Finitely Generated Extensions of Difference Fields

Richard M. Cohn

Let \( \mathcal{J}, \mathcal{K}, \mathcal{K}' \) be difference fields such that \( \mathcal{J} \subseteq \mathcal{K} \subseteq \mathcal{K}' \). We shall prove that if \( \mathcal{K}' \) is a finitely generated extension of \( \mathcal{J}, \mathcal{K}' = \mathcal{J}(\alpha_1, \alpha_2, \ldots, \alpha_n) \), then \( \mathcal{K} \) is also a finitely generated extension of \( \mathcal{J} \).

We introduce a new notation for the \( \alpha_i \). Let \( \beta_1, \ldots, \beta_q \) denote a subset of the \( \alpha_i \) annulling no nonzero difference polynomial with coefficients in \( \mathcal{K} \) and such that each \( \alpha_i \) annuls some nonzero difference polynomial with coefficients in \( \mathcal{K}(\beta_1, \ldots, \beta_q) \). We denote the \( \alpha_i \) not included among the \( \beta_i \) by \( \gamma_1, \ldots, \gamma_p, p = n - q \).

Let \( \Lambda \) be the reflexive prime difference ideal in \( \mathcal{K}(\beta_1, \ldots, \beta_q; \gamma_1, \ldots, \gamma_p) \) with the generic zero \( u_i = \beta_i, \ i = 1, \ldots, q; \gamma_j = \gamma_j, \ j = 1, \ldots, p \). We denote a characteristic set of \( \Lambda \) by

\[
(1) \quad A_{10}, \ldots, A_{1k_1}; \ A_{20}, \ldots, A_{2k_2}; \ldots; \ A_{p0}, \ldots, A_{pk_p},
\]

where \( A_{i0} \) introduces \( \gamma_i \). Let \( \mathcal{G} \) be the difference field formed by adjoining the coefficients of the \( A_{ij} \) to \( \mathcal{J} \). Evidently \( \mathcal{G} \subseteq \mathcal{K} \). The result stated above will follow when we show that \( \mathcal{G} = \mathcal{K} \).

We shall describe what we mean by the characteristic sequences \( B_{ij}, i = 1, \ldots, p; j = 0, 1, \ldots, \) of \( \Lambda \) formed from (1). This concept has been previously defined only in special cases.

Let \( t_i \) denote the order of \( A_{i0} \) in \( \gamma_i \). We let \( B_{10} = A_{10} \). Suppose \( B_{10}, \ldots, B_{1,k-1} \) have been defined. Then, if there is an \( A_{ij} \) of order \( t_i + k \) in \( \gamma_i \), we let \( B_{ik} \) be that \( A_{ij} \). Otherwise \( B_{ik} \) is defined as the remainder of the transform of \( B_{1j} \) with respect to the chain \( B_{10}, \ldots, B_{1,k-1} \). It is easy to see that, for any \( r, B_{1r} \) is of order \( t_i + r \) in \( \gamma_i \) and, unless it is equal to some \( A_{ij} \), of the same degree in the \( (t_i + r) \)th transform of \( \gamma_i \) as is \( A_{ij} \) in the \( (t_i + r) \)th transform of \( \gamma_i \).

Let \( B_{20} = A_{20} \). Suppose \( B_{20}, \ldots, B_{2,k-1} \) have been defined. Then if

Received by the editors March 1, 1954.

1 The brackets \( \langle \ \rangle \) denote field adjunction of the enclosed elements and their transforms so as to form a difference field. Similarly, brackets \( \{ \ \} \) denote ring adjunction of the enclosed elements and their transforms. Field and ring adjunctions in the usual sense are denoted by brackets \( \langle \ \rangle \) and \( \{ \ \} \) respectively. For other terms used see [1] (where the term “basic set” corresponds to our “characteristic set”) and [3].

2 If \( p = 0 \), \( \Lambda \) is the ideal consisting only of 0, and no \( A_{ij} \) are defined.

3 If \( p = 0 \), we define \( \mathcal{G} \) to be \( \mathcal{J} \).

4 Throughout this discussion we form the remainder treating the \( B_{ij} \) not as difference polynomials but as polynomials as in Chapter IV of [2]. The \( \gamma_{ij} \), \( j \geq t_i \), are ordered lexicographically. The remaining \( \gamma_{ij} \) and the \( u_{ij} \) precede them and are ordered among themselves in any convenient way. Of course, only a finite number of indeterminates are present and need be ordered at any step.
there is an $A_{2j}$ of order $t_2 + k$ we let $B_{2k}$ be that $A_{2j}$. Otherwise $B_{2k}$ is defined as the remainder of the transform of $B_{2,k-1}$ with respect to the chain $B_{10}, \ldots, B_{1r}; B_{20}, \ldots, B_{2,k-1}$, where $r$ is chosen as the least integer such that no transform of $y_{10}$ occurring in $B_{20}, \ldots, B_{2,k-1}$ or the transform of $B_{2,k-1}$ is of order exceeding $t_1 + r$. Proceeding similarly we let $B_{30} = A_{30}$. When $B_{30}, \ldots, B_{3,k-1}$ have been defined, we define $B_{3k}$ as the $A_{3j}$ of the proper order, if such exists, or as the remainder of the transform of $B_{3,k-1}$ with respect to $B_{10}, \ldots, B_{1s}; B_{20}, \ldots, B_{2r}$, where $s$ and $r$ are such that no transform of $y_{20}$ occurring in $B_{30}, \ldots, B_{3,k-1}$ or the transform of $B_{3,k-1}$ is of order exceeding $t_2 + r$, and that no transform of $y_{10}$ occurring in these polynomials or in $B_{20}, \ldots, B_{2r}$ is of order exceeding $t_1 + s$.

Continuing in this way we define the $B_{ij}$, $i = 1, \ldots, p; j = 0, 1, \ldots$. Each $B_{ij}$ is order $t_i + j$ in $y_i$, and it is either a polynomial of the characteristic set of $\Lambda$ which is of this order in $y_i$ and free of $y_k$, $k > i$, or it is of the same degree in the $(t_i+j)$th transform of $y_i$ as is $B_{i-1,j-1}$ in the $(t_i-1+j)$th transform of $y_i$. Of course, $B_{ij}$ is free of $y_k$, $k > i$.

Given an integer $r \geq 0$ we let $s_p$ denote the maximum of $t_p$ and $r$. Let $r_p = s_p - t_p$. Then define $s^{(p-1)}$ to be the maximum of $t_{p-1}$, $r$, and the order of the highest transform of $y_{p-1}$ appearing in the polynomials $B_{p0}, \ldots, B_{pr_p}$, and let $r_{p-1} = s_{p-1} - t_{p-1}$. We define $s_{p-2}$ as the maximum of $t_{p-2}$, $r$, and the order of the highest transform of $y_{p-2}$ occurring in $B_{p-1,0}, \ldots, B_{p-1,r_{p-1}}; B_{p0}, \ldots, B_{pr_p}$. Continuing in this way we define successively $s_{p-3}, s_{p-4}, \ldots, s_1$ and let $r_i = s_i - t_i$, $i = 1, \ldots, p$. Then

(2) \[ B_{10}, \ldots, B_{1r_1}; B_{20}, \ldots, B_{2r_2}; \ldots; B_{p0}, \ldots, B_{pr_p} \]

is a chain. For $s$ such that no $u_{ij}, j > s$, occurs in (2) we define $\Lambda_{sr}$ as the prime p. i. (polynomial ideal) in the indeterminates $u_{ij}$, $i = 1, \ldots, q; j = 0, 1, \ldots, s$, and $y_{km}$, $k = 1, \ldots, p; m = 0, 1, \ldots, s$, which consists of those polynomials of $\Lambda$ which involve only these $u_{ij}$ and $y_{km}$. Then (2) constitutes a characteristic set for $\Lambda_{sr}$ with $B_{ij}$ introducing $y_{i,t_i+j}$. The parametric indeterminates of $\Lambda_{sr}$ corresponding to this choice of characteristic set are those $u_{ij}$ occurring among its indeterminates and the $y_{km}$ with $m < l_m$. We note that all coefficients of the $B_{ij}$ are rational combinations of the coefficients appearing in (1) and their transforms.

Let $\lambda$ be any element of $\mathcal{C}$. It will evidently suffice to show that $\lambda$ is in $\mathcal{G}$. We choose a positive integer $r$ such that $\lambda$ is in the field formed by adjoining to $\mathcal{F}$ the $\alpha_{ij}$, $i = 1, \ldots, n; j = 0, \ldots, r$. Let $s \geq r$ be such that, with the $r$ just chosen, (2) is a characteristic set of

---

6 Following Chapter IV of [2] we use this term to distinguish ideals of polynomials in the usual sense from difference ideals.
a prime $p$. By the last remark of the preceding paragraph the coefficients of (2) are in $G$. Since also $G \subseteq \mathcal{C}$ it is readily seen that (2) is the characteristic set of a prime $p$ with coefficients in $G$ and involving the same indeterminates as $\Lambda_r$. Similarly (2) is the characteristic set of a prime $p'$ with coefficients in $G(\lambda)$ and involving the same indeterminates as $\Lambda_r$.

We obtain a generic zero of $\Lambda_r$, $\Pi$, or $\Pi'$ by putting $u_{ij} = b_{ij}$; $y_{ij} = r_{ij}$ for the appropriate ranges of the subscripts. We shall denote by $\delta_k$, where $k$ ranges over a suitable set of integers, those $b_{ij}$ and $r_{ij}$ of the generic zero which have been equated to the $u_{ij}$ and $y_{ij}$ of the previously described set of parametric indeterminates of $\Lambda_r$ (which are also, of course, a set of parametric indeterminates for either $\Pi$ or $\Pi'$). The remaining $y_{ij}$ of the generic zero shall henceforth be denoted by $e_m$, where $m$ ranges over a suitable set of integers.

The degree of $G(\delta_k, e_m)$ with respect to $G(\delta_k)$ is given by the product of the degrees of the polynomials of (2) in the indeterminates of $\Pi$ which they respectively introduce. We see in the same way that this product is the degree of $G(\lambda)(\delta_k, e_m)$ with respect to $G(\lambda)(\delta_k)$. But the fields $G(\lambda)(\delta_k, e_m)$ and $G(\delta_k, e_m)$ coincide because, by the stipulations concerning $r$ and $s$, $\lambda$ is in $G(\delta_k, e_m)$. Hence the degrees of $G(\delta_k, e_m)$ with respect to its two subfields $G(\delta_k)$ and $G(\lambda, \delta_k)$ are equal. Since these degrees are finite it follows that these subfields must be identical. In other words, $\lambda$ is in $G(\delta_k)$.

We thus see that there exist elements $P$ and $Q$ in $G[\delta_k]$, with $P$ not equal to zero, such that $P\lambda = Q$. Now the $\delta_k$ annul no nonzero polynomial with coefficients in $G(\lambda)$. Hence the relation $P\lambda = Q$ must be an identity in the $\delta_k$. By equating coefficients of a suitable power product of the $\delta_k$ on both sides of this equation we find $p\lambda = q$, $p$ and $q$ in $G$, and $p \neq 0$. Hence $\lambda$ is in $G$. This completes the proof.

References


Rutgers University

* This follows from the work on pp. 89 and 90 of [2]. The inductive argument given there shows that a generic zero of $\Pi$ can be constructed by transcendental adjunctions followed by successive algebraic adjunctions of degrees equal to the degrees of the polynomials of the characteristic set in the indeterminates they introduce.