Braun

Title for spine of Bound Copy

HILBERT'S SEVENTEENTH PROBLEM.

ACKNOWLEDGMENT

I wish to acknowledge the great debt I owe to my Research Director, Dr. John Denton of McGill University. If there is anything of value in this paper, then it was a reflection of his constant generous encouragement and inspiration.

John Brown

McGill 1965.

CONTENTS.

§ 1. INTRODUCTION.

1.1. A rational function $f(x_1,x_2,\ldots,x_n)$ having real coefficients is *positive definite* if its values are non-negative for all real values of $x_1,x_2,\ldots,x_n$. Hilbert conjectured that such a function can be written as a sum of squares of rational functions with real coefficients, and this appears as the seventeenth in his celebrated list of problems. [1].

The problem was solved by Artin in 1927, [2], using the typical non-constructive machinery of modern algebra, and in 1955 Artin asked Kreisel if the proof could be made constructive. Kreisel asserted that this was possible, and published indications of his method in two places, [3] and [4]. Although [3] gives more detail than [4], both papers are rather cryptic, neither giving a complete connected account: moreover, for the logical part of the argument, Kreisel uses the Hilbert-Bernays ε-theorems.

Here, using a direct application of the Herbrand theorem, we give a constructive proof of the following :-

> If $f(y_1,y_2,\ldots,y_k)$ is a positive definite rational function with rational coefficients, then it may be written as a sum of squares of rational functions with rational coefficients.

This result is then extended to the case where $f(y_1,y_2,\ldots,y_k)$ has real coefficients.

1.2. The proof follows the plan indicated in this section. We first outline a formal system of the predicate calculus, and a set of axioms for real closed fields. In this formalism we construct a formula F whose intuitive interpretation is

(Axioms of a real closed field) → ($f(y_1,y_2,\ldots,y_k)$ is positive definite).

Since the axioms are complete [5], a proof of F exists within the predicate calculus.

In his thesis of 1928, Herbrand has shown that since a derivation of F exists, a sequence of quantifier-free formulae may be constructed such that at some point in the sequence a formula R_F is obtained which is truth-functionally valid. The terms occurring in R_F may be interpreted as elements of fields obtained by successive algebraic extensions of a field *F*, namely the field of rational functions of $y_1,y_2,\ldots,y_k$, having rational coefficients, and the form of R_F gives immediate representations of $f(y_1,y_2,\ldots,y_k)$ as sums of squares in these fields.

We show the construction of these various fields, and then describe how the steps may be re-traced back to the ground field *F*, reducing the representations of $f(y_1,y_2,\ldots,y_k)$ as sums of squares exhibited in R_F to the required representation in *F* itself.

Finally we extend this to the case where the coefficients of $f(y_1,y_2,\ldots,y_k)$ are real.

§ 2. DESCRIPTION OF THE FORMAL SYSTEM.

2.1 We use the symbols 'x', 'y', and 'z' as formal variables, 'f^n' (or 'f') as an n-place function symbol, and 'P^n' (or 'P') as an n-place predicate symbol. 't' will denote a term, 'F', 'G', and 'H' will denote formulae, and 'a', 'b', and 'c' will denote constants. These symbols will be extended where necessary by inserting appropriate subscripts, or by other suitable means.

For negation, conjunction, disjunction, implication and equivalence we use '-', '&', 'v', '→', and '↔' respectively, and for universal and existential quantification we use 'A' and 'E' respectively.

In constructing terms and formulae following the usual rules, we use parentheses economically, omitting them whenever no ambiguity arises. Commas are treated equally parsimoniously, omitting them from terms constructed from function symbols, and from predicates constructed from predicate symbols.

The symbol '=' will be used as a name for a two-place predicate symbol, '+' and '.' as names for distinct binary operation symbols, '-' and '$^{-1}$' as names for distinct unary function symbols, and '0' and '1' as names for distinct constants. All of these may be interpreted naively to have their customary meanings, and where they occur we shall follow normal usage: in particular, using the usual rules of precedence, we omit parentheses wherever possible. In keeping with this, '≠' will denote

the negation of '=', 't^n' will mean '$t \cdot t \cdot \ldots \cdot t$' (n times), '$n \cdot t$' will mean '$t+t+\ldots+t$' (n times), and '$t_1 - t_2$' will mean '$t_1 + (-t_2)$'.

2.2 The formulae below named by the symbol '*A*' with subscripts as shown, are taken as the axioms of a real closed field.

A_1 $\quad Ax\ x = x$

A_2 $\quad AxAyAz\ x \neq y \vee z \neq y \vee x = z$

A_3 $\quad AxAyAz\ x \neq y \vee x+z = y+z$

A_4 $\quad AxAy\ x \neq y \vee (-x) = (-y)$

A_5 $\quad AxAyAz\ x \neq y \vee x \cdot z = y \cdot z$

A_6 $\quad AxAy\ x \neq y \vee x^{-1} = y^{-1}$

A_7 $\quad AxAyAz\ (x+y)+z = x+(y+z)$

A_8 $\quad AxAy\ x+y = y+x$

A_9 $\quad Ax\ 0+x = x$

A_{10} $\quad Ax\ x+(-x) = 0$

A_{11} $\quad AxAyAz\ (x \cdot y) \cdot z = x \cdot (y \cdot z)$

A_{12} $\quad AxAy\ x \cdot y = y \cdot x$

A_{13} $\quad Ax\ 1 \cdot x = x$

A_{14} $\quad Ax\ x=0 \vee x \cdot (x^{-1}) = 1$

A_{15} $\quad 1 \neq 0$

A_{16} $\quad AxAyAz\ x \cdot (y+z) = x \cdot y + x \cdot z$

A_{17} $\quad AxEy\ y^2 = x \vee y^2 = (-x)$

$A_{18,1}$ $\quad Ax_1Ax_2Ax_3Ey\ y^3 + x_1 \cdot y^2 + x_2 \cdot y + x_3 = 0$

$A_{18,2}$ $\quad Ax_1Ax_2Ax_3Ax_4Ax_5Ey\ y^5+x_1\cdot y^4+x_2\cdot y^3+x_3\cdot y^2+x_4\cdot y+x_5 = 0$

.
.
.

$A_{18,n}$ $\quad Ax_1Ax_2\ldots Ax_{2n+1}Ey\ y^{2n+1}+x_1\cdot y^{2n}+\ldots+x_{2n+1} = 0$

A_{19} $\quad AxAyAz\ x^2+y^2+z^2\neq o\ v\ (x=o\ \&\ y = o\ \&\ z = o)$

In dealing with any particular case a finite number of axioms of the form $A_{18,i}$ are required : exactly which are needed is determined by the nature of the given function $f(y_1,y_2,\ldots,y_k)$. We will assume that the formula

$A_{18,1}\ \&\ A_{18,2}\ \&\ldots\&\ A_{18,n}$, denoted by '$A_{18}$'

contains among its conjuncts those axioms required for the case on hand. The fact that the value of n may change from case to case is not important.

We will denote the formula

$A_1\ \&\ A_2\ \&\ldots\&\ A_{16}$ by 'S'

and $A_1\ \&\ A_2\ \&\ldots\&\ A_{19}$ by 'K'

§ 3. ALGEBRAIC PRELIMINARIES.

The following results are required for the main proof. Although their proofs can be formalised easily, they are treated informally for clarity.

3.1 <u>In a field in which K holds, any representation of zero as a sum of squares is trivial</u>.

The proof is by induction.

From A_{19},

$$\left(\sum_{i=1}^{m} x_i^2 = o\right) \rightarrow (x_1 = x_2 = \ldots = x_m = o)$$

holds for m = 1,2,3.

Now suppose that it holds for m = 1,2,3,...,s.

and that

$$\sum_{i=1}^{s+1} x_i^2 = 0$$

Then from A_{17} we have for some y,

$$\text{either } \sum_{i=1}^{s-1} x_i^2 = y^2 \quad \text{or} \quad \sum_{i=1}^{s-1} x_i^2 = -y^2$$

In the former case, $y^2+x_s^2+x_{s+1}^2 = 0$

In the latter case, $x_1^2+x_2^2+\ldots+x_{s-1}^2+y^2 = 0$

Since these are sums of 3 and s squares respectively, the required result follows easily from the inductive assumption.

3.2. In a field in which S holds, if y_1 and y_2 can be expressed as sums of squares, then so also can

(i) y_1+y_2 (ii) $y_1 \cdot y_2$ and (iii) $y_1^{-1}(y_1 \neq o)$.

The proofs of (i) and (ii) are trivial, and for (iii) we have

$$\left(\sum_{i=1}^{m} x_i^2\right)^{-1} = \sum_{i=1}^{m} u_i^2, \text{ where } u_i = x_i \cdot \left(\sum_{j=1}^{m} x_j^2\right)^{-1}$$

Corollary: In a field in which S holds, if $x_1 \cdot x = x_2$ where x_1 and x_2 can be represented (non-trivially) as sums of squares, then either

(1) 0 can be expressed as a non-trivial sum of squares,

or (2) x can be expressed as a sum of squares.

(for if $x_1 = 0$ (1) holds, and if $x_1 \neq 0$, then from (ii) and (iii) above, (2) holds.)

3.3 To clarify the next two sections we define (for sections 3.3 and 3.4 only) a *representation* in a field K to be an equation of the form

$$u = \sum_{i=1}^{n} a_i^2$$

where $a_i \in K$ $(i = 1, 2, \ldots, n)$, and where 'u' denotes either a prescribed element of K (denoted by 'f'), or else 0. The lemma of this section may now be stated thus :-

If f and t are elements of a field K in which S holds, then from a representation in $K(\sqrt{t})$ and in $K(\sqrt{-t})$ we can find a representation in the ground field K.

Proof: Let the given representations be

$$u_1 = \sum_{i=1}^{m} (a_i + b_i \cdot \sqrt{t})^2 \quad \text{where } a_i \in K \ , \ b_i \in K \ , \ (i=1,2,\ldots,m)$$

and $$u_2 = \sum_{j=1}^{n} (c_j + d_j \cdot \sqrt{t})^2 \quad \text{where } c_j \in K \ , \ d_j \in K \ , \ (j=1,2,\ldots,n)$$

It may be that on squaring out and collecting terms, we find

that in one of these the coefficient of $\sqrt{t}$ or of $\sqrt{-t}$ does not vanish. Suppose for definiteness that

$$u_1 = \sum_{i=1}^{m} a_1^2 + 2\Big(\sum_{i<j} \sum_{j=1}^{m} a_i b_j\Big)\cdot\sqrt{t} + t\cdot\sum_{i=1}^{m} b_i^2$$

$$\text{and that} \quad \sum_{i<j} \sum_{j=1}^{m} a_i b_j \neq 0.$$

Then $u_1 = \sum_{i=1}^{m} (a_i + b_i\cdot c)^2$ exhibits the required representation

where $c = \sqrt{t} = (u_1 - \sum_{i=1}^{m} a_i^2 - t\cdot\sum_{i=1}^{m} b_i^2)\cdot(2\sum_{i<j} \sum_{j=1}^{m} a_i\cdot b_j)^{-1}$

and hence $c \varepsilon K$.

Alternatively the coefficients of $\sqrt{t}$ and $\sqrt{-t}$ both vanish, and we have

$$u_1 = \sum_{i=1}^{m} a_i^2 + t\cdot\sum_{i=1}^{m} b_i^2$$

$$\text{and} \quad u_2 = \sum_{j=1}^{n} c_j^2 - t\cdot\sum_{j=1}^{n} d_j^2$$

If one of the coefficients of t vanishes, this gives a representation of 0 as a sum of squares, and otherwise we can eliminate t, obtaining

$$u_1\cdot\sum_{j=1}^{n} d_j^2 + u_2\cdot\sum_{i=1}^{m} b_i^2 = \sum_{i=1}^{m} a_i^2 \cdot \sum_{j=1}^{n} d_j^2 + \sum_{i=1}^{m} b_i^2\cdot\sum_{j=1}^{n} c_j^2$$

We may now replace u_1 and u_2 by their values. If $u_1 = u_2 = 0$, then from (i) and (ii) of 3.2 we have 0 expressed as a sum of squares. If $u_1 = 0$, $u_2 = f$, or if $u_1 = f$, $u_2 = 0$ we solve for f and obtain from 3.2 a representation of f as a sum of squares. Finally if $u_1 = u_2 = f$, then either $\Sigma d_j^2 + \Sigma b_i^2 = 0$,

giving 0 as a sum of squares, or else we again solve for f, and from 3.2 obtain f as a sum of squares.

3.4 If K is a field in which S holds, f a fixed element of K, and p(x) a polynomial of odd degree in $K[x]$, then from a representation in $K(\alpha)$ (where $p(\alpha) = 0$) we can find a representation in the ground field K.

Remark. We wish to apply this result to fields as defined in section 7.5, and so we anticipate the construction described therein, consequently making the following assumptions in the proof:

(i) In obtaining the initial representation we obtain a polynomial q(x) (corresponding to $p_{n+1}(x)$ of section 7.5), of odd degree, which is a divisor of p(x). The adjoined root α is a root of q(x).

(ii) The initial representation holds true no matter which root of q(x) is adjoined. In particular, if $q^*(x)$ is any odd-degree factor of q(x), then the representation holds if we take α as a root of $q^*(x)$.

(iii) Each element in the representation can be reduced to a polynomial in α, so that we may assume that we are given

$$u = \sum_{i=1}^{m} [h_i(\alpha)]^2 \quad (h_i(x) \in K[x],\ i=1,2,\ldots,m)$$

(iv) If a representation as in (iii) is found to hold when α is replaced by β, a root of some other odd-degree polynomial in $K[x]$, then the corresponding field $K(\beta)$ can be constructed.

Proof: Using the above notation, we have

$$u - \sum_{i=1}^{m} [h_i(x)]^2 \equiv 0 \pmod{q(x)}$$

I. It may be that $q(x)$ is a divisor of the left side, and that the degree of $q(x)$ is greater than 1. Then we have

$$u - \sum_{i=1}^{m} [h_i(x)]^2 = r(x) \cdot q(x)$$

We may assume that each $h_i(x)$ has been reduced to a polynomial of degree less than that of $q(x)$ by taking the remainder on division by $q(x)$ in the usual way. Then if $\deg.q(x) = 2n + 1$, the left side has even degree $\leq 4n$, and hence $r(x)$ has odd degree less than $2n + 1$. We may therefore put

$$u = \sum_{i=1}^{m} [h_i(\beta)]^2$$

where β is a root of $r(x)$, and from remark (iv), the construction of $K(\beta)$ can be carried out, and the process repeated, starting with

$$u - \sum_{i=1}^{m} [h_i(x)]^2 \equiv 0 \pmod{r(x)},$$

where $\deg.r(x) < \deg.q(x)$.

II. Alternatively, it may be that $u - \Sigma[h_i(x)]^2$ is identically zero. In this case, either 'x' does not occur in any of the $h_i(x)$, so that $h_i(x) = c_i \in K$ $(i=1,2,\ldots,m)$ and we have the representation

$$u = \sum_{i=1}^{m} c_i^2 ,$$

or else the coefficient of x^{2s} vanishes (where s is the highest power of x occurring among the terms of the $h_i(x)$) thus exhibiting zero as a sum of squares.

III. If I and II do not arise, then it may be that $q(x)$ is linear, say $q(x) = ax + b$, $a \neq 0$. In this case,

$$u = \sum_{i=1}^{m} [h_i((-b)\cdot(a^{-1}))]^2$$

gives the required representation.

IV. Finally, if cases I, II, and III do not apply, we have

$$u - \sum_{i=1}^{m} [h_i(x)]^2 \equiv 0 \pmod{q(x)}$$

where the left side is not identically zero, $q(x)$ is not a divisor of the left side, and $q(x)$ has odd degree greater than 1. In this case the left side and $q(x)$ must have a common factor which(since I does not arise) is a proper divisor of $q(x)$. We can find this (greatest) common divisor, say $g(x)$, and then define

$$h(x) = g(x) \text{ (if deg.}g(x) \text{ is odd)}$$

and $$h(x) = q(x)/g(x) \text{ (if deg.}g(x) \text{ is even).}$$

Clearly $h(x)$ is an odd-degree factor of $q(x)$ and hence from remark (ii) we have

$$u - \sum_{i=1}^{m} [h_i(x)]^2 \equiv 0 \pmod{h(x)}$$

where $\deg.h(x) < \deg.q(x)$,

and the process may be repeated starting with this equation.

Since these cases are exhaustive, either the process terminates with II or III, or we obtain a representation where the degree of the (odd-degree) 'defining polynomial' has been reduced. Hence if II does not arise, after a finite number of steps the defining polynomial is reduced to a linear one, and the process terminates with III.

§4. THE HERBRAND METHOD.

4.1 The Herbrand method provides a formal procedure which reflects the intuitive 'indirect' method of proof. Since the main theorem is not well known, it is described here in some detail, and some idea of the motives underlying the various steps is provided. In this section a simple example is discussed, entirely at the intuitive level.

Consider the formula G:

$$Ay_1Ex_1\ Px_1y_1\ v\ Ex_2Ay_2\ \text{-}Py_2x_2 \quad \ldots\ldots\ldots\ldots(1)$$

To 'prove' this indirectly, intuitively, we would assume the satisfiability of its negation, (-G):

$$Ey_1Ax_1\ \text{-}Px_1y_1\ \&\ Ax_2Ey_2\ Py_2x_2 \quad \ldots\ldots\ldots\ldots(2)$$

and search for a contradiction. Now the meaning of (2) can be conveyed by the formula

$$Ax_1\ \text{-}Px_1y_1\ \&\ Ax_2\ Py_2(x_2)x_2 \quad \ldots\ldots\ldots\ldots(3)$$

where 'y_1' denotes a term whose existence is asserted by the 'Ey_1' of (2), and '$y_2(x_2)$' denotes a term functionally dependent on x_2, and whose existence is asserted by the 'Ey_2' of (2).

The satisfiability of (-G) is equivalent to the validity of (3), in which the roles of the symbols 'y_1' and 'y_2' have changed. Clearly, then, the satisfiability of (-G) is equivalent to the invalidity of the negation of (3), namely

$$Ex_1\ Px_1y_1\ \ v\ \ Ex_2\ \text{-}Py_2(x_2)x_2 \quad \ldots\ldots\ldots\ldots(4)$$

(This formula is a *functional form* of G, denoted by 'fn.(G)')

If x_1 and x_2 are replaced by terms in (4), and the existential quantifiers are removed, we have a *substitution instance* of fn.(G).

For example, if t_1 and t_2 are terms, then

$$Pt_1y_1 \ v \ -Py_2(t_2)t_2 \quad \ldots\ldots\ldots\ldots(5)$$

is such an instance. The invalidity of (4) means that every such substitution instance is 'false', and indeed any finite disjunction of substitution instances is 'false'. (If D is any finite set of terms, then the disjunction of all possible substitution instances of fn.(G) using terms of D is a *Herbrand Expansion of* G *over* D , denoted by ' R(D,G) '.)

Summarising the discussion so far, we have obtained from G a formula fn.(G), intuitively equivalent to G when the functional terms it contains are appropriately interpreted. Now fn.(G) is valid if we can exhibit a disjunction of substitution instances which is 'true'.

This is done by constructing a finite set of terms D, and showing that R(D,G) is 'true'. Since R(D,G) is a disjunction of substitution instances, at least one substitution instance is 'true', and thus G is 'proved'.

In this case y_1 is a term, and $y_2(t)$ is a term where t is a term. We may therefore construct a sequence of terms

$$y_1, \quad y_2(y_1), \quad y_2(y_2(y_1)), \ \ldots$$

Taking D as the set $\{y_1, y_2(y_1)\}$, we find R(D,G) to be

$$(Py_1y_1 \ v \ \underline{-Py_2(y_1)y_1}) \ v \ (Py_1y_1 \ v \ -Py_2(y_2(y_1))y_2(y_1) \ )$$
$$v \ (\underline{Py_2(y_1)y_1} \ v \ -Py_2(y_1)y_1) \ v \ (Py_2(y_1)y_1 \ v \ -Py_2(y_2(y_1))y_2(y_1))$$

The underlined disjuncts show that R(D,F) is truth-functionally valid, as required.

Interpreted intuitively, as illustrated above, the Herbrand method consists of attempting to construct a counter-example to a given formula, making the 'best' (in some sense) effort to do so, and exhibiting a contradiction.

The process exemplified above is described in detail following the statement of the Herbrand Theorem :-

4.2 Given any formula F of the predicate calculus, we can effectively construct a finite set of terms D and thence a quantifier-free formula R(D,F) such that R(D,F) is truth-functionally valid if and only if a proof of F exists within the predicate calculus.

4.3 Construction of fn(F)

The given formula F is first *rectified* by arranging that the quantified variables are pairwise distinct, and that no variable occurs both free and bound. In a notation designed specifically to accommodate the Herbrand Theorem this can be done by including in the ordinary inductive definition of formulation the clauses

'If G_1 and G_2 are formulae, then $(G_1 \ \& \ G_2)$ and $(G_1 \ v \ G_2)$ are formulae iff no variable occurring in G_1 is bound in G_2 and no variable occurring in G_2 is bound in G_1.',

and, 'If F is a formula, then(AzF) and(EzF) are formulae iff z does not occur bound in F.', and then arranging that all connectives are written in terms of '&', 'v' and '-'.

Clearly alphabetic changes can easily be made to bring a formula into rectified form. For example, if F is

$$(AxAyEzPxyz) \rightarrow -(AxEyAzEt(Qxctv\text{-}Rxzy))$$

where P, Q, and R are three-place predicate symbols, and c is a constant or a free variable, then a rectified form of F is

$$-(Ax_1Ax_2Ey_1Px_1x_2y_1) \vee -(Ax_3Ey_2Ax_4Ey_3(Qx_3cy_3 \vee -Rx_3x_4y_4))$$

Next, we *rationalise* F by writing an equivalent formula which has negation signs 'pushed in' until they occur only immediately preceding predicate symbols, and then removing 'double' negation signs. Formally, formulae of the forms -AyF, -ExF, -(F & G), -(FvG), and --F, are replaced by Ey-F, Ax-F, -Fv-G, -F&-G, and F, respectively.

In our example above, this form, denoted by 'rat·(F)' is

$$(Ex_1Ex_2Ay_1\text{-}Px_1x_2y_1) \vee (Ex_3Ay_2Ex_4Ay_3(-Qx_3cy_3 \,\&\, Rx_3x_4y_2))$$

In this example we have arranged that existentially and universally quantified variables are denoted by 'x' and 'y' respectively, and we employ this convention throughout.

From rat·(F) we construct fn(F) as follows :-

(1) If no universal quantifiers occur in rat·(F), then fn(F) is rat·(F). Otherwise,

(2) If 'Ay_i' occurs for some i, and is not in the scope of any existential quantifier, then the symbols 'Ay_i' are deleted, and other occurrences of y_i left unchanged.

(3) If 'Ay_i' occurs for some i, and is within the scopes of $Ex_{i_1}, Ex_{i_2}, \ldots, Ex_{i_k}$ in left to right order, then the symbols 'Ay_i' are deleted, and each remaining occurrence of 'y_i' is replaced by the function symbol '$y_i(x_{i_1}x_{i_2}\ldots x_{i_k})$'.

When all occurrences of universal quantifiers have been deleted by repeated application of (2) and (3), the remaining formula is fn(F).

In our example, fn(F) is

$$(Ex_1Ex_2\text{-}Px_1x_2y_1(x_1x_2)) \vee (Ex_3Ex_4(\text{-}Qx_3cy_3(x_3x_4) \;\&\; Rx_3x_4y_2(x_3))$$

4.4. Construction of $R(D', F)$

To obtain a Herbrand expansion of F over a given non-empty finite set of terms D', we note first that if fn(F) is quantifier free, then $R(D', F)$ is simply fn(F).

Otherwise, suppose all the quantifiers occurring in fn(F) are $Ex_1, Ex_2, \ldots Ex_n$ in left to right order.

Let $t_1, t_2, \ldots, t_n)$ be any ordered n-tuple of terms (not necessarily distinct) of D'. Deleting each occurrence of the symbols $Ex_1, Ex_2, \ldots Ex_n$ from fn(F) (and parentheses in accordance with the rules of formulation) and replacing each remaining occurrence of x_i by t_i ($i = 1, 2, \ldots, n$) gives a substitution instance of fn(F).

The disjunction of all possible substitution instances using terms from D' is $R(D',F)$. In our example, if $D' = \{c\}$, then $R(D',F)$ would be the single substitution instance

$$(-Pccy_1(cc)) \vee (-Qccy_3(cc) \,\&\, Rccy_2(c))$$

4.4. Construction of $\{D_i\}$

We now define a sequence of sets of terms inductively, thus :-

D_1 consists of all free variables (not functional symbols) and constants occurring in fn(F). If this is null, then D_1 consists of the single symbol '1'

D_{i+1} consists of all terms of D_i together with all terms occurring in $R(D_i,F)$.

(Hence D_{i+1} consists of all terms of D_i together with new terms formed by substituting terms of D_i into the functional variables occurring in fn(F)).

In our example, fn(F) contained an occurrence of 'c' (unbound), and functional variables $y_1(x_1x_2)$, $y_2(x_3)$, and $y_3(x_3x_4)$.

Hence D_1 is {c}, D_2 is $\{c, y_1(cc), y_2(c), y_3(cc)\}$

D_3 consists of 37 terms in all. (e.g. $y_1(y_1(cc)y_2(c))$, $y_2(y_2(c))$, etc)

According to the Herbrand Theorem, if a derivation of F is possible in the predicate calculus, then for some finite integer $p>0$, $R(D_p,F)$ is truth-functionally valid.

In this paper no specific use will be made of the sequence $\{D_i\}$, and it will be sufficient for our purpose to assert that we can construct a finite set of terms D (i.e. any finite set containing D_p) such that $R(D, F)$ is truth-functionally valid.

An alternative description of the above constructions is given in [6], pp.700-702.

§ 5. COMPLETENESS OF K

In the problem in hand we are concerned with the formula H:

$$Ay_1Ay_2\ldots Ay_kEx\ f(y_1y_2\ldots y_k) = x^2$$

where $f(y_1y_2\ldots y_k)$ is the name in our formalism for a given rational function $f(y_1,y_2,\ldots,y_k)$ with rational coefficients, and with the formula F: $K \rightarrow H$.

The crux of our proof will be that a finite set of terms D can be effectively constructed such that $R(D,F)$ is truth-functionally valid, by the Herbrand theorem. However this in turn depends upon the existence of a proof of F, as stipulated in the Herbrand theorem. We must show, therefore, that if $f(y_1,y_2,\ldots,y_k)$ really is positive definite, then a derivation of F exists.

Now Tarski has shown [5] that if G is any formula where '=' and '<' are the only predicate symbols and '+', '·', '-', and '$^{-1}$' the only operation symbols, then a formula U(G) in the same system can be found, quantifier-

free, such that G ↔ U(G) follows from the axioms of a complete ordered field. (i.e. from a set of axioms equivalent to K. see [5], p 49). In the present case, U(H) has no variables, and so is completely decidable. Since U(H) ↔ H follows from K, K → H is thus completely decidable. This establishes that if $f(y_1,y_2,\ldots,y_k)$ is a positive definite rational function with rational coefficients, then a derivation of F exists.

(We return to Tarski's 'completeness' result in section 9 , when the main result is extended to the case where the given function has real coefficients).

§ 6. APPLICATION OF THE HERBRAND THEOREM TO THE CENTRAL PROBLEM.

6.1. Suppose that a given rational function $f(y_1,y_2,\ldots,y_k)$ with rational coefficients is positive definite. The algebraic representation of this function is of course a term of our formal system, and we denote it by '$f(y_1y_2\ldots y_k)$'.

From § 5, the formula H, namely

$$Ay_1Ay_2\ldots Ay_k \; Ex \;\; f(y_1y_2\ldots y_k) = x^2$$

is provable from K. i.e. within the predicate calculus a proof exists for F, namely

$$(A_1 \;\&\; A_2 \;\&\; \ldots \;\&\; A_{18} \;\&\; A_{19}) \rightarrow H.$$

Hence, applying the Herbrand Theorem, a finite domain of terms D can be effectively constructed such that R(D,F) is truth-functionally valid.

6.2 Following the process in §4, we first rectify F. In doing this we will retain the symbols 'y_1', 'y_2',...,'y_k' in the sub formula H, replace the 'y' of A_{17} by 'r' and that of $A_{18,j}$ by 'r_{2j+1}' (j=1,2,...,n). Next, F is written in rational form, and finally the universal quantifiers are deleted replacing occurrences of the universally quantified variables by function symbols where this is appropriate, as prescribed. In the interest of clarity, fn(F) thus obtained is shown below, using the symbol '$\overline{r_{2j+1}}$' to denote the function symbol '$r_{2j+1}(x_{j,1},x_{j,2},\ldots,x_{j,2j+1})$' (j = 1,2,...,n).

$$(Ex_2\ x_2 \neq x_2)\ v\ (Ex_3Ex_4Ex_5\ \ 3 = x_4\ \&\ x_5 = x_4\ \&\ x_3 \neq x_5)$$
$$v(Ex_6Ex_7Ex_8\ x_6 = x_7\ \&\ x_6+x_8 \neq x_7+x_8)$$
$$v\ (Ex_9Ex_{10}\ x_9 = x_{10}\ \&\ (-x_9) \neq (-x_{10}))$$
$$v\ (Ex_{11}Ex_{12}Ex_{13}\ x_{11} = x_{12}\ \&\ x_{11}\cdot x_{13} \neq x_{12}\cdot x_{13})$$
$$v\ (Ex_{14}Ex_{15}\ \ x_{14} = x_{15}\ \&\ \ x_{14}^{-1} \neq x_{15}^{-1})$$
$$v\ (Ex_{16}Ex_{17}Ex_{18}\ \ (x_{16}+x_{17}) + x_{18} \neq x_{16}+(x_{17}+x_{18}))$$
$$v\ (Ex_{19}Ex_{20}\ \ x_{19} + x_{20} \neq x_{20}+x_{19})$$
$$v\ (Ex_{21}\ 0 + x_{21} \neq x_{21})\ \ v\ \ (Ex_{22}\ \ x_{22} + (-x_{22}) \neq 0)$$
$$v\ (Ex_{23}E_{24}\ Ex_{25}\ \ (x_{23}\cdot x_{24})\cdot x_{25} \neq x_{23}\cdot(x_{24}\cdot x_{25}))$$
$$v\ (Ex_{26}Ex_{27}\ x_{26}\cdot x_{27} \neq x_{27}\cdot x_{26})$$
$$v\ (Ex_{28}\ 1\cdot x_{28} \neq x_{28})\ v\ (Ex_{29}\ \ x_{29} \neq 0\ \&\ x_{29}\cdot(x_{29}^{-1}) \neq 1)\ v\ (1 = 0)$$
$$v\ (Ex_{30}Ex_{31}Ex_{32}\ \ x_{30}(x_{31} + x_{32}) \neq x_{30}\cdot x_{31} + x_{30}\cdot x_{32})$$
$$v\ (Ex_{33}\ \ r(x_{33})^2 \neq x_{33}\ \&\ r(x_{33})^2 \neq (-x_{33}))$$

$$v\ (Ex_{1,1}Ex_{1,2}Ex_{1,3}\ \overline{r}_3^{\,3} + x_{1,1}\cdot\overline{r}_3^{\,2} + x_{1,2}\cdot\overline{r}_3 + x_{1,3}\neq 0)$$

$$v\ (Ex_{2,1}Ex_{2,2}Ex_{2,3}Ex_{2,4}Ex_{2,5}$$

$$\overline{r}_5^{\,5} + x_{2,1}\cdot\overline{r}_5^{\,4} + x_{2,2}\cdot\overline{r}_5^{\,3} + x_{2,3}\cdot\overline{r}_5^{\,2} + x_{2,4}\cdot\overline{r}_5 + x_{2,5}\neq 0)$$

$$v$$
$$\vdots$$
$$v\ (Ex_{n,1}Ex_{n,2}\ldots Ex_{n,2n+1}\ \overline{\overline{r_{2n+1}}}^{\,2n+1} + x_{n,1}\cdot\overline{\overline{r_{2n+1}}}^{\,2n} + \ldots + x_{n,2n+1}\neq 0)$$

$$v\ (Ex_{34}Ex_{35}Ex_{36}\ x_{34}^{\,2} + x_{35}^{\,2} + x_{36}^{\,2} = 0\ \&\ (x_{34}\neq 0\ v\ x_{35}\neq 0\ v\ x_{36}\neq 0)$$

$$v\ (Ex_1\ f(y_1y_2\ldots y_k) = x_1^{\,2}).$$

The first sixteen disjuncts correspond to A_1 to A_{16} and contain no universal quantifiers. The constants 0 and 1 appear. The 17th to $(17 + n)^{th}$ disjuncts corresponding to A_{17} and $A_{18,1}$ to $A_{18,n}$ contain the only occurrences of functional terms, namely $r(x_{33})$ and $r_{2j+1}\ (x_{j,2},\ldots,x_{j,2j+1})$ $(j = 1,2,\ldots,n)$. The last disjunct corresponding to H contains the free variables $y_1, y_2, \ldots, y_k$.

Following the process for obtaining D, the set of terms for which R(D,F) is truth-functionally valid, we see that D consists of

(i) $0,\ 1,\ y_1,\ y_2,\ldots,y_k$.

(ii) terms of the forms $-t_1$, t_1^{-1}, $t_1 + t_2$, and $t_1\cdot t_2$ where t_1 and t_2 are terms of D.

(iii) terms of the form $r(t_1)$ and $r_{2j+1}\ (t_1t_2\ldots t_{2j+1})$ where $t_1, t_2, \ldots, t_{2j+1}$ are terms of D. $(j = 1,2,\ldots,n)$.

D provides the terms to be substituted in fn(F), the disjunction of the substitution instances constituting R(D,F). Terms will occur in R(D,F) which do not occur in D itself (e.g. if $t \in D$, then r(t) occurs in a disjunct of R(D,F) corresponding to A_{17}, but r(t) need not be a term of D). We define D* to be the set of all terms occurring in R(D,F).

6.3 Since D* is finite, it can be completely ordered, and we choose an ordering where the condition holds that if t_1 occurs in t_2 , then t_1 precedes t_2 in the ordering. (e.g. trivially t_1 precedes $t_1 + t_2$, and importantly if t_2 is $r(t_1)$ or $r_{2j+1}(t_{k_1}, t_{k_2}, \cdots, t_{k_{2j+1}})$, where for some i t_{k_i} is t_1, then t_1 precedes t_2.)

Having established this ordering we now construct a sequence of infinite nested sets

$$D_o \subset D_1 \subset \ldots \subset D_q$$

as follows :-

(1) D_o consists of 0,1, and all possible terms built up from these using '+', '-', '.', and '$^{-1}$'.

(2) D_1 consists of all terms of D_o together with $y_1, y_2, \ldots, y_k$, and all terms built up from these using '+', '-', '.', and '$^{-1}$'.

(3) Having obtained D_i ($i \geq 1$), we find t_{i+1}, the first term in the ordering of D* which is not in D_i. If no such term exists, then $D_i = Dq$, and the sequence terminates.

Otherwise, D_{i+1} consists of all terms of D_i together with t_{i+1}, and all terms built up from these using '+', '-', '·', and '$^{-1}$'.

Since D* is finite, it is obvious that the above process terminates giving $D_0 \subset \ldots \subset Dq$, and that $D^* \subset D_q$. Each set D_{i+1} in the sequence ($i \geq 1$) is brought about by inserting exactly one new <u>functional</u> term into D_i, and closing the resulting set under the rational operations.

§ 7. CONSTRUCTION OF FIELDS.

7.1 Truth Assignments.

The only predicate symbol occurring in fn(F), and hence in R(D,F), is the dyadic symbol '='. If we have a rule for allocating truth values to formulae of the kind '$t_1 = t_2$' where t_1 and t_2 are terms of D*, then the component disjuncts of R(D,F) may be evaluated. We call T a *truth-assignment* to D* where T is a function whose domain is the set of all formulae '$t_1 = t_2$', for all $(t_1,t_2) \in D^* \times D^*$ and which ranges over two values, say 'true' and 'false'.

If T is such that it makes each instance of an axiom 'true', we shall say that T *satisfies* that axiom, (e.g. if D* is $\{t_1,t_2,\ldots,t_m\}$, and T makes '$t_i = t_i$' 'true' ($i = 1,2\ldots,m$), then T satisfies A_1 on D*).

We should note at this point that if T satisfies an axiom, A_i, on D*, then in R(D,F) it makes all disjuncts corresponding to that axiom <u>false</u>. (Since A_i appears in F in the form ...v-A_iv....vH) Now the Herbrand Theorem states that R(D,F) is 'truth functionally valid'. In other words, no matter how T is constructed to D*, R(D,F) will have value 'true'. We are going to construct a multiplicity of truth-assignments T to D*, so as to satisfy the axioms A_1 & A_2 &...& A_{18} - i.e. all these truth assignments make all the substitution instances of the disjuncts of R(D*,F) corresponding to these axioms 'false'. For every such T, since R(D*,F) comes out 'true', there must be therefore at least one substitution instance corresponding to (-A_{19} v H) which is 'true' and hence for each such T a 'true' representation of zero as a sum of squares, or of f as a sum of squares is thus exhibited.

The remainder of this chapter is devoted to the constructions of truth-assignments to D* which satisfy S. We do this by defining truth-assignment T_o to D_o (as defined in 6.3) and then showing how to extend any T_i to D_i either to T_{i+1} on D_{i+1} or to T'_{i+1} and T''_{i+1} on D_{i+1}; depending on whether the functional term which generates D_{i+1} from D_i is an 'odd-root' or 'square root' term, respectively. ($1 \leqq i < q$).

7.2 Construction of T_o to D_o.

We define functions P_o and Q_o whose domains are D_o, and which range over the integers, below. The symbols used to denote operations and equality in the range are those of our formal system, of course, but are to be interpreted as operations among the integers. Intuitively, P_o and Q_o indicate the numerator and denominator respectively of the rational numbers obtained when the symbols of our formalism are given their intuitive interpretation.

1) $P_o(0) = 0$ and $Q_o(0) = 1$

2) $P_o(1) = 1$ and $Q_o(1) = 1$

3) $P_o(-t) = -P_o(t)$, and $Q_o(-t) = Q_o(t)$.

4) If $P_o(t) \neq 0$, then $P_o(t^{-1}) = Q_o(t)$ and $Q_o(t^{-1}) = P_o(t)$

5) If $P_o(t) = 0$, then $P_o(t^{-1}) = 0$ and $Q_o(t^{-1}) = 1$

6) $P_o(t_1+t_2) = P_o(t_1)\cdot Q_o(t_2) + P_o(t_2)\cdot Q_o(t_1)$
and $Q_o(t_1+t_2) = Q_o(t_1)\cdot Q_o(t_2)$

7) $P_o(t_1\cdot t_2) = P_o(t_1)\cdot P_o(t_2)$
and $Q_o(t_1\cdot t_2) = Q_o(t_1)\cdot Q(t_2)$.

T_o may now be defined thus :-

If t_1 and t_2 are terms of D_o, then the formula '$t_1 = t_2$' has value 'true' under T_o iff $P_o(t_1)\cdot Q_o(t_2) = P_o(t_2)\cdot Q_o(t_1)$.

The mapping $t \rightarrow \frac{P_o(t)}{Q_o(t)}$ makes each term where the denominator is non-zero correspond to a rational number, terms having zero denominator being mapped into 0. (clause 5 above). Since the definition ensures that

$Q_o(t)$ can never be zero, it is now simple to prove that T_o satisfies the axioms S, and also A_{19}. We remark that in our formal system the terms of D_o are simply juxtapositions of symbols, and formulae of the kind '$t_1 = t_2$' have no 'real' meaning: there is no reason why a specific instance '$t = t$' should not be assigned a value 'false', and in any case a statement of the kind ' '$t_1 = t_2$' is 'true' ' while not strictly nonsense, is - if considered by itself - strictly meaningless. However, as soon as T_o is imposed, the system of terms D_o with T_o (interpreting 'true' naively) crystallizes immediately into a replica of the rational number field. Under each of the truth-assignments defined below, a corresponding field appears and in taking a step from D_i to D_{i+1} we will speak of 'extending' D_i by the 'adjunction' of some term, though strictly speaking these words should not be used. The process belongs strictly to our formalism, the extension and adjunction taking place in the algebraic counterpart.

We will use the notation '$D_i:T_i$' $(o \leqq i \leqq q)$ where T_i is a truth assignment to D_i satisfying the axioms S to indicate the corresponding field, and when the final branching array of fields has been constructed, each branch will be a sequence of fields (originating with the rational number field) each obtained from its predecessor by algebraic extension, except in the very first case where $D_o:T_o$ is extended to $D_1:T_1$ by adjoining $y_1, y_2, \ldots, y_k$, where these are treated as transcendentals (independent) over $D_o:T_o$.

In this first case the interpretation of D_o and the predicate '=' as the rational number field is so marked that had it not been necessary to exhibit the effective construction of T_o , we might have defined it simply as the 'natural' truth assignment to D_o (possibly with some suitable remark to rebut the accusation that the mapping of a term with zero denominator into zero is unnatural !)

7. Construction of T_1 to D_1

As before, we construct functions P_1 and Q_1 with domains D_1 ranging over the ring of polynomials in $y_1, y_2, \ldots, y_k$, having coefficients in D_o:T_o, thus :-

1) If $t \in D_o$, then $P_1(t) = t$ and $Q_1(t) = 1$.

2) $P_1(y_i) = y_i$ and $Q_1(y_i) = 1$ $(i = 1,2,\ldots,k)$

3) $P_1(-t) = -P_1(t)$, and $Q_1(-t) = Q_1(t)$

4) If $P_1(t) \neq 0$, then $P_1(t^{-1}) = Q_1(t)$ and $Q_1(t^{-1}) = P_1(t)$

5) If $P_1(t) = 0$, then $P_1(t^{-1}) = 0$ and $Q_1(t^{-1}) = 1$.

6) $P_1(t_1+t_2) = P_1(t_1)\cdot Q_1(t_2) + P_1(t_2)\cdot Q_1(t_1)$
and $Q_1(t_1+t_2) = Q_1(t_1)\cdot Q_1(t_2)$

7) $P_1(t_1\cdot t_2) = P_1(t_1)\cdot P_1(t_2)$ and
$Q_1(t_1\cdot t_2) = Q_1(t_1)\cdot Q_1(t_2)$.

We now define T_1 as in the previous case :-

If $t_1 \varepsilon D_1$ and $t_2 \varepsilon D_1$, then '$t_1 = t_2$' is 'true' under T_1 iff $P_1(t_1)\cdot Q_1(t_2) = P_1(t_2)\cdot Q_1(t_1)$.
(We remark that the condition

'$P_1(t_1)\cdot Q_1(t_2) = P_1(t_2)\cdot Q_1(t_1)$' .... (1)

is equivalent to

'$P_1(t_1)\cdot Q_1(t_2)$ and $P_1(t_2)\cdot Q_1(t_1)$ have the equations of their corresponding coefficients 'true' under T_o'

but since $D_o:T_o$ has already been established as a field, and the polynomials in (1) are elements of $D_o:T_o\ [y_1,y_2,\ldots,y_k]$, the truth value of (1) is decided by the ordinary operations among polynomials over $D_o:T_o$, and the definition of 'equality' of two polynomials.)

As in the discussion of T_o, it now follows easily that T_1 to D_1 satisfies A_1 & A_2 & ...& A_{16}, as well as A_{19}. The map $t \to \frac{P_1(t)}{Q_1(t)}$ maps terms of D_1 onto elements of the field $D_1:T_1$, namely the field of rational functions of $y_1,y_2,\ldots,y_k$ with rational coefficients, zero-denominator terms mapping into zero.

7.4 Extension of $D_i:T_i$ to $D_{i+1}:T'_{i+1}$ and $D_{i+1}:T''_{i+1}$, by the adjunction of a 'square root', $r(t)(1\leq i<q)$.

Remark: There may be many truth-assignments to D_i, $(1<i<q)$ which satisfy S; the construction below applies to every such truth-assignment.

We define T'_{i+1} to coincide with T_i on D_i, and also to make the formula '$r(t)^2 = t$' 'true', and from these conditions we establish a procedure for assigning values to any formula '$t_1 = t_2$', $t_j \epsilon D_{i+1}$'$(j = 1,2)$.

First, we note that any formula of the kind '$p + q\cdot r(t) = 0$'...(1) where p and q are in $D_i:T_i$, is

immediately decided, for either $q = 0$ (in $D_i:T_i$) and (1) is equivalent to '$p = 0$' which is decidable in $D_i:T_i$, or else $q \neq 0$, and (1) is assigned the value 'true' iff $t = p^2 \cdot (q^{-1})^2$, which is decided in $D_i:T_i$.

Next, if in any term t_1 of D_{i+1} we replace '$r(t)$' in each occurrence by a variable 'z', then by definition of D_{i+1}, t_1 is a rational function of z with coefficients in $D_i:T_i$. Regarding z as a transcendental element over $D_i:T_i$, t_1 is thus an element of the extension field $D_i:T_i(z)$. By the usual operations in this extension field, the representation can be further reduced to the quotient of two polynomials. An effective procedure for this can be obtained by following the pattern established in 8.3, thus :-

1) If $t \varepsilon D_i:T_i$, then $P_{i+1}(t) = t$ and $Q_{i+1}(t) = 1$
2) $P_{i+1}(z) = z$ and $Q_{i+1}(z) = z$
3) $P_{i+1}(-t) = -P_{i+1}(t)$ and $Q_{i+1}(-t) = Q_{i+1}(t)$
4) If $P_{i+1}(t) \neq 0$, then $P_{i+1}(t^{-1}) = Q_{i+1}(t)$, and $Q_{i+1}(t^{-1}) = P_{i+1}(t)$.
5) If $P_{i+1}(t) = 0$, then $P_{i+1}(t^{-1}) = 0$ and $Q_{i+1}(t^{-1}) = 1$
6) $P_{i+1}(t_1+t_2) = P_{i+1}(t_1) \cdot Q_{i+1}(t_2) + P_{i+1}(t_2) \cdot Q_{i+1}(t_1)$ and $Q_{i+1}(t_1+t_2) = Q_{i+1}(t_1) \cdot Q_{i+1}(t_2)$
7) $P_{i+1}(t_1 \cdot t_2) = P_{i+1}(t_1) \cdot P_{i+1}(t_2)$ and $Q_{i+1}(t_1 \cdot t_2) = Q_{i+1}(t_1) \cdot Q_{i+1}(t_2)$.

The map $t_1 \to \frac{P_{i+1}(t_1)}{Q_{i+1}(t_1)}$ exhibits the reduction of t_1 to the quotient of two polynomials.

We may now reduce both polynomials to the form '$p + q \cdot z$', by taking the linear remainder on division by $(z^2 - t)$ in the usual way. To deal with a formula '$t_1 = t_2$', we put it in the form '$t_3 = 0$' (where t_3 is $t_1 - t_2 \in D_{i+1}$) and pursuing the above process, obtain a formula

$$'\frac{p_1 + q_1 \cdot z}{p_2 + q_2 \cdot z} = 0'.$$

Replacing 'z' by '$r(t)$', we have from (1) a method of determining whether '$p_1 + q_1 \cdot r(t) = 0$' or '$p_2 + q_2 \cdot r(t) = 0$' is 'true' or 'false', and hence reach the definitive statement:- '$t_1 = t_2$' is 'true' under T'_{i+1}, iff $t = p_1^2 \cdot (q_1^{-1})^2$ or $t = p_2^2 \cdot (q_2^{-1})^2$.

The above process mirrors precisely the adjunction of an element $r(t)$ to the field $D_i : T_i$, where $r(t)$ is a root of the polynomial $x^2 - t$, except that we have made no use of the reducibility or irreducibility of the polynomial $x^2 - t$. It can be proved without difficulty - the proof being modelled in rather an obvious way on the last observation - that under T'_{i+1}, the terms of D_{i+1} form a field which we shall denote as usual by '$D_{i+1} : T'_{i+1}$'. Of course, either $x^2 - t$ is reducible over $D_i : T_i$, or it is not. In the former case, the field $D_{i+1} : T'_{i+1}$ will be simply

a repetition of $D_i:T_i$, though from our point of view, because of the new symbols involved, we will regard it as distinct: in the latter case, $D_{i+1}:T'_{i+1}$ will be a non-trivial algebraic extension of $D_i:T_i$.

Now in all of the above discussion, if we had replaced the prescription '$r(t)^2 = t$' 'true'' by the alternative '$r(t)^2 = -t$ 'true'', the whole discussion could have been carried through on this basis, making the obvious changes required. This would lead to a field obtained by adjoining $r(t)$ to $D_i:T_i$, where $r(t)$ is a root of the polynomial $x^2 + t$. If we call this $D_{i+1};T''_{i+1}$, then we obtain two extension fields $D_{i+1}:T'_{i+1}$ and $D_{i+1}:T''_{i+1}$, which is exactly what we would expect in adjoining a square root.

7.5 Extension of $D_i:T_i$ to $D_{i+1}:T_{i+1}$ by the adjunction of an 'odd root' $r_{2j+1}(t_1 t_2 \ldots t_{2j+1})$ $(1 \leq j \leq n)$.

We assume D_{i+1} to have been obtained from D_i by including with D_i a term $r_{2j+1}(t_1 t_2 \ldots t_{2j+1})$ and closing the set under the rational operations. We denote this new term by the symbol 'r', and the polynomial '$r^{2j+1} + t_1 . r^{2j} + \ldots + t_{2j+1}$' by $p(r)$, deg. $p(r) = 2j+1 = m$.

I. First we show how to define T_{i+1} for any given finite set of formulae of the form '$t_k = 0$', where each term t_k is written as a polynomial $h_k(r)$ with coefficients in $D_i:T_i$ and where $h_k(r)$ has degree $<m$.

We construct a sequence of polynomials $\{p_k(r)\}$ thus:-

(i) $p_1(r) = p(r)$

(ii) $p_{s+1}(r) =$ the g.c.d. $(h_s(r), p_s(r))$

or $\dfrac{p_s(r)}{(h_s(r), p_s(r))}$, whichever has <u>odd</u> degree

and then define

(iii) '$t_k = 0$' 'true' iff $p_{k+1}(r)$ is a factor of $h_k(r)$.

(In this way the last in the sequence $\{p_k(r)\}$ of odd-degree polynomials, say $p_{n+1}(r)$, is a factor of each element of the sequence, and the decisions on the formulae '$t_k = 0$' ($k = 1,2,\ldots n$) are exactly those which would be reached by considering algebraically the corresponding equation '$h_k(\alpha) = 0$', where α is a root of $p_{n+1}(x)$.)

II. Next we show that the procedure in I can be extended to all formulae of the kind '$t = 0$', where t is a polynomial in r, coefficients in $D_i:T_i$.

Since $D_i:T_i$ is an algebraic extension of the field of rational functions in $y_1, y_2, \ldots y_k$ with rational coefficients, it is denumerable, and hence the set of all polynomials of degree $<m$ is denumerable. This set may therefore be completely ordered. We select some such ordering, and this ordering now remains fixed for the rest of the discussion.

Now the given term t, being a polynomial in r, can be reduced to a polynomial of degree <m, by taking the remainder on division by p(r) in the usual way. This new polynomial must occur as some definite k^{th} term in the fixed ordering chosen. In this way, we have satisfied the conditions of I, which now gives us a value for the formula 't = 0'.

III. Next, for any general term t, the formula 't = 0' may be decided by II, if we can reduce t to a polynomial in r. From the well established pattern this becomes almost trivial, as follows :-

We define functions $P_{i+1}(t)$ and $Q_{i+1}(t)$ precisely as in the previous section (though 'z' is used instead of 'r' in the definition of that section), and so obtain as usual a mapping $t \rightarrow \frac{P_{i+1}(t)}{Q_{i+1}(t)}$

Since $P_{i+1}(t)$ and $Q_{i+1}(t)$ are polynomials in r, II provides values of the formula '$Q_{i+1}(t) = 0$'. We now define

1) If $Q_{i+1}(t) = 0$, then $P^{*}_{i+1}(t) = 0$ and $Q^{*}_{i+1}(t) = 1$

2) If $Q_{i+1}(t) \neq 0$, then $P^{*}_{i+1}(t) = P_{i+1}(t)$
and $Q^{*}_{i+1}(t) = Q_{i+1}(t)$

Now we can define 't = 0' 'true', iff $P^{*}_{i+1}(t) = 0$ is'true', which is decidable from II.

IV. Finally, for the general formula '$t_1 = t_2$', we put '$t_1 - t_2$' for t, and define '$t_1 = t_2$' 'true', iff '$t = 0$' is 'true', which is established from III.

Remarks. (1) In obtaining 'true' representations of 0 or $f(y_1 y_2 \ldots y_k)$ as sums of squares in D_{i+1}, a finite number of truth values of formulae of the kind '$t_1 = t_2$' has to be established - since the origin of these representations is $R(D,F)$, which has only a finite number of such formulae as sub-formulae. In this way, the truth values required could be assigned by considering a finite number of polynomials (as in I), and thereby obtaining some $p_{n+1}(r)$ which becomes the 'defining polynomial' of α where $D_{i+1}:T_{i+1}$ is simply $D_i:T_i(\alpha)$. The representations will clearly remain true if α is regarded as a root of any factor of $p_{n+1}(r)$.

(2) Altering the ordering of polynomials of degree $<m$ will in general change the defining polynomial, but this is unimportant: exactly which root of $p(x)$ is adjoined to $D_i:T_i$ does not affect the result, provided α is always a root of an odd-degree factor of $p(x)$. This apparent uncertainty as to precisely which root of $p(x)$ is adjoined to $D_i:T_i$ exists only because the ordering of the polynomials of degree $<m$ has not been specified: once this ordering is fixed, T_{i+1} is completely defined and the field $D_{i+1}:T_{i+1}$ established.

(3) As a consequence of the definition of $Q^*_{i+1}(t)$, we find that the map $t \to \frac{P^*_{i+1}(t)}{Q^*_{i+1}(t)}$ exhibits terms of D_{i+1} as rational functions of r with coefficients in $D_i:T_i$. Moreover, $Q^*_{i+1}(t)$ is relatively prime to $p_{n+1}(t)$ for all $t \in D_{i+1}$, and so operating in the ring $D_i:T_i[r]$, we can find for each t a polynomial $Q^{*\,-1}_{i+1}(t)$ such that

$$Q^*_{i+1}(t) \cdot Q^{*\,-1}_{i+1}(t) \equiv 1 \pmod{p_{n+1}(r)}$$

In this way, each element may be represented as a polynomial in r, coefficients in $D_i:T_i$, by the map

$$t \to P^*_{i+1}(t) \cdot Q^{*\,-1}_{i+1}(t).$$

That $p_{n+1}(r)$ has odd degree follows from I (i) and (ii), and from this observation together with the mapping shown above of terms of D_{i+1} onto polynomials of $D_i:T_i[r]$, the proof that $D_{i+1}:T_{i+1}$ really is a field with the required properties is now trivial.

§8. SUMMARY OF THE MAIN PROOF.

From any given positive definite function $f(y_1,y_2,\ldots y_k)$, we construct the formula F, and from §5, a proof of F exists.

From §6, we construct a finite set of terms D, and a quantifier free formula R(D,F) whose truth-functional validity is assured by the Herbrand Theorem.

From §6·3 we construct a finite set D^*, consisting of all terms occurring in R(D,F), and a sequence of sets

$$D_0 \subset D_1 \subset \ldots \subset D_q, \quad D^* \subset D_q.$$

From §7, we show how to construct a truth-assignment T_1 to D_1, so that $D_1:T_1$ is the field of rational functions in $y_1, y_2, \ldots y_k$, with rational coefficients.

Also from §7, we show how to extend any field $D_i:T_i$ in two ways, to fields $D_{i+1}:T_{i+1}'$ and $D_{i+1}:T_{i+1}''$, by the adjunction of a 'square root', or to a single field $D_{i+1}:T_{i+1}$, by the adjunction of an 'odd root.'
In this way, if D* contained m distinct 'square root' terms, then the construction of §7 leads to 2^m distinct fields of the form $D_q:T_q$.

Now in <u>each</u> of these fields, $D_q:T_q$, from §7·1, representations of $f(y_1,\ldots,y_k)$ or of zero as sums of squares are obtained.

In the cases where $D_q:T_q'$ and $D_q:T_q''$ arose from the adjunction of a square root to some $D_{q-1}:T_{q-1}$, §3·3 shows the construction of representations of $f(y_1,y_2,\ldots y_k)$ or of 0 as sums of squares in $D_{q-1}:T_{q-1}$. from those in $D_q:T_q'$ and $D_q:T_q''$.

Alternatively, where $D_q:T_q$ arose from some $D_{q-1}:T_{q-1}$ by the adjunction of an odd root, §3·4 shows the construction of a representation of $f(y_1y_2\ldots y_k)$ or of 0 as a sum of squares in $D_{q-1}:T_{q-1}$, from a representation in $D_q:T_q$.

Applying this to every field $D_q:T_q$, we obtain then at least one representation of f as a sum of squares in every field $D_{q-1}:T_{q-1}$.

Repeating this process (q-1) times, we obtain ultimately a representation of f or of zero as a sum of squares in $D_1:T_1$. However no non-trivial representation of zero as a sum of squares is possible in $D_1:T_1$ (since A_{19} holds, see 3·1), and hence we obtain as required, a representation of $f(y_1,y_2,\ldots,y_k)$ as a sum of squares in $D_1:T_1$, the field of rational functions of $y_1,y_2,\ldots,y_k$, with rational coefficients. This completes the main proof.

§9. EXTENSION TO CASES WHERE $f(y_1,y_2,\ldots,y_k)$ HAS REAL COEFFICIENTS.

9.1 Outline of the method.

From the given function $f(y_1,y_2,\ldots,y_k)$, we find a formula G, namely.

$$Ay_1Ay_2\ldots Ay_k \text{ Ex } f(y_1y_2\ldots y_k\ z_1z_2\ldots z_s) = x^2$$

where the function symbol $f(y_1y_2\ldots y_k\ z_1z_2\ldots z_s)$ denotes the formal representation of the given function $f(y_1,y_2,\ldots,y_k)$, and $z_1,z_2,\ldots,z_s$ denote the given real coefficients.

From G, we obtain a formula U'(G) of the form

$$G_1 \text{ v } G_2 \text{ v}\ldots\text{v } G_p$$

such that $U'(G) \leftrightarrow G$ follows from K. We are interested in fact only in the particular implication $U'(G) \rightarrow G$

Now each of the disjuncts of U'(G) essentially gives a condition for the positive definiteness of $f(y_1,y_2,\ldots,y_k)$ (since clearly $G_r \rightarrow G$ follows from K, $1 \leq r \leq p$). We construct a set of p formulae $\{F_r\}$, where F_r is

$$K \rightarrow (G_r \rightarrow G) \quad (1 \leq r \leq p).$$

i.e. $(A_1 \,\&\, A_2 \,\&\ldots\&\, A_{16} \,\&\, A_{17} \,\&\, A_{18}) \rightarrow (-A_{19} \vee - G_r \vee G)$

For each r $(1 \leq r \leq p)$, we now apply the method employed in the main proof, where the coefficients were rational, and obtain in the 'final' fields $D_q:T_q$ (which 'contain' D*) representations of 0 or of f as sums of squares, or counter-examples to G_r. It turns out that a counter-example to G_r in any field $D_q:T_q$ is also a counter-example in $D_1:T_1$, so that if f really is positive definite, then for at least one valve of r, no such counter example to G_r exists. In this case, exactly as in the main proof, $R(D,F_r)$ provides representations of 0 or of f as sums of squares in each field $D_q:T_q$, and these are reduced as before to a single representation in $D_1:T_1$.

9.2 Details of modified method.

The main result of [5] is that if G is a formula of our formal system, then we can find a corresponding formula U(G) such that $U(G) \leftrightarrow G$ follows from the axioms of a real closed field. U(G) is quantifier-free, and has as variables exactly the free variables of G, and it is in

normal disjunctive form. The atomic sub formulae of U(G) have the form 'h = 0' or 'h > 0', where 'h' denotes a polynomial in the variables of U(G).

Applying this to the present case, if the given function $f(y_1,y_2,\ldots,y_k)$ has $\underline{s}$ real coefficients, we replace these in some order by the variables $z_1,z_2,\ldots,z_s$, and denote the resulting expression by the symbol '$f(y_1y_2\ldots y_kz_1z_2\ldots z_s)$' of our formalism. We let G (as indicated in 9.1) be the formula.

$$Ay_1Ay_2\ldots Ay_k\ Ex\ f(y_1y_2\ldots y_kz_1z_2\ldots z_s) = x^2$$

Then U(G) is a formula

$$G_1 \vee G_2 \vee \ldots \vee G_p, \quad \text{where } G_r\ (1\leq r\leq p) \text{ is}$$

$$g_{r,1}=0 \ \& \ g_{r,2}=0 \ \& \ \ldots \ \& \ g_{r,m_r}=0 \ \& \ h_{r,1}>0 \ \& \ h_{r,2}>0 \ \& \ \ldots \ \& \ h_{r,n_r}>0$$

where each symbol 'g' and 'h' with subscripts denotes a polynomial in $z_1,z_2,\ldots,z_s$.

Obviously U(G) is not within our formalism, since the predicate '>' is involved. However if we replace occurrences of '>' in G_r $(1\leq r\leq p)$, denoting the resulting subformula by 'G'_r', according to the prescription

' x>y ' is equivalent to ' $Ez(z\neq 0 \ \& \ x-y=z^2)$ '

we get for G'_r $(1\leq r\leq p)$ the formula

$$g_{r,1}(z_1\ldots z_s) = 0 \ \& \ \ldots \ \& \ g_{r,m_r}(z_1\ldots z_s) = 0$$

$$\& \ Ew_{r,1}(w_{r,1}\neq 0 \ \& \ h_{r,1}(z_1\ldots z_s)=w_{r,1}^2)$$

$$\& \ Ew_{r,2}(w_{r,2}\neq 0 \ \& \ h_{r,2}(z_1\ldots z_s)=w_{r,2}^2)$$

$$\& \ \ldots \ \& \ Ew_{r,n_r}(w_{r,n_r}\neq 0 \ \& \ h_{r,n_r}(z_1\ldots z_s)=w_{r,n_r}^2)$$

Now each G'_r, and their disjunction, say $U'(G)$, are formulae within our system, equivalent to G_r and $U(G)$ respectively. The formula $U'(G) \rightarrow G$ follows from K, and hence the disjunction $F_1 \vee F_2 \vee \ldots \vee F_p$ is provable, where (for $1 \leqq r \leqq p$), we have for F_r the formula

$$K \rightarrow (G'_r \rightarrow G).$$

which we interpret as

$$A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_{18} \rightarrow (-A_{19} \vee -G'_r \vee G)$$

The process described in the main proof is now carried out, making the obvious necessary modifications. For example, D_1 will now consist of rational functions of $y_1, y_2, \ldots y_k\ z_1, z_2, \ldots, z_s$, $w_{r,1}$, $w_{r,2}, \ldots$, w_{r,n_r}, and in defining T_1 on D_1, we may prescribe that T_1 satisfies G'_r. (i.e. we stipulate that T_1 makes '$g_{r,j}(z_1 \ldots z_s) = 0$' 'true' $(1 \leqq j \leqq m_r)$, and '$h_{r,j}(z_1 \ldots z_s) = w_{r,j}^2$' 'true' $(1 \leqq j \leqq n_r)$, for each r, $(1 \leqq r \leqq p)$.)

In this way, when we examine the Herbrand Expansions $R(D,F_r)$ $(1 \leqq r \leqq p)$, we find that it exhibits 'true' representations of zero or of f as squares under all truth-assignments constructed as prescribed. That this is so is clear from the fact that each 'final' field $D_q{:}T_q$ has its truth-assignment T_q defined as an extension of T_1, and hence each T_q satisfies G'_r, as well as the axioms $A_1, A_2, \ldots A_{18}$. This leaves in $R(D,F_r)$ a disjunct corresponding to '$-A_{19}$' or to 'G'_r''true'.

The representations in each $D_q:T_q$ are as before reduced to a single representation in $D_1:T_1$, as required.

Finally, the p representations thus obtained (corresponding to each formula F_r) may be withdrawn from our formalism by replacing $z_1,z_2,\ldots,z_s$, and hence $w_{r,1},w_{r,2},\ldots,w_{r,n_r}$, by their given real values. If the given function really is positive definite, then U(G) is true, and some disjunct G_r is therefore true. The representation of f arising from the corresponding F_r then gives the 'correct' solution.

Remark: It is interesting to note that the real coefficients occurring in the final representation either occur in f itself, or else they arise in the evaluation of $w_{r,1},w_{r,2},\ldots,w_{r,n_r}$, and hence these new real coefficients are square roots of polynomials in the given real coefficients.

9.3. Illustrative example.

Suppose the given function is

$f(y_1) = a_1y_1^2 + a_2y_1 + a_3$,

where a_1,a_2,a_3 are the real coefficients.

Then we have $f(y_1z_1z_2z_s) = z_1 \cdot y_1^2 + z_2 \cdot y_1 + z_3$

G is then

$Ay_1Ex_1\ f(y_1z_1z_2z_3) = x_1^2$

and U'(G) is found to be $G_1'\ v\ G_2'$, where

G_1' is $(z_1 = 0 \ \& \ z_2 = 0 \ \& \ Ew_1(w_1 \neq 0 \ \& \ z_3 = w_1^2)$

and G_2' is $(Ew_2(w_2 \neq 0 \ \& \ z_1 = w_2^2) \ \& \ Ew_3(w_3 \neq 0 \ \& \ -z_2^2 + 4z_1 \cdot z_3 = w_3^2))$

In dealing with F_1, the final representation in $D_1:T_1$ would be

$$f(y_1 z_1 z_2 z_3) = w_1^2$$

and in dealing with F_2 it would be

$$f(y_1 z_1 z_2 z_3) = (w_2 \cdot y_1 + z_2 \cdot (2w_2)^{-1})^2 + (w_3 \cdot (2w_2)^{-1})^2$$

Now replacing z_1, z_2, z_3, by the given coefficients a_1, a_2, a_3, respectively, and interpreting the result as indicated in 9.2, we have:-

If G_1 is satisfied (i.e. if $a_1 = 0$, and $a_2 = 0$, and $a_3 > 0$) then

$$a_1 y_1^2 + a_2 y_1 + a_3 = (\sqrt{a_3})^2$$

and if G_2 is satisfied (i.e. if $a_1 > 0$ and $-a_2^2 + 4a_1 a_3 > 0$) then

$$a_1 y_1^2 + a_2 y_1 + a_3 = \left(\sqrt{a_1} y_1 + \frac{a_2}{2\sqrt{a_1}}\right)^2 + \left(\frac{\sqrt{-a_2^2 + 4a_1 a_3}}{2\sqrt{a_1}}\right)^2$$

Now if $f(y_1)$ really is positive definite, then either its coefficients satisfy G_1 - in other words $f(y_1)$ is a positive constant - or else they satisfy G_2, which we recognise as the familiar 'negative discriminant' condition for a definite quadratic function, and the appropriate corresponding representation of $f(y_1)$ holds.

§10 REFERENCES.

1. D. HILBERT Mathematical problems.
Bulletin of the American Mathematical Society 8(1902) 437-479

2. E. ARTIN Uber die Zerlegung Definiter Funktionen in Quadrate.
Abhandlungen aus dem mathematischen seminar der Hamburger Universitat.
5(1927) 100-115

3. G. KREISEL Sums of squares.
Summaries of the summer institute for symbolic logic.
Cornell University.(2nd Ed.)(1960) 313-330

4. G. KREISEL Mathematical significance of consistency proofs.
Journal of Symbolic Logic. 23(1958) 155-182

5. A. TARSKI A decision method for elementary algebra and geometry.
2nd. (revised) Edition (1951)

6. B. DREBDEN False Lemmas in Herbrand.
Bulletin of the American Mathematical Society.69(1963) 699-706