)] \vee Q(y)]$ is not.

The quantifiers q_j, $j = 1,2,\ldots n$ are said to form the prefix of X while the formula Z is called the matrix of X.

We note that every predicate that is free of quantifiers is in prenex normal form.

With every predicate X (which contains only the connectives $\vee, \wedge, \sim$) we associate a predicate P(X) in prenex normal form by the syntactical transform P defined inductively as follows:

(2.15) (1) $P(X) = X$ if X is free of quantifiers; Otherwise,

(2) $P(\sim X) = P(N(X))$

(3) $P\left([X * (q_z)Y]\right) = P\left([(q_z)\ [X * Y]]\right)$

$P\left([(q_z)Y * X]\right) = P\left([(q_z)\ [Y * X]]\right)$

where (q_z) denotes either an existential or universal quantifier with variable z that does not appear in X; Y is a predicate of

order one with free variable z, and the symbol $*$ denotes either the connective $\vee$ or the connective $\wedge$ (it being understood that the same connective appears on both sides of the identity).

(4) $P\left(\left[\left(q_z\right) Y\right]\right) = \left(q_z\right) P(Y)$ where $\left(q_z\right)$ and Y are defined as in (3)

Moreover, it is well known that

(2.16) For every predicate X we have

(1) $P(X) \simeq X$.

(2) P(X) contains only extralogical symbols that appear already in X.

We shall now classify all predicates X which are in prenex normal form in a natural way according to the number of blocks of quantifiers of the same type which appear in the prefix.

(2.17) A predicate X in prenex normal form is called <u>existential</u> (<u>universal</u>) if it contains no universal (existential) quantifiers.

A predicate X is said to belong to <u>Class 0</u> if it is free of quantifiers.

We note that a predicate of Class 0 is both universal and existential.

We now define inductively:

A predicate X in prenex normal form is said to be of <u>class n</u> ($n \geq 1$) if X is of class n-1 or if, in reading the prefix of X from one end to the other, exactly n-1 changes from universal to existential or existential to universal quantifier occur.

(2.18) We have:-

(a) Class $\mathfrak{n}$ is contained in class $\mathfrak{m}$ for all $n \leq m$.

(b) Class $\mathfrak{1}$ consists precisely of the existential and universal predicates of L.

Thus for example the sentence.

$X = (Ex)(y)\ (z)\ (Ew)\ Q\ (x,y,z,w)$ belongs to all classes $\mathfrak{n}\geq 3$

while the sentence

$Y = (x)\ (Ey)\ (z)\ (Ew)\ Q\ (x,y,z,w)$ belongs to all classes $\mathfrak{n}\geq 4$

and the sentence

$Z = (\pi)\ (y)\ (Ez)\ (Ew)\ Q\ (x,y,z,w)$ belongs to all classes $n \geq 2$.

Given the one-place relation R we define a syntactical transform $X \to X_R$ on the set S of sentences of L inductively as follows:

(2.19) $X_R = X$ if X is atomic

$(\sim X)_R = \sim X_R$

$(X \vee Y)_R = X_R \vee Y_R$

$[(y)\ Z\ (y)]_R = (y)\ [R(y) \supset [Z(y)]_R]$

$(Ey)\ Z\ (y) = (Ey)\ [R(y) \wedge [Z(y)]_R]$

X_R is called the relativised transform of X with respect to R and is said to be obtained from X by relativisation with respect to R.

For example if

$X = (Ew)\ (x)\ [(Ey)\ F\ (x,y,w) \supset (z)\ G\ (y,z,a)]$ then

$X = (Ew)[R(w) \wedge (x)[R(x) \supset [(Ey)\ [R(y) \wedge F\ (x,y,w)]] \supset [(z)\ [R(z) \supset G(y,z,a)]]]$.

We note that the property of " provability" is not invariant under relativization. Indeed the sentence

$X = (Ex)\ (Ey)\ [Q(x,y) \vee \sim Q(x,y)]$ is a theorem while

$X_R = (Ex)\ [R(x) \wedge (Ey)\ [R(y) \wedge [Q\ (x,y,) \vee \sim Q(x,y)]]]$ is not.

However we do have the following result;

(2.20) If the sentence X does not include any constants then X_R is a theorem only if the sentence $E(x)\ R(x) \supset X_R$ is a theorem. If X does include a number of individual constants $a_1, \ldots a_u$ $(n \geq 1)$ then X is a theorem only if the sentence $[R(a_1) \wedge \ldots \wedge R(a_u)] \supset X_R$ is a theorem.

Proof (2.20) is easily seen to hold for all axioms X of L and is in fact, preserved under all rules of inference. It follows that:

(2.21) If a sentence X is defined in a set of sentences K and if X is deducible from K then X_R is defined in the set K_R and X_R is deducible from K_R where K_R is given by $K_R = \{Y_R \mid Y \in K\} \cup \{R(a) \mid$ a is an individual constant which occurs in $K\}$, if K includes some individual constant. Otherwise, $K_R = \{Y_R \mid Y \in K\} \cup \{[(Ex)\ R(x)]\}$.

Let K be a non-empty set of sentences in prenex normal form. We shall introduce a set of functors of order $n \geq 0$ which are not contained in K by the following procedure:

(2.22) For any sentence $X = (q_1) \ldots (q_u)\, Z(x_1, \ldots x_u)$ in K, let q_i be an existential quantifier in X, $(q_i) = (E x_i)$ where $1 \leq i \leq u$. Let m be the number of universal quantifiers which precede q_i (reading from left to right) in the prefix of X, $0 \leq m \leq i-1$. We then introduce a functor φ_i of m places called the Herbrand functor associated with q_i subject to the conditions that

(1) different functors correspond to different integers i for which q_i is an existential quantifier in the particular sentence X under consideration.

(2) Different functors correspond to different X in K.

Given the set $\bar{\varphi}$ of Herbrand functors assiciated with the set K; in particular, given the set $\{\varphi_i\}$ of Herbrand functors associated with an arbitrary sentence X in K we define a syntactical transform H on the set of sentences K (the sentence X) as follows:

(2.23) (1) $H(X) = X$, if X is universal (see 2.17) Otherwise

(2) Let $X = (q_1) \ldots (q_u)\, Z(x_1, \ldots x_u)$ then

$H(X) = (q_{j_1}) \ldots (q_{j_\ell})\, Z(x_1', \ldots x_u')$

where $q_{j_1}, \ldots q_{j_\ell}$ denote the universal quantifiers of X in the order in which they appear in the prefix of X, $\ell < u$ and the symbols x_j' are given by:

$x_j' = x_j$ if q_j is a universal quantifier in X; otherwise

$x_j' = \varphi_j(x_{j_1}, \ldots x_{j_\ell})$ where φ_j is the Herbrand functor associated with q_j and $x_{j_1}, \ldots, x_{j_\ell}$ are the variables in universal quantifiers which precede q_j in the prefix of X.

H (X) is called the Herbrand transform of X with respect to the set $\{\varphi_i\}$

Thus if $X = (Ey_1)(x_1)(Ey_2)(x_2)(Ey_3)(Ey_4)\, Z(x_1, x_2, y_1, y_2, y_3, y_4)$

Then $H(X) = (x_1)(x_2)\left[Z(x_1, x_2, \varphi_1, \varphi_2(x_1), \varphi_3(x_1, x_2), \varphi_4(x_1, x_2))\right]$

We note that φ_1 is a functor of o places, that is, an individual constant.

The set of sentences $\{H(X) \mid X \in K\}$ will be denoted by K_H. We now prove:

(2.24) If the set K of sentences in prenex normal form is consistent then so is K_H.

Proof: Suppose that K_H is contradictory.

Then there exist sentences $Y_1, \ldots Y_r$ in K such that the sentence $[Y_1 \wedge \ldots \wedge Y_r] \supset W$ is provable where $W = W' \wedge \sim W'$ is chosen so that W' does not contain any functors (constants) which appear in $Y_1, \ldots Y_r$.

It follows by the deductive theory of the propositional calculus that the sentence $Y_\mu \supset Q_\mu$ is provable for every integer $\mu = 1, 2, \ldots$ where Q_μ is defined by the identity $Q_\mu = [Y_1 \wedge \ldots \wedge Y_{\mu-1} \wedge Y_{\mu+1} \wedge \ldots \wedge Y_r] \supset W$.

Let X_μ be the sentence of K which corresponds to Y_μ $\mu = 1, 2, \ldots$

We shall show that the sentence $X_\mu \supset Q_\mu$ is likewise provable.

Let $m = n - \ell$ be the number of existential quantifiers which appear in X_μ (where n is the total number of quantifiers). If $m = 0$ then $X_\mu = Y_\mu$ and there is nothing to prove.

If $m \geq 1$ then $X = \ldots\ldots (q_{k_1}) \ldots (q_{k_m}) \ldots Z(x_1, \ldots x_n)$

where we have indicated only the existential quantifiers q_{k_j} which appear in X $j = 1, 2, \ldots m$.

We now define the sentences $Q_0, \ldots Q_m$ inductively as follows:

$Q_0 = Y_\mu = (q_{j_1}) \ldots (q_{j_\ell})\ Z$.

To define Q_1 we replace the term $\varphi_{k_m}(\ldots\ldots)$ in the matrix Z of Q by the variable x_{k_m} and we insert the quantifier $(Ex_{k_m}) = (q_{k_m})$ among the quantifiers $q_{j_1}, \ldots q_{j_\ell}$ in the order in which these quantifiers appear in the prefix of X.

We note that φ_{k_m} is the Herbrand functor of $\mathfrak{M}_\mu$ which corresponds to the quantifier (q_{k_m}) in X_μ. In general we obtain Q_ρ from $Q_{\rho-1}$ $\rho = 1, 2, \ldots m$ by replacing the term $\varphi_{k_t}(\ldots\ldots)$ $t = m - \rho + 1$ of $Q_{\rho-1}$ by the variable x_{k_t} and inserting among the quantifiers of $Q_{\rho-1}$ the existential quantifier (Ex_{k_t}) according to the order in which these quantifiers appear in X. Thus if

$Q_{\rho-1} = (x_{j_1}) \ldots (x_{j_s})\ Z^{\rho-1}(x_{j_1}, \ldots x_{j_s}, \varphi_{k_t}(x_{j_1}, \ldots x_{j_s}))$

where $(x_{j_1})\ldots(x_{j_s})$ are the universal quantifiers which precede (Ex_{k_t}) in X_μ then

$Q_\rho = (x_{j_1})\ldots(x_{j_s})\,(Ex_{k_t})\; Z^{\rho-1}\,(x_{j_1},\ldots x_{j_s}\,,\, x_{k_t})$

It is easily seen that $Q_{1\mu} = X_\mu$. Hence in order to show that $[X_\mu \supset Q_\mu]$ is a theorem of L is suffices to show that the provability of $[Q_{\rho-1} \supset Q_\mu]$ entails that of $[Q_\rho \supset Q_\mu]$ (since $[Q_0 \supset Q_\mu]$ is provable by assumption). This in turn, follows directly by a simple application of the rule of deduction (2.5)- (g) since, by the assumption of (2.22), the sentence Q_μ does not contain the functor φ_{k_t}.

Thus $[X_\mu \supset Q_\mu]$ is provable for each $\mu = 1, 2, \ldots r$

Transforming, by the rules of the propositional calculus, it follows that the set $\{Y_1, Y_2, \ldots Y_{\mu-1}, X_\mu, Y_{\mu+1}, \ldots Y_r\}$ obtained by replacing Y_μ by X_μ in the set $\{Y_1, \ldots Y_r\}$ is contradictory, and again, since μ is arbitrary, a repeated application of the above argument for $\mu = 1, 2, \ldots r$ enables us to establish that the set $\{X_1, \ldots X_r\}$ is contradictory. This, in accordance with (2.7), contradicts the consistency of K. Hence K_H is consistent.

In concluding this chapter we introduce the following definitions:

(2.25) A set K of sentences is said to be <u>disjunctive</u> if for any sentences X, Y in K we also have $X \vee Y$ in K. K is <u>quasi-disjunctive</u> if for any sentences X, Y in K there exists a sentence Z in K such that $Z \simeq [X \vee Y]$. Conjunctive and quasi-conjunctive sets are defined similarly.

With each non-empty set K of formulae (sentences) in L we associate a set ψ_K of constants called the <u>set of constants associated with K</u> inductively as follows:

(2.26) (1) $a \in \psi_K$ for any constant a which appears in (some of the) formulae of K.

(2) If $a_1, \ldots a_u \in \psi_K (n > 0)$ and ζ is a functor of n places

which appears in K then $\sigma(a_1, \ldots a_u) \in \Psi_K$

We note that Ψ_K may be empty. In fact Ψ_K is empty when and only when the set I_K of individual constants that appear in K is empty. If we include in I_K (in the event that I_K is empty) an arbitrary but fixed individual constant c of L we thus ensure that the resulting set Ψ_K^c of constants associated with K is non-empty.

Thus if we define: $\bar{\Psi}_K = \Psi_K$ if I_K is non-empty

$\bar{\Psi}_K = \Psi_K^c$ if I_K is empty,

we may (and shall) assume that the set of constants associated with a given set K is always non-empty.

Chapter 3: Semantic theory of the language L

In this chapter we shall be concerned with the semantic theory of the language L. Our aim is to establish the important result, via the extended completeness theorem of the lower predicate calculus, that a set K of sentences in L can be "interpreted" or "realized" in a mathematical system if and only if K is consistent.

We have assumed that our formal language L is sufficiently comprehensive so that, for any given mathematical system M (see 0.1) we can correlate the constants, functions (operations), and relations of M in one-one correspondence with some of the constants, functors, and relation symbols of L. In view of this correspondence, we may (and shall), for simplicity's sake, identify these constants, functors, and relation symbols of L with their images in M. (We shall however continue to employ the terms "functor" and "relation symbol" when referring explicity to extralogical symbols of L.) It is thus assumed (when no ambiguity results) that the constants, functions, and relations of a system M actually occur in L and denote themselves; so that the expressions $R(a_1, \ldots a_n)$ where $R(x_1, \ldots x_n) \in M$ and $a_1, \ldots a_n \in M$ are regarded as atomic sentences of L.

(3.0) A formula X in L is said to be <u>defined in a system M</u> if all the extralogical symbols that appear in X belong to M.

(3.1) For any sentence X which is defined in a system M, we define the <u>satisfiability</u> of X by M, inductively as follows:

(1) An atomic sentence $X = R(a_1, \ldots a_n)$ is satisfied by M precisely when it holds in M.

(2) A sentence of the form $X = \sim X'$ is satisfied by M if and only if X' is not satisfied by M.

(3) A sentence of the form $X = X_1 \vee X_2$ is satisfied by M if and only if either X_1 or X_2 (or both) is (are) satisfied by M.

(4) A sentence of the form X =(y) F (y) where F is a unary predicate is satisfied by M if and only if the sentence F(a) is satisfied by M for <u>all</u> constants $a \in M$.

(5) A sentence of the form $X = (Ey)\ F(y)$ where F is a unary predicate is satisfied by M if and only if the sentence F(a) is satisfied by M for some constant $a \in M$.

(3.2) Let K be a set of sentences in L. A system M is said to be a model of K if every sentence X in K is satisfied by M. We note that any system M' isomorphic to M is a gain a model of K.

In general a model M of a set K may include n-ary functions and relations ($n \geq 1$) which do not occur as extralogical symbols in K, but if we delete these from the system M the modified system M' is again a model of K. Hence we may (and shall) assume, for the sake of simplicity, that a model M of K contains only n-ary functions and relations($n \geq 1$) which appear in K. For emphasis, we shall occasionally refer to such a model as a K-model.

(3.3) A sentence X is said to be universally valid if it is satisfied by all systems M in which it is defined, that is if any system M in which X is defined is a model of X.

It is easily seen that all "axioms" (primitive theorems) of L are universally valid. Now if a sentence X in which the k-ary functor φ occurs ($k \geq o$), is provable in L, it is easily seen that the sentence X' obtained by replacing φ by any other k-ary functor ψ (at all occurrences of φ in X) is likewise provable in L. It follows then (see Robinson [2] p.p. 61-62) that the property of universal validity is preserved by the rules of inference (2.5)-(e), (f),(g) of L. Thus we have:

(3.4) Every theorem of L is universally valid. As a corollary it follows that:

(3.5) Two sentences X and Y are equivalent ($X \simeq Y$) only if any system M in which both X and Y are defined either satisfies both X and Y or satisfies neither X nor Y.

It is easily seen that no contradictory set K of sentences can possess a model, in other words:

(3.6) If K possesses a model, then K is consistent. We now prove:

(3.7) Every non-empty and consistent set K of sentences in L which is free of quantifiers possesses a model.

Proof: The sentences of K are all obtained by applying connectives to atomic sentences. Let S_K be the set of atomic sentences which appear in the sentences of K. With every $X \in S_K$ we associate a propositional variable p_X of the propositional calculus C such that different p_X correspond to different $X \in S_K$. For every $Y \in K$ we define a formula $\xi(Y)$ of C, inductively, as follows:

(1) $\xi(Y) = p_Y$, if Y is atomic.

(2) $\xi(Y \vee Z) = \xi(Y) \vee \xi(Z)$; $\xi(\sim Y) = \sim \xi(Y)$

Let $K' = \{ \xi(Y) \mid Y \in K \}$. By (2.5) - (a), if K' is contradictory then so is K so that our assumption implies that K is consistent. it follows by (1.9) that there exists an admissible valuation W for the propositional variables tnat occur in K'.

Let A_K be the set of all constants associated with K (see 2.26) and let ϕ_K be the set of all functors of order $n \geq 0$ tnat occur in K. (We note that K includes some constants since it is non-empty and free of quantifiers by assumption). Clearly A_K is closed with respect to ϕ_K. Let R_K be the set of relation symbols that appear in the sentences of K. Then R_K is non-empty. We shall show that $M_K = (A_K , \phi_K , R_K)$ is a K-model.

Let R be an m-ary relation of R_K ($m \geq 1$) and let $a_1 , \ldots a_m \in A_K$. If the atomic sentence $R(a_1 , \ldots a_m)$ belongs to S_K then we define that $R(a_1 , \ldots a_m)$ holds or does not hold in M_K according as the corresponding propositional variable $\xi([R(a_1 , \ldots a_m)])$ obtains the truth value 1 or 0 under W. If $R(a_1 , \ldots a_m)$ does not belong to S_K then we define arbitrarily that it holds in M_K. It follows readily that M_K is a mathematical system in which the set K (every sentence of K) is defined and which contains only functions and relations of $n \geq 1$ places which appear in K. Also every sentence Y in K is satisfied in M_K since W is an admissible valuation of K'. Hence M_K is a K-model, as required.

It follows that:

(3.8) Every non-empty and consistent set G of universal sentences (see 2.17) in L possesses a model.

Proof: Given the set G of universal sentences in L, let A_G be the set of all constants associated with G. We define a set G' of sentences in L which are free of quantifiers as follows:

(1) $Y \in G'$ for any sentence $Y \in G$ which is free of quantifiers.

(2) If $Y = (x_1)\ldots(x_u)\, Z(x_1, \ldots x_u)$ where "Z" is any sentence in G then we include in G' all different sentences of the form $Y' = Z(a_1 \ldots a_u)$ where $a_1, \ldots a_u \in A_G$.

For each sentence $Y \in G$ and for each sentence Y' associated with Y by (2) the sentence $Y \supset Y'$ is provable by (2.5) —(c). It follows, by the rules of deduction of the propositional calculus, that a sentence of the form $[Y_1' \wedge \ldots \wedge Y_r'] \supset W$ where $Y_i' \in G'$ $i = 1, 2, \ldots r$ and W is arbitrary, is provable only if the sentence $[Y_1 \wedge \ldots \wedge Y_r] \supset W$ is provable where $Y_i \in G$. Thus G' is consistent since G is consistent by assumption. By (3.7) G' possesses a model $M = (A_{G'}, \phi_{G'}, R_{G'})$. It is easily seen that M, by definition of G', is a model of G as required.

We are now in a position to prove the extended completeness theorem of the lower predicate calculus (the language L):

(3.9) Theorem: There exists a model M for every non-empty and consistent set K of sentences in L.

Proof: By (2.16) and (3.5) we may assume, without loss of generality, that the sentences of K are in prenex normal form. Let $\overline{\varphi}$ be a set of Herbrand functors (see 2.22) associated with the existential quantifiers that occur in K. Let K_H be the set of all Herbrand transforms (see 2.23) of the sentences of K with respect to $\overline{\varphi}$. Then K_H is consistent by (2.24). Also the sentences of K_H are all universal (by definition of K_H) so that, in view of (3.8) it suffices to show that every model of K_H is a model of K.

Let X be any sentence of K. Then X may be obtained from a sentence $Y \in K_H$ by the chain of sentences $Q_0 = Y, Q_1 \ldots, Q_m = X$ as described in the proof of (2.24). Suppose that the sentence Q_{p-1} $1 \leq p \leq m$ is satisfied by a system M. It follows immediately from the definition of Q_p that Q_p is likewise defined in and satisfied by M. It follows by induction, that the sentence $X = Q_m$, is satisfied by every model M of $Y = Q_0$. This completes the proof of (3.9).

The following results may be regarded as corollaries to (3.9). We first prove the converse of (3.4)-the so-called "Godel's completeness theorem".

(3.10) Every universally valid sentence is provable in L.

Proof: Suppose that the universally valid sentence X is not provable in L. It follows by (1.7) that the set $S = \{\sim X\}$ is consistent, so that by (3.9) there exists a system M which does not satisfy X although X is defined in M (as $\sim X$ is defined in M). This contradicts the universal validity of X.

The converse of (3.5) now follows readily:

(3.11) If X and Y are two sentences which are simultaneously satisfied or not satisfied in every system M in which both X and Y are defined, then $X \simeq Y$.

We may generalize (3.4), (3.5), (3.10), and (3.11) in the following results:

(3.12) Let K be a consistent set (possibly empty) of sentences in L. Then any sentence X which is deducible from K is satisfied by all models of K in which it is defined. Conversely any sentence Y which is satisfied by every model of K in which it is defined is deducible from K. Thus, the sentences of L which are satisfied by all models of K in which they are defined are precisely the sentences that can be deduced from K.

Chapter 4 Formalized Algebraic Theories

In this chapter we shall show that certain algebraic criteria and various algebraic systems can be formalized or axiomatized within the language L. This will enable us to apply the semantic theory of L to certain results in the metamathematics of algebra and consequently to certain results in algebra as well.

(4.0) Let K be a consistent and non-empty set of sentences in L. A binary relation symbol **I** is called a relation of equality (with respect to K) if:

(a) The sentences-

(i) $(x)[I(x,x)]$

(ii) $(x)(y)[I(x,y) \supset I(y,x)]$

(iii) $(x)(y)(z)[[I(x,y) \wedge I(y,z)] \supset I(x,z)]$

are deducible from K.

(b) For every functor of n places ($n \geq o$) which appears in K the sentence-

(iv) $(x_1)..(x_n)(y_1)..(y_n)[[I(x_1,y_1) \wedge .. I(x_n,y_n)] \supset I(\alpha(x_1,..x_n),\alpha(y_1,..y_n))]$

is deducible from K.

(c) For every relation symbol R of n places ($n \geq 1$) which appears in K the sentence-

(v) $(x_1)..(x_n)(y_1)..(y_n)[[I(x_1,y_1) \wedge .. I(x_n,y_n)] \supset [R(x_1,..x_n) \equiv R(y_1,..y_n)]]$

is deducible from K.

(4.1) A consistent and non-empty set K of sentences (where, for syntactical simplicity, it is assumed that the sentences are in prenex normal form) is called an L-theory if a relation of equality appears in K. The sentences that belong to an L-theory are called its axioms. It is clear by (3.12) that a set K is an L-theory if and only if every model of K is an algebraic system.

We note that the relation $\equiv$ of an algebraic system M is unique; that is any binary relation of M satisfying the postulates(1)-(5)of (0.4) must coincide with $\equiv$. Likewise, it is easy to show that any two relations of equality with respect to a given set K are K-equivalent. We may (and shall) therefore assume that only one relation of equality appears in a given L-theory K. In conformity with (0.4) we shall denote it by $\equiv$ so that the expression $t_1 \equiv t_2$ where t t are any terms of L denotes an atomic formula of L.

We shall now exhibit a series of L-theories which are associated with certain "concrete" algebraic systems. In subsequent chapters of this paper we shall be concerned with the deductive properties of such theories as well as certain properties of consistency and completeness. It can be shown that such properties are (in a sense which is made precise in Robinson [2]p.p. 72-74; Robinson [3] p.p. 28-31)independent of the particular formalization of the concept under consideration, that is, of the particular form of the symbols that appear in the theories. Thus it is our intention to merely point out the existence of such theories, the particular form or structure of the axioms being irrelevant to our purposes.

Let G_A be an L-theory which, in addition to (4.0)--(i),(ii),(iii), includes the axioms:

(4.2) (i) $(x)(y)(z)(u)\left[\left[(x \equiv z) \wedge (y \equiv u)\right] \supset \left[G(x,y) \equiv G(z,u)\right]\right]$

(ii) $(x)\left[G(x,o) \equiv x\right]$

(iii) $(x)\,(Ey)\left[G(x,y) \equiv o\right]$

(iv) $(x)(y)(z)\left[G\left(x, G(y,z)\right) \equiv G\left(G(x,y), z\right)\right]$

(v) $(x)\,(y)\left[G(x,y) \equiv G(y,x)\right]$

The term $G(x,y)$ is called the sum of x and y while the individual constant o is the neutral element with respect to G. It is clear that G is an L-theory for the concept of an (additive) abelian group; that is, the class of all models of G_A coincides with the class of all abelion groups. We say that the concept of an abelian group is elementarily defined in L by the set G_A.

We now define terms $G_n(x)$, n=o,1,... by the following recursion scheme:

(4.3) (i) $G_o(x) = o$

(ii) $G_{n+1}(x) = G(G_n(x),x)$

Then $G_n(x)$ is the term "nx" in ordinary algebraic notation. Thus the sentence $(x)(Ey)\,[x = G_n(y)]$ is satisfied by a system M if and only if for all $a \in M$ there exists a constant $b \in M$ such that $nb = a$ $(n \geq o)$

Let N be defined by the following (infinite) set of axioms:

(4.4) (i) $(Ex\ (Ey) \sim[x = y]$

(ii) $(x)\ (Ey)\ [x = G_n(y)]$; n=0,1,...

(iii) $(x)(y)[[y = G_n(x)] \wedge \sim[x = o]] \supset \sim[y = o]$; n = 0,1,...

Then $G_A' = G_A \cup N$ is an L-theory for the concept of a completely divisible (axiom (ii)) torsion-free (axiom (iii)) abelian group which contains at least two different elements. We note that axiom (iii) asserts in ordinary algebraic notation, that $nx \neq o$ for all $x \neq o$ that is every non zero element has infinite order.

Let S_o consist of the axioms:

(4.5) (i) $(Ex)\ [x = x]$

(ii) $(x)(y)(z)(w)\ [[Q(x,y)] \wedge [x = z] \wedge [y = w]] \supset Q(z,w)$

(iii) $(x)(y)(z)\ [Q(x,y) \wedge Q(y,z)] \supset Q(x,z)$

(iv) $(x)\ (y)\ [x = y \vee Q(x,y) \vee Q(y,x)]$

(v) $(x)(y)\ [Q(x,y) \supset \sim[x = y]]$

together with axioms (i), (ii), (iii) of (4.0). It is clear that S_o is an L-theory for the concept of a (totally) ordered set where

$Q(x,y)$ denotes, in ordinary algebraic notation, the ordering relation "$x<y$".

(4.6) Let us define the axioms Y and Z by the identities:

$Y = (x)\,(Ey)\,Q(x,y)$; $Z = (x)(y)(z)\,\left[Q(x,y) \supset Q\big(C(x,z), C(y,z)\big)\right]$

then we have:

(a) $S_0' = S_0 \cup \{Y\}$ is an L-theory for the concept of an (infinite) ordered set which contains no last element.

(b) $G_0 = G_A \cup S_0 \cup \{Z\}$ is an L-theory for the concept of an ordered abelian group.

Again if we adjoin to S_0 the axioms:

(4.7) (i) $(Ex)\,(Ey) \sim [x = y]$

(ii) $(x)\,(y)\,(Ez)\,\left[Q(x,y) \supset [Q(x,z) \wedge Q(z,y)]\right]$

then we obtain the L-theory S_0'' for the concept of an (infinite) densely ordered set.

Let us now define a sequence $\{X_n\}$ $n = 1,2,\ldots$ of axioms by the identity:

$X_n = (Ex_1)\ldots(Ex_n)\,\left[Q(x_1,x_2) \wedge \ldots \wedge Q(x_{n-1}, x_n)\right]$

It is clear that $S_0^* = S_0 \cup \{X_n\}$ $n = 1,2,\ldots$ is an L-theory for the concept of an infinite ordered set.

(4.8) We leave it to the reader to verify that the concept of a commutative ring with distinct unity and zero elements is elementarily defined in L by an L-theory R_C containing the functors C and $\overline{\alpha}$ (where the term $\overline{\alpha}(x,y)$ denotes the product of x and y) and the individual constants o and 1 (where 1 now denotes the neutral element with respect to $\overline{\alpha}$). It follows readily that there exist L-theories J and K_F which are defined in R_C and such that the concepts of an integral domain and (commutative) field are elementarily defined in L by the sets J and K_F respectively.

We now define terms $\overline{\alpha}_n(x)$ $n = o,1,\ldots$ by the recursion scheme:

(i) $\Pi_0(x) = 1$

(ii) $\Pi_{n+1}(x) = \Pi(\Pi_n(x), x)$

Then $\Pi_n(x)$ is the term "x^n" in ordinary algebraic notation.

(4.9) It is now easily seen that for every non-negative integer n the equation $x_n y^n + x_{n-1} y^{n-1} + \dots + x_1 y = x_0$ written in ordinary algebraic notation (regarding the coefficients x_i as variables) can be formalized in L as an (atomic) predicate $R_n(x_0, x_1, \dots x_n, y)$ of the variables $x_0, x_1, \dots x_n, y$ which is defined in R_c.

Thus, for n=2 we have:

$R(x_0, x_1, x_2, y) = \left[C\left(\Pi\left(x_2, \Pi_2(y)\right); \Pi\left(x_1, \Pi_1(y)\right)\right)\right] \neq x_0$

(4.10) In order to obtain an L-theory K_F^* for the concept of an algebraically closed field it suffices to adjoin to K_F the infinite sequence $\{X_n\}$ of axioms n = 2,3,... defined by:

$X = (x_0)(x_1)\dots(x_n)(Ey)\left[\left[x_n \neq 0\right] \vee \left[R_n(x_0 x_1, \dots x_n, y)\right]\right]$

We now define an infinite sequence $\{Y_n\}$ of axioms n = 1,2,... by the identity:

$Y = (x)(y)\left[G_{p_n}(x) \neq y\right] \supset \left[y \neq 0\right]$

where p_n denotes the n^{th} prime number in order of magnitude; that is, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ etc.

(4.11) It is clear that $Kp_n = K_F \cup Y_n$ is an L-theory for the concept of a field of characteristic p_n ($n \geq 1$) while the infinite set $Kp_0 = K_F \cup \{\sim Y_n\}$ n = 1,2,... is an L-theory for the concept of a field of characteristic zero. Hence the concept of a field of specified characteristic $p \geq 0$ can be formalized in L.

By way of example illustrating the importance of (3.12) we now prove:

Theorem: Let X be a sentence which is defined in the set K_F of axioms for the concept of a field and which is satisfied by all fields of characteristic zero. Then there exists an integer q such that X is satisfied by all fields of characteristic $p \geq q$.

Proof: Let Kp_o be defined by (4.11). Then X is defined in Kp_o and hence, by our assumption, is satisfied by all models of Kp_c. It follows by (3.12) that X can be deduced from the set $Kp_o = K_F \cup \{\sim Y_n\}$ $n = 1,2,\ldots$ Hence there must exist a finite subset $H = \{\sim Y_1, \sim Y_3, \ldots Y_q\}$ such that X is deducible from the set $K_F \cup H$.

New the set $K_f \cup H$ is satisfied by all fields of characteristic $p \geq q$. It follows, by (3.12) again, that X is likewise satisfied by all such fields.

(4.12) Let Z be defined by (4.6) and let Z' be given by:

$$Z = (x)(y)(z)\left[\left[Q(x,y) \wedge Q(o,z)\right] \supset Q\left(\pi(z,x), \pi(z,y)\right)\right]$$

It is then clear that if we adjoin to R_c or K_F the axioms of S_o together with the axioms Z and Z' then we obtain an L-theory R_o or K_o for the concept of an ordered ring or ordered field respectively.

(4.13) By a real closed field we shall understand an ordered field in which every non-negative element has a square root and every polynomial of odd degree has at least one root. It is then clear that if Y is defined by the identity;

$$Y = (y)\,(Ez)\left[\sim Q(y,o)\right] \supset \left[\pi(z,z) = y\right]$$

then $K_F \cup Y \cup \{X_3, X_5 \ldots X_{2n+1} \ldots\}$ where X_j is defined by (4.10) is an L-theory for the concept of a real closed field.

Chapter 5 Completeness and Model-Completeness

In this chapter we shall introduce the concepts of completeness and model-completeness and establish some of their properties. Whenever we deal with a set K of sentences in L we shall, in order to avoid trivial cases, assume that K is non- empty and consistent.

(5.0) A sentence X is said to be decidable in a set K of sentences if either X or $\sim X$ is deducible from K. (We observe that this notion does not entail the existence of a concrete decision procedure). By (3.12) we obtain an equivalent semantical characterization of the notion of decidability namely:

(5.1) A sentence X is decidable in a set K if and only if either X is satisfied by all models of K in which it is defined or it is satisfied by none.

(5.2) A set K is said to be complete if every sentence which is defined in K (see 2.8) is also decidable in K. In view of (2.16) we may say, without loss of generality, that a set K is complete if and only if every sentence in prenex normal form which is defined in K is also decidable in K. We may therefore introduce a modified notion of completeness called "n-completeness" as follows.

(5.3) A set K is said to be n-complete ($n \geq o$) if every sentence of class n (see 2.18) which is defined in K is also decidable in K. We note by the above remark, that a set K is complete if and only if it is n-complete for every $n \geq o$. It follows from (2.14) that:

(5.4) A set K is 1-complete if and only if every existential (universal) sentence which is defined in K is also decidable in K.

(5.5) Let M be a given (mathematical) system. Let D(M) be the set of all atomic sentences of the form $R(a_1, \ldots a_n)$ $n \geq 1$ which are defined in M (that is $R \in M$ and $a_1 \ldots a_n \in M$) and which hold in M together with the set of all sentences of the form $\sim R(a_1, \ldots a_n)$ where $R(a_1, \ldots a_n)$ is an atomic sentence which is defined in M but which does not hold in M. D(M) is called the diagram of M. Thus if M is a model of K (see 4.12),

then the sentences $\sim[1 \equiv 0]$ and $Q(\pi(1,0,), \sigma(0,1)$ are included in D(M).

The following results follow readily from (0.1) and (5.5).

(5.6) Let M_1 and M_2 be two systems, Then M_2 is a (proper) extension of M_1 if and only if $D(M_1)$ is a (proper) subset of $D(M_2)$. In symbols, $M_1 \subseteq M_2$ if and only if $D(M_1) \subseteq D(M_2)$.

(5.7) Every model of D(M) is an extension of M and conversely, every extension of M is a model of D(M); that is, the models of D(M) are precisely the extensions of M. More generally, for any consistent set K, the models of $K \cup D(M)$ are precisely the models of K which are extensions of M.

We note that an extension M* of a given model M of a fixed set K need not be a model of K. Indeed the ordered field M of real numbers is a model of K_0 (above) and if we let M* be the field of complex numbers we may define a relation $a+bi \leq c+di$ in M* which holds in M* if and only if $a+b \leq c+d$ holds in M. Then M* is an extension of M in the sense of (0.1), but clearly, M* is not a model of K_0.

(5.8) A (non-empty and consistent) set K of sentences is said to be <u>model-complete</u> if the set $K \cup D(M)$ is complete for every model M of K. It follows from (5.7) and (5.1) that:

(5.9) A set K is model-complete if and only if, for every sentence X which is defined in any given model M of K, if X is satisfied by M, then X is satisfied by all extensions of M which are models of K.

By way of example let S_0 be an L-theory for the concept of an infinite ordered set (see 4.5). It can be shown by a direct application of (5.4) that S_0 is 1-complete. (Since the proof is somewhat detailed and since this result is not essential for our purposes we refer the interested reader to Robinson [4]). It is easily seen however that the sentence $Z = (Ex)(y)[x \equiv y \vee Q(x,y)]$ (which asserts, in ordinary mathematical terminology that

there exists a first element for the set) is not decidable in S_o. Indeed Z is satisfied by the ordered set of positive integers but is not satisfied, by the ordered set of integers. Thus, by (5.1) S is not 2-complete and hence by (5.3), is certainly not complete.

Again, the ordered set M of positive integers and the ordered set M* of non-negative integers are both models of S_o, M* being an extension of M. Yet the sentence $Z = (x)\,[(x \neq 1) \vee Q(1, x)]$ is satisfied by M but not by M*; so that by (5.9), S_o is not model-complete.

It is to be noted that the concepts of completeness and model-completeness are not comparable. That is, there exists sets K which are model-complete but not complete, and vice versa. In fact, let K* be an L-theory for the concept of an algebraically closed field. (see 4.10). Since the characteristic of an arbitrary model M of K* is not specified it follows that any sentence defined in K* which touches upon the characteristic of M, (for example, the sentence $(x)\,(y)\,[G(x,x) \neq y \supset y \neq 0]$ which asserts that the field is of characteristic 2) is undecidable in K*. Thus K* is not complete. On the other hand, it will be shown in chapter 8 that K* is model complete.

(5.10) Conversely, we shall now specify a set K which is complete but not model-complete. Let $M = (A, \phi, \mathcal{R})$ be any system such that $A = \{a_1, a_2 \ldots\}$ is a denumerable set of constants and consists of the single binary relation P such that the atomic sentences of the form $P(a_n, a_{n+1})$, and only those, hold in M. $n = 1, 2, \ldots$

Let K be the set of all sentences which contain no constants and which contain only the relation symbol P and which are satisfied by M. K is non-empty since it contains the sentence $Y = (Ex)\,(Ey)P(x,y)$. Also K is consistent by (3.6) since M is a model of K. Moreover K is complete since, for every sentence Y which contains only the relation P and is free of constants, either Y or $\sim Y$ is satisfied by M. That is, either Y or $\sim Y$ is contained in K and, a fortiori,

deducible from that set.

We now define a system M* by the conditions: $A^* = A \cup \{a_0\}$ $\phi^* = \phi$, $D(M^*) = D(M) \cup \{[P(a_0, a_1)]\}$. Then $M \subset M^*$ by (5.6). Moreover M* is also a model of K since it is in fact, isomorphic to M under the one-one correspondence indicated by: $a_n \in M \leftrightarrow a_{n-1} \in M^*$, $n = 1,2,3,\ldots$ The sentence $Y^* = (Ex)\ P(x,a_1)$ is defined in M but is not satisfied by M although it is satisfied by an extension M* of M which is a model of K. This, in conjunction with (5.9), shows that K is not model complete, as required.

It can be shown that, under certain conditions, the model-completeness of a set K entails the completeness of K (Robinson [3] pp. 72-77). We shall now investigate one of these conditions which will prove to be useful in the sequel.

(5.11) A system M_0 is said to be a <u>prime model</u> of a set of sentences K if :

(1) M_0 is a model of K

(2) M_0 can be embedded in any model M of K. That is, every model M of K is an extension of M_0. (It is understood that, if K includes any constants, then these shall correspond to themselves in the isomorphism from M_0 into M).

For example, the field of rational numbers is a prime model of the L-theory K_{P_0} for the concept of a field of characteristic zero (see 4.11). No prime model exists if the characteristic of the field is not specified.

It is quite possible that a prime model M_0 of a given set K be a proper extension of another prime model M_0' of the same set K. Indeed let S_0' be an L-theory for the concept of an ordered set which contains no last element (see (4.6)-(a). It is clear that any ordered set M of ordinal type ω (for example, the natural numbers) is a prime model of S_0' yet M has a proper subsystem M' (of the same type ω) which is isomorphic to M.

It is also possible that a set K possess two prime models

M_o and M'_o which are not isomorphic. Indeed, let S''_o be an L-theory for the concept of a densely ordered set (see 4.7) Let M_o be a densely ordered set with first and last elements, and let M'_o be a densely ordered set without first and last elements. Then clearly both M_o and M'_o are prime models of S''_o . We now prove:

(5.12) Theorem: (The prime-model test). Every model-complete set K of the sentences which possesses a prime model M_o is complete.

Proof: Let X be any sentence which is defined in K. Then X is defined also in M_o and so either X or $\sim X$ is satisfied by M_o. If X is satisfied by M_o then X is satisfied by all models of K which are extensions of M_o since K is model-complete, by assumption. That is, X is satisfied by all models of K so that X is deducible from K. Similarly, if $\sim X$ is satisfied by M_o, then $\sim X$ is deducible from K. Thus X is decidable in K, as required.

Chapter 6 Model-Completeness and Persistence

We shall now introduce an alternative approach to the concept of model-completeness, via the notion of persistence.

Let K be a consistent set (possibly empty) of sentences. In what follows we shall consider only predicates which are partially defined in K (see 2.8). This apparent restriction is in accordance with the remark following (3.2)

(6.0) A predicate $Q(x_1, \ldots x_u)$ $n \geq o$ is said to be <u>persistent with respect to K</u> if for any n-tuple $a_1, \ldots a_u$ of constants which belong to a model M of K the sentence $Q(a_1, \ldots a_u)$ can be deduced from the set $K \cup D(M)$;; that is, by (5.7) and (3.12), $Q(a_1, \ldots a_u)$ is satisfied by a model M of K only if it is also satisfied by all models of K which are extensions of M. In particular, a sentence X is persistent with respect to K if X is deducible from the set $K \cup D(M)$ for every model M of K which satisfies X.

For example, every sentence X which is deducible from K is persistent with respect to K. Again, if K is a set of axioms for the concept of a field then the predicate –

$Q(x,y) = (Eu)(Ev)\left[G(v,u) \doteq y \wedge \Pi(v,v) \doteq u\right]$

which asserts that the difference "y-x" possesses a square root is persistent with respect to K; while the predicate $\sim Q(x,y)$ is not. More generally it is easy to show (see Robinson [3] p. 13) that:

(6.1) Every existential predicate is persistent with respect to the empty set ϕ (and hence with respect to any consistent set K).

Using (6.1) we now prove:

(6.2) The diagram D(M) of any model M of K is o-complete.

<u>Proof</u>: We must show that every sentence X which is defined in an arbitrary model M of K and which is free of quantifiers is decidable in the set D(M).

Suppose then that X is defined in M so that either X or $\sim X$ is satisfied by M. If X is satisfied by M then X is also satisfied

by all extensions of M by (6.1). Since X is free of quantifiers. Thus X is deducible from D(M) by (5.7) and (3.12). Similarly $\sim X$ is satisfied by M only if $\sim X$ is deducible from D(M) (since $\sim X$ is likewise free of quantifiers). In any case, X is decidable in D(M).

We note that since the negation of an existential sentence which contains at least one quantifier is not existential, the set D(M) is not in general, 1-complete. Indeed, if M is the field of rational numbers then the sentence $(Ex)\left[\pi(x,x) = 2\right]$ is not decidable in D(M) since it is satisfied by the field of real numbers (which is an extension of M) but it is not satisfied by M itself.

We now prove the converse of (6.1) namely that any predicate which is persistent with respect to a given set K is K-equivalent to an existential predicate. More precisely:

(6.3) Let $Q(x_1,\ldots x_u)$ be a predicate which is persistent with respect to a given set K. Then there exists an existential predicate $Q^*(x_1,\ldots x_n) = (Ey_1)\ldots(Ey_m)R(x_1,\ldots x_u, y_1,\ldots y_m)$ where $m \geq o$ such that:

(1) Q^* is defined in the set $K \cup \{Q\}$

(2) Q and Q^* are K-equivalent.

Proof: We first prove (6.3) in the case that $n = o$. We must show that a sentence X is persistent with respect to K only if there exists an existential sentence Y which is defined in the set $K \cup \{X\}$ such that the sentence $X \equiv Y$ can be deduced from K.

Suppose then that the sentence X is persistent with respect to K. If the set $H = K \cup \{X\}$ is contradictory then $\sim X$ is deducible from K, by (1.7), so that the sentence $Y = (Ex)\left[Q(x) \wedge \sim Q(x)\right]$ where Q(x) is an arbitrary unary predicate which is defined in K clearly satisfies the requirements of (6.3). Hence we shall assume at the outset that the set H is consistent.

It is easily seen that the set E of all existential sentences of L is quasi disjunctive. (2.25). Let $F \subseteq E$ be the set of all

existential sentences Z which are defined in H and such that the sentence $Z \supset X$ is deducible from K. It follows readily that F is likewise quasi disjunctive.

Let $G = \{\sim Z \mid Z \in F\}$. If $J = H \cup G$ is consistent then J possesses a model M by (3.9). Since X is persistent with respect to K it follows that X is deducible from the set $K \cup D(M)$. If, in addition, X is deducible from K alone, then it suffices to choose $Y = (Ex)\,[Q(x) \vee \sim Q(x)]$ where $Q(x)$ is defined as above.

Let us then suppose that X is deducible from $K \cup D(M)$ but that X is not deducible from K alone. By (2.6) - (a) it follows that there exist sentences $Z_1, \ldots Z_n \in D(M)$, $n \geq 1$, such that the sentence $[Z_1 \wedge \ldots \wedge Z_n] \supset X$ is deducible from K alone. We write $Z_1 \wedge \ldots \wedge Z_n = Z(a_1, \ldots a_k)$ $k \geq 0$ where $a_1, \ldots a_k$ are the individual constants that appear in Z but do not occur in the sentences of H. It follows by (2.6) -(g) that the sentence $[(Ex_1) \ldots (Ex_k)\, Z(x_1, \ldots x_k)] \supset X$ is deducible from K. Now the sentence $V = (Ex_1) \ldots (Ex_k)\, Z(x_1, \ldots x_k)$ belongs to F (by definition of F) so that the sentence $\sim V$ belongs to G. Also $\sim V$ is satisfied by M since M is a model of G. On the other hand, the sentences $Z_1, \ldots Z_n$ all belong to D(M) so that V is satisfied by M which is a contradiction.

Thus the only case left to consider is the case that $J = H \cup G$ is contradictory. Since H is consistent by assumption, it follows by (2.7) that for some positive integer $n \geq 1$, there exist sentences $Y_1, \ldots Y_n \in F$ (i.e., $\sim Y_1, \ldots \sim Y_n \in G$) such that the set $K \cup \{\sim Y_1, \ldots \sim Y_n, X\}$ is contradictory. By (1.7) and (2.14) it follows that the sentence $X \supset [Y_1 \vee \ldots \vee Y_n]$ can be deduced from K. Now F is quasi-disjunctive so that there exists a sentence Y F such that $Y_1 \vee \ldots \vee Y_n \simeq Y$. Hence by (2.12) the sentence $X \supset Y$ is deducible from K. But $Y \supset X$ is deducible from K by the defining property of F. Thus Y satisfies the requirements of (6.3).

We now consider the case $n \geq 1$. Let $Q(x_1 \ldots x_u)$ be persistent with respect to K. Let $a_1 \ldots a_u$ be a set of individual constants which occur neither in Q nor in K. Then $X = Q(a_1, \ldots a_u)$ is a sentence which is persistent with respect to K so that, by what we have already proven, we can assert the existence of an existential sentence $Y = (Ey_1) \ldots (Ey_m)\ Z(y_1, \ldots y_m)$ which is K-equivalent to X and which is defined in the set $K \cup \{X\}$. We may assume a priori that the matrix Z of Y contains all the constants $a_1, \ldots a_u$ for, if not, we may conjoin to Z a provable sentence which is free of quantifiers and which contains these constants.

Hence we may write $Z = (Ey_1) \ldots (Ey_m)\ R(a_1, \ldots a_u, y_1 \ldots y_m)$ and by assumption the sentence—

$$\left[Q(a_1, \ldots a_u) \equiv \left[(Ey_1) \ldots (Ey_m)\ R(a_1, \ldots a_u, y_1, \ldots y_m) \right] \right]$$

is deducible from K. But the constants $a_1 \ldots a_u$ do not occur in either K or in the predicates Q and R by assumption, so that (2.6)-(e) in conjunction with the above establishes the conclusion of (6.3) in the general case.

We leave it to the reader to verify that:

(6.4) The following conditions are equivalent:

(1) Every universal sentence is persistent with respect to K.

(2) Every universal predicate is persistent with respect to K.

(3) Every universal predicate which is defined in K is persistent with respect to K.

(6.5) A (consistent and non-empty) set K of sentences which satisfies one (and hence all) of the conditions (1), (2), (3) of (6.4) is said to be <u>pre-complete</u>.

It is easily verified that:

(6.6) Every model complete set K is also pre-complete.

We now prove.

(6.7) For a set K to be pre-complete it is necessary (and obviously) sufficient) that <u>every</u> predicate Q be persistent with respect to K.

Proof: By (2.16) it suffices to consider only sentences in prenex normal form. We observe first of all, that the pre-completeness of a set K, in conjunction with (6.1), implies that every predicate of class 1 is persistent with respect to K. Hence we may proceed by induction on the class number n (see 2.17, 2.18) to which Q belongs. Suppose then that we have already proved (6.7) for all predicates of class $m \geq 1$. Let $Q(x_1, \ldots x_n)$ be a predicate of class m + 1 but not of class m. We consider two cases:

Suppose that the last quantifier in the prefix of Q is universal. That is, Q is of the form -

$$Q(x_1, \ldots x_n) = (q_1) \ldots (q_{k-1})(Ey_k)(y_{k+1}) \ldots (y_\ell)\ R(x_1, \ldots x_n, y_1, \ldots y_\ell)$$

where $k \geq 1$, R is free of quantifiers and the quantifier q_i contains the variable y_i i = 1,2,... k-1; while the quantiers after (Ey_k) are all universal. Now the predicate

$$S(x_1, \ldots x_n, y_1, \ldots y_k) = (y_{k+1}) \ldots (y_\ell)\ R(x_1, \ldots x_n, y_1, \ldots y_\ell)$$

is universal and hence is persistent with respect to K by assumption. It follows by (6.3) that there exists an existential predicate $S^*(x_1, \ldots x_n y_1, \ldots y_k)$ which is K-equivalent to S. Substituting S* for S in Q it follows by (2.12) that we obtain a predicate $Q^*(x_1, \ldots x_n)$ which is K-equivalent to Q. But Q* is now a predicate of class m and so is persistent with respect to K by our induction hypothesis. Hence Q, by (3.5), is likewise persistent with respect to K.

Now assume that the last quantifier in the prefix of Q is existential. That is, Q is of the form-

$$Q(x_1, \ldots x_n) = (q_1) \ldots (q_{k-1})(y_k)\ (Ey_{k+1}) \ldots (Ey_\ell)\ R(x_1, \ldots x_n, y_1, \ldots y_\ell)$$

where $k \geq 1$; (y_k) is the last universal quantifier in the prefix of Q while the q_i and R are defined as before. Now the predicate

$$S(x_1, \ldots x_n, y_1 \ldots y_k) = (Ey_{k+1}) \ldots (Ey_\ell) R(x_1, \ldots x_n, y_1, \ldots y_\ell)$$

is existential so that its negation $S_0(x_1, \ldots x_n, y_1, \ldots y_k) = (y_{k+1}) \ldots (y_\ell)[\sim R]$ is universal. It follows as before that there exists an existential predicate $S_0^*(x_1, \ldots x_n, y_1, \ldots y_k) = (Ey_{k+1}) \ldots (Ey_\rho) R^*(x_1, \ldots x_n, y_k, \ldots y_\rho)$ which is K-equivalent to S_0, so that by (2.14) the predicate

$$\overline{S_0^*} = (y_{k+1}) \ldots (y_\rho)[\sim R^*]$$

is K-equivalent to S. It follows by (2.12) that the predicate $Q^*(x_1,\ldots x_u) = (q_1)\ldots(q_{k-1})(y_k)(y_{k+1})\ldots(y_p)[\sim R^*]$ is K-equivalent to Q. But Q^* is of class m and so is persistent with respect to K by our induction hypothesis. Hence Q is likewise persistent with respect to K. This completes the proof of (6.7). We now prove:

(6.8) If a set K is both pre-complete and 1-complete then K is complete.

Proof: Let X be any sentence which is defined in K. Then X is persistent with respect to K by (6.7) since K is pre-complete. By (6.3) there exists an existential sentence Y which is defined in K and which is K-equivalent to X. Since K is 1-complete it follows that Y is decidable in K, and hence so is X.

We note that the hypothesis of (6.8) is not a necessary condition for completeness. In fact let M be the ordered set of positive integers and let K be the set of all sentences formulated in terms of theequality relation $=$ and the ordering relation Q which are satisfied by M. An argument similar to that of (5.10) shows that K is complete. But K is not pre-complete since the sentence $(x)\left[x = 1 \vee Q(1,x)\right]$ is satisfied by M but is not satisfied by the ordered set of non-negative integers which is a model of K (since it is in fact isomorphic to M) and an extension of M.

The following results shall be useful:

(6.9) If the set $K \cup D(M)$ is 1-complete for every model M of K then it is also pre-complete for every model M of K.

Proof: Let M be any model of K and let X be a universal sentence which is satisfied by a model M^* of the set $K \cup D(M)$. Now $K \cup D(M^*)$ is also 1-complete and X is satisfied by M^* so by (5.1), and (5.7) X is satisfied by all models of K which are extensions of M^*. But M^* is by (5.7) and by definition an extension of M so that X is satisfied by all models of $K \cup D(M)$ which are extensions of M^*. Thus the set $K \cup D(M)$ is

pre-complete by (6.4).

(6.10) If the set $K \cup D(M)$ is precomplete where M is a given model of K then it is also 1-complete.

Proof: Let X be a universal sentence which is defined in the set $K \cup D(M)$. If X is satisfied by M then X is deducible from the set $K \cup D(M)$ by (6.0) since $K \cup D(M)$ is pre-complete. If $\sim X$ is satisfied by M we write $X = (y_1) \ldots (y_\mu)\, Q(y_1, \ldots y_\mu)$ so that by (2.14) and (3.5) the sentence $X' = (Ey_1) \ldots (Ey_\mu) \sim Q(y_1, \ldots y_\mu)$ is satisfied by M. But X is existential and so by (6.1) is satisfied by all models of K which are extensions of M. That is X' (and hence $\sim X$) is deducible from $K \cup D(M)$. In any case, X is decidable in $K \cup D(M)$. Hence by (5.4) $K \cup D(M)$ is 1-complete.

(6.11) If the set K is pre-complete then the set $K \cup D(M)$ is both pre-complete and 1-complete. for every model M of K.

Proof: Let K be pre-complete. By (6.10) it suffices to show that the set $K \cup D(M)$ is pre-complete for every model M of K.

Suppose that for some model M_0 of K the set $K \cup D(M_0)$ is not pre-complete. Then there exists a sentence X such that X is satisfied by a model M_1 of $K \cup D(M_0)$ but X is not satisfied by an extension M_2 of M_1 which is a model of $K \cup D(M_0)$. But then both M_2 and M_1 are models of K and extensions of M_0. This contradicts the pre-completeness of K.

(6.12) A set K is model-complete if and only if the set $K \cup D(M)$ is 1-complete for every model M of K.

Proof: Necessity is obvious by definition of model-completeness. Conversely, suppose that the set $K \cup D(M)$ is 1-complete for every model M of K. It follows by (6.9) that the set $K \cup D(M)$ is also precomplete for every model M of K. Hence by (6.8) $K \cup D(M)$ is complete for every model M of K; that is, K is model-complete.

The importance of the above result lies in the fact that in order to establish the model-completeness of a set K it

suffices by (5.4) to consider only existential sentences which are defined in an arbitrary model M of K. We shall now show that the concepts of model-completeness and pre-completeness coincide. More precisely::

(6.13) For a set K to be model-complete it is necessary and sufficient that K be pre-complete.

Proof: In view of (6.6) it suffices to show that every pre-complete set K is also model-complete. This on the other hand follows directly from (6.11) and (6.12).

It follows by (6.7) that every predicate in a model-complete set K is persistent with respect to K and conversely. Hence by (6.1) and (6.3) it follows that a model-complete set K is fully characterized by the deductive property that every predicate (which is partially defined in K) is K-equivalent to an existential predicate.

Chapter 7 The Test for Model-Completeness

In this chapter we shall establish a simplified semantical characterization of the notion of Model-completeness. By way of example we shall show that certain group theoretical concepts are model-complete and also complete.

(7.0) An existential sentence Y will be called primitive if the matrix Z of Y is a conjunction of atomic formulae and (or) of negations of such formulae. (It is understood that this definition includes the possibility that Z consist of a single atomic formula or of the negation of such a formula.)

Since every formula in the propositional calculus C is equivalent in the sense of (1.8) to a disjunctive normal formula, it follows by (2.5) -(a), (2.12), and (2.16) that:

(7.1) Every existential sentence in L is equivalent to a disjunction of primitive sentences; that is, for every existential sentence X there exist primitive sentences $Y_1, \ldots Y_u$ $(n \geq 1)$ such that $X \simeq [Y_1 \vee \ldots \vee Y_u]$. We now prove:

(7.2) Theorem: Let K be a consistent and non-empty set of sentences. Then the following conditions are equivalent:

(a) K is model-complete.

(b) For every pair of models M and M* of K such that $M \subseteq M^*$ any primitive sentence Y which is defined in M can be satisfied by M* only if it is already satisfied by M.

(c) Every primitive sentence Y which is defined in a model M of K is decidable in the set $K \cup D(M)$.

Proof: Suppose that K is model-complete while condition (b) does not hold. Then there exist models $M \subseteq M^*$ of K and a primitive sentence Y which is defined in M but is not satisfied by M although it is satisfied by M*. Now both M and M* are models of $K \cup D(M)$ by (5.7) so that Y is not decidable in the set $K \cup D(M)$. This contradicts the model completeness of K

and shows that (a) implies (b).

Now suppose that condition (b) is satisfied. Let Y be a given primitive sentence which is defined in a model M of K. Suppose that Y is satisfied by some model M* of $K \cup D(M)$. Then $M \subseteq M^*$ by (5.7) so that our assumption implies that Y is also satisfied by M. Now Y is persistent with respect to K by (6.1) and hence is deducible from the set $K \cup D(M)$; so that (b) implies (c). That condition (c) implies (a) follows readily from (7.1), (6.12), (5.4), in conjunction with (2.14).

Thus (7.2) strengthens the remark following (6.12) in so far as conditions (b) and (c) assert that primitive sentences only need be considered. Condition (b) will be used as a test for model completeness in this and in the next chapter.

(7.3) We shall now present an alternative and more direct proof of (7.2) which is independent of the notions of n-completeness and pre-completeness developed in chapters 5 and 6. It remains only to show that condition (c) implies condition (a).

Indeed suppose that condition (c) is satisfied but that K is not model complete. Then there exists a model M of K and a sentence X which is defined in M but Which is not decidable in the set $K \cup D(M)$. If so, there exists sentences of this kind which are in prenex normal form and for which the number of quantifiers is a minumum; where it is understood that all such models M of K are taken into account.

Let X be such a sentence. We may suppose that X begins with an existential quantifier. For if X does not include any quantifiers then X is decidable in the set D(M) by (6.2) and, a fortiori, in the set $K \cup D(M)$. Again, if X begins with a universal quantifier we may consider instead the negation X' of X which does begin with an existential quantifier, and which is likewise undecidable in $K \cup D(M)$ by (2.14). (We note that X' has the same number of quantifiers as X and hence shares its minimal property.)

Hence suppose $X = (Ez)\,V(z)$ where X is defined in a model M of K but is not decidable in $K \cup D(M)$. Since the sentence $\sim X$ is not deducible from $K \cup D(M)$ it follows by (1.7) that the set $K \cup D(M) \cup \{X\}$ is consistent. Hence there exists by (3.9) and (5.7) a model M^* of K which is an extension of M and which satisfies X. That is, M^* contains a constant c such that $V(c)$ is satisfied by M^*. It follows by the minimal property of X, that the sentence $V(c)$ is deducible from the set $K \cup D(M^*)$ and hence by (2.6) -(d) so is the sentence $X = (Ez)\,V(z)$.

Now by (5.6) the set $K \cup D(M^*)$ contains, in addition to the sentences of $K \cup D(M)$ only certain atomic formulae and their negations. Then (2.6) -(a) implies that there is a conjunction $W(b_1, \ldots b_\mu)$ of a finite number of these sentences such that the sentence $[W(b_1, \ldots b_\mu)] \supset X$ is deducible from $K \cup D(M)$ where $b_1, \ldots b_\mu$ denote the individual constants which occur in W but which do not belong to M.

It follows that the constants $b_1, \ldots b_\mu$ cannot occur in the sentence X or in the sentences of $K \cup D(M)$ so that by (2.6) -(g) we may infer that the sentence $[(Ex_1) \ldots (Ex_\mu)\ W(x_1, \ldots x_\mu)] \supset X$ is deducible from $K \cup D(M)$. But the sentence $Y = (Ex_1) \ldots (Ex_\mu) W(x_1 \ldots x_\mu)$ is a primitive sentence which is defined in M and which is satisfied by M^*. Hence by our hypothesis Y is deducible from the set $K \cup D(M)$. It follows by (2.6) -(b) that the sentence X is likewise deducible from $K \cup D(M)$ which is a contradiction. Hence K is model-complete.

Let G'_A be an L-theory for the concept of a completely divisible torsion free abelion group which contains at least two different elements (see4.4). A group of this type (that is, a model of G'_A) will be called here a group of <u>type D.</u>

It is easily seen that in a group of type D the equation $ny = x$, $(n \geq 1)$ possesses a unique solution y for any given x.

Let $r = {}^{m}/_{n}$ be any positive rational number where m and n are positive integers. We then define $\vdash x$ as the unique solution y of the equation $ny = m\,x$ and we set $\vdash x = (-r)\,(-x)$ for any negative rational r. It is then clear that the rational numbers may be regarded as a (left) operator ring for any group of type D; that is, any group of type D may be regarded as a (left) R-module where R denotes the ring of rational numbers.

In the discussion of groups of type D "linear dependence" will be understood to mean linear dependence with respect to the rational numbers as operator ring. Given two groups M and M* of type D such that $M \subseteq M^*$ we shall say that <u>M* is of rank n over M</u> if n is the maximum number of linearly independent elements in the difference group M* - M. The rank of M* over M, if finite, will be denoted by $(M^*:M)$. We note $(M^* : M) \geq 1$ if $M \subset M^*$ while $(M^* : M) = 0$ if and only if $M^* = M$. We are now in a position to prove:

(7.4) The elementary theory G_n' for the concept of a group of type D is model-complete.

<u>Proof</u>: Suppose that G_n' is not model-complete Then by condition (b) of (7.2) there exist groups M and M^* of type D such that $M \subseteq M^*$ and a primitive sentence $Y = (Ey_1)\ldots(Ey_u)\ Z(y_1,\ldots y_u)$ which is defined in M and which is satisfied by M^* although it is not satisfied by M.

Translated into ordinary algebraic language Y states that a particular system of equations and inequalities of the type:

(7.5) $\alpha = \beta,\ \alpha \neq \beta,\ \alpha + \beta = \gamma,\ \alpha + \beta \neq \gamma$ possesses a solution where the Greek letters stand for constants of M or for the "unknowns" $y_1, \ldots y_u$. Let $y = a_i$, $a_i \in M^*$ be a solution of (7.5). Let $M'' = M(a_1, \ldots a_u)$ be the group (necessarily of type D) obtained by adjoining the elements $a_1, \ldots a_u$ to M; i.e. M'' consists of all elements of the form $a + r_1 a_1 + \ldots + r_n a_n$ where $a \in M$ and the r_i are

rational, $i = 1,2,\ldots n$.

It is easily verified that any $n+1$ elements in the difference group $M''-M$ are linearly dependent. That is $(M'':M) \leq n$ so that there exist extensions of M which are of finite rank over M and in which (7.5) possesses a solution. Let M_o be an extension of this type whose rank m_o over M is as small as possible. If $m_o = o$ then $M_o = M$ which is impossible. If $m_o > 1$ let M_o^* be any group of type D between M and M_o which is obtained by adjoining to M $m_o - 1$ elements of M_o which are linearly independent with respect to M (i.e such that the corresponding elements in the difference group $M_o - M$ are linearly independent). Then M_o^* is of rank $m_o - 1$ over M and so (7.5) cannot possess a solution in M_o^* by the minimal property of m_o. Also M_o is of rank 1 over M_o^*. Accordingly we may assume at the outset that M_o is of rank $m_o = 1$ over M.

It follows that every element $a' \in M_o$ can be written uniquely in the form $a' = a + r a_o$ where $a \in M$, r is rational and a_o is an arbitrary but fixed element of M_o which does not belong to M. In particular, then (7.5) is satisfied by certain elements $y_i = a_i + r_i a$ where $a_i \in M$ and r_i are rational, $i = 1,2,\ldots n$.

Substituting these expressions in (7.5) and transferring all terms to the left hand side we obtain a finite number of expressions of the form:

$$(7.6) \qquad \begin{aligned} b_j + s_j a_o &= o \qquad j = 1,2,\ldots \ell \\ b_j + s_j a_o &\neq o \qquad j = \ell+1,\ldots p \end{aligned}$$

where $b_j \in M$ and the s_j are rational. Thus $y = a_o$ is a solution of the system of equations and inequalities:

$$(7.7) \qquad \begin{aligned} b_j + s_j y &= o \qquad j = 1,2,\ldots \ell \\ b_j + s_j y &\neq o \qquad j = \ell+1,\ldots p \end{aligned}$$

We note that this system cannot have a solution in M for if (7.7) were satisfied by some $y = a \in M$ then (7.5) would be satisfied by the set $y_i = a_i + r_i a$ which is contrary to

assumption. On the other hand since a_0 is linearly independent of all the elements of M it follows that $b_j = 0$, $s_j = 0$ for $j = 1,2, \ldots \ell$ in (7.6) and (7.7) and so the first ℓ conditions of (7.7) hold identically.

We may also assume that $s_j \neq 0$ for $j = \ell + 1, \ldots p$ since otherwise the inequality in question holds or does not hold independently of the value of y. Accordingly we may write the inequalities of (7.7) in the form:

(7.8) $y \neq c_j$ where $c_j = -s_j^{-1} b_j$ $j = \ell + 1, \ldots p$

and every solution of (7.8) is a solution of (7.7). But M is infinite (torsion free) and so we only have to choose an element $y = a \in M$ which is different from all c_j, $j = \ell + 1, \ldots p$ in order to obtain a solution of (7.8) in M. But if so then (7.7) and hence (7.5) also possess solutions in M. Thus the original assumption that (7.5) has no solution in M leads to a contradiction, and this proves (7.4)

We now consider ordered abelion groups. Let G_{AO} be an L-theory for the concept of a completely divisible ordered abelian group which contains at least two different elements. (see (4.6) - (b) and (4.4) - (iii). Such a group (i.e a model of G_{AO}) will be called here a group of type DO . We now prove:

(7.9) The elementary theory G_{Ac} for the concept of a group of type DO is model-complete.

Proof: We proceed as in the proof of (7.4) and employ (7.2)-(b). A primitive statement $Y = (Ey_1) \ldots (Ey_u) Z(y_1, \ldots y_u)$ which is defined in a group M of type DO now amounts to the assertion that a particular finite system of equations and inequalities of the type:

(7.10) $\alpha = \beta$ $\quad \alpha + \beta = \gamma$ $\quad \alpha < \beta$

$\alpha \neq \beta$ $\quad \alpha + \beta \neq \gamma$ $\quad \alpha \geq \beta$

possesses a solution. In these expressions the Greek letters stand either for constants of M or for the unknowns $y_1, \ldots y_u$.

We observe that $\alpha \geq \beta$ is the negation of $\alpha < \beta$. We shall show that the assumption that (7.10) possesses a solution in an extension M_o of M which is of type DO but does not possess a solution in M leads to a contradiction.

Since every ordered abelian group (containing at least two elements) is necessarily torsion free it follows that every group of type DO is a group of type D. We may therefore again introduce the ring of rational numbers as operator ring. Using the same arguments as before, we may again confine ourselves to the assumption that M_o is of rank $m_o = 1$ over M.

Then (7.10) is satisfied by certain elements $y_i = a_i + r_i a_o$ of M where $a_i \in M$ r_i rational $i = 1,2,\ldots n$ and a_o is defined as before. We now carry out the substitution $y_i = a_i + r_i y$ $i = 1,2,\ldots n$ in (7.10) and transfer all the non-vanishing terms to the left hand side. There results a system of equations and inequalities of the form:

$$(7.11) \qquad \begin{array}{llll} b_j + s_j y = o & & b_j + s_j y < o \\ b_j + s_j y \neq o & & b_j + s_j y \geq o \end{array}$$

where the b_j all belong to M and s_j are rational. This system is satisfied in M_o by $y = a_o$ but it cannot be satisfied in M for, in that case, (7.10) would also be satisfied in M.

Now $b_j + s_j y \neq o$ is equivalent to a disjunction which may be written briefly as:

$$[(b_j + s_j y) > o] \vee [(b_j + s_j y) < o]$$

and similarly $b_j + s_j y \geq o$ is equivalent to:

$$[b_j + s_j y = o] \vee [b_j + s_j y > o].$$

In each case $y = a_o$ must satisfy at least one member of the disjunction and we may then omit the other member. Thus the system (7.11) is replaced by an equivalent system of the form:

$$(7.12) \qquad \begin{array}{l} b_j + s_j y = o \\ b_i + s_j y < o \\ b_j + s_j y > o \end{array}$$

But $b_j + s_j y = o$ entails $b_j = o$, $s_j = o$ for all expressions of the first type in (7.12) while we may assume that $s_j \neq o$ for the expressions of the second and third type. Accordingly (7.12) may be reduced to a system

(7.13) $\quad y > c_j \qquad j = 1,2,\ldots \ell$

$\qquad\quad y < c_j \qquad j = \ell + 1,\ldots p$

where $c_j \in M, 1 \leq j \leq p$ and one or the other of the two sets may be empty. We now show that (7.13) is already satisfied by M.

Indeed suppose first that neither set in (7.13 is empty. Put

$$c' = \max. c_j \qquad 1 \leq j \leq \ell$$

$$c'' = \min. c_j \qquad \ell + 1 \leq j \leq p$$

Then $c' < c''$ since $c' < a_o \leq c''$. It follows that $y = a = \frac{1}{2}(c' + c'')$ is a solution of (7.13) and $a \in M$. Similar definitions are effective if just one of the two sets in (7.13) is empty. If both sets are empty, there is nothing to prove. In any case we arrive at a contradiction. This completes the proof of (7.9).

Now let M be any group of type D and let $a \neq o$ be an arbitrary but fixed element of M. It is clear that the set $A = \{ra \mid r \in R\}$ where R denotes the ring of rational numbers is a group of type D — in fact — a subgroup of M. Also the mapping $ra \to r$ is an isomorphism of A onto the additive group of rational numbers. Hence the additive group of rational numbers is a prime model (see 5.11) of the theory G'_A (see 7.4). Likewise the ordered additive group of rational numbers is a prime model of the theory G_{Ao} (see 7.9). Hence by (5.12) we have:

(7.14) The elementary theory G'_A for the concept of a group of type D and the elementary theory G_{Ao} for the concept of a group of type DO are both complete.

Chapter 8 Model-Complete Fields With Applications.

In this chapter we shall show that the elementary L-theories of algebraically closed and real closed fields are both model complete (and complete). Assuming the reader to be familiar with elementary field theory, we shall also give examples of some interesting applications to algebra. We begin with algebraically closed fields and the following well known result (see Zariski and Samuel [1]):

(8.0) Let M be any field. Then there exists a field $\overline{M}$ such that:

(i) $\overline{M}$ is an algebraic extension of M.

(ii) $\overline{M}$ is algebraically closed.

(iii) $\overline{M}$ is unique up to an isomorphism over M.

$\overline{M}$ is called the algebraic closure of M. We observe that (8.0)-(iii) asserts that every isomorphism from a field M onto a field M′ can be extended to an isomorphism from $\overline{M}$ onto $\overline{M'}$. We are now in a position to prove:

(8.1) The elementary theory of algebraically closed fields is model-complete.

Proof: Let K* be an L-theory for the concept of an algebraically closed field (see 4.10). Assuming that K* is not model-complete, (7.2)-(b) asserts the existence of a primitive sentence Y which is defined in an algebraically closed field M and which is satisfied by an algebraically closed extension M′ of M although it is not satisfied by M.

In ordinary algebraic notation Y is equivalent to the assertion that a particular finite system of equations and inequalities of the type:

$$\alpha = \beta \qquad \alpha + \beta = \gamma \qquad \alpha\beta = \delta$$
$$\alpha \neq \beta \qquad \alpha + \beta \neq \gamma \qquad \alpha\beta \neq \gamma$$

possesses a solution, where the Greek letters stand either for elements of M or for the "unknowns" $y_1, \ldots y_\mu$ of the sentence

$Y = (Ey_1)\ldots(Ey_u)\ Z\ (y_1,\ldots y_u)$. Now we may replace the inequalities in (8.2) by equations, by introducing for each inequality a new unknown y_j, and by replacing the inequality in question by the equivalent-

$$(\alpha-\beta)\ y_j-1 = 0 \qquad (\alpha+\beta+\gamma)y_j-1 = 0 \qquad (\alpha\beta-\gamma)y_j-1=0$$

respectively. It follows that (8.2) is equivalent to a finite system of polynomial equations:

(8.3) $\rho_k(y_1, y_2, \ldots y_m) = 0, m \geq n, \quad k \geq 1$, with coefficients in M.

Suppose then that (8.3) possesses a solution in an algebraically closed extension M' of M although it does not possess a solution in M. Let the solution be given by $y_1 = a_1$, $y_2 = a_2 \ldots y_m = a_m$. Then (8.3) possesses a solution also in the algebraic closure M'' of $M(a_1, \ldots a_m)$ and the degree of transcendence of M'' over M is finite ($\leq m$). Now let M_0 be an algebraically closed field between M and M'', $M \subseteq M_0 \subseteq M''$ in which (8.3) possesses a solution and such that the degree of transcendence m_0 of M_0 over M, $m_0 \geq 1$ is a minimum. We may then assume that $m_0 = 1$; for if this is not the case a priori, then we may always replace M by the algebraic closure of $M(b_1 \ldots b_{m_0-1})$ where $b_1, \ldots b_{m_0-1}$ are $m_0 - 1$ elements of $M_0 - M$ which are algebraically independent with respect to M. Suppose then that $m_0 = 1$.

We have thus established the existence of algebraically closed fields M and M_0 such that M_0 is an extension of M of degree of transcendence 1 over M and such that (8.3) possesses a solution in M_0 but not in M. Now let M^* be any algebraically closed proper extension of M. Let a^* be any element of M^* which does not belong to M. Then a^* is transcendental over M so that the algebraic closure M^{**} of $M(a^*)$ is isomorphic to M_0 (since M_0 is also the algebraic closure of a simple transcendental extension of M) over M. The fact that Y is satisfied by M_0 therefore entails that Y is satisfied by M^{**} and hence by M^* since $M(a^*) \subseteq M^*$. In other words, Y is satisfied by all proper extensions of M which are algebraically closed.

Let K_0 be the set of all sentences of the form $\sim[c \mp b]$ where c is an arbitrary but fixed (individual) constant of L which is not contained in M, and b varies over all the elements of M. Put $K_1 = K^* \cup D(M) \cup K_0$. Then the models of K_1 are precisely the algebraically closed proper extensions of M. It follows by (3.12) and the above that Y is deducible from K_1 and hence by (2.6)-(a) there exists a finite subset of K_0, say - $\{\sim[c \mp b_1], \ldots \sim[c \mp b_\ell]\}$ such that the sentence: $[\sim[c \mp b_1] \wedge \ldots \sim[c \mp b_\ell]] \supset Y$ is deducible from $K^* \cup D(M)$. It follows by (8.6) = (g) that the sentence; $\forall = [(Ey)[\sim[y \mp b_1] \wedge \ldots \wedge \sim[y \mp b_\ell]]] \supset Y$ is also deducible from $K^* \cup D(M)$. But M is a model of $K^* \cup D(M)$ and since M is infinite (algebraically-closed) it follows that for any finite set $\{b_1, \ldots b_\ell\}$ of elements of M we can find an element of M which is different from all these. Thus the implicans of $\forall$ is satisfied by M and we conclude that the implicate, which is Y, is likewise satisfied by M. We have therefore arrived at a contradiction which proves (8.1).

By way of example we now prove the known result that:

(8.4) A system of polynomial equations--

$p_j(x, \ldots x) = 0$; $j = 1, 2, \ldots m$ which has a solution is some extension of its field of coefficients F must already have a solution in the algebraic closure of F.

Proof: Let K* be a set of axioms for the concept of an algebraically closed field and let M be the algebraic closure of F. It is then not difficult to formulate a sentence X which is defined in $K^* \cup D(M)$ and which asserts that the system of polynomial equations (above) possesses a solution. Now if X is satisfied by some extension F' of F then it is also satisfied by the algebraic closure M' of F'. But M' is an extension of M and a model of K* so that the model completeness of K* implies that X is already satisfied by M as required.

Let us now consider real closed fields. We begin with the following algebraic preliminaries (see Van Der Waerden [1] p.p.225-232) :

(8.5) A field M is said to be formally real if (-1) is not expressible in M as a sum of squares (or equivalently, if a sum of squares vanished in M only if each term vanishes individually). For example, every ordered field is formally real. We observe that every subfield of a formally real field is formally real.

(8.6) Let M be a formally real field. Then the following conditions are equivalent:

(1) M is a real closed field (see 4.13)

(2) $M(i)$ is algebraically closed where $i = \sqrt{-1}$

(3) No proper algebraic extension of M is formally real.

(8.7) It follows by (8.6)-(2) that the roots of a polynomial $f(x)$ with coefficients in a real closed field M must lie in $M(i)$ and therefore always occur in conjugate pairs $a + bi$, $a-bi$. By factoring $f(x)$ into linear factors in $M(i)$ and combining pairs of conjugate factors it follows that every polynomial $f(x)$ over M can be decomposed into linear and quadratic factors irreducible in M. As a corollary we have:

(8.8) Let M be a real closed field and let $M(c)$ be a simple transcendental ordered extension of M. Then the ordering of $M(c)$ is uniquely determinded by the ordering of M together with the set of relations $a<c$, $c<a$ or $c=a$, whichever holds in $M(c)$, where a varies over all constants of M.

Proof: It is sufficient to show that the set of relations $a<c$, $c<a$, $c = a$ determines uniquely whether an arbitrary element of $M(c)$ is positive or negative or zero. The general element a^* of $M(c)$ is of the form:

$$a^* = b\left(\frac{c^k + a_{k-1}c^{k-1} + \ldots + a_1 c + a_0}{c^m + b_{m-1}c^{m-1} + \ldots + b_1 c + b_0}\right)$$

where $b, a_0, \ldots a_{k-1}, b_0 \ldots b_{m-1} \in M$. We may disregard the case that

a* reduces to an element of M. Then both numerator and denominator of a* may be decomposed by (8.7) into linear and quadratic factors:

(8.9) $$a^* = b\left(\frac{\prod(c-\alpha_\delta)\prod\left((c-\beta_\delta)^2+\gamma_\delta^2\right)}{\prod(c-\alpha'_\delta)\prod\left((c-\beta'_\delta)^2+(\gamma'_\delta)^2\right)}\right)$$

where $\alpha_\delta, \alpha'_\delta, \beta_\delta, \beta'_\delta, \gamma_\delta, \gamma'_\delta$ all belong to M. The quadratic factors of (8.9) are necessarily positive, while the sign of the linear factors is determined by our given ordering relations. Hence the sign of a* is determined by these relations together with the sign of b. This proves (8.8).

(8.10) Theorem of Artin Schreier) For every ordered field M there exists a field R such that:

(i) R_M is real closed.

(ii) R_M is an algebraic extension of M whose order preserves the order of M.

(iii) R_M is unique up to an isomorphism over M.

For example if M is the field of rational numbers then R_M is the field of all real algebraic numbers. We note that (8.10) - (iii) asserts that every (order preserving isomorphism from an ordered field M onto an ordered field M' can be extended to an isomorphism from R_M onto $R_{M'}$. As a corollary we have:

(8.11) If M is a subfield of a real closed field M* then M has a unique real closed algebraic extension M', $M \subseteq M' \subseteq M^*$ which is isomorphic to R_M over M.

Proof: Let M' denote the subfield of all elements of M* which are algebraic over M. Since M* is real closed it follows by (8.6)-(2) that M* (i) is algebraically closed and hence so is M'(i). That is, M' is a real closed field. Now every algebraic extension of M in M* is contained in M' and by (8.6)-(3) no proper subfield of M' containing M can be real closed. Therefore M is the only real closed algebraic extension of M in M*.

M' will be called the real closure of M* in M. Indeed, by (8.10), M' is isomorphic to R_M over M. We are now in a position to prove:

(8.12) The elementary theory of real closed fields is model-complete.

Proof: Let K_R be a set of axioms for the concept of a real closed field. Assuming that K_R is not model-complete then (7.2)-(b) asserts the existence of a primitive sentence $Y = (Ey_1)\ldots(Ey_n)Z(y_1,\ldots y_n)$ whose constants belong to a real closed field M and which involves only the operations of addition and multiplication and the relations of equality and order and which is satisfied by a real closed extension M' of M although it is not satisfied by M.

Thus M' contains constants $c_1,\ldots c_n$ such that $Z(c_1,\ldots c_n)$ is satisfied by M'. Since Z is free of quantifiers it follows that Z is also satisfied by the ordered field $M(c_1,\ldots c_n)$. Now the degree of transcendence of $M(c_1,\ldots c_n)$ over M is finite ($\leq n$). Let M_0 be a real closed extension of M which satisfies Y and such that the degree of transcendence m_0 of M_0 over M is a minimum. Now Y is not satisfied by M so that $m_0 \geq 1$; (We observe that no proper real closed extension of M can be algebraic over M by (8.6)-(3)) and hence by extending M if necessary, as in the proof of (8.1), we may suppose more precisely that $m_0 = 1$.

Let c be an arbitrary but fixed element of M which does not belong to M. Then c is transcendental over M by (8.6)-(3).

Let K_0 be the set $\{\sim[a = c]\}$ together with all atomic sentences of the form Q (a , c) and Q (c,a) which hold in M(c) where a varies over all elements of M. Put $K_1 = K_0 \cup K_R \cup D(M)$. Then K_1 is consistent since M_0 is a model of K_1. Let M_1 be any other model of K_1. Then M_1 is a real closed extension of a simple transcendental extension M_2 of M which is obtained from M by the adjunction of c. Moreover, according to (8.8), the inclusion of K_0 in K_1 ensures that the ordering of M_2 is the same as the ordering of M (c) i.e.

M_2 coincides with M(c). Now M_0 is algebraic over M(c) since $m_0 = 1$; so that by (8.11) it follows that there exists an order preserving isomorphism from the real closure M_2' of M_2 in M_1 onto M_0. That is M_2' is isomorphic to M_0 so that Y is satisfied by M_2'. Hence Y is also satisfied by M_1 since M_1 is an extension of M_2'.

We have thus shown that Y is satisfied by all models of K_1. It follows that Y is deducible from a finite subset of K_1 or, more particularly, there exist (individual) constants $a_1, \ldots a_j, a_{j+1}, \ldots a_\ell, a_{\ell+1}, \ldots a_p$ in M such that the sentence $V(c) \supset Y$ is deducible from $K_R \cup D(M)$ where V(c) is given by the identity:

$V(c) = Q(a_1, c) \wedge \ldots \wedge Q(a_j, c) \wedge Q(c, a_{j+1}) \wedge \ldots \wedge Q(c, a_\ell) \wedge \sim[a_{\ell+1} \doteq c] \wedge \ldots \wedge \sim[a_p \doteq c]$.

It follows by (2.6)-(g) that the sentence $X = [(Ex)V(x)] \supset Y$ is likewise deducible from $K_R \cup D(M)$. We now show that the sentence $X = (Ex)V(x)$ is satisfied by M.

In ordinary algebraic language we have to find a solution x in M to a system of inequalities:

$$(8.13) \qquad \begin{array}{ll} a_i < x & i = 1, \ldots j \\ a_i > x & i = j+1, \ldots \ell \\ a_i \neq x & i = \ell+1, \ldots p \end{array}$$

where it is known that the system possesses a solution $x = c$ in an extension M_2 of M. Since the inequalities $a_i \neq x$ are equivalent to disjunctions:

$$(a_i < x) \vee (a_i > x) \qquad i = \ell + 1, \ldots p$$

and since c satisfies at least one of the disjuncts in each case, but cannot satisfy the other, it follows that we may replace (8.13) by a system:

$$(8.14) \qquad \begin{array}{ll} a_i < x & i = 1, 2, \ldots j \\ a_i > x & i = j+1 \ldots p. \end{array}$$

One or the other of these two sets may be empty. If both are empty there is nothing to prove. If the second set is empty but not the first then (8.14) is satisfied in M by $x = \text{max. } a_i + 1$. If the first set is empty, but not the second then (8.14) is satisfied in M by $x = \text{min. } a_i - 1$.

Finally, if neither set is empty then (8.14) is staisfied in M by $x = \frac{1}{2}(a' + a'')$ where: $a' = \text{max. } a_i$, $1 \leq i \leq j$; and $a'' = \text{min } a_i$, $j \leq i \leq p$.

We note that $a' \leq a''$ since (8.14) is satisfied by c in M_2 and M_2 preserves the order of M.

In any case we have shown that the sentence X' is satisfied by M_1. Since the sentence $X = X' \supset Y$ is deducible from $K_R \cup D(M)$ it is likewise satisfied by M. It follows that Y is satisfied by M, which is a contradiction. This completes the proof of (8.12).

We now consider the question of completeness. We have shown earlier (see page 33) that the elementary theory of algebraically closed fields is not complete. However, let M be any algebraically closed field of characteristic zero. Then the prime field M_0 of M is isomorphic to the field R of rational numbers so that the field of algebraic numbers is isomorphic by (8.0) to the algebraic closure $\overline{M}_0$ of M_0. But the subfield M_1 of M consisting of all elements of M which are algebraic over M_0 is again algebraically closed so that M_1 is also isomorphic to $\overline{M}_0$ by (8.0). That is, M contains an algebraically closed subfield isomorphic to the field of all algebraic numbers (of characteristic 0). Similarly, every algebraically closed field of characteristic $p > 0$ contains an algebraically closed subfield isomorphic to the field of algebraic numbers of characteristic p. It follows by (5.12) that:

(8.15) The L-theory K* for the concept of an algebraically closed field of specified characteristic $p \geq 0$ (see(4.10) and 4.11) is complete.

Now let M be any real closed field. Then M has characteristic zero so that the prime field M_0 of M is isomorphic to R (above). Then the real closure M_0^* of M_0 is isomorphic by (8.10) to the field of real algebraic numbers. But by (8.11) the real closure of M_0 in M is also isomorphic to M_0^* so that M contains a real closed subfield isomorphic to the field of real algebraic numbers. It follows by (5.12) again that:

(8.16) The L-theory K_R for the concept of a real closed field is complete.

Hilbert's problem on definite forms (see Hilbert [1] p.p. 465 - 466) was originally solved by E. Artin by means of the concept of a formally real field. His result may be stated as follows:

(8.17) Theorem Let $f(x_1,\ldots x_n) = \frac{p(x_1,\ldots x_n)}{q(x_1,\ldots x_n)}$ be a rational function with coefficients in the field R of real numbers. Suppose that $f(a_1,\ldots a_n) \geq o$ for all real numbers $a_1,\ldots a_n$ for which $q(a_1,\ldots a_n) \neq o$. Then there exists rational functions $f_1,\ldots f_k$ with coefficients in R such that $f(x_1,\ldots x_n) = \sum_{i=1}^{k} (f_i(x_1,\ldots x_n))^2$.

Using the fact that the theory of real closed fields is model-complete we shall prove (8.17) in the more general case that the field R of coefficients (above) is any real closed field. We shall also require certain algebraic results which we introduce as follows:

(8.18) Let M be any field. A multiplicative subset C of the elements of M (i.e $a \in C$, $b \in C$ implies $ab \in C$) which includes the unit element 1 but does not include o will be called a core of M.

For example the set $\{1\}$, consisting of the unit element of M alone is a core of M. Again, the set consisting of all the positive elements of any ordered subfield M of M, is a core of M.

(8.19) Let M be any field with core C. M is said to be formally real with respect to C if for any $a_1,\ldots a_n \in C$; $b_1,\ldots b_n \in M$ we have:

$$\sum_{i=1}^{n} a_i (b_i)^2 = o$$

only if each $b_i = o$ $\quad i = 1, 2, \ldots n$.

We observe that for $C = \{1\}$ this definition reduces to that of (8.5). Also, if M is formally real with respect to a core C then any subfield M_o of M is likewise formally real with respect to C.

(8.20) Let M be a formally real field. A set J of elements of M is called a pseudo-ideal if it satisfies the following conditions:

(i) J is a semi-module. That is, for any $a \in J$, $b \in J$ we also have $a + b \in J$ and $ab \in J$.

(ii) The square of every element of M, other than o, belongs to J.

(iii) 0 does not belong to J.

We note that the set of pseudo ideals in M is not empty. For example, the set of all finite sums $b_1^2 + b_2^2 + \ldots + b_k^2$, where $k \geq 1$; $b_j \neq o$ $j = 1,2,\ldots k$ is a pseudo ideal. More generally, if M is formally real with respect to a given core C then the set of all finite sums $a_1 b_1^2 + a_2 b_2^2 + \ldots + a_k b_k^2$, $k \geq 1$, $b_j \neq o$, $a_j \in C$, $j = 1,\ldots k$ is a pseudo ideal.

(8.21) Let J be a pseudo-ideal in a field M and let $a \neq o$ be an element of M such that $(-a)$ does not belong to J. Then there exists a pseudo-ideal J* which contains the element a such that $J \subseteq J^*$.

Proof: Let J and a satisfy the conditions of (8.21) and let J* be the set of all finite sums $-a_1 a^{j_1} + a_2 a^{j_2} + \ldots + a_k a^{j_k}$ where $k \geq 1$, $a_m \in J$ and j_m is a non-negative integer ; $m = 1,2, \ldots k$. It is easily seen that J* is a semi module such that $J \cup \{a\} \subseteq J^*$ and hence J* also satisfies (8.20)-(ii).

Suppose now that $o \in J^*$. Then there exists an identity $a_1 a^{j_1} + a_2 a^{j_2} + \ldots + a_k a^{j_k} = o$ where $k \geq 1$, and the a_i, j_i are defined as above.

We may number the indices of a in the above identity in such a way that j_m is even for $m = 1,\ldots \ell$ while j_m is odd for $m = \ell + 1,\ldots k$. There must be both even and odd j_m, for if the powers of a were all even then $\sum_{i=1}^{k} a_i a^{j_i}$ would belong to J (which is impossible since $o \notin J$); while if the j_m were all odd then we would have

$$-\left(\sum_{i=1}^{k} a_i a^{j_i}\right) = (-a) \sum_{i=1}^{k} a_i a^{j_i - 1} = o.$$

This implies that $\sum_{i=1}^{k} a_i a^{j_i - 1} = o$ which is likewise impossible since the $j_i - 1$ are now all even.

Accordingly we put-

$b = \sum_{i=1}^{l} a_i \, a^{j_i} \quad c = \sum_{i=l+1}^{k} a_i \, a^{j_i}$

Then $b \in J$ and so $b \neq o$. Our identity is now of the form $b + ac = o$ and furthermore we have:

$-a = c/b = cb/b^2 = ba_{l+1}(a^{p_{l+1}}/b)^2 + \ldots + ba_k (a^{p_k}/b)^2$ where

$p_m = \frac{1}{2}(j_m - 1)$ $m = l+1, \ldots k.$

We observe that the p_m are all integers. Accordingly, the representation of $-a$ as above shows that $-a \in J$. But this is contrary to assumption, and shows that the original identity cannot exist. It follows that J^* satisfies all the requirements of (8.21).

A pseudo-ideal J in M is said to be <u>maximal</u> if there does not exist any pseudo ideal in M which includes J as a proper subset.

(8.22) In order that a pseudo ideal J in M be maximal it is necessary and sufficient that for every element $a \neq o$ of M either $a \in J$ or $-a \in J$.

<u>Proof:</u> Suppose that for some element $a \neq o$ of M the pseudo ideal J includes neither a nor -a. Then by (8.21) there exists a pseudo ideal J^* which includes a such that $J \subseteq J^*$. Also $J^* \neq J$ since J does not include a. Thus J cannot be maximal, and the condition is necessary.

Now suppose that J satisfies the condition of (8.22), but that there exists another pseudo ideal J^* which includes J as a proper subset. Select any $b \in J^* - J$. Then $b \notin J$ and so $-b \in J$. Hence $-b \in J^*$. But if so, then $o = b + (-b)$ would also belong to J^* which is impossible. This proves that the condition of (8.22) is also sufficient.

It is not difficult to verify that the union of a monotonic set of pseudo ideals is again a pseudo ideal. Hence by Zorn's lemma, every pseudo ideal is included in a maximal pseudo ideal. More precisely, we may state the following:

(8.23) Let J be a pseudo ideal in the field M and let $a \neq o$ be

an element of M which does not belong to J. Then there exists a maximal pseudo ideal which includes J and -a (and hence does not include a).

Proof: By (8.21) J is contained in a pseudo ideal J* which includes -a, and J* in turn, is included in a maximal pseudo ideal.

(8.24) Now suppose that M is an ordered field, and let J be the set of all positive elements of M. Clearly, J is a pseudo ideal. Also the condition of (8.22) is satisfied so that J is a maximal pseudo ideal. Conversely, if J is a maximal pseudo ideal in the field M, then an ordering of M is defined by putting $a > o$ for all $a \in J$.

(8.25) Let M be a field with core C. An element a M is said to be totally positive with respect to C if a is non-negative for all orderings of M for which the elements of C are all positive. (a is totally positive if it is totally positive with respect to the core $C = \{1\}$, i.e. if a is non-negative for all orderings of M).

(8.26) Theorem: Let M be a formally real field with core C. Then every element $a \in M$ which is totally positive with respect to C can be represented in the form:

$a = a_1 b_1^2 + \ldots + a_u b_u^2$ where $a_j \in C$; $b_j \neq o$ $j = 1,2,\ldots n$.

Proof: The set of all elements of the form $a_1 b_1^2 + \ldots + a_u b_u^2$ where $a_j \in C$ $b_j \neq o$ constitute a pseudo ideal J of M. If $a \notin J$ then there exists by (8.23) a maximal pseudo ideal J' which contains J and -a. It follows by (8.24) that there exists an ordering of M for which the elements of C are all positive as well as -a (since $C \cup \{a\} \subseteq J$). It follows that a is not totally positive with respect to C. This proves (8.26).

We mention at this point that the above result was also proved by A. Robinson (see Robinson [8] page 264) using a metamathematical argument.

We require the following lemma (see Van Der Waerden [1]:
(8.27) A real closed field R can be ordered in one and only one way; namely-an element c is positive if and only if c is a non zero square.

As a corollary to (8.26) in conjunction with (8.18) and (8.27) we have:
(8.28) Let M be any field which contains a real closed (ordered) subfield, R. Suppose that M is formally real with respect to the positive elements of R; that is the identity $\sum_{i=1}^{n} r_i a_i^2 = 0$ where $r_i \in R, r_i > 0$ can hold only if $a_i = 0$ for all i, $i = 1,2,\ldots n$. Let c be any element of M which is non-negative for every ordering of M which preserves the ordering of R. Then there exists an identity $c = \sum_{i=1}^{k} a_i^2$ where $a_i \in M$, $k \geq 1$.

Now let M be the field of rational functions in $n \geq 1$ indeterminates with coefficients in a real closed field R. Let $f(x_1,\ldots x_n) = \frac{p(x_1,\ldots x_n)}{q(x_1,\ldots x_n)}$ belong to M such that f satisfies the conditions of (8.17); that is $f(a_1,\ldots a_n) \geq 0$ for all $a_1,\ldots a_n \in R$ for which $q(a_1 \ldots a_n) \neq 0$. If there does not exist an identity of the form: $f(x_1 \ldots x_n) = \sum_i \left(f_i(x_1,\ldots x_n)\right)^2$ in M then it follows by (8.28) that there exists an ordering of M which preserves the ordering of R such that $f(x_1,\ldots x_n) < 0$. Now by (8.10) M may be embedded in a real closed (ordered) field R* whose ordering preserves the ordering of M, and hence $f(x_1 \ldots x_n) < 0$ in R*.

Let X be a sentence in L which is defined in R and which asserts in ordinary algebraic language that: "There exist elements $y_1,\ldots y_n$ such that $f(y_1,\ldots y_n) < 0$" (Such a sentence is easily formulated as a predicate $Q(a_1,\ldots a_k)$ of the coefficients $a_1,\ldots a_k$ of f taken in some arbitrary but fixed order.).

Clearly X is satisfied by R*. (It suffices to choose for the y_i, the indeterminates x_i themselves $i = 1,2,\ldots n$.) Since the L-theory K_R for the concept of a real closed field is model-

complete, and since the sentence X above is primitive, it follows by (7.2) that X is already satisfied by R. In other words, there exists elements $b_1, \ldots b_n \in R$ such that $f(b_1, \ldots b_n) < o$, where we note that the element $f(b_1, \ldots b_n)$ now belongs to R. This contradicts the assumption of (8.17) above. Thus, we have established (8.17) in the general case that R is any real closed field.

The above result was also proved by Robinson as a corollary to a more general result (Theorem (4.9) of Robinson [8]). The argument used is independent of the embedding theorem (8.10) for real closed fields; and involves in addition to (8.26) and the model-completeness of K_R only certain algebraic concepts such as "definite" and "totally definite" functions (and the fact that these concepts can be formalized in the language L). Other interesting results on the representation of rational functions are also obtained. For these, we refer the reader to Robinson [8]. Finally we prove:

(8.29) Let $f(x_1, \ldots x_n) = \frac{p(x_1, \ldots x_n)}{q(x_1, \ldots x_n)}$ be a given rational function of degree m in $n \geq 1$ indeterminates over a real closed field R. Suppose that $f(a_1, \ldots a_n) \geq o$ for every n-tuple $a_1, \ldots a_n \in R$ for which $q(a_1, \ldots a_n) \neq o$. Then there exists positive integers λ and μ which depend only on m and n and not on the coefficients of f such that the identity $f = \sum_{i=1}^{\ell} (f_i)^2$ is satisfied for a number $\ell \leq \lambda$ of rational functions such that the degrees of their numerators and denominators do not exceed μ.

Proof: We observe first of all that the condition:
"There exist rational functions f such that the identity $f = \sum (f_i)^2$ is satisfied".
may be regarded as a property of $y_1, \ldots y_s$ where $y_1, \ldots y_s$ are the coefficients of f (regarded as variables) arranged in an arbitrary but definite order; but in this form, the property cannot be expressed as a predicate $Q(y_1, \ldots y_s)$ in the language L. However, some reflection shows, that the assertion that

an identity $f = \sum (f_i)^2$ exists with a specified upper bound λ on the number of summands required, and a specified upper bound μ on the degrees of the numerators and denominators of the functions f_i can be formalized as a predicate of the coefficients $y_1, \ldots y_s$. (We observe that a formalization of the identity above for a fixed number of summands and where the degrees of the numerators and denominators of the f_i are likewise fixed is easily obtained since the coefficients of the f_i are then uniquely determined by equations involving only the rational operations in R and the coefficients $y_1, \ldots y_s$ of f; and, by our assumption, there are only a finite number of cases to consider.) In other words, for every assigned pair of positive integers λ and μ we may formalize in L a predicate $Q_{\lambda\mu}(y_1, \ldots y_s)$ which asserts that: "There exist $m \leq \lambda$ rational functions $f_1, f_2, \ldots f_m$ whose degrees do not exceed μ, such that the identity $f = \sum_{i=1}^{m} (f_i)^2$ is satisfied."

For any set $a_1, \ldots a_s$ of individual constants which do not occur in the set K_R let K_1 be the infinite set of sentences given by:

$K_1 = \{\sim Q_{\lambda_1\mu_1}(a_1, \ldots a_s), \sim Q_{\lambda_2\mu_2}(a_1, \ldots a_s), \ldots\}$ where the λ_i, μ_i, range through all positive integers. Furthermore, let $S(y_1, \ldots y_s)$ be the sentence (or predicate of the coefficients) in L which asserts that $f(c_1, \ldots c_n) \geq 0$ for all $c_1, \ldots c_n$ for which $q(c_1, \ldots c_n) \neq 0$.

Let $K = K_1 \cup K_R \cup \{S(a_1, \ldots a_s)\}$. If K is consistent, then K possesses a model R by (3.9). R is then a real closed field such that the rational function $f(x_1, \ldots x_n)$ with coefficients $a_1, \ldots a_s \in R$ is never negative over R but f does not have a representation of the form $f = \sum (f_i)^2$. This contradicts (8.17) and shows that K is contradictory.

It follows by (1.7) and (2.14) that there exists a finite set of positive integers:

$\lambda_{j_1} < \ldots < \lambda_{j_k}$, $\mu_{j_1} < \ldots < \mu_{j_k}$ $(k \geq 1)$ such that the sentence:

$S(a_1, \ldots a_s) \supset [Q_{\lambda_{j_1}\mu_{j_1}}(a_1, \ldots a_s) \vee \ldots \vee Q_{\lambda_{j_k}\mu_{j_k}}(a_1, \ldots a_s)]$

is deducible from K_R. But the sentence-

$Q_{\lambda_{j_k}\mu_{j_i}}(a_1,\ldots a_s) \supset Q_{\lambda_{j_k}\mu_{j_k}}(a_1,\ldots a_s)$

is deducible from K_R, for all $i<k$. It follows that the sentence:

$S(a_1,\ldots a_s) \supset Q_{\lambda_{j_k}\mu_{j_k}}(a_1,\ldots a_s)$

is deducible from K_R. Since the constants $a_1,\ldots a_s$ do not occur in K_R it follows that the sentence:

(8.30) $(y_1),\ldots(y_s)\left[S(y_1,\ldots y_s) \supset Q_{\lambda_{j_k}\mu_{j_k}}(y_1,\ldots y_s)\right]$

is likewise deducible from K_R. Interpreting (8.30) semantically, we obtain a proof of (8.29).

Thus we have proven the existence of upper bounds for the number and degrees of the summands required to represent any "positive" rational function f as a sum of squares as in (8.17). These bounds are independent of the particular (real closed) field R of coefficients of f.

Chapter 9 Relative Model-Completeness

In subsequent chapters of this paper we shall require a generalization or relativisation of the notion of model-completeness. This latter notion - called relative model-completeness, will be introduced in this chapter.

Let K and K* be two non-empty and consistent sets of sentences in L.

(9.0) K* is said to be model-consistent relative to K if the set $K^* \cup D(M)$ is consistent for every model M of K. By (5.7) and (3.9) an equivalent semantic condition is that every model M of K can be embedded in (i.e possesses an extension which is) a model of K*.

(9.1) K* is said to be associated with K if (every sentence of) K is deducible from the set $K^* \cup D(M)$ for any model M of K. By (3.12) and (5.7) an equivalent condition is that - every model of K* which is an extension of a model of K is itself a model of K.

We observe that K* is associated with K if K is a subset of K* or if K is deducible from K*; while every non-empty and consistent set K is associated with and is model consistent relative to itself.

(9.2) Let K and K* be two non empty sets of sentences such that K is consistent and K* is model consistent relative to K. K* is said to be model-complete relative to K if the set $K^* \cup D(M)$ is complete for every model M of K. For $K^* = K$ this definition reduces to that of ordinary model completeness (see 5.8).

The following test for relative model-completeness is a generalization of the test for ordinary model completeness given by (7.2):

(9.3) Theorem: Let K and K* be two non-empty and consistent sets of sentences such that:

(i) Every sentence of K* is defined in K.

(ii) K* is model consistent relative to K.

(iii) K* is associated with K.

In order that K* be model-complete felative to K it is necessary and sufficient that for every model M of K every primitive sentence X which is defined in M is decidable in the set $K^* \cup D(M)$.

Proof: It is clear that the condition of the theorem is necessary; while a proof of sufficiency is obtained by a simple generalization of the argument of (7.3) using the fact that by (9.1) and our assumption, every model M* of $K^* \cup D(M)$ is also a model of K.

Instead of applying the above test directly, it is found convenient in certain cases to estaolish relative model-completeness by means of known instances of ordinary model-complete ess. This can be achieved by means of the following theorem:

(9.4) Theorem: Let K and K* be two non-empty sets of sentences such that K is consistent, K* is model-complete, and K* is model-consistent relative to K. Suppose further that for every model M of K the set $K^* \cup D(M)$ possesses a prime model (see 5.11). Then K* is model complete relative to K.

Proof: Suppose that the hypothesis of (9.4) is satisfied. For a given model M of K, let M_o^* be a prime model of $K^* \cup D(M)$, and let X be any sentence which is defined in M_o^*. Since K* is model-complete either X or $\sim X$ is deducible from the set $K^* \cup D(M_o^*)$. It will be sufficient to consider the former case.

By (5.6) $K^* \cup D(M_o^*)$ contains in addition to $K^* \cup D(M)$ only certain atomic sentences and their negations. We may therefore conclude that there exists a conjunction $W(b_1, \ldots b_u)$ of a finite number of these such that the sentence $W(b_1, \ldots b_u) \supset X$ is deducible from $K^* \cup D(M)$; where $b_1, \ldots b_u$ denote the individual constants which occur in W but do not belong to M.

It follows by (2.6)-(g) that the sentence:
$[(Ex_1)\ldots(Ex_u)W(x_1,\ldots x_u)] \supset X$ is likewise deducible from $K^* \cup D(M)$.

Now let M^* be any model of $K^* \cup D(M)$. Then M^* contains a subsystem M_1^* which is isomorphic to M_0^*. It follows that the sentence $Y = (Ex_1)\ldots(Ex_u)\ W\ (x_1,\ldots x_u)$ is satisfied by M_1^* (since it is satisfied by M_0^*). But Y is existential and so by (6.1) is satisfied by all extensions of M^* and in particular by M^* It follows by (3.12) that Y is deducible from $K^* \cup D(M)$ and hence by (2.6)-(b) so is X. This completes the proof of (9.4)

The following examples will clarify these notions. They will also be useful in the sequel.

(9.5) Let K be a set of axioms for the concept of an integral domain (with distince o and 1). Then K can be enlarged to yield a set of axioms K^* for the concept of an algebraically closed field (without introducing any new extralogical symbols) by (4.10). It is then clear that K^* is model-consistent relative to K since every integral domain M can be embedded in the algebraic closure M_c^* of its field of quotients. Also K^* is obviously associated with K (see remark following (9.1)) and K^* is model-complete by (8.1).

Now let M be any model of K i.e any integral domain, It is clear that M_c^* (above) is a prime model of the set $K^* \cup D(M)$. Thus the hypothesis of (9.4) is satisfied and we conclude that K^* is model complete relative to K.

(9.6) Again let K_f be a set of axioms for the concept of a field, and let K_p be a set of axioms for the concept of a field of given characteristic $p \geq o$ (see 4.11). Let K_F^* and K_p^* be the corresponding sets which assert in addition that the field is algebraically closed. Then by (8.1), again, both K_f^* and K_p^* are model-complete.

Clearly K_F^* is associated with and is model consistent relative to both K_f and K_p (although K_p is not a subset of K_F^* nor is K_p deducible from K_F^*). Likewise K_p^* is associated with and is model consistent relative to K_p although K_p^* is not model

consistent relative to K_f. We may conclude as before that K_f^* is model-complete relative to K_f and K_p; and K_p^* is model-complete relative to K_p.

(9.7) Let R_o be a set of axioms for the concept of a commutative ordered ring in which o and 1 are distinct (see 4.12) and let K_R be a set of axioms for the concept of a real closed (ordered) field containing the same extralogical symbols as R_o. Then K_R is model-complete by (8.12).

Let M be any model of R_o. Then M is an integral domain (since it is an ordered ring) and therefore can be extended to its field of quotients and further to the real closure M_o of that field. It is clear then that M_o is a prime model of the set $K_R \cup D(M)$. It follows that all conditions of (9.4) are satisfied so that K_R is model-complete relative to R_o. In particular we have:

(9.8) The set K_R is model complete relative to the set K_c of axioms for the concept of an ordered field. We now prove:

(9.9) If a set K* is model-complete relative to K and if (every sentence of) K is deducible from and defined in K*, then K* is model complete in the absolute sense.

Proof: By (3.12) and our assumption every model of K* is a model of K. Now $K^* \cup D(M)$ is complete for every model M of K so that $K^* \cup D(M^*)$ is complete for every model M* of K* ; i.e K* is model-complete.

(9.10) Let K, K_1^* , K_2^* be three non-empty and consistent sets of sentences such that both K_1^* and K_2^* are:

(i) defined in K and model consistent relative to K.

(ii) associated with K

(iii) model complete relative to K.

Then the class of models of K_1^* which are extensions of models of K coincides with the class of models of K_2^* which are extensions of models of K.

Proof: By (3.12) and (5.7) the conclusion of (9.10) is equivalent

to the assertion that for any given model M of K, K_1^* is deducible from $K_2^* \cup D(M)$ and K_2^* is deducible from $K_1^* \cup D(M)$. Accordingly, we only have to show that if a sentence X which is defined in M is deducible from $K_1^* \cup D(M)$ then it is also deducible from $K_2^* \cup D(M)$. In view of the relative model-completeness of K_1^* and K_2^* the alternative assumption is that for some model M of K and for some sentence X which is defined in M, X is deducible from $K_1^* \cup D(M)$ and $\sim X$ is deducible from $K_2^* \cup D(M)$. If so, there exist sentences X of this kind which are in prenex normal form and we may suppose, as in the proof of (7.3), that the number of quantifiers in X is a minimum and that X begins with an existential quantifier; $X = (Ez)\ V(z)$.

Suppose then that X is deducible from $K_1^* \cup D(M)$ while $\sim X$ is deducible from $K_2^* \cup D(M)$. Let M_1^* be a model of $K_1^* \cup D(M)$. Then X is satisfied by M_1^* and so M_1^* contains a constant b such that V(b) is satisfied by M_1^*. But M_1^* is also a model of K(since K* is associated with K) and so the set $K_1^* \cup D(M_1^*)$ is complete. Consequently V(b) is deducible from $K_1^* \cup D(M_1^*)$. It then follows from the minimal property of X and the relative model-completeness of K* that V(b) must be deducible also from $K_2^* \cup D(M_1^*)$. This entails that $X = (Ez)V(z)$ is deducible from $K_2^* \cup D(M_1^*)$. On the other hand since $D(M) \subseteq D(M^*)$, and since $\sim X$ is supposed to be deducible from $K_2^* \cup D(M)$, $\sim X$ must be deducible, a fortiori, from the set $K_2^* \cup D(M_1^*)$. This shows that the set $K_2^* \cup D(M_1^*)$ is contradictory. This is impossible since K_2^* is model consistent relative to K. Thus (9.10) is proved.

... (9.10) shows, for example, that the class of all algebraically closed fields occupies a unique model-theoretic position relative to the class of all fields. A similar remark applies to the class of all real closed (ordered) fields relative to the class of all (ordered) fields.

Chapter 10 Some Problems of Definability in L.

Let us consider the following algebraic results (see Van Der Waerden [1] pp. 219-221):

(10.0) Let $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ be any polynomial with coefficients in an ordered field K. Let m be the larger of the two elements 1 and $|a_1| + \ldots + |a_n|$ where the absolute value $|a|$ of an element $a \in K$ is defined as the non-negative one of the elements a, -a. Then $f(s) > 0$ for $s < m$ and $(-1)^n f(s) > 0$ for $s < -m$. In other words, if f(x) has roots in K they lie within the range $-m \leq x \leq m$.

(10.1) Sturm's Theorem: Let $X = p(x)$ be a polynomial over the field of real numbers. Let the polynomials $X_1, X_2 \ldots X_r$ be determined as follows:

$$X_1 = p'(x) \text{ (differentiation)}$$
$$X = Q_1 X_1 - X_2$$
$$X = Q_2 X_2 - X_3 \text{ (Euclidean algorithm)}$$
$$\ldots\ldots\ldots\ldots$$
$$X_{r-1} = Q_r X_r$$

For every real number a which is not a root of f(x) let $\varphi(a)$ be the number of variations in sign in the number sequence $X(a), X_1(a), \ldots X_r(a)$ in which all zeros are omitted. If b and c are any real numbers ($b < c$) for which f(x) does not vanish then the number of distinct real roots in the interval $b \leq x \leq c$ is equal to $\varphi(b) - \varphi(a)$.

Now let $p(x) = y_0 + y_1 x + \ldots + y_n x^n$ be a polynomial in the indeterminate x where the y_i are parameters in the field R of rational numbers. Then the property of p(x) of possessing (or not possessing) a real root may be regarded as a predicate of its coefficients, say $Q^*(y_0, \ldots y_n)$. As stated this predicate is formulated with reference to the more comprehensive field R* of real (or real algebraic) numbers.

However (10.0) and (10.1) show that there exists a predicate $Q(y_0, \ldots y_n)$ formulated in L in terms of the functors Γ and Π and the relations

Q and $\mp$ such that whenever Q $(y_0,\ldots y_n)$ holds in R for rational $y_0,\ldots y_n$ then Q* $(y_0,\ldots y_n)$ holds in R* and conversely whenever Q*$(y_0,\ldots y_n)$ holds in R* for rational $y_0,\ldots y_n$ then Q$(y_0,\ldots y_n)$ holds in R. (We note that the condition $\varphi(-m) - \varphi(m) \geq 1$ where m is defined by (10.0) can be formalized as a predicate of $y_0,\ldots y_n$ since there are only a finite number of cases to consider.) Instead of considering such a situation for two particular systems R and R* as above we shall be concerned in this chapter with predicates Q and Q* which are defined with respect to two different sets of axioms K and K* related in a manner similar to the above.

Let K and K* be two consistent sets of sentences:

(10.2) A predicate Q* $(x_1,\ldots x_n)$ $n \geq o$ which is partially defined in K is said to be <u>persistent with respect to K* over K</u> if, for any set $a_1,\ldots a_n$ of constants which belong to a given model M of K the sentence Q* $(a_1,\ldots a_n)$ can be satisfied by M only if it is satisfied by all models of K* which are extensions of M (compare (6.0)

(10.3) A predicate Q* $(x_1,\ldots x_n)$ $n \geq o$ which is defined in K is said to be <u>invariant with respect to K* over K</u> if both Q* and $\sim$Q* are persistent with respect to K* over K; or equivalently, if for any set $a_1,\ldots a_n$ of constants which belong to a given model M of K the sentence Q*$(a_1,\ldots a_n)$ is either satisfied by <u>all</u> models of K* which are extensions of M, or it is satisfied by none.

(10.4) In particular, a sentence X* which is defined in K is invariant with respect to K* over K if for any given model M of K, X* is satisfied either by all models of K* which are extensions of M, or by none.

(10.5) Let M be a given mathematical system and let R be a given unary relation which does not belong to M. If we adjoin R to M we may define a new system M by postulating in addition that R(a) hold for all constants $a \in M$. A quick glance at (2.19) shows that if X is satisfied by M, then X_R is satisfied by M_R where X_R is the relativised transform of X with respect to R. Conversely, if X is

defined in M for given X and M, and if X_R is satisfied by M_R then X is satisfied by M.

(10.6) Moreover, let M* be any extension of M which does not include R and let the system $\overline{M}_R$ be obtained by adjoining R to M* and by postulating in addition that R(a) holds in $\overline{M}_R$ for all constants $a \in M$ while R(a) does not hold in $\overline{M}_R$ for any constant $a \in \overline{M}$ which does not belong to M. Then a sentence X which is defined in M can be satisfied by M if and only if X_R is satisfied by $\overline{M}_R$. We now prove:

(10.7) Theorem: Let K and K* be two non-empty and consistent sets of sentences such that K* is defined in K and K* is model consistent relative to K. Let X* be a sentence which is defined in K* and which is invariant with respect to K* over K. Then there exists a sentence X which is defined in K such that X is satisfied by a given model M of K if and only if X* is satisfied by all models of K* which are extensions of M.

Proof: For given K, K* and X* which satisfy the conditions of the theorem let R be a given one place relation symbol which does not occur in K (and hence does not occur in K* or in X* either). Suppose that we can find a sentence X which is defined in K such that the equivalence $[X^* \equiv X_R]$ is deducible from $K_R \cup K^*$ where K_R is given by (2.21). Let M and M* be models of K and K* respectively such that $M \subseteq M^*$. Define $\overline{M}_R$ as in (10.6). Then $\overline{M}_R$ is a model of K*. Also $\overline{M}_R$ is a model of K_R by (10.6).

Now suppose that X* is satisfied by M*. It follows that X* is satisfied also by $\overline{M}_R$. Since the sentence $X^* \equiv X_R$ is deducible from $K^* \cup K_R$ we conclude by (3.5) and (3.12) that X_R is also also satisfied by $\overline{M}_R$ and hence by (10.6) X is satisfied by M. A similar argument shows tnat if $\sim X^*$ is satisfied by M* then $\sim X$ is satisfied by M. Thus, in order to prove (10.7) we only have to find a sentence X which is defined in K such that $X^* \equiv X_R$ is deducible from $K^* \cup K_R$

Let P be the set of all sentences X which are defined in K and such that the sentence $X^* \supset X_R$ is deducible from $K^* \cup K_R$ P is

non-empty as, by (2.21), all provable sentences which are defined in K belong to P. Also (2.19) together with (1.5) - (b) implies that P is conjunctive (see 2.25)

Let $P_R = \{X_R \mid X \in P\}$ and consider the set $S = K^* \cup K_R \cup P_R \cup \{\sim X^*\}$. Suppose first that this set is consistent and hence by (3.9) that is possesses a model M'. Then M' is a model of K^*. Also the constants $a \in M'$ such that $R(a)$ holds in M' (together with the relations and functions of M') constitute a model M of K ; and if we delete the relation R from M' we obtain by (10.5) a model M of K. Now the diagram $D(M_R)$ is obtained from $D(M)$ by adjoining to $D(M)$ the atomic sentences $R(a)$ for all constants $a \in M$. The set $S' = K^* \cup K_R \cup D(M_R)$ is consistent since M' is a model of S'. We propose to show that $\sim X^*$ must be deducible from S'.

Suppose on the contrary that $\sim X^*$ is not deducible from S'. Then by (1.7) it follows that the set $S' \cup \{X^*\} = K^* \cup K_R \cup D(M_R) \cup \{X^*\}$ is consistent and hence possesses a model M''. M'' is a model of $D(M_R)$ and hence $M \subseteq M''$. That is M'' is an extension of M which satisfies X^* while M' is an extension of M which satisfies $\sim X^*$. The same still applies if we remove the relation R from both M' and M'' although the resultant sets are both models of K^*. This is contrary to the assumption that X^* is invariant with respect to K^* over K and proves that $\sim X^*$ must be deducible from S'.

We conclude by (2.6) -(a) that there exists a sentence Y which is a conjunction of a finite number of elements of $D(M_R)$ such that the sentence $Y \supset \sim X^*$ and with it $X^* \supset \sim Y$ is deducible from $K^* \cup K_R$. Now the conjuncts of Y are either of the form $R(a)$, $a \in M$ or they are atomic sentences which are given in terms of the constants and relations of M, or the negations of such sentences. We may write Y as a disjunction or again as an implication of the form- $[R(a_1) \wedge \ldots \wedge R(a_u)] \supset Z$ where Z is a disjunction of atomic sentences of the type just described

and (or) of the negations of such sentences. Moreover by adding if necessary, suitable elements of $D(M_R)$ to the original Y we may ensure that the constants contained in Z are precisely $a_1, \ldots a_n$; i.e. $Z = Z(a_1 \ldots a_n)$. Then the sentence $X^* \supset [R(a_1) \wedge \ldots \wedge R(a_u) \supset Z]$ is deducible from $K^* \cup K_R$. Furthermore, the conjunction $R(a_1) \wedge \ldots \wedge R(a_n)$ may be shortened (if necessary) by omitting from it all sentences $R(a_j)$ such that a_j occurs in K, for these sentences are already included in K_R (see 2.21) Suppose that this applies for $j = m+1, \ldots n$. Then the sentence $X^* \supset [R(a_1) \wedge \ldots \wedge R(a_m) \supset Z]$ is deducible from $K^* \cup K_R$. (If m =o we omit the conjunction and the sign of implication which follows it.) Since $a_1, \ldots a_u$ are (individual) constants which are not included in either K^*, K_R or X^* it follows that the sentence:

$X^* \supset [(x_1) \ldots (x_u) [R(x_1) \wedge \ldots \wedge R(x_m) \supset Z(x_1, \ldots x_u, a_{m+1} \ldots a_u)]]$

is deducible from $K^* \cup K_R$ by (2.6)-(f).

Hence by (2.16) the sencence $X^* \supset V$ is likewise deducible from $K^* \cup K_R$ where:

$V = (x_1) [R(x_1) \supset [(x_2) R(x_2) \supset \ldots \supset [R(x_u) \supset Z]] \ldots]$. But v is the relativised transform of the sentence W which is defined by the identity: $W = (x_1) \ldots (x_u) Z(x_1, \ldots x_m, a_{m+1} \ldots a_n)$ i.e $V = W_R$ and W is defined in K. We have therefore shown that $W \in P$, by definition of P, and $V \in P_R$. But M' is a model of P_R so that M satisfies V. We infer that M satisfies at the same time the sentence-

$[R(a_1) \wedge \ldots \wedge R(a_n) \supset Z(a_1 \ldots a_m, a_{m+1}, \ldots a_n)]$. Now $[R(a_1) \wedge \ldots \wedge R(a_u)]$ is satisfied by M' and so $Z(a_1, \ldots a_u)$ is likewise satisfied by M'. On the other hand, Z is by definition a disjunction of atomic sentences whose negations hold in M, (and hence in M') and (or) of the negations of such sentences if the sentences themselves hold in M (and hence in M'). It follows that M' satisfies $\sim Z$ and this contradicts the result just obtained.

We conclude that M' cannot exist; that is, the set $S = K^* \cup K_R \cup P_R \cup \{\sim X^*\}$ is contradictory. It follows by (1.7) that there exists a finite conjunction of elements of P_R and, more particularly, since P is conjunctive, a single element X_R of P such that $X_R \supset X^*$ is deducible from $K^* \cup K_R$. But at the same time $X^* \supset X_R$ is deducible from $K^* \cup K_R$ by the defining property of P. Hence by (1.5)-(b) the sentence $X^* \equiv X_R$ is deducible from $K^* \cup K_R$.

This completes the proof of (10.7).

We now consider the corresponding problem for predicates in general:

(10.8) Theorem: Let K and K* be two non-empty and consistent sets of sentences such that K* is defined in K and K* is a model consistent relative to K. Let $Q^*(x_1, \ldots x_u)$ $n \geq o$ be a predicate which is defined in K* and which is invariant with respect to K* over K. Then there exists a predicate $Q(x_1, \ldots x_n)$ which is defined in K such that for any model M of K containing constants $a_1, \ldots a_n$, the sentence $Q(a_1, \ldots a_u)$ is satisfied by M if and only if $Q^*(a_1, \ldots a_u)$ is satisfied by all models of K* which are extensions of M.

Proof: Let $b_1, \ldots b_n$ be a set of individual constants which do not occur in K (and hence do not occur in K*). We adjoin these constants to K and K* obtaining sets K_o and K_o^* respectively (That is, we adjoin to K and K* provable sentences which involve $b_1, \ldots b_n$). We thus ensure that the sentence $X^* = Q(b_1, \ldots b_n)$ is defined in K .

We claim that X* is invariant with respect to K_o^* over K_o. Indeed let M be any model of K_o (and hence of K) and let M_1^*, M_2^* be two models of K_o^* (and hence of K*) Then the constants $b_1, \ldots b_u$ occur in all three systems. Now $Q^*(x_1, \ldots x_u)$ is invariant with respect to K* over K, and hence so is $Q^*(b_1, \ldots b_n) = X^*$. Applying (10.7) we find that there exists a sentence X which is defined in K_o such that X is satisfied by any model M

of K_o if and only if X* is satisfied by all models of K_c^* which are extensions of M. Moreover we may assume that X includes the constants $b_1, \ldots b_n$ effectively for if this is not the case a priori, we only have to conjoin a number of provable sentences to X which do contain these constants. Accordingly we may write $X = Q(b_1, \ldots b_n)$. We propose to show that the predicate $Q(x_1, \ldots x_n)$ satisfies the conclusion of (10.8).

Let M be any model of K and let $a_1, \ldots a_n$ be a set of constants of M. Also, let M* be an extension of M which is a model of K*. We note that the predicate $Q(x_1, \ldots x_n)$ is independent of the choice of the b_i (except that these constants must not be included in K or K*.) Accordingly we may assume in addition that the b_i are not included in M or M* either. We now enlarge the system M by adding the constants $b_1, \ldots b_n$ and we define that in the enlarged structure M_c a relation involving any of the b_i shall hold in M_o precisely if the relation obtained from it after replacing the b_i by the corresponding a_i holds in M. The system M_o^* is defined in a similar manner. Then M_o is a model of K_o and M_o^* is a model of K_o^*.

Suppose that $Q^*(a_1, \ldots a_\mu)$ is satisfied by M*. Then the semantic interpretation of this fact, shows that $X^* = Q^*(b_1, \ldots b_n)$ is satisfied by M_o^*. It follows that $X = Q(b_1 \ldots b_\mu)$ is satisfied by M_o and hence that $Q(a_1, \ldots a_n)$ is satisfied by M. Similarly if $\sim Q^*(a_1 \ldots a_\mu)$ is satisfied by M* then $\sim Q(a_1, \ldots a_\mu)$ is satisfied by M. This establishes the theorem.

(10.9) We note that the predicate Q whose existence is affirmed by (10.8) is by necessity persistent with respect to K. For let $a_1, \ldots a_n$ be any constants which belong to a model M of K and such that $Q(a_1, \ldots a_n)$ is satisfied by M. It follows that $Q^*(a_1, \ldots a_n)$ is satisfied by all models of K* which are extensions of M. Now let M′ be any other model of K which is an extension of M. We must show that M′ also satisfies X.

Let M* be an extension of M' which is a model of K*. Such an M* exists since K* is model consistent relative to K. Then M* is also an extension of M and so Q* $(a_1,\ldots a_n)$ is satisfied by M*. It then follows directly from the defining property of Q that $Q(a_1,\ldots a_n)$ is satisfied by M', as required.

(10.10) We observe also that the predicate Q is essentially unique in the sense that by (3.12) any two predicates Q_1 and Q_2 of order n which satisfy the conclusion of (10.8) are necessarily K-equivalent. Moreover, since Q is persistent with respect to K, it can be replaced (see (6.3)) by an existential predicate. Again, an argument similar to (10.9) shows that $\sim Q$ is likewise persistent with respect to K so that by (2.14), Q can be replaced equally well by a universal predicate. The predicate Q will be called <u>the projection of Q* from K* onto K.</u>

The following theorem links the notion of relative model-completeness with the subject matter of this chapter:

(10.11) <u>Theorem</u>. Let K and K* be two non-empty and consistent sets of sentences such that K* is defined in K, K* is model consistent relative to K, and K* is model-complete relative to K. Then any predicate Q* $(x_1,\ldots x_n)$ which is defined in K* possesses a projection from K* onto K.

<u>Proof:</u> Let Q* $(x_1,\ldots x_n)$ be a predicate which is defined in K*. Let M be any model of K and let $a_1,\ldots a_n$ be any constants of M. Then $K^* \cup D(M)$ is complete by assumption and so either Q* $(a_1,\ldots a_n)$ is deducible from $K^* \cup D(M)$ and hence is satisfied by all models of K* which are extensions of M, or $\sim Q^*$ is deducible from $K^* \cup D(M)$ and hence is satisfied by all models of K* which are extensions of M. In other words Q* is invariant with respect to K* over K so that Q* possesses a projection from K* onto K by (10.8).

Chapter 11 Applications to Field Theory.

We shall now apply the theory of the preceding chapter to obtain some concrete algebraic results.

(11.0) Let K_F be a set of axioms for the concept of a field and let K_F^* be a set of axioms for the concept of an algebraically closed field. It has been shown (see (9.6) that K_F^* is model-complete relative to K_F. Also K_F^* is defined in and is model-consistent relative to K_F so that by (10.11) every predicate which is defined in K_F^* possesses a projection from K_F^* onto K_F.

(11.1) Again, we may take $K = K_F \cup D(M)$, $K^* = K_F^* \cup D(M)$ where M is a particular field (any model of K). Then the class of all models of K coincides with the totality of fields which are extensions of M , and the class of models of K* is the totality of all algebraically closed fields which are extensions of M . It is easily verified that K* is model-consistent relative to K. Furthermore, since K_F^* is model-complete, $K_F^* \cup D(M)$ is model-complete a fortiori, and it is clear that all remaining conditions of (9.4) are satisfied. We conclude that $K_F^* \cup D(M)$ is model-complete relative to $K_F \cup D(M)$ and hence by (10.11) again we conclude further that every predicate $Q^*(x_1, \ldots x_u)$ which is defined in $K_F^* \cup D(M)$ possesses a projection from $K_F^* \cup D(M)$ onto $K_F \cup D(M)$.

Let us now consider the well-known "Hilbert's Nullstellensatz" which we state as follows:

(11.2) Let $f(x_1, \ldots x_n)$, $f_1(x_1, \ldots x_n), \ldots f_r(x_1, \ldots x_n)$ be polynomials in the polynomial ring $M[x_1, \ldots x_n]$ for a given field M such that f vanishes for all joint zeros of the polynomials $f_1, \ldots f_r$. Then f^ρ belongs to the ideal $(f_1, \ldots f_r)$ for some positive integer ρ.

Now the statement of the theorem above is incorrect if by "all the joint zeros" we mean "all the joint zeros in M". In actual fact the premiss of the theorem is supposed to contain the

clause-

(11.3) "...such that f vanishes for all joint zeros of $f_1,\ldots f_r$ in all fields which are (finite) extensions of M"

and it is with this interpretation that the theorem is usually proved (compare Artin [1] p.p. 7-11, 49-57).

Since every field can be embedded in an algebraically closed field by (8.0) it follows that (11.3) may be weakened, at least formally, by replacing it by:

(11.4) "... such that f vanishes for all joint zeros of $f_1,\ldots f_r$ in <u>all</u> algebraically closed fields which are extensions of M"

Again, since the concept of an algebraically closed field is model-complete and since the condition "f vanishes at at all joint zeros of $f_1,\ldots f_r$" can be easily formalized in the language L it follows that (11.4) is already satisfied if we require only

(11.5) "... such that f vanishes for all joint zeros of $f_1,\ldots f_r$ in the algebraic closure of M.

We observe that the premiss of (11.2) when interpreted in the sense of (11.4) is <u>not</u> easily seen to be elementarily definable in L as a predicate- in M- (i.e which is defined in M) of the coefficients of the polynomials $f, f_1,\ldots f_r$. Indeed the sentence (or predicate of the coefficients):

(11.6) $(x_1)\ldots(x_n)\ [f_1(x_1,\ldots x_n)=0 \wedge \ldots \wedge f_r(x_1,\ldots x_n)=0 \supset f(x_1,\ldots x_n)=0]$

when written out in detail within the lower predicate calculus is certainly defined in M. But, it is clear that (11.6) is not equivalent to the condition (11.4) except when M is algebraically closed. (We observe that in the latter case M coincides with its algebraic closure).

Nevertheless, the general theory of chapter 10 shows, without further algebra, that the predicate in question can be formulated with reference to M only. Indeed, let $f, f_1,\ldots f_r$ be the general polynomials of the variables (indeterminates) $x_1,\ldots x_n$

and of degrees m, $m_1, \ldots m_r$ with indeterminate coefficients. We arrange all these coefficients in an arbitrary but definite order $y_1, \ldots y_k$ say. Then (11.6) may be written as a predicate $Q^*(y_1, \ldots y_k)$ of $y_1, \ldots y_k$ which is defined in K_F^*.

Now let $Q(y_1, \ldots y_k)$ be the projection of $Q^*(y_1, \ldots y_k)$ from K_F^* onto K_F (see 11.0). Then for any set of constants $a_1, \ldots a_k$ in an arbitrary field M, $Q(a_1, \ldots a_k)$ is satisfied by M if and only if (11.6) is satisfied by all algebraically closed fields which are extensions of M. Thus Q is the required predicate; that is, Q is defined in M and is equivalent to (11.4). Q is independent of the characteristic of M.

Consider now the conclusion of (11.2). This states that there exists a positive integer ρ and polynomials $g_i(x_1, \ldots x_n)$ such that:

(11.7) $\left(f(x_1, \ldots x_n)\right)^\rho = g_1(x_1, \ldots x_n) f_1(x_1, \ldots x_n) + \ldots + g_r(x_1, \ldots x_n) f_r(x_1 \ldots x_n)$.

It will be seen that in this form the conclusion cannot be formulated within the lower predicate calculus.. On the other hand, if we specify any pair of positive integers ρ, μ then an argument similar to the one employed in the proof of (8.29) shows that the expression: "There exists polynomials $g_1, \ldots g_r$ of degrees not exceeding μ such that the identity (11.7) is satisfied" can indeed be formulated in L as a predicate of $y_1, \ldots y_k$. We denote this predicate by $Q\rho\mu(y_1, \ldots y_k)$.

Now let $a_1, \ldots a_k$ be an arbitrary set of individual constants which do not occur in K and consider the set of sentences:

$S = K_F \cup Q(a_1, \ldots a_k) \cup \{\sim Q\rho\mu(a_1, \ldots a_k)\}$ where $\{\sim Q\rho\mu(a_1, \ldots a_k)\}$ denotes the set of all sentences of the form-

$\sim Q\rho\mu(a_1, \ldots a_k)\}\ \rho, \mu = 1, 2, 3, \ldots$

If S is consistent then there exists polynomials $f, f_1, \ldots f_r$ with coefficients $a_1, \ldots a_k$ in a field M such that f vanishes for all joint zeros of $f_1, \ldots f_r$ in all algebraically closed extensions of M although the conclusion of (11.2) is not satisfied; since (11.7) then does not hold for any ρ and any $\{g_i(x_1, \ldots x_n)\}$. This is impossible and

shows that S is contradictory.

We conclude that there exist positive integers $\rho_1, \ldots \rho_\ell, \mu_1, \ldots \mu_\ell$ such that the sentence:

(11.8) $Q(a_1, \ldots a_k) \supset [Q_{\rho_1 \mu_1}(a_1, \ldots a_k) \vee \ldots \vee Q_{\rho_\ell \mu_\ell}(a_1, \ldots a_k)]$

is deducible from K_f. Now if $f^\rho = \sum g_i f_i$ then for any positive integer λ we have $f^{\rho+\lambda} = \sum G_i f_i$ where $G_i = f^\lambda g_i$. Hence for all ρ, μ it follows that the sentence-

$[Q_{\rho\mu}(a_1, \ldots a_k) \supset Q_{\rho+\lambda, \mu+m\lambda}(a_1, \ldots a_k)]$ is deducible from K_f, where m is the degree of f as before. It follows that if ρ_0 is the maximum of the ρ_i in the implicate of (11.8), then we may replace all $Q_{\rho_i \mu_i}$ by $Q_{\rho_0, \mu_i + m(\rho_0 - \rho_i)}$. Again if μ_0 is the greatest among the numbers $u_i + m(\rho_0 - \rho_i)$ then we also have that the sentence-

$[Q_{\rho_0, \mu_i + m(\rho_0 - \rho_i)}(a_1, \ldots a_k) \supset Q_{\rho_0 \mu_0}(a_1, \ldots a_k)]$ is deducible from K_f. We conclude that the sentence

$Q(a_1, \ldots a_k) \supset Q_{\rho_0 \mu_0}(a_1, \ldots a_k)$

is deducible from K_f and by our assumption on the a_i it follows that the sentence

$(x_1) \ldots (x_k) [Q(x_1, \ldots x_k) \supset Q_{\rho_0 \mu_0}(x_1, \ldots x_k)]$

is likewise deducible from K_f.

Thus, we have established the existence of upper bounds for ρ and for the degrees of the polynomials g_i (in the representation (11.7) for the conclusion of (11.2)) for given degrees of $f, f_1, \ldots f_\nu$. These bounds are independent of the particular field of coefficients and even of the characteristic of the field.

We now consider ordered fields. Let K_o be a set of axioms for the concept of an ordered field and let K_o^* be a set of axioms (defined in K) for the concept of a real closed (ordered) field. It was shown in chapter 9 (see 9.8) that K_o^* is model-complete relative to K_o. The remaining conditions of (10.11) are also satisfied, and we conclude that every predicate which is defined in K_o^* possesses a projection from K_o^* onto K_o.

(11.9) Theorem: Let $f(x_1, \ldots x_n)$ and $g(x_1, \ldots x_n)$ be two

polynomials with coefficients in an ordered field M such that $g(x_1,\ldots x_n)$ is of positive degree and irreducible in M and such that $f(x_1,\ldots x_n) \geq o$ for all $x_1,\ldots x_n$ in the real closure M_0^* of M for which $g(x_1,\ldots x_n) = o$. Then there exist polynomials $h(x_1,\ldots x_n)$, $h_1(x_1,\ldots x_n)\ldots$, $h_r(x_1,\ldots x_n)$ $k(x_1,\ldots x_n)$ with coefficients in M and positive elements $c_1,\ldots c_r$ of M such that

(11.10) $$\left(h(x_1,\ldots x_n)\right)^2 f(x_1,\ldots x_n) = \sum_{i=1}^{r} c_i (h_i(x_1,\ldots x_n))^2 + k(x_1,\ldots x_n) g(x_1,\ldots x_n)$$

and such that $h(x_1,\ldots x_n)$ does not belong to the ideal (g) i.e $h(x_1,\ldots x_n)$ is not divisible by g. Moreover there are bounds for the number of squares r required in (11.10) and for the degrees of the polynomials $h, h_1,\ldots h_r, k$. These bounds depend only on the degrees of f and g and not on the coefficients of f and g or on the particular choice of M.

Proof: Suppose that the assumptions of the theorem are satisfied for given f and g with coefficients in an ordered field M but that no identity of the form (11.10) exists. It follows that there can be no identity of the type $f = \sum_{i=1}^{r} c_i (g_i)^2$ in the field of fractions M^* of the quotient ring $M[x_1,\ldots x_n] / (g)$.

Now M is a subfield of M^* so that by (8.26) and the example following (8.18) it follows that the element f of M^* is not totally positive with respect to the positive elements C of M. In other words there exists an ordering of M^* which preserves the ordering of M such that $f < o$. Let $\xi_1,\ldots \xi_n$ be the elements of M^* which correspond to the indeterminates $x_1,\ldots x_n$. Then for the ordering just selected we have $f(\xi_1,\ldots \xi_n) < o$, $g(\xi_1,\ldots \xi_n) = o$.

Let us formulate a sentence X in L in terms of the coefficients of f and g which is defined in K . and which asserts: " $f(x_1,\ldots x_n) \geq o$ for all $x_1,\ldots x_n$ for which $g(x_1,\ldots x_n) = o$" Then $\sim X$ is satisfied by M^* and hence is satisfied by the real closure of M^*. (We note that the prenex normal transform of $\sim X$ is existential). Since the set K_0^* is model-complete $\sim X$ is also satisfied by all other real closed extensions of M and in particular, by M_β^*. This is contrary to the hypothesis of the theorem and proves

that an identity (11.10) exists.

Now let f and g be the general polynomials of n variables $x_1, \ldots x_n$ and of degrees ℓ and m respectively with indeterminate coefficients. We arrange all these coefficients in a definite order $y_1, \ldots y_k$ in such a way that the coefficients of g, $y_1, \ldots y_j$ say are followed by the coefficients of f. Then the statement X defined above becomes a predicate of $y_1, \ldots y_k$, $X = R^*(y_1, \ldots y_k)$. Let $R(y_1, \ldots y_k)$ be the projection of R^* from K_o^* onto K_o.

Next we formulate a predicate $T(y_1, \ldots y_j)$ which states in terms of the relation τ, and the functors ζ and π that $g(x_1, \ldots x_n)$ is irreducible and of positive degree (i.e does not reduce to a constant). Such a predicate can be obtained without difficulty by means of a conjunction of sentences which affirm that g cannot be written as the product of two polynomials of degrees s and m-s, $1 \leq s \leq m-1$ (we note that $T(y_1, \ldots y_j)$ implies irreducibility in M; not absolute irredicibility.) Thus the conjunction: $\left[T(y_1, \ldots y_j) \wedge R(y_1, \ldots y_k)\right]$ states that g is of positive degree and irreducible in the field M and that $f \geq o$ whenever $g = o$ in any real closed extension of M.

For given positive integers ν and μ we formulate in L a predicate $Q_{\nu\mu}(y_1, \ldots y_k)$ which states that there exist polynomials $h, h_1, \ldots h_\nu, k$ of degrees not exceeding μ and positive elements $c_1, \ldots c_\nu$ such that the identity (11.10) is satisfied, and such that h is not divisible by g. (We note that the c_i appear as quantified variables in the formal predicate). Then for <u>any</u> set of (individual) constants $a_1, \ldots a_k$ the sentence:

(11.11) $\left[Q_{\nu\mu}(a_1, \ldots a_k) \supset Q_{\nu_o\mu_o}(a_1, \ldots a_k)\right]$ is deducible from K provided $\nu \leq \nu_o$, $\mu \leq \mu_o$. Now consider the infinite set of sentences: $S = K_o \cup \left\{T(a_1, \ldots a_j),\ R(a_1, \ldots a_k) \sim Q_{\nu\mu}(a_1, \ldots a_k)\right\}$ where ν, μ vary over all positive integers. If S were consistent, there would exist polynomials $f(x_1, \ldots x_n), g(x_1, \ldots x_u)$ with coefficients in an ordered field M and satisfying the assumptions of (11.9) and yet not satisfying an identity of the type (11.10). This is

impossible in view of the first part of the theorem, which has been already proved.

We conclude that $\mathfrak{S}$ is contradictory and hence that a finite disjunction of the sentences $Q_{\nu\mu}(a_1,\ldots a_k)$ is deducible from the set $K_0 \cup \{T(a_1,\ldots a_j),\ R(a_1,\ldots a_k)\}$. Using (11.11) it follows that this disjunction can be replaced by a single sentence $Q_{\nu_0\mu_0}(a_1,\ldots a_k)$. Thus the sentence

(11.12) $\left[[T(a_1,\ldots a_j) \wedge R(a_1\ldots a_k)] \supset Q_{\nu_0\mu_0}(a_1,\ldots a_k)\right]$ is deducible from K. Interpreting (11.12) semantically, we see that the integers ν_0, μ_0 may serve as the bounds whose existence was to be proved.

(11.13) Let us consider in particular the case $n = 1$ and $x_1 = x$. Since every polynomial is now congruent modulo g to a polynomial of degree less than g, it is sufficient to consider the case $\ell \leq m$. Moreover since h is not divisible by g and since $M[x_1,\ldots x_n]/(g)$ is now a field it follows that h possesses an inverse modulo g. Accordingly, we may replace (11.10) by

$$f(x) \equiv \sum_{i=1}^{r} c_i (h_i(x))^2 \qquad \text{mod } g(x)$$

where the number r depends only on the degree of $g(x)$ and not on the field of coefficients of f and g.

We may look upon this result in a different way. Let M be an ordered field and let $g(x)$ be an irreducible polynomial of degree $m > 1$ with coefficients in M. Let $M(d)$ be the field obtained by adjoining a root d of g to M and suppose that $M(d)$ is formally real. Let s be an element of $M(d)$, $s \neq o$. Then s can be written in the form:

$$s = b_0 + b_1 d + \ldots + b_\lambda d^\lambda = f(d) \text{ say where } \lambda < m;$$

$$f(x) = b_0 + b_1 x + \ldots + b_\lambda x^\lambda; \text{ and we have:}$$

(11.14) The following conditions are equivalent:

(i) $f(x) \geq o$ for all values $x \in M^*$ for which $g(x) = o$ where M^* is the real closure of M.

(ii) $s = f(d)$ is totally positive in $M(d)$; that is $s \geq o$ in all possible orderings of $M(d)$.

(iii) Let $M_1 = M(d)\ M_2, \ldots M_R$ be the subfields of M^* (We note that $M(d) \subseteq M^*$ since $d \in M^*$ (i) where $i = \sqrt{-1}$ and if $d \notin M^*$ then we obtain from $g(d) = o$ that there exist elements $c_0, c_1 \in M^*$ $c_1 \neq o$ such that $c_0 + c_1 i = o$. Hence $i \in M^*$, which is impossible.) which are conjugate to $M(d)$ with respect to M. Then the conjugates of s in $M_1, \ldots M_R$, $s_1 = s, s_2, \ldots s_R$ are all non-negative.

Proof: (i) implies (ii). For if there exists an ordering of M(d) such that $s < o$ then this ordering can be continued in the real closure M^* of M by (8.10). We then have $g(d) = o$ and $f(d) < o$ in M^* which contradicts (i)

(ii) implies (iii). For, any ordering of M_j $j > 1$ that continues the order of M induces an ordering of $M_1 = M(d)$ which continues the order of M. This ordering of M(d) is obtained by determining the positivity of any element of M(d) in accordance with the positivity of the corresponding element of M_j. Hence $s_j < o$ entails $s < o$ in the ordering of M(d) just obtained.

Finally (iii) implies (i). For if (i) is not satisfied then there exists an element $d^* \in M^*$ such that $g(d^*) = o$ and $s^* = f(d^*) < o$. (We note that $f(d^*) = o$ is impossible since f is of lower degree than g and does not vanish identically.) Then d^* is one of the conjugates of d and generates a subfield $M(d^*)$ of M^* while $s^* = f(d^*)$ is the corresponding conjugate of $s = f(d)$. This contradicts (iii).

Combining (11.14) and 11.13) we obtain:

(11.14) Theorem: Let M' be a finite algebraic and formally real extension of an ordered field M. Then every totally positive element β of M' can be represented in the form:

$$\beta = \sum_{i=1}^{r} c_i \gamma_i^2$$

where $c_i \in M$, $c_i \geq o$ and $\gamma_i \in M'$ $i = 1, 2, \ldots r$. The integer r depends only on the degree of M' over M. and not on the particular choice of M or M' or of β. As a corollary we have:

(11.15) Theorem: If there exists a positive integer m such that

every positive element of M can be represented as a sum of m squares of elements of M then every totally positive element β of M' can be represented in the form:

$$\beta = \sum_{i=1}^{k} \gamma_i^2$$

where $\gamma_i \in M'$ $i = 1, 2, \ldots k$ where $k = rm$ may now depend on M but not on M' or β.

Thus we have shown that if M is an ordered field such that every positive element of M can be represented as a sum of squares and there exists a uniform bound to the number of squares required then there also exists a uniform bound to the number of squares required to express a totally positive element of M' as a sum of squares of elements of M'; where M' is any finite algebraic extension of M.

BIBLIOGRAPHY

E. Artin

1 Elements of Algebraic Geometry. New York University Institute of Mathematical Sciences, Spring, 1955.

D. Hilbert

1 Mathematical Problems. Bulletin of the American Mathematical Society, Vol. 8, 1901-1902, Macmillan, 1902.

D. Hilbert and W. Ackerman.

1 Principles of Mathematical Logic. Chelsea, New York, 1950.

Abraham Robinson

1 Outline of an Introduction to Mathematical Logic. Canadian Mathematical Bulletin vol. 1, Nos. 1-3, vol. 11 No. 1, 1958-59.

2 Théorie Métamathématique Des Idéaux. Collection De Logique Mathematique. ser A, No. 8, Paris Louvain, 1955.

3 Complete Theories. Studies in Logic and the Foundations of Mathematica, North Holland Publishing Company, Amsterdam, 1956.

4 Completeness and Persistence In the Theory of Models Zeitschrift für Mathematische Logik und Grundlagen der Mathematik, vol. 11, 1956, p.p. 15-26.

5 On the Metamathematics of Algebra. Studies in Logic and the Foundations of Mathematics, North-Holland Publishing Company, Amsterdam, 1951.

6 On a Problem of L. Henkin. Journal of Symbolic Logic, vol. 21, 1956, p.p. 33-35.

7 Apercu Métamathematique Sur Les Nombres Réels. Deux Conferences Prononcées a l'Universite De Montréal, University of Montreal, February, 1956

8 On Ordered Fields And Definite Functions Mathematische Annalen, Vol. 130, 1955, p.p. 257 - 271.

9 Further Remarks on Ordered Fields and Definite Functions. Ibid, 1956, p.p. 405-409.

10 Some Problems of Definability in the Lower Predicate Calculus. Fundamenta Mathematicae, vol 44, 1957, p.p. 309-329.

11 Relative Model-Completeness and the Elimination of Quantifiers. Dialectica, Vol. 12, Nos. 3 and 4, 1958.

A. Tarski and J.C.C. McKinsey.

1. A Decision Method for Elementary Algebra and Geometry. Second Edition, University of California Press, Berkeley and Los Angeles, 1951

B.L. Van Der Waerden

1 Modern Algebra vol. 1, Frederick Ungar Publishing Co., New York, 1949.

O. Zariski and P. Samuel

1 Commutative Algebra. Vol. 1, Van Nostrand, 1958.

L. Gillman and M. Jerison.

1 Rings of Continuous Functions, Van Nostrand, New York, 1960, p.p. 172-173.