PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Effective Procedures in Field Theory

A. Frohlich and J. C. Shepherdson

Phil. Trans. R. Soc. Lond. A 1956 **248**, 407-432
doi: 10.1098/rsta.1956.0003

EFFECTIVE PROCEDURES IN FIELD THEORY

By A. FRÖHLICH,* *University College of North Staffordshire, Keele, Staffs*
and J. C. SHEPHERDSON, *University of Bristol*†

(*Communicated by H. A. Heilbronn, F.R.S.—Received* 24 *March* 1955)

CONTENTS

Van der Waerden (1930*a*, pp. 128–131) has discussed the problem of carrying out certain field theoretical procedures effectively, i.e. in a finite number of steps. He defined an 'explicitly given' field as one whose elements are uniquely represented by distinguishable symbols with which one can perform the operations of addition, multiplication, subtraction and division in a finite number of steps. He pointed out that if a field K is explicitly given then any finite extension K' of K can be explicitly given, and that if there is a splitting algorithm for K, i.e. an effective procedure for splitting polynomials with coefficients in K into their irreducible factors in $K[x]$, then (**1**) there is a splitting algorithm for K'. He observed in (1930*b*), however, that there was no general splitting algorithm applicable to all explicitly given fields K, or at least that such an algorithm would lead to a general procedure for deciding problems of the type 'Does there exist an n such that $E(n)$?', where E is an arbitrarily given property of positive integers such that there is an algorithm for deciding for any n whether $E(n)$ holds.

In this paper we review these results in the light of the precise definition of algorithm (finite procedure) given by Church (1936), Kleene (1936) and Turing (1937) and discuss the existence of a number of field theoretical algorithms in explicit fields, and the effective construction of field extensions. We sharpen van der Waerden's result on the non-existence of a general splitting algorithm by constructing (§7) a particular explicitly given field which has no splitting algorithm. We show (§7) that the result on the existence of a splitting algorithm for a finite extension field does not hold for inseparable extensions, i.e. we construct a particular explicitly given field K and an explicitly given inseparable algebraic extension $K(\alpha)$ such that K has a splitting algorithm but $K(\alpha)$ has not.(**2**) We note also (in §6) that there exist two isomorphic explicitly given fields, one of which possesses a splitting algorithm but the other of which does not. Thus the sort of properties of fields we are interested in depend not only on the abstract field but also on the particular representation chosen. It is necessary therefore to state rather carefully our definitions of explicit ring, extension ring, splitting algorithm, etc., and to introduce the concept of explicit isomorphism (**3**) and homomorphism. This occupies §§**1**, 2 and 3. On the basis of these definitions we then discuss the existence of some fundamental field theoretical algorithms in explicit fields and their extension fields. This leads also to a classification of the types of extension fields which can be effectively constructed.

* Present address: King's College London.
† Part of this work was done while at the Institute for Advanced Study, Princeton, N.J., U.S.A.

(**1**) Provided that K' is obtained from K by transcendental or *separable* algebraic extensions only.

(**2**) This sharpens a result of Kneser (1953) who proved there was no *general* splitting algorithm for inseparable extension fields $K(\alpha)$ of explicitly given fields K with splitting algorithms.

(**3**) In §§5, 6 we give examples of explicit fields which are isomorphic but not explicitly isomorphic.

1. Effective procedures

We shall suppose that the symbols used to represent the elements of the algebraic systems we deal with take the form of finite sequences (4) (which we call *words*) of elements from some finite set or *alphabet* $A = \{a_1, \ldots, a_k\}$ of primitive symbols or *letters* $a_1, \ldots, a_k$. It is convenient to define a fixed $(1, 1)$ correspondence between the words of a given alphabet A and the positive integers which is *effective* in the sense that a machine could be constructed which when supplied with an integer n would give the corresponding word $W(n)$, and conversely when supplied with a word W would give the corresponding integer $n(W)$. This can be done most simply by correlating the integer n with the nth word in the series

$$a_1, a_2, \ldots, a_k; \quad a_1a_1, a_1a_2, \ldots, a_1a_k; \quad a_2a_1, \ldots, a_2a_k; \quad \ldots; \quad a_ka_1, \ldots, a_ka_k; \quad a_1a_1a_1, a_1a_1a_2, \ldots,$$

obtained by letting a word W_1 precede a word W_2 if W_1 is of lesser length or if W_1 is of the same length as W_2 but the first letter, α (reading from the left), of W_1 which differs from the corresponding letter, β, of W_2 precedes β in the preliminary ordering $a_1, a_2, \ldots, a_k$ of the letters. We now define a *recursively enumerable set* of words of A to be a set of words $W, \ldots,$ whose corresponding numbers $n(W), \ldots,$ form a recursively enumerable set of positive integers, i.e. the set $\{f(1), f(2), \ldots\}$ of values of a general recursive (5) function $f(n)$. Similarly, a set of words is said to be *recursive* if the corresponding integers form a recursive set, i.e. a set C such that $n \in C . \equiv . f(n) = 0$ for some recursive function f. If S is a set of words of the alphabet A we say there is an *algorithm* for deciding whether a word of S has the property P if there is a mechanical procedure for deciding this; more precisely, if there is a partially recursive (6) function f defined for all integers which are the numbers of words in S, (7) such that if n is the number of a word in S then $f(n) = 0$ if and only if the word $W(n)$ has the property P. If $S_1, \ldots, S_i$ are sets of words of the alphabet A we may define similarly the meaning of the phrase 'there is an algorithm for deciding whether the words $W_1, \ldots, W_i$ of $S_1, \ldots, S_i$ respectively, satisfy the relation $P(W_1, \ldots, W_i)$'. If S is a set of words of the alphabet A and $\phi(W)$ a function (not necessarily single-valued), defined for all $W \in S$, whose value is a word of A, then we say there is an algorithm for computing a value of $\phi(W)$ for $W \in S$ if there is a partly recursive (single-valued) function $f(n)$ defined (7) for all n which are the numbers of words in S such that if n is the number of a word in S then $W(f(n))$ is a value of $\phi(W(n))$. Functions of several variables are treated similarly.

We shall follow the usual practice of using these precise definitions of algorithm, etc., only when proving the non-existence of algorithms; when we actually construct an algorithm we shall merely satisfy ourselves that it can be carried out 'mechanically', and rely for the rest on the assumption (which has by now been extensively confirmed) that 'general recursive' is a satisfactory interpretation of 'effectively calculable'. The non-existence

(4) In practice we shall violate this convention by using non-linear combinations of symbols involving sub- and superscipts; we do this in order to depart as little as possible from accepted mathematical symbolism; the justification for it is that if we wished we could introduce new symbols $\uparrow$ and $\downarrow$ and agree that x_u, x^v were simply to be regarded as abbreviations for $x \downarrow u \downarrow$ and $x \uparrow v \uparrow$ respectively. (Where, as usual in the case of repeated or mixed sub- and superscripts, one must indicate either by brackets or tacitly the order of their application.)

(5) In the sense of Kleene (1936).

(6) In the sense of Kleene (1938).

(7) In general such an f will be defined also for some n which are not numbers of words in S.

proofs nearly all depend on Kleene's result that there exists a recursively enumerable but non-recursive set of positive integers, i.e. there exists a recursive function $\lambda(n)$(8), defined for all positive integers n, such that $\lambda(n) \neq \lambda(m)$, if $n \neq m$, and that the integers m satisfying $(\exists n)\,(\lambda(n) = m)$ form a non-recursive class. We shall often make tacit use of well-known properties of general recursive functions and algorithms, in particular of the following basic lemma:

Basic lemma. *If S is any set of words of the alphabet A and S' is a recursively enumerable set of words of A, if for each word W of the set S there exists a word W' of the set S' such that $\phi(W, W')$, if there is an algorithm for deciding, for $W \in S$, $W' \in S'$ whether $\phi(W, W')$ holds, then there is an algorithm for computing, for $W \in S$ a word $W' \in S'$ such that $\phi(W, W')$.* Such an algorithm can be obtained by enumerating the words of S' one after another and testing each one to see whether $\phi(W, W')$ is satisfied; eventually one will be reached for which this is so. A similar result applies to finite sequences of words.

2. Explicit rings

In this section we confine ourselves to rings(9) and fields, since it is only with these structures that we deal later. But it is clear that similar definitions could be framed for any type of algebra in the general sense of Robinson (1951) or even for a model of an axiomatic system of a more general kind containing perhaps elements of infinitely many types. Following (more or less) van der Waerden we define:

Definition 2·1. *A ring R is said to be explicit if its elements are the equivalence classes $\{P\}, \{Q\}, \ldots$, into which a recursively enumerable* (10) *set S of words $P, Q, \ldots$ of some alphabet A is divided by an equivalence relation $E(P, Q)$ and if there are algorithms for deciding, for words P, Q, T of S whether or not the relations $\{P\} \equiv \{Q\}$* (which is the same as $E(P, Q)$) *$\{P\} + \{Q\} \equiv \{T\}$, $\{P\} \times \{Q\} \equiv \{T\}$ hold. An explicit ring which is a field, integral domain, unique factorization domain (u.f.d.), etc., is called an explicit field, integral domain, u.f.d., etc.* Here the operations '$+$', '$\times$' stand for the ring operations and '$\equiv$' for the relation of identity of elements of the ring. It is convenient (and we shall do this in the future) to follow the usual convention and let $P = Q$ (e.g. $\frac{1}{2} = \frac{2}{4}$) be the relation which holds between words P, Q when they belong to the same equivalence class (i.e. represent the same element of R) and $P + Q$, $P \times Q$ stand for elements of the equivalence classes $\{P\} + \{Q\}$, $\{P\} \times \{Q\}$.(10a). If it is necessary to distinguish between operations in different rings we denote the relations and operations for R by the subscript R, thus, $=_R$, $+_R$, $\times_R$.

The above definition differs from van der Waerden's(11) in that we allow each element of the ring to be represented by more than one element of S but impose the condition that there should be an algorithm for deciding when two words P, Q represent the same element;

(8) λ is used as a constant throughout this paper and refers to a particular function with this property.

(9) By 'ring' we mean commutative ring throughout.

(10) This requirement is only apparently weaker than the requirement that S should be recursive since by mapping the nth element of S onto $W(n)$, we can get effectively to a representation of R in which the set of representing words is recursive, consisting in fact of the set of all words.

(10a) We shall also frequently fail to distinguish between the word P and the equivalence class $\{P\}$, e.g. we shall speak of the element P of R when we really mean the element $\{P\}$ of R. Only if confusion could arise shall we be careful to distinguish between P and $\{P\}$.

(11) Quoted on p. 407.

this is clearly in accordance with practical usage where we use all the symbols $\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \ldots$ to represent the same rational number. It differs also in that we require algorithms for deciding whether $P+Q=T$, $P\times Q=T$, whereas he requires algorithms for computing $P+Q$, $P\times Q$. However, these requirements are easily seen to be equivalent; this follows from the basic lemma and the fact that R is supposed to be a ring so that, for given P, Q, there do exist T_1, T_2 such that $P+Q=T_1$, $P\times Q=T_2$. In fact, a similar argument shows that there is an algorithm for computing the difference $P-Q$ of two elements of R and, in the case of explicit fields, the quotient P/Q $(Q\neq 0)$.

We shall say that an explicit ring R is *explicitly given* when the algorithms for generating the words representing the elements of R and for testing the relations $P=Q$, $P+Q=T$, $P\times Q=T$ are actually given. More precisely we say that *the positive integer t is a table of the explicit ring R*(12) when, in some standard recursive enumeration of ordered quadruples of positive integers,(13) t is the number of the quadruple $\langle t_1, t_2, t_3, t_4\rangle$, where $t_1, \ldots, t_4$ define(14) respectively recursive functions $f_1(x), f_2(x,y), f_3(x,y,z), f_4(x,y,z)$ such that the set S of words which represent elements of R is the set $\{W(f_1(1)), W(f_1(2)), \ldots\}$ and such that for all positive integers x, y, z,

$$W(f_1(x)) = W(f_1(y)) \,.\equiv.\, f_2(x,y) = 0,$$
$$W(f_1(x)) + W(f_1(y)) = W(f_1(z)) \,.\equiv.\, f_3(x,y,z) = 0,$$
$$W(f_1(x)) \times W(f_1(y)) = W(f_1(z)) \,.\equiv.\, f_4(x,y,z) = 0.\text{(14}a\text{)}$$

Furthermore, we consider a ring to be given when a table of it is given. It is clear that there is a general procedure for determining the functions f_1, f_2, f_3, f_4 from the table t, i.e. that one could construct machines M_1, M_2, M_3, M_4 such that M_1 when supplied with two positive integers t, x such that t was the table of an explicit ring determining functions f_1, f_2, f_3, f_4, would give the value of $f_1(x)$, and similarly for M_2, M_3, M_4. So when one is given the table of a ring one is in a position to perform all arithmetical computations in it. Note, however, that the correspondence between explicit rings and their tables is one-many, that there is no algorithm for deciding of a positive integer t whether it is a table of some explicit ring, that there is no algorithm, applicable to pairs t_1, t_2 of positive integers which are tables of explicit rings, for deciding whether t_1, t_2 are tables of the same explicit ring, nor for deciding whether they are tables of explicit rings which are isomorphic. So although one can perform arithmetical computations in an explicitly given ring one may not know very much about the ring; in fact, as we shall see below (p. 418) even if we know that a positive integer t is the table of an explicit ring which is isomorphic either to the rational field Q or to the field $Q(i)$ there is no general method of deciding which of these cases holds.(15) However, there is an algorithm for finding the zero of an explicitly given ring, i.e. an algorithm which enables one when supplied with a positive integer t which is known to be the table of an explicit ring R_t to find a word which represents its zero element; indeed, one has only to take any

(12) With respect to some fixed alphabet A. Clearly if we wish we can always use a single letter alphabet $\{a\}$; in practice it would be more convenient to use the rather large alphabet consisting of all signs available in print.

(13) Say that in which the number of the quadruple $\langle t_1, t_2, t_3, t_4\rangle$ is $\phi(\phi(\phi(t_1, t_2), t_3), t_4)$ where $\phi(x,y) = x+\frac{1}{2}(x+y-1)\,(x+y-2)$.

(14) In the sense of Kleene (1936).

(14a) Here ' $\equiv$ ' stands for material equivalence, 'if and only if'.

(15) In this connexion see Krull's comment (1953a) on Kneser's paper (1953).

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

word P representing an element of R_t and enumerate words Q of R_t until one is found such that $P+Q=P$. Similarly, there is an algorithm for finding the unit element of an explicitly given field.(16)

We shall say that an explicit ring is an *explicit representation* of any ring to which it is isomorphic. We note here that any finite ring has an explicit representation, for we can represent each element by a different word and write out the addition and multiplication table in full. The ring of integers has a familiar explicit representation—in the scale of ten, with alphabet $\{0, 1, \ldots, 9, -\}$, the representing words being 0, 1, -1, 2, -2, ..., 10, -10, 11, -11, ..., and the rules for addition and multiplication being the usual ones, which are well known to be effective. The field of rational numbers also has a well-known explicit representation where the elements are represented in the form $\pm p/q$, p being a non-negative and q a positive integer represented as above.

In classical algebra it is customary to more or less identify isomorphic rings, since any algebraic property which one possesses is shared by the other. But this is no longer true of the non-purely algebraic properties such as effective computability with which we are dealing; in an arbitrary isomorphism $W \leftrightarrow W'$ there may be no algorithm for finding the word W' given W or vice versa. So we define a narrower concept of *explicit isomorphy* to replace the classical concept of isomorphy.

2·2. Definition. *An explicit homomorphism (isomorphism) θ of R_1 $\begin{Bmatrix}\text{into}\\ \text{onto}\end{Bmatrix}$ R_2 is a homomorphism (isomorphism) $P_1 \to \theta(P_1)$ of R_1 $\begin{Bmatrix}\text{into}\\ \text{onto}\end{Bmatrix}$ R_2 such that there is an algorithm for deciding, for words $P_1 \in R_1$, $P_2 \in R_2$, whether or not $P_2 =_{R_2} \theta(P_1)$.*

The basic lemma shows that an equivalent definition is obtained by requiring an algorithm for computing $\theta(P_1)$ instead of for deciding whether $P_2 = \theta(P_1)$. From this alternative form of the definition one sees at once that if $\theta: R_1 \to R_2$, $\theta_1: R_2 \to R_3$ are explicit homo- or isomorphisms, then so is $\theta_1\theta: R_1 \to R_3$: also that if θ is an explicit isomorphism of R_1 onto R_2 then θ^{-1} is an explicit isomorphism of R_2 onto R_1. Hence if we make the obvious definition:

2·3. Definition. *Two explicit rings R_1, R_2 are said to be explicitly isomorphic if there is an explicit isomorphism of R_1 onto R_2.*

We see that the relation of explicit isomorphy is an equivalence relation.

It is clear that in discussing properties concerned with effective computability we usually do not need to distinguish between explicitly isomorphic rings. Some(17) well-known rings have the property that all their explicit representations are explicitly isomorphic:

2·4. Theorem. *If R is a finite ring, or the ring of integers, or the field of rational numbers, then all explicit representations of R are explicitly isomorphic.*

Proof. For finite rings the result is trivial; we can simply write out an isomorphism table containing all pairs of corresponding elements. Suppose then that R, R' are two explicit representations of the ring of integers. Let W_1, W_1' be words of R, R' respectively representing the element 1. For each word W of R we can find a positive integer n such that

$$W = W_1 + \ldots (n \text{ times}) \ldots W_1 \quad \text{or} \quad W = -(W_1 + \ldots (n \text{ times}) \ldots W_1).$$

(16) This result does *not* hold for explicit rings.

(17) But not all, as we shall see in §6.

Let us associate W with n in the first case and with $-n$ in the other. We now get an explicit isomorphism between R and R' by mapping W on W' if and only if they are associated with the same integer. A similar treatment may be used for the field of rationals.

We now define the 'explicit' analogues of some other classical concepts. Throughout these definitions R_1, R_2 denote two explicit rings whose elements are represented by words of the sets S_1, S_2 of the alphabets A_1, A_2.

2·5. DEFINITION. *R_1 is said to be an explicit extension of R_2 and R_2 is said to be an explicit sub-ring of R_1 if $A_2 \subseteq A_1$, $S_2 \subseteq S_1$ and, for P_2, $Q_2 \in S_2$, $P_2 =_{R_1} Q_2$ is equivalent to $P_2 =_{R_2} Q_2$ and $P_2 +_{R_1} Q_2 =_{R_1} P_2 +_{R_2} Q_2$, $P_2 \times_{R_1} Q_2 =_{R_1} P_2 \times_{R_2} Q_2$. If, in addition, there is an algorithm for deciding for an arbitrarily given word P of S_1 whether there exists $Q \in S_2$ such that $P =_{R_1} Q$(18), then R_1 is said to be a completely explicit extension of R_2.* Note that according to this definition an explicit extension is not necessarily an extension in the classical sense, since the element $\{P_2\}_{R_1}$ which corresponds in R_1 to the element $\{P_2\}_{R_2}$ of R_2 may not coincide with it but may contain additional words. But no error should arise since R_2 is isomorphic to a sub-ring of R_1. It has the effect that we consider the ring of rationals given in the form p/q to be an explicit extension of the ring of integers given in the form $p/1$, even though there are other words (pk/k) in the ring of rationals which represent these integers. Note that the relation of (completely) explicit extension is transitive.

2·6. DEFINITION. *Two explicit extension rings R_1, R_2 of R are said to be explicitly isomorphic over R if there is an explicit isomorphism of R_1 onto R_2 in which all elements of R remain fixed.*

2·7. DEFINITION. *If R, R_1 are explicit rings and $\bar{R}$ is an extension ring of R, then R_1 is said to be an explicit extension of R corresponding to $\bar{R}$ if it is an explicit extension of R and if it is (classically) isomorphic to $\bar{R}$ over R.*

3. EXPLICITNESS OF CERTAIN EXTENSION RINGS

3·1. THEOREM. *If R is an explicit ring with identity element then there exists an explicit extension of R corresponding to the ring $R[x]$ of polynomials in one indeterminate over R; this extension is a completely explicit extension and is unique to within explicit isomorphism over R.*

Proof. Such an extension R_0 may be obtained by adding new symbols,(19) 'x', '$+$', '0', ..., '9', to the alphabet of R, representing the elements of $R[x]$ by words of the form $P_0 + P_1 x + P_2 x^2 + \ldots + P_n x^n$, where $P_0, \ldots, P_n$ are words of R, and defining equality, addition and multiplication in the familiar way. This extension is a completely explicit extension, since the condition that a word of the above form should be equal to a word of R is simply that all of $P_1, \ldots, P_n$ should be equal to zero in R, and there is obviously an effective test for this. Suppose now that R_1 is another explicit extension of R corresponding to $R[x]$. By hypothesis there exists an isomorphism θ of R_1 onto $R[x]$ over R. Let X be a word of R_1 corresponding to the element x of $R[x]$ under θ. Given any word P of R_1 we can enumerate the elements of R_0 and corresponding to each element $P_0 + P_1 x + P_2 x^2 + \ldots + P_n x^n$ we can compute a word(20) $P_0 +_{R_1} P_1 X +_{R_1} P_2 X^2 +_{R_1} \ldots +_{R_1} P_n X^n$ of R_1 and test whether this is equal (in R_1) to P. Since each word P of R_1 is the image under θ of some element of $R[x]$ we shall

(18) I.e. for deciding whether a given element of R_1 belongs to R_2.

(19) Together with a symbol $\uparrow$ to deal with the superscripts in x^2, x^3, ... as mentioned in footnote (4), p. 408.

(20) Here $P_1 X$ stands for $P_1 \times_{R_1} X$, and X^2 for $X \times_{R_1} X$.

eventually find an element $P_0+P_1x+\ldots+P_nx^n$ of R_0 such that $P={}_{R_1}P_0+{}_{R_1}P_1X+{}_{R_1}\ldots+{}_{R_1}P_nX^n$. The mapping in which each P is mapped on this corresponding element $P_0+P_1x+\ldots+P_nx^n$ of R_0 is an explicit isomorphism from R_1 onto R_0 over R.

By repeated application of theorem 3·1 or by a similar treatment we obtain

3·11. Corollary. *The result of theorem* 3·1 *holds also for the ring* $R[x_1, \ldots, x_n]$ *of polynomials in n independent indeterminates over R.*

For rings of polynomials in $\aleph_0$ indeterminates we have:

3·2. Theorem. *If R is an explicit ring with identity element there exists a completely explicit extension of R corresponding to the ring* $R[x_1, x_2, \ldots]$ *of polynomials in* $\aleph_0$ *indeterminates over R.*

Proof. Such an extension R_0 may be obtained by adding the symbols 'x', '0', ..., '9' (together with sub- and superscript symbols $\uparrow$, $\downarrow$ as mentioned in footnote(4), p. 408) to the alphabet of R, representing the elements of $R[x_1, x_2, \ldots]$ by words of the form $T_1+\ldots+T_k$, where each T_i is of the form $P_ix_1^{r_1}x_2^{r_2}\ldots x_n^{r_n}$, P_i being a word of R and $r_1, r_2, \ldots, r_n$ non-negative integers (written in the scale of ten), and defining equality, addition and multiplication in the usual way. We shall see in § 6 that in contrast to the finite case the extension postulated in 3·2 is not unique. However, if we call the above defined explicit extension R_0 the *standard explicit extension of R corresponding to* $R[x_1, x_2, \ldots]$ we obtain, by an argument similar to that used in the uniqueness part of 3·1:

3·21. Theorem. *If* R_1 *is an explicit extension of R which is isomorphic over R to* $R[x_1, x_2, \ldots]$ *by an isomorphism* θ *such that the set* S_1, *of words of* R_1 *which are images under* θ *of the set* $\{x_1, x_2, \ldots\}$, *is recursively enumerable, then* R_1 *is explicitly isomorphic over R to the standard explicit extension* R_0 *of R corresponding to* $R[x_1, x_2, \ldots]$.

3·3. Theorem. *If R is an explicit integral domain then there exists an explicit extension* R' *of R corresponding to the quotient field* $\bar{R}$ *of R;* R' *is unique to within explicit isomorphism over R; it is a completely explicit extension of R if and only if R has a divisibility algorithm.*(21)

Proof. Add a new symbol '/' to the alphabet of R and take for the elements of R' words of the form P or P/Q, where P, Q are elements of R and $Q\neq_R 0$.(22) Now define $P/Q=_{R'}T/S$ if and only if $P\times_R S=_R Q\times_R T$, $P/Q=_{R'}T$ if and only if $P=Q\times_R T$, and $P=_{R'}Q$ if and only if $P=_R Q$. Define addition and multiplication similarly in the familiar way. Then R' has the required properties. Since P/Q is equal to a word of R if and only if $Q\,|\,P$ it follows that the extension is a completely explicit extension if and only if R has a divisibility algorithm.

Suppose now that R'' is any other explicit extension of R corresponding to $\bar{R}$. If W'' is any word of R'' we can find(23) a pair of words P, Q $(Q\neq 0)$ of R such that $W''\times_{R''}Q=_{R''}P$. The mapping θ defined by $\theta(W'')=P/Q$ gives an explicit isomorphism of R'' onto R' over R.

3·4. Theorem. *If K is an explicit field then there exists a completely explicit extension of K corresponding to the field* $K(\alpha)$ *where* α *is transcendental or algebraic over K.*

Proof. For α transcendental the result follows from 3·1, 3·3. Suppose now that α is algebraic and that $f(x)=0$ is the irreducible equation for α over K. Let K' be the explicit extension of K corresponding to $K[x]$. Define K'' to have the same words and definition of addition

(21) I.e. an algorithm for deciding of arbitrary words P, $Q(Q\neq 0)$ of R whether $Q|P$.

(22) This set of words is easily seen to be recursively enumerable.

(23) By enumerating the pairs P, Q of words of R with $Q\neq 0$ and testing each pair in turn.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

and multiplication as K' but to have equality defined by $p(x) =_{K''} q(x)$ if and only if $f(x) \mid (p(x) - q(x))$. This is effective since there is a divisibility algorithm in K'. K'' is an explicit extension of K corresponding to $K(\alpha)$. It is a completely explicit extension since $p(x)$ will represent a word of K if and only if its remainder on division by $f(x)$ is of 0th degree in x, and this can be tested.

We may sum up these results in:

3·5. THEOREM. *If K is an explicit field and $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a finite extension field of K then there exists an explicit extension of K corresponding to $K(\alpha_1, \ldots, \alpha_n)$; this is a completely explicit extension and is unique to within explicit isomorphism over K. All finite extensions of prime fields have explicit representations which are unique to within explicit isomorphism.*

Proof. The existence of a completely explicit extension of K corresponding to $K(\alpha_1, \ldots, \alpha_n)$ follows from 3·4. Let now $K_1, \overline{K}_1$ be two explicit extensions of K, isomorphic to $K(\alpha_1, \ldots, \alpha_n)$ over K by isomorphisms $\theta, \bar{\theta}$. Let $W_i, \overline{W}_i (i = 1, \ldots, n)$ be words of $K_1, \overline{K}_1$ respectively which are images under $\theta, \bar{\theta}$ respectively of α_i. Then the mapping $W_i \leftrightarrow \overline{W}_i (i = 1, \ldots, n)$ defines an isomorphism of K_1 onto $\overline{K}_1$ over K. This is an explicit isomorphism; to see whether $W \leftrightarrow \overline{W}$ we can proceed as follows: enumerate the rational functions $\phi(x_1, \ldots, x_n)/\psi(x_1, \ldots, x_n)$ of n variables $x_1, \ldots, x_n$ with coefficients in K; for each one compute $\psi(\overline{W}_1, \ldots, \overline{W}_n)$ and if it is non-zero test $\phi(\overline{W}_1, \ldots, \overline{W}_n)/\psi(\overline{W}_1, \ldots, \overline{W}_n)$ for equality with $\overline{W}$ (in $\overline{K}_1$); continue this procedure until a ϕ/ψ is found for which this occurs; now test whether $\phi(W_1, \ldots, W_n)/\psi(W_1, \ldots, W_n)$ is equal (in K_1) to W; $W \leftrightarrow \overline{W}$ holds if and only if this is so.

The existence and uniqueness of the explicit representations of the prime fields themselves has been shown in 2·4. Suppose now that K_1 is any extension field of a prime field K and $\overline{K}$ is an explicit field isomorphic to K_1. Then if W_1 is a word of $\overline{K}$ representing the identity element, the elements $W_1, W_1 + W_1, \ldots, W_1 + \ldots$ (p times) $\ldots + W_1$, if K is of characteristic p, or the elements 0 (i.e. $W_1 - W_1$), $\pm W_1, \frac{\pm W_1}{W_1 + W_1}, \pm \frac{W_1 + W_1}{W_1}, \ldots$, if K is of characteristic 0, constitute, with the definition of equality, addition and multiplication as in $\overline{K}$, an explicit sub-field of $\overline{K}$ isomorphic to K. So if $K(\alpha_1, \ldots, \alpha_n)$ is a finite extension of a prime field K and $\overline{K}$ is an explicit representation of $K(\alpha_1, \ldots, \alpha_n)$, then $\overline{K}$ contains an explicit sub-field K' isomorphic to K and is easily seen to be an explicit extension of K' corresponding to $K'(\alpha_1, \ldots, \alpha_n)$. The uniqueness (to within explicit isomorphy) of K now follows from the first result and the uniqueness of the explicit representations of the prime fields.

By theorems 3·2 and 3·3 there exists an explicit extension of a given explicit field K corresponding to the field $K(x_1, x_2, \ldots)$ obtained by the adjunction of $\aleph_0$ transcendentals. As we shall see later this explicit extension is not unique, so it is convenient to call the particular extension defined via 3·2 and 3·3 (in which we may say the elements are represented as rational functions of $x_1, x_2, \ldots$) the *standard explicit extension of K corresponding to $K(x_1, x_2, \ldots)$*. An analogous result to 3·21 holds for this standard explicit extension.

The uniqueness of the explicit extensions defined in § 3 allows us to introduce the following convention. If K is an explicit field (or ring), and if R is an explicit polynomial ring, defined as an explicit extension of K as in 3·1 by introducing the new symbol x to represent the generating indeterminate of R over K, we shall call R *the explicit polynomial extension of K in the indeterminate x*. Similarly, we shall speak of *the explicit finite, or standard polynomial extension R of the explicit field K in the indeterminates $x_1, x_2, \ldots, x_n$, or the indeterminates $x_1, x_2, \ldots$* ad inf., and of

the explicit finite, or standard transcendental extension $\overline{K}$ *of* K *by the independent transcendentals* $x_1, x_2, \ldots, x_n$, or $x_1, x_2, \ldots$ ad inf. The same convention will also be applied to finite algebraic extensions, etc.

4. Splitting algorithms in finite and standard extension fields

4·1. Definition. *The explicit u.f.d.* R *is said to have a factorization algorithm if there is an algorithm which, when applied to any word* W *of* R *will yield words* $W_1, \ldots, W_n$ *representing irreducible elements of* R *such that* $W = W_1 \times W_2 \times \ldots \times W_n$, *none of the* $W_1, \ldots, W_n$ *being units except possibly when* $n = 1$.

The explicit representation of the ring of integers is well known to have such a factorization algorithm.

4·2. Theorem. *The explicit u.f.d.* R *has a factorization algorithm if and only if it has an algorithm for deciding whether an element is irreducible.*

Proof. If W splits into $W_1 \times \ldots \times W_n$ as in 4·1 then it is irreducible if and only if $n = 1$.

Conversely, if there is an algorithm for deciding whether an element is irreducible there is an algorithm for deciding of each element W whether it is (*a*) reducible, (*b*) a unit or (*c*) irreducible but not a unit, since if W is irreducible it is a unit if and only if W^2 is also irreducible. So we can enumerate the irreducible non-units and hence also the finite products $W_1 \times W_2 \times \ldots \times W_n$ of irreducible non-units. We can also enumerate the units. Since any word W is either a unit or a product of irreducible non-units we have only to compare it with each element of the preceding enumeration until we find one equal to it; this gives a factorization of the type required in 4·1.

4·3. Theorem. *Let* R *be an explicit u.f.d.,* R_n *the explicit polynomial extension of* R *in the indeterminates* $x_1, \ldots, x_n$, R_ω *the explicit standard polynomial extension of* R *in the indeterminates* $x_1, x_2, \ldots$. *Then if there is a factorization algorithm in* R_1 *there is one in* R_n $(n = 1, 2, \ldots)$ *and in* R_ω.

Proof. This is essentially a well-known result of Kronecker. Given a polynomial $f(x_1, \ldots, x_n)$ we take m greater than its degree, make the substitution $x_i = t^{m^{i-1}} (i = 1, \ldots, n)$, factorize the resulting polynomial in t and examine whether these factors correspond to polynomials in $x_1, \ldots, x_n$. (See, for example, van der Waerden 1930*a* p. 129.) Given an element of R_ω we first find the number n of transcendentals $x_1, \ldots, x_n$ involved in it and factorize it in R_n as above.

4·4. Definition. *If* R *is an explicit u.f.d. and* R_1 *the explicit polynomial extension of* R *in the indeterminate* x, *then we say* R *has a splitting algorithm if* R_1 *has a factorization algorithm; we say* R *has a root algorithm if there is an algorithm for deciding whether a given element of* R_1 *has a root in* R.

So a splitting algorithm is an algorithm for splitting polynomials in one variable over R into their irreducible factors over R. 4·3 shows that a splitting algorithm implies the existence of an algorithm for splitting polynomials in several variables into their irreducible factors.

We have the classical result of Kronecker (1882, pp. 79, 80):

4·41. Theorem. *An explicit ring with a factorization algorithm and only a finite number of units has a splitting algorithm.*

We have also the classical result that (any explicit representation of) the rational field has a splitting algorithm, so:

4·42. Theorem. *All the prime fields have splitting algorithms.*

4·43. Theorem. *An explicit field* K *has a splitting algorithm if and only if it has a root algorithm.*

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Proof. The 'only if' part is obvious; if we can split a polynomial into its irreducible factors we have only to examine the degrees of these factors to see whether the polynomial has a linear factor.

For the converse we note first that, since the factors of $f(x)$ are of degree less than or equal to that of $f(x)$ it is enough to show that for each positive integer r we can decide whether a given polynomial $f(x)$ has rth degree factors and that we can find them if it has. Secondly, we note that it is enough to produce *one* proper factor of $f(x)$, since we can then find the quotient $g(x)$ of $f(x)$ by this and apply the same procedure to $g(x)$. Take now the case $r = 1$. By hypothesis we can decide whether $f(x)$ has a linear factor. If it has we can find one, since we have only to enumerate the elements $W_1, W_2, \ldots$ of K in turn until we find a W such that $f(W) = 0$ and then we have $x - W$ as a factor. Applying the above-mentioned procedure of dividing out by the known factors we can in this way obtain all the linear factors of $f(x)$, i.e. all the roots of $f(x)$ which lie in K. Suppose now that $r > 1$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x) = 0$ in some splitting field of $f(x)$. The rth degree factors of $f(x)$ in any field must be of the form $g(x) \equiv (x - \alpha_{i_1}) \ldots (x - \alpha_{i_r})$ for some set of $i_1, \ldots, i_r$ chosen from $1, 2, \ldots, n$. Now consider the coefficients of $g(x)$; the coefficient of x^0 is $(-1)^r \alpha_{i_1} \ldots \alpha_{i_r}$ and is a root of the equation $h_0(x) = 0$, where $h_0(x) \equiv \Pi(x - (-1)^r \alpha_{i_1} \ldots \alpha_{i_r})$, the product being taken over all sets of distinct $i_1, \ldots, i_r$, lying between 1 and n. The coefficients of $h_0(x)$ are calculable symmetric functions of the α_i so they can be explicitly evaluated in terms of the coefficients of $f(x)$. Similarly for the coefficients of $x^1, \ldots, x^{r-1}$ in $g(x)$ we may calculate polynomials $h_1(x), \ldots, h_{r-1}(x)$ in $K[x]$ such that the coefficient of x^i in $g(x)$ is a root of $h_i(x) = 0$. Each of these equations has in K only a finite number of roots, all of which, as we have shown above, can be found. So we obtain a finite number of sets $\{\xi_0, \xi_1, \ldots, \xi_{r-1}\}$ consisting of roots in K of

$$h_0(x) = 0, \ldots, h_{r-1}(x) = 0$$

respectively. For each such set we take the polynomial $x^r + \xi_{r-1} x^{r-1} + \ldots \xi_0$ and test whether it is a factor of $f(x)$. In this way we shall obtain an rth degree factor of $f(x)$ if it has one; if it has not we shall discover this.

4·5. THEOREM. *Let K be an explicit field, $K_n (n = 1, 2, \ldots)$ the explicit transcendental extension of K by the independent transcendentals $x_1, \ldots, x_n$, and K_ω the explicit standard transcendental extension of K by the independent transcendentals $x_1, x_2 \ldots$. Then if K has a splitting algorithm so have $K_n (n = 1, 2, \ldots)$ and K_ω.*

Proof. See van der Waerden (1930*a*, pp. 130, 131); the result for K_ω follows from the fact that the coefficients of a polynomial over K_ω involve only a finite number n of the $x_1, x_2, \ldots$, and that the splitting over K_ω is then the same as over K_n.

4·6. THEOREM. *Let K be an explicit field, K' the explicit extension of K by $\alpha_1, \ldots, \alpha_n$, where $\alpha_1, \ldots, \alpha_n$ are separable and algebraic over K. Then if K has a splitting algorithm so has K'.*

Proof. See van der Waerden (1930*a*, pp. 130, 131).

This does not hold for inseparable extensions (see 7·27); however, we have:

4·7. THEOREM. *Let K be an explicit field of characteristic p with a splitting algorithm, K' the explicit extension of K by $\alpha_1, \ldots, \alpha_n$, where $\alpha_1, \ldots, \alpha_n$ are algebraic over K. Then K' has a splitting algorithm if and only if it has a p-th root algorithm, i.e. an algorithm for determining of an arbitrary element of K' whether it has a p-th root in K'.*

Proof. The 'only if' part is trivial, since the element W of K' has a pth root in K' if and only if $x^p - W$ is reducible.

For the converse we shall show first that it is sufficient to prove the result in the case $n = 1$. For suppose the result is true for $n = n_0$. Let K' be the explicit extension of K by $\alpha_1, \ldots, \alpha_{n_0}$ and K'' the explicit extension of K by $\alpha_1, \ldots, \alpha_{n_0}, \alpha_{n_0+1}$. Suppose that K'' has a pth root algorithm; then this algorithm will say whether an element of K' has a pth root in K'' and, if it has we can find it and, since K'' is a completely explicit extension of K', we can test to see whether this pth root belongs to K'. So K' has a pth root algorithm. So by the induction hypothesis it has a splitting algorithm. Now it follows from the case $n = 1$ that K'' has a splitting algorithm.

Suppose then that $n = 1$, that K' is the explicit extension of K by α, and that K has a splitting algorithm and K' a pth root algorithm. Let $g(x) = 0$ be the irreducible equation for α in $K[x]$. By inspection we can find the highest power of p, say p^e, such that $g(x) = g_1(x^{p^e})$, where $g_1(x)$ is a polynomial in $K[x]$. $g_1(x)$ is then irreducible and separable over K, and α^{p^e} is a root of it. If K^* is the explicit extension of K by α^{p^e} then, as a separable extension of K, K^* has a splitting algorithm, and $K(\alpha) = K^*(\alpha^{p^{e-1}}, \alpha^{p^{e-2}}, \ldots, \alpha)$, where α^{p^h} satisfies the irreducible equation $x^p - \alpha^{p^{h+1}} = 0$ over $K^*(\alpha^{p^{e-1}}, \ldots, \alpha^{p^{h+1}})$ for $h = 0, \ldots, e-2$, and over K^* for $h = e-1$. By 3·5 K' is explicitly isomorphic over K to the explicit extension of K^* by $\alpha^{p^{e-1}}, \ldots, \alpha$. Hence by the same inductive argument as used above it is sufficient to prove the theorem for one of these successive adjunctions, i.e. we can assume that α is a root of an irreducible equation of the form $g(x) = x^p - W$, where W is a word in K. Now let $f(x)$ be a polynomial with coefficients in K'. $f(x)^p$ has coefficients in K and can thus be split into its irreducible factors in $K[x]$. Each such factor $h(x)$ is either irreducible in $K'[x]$ or is the pth power of an irreducible polynomial in $K'[x]$, and the latter is the case if and only if $h(x)$ is a polynomial in x^p and each coefficient is a pth power in K', which by hypothesis can be decided. Hence we can find the irreducible factors of $f(x)$ in $K'[x]$, i.e. K' has a splitting algorithm.

In the case where K is a prime field 4·6 holds without the condition that $\alpha_1, \ldots, \alpha_n$ be separable. In fact

4·8. THEOREM. *If K is an explicit representation of a prime field and K' an explicit extension of K by a finite set of elements $\alpha_1, \ldots, \alpha_n$, then K' has a splitting algorithm.*

Proof. As pointed out by Krull (1953*a*) any finite extension of a prime field can be obtained by first adjoining a finite set of independent transcendentals $x_1, \ldots, x_i$ and then making a finite number of simple separable algebraic extensions by $\beta_1, \ldots, \beta_j$. Theorem 4·8 now follows from 4·5, 4·6 by the uniqueness theorem 3·5 or alternatively from the fact that Krull has shown that one has an effective procedure for finding $x_1, \ldots, x_i, \beta_1, \ldots, \beta_j$ from $\alpha_1, \ldots, \alpha_n$.

It is worth pausing here to see to what extent the algorithmic procedures described above are 'general' in the sense that the particular techniques of computation used do not depend on the particular explicit fields considered. In most of the cases this is fairly clear, so we shall content ourselves with mentioning only one or two cases which have been commented on in the literature. The procedure of theorem 4·6 is general to the extent that we could in theory construct a machine which, when supplied with (1) a table t of the explicit field K;

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

(2) a (description number (see Turing 1937) of a) machine M which effects the splitting of polynomials with coefficients in K; (3) a table t' of an explicit field K' which is an explicit algebraic extension of K by a finite number of separable elements $\alpha_1, \ldots, \alpha_n$; (4) *words* $W_1, \ldots, W_n$ of K' *representing the elements* $\alpha_1, \ldots, \alpha_n$,(24); (5) a polynomial $f(x)$ in $K'[x]$ (given in the form $P_0+P_1x+\ldots+P_mx^m$, where $P_0, \ldots, P_m$ are words of K'), would produce the irreducible factors of $f(x)$ in $K'[x]$. But the information contained in (4) is very necessary and there is no general procedure for finding it.(25) In fact this is true even if we fix K as the usual explicit representation Q of the rational field and consider only those K' isomorphic to either Q or $Q(i)$. In this case data (1), (2) are fixed, so if (4) were indeed unnecessary we should have a machine M_0 which when supplied with (3) the table t' of an explicit field K' which is known to be an explicit extension of Q corresponding to either Q or $Q(i)$ and (5) a polynomial $f(x)$ in $K'[x]$, would tell us whether $f(x)$ was irreducible in $K'[x]$. To see that this is impossible(26) define for each positive integer m an explicit field K_m as follows: K_m is obtained by taking the standard explicit extension Q_ω of Q by infinitely many independent transcendentals $x_1, x_2, \ldots$, leaving addition and multiplication unchanged but altering the definition of equality of words in the obvious way so as to make $x_n = i$ if n is the least y such that $\lambda(y) = m$,(27) $x_n = 1$ otherwise. Clearly there is an algorithm for computing a table t_m of K_m. But K_m is isomorphic to $Q(i)$ if $(\exists y)\,(\lambda(y) = m)$ and to Q otherwise, so the polynomial $1+x^2$ is reducible in K_m if and only if $(\exists y)\,(\lambda(y) = m)$. So if the machine M_0 existed we would only have to compute t_m, feed t_m and the polynomial $1+x^2$ into M_0 and see whether M_0 said 'reducible' or 'irreducible' in order to determine whether $(\exists y)\,(\lambda(y) = m)$. Since there is no algorithm for deciding this it follows that no such machine M_0 can exist. This example yields also the result of van der Waerden (1930*b*) that there is no general algorithm for splitting polynomials over an explicitly given field, i.e. that there is no machine which when supplied with a table t of an explicitly given field K and a polynomial $f(x)$ in $K[x]$ will produce the irreducible factors of $f(x)$ in $K[x]$. Since we have seen this to be the case even if K is restricted to being isomorphic to one of the fields Q, $Q(i)$ one may ask whether van der Waerden's argument (which is essentially taking $x_n^2 = p_n$, the nth prime number, where we took $x_n = 1$) really shows any difference between the finite and infinite algebraic extensions of Q. It does in the following sense: For explicit fields isomorphic to finite algebraic extensions $Q(\alpha_1, \ldots, \alpha_n)$ there is a splitting procedure which is general to the extent that one has a machine which will give the splitting when supplied with the table, the polynomial, and words representing $\alpha_1, \ldots, \alpha_n$; in the infinite case this fails; there is no machine which will split polynomials when supplied with the table, the polynomial and (a description number of) a machine for enumerating words representing $\alpha_1, \alpha_2, \ldots$ (and the corresponding irreducible equations(28)). In §7 we shall see that this result can be strengthened, that there are particular explicit fields of this type without splitting algorithms, whereas as we have seen above (4·8) every *finite* explicit extension of a prime field has a splitting algorithm.

(24) We do not need to know the irreducible equations satisfied by $\alpha_1, \ldots, \alpha_n$—we can find these by a simple procedure of enumeration and testing.

(25) See Krull (1953*a*).

(26) The following argument is a slight modification of van der Waerden's proof in (1930*b*).

(27) Where λ is the function defined on p. 409.

(28) As a matter of fact these can be found from the α's as mentioned in footnote (24).

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

5. Explicitness of algebraic dependence in infinite extensions

We recall the definition of a transcendence basis(28*a*) of a field $\overline{K}$ over a subfield K as a set U of elements of $\overline{K}$, such that $\overline{K}$ is algebraic over $K(U)$, but not over $K(U')$ for any proper subset U' of U.

5·1. Definition. *Let $\overline{K}$ be an explicit extension field of an explicit field K. A set U of words of K is said to be an explicit transcendence basis of $\overline{K}$ over K if the set of elements of $\overline{K}$ represented by words of U forms a transcendence basis of $\overline{K}$ over K, and U is a recursively enumerable set.*

According to this definition an explicit transcendence basis may contain many words representing the same element of $\overline{K}$. If $\overline{K}$ is of finite degree of transcendence over K this is inevitable, but if $\overline{K}$ is of infinite degree of transcendence we can find an explicit transcendence basis $\{W(f(1)), W(f(2)), \ldots\}$ such that, if $n \neq m$, $W(f(n)) \neq_{\overline{K}} W(f(m))$. In fact, we have only to take an enumeration $W(g(1)), W(g(2)), \ldots$ of any given transcendence basis and define $f(1) = g(1)$, and, for $n > 1$, $f(n) = g(n_0)$, where n_0 is the least m such that $W(g(m)) \neq_{\overline{K}}$ to any of $W(f(1)), \ldots, W(f(n-1))$. In view of this remark we see that an explicit extension field $\overline{K}$ of an explicit field K which has an explicit transcendence basis over K, has one of the forms $\{u_1, \ldots, u_N\}$, or $\{u_1, u_2, \ldots, \text{ad inf.}\}$, where the u_i are words satisfying $u_n \neq_{\overline{K}} u_m$ for $n \neq m$. We shall make tacit use of this remark in future.

Without proof we state the obvious:

5·11. Theorem. *If K_0 is an explicit field, and if for $i = 1, \ldots, r$, K_i is an explicit extension of K_{i-1} with an explicit transcendence basis over K_{i-1} then K_r is an explicit extension field of K_0, with an explicit transcendence basis over K_0.*

The following definition gives, as will be seen, an equivalent characterization of those explicit fields having explicit transcendence bases in terms of the existence of an algorithm independent of any particular basis.

5·2. Definition. *Let $\overline{K}$ be an explicit extension field of an explicit field K. An algebraic dependence algorithm of $\overline{K}$ over K is an algorithm for deciding for any given finite set T of words of $\overline{K}$ and any given word W of K, whether or not W is algebraically dependent over K on T.*

5·3. Theorem. *Let $\overline{K}$ be an explicit extension field of an explicit field K. Then $\overline{K}$ has an explicit transcendence basis over K if and only if there exists an algebraic dependence algorithm of $\overline{K}$ over K.*

The proof of this theorem will be based on two lemmas. In both of these K stands for an explicit field and $\overline{K}$ for an explicit extension field of K which has an explicit transcendence basis over K.

5·31. Lemma. *There exists an algorithm to decide for any explicit transcendence (29) basis $U = \{u_1, u_2, \ldots\}$ of $\overline{K}$ over K (where $u_m \neq u_n$ for $m \neq n$), any finite (or empty) subset $U' = \{u_{i_1}, \ldots, u_{i_m}\}$ of U, and any word W of $\overline{K}$ whether W is algebraically dependent on U' over K.*

Proof. The algorithm proceeds thus: Enumerate the polynomials in infinitely many indeterminates $t, x_1, x_2, \ldots$ with coefficients in K. As each such polynomial is enumerated

(28*a*) In van der Waerden (1930*a*) the term 'algebraic basis' is used.

(29) As on pp. 410 we suppose the basis is given by being given a recursive function $f(n)$ (or, more exactly, a positive integer defining $f(n)$) which enumerates the words of the basis, i.e. such that the basis consists of the words $\{W(f(1)), W(f(2)), \ldots\}$.

replace t by W and each x_i by the corresponding u_i and determine whether the resulting word of $\overline{K}$ is equal to 0. Since W is algebraically dependent on U over K we shall ultimately find a polynomial $\phi(t, x_1, \ldots, x_n)$ such that $\phi(W, u_1, \ldots, u_n) = 0$. When such a polynomial is reached rearrange it as a polynomial in the x's distinct from $x_{i_1}, \ldots, x_{i_m}$ with coefficients non-zero polynomials ψ_j in $t, x_{i_1}, \ldots, x_{i_m}$. Take any of these coefficients ψ_j and replace in it t by W and $x_{i_1}, \ldots, x_{i_m}$ by $u_{i_1}, \ldots, u_{i_m}$ respectively and test to see whether the resulting word of $\overline{K}$ is equal to zero; W is algebraically dependent on U' over K if and only if this is so.

5·32. LEMMA. *There exists an algorithm to find for any explicit transcendence basis $U = \{u_1, u_2, \ldots\}$ of $\overline{K}$ over K (where $u_m \neq u_n$ for $m \neq n$) and any word W of $\overline{K}$ the*(30) *finite subset U_1 of U such that W is algebraically dependent over K on U_1 but not on any proper subset of U_1.*

Proof. As in 5·31 find a polynomial $\phi(t, x_1, \ldots, x_n)$ such that $\phi(W, u_1, \ldots, u_n) =_{\overline{K}} 0$. This gives W algebraically dependent on $u_1, \ldots, u_n$. U_1 is a subset of $\{u_1, \ldots, u_n\}$ which obviously can now be found by applying the procedures of 5·31 to determine the dependence of W on subsets of $\{u_1, \ldots, u_n\}$.

Proof of 5·3. Let K be an explicit field and $\overline{K}$ an explicit extension field of K having an explicit transcendence basis $U_0 = \{u_1, u_2, \ldots\}$ (where, for $m \neq n$, $u_m \neq u_n$) over K. By 5·31 the existence of an algebraic dependence algorithm will be established if we can show that there is an effective method for obtaining, from a given finite set T_0 of words of $\overline{K}$, an explicit transcendence basis $\overline{U}$ and a finite (or empty) subset $\overline{U}'$ of $\overline{U}$ such that a word in $\overline{K}$ is algebraic over $K(\overline{U}')$ if and only if it is algebraic over $K(T_0)$. Such a method may be obtained by a procedure of successive replacement of elements of the basis by elements of T_0. The basic step is one by which, starting from a finite set $T = \{t_1, \ldots, t_m\}$ of words of $\overline{K}$, an explicit transcendence basis U of $\overline{K}$ over K and a finite subset U' of U, we obtain a set $T_1 = \{t_1, \ldots, t_{m-1}\}$, an explicit transcendence basis U_1 and a finite subset U_1' of U_1 such that a word W of $\overline{K}$ is algebraic over $K(T \cup U')$ if and only if it is algebraic over $K(T_1 \cup U_1')$. Clearly starting with T as the given set $T_0 = \{t_1, \ldots, t_{m_0}\}$, U as the basis U_0 and U' as the empty set we shall, after m_0 repetitions of the basis step, arrive at a basis $\overline{U}$ and finite subset $\overline{U}'$ of $\overline{U}$ such that a word W is algebraic over $K(T_0)$ if and only if it is algebraic over $K(\overline{U}')$. The basic step is accomplished as follows: Find, by the method of 5·32, the subset $V = \{u_{i_1}, \ldots, u_{i_n}\}$ of U such that t_m is algebraically dependent over K on V but not on any proper subset of V. If $V \subseteq U'$ then take $U_1 = U$, $U_1' = U'$. If $V \not\subseteq U'$ let i_0 be the least i such that $u_i \in V$, but $u_i \notin U'$, define U_1 to be the same as U except that u_{i_0} is replaced by t_m and define $U_1' = U' \cup \{t_m\}$. It is easily seen hat U_1 is an explicit transcendence basis and that U_1' has the desired algebraic properties.

Suppose conversely that there exists an algebraic dependence algorithm of the explicit field $\overline{K}$ over its explicit subfield K. If $\overline{K}$ is of finite degree of transcendence over K then the existence of an explicit transcendence basis of $\overline{K}$ over K is trivial. So we may assume that $\overline{K}$ is of infinite degree of transcendence over K. Let $W(f(1)), W(f(2)), \ldots$ be a recursive enumeration of the words of $\overline{K}$. We define $g(1) = f(m_0)$, where m_0 is the least m such that $W(f(m))$ is not algebraic over K, and for $n > 1$, $g(n) = f(m_0)$, where m_0 is the least m such that $W(f(m))$ is algebraically independent over K of the set $W(g(1)), \ldots, W(g(n-1))$. Since $\overline{K}$ has an algebraic dependence algorithm over K, $g(n)$ is a recursive function and the set $W(g(1)), \ldots$ is an explicit transcendence basis of $\overline{K}$ over K.

(30) U_1 is easily seen to be unique.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

We now define, for any explicit field K, explicit extension fields Σ and Ω of K(31) which will be used as examples in some existence theorems.

Let $p_1, p_2, \ldots$ be the sequence of rational primes in ascending order of magnitude. Let R be the standard polynomial extension of K in the indeterminates $t, x_1, x_2, \ldots$ ad inf. Let $\mathfrak{a}$ be the ideal in R generated by $x_{2n}^{p_n} - t$, all n, and $\mathfrak{b}$ be the ideal in R generated by $x_{\lambda(n)}^{p_n} - t$, all n.(32)

There clearly exists an algorithm in R for deciding whether a word W of R lies in $\mathfrak{a}$. This allows us to define an explicit ring $R_{\mathfrak{a}}$ which is a homomorphic image of R with $\mathfrak{a}$ as kernel of the homomorphism. In fact we have only to take the words of $R_{\mathfrak{a}}$ as the words of R, define addition and multiplication in $R_{\mathfrak{a}}$ to be the same as in R but define $W =_{R_{\mathfrak{a}}} W'$ to hold if and only if $W -_R W'$ is in $\mathfrak{a}$. Similarly there exists an explicit ring $R_{\mathfrak{b}}$ which is the homomorphic image of R under a homomorphism with kernel $\mathfrak{b}$. To prove this we have only to show that there is an algorithm for deciding whether a word W of R lies in $\mathfrak{b}$. Such an algorithm may be obtained as follows: Given a word W of R represent it as a polynomial in t and the x_i, i.e. as a sum of terms of the form $ut^{\mu}\prod_{i=1}^{N} x_i^{\nu_i}$, where u lies in K. For each $i = 1, \ldots, N$ we now find all natural numbers r such that $p_r \leqslant \nu_i$, and for these r we evaluate the corresponding $\lambda(r)$. If $\lambda(r) \neq i$ for all r with $p_r \leqslant \nu_i$, then we write $\bar{\nu}_i = \nu_i$, $\bar{\mu}_i = 0$. If, on the other hand, $\lambda(r_0) = i$ and $p_{r_0} \leqslant \nu_i$, then $\bar{\nu}_i$, $\bar{\mu}_i$ are uniquely defined by $\nu_i = p_{r_0}\bar{\mu}_i + \bar{\nu}_i$, $0 \leqslant \bar{\nu}_i < p_{r_0}$, and may easily be computed. We now observe that $ut^{\mu}\prod_{i=1}^{N} x_i^{\nu_i} - ut^{\mu+\Sigma\bar{\mu}_i}\prod_{i=1}^{N} x_i^{\bar{\nu}_i}$ lies in $\mathfrak{b}$. Repeating this procedure for all terms of F we can thus derive a polynomial F^* such that (i) $W - F^*$ lies in $\mathfrak{b}$, (ii) the degree of x_m in F^* is less than p_n whenever $m = \lambda(n)$. Hence W lies in $\mathfrak{b}$ if and only if F^* lies in $\mathfrak{b}$ which is easily seen to be the case if and only if $F^* =_R 0$.

By a purely algebraic argument it is now easy to conclude that $\mathfrak{a}$, $\mathfrak{b}$ are prime ideals, and that $R_{\mathfrak{a}}$ and $R_{\mathfrak{b}}$ have no divisors of zero. Let then Ω be the explicit quotient field of $R_{\mathfrak{a}}$ and Σ be the explicit quotient field of $R_{\mathfrak{b}}$. These are both explicit extension fields of K.

5·4. THEOREM. *Every explicit field K has an explicit extension field which does not possess an explicit transcendence basis over K. In particular $\Sigma(K)$ is such a field.*

Proof. The existence of an explicit transcendence basis would by 5·3 imply the existence of an algorithm to decide for all m whether x_m is algebraic over $K(t)$, i.e. an algorithm to decide whether $(\exists n)\,(m = \lambda(n))$, and we know that no such algorithm exists.

5·5. THEOREM. *Every explicit field K has explicit extension fields which are isomorphic over K, but not explicitly isomorphic over K. In particular the two fields $\Omega(K)$, $\Sigma(K)$ have this property.*

Proof. Let $\mu(n)$ be a (non-recursive) function of natural numbers, taking no value twice and having as its set of values the natural numbers not in the set $\{\lambda(1), \lambda(2), \ldots\}$. The mapping $x_{2n} \to x_{\lambda(n)}$, $x_{2n-1} \to x_{\mu(n)}$ defines in an obvious way an isomorphism of $\Omega(K)$ onto $\Sigma(K)$ over K. $\Omega(K)$ has the explicit transcendence basis $\{t, x_1, x_3, \ldots, x_{2n-1}, \ldots\}$. Hence by 5·3 there exists an algebraic dependence algorithm for $\Omega(K)$ over K, and the same is true of any field which is explicitly isomorphic to $\Omega(K)$ over K. But we have seen in 5·4 that $\Sigma(K)$ has no algebraic dependence algorithm over K. Hence $\Omega(K)$, $\Sigma(K)$ are not explicitly isomorphic over K.

(31) We shall write $\Sigma = \Sigma(K)$, $\Omega = \Omega(K)$ when it is necessary to indicate the dependence of Σ, Ω on K.

(32) See p. 409 for the definition of λ.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

5·51. COROLLARY. *There exist two explicit fields which are isomorphic but not explicitly isomorphic.*

Proof. This is true of $\Omega(K)$, $\Sigma(K)$ if K is an explicit representation of a prime field, for in this case 'isomorphism' and 'isomorphism over K' and, similarly, 'explicit isomorphism' and 'explicit isomorphism over K' are equivalent.

6. CANONICAL EXTENSION FIELDS

6·1. DEFINITION. *Let $\overline{K}$ be an explicit extension field of an explicit field K. A recursively enumerable set $U = \{u_1, u_2, \ldots\}$ of words in $\overline{K}$ is called a canonical basis of $\overline{K}$ over K, if, denoting the empty set by U_0 and the set $\{u_1, u_2, \ldots, u_n\}$ by U_n,*

(i) *there exists an algorithm to decide for all n whether u_n is algebraic over $K(U_{n-1})$,*

(ii) *there exists an algorithm to find, for all n such that u_n is algebraic over $K(U_{n-1})$, an irreducible equation of u_n over $K(U_{n-1})$,*

(iii) *$\overline{K}$ is isomorphic over K to the union of the fields $K(U_n)$, all n.*

If $\overline{K}$ has a canonical basis over K then $\overline{K}$ is called a canonical extension of K.

We have the usual transitivity theorem:

6·11. THEOREM. *If for $i = 1, \ldots, r$, K_i is a canonical extension of the explicit field K_{i-1} then K_r is a canonical extension of K_0.*

The importance of the concept of canonical extension lies in the fact that it indicates a method of constructing infinite explicit extension fields by means of repeated adjunctions of a single element as in the theorems of § 3. In fact assume that $K = K_0$ is an explicit field and that for $n = 1, 2, \ldots, K_n$ is a simple extension field of K_{n-1}, $K_n = K_{n-1}(\alpha_n)$. By the results of § 3 there exist, for all n, explicit fields $\overline{K}_n$ corresponding to the fields K_n, $\overline{K}_n$ being an explicit extension of $\overline{K}_{n-1}$. ($\overline{K}_0$ is defined to be K_0.) The fields $\overline{K}_n$ are then unique to within explicit isomorphism. We assert, under certain conditions, the existence of a canonical extension field $\overline{K}$ of K corresponding to the union of the fields K_n. More precisely we assert:

6·12. THEOREM. *Let K be an explicit field and $K_1 = K(\alpha_1, \alpha_2, \ldots)$ be an extension field of K such that*

(i) *there is an algorithm for deciding for each n whether α_n is algebraic or transcendental over $K(\alpha_1, \ldots, \alpha_{n-1})$.*

(ii) *there is an algorithm for finding, for those n such that α_n is algebraic over $K(\alpha_1, \ldots, \alpha_{n-1})$, a polynomial*(33) *$\phi_n(x_1, \ldots, x_{n-1}, x_n)$ in $x_1, \ldots, x_n$ with coefficients in K such that $\phi_n(\alpha_1, \ldots, \alpha_{n-1}, x) = 0$ is an irreducible equation for α_n over $K(\alpha_1, \ldots, \alpha_{n-1})$.*

Then there is a canonical explicit extension $\overline{K}$ of K corresponding to K_1.

Proof. Let K' be the standard transcendental extension of K by the independent transcendentals $x_1, x_2, x_3, \ldots$. We first define inductively a sequence of explicit fields $K^0, K^1, K^2, \ldots$ corresponding to the fields $K, K(\alpha_1), K(\alpha_1, \alpha_2), \ldots$. We put $K^0 = K$ and for $n > 0$ we define K^n as follows: Let P_n be the set of words of K' which are *polynomials* in $x_1, \ldots, x_n$ with coefficients in K; we define an equivalence relation $=_n$ on P_n by putting $f(x_1, \ldots, x_n) =_n g(x_1, \ldots, x_n)$ if

(33) It might seem more reasonable to allow ϕ_n to be a polynomial in x_n whose coefficients were rational functions of $x_1, \ldots, x_{n-1}$; however from such a ϕ_n we can effectively get a polynomial in $x_1, \ldots, x_n$ with the desired properties by multiplying by the least common multiple of the denominators of these rational functions with coefficients in K, so we may as well assume from the start that we are given a polynomial ϕ_n with coefficients in K.

and only if either (*a*) α_n is transcendental over $K(\alpha_1, \ldots, \alpha_{n-1})$ and when f, g are expressed as polynomials in x_n whose coefficients are polynomials in $x_1, \ldots, x_{n-1}$ these corresponding coefficients are equal(**34**) in K^{n-1}, or (*b*) α_n is algebraic over $K(\alpha_1, \ldots, \alpha_{n-1})$ and the difference $f(x_1, \ldots, x_n) - g(x_1, \ldots, x_n)$ is, as a polynomial in x_n with coefficients in K^{n-1} divisible by the polynomial $\phi_n(x_1, \ldots, x_{n-1}, x_n)$ in x_n with coefficients in K^{n-1}. We now take as the set of words of K^n the set of elements of K' of the form $f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n)$ with $g(x_1, \ldots, x_n) \neq_n 0$, we define addition and multiplication as in K' and define equality by putting $f/g =_{K^n} f_1/g_1$, if and only if $fg_1 =_n f_1 g$. It is easily seen by induction that K^n is an explicit extension field of K which is isomorphic to $K(\alpha_1, \ldots, \alpha_n)$ by the isomorphism defined by $x_i \leftrightarrow \alpha_i\ (i = 1, \ldots, n)$. It is also clear that K^n is an explicit extension field of K^{n-1}. We now define the set of words of $\overline{K}$ to be the union of the sets of words of all the K^n, we define addition and multiplication of words in the same way as in K' and we define $W =_{\overline{K}} W_1$ to be the same as $W =_{K^n} W$, where n is the least integer such that W, W_1 are both words of K^n. $\overline{K}$ is clearly isomorphic to K_1 by the isomorphism defined by $x_i \leftrightarrow \alpha_i\ (i = 1, \ldots, n)$; to see that $\overline{K}$ is an explicit field we note that a word of K' can be effectively expressed in the form $f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n)$, where f, g are coprime; to decide whether it is a word of $\overline{K}$ we have then only to decide whether $g(x_1, \ldots, x_n) \neq_n 0$, and to decide when $f(x_1, \ldots, x_n)/g(x_1, \ldots, x_n) =_{\overline{K}} f_1(x_1, \ldots, x_n)/g_1(x_1, \ldots, x_n)$ we have only to decide whether $fg_1 - f_1 g =_n 0$, so the explicitness of $\overline{K}$ will be shown if we can show that there is an algorithm for deciding when a polynomial $f(x_1, \ldots, x_n)$ is $=_n 0$. However our definition of $=_n$ shows that this can be decided by a step-by-step procedure involving the $=_{n-1}$ of certain other polynomials and so on. (In fact the main decision required is as to whether a polynomial $f(x_n)$ from $K^{n-1}[x_n]$ is divisible by a polynomial $\phi_n(x_n)$ from $K^{n-1}[x_n]$; this is true if and only if all the coefficients of the remainder computed by the usual division algorithm are equal to zero in K^{n-1} and this is easily reduced to the question of the $=_{n-1}$ of certain polynomials in $x_1, \ldots, x_{n-1}$.) We see also that $\overline{K}$ is an explicit extension field of each of the K^n and that (by (i), (ii) and the fact that $x_i \leftrightarrow \alpha_i$ gives an isomorphism $\overline{K} \leftrightarrow K_1$) the set of elements $x_1, x_2, \ldots$ form a canonical basis for $\overline{K}$ over K.

6·1 defines canonical extensions in terms of a particular set of words. In the following theorem we see that these fields can in fact be characterized by the existence of an algorithm, and hence the definition is invariant under explicit isomorphism over K.

6·2. THEOREM. *$\overline{K}$ is a canonical extension field of the explicit field K, if and only if $\overline{K}$ is an explicit extension field of K, and*

(i) *there exists an algebraic dependence algorithm of $\overline{K}$ over K, and* (ii) *there exists an algorithm to find for any finite set T of words in $\overline{K}$ and any word w(**35**) in $\overline{K}$ which is algebraically dependent on T over K, an irreducible equation of w over $K(T)$.*

$K(T)$ here stands for the explicit extension field of K given by adjoining the elements of T to K. The proof of 6·2 is based on a series of lemmas:

6·21. LEMMA. *Let $\overline{K}$ be any explicit field. Then there exists an algorithm to find, for any explicit subfield K of $\overline{K}$ and any element w of $\overline{K}$, algebraic over K, an irreducible equation of w over K, if we are given*: (i) *an irreducible equation of an element v of $\overline{K}$ over K,* (ii) *an irreducible equation of w over $K(v)$.*

(**34**) It will be seen from the inductive definition that these coefficients do in fact belong to K^{n-1}, i.e. that the set of words of K^{n-1} includes P_{n-1}.

(**35**) From this point on we change our notation slightly and use lower case letters to denote words.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Proof. We work in the explicit polynomial extension of $\overline{K}$ in an indeterminate x. Assume first that w is separable over $K(v)$, and v separable over K. Let $F(x)$ be the given polynomial, irreducible in $K(v)\,[x]$, whose root is w. We can evaluate the symmetric functions in K of the coefficients of $F(x)$, using the fact that the symmetric functions of v in K are given by the coefficients of an irreducible equation of v in K. Hence we can, in a finite number of steps, find the norm $F_0(x)$ of $F(x)$ in $K[x]$. Then we can determine the highest power r of $F(x)$ dividing $F_0(x)$, $F_0(x)$ is then the rth power of the irreducible polynomial in $K[x]$ with root w. If the degree of $F_0(x)$ is $\bar{r}$ we have now only to test the polynomials of $K[x]$ of degree $\bar{r}/r$ as to whether they divide $F_0(x)$, and after a finite number of steps we are bound to find a factor $F_1(x)$ of $F_0(x)$ of degree $\bar{r}/r$. $F_1(x)$ will then be irreducible in $K[x]$ and have root w.

Next we drop the restriction of separability. We may now assume the characteristic of K to be a prime p. Let $g(x)$ be the given irreducible polynomial in $K[x]$ with root v, and $f(x)$ the given irreducible polynomial in $K(v)[x]$ with root w. Let $n = n_0 p^e$ be the degree, and n_0 the reduced degree of $g(x)$. n_0 and p^e can be effectively computed—we have only to find the highest power $p^s \leqslant n$, such that $g(x)$ is a polynomial in x^{p^s}. At the same time we can find the polynomial $G(x)$ such that $G(x^{p^e}) = g(x)$. $G(x)$ is a polynomial in $K[x]$ irreducible in $K[x]$ and having root $\bar{v} = v^{p^e}$. By repeated trials we then obtain in a finite number of steps the least possible integer l such that $(f(x))^l = \bar{f}(x)$ has coefficients in $K(\bar{v})$. In fact $l \leqslant p^e$. $\bar{f}(x)$ is irreducible in $K(\bar{v})$, for if $\bar{f}(x) = d(x)\,d_1(x)$, where $d(x), d_1(x) \in K(\bar{v})\,[x]$ and $d(x)$ is of degree >0, then $f(x) \mid d(x)$. Hence $d(x) = f(x)^q \,.\, d_2(x)$, where $(d_2(x), f(x)) = 1$. But $d_2(x) \mid \bar{f}(x)$. Hence $d_2(x)$ is a constant, $q = l$, and so $d_1(x)$ is also a constant.

Let now $m = m_0 p^h$ be the degree of $\bar{f}(x)$ and m_0 be its reduced degree. Again we can find the polynomial $F(x)$ such that $F(x^{p^h}) = \bar{f}(x)$. $F(x)$ is irreducible in $K(\bar{v})\,[x]$, and has the root $\overline{w} = w^{p^h}$. Also both $F(x)$ and $K(\bar{v})$ are separable. Hence, as was proved earlier, we can find the polynomial $F_1(x)$, irreducible in $K[x]$, having root $\overline{w}$. Finally $f_1(x) = F_1(x^{p^h})$ is the required polynomial in $K[x]$, irreducible in $K[x]$ and having root w.

6·22. Lemma. *Let $\overline{K}$ be an explicit field. There exists an algorithm to find, for any explicit subfield K of $\overline{K}$, and for any elements v, w of $\overline{K}$ algebraic over K an irreducible equation of w over K, and of v over $K(w)$, if we are given* (i) *an irreducible equation of v over K, and* (ii) *an irreducible equation of w over $K(v)$.*

Proof. Let the given equation of v over K have degree n, and the given equation of w over $K(v)$ have degree m. By 6·21 we can find an irreducible equation of w over K. Let its degree be M. As we have $[K(v,w):K(v)]\,[K(v):K] = [K(v,w):K(w)]\,[K(w):K]$, it follows that v must satisfy an irreducible equation of degree $N = m\,.\,n/M$ over $K(w)$. All we have to do then is to test the polynomials of degree N in $K(w)\,[x]$ until we find one with root v. This will be the required polynomial.

6·23. Lemma. *If the explicit extension field $\overline{K}$ of the explicit field K has a canonical basis over K, then it has an explicit transcendence basis over K. Hence by* 5·3 *there exists an algebraic dependence algorithm of $\overline{K}$ over K.*

Proof. Let $U = \{u_1, u_2, \ldots\}$ be the postulated canonical basis. If $\overline{K}$ has finite degree of transcendence over K the result is trivial so we may assume that $\overline{K}$ is of infinite degree of transcendence over K.

We define $f(1) = \min m$, such that u_m is transcendental over $K(U_{m-1})$;

$$f(n+1) = \min m > f(n)$$

such that u_m is transcendental over $K(U_{m-1})$. Then, by 6·1 (i), $f(n)$ is a recursive function, and $\{u_{f(1)}, u_{f(2)}, \ldots\}$ is an explicit transcendence basis of $\overline{K}$ over K.

Just as an explicit ring is determined by four recursive functions (see pp. 410) so a canonical basis is determined by three functions, namely: (i) a recursive function $f(n)$ which enumerates the basis $U = \{W(f(1)), W(f(2)), \ldots\}$, (ii) a recursive function $g(n)$ such that $g(n) = 0$ if and only if u_n is algebraic over $K(U_{n-1})$, (iii) a partial recursive function $h(n)$, defined for those n such that $g(n) = 0$, whose value denotes in some way(36) an irreducible equation of u_n over $K(u_{n-1})$. As on pp. 410 let us call such a set of three functions, or more precisely some positive integer defining them (in a similar manner to that used in pp. 410), a *table* of the canonical basis.

6·24. Lemma. *There is an algorithm by which, when supplied with (the table of) a canonical basis $U = \{u_1, u_2, \ldots\}$ of $\overline{K}$ over K, a non-negative integer n and an element w of $\overline{K}$ algebraic over $K(U_n)$, we obtain an irreducible equation of w over $K(U_n)$.*

Proof. Enumerate the rational functions $f(x_1, \ldots, x_n)/g(x_1, \ldots, x_m)$ of $x_1, x_2 \ldots$ with coefficients in K. For each of these test whether $g(u_1, \ldots, u_m) =_{\overline{K}} 0$; if it is not then test whether $f(u_1, \ldots, u_m)/g(u_1, \ldots, u_m) =_{\overline{K}} w$. Since there exists a rational function f/g with this property it follows by the basic lemma that we shall eventually find one. We then have, for some m, an irreducible (linear) equation $x - f(u_1, \ldots, u_m)/g(u_1, \ldots, u_m) = 0$ for w over $K(U_m)$. If $m \leqslant n$ this is also the desired irreducible equation for w over $K(U_n)$. If $m > n$ we apply the procedure of 6·21 $m-n$ times in order to get an irreducible equation for w over $K(U_n)$.

6·25. Lemma. *If $U = \{u_1, u_2, \ldots\}$ is a canonical basis of $\overline{K}$ over K and w is any word of $\overline{K}$ then $V = \{w, u_1, u_2, \ldots\}$ is a canonical basis of $\overline{K}$ over K and there is an algorithm for obtaining (a table of) V from (a table of) U and w.*

Proof. We have to show there exist algorithms for deciding for all n whether u_n is algebraic over $K(U_{n-1} \cup \{w\})$, and in case it is, for producing a corresponding irreducible equation. The existence of the first algorithm follows immediately from the fact (6·23) that $\overline{K}$ has an algebraic dependence algorithm over K. The existence of the second algorithm follows from 6·22, 6·24.

Proof of 6·2. Suppose $\overline{K}$ is a canonical extension of K. We have already shown (6·23) that $\overline{K}$ has an algebraic dependence algorithm over K so it only remains for us to show that there is an algorithm for providing, given a finite set T of n elements of $\overline{K}$ and an element w of $\overline{K}$ algebraic over $K(T)$, an irreducible equation of w over $K(T)$. Such an algorithm is the following: By successive applications of the procedure of 6·25 we can obtain, starting from a given canonical basis U_0 another basis U such that $U_n = T$. The procedure of 6·24 applied to U, n, w will now give the desired irreducible equation.

Conversely suppose that $\overline{K}$ is an explicit extension of K satisfying (i), (ii) of 6·2. Then any recursive enumeration $\{W(f(1)), W(f(2)), \ldots\}$ of the words of $\overline{K}$ is a canonical basis of $\overline{K}$ over K.

6·26. Corollary. *If $\overline{K}$ is a canonical extension of an explicit field K, and T a finite set of elements of $\overline{K}$, then $\overline{K}$ is a canonical and completely explicit extension of $K(T)$.*

(36) E.g. by being the number, in some standard enumeration of the finite sets of positive integers, of the set $\{n(W_1), n(W_2), \ldots, n(W_k)\}$ of numbers of the words $W_1, \ldots, W_k$ which are the coefficients in the irreducible equation $W_1 + W_2 x + \ldots + W_k x^{k-1} = 0$ for u_n over $K(u_{n-1})$.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Proof. If U is a canonical basis of $\overline{K}$ over K, with $U_n = T$, then $\{u_{n+1}, u_{n+2}, \ldots\}$ is a canonical basis of $\overline{K}$ over $K(T)$.

If w is an element of $\overline{K}$ algebraic over $K(T)$, then $w \in K(T)$ if and only if its irreducible equation over $K(T)$, which can be found by 6·2, is linear.

To show that the concept of canonical extension is in fact narrower than that of explicit extension with explicit transcendence basis, and also to show that isomorphic canonical extensions are not necessarily explicitly isomorphic we again construct a number of examples.

Let K be any explicit field. Let $\Phi = \Phi(K)$ be its standard transcendental extension by the independent transcendentals $x_1, x_2, \ldots$. Let $\Psi = \Psi(K)$ be the subfield of Φ generated by K and $x_n^2, x_{\lambda(n)}$, all n. The set of generators $x_n^2, x_{\lambda(n)}$, all n, of Ψ over K is recursively enumerable. Hence the set of words of Ψ is recursively enumerable. So, since all fundamental field operations in Ψ, i.e. addition, multiplication, and equating, are the same as in Φ it follows that Ψ is an explicit subfield of Φ. We then have

6·3. THEOREM. *Φ is an explicit extension field of the explicit field Ψ with an explicit transcendence basis over Ψ, but it is not a canonical extension of Ψ.*

Proof. Φ is algebraic over Ψ, hence it has an explicit transcendence basis over Ψ, that is, the null set. But there exists no algorithm to decide for arbitrarily given n whether $(\exists m)(n = \lambda(m))$, i.e. whether $x_n \in \Psi$. Hence by 6·26 Φ is not a canonical extension of Ψ.

We now give another example, not involving transcendental extensions. Let Q be an explicit representation of the rational field, let K_0 be the field $Q(\alpha_1, \alpha_2, \ldots)$, where $\alpha_n^2 = p_{\lambda(n)}$, and let K_1 be the field $Q(\beta_1, \beta_2, \ldots)$, where $\beta_n^2 = p_n$. By 6·12 there exists a canonical extension Λ of K with canonical basis $\{u_1, u_2, \ldots\}$ such that Λ is isomorphic to K_0 via the isomorphism defined by $u_i \leftrightarrow \alpha_i$ $(i = 1, 2, \ldots)$, and similarly there exists a canonical extension Π of K with canonical basis $v_1, v_2, \ldots$, such that Π is isomorphic to K_1 via the isomorphism defined by $v_i \leftrightarrow \beta_i$. The mapping $u_n \rightarrow v_{\lambda(n)}$ defines an explicit isomorphism of Λ into Π. The image of Λ under this isomorphism will be an explicit subfield $\overline{\Lambda}$ of Π. Just as in 6·3 we can show:

6·31. THEOREM. *Π is an explicit extension of $\overline{\Lambda}$ with an explicit transcendence basis over $\overline{\Lambda}$, but it is not a canonical extension of $\overline{\Lambda}$.*

Finally we prove:

6·32. THEOREM. *Let the explicit field K have a splitting algorithm. Then $\Phi(K)$ and $\Psi(K)$ are canonical extensions of K, isomorphic over K, but not explicitly isomorphic over K.*

Proof. Φ is clearly a canonical extension of K. But Ψ also has a canonical basis over K, namely $Y = \{y_1, y_2, \ldots\}$, where $y_{2n} = x_{\lambda(n)}$, $y_{2n-1} = x_n^2$. In fact y_{2n} satisfies an equation over $K(Y_{2n-1})$ if and only if $x_{\lambda(n)}^2$ occurs in the set Y_{2n-1}, i.e. if and only if $\lambda(n) \leqslant n$, which can clearly be tested; also $y_{2n-1} = x_n^2$ satisfies an equation over $K(Y_{2n-2})$, if and only if $n = \lambda(m)$ for some $m \leqslant n-1$ and again this can be tested. At the same time it is clear that when y_m is algebraic over $K(Y_{m-1})$ we can also find its irreducible equation.

$\Phi(K)$ is an extension of K by the independent transcendentals $x_1, x_2, \ldots$, and $\Psi(K)$ is an extension of K by the independent transcendentals $x_{\lambda(n)}, x_m^2$, where m runs through all integers not of the form $\lambda(n)$ for any n. Hence $\Phi(K)$, $\Psi(K)$ are clearly isomorphic over K. But they are not explicitly isomorphic. For by 4·5 $\Phi(K)$ has a splitting algorithm, while in $\Psi(K)$ there evidently does not even exist an algorithm for splitting the polynomials of the form $t^2 - x_n^2$.

6·32 provides an example for the non uniqueness of canonical extensions. However by imposing a purely algebraic condition we can enforce uniqueness in a strong sense:

6·4. DEFINITION. *An algebraic extension field $\overline{K}$ of a field K is said to be strongly automorphic if every isomorphism of a finite subfield $K(\alpha_1, \ldots, \alpha_n)$ of $\overline{K}$ into $\overline{K}$ over K can be extended to an automorphism of $\overline{K}$ over K.*

6·41. LEMMA. *$\overline{K}$ is strongly automorphic over K if and only if for every field K^* isomorphic to $\overline{K}$ over K every isomorphism of a finite subfield $K(\alpha_1, \ldots, \alpha_n)$ of $\overline{K}$ into K^* over K can be extended to an isomorphism of $\overline{K}$ onto K^*.*

Proof. Trivial.

6·42. LEMMA. *Every normal algebraic extension $\overline{K}$ of K is strongly automorphic over K.*

Proof. This is a well-known result of Galois Theory.

Trivially we have:

6·43. LEMMA. *Every algebraic extension $\overline{K}$ of K, such that the only isomorphism of any subfield K' of $\overline{K}$ into $\overline{K}$ is the identical one, is strongly automorphic.*

6·44. THEOREM. *Let $\overline{K}$ be a canonical extension of an explicit field K corresponding to an algebraic, strongly automorphic extension field of K. If $\overline{K}_1$ is an explicit extension of K, which is isomorphic to $\overline{K}$ over K, then $\overline{K}_1$ is explicitly isomorphic to $\overline{K}$ over K.*

Proof. We use the well known fact that if the algebraic extension $\overline{K}$ of K is isomorphic over K to a field K^*, then every isomorphism of $\overline{K}$ into K^* over K is an isomorphism onto K^*.

An isomorphism of $\overline{K}$ over K into $\overline{K}_1$ is uniquely determined by the images of the elements $u_1, u_2, \ldots$ where $U = \{u_1, u_2, \ldots\}$ is a canonical basis of $\overline{K}$ over K. It thus suffices to show that there exists an algorithm to find for all n, and for any mapping θ_n of the set U_n into $\overline{K}_1$ which defines an isomorphism of $K(U_n)$ into $\overline{K}_1$, a mapping θ_{n+1} of U_{n+1} into $\overline{K}_1$ which defines an isomorphism of $K(U_{n+1})$ into $\overline{K}_1$, such that $\theta_n(u_r) = \theta_{n+1}(u_r)$, for $r \leqslant n$.

Assume then that θ_n is given in the prescribed manner. Let $f(x)$ be the given irreducible polynomial in $K(U_n)[x]$ with root u_{n+1}. Let $\theta_n(f(x)) = f_1(x)$ be the polynomial in $\overline{K}_1[x]$ obtained by applying the isomorphism θ_n to the coefficients of $f(x)$. By 6·41 there exists a root of $f_1(x)$ in $\overline{K}_1$. If we now enumerate the elements of $\overline{K}_1$ in turn we must after a finite number of steps find one element, say w, such that $f_1(w) =_{\overline{K}_1} 0$. We put $\theta_{n+1}(u_r) = \theta_n(u_r)$ for $r \leqslant n$, $\theta_{n+1}(u_{n+1}) = w$. Then θ_{n+1} clearly defines an isomorphism of $K(U_{n+1})$ into $\overline{K}_1$.

6·45. COROLLARY. *If $\overline{K}$ is a normal, algebraic, canonical extension of an explicit representation K of a prime field, then every explicit field isomorphic to $\overline{K}$ is explicitly isomorphic to $\overline{K}$.*

Proof. By 6·44, 6·42 and the uniqueness of the explicit representation of a prime field.

To give an example of a non-normal field extension for which the conditions of 6·44 are satisfied we use 6·43. Let Q be an explicit representation of the rational field. Let $p_1, p_2, \ldots$ be the sequence of natural primes, and let $K_0 = Q$, $K_n = K_{n-1}(u_n)$ with $u_n^3 - p_n = 0$. Then the field $\overline{K}$ with canonical basis $\{u_1, u_2, \ldots\}$ as defined in 6·12 satisfies the conditions of 6·43.

We finally construct an example of an *algebraic* extension field of the rationals which has two non explicitly isomorphic explicit representations. We first need:

6·51. LEMMA. *There exists a recursive function $\mu(n)$ taking no value twice such that there is no algorithm for saying correctly of a given positive integer m either 'if there exists an n such that $m = \mu(n)$ then n is even' or 'if there exists an n such that $m = \mu(n)$ then n is odd'.*

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

Proof. Let G, H be two non intersecting recursively enumerable sets which are recursively inseparable, i.e. such that there exist no recursive sets G_1, H_1 satisfying $G \subseteq G_1$, $H \subseteq H_1$, $G_1 \cap H_1 = \phi$. (The existence of such sets is easily shown; see for example (Trachtenbrot 1953).) Let g, h be recursive functions enumerating G, H respectively without repetitions. Define for $n = 1, 2, \ldots, \mu(2n) = g(n), \mu(2n-1) = h(n)$. This function μ satisfies the conditions of the theorem since the existence of an algorithm of the type mentioned would imply the existence of two recursive sets E, O, consisting respectively of those m for which the answer is 'even', 'odd', such that $E \cap O = \phi$, $G \subseteq E$, $H \subseteq O$, contrary to the recursive inseparability of G, H.

Now let K be an explicit representation of the rational field. Let $\overline{K}$ be the canonical extension of K with the canonical basis $U = \{u_1, u_2, \ldots\}$, where $u_n^2 - p_n =_{\overline{K}} 0$. Such a field exists by 6·12 and is essentially unique by 6·44. Let $\overline{K}'$ be the canonical extension field of $\overline{K}$ with canonical basis $V = \{v_1, v_2, \ldots\}$, where $v_n^2 - u_{\mu(n)} =_{K'} 0$, and $\overline{K}''$ the canonical extension field of $\overline{K}$ with canonical basis $W = \{w_1, w_2, \ldots\}$ where $w_n^2 - (-1)^n u_{\mu(n)} =_{\overline{K}''} 0$, $\mu(n)$ being the function defined in 6·51. Both these fields exist by 6·12, and are essentially unique by 6·44. We then have

6·52. THEOREM. *$\overline{K}'$ and $\overline{K}''$ are isomorphic canonical algebraic extensions of K, but they are not explicitly isomorphic.*

Proof. $\overline{K}'$ and $\overline{K}''$ are clearly algebraic over K. By 6·11 they are canonical extensions of K.

The automorphism of $\overline{K}$ defined by $u_{\mu(n)} \to (-1)^n u_{\mu(n)}, u_m \to u_m$, if $m \neq \mu(n)$, can be extended to an isomorphism $v_n \to w_n$ of $\overline{K}'$ onto $\overline{K}''$.

Suppose now that there exists an explicit isomorphism θ of $\overline{K}'$ onto $\overline{K}''$. The only roots of $x^2 - p_m = 0$ in $\overline{K}'$ and $\overline{K}''$ are $\pm u_m$. Hence for all m, $\theta(u_m) = \pm u_m$. The only roots of $x^4 - p_{\mu(n)} = 0$ in $\overline{K}'$ are $\pm v_n$, and in $\overline{K}''$ are $\pm w_n$. Hence $\theta(v_n) = \pm w_n$, and $\theta(u_{\mu(n)}) = (-1)^n u_{\mu(n)}$. If m is any integer we can thus find $\theta(u_m) = \pm u_m$ and depending on the sign appearing we can say 'if $m = \mu(n)$ then n is even (odd)', which is impossible.

7. SPLITTING ALGORITHMS IN EXPLICIT EXTENSION FIELDS

7·1. THEOREM. *If $\overline{K}$ is a completely explicit extension of an explicit field K and $\overline{K}$ has a splitting algorithm then so has K.*

Proof. Let $K[x]$, $\overline{K}[x]$ denote explicit polynomial extensions in x of the fields K, $\overline{K}$. Let $f(x)$ be an element of $K[x]$. We can find its irreducible factors in $\overline{K}[x]$. Forming the various products of these factors we can decide for each polynomial of $\overline{K}[x]$ obtained in this way whether it lies in $K[x]$. As there are only a finite number of such products to be considered we get after a finite number of trials a non-constant irreducible factor of $f(x)$ in $K[x]$. Hence K has a splitting algorithm.

The converse of 7·1 is not true however, even if the condition that $\overline{K}$ be a completely explicit extension of K is strengthened to the condition that $\overline{K}$ be a canonical extension of K. In fact:

7·11. THEOREM. *If K is any explicit field then K has a canonical extension which has no splitting algorithm.*

Proof. Take the canonical extension $\Psi'(K)$. We have seen in 6·32 that this has no splitting algorithm.

The field $\Psi(K)$ is a transcendental extension of K. However for some(37) explicit field K with splitting algorithm it is also possible to find an algebraic extension of K without splitting algorithm. In fact

7·12. THEOREM. *There exists a canonical extension field of the rational field which is algebraic but has no splitting algorithm.*

Proof. The field Λ defined in §6 has this property since there is not even an algorithm for splitting polynomials of the form x^2-p_n.

Our next and last example is that of a simple, non-separable, algebraic, explicit extension field $\overline{K}$ of an explicit field K, such that K has a splitting algorithm but $\overline{K}$ has not.

Let Δ be an explicit representation of $GF(2)$. Let K_0 be the standard explicit extension field of Δ by the independent transcendentals $x_0, x_1, y_1, y_2, y_3 \ldots$ and let K be the canonical extension of K_0 with canonical basis $\{u_1, u_2 \ldots\}$, where $u_n^2-x_{\lambda(n)}-x_0y_n^2=_K 0$. Finally let $\overline{K} = K(v)$ where $v^2-x_0 =_{\overline{K}} 0$.

We first prove:

7·21. LEMMA. *$\overline{K}$ has no splitting algorithm.*

Proof. K_0 is a purely transcendental extension of Δ by the independent transcendentals $x_0, x_1, y_1, \ldots$. If we put $z_n = u_n - vy_n$, then $z_n^2 = x_{\lambda(n)}$ and $\overline{K}$ is a purely transcendental extension of Δ in the independent transcendentals $v, z_1, z_2, \ldots, y_1, y_2, \ldots$, and x_n for all n not of the form $\lambda(m)$ for any m. Thus t^2-x_n has a root in $\overline{K}$ if and only if $(\exists m)\,(\lambda(n) = m)$. But there is no algorithm for deciding this.

7·22. LEMMA. *Let K' be a subring of K which is the ring extension of Δ by elements*

$$x_0, x_{j_\mu}, y_{i_\nu}, u_{i_\nu} (\mu = 1, \ldots, m;\ \nu = 1, \ldots, n), \tag{7·221}$$

where, for all μ, ν,

$$j_\mu \neq \lambda(i_\nu); \tag{7·222}$$

then K' is a polynomial ring over Δ in the algebraically independent indeterminates (7·221).

Proof. Let $\overline{K}'$ be the subring of $\overline{K}$ which is the ring extension of Δ by the elements

$$v, x_{j_\mu}, y_{i_\nu}, x_{\lambda(i_\nu)}. \tag{7·223}$$

By the definition of $\overline{K}$, and by (7·222), $\overline{K}'$ is a polynomial ring over Δ in the $m+2n+1$ independent indeterminates (7·223). Observing that any algebraic relation over Δ between the indeterminates

$$v, x_{j_\mu}, y_{i_\nu}, u_{i_\nu}-vy_{i_\nu}, (\mu = 1, \ldots, m, \nu = 1, \ldots, n) \tag{7·224}$$

could, by squaring and substituting $(u_{i_\nu}-vy_{i_\nu})^2 = x_{\lambda(i_\nu)}$ give such a relation between the elements (7·223), it follows that the ring extension of Δ by the elements (7·224) is again a polynomial ring over Δ in the $m+2n+1$ independent indeterminates (7·224), or, equally well in the independent indeterminates

$$v, x_{j_\mu}, y_{i_\nu}, u_{i_\nu}. \tag{7·225}$$

Observing that $v^2 = x_0$, the lemma follows.

7·23. LEMMA. *Every polynomial in the elements $x_0, x_1, x_2, \ldots, y_1, y_2, \ldots, u_1, u_2, \ldots$ with coefficients in Δ can, in a finite number of steps, be expressed as a polynomial in a set of elements of the form* (7·221) *satisfying* (7·222).

(37) But clearly not all—e.g. not for an algebraically closed K.

Proof. Let P be a polynomial in $x_0, x_1, \ldots, x_q, y_1, \ldots, y_p, u_1, \ldots, u_r$. Evaluate $\lambda(i)$ for $i \leqslant \max(p, r)$ and substitute for the corresponding $x_{\lambda(i)}$ the expression $u_i^2 - x_0 y_i^2$.

7·24. Lemma. *A polynomial P in the set of indeterminates* (7·221) *satisfying* (7·222) *is the square of a polynomial in the ring extension of Δ by the x_n, all $n \geqslant 0$, the y_n, u_n all $n \geqslant 1$, if and only if the exponents in P are even.*

Proof. If all exponents in P are even then P is obviously a square.

Assume conversely that $P = Q^2$, where Q is a polynomial of the type indicated. It follows from 7·23(38) that Q is a polynomial in a set of indeterminates of the form (7·221) satisfying (7·222), possibly with m, n replaced by $m_1 \geqslant m, n_1 \geqslant n$. But in Q^2 all exponents are even, which is the required result.

7·25. Lemma. *There exists an algorithm to decide whether an element of K has a square root in K.*

Proof. Every element of K can in a finite number of steps be represented in the form P, or P/Q, and hence in the form P or PQ/Q^2, where P, Q are polynomials over Δ in the x_n, y_n, u_n. It thus suffices to prove 7·25 for an element of K represented by a polynomial P over Δ in the x_n, y_n, u_n.

Since K is the quotient field of the polynomial domain $\Delta[x_0, y_1, y_2, \ldots, u_1, u_2, \ldots, x_{i_1}, x_{i_2}, \ldots]$ (where $i_1, i_2, \ldots$ is the set of those positive integers not in the set $\{\lambda(1), \lambda(2), \ldots\}$), which is a u.f.d., it follows that P is the square of an element in K if and only if it is the square of an element of the ring extension of Δ by the elements x_n, y_n, u_n. Hence we have only to apply the algorithm 7·23 and, by 7·24, to inspect the exponents.

7·26. Lemma. *There exists a splitting algorithm for K.*

Proof. Let $g(t)$ be a polynomial in $K[t]$. Then $g(t)^2$ has coefficients in K_0. By 4·5 K_0 has a splitting algorithm. An irreducible factor of $g(t)^2$ in $K_0[t]$ is either irreducible in $K[t]$ or is the square of an irreducible polynomial in $K[t]$, and the latter is the case if and only if all exponents are even and all the coefficients have square roots in K. But by 7·25 we have an algorithm for deciding this. Hence the lemma.

We conclude

7·27. Theorem. *There exists an explicit field K and an explicit extension $\overline{K}$ of K corresponding to a simple algebraic extension of K, such that K has a splitting algorithm but $\overline{K}$ has not.*

The examples given show that even with strong restrictions the existence of a splitting algorithm in an extension field is not implied by the existence of such an algorithm in the base field. A characterization of a class of extension fields with splitting algorithms is given by

7·3. Theorem. *Let $\overline{K}$ be an explicit algebraic extension of an explicit field K with splitting algorithm. Then $\overline{K}$ has a splitting algorithm if and only if there exists an algorithm to find the roots in $\overline{K}$ of a polynomial with coefficients in K.*

Proof. Assume that there exists an algorithm to decide whether a polynomial in $K[x]$ has a root in $\overline{K}$. Enumerating the polynomials in $K[x]$, and testing them in turn we can in a finite number of steps find one, $F(x)$ say, such that $f(x) | F(x)$, $f(x)$ being a given polynomial in $\overline{K}[x]$. By hypothesis we can find all the roots of $F(x)$ in $\overline{K}$. The roots of $f(x)$ are among

(38) We use here not the existence of an algorithm to bring Q to this form, but merely the corollary that there exists an expression of this form for Q.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

these and can thus be found. Hence $\overline{K}$ has a root algorithm, and hence (4·43) a splitting algorithm.

The converse is trivial.

We shall call an extension field $\overline{K}$ of a field K separable in the wider sense if the maximal algebraic extension in $\overline{K}$ of every field K' between $\overline{K}$ and K is separable.

We shall use:

7·41. LEMMA. *Let K be an explicit field with splitting algorithm. Then there exists a general algorithm for splitting the polynomials of any given explicit polynomial domain $K'[x]$, whenever K' is a finite explicit extension field of K separable in the wider sense and of the form $K' = K(v'_1, \ldots, v'_m)$, where v'_n is given as a transcendental over K'_{n-1} or is given by an irreducible equation over K'_{n-1}, where $K'_0 = K$, $K'_n = K(v'_1, \ldots, v'_n)$ $(n = 1, \ldots, m)$.*

For the proof see van der Waerden (1930*a*, pp. 130, 131). Van der Waerden states only the existence of a splitting algorithm for a simple extension, separable in the wider sense. But his proof in fact establishes the existence of a general splitting algorithm for all simple extensions separable in the wider sense. The step from simple to finite extensions is trivial.

7·42. THEOREM. *If K is an explicit field and $\overline{K}$ an explicit extension field of K, separable in the wider sense, and if K has a splitting algorithm, and $\overline{K}$ an algebraic dependence algorithm over K, then $\overline{K}$ is a canonical extension of K.*

Proof. Let $U = \{u_1, u_2, \ldots\}$ be a recursively enumerable set of words of $\overline{K}$. Let U_0 be the empty set, $U_n = \{u_1, u_2, \ldots, u_n\}$ and K_n the explicit subfield of $\overline{K}$ generated by K and U_n. We shall prove that if u_n is algebraic over K_{n-1} then we can find an irreducible equation for u_n over K_{n-1}. The theorem then follows by taking for U the set of all words in $\overline{K}$.

Let then u_n be algebraic over K_{n-1}. We may assume that we have already found an irreducible equation for u_r over K_{r-1} for $1 \leqslant r < n$, whenever u_r is algebraic over K_{r-1}. By testing in turn all polynomials in $K_{n-1}[x]$ we can find in a finite number of steps one which has root u_n. The general algorithm of 7·41 applies to K_{n-1}. Hence by splitting the polynomial obtained into irreducible factors and testing these in turn we shall find one with root u_n.

7·43. COROLLARY. *Every explicit algebraic extension of a perfect explicit field with splitting algorithm, in particular of a prime field, is canonical, and hence if it is a normal extension it is unique to within explicit isomorphism over the base field.*

Proof. By 7·42 and 6·44.

7·5. THEOREM. *Let K be an explicit field with splitting algorithm, and let C be a recursively enumerable set of separable polynomials with coefficients in K. Then there exists a canonical extension $\overline{K}$ of K corresponding to the splitting field of the polynomials in C.*

Proof. Let $\{f_1(x), f_2(x), \ldots\}$ be a recursive enumeration of the set C of polynomials. We define $\overline{K}$ using the same sort of procedure as in 6·12. Let K' be the standard polynomial extension of K in the indeterminates $x_1, x_2, \ldots$. We first define inductively a sequence of explicit fields $K = K^0, K^1, K^2, \ldots$ as follows: the words of K^n are to consist of the words of K' which are polynomials in $x_1, \ldots, x_n$ only, addition and multiplication in K^n are defined to be the same as in K', and equality in K^n is defined by: $f(x_1, \ldots, x_n) =_{K^n} g(x_1, \ldots, x_n)$ if and only if the difference $f(x_1, \ldots, x_n) - g(x_1, \ldots, x_n)$ is, as a polynomial in x_n with coefficients in K^{n-1}, divisible by the polynomial $\phi_n(x_1, \ldots, x_{n-1}, x_n)$ in x_n with coefficients in K^{n-1}. Here $\phi_n(x_1, \ldots, x_{n-1}, x_n)$ is defined thus: If the polynomials $f_1(x), \ldots, f_n(x)$ all split into linear

factors in $K^{n-1}[x]$ then $\phi_n(x_1, \ldots, x_{n-1}, x_n) = x_n - x_1$. Otherwise let $f_r(x)$ be the first of $f_1(x), \ldots, f_n(x)$ which does not split completely into linear factors in $K^{n-1}[x]$ and let $\phi_n(x_1, \ldots, x_{n-1}, x_n)$ be the first(39) polynomial in $x_1, \ldots, x_n$ such that $\phi_n(x_1, \ldots, x_{n-1}, x)$ is a non-linear irreducible factor of $f_r(x)$ in $K^{n-1}[x]$. Finally we define the words of $\overline{K}$ to be the words of $\overline{K}'$, addition and multiplication in $\overline{K}$ to be the same as in K', and we define $W =_{\overline{K}} W_1$ to be the same as $W =_{K^n} W_1$ where n is the least integer such that W, W_1 are both words of K^n. Using the results of 7·41 it follows as in 6·12 that $\overline{K}$ is an explicit field—and it is obviously isomorphic to the splitting field of the set of polynomials in C.

7·6. THEOREM. *Let K be a perfect explicit field. Then K has a canonical extension corresponding to its algebraic closure if and only if it has a splitting algorithm.*

Proof. If K has a splitting algorithm then the required extension field exists by 7·5. Conversely if $\overline{K}$ is a canonical extension of K corresponding to its algebraic closure, then $\overline{K}$ is algebraically closed and so by 4·43 has a splitting algorithm. By 6·26 $\overline{K}$ is a completely explicit extension of K; hence by 7·1 K has a splitting algorithm.

REFERENCES

Church, A. 1936 *Amer. J. Math.* **58**, 345.
Hermann, G. 1926 *Math. Ann.* **95**, 736.
Kleene, S. C. 1936 *Math. Ann.* **112**, 727.
Kleene, S. C. 1938 *J. Symb. Log.* **3**, 150.
Kneser, M. 1953 *Math. Z.* **57**, 238.
Kronecker, L. 1882 *J. reine angew. Math.* **92**, 11.
Krull, W. 1953*a* *Math. Z.* **59**, 57.
Krull, W. 1953*b* *Math. Z.* **59**, 296.
Robinson, A. 1951 *The metamathematics of algebra*. Amsterdam: North-Holland Publishing Company.
Trachtenbrot, B. A. 1953 *C.R. Acad. Sci. U.R.S.S.* **88**, 953.
Turing, A. M. 1937 *Proc. Lond. Math. Soc.* (2), **42**, 230.
van der Waerden, B. L. 1930*a* *Moderne Algebra*, **1** (1st ed.). Berlin: Julius Springer.
van der Waerden, B. L. 1930*b* *Math. Ann.* **102**, 738.

(39) In the standard enumeration of the words of K'.

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES