PACIFIC JOURNAL OF MATHEMATICS
Vol. 74, No. 1, 1978

ALGEBRAIC NUMBERS, A CONSTRUCTIVE DEVELOPMENT

W. JULIAN, R. MINES AND F. RICHMAN

The theory of algebraic numbers is developed in the context of abstract fields with equality and inequality. Of classical interest is that any commutative local ring without nilpotent elements may be considered a field in this context. Procedures are given for deciding whether two complex algebraic numbers are equal or not, for factoring polynomials over algebraic number fields and for deciding whether a given algebraic number is in a given algebraic number field.

The purpose of this paper is to provide a constructive development of algebraic numbers, that is, complex roots of nonzero polynomials with rational coefficients. The constructive theory of complex numbers that we need is provided by Bishop [1]. For simplicity and power we use an axiomatic definition of a field with equality and inequality modeled on Bishop's complex numbers. By using conventional notation we make the subject appear similar to the classical development, while retaining the constructive finitistic interpretation.

A side effect of this axiomatic approach is that our fields can be interpreted classically as commutative local rings without nilpotent elements, with the maximal ideals consisting of those elements that are not different from zero. This gives some classical insight into the constructivist's notion of numbers that are not known to be zero or to be different from zero, and clarifies the problems that the constructivist faces in proving theorems about fields. Heyting [3] and others have given intuitionistic axioms for fields before but their axioms are more restrictive and their development emphasizes logical subtleties.

The real, complex, and p-adic numbers, as developed by Bishop, are examples of fields with elements x and y for which one can neither assert $x = y$ nor assert $x \neq y$. A field having the property that for each pair of elements x and y either $x = y$ or $x \neq y$ is called a *discrete field*. One might think that classical field theory would go through *in toto* for discrete fields, but this is not the case. For example, the characteristic of a discrete field need not be ∞ or a finite prime number, and it is not always possible to factor a polynomial into a product of irreducible polynomials.

Some peculiarly constructive questions about algebraic numbers which we shall consider are:

(1) Given two algebraic numbers, can one tell whether they are equal?

(2) Given an algebraic number field k and a polynomial $f \in k[X]$ can one factor f into irreducible factors?

(3) Given an algebraic number field k and an algebraic number α, can one tell whether $\alpha \in k$?

The complex numbers are not a discrete field, as was pointed out above. However, if α and β are complex numbers, in the sense of Bishop, and f and g are polynomial with rational coefficients such that $f(\alpha) = 0 = g(\beta)$, then Theorem 3.6 gives an effective procedure for determining whether $\alpha = \beta$ or $\alpha \neq \beta$. Question 1 has not been considered in this form before.

Theorem 3.6 will also be used in a subsequent paper, with the p-adic numbers replacing the complex numbers, to allow us to extend valuations from the field of rational numbers to algebraic number fields. Moreover there is a classical interpretation of Theorem 3.6, namely:

Let E be a commutative local ring without nonzero nilpotent elements, and k a subfield of E. If $\alpha, \beta \in E$ are algebraic over k, then either $\alpha = \beta$ or $\alpha - \beta$ is a unit.

Question 2 was answered affirmatively by Kronecker [4], in the setting of abstract extensions of the rationals rather than subfields of the complex numbers, no doubt because of the lack of a constructive theory of complex numbers at the time. Van der Waerden [6] extended Kronecker's argument to prove that if α is separable algebraic over k, and if one can factor polynomials over k, then one can factor polynomials over $k(\alpha)$. Kronecker used a splitting field in his argument, paying no attention to the difficulties involved in the construction of such fields. It is very likely impossible to construct splitting fields in the general situation; we do it here for countable fields (Corollary 3.9). This construction may be used to obtain another proof of van der Waerden's theorem for arbitrary discrete fields, which we shall present in another paper. The countable case is presented here (Theorem 4.2). It is interesting to note that we must prove the primitive element theorem (Theorem 4.1) in order to factor polynomials over algebraic number fields (Theorem 4.2), whereas classically one proves the primitive element theorem by factoring polynomials over algebraic number fields. The affirmative answer to question 3 follows from the affirmative answer to question 2.

For our counterexamples we shall employ Brouwer's notion of a fugitive sequence. A *fugitive sequence* is a sequence *of* 0's and 1's containing at most one 1, for which we have no idea whether a 1 ever appears, or in what positions it might appear if it does.

An example of such a sequence is:

$$a_n = \begin{cases} 0 & \text{if } a_m = 1 \text{ for some } m < n \text{ or if there is no sequence} \\ & \text{of 100 consecutive 6's in the first } n \text{ places of the} \\ & \text{decimal expansion of } \pi \\ 1 & \text{otherwise .} \end{cases}$$

1. **Fields.** Examining the real numbers as developed by Bishop we are led to equip every set with an equality relation and an inequality relation satisfying:

1. $x = x$
2. $x = y \Rightarrow y = x$
3. $x = y$ and $y = z \Rightarrow x = z$
4. $x \neq y \Rightarrow y \neq x$
5. $x = y$ and $y \neq z \Rightarrow x \neq z$
6. $x = y$ and $x \neq y$ is impossible.

Inequality is to be thought of as a positive notion of distinctness rather than the denial of equality. A set is *discrete* if for any pair x and y either $x = y$ or $x \neq y$. The real numbers constitute an example of a set that cannot be asserted to be discrete, for if $\{a_n\}$ is a fugitive sequence, then comparing the real number $\sum a_n/n$ with 0 would resolve the question of whether $a_n = 1$ for some n or not.

A *function* f from one set to another must respect both equality and inequality in the sense that:

1. $x = y \Rightarrow f(x) = f(y)$
2. $f(x) \neq f(y) \Rightarrow x \neq y$.

It is easy to check that the composition of functions is a function. For functions of two or more variables it is natural to introduce the Cartesian product $X \times Y$ of the sets X and Y. Equality and inequality are defined on $X \times Y$ by:

$$(x_1, y_1) = (x_2, y_2) \Longleftrightarrow x_1 = x_2 \text{ and } y_1 = y_2$$
$$(x_1, y_1) \neq (x_2, y_2) \Longleftrightarrow x_1 \neq x_2 \text{ or } y_1 \neq y_2 .$$

The "or" in the last equivalence is to be understood in the positive sense that we can determine which of the alternatives holds. These definitions make $X \times Y$ into the product of X and Y in the category of sets and functions as specified above.

The complex numbers, as developed by Bishop, motivates the following definition of an abstract field. A *field* is a set k, with distinguished elements 0 and 1, and two functions $+$ and $\cdot$ from $k \times k$ to k which satisfy:

1. $a + b = b + a$ and $ab = ba$

2. $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$
3. $a(b + c) = ab + ac$
4. $a + 0 = a$ and $a1 = a$
5. For each $a, a + b = 0$ for some b;
   For each $a \neq 0, ab = 1$ for some b.
6. For each integer $n > 0, a^n = 0$ implies $a = 0$
7. $0 \neq 1$.

Note that since $+$ is a function, if $a + b \neq 0 = 0 + 0$, then either $a \neq 0$ or $b \neq 0$. Note also that a commutative local ring with no nilpotent elements is a field if $a \neq b$ is interpreted to mean $a - b$ is a unit. Thus theorems about fields, in this sense, may be interpreted as theorems about such rings. A discrete field is a field in the classical sense.

Heyting has given axioms for fields which are similar to ours [3, pp. 51, 52]. Many of his axioms may be derived from the assumption (which he does not make) that addition and multiplication are binary functions that respect inequality. The only substantive difference between the two sets of axioms is Heyting's axiom that if $a \neq b$ is impossible, then $a = b$. This corresponds to Bishop's Lemma 5 for real numbers [1, p. 24]. Generally speaking, the fewer appeals one makes to this axiom, the cleaner and more straightforward one's arguments will be. Bishop repeatedly avoids invoking Lemma 5 in [1]. Our sixth axiom, which is a consequence of Heyting's axiom, must be stated explicitly when Heyting's axiom is dropped.

A *prime field* is a field with no proper subfields, that is, every element can be written as $(n \cdot 1)/(m \cdot 1)$ where n and m are integers and $m \cdot 1 \neq 0$. The ring of integers localized at 2 is an example of a prime field that is not discrete. Every field has a unique prime subfield.

If k is a field with a discrete prime subfield then the *characteristic* of k is defined to be

$$\inf \{n : n \cdot 1 = 0\}$$

where the infimum is taken in the one point compactification of the positive integers. Thus the field of rational numbers has characteristic ∞.

The characteristic of a discrete field need not be an integer or ∞. For example let $\{a_n\}$ be a fugitive sequence, and define $\{p_n\}$ by

$$p_n = \begin{cases} 0 \text{ if } a_n = 0 \\ \text{the } n\text{th prime of the form } 4m + 1 \text{ if } a_n = 1 . \end{cases}$$

Let P be the subgroup of the integers Z generated by $\{p_n\}$. Define $R = Z$ where $a = b$ if $a - b \in P$, and $a \neq b$ if $a - b \notin P$. Then R

under multiplication and addition is a discrete integral domain. Its quotient field k is a prime field. The characteristic of k is an element of the one point compactification of the positive integers, but we do not know if it is ∞ or not. Notice also that we can not tell if $x^2 + 1$ is irreducible over k.

For a discrete field k, the Euclidean algorithm will produce the GCD of any two nonzero elements of $k[x]$. However, it is not always possible to factor into irreducible polynomials, as in the above example. Hence classical arguments that rely on such factorizations must often be replaced by arguments that rely on the Euclidean algorithm instead.

Van der Waerden [7] observed that the polynomial $x^2 + 1$ cannot be factored into irreducible polynomials over a subfield of the complex numbers that might or might not contain i. The following is a slight variation on van der Waerden's field. Let $\{a_n\}$ be a fugitive sequence, and W be the subfield of the complex numbers generated by the rational numbers and the numbers ia_n. We shall often use this field for counterexamples. Note that W is a discrete subfield of the Gaussian numbers.

Following Hermann [2] we call a discrete field k *factorial* if every polynomial in $k[x]$ can be written as a product of irreducible polynomials. The following theorem is due to Kronecker [4].

THEOREM 1.1 (Kronecker). *The rational numbers Q form a factorial field.*

Proof. Let $f \in Q[x]$ be degree $n > 1$. We shall either exhibit a proper factor of f, or show that any factorization of f is trivial. We may assume that f has integer coefficients and, by Gauss's lemma, it suffices to consider factors with integer coefficients. Consider $f(0), f(1), \cdots, f(n)$. If $f(j) = 0$ then f admits the proper factor $x - j$. Otherwise, if g is a factor of f, then $g(j)$ divides $f(j)$ for each j, so there are only finitely many possibilities for $g(j)$. Since deg $g \leqq n$ we can use Lagrange's interpolation formula to exhibit a finite number of polynomials g among which are all factors of f with integer coefficients. We then test those that have integer coefficients to see if they indeed divide f.

2. Vector spaces. From a constructive point of view, a finitely generated vector space over a discrete field need not be finite dimensional—we may possess a finite set of generators yet not be able to construct a finite basis. For example consider the vector space $Q(i)$ over the van der Waerden field W. Then $\{1, i\}$ generates $Q(i)$ over W but the cardinality of a finite basis for $Q(i)$ over W would answer the question of whether $a_n = 1$ for some n or not.

The problem in the above example is that we cannot tell whether i is in the subspace generated by 1 or not. Following Brouwer we say that a subset A of a set S is *detachable* if the question "is x in A?" can be answered for any x in S. Subspaces of discrete vector spaces may fail to be detachable, even if they are finitely generated. The subspace generated by 1 in the above example is not detachable. However, summands of discrete vector spaces are detachable since to tell if x is in the summand, we simply check to see if the projection of x onto the summand is equal to x. Thus the following theorem implies that certain subspaces of finite dimensional spaces are detachable.

THEOREM 2.1. *Let V and W be finite dimensional vector spaces over a discrete field k. If $T: V \to W$ is a linear transformation, then* ker T *and* im T *are finite dimensional summands of V and W respectively.*

Proof. Let A be the matrix of T with respect to bases for V and W. By elementary row and column operations we can diagonalize A. But this amounts to constructing new bases for V and W for which the matrix of T is diagonal, in which case $\ker T$ and $\operatorname{im} T$ are clearly finite dimensional summands.

COROLLARY 2.2. *A finitely generated subspace of a finite dimensional vector space over a discrete field is a finite dimensional summand.*

Proof. Any such subspace is the image of a linear transformation between two finite dimensional spaces.

COROLLARY 2.3. *If $k \subseteqq E \subseteqq F$ are discrete fields such that E/k is finite dimensional and F/k is finite dimensional, then F/E is finite dimensional.*

Proof. Choose $v_1, \cdots, v_s$ in a basis for F/k such that $v_i \notin V_{i-1} = Ev_1 + \cdots + Ev_{i-1}$, and $V_s = F$. This can be done because V_{i-1} is detachable, being a finitely generated subspace of F/k and hence a summand of F/k. Then $v_1, \cdots, v_s$ is a basis for F/E.

COROLLARY 2.4. *Let V be a finite dimensional vector space over a discrete field k. Then the intersection of any two finitely generated subspaces of V is finitely generated.*

Proof. Let A and B be finitely generated subspaces of V. Let

C be a complementary summand of B in V. Then projection on C, restricted to A, is a linear transformation from A to C whose kernel is $A \cap B$. Hence $A \cap B$ is finitely generated.

3. Algebraic extensions. Let E be a field and R a subring of E. An element $\alpha \in E$ is said to be *integral over* R if α satisfies a monic polynomial in $R[x]$. We have the usual characterization [8; p. 254].

THEOREM 3.1. *Let E be a field, R a subring of E, and $\alpha \in E$. The the following are equivalent:*

(1) *α is integral over R.*

(2) *$R[\alpha]$ is finitely generated as an R-module.*

(3) *E has a finitely generated faithful R-submodule M such that $\alpha M \subseteqq M$.*

Proof. The only problem is $(3) \Rightarrow (1)$. Let $m_1, \cdots, m_s$ be a set of generators of M. Then $\alpha m_i = \sum r_{ij} m_j$ where $r_{ij} \in R$. Let $\Delta = \det(r_{ij} - \alpha\delta_{ij})$. By Cramer's rule have we $\Delta m_j = 0$ for $1 \leqq j \leqq s$. Since M is faithful, this implies that $\Delta = 0$. This gives the desired monic polynomial.

COROLLARY 3.2. *The elements in E that are integral over R form a subring.*

Proof. Suppose α and β are integral over R. Then $R[\alpha]$ is a finitely generated R-module, and $R[\alpha, \beta]$ is a finitely generated $R[\alpha]$-module. Hence $R[\alpha, \beta]$ is a (faithful) finitely generated R-module, so every element of $R[\alpha, \beta]$ is integral over R.

If R is a field and α is integral over R, then we say that α is *algebraic over* R. If in addition R is discrete, then $R[\alpha]$ is a field, for if $0 \neq \beta \in R[\alpha]$, then we can find a monic polynomial f in $R[x]$ such that $f(\beta) = 0$ and $f(0) \neq 0$. Then $f(0) = f(0) - f(\beta) = \lambda\beta$ for some λ in $R[\beta]$, so $\lambda/f(0) = \beta^{-1} \in R[\beta]$.

If R is not discrete, then $R[\alpha]$ need not be a field. To see this let E be the 2-adic integers with "$a \neq b$" defined as "$a - b$ is a unit." Let $R \subseteqq E$ be the rational 2-adic integers. Then R and E are fields, but R is not discrete. Let α be the root of $x^2 + x + 2$ in E that is a unit. Then α^{-1} is a root of $2x^2 + x + 1$ so α is not integral over R, and hence α^{-1} is not in $R[\alpha]$.

LEMMA 3.3. *Let E be a field, k a discrete subfield, and $\alpha \in E$. If f, $g \in k[x]$ and $(f, g) = 1$ and $f(\alpha)g(\alpha) = 0$, then $f(\alpha) = 0$ or $g(\alpha) = 0$.*

Proof. By the Euclidean algorithm $s(\alpha)f(\alpha) + t(\alpha)g(\alpha) = 1 \neq 0$ so $s(\alpha)f(\alpha) \neq 0$ or $t(\alpha)g(\alpha) \neq 0$. Hence $g(\alpha) = 0$ or $f(\alpha) = 0$, respectively.

LEMMA 3.4. *Let k be discrete field and S a finite set of monic polynomials in $k[x]$. Then we can construct a finite set P of monic polynomials in $k[x]$ such that every polynomials in S is a product of polynomials in P, and if p_i and p_j are in P then either $p_i = p_j$ or $(p_i, p_j) = 1$.*

Proof. Simply choose P from among the finite set of monic polynomials obtained by closing the set S under the taking of GCD's.

LEMMA 3.5. *Let k be a discrete field and g a nonconstant polynomial in $k[x]$. Then we can factor g into relatively prime polynomials of the form $f^m(x^q)$ where m is a positive integer, q is either 1 or a power of the finite characteristic of k, and $f \in k[x]$ is relatively prime to its derivative f'.*

Proof. We may assume that g is monic. If $\deg g = 1$ the conclusion is clear. If $\deg g > 1$ and $g' \neq 0$, compute (g, g'). If $(g, g') = 1$ we are done. Otherwise (g, g') is a proper factor of g, so by Lemma 3.4 we can write g as a product of polynomials h_i of degrees smaller than $\deg g$ such that, for all i and j, either $h_i = h_j$ or $(h_i, h_j) = 1$. Since $\deg h_i < \deg g$ we can write h_i in the desired form, by induction, and this expresses g as desired.

If $g' = 0$, then char $k = p < \infty$ and $g(x) = h(x^p)$ for some h in $k[x]$. By induction h can be written as desired; hence so can g.

THEOREM 3.6. *Let E be a field and k a discrete subfield of E. If $\alpha, \beta \in E$ are algebraic over k, then $\alpha = \beta$ or $\alpha \neq \beta$.*

Proof. Choosing a monic polynomial which is satisfied by α and one which is satisfied by β and letting g be their product, we obtain a monic polynomial $g \in k[x]$ such that $g(\alpha) = g(\beta) = 0$. Applying Lemma 3.5, we may write

$$g(x) = f_1^{m_1}(x^{q_1}) \cdots f_r^{m_r}(x^{q_r})$$

where

$$(f_j^{m_j}(x^{q_j}), f_i^{m_i}(x^{q_i})) = 1\ , \quad \text{if} \quad i \neq j \quad \text{and}$$
$$(f_i, f_i') = 1 \quad \text{for} \quad i = 1, \cdots, r$$

applying Lemma 3.3 gives integers i and j so that

$$f_i^{m_i}(\alpha^{q_i}) = 0 = f_j^{m_j}(\beta^{q_j}) .$$

If $i \neq j$, then there exist $s(x), t(x) \in k[x]$ so that

$$s(x)f_i^{m_i}(x^{q_i}) + t(x)f_j^{m_j}(x^{q_j}) = 1 .$$

Replacing α for x in the above we see that $f_j^{m_j}(\alpha^{q_j}) \neq 0$, so $a \neq \beta$. If $i = j$, then we have $f_i(\alpha^{q_i})^{m_i} = 0 = (f_i(\beta^{q_i}))^{m_i}$. By part 6 of the definition of fields we have $f_i(\alpha^{q_i}) = 0 = f_i(\beta^{q_i})$. Noting $q = p^n$ for some prime p, dropping the subscript i, and writing $F(x) = f(x^q)$ we have: $F(\alpha) = 0 = F(\beta)$ and $(f, f') = 1$. Using Taylor series,

$$f(y) = (y - \beta^q)f'(\beta^q) + (y - \beta^q)^2K(y)$$
$$0 = (\alpha^q - \beta^q)[f'(\beta^q) + (\alpha^q - \beta^q)K(\alpha^q)] .$$

Since $(f, f') = 1$ and $f(\beta^q) = F(\beta) = 0$, we have

$$0 \neq f'(\beta^q) = [f'(\beta^q) + (\alpha^q - \beta^q)K(\alpha^q)] + [-(\alpha^q - \beta^q)K(\alpha^q)] .$$

So either

$$(\alpha^q - \beta^q)K(\alpha^q) \neq 0 , \quad \text{or} \quad f'(\beta^q) + (\alpha^q - \beta^q)K(\alpha^q) \neq 0 .$$

Thus either $0 \neq (\alpha^q - \beta^q) = (\alpha - \beta)^q$ giving $a \neq \beta$, or $\alpha^q - \beta^q = 0$ so $(\alpha - \beta)^q = 0$, and by part 6 of the definition of a a field, $\alpha - \beta = 0$ so $\alpha = \beta$.

THEOREM 3.7. *Let E be a field, k a discrete subfield, and $\alpha \in E$ algebraic over k. The $k[\alpha]$ is a finite dimensional vector space over k if and only if α satisfies an irreducible polynomial over k.*

Proof. If α satisfies an irreducible polynomial of degree n over k, then $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ form a basis for $k[\alpha]$ over k. If $k[\alpha]$ has a basis $v_1, \cdots, v_n$ over k, then write

$$\alpha v_i = \sum a_{ij}v_j$$

and α satisfies the polynomial:

$$f(x) = \det (a_{ij} - \delta_{ij}x)$$

which has degree n. If f has a proper factor then, by Lemmas 3.3 and 3.4, there is a nonzero polynomial of degree less than n satisfied by α. Then $k[\alpha]$ would be generated by $1, \alpha, \cdots, \alpha^r$ where $r < n - 1$, which contradicts the existence of a basis $v_1, \cdots, v_n$.

In classical field theory the problem of adjoining a root of a polynomial is easily solved by taking the prime ideal P in $k[x]$ generated by an irreducible factor of the given polynomial, and then forming the field $k[x]/P$. From the constructive viewpoint, this is not always possible unless k is factorial. If k is countable, we can overcome the fact that factorization of polynomials is not always possible, by using the Euclidean algorithm to construct a prime ideal containing the given polynomial.

THEOREM 3.8. *Let k be a countable discrete field and q a nonconstant polynomial in $k[x]$. Then there is a countable discrete field E containing k, and $\alpha \in E$, such that $q(\alpha) = 0$.*

Proof. We construct a sequence of nonconstant polynomials $p_j \in k[x]$ such that:
(1) $p_0 = q$
(2) p_{j+1} divides p_j
(3) $f \in k[x] \Rightarrow$ for some j either p_{j+1} divides f or $(p_{j+1}, f) = 1$.

Let $f_1, f_2, \cdots$ be an enumeration of $k[x]$. Let $p_0 = q$. To construct p_{j+1} consider $(p_j, f_j) = d$. If $d = 1$ let $p_{j+1} = p_j$, otherwise let $p_{j+1} = d$. Then p_{j+1} divides p_j and either $(p_{j+1}, f_j) = 1$ or p_{j+1} divides f_j. Let $E = k[x]$ with equality defined by $f = g$ if p_j divides $f - g$ for some j, and inequality defined by $f \neq g$ if $(p_j, f - g) = 1$ for some j. It is easy to see that E is a discrete extension field of k and that x is a root of q in E.

COROLLARY 3.9. *Let $f(x)$ be a monic polynomial of degree $n \geqq 1$ over a countable discrete field k. Then there exists a countable discrete field E containing k and elements $\alpha_1, \cdots, \alpha_n \in E$ such that*

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) .$$

Proof. Repeated application of Theorem 3.8.

As usual the field generated by $\alpha_1, \cdots, \alpha_n$ over k is called a *splitting field* for f. Classically, the splitting field is unique. However, this is not the case from the constructive viewpoint. Consider the van der Waerden field W. Both the Gaussian numbers $W(i)$ and the field $W(\alpha)$ constructed by Theorem 3.8 for the polynomial $x^2 + 1$ over the field W, are splitting fields for $x^2 + 1$ over W. If $i \in W$, then depending upon the ordering of the polynomials of $W[x]$ we have α equal to i or $-i$. As there is no prior way of deciding which of these occurs, we are unable to decide in advance where to send α by a W-isomorphism of $W(\alpha)$ to $W(i)$. Thus we can not construct an isomorphism between $W(\alpha)$ and $W(i)$ over W.

We can construct an algebraic closure of a countable field k by counting the polynomials in $k(x)$, building a tower of splitting fields, and then taking the union of this tower.

4. Separability.

If k is a discrete field, and $f \in k[x]$, then f is *separable* if we can write f as a product of polynomials g such that $(g, g') = 1$. An element α in an extension field of k is *separable over* k if it satisfies a separable polynomial in $k[x]$. By Lemmas 3.3 and 3.4 the element α satisfies a polynomial h such that $(h, h') = 1$, since the property $(g, g') = 1$ is inherited by factors of g. The following parallels Pollard [5; Theorem 4.7].

THEOREM 4.1. *Let E be a field and k a discrete subfield of E. Suppose $\alpha, \beta \in E$ are algebraic over k and α is separable. Then there is a θ in E such that $k[\theta] = k[\alpha, \beta]$.*

Proof. Let f and g be nonzero elements of $k[x]$ such that $f(\alpha) = g(\beta) = 0$ and $(f, f') = 1$. By replacing k by the subfield generated by the coefficients of f and g we can assume that k is countable. By systematically looking at polynomials in the various coefficients of f and g over the prime field, we can, for each integer N, decide whether $|k| \leqq N$ or $|k| > N$. Moreover we may then take E to be $k[\alpha, \beta]$ which is countable and, by Theorem 3.6, discrete. Hence, by Corollary 3.9, we can construct a countable discrete field $F \supseteqq E$ such that the polynomials f and g factor completely over F.

Let $\alpha_1, \cdots, \alpha_n$ and $\beta_1, \cdots, \beta_m$ be the distinct roots of f and g in F, with $\alpha_1 = \alpha$ and $\beta_1 = \beta$. If $|k| \leqq m(n-1)$, then E is finite and we can pick θ to be a generator of the multiplicative group of E. If $|k| > m(n-1)$, then we can choose $c \in k$ such that

$$c(\alpha_i - \alpha_1) \neq \beta_1 - \beta_j$$

for $1 \leqq j \leqq m$ and $2 \leqq i \leqq n$. We show that $\theta = c\alpha + \beta$ works.

Now $g(\theta - c\alpha) = g(\beta) = 0$ so α satisfies both $f(x)$ and $g(\theta - cx)$. Moreover, by the choice of c, these polynomials have only one common root in F. If $h(x) = (f(x), g(\theta - cx)) = s(x)f(x) + t(x)g(\theta - cx)$ then h has coefficients in $k[\theta]$, and $h(\alpha) = 0$. Since h is a factor of f it is a product of distinct linear factors over F. Since h is also a factor of $g(\theta - cx)$, which has but one root in common with f, we must have $h(x) = x - \alpha$. But h has coefficients in $k[\theta]$. Hence $\alpha \in k[\theta]$, so $\beta = \theta - c\alpha \in k[\theta]$ and we are done.

THEOREM 4.2. *Let E be a field and k a countable discrete factorial subfield. Let $\alpha \in E$ be separable algebraic over k. Then $k[\alpha]$ is factorial.*

Proof. Let $g(x)$ be a polynomial with coefficients in $k[\alpha]$, and $E' \supseteqq k[\alpha]$ be a countable discrete field containing a root β of $g(x)$.

Then $k[\alpha, \beta] = k[\theta]$ for some θ, by Theorem 4.1. As k is factorial, $[k[\theta]: k]$ and $[k[\alpha]: k]$ are finite by Theorem 3.7. So $[k[\theta]: k[\alpha]]$ is finite by Corollary 2.3. Thus β satisfies an irreducible polynomial over $k[\alpha]$, by Theorem 3.7, which must be a factor of $g(x)$. By induction on the degree of g we are done.

THEOREM 4.3. *Let k be an algebraic number field, that is, finitely generated extension of the rationals contained in the complex numbers. Then*

(1) *k is discrete.*
(2) *$k = Q(\alpha)$ for some complex number α.*
(3) *k is factorial.*
(4) *k is a finite dimensional vector space over Q.*
(5) *k is a detachable subfield of the algebraic numbers.*

Proof. Since the rational numbers are a discrete subfield of the complex numbers, the field k is discrete by Theorem 3.6. Every element of k is separable over Q by Lemma 3.5. By repeated application of Theorem 4.1, we can find α in k so that $k = Q(\alpha)$. The rational numbers are a factorial field by Theorem 1.1. Hence k is factorial by Theorem 4.2. By Lemma 3.3 an element algebraic over a factorial field satisfies an irreducible polynomial over that field. Hence k is a finite dimensional vector space over Q by Theorem 3.7. Moreover, if β is an algebraic number then $\beta \in k$ if and only if the irreducible polynomial of β over k is linear, and so k is detachable.

REFERENCES

1. E. Bishop, *Foundations of Constructive Analysis*, McGraw-Hill, 1967.

2. G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann., **95** (1926), 736–788.

3. A. Heyting, *Intuitionism An Introduction*, North-Holland Publishing Company, 1971.

4. L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraishen Grossen* (section 4), Journal für die reine und angewandte Mathematik, **92** (1882), 1–122.

5. H. Pollard, *The theory of algebraic numbers*, Carus Mathematical Monograph 9, MAA, 1950.

6. B. L. van der Waerden, *Modern Algebra* (section 42), Ungar 1953 (second edition).

7. ———, *Eine Bemerkung über die Unzerlegbarkeit von Polynomen*, Math. Ann., **102** (1930), 738–739.

8. O. Zariski, and P. Samuel, *Commutative Algebra*, Vol I, Van Nostrand, 1958.

Received March 17, 1977.

NEW MEXICO STATE UNIVERSITY
LAS CRUCES, NM 88003