FINITELY GENERATED PATHOLOGICAL EXTENSIONS OF DIFFERENCE FIELDS

BY

ALBERT E. BABBITT, JR.

1. **Introduction.** The study of algebraic difference equations has led to the discovery of difference field extensions which possess properties quite unlike those exhibited by analogous structures in classical Galois theory or the Galois theory for differential fields developed by E. R. Kolchin [13]. Specifically, J. F. Ritt [15] pointed out that a difference field $\mathfrak{F}$(1) may have extensions $\mathfrak{G}$ and $\mathfrak{K}$ which cannot both be embedded in any one extension of $\mathfrak{F}$, while R. M. Cohn [3] showed that $\mathfrak{F}$ may have a proper extension $\mathfrak{K}$ which does not admit two distinct $\mathfrak{F}$-isomorphisms into any extension of $\mathfrak{F}$. In the first case, $\mathfrak{G}$ and $\mathfrak{K}$ are called *incompatible* extensions of $\mathfrak{F}$; in the second case, $\mathfrak{K}$ is termed a *monadic* extension of $\mathfrak{F}$. For the sake of brevity, we use the term *pathological* to designate an extension which either is incompatible with some other extension of $\mathfrak{F}$ or is a monadic extension of $\mathfrak{F}$.

The existence of pathological extensions has implications for both the abstract and the analytic theory of difference equations [5]. The fundamental importance of incompatible extensions, for example, becomes clear when one examines the body of theorems in difference algebra concerning specializations. Indeed the standard theorems of algebraic geometry regarding specializations go over to difference algebra only if one imposes conditions precluding incompatibility [6]. The existence of monadic extensions on the other hand, threatens seriously to complicate the task of constructing a Galois theory for difference fields.

Thus the significance of pathological extensions to difference algebra is unquestionably great, but our knowledge of these extensions is quite limited. Cohn [5] has shown that a difference field admits finitely generated pathological extensions only if it admits such extensions of order zero, i.e. algebraic over the ground field. Hence fields which are algebraically closed admit no finitely generated pathological extensions. These are the only general results regarding finitely generated pathological extensions yet obtained.

In view of Cohn's results it is natural to inquire if the existence of finitely generated pathological extensions of order zero in turn implies the existence of pathological extensions which are of finite degree over the ground field. Our primary purpose in this paper is to investigate this supposition; our principal result is that this supposition is true.

In §2 we prove a decomposition theorem for normal extensions of order

Received by the editors June 1, 1960.

(1) All fields are assumed to be of characteristic zero.

zero and apply this theorem to prove the aforementioned principal result. An extension $\mathfrak{F}\langle\alpha\rangle$ is said to be a *benign extension* of $\mathfrak{F}$ if $\mathfrak{F}(\alpha)$ is a normal extension of $\mathfrak{F}$ and if $[\mathfrak{F}(\alpha):\mathfrak{F}]=$l.d. $(\mathfrak{F}\langle\alpha\rangle/\mathfrak{F})$ [8]. Roughly speaking, the decomposition theorem asserts that a normal extension of order zero is given by an extension of limit degree one, i.e. an extension of finite degree, followed by a series of benign extensions. As a consequence of this theorem we deduce that the classical difference field of rational functions of one variable with complex coefficients has no finitely generated pathological extensions.

In §3 we begin an investigation of extensions of order zero and limit degree one. For a given normal field extension $\mathfrak{G}$ of a difference field $\mathfrak{F}$, the transforming operation on $\mathfrak{F}$ may be extended to $\mathfrak{G}$ in $[\mathfrak{G}:\mathfrak{F}]$ ways if any. A theorem is proved giving the number of distinct (up to isomorphism) classes of such extensions in terms of the number of automorphisms of the various extensions.

In §4 we apply previous results to the study of pathological extensions of order zero and limit degree one. It is shown that the (algebraic) Galois group of a monadic extension admits an automorphism leaving no nontrivial element fixed.

In §5 we examine the intermediate fields of an extension of order zero and limit degree one.

While our notation and nomenclature follow closely that given in Cohn [3; 5; 8], several points need clarification. A *difference field* is an ordered pair $(\mathfrak{F}, \sigma)$, the first element of which is a field(1); the second, a nonzero endomorphism of the field, called the *transforming map*. If σ is an automorphism, $(\mathfrak{F}, \sigma)$ is called an *inversive* difference field. Unless the notation is inconvenient or ambiguous, we shall write $\mathfrak{F}$ as an abbreviation for $(\mathfrak{F}, \sigma)$. $(\mathfrak{G}, \mu)$ is an extension of $(\mathfrak{F}, \sigma)$ if $\mathfrak{F}\subset\mathfrak{G}$ and the restriction of μ to $\mathfrak{F}$ is σ. For simplicity, we shall frequently use the same symbol for the transforming map on $\mathfrak{F}$ and $\mathfrak{G}$.

An *inversive closure* of a difference field $(\mathfrak{F}, \sigma)$ is an extension of $(\mathfrak{F}, \sigma)$ which is minimal in the set of extensions of $(\mathfrak{F}, \sigma)$ which are inversive difference fields. An inversive closure $(\mathfrak{G}, \sigma)$ of $(\mathfrak{F}, \sigma)$ has the property that if $\alpha\in\mathfrak{G}$, then $\sigma^{m(\alpha)}(\alpha)\in\mathfrak{F}$ for a sufficiently large non-negative integer $m(\alpha)$. The existence of inversive closures is proved in Cohn [4].

Many terms, particularly "field," "extension," "isomorphism," "automorphism," and "group" are used both in their algebraic sense and in the sense of difference algebra. Usually the context will indicate the usage intended, but if necessary to avoid confusion we use an adjective, usually "algebraic," to indicate the former meaning is intended, or one of "difference" or "transformal" to signify the latter.

The author wishes to thank Professors R. M. Cohn and E. R. Kolchin for their many helpful suggestions during the preparation of this paper. In particular, the former is responsible for the observation that Theorems 2.10 and 2.11 are consequences of the decomposition theorem.

2. **Finitely generated extensions of order zero.** Throughout this section

we assume that every extension is finitely generated and of order zero. As shown in the proof of Theorem 1 of Cohn [5], every such extension is simply generated.

If $\mathfrak{G}$ is an extension of the difference field $\mathfrak{F}$ and α is an element of $\mathfrak{G}$, then α is called *normal* over $\mathfrak{F}$ if $\mathfrak{F}(\alpha)$ is a normal field extension of $\mathfrak{F}$. We say the difference field $\mathfrak{G}$ is a *normal extension* of $\mathfrak{F}$ if it is normal in the usual sense. It is clear that if $\alpha\in\mathfrak{G}$ is normal over $\mathfrak{F}$, then $\mathfrak{F}\langle\alpha\rangle$ is a normal extension of $\mathfrak{F}$.

Let $\mathfrak{G}=\mathfrak{F}\langle\alpha\rangle$ and suppose $[\mathfrak{F}(\alpha, \alpha_1):\mathfrak{F}(\alpha)]=$l.d. $(\mathfrak{G}/\mathfrak{F})$. Then α is termed a *standard generator* of $\mathfrak{G}$ over $\mathfrak{F}$. Given a generator λ of $\mathfrak{G}$ over $\mathfrak{F}$, we can find a standard generator by the following procedure.

Let $[\mathfrak{F}(\lambda, \cdots, \lambda_{i+1}):\mathfrak{F}(\lambda, \cdots, \lambda_i)]=$l.d. $(\mathfrak{G}/\mathfrak{F})$, and choose $\alpha\in\mathfrak{G}$ so that $\mathfrak{F}(\alpha)=\mathfrak{F}(\lambda, \cdots, \lambda_i)$. Then $\mathfrak{F}(\alpha, \alpha_1)=\mathfrak{F}(\lambda, \cdots, \lambda_{i+1})$ so that α is a standard generator of $\mathfrak{G}$ over $\mathfrak{F}$.

In an analogous fashion, if a normal generator of $\mathfrak{G}$ over $\mathfrak{F}$ is given, we can find a *normal standard generator* for $\mathfrak{G}$ over $\mathfrak{F}$.

For any extension $\mathfrak{G}$ of $\mathfrak{F}$ we denote by $\mathfrak{G}^1_{\mathfrak{F}}$, or $\mathfrak{G}^1$ if there is no danger of ambiguity, the set of elements α in $\mathfrak{G}$ such that l.d. $(\mathfrak{F}\langle\alpha\rangle/\mathfrak{F})=1$. $\mathfrak{G}^1_{\mathfrak{F}}$ is called the *core* of $\mathfrak{G}$ over $\mathfrak{F}$.

THEOREM 2.1. *If $\mathfrak{G}$ is a finitely generated normal extension of order zero of the inversive difference field $\mathfrak{F}$, then $\mathfrak{G}^1_{\mathfrak{F}}$ is a simple, normal, inversive difference field extension of $\mathfrak{F}$ of order zero and of limit degree one. Further the core of $\mathfrak{G}^1_{\mathfrak{F}}$ over $\mathfrak{F}$ is $\mathfrak{G}^1_{\mathfrak{F}}$.*

Proof. Let α, β be elements of $\mathfrak{G}^1$. Since l.d. $(\mathfrak{F}\langle\alpha, \beta\rangle/\mathfrak{F}\langle\alpha\rangle)\leqq$l.d. $\mathfrak{F}\langle\beta\rangle/\mathfrak{F})=1$ and l.d. $(\mathfrak{F}\langle\alpha\rangle/\mathfrak{F})=1$, it follows from Theorem 1 of Cohn [8] that l.d. $(\mathfrak{F}\langle\alpha, \beta\rangle/\mathfrak{F})=1$. Thus l.d. $(\mathfrak{F}\langle\gamma\rangle/\mathfrak{F})=1$ for $\gamma\in\mathfrak{F}\langle\alpha, \beta\rangle$, and hence $\mathfrak{F}\langle\alpha, \beta\rangle\subset\mathfrak{G}^1$. Therefore $\mathfrak{G}^1$ is a difference field extension of $\mathfrak{F}$. It is obvious that the conjugates over $\mathfrak{F}$ of any element of $\mathfrak{G}^1$ are in $\mathfrak{G}^1$ so that $\mathfrak{G}^1$ is normal over $\mathfrak{F}$. By Cohn [7] $\mathfrak{G}^1$ is finitely generated and hence simply generated, say $\mathfrak{G}^1=\mathfrak{F}\langle\alpha\rangle$. Clearly l.d. $(\mathfrak{G}^1/\mathfrak{F})=1$ since $\alpha\in\mathfrak{G}^1$. We may assume α is a standard generator of $\mathfrak{G}^1$ and hence $[\mathfrak{F}(\alpha, \alpha_1):\mathfrak{F}(\alpha)]=1$ implying $\mathfrak{F}(\alpha_1)\subset\mathfrak{F}(\alpha)$. But $[\mathfrak{F}(\alpha):\mathfrak{F}]=[\mathfrak{F}(\alpha_1):\mathfrak{F}]$ since $\mathfrak{F}$ is inversive and thus $\mathfrak{G}^1=\mathfrak{F}(\alpha)$, $\sigma(\mathfrak{G}^1)=\mathfrak{F}(\alpha_1)=\mathfrak{F}(\alpha)=\mathfrak{G}^1$, where σ is the restriction of the transforming map of $\mathfrak{G}$ to $\mathfrak{G}^1$, so that $\mathfrak{G}^1$ is inversive. In addition, since l.d. $(\mathfrak{F}\langle\alpha\rangle/\mathfrak{F})=1$, α is in the core $\mathfrak{K}$ of $\mathfrak{G}^1_{\mathfrak{F}}$ over $\mathfrak{F}$, implying $\mathfrak{K}=\mathfrak{G}^1_{\mathfrak{F}}$.

Let $\mathfrak{G}$ be a difference field extension of $\mathfrak{F}$, and let α be a generator of $\mathfrak{G}$ for which $[\mathfrak{F}(\alpha):\mathfrak{F}]$ is minimal. We call $[\mathfrak{F}(\alpha):\mathfrak{F}]$ the *minimal degree* of $\mathfrak{G}$ over $\mathfrak{F}$, written m.d. $(\mathfrak{G}/\mathfrak{F})$, and say α is a *minimal generator* of $\mathfrak{G}$ over $\mathfrak{F}$. If m.d. $(\mathfrak{G}/\mathfrak{F})=$l.d. $(\mathfrak{G}/\mathfrak{F})$, then $\mathfrak{G}$ is called a *mild* extension of $\mathfrak{F}$. If the mild extension $\mathfrak{G}$ has a minimal generator which is normal over $\mathfrak{F}$, then $\mathfrak{G}$ is said to be a *benign extension* of $\mathfrak{F}$. In general, we see for any extension $\mathfrak{G}$ of $\mathfrak{F}$, that l.d. $(\mathfrak{G}/\mathfrak{F})\leqq$m.d. $(\mathfrak{G}/\mathfrak{F})$.

We call two difference fields $\mathfrak{F}$ and $\mathfrak{G}$ *equivalent* and write $\mathfrak{F}\simeq\mathfrak{G}$, if there exist identical inversive closures of $\mathfrak{F}$ and $\mathfrak{G}$.

LEMMA 2.1. *Let* $\mathfrak{F} \simeq \mathfrak{G}$ *and let* $\alpha^1, \cdots, \alpha^n$ *be elements in an extension of a common inversive closure* $\bar{\mathfrak{F}} = \bar{\mathfrak{G}}$, *of* $\mathfrak{F}$ *and* $\mathfrak{G}$ *such that* $\mathfrak{F}\langle \alpha^1, \cdots, \alpha^{i+1} \rangle$ *is a mild extension of* $\mathfrak{F}\langle \alpha^1, \cdots, \alpha^i \rangle$ *with minimal generator* $\alpha^{i+1} (0 \leqq i \leqq n-1)$. *Then there exist non-negative integers* $m_1, \cdots, m_n$ *such that* $\mathfrak{G}\langle \alpha_{r_1}^1, \cdots, \alpha_{r_{i+1}}^{i+1} \rangle$ *is a mild extension of* $\mathfrak{G}\langle \alpha_{r_1}^1, \cdots, \alpha_{r_i}^i \rangle$ *with minimal generator* $\alpha_{r_{i+1}}^{i+1}$, *for all integers* $r_i \geqq m_i$ $(0 \leqq i \leqq n-1)$.

Proof. We use induction on n. Since $\mathfrak{F}\langle \alpha^1 \rangle$ is a mild extension of $\mathfrak{F}$ and α^1 is a minimal generator, we have

$$[\mathfrak{F}(\overset{1}{\alpha}) : \mathfrak{F}] = [\mathfrak{F}(\overset{1}{\alpha}, \cdots, \overset{1}{\alpha_{i+1}}) : \mathfrak{F}(\overset{1}{\alpha}, \cdots, \overset{1}{\alpha_i})] \qquad (i \geqq 0).$$

Equivalently, if $f(x)$ is the unitary, irreducible polynomial vanishing at α^1 in $\mathfrak{F}[x]$, then $f_{i+1}(x)$ is irreducible over $\mathfrak{F}(\alpha^1, \cdots, \alpha_i^1)$. Since the coefficients of $f(x)$ are $\in \mathfrak{F} \subset \bar{\mathfrak{F}} = \bar{\mathfrak{G}}$, we have $f_{m_1}(x) \in \mathfrak{G}[x]$ for sufficiently large m_1. Then for any integer $r_1 \geqq m_1$, $f_{r_1+i}(x)$ is irreducible over $\mathfrak{G}(\alpha_{r_1}^1, \cdots, \alpha_{r_1+i-1}^1)(i \geqq 0)$. For otherwise for sufficiently large j, $f_{r_1+i+j}(x)$ would be reducible over

$\mathfrak{F}(\overset{1}{\alpha_{r_1+j}}, \cdots, \overset{1}{\alpha_{r_1+j+i-1}})$, a fortiori over $\mathfrak{F}(\overset{1}{\alpha}, \cdots, \overset{1}{\alpha_{r_1+j+i-1}})$, which is impossible.

Assume the theorem true for the case $n-1$. Since $\mathfrak{F}\langle \alpha^1, \cdots, \alpha^{n-1} \rangle \simeq \mathfrak{G}\langle \alpha_{r_1}^1, \cdots, \alpha_{r_{n-1}}^{n-1} \rangle$ for any integers $r_1, \cdots, r_{n-1}$, the lemma follows by applying the result for $n=1$ with α^n assuming the role of α^1, $\mathfrak{F}\langle \alpha^1, \cdots, \alpha^{n-1} \rangle$ that of $\mathfrak{F}$, and $\mathfrak{G}\langle \alpha_{r_1}^1, \cdots, \alpha_{r_{n-1}}^{n-1} \rangle$ that of $\mathfrak{G}$.

LEMMA 2.2. *Let* $\mathfrak{F} \simeq \mathfrak{G}$ *and let* $\alpha^1, \cdots, \alpha^n$ *be elements in an extension of a common inversive closure of* $\mathfrak{F}$ *and* $\mathfrak{G}$ *such that* α^{i+1} *is normal over* $\mathfrak{F}\langle \alpha^1, \cdots, \alpha^i \rangle$ $(0 \leqq i \leqq n-1)$. *Then there exist non-negative integers* $m_1, \cdots, m_n$ *such that* $\alpha_{r_{i+1}}^{i+1}$ *is normal over* $\mathfrak{G}\langle \alpha_{r_1}^1, \cdots, \alpha_{r_i}^i \rangle$ *for all integers* $r_i \geqq m_i$ $(0 \leqq i \leqq n-1)$.

Proof. Since the ideas here are quite similar to those used in establishing Lemma 2.1, we merely sketch a proof. Let $f(x)$ be the unitary irreducible polynomial in $\mathfrak{F}[x]$ vanishing at α^1. Since α^1 is normal over $\mathfrak{F}$, the zeros of $f(x)$ can be written as polynomials in α^1 with coefficients in $\mathfrak{F}$. Hence there exists a non-negative integer m_1 such that for any integer $r_1 \geqq m_1$ we have $f_{r_1}(x) \in \mathfrak{G}[x]$ and each zero of $f_{r_1}(x)$ can be written as a polynomial in $\alpha_{r_1}^1$ with coefficients in $\mathfrak{G}$. Then clearly $\alpha_{r_1}^1$ is normal over $\mathfrak{G}$. The lemma now follows by induction on n.

The following theorem is a direct consequence of Lemmas 2.1 and 2.2.

THEOREM 2.2. *Let* $\mathfrak{F} \simeq \mathfrak{G}$ *and let* $\alpha^1, \cdots, \alpha^n$ *be elements in an extension of a common inversive closure of* $\mathfrak{F}$ *and* $\mathfrak{G}$ *such that* $\mathfrak{F}\langle \alpha^1, \cdots, \alpha^{i+1} \rangle$ *is a benign extension of* $\mathfrak{F}\langle \alpha^1, \cdots, \alpha^i \rangle$ *with normal minimal generator* α^{i+1}, $(0 \leqq i \leqq n-1)$. *Then there exist non-negative integers* $m_1, \cdots, m_n$ *such that* $\mathfrak{G}\langle \alpha_{r_1}^1, \cdots, \alpha_{r_{i+1}}^{i+1} \rangle$ *is a benign extension of* $\mathfrak{G}\langle \alpha_{r_1}^1, \cdots, \alpha_{r_i}^i \rangle$ *with normal minimal generator* $\alpha_{r_{i+1}}^{i+1}$ *for all integers* $r_i \geqq m_i$, $(0 \leqq i \leqq n-1)$.

THEOREM 2.3 (DECOMPOSITION THEOREM). *Let $\mathfrak{F}$ be an inversive difference field and let $\mathfrak{G}$ be a finitely generated normal extension of $\mathfrak{F}$ of order zero. Then there exist elements $\alpha^1, \cdots, \alpha^s$ in $\mathfrak{G}$ such that $\mathfrak{G} \simeq \mathfrak{G}^1_{\mathfrak{F}}\langle \alpha^1, \cdots, \alpha^s \rangle$ and $\mathfrak{G}^1_{\mathfrak{F}}\langle \alpha^1, \cdots, \alpha^{i+1} \rangle$ is a benign extension of $\mathfrak{G}^1_{\mathfrak{F}}\langle \alpha^1, \cdots, \alpha^i \rangle$ with normal minimal generator α^{i+1}, $(0 \leqq i \leqq s-1)$.*

Proof. The proof is in two parts.

Part 1. We may suppose that $\mathfrak{G}^1_{\mathfrak{F}} = \mathfrak{F}$. Assume $\mathfrak{G}$ does not contain a normal extension of $\mathfrak{F}$ different from $\mathfrak{F}$ and of limit degree less than n, where $n = \text{l.d.}\ (\mathfrak{G}/\mathfrak{F})$.

Let λ be a normal standard generator of $\mathfrak{G}$ over $\mathfrak{F}$ which minimizes $[\mathfrak{F}(\lambda) : \mathfrak{F}]$. Since $\mathfrak{F}$ is inversive $[\mathfrak{F}(\lambda_1) : \mathfrak{F}] = [\mathfrak{F}(\lambda) : \mathfrak{F}]$. The Galois group of $\mathfrak{F}(\lambda, \lambda_1)$ over $\mathfrak{F}(\lambda)$ is isomorphic with that of $\mathfrak{F}(\lambda_1)$ over $\mathfrak{F}(\lambda) \cap \mathfrak{F}(\lambda_1)$ (Theorem 1, p. 149, Bourbaki [1]), and thus $[\mathfrak{F}(\lambda_1) : \mathfrak{F}(\lambda) \cap \mathfrak{F}(\lambda_1)] = [\mathfrak{F}(\lambda, \lambda_1) : \mathfrak{F}(\lambda)] = n$. Choosing μ so that $\mathfrak{F}(\mu) = \mathfrak{F}(\lambda) \cap \mathfrak{F}(\lambda_1)$, we see that $\mu_1 \in \mathfrak{F}(\lambda_1)$, and hence $\mathfrak{F}(\mu, \mu_1) \subset \mathfrak{F}(\lambda_1)$. Since $\mathfrak{F}\langle \mu \rangle$ is a normal extension of $\mathfrak{F}$, it follows from our assumption that either $\mathfrak{F}\langle \mu \rangle = \mathfrak{F}$ or l.d. $(\mathfrak{F}\langle \mu \rangle / \mathfrak{F}) = n$. In the former case we have $n = [\mathfrak{F}(\lambda_1) : \mathfrak{F}] = [\mathfrak{F}(\lambda) : \mathfrak{F}]$ from which it follows that $\mathfrak{G}$ is a benign extension of $\mathfrak{F}$ with normal minimal generator λ. In the latter case $n \leqq [\mathfrak{F}(\mu, \mu_1) : \mathfrak{F}(\mu)] \leqq [\mathfrak{F}(\lambda_1) : \mathfrak{F}(\lambda) \cap \mathfrak{F}(\lambda_1)] = n$, implying $\mathfrak{F}(\mu, \mu_1) = \mathfrak{F}(\lambda_1)$ and $\mathfrak{F}\langle \mu \rangle = \mathfrak{F}\langle \lambda_1 \rangle$, so that μ is a normal standard generator of $\mathfrak{F}\langle \lambda_1 \rangle$ over $\mathfrak{F}$ of degree $[\mathfrak{F}(\mu) : \mathfrak{F}] = [\mathfrak{F}(\mu, \mu_1) : \mathfrak{F}] / [\mathfrak{F}(\mu, \mu_1) : \mathfrak{F}(\mu)] = [\mathfrak{F}(\lambda_1) : \mathfrak{F}] / n = [\mathfrak{F}(\lambda) : \mathfrak{F}] / n$. Since $\mathfrak{G} = \mathfrak{F}\langle \lambda \rangle$ does not have a normal standard generator over $\mathfrak{F}$ of degree less than $[\mathfrak{F}(\lambda) : \mathfrak{F}]$, the same must be true of the isomorphic field $\mathfrak{F}\langle \lambda_1 \rangle$, so that $n = 1$. This implies that l.d. $(\mathfrak{F}\langle \lambda \rangle / \mathfrak{F}) = 1$ and thus $\lambda \in \mathfrak{G}^1_{\mathfrak{F}} = \mathfrak{F}$ and $\mathfrak{G} = \mathfrak{F}$.

Part 2. We now assume that $\mathfrak{G}$ contains a normal extension $\mathfrak{K}$ of $\mathfrak{G}^1_{\mathfrak{F}} = \mathfrak{F}$ of limit degree k $(1 < k < n)$. We make the induction assumption that the theorem holds for extensions of limit degree $< n$.

Working in an inversive closure $\bar{\mathfrak{G}}$ of $\mathfrak{G}$, we see that the inversive closure $\overline{\mathfrak{K}}$ of $\mathfrak{K}$ is a normal extension of $\mathfrak{F}$ since $\mathfrak{K}$ is, and thus the composite $\mathfrak{G}\overline{\mathfrak{K}}$ is a normal, finitely generated extension of $\overline{\mathfrak{K}}$. By Theorem 2.1 $(\mathfrak{G}\overline{\mathfrak{K}})^1_{\overline{\mathfrak{K}}}$ is inversive and we may write $(\mathfrak{G}\overline{\mathfrak{K}})^1_{\overline{\mathfrak{K}}} = \overline{\mathfrak{K}}\langle \beta \rangle$ for some $\beta \in \mathfrak{G}\overline{\mathfrak{K}}$. Since $\overline{\mathfrak{K}}\langle \beta \rangle$ is inversive we may replace β by any transform of itself, and since $\beta \in \bar{\mathfrak{G}}$ we may in fact take $\beta \in \mathfrak{G}$. Hence we may suppose that β is a standard generator of $\mathfrak{K}\langle \beta \rangle$ over $\mathfrak{K}$, so that $\beta_1 \in \mathfrak{K}(\beta)$. Let $\beta_1 = \sum_{i=0}^{r} h_i \beta^i$ where $h_i \in \mathfrak{K}$ and β^i denotes the ith power of β $(1 \leqq i \leqq r)$. If we restrict the automorphisms of $\mathfrak{G}$ over $\mathfrak{F}$ to $\mathfrak{K}(\beta)$, we obtain all the relative isomorphism of $\mathfrak{K}(\beta)$ over $\mathfrak{F}$. Consequently, every conjugate $\beta_1^{(j)}$ of β_1 with respect to $\mathfrak{F}$ can be written $\beta_1^{(j)} = \sum_{i=0}^{r} p(h_i)(p(\beta))^i$ where p is the restriction of some automorphism of $\mathfrak{G}$ to $\mathfrak{K}(\beta)$. Since $\mathfrak{K}$ is normal, each $p(h_i)$ is in $\mathfrak{K}$, and hence each $\beta_1^{(j)}$ is in $\mathfrak{K}(\mathfrak{b})$ where $\mathfrak{b}$ denotes the set of conjugates of β over $\mathfrak{F}$. It follows that $\mathfrak{K}(\mathfrak{b}) = \mathfrak{K}\langle \mathfrak{b} \rangle$, whence l.d. $(\mathfrak{K}\langle \mathfrak{b} \rangle / \mathfrak{K}) = 1$. Therefore l.d. $(\mathfrak{K}\langle \mathfrak{b} \rangle / \mathfrak{F}) = \text{l.d.}\ (\mathfrak{K}\langle \mathfrak{b} \rangle / \mathfrak{K})$ l.d. $(\mathfrak{K} / \mathfrak{F}) = 1 \cdot k = k$. Since $\mathfrak{K}$ is normal over $\mathfrak{F}$, so is $\mathfrak{K}(\mathfrak{b})$. Summarizing, we have that $\mathfrak{K}\langle \mathfrak{b} \rangle$ is a normal extension of $\mathfrak{F}$, $(\mathfrak{K}\langle \mathfrak{b} \rangle)^1_{\mathfrak{F}} = \mathfrak{F}$, and l.d. $(\mathfrak{K}\langle \mathfrak{b} \rangle / \mathfrak{F}) = k < n$. By the induction hypoth-

esis we may therefore write $\mathfrak{K}\langle\mathfrak{b}\rangle \simeq \mathfrak{F}\langle\alpha^1, \cdots, \alpha^l\rangle$ where each $\alpha^i \in \mathfrak{K}\langle\mathfrak{b}\rangle$ and $\mathfrak{F}\langle\alpha^1, \cdots, \alpha^i\rangle$ is a benign extension of $\mathfrak{F}\langle\alpha^1, \cdots, \alpha^{i-1}\rangle$ with normal minimal generator $\alpha^i (1 \leqq i \leqq l)$.

Now $\mathfrak{G}\overline{\mathfrak{K}}$ is a finitely generated normal extension of $\overline{\mathfrak{K}}\langle\mathfrak{b}\rangle$. Since obviously l.d. $(\overline{\mathfrak{K}}\langle\mathfrak{b}\rangle/\overline{\mathfrak{K}}) = 1$, $\overline{\mathfrak{K}}\langle\mathfrak{b}\rangle$ must coincide with $(\mathfrak{G}\overline{\mathfrak{K}})^{\frac{1}{\overline{\mathfrak{K}}}}$ and hence is inversive. Because l.d. $(\mathfrak{G}\overline{\mathfrak{K}}/\overline{\mathfrak{K}}\langle\mathfrak{b}\rangle) \leqq$ l.d. $(\mathfrak{G}/\mathfrak{K}\langle\mathfrak{b}\rangle) =$ l.d. $(\mathfrak{G}/\mathfrak{F})/$l.d. $(\mathfrak{K}\langle\mathfrak{b}\rangle/\mathfrak{F}) = n/k < n$, we conclude by the induction hypothesis that there exist elements $\gamma^{l+1}, \cdots, \gamma^s \in \mathfrak{G}\overline{\mathfrak{K}}$ such that $\mathfrak{G}\overline{\mathfrak{K}} \simeq \overline{\mathfrak{K}}\langle\mathfrak{b}\rangle\langle\gamma^{l+1}, \cdots, \gamma^s\rangle$ where $\overline{\mathfrak{K}}\langle\mathfrak{b}\rangle\langle\gamma^{l+1}, \cdots, \gamma^i\rangle$ is a benign extension of $\overline{\mathfrak{K}}\langle\mathfrak{b}\rangle\langle\gamma^{l+1}, \cdots, \gamma^{i-1}\rangle$ with normal minimal generator $\gamma^{i+1} (l+1 \leqq j \leqq s)$. Since $\overline{\mathfrak{K}}\langle\mathfrak{b}\rangle \simeq \mathfrak{K}\langle\mathfrak{b}\rangle \simeq \mathfrak{F}\langle\alpha^1, \cdots, \alpha^l\rangle$, it follows from Theorem 2.2 that if we set $\alpha^i = \gamma_m^j (l+1 \leqq j \leqq s)$ with m a sufficiently large non-negative integer, then $\mathfrak{F}\langle\alpha^1, \cdots, \alpha^{i+1}\rangle$ is a benign extension of $\mathfrak{F}\langle\alpha^1, \cdots, \alpha^i\rangle$ with normal minimal generator α^{i+1} $(0 \leqq i \leqq s-1)$. Clearly

$$\mathfrak{G} \simeq \mathfrak{G}\overline{\mathfrak{K}} \simeq \overline{\mathfrak{K}}\langle\mathfrak{b}\rangle\langle\gamma^{l+1}, \cdots, \gamma^s\rangle \simeq \mathfrak{F}\langle\alpha^1, \cdots, \alpha^s\rangle.$$

This completes the proof of the theorem.

If $\mathfrak{G}$ is a finitely generated, normal extension of $\mathfrak{F}$ of order zero, then a finite sequence $\alpha^1, \cdots, \alpha^s$ of elements of $\mathfrak{G}$ as in the statement of Theorem 2.3 is said to define a *benign decomposition* of $\mathfrak{G}$ over $\mathfrak{F}$.

Before applying the Decomposition Theorem we need several preliminary results. Let $\mathfrak{G}$ be a difference field and $\alpha \in \bar{\mathfrak{G}}$. We define the *inverseness* of α relative to $\mathfrak{G}$, denoted by $i(\alpha/\mathfrak{G})$, to be the smallest non-negative integer m for which $\alpha_m \in \mathfrak{G}$.

LEMMA 2.3. *Let h be an isomorphism of $(\mathfrak{G}, \sigma)$ into $(\mathfrak{K}, \mu)$. Then h can be extended to a unique isomorphism of $(\bar{\mathfrak{G}}, \sigma)$ into $(\overline{\mathfrak{K}}, \mu)$. Conversely, if $\bar{\mathfrak{G}}$ and $\overline{\mathfrak{K}}$ are contained in some common over-field and if $\bar{h}$ is a nontrivial isomorphism of $(\bar{\mathfrak{G}}, \sigma)$ into $(\overline{\mathfrak{K}}, \mu)$, then the restriction of $\bar{h}$ to $(\mathfrak{G}, \sigma)$ is nontrivial.*

Proof. Let $\alpha \in (\bar{\mathfrak{G}}, \sigma)$ and define $\bar{h}(\alpha) = \mu^{-m} h \sigma^m(\alpha)$, where $m = i(\alpha/\mathfrak{G})$. Let $\beta \in (\bar{\mathfrak{G}}, \sigma)$ and set $n = i(\beta/\mathfrak{G})$, $r = \max(m, n)$, and $s = i(\alpha+\beta/\mathfrak{G})$. Clearly $s \leqq r$. If $m \neq n$, it is easy to show $s = r$, and in this case, using the fact $h\sigma(\gamma) = \mu h(\gamma)$, for all $\gamma \in \mathfrak{G}$, we have

$$\begin{aligned}
\bar{h}(\alpha + \beta) &= \mu^{-s} h \sigma^s(\alpha + \beta) = \mu^{-s} h \sigma^s(\alpha) + \mu^{-s} h \sigma^s(\beta) \\
&= \mu^{-s} h \sigma^{s-m}(\sigma^m(\alpha)) + \mu^{-s} h \sigma^{s-n}(\sigma^n(\beta)) \\
&= \mu^{-s} \mu^{s-m} h(\sigma^m(\alpha)) + \mu^{-s} \mu^{s-n} h(\sigma^n(\beta)) \\
&= \mu^{-m} h \sigma^m(\alpha) + \mu^{-n} h \sigma^n(\beta) = \bar{h}(\alpha) + \bar{h}(\beta).
\end{aligned}$$

If $m = n = r$, let $t = r - s$. Then

$$\begin{aligned}
\bar{h}(\alpha) + \bar{h}(\beta) &= \mu^{-r} h \sigma^r(\alpha) + \mu^{-r} h \sigma^r(\beta) = \mu^{-r} h \sigma^r(\alpha + \beta) \\
&= \mu^{-r} h \sigma^t(\sigma^s(\alpha + \beta)) = \mu^{-r} \mu^t h \sigma^s(\alpha + \beta) \\
&= \mu^{-s} h \sigma^s(\alpha + \beta) = \bar{h}(\alpha + \beta).
\end{aligned}$$

Similarly $\bar{h}(\alpha\beta) = \bar{h}(\alpha)\bar{h}(\beta)$. Furthermore, $\bar{h}\sigma(\alpha) = \mu^{-m+1}h\sigma^{m-1}(\sigma(\alpha))$ $=\mu^{-m+1}h\sigma^m(\alpha) = \mu\bar{h}(\alpha)$. Thus $\bar{h}$ is an isomorphism of $\bar{\mathcal{G}}$ into $\overline{\mathcal{H}}$ extending h. That $\bar{h}$ is unique is obvious.

Conversely, let $\bar{h}$ be an isomorphism of $\bar{\mathcal{G}}$ which leaves each element of $\mathcal{G}$ invariant. Let $\alpha\in\bar{\mathcal{G}}$ and set $m = i(\alpha/\mathcal{G})$. Then $\alpha = \sigma^{-m}(\sigma^m(\alpha))$ and $\bar{h}(\alpha)$ $= \bar{h}\sigma^{-m}(\sigma^m(\alpha)) = \sigma^{-m}\bar{h}(\sigma^m(\alpha)) = \sigma^{-m}(\sigma^m(\alpha)) = \alpha$.

From Lemma 2.3 we easily deduce a further lemma and theorem.

LEMMA 2.4. *Let $\mathcal{F}$ be an inversive field. Then $\mathcal{G}$ and $\mathcal{H}$ are incompatible extensions of $\mathcal{F}$ if and only if $\bar{\mathcal{G}}$ and $\overline{\mathcal{H}}$ are incompatible extensions of $\mathcal{F}$. $\mathcal{G}$ is a monadic extension of $\mathcal{F}$ if and only if $\bar{\mathcal{G}}$ is a monadic extension of $\mathcal{F}$.*

THEOREM 2.4. *Let $\mathcal{F}$ be an inversive difference field and let $\mathcal{G}$ and $\mathcal{H}$ be equivalent finitely generated extensions of $\mathcal{F}$ of order zero. Then $\mathcal{G}$ is incompatible with an extension $\mathcal{K}$ of $\mathcal{F}$ if and only if $\mathcal{H}$ and $\mathcal{K}$ are incompatible extensions of $\mathcal{F}$. $\mathcal{G}$ is a monadic extension of $\mathcal{F}$ if and only if $\mathcal{H}$ is a monadic extension of $\mathcal{F}$.*

Let $\mathcal{F}$ be an inversive difference field and let $\mathcal{G}$ and $\mathcal{H}$ be extensions of $\mathcal{F}$. If $\mathcal{G}_N$ and $\mathcal{H}_N$ represent difference fields formed by extending the transforming maps of $\mathcal{G}$ and $\mathcal{H}$ to the minimal normal extension of $\mathcal{F}$ containing $\mathcal{G}$ and $\mathcal{H}$ respectively, then $\mathcal{G}_N$ and $\mathcal{H}_N$ are incompatible extensions of $\mathcal{F}$ whenever $\mathcal{G}$ and $\mathcal{H}$ are.

THEOREM 2.5. *Let $\mathcal{F}$ be an inversive difference field, and let $\mathcal{G}$ and $\mathcal{H}$ be finitely generated, normal extensions of $\mathcal{F}$. Then $\mathcal{G}$ and $\mathcal{H}$ are incompatible extensions of $\mathcal{F}$ if and only if $\mathcal{G}^1_{\mathcal{F}}$ and $\mathcal{H}^1_{\mathcal{F}}$ are incompatible extensions of $\mathcal{F}$.*

Proof. The sufficiency of this condition is obvious. To prove the converse we assume that $\mathcal{G}^1 = \mathcal{G}^1_{\mathcal{F}}$ and $\mathcal{H}^1 = \mathcal{H}^1_{\mathcal{F}}$ have isomorphisms over $\mathcal{F}$ into an extension $(\mathcal{K}, \mu)$ of $\mathcal{F}$. We may take $\mathcal{K}$ to be algebraically closed. Let $\alpha^1, \cdots, \alpha^m$ and $\beta^1, \cdots, \beta^n$ define benign decompositions of the respective extensions $\mathcal{G}$ and $\mathcal{H}$ of $\mathcal{F}$. By Theorem 2.4 it is sufficient to show that $\mathcal{G}^1\langle\alpha^1, \cdots, \alpha^m\rangle$ and $\mathcal{H}^1\langle\beta^1, \cdots, \beta^n\rangle$ have isomorphisms into $\mathcal{K}$ over $\mathcal{F}$. This in turn will follow if we establish the following:

Let $(\mathcal{L}, \sigma)$ be an extension of $(\mathcal{F}, \sigma)$; let $(\mathfrak{M}, \sigma)$ be a benign extension of $(\mathcal{L}, \sigma)$; and let ϕ be an isomorphism of $(\mathcal{L}, \sigma)$ over $(\mathcal{F}, \sigma)$ onto $(\mathcal{L}', \mu)$ in the extension $(\mathcal{K}, \mu)$ of $(\mathcal{F}, \sigma)$. Then ϕ can be extended to an isomorphism of $(\mathfrak{M}, \sigma)$ into $(\mathcal{K}, \mu)$ over $(\mathcal{F}, \sigma)$.

To prove this let α be a minimal generator for $(\mathfrak{M}, \sigma)$ over $(\mathcal{L}, \sigma)$, and set $f(x)$ equal to the unitary irreducible polynomial in $\mathcal{L}[x]$ vanishing at α, $g(x)$ the polynomial in $\mathcal{L}'[x]$ obtained from $f(x)$ by replacing the coefficients in $f(x)$ by their images under ϕ. Then ϕ can be extended to an algebraic isomorphism ϕ_0 of $\mathcal{L}(\alpha)$ onto $\mathcal{L}'(\beta)$, $\phi_0(\alpha) = \beta$, where β is any zero of $g(x)$. Since α is a minimal generator of a benign extension of $\mathcal{L}$, $f_1(x)$ is irreducible over $\mathcal{L}(\alpha)$ and ϕ_0 can be extended to an isomorphism ϕ_1 of $\mathcal{L}(\alpha, \alpha_1)$ onto $\mathcal{L}'(\beta, \gamma)$, $\phi_1(\alpha_1) = \gamma$, where γ is any zero of $h(x)$, the polynomial obtained from $f_1(x)$ by

replacing the coefficients in $f_1(x)$ by their images under ϕ_0. Since $f_1(x) \in \mathfrak{L}[x]$ and $\phi\sigma(a) = \mu\phi(a)$, $a \in \mathfrak{L}$, it follows that $\beta_1 = \mu(\beta)$ is a zero of $h(x)$. Hence we can take $\gamma = \beta_1$. A straightforward induction argument now yields the desired result.

It is easy to see that a benign proper extension of an inversive field always has nontrivial automorphisms, for such an extension is formed by adjoining the zeros of a reflexive prime difference ideal which has a characteristic set consisting of one difference polynomial of order zero. It is not so obvious, however, that an intermediate extension should likewise be amonadic.

THEOREM 2.6. *Let $\mathfrak{F}\langle\lambda\rangle$ be a benign extension of the inversive difference field $\mathfrak{F}$, and let $\mathfrak{K}$ be a difference field intermediate to $\mathfrak{F}$ and $\mathfrak{F}\langle\lambda\rangle$ different from $\mathfrak{F}$. Then $\mathfrak{K}$ is an amonadic extension of $\mathfrak{F}$.*

Proof. We assume the contrary and produce a contradiction. Without loss of generality we may take $\mathfrak{K} = \mathfrak{F}\langle\alpha\rangle$.

Let $(\mathfrak{G}, \sigma)$ be an inversive closure of $\mathfrak{F}\langle\lambda\rangle$, and set $\mathfrak{K}$ equal to the inversive closure of $\mathfrak{F}\langle\alpha\rangle$ in $\mathfrak{G}$. Let G be the algebraic Galois group of $\mathfrak{G}$ over $\mathfrak{F}$, H the (closed) subgroup of G corresponding to the subfield $\mathfrak{K}$. Since $\mathfrak{F}\langle\lambda\rangle$ is a benign extension of $\mathfrak{F}$ with normal minimal generator λ and since $\mathfrak{F}$ is inversive, the fields $\mathfrak{F}(\lambda_i)$ and $\mathfrak{F}(\lambda_j)(-\infty < i < j < \infty)$ are linearly disjoint and have isomorphic Galois groups over $\mathfrak{F}$. Hence we can represent G as an infinite direct product of finite groups all isomorphic to the Galois group G_λ of $\mathfrak{F}(\lambda)$ over $\mathfrak{F}$. We designate the elements of G_λ and their isomorphic images by p's with subscripts and elements of G by $(\cdots, p_i, p_j, p_k, \cdots)$.

Let $x \in G$. Then if $s\sigma(x) = \sigma s(x)$ for every $x \in \mathfrak{K}$, we must have $s \in H$ since $\mathfrak{F}\langle\alpha\rangle$ is a monadic extension of $\mathfrak{F}$ and by Lemma 2.4 the same is true of $\mathfrak{K}$.

Let $s = (\cdots, p_0, p_1, p_2, \cdots)$ be any element of G, and define $s^* = \sigma^{-1}s\sigma$. It is easy to see that $s^* = (\cdots, p_1, p_2, p_3, \cdots)$, i.e., if p_0 acts on λ_0, p_1 on λ_1, etc., in s, then p_1 acts on λ_0, p_2 on λ_1, etc. in s^*.

With the above definition of s^*, it follows that if $\mathfrak{K}$ is a monadic extension of $\mathfrak{F}$ and if $s^{-1}s^* \in H$, then $s \in H$.

Let $\alpha \in \mathfrak{F}(\lambda_a, \cdots, \lambda_{a+i})$. We can choose elements $p_a, \cdots, p_{a+i}$, where p_{a+j} acts on λ_{a+j} $(0 \leqq j \leqq i)$ so that $P = (\cdots p_{a-1}, p_a, \cdots, p_{a+i}, p_{a+i+1}, \cdots)$ is not in H no matter what choice is made for $p_{a-1}, p_{a-2}, \cdots$; $p_{a+i+1}, p_{a+i+2}, \cdots$. Thus for some integer k with $0 \leqq k \leqq i$ (namely for $k = i$) it is possible to select a set of p's acting on $\lambda_a, \cdots, \lambda_{a+k}$, such that $P = (\cdots, p_{a-1}, p_a, \cdots, p_{a+k}, p_{a+k+1}, \cdots) \notin H$ no matter what choice is made for $p_{a-1}, p_{a-2}, \cdots; p_{a+k+1}, p_{a+k+2}, \cdots$. Let such a k be chosen as small as possible.

Let $P = (\cdots, p_{a-1}, p_a, \cdots, p_{a+k}, p_{a+k+1}, \cdots)$ represent an arbitrary completion of $p_a, \cdots, p_{a+k}$ to an element in G, and set $S = P^{-1}P^*$. Since $P \notin H$ and $\mathfrak{K}$ is a monadic extension of $\mathfrak{F}$, we must have $s \notin H$. But setting $s_i = p_i^{-1}p_{i+1}$ $(-\infty < i < \infty)$ we see that $s_a, \cdots, s_{a+k-1}$ are determined by

$p_a, \cdots, p_{a+k}$, the other s_i being arbitrary since we can complete $p_a, \cdots, p_{a+k}$ in such a fashion as to obtain any desired set $s_{a-1}, s_{a-2}, \cdots ; s_{a+k}, s_{a+k+1}, \cdots$. If $k>0$ this contradicts the choice of k. If $k=0$ all of the s_i are arbitrary and can be chosen so that $S=e$. This implies $e \notin H$ which is impossible.

THEOREM 2.7. *Let $\mathfrak{F}$ be an inversive difference field and let $\mathfrak{F}\langle\alpha\rangle$ be a simple extension of $\mathfrak{F}$ of order zero such that* l.d. $(\mathfrak{F}\langle\alpha\rangle/\mathfrak{F})>1$. *Then $\mathfrak{F}\langle\alpha\rangle$ is an amonadic extension of $\mathfrak{F}$.*

Proof. Let $\mathfrak{G}$ be a finitely generated, normal extension of $\mathfrak{F}$ containing $\mathfrak{F}\langle\alpha\rangle$, and let $\lambda^1, \cdots, \lambda^n$ define a benign decomposition of $\mathfrak{G}$ over $\mathfrak{F}$. Now $\alpha \notin \mathfrak{G}_{\mathfrak{F}}^1$ because l.d. $(\mathfrak{F}\langle\alpha\rangle/\mathfrak{F})>1$. Therefore if we denote the inversive closure of $\mathfrak{G}_{\mathfrak{F}}^1\langle\lambda^1, \cdots, \lambda^i\rangle$ by $\mathfrak{K}_i (0 \leqq i \leqq n)$ so that $\mathfrak{K}_0 = \mathfrak{G}_{\mathfrak{F}}^1$, and let ν denote the smallest positive integer for which $\alpha \in \mathfrak{K}_\nu$, then $1 \leqq \nu \leqq n$. As $\mathfrak{G}_{\mathfrak{F}}^1\langle\lambda^1, \cdots, \lambda^{\nu-1}\rangle\langle\lambda^\nu\rangle$ is a benign extension of $\mathfrak{G}_{\mathfrak{F}}^1\langle\lambda^1, \cdots, \lambda^{\nu-1}\rangle$ and $\mathfrak{G}_{\mathfrak{F}}^1\langle\lambda^1, \cdots, \lambda^{\nu-1}\rangle \simeq \mathfrak{K}_{\nu-1}$, it follows from Theorem 2.2 that $\mathfrak{K}_{\nu-1}\langle\lambda_m^\nu\rangle$ is a benign extension of $\mathfrak{K}_{\nu-1}$ for a sufficiently large non-negative integer m. Since for a sufficiently large non-negative integer r we have $\alpha_r \in \mathfrak{K}_{\nu-1}\langle\lambda_m^\nu\rangle$ and $\alpha_r \notin \mathfrak{K}_{\nu-1}$, it follows from Theorem 2.6 that $\mathfrak{K}_{\nu-1}\langle\alpha_r\rangle$ is an amonadic extension of $\mathfrak{K}_{\nu-1}$. By Theorem 2.4 it follows that $\mathfrak{K}_{\nu-1}\langle\alpha\rangle$ is an amonadic extension of $\mathfrak{K}_{\nu-1}$. This implies $\mathfrak{F}\langle\alpha\rangle$ is an amonadic extension of $\mathfrak{F}$.

The results of this section together with Theorems 1 and 2 of [5] give

THEOREM 2.8. *If an inversive difference field admits a finitely generated pathological extension, then it admits a pathological extension of finite degree of the same type.*

As an application of Theorem 2.8 we prove

THEOREM 2.9. *The difference field $\mathfrak{C}\langle x\rangle$ of rational functions of x with complex coefficients, with transforming defined by $f(x) \to f(x+1)$, has no finitely generated pathological extensions.*

Proof. By Theorem 2.8 our result will follow if we show that $\mathfrak{C}\langle x\rangle$ has no proper extensions of limit degree one. Suppose, on the contrary, that α is a standard generator of an extension of $\mathfrak{C}\langle x\rangle$ of limit degree one. Then α_1 is a rational function of α with coefficients in $\mathfrak{C}\langle x\rangle$. But the transforming operation on $\mathfrak{C}\langle x\rangle$ is such that α_1, considered as an algebraic function of x, must have at least one branch point not occurring among the set of branch points of the algebraic function α. This contradicts the fact that α_1 is rational in α.

The material in this section also enables us to give generalizations of Theorems 1 and 2 of Cohn [5].

LEMMA 2.5. *Let $\mathfrak{G}=\mathfrak{F}\langle\beta_1, \cdots, \beta_q\rangle$ be an extension of the difference field $\mathfrak{F}$ of transformal transcendence degree q, and let $\mathfrak{K}$ be a finitely generated extension of $\mathfrak{G}$ of order zero and limit degree one. Then $\mathfrak{K}$ is generated by adjoining to $\mathfrak{G}$ elements which are algebraic over $\mathfrak{F}$.*

Proof. It is clearly sufficient to prove the lemma with the added hypothesis that $\mathfrak{F}$ is algebraically closed in $\mathfrak{G}$. Thus we must show $\mathfrak{K}=\mathfrak{G}$.

Our proof is by induction on q. Setting $q=1$, we write β for β_1 and let α be any element in $\mathfrak{K}$.

Since l.d. $(\mathfrak{K}/\mathfrak{G})=1$, there is an integer r such that for any positive integer k, $\alpha_{r+k}\in\mathfrak{G}(\alpha, \cdots, \alpha_r)$. Choose k so large that the set S of transforms of β occurring in the minimal equations with unit initial coefficients for $\alpha_1, \cdots, \alpha_r$, and the set T of transforms of β occurring in the minimal equation with unit initial coefficient for α_{r+k} are disjoint.

Let the rational expression for α_{r+k} in terms of $\alpha, \cdots, \alpha_r$ and transforms of β be arranged as a rational function in members of T with coefficients which are rational combinations of other $\beta_i, \alpha, \cdots, \alpha_r$, and with one coefficient unity. Let S' be the set of β_i appearing in these coefficients, and let $U=S\cup S'$. Then $U\cap T=\varnothing$.

We now adjoin to the field $\mathfrak{F}$ (not to the difference field) new algebraically independent sets $U', U'', \cdots$, each with as many members as U. The $\mathfrak{F}$-isomorphism mapping $U\to U^{(i)}$, $T\to T$, extends to an isomorphism mapping $\alpha, \cdots, \alpha_r; \alpha_{r+k}$ into $\alpha^{(i)}, \cdots, \alpha_r^{(i)}; \alpha_{r+k}^{(i)}$.

If the rational expression for α_{r+k} contains a coefficient which is not algebraic over $\mathfrak{F}$, then since the $U^{(i)}$ are algebraically independent it is easy to see that this coefficient has distinct images under these isomorphisms. Then the $\alpha_{r+k}^{(i)}$ are all distinct. Since they are the solutions of the minimal equation for α_{r+k}, which is unaltered by the isomorphisms, this is impossible. Hence every coefficient is algebraic over $\mathfrak{F}$. But these coefficients are in $\mathfrak{K}$, and since $\mathfrak{F}$ is algebraically closed in $\mathfrak{K}$, the coefficients must be in $\mathfrak{F}$. Thus $\alpha_{r+k}\in\mathfrak{G}$, and so $\alpha\in\mathfrak{G}$, implying $\mathfrak{G}=\mathfrak{K}$.

To complete the proof by induction, we set $\mathfrak{G}=\mathfrak{F}\langle\beta_1, \cdots, \beta_q\rangle$ and assume the lemma true for $q'<q$. By the induction hypothesis $\mathfrak{K}$ is generated by adjoining to $\mathfrak{G}$ a set A of elements algebraic over $\mathfrak{F}\langle\beta_1\rangle$. Since $\mathfrak{F}\langle\beta_1\rangle\langle A\rangle$ and $\mathfrak{G}$ are linearly disjoint over $\mathfrak{F}\langle\beta_1\rangle$, $\mathfrak{F}\langle\beta_1\rangle\langle A\rangle$ is of limit degree one over $\mathfrak{F}\langle\beta_1\rangle$. Hence $\mathfrak{F}\langle\beta_1\rangle\langle A\rangle$ is generated by adjoining to $\mathfrak{G}$ elements algebraic over $\mathfrak{F}$.

THEOREM 2.10. *Let $\mathfrak{G}=\mathfrak{F}\langle\beta_1, \cdots, \beta_q\rangle$ be an extension of $\mathfrak{F}$ of transformal transcendence degree q; let $\mathfrak{K}$ and $\mathfrak{K}$ be finitely generated incompatible extensions of $\bar{\mathfrak{G}}$, an inversive closure of $\mathfrak{G}$. Then there exist elements c and d of $\mathfrak{K}$ and $\mathfrak{K}$ respectively which generate incompatible extensions of $\mathfrak{F}$ of order zero.*

Proof. Since the least normal extensions of $\mathfrak{K}$ and $\mathfrak{K}$ are incompatible extensions of $\bar{\mathfrak{G}}$, there is no loss of generality if we assume $\mathfrak{K}$ and $\mathfrak{K}$ to be normal extensions of $\bar{\mathfrak{G}}$. Then by Theorem 2.5, $\mathfrak{K}\frac{1}{\bar{\mathfrak{G}}}$ and $\mathfrak{K}\frac{1}{\bar{\mathfrak{G}}}$ are incompatible extensions of $\bar{\mathfrak{G}}$. With the aid of Lemma 2.3, it is easy to show that this in turn implies the existence of finitely generated incompatible extensions $\mathfrak{K}^*$ and $\mathfrak{K}^*$ (contained in $\mathfrak{K}$ and $\mathfrak{K}$ respectively) of $\mathfrak{G}$ which are of order zero and limit degree one. Hence by Lemma 2.5, $\mathfrak{K}^*$ and $\mathfrak{K}^*$ are generated by the adjunction

to $\mathfrak{G}$ of elements c and d respectively which are algebraic over $\mathfrak{F}$. If $\mathfrak{F}\langle c\rangle$ and $\mathfrak{F}\langle d\rangle$ are not incompatible extensions of $\mathfrak{F}$, we can find an extension $\mathfrak{L}$ of $\mathfrak{F}$ containing difference subfields isomorphic to $\mathfrak{F}\langle c\rangle$ and $\mathfrak{F}\langle d\rangle$. Adjoining q elements annulling no nonzero difference polynomial with coefficients in $\mathfrak{L}$ (and hence annulling no polynomial with coefficients in $\mathfrak{F}$), we obtain an extension of $\mathfrak{L}$ which contains a difference subfield isomorphic to $\mathfrak{G}$. Hence we can construct an extension of $\mathfrak{G}$ which contains difference subfields isomorphic to $\mathfrak{G}\langle c\rangle$ and $\mathfrak{G}\langle d\rangle$, i.e., $\mathfrak{G}\langle c\rangle$ and $\mathfrak{G}\langle d\rangle$ are not incompatible extensions of $\mathfrak{G}$.

THEOREM 2.11. *Let $\mathfrak{G}=\mathfrak{F}\langle\beta_1, \cdots, \beta_q\rangle$ be an extension of $\mathfrak{F}$ of transformal transcendence degree q, and let $\mathfrak{K}$ be a finitely generated monadic extension of $\bar{\mathfrak{G}}$, an inversive closure of $\mathfrak{G}$. Then there exists an element a in $\mathfrak{K}$ which generates a monadic extension of $\mathfrak{F}$ of order zero.*

Proof. By Theorem 2.8, we may assume $\mathfrak{K}$ is a monadic extension of $\bar{\mathfrak{G}}$ of order zero and limit degree one. By Lemma 2.3, there exists a monadic extension $\mathfrak{K}^*$ of $\mathfrak{G}$, $\mathfrak{K}^*\subset\mathfrak{K}$, of order zero and limit degree one. By Lemma 2.5, there exists an element a in $\mathfrak{K}^*$ such that $\mathfrak{K}=\mathfrak{G}\langle a\rangle$ and a is algebraic over $\mathfrak{F}$. If $\mathfrak{F}\langle a\rangle$ is not a monadic extension of $\mathfrak{F}$, then there exists an extension $\mathfrak{L}$ of $\mathfrak{F}$ containing two difference subfields isomorphic to $\mathfrak{F}\langle a\rangle$. By adjoining to $\mathfrak{L}$ q elements annulling no nonzero difference polynomial with coefficients in $\mathfrak{L}$, we obtain a difference field into which $\mathfrak{G}\langle a\rangle$ has two distinct isomorphisms.

3. **Extensions of limit degree one.** On the basis of the results obtained in §2, it is natural to proceed to a more detailed investigation of the structure of normal extensions of order zero and of limit degree one (that is, difference field extensions which as field extensions are of finite degree and normal). The remainder of this paper will be devoted to this task.

Let $(\mathfrak{G}, \sigma)$ be a normal extension of the inversive difference field $(\mathfrak{F}, \sigma)$ of limit degree one with standard generator α. If $s_1=e, s_2, \cdots, s_n$ denote the elements of the Galois group G of $\mathfrak{G}$ over $\mathfrak{F}$, then the composite mappings $\sigma s_1=\sigma, \sigma s_2, \cdots, \sigma s_n$ are automorphisms of $\mathfrak{G}$ whose restrictions to $\mathfrak{F}$ give σ. Thus each $\sigma_i=\sigma s_i$ defines a difference field extension $(\mathfrak{G}, \sigma_i)$ of $(\mathfrak{F}, \sigma)$ of limit degree one. Since there are no more than n extensions of σ to $\mathfrak{G}$, we have proved

THEOREM 3.1. *If $(\mathfrak{G}, \sigma)$ is a finitely generated, normal extension of the inversive difference field $(\mathfrak{F}, \sigma)$ of limit degree one, then there are precisely $n=[\mathfrak{G}:\mathfrak{F}]$ extensions $(\mathfrak{G}, \sigma_i)(1\leqq i\leqq n)$ of $(\mathfrak{F}, \sigma)$ each of limit degree one. The σ_i are given by σs_i, where $s_i\in G(1\leqq i\leqq n)$.*

The relation of this theorem to [5] becomes clear if each extension $(\mathfrak{G}, \sigma_i)$ is thought of as arising from the adjunction to $(\mathfrak{F}, \sigma)$ of a solution of a reflexive prime difference ideal in the decomposition of $\{A(y)\}$, where $A(y)$ is an algebraically irreducible, normal difference polynomial of order zero with coefficients in $\mathfrak{F}$. We are further assuming that each of the reflexive prime

difference ideals has a characteristic set of length two, the second member of which is of degree one in y_1. In [5] the development is now continued by examining the pathology of the $(\mathfrak{G}, \sigma_i)$ with reference to the manifold of $\{A(y)\}$. In our particular case the Galois group G together with a set of automorphisms of G becomes the primary tool of our investigation.

Evidently $(\mathfrak{G}, s_i\sigma)$ is also an extension of $(\mathfrak{F}, \sigma)$, and hence $s_i\sigma = \sigma s_j$ for some $s_j \in G$. Thus the mapping $s_i \to s_i^*$, where $s_i^* = \sigma^{-1}s_i\sigma$ is an automorphism of G. Furthermore the fixed points of the mapping are those elements of G which commute with σ and thus are automorphisms of the difference field $(\mathfrak{G}, \sigma)$ over $(\mathfrak{F}, \sigma)$. We denote the totality of such elements by G_σ, and call it the *transformal Galois group* of $(\mathfrak{G}, \sigma)$ over $(\mathfrak{F}, \sigma)$. The automorphism $s_i \to s_i^*$ is called the *σ-automorphism* of G. Similarly we see that s_j is an element of G_{σ_i}, the transformal Galois group of $(\mathfrak{G}, \sigma_i)$, if and only if s_j is a fixed point of the σs_i-automorphism $s_k \to s_i^{-1}s_k^*s_i$. For ease of notation we designate $(\mathfrak{G}, \sigma_i)$ by $\mathfrak{G}_i$ and G_{σ_i} by G_i.

We are interested not only in the automorphisms of a given $\mathfrak{G}_i$, but also in the $\mathfrak{F}$-isomorphisms of $\mathfrak{G}_i$ onto $\mathfrak{G}_j$. For any σ_i and any $s \in G$, $s\sigma_i s^{-1} = \sigma_j$ for a unique j. If $j = i$, then $s \in G_i$. If $j \neq i$, then s is an $\mathfrak{F}$-isomorphism of $\mathfrak{G}_i$ onto $\mathfrak{G}_j$. Thus each element of G either is an automorphism of $\mathfrak{G}_i$ or else is an isomorphism of $\mathfrak{G}_i$ onto some $\mathfrak{G}_j$ with $j \neq i$. Hence we can exploit the fact that the fields $\mathfrak{G}_i$ are algebraically indistinguishable by employing G in a dual role—as the source of automorphisms of the difference fields and of the relative isomorphisms among the various difference fields.

From the above discussion it follows that the difference fields $\mathfrak{G}_i (1 \leqq i \leqq n)$ are divided into equivalence classes of isomorphic difference fields. The following theorem enables us to compute the number of classes from the order of the G_i.

THEOREM 3.2. *The number of isomorphism classes is equal to* $n^{-1} \sum_{j=1}^{n} \operatorname{ord} G_j$.

Proof. Let $K_1, \cdots, K_r$ denote the isomorphism classes and let k_i denote the number of elements in $K_i (1 \leqq i \leqq r)$. G operates transitively on K_i so that k_i divides n. Writing $n = k_i h_i$ we see that the number of elements of G which are automorphisms of a particular difference field $\mathfrak{G}_j \in K_i$ is equal to h_i, that is $h_i = \operatorname{ord} G_j (\mathfrak{G}_j \in K_i)$. Thus

$$rn = \sum_{i=1}^{r} k_i h_i = \sum_{i=1}^{r} \sum_{\mathfrak{G}_j \in K_i} h_i = \sum_{i=1}^{r} \sum_{\mathfrak{G}_j \in K_i} \operatorname{ord} G_j = \sum_{j=1}^{n} \operatorname{ord} G_j.$$

COROLLARY. $\sum_{i=1}^{r} h_i^{-1} = 1$.

Proof. Since $\sum_{i=1}^{r} k_i = n$, we have

$$\sum_{i=1}^{r} h_i^{-1} = \sum_{i=1}^{r} n^{-1} k_i = 1.$$

It should be noted that while $\mathfrak{G}_i \approx \mathfrak{G}_j$ implies $G_i \approx G_j$, the converse is false. In fact, as we shall see in Example 1, §4, G_i may be isomorphic to G_j even though $\mathfrak{G}_i$ and $\mathfrak{G}_j$ are incompatible extensions of $\mathfrak{F}$.

4. **Pathological extensions of limit degree one.** We turn now to the special case which motivated this investigation. The notation and assumptions of §3 remain in force throughout this section.

THEOREM 4.1. *$\mathfrak{G}_i$ is a monadic extension of $(\mathfrak{F}, \sigma)$ if and only if $G_i = \{e\}$. Furthermore, if one $\mathfrak{G}_i$ is a monadic extension of $(\mathfrak{F}, \sigma)$, then $\mathfrak{G}_j$ is a monadic extension of $(\mathfrak{F}, \sigma)$ for every j.*

Proof. The first statement follows from the fact that $\mathfrak{G}$ is a normal extension of $\mathfrak{F}$. The second statement is an immediate consequence of the corollary to Theorem 3.2.

Thus a necessary condition that a $\mathfrak{G}_i$ be a monadic extension of $(\mathfrak{F}, \sigma)$ is that G admit an automorphism leaving only the neutral element fixed. Furthermore, this condition is independent of σ and is a function of $\mathfrak{F}$ and $\mathfrak{G}$ only. J. G. Thompson [16] has shown that if a finite group admits an automorphism of prime order leaving only the neutral element fixed, then the group must be nilpotent. Previously, Burnside [2], B. H. Neumann [14], W. Feit [9], and G. Higman [12] had obtained results on this problem, but little is known if the automorphism is of composite order, other than that the group may even be solvable but not nilpotent [10].

In connection with the above remarks it should be noted that the second assertion of Theorem 4.1 can be proved in a purely group-theoretic context as follows:

The mapping $s_i \to s_i^* s_i^{-1}$ of G is one-to-one if $s_i \to s_i^*$ leaves only the neutral element fixed; for if $s_i^* s_i^{-1} = s_j^* s_j^{-1}$, then $(s_j^{-1} s_i)^* = s_j^{-1} s_i$ implying $s_i = s_j$. The second part of Theorem 4.1 is simply the assertion that only the neutral element of G is mapped into a conjugate by $s_i \to s_i^*$. Suppose such were not the case. Let $s_i^* = s_j s_i s_j^{-1}$ and let s_k be the unique solution of the equation $s_x^* = s_j s_x$. Then $(s_i s_k)^* = (s_j s_i s_j^{-1})(s_j s_k) = s_j(s_i s_k)$ implying $s_k = s_i s_k$ or $s_i = e$.

We have seen that an abstract finite group G can be the Galois group of a monadic extension only if G admits an automorphism leaving only the neutral element fixed. Turning now to the other extreme we ask, "What restriction must be placed on G if the $\mathfrak{G}_i$ are to be mutually incompatible?" Here the criterion is particularly simple and is given in the corollary to Theorem 4.4.

THEOREM 4.2. *$\mathfrak{G}_i$ and $\mathfrak{G}_j$ are compatible extensions of $(\mathfrak{F}, \sigma)$ if and only if they are isomorphic over $(\mathfrak{F}, \sigma)$.*

Proof. Suppose $\mathfrak{G}_i$ and $\mathfrak{G}_j$ are compatible. Then there exist isomorphisms θ, ϕ of $\mathfrak{G}_i$, $\mathfrak{G}_j$ respectively onto fields $(\mathfrak{K}, \mu)$, $(\mathfrak{K}, \mu)$ contained in an extension $(\mathfrak{L}, \mu)$ of $(\mathfrak{F}, \sigma)$. Since $\mathfrak{K}$ and $\mathfrak{K}$ are isomorphic and are normal extensions of $\mathfrak{F}$ they must be identical. It now follows that $\phi^{-1}\theta$ gives an isomorphism of $\mathfrak{G}_i$ onto $\mathfrak{G}_j$ over $(\mathfrak{F}, \sigma)$. The converse is obvious.

THEOREM 4.3. *The n transformal Galois groups* G_i $(1 \leqq i \leqq n)$ *satisfy* $G_i \cap \mathfrak{Z}(G) = G_j \cap \mathfrak{Z}(G)$ $(1 \leqq i, j \leqq n)$, *where* $\mathfrak{Z}(G)$ *is the center of* G.

Proof. Let $s \in G_i \cap \mathfrak{Z}(G)$. Since $s \in G_i$ we have $s^* = s_i s s_i^{-1}$. Now $s \in \mathfrak{Z}(G)$ gives $s^* = s$ implying $s \in G_1$. But $s \in G_1 \cap \mathfrak{Z}(G)$ implies $s_j s s_j^{-1} = s = s^*$. Thus $s \in G_j \cap \mathfrak{Z}(G)$. Interchanging the roles of G_i and G_j we obtain the theorem.

COROLLARY. *The n transformal Galois groups* G_i $(1 \leqq i \leqq n)$ *are all equal if and only if they are in* $\mathfrak{Z}(G)$.

Proof. By Theorem 4.3 it follows that if the groups are in $\mathfrak{Z}(G)$ then they are equal. Suppose $G_i = G_j$ $(1 \leqq i, j \leqq n)$ and let $s \in G_i$. Then $s^* = s$ since $s \in G_1$ and $s_j s s_j^{-1} = s^* = s$ $(1 \leqq j \leqq n)$ since $s \in G_j$. Hence $s \in \mathfrak{Z}(G)$.

An extension $\mathfrak{G}_i$ of $(\mathfrak{F}, \sigma)$ is said to be an *isolated extension* of $(\mathfrak{F}, \sigma)$ if $\mathfrak{G}_i$ is incompatible with each $\mathfrak{G}_j$ $(j = 1, 2, \cdots, i, \cdots, n)$. By Theorem 4.2, $\mathfrak{G}_i$ is isomorphic to no $\mathfrak{G}_j$ $(j \neq i)$, and hence each $s \in G$ must give an automorphism of $\mathfrak{G}_i$. Conversely, if $G_i = G$, then $\mathfrak{G}_i$ must be an isolated extension of $(\mathfrak{F}, \sigma)$. For if not, it follows from Theorem 4.2 that $\mathfrak{G}_i \approx \mathfrak{G}_j$ for some j $(j \neq i)$. But since $G_i = G$ this implies the existence of an element $s \in G$ which gives an automorphism of $\mathfrak{G}_i$ and an isomorphism of $\mathfrak{G}_i$ onto $\mathfrak{G}_j$. This is clearly impossible, and we have proved the following

THEOREM 4.4. *An extension* $\mathfrak{G}_i$ *is an isolated extension of* $(\mathfrak{F}, \sigma)$ *if and only if* $G_i = G$.

COROLLARY. *If the extensions* $\mathfrak{G}_i$ $(1 \leqq i \leqq n)$ *are mutually incompatible, then* G *is Abelian.*

Proof. To say that the $\mathfrak{G}_i (1 \leqq i \leqq n)$ are mutually incompatible is to say that each $\mathfrak{G}_i$, $(1 \leqq i \leqq n)$ is isolated, i.e., $G_i = G$ $(1 \leqq i \leqq n)$ by Theorem 4.4. By the corollary to Theorem 4.3 we must have $\mathfrak{Z}(G) = G$.

Returning now to more general considerations, we have shown that for any $\mathfrak{G}_i$, k_i ord $G_i = n$, where k_i is the number or extensions $\mathfrak{G}_j$ in the isomorphism class of $\mathfrak{G}_i$. In particular either all the $\mathfrak{G}_i$ are monadic or at least two of the extensions are incompatible. These results do not depend on any restrictive property of the group G. It is natural to expect that the imposition of a restriction on G will in turn limit the range of possibilities for the $\mathfrak{G}_i$. Thus if G is of prime order, either the $\mathfrak{G}_i$ are all monadic or mutually incompatible. As a further example suppose G is of order $n = pq$, where p and q are distinct primes. We shall show that there are four possibilities in this case:

(1) The $\mathfrak{G}_i$ $(1 \leqq i \leqq n)$ are monadic.

(2) The $\mathfrak{G}_i$ $(1 \leqq i \leqq n)$ are mutually incompatible.

(3) There are p isomorphism classes of fields each with transformal Galois group of order p, or there are q classes with group of order q.

(4) There is one isolated extension, a extensions with transformal Galois group of order p, and b extensions with group of order q, where a, b is a solution of the Diophantine equation $qx + py = n - 1$.

Proof. Suppose there are no monadic or isolated extensions. Denoting by a the number of classes of extensions with group of order p and by b the number with group of order q, we have by the corollary to Theorem 3.2, $a/p + b/q = 1$, or $aq + bp = pq$. Then $p \mid a$, $q \mid b$ and we may write $pqm + pqm' = pq$, where m and m' are positive integers. Then $m + m' = 1$, implying either $m = 0$ or $m' = 0$, i.e. either $a = 0$, $b = q$, or $a = p$, $b = 0$.

Suppose there is an isolated extension. Then it is easy to see that the total number of isolated extensions is the order of $\mathfrak{Z}(G)$. However the center of a group of order pq is either the entire group or the neutral element. Hence either all the extensions are isolated or just one is. In the latter case, using a and b as before, we have by the corollary to Theorem 3.2:

$$a/p + b/q + 1/pq = 1,$$

or

$$aq + bp = n - 1.$$

It is easy to see that this equation has just one positive solution.

We conclude this section with several examples.

EXAMPLE 1. Define the transform of a rational function $f(x)$ with coefficients in the complex field $\mathfrak{C}$ to be $f^*(x)$, the function obtained by replacing each coefficient in $f(x)$ by its complex conjugate. The field $(\mathfrak{F}, \sigma)$ is then $\mathfrak{C}(x)$ with σ defined by the above. Let $\mathfrak{G} = \mathfrak{F}(\alpha)$, where α is a fourth root of x. The Galois group G of $\mathfrak{G}$ over $\mathfrak{F}$ is the cyclic group of order four, and if $\mathfrak{G}_1$ is defined by the specification that α is its own transform, then the σ-automorphism of G is given by

$$s_i^* = s_i \qquad (i = 1, 2).$$
$$s_3^* = s_4$$

where s_2 is the element of order two in G. It is easy to see that G_i $(1 \leqq i \leqq 4)$ is the subgroup of order two. Furthermore, the formula $1/4(\sum_{i=1}^{4} \text{ord } G_i)$ shows that there are two isomorphism classes easily verified to be $\{\mathfrak{G}_1, \mathfrak{G}_2\}$, $\{\mathfrak{G}_3, \mathfrak{G}_4\}$.

Even in a case as simple as the present example we observe basic differences from the situation in algebra and differential algebra. Consider, for example, the field $\mathfrak{G}_1$ and the fixed field of G_1, $\mathfrak{F}\langle\alpha^2\rangle$. It can be shown that $\mathfrak{F}\langle\alpha^2\rangle$ admits a nontrivial automorphism over $\mathfrak{F}$. However, since $\mathfrak{F}\langle\alpha^2\rangle$ is the fixed field of G_1, the automorphism cannot be extended to an automorphism of $\mathfrak{G}_1$ over $\mathfrak{F}$. Thus we have the anomalous fact that an intermediate difference field may have as many automorphisms as the given extension, some of which cannot be obtained by restricting automorphisms of the given extension.

EXAMPLE 2. If the transforming operation on $\mathfrak{F}$ is the identity, then $\mathfrak{G}_1$ is isolated and the group G_i is the normalizer of $s_i (1 \leqq i \leqq n)$. Furthermore the extension $\mathfrak{G}_i$ is isolated if and only if $s_i \in \mathfrak{Z}(G)$. Evidently the intermediate

difference fields contained in $\mathcal{G}_i$ are those intermediate algebraic fields $\mathfrak{K}$ which are the fixed fields of subgroups H with the property $s_iHs_i^{-1}=H$. (We return to such considerations in §5.) In particular consider the difference field $(\mathfrak{F}, \sigma)=R\langle a, b, c\rangle$, where R is the field of rational numbers and a, b, and c independent indeterminates each equal to its transform. If $A(y)=y^3+ay^2+by+c$, then by adjoining the Galois resolvent of $A(y)$ to $(\mathfrak{F}, \sigma)$ we obtain a field $\mathcal{G}$ whose Galois group is the symmetric group of order 3!. Then the transformal Galois groups are given by

$$G_i = \begin{cases} G & \text{if } i = 1, \\ s_1, s_i & \text{if } 2 \leqq i \leqq 4, \\ s_1, s_5, s_6 & \text{if } i = 5, 6, \end{cases}$$

where s_1 is the neutral element of G; s_2, s_3, s_4 are the elements of order two; and s_5, s_6 are the elements of order three. Using the condition for isomorphisms between fields given in §3, we find that $\mathcal{G}_i \approx \mathcal{G}_j$ if and only if s_j is conjugate to s_i. Hence there are three isomorphism classes

$$\{\mathcal{G}_1\}, \{\mathcal{G}_2, \mathcal{G}_3, \mathcal{G}_4\}, \{\mathcal{G}_5, \mathcal{G}_6\}.$$

We observe that the elements of the second class have unequal Galois groups.

In general, if $s \in G$ establishes an isomorphism from $\mathcal{G}_i$ onto $\mathcal{G}_j$ and if $s_k \in G_i$, then the mapping $s_k \rightarrow ss_ks^{-1}$ is an isomorphism of G_i onto G_j. Thus we have

THEOREM 4.6. *$G_i = G_j$ for every j such that $\mathcal{G}_i \approx \mathcal{G}_j$ if and only if G_i is normal.*

As in Example 2 the normal difference fields generated by the adjunction of the roots of the general equation of order $n \geqq 3 (n \neq 6)$ will give neither mutually incompatible extensions nor monadic extensions since the corresponding Galois group is the symmetric group. This follows from the fact that the symmetric group of order $n (n \geqq 3,\ n \neq 6)$ is complete, i.e. has no center and every automorphism is inner.

Since the Galois group of a given extension remains unchanged if the definition of transforming in the ground field is altered, we can never expect to obtain sufficient conditions for the extension to be pathological by imposing restrictions on the Galois group alone. This observation is borne out by

EXAMPLE 3. Let the field $\mathfrak{F}$ be the field of rational functions of x with coefficients in the field of complex numbers; let $\mathcal{G}$ be the splitting field of y^9-x. If the transforming map σ on $\mathfrak{F}$ is the identity, then the $\mathcal{G}_i$ are mutually incompatible; if

$\sigma: f(x) \rightarrow f^*(x)$, then the $\mathcal{G}_i$ are monadic; if

$\sigma: f(x) \rightarrow f^*(x^2)$, then the $\mathcal{G}_i$ all have transformal Galois groups of order three.

As we saw in Example 2, the nature of the transforming operation may be sufficient to guarantee the nonexistence of certain types of extensions.

Thus if the transforming operation on the ground field is the identity, we can never obtain monadic extensions. However, if $(\mathfrak{F}, \sigma)$ is as in Example 1, then the adjunction of the zeros of y^3-x gives mutually incompatible extensions of $(\mathfrak{F}, \sigma)$, whereas in Example 3 we obtained monadic extensions, and in Example 1 two isomorphism classes of two fields each.

5. **Intermediate difference fields.** It is natural to ask how much of the fundamental theorem of Galois theory can be taken over to the extensions of difference fields of limit degree one. Example 1 and the existence of monadic extensions indicate that we cannot hope to obtain an analogue by replacing the set of intermediate algebraic fields by the set of intermediate difference fields and restricting the group G to G_i.

THEOREM 5.1. (a) *The difference fields intermediate to* $(\mathfrak{F}, \sigma)$ *and* $\mathfrak{G}_i$ *are those intermediate algebraic fields* $\mathfrak{K}$ *whose corresponding group* $G(\mathfrak{K})$, *the subgroup of* G *leaving* $\mathfrak{K}$ *invariant, is invariant under the* σ_i*-automorphism of* G. (b) *If* $(\mathfrak{K}, \sigma_i)$ *is an intermediate, normal difference field, then the transformal Galois group of* $(\mathfrak{K}, \sigma_i)$ *over* $(\mathfrak{F}, \sigma)$ *is isomorphic to the factor group* $G^{(i)}(\mathfrak{K})/G(\mathfrak{K})$, *where* $G^{(i)}(\mathfrak{K})$ *is the totality of elements* $s\in G$ *such that* $[s, \sigma_i]\in\mathfrak{G}(\mathfrak{K})$, *where* $[s, \sigma_i]=s^{-1}\sigma_i^{-1}s\sigma_i$. (c) *If* $(\mathfrak{K}, \sigma_i)$ *is normal and* $G_i(\mathfrak{K})$ *is the sub-group of* G_i *leaving* $(\mathfrak{K}, \sigma_i)$ *invariant, then* $[G_i: G_i(\mathfrak{K})]\leqq[G^{(i)}(\mathfrak{K}): G(\mathfrak{K})]\leqq\text{ord } G_i$. (d) *If* $[\mathfrak{G}: \mathfrak{F}]$ *is not prime, then there exists an intermediate difference field except possibly for the case in which* G *is an Abelian group of prime-power order.*

Proof. (a) If $\sigma_i^{-1}G(\mathfrak{K})\sigma_i=G(\mathfrak{K})$, then $\sigma_i^{-1}s\sigma_i(\lambda)=\lambda$ for any $s\in G(\mathfrak{K})$, any $\lambda\in\mathfrak{K}$. Hence $s\sigma_i(\lambda)=\sigma_i(\lambda)$ and thus $\sigma_i(\lambda)\in\mathfrak{K}$. The converse follows by reversing the steps.

(b) Since $(\mathfrak{K}, \sigma_i)$ is a difference field we have, by (a), $\sigma_i^{-1}G(\mathfrak{K})\sigma_i=G(\mathfrak{K})$. Then it is easy to see that the map $sG(\mathfrak{K})\to\sigma_i^{-1}sG(\mathfrak{K})\sigma_i$ is well-defined and is in fact an automorphism of $G/G(\mathfrak{K})$. Since the transforming operation in $(\mathfrak{K}, \sigma_i)$ is given by restricting σ_i to $\mathfrak{K}$, it follows that the restriction of the σ_i-automorphism of G to $G/G(\mathfrak{K})$ corresponds in the natural isomorphism between $G/G(\mathfrak{K})$ and the Galois group H of $\mathfrak{K}$ over $\mathfrak{F}$ to the σ_i-automorphism of H.

If a coset $sG(\mathfrak{K})$ is left fixed by the σ_i-automorphism, then a simple computation shows $[s, \sigma_i]\in G(\mathfrak{K})$, and conversely if $[s, \sigma_i]\in G(\mathfrak{K})$ then $sG(\mathfrak{K})$ is left fixed by the σ_i-automorphism. The totality of elements $s\in G$ for which $[s, \sigma_i]\in G(\mathfrak{K})$ form a subgroup $G^{(i)}(\mathfrak{K})$ of G and clearly $G(\mathfrak{K})\subset G^{(i)}(\mathfrak{K})$. Furthermore $G^{(i)}(\mathfrak{K})$ is invariant under the σ_i-automorphism of G. Then, as in the proof of the corresponding theorem in algebra, we show $G^{(i)}(\mathfrak{K})/G(\mathfrak{K})$ is isomorphic to the transformal Galois group of $(\mathfrak{K}, \sigma_i)$ over $(\mathfrak{F}, \sigma)$.

(c) Let $s_j, s_k\in G^{(i)}(\mathfrak{K})$ and suppose $[s_j, \sigma_i]=[s_k, \sigma_i]$. Then $s_ks_j^{-1}=s_i^{-1}(s_ks_j^{-1})^*s_i$ and thus $s_ks_j^{-1}\in G_i$. Conversely, if $s_ks_j^{-1}\in G_i$, then $[s_j, \sigma_i]=[s_k, \sigma_i]$. Since G_i is a subgroup of $G^{(i)}(\mathfrak{K})$, it follows that the number m of elements of $G(\mathfrak{K})$ of the form $[s_j, \sigma_i]$ is equal to $[G^{(i)}(\mathfrak{K}): G_i]$. Hence

m = ord $G^{(i)}(\mathfrak{C})$/ord G_i = $[G^{(i)}(\mathfrak{C}): G(\mathfrak{C})]$(ord $G(\mathfrak{C})$/ord G_i), or $[G^{(i)}(\mathfrak{C}): G(\mathfrak{C})]$/ord $G_i = m$/ord $G(\mathfrak{C}) \leqq 1$. Hence $[G^{(i)}(\mathfrak{C}): G(\mathfrak{C})] \leqq$ ord G_i.

Now defining $G_i(\mathfrak{C}) = G(\mathfrak{C}) \cap G_i$, we have $[G_i: G_i(\mathfrak{C})] =$ ord G_i/ord $G_i(\mathfrak{C})$ = ord G_i/ord $(G(\mathfrak{C}) \cap G_i)$ = ord $(G(\mathfrak{C}) \cdot G_i)$/ord $G(\mathfrak{C})$, by the First Isomorphism Theorem. But $G(\mathfrak{C}) \subset G^{(i)}(\mathfrak{C})$, and $G_i \subset G^{(i)}(\mathfrak{C})$. Hence ord $(G(\mathfrak{C}) \cdot G_i) \leqq$ ord $G^{(i)}(\mathfrak{C})$, and thus $[G_i: G_i(\mathfrak{C})] \leqq [G^{(i)}(\mathfrak{C}): G(\mathfrak{C})]$.

It can be shown that $G_i/G_i(\mathfrak{C})$ is isomorphic to a subgroup of H but not necessarily to H itself. Furthermore, Example 1 shows that $G^{(i)}(\mathfrak{C})$ may be greater than the product of G_i and $G(\mathfrak{C})$.

(d) If $\mathfrak{G}_i$ is not a monadic extension of $(\mathfrak{F}, \sigma)$, then the field corresponding to G_i is an intermediate difference field, or if $G_i = G$ then any intermediate algebraic field is a difference field. If $\mathfrak{G}_i$ is monadic then by Herstein [11] there exists a Sylow p-group fixed under the σ_i-automorphism of G for every prime p dividing the order of G. Hence if there are no intermediate difference fields then the order of G must be a power of a prime. But then the center of G is a nontrivial characteristic subgroup and hence the fixed field of the center is a difference field. Thus if there are no intermediate difference fields, G must be Abelian.

Part (c) can be strengthened when $\mathfrak{G}_i$ is a monadic extension of $(\mathfrak{F}, \sigma)$. For simplicity we take $i = 1$ and let $(\mathfrak{C}, \sigma)$ be an intermediate difference field. We claim $(\mathfrak{C}, \sigma)$ is a monadic extension of $(\mathfrak{F}, \sigma)$. For suppose there exist elements s, s_1, $s_2 \in G$ such that s_1 and s_2 are isomorphisms of $(\mathfrak{C}, \sigma)$ into $(\mathfrak{G}, \sigma s^{-1})$ and thus $s_i^{-1} s s_i^* \in H$, $i = 1, 2$, where $H = G(\mathfrak{C})$. For fixed s, the element $s_x^{-1} s s_x^*$ ranges over G as s_x ranges over G, for if $s_x^{-1} s s_x^* = s_y^{-1} s s_y^*$, then $(s_x s^{-1})^* = s^{-1} s_x s_y^{-1} s$ implying $s_x = s_y$ since only the identity is mapped into a conjugate by the σ-automorphism of G. But if $s_1^{-1} s s_1^* \in H$, so is $(s_1 h)^{-1} s (s_1 h)^*$, $h \in H$, and by the previous sentence H is exhausted by elements of this form. Hence $s_2 \in s_1 H$ and $(\mathfrak{C}, \sigma)$ is a monadic of $(\mathfrak{F}, \sigma)$.

Extensions of the type mentioned in (d) can be realized. For example, let $(\mathfrak{F}, \sigma)$ be an inversive difference field and let λ be a generic zero of $\{y_2 - y y_1\}$, where $y_2 - y y_1$ is a difference polynomial of $\mathfrak{F}\{y\}$. The inversive closure $\mathfrak{G}$ of $\mathfrak{F}\langle\lambda\rangle$ contains no square root of λ, for otherwise a square root of λ_n would be in $\mathfrak{F}\langle\lambda\rangle$ for some $n \geqq 0$, and thus $y_n^2 = \lambda_n$ would be reducible, contradicting the fact that $(\mathfrak{F}, \sigma)$ is inversive. If now γ is a solution of $y^2 - \lambda$ in $\mathfrak{G}\{y\}$, with $\gamma_2 = \gamma\gamma_1$, then, using the fact that λ and λ_1 are algebraically independent over $\mathfrak{F}$, we find that the Galois group G of $\mathfrak{G}\langle\gamma\rangle$ over $\mathfrak{G}$ is the four group. The σ-automorphism of G leaves no element other than the identity fixed and permutes regularly the three subgroups of order two.

The nature of the $\mathfrak{G}_i$ clearly depends on the ground field $\mathfrak{F}$. Thus if $\mathfrak{F}$ is extended to the intermediate field $\mathfrak{K}$, $\mathfrak{G}_i$ may be a monadic or an isolated extension of $(\mathfrak{K}, \sigma)$ though neither was the case originally. Hence if $G(\mathfrak{K}) \cap G_i = \{e\}$ or $G(\mathfrak{K}) \cap G_i = G(\mathfrak{K})$, then $\mathfrak{G}_i$ is a monadic or an isolated extension of $(\mathfrak{K}, \sigma)$ respectively.

EXAMPLE. Let $(\mathfrak{F}, \sigma)$ be as in Example 1; let $\mathfrak{G}=\mathfrak{F}(\alpha)$, where α is a sixth root of x. Then G is the cyclic group of order six whose elements are given by

$$s_i(\alpha) = \omega^{i-1}\alpha \qquad (1 \leqq i \leqq 6)$$

while $G_i = \{s_1, s_4\}$ $(1 \leqq i \leqq 6)$. Then each $\mathfrak{G}_i$ is an isolated extension of the fixed field of $G_i (1 \leqq i \leqq 6)$, but a monadic extension of the fixed field of $\{s_1, s_3, s_5\}$.

REFERENCES

1. N. Bourbaki, *Algèbre*, Chapter IV-V, Actualités Sci. Ind. 1102, Paris, Hermann et Cie, 1960.

2. W. Burnside, *Theory of groups*, 2nd ed., New York, Dover, 1950.

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

4. ———, *Inversive difference fields*, Bull. Amer. Math. Soc. vol. 55 (1949) pp. 597–603.

5. ———, *Extensions of difference fields*, Amer. J. Math. vol. 74 (1952) pp. 507–530.

6. ———, *Specializations over difference fields*, Pacific J. Math. vol. 5 (1955) pp. 887–905.

7. ———, *Finitely generated extensions of difference fields*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 3–5.

8. ———, *An invariant of difference field extensions*, Proc. Amer. Math. Soc. vol. 7 (1956) pp. 656–661.

9. W. Feit, *On the structure of Frobenius groups*, Canad. J. Math. vol. 9 (1957) pp. 587–596.

10. D. Gorenstein, *Finite groups which admit an automorphism with few orbits*, Canad. J. Math. vol. 12 (1960) pp. 73–100.

11. I. N. Herstein, *A remark on finite groups*, Proc. Amer. Math. Soc. vol. 9 (1958) pp. 255–257.

12. G. Higman, *Groups and rings which have automorphisms without non-trivial fixed elements*, J. London Math. Soc. vol. 32 (1957) pp. 321–334.

13. E. R. Kolchin, *Galois theory of differential fields*, Amer. J. Math. vol. 75 (1953) pp. 753–824.

14. B. H. Neumann, *Groups with automorphisms leaving only the neutral element fixed*, Arch. Math. vol. 7 (1956) pp. 1–5.

15. J. F. Ritt, *Complete difference ideals*, Amer. J. Math. vol. 63 (1941) pp. 681–690.

16. J. G. Thompson, *Frobenius groups and a related problem*, Notices Amer. Math. Soc. vol. 5 (1958) p. 695.

U. S. ARMY SIGNAL R/D LABORATORY
FORT MONMOUTH, N. J.