ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 12, Number 1, Winter 1982

SEPARABILITY AND FACTORING POLYNOMIALS

RAY MINES AND FRED RICHMAN

ABSTRACT. The basic facts about separable extensions of discrete fields and factoring polynomials are developed in the constructive spirit of Errett Bishop. The ability to factor polynomials is shown to be preserved under finite separable extensions, while the ability to factor separable polynomials is preserved under arbitrary finite extensions. A method is given for converting any procedure that finds roots into one which finds arbitrary factors. Thus the rational root test gives rise to an effective procedure for factoring polynomials over the rational numbers, providing a new proof of a well known theorem of Kronecker.

0. Introduction. This paper contains a constructive development of the basic facts about separability and factoring of polynomials over discrete fields. The point of view is that of [1] and we build on the results of that paper. We summarize the main results in [1] upon which we shall draw.

Every set comes equipped with an equality relation $=$ and an inequality relation $\neq$ with the usual properties. A set is *discrete* if for every pair x and y, either $x = y$ or $x \neq y$. A *field* is a set with distinguished elements 0 and 1, and binary functions $+$ and $\times$ satisfying the usual axioms of a field. In addition we require that $0 \neq 1$ and the peculiarly constructive axioms:

1) For each positive integer n, if $a^n = 0$, then $a = 0$;
2) If $a + b \neq 0$, then $a \neq 0$ or $b \neq 0$; and
3) If $ab \neq 0$, then $a \neq 0$.

The *characteristic* of a discrete field is the infimum, in the one point compactification of the positive integers, of the set $\{n: n \times 1 = 0\}$. The field of rational numbers has characteristic infinity. A *prime field* is a field in which every element is equal to an element of the form $(n \times 1)/(m \times 1)$ where n and m are integers and $m \times 1 \neq 0$. Every discrete field contains a unique prime field. A discrete field k is *factorial* if every polynomial with coefficients in k is equal to a product of irreducible polynomials. We will have occasion to use the following characterization of integral elements, whose statement is similar, and proof is identical, to that of [1; Theorem 3.1].

Received by the editors on March 11, 1980, and in revised form on September 2, 1980.

THEOREM A. *Let E be a field, R a subring of E, and α an element of E. Then the following are equivalent.*

1) *α satisfies a monic polynomial of degree n with coefficients in R.*

2) *$R[\alpha]$ is generated by n elements as an R-module.*

3) *E has a faithful R-submodule M, generated by n elements, such that $\alpha M \subset M$.*

We also will use the following remark concerning inverses in an algebraic extension, which appears after [**1**; Corollary 3.2].

REMARK B. *Let α be integral over a discrete field R. Then $R[\alpha]$ is a field.*

PROOF. If $0 \neq \theta \in R[\alpha]$, then there is a monic polynomial f in $R[x]$ such that $f(\theta) = 0$ and $f(0) \neq 0$. So $f(0) = f(0) - f(\theta) = \lambda\theta$ for some λ in $R[\theta]$, whence $\lambda/f(0) = \theta^{-1} \in R[\theta]$.

In the first two sections we develop the theory of separable extensions and perfect fields. The construction of the perfect closure differs from the standard one. The heart of the paper is section three. Here we define a *separably factorial* field as one for which each separable polynomial is a product of irreducible polynomials. We prove that a simple extension of a separably factorial field is separably factorial, and that a separable extension of a factorial field is factorial. This theorem has a history dating back to Kronecker. In [**2**] Kronecker proved that algebraic number fields are factorial. Van der Waerden showed that separable extensions of factorial fields are factorial and included the result in [**5**]. His proof relies on the norm of algebraic elements and there are constructive problems in defining the norm. Seidenberg overcame these problems by defining a norm map by means of a generic splitting field [**4**]. Our method is to show that a field is (separably) factorial if and only if for each (separable) polynomial f either there is an element α with $f(\alpha) = 0$ or else $f(\alpha) \neq 0$ for all α. Thus the rational root test shows that the rational number field is factorial. This allows us to avoid the norm entirely.

1. Separability. If k is a discrete field, and $f \in k[x]$, then f is a *separable polynomial* if f can be written as a product of polynomials g with $(g, g') = 1$. An element in an extension field of k is *separable over k* if it satisfies a separable polynomial in $k[x]$. We shall show that if E is a field containing the discrete field k, then the elements of E that are separable over k form a subfield.

THEOREM 1.1. *Let k be a discrete field of finite characteristic p, let $a \in k$, and let $q = p^n$. If $x^q - a$ is reducible in $k[x]$, then $a = b^p$ for some b in k.*

PROOF. Let $x^q - a = f(x)g(x)$. By passing to the field generated by the coefficients of f and g we may assume that k is countable. By [**1**; Theorem

3.8] there is a discrete extension field E of k, and an element $\alpha \in E$, such that $\alpha^q = a$. Then $x^q - a = (x - \alpha)^q$ does not admit relatively prime factors in $k[x]$, so by [**1**; Lemma 3.5] we can write $x^q - a = h(x)^m$ for some h in $k[x]$ and $m > 1$. Note that m is a power of p since m divides p^n. As $h(0)^m = -a$, we can set $b = -h(0)^{m/p}$.

The following is an improvement of (**1**; Theorem 4.1] in that the element α is not required to be separable over k.

COROLLARY 1.2. *Let E be a field and k a discrete subfield of E. Suppose $\rho \in E$ is algebraic over k, and $\alpha \in E$ is separable over $k[\rho]$. Then $k[\alpha, \rho] = k[\theta]$ for some θ in E.*

PROOF. By [**1**; Theorem 3.1] the element α is algebraic over k. By [**1**; Lemma 3.3] and [**1**; Lemma 3.5] we can find a separable polynomial g in $k[x]$ such that $g(\alpha^q) = 0$ where either $q = 1$ or k has finite characteristic p and q is a power of p. Then $k[\alpha^q, \rho] = k[\theta]$ for some $\theta \in E$ by [**1**; Theorem 4.1]. If $q = 1$ we are done, so we may assume that k has finite characteristic p and q is a positive power of p. The GCD of $x^q - \alpha^q$ with the separable polynomial over $k[\rho]$ satisfied by α is a proper factor of $x^q - \alpha^q$ over $k[\theta]$. Hence by Theorem 1.1 we have $\alpha^{q/p} \in k[\theta]$ so $x^{q/p} - \alpha^{q/p}$ is a polynomial with coefficients in $k[\theta]$ satisfied by α. Continuing in this manner we get $\alpha \in k[\theta]$ so $k[\alpha, \rho] = k[\theta]$.

COROLLARY 1.3. *If α and ρ are algebraic over a factorial field k, and either α is separable over $k[\rho]$ or ρ is separable over $k[\alpha]$, then ρ satisfies an irreducible polynomial over $k[\alpha]$.*

PROOF. We have $k \subset k[\alpha] \subset k[\alpha, \rho] = k[\theta]$ by Corollary 1.2. As k is factorial, $k[\alpha]$ and $k[\theta]$ are finite dimensional over k by [**1**; Theorem 3.7]. Hence $k[\alpha, \rho]$ is finite dimensional over $k[\alpha]$ by [**1**; Corollary 2.3]. By [**1**; Theorem 3.7] we can find an irreducible polynomial over $k[\alpha]$ that is satisfied by ρ.

The next theorem provides a method for checking the separability of an element in an extension field. The fact that we may be unable to find an irreducible polynomial for an element prevents us from proving that a finitely generated algebraic extension E/k is separable if and only if $E = k(E^p)$, [**6**; Theorem 8, page 69]. The theorem is true if the extension E/k is finite dimensional.

THEOREM 1.4. *Let E be a field of finite characteristic p. Let k be a discrete subfield of E and $\alpha \in E$. Then α is separable over k if and only if $\alpha \in k(\alpha^p)$.*

PROOF. If $\alpha \in k(\alpha^p)$, then α is algebraic over k, so $\alpha \in k[\alpha^p] = k(\alpha^p)$ by Remark B. This gives a polynomial $f \in k[x]$ such that $f' = 1$ and $f(\alpha) = 0$. Hence α is separable over k. Conversely, suppose $f \in k[x]$ is

a separable polynomial such that $f(\alpha) = 0$. Let $g(x)$ be the GCD of $f(x)$ and $x^p - \alpha^p$ in $k(\alpha^p)$. Since f is separable $g(x) \neq x^p - \alpha^p$, and since $f(\alpha) = 0$ we have $g(x) \neq 1$. Thus g is a proper factor of $x^p - \alpha^p$ so $\alpha \in k(\alpha^p)$ by Theorem 1.1.

THEOREM 1.5. *Let θ be separable over a discrete field k. Then every element of $k[\theta]$ is separable over k.*

PROOF. If $\alpha \in k[\theta]$, then α is algebraic over k, so by [**1**; Lemma 3.5] either α satisfies a separable polynomial over k or k has finite characteristic p. So we may assume the latter, and by Theorem 1.4 it suffices to show that $\alpha \in K = k[\alpha^p]$. Since θ is separable over K we can find a separable polynomial $f \in k[x]$ of degree $n > 0$ such that $f(\theta) = 0$. We proceed by induction on n. If $n = 1$, then $\theta \in K$ so $\alpha \in K$ and we are done. If $n > 1$ let $\alpha = g(\theta)$ where $g \in k[x]$ and $\deg g < n$. Then $\alpha^p = h(\theta^p)$ where $h \in K^p[x]$ and $\deg h = \deg g$. If $\deg h = \deg g = 0$, then $\alpha \in K$. If $\deg h > 0$, then $h(x) - \alpha^p$ is a polynomial in $K[x]$ of degree less than n satisfied by θ^p. Hence $K(\theta) = K(\theta^p)$ can be generated by fewer than n elements as a vector space over K, so we can obtain a polynomial in $K[x]$ of degree less than n that is satisfied by θ. Taking the GCD with f we can make this polynomial separable, and by induction we are done.

THEOREM 1.6. *Let E be a field and k a discrete subfield. Then the elements of E that are separable over k form a (discrete) subfield.*

PROOF. Suppose α and ρ are separable over k. Then by [**1**; Theorem 4.1] we can find θ in E such that $k[\alpha, \rho] = k[\theta]$. By Theorem 1.5 it will suffice to show that θ is separable over k, and we may assume that k has finite characteristic p. Then $k[\theta] = k[\alpha, \rho] = k[\alpha^p, \rho^p] \subset k[\theta^p]$ where the second equality comes from Theorem 1.4. Discreteness follows from [**1**; Theorem 3.6] since separable elements are algebraic.

Let E be a field containing a discrete subfield k. The *separable closure* of k in E is the subfield of E consisting of those elements that are separable over k. The field k is *separably closed* in E if the separable closure of k in E is k. The following theorem shows that the separable closure of k in E is separably closed.

THEOREM 1.7. *Let E be a field and k a discrete subfield of E. Suppose $\rho \in E$ is separable over k, and $\alpha \in E$ is separable over $k[\rho]$. Then α is separable over k.*

PROOF. By Corollary 1.2 we can write $k[\rho, \alpha] = k[\theta]$. Applying Theorem 1.4 we have $k[\theta^p] = k[\alpha^p, \rho^p] = k[\rho, \alpha^p] = k[\rho, \alpha] = k[\theta]$ so θ is separable over k. Thus α is separable over k by Theorem 1.5.

2. Perfect fields. A discrete field k is *perfect* if each polynomial in $k[x]$ is separable.

THEOREM 2.1. *A discrete field k is perfect if and only if for each prime p and each element $a \in k$ there exists a $b \in k$ with either $pb = a$ or $b^p = a$.*

PROOF. Assume k is perfect and let p be a prime and $a \in k$. If $p \neq 0$ in k, then $p^{-1} \in k$ and $b = p^{-1}a$ satisfies $pb = a$. If $p = 0$ in k, then $x^p - a$, being a product on polynomials which are relatively prime to their derivatives, must be reducible and, by Theorem 1.1, there is a $b \in k$ with $b^p = a$.

To prove the converse, let $f \in k[x]$. By [**1**; Lemma 3.5] we can assume that $f(x) = g(x^q)$ where $(g, g') = 1$ and either $q = 1$ or k has finite characteristic p and $q = p^e$. If $q = 1$, then f is separable. If $q = p^e$, then each coefficient of g is of the form b^q so $f(x) = g(x^q) = [h(x)]^q$ for some $h(x)$ in $k[x]$, and again f is separable.

COROLLARY 2.2. *If k is a discrete prime field, then k is perfect.*

DEFINITION. Let k be a subfield of a discrete field K. Then K is a *perfect closure* of k if

a) K is perfect

b) If $\alpha \in K$, then either $\alpha \in k$ or k has finite characteristic p and $\alpha^{p^e} \in k$ for some positive integer e.

THEOREM 2.3. *Every discrete field has a perfect closure.*

PROOF. Let $\{p_n : n < \omega\}$ be an enumeration of the primes in increasing order. For each n, define $\phi_n : k \to k$ by $\phi_n(x) = x^p$ if there exists $j \leqq n$ with $p = p_j$ and $p = 0$ in k. Otherwise let $\phi_n(x) = x$. Let K be the direct limit of the system of maps $\{\phi_n\}$. Suppose $\alpha \in K$ and p is a prime. If $p \neq 0$ in K, then $b = p^{-1}a$ satisfies $pb = a$. So assume that $p = 0$ in K and let $\psi_n = \psi_{n+1}\phi_n$ be the embedding maps $k \to K$ of the direct limit. There exists n and an element a in k so that $\psi_n(a) = \alpha$. Pick n large enough so that $p_n \geqq p$, so that $\phi_n(a) = a^p$. Then $\alpha = \psi_n(a) = \psi_{n+1}(\phi_n(a)) = \psi_n(a^p) = [\psi_n(a)]^p$. Thus K is perfect. If $\alpha \in K$, choose n and $a \in k$ so that $\psi_n(a) = \alpha$. If $p_1, \ldots, p_n$ are not zero in k, then $\alpha \in k$. Otherwise there exists a prime $p = p_j$ with $j \leqq n$ which is zero in k. Then $\phi_{n-1} \circ\circ\circ \phi_1(a) = a^{p^{n-j}}$ and so $\alpha^{p^{n-j}} = [\psi_n(a)]^{p^{n-j}} = \psi_n(a^{p^{n-j}}) = \psi_n(\phi_{n-1} \circ\circ\circ \phi_1(a)) = \psi_1(a) = a \in k$.

THEOREM 2.4. *If K and L are perfect closures of the discrete field k, then there is an isomorphism of K and L over k.*

PROOF. Define f from K to L as follows. Given $\alpha \in K$ either $\alpha \in k$, in which case we set $f(\alpha) = \alpha$, or k has finite characteristic p and $\alpha^{p^e} \in k$. In

this latter case, there is $\lambda \in L$ such that $\lambda^{p^e} = \alpha^{p^e}$, by Theorem 2.1, and we set $f(\alpha) = \lambda$.

THEOREM 2.5. *A discrete field k is perfect if and only if each algebraic element of an arbitrary extension field of k is separable over k.*

PROOF. If k is perfect, then each polynomial in $k[x]$ is separable, so clearly every element algebraic over k is separable. Conversely let p be a prime and $a \in k$. Clearly we may assume that $p = 0$ in k. Let $K \supset k$ be a perfect field and let $b \in K$ be such that $b^p = a$. As b is separable over k it follows that $b \in k$. By Theorem 2.1 we conclude that k is perfect.

3. Separably factorial fields. Recall that a discrete field k is *factorial* if each polynomial in $k[x]$ can be written as a product of irreducible polynomials. If each separable polynomial in $k[x]$ can be written as a product of irreducible polynomials, then the field k is *separably factorial.* In [1] it was shown that a finite separable extension of a countable factorial field is factorial [1; Theorem 4.2]. In this section we shall remove the countability condition, and also show that a finite extension of a separably factorial field is separably factorial. In so doing we reduce the problem of factoring a polynomial to that of finding a root of another polynomial.

LEMMA 3.1. *If K/k is separable $f \in k[x]$ splits in K, then f is a separable polynomial.*

PROOF. Let $\alpha \in K$ be a root of f. The element α satisfies a separable polynomial $g(x) \in k[x]$. Let $h(x) = \mathrm{GCD}(g(x), f(x))$. Then $h(\alpha) = 0$ and h is separable. By induction $f(x)/h(x)$ is a separable polynomial. This completes the proof.

The problem of constructing a splitting field for a polynomial over an arbitrary field, which is very likely unsolvable, is avoided in the following proof. Seidenberg uses a similar idea to define the norm [4].

THEOREM 3.2. *Let k be a discrete subfield of the field E, and let $h(x) \in k[x]$ be a monic (separable) polynomial. Then there exists a (separable) polynomial $q(x) \in k[x]$ such that the coefficients of any monic factor of h in $E[x]$ are roots of $q(x)$.*

PROOF. Let h be of degree $n \geqq 1$ and let $\{r_i : i = 1, \ldots, n\}$ be a set of algebraically independent elements over k. Define $A_i \in k[r_1, \ldots, r_n]$ and $H(x) \in k[A_0, \ldots, A_{n-1}, x]$ by

$$H(x) = \prod(x - r_i) = x^n + A_{n-1}x^{n-1} + \cdots + A_0.$$

As $H(r_i) = 0$ for each i, it follows that the r_i are algebraic over $k[A_0, \ldots, A_{n-1}]$. Define $Q(x) \in k[r_1, \ldots, r_n, x]$ by $Q(x) = \Pi(x - \lambda)$ where λ ranges over all the elementary symmetric polynomials in subsets of the r_i. As the

elements A_i are the elementary symmetric polynomials in all the r_i and the coefficients of Q are symmetric polynomials in all the r_i it follows that $Q(x) \in k[A_0, \ldots, A_{n-1}, x]$, see [5; page 81]. Now the coefficients of any factor of H in $k[r_1, \ldots, r_n, x]$ are elementary symmetric polynomials in a subset of the r_i. It follows that any such coefficient is a root of Q. Suppose that $h(x) = f(x)g(x)$ in $E[x]$, with

$$f(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$$

and

$$g(x) = x^s + c_{s-1}x^{s-1} + \cdots + c_0.$$

Define

$$F(x) = \prod_{i=1}^{m}(x - r_i) = x^m + B_{m-1}x^{m-1} + \cdots + B_0$$

and

$$G(x) = \prod_{i=m+1}^{n}(x - r_i) = x^s + C_{s-1}x^{s-1} + \cdots + C_0.$$

The B_i and C_j are algebraically independent over k because the A_i are algebraically independent, the extension $k(C, B)/k(A)$ is algebraic, and the theorem on invariance of transcendence degree holds [3; pages 200, 201]. So we can define a ring homomorphism from $k[B, C]$ to E by $B_i \to b_i$ and $C_j \to c_j$. Under this map F goes to f, G goes to g, and A_i goes to a_i. Define q as the image of Q and note that q is independent of f and g. The coefficients of F and G are roots of Q, so the coefficients of f and g are roots of q.

It remains to show that q is separable if h is separable. Let k_0 be a countable subfield of k containing the coefficients of h. Let K be a splitting field for h over k_0. The polynomial q splits in K as the roots of q are combinations of the roots of h. By Lemma 3.1 it follows that q is separable.

COROLLARY 3.3. a) *If k is separably closed in K and the monic separable polynomial $g \in k[x]$ has a monic factor $f \in K[x]$, then $f \in k[x]$.*

b) *If k is algebraically closed in K and the monic polynomial $g \in k[x]$ has a monic factor $f \in K[x]$, then $f \in k[x]$.*

PROOF. The coefficients of any factor of g in $K[x]$ satisfy a monic (separable if g is separable) polynomial in $k[x]$. As k is algebraically (separably) closed in K, these coefficients must be in k.

THEOREM 3.4. *A discrete field k is (separably) factorial if and only if for each (separable) $f \in k[x]$, either there exists an $\alpha \in k$ with $f(\alpha) = 0$, or for all $\alpha \in k, f(\alpha) \neq 0$.*

PROOF. If k is separably factorial, then we can determine the linear factors of f, so the condition is clearly necessary. To prove the converse let $q(x) \in k[x]$ be a monic polynomial so that the coefficients of any factor of f in $k[x]$ are roots of q (Theorem 3.2). Using induction on the degree of q and the condition of the theorem we can determine the finite set of elements of k which are roots of q. Thus we can obtain a finite set of polynomials containing all the monic factors of f in $k[x]$. The elements of this set can now be tested to see whichare the factors.

As a consequence of this theorem we are able to give a simple proof of Kronecker's theorem [**2**; page 77].

COROLLARY 3.5 (KRONECKER). *The field of rational numbers is factorial.*

PROOF. The usual rational root test is a method for deciding whether a polynomial with rational coefficients has a rational root.

LEMMA 3.6. *Let E be a field and k a discrete subfield. Suppose $\theta \in E$ satisfies the monic polynomial $f \in k[x]$ of degree $n > 0$, If $\alpha \in k[\theta]$, then either $\theta \in k[\alpha]$ or α satisfies a polynomial in $k[x]$ of degree less than n.*

PROOF. Write $\alpha^i = \sum_{j=0}^{n-1} a_{ij}\theta^j$ for $i = 0, \ldots, n-1$. By row operations we can put the matrix $[a_{ij}]$ into upper triangular form. One can now see if there is a zero on the diagonal. If there is, then the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is linearly dependent over k and so α satisfies a polynomial of degree less than n. If all the diagonal elements are nonzero, then the determinant of $[a_{ij}]$ is nonzero, and so $\theta \in k[\alpha]$.

The following theorem is of classical interest in addition to setting the stage for a purely constructive counterexample. In section four an example will be given to show that it is necessary to assume that k is separably closed in K.

THEOREM 3.7. *Let $k \subset K \subset E$ be fields with k discrete and separably closed in K. Let $\alpha \in E$ be algebraic over k. Then $k(\alpha)$ is separably closed in $K(\alpha)$. Moreover if α is separable and k is algebraically closed in K, then $k[\alpha]$ is algebraically closed in $K[\alpha]$.*

PROOF. Let $\rho \in K[\alpha]$ be separable over $k[\alpha]$. By Corollary 1.2 there is a $\theta \in k[\alpha, \rho]$ so that $k[\alpha, \rho] = k[\theta]$. By [1; Lemma 3.5] θ^q is separable over k, where either $q = 1$, or k has finite characteristic p and $q = p^m$. Then, by Theorem 1.5, $k(\alpha^q)$ is separable over k. Let α^q satisfy $f(x) \in k[x]$, a separable polynomial of degree n. We proceed by induction on n to prove that $\theta^q \in k[\alpha^q]$. If $n = 1$, then $\alpha^q \in k$ so $\theta^q \in K$ and thus $\theta^q \in k$ since k is separably closed in K. Now suppose that $n > 1$. As $\theta^q \in K[\alpha^q]$, it follows that θ^q satisfies a polynomial of degree $\leqq n$ over K. But θ^q satisfies a separable polynomial over k. Taking GCD's of these two polynomials and using

Corollary 3.3 one obtains a separable polynomial of degree $\leqq n$ in $k[x]$ which θ^q satisfies. By Lemma 3.6 $\theta^q \in k[\alpha^q]$ or else α^q satisfies a polynomial of degree less than n and we are done by induction. Thus $\theta^q \in k[\alpha^q]$. Therefore θ is separable and purely inseparable over $k[\alpha]$ and so is an element of $k[\alpha]$.

Now suppose that k is algebraically closed in K, and that α is separable over k. Let $\theta \in K(\alpha)$ be algebraic over $k(\alpha)$. By Corollary 1.2 we may assume that $k(\alpha, \theta) = k[\theta]$. Let α satisfy a monic polynomial of degree n in $k[x]$. We proceed by induction on n to show that $\theta \in k(\alpha)$. As $\theta \in K(\alpha)$ it follows that θ satisfies a monic polynomial in $K[x]$ of degree less than or equal to n. The element θ is also algebraic over k. Applying Corollary 3.3 to the GCD of the polynomials θ satisfies over k and K we obtain a polynomial of degree less than or equal to n in $k[x]$ satisfied by θ. By Lemma 3.6 either $\theta \in k[\alpha]$ or else α satisfies a monic polynomial of degree less than n. In the latter case induction shows that $\theta \in k[\alpha]$.

LEMMA 3.8. *Let k be a separably factorial subfield of a field E. Let $\alpha, \rho \in E$ be such that α is algebraic over k and ρ is separable over $k(\alpha)$. Then ρ satisfies an irreducible polynomial over $k(\alpha)$.*

PROOF. By [1; Theorem 3.7], to prove that ρ satisfies an irreducible polynomial over $k[\alpha]$ is the same as proving that $k[\alpha, \rho]$ is finite dimensional over $k[\alpha]$. If α is separable over k, then by Corollary 1.2 and Theorem 1.6 there exists $\theta \in k[\alpha, \rho]$, separable over k, so that $k[\alpha, \rho] = k[\theta]$. As k is separably factorial, $k[\theta]$ and $k[\alpha]$ are both finite dimensional over k. Therefore, by [1; Corollary 2.3], $k[\theta]$ is finite dimensional over $k[\alpha]$. Thus we may assume that k has finite characteristic p. As ρ is separable over $k[\alpha]$, we can write $k[\alpha, \rho] = k[\theta]$ for some θ separable over $k[\alpha]$ by Corollary 1.2 and Theorem 1.5. Choose $q = p^n$ so that $\lambda = \theta^q$, and hence α^q, is separable over k. Then $k[\lambda]/k$ and $k[\alpha^q]/k$ are finite dimensional as k is separably factorial [1; Theorem 3.7.] Therefore $k[\lambda]/k[\alpha^q]$ is finite dimensional. Let $\{1, \lambda, \lambda^2, \ldots, \lambda^s\}$ be a basis for $k[\lambda]/k[\alpha^q]$. As $\lambda \in k[\lambda, \alpha]$ and θ is separable over $k[\alpha]$ we have $k[\theta] = k[\lambda, \alpha]$ by Theorem 1.4. Thus $\{1, \lambda, \ldots, \lambda^s\}$ generates $k[\theta]/k[\alpha]$. Suppose $\sum a(i)\lambda^i = 0$ with $a(i) \in k(\alpha)$. Then $0 = (\sum a(i)\lambda^i)^q = \sum a(i)^q \lambda^{iq}$, where $a(i)^q \in k(\alpha^q)$. As λ is separable over k it follows that $k(\alpha^q, \lambda) = k(\alpha^q, \lambda^q)$. Thus $\{\lambda^{iq}: i = 1, \ldots, s\}$ is a basis for $k(\alpha^q, \lambda)$ over $k(\alpha^q)$. Therefore $a(i) = 0$ for all i.

We are now able to prove the results on preservation of (separable) factoriality under extension. This theorem has a long history beginning with Kronecker who proved it for algebraic number fields [2]. Van der Waerden extended the result to finite separable extensions and included a proof in [5]. This proof uses the norm of an element and it is unclear if van der Waerden means the norm defined in terms of a splitting field and

the conjugates of an element therein, as defined on page 178 of [5], or the norm defined in terms of the field polynomial as defined on page 132 of [5]. The proof also uses several properties of the norm which, while true, are not at all obvious from the second definition. Seidenberg has read van der Waerden's proof as using the first definition which he properly points out is nonconstructive [4]. Because of these difficulties, Seidenberg redefines a norm using a generic splitting field, similar to the idea behind our proof of Theorem 5.2, and then repeats van der Waerden's proof. We have given a proof of the theorem, via conjugates, for countable fields in [1; Theorem 4.2]. The following theorem removes the countability restriction.

THEOREM 3.9. *Let K be a discrete field, k a separably factorial subfield, and $\alpha \in K$ algebraic over k. Then $F = k[\alpha]$ is separably factorial. Moreover, if α is separable and k is factorial, then F is factorial.*

PROOF. Let $f \in F[x]$ be separable. Let k_0 be the separable closure within k of the field generated by the coefficients of a nonzero polynomial satisfied by α, together with the coefficients of all powers of α which occur in the coefficients of f. Then k_0 is a countable field. As we can determine whether separable polynomials over k_0 have roots in k, and hence in k_0, it follows, by Theorem 3.4, that k_0 is a separably factorial field. To complete the proof of the theorem it will suffice, by Theorem 3.4, to find the roots of f that lie in $k_0[\alpha] = F_0$ since, by Theorem 3.7, we have $k_0[\alpha]$ is separably closed in $k[\alpha]$, and the coefficients of f lie in F_0.

As F_0 is countable, we can construct a splitting field L of f over F_0 (see [1; Corollary 3.9]). Let $r_1, \ldots, r_s$ be the roots of f in L. By Lemma 3.8 we can find irreducible polynomials $g_i \in F_0[x]$ that are satisfied by the r_i. If g_i is linear, then $r_i \in F_0$ and we have found a root of f in F_0. If no g_i is linear, then f has no roots in F_0.

The second statement is proved in exactly the same way except k_0 is replaced by the algebraic closure and we appeal to Corollary 1.3 rather than to Lemma 3.8 in the last paragraph.

In [1; page 100] it was shown that even when a splitting field of a polynomial can be constructed, it need not be unique. However splitting fields for separable polynomials over separably factorial fields exist and are unique. The proof proceeds along the usual classical lines, using Theorem 3.9.

COROLLARY 3.10. *Let k be a separably factorial field, and $f(x) \in k[x]$ be a separable polynomial. Then there is a separably factorial field K containing k, such that f is a product of linear factors in $K[x]$ and K is generated over k by the roots of f. Moreover any two such fields K are isomorphic over k.*

4. Examples. In this section we give an example of a field that is separably factorial but not factorial. The same example also shows that in Theorem 3.7 the field k must be separably closed in K. This example has been used by Seidenberg [3] to show that a factorial field need not satisfy his 'condition P', and that an inseparable extension of a factorial field need not be factorial.

THEOREM 4.1. *Let F be the Galois field with two elements, and let $K = F(b, s, t)$ where b, s and t are indeterminates. Let $k = F(a, b) \subset K$, where $a = bs^2 + t^2$. Then k is algebraically closed in K.*

PROOF. Note that a and b are algebraically independent over F, as the elements b, s and t are algebraically independent over F. As K has transcendence degree 3 over F, and k has transcendence degree 2 over F, while K is algebraic over $k(s)$ as $K^2 \subset k(s)$, it follows that s is transcendental over k. Now let $\alpha \in K$ be algebraic over k, and let $f \in F[a, b, x]$ be a nonzero polynomial with $f(\alpha) = 0$. Let $r \in F[a, b]$ be the leading coefficient of f. Then $r\alpha$ is integral over $F[a, b]$. Now $(r\alpha)^2 \in k(s)$ is also integral over $F[a, b]$. As s is transcendental and $F[a, b]$ is integrally closed in $F(a, b)$ it follows that $w = (r\alpha)^2 \in F[a, b]$. Write $r\alpha = p/q + (u/v)t$ where $p, q, u, v \in F[a, b, s]$. Then $w = p^2/q^2 + (u^2/v^2)(a + bs^2)$ so

$$(*) \qquad p^2v^2 + u^2q^2(a + bs^2) = wq^2v^2.$$

If $u = 0$, then $r\alpha = p/q$ is integral over $F[a, b]$ and in $F(a, b)$, so $r\alpha \in F[a, b]$ and hence $\alpha \in k$ as desired. Otherwise, let n be the largest power of s dividing u^2q^2. The coefficient of s^n on the left hand side of equation $(*)$ contains only even powers of b and is nonzero as it contains an odd power of a. Hence w, and so wq^2v^2, contains only even powers of b. But the coefficient of s^{n+2} on the left hand side of $(*)$ contains an odd power of b. Thus $u \neq 0$ is impossible.

THEOREM 4.2. *If $F_1 \subset F_2 \subset \cdots$ are factorial fields, and F_i is algebraically closed in F_{i+1} for each i, then $F = \bigcup F_i$ is factorial.*

PROOF. We first note that each F_i is algebraically closed in F. If $f \in F[x]$, then $f \in F_i[x]$ for some i. Since F_i is factorial we can decide if f has a root in F_i. As F_i is algebraically closed in F, this settles whether f has a root in F. By Theorem 3.4 it follows that F is factorial.

EXAMPLE 4.3. Let $\{a_j\}$ be a nondecreasing fugitive sequence of 0's and 1's. Let $F_i = k$ of Theorem 4.1 if $a_i = 0$, and $F_i = K$ of the same theorem if $a_i = 1$. Then $F = \bigcup F_i$ is factorial by Theorem 4.2. Consider $F[\alpha]$ where $\alpha^2 = a$. The polynomial $x^2 - b$ has a root in $F[\alpha]$ if and only if $F = K$, in which case $(\alpha + t)/s$ is a root. Hence if we could decide whether

$x^2 - b$ had a root in $F[\alpha]$, we could decide whether $a_j = 1$ for some j or not. Thus $F[\alpha]$ is not factorial. However by Theorem 3.9, $F[\alpha]$ is separably factorial.

Theorem 4.1 also gives a classical example to show that the condition of separability is needed in Theorem 3.7. For k is algebraically closed in K and $k(\alpha)$ is not algebraically closed in $K(\alpha)$, since the polynomial $x^2 - b$ has a root in $K(\alpha)$ but not in $k(\alpha)$.

References

1. W. Julian, R. Mines and F. Richman, *Algebraic numbers, a constructive development*, Pac. J. Math. **74** (1978), 91–102.

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

3. A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313.

4. ———, *Constructions in a polynomial ring over the ring of integers*, Amer. J. Math. **100** (1978), 685–703.

5. B. L. van der Waerden, *Modern Algebra*, Ungar, New York, 1953.

6. O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1, D. van Nostrand, Princeton, NJ, 1958.

New Mexico State University, Las Cruces, NM 88003