TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 158, Number 2, August 1971

THE EXISTENCE OF SOLUTIONS OF ABSTRACT PARTIAL DIFFERENCE POLYNOMIALS

BY
IRVING BENTSEN(1)

Abstract. A partial difference (p.d.) ring is a commutative ring R together with a (finite) set of isomorphisms (called transforming operators) of R into R which commute under composition. It is shown here that (contrary to the ordinary theory [R. M. Cohn, *Difference algebra*]) there exist nontrivial algebraically irreducible abstract p.d. polynomials having no solution and p.d. fields having no algebraically closed p.d. overfield. If F is a p.d. field with two transforming operators, then the existence of a p.d. overfield of F whose underlying field is an algebraic closure of that of F is a necessary and sufficient condition for every nontrivial algebraically irreducible abstract p.d. polynomial P in the p.d. polynomial ring $F\{y^{(1)}, y^{(2)}, \ldots, y^{(n)}\}$ to have a solution η (in some p.d. overfield of F) such that: η has $n-1$ transformal parameters, η is not a proper specialization over F of any other solution of P, and, if Q is a p.d. polynomial whose indeterminates appear effectively in P and Q is annulled by η, then Q is a multiple of P. P has at most finitely many isomorphically distinct such solutions. Necessity holds if F has finitely many transforming operators.

1. **Introduction.** The primary objective of this paper is to initiate a study of conditions under which abstract partial difference polynomials possess solutions.

Richard M. Cohn [4] has established in the theory of ordinary difference algebra (one transforming operator) that every nontrivial abstract difference polynomial P has a solution. Furthermore, if P is algebraically irreducible in $F\{y^{(1)}, y^{(2)}, \ldots, y^{(n)}\}$, P has at least one solution η such that the dimension of $F\langle\eta\rangle/F$ is $n-1$ and for each k such that transforms of $y^{(k)}$ appear effectively in P no difference polynomial in $F\{y^{(1)}, y^{(2)}, \ldots, y^{(n)}\}$ with effective order in $y^{(k)}$ less than that of P is annulled by η [3, Theorems IV and IV′]; [4, Theorem 1, Chapter 6].

Presented to the Society, June 30, 1966; received by the editors April 18, 1967 and, in revised form, October 9, 1970.

AMS 1970 *subject classifications.* Primary 12H10, 39A10; Secondary 12F05, 12F20, 39A30.

Key words and phrases. Partial difference ring, ring isomorphisms commuting under composition, inversive closure, abstract partial difference polynomial, existence of solutions of abstract partial difference polynomials, algebraic closure, partial difference kernel, prolongation of partial difference kernel, realizations of partial difference kernels, specialization over partial difference field, compatibility property $\mathscr{P}^*$, stepwise compatibility condition, transformally independent set, primary difference field extension, regular difference field extension, quasi-linearly disjoint field extensions.

(1) Part of a dissertation presented for the degree of Doctor of Philosophy at Rutgers, The State University. The research was supported in part by National Science Foundation grants GP-1992 to Rutgers, The State University and GP-5281 to the University of Vermont.

A counterexample to the conjecture that every nontrivial partial difference polynomial has a solution is presented here (Example (3.8)(bis), §6). This example also establishes the existence of a partial difference field having no algebraically closed difference overfield, another divergence from the ordinary theory (Example (3.8)).

A principal result obtained (Theorems (6.2) and (6.1)) is the equivalence of the following statements for a partial difference field F with two transforming operators:

(a) F may be extended to a partial difference field whose underlying field is the algebraic closure of that of F.

(b) Every nontrivial algebraically irreducible partial difference polynomial P in a partial difference polynomial ring $F\{y^{(1)}, y^{(2)}, \ldots, y^{(n)}\}$ has a solution η such that η has $n-1$ transformal parameters, is not a proper specialization over F of any other solution of P, and if Q is a partial difference polynomial in some of the indeterminates of P which is annulled by η, then Q is a multiple of P.

(c) If a is any element separably algebraic and normal over the underlying field of F, F may be extended to a partial difference field $F\langle a\rangle$.

Conditions (a) and (c) are equivalent for partial difference fields with n operators.

A theory of partial difference kernels and their realizations, corresponding to the theory employed by Cohn [4, Chapter 6] for the ordinary case, is developed in §4 and §5 and applied to obtain the result (a) implies (b). The existence of difference fields having incompatible extensions creates complications in the development of the theory of partial difference kernels not found in the ordinary theory. A partial difference kernel which satisfies the "compatibility" condition property $\mathscr{P}^*$ introduced in §4 has a generic prolongation which also satisfies $\mathscr{P}^*$. The union of a sequence of such prolongations is a partial difference field in which the kernel is realized. In particular, if (a) holds and there are two operators, a partial difference polynomial P gives rise to a kernel with property $\mathscr{P}^*$, and the realization of the kernel yields a solution for P. In fact, $\mathscr{P}^*$ is a necessary and sufficient condition for a kernel to have a "principal" realization (see (5.1)). It is anticipated that the theory of partial difference kernels will play a significant role in the further investigation of systems of partial difference polynomials and their solutions.

The needed results concerning inversive closure are compiled in §3.

I wish to express my appreciation to Professor Richard M. Cohn for his many helpful suggestions during the preparation of this paper.

2. **Definitions and notation.** In general, our terminology and notation will follow closely that of R. M. Cohn [4] with the obvious generalizations to partial difference algebra.

The system $D=(A, \{\sigma_i : 1 \leqq i \leqq m\})$ consisting of a commutative ring A, together with a collection of isomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_m$ of A into A (not necessarily distinct in their action on A) which commute pairwise on the elements of A, is called a *partial difference ring* with m transforming operators. If $m=1$, D is the ordinary difference ring. We refer to A as the underlying ring of D and to the σ_i as the *defining transforming operators* of D. D is called a *partial difference domain* (*field*) if A is a domain (field).

A *partial difference subring* of D is a partial difference ring D' whose underlying ring A' is a subring of A stable under the action of each of the defining transforming operators σ_i of D and whose set of defining transforming operators are the restrictions σ_i' of σ_i, $1 \leqq i \leqq m$, to A'. We refer to D as a *partial difference overring* of D'.

For $a \in D$, the element $\sigma_1^{\mu_1}\sigma_2^{\mu_2}\cdots\sigma_m^{\mu_m}a$ (the $\mu_i \geqq 0$) is called a *transform* of a of (total) order $\nu = \sum_{i=1}^m \mu_i$. This transform of a is denoted by a_v, where v is the m-tuple $(\mu_1, \ldots, \mu_m)$. We say that a_v is a transform of a of *partial order* μ_i with respect to σ_i. Any element in a partial difference ring is a transform of itself of order zero.

If S is a set of elements in D then the intersection of all partial difference subrings of D which contain the elements of D' together with all transforms of the elements of S is a unique partial difference subring of D, said to be generated over D' by S, and denoted $D'\{S\}$.

Let B be a partial difference ring with identity and D a partial difference overring of B which contains a set of elements $y^{(1)}, y^{(2)}, \ldots, y^{(n)}$ such that the set of all transforms of the elements $y^{(1)}, y^{(2)}, \ldots, y^{(n)}$ form an algebraically independent set over (the underlying ring of) B. Then $B\{y^{(1)}, y^{(2)}, \ldots, y^{(n)}\}$ is an *n-fold partial difference polynomial ring* over B. The existence of partial difference polynomial rings is established by Kreimer [5, p. 487]. The elements of a partial difference polynomial ring are called *partial difference polynomials.* A partial difference polynomial P in $B\{y^{(1)}, \ldots, y^{(n)}\}$ may be regarded as an integral rational expression in a finite subset of the $y_v^{(k)}$ with coefficients in the underlying ring of B. We shall restrict our attention to partial difference polynomials over partial difference fields. A *solution* for a partial difference polynomial P in $F\{y^{(1)}, \ldots, y^{(n)}\}$ is an n-tuple $a = (a^{(1)}, a^{(2)}, \ldots, a^{(n)})$ of elements in some partial difference overfield of F which when substituted into P (each $y_v^{(k)}$ in P replaced by $a_v^{(k)}$) annuls P.

Let F be a partial difference subfield of a partial difference field G and S a set of elements of G. Then $F\langle S\rangle$ will denote the (unique) partial difference subfield of G which is the intersection of all partial difference subfields of G which contain the elements of F and S. $F\langle S\rangle$ is said to be obtained from F by *difference field adjunction* of S to F. If G_1 and G_2 are partial difference subfields of G then $\langle G_1, G_2\rangle$ will denote the (unique) partial difference subfield of G which is the intersection of all partial difference subfields of G which contain G_1 and G_2. If M, L_1, L_2 are the underlying fields of G, G_1, G_2, then the intersection (L_1, L_2) of all subfields of M which contain L_1 and L_2 is the underlying field of $\langle G_1, G_2\rangle$. With F and G as above, we refer to the pair F, G as a *partial difference field extension*, denoted G/F.

Let $D = (A, \{\sigma_i : 1 \leqq i \leqq m\})$ and $D' = (A', \{\sigma_i' : 1 \leqq i \leqq m\})$ be partial difference rings. A *difference homomorphism* (or simply homomorphism) of D into (onto) D' is a homomorphism ϕ of A into (onto) A' such that $\phi\sigma_i a = \sigma_i'\phi a$, $a \in A$, $1 \leqq i \leqq m$. The definitions of isomorphism and automorphism of partial difference rings (fields) and partial difference field extensions follow as expected. (A more general definition of homomorphism and isomorphism is given by A. Bialynicki-Birula [2]; however, that generality is less suitable for our purposes, since our particular interest is difference field extensions rather than difference fields, in which the effect of incompatible extensions is of particular concern.)

G^0 will denote a partial difference ring obtained from a partial difference ring G by deletion of one transforming operator. If G is an ordinary difference ring, then G^0 will denote the underlying ring of G.

Such terms as algebraically closed, algebraic closure, free, linearly disjoint, quasi-linearly disjoint, primary and regular, when applied to partial difference fields (partial difference field extensions), will refer to their underlying fields (underlying field extensions).

Throughout the remainder of the paper, the adjective "partial" will be understood and the term "ordinary" used to emphasize the case of one transforming operator.

Familiarity with the following statements about field extensions is assumed.

(2.1) Let k, K, L, E be fields having a common overfield such that $k \subseteq K$, $k \subseteq E \subseteq L$. Then K and L are (linearly disjoint, quasi-linearly disjoint, free) over k if and only if K and E are (linearly disjoint, quasi-linearly disjoint, free) over k, and (K, E) and L are (linearly disjoint, quasi-linearly disjoint, free) over E.

Corollary. Let k, K, L, E, E' be fields having a common overfield such that $k \subseteq K$, $k \subseteq E \subseteq L$, $k \subseteq E' \subseteq L$. Then K and E are (linearly disjoint, quasi-linearly disjoint, free) over k and (K, E) and L are (linearly disjoint, quasi-linearly disjoint, free) over E if and only if K and E' are (linearly disjoint, quasi-linearly disjoint, free) over k and (K, E') and L are (linearly disjoint, quasi-linearly disjoint, free) over E'.

(2.2) Let (M, τ_1, τ_2) be a free join of the pair of field extensions K_1/k, K_2/k. If (K_1, τ_1) and (K_2, τ_2) are quasi-linearly disjoint over k, then every free join of the pair of extensions K_1/k and K_2/k is equivalent to (M, τ_1, τ_2) [8, p. 195].

(2.3) Let (M, τ_1, τ_2) be a free join of the pair of field extensions K_1/k, K_2/k. Then K_1 and K_2 are quasi-linearly disjoint over k and M/K_2 is a primary (regular) extension if and only if K_1/k is a primary (regular) extension [6, p. 61].

3. **Inversive closure; compatibility.** The difference ring $D = (A, \{\sigma_i : 1 \leqq i \leqq m\})$ is said to be *inversive with respect to* σ_i if σ_i is an automorphism of A; D is termed *inversive* if all of the transforming operators of D are automorphisms of A.

The *inversive closure* of D is an inversive difference overring E of D with the property that for each element $a \in E$ there exists a composition ρ of the transforming operators of E which is dependent upon a such that $\rho a \in D$.

(3.1) Theorem. *Every difference ring has an inversive closure. If E_1 and E_2 are inversive closures of a difference ring D, then the difference field extensions E_1/D and E_2/D are isomorphic. If E is an inversive difference overring of D, then there* *exists a unique difference subring of E which is an inversive closure of D. If D is a difference domain (field) then its inversive closure is a difference domain (field).*

(3.1) is a generalization of [4, Theorem II, Chapter 2] to partial difference rings.

Proof. From the difference ring $D=(A, \{\sigma_i : 1 \leqq i \leqq m\})$ we obtain the ordinary difference ring (A, ρ) where ρ denotes $\sigma_1\sigma_2 \cdots \sigma_m$. By [4, Theorem II, Chapter 2], (A, ρ) has an inversive closure (A', ρ'). For $a \in A'$, let $r=r(a)$ be the smallest nonnegative integer such that $(\rho')^r a \in A$. For each i, define σ_i' by $\sigma_i' a=(\rho')^{-r}\sigma_i(\rho')^r a$, $a \in A'$. Thus $E_1=(A', \{\sigma_i' : 1 \leqq i \leqq m\})$ is an inversive closure of D.

Let E_2 be another inversive closure of D and let ρ_1' and ρ_2' be the products of the transforming operators of E_1 and of E_2 respectively. With $r=r(a)$ defined for elements of E_1 as above, we define $\psi: E_1 \to E_2$ by $\psi a=(\rho_2')^{-r}(\rho_1')^r a$. To verify that $\psi\sigma_i'=\sigma_i''\psi$, one uses the facts that if δ is any product of transforming operators of E_1, then $r(\delta a) \leqq r(a)$ and if $s \geqq r(a)$, $(\rho_2')^{-s}(\rho_1')^s a=(\rho_2')^{-r}(\rho_1')^r a$. ψ is a difference isomorphism of E_1/D onto E_2/D.

The proofs of the remaining statements are as for ordinary difference rings.

(3.2) Let D' and E' denote inversive closures of the difference rings D and E. If ψ is a difference homomorphism of D onto E then ψ has a unique extension to a difference homomorphism of D' onto E'.

(3.3) Let D be a difference domain with underlying ring R. If K is a field of quotients of R, D extends uniquely to a difference field E with underlying field K. E is called the *difference quotient field* of D. If E and E' are difference quotient fields of D, then E/D and E'/D are isomorphic. If D is inversive, then E is inversive. If D is a difference subring of a difference field G, then G contains a unique difference subfield E which is a quotient field of D. Furthermore, if G is inversive, then the inversive closure of E in G is the quotient field of the inversive closure of D in G.

(See [4, Theorem III, p. 68] for the existence theorem for ordinary difference fields.)

Let H be an inversive difference field (ring) and for any difference subfield (subring) G of H let G^* denote the inversive closure of G in H.

(3.4) For F, G, G_1, G_2 difference subfields of an inversive difference field H, we note the following properties of the operation $*$:

(a) $F \subseteq G$ implies $F^* \subseteq G^*$.

(b) If G is inversive, then $G^*=G$. Hence, for arbitrary G, $G^{**}=G^*$.

(c) $\langle G_1, G_2\rangle^*=\langle G_1^*, G_2^*\rangle$.

(d) If τ is an isomorphism of G_1 onto G_2 then τ has a unique extension to an isomorphism of G_1^* onto G_2^*.

(e) If F contained in G_1 and G_2 is such that G_1 and G_2 are (free, linearly disjoint, quasi-linearly disjoint) over F, then G_1^* and G_2^* are (free, linearly disjoint, quasi-linearly disjoint) over F^*.

(f) Let G be inversive and let $*'$ denote the inversive closure operation defined with respect to G on the difference subfields of G. Then $F \subseteq G$ implies $F^{*\prime}=F^*$.

(g) Let $F \subseteq F_0 \subseteq G$, where F_0 is (the algebraic part, the purely inseparable part, the separable part) of G over F. Then F_0^* is (the algebraic part, the purely inseparable part, the separable part) of G^* over F^*.

(3.5) Let G be a difference overfield of F and H an inversive closure of G.

(a) If G is an (algebraic closure, perfect closure, separable algebraic closure) of F, then H is respectively an (algebraic closure, perfect closure, separable algebraic closure) of F^*.

(b) If in (a), F is inversive, then G is inversive.

(c) If G/F is a primary (regular) extension, then H/F^* is a primary (regular) extension.

Proof. Let ρ denote the composition of the operators of H, each factor of which is of partial order 1. Let H', G', F' denote the ordinary difference fields defined on the underlying fields of H, G, F by ρ and suitable contractions of ρ. Then H' is an inversive closure of G'.

By [4, Corollary II, Theorem I, Chapter 6], there exists a difference overfield E of H' whose underlying field is an algebraic closure of the underlying field of H'. E is inversive since H' is. Then for each assumption on G over F, G' is respectively the algebraic part, purely inseparable part, separable part of E over F'. Hence by (3.4(g)) and (3.4(b)), H' is the algebraic part, purely inseparable part, separable part of E over the inversive closure F_1' of F' in H'. Since E is an algebraic closure of H' it thus follows that the underlying field of H' is an algebraic closure, perfect closure, separable algebraic closure of the underlying field of F_1'. The underlying field of F_1' coincides with that of F^*; hence (a) is established.

(b) follows from the fact that an overfield of a field K can contain at most one (algebraic closure, perfect closure, separable algebraic closure) of K.

Now to prove (c). Suppose G/F is primary. Let F_0 denote the purely inseparable part of G over F. Then F_0 is also the algebraic part of G over F and hence by (3.4(g)), F_0^* is both the purely inseparable part of H over F^* and the algebraic part of H over F^*. Thus H/F^* is primary.

Now suppose G/F is regular. Then, together with the notation used in the proof of (a), we denote by $E^{(1)}$ the algebraic part of E over F' and by $E^{(2)}$ the algebraic part of E over F_1'. Because E is inversive, it follows by (3.4(g)) that $E^{(2)}$ is an inversive closure of $E^{(1)}$. Since G/F is regular, G' and $E^{(1)}$ are linearly disjoint over F' [6, Theorem 2, Chapter 3]. By (3.4(e)), H' and $E^{(2)}$ are linearly disjoint over F_1'. Hence H'/F_1' is a regular extension, and thus H/F^* is a regular extension.

In the remainder of the paper, the context, together with (3.4(f)), will make clear the inversive difference field (ring) with respect to which the operation * is defined. (If no inversive overfield (overring) is indicated, * will denote some inversive closure, whose existence is asserted by (3.1).)

The difference field extensions G/F and H/F are said to be *compatible* if there exists a difference field extension E/F such that G/F and H/F have isomorphisms into E/F. Otherwise they are said to be *incompatible*.

The existence of incompatible extensions [4, Example 4, p. 59] plays an important part in the development of the theory of difference algebra. Of particular concern here is the fact that the presence of incompatible extensions can inhibit the extension of difference isomorphisms for difference field extensions (see [4, Example 1, p. 277]).

In each of the definitions and theorems in the remainder of this paper the terms primary, quasi-linearly disjoint and separable algebraic may be replaced by regular, linearly disjoint and algebraic respectively. Then in §4 we may speak of a kernel which satisfies property $\mathscr{R}^*$ rather than property $\mathscr{P}^*$.

The main idea of the following theorem has been established by Kreimer [5, Theorem 5.2, p. 489].

(3.6) THEOREM. *Let G/F be a primary extension of an inversive difference field F and let τ be a difference isomorphism of F into G. τ has an extension to a difference isomorphism τ_1 of G into a difference overfield E of G such that $E=\langle G, \tau_1 G\rangle$, G and $\tau_1 G$ are quasi-linearly disjoint over τF, and E/G is a primary extension. Furthermore, if G is inversive, then E is inversive.*

If $\bar{E}$ is a difference overfield of G such that τ has an extension to a difference isomorphism τ' of G into $\bar{E}$ and $\bar{E}$ is the free join of G and $\tau' G$ over τF, then there exists a unique difference isomorphism ψ of E/G onto $\bar{E}/G$ such that $\psi\tau_1\alpha=\tau'\psi\alpha$ for $\alpha \in G$.

Proof. τF is an inversive difference subfield of G. Extend τ to an isomorphism $\bar{\tau}$ of G onto a difference overfield H of τF. $H/\tau F$ is primary. Thus by the generalization to m operators of the corollary to Lemma 1, Chapter 7 [4], with F, G, G' of the corollary corresponding to τF, H, G respectively, there exists a difference field extension $E/\tau F$ such that $H/\tau F$ and $G/\tau F$ have isomorphisms ϕ and η respectively into $E/\tau F$ with the images of H and G quasi-linearly disjoint over the underlying field of τF. Without loss of generality we may assume G is a difference subfield of E and, with τ_1 denoting the composition map $\phi\bar{\tau}$, E is the compositum of G and $\tau_1 G$. Then G and $\tau_1 G$ are quasi-linearly disjoint over τF. Hence since in particular E is the free join of G and $\tau_1 G$ over τF and $\tau_1 G/\tau F$ is primary, it follows by the sufficiency of (2.3) that E/G is primary. By (3.4(c)), G inversive implies $E=\langle G, \tau_1 G\rangle$ is inversive.

$\tau'\tau_1^{-1}$ is an isomorphism of $\tau_1 G/\tau F$ onto $\tau' G/\tau F$. This with the identity automorphism of G assures by (2.2) the existence of a unique isomorphism ψ of the underlying field M of E onto the underlying field $\bar{M}$ of $\bar{E}$ which leaves fixed the members of G and coincides with $\tau'\tau_1^{-1}$ on the members of $\tau_1 G$. Since the structure of difference field induced on $\bar{M}$ by E and ψ coincides with $\bar{E}$ on the underlying fields of G and $\tau' G$, and since G and $\tau' G$ are quasi-linearly disjoint over τF (by virtue of ψ) it follows by [4, Theorem X of the Introduction] applied to each difference operator that the difference field determined by E and ψ coincides with $\bar{E}$. Thus ψ is a difference isomorphism of E onto $\bar{E}$. The uniqueness of ψ in the sense of the statement of the theorem follows from the uniqueness of ψ in the above sense.

A difference field G is said to satisfy the *universal compatibility condition* if every pair of extensions of G is compatible. $G=(K, \{\sigma_i : 1 \leqq i \leqq m\})$ is said to satisfy the *stepwise compatibility condition* if there exists an ordering of the transforming operators of G such that for each integer k, $1 \leqq k \leqq m$, the difference field $G_k=(K, \sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_k})$ satisfies the universal compatibility condition.

Note. It is apparent from the fundamental theorem of compatibility for partial difference fields (an easy generalization of [4, Theorem I, Chapter 7]) that any difference field whose underlying field is separably algebraically closed or algebraically closed, as well as the inversive closure of such a field (3.5(a)), satisfies the stepwise compatibility condition.

(3.7) THEOREM. *If G is a difference field such that a difference field G^0 obtained from G by deletion of one transforming operator satisfies the stepwise compatibility condition, then there exists a difference overfield H of G whose underlying field is an algebraic closure of that of G.*

Proof. Let m denote the number of transforming operators in the definition of G. If G is an ordinary difference field $(m=1)$ then G has an algebraic closure by [4, Corollary II to Theorem I, Chapter 6].

Assume the statement of the theorem to be true for $m=q$, q a positive integer. Let G denote a difference field with $q+1$ transforming operators such that, for some ordering $\sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_{q+1}}$ of its transforming operators, the difference field $G^0=(K, \sigma_{i_1}, \sigma_{i_2}, \ldots, \sigma_{i_q})$ satisfies the stepwise compatibility condition. Then, a fortiori, G^0 satisfies the condition on G of the statement of the theorem. Hence, by the inductive assumption, there exists a difference overfield H of G^0 whose underlying field is an algebraic closure of K. Since any pair of extensions of G^0 is compatible, we may, by the generalization of [4, Theorem I, Chapter 9] to partial difference fields, extend $\sigma_{i_{q+1}}$, considered as a difference isomorphism of G^0 into G^0, to a difference isomorphism $\bar{\sigma}_{i_{q+1}}$ of H into a difference overfield of H. For each element $\alpha \in H$, $\bar{\sigma}_{i_{q+1}}\alpha$ is algebraic over the underlying field of $\bar{\sigma}_{i_{q+1}}G^0$ and hence also over K. Thus (since K admits at most one algebraic closure in any given overfield of K) $\bar{\sigma}_{i_{q+1}}\alpha \in H$. Hence H, together with $\bar{\sigma}_{i_{q+1}}$, determines a difference overfield $\bar{H}$ of G whose underlying field is an algebraic closure of that of G. The proof is completed by induction.

Although any ordinary difference field G has a difference overfield H whose underlying field is an algebraic closure of that of G, the following example shows that this result cannot be generalized to difference fields having several operators.

(3.8) EXAMPLE. Let $K=R(i, b)$, where R is the field of rational numbers, i is the square root of -1, and b the positive square root of 2. Let σ and τ denote the automorphisms of K such that

$$\sigma i = i, \qquad \sigma b = -b,$$
$$\tau i = -i, \qquad \tau b = b.$$

Then $F=(K, \sigma, \tau)$ is a difference field. There exists no difference overfield of F

whose underlying field is an algebraic closure of K. For suppose the contrary. Then there exists a difference overfield G of F which contains an element a such that $a^2=b$. Let σ', τ' denote the transforming operators of G which are the extensions of σ and τ respectively. Since $(\sigma'a)^2=\sigma'a^2=-b$ and $(\tau'a)^2=\tau'a^2=b$, we have $\sigma'a=\alpha ia$ and $\tau'a=\beta a$, where α and β denote plus or minus 1. Then

$$\sigma'\tau'a = \sigma'\beta a = \alpha\beta ia, \qquad \tau'\sigma'a = \tau'\alpha ia = -\alpha\beta ia.$$

Thus σ' and τ' do not commute at a, which contradicts the assumption that G is a difference field.

The following example shows that the converse of (3.7) is not true.

(3.9) EXAMPLE. Let $G=(R, \sigma, \tau)$ be the difference field with two transforming operators, both of which are the identity automorphism on the field R of rationals. σ and τ extend trivially to the identity automorphism of the algebraic closure L of R to form the difference field $H=(L, \bar{\sigma}, \bar{\tau})$. Let G^0 denote either difference field (R, σ) or (R, τ), and M the field $R(i)$, where $i^2=-1$. Let G_1^0 and G_2^0 denote the difference overfields of G^0 defined on M such that $i\to i$ and $i\to -i$ respectively. Then the pair G_1^0/G^0 and G_2^0/G^0 of extensions is incompatible. Hence for either definition of G^0, G^0 does not satisfy the universal compatibility condition. (Verification of the incompatibility may be found in [4, Example 4, pp. 59–60].)

4. **Difference kernels and their prolongations.** Let $F=(K, \{\sigma_i : 1\leqq i\leqq m\})$ be an inversive difference field and F^0 a difference field obtained from F by deletion of a transforming operator σ_{i_0}, $1\leqq i_0\leqq m$. Regard σ_{i_0} as an automorphism of F^0. A *difference kernel* $\mathscr{K}$ *over* F is an ordered pair $(F^0\langle a_0, a_1, \ldots, a_r\rangle, \tau)$, where $F^0\langle a_0, a_1, \ldots, a_r\rangle$ denotes a difference field generated over F^0 by a set of l-tuples $a_0, a_1, \ldots, a_r$, and τ denotes a difference isomorphism of $F^0\langle a_0, a_1, \ldots, a_{r-1}\rangle$ onto $F^0\langle a_1, \ldots, a_r\rangle$ such that $\tau a_j^{(k)}=a_{j+1}^{(k)}, j=0, 1, 2, \ldots, r-1; k=1, 2, \ldots, l$, and such that the restriction of τ to F^0 coincides with σ_{i_0}. r is called the *length* of the kernel. For the case $r=0$, the interpretation is that τ is the difference automorphism $\sigma_{i_0}$of F^0. If $m=1$, then $\mathscr{K}$ is the ordinary difference kernel as defined in [4]. The existence of partial difference kernels is a consequence of the existence of partial difference field extensions, as shown in the remark at the beginning of §5.

A *prolongation* of $\mathscr{K}$ is a difference kernel $\mathscr{K}_1$ consisting of a difference overfield $F^0\langle a_0, \ldots, a_r, a_{r+1}\rangle$ of $F^0\langle a_0, \ldots, a_r\rangle$ together with an extension τ_1 of τ such that $\tau_1: a_r^{(k)}\to a_{r+1}^{(k)}, k=1, \ldots, l$. (If a kernel is of length 1 or 0, then the expressions $F^0\langle a_1, a_2, \ldots, a_{r-1}\rangle$ and $F^0\langle a_0, a_1, \ldots, a_{r-1}\rangle$ respectively will be interpreted as F^0.)

A prolongation $\mathscr{K}_1$ of $\mathscr{K}$ is called *generic* if $F^0\langle a_0, \ldots, a_{r+1}\rangle^*$ is a free join of $F^0\langle a_0, \ldots, a_r\rangle^*$ and $F^0\langle a_1, \ldots, a_{r+1}\rangle^*$ over $F^0\langle a_1, \ldots, a_r\rangle^*$. By (3.1) and (3.4(c)) this definition is not ambiguous.

Note that if $\mathscr{K}_1$ is a prolongation of $\mathscr{K}$ such that $F^0\langle a_0, \ldots, a_r\rangle$ and $F^0\langle a_1, \ldots, a_{r+1}\rangle$ are free over $F^0\langle a_1, \ldots, a_r\rangle$, then by (3.4(c)), and (3.4(e)), $\mathscr{K}_1$ is a generic prolongation of $\mathscr{K}$.

We shall say that a kernel $\mathscr{K}$ satisfies *property* $\mathscr{P}$ if there exists a difference overfield E_1 of $F^0\langle a_0, a_1, \ldots, a_r\rangle$, a difference subfield E of E_1 which contains $F^0\langle a_0, \ldots, a_{r-1}\rangle$, and an extension of τ to a difference isomorphism $\hat{\tau}$ of E into E_1 such that

(a) E_1/E is primary;

(b) E and $F^0\langle a_0, \ldots, a_r\rangle$ are free over $F^0\langle a_0, \ldots, a_{r-1}\rangle$; and

(c) if $r>0$, $E_1=\langle E, \hat{\tau}E\rangle$; if $r=0$, $\hat{\tau}E\subseteq E$.

$\mathscr{K}$ will be said to satisfy *property* $\mathscr{P}^*$ (with respect to $(G, G_1, \bar{\tau})$) if there exists an inversive difference overfield G_1 of $F^0\langle a_0, \ldots, a_r\rangle$, an inversive difference subfield G of G_1 which contains $F^0\langle a_0, \ldots, a_{r-1}\rangle$ and an extension of τ to an isomorphism $\bar{\tau}$ of G into G_1 such that

(a) G_1/G is primary;

(b) G and $F^0\langle a_0, \ldots, a_r\rangle^*$ are free over $F^0\langle a_0, \ldots, a_{r-1}\rangle^*$; and

(c) if $r>0$, $G_1=\langle G, \bar{\tau}G\rangle$; if $r=0$, $\bar{\tau}G\subseteq G$.

(4.1) THEOREM. *The properties $\mathscr{P}$ and $\mathscr{P}^*$ are equivalent.*

Proof. With E, E_1 and $\hat{\tau}$ as in the definition of property $\mathscr{P}$, let G_1 denote an inversive closure of E_1 and G the inversive closure of E in G_1. By (3.4(d), (c)) $\hat{\tau}$ extends uniquely to an isomorphism $\bar{\tau}$ of G into G_1 such that, if the length r of $\mathscr{K}$ is greater than or equal to 1, $G_1=\langle G, \bar{\tau}G\rangle$, and if $r=0$, then by (3.4(a)) $\bar{\tau}G\subseteq G$. Thus by (3.4(e)) and (3.5(c)), $\mathscr{P}$ implies $\mathscr{P}^*$.

With G, G_1 and $\bar{\tau}$ as in the definition of $\mathscr{P}^*$, let E denote the separable part of G over $F^0\langle a_0, \ldots, a_{r-1}\rangle$. Then E is a difference overfield of $F^0\langle a_0, \ldots, a_{r-1}\rangle$ such that E and $F^0\langle a_0, \ldots, a_r\rangle$ are free over $F^0\langle a_0, \ldots, a_{r-1}\rangle$.

Let $\hat{\tau}$ denote the contraction of $\bar{\tau}$ to a difference isomorphism of E into G_1. If $r=0$ then for any element $b\in E$, $\hat{\tau}b\in G$ and $\hat{\tau}b$ is separably algebraic over $\hat{\tau}F^0=F^0$. Hence $\hat{\tau}E\subseteq E$. For $r=0$, let E_1 denote $\langle E, F^0\langle a_0\rangle\rangle$. If $r>0$, let E_1 denote $\langle E, \hat{\tau}E\rangle$. In either case E_1 is a difference overfield of $F^0\langle a_0, \ldots, a_r\rangle$. G/E is primary and G_1/G is primary. Hence G_1/E is primary. Therefore E_1/E is primary. Thus $\mathscr{P}^*$ implies $\mathscr{P}$.

A difference kernel $\mathscr{K}$ is said to satisfy *property* $\mathscr{Q}^*$ if it satisfies $\mathscr{P}^*$ strengthened by replacement of the word "free" by "quasi-linearly disjoint."

(4.2) THEOREM. *$\mathscr{K}$ satisfies $\mathscr{Q}^*$ if and only if*

$$F^0\langle a_0, \ldots, a_r\rangle^*/F^0\langle a_0, \ldots, a_{r-1}\rangle^*$$

is primary.

Proof. Sufficiency is trivial with $G_1=F^0\langle a_0, \ldots, a_r\rangle^*$, $G=F^0\langle a_0, \ldots, a_{r-1}\rangle^*$, and (3.4(d), (c)).

Necessity is immediate from the following observation about field extensions: If L, L', M, M' are fields such that $L\subseteq L'\subseteq M'$, $L\subseteq M\subseteq M'$, L'/L and M/L are quasi-linearly disjoint, and M'/M is primary, then $(M, L')/M$ is primary, and hence by the quasi-linear disjointness, L'/L is primary (see (2.3)).

REMARK. By (3.5(c)), $F^0\langle a_0, \ldots, a_r\rangle / F^0\langle a_0, \ldots, a_{r-1}\rangle$ is primary implies $F^0\langle a_0, \ldots, a_r\rangle^* / F^0\langle a_0, \ldots, a_{r-1}\rangle^*$ is primary. The converse holds if $F^0\langle a_0, \ldots, a_{r-1}\rangle^*$ and $F^0\langle a_0, \ldots, a_r\rangle$ are quasi-linearly disjoint over $F^0\langle a_0, \ldots, a_{r-1}\rangle$.

The examples (4.5) and (6.3) establish the existence of kernels which satisfy $\mathscr{Q}^*$, and hence $\mathscr{P}^*$. The following is an example of a kernel which does not satisfy $\mathscr{P}^*$ (as interpreted for the case of characteristic 0).

EXAMPLE (3.8)(bis). Let b, K and F be as in (3.8). Let $F^0 = (K, \sigma)$ be the ordinary difference field obtained from F by deletion of τ. There exists a difference overfield H of F^0 whose underlying field is an algebraic closure of K. By (3.5(b)) H is inversive. There exists an element $a \in H$, $a \notin F^0$ such that $a^2 = b$. Thus we have the kernel $\mathscr{K} = (F^0\langle a\rangle, \tau)$, where τ is the transforming operator of F regarded as a difference automorphism of F^0.

Suppose $\mathscr{K}$ satisfies $\mathscr{P}^*$. Then there exist inversive difference overfields G_1 and G of $F^0\langle a\rangle$ and F^0 respectively such that G_1/G is primary. Thus $a \in G$. Furthermore, there exists a difference isomorphism $\bar{\tau}$ of G into G which coincides with τ on F^0. Then G together with $\bar{\tau}$ defines a difference overfield of F which contains a. But this is impossible, as demonstrated in the Example (3.8).

(4.3) THEOREM. *Any difference kernel which satisfies $\mathscr{P}^*$ has a generic prolongation which satisfies $\mathscr{P}^*$. If $\mathscr{K}_1$ is a generic prolongation of a difference kernel $\mathscr{K}$ and satisfies $\mathscr{P}^*$, then there exists a triple $(G, G_1, \bar{\tau})$ with respect to which $\mathscr{K}$ satisfies $\mathscr{P}^*$ and through which a generic prolongation $\mathscr{K}'$ of $\mathscr{K}$ can be obtained such that $\mathscr{K}'$ is equivalent to $\mathscr{K}_1$ in the sense of isomorphism. If a kernel satisfies $\mathscr{Q}^*$, then all generic prolongations of the kernel are equivalent and satisfy $\mathscr{Q}^*$.*

Proof. Suppose $\mathscr{K} = (F^0\langle a_0, \ldots, a_r\rangle, \tau)$ satisfies $\mathscr{P}^*$ with respect to $(G, G_1, \bar{\tau})$. Then by (3.6) (with G, $\bar{\tau}$, G_1 here corresponding to F, τ, G of (3.6) for both cases $r>0$ and $r=0$), there exist an inversive difference overfield G_2 of G_1 and an extension $\bar{\tau}_1$ of $\bar{\tau}$ such that $G_2 = \langle G_1, \bar{\tau}_1 G_1\rangle$ and G_2/G_1 is a primary extension. Let a_{r+1} denote $\bar{\tau}_1 a_r$. The contraction of $\bar{\tau}_1$ to an isomorphism

$$\tau_1 : F^0\langle a_0, \ldots, a_r\rangle \to F^0\langle a_1, \ldots, a_{r+1}\rangle$$

is an extension of τ which together with $F^0\langle a_0, \ldots, a_{r+1}\rangle$ forms a prolongation $\mathscr{K}_1$ of $\mathscr{K}$.

Since G and $F^0\langle a_0, \ldots, a_r\rangle^*$ are free over $F^0\langle a_0, \ldots, a_{r-1}\rangle^*$, $\bar{\tau}_1 G$ and $F^0\langle a_1, \ldots, a_{r+1}\rangle^*$ are free over $F^0\langle a_1, \ldots, a_r\rangle^*$. Furthermore, since G_1 and $\bar{\tau}_1 G_1$ are quasi-linearly disjoint, hence free, over $\bar{\tau}_1 G$, G_1 and $(\bar{\tau}_1 G)\langle a_{r+1}\rangle^*$ are free over $\bar{\tau}_1 G$. Hence by the corollary to (2.1), $F^0\langle a_0, \ldots, a_r\rangle^*$ and $F^0\langle a_1, \ldots, a_{r+1}\rangle^*$ are free over $F^0\langle a_1, \ldots, a_r\rangle^*$, and also G_1 and $F^0\langle a_0, \ldots, a_{r+1}\rangle^*$ are free over $F^0\langle a_0, \ldots, a_r\rangle^*$. Hence $\mathscr{K}_1$ is a generic prolongation of $\mathscr{K}$ which satisfies $\mathscr{P}^*$.

Suppose that $\mathscr{K}$ satisfies $\mathscr{Q}^*$. Then by (3.4(d)), (3.4(c)) and (4.2), $\mathscr{K}$ satisfies $\mathscr{P}^*$ with G and G_1 denoting $F^0\langle a_0, \ldots, a_{r-1}\rangle^*$ and $F^0\langle a_0, \ldots, a_r\rangle^*$ respectively. Then in the notation of the first paragraph it follows by (3.4(c), (d)) that $F^0\langle a_0, \ldots, a_{r+1}\rangle^* = G_2$. Thus $\mathscr{K}_1$ is a generic prolongation of $\mathscr{K}$ which satisfies $\mathscr{Q}^*$.

Now let $(F^0\langle a_0, \ldots, a_r, b\rangle, \eta)$ be another generic prolongation of $\mathscr{K}$. Then the inversive closure E of $F^0\langle a_0, \ldots, a_r, b\rangle$ is the free join of $F^0\langle a_0, \ldots, a_r\rangle^{*\prime}$ and $F^0\langle a_1, \ldots, a_r, b\rangle^{*\prime}$ over $F^0\langle a_1, \ldots, a_r\rangle^{*\prime}$, where $*\prime$ denotes inversive closure in E. Furthermore, by (3.1), $F^0\langle a_0, \ldots, a_r\rangle^{*\prime}$ may be identified with $F^0\langle a_0, \ldots, a_r\rangle^*$ and hence E may be regarded as a difference overfield of $F^0\langle a_0, \ldots, a_r\rangle^*$. By (3.4(c), (d)) η extends to an isomorphism $\bar{\eta}$ of $F^0\langle a_0, \ldots, a_r\rangle^{*\prime}$ onto $F^0\langle a_1, \ldots, a_r, b\rangle^{*\prime}$ such that $\bar{\tau}_1$ and $\bar{\eta}$ coincide on the elements of $F^0\langle a_0, \ldots, a_{r-1}\rangle^*$. Then by the preceding paragraph, together with (3.6), there exists a difference isomorphism ψ of G_2/G_1 onto E/G_1 such that $\psi\bar{\tau}_1\alpha=\bar{\eta}\psi\alpha$ for $\alpha \in G_1$. Hence the contraction of ψ to $F^0\langle a_0, \ldots, a_{r+1}\rangle$ establishes the equivalence in the sense of isomorphism of generic prolongations of $\mathscr{K}$.

Now to prove the second statement. Suppose $\mathscr{K}_1=(F^0\langle a_0, \ldots, a_r, a_{r+1}\rangle, \tau_1)$ is a generic prolongation of $\mathscr{K}$ which satisfies $\mathscr{P}^*$ with respect to, say, $(H_1, H_2, \bar{\tau}_1)$. Let G be the separable part of H_1 over $F^0\langle a_0, \ldots, a_{r-1}\rangle^*$. $\bar{\tau}_1 G \subseteq H_1$. For if $\alpha \in \bar{\tau}_1 G$, α is separably algebraic over $F^0\langle a_1, \ldots, a_r\rangle^*$ and hence also over H_1. Thus since H_2/H_1 is primary, $\alpha \in H_1$. Furthermore, if $r=0$, then α is separably algebraic over F^0, and hence $\bar{\tau}_1 G \subseteq G$. Let G_1 denote the separable part of H_1 over $F^0\langle a_0, \ldots, a_r\rangle^*$ for the case $r=0$, and if $r>0$, let G_1 denote $\langle G, \bar{\tau}_1 G\rangle$. Then $F^0\langle a_0, \ldots, a_r\rangle^* \subseteq G_1$, and $G \subseteq G_1 \subseteq H_1$. With the foregoing observations it is easily verified that $\mathscr{K}$ satisfies $\mathscr{P}^*$ with respect to $(G, G_1, \bar{\tau}_1|G)$.

Let G_2 denote $\langle G_1, \bar{\tau}_1 G_1\rangle$. Then $F^0\langle a_0, \ldots, a_r, a_{r+1}\rangle^* \subseteq G_2 \subseteq H_2$ and G_2 is inversive. We shall show that

(1) $$G_1 \text{ and } \bar{\tau}_1 G_1 \text{ are free over } \bar{\tau}_1 G.$$

With this it follows from the last statement of (3.6) that any generic prolongation of $\mathscr{K}$ constructed through $(G, G_1, \bar{\tau}_1|G)$ as in the proof of the first statement of (4.3) is equivalent to $\mathscr{K}_1$.

Since G_1 is algebraic over $F^0\langle a_0, \ldots, a_r\rangle^*$,

(2) $$G_1 \text{ and } F^0\langle a_0, \ldots, a_{r+1}\rangle^* \text{ are free over } F^0\langle a_0, \ldots, a_r\rangle^*.$$

By the assumption that $\mathscr{K}_1$ is a generic prolongation of $\mathscr{K}$ and (2) it follows by the corollary to (2.1) that $\bar{\tau}_1 G$ and $F^0\langle a_1, \ldots, a_{r+1}\rangle^*$ are free over $F^0\langle a_1, \ldots, a_r\rangle^*$, and

(3) $$G_1 \text{ and } \langle \bar{\tau}_1 G, F^0\langle a_1, \ldots, a_{r+1}\rangle^*\rangle \text{ are free over } \bar{\tau}_1 G.$$

$\bar{\tau}_1 G_1$ is algebraic over $F^0\langle a_1, \ldots, a_{r+1}\rangle^*$ and hence also over

$$\langle \bar{\tau}_1 G, F^0\langle a_1, \ldots, a_{r+1}\rangle^*\rangle.$$

Thus

(4) $$\langle G_1, F^0\langle a_1, \ldots, a_{r+1}\rangle^*\rangle \text{ and } \bar{\tau}_1 G_1 \text{ are free over } \langle \bar{\tau}_1 G, F^0\langle a_1, \ldots, a_{r+1}\rangle^*\rangle.$$

By (3) and (4) and (2.1), (1) holds.

A difference kernel $\mathscr{K}=(F^0\langle a_0,\dots,a_r\rangle,\tau)$ is said to satisfy the *stepwise compatibility condition* if the difference field $F^0\langle a_0,\dots,a_{r-1}\rangle$ satisfies the stepwise compatibility condition.

(4.4) THEOREM. *Any difference kernel which satisfies the stepwise compatibility condition also satisfies property* $\mathscr{P}^*$.

Proof. Suppose a kernel $(F^0\langle a_0,\dots,a_r\rangle,\tau)$ satisfies the stepwise compatibility condition. Then the difference field $F^0\langle a_0,\dots,a_{r-1}\rangle^*$ satisfies the stepwise compatibility condition. Furthermore, by (3.7) and (3.5(b)), there exists an inversive difference overfield G of $F^0\langle a_0,\dots,a_{r-1}\rangle^*$ which is an algebraic closure of $F^0\langle a_0,\dots,a_{r-1}\rangle^*$. Since any pair of extensions of $F^0\langle a_0,\dots,a_{r-1}\rangle^*$ is compatible we may assume that G and $F^0\langle a_0,\dots,a_r\rangle^*$ have a common difference overfield H and, furthermore, by the extension of isomorphisms theorem for difference fields (obvious generalization of [4, Theorem I, Chapter 9]) τ has an extension to an isomorphism $\bar\tau$ of G into a difference overfield $\bar H$ of H. If $r=0$, $\bar\tau$ is an automorphism of G since F is inversive and G is an algebraic closure of F^0. (See (3.5(b)).) If $r\geqq 1$, let G_1 denote $\langle G,\bar\tau G\rangle$ and if $r=0$ let G_1 denote $\langle G, F^0\langle a_0\rangle^*\rangle$. From the definition of G it follows that G and $F^0\langle a_0,\dots,a_r\rangle^*$ are free over $F^0\langle a_0,\dots,a_{r-1}\rangle^*$ and that G_1/G is regular, hence primary.

The stepwise compatibility condition is not a necessary condition for a kernel to satisfy property $\mathscr{P}^*$. In fact, the following example shows the existence of a kernel which satisfies $\mathscr{Q}^*$ and does not satisfy the stepwise compatibility condition.

(4.5) EXAMPLE. Let $F=(K,\sigma,\tau)$ and $F^0=(K,\sigma)$ be as in Example (3.8)(bis) (preceding (4.3)). Let x denote an element transcendental over K. Then σ may be extended to an automorphism σ' of $K(x)$, with $x\to x$, to define a difference field $F^0\langle x\rangle$. Thus the pair $(F^0\langle x\rangle,\tau)$ is a difference kernel $\mathscr{K}$ over F. Since the kernel of Example (3.8)(bis) does not satisfy property $\mathscr{P}^*$, it follows by (4.4) that F^0 does not satisfy the stepwise compatibility condition. On the other hand, $K(x)/K$ is primary. Hence by (4.2) and the remark following it, $\mathscr{K}$ satisfies $\mathscr{Q}^*$.

5. **Realizations of difference kernels.** Let $\mathscr{J}$ be an indexing set and $a=\{a_j : j\in\mathscr{J}\}$ an indexing of elements in a difference overfield G of a difference field F. A *specialization* of a over F is a difference homomorphism ϕ of $F\{a\}$ into a difference overfield of F such that ϕ leaves fixed the elements of F. The image $\phi a=\{\phi a_j : j\in\mathscr{J}\}$ is also called a specialization of a over F. A specialization ϕ is called *generic* if ϕ is an isomorphism. Otherwise it is termed *proper*.

Note. With a as above, if $\phi\colon a\to b$ is a generic specialization over F, then ϕ has a unique extension to a difference isomorphism ϕ' of $F\langle a\rangle$ onto $F\langle b\rangle$ (see (3.3)).

Let $\mathscr{K}=(F^0\langle a_0,\dots,a_r\rangle,\tau)$ be a kernel over the inversive difference field F (where the a_j are l-tuples). Let α denote an l-tuple in a difference overfield H of F and ξ that transforming operator of H which is the extension of σ_{i_0}. Then with the notation $\alpha_0=\alpha$, $\alpha_j=\xi^j\alpha$, $j=1,2,\dots$, we say that α is a *realization* of $\mathscr{K}$ in H over

F if the set $(\alpha_0, \ldots, \alpha_r)$ is a specialization over F^0 of $(a_0, \ldots, a_r)$, with $a_j^{(k)} \to \alpha_j^{(k)}$, $1 \leqq k \leqq l$, $0 \leqq j \leqq r$. We shall also speak of ξ as the realization of τ in H over F. α is called a *regular realization* of $\mathscr{K}$ if the specialization is generic. If there exists a sequence of kernels $\mathscr{K}_0, \mathscr{K}_1, \ldots, \mathscr{K}_h, \ldots$, with $\mathscr{K}_0 = \mathscr{K}$, such that, for each nonnegative integer h, $\mathscr{K}_{h+1}$ is a generic prolongation of $\mathscr{K}_h$ and α is a regular realization over F of $\mathscr{K}_h$, then we shall refer to α as a *principal realization* of $\mathscr{K}$. (This is the analogue to the definition of principal realization given in [4].)

REMARK. It is apparent that if β is an l-tuple of elements in a difference overfield H of an inversive difference field F, and if ξ is one of the transforming operators of H, then a kernel of length s is obtained by letting F^0 denote the difference field obtained from F by deletion of the contraction of ξ and letting ξ' denote the contraction of ξ to the difference isomorphism of $F^0\langle\beta, \xi\beta, \ldots, \xi^{s-1}\beta\rangle$ onto $F^0\langle\xi\beta, \xi^2\beta, \ldots, \xi^s\beta\rangle$. Clearly β is a regular realization of this kernel in H/F.

We shall say that two realizations α and β of a kernel $\mathscr{K}$ are *equivalent*, or isomorphic, *realizations* of $\mathscr{K}$ if the extensions $F\langle\alpha\rangle/F$ and $F\langle\beta\rangle/F$ are isomorphic, with $\alpha^{(k)} \to \beta^{(k)}$, $1 \leqq k \leqq l$.

(5.1) THEOREM. *The following statements about a difference kernel $\mathscr{K}$ are equivalent*:

(a) *$\mathscr{K}$ satisfies $\mathscr{P}^*$.*

(b) *$\mathscr{K}$ has a principal realization.*

(c) *$\mathscr{K}$ has a regular realization.*

Proof. (a) $\Rightarrow$ (b). Suppose $\mathscr{K}$ satisfies $\mathscr{P}^*$. Then by repeated application of (4.3), there exists a sequence of kernels $\mathscr{K}_0, \mathscr{K}_1, \ldots, \mathscr{K}_h, \ldots$, with $\mathscr{K}_0 = \mathscr{K}$, such that for each nonnegative integer h, $\mathscr{K}_{h+1}$ is a generic prolongation of $\mathscr{K}_h$ which satisfies $\mathscr{P}^*$. The union of the difference fields $F^0\langle a_0, \ldots, a_{r+h}\rangle$, $h = 0, 1, 2, \ldots$, together with the union of the isomorphisms τ_h, determines a structure of difference overfield H of F in which $a = a_0$ is a principal realization of $\mathscr{K}$ over F.

(b) $\Rightarrow$ (c). Trivial.

(c) $\Rightarrow$ (a). Suppose α is a regular realization of a kernel $\mathscr{K} = (F^0\langle a_0, a_1, \ldots, a_r\rangle, \tau)$. Let H denote the inversive closure of $F\langle\alpha\rangle$, and with T denoting that transforming operator of H which is the realization of τ, let H^0 denote the difference field obtained from H by deletion of T. Then regard T as a difference isomorphism of H^0 into H^0. H^0 is inversive. Let D denote the separable part of H^0 over $F^0\langle\alpha_0, \ldots, \alpha_{r-1}\rangle^*$. If $r=0$, let D_1 denote the separable part of H^0 over $F^0\langle\alpha_0, \ldots, \alpha_r\rangle^*$, and if $r \geqq 1$, let D_1 denote the compositum $\langle D, TD\rangle$ in H^0. D and $F^0\langle\alpha_0, \ldots, \alpha_r\rangle^*$ are free over $F^0\langle\alpha_0, \ldots, \alpha_{r-1}\rangle^*$, and H^0/D, and hence D_1/D, is primary. By (3.4(g), (b)) and the uniqueness of the separable part of a field extension, D is inversive, and for $r=0$, D_1 is inversive. For $r \geqq 1$, $D_1 = \langle D, TD\rangle$ is inversive (3.4(d), (c)). Let $\bar{T}$ denote the restriction of T to a difference isomorphism of D into H^0. If $r \geqq 1$, $D_1 = \langle D, \bar{T}D\rangle$ and, for $r=0$, $\bar{T}D \subseteq D$.

Since the specialization over F^0 of $(a_0, \ldots, a_r)$ onto $(\alpha_0, \ldots, \alpha_r)$ is generic, it extends uniquely to a difference isomorphism of $F^0\langle a_0, \ldots, a_r\rangle$ onto $F^0\langle \alpha_0, \ldots, \alpha_r\rangle$, which in turn extends to a difference isomorphism of $F^0\langle a_0, \ldots, a_r\rangle^*$ onto $F^0\langle \alpha_0, \ldots, \alpha_r\rangle^*$, and thence by construction to a difference isomorphism ϕ of a difference overfield G_1 of $F^0\langle a_0, \ldots, a_r\rangle^*$ onto D_1. Let G denote the difference subfield of G_1 whose image under ϕ is D. τ extends uniquely to a difference isomorphism $\bar{\tau}$ of G into G_1 such that, for $\gamma \in G$, $\phi\bar{\tau}\gamma = \overline{T}\phi\gamma$. Then with respect to $(G, G_1, \bar{\tau})$, $\mathscr{K}$ satisfies $\mathscr{P}^*$.

COROLLARY. *If a kernel $\mathscr{K}$ over F satisfies $\mathscr{Q}^*$, then $\mathscr{K}$ has a principal realization over F and all principal realizations of $\mathscr{K}$ are equivalent.*

Proof. The assumption on $\mathscr{K}$ implies that $\mathscr{K}$ satisfies $\mathscr{P}^*$ and hence has a principal realization. Suppose α and β are principal realizations of $\mathscr{K}$. Let $\mathscr{K}, \mathscr{K}_1, \mathscr{K}_2, \ldots$ and $\mathscr{K}, \mathscr{K}'_1, \mathscr{K}'_2, \ldots$ be the sequences of kernels associated with α and β respectively in the sense of the definition of principal realization. Since $\mathscr{K}$ satisfies $\mathscr{Q}^*$ it follows by application of (4.3) in an induction on h that $\mathscr{K}_h$ and $\mathscr{K}'_h$ are equivalent in the sense of isomorphism of kernels. Thus since for each nonnegative integer h, α is a regular realization of $\mathscr{K}_h$ and β is a regular realization of $\mathscr{K}'_h$ there exists, by a composition of maps, a difference isomorphism ϕ_h of $F^0\langle \alpha_0, \ldots, \alpha_{r+h}\rangle/F^0$ onto $F^0\langle \beta_0, \ldots, \beta_{r+h}\rangle/F^0$ such that $\alpha_j^{(k)} \to \beta_j^{(k)}$, $0 \leqq j \leqq r+h$, $1 \leqq k \leqq l$. The union of the ϕ_h defines a difference isomorphism of $F\langle\alpha\rangle$ onto $F\langle\beta\rangle$ with $\alpha \to \beta$.

REMARK. Every principal realization of a difference kernel is equivalent to one constructed as in the proof of (a) implies (b) of (5.1). This follows from (c) implies (a) of (5.1) and the second statement of (4.3).

(5.2) THEOREM. *If α is a principal realization of a kernel $\mathscr{K}$ then α is not a proper specialization over F of any other realization of $\mathscr{K}$.*

To prove the theorem we employ the following lemmas:

LEMMA 1. *Let L and M be fields, R and R_i, $i=1, 2, 3$, subrings of L such that $R=[R_1, R_2]$, R_3 is contained in $R_1 \cap R_2$, R_3 contains the identity element of L. Let η be a homomorphism of R into M such that the contractions of η to R_1 and R_2 are isomorphisms and such that the quotient fields in M of ηR_1 and ηR_2 are free over the quotient field of ηR_3. Then η is an isomorphism of R into M.*

Proof. For any subring P of L (or M), let P' denote its field of quotients in L (or M). Let S denote a set of generators of R_2 over R_3 and T a maximal algebraically independent subset of S over R_1. T is an algebraically independent set over R_3. Then ηT is an algebraically independent set over ηR_3 and hence over $(\eta R_3)'$. Then ηT is an algebraically independent set over $(\eta R_1)'$ since $(\eta R_1)'$ and $(\eta R_2)'$ are assumed to be free over $(\eta R_3)'$. Thus no nonzero element of $R_1[T]$ is mapped onto zero by η, and hence η may be extended to a homomorphism $\bar{\eta}$ of $R'_1(T)[S]$ onto $(\eta R_1)'(\eta T)[\eta S]$.

Since the elements of S are algebraic over $R_1'(T)$ it follows that $R_1'(T)[S]$ is a field which may be identified with $R_1'(S)=R'$ and hence $\bar{\eta}$ is an isomorphism of R' into M. Thus η is an isomorphism.

LEMMA 2. *Let* $\mathscr{K}_1=(F^0\langle a_0,\dots,a_s,a_{s+1}\rangle,\tau_1)$ *and* $\mathscr{K}'_1=(F^0\langle b_0,\dots,b_s,b_{s+1}\rangle,\tau_1')$, $s\geqq 0$, *be kernels such that* $\mathscr{K}_1$ *is a generic prolongation of* $\mathscr{K}=(F^0\langle a_0,\dots,a_s\rangle,\tau)$ *and such that there exists a specialization* ϕ *over* F^0 *of* $(b_0,\dots,b_{s+1})$ *onto* $(a_0,\dots,a_{s+1})$. *If* ϕ *contracts to a generic specialization of* $(b_0,\dots,b_s)$ *onto* $(a_0,\dots,a_s)$ *over* F^0 *then* ϕ *is generic.*

Proof. With ϕ as in the statement, the contraction of ϕ to

$$\phi_1\colon (b_0,\dots,b_s)\to(a_0,\dots,a_s)$$

extends to an isomorphism of $F^0\langle b_0,\dots,b_s\rangle$ onto $F^0\langle a_0,\dots,a_s\rangle$. It thus follows by the isomorphisms τ_1 and τ_1' that the contraction of ϕ to

$$\phi_2\colon (b_1,\dots,b_{s+1})\to(a_1,\dots,a_{s+1})$$

is an isomorphism of $F^0\{b_1,\dots,b_{s+1}\}$ onto $F^0\{a_1,\dots,a_{s+1}\}$. By (3.2), ϕ extends uniquely to a homomorphism ϕ' of $F^0\{b_0,\dots,b_{s+1}\}^*$ onto $F^0\{a_0,\dots,a_{s+1}\}^*$; and furthermore ϕ' contracts to an isomorphism of $F^0\{b_0,\dots,b_s\}^*$ onto $F^0\{a_0,\dots,a_s\}^*$ which is an extension of ϕ_1, and ϕ' contracts to an isomorphism of $F^0\{b_1,\dots,b_{s+1}\}^*$ onto $F^0\{a_1,\dots,a_{s+1}\}^*$ which is an extension of ϕ_2. ϕ' maps $F^0\{b_1,\dots,b_s\}^*$ onto $F^0\{a_1,\dots,a_s\}^*$. Since $\mathscr{K}_1$ is a generic prolongation of $\mathscr{K}$, it follows from the last statement of (3.3) and an application of Lemma 1 that ϕ' is an isomorphism. Hence ϕ is generic.

Proof of (5.2). Suppose α is a principal realization of $\mathscr{K}$ and β a realization of $\mathscr{K}$ such that there exists a specialization ϕ over F of β onto α with $\beta^{(k)}\to\alpha^{(k)}$, $1\leqq k\leqq l$. Then ϕ is generic if for each nonnegative integer j the contraction of ϕ to $\phi_j\colon F^0\{\beta_0,\dots,\beta_j\}\to F^0\{\alpha_0,\dots,\alpha_j\}$, $\beta_i\to\alpha_i$, $i=0,1,\dots,j$, is an isomorphism.

It is already apparent that ϕ_r (where r is the length of $\mathscr{K}$) is an isomorphism, since the composition of the specialization over F^0 of $(a_0,\dots,a_r)$ onto $(\beta_0,\dots,\beta_r)$ with the homomorphism ϕ_r agrees on the elements of $F^0\{a_0,\dots,a_r\}$ with the assumed generic specializations, over F^0, of $(a_0,\dots,a_r)\to(\alpha_0,\dots,\alpha_r)$.

Suppose now that for a nonnegative integer k, ϕ_{r+k} is an isomorphism. Then by Lemma 2, ϕ_{r+k+1} is an isomorphism, and hence by finite induction, ϕ_j is an isomorphism for $j=0,1,2,\dots$, which completes the proof.

W. Strodt and R. Cohn have obtained the analogues to Theorems I and V, Chapter 3, [4], needed in the proofs of the following remark and Corollary 1 to (6.1).

REMARK. By an argument analogous to the proof of Lemma VII, Chapter 6, [4], it may be shown that, for any l-tuple α of elements in a difference overfield of an inversive difference field F, there exists a kernel $\mathscr{K}$ such that α is the unique principal realization of $\mathscr{K}$ over F and every realization of $\mathscr{K}$ is a specialization of α over F.

A set T of elements in a difference field G is said to be *transformally independent* over a difference subfield F of G if the set of transforms of the elements of T in G is an algebraically independent set over the underlying field of F. Evidently, a subset T of an inversive difference field H is transformally independent over a difference subfield F of H if and only if T is transformally independent over F^*. We shall say that an indexing $a=\{a^{(i)} : i \in \mathscr{I}\}$ of elements in a difference overfield of a difference field F is *transformally independent* over F if and only if the $a^{(i)}$ are distinct and form a transformally independent set over F. The term "transformally independent," when written in connection with difference kernels, shall be read as "algebraically independent" when the kernel is interpreted as an ordinary difference kernel.

If for a kernel $\mathscr{K}=(F^0\langle a_0, \ldots, a_r\rangle, \tau)$, S is a subindexing of a_0, then let S_j denote the corresponding subindexing of a_j.

LEMMA. *Let $\mathscr{K}_1$ be a generic prolongation of a kernel $\mathscr{K}=(F^0\langle a_0, \ldots, a_r\rangle, \tau)$.*

(a) *If S is a subindexing of a_0 such that S_r is transformally independent over $F^0\langle a_0, \ldots, a_{r-1}\rangle$, then S_{r+1} is transformally independent over $F^0\langle a_0, \ldots, a_r\rangle$. Furthermore, $\bigcup_{i=0}^{r+1} S_i$ is a transformally independent set over F^0.*

(b) *If S is a subindexing of a_0 which is transformally independent over $F^0\langle a_1, \ldots, a_r\rangle$, then S is transformally independent over $F^0\langle a_1, \ldots, a_{r+1}\rangle$ and $\bigcup_{i=0}^{r+1} S_i$ is transformally independent over F^0.*

Proof of (a). By the isomorphism τ_1 and the assumption on S, S_{r+1} is transformally independent over $F^0\langle a_1, \ldots, a_r\rangle$ and hence also over $F^0\langle a_1, \ldots, a_r\rangle^*$. Thus, since the prolongation is generic, S_{r+1} is transformally independent over $F^0\langle a_0, a_1, \ldots, a_r\rangle^*$ and hence also over $F^0\langle a_0, a_1, \ldots, a_r\rangle$.

For each i, $0 \leqq i \leqq r+1$, S_i is transformally independent over $F^0\langle a_0, a_1, \ldots, a_{i-1}\rangle$. This is true by assumption for $i=r$, and by the preceding for $i=r+1$. For $i<r$, S_r is transformally independent over $F^0\langle a_{r-i}, \ldots, a_{r-1}\rangle$ and the composition of certain restrictions of τ is an isomorphism of $F^0\langle a_0, \ldots, a_i\rangle$ onto $F^0\langle a_{r-i}, \ldots, a_r\rangle$. Hence S_i is transformally independent over $F^0\langle a_0, \ldots, a_{i-1}\rangle$. Then for each i, $0 \leqq i \leqq r+1$, S_i is transformally independent over $F^0\langle S_0, \ldots, S_{i-1}\rangle$. Thus $\bigcup_{i=0}^{r+1} S_i$ is a transformally independent set over F^0.

Proof of (b). S is transformally independent over $F^0\langle a_1, \ldots, a_r\rangle^*$. Thus since the prolongation is generic, S is transformally independent over $F^0\langle a_1, \ldots, a_{r+1}\rangle^*$ and hence also over $F^0\langle a_1, \ldots, a_{r+1}\rangle$.

It follows from the assumption on S that $S=S_0$ is transformally independent over F^0. Suppose i is an integer, $0 \leqq i \leqq r$, such that $S_0 \cup S_1 \cup \cdots \cup S_i$ is transformally independent over F^0. Then, since the restriction of τ_1 to F^0 is an automorphism of F^0, $S_1 \cup S_2 \cup \cdots \cup S_{i+1}$ is transformally independent over F^0. But by the preceding paragraph S_0 is transformally independent over $F^0\langle S_1, S_2, \ldots, S_{i+1}\rangle$. Hence $S_0 \cup S_1 \cup \cdots \cup S_{i+1}$ is transformally independent over F^0. Thus in particular $\bigcup_{i=0}^{r+1} S_i$ is transformally independent over F^0.

The following theorem is used in the proof of (6.1).

(5.3) THEOREM. *Let α be a principal realization of a kernel*

$$\mathscr{K} = (F^0\langle a_0, \ldots, a_r\rangle, \tau).$$

(a) *If S is a subindexing of a_0 such that S_r is transformally independent over $F^0\langle a_0, \ldots, a_{r-1}\rangle$, then the corresponding subindexing T of α is transformally independent over F.*

(b) *If S is a subindexing of a_0 which is transformally independent over $F^0\langle a_1, \ldots, a_r\rangle$ then the corresponding subindexing T of α is transformally independent over F.*

Proof of (a). For each nonnegative integer h there exists a kernel

$$\mathscr{K}_h = (F^0\langle a_0, a_1, \ldots, a_r, \ldots, a_{r+h}\rangle, \tau_h)$$

obtained from $\mathscr{K}$ by a sequence of generic prolongations and such that α is a regular realization of $\mathscr{K}_h$. From part (a) of the lemma with an obvious induction we have $S \cup S_1 \cup \cdots \cup S_{r+h}$ is transformally independent over F^0 and hence (with τ' denoting the realization of τ) $T \cup \tau' T \cup \tau'^2 T \cup \cdots \cup \tau'^{r+h} T$ is transformally independent over F^0. Thus any finite collection of transforms of members of T whose orders relative to τ' are less than or equal to $r+h$ must be algebraically independent over the underlying field of F. This being true for each nonnegative integer h implies T is transformally independent over F.

Proof of (b). Analogous to that of (a).

6. **An existence theorem.** It has been established that every nontrivial ordinary algebraically irreducible difference polynomial has an abstract solution ([3, Theorem IV′]; [4, Theorem I, Chapter 6]). We shall see that this result cannot be extended to partial difference polynomials.

EXAMPLE (3.8)(bis). Let F and b be as in Example (3.8). If a is a solution for $P = y^2 - b$ regarded as a difference polynomial in the simple polynomial difference ring $F\{y\}$, then $a^2 = b$, which, as demonstrated in (3.8), is impossible.

(6.1) THEOREM. *Let F be an inversive difference field with two transforming operators. If there exists a difference field F^0 obtained from F by deletion of one of the transforming operators such that every pair of extensions of F^0 is compatible, then every nontrivial algebraically irreducible partial difference polynomial P in a polynomial difference ring $F\{y^{(1)}, \ldots, y^{(n)}\}$ has a solution η with the following properties: η is not a proper specialization over F of any solution of P; if a transform of $y^{(k)}$ appears effectively in P, then $\eta^{(1)}, \ldots, \eta^{(k-1)}, \eta^{(k+1)}, \ldots, \eta^{(n)}$ are distinct and form a transformally independent set over F; if Q is a nontrivial difference polynomial in $F\{y^{(1)}, \ldots, y^{(n)}\}$ which is annulled by η and effectively involves only those transforms of the $y^{(k)}$ which appear effectively in P, then Q is a multiple of P.*

Proof. Let σ_1 and σ_2 denote the transforming operators which define F on the field K, as well as their extensions which define $F\{y^{(1)}, \ldots, y^{(n)}\}$. Suppose (K, σ_1) is the difference field F^0 of the hypothesis. We first assume that for each k, $1 \leqq k \leqq n$, some transform of $y^{(k)}$ appears effectively in P. Since F is inversive we may, without loss of generality, assume that P is in standard position in $F\{y^{(1)}, \ldots, y^{(n)}\}$, i.e. there exist integers b and b', not necessarily distinct, such that a transform of $y^{(b)}$ of partial order zero with respect to σ_1 and a transform of $y^{(b')}$ of partial order zero with respect to σ_2 appear effectively in P. Let $y^{(k)}_{i,j}$, $i \geqq 0, j \geqq 0$, denote the transform of $y^{(k)}$ of partial order i with respect to σ_1 and partial order j with respect to σ_2. Let W denote the set of $y^{(k)}_{i,j}$ which appear effectively in P. For each k, $1 \leqq k \leqq n$, let q_k denote the maximum value of j such that, for some i, $y^{(k)}_{i,j} \in W$. For convenience of notation, let us assume the existence of an integer h, $0 \leqq h \leqq n$, such that $q_k = 0$ for $k \leqq h$ and $q_k > 0$ for $k > h$.

By a procedure analogous to that of [4, Theorem I, Chapter 6], we construct a difference kernel for P over F. We do this first with the assumption $h < n$. Let

$$Y = \{y^{(k)}_{i,j} : i = 0; k \leqq h \text{ implies } j \text{ equals } 0 \text{ or } 1; k > h \text{ implies } 0 \leqq j \leqq q_k\}.$$

The number of elements of Y is $t = 2h + \sum_{k=h+1}^{n} (q_k + 1)$. Let the elements of Y be ordered lexicographically on the (k, j) by the indexing

$$z = \left\{ z^{(u)} : 1 \leqq u \leqq t, z^{(u)} = y^{(k)}_{0,j}; \right.$$
$$\left. u = 2k - 1 + j \text{ when } k \leqq h; u = k + h + j + \sum_{s=h}^{k-1} q_s \text{ when } k > h \right\}.$$

Then a suitable contraction of σ_1 defines the ordinary t-fold polynomial difference ring $F^0\{z\}$. The set W is in $F^0\{z\}$. Thus P may be interpreted as an ordinary difference polynomial in $F^0\{z\}$. Let $\gamma = (\gamma^{(1)}, \ldots, \gamma^{(t)})$ denote a generic zero of a principal component of the manifold of P over $F^0\{z\}$ (the existence of which is asserted by [4, Theorem I, Chapter 6]).

Let z_0 be that subindexing of z consisting of all coordinates of z except those of the form $y^{(k)}_{0,j}$ with $j = 1$ when $k \leqq h$ and $j = q_k$ when $k > h$. Let z_1 be that subindexing of z consisting of all coordinates of z except those of the form $y^{(k)}_{0,j}$ with $j = 0$. Both z_0 and z_1 have $l = t - n$ coordinates and the union of their sets of coordinates is the set of coordinates of z. With respect to the ordering of the coordinates of z_0 and of z_1 induced by the ordering of the coordinates of z, if the vth coordinate of z_0 in $y^{(k)}_{0,j}$, then the vth coordinate of z_1 is $y^{(k)}_{0,j+1}$ for $1 \leqq v \leqq l$.

Replace the coordinates of z in z_0 by the corresponding coordinates of γ. Let the resulting indexing be denoted by a_0. Form a_1 similarly from z_1.

a_0 is transformally independent over F^0. Let k' denote any one of the integers $h < k' \leqq n$. Then there exists a nonnegative integer i' dependent upon k' such that $y^{(k')}_{i',q_{k'}}$ appears effectively in P; that is, for $u' = k' + h + q_{k'} + \sum_{s=h}^{k'-1} q_s$, $\sigma_1^{i'} z^{(u')}$ appears effectively in P. Hence, by the definition of γ, it follows that $\gamma^{(1)}, \ldots, \gamma^{(u'-1)}, \gamma^{(u'+1)}$,

$\ldots, \gamma^{(t)}$ are distinct and form a transformally independent set over F^0. But u' is not in the domain of z_0. Hence a_0 is transformally independent over F^0.

We see also that a_1 is transformally independent over F^0. By the assumption that P is in standard position in $F\{y^{(1)}, \ldots, y^{(n)}\}$, there exists an integer k'', $1 \leqq k'' \leqq n$, such that for some nonnegative integer i'', $y^{(k'')}_{i'',0}$ appears effectively in P; that is, for $u'' = 2k'' - 1$ if $k'' \leqq h$ or $u'' = k'' + h + \sum_{s=h}^{k''-1} q_s$ if $k'' > h$, $\gamma^{(1)}, \ldots, \gamma^{(u''-1)}$, $\gamma^{(u''+1)}, \ldots, \gamma^{(t)}$ are distinct and form a transformally independent set over F^0, and hence, by the definition of z_1, it follows that a_1 is transformally independent over F^0.

Let σ_1' denote the difference operator of $F^0\langle\gamma\rangle$. Since a_0 and a_1 are transformally independent over F^0 the automorphism σ_2 of K can be extended to an isomorphism τ of the underlying field of $F^0\langle a_0\rangle$ onto the underlying field of $F^0\langle a_1\rangle$ in such a way that $\tau(\sigma_1')^i a_0^{(v)} = (\sigma_1')^i a_1^{(v)}$, $i = 0, 1, 2, \ldots$, $1 \leqq v \leqq l$. But then τ is obviously a difference isomorphism of $F^0\langle a_0\rangle$ onto $F^0\langle a_1\rangle$ which contracts to σ_2 on F^0 and is such that $\tau a_0^{(v)} = a_1^{(v)}$, $1 \leqq v \leqq l$. Thus for the case $h < n$ we have the desired kernel $\mathscr{K} = (F^0\langle a_0, a_1\rangle, \tau)$.

If $h = n$, then P may be interpreted as an ordinary difference polynomial in $F^0\{y^{(1)}, \ldots, y^{(n)}\}$. Letting $a_0 = (a^{(1)}, \ldots, a^{(n)})$ be a generic zero for a principal component of the manifold of P over $F^0\{y^{(1)}, \ldots, y^{(n)}\}$, and τ denote the difference automorphism of F^0 which coincides with σ_2, we again have the desired kernel $\mathscr{K} = (F^0\langle a_0\rangle, \tau)$.

By the assumption that any pair of extensions of F^0 is compatible and by [4, Theorem X, Chapter 7], the kernel of length 1 constructed above satisfies the stepwise compatibility condition. The compatibility condition on F^0 trivially implies the stepwise compatibility condition on the kernel of length 0. Hence, in either case, by (4.4) and (5.1) there exists a principal realization α of the kernel $\mathscr{K}$.

Since for each k, $1 \leqq k \leqq n$, there exists a coordinate $a_0^{(v_k)}$ of a_0 which is assigned to $y^{(k)}_{0,0}$, a solution for P over $F\{y^{(1)}, \ldots, y^{(n)}\}$ may be obtained by assigning to $y^{(k)}$, for each k, that coordinate of α which corresponds to $a_0^{(v_k)}$. We denote this solution by $\eta = (\eta^{(1)}, \ldots, \eta^{(k)}, \ldots, \eta^{(n)})$ with $\eta^{(k)} = \alpha^{(v_k)}$.

Suppose Q is a nontrivial difference polynomial in $F\{y^{(1)}, \ldots, y^{(n)}\}$ whose indeterminates consist of a subset of W and such that Q is annulled by η. Then, since α is a regular realization of $\mathscr{K}$, Q may be interpreted as a polynomial in $F^0\{z\}$ which is annulled by γ. Since P is in standard position, P effectively involves an indeterminate of the form $y^{(k)}_{0,j} = z^{(\bar{u})}$. If the resultant R over K of P and Q with respect to $y^{(k)}_{0,j}$ is not zero, then R is a nontrivial polynomial effectively involving a subset of the elements of W excluding $y^{(k)}_{0,j}$ and R is annulled by γ. But then either $\gamma^{(1)}, \ldots, \gamma^{(\bar{u}-1)}, \gamma^{(\bar{u}+1)}, \ldots, \gamma^{(t)}$ is a transformally dependent set over F^0; or $\gamma^{(1)}, \ldots, \gamma^{(\bar{u}-1)}, \gamma^{(\bar{u}+1)}, \ldots, \gamma^{(t)}$ are distinct and form a transformally independent set over F^0 and the effective order of $F\langle\gamma\rangle$ over $F\langle\gamma^{(1)}, \ldots, \gamma^{(\bar{u}-1)}, \gamma^{(\bar{u}+1)}, \ldots, \gamma^{(t)}\rangle$ is less than the effective order of P in $z^{(\bar{u})}$. In either case we are led to a contradiction to the definition of γ. Therefore $R \equiv 0$, and, since P is irreducible, Q is a multiple of P.

For each k, $1 \leqq k \leqq n$, $\eta^{(k)}$ is transformally algebraic over $F\langle \eta^{(1)}, \ldots, \eta^{(k-1)}, \eta^{(k+1)}, \ldots, \eta^{(n)} \rangle$ since P effectively involves a transform of $y^{(k)}$ and is annulled by η, and yet, with P considered as a difference polynomial in $y^{(k)}$ with coefficients in $F\{y^{(1)}, \ldots, y^{(k-1)}, y^{(k+1)}, \ldots, y^{(n)}\}$, it follows by the preceding result that these coefficients are not annulled by $\eta^{(1)}, \ldots, \eta^{(k-1)}, \eta^{(k+1)}, \ldots, \eta^{(n)}$.

To see that $\eta^{(1)}, \ldots, \eta^{(k-1)}, \eta^{(k+1)}, \ldots, \eta^{(n)}$ are distinct and form a transformally independent set over F, consider the kernel $\mathscr{K}$ above. If $h < k \leqq n$, let S denote the subindexing of a_0 defined on

$$\{1, 2, \ldots, h, h+q_{h+1}, h+q_{h+1}+q_{h+2}, \ldots, h+q_{h+1}+\cdots+q_{k-1}, \\ h+q_{h+1}+\cdots+q_{k+1}, \ldots, h+q_{h+1}+\cdots+q_n\}.$$

If $k \leqq h \leqq n$, let S denote that subindexing of a_0 defined on $\{1, \ldots, k-1, k+1, \ldots, h, h+q_{h+1}, h+q_{h+1}+q_{h+2}, \ldots, h+q_{h+1}+\cdots+q_n\}$.

In the first case $\tau S = S_1$ is a subindexing of a_1 which is transformally independent over $F^0\langle a_0 \rangle$. This follows from the definition of γ and the effective presence in P of $y^{(k)}_{i,q_k}$ for some i. Thus (5.3(a)) is applicable.

In the second case, since for some i, $y^{(k)}_{i,0}$ appears effectively in P, S is transformally independent over $F^0\langle a_1 \rangle$ when $h < n$, and if $h = n$, S is transformally independent over F^0. Thus (5.3(b)) is applicable. In either case the subindexing T of α corresponding to S is transformally independent over F. Since the coordinates of η other than $\eta^{(k)}$ transform under suitably many applications of the extension of σ_2 to distinct coordinates of T, it follows that $\eta^{(1)}, \eta^{(2)}, \ldots, \eta^{(k-1)}, \eta^{(k+1)}, \ldots, \eta^{(n)}$ are distinct and form a transformally independent set over F.

Now to show that η is not a proper specialization over F of any solution of P. Suppose $\lambda = (\lambda^{(1)}, \ldots, \lambda^{(n)})$ is a solution of P over $F\{y^{(1)}, \ldots, y^{(n)}\}$ such that the n-tuple λ specializes over F to the n-tuple η. We present the argument for the case $h < n$. That for $h = n$ is the same except for notational changes.

Let β denote the l-tuple of those transforms of the coordinates of λ which are substituted into the coordinates of z_0, with $\beta^{(v)}$ substituted into $z_0^{(v)}$, $1 \leqq v \leqq l$. Let β_1 be defined as was β, with z_0 replaced by z_1 in the definition. We construct the kernel $\overline{\mathscr{K}}$ by contracting the extension of σ_2 in the definition of $F\langle \lambda \rangle$ to a difference isomorphism $\bar{\tau}$ of $F^0\langle \beta \rangle$ onto $F^0\langle \beta_1 \rangle$. With the obvious correspondence of coordinates, α is a specialization over F of β, and hence, with the appropriate identification of coordinates as indicated by the definitions of z, z_0 and $z_1, (\alpha, \alpha_1)$ is a specialization over F^0 of (β, β_1). This specialization over F^0 must be generic since (α, α_1) is equivalent to a generic zero of a principal component of the manifold of P over F^0. Hence β is a regular realization of $\mathscr{K}$ in $F\langle \lambda \rangle / F$. But then, by (5.2), α is a generic specialization of β over F, and thus η is a generic specialization of λ over F.

To complete the proof, we relax the above restriction that each $y^{(k)}$ has transforms which appear effectively in P. We may proceed as in the first paragraph of [4, p. 170], with λ interpreted as a solution of the kind whose existence has been established above for the restricted case. Verification that the three conclusions of the theorem hold is then straightforward. Lemma 1 of (5.2) may be used to show that η is not a proper specialization over F of any other solution of P.

COROLLARY 1. *If F and P are as in the theorem, then P has at most a finite number of isomorphically distinct solutions of the type described in the theorem.*

Proof. Theorems III and V, Chapter 3, and Theorem III, Chapter 4, [4], generalize to partial difference rings. Thus $F\{y^{(1)}, \dots, y^{(n)}\}$ is a Ritt difference ring, and hence the manifold $M\{P\}$ of the perfect difference ideal $\{P\}$ has a unique irredundant representation as the union of a finite number of irreducible manifolds. Any solution of P which is not a proper specialization of any other solution of P is a generic zero of one of these irreducible components of $M\{P\}$, and all generic zeros for each such component of $M\{P\}$ are equivalent.

COROLLARY 2. *The conclusion of* (6.1) *holds if* $F=(K, \sigma_1, \sigma_2)$ *is inversive and K is separably algebraically closed or algebraically closed.*

Proof. By the fundamental theorem of compatibility [4, Theorem I, p. 198] F satisfies the hypothesis of (6.1).

A weakening of the hypothesis of (6.1) leads to the following theorem, the statements of which are implied by the stepwise compatibility condition (see (3.7)). The Example (3.9) shows that statement (a) does not imply the stepwise compatibility condition for F^0.

(6.2) THEOREM. *For a difference field F with two transforming operators, the following statements are equivalent*:

(a) *F may be extended to a difference field whose underlying field is the algebraic closure of that of F.*

(b) *Every nontrivial algebraically irreducible partial difference polynomial P in a polynomial difference ring* $F\{y^{(1)}, \dots, y^{(n)}\}$ *has a solution* η *with the properties stated in* (6.1).

(c) *If a is any element separably algebraic and normal over the underlying field of F, F may be extended to a difference field* $F\langle a\rangle$.

Proof. (a) $\Rightarrow$ (b). Let G denote a difference overfield of F defined on the algebraic closure of the underlying field K of F. By (3.5(a)) the inversive closure G^* of G is algebraically closed. Let P be a nontrivial algebraically irreducible partial difference polynomial in $F\{y^{(1)}, \dots, y^{(n)}\}$ and P' a nontrivial irreducible factor of P in $G^*\{y^{(1)}, \dots, y^{(n)}\}$. Let λ be a solution of P' of the type whose existence is asserted by Corollary 2 to (6.1). Then λ is a solution of $P \in F\{y^{(1)}, \dots, y^{(n)}\}$. Let M denote an irreducible component of the manifold of P over $F\{y^{(1)}, \dots, y^{(n)}\}$ which contains λ and let η be a generic zero of M. Then η is a solution of P which specializes over F to λ, and η is not a proper specialization over F of any other solution of P. Since every indeterminate $y_{i,j}^{(k)}$ which appears effectively in P also appears in P', it follows that for each k, $1 \leqq k \leqq n$, such that some transform of $y^{(k)}$ appears effectively in P, we have by Corollary 2 to (6.1) that $\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(k-1)}, \lambda^{(k+1)}, \ldots, \lambda^{(n)}$ are distinct and form a transformally independent set over G^* and hence also over F, and thus $\eta^{(1)}, \ldots, \eta^{(k-1)}, \eta^{(k+1)}, \ldots, \eta^{(n)}$ are distinct and form a transformally independent set over F.

Let W be the set of those $y_{i,j}^{(k)}$ which appear effectively in P and let Q be a nontrivial difference polynomial in $F\{y^{(1)}, \ldots, y^{(n)}\}$ annulled by η and effectively involving only those $y_{i,j}^{(k)}$ in W. Let R be the resultant over K of P and Q with respect to one of the elements $y_{i',j'}^{(k')}$ of W. Then R is identically zero, for otherwise, since R is annulled by η and hence by λ, R regarded as a nontrivial difference polynomial over G^* is, by Corollary 2 to (6.1), a multiple of P'. But this is impossible since P' effectively involves $y_{i',j'}^{(k')}$ and R does not. Therefore P and Q have a nontrivial common divisor over K and, hence, by the irreducibility of P over F, Q is a multiple of P.

(b) $\Rightarrow$ (c) is trivial.

To prove (c) $\Rightarrow$ (a), note first that, by the simplicity of finitely generated separably algebraic field extensions it follows from (c) that for elements $a_1, \ldots, a_r$ in an overfield of the underlying field K of F, where the a_i are separably algebraic and normal over K, one can extend F to a difference field $F\langle a_1, \ldots, a_r\rangle$.

We now show that (c) implies F can be extended to a difference field defined on the separable closure of K. (This will complete the proof if the characteristic is 0, or if the characteristic is positive and K is perfect.) Let L_0 be the separable part of an algebraic closure L of K. Let $\mathcal{S}$ be the collection of finite normal extensions of K in L_0. For each member of $\mathcal{S}$ select one simple generator and let S be this collection of elements of L_0. Let T be a transformally independent set over F, where the cardinality of T equals that of S. Assume further that a 1-1 correspondence $\alpha^{(i)} \leftrightarrow y^{(i)}$ between the members of S and T has been specified. For each $y^{(i)} \in T$, let $P^{(i)}(y^{(i)})$ denote a zero order difference polynomial in $F\{T\}$ (zero order with respect to each transforming operator) which, when regarded as an algebraic polynomial over K, is a minimal polynomial belonging to $\alpha^{(i)}$, and let ϕ denote the system in $F\{T\}$ consisting of the $P^{(i)}(y^{(i)})$.

If there exists a solution over F for the system ϕ, then there exists a difference overfield G of F with underlying field L_0. To see this, suppose ϕ has a solution $S'=\{\beta^{(i)}\}$. Then the underlying field M of $F\langle S'\rangle$ is separable algebraic over K. For suppose $\eta \in M$. Then there exists a field K' between K and M generated over K by finitely many transforms of finitely many elements of S' and such that $\eta \in K'$. Since $\beta^{(i)}$ is separably algebraic over K, any transform $\rho\beta^{(i)}$ is separably algebraic over ρK and hence also over K. Thus K' is a separable algebraic extension of K, and hence η is separably algebraic over K.

Thus we may without loss of generality assume $K \subseteq M \subseteq L_0$. Indeed $M=L_0$. For if $\gamma \in L_0$, then $K(\gamma)/K$ has a finite separable normal closure N/K in L_0/K. There exists an element $\alpha^{(i)}$ in S which generates N over K, that is, N is a splitting field over K for $P^{(i)}(y^{(i)})$, and hence, by the uniqueness of splitting fields, $K(\gamma) \subseteq K(\beta^{(i)}) \subseteq M$. Thus $L_0 \subseteq M$, which gives the desired equality.

To establish that (c) implies ϕ has a solution we use the following criterion: Let U be a transformally independent set over the difference field F. Then a system Σ of difference polynomials in $F\{U\}$ has a solution over F if and only if the identity element is not in the perfect difference ideal $\{\Sigma\}$ in $F\{U\}$.

Necessity is obvious. Suppose $1 \notin \{\Sigma\}$. It can be established by a standard argument using Zorn's lemma that there exists a maximal perfect difference ideal ψ in $F\{U\}$ containing the elements of Σ, but not containing the identity element. Lemma I, Chapter 3 of [4] generalizes to the result: If A and B are sets of elements in a partial difference ring D, then $\{A\}\{B\}\subseteq\{AB\}$. With this one routinely establishes that ψ is a reflexive prime difference ideal in $F\{U\}$. Hence the difference ring $F\{U\}/\psi$ of residue classes is an integral domain. Furthermore the difference quotient field H of $F\{U\}/\psi$ "contains" F as a difference subfield. The set $\bar{U}$ of residue classes of the elements of U is a generic zero of ψ in H/F and a fortiori is a solution of Σ.

Now suppose ϕ has no solution. Then by the above criterion, ϕ generates the unit ideal in $F\{T\}$, and hence there exists a finite subset T' of T such that the subset ϕ' of ϕ corresponding to T' generates the unit ideal in $F\{T'\}$, that is, ϕ' is a finite set of irreducible, normal, separable difference polynomials over F which, by the above criterion, has no solution over F. But by the first paragraph this is impossible in the presence of condition (c). Hence condition (c) implies that ϕ has a solution and F extends to a difference field G on L_0.

It remains to show that, if F is of positive characteristic p, G may be extended to a difference field whose underlying field is the algebraic closure of that of F. This may be accomplished by introducing the transforming operator $\tau: b \to b^p$ on L_0. τ commutes with each of the transforming operators of G and τ transforms K into K. Thus τ together with G and F determines the new difference fields G' and F' on L_0 and K respectively such that G' is a difference overfield of F'. Evidently the underlying field of the inversive closure G'^* of G' is perfect and hence contains a perfect closure L_1 of L_0 which, of course, is an algebraic closure of K. Hence the defining operators of G'^* transform L_1 into L_1, and thus the operators which define G may be extended to form the desired difference field H on L_1.

Remark. Evidently, the equivalence of conditions (a) and (c) holds for difference fields with m operators.

Although there may exist a difference polynomial over a difference field F which has no solution (e.g. Example (3.8)(bis) preceding (6.1)) there may still exist a polynomial over F which has a solution of the type in Theorem (6.1), e.g. the trivial polynomial $y_{0,0}$ in $F\{y\}$.

The following example shows that there exists a difference polynomial over an inversive partial difference field which is of partial order greater than zero with respect to each transforming operator and has a solution of the type described in (6.1), though the ground field need not satisfy condition (a) of (6.2) (see (3.8)).

(6.3) Example. Let $F=(K, \sigma_1, \sigma_2)$ be an inversive partial difference field, $P=y_{10}+y_{01}+y_{12}$ be a difference polynomial in a simple polynomial difference ring $F\{y\}$, $F^0=(K, \sigma_1)$, and (a_{00}, a_{01}, a_{02}) denote a generic zero of a principal component of the manifold of P where P is regarded as an ordinary difference polynomial in $F^0\{y_{00}, y_{01}, y_{02}\}$. Then there exists a difference isomorphism τ of $F^0\langle a_{00}, a_{01}\rangle$ onto $F^0\langle a_{01}, a_{02}\rangle$ such that $a_{00}\to a_{01}$ and $a_{01}\to a_{02}$ and whose contraction to K is σ_2. Then $(F^0\langle a_{00}, a_{01}, a_{02}\rangle, \tau)$ is a difference kernel $\mathscr{K}$.

Since

$$\text{ord } F^0\langle a_{00}, a_{01}, a_{02}\rangle / F^0\langle a_{00}, a_{01}\rangle = 1 \qquad [4, \text{Theorem I, p. } 162],$$

the element a_{02} is transcendental over the underlying field of $F^0\langle a_{00}, a_{01}\rangle$. The underlying field of $F^0\langle a_{00}, a_{01}, a_{02}\rangle$ is a simple transcendental extension, and hence a primary extension, of the underlying field of $F^0\langle a_{00}, a_{01}\rangle$. Hence by (4.2) and the succeeding remark, $\mathscr{K}$ satisfies $\mathscr{Q}^*$. Thus by the corollary to (5.1), $\mathscr{K}$ has a principal realization and all principal realizations of $\mathscr{K}$ are equivalent. If α is a principal realization of $\mathscr{K}$ then α is a solution for P satisfying the properties stated in (6.1).

References

1. A. E. Babbitt, Jr., *Finitely generated pathological extensions of difference fields*, Trans. Amer. Math. Soc. **102** (1962), 63–81. MR **24** #A3160.

2. A. Bialynicki-Birula, *On Galois theory of fields with operators*, Amer. J. Math. **84** (1962), 89–109. MR **25** #5060.

3. R. M. Cohn, *Manifolds of difference polynomials*, Trans. Amer. Math. Soc. **64** (1948), 133–172. MR **10**, 4.

4. ———, *Difference algebra*, Interscience Tracts in Pure and Appl. Math., no. 17, Interscience, New York, 1965. MR **34** #5812.

5. H. F. Kreimer, *The foundations for an extension of differential algebra*, Trans. Amer. Math. Soc. **111** (1964), 482–492. MR **28** #3034.

6. Serge Lang, *Introduction to algebraic geometry*, Interscience Tracts in Pure and Appl. Math., no. 5, Interscience, New York, 1958. MR **20** #7021.

7. W. C. Strodt, *Systems of algebraic partial difference equations*, Unpublished Master's Essay, Columbia University, New York, 1937.

8. O. Zariski and P. Samuel, *Commutative algebra*. Vol. 1, University Series in Higher Math., Van Nostrand, Princeton, N. J., 1958. MR **19**, 833.

Hobart and William Smith Colleges,
Geneva, New York 14456