Some problems of definability in the lower predicate calculus

by

A. Robinson (Toronto)

1. Introduction. The present paper [1]) arose out of the consideration of the following problem.

Let M be an ordered field such that every positive element of M can be represented as a sum of squares of elements of the field and such that there exists a uniform bound to the number of squares required for the purpose. Let M' be a finite algebraic extension of M. Is there 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'?

It will be shown in due course (section 5, below) that the answer to this question is in the affirmative. Its investigation led to another type of problem which can be introduced conveniently by means of the following example.

Let

$$p(x)=y_0+y_1x+\ldots+y_nx^n$$

be a polynomial of the variable x where $y_0,\ldots,y_n$ are parameters which take values in the field of rational numbers, R. Then the property of $p(x)$ of possessing (or not possessing) a real root may be regarded as a predicate of its coefficients, $Q^*(y_0,\ldots,y_n)$, say. We note that, as stated, this predicate is not formulated within the field of the coefficients, R, but with reference to the more comprehensive field of real (or real algebraic) numbers, R^*. However, Sturm's test shows that there exists a predicate $Q(y_0,\ldots,y_n)$, formulated within the language of the lower predicate calculus in terms of the relation of addition, multiplication, equality, and order, such that whenever $Q(y_0,\ldots,y_n)$ holds in R, for rational $y_0,\ldots,y_n$, $Q^*(y_0,\ldots,y_n)$ holds in R^*, and conversely, whenever $Q^*(y_0,\ldots,y_n)$ holds in R^*, for rational $y_0,\ldots,y_n$, $Q(y_0,\ldots,y_n)$ holds in R.

---

[1]) This paper was written while the author was a Fellow of the Summer Research Institute of the Canadian Mathematical Congress, Kingston, Ontario, 1956. The author is indebted to A. H. Lightstone for suggesting a number of improvements in the presentation.

Instead of considering such a situation for two particular structures R and R^*, as above, we shall be concerned here (section 3, below) with predicates Q, Q^*, which are defined with reference to two different sets of axioms, K and K^*, and which are related in a manner similar to that just described.

It turns out that the treatment of this subject calls for the extension of some concepts which have been defined elsewhere. More particularly, it involves a certain relativisation of the notion of model-completeness (see [7], [8]). The analysis of this generalised notion occupies the first part of the present paper (section 2).

The various topics detailed above will be investigated partly because of their intrinsic interest and partly for the sake of the applications mentioned earlier. We should also point out that (as is only natural) the application of some of our general results can be replaced by more special arguments in certain particular cases (*e. g.* in section 5).

We shall use the formal language of the lower predicate calculus, with the terminology explained in [8]. In particular, we use the terms *statement* for a well-formed formula (wff) without free variables, and *predicate* for any other wff. *Relations* are what have been called elsewhere *atomic predicates*, and by a *constant* we always mean an *individual* constant. A wff, X, is *defined* in a set of statements, K, if all the relations and constants of X occur in K, and X is *defined* in a structure, M, if all the relations and constants of X occur in M.

For a given structure M, the *diagram* N of M is the set of all atomic statements (*e. g.* $R(a,b,c)$) which are defined and hold in M, and of the negations of the atomic statements which are defined but do not hold in M. A set of statements K is *complete* if for every statement X which is defined in K, either X or $\sim X$ is deducible from K. A set K, supposed non-empty and consistent, is *model-complete* if for every model M of K the set $K \cup N$ is complete, where N is the diagram of M. In this context, it is understood here and elsewhere that M contains no relations other than the relations of K.

In section 3 we shall also require the notion of *relativisation* with respect to a given one place relation $R(x)$. This syntactical transformation, which goes back at least as far as [3] (compare also [13]), is defined as follows.

Let X be a given statement. In order to obtain the relativised transform, X_R, of X with respect to R, we consider the quantifiers of X in turn, and we replace any universal quantifier, (y), whose scope in X is the wff Z by $(y)[R(y) \supset Z]$. Similarly, we replace any existential quantifier, $(\exists y)$, with scope Z, by $(\exists y)[R(y) \wedge Z]$. We note that the order in which these operations are carried out does not affect the final result. For example, the statement

$$X = (\exists w)(x)\big[[(\exists y)F(x,y,w)]\supset[(z)G(y,z,a)]\big]$$

is transformed into

$$X_R = (\exists w)\Big[R(w) \wedge \Big[(x)\Big[R(x) \supset [(\exists y)[R(y) \wedge F(x,y,w)]] \supset \big[(z)[R(z) \supset G(y,z,a)]\big]\Big]\Big]\Big].$$

Correspondingly, for any given structure M which does not include R, we define the structure M_R by postulating in addition that R be satisfied for all constants a of M. Then it is not difficult to see that if X holds in M, X_R holds in M_R. Conversely, if X is defined in M, for given X and M, and if X_R holds in M_R then X holds also in M. Moreover, if X holds in M and if M^* is any extension of M such that M^* does not include R, then X_R holds in the structure $\mathbf{M}$ which is obtained by postulating, in addition to the existing relations of M^*, that $R(a)$ holds in $\mathbf{M}$ for all constants of M and that $R(a)$ does not hold in $\mathbf{M}$ for any constant of $\mathbf{M}$ which does not belong to M.

It is known that if X is provable and does not include any constants then X_R is deducible from the statement $(\exists x)R(x)$; while if X is provable and contains a number of constants $a_1, \ldots, a_n$, then X is deducible from the statement $R(a_1) \wedge \ldots \wedge R(a_n)$. We conclude that if the statement X is defined in a set of statements K and is deducible from that set, then X_R is deducible from the set K_R, where K_R is the set of statements Y_R for all $Y \in K$, together with all the statements $R(a)$ for the constants a which are included in K. However, if K does not contain any constants then K_R shall include instead the statement $(\exists x)R(x)$.

2. Relative model-completeness. Let K and K^* be two non-empty and consistent sets of statements. We shall say that K^* is *associated* with K if the following conditions are satisfied ((2.1)-(2.3)):

(2.1) K^* does not include any relations or constants which are not also included in K.

(2.2) K^* is *model-consistent relative to* K. That is to say, every model M of K can be embedded in (*i. e.* possesses an extension which is) a model of K^*. An equivalent condition is that for any model M of K, the set $K^* \cup N$ is consistent, where N is the diagram of M.

(2.3) Every model of K^* which is an extension of a model of K is itself a model of K. In deductive terms — if M is a model of K and N its diagram, then K must be deducible from $K^* \cup N$. This condition is satisfied, for example, if K is a subset of K^*.

We note that any non-empty and consistent set is associated with itself.

Let K and K^* be two non-empty sets of statements, K consistent and K^* model-consistent relative to K. Then K^* will be said to be *model-complete relative to* K if for every model M of K the set $K^* \cup N$ is complete, where N is the diagram of M. For $K^*=K$, this definition reduces to ordinary model-completeness (see [7], [8]).

We recall that a statement X is said to be *primitive* (see [8]) if it is of the form

(2.4) $$X = (\exists y_1)\ldots(\exists y_n) Z(y_1, \ldots, y_n), \quad n \geqslant 0,$$

where the *matrix* Z does not contain any quantifiers and is a conjunction of atomic formulae and (or) of the negations of such formulae.

The following test for relative model-completeness is a generalization of the test for ordinary model-completeness given in [7] and [8]. The proof involves a refinement of the methods used there.

(2.5) THEOREM. *Let K and K^* be two non-empty and consistent sets of statements, such that K^* is associated with K. In order that K^* be model-complete relative to K it is necessary and sufficient that for every model M of K, with diagram N, and for every primitive statement X defined in M, either X or $\sim X$ be deducible from $K^* \cup N$.*

Proof. Since the definition of relative model-completeness requires that for *every* statement X which is defined in M, and hence in $K^* \cup N$, either X or $\sim X$ must be deducible from $K^* \cup N$, it is apparent that the condition of the theorem is necessary. In order to prove that it is also sufficient, we suppose that there exists a model M of K and a statement X which is defined in M such that neither X nor $\sim X$ is deducible from $K^* \cup N$. If so, there exist statements of this kind which are in prenex normal form, and among these we may choose one for which the number of quantifiers is a minimum (where all possible M are taken into account). Moreover, we may suppose that X begins with an existential quantifier. For if X does not include any quantifiers at all then either X or $\sim X$ must be deducible from N alone, while if X begins *a priori* with a universal quantifier then we may consider instead the statement X' which is obtained by writing $\sim X$ in prenex normal form, in the usual way.

Suppose then that X begins with an existential quantifier,

$$X = (\exists z) V(z),$$

and that X is defined in a model M of K but that neither X nor $\sim X$ is deducible from $K^* \cup N$. It follows that X is consistent with $K^* \cup N$ — there exists a model M^* of K^* which is also a model of N (and hence

an extension of M) such that X holds in M^*. Thus M^* includes a constant a such that $V(a)$ holds in M. But M^* is also a model of K, by (2.3), and so, by the minimum property of X, $V(a)$ must be deducible from $K^* \cup N^*$, where N^* is the diagram of M^*. It follows that $X = (\exists z) V(z)$ also is deducible from $K^* \cup N^*$, and we propose to show that this entails that X is deducible already from $K^* \cup N$. Now $K^* \cup N^*$ contains in addition to the statements of $K^* \cup N$, only certain atomic statements and their negations. It follows that there is a conjunction of a number of these, $W(b_1, \ldots, b_n)$ say, such that

(2.6) $$W(b_1, \ldots, b_n) \supset X$$

is deducible from $K^* \cup N$. The constants $b_1, \ldots, b_n$ are supposed to be just those constants of W which do not belong to M and hence, do not occur in X or in $K^* \cup N$. Accordingly, we may infer that

$$[(\exists x_1)\ldots(\exists x_n) W(x_1, \ldots, x_n)] \supset X$$

also is deducible from $K^* \cup N$. Thus, in order to prove that X is deducible from $K^* \cup N$ it only remains for us to show that

$$Y = (\exists x_1)\ldots(\exists x_n) W(x_1, \ldots, x_n)$$

is deducible from $K^* \cup N$. But Y is a primitive statement which is defined in M and which holds in M^*. It therefore follows from the assumptions of the theorem that Y is actually deducible from $K^* \cup N$. This leads to a contradiction and completes the proof.

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

(2.7) THEOREM. *Let K and K^* be two non-empty sets of statements such that K is consistent and K^* is model-consistent relative to K. Suppose that K^* is model-complete in the ordinary sense. Suppose further that for every model M of K there exists a model M_0^* of K^* which is an extension of M, such that any other model of K^* which is an extension of M possesses a partial structure which is an extension of M and which is isomorphic to M_0^* by an isomorphism which centralises the elements of M. Then K^* is model-complete relative to K.*

Remark. We observe that M_0^* is a *prime-model* of $K^* \cup N$ in the sense defined in [8].

Proof of (2.7). For a given model M of K, let M_0^* be a prime-model of $K^* \cup N$. (Such an M_0^* exists according to the assumption of the theorem). Let X be any statement which is defined in M. Since K^* is model-

-complete, either X or $\sim X$ must be deducible from $K^*\cup N_0^*$ where N_0^* is the diagram of M_0^*. It will be sufficient to consider the former case. We employ the same procedure as in the last part of the proof of (2.5). Since $K^*\cup N_0^*$ contains in addition to the statements of $K^*\cup N$ only certain atomic statements and their negations, we may conclude that there exists a conjunction of a finite number of these, $W(b_1,\ldots,b_n)$, such that

$$W(b_1,\ldots,b_n)\supset X$$

is deducible from $K^*\cup N$. In this formula, the constants are distinguished in the same way as in (2.6), and we conclude again that

$$[(\exists x_1)\ldots(\exists x_n)W(x_1,\ldots,x_n)]\supset X$$

is deducible from $K^*\cup N$. And again it only remains for us to show that

$$Y=(\exists x_1)\ldots(\exists x_n)W(x_1,\ldots,x_n)$$

is deducible from $K^*\cup N$. However, at this point the argument diverges from that used in the proof of (2.5). We have to show that Y holds in all models of $K^*\cup N$. Let M^* be such a model, then M^* contains a partial structure M_1^*, which is isomorphic to M_0^* in the manner described in the statement of the theorem. It follows that Y holds in M_1^*. But Y is primitive and so it holds also in all extensions of M_1^*, *e. g.* in M^*. This completes the proof.

Thus, let K_F be a set of axioms (*i. e.* statements) for the concept of a (commutative) field formulated in terms of the relation of equality, $E(x,y)$, addition, $S(x,y,z)$, and multiplication, $P(x,y,z)$, and without constants, and let K_p be a set of axioms for the concept of a field of given characteristic $p\geqslant 0$, formulated in a similar way. Also, let K_F^*, K_p^* be corresponding sets which specify in addition that the field is algebraically closed. It is known (see [8]) that K_F^* is model-complete, and it follows that the same applies to K_p^*. Also, K_F^* is associated with K_F^* and with K_p (although K_F^* is not an extension of K_p) and K_p^* is associated with K_p but not with K_F, for $p=0,2,3,\ldots$ A quick check shows that the test of Theorem (2.7) applies. Thus, K_F^* is model-complete relative to K_F and also relative to K_p, and K_p^* is model-complete relative to K_p, $p=0,2,3,\ldots$

Again, let K_Q be a set of axioms for the concept of an ordered field, containing a relation of order in addition to the relations mentioned above, and let K_Q^* be an extension of K_Q which expresses the concept of a real-closed ordered field (see [8]). Then K_Q^* is model-complete in the ordinary sense and associated with K_Q and, again by (2.7), model-complete relative to that set.

Next we prove

(2.8) THEOREM. *Let K, K_1^*, K_2^* be three non-empty and consistent sets of statements such that both K_1^*, and K_2^* are associated with K and model-complete relative to that set. 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. The conclusion of the theorem is equivalent to the assertion that, for any given model M of K, with diagram N, K_2^* is deducible from $K_1^*\cup N$ and K_1^* is deducible from $K_2^*\cup N$. Accordingly, we only have to show that if a statement X which is defined in M is deducible from $K_1^*\cup N$ then it is deducible also from $K_2^*\cup N$. 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 statement X which is defined in M, X is deducible from $K_1^*\cup N$ and $\sim X$ is deducible from $K_2^*\cup N$. If so, there exist statements X of this kind which are in prenex normal form and we may suppose, as in the proof of (2.5), that the number of quantifiers in X is a minimum and that X begins with an existential quantifier, $X=(\exists z)V(z)$.

Suppose then that X is deducible from $K_1^*\cup N$ while $\sim X$ is deducible from $K_2^*\cup N$. Let M_1^* be a model of $K_1^*\cup N$ and let N_1^* be the diagram of M_1^*. Then X holds in M_1^* and so M_1^* contains a constant a such that $V(a)$ holds in M_1^*. But M_1^* is a model of K, by (2.3), and so $K_1^*\cup N_1^*$ is complete, and $V(a)$ is deducible from $K_1^*\cup N_1^*$. It then follows from the minimum property of X that $V(a)$ must be deducible also from $K_2^*\cup N_1^*$. This entails that $X=(\exists z)V(z)$ is deducible from $K_2^*\cup N_1^*$. On the other hand, since $N_1^*\supseteq N$ and since $\sim X$ is supposed to be deducible from $K_2^*\cup N$, $\sim X$ must be deducible also from $K_2^*\cup N_1^*$. This is impossible since $K_2^*\cup N_1^*$ is consistent, by (2.2). Accordingly, the theorem is proved.

The situation is simplified in various ways if we add the assumption that K is deducible from K^*, or even that K is a subset of K^*. However, the example $K=K_p$, $K^*=K_F^*$ shows that neither of these conditions need be satisfied.

Theorem (2.8) shows 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 real-closed ordered fields relative to the class of all ordered fields.

3. Some problems in definability. In this section, we shall discuss the second topic mentioned in the introduction.

Let K and K^* be two sets of statements. A statement X^* which is defined in K^* will be said to be *invariant* with respect to K^* over K

if for any given model M of K, X^* is either satisfied in all models of K^* which are extensions of M, or in none.

(3.1) THEOREM. *Let K and K^* be two non-empty and consistent sets of statements such that conditions* (2.1) *and* (2.2) *are satisfied, and let X^* be a statement which is defined in K^* and is invariant with respect to K^* over K. Then there exists a statement X which is defined in K such that X holds in any given model M of K if and only if X^* holds in all models of K^* which are extensions of M.*

Remark. It is clear that if such a statement X exists then it is essentially unique, *i. e.* if the conclusion of the theorem is satisfied for $X=X_1$ and $X=X_2$ then the equivalence $X_1 \equiv X_2$ is deducible from K. X will be called the *projection of X^* from K^* onto K.*

Proof of (3.1). For given K, K^* and X^* which satisfy the conditions of the theorem, we relativise K (see section 1) with respect to a relation $R(x)$ which is not contained in K, and hence is not contained in K^* or X^* either. Suppose that we can find a statement X which is defined in K such that the equivalence

$$X^* \equiv X_R$$

is deducible from the set $K^* \cup K_R$. Let M and M^* be models of K and K^* respectively, such that $M \subseteq M^*$. Define $\boldsymbol{M}$ as in section 1 by postulating, in addition to the existing relations of M^*, that $R(a)$ shall hold in $\boldsymbol{M}$ for all elements a of M, and $R(a)$ shall not hold for the elements of M^* which do not belong to M. Then $\boldsymbol{M}$ is a model of K^* as well as of K_R.

Now suppose that X^* holds in M^*. It follows that X^* holds also in $\boldsymbol{M}$. And since $X^* \equiv X_R$ is deducible from $K^* \cup K_R$ we conclude that X_R also holds in $\boldsymbol{M}$, and hence that X holds in M. A similar argument shows that if $\sim X^*$ holds in M^* then $\sim X$ holds in M. Thus, in order to prove the theorem, we only have to find a statement X such that $X^* \equiv X_R$ is deducible from $K^* \cup K_R$.

Let P be the set of all statements X which are defined in K and such that

$$X^* \supset X_R$$

is deducible from $K^* \cup K_R$. P is not empty since it includes all provable statements which are defined in K. Also, P is *conjunctive*, that is to say, $X \in P$ and $Y \in P$ together entail $X \wedge Y \in P$. Indeed, if $X^* \supset X_R$ and $X^* \supset Y_R$ are deducible from $K^* \cup K_R$ then $X^* \supset [X_R \wedge Y_R]$ also is deducible from that set, and $X_R \wedge Y_R$ is identical with $[X \wedge Y]_R$.

Let P_R be the set of all X_R for $X \in P$ and consider the set

$$S = K^* \cup K_R \cup P_R \cup \{\sim X^*\}.$$

Suppose first that this set is consistent and hence, that it possesses a model $\boldsymbol{M}'$. Then $\boldsymbol{M}'$ is a model of K^*. Also, the constants of $\boldsymbol{M}'$ which satisfy $R(a)$ constitute a model M_R of K_R, and if we disregard the relations $R(a)$ in M_R then we obtain a model M of K. Let N be the diagram of M, then the diagram N_R of M_R is obtained by adding to N the atomic statements $R(a)$ for all constants a of N. The set $S' = K^* \cup K_R \cup N_R$ is consistent since $\boldsymbol{M}'$ is a model of this set. We propose to show that $\sim X^*$ must be deducible from S'.

Suppose on the contrary that $S' \cup \{X^*\} = K^* \cup K_R \cup N_R \cup \{X^*\}$ is consistent and hence, that it possesses a model $\boldsymbol{M}''$. Then the constants a of $\boldsymbol{M}''$ which satisfy $R(a)$ constitute a model M_R'' of K_R such that M_R'' is an extension of M_R. It follows that $\boldsymbol{M}''$ is an extension of M which satisfies X^* while $\boldsymbol{M}'$ is an extension of M which satisfies $\sim X^*$. The same still applies if we remove the relation $R(x)$ from $\boldsymbol{M}'$ and $\boldsymbol{M}''$ 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 that there exists a statement Y which is a conjunction of a finite number of elements of N_R such that $Y \supset \sim X^*$, and with it $X^* \supset \sim Y$, is deducible from $K^* \cup K_R$. Now the conjuncts of Y are either of the form $R(a)$ or they are atomic formulae which are given in terms of the constants and relations of M, or the negations of such formulae. We may write $\sim Y$ as a disjunction, or again as an implication of the form

$$R(a_1) \wedge \ldots \wedge R(a_n) \supset Z$$

where Z is a disjunction of atomic formulae of the type just described and (or) of the negations of such formulae. Moreover, by adding, if necessary, suitable elements of N_R to the original Y, we may ensure that the constants contained in Z are precisely $a_1, \ldots, a_n$, $Z = Z(a_1, \ldots, a_n)$. Then

$$X^* \supset [R(a_1) \wedge \ldots \wedge R(a_n) \supset Z]$$

is deducible from $K^* \cup K_R$. Furthermore, the conjunction $R(a_1) \wedge \ldots \wedge R(a_n)$ may (possibly) be shortened by omitting from it all terms $R(a_j)$ such that a_j is contained in K, for these terms are already included in K_R, by definition (see section 1, above). Suppose that this applies for $j = m+1, \ldots, n$, then

$$X^* \supset [R(a_1) \ \ldots \ R(a_m) \supset Z]$$

is deducible from $K^* \cup K_R$. (If $m=0$, we omit the conjunction and the sign of implication which follows it.) Since $a_1, \ldots, a_m$ are not included in either K^*, K_R, or X^* it follows that the statement

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

is deducible from $K^* \cup K_R$. A slight modification of (3.2) then shows that the statement

(3.3) $$X^* \supset V$$

is deducible from $K^* \cup K_R$, where

$$V = (x_1)\Big[R(x_1) \supset \Big[(x_2)\,[R(x_2) \supset \ldots [R(x_m) \supset Z(x_1, \ldots, x_m, a_{m+1}, \ldots, a_m)] \ldots\Big]\,.$$

But V is the relativised transform of the statement W which is defined by

$$W = (x_1) \ldots (x_m) Z(x_1, \ldots, x_m, a_{m+1}, \ldots, a_n)\,,$$

i. e. $V = W_R$, and W is defined in K. Referring to (3.3), we now see that W belongs to P, by the definition of this set, and V belongs to P_R. But $\boldsymbol{M}'$ is a model of P_R and so $\boldsymbol{M}'$ satisfies V. We infer that $\boldsymbol{M}'$ satisfies at the same time

$$R(a_1) \wedge \ldots \wedge R(a_m) \supset Z(a_1, \ldots, a_m, a_{m+1}, \ldots, a_n)\,.$$

Now $R(a_1) \wedge \ldots \wedge R(a_m)$ holds in $\boldsymbol{M}'$ and so $Z(a_1, \ldots, a_n)$ also holds in that structure. On the other hand, Z is a disjunction of atomic formulae whose negations hold in M, and hence in $\boldsymbol{M}'$, and (or) of the negations of such formulae, if the formulae themselves hold in M and hence in $\boldsymbol{M}'$. If follows that $\sim Z$ holds in $\boldsymbol{M}'$ and this contradicts the result just obtained. We conclude that $\boldsymbol{M}'$ cannot exist, *i. e.* the set

$$S = K^* \cup K_R \cup P_R \cup \{\sim X^*\}$$

must be contradictory. It follows that there exists a finite conjunction of elements of P_R and more particularly (since P_R is conjunctive) a single element X_R of P_R 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. This shows that

$$X^* \equiv X_R$$

is deducible from $K^* \cup K_R$ and completes the proof of the theorem.

Next, we consider the corresponding problem for predicates.

Let K and K^* be two sets of statements. A predicate $Q^*(x_1, \ldots, x_n)$, $n \geq 1$, which is defined in K will be said to be *invariant* with respect to K^* over K if for any set of constants, $a_1, \ldots, a_n$, which belong to a model M of K, either the statement $Q^*(a_1, \ldots, a_n)$ holds in all extensions of M which are models of K^*, or the statement $\sim Q^*(a_1, \ldots, a_n)$ holds in all extensions of M which are models of K^*.

(3.4) THEOREM. *Let K and K^* be two non-empty and consistent sets of statements such that conditions (2.1) and (2.2) are satisfied, and let $Q^*(x_1, \ldots, x_n)$ be a predicate which is defined in K^* and 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 statement $Q(a_1, \ldots, a_n)$ holds in M if and only if $Q^*(a_1, \ldots, a_n)$ holds in all models of K^* which are extensions of M.*

Remark. If the conclusion of the theorem is satisfied for $Q = Q_1$ and $Q = Q_2$ then the statement

$$(x_1) \ldots (x_n)[Q_1(x_1, \ldots, x_n) \equiv Q_2(x_1, \ldots, x_n)]$$

is deducible from K. In this sense, Q is essentially unique. It will be called the *projection* of Q^* from K^* onto K.

Proof of (3.4). Let $b_1, \ldots, b_n$ be a set of constants which are not contained in K (and hence, are not contained in K^*). We adjoin these constants to K and K^*, obtaining sets K_0 and K_0^* respectively. That is to say (see [7]) we add to K and K^* provable statements which involve $b_1, \ldots, b_n$. By this device, we ensure that the statement

$$X^* = Q^*(b_1, \ldots, b_n)$$

is defined in K_0.

We maintain that X^* is invariant with respect to K_0^* over K_0. Indeed, let M_0 be any model of K_0, and hence of K, and let M_1^*, M_2^* be two models of K_0^* (and hence of K^*) which are extensions of M. Then the constants $b_1, \ldots, b_n$ are contained in all three of these structures. Since $Q^*(x_1, \ldots, x_n)$ is invariant with respect to K^* over K, $X^* = Q^*(b_1, \ldots, b_n)$ holds either in both M_1^* and M_2^* or it holds neither in M_1^* nor in M_2^*. This shows that X^* is invariant with respect to K_0^* over K_0. Applying (3.1) we find that there exists a statement X which is defined in K_0 such that X holds in any model M_0 of K_0 if and only if X^* holds in all models of K_0^* which are extensions of M_0. Moreover, we may assume that X includes the constants $b_1, \ldots, b_n$ effectively for if this is not the case from the outset then we only have to add a number of provable statements which include these constants, to X in conjunction. 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 conditions of the theorem.

Let M be a 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 suppose in addition that the b_i are not included in M or M^*

either. We now enlarge the structure M by adding the constants $b_1, \dots, b_n$, and we define that in the enlarged structure M_0, a relation involving any of the b_i shall hold precisely if the relation obtained from it after replacing the b_i by the corresponding a_i holds in M. We also define a structure M_0^* which is obtained in the same way by adding the b_i to M^* and proceeding as before. Then M_0 is a model of K_0 and M_0^* is a model of K_0^*.

Suppose now that $Q^*(a_1, \dots, a_n)$ holds in M. Then the straightforward semantic interpretation of this fact shows that $X^* = Q^*(b_1, \dots, b_n)$ holds in M_0. It follows that $X = Q(b_1, \dots, b_n)$ holds in M_0 and hence that $Q(a_1, \dots, a_n)$ holds in M. A similar argument shows that if $\sim Q^*(a_1, \dots, a_n)$ holds in M^* then $\sim Q(a_1, \dots, a_n)$ holds in M. This establishes the theorem.

We note that the statement X whose existence is affirmed by Theorem (3.1) is by necessity persistent with respect to K, according to the definition given in [8]. For if X holds in a model M of K then X^* holds in 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 have to show that X holds also in M'.

Let M^* be an extension of M' which is a model of K^*. Such an M^* exists since K^* is model-consistent with respect to K. Then M^* is also an extension of M, and so X^* holds in M^*. It then follows directly from the defining property of X that X holds in M'.

Since X is persistent with respect to K it can be replaced by a statement in prenex normal form with existential quantifiers only (see [2], [4], [9], [14]). Moreover, $\sim X$ also is persistent with respect to K, and so X can be replaced equally well by a statement in prenex normal form with universal quantifiers only. These results can also be obtained directly by a suitable restriction on the statements of the set P which occurs in the proof of (3.1). Similar remarks apply to the predicate $Q(x_1, \dots, x_n)$ of Theorem (3.4).

The following theorem links the notion of relative model-completeness with the subject of the present section:

(3.5) THEOREM. *Let K and K^* be two non-empty and consistent sets of statements such that* (2.1) *and* (2.2) *are satisfied and such that K^* is model-complete relative to K. Then any statement X^* which is defined in K^* possesses a projection from K^* onto K. Similarly, any predicate $Q^*(x_1, \dots, x_n)$ which is defined in K^* possesses a projection from K^* onto K.*

Proof. Let X^* be a statement which is defined in K^* and let M be any model of K with diagram N. Then $K^* \cup N$ is complete, by assumption and so either X^* is deducible from $K^* \cup N$ and hence holds in all models of K^* which are extensions of M, or $\sim X^*$ is deducible from $K^* \cup N$ and holds in all models of K^* which are extensions of M. Thus X^* is invariant with respect to K^* over K. The first part of (3.5) now follows immediately from (3.1). The second part of the theorem is proved in the same way.

4. Application to field theory. Let K be a set of axioms for the concept of a (commutative) field, $K = K_F$, and let $K^* = K_F^*$ be a set of axioms for the concept of an algebraically closed field (compare section 2 above). It has been shown in section 2 that K_F^* is model-complete relative to K_F. Moreover, conditions (2.1) and (2.2) are satisfied and so, by (3.5), every predicate which is defined in K_F^* possesses a projection from K_F^* onto K_F.

Again, we may take $K = K_F \cup N_0$, $K^* = K_F \cup N_0$, where N_0 is the diagram of a particular field M_0. Thus, the class of models of K coincides with the totality of fields which are extensions of M_0, and the class of models of K^* is the totality of all algebraically closed fields which are extensions of M_0. (Instead of including the diagram of a particular field one might wish to include statements specifying the characteristic of the field but the same effect can be obtained equally well by including the prime field of the characteristic in question.) A direct check shows that conditions (2.1)-(2.3) are satisfied so that K^* is associated with K. Furthermore, since K_F^* is model-complete, $K_F^* \cup N_0$ is model-complete *a fortiori*, and it will be seen that the remaining conditions of Theorem (2.7) are satisfied as well. We conclude that $K_F^* \cup N_0$ is model-complete relative to $K_F \cup N_0$ and, referring to Theorem (3.5), we conclude further that every predicate $Q^*(x_1, \dots, x_n)$ which is defined in $K_F^* \cup N_0$ possesses a projection from $K_F^* \cup N_0$ onto $K_F \cup N_0$.

In current usage in Algebra, the fact that a particular property applies, not within a specified field of coefficients M, but within some extension of M, is frequently understood implicitly. The following version of the theorem of Hilbert-Netto differs only inessentially from that given in [15]:

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

Now this theorem 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

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

— and it is with this interpretation that the theorem is usually proved. Since every field can be embedded in an algebraically closed field, (4.2) may be weakened, at least formally, by replacing it by

(4.3) "..., such that f vanishes for all joint zeros of $f_1,\dots,f_r$, in all algebraically closed fields which are extensions of M".

Again, since the concept of an algebraically closed field is model-complete (or else, by purely algebraic arguments) it follows that (4.3) is already satisfied if we require only

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

In [5] and [6], it is shown by arguments which involve a certain amount of algebra that the premiss of (4.1), when interpreted in the sense of (4.3), can be formulated as a predicate — in M — of the coefficients of the polynomials $f,f_1,\dots,f_r$. Reviewing [5] in [1], one of the leading authorities in our field expresses his surprise that such arguments were employed seeing that there exists a simple and straightforward way of formalising the clause in question. It appears that this refers to the statement (or predicate of the coefficients)

$$(4.5)\qquad (x_1)\dots(x_n)[f_1(x_1,\dots,x_n)=0\wedge\dots\wedge f_r(x_1,\dots,x_n)=0\supset f(x_1,\dots,x_n)=0]$$

when written out in detail within the lower predicate calculus. However, it will now be clear that the expression which is actually to be formalised (*i. e.* (4.3)) is not equivalent to (4.5) except when M is algebraically closed.

Nevertheless, the general theory of section 3 shows, without further algebra, that the predicate in question can be formulated with reference to M only, as required. Indeed, let $f,f_1,\dots,f_r$ be the general polynomials of the variables $x_1,\dots,x_n$, and of degrees $m,m_1,\dots,m_r$, with indeterminate coefficients. We range all these coefficients in an arbitrary but definite order, $y_1,\dots,y_k$, say. Then (4.5) may be written as a predicate of $y_1,\dots,y_k$ in terms of the relations of equality, addition, and multiplication, and without constants. We denote this predicate by $Q^*(y_1,\dots,y_k)$.

Now let $Q(y_1,\dots,y_k)$ be the projection of $Q^*(y_1,\dots,y_k)$ from K_F^* onto K_F. Then for any given set of elements $a_1,\dots,a_k$ in an arbitrary field M, $Q(a_1,\dots,a_k)$ holds in M if and only if (4.5) holds in all algebraically closed field which include M. Q is the required predicate. It is independent of the characteristic of M.

Consider now the conclusion of the theorem of Hilbert-Netto, (4.1). This states that there exists a positive integer ϱ and polynomials $g_i(x_1,\dots,x_n)$ such that

$$(4.6)\qquad (f(x_1,\dots,x_n))^\varrho=g(x_1,\dots,x_n)f(x_1,\dots,x_n)+\dots+g_r(x_1,\dots,x_n)f_r(x_1,\dots,x_n)\,.$$

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 and μ then it is not difficult to verify that the expression

"There exist polynomials $g_1,\dots,g_r$ of degrees not exceeding μ such that the identity (4.6) is satisfied"

— can indeed be formulated within the lower predicate calculus as a predicate of the indeterminate coefficients of $f,f_1,\dots,f_r$. We denote this predicate by $Q_{\varrho\mu}(y_1,\dots,y_k)$.

Now let $a_1,\dots,a_k$ be an arbitrary set of constants and consider the set of statements

$$S=K_F\cup\{Q(a_1,\dots,a_k)\}\cup\{\sim Q_{\varrho\mu}(a_1,\dots,a_k)\}$$

where $\{\sim Q_{\varrho\mu}(a_1,\dots,a_k)\}$ indicates the set of all statements $\sim Q_{\varrho\mu}(a_1,\dots,a_k)$, $\varrho,\mu=1,2,3,\dots$ If S is consistent there exist polynomials $f,f_1,\dots,f_r$ with coefficients $a_1,\dots,a_k$ in a field M such that f vanishes for all joint zeros of $f_1,\dots,f_r$ in all algebraically closed extensions of M, although the conclusion of the theorem of Hilbert-Netto is not satisfied ((4.6) does not hold for any ϱ and $g_i(x_1,\dots,x_n)$). This is impossible and shows that S is contradictory. It follows that there exist positive integers $\varrho_1,\dots,\varrho_l$, $\mu_1,\dots,\mu_l$, such that the statement

$$(4.7)\qquad Q(a_1,\dots,a_k)\supset Q_{\varrho_1\mu_1}(a_1,\dots,a_k)\vee\dots\vee Q_{\varrho_l\mu_l}(a_1,\dots,a_k)$$

is deducible from K. Now if

$$f^\varrho=\sum g_if_i$$

then for any positive λ

$$f^{\varrho+\lambda}=\sum G_if_i$$

where $G_i=f^\lambda g_i$. We conclude that, for all ϱ,μ,

$$Q_{\varrho\mu}(a_1,\dots,a_k)\supset Q_{\varrho+\lambda,\mu+m\lambda}(a_1,\dots,a_k)$$

is deducible from K_F, where m is the degree of f, as before. It follows that if ϱ_0 is the maximum ϱ in the implicate of (4.7), then we may replace all $Q_{\varrho_i\mu_i}$ by $Q_{\varrho_0,\mu_i+m(\varrho_0-\varrho_i)}$. Again, if μ_0 is the greatest among the numbers $\mu_i+m(\varrho_0-\varrho_i)$ then we also have that

$$Q_{\varrho_0,\mu_i+m(\varrho_0-\varrho_i)}(a_1,\dots,a_k)\supset Q_{\varrho_0\mu_0}(a_1,\dots,a_k)$$

is deducible from K_F. (4.7) then entails that

$$Q(a_1,\dots,a_k)\supset Q_{\varrho_0\mu_0}(a_1,\dots,a_k)$$

is deducible from K_F, and the same therefore applies to the statement

$$(x_1)\dots(x_k)[Q(x_1,\dots,x_k)\supset Q_{\varrho_0\mu_0}(x_1,\dots,x_k)]\,.$$

Thus, we have established the existence of upper bounds for ϱ and for the degrees of the polynomials g_i, for given degrees of $f, f_1, \ldots, f_r$. These bounds are independent of the particular field of coefficients and even of the characteristic of the field. The result is not new (compare [6], chapter 8) but its derivation has been simplified here considerably by the use of the projection of a predicate from K_F^* to K_F.

5. Application to ordered fields. In this section we let $K = K_Q$ and $K^* = K_Q^*$, where K_Q is a set of axioms for the concept of an ordered field formulated in terms of the relations of equality, order, multiplication and addition, and without constants, and K_Q^* is a set of axioms for the concept of a real closed ordered field formulated in a similar way (compare [8] and section 2 above). It was shown in section 2 that K_Q^* is model-complete relative to K. The remaining conditions of Theorem (3.5) are also satisfied, and we conclude that every predicate which is defined in K_Q^* possesses a projection from K_Q^* onto K_Q.

(5.1) 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 $f(x_1, \ldots, x_n) \geqslant 0$ for all $x_1, \ldots, x_n$ in the real closure M^* of M, for which $g(x_1, \ldots, x_n) = 0$. 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

$$(5.2)\qquad \big(h(x_1, \ldots, x_n)\big)^2 f(x_1, \ldots, x_n) = \sum_{i=1}^{r} c_i \big(h_i(x_1, \ldots, x_n)\big)^2 + k(x_1, \ldots, x_n)\, g(x_1, \ldots, x_n)$$

and such that $h(x_1, \ldots, x_n)$ does not belong to (g) (i. e. is not divisible by g). Moreover, there are bounds for the number of squares r required in (5.2) 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 a field M, but that no identity of the type of (5.2) exists. It follows that there can be no identity

$$f = \sum_{i=1}^{r} c_i g_i^2$$

in the field of fractions M' of the quotient ring $M[x_1, \ldots, x_n]/(g)$. This in turn entails (compare [10]) that there exists an ordering of M' which

continues the ordering of M, such that $f < 0$. 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,

$$(5.3)\qquad f(\xi_1, \ldots, \xi_n) < 0, \quad g(\xi_1, \ldots, \xi_n) = 0\,.$$

Now the statement "there exist $x_1, \ldots, x_n$, such that $f(x_1, \ldots, x_n) < 0$ and $g(x_1, \ldots, x_n) = 0$" can be formulated in the lower predicate calculus in terms of the relations of K_Q and the coefficients of f and g. Let this formal statement be called X. Then X holds in the real closure of M' and since K_Q^* is model-complete, X holds also in all other real-closed extensions of M, and, in particular, in the real closure of M. This is contrary to the hypothesis of the theorem and proves that an identity (5.2) exists.

So far, we have followed the reasoning of [10] and [11]. To prove the existence of the required bounds, we have to make use of a different kind of argument. We 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 range 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_Q^* onto to K_Q.

Next we formulate a predicate $T(y_1, \ldots, y_j)$ which states, in terms of the relations of equality, addition and multiplication, 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 formulae which affirm that g cannot be written as the product of two polynomials of degrees s and $m-s$, $1 \leqslant s \leqslant m-1$. Note that $T(y_1, \ldots, y_j)$ implies irreducibility in the given field, not absolute irreducibility. Thus the conjunction $T(y_1, \ldots, y_j) \wedge R(y_1, \ldots, y_k)$ states that g is of positive degree and irreducible in the field under consideration, and that $f \geqslant 0$ whenever $g = 0$ in any real-closed extension of the given field.

On the other hand, for given positive integers r and μ, it is not difficult to formulate a predicate $Q_{r\mu}(y_1, \ldots, y_k)$ which states that there exist polynomials $h, h_1, \ldots, h_r, k$ of degrees not exceeding μ and positive elements $c_1, \ldots, c_r$ such that the identity (5.2) is satisfied and such that h is not divisible by g. (Note that the c_i appear as quantified variables in the formal predicate.) Then for any set of constants $a_1, \ldots, a_k$, the statement

$$(5.4)\qquad Q_{r\mu}(a_1, \ldots, a_k) \supset Q_{r_0\mu_0}(a_1, \ldots, a_k)$$

is deducible from K_Q provided $r_0 \geqslant r$, $\mu_0 \geqslant \mu$.

Now consider the set of statements

$$S = K_Q \cup \{T(a_1, \ldots, a_j), R(a_1, \ldots, a_k), \sim Q_{r\mu}(a_1, \ldots, a_k)\}$$

where r, μ vary over all positive integers. If S were consistent there would exist polynomials $f(x_1, \dots, x_n)$, $g(x_1, \dots, x_n)$ with coefficients in an ordered field M and satisfying the assumptions of Theorem (5.1) yet not satisfying any identity of the type of (5.2). This is impossible in view of the first part of the theorem, which has been proved already. We conclude that S is contradictory and hence, that a finite disjunction of the statements $Q_{r\mu}(a_1, \dots, a_k)$ is deducible from

$$K_Q \cup \{T(a_1, \dots, a_j), R(a_1, \dots, a_k)\}.$$

(5.4) then shows (compare a similar argument in section 4 above) that this disjunction can be replaced by a single statement $Q_{r_0\mu_0}(a_1, \dots, a_k)$. Thus

$$T(a_1, \dots, a_j) \wedge R(a_1, \dots, a_k) \supset Q_{r_0\mu_0}(a_1, \dots, a_k) \tag{5.5}$$

is deducible from K_Q. The integers r_0 and μ_0 may serve as the bounds whose existence was to be proved.

Let us consider in particular the case $n=1$, $x_1 = x$. Since every polynomial is now congruent modulo g to a polynomial of degree less than g, it is sufficient to consider the case $l \leqslant m$. Moreover, since h is not divisible by g it possesses an inverse modulo g. Accordingly, we may replace (5.2) by

$$f(x) \equiv \sum_{i=1}^{r} c_i \big(h_i(x)\big)^2 \quad \bmod g(x)$$

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 $M(\alpha)$ be the field obtained by adjoining a root α of g to M, and suppose that M is formally real. Let β be an element of $M(\alpha)$, $\beta \neq 0$. Then β can be written as

$$\beta = b_0 + b_1\alpha + \dots + b_\lambda \alpha^\lambda = f(\alpha),$$

say, where

$$f(x) = b_0 + b_1 x + \dots + b_\lambda x^\lambda, \qquad \lambda < m.$$

Now consider the following conditions:

(5.6) $f(x) > 0$ for all values $x \in M^*$ for which $g(x) = 0$, where M^* is the real closure of M.

(5.7) $\beta > 0$ in all possible orderings of $M(\alpha)$.

(5.8) Let $M_1 = M(\alpha)$, $M_2, \dots, M_s$ be the subfields of M^* which are conjugate to $M(\alpha)$ with respect to M. Then the conjugates of β in $M_1, \dots, M_s$, $\beta_1 = \beta$, $\beta_2, \dots, \beta_s$ are all positive.

Thus, if M is the field of rational numbers, the fields M_i are the real conjugate fields of $M(\alpha)$ and the condition (5.8) states that β is totally positive in $M(\alpha)$. We shall use the same terminology for the more general case considered here.

(5.6) entails (5.7). For if there exists an ordering of $M(\alpha)$ such that $\beta < 0$ then this can be continued into the real closure of M, M^*. We then have, in M^*,

$$g(\alpha) = 0, \qquad f(\alpha) < 0.$$

Thus the statement "there exists an x such that $g(x) = 0$, $f(x) < 0$" holds in M^*, and this contradicts (5.6).

(5.7) entails (5.8). For any ordering of M_i, $i > 1$, that continues the order of M induces an ordering of $M_1 = M(\alpha)$ which continues the order of M. This ordering of $M(\alpha)$ is obtained by determining the positivity of any element of $M(\alpha)$ in accordance with the positivity of the corresponding element of M_i. Hence $\beta_i < 0$ entails $\beta < 0$ in the ordering of $M(\alpha)$ just defined. This contradicts (5.7).

Finally, (5.8) entails (5.6). For if (5.6) is not satisfied, then there exists an element α' in the real closure of M such that $g(\alpha') = 0$, $\beta' = f(\alpha') < 0$. ($f(\alpha') = 0$ is impossible since f is of lower degree than g and does not vanish identically.) Then α' is one of the conjugates of α and generates a subfield $M(\alpha')$ of M^*, while β' is the corresponding conjugate of β. It follows that β is not totally positive, contradicting (5.8).

Combining these results, we see that (5.6) and (5.8) are equivalent. Hence, from Theorem (5.1),

(5.9) 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*

$$\beta = \sum_{i=1}^{r} c_i \gamma_i^2, \quad c_i \geqslant 0, \quad c_i \in M, \quad \gamma_i \in M', \quad i = 1, \dots, r. \tag{5.10}$$

The integer r depends only on the degree of M' over M. It does not depend on the particular choice of M or of M' or of β.

(5.11) Corollary. *If there exists a positive integer ϱ such that every positive element of M can be represented as the sum of ϱ squares of elements of M then (5.10) may be replaced by*

$$\beta = \sum_{i=1}^{s} \gamma_i^2, \quad \gamma_i \in M', \quad i = 1, \dots, s,$$

where s (i. e. $s = r\varrho$) may now depend on M but not on M' or β.

For example, if M is the field of rational numbers then $\varrho=4$. However, in that case a well-known theorem of Hilbert's (first proved by Siegel [12]) states that s is even independent of the degree of M' over M, more precisely, $s=4$.

Theorem (5.1) overlaps with theorem 3.1 of [11] for certain particular cases. [11] includes the consideration of a general variety V in place of the variety (primal) of a single polynomial, $g(x_1,\dots,x_n)$, with which we are concerned in the present paper. Also, in [11] we admit ancillary conditions of the form $g_i(x_1,\dots,x_n)>0$. It appears that there would be no difficulty in including the latter possibility also in the present analysis. On the other hand, it does not seem an easy matter to prove the existence of bounds r and μ as in (5.1) above for general irreducible V, such that these bounds depend only on the degrees of the polynomials of a specified basis of the prime ideal which belongs to V (but not on their particular coefficients). The reason is that, so far as the present author knows, it has not yet been established that the property of a set of polynomials to generate a prime ideal can be represented as a predicate of the coefficients of these polynomials within the lower predicate calculus. The question does not arise in the corollary (3.9) of [11] because in that corollary the variety V is kept constant implicitly.

The present paper also goes beyond [11] in admitting ordered fields M which are not real-closed. Both extensions — to arbitrary ordered fields M and to variable coefficients of $g(x_1,\dots,x_n)$ — were required in order to derive (5.9) and its corollary (5.11), which formed the starting point of the present investigation.

References

[1] L. Henkin, Review of ref. 5, J. Symbolic Logic 20 (1955), p. 185-186.

[2] — *Two concepts from the theory of models*, J. Symbolic Logic 21 (1956), p. 28-32.

[3] J. Herbrand, *Recherches sur la théorie de la démonstration*, Travaux de la Sociéte des Sciences et des Lettres de Varsovie, Cl. III, 33 (1930).

[4] J. Łoś, *On the extending of models (I)*, Fund. Math. 42 (1955), p. 38-54.

[5] A. Robinson, *Les rapports entre le calcul déductif et l'interprétation sémantique d'un système axiomatique*, Colloque international: Les méthodes formelles en axiomatique, Paris 1950 (published 1953), p. 35-52.

[6] — *Théorie métamathématique des idéaux*, Collection de Logique Mathématique, ser. A, N° 8, Paris-Louvain 1955.

[7] — *Ordered structures and related concepts*, Symposium on the Mathematical Interpretation of Formal Systems, Amsterdam 1954 (published 1956), p. 51-56.

[8] — *Complete Theories*, Amsterdam 1956.

[9] — *Note on a problem of L. Henkin*, J. Symbolic Logic 21 (1956), p. 33-35.

[10] — *On ordered fields and definite functions*, Math. Ann. 130 (1955), p. 257-271.

[11] — *Further remarks on ordered fields and definite functions*, Math. Ann. 130 (1956), p. 405-409.

[12] C. L. Siegel, *Darstellung total positiver Zahlen durch Quadrate*, Math. Zeit. 11 (1921), p. 246-275.

[13] A. Tarski, A. Mostowski and R. M. Robinson, *Undecidable Theories*, Amsterdam 1953.

[14] A. Tarski, *Contribution to the theory of models I, II*, Indagationes Math. 16 (1954), p. 572-581, 582-588.

[15] B. L. v. d. Waerden, *Moderne Algebra*, vol. 2, Berlin 1937.

UNIVERSITY OF TORONTO

Reçu par la Rédaction le 1.8.1956

Added in proof. G. Kreisel has recently published abstracts of some very interesting work which is related to the contens of sections 4 and 5 above. See Bulletin of the American Mathematical Society 63 (1957), p. 99-100.