EXTENSIONS OF DIFFERENTIAL FIELDS. III

E. R. KOLCHIN

The purpose of the present note is to show how the point of view of a preceding paper[1] can be used in developing the concepts of resolvent, dimension, and order introduced by J. F. Ritt in his theory of algebraic differential equations.[2] The present development, in addition to being simpler in some instances, has the advantage of being valid for abstract differential fields as opposed to fields of meromorphic functions of a complex variable, as used by Ritt. I shall also take the opportunity to correct mistakes in a related paper.[3] The notation and definitions used will be as in Extensions I and II.

1. Resolvents, dimension, and order. Let $\mathcal{F}$ be a differential field (ordinary or partial) of characteristic 0, and let $y_1, \cdots, y_n$ be unknowns. If Π is a prime differential ideal in $\mathcal{F}\{y_1, \cdots, y_n\}$ other than $\mathcal{F}\{y_1, \cdots, y_n\}$ itself then Π has a generic solution $\eta_1, \cdots, \eta_n$.

If the degree of differential transcendency of $\mathcal{F}\langle\eta_1, \cdots, \eta_n\rangle$ over $\mathcal{F}$ is q then $0 \leqq q < n$, and precisely q of the elements $\eta_1, \cdots, \eta_n$ are differentially algebraically independent over $\mathcal{F}$. Suppose, say, that $\eta_1 \cdots, \eta_q$ are independent in this way, that is, that Π does not contain a nonzero differential polynomial in $y_1, \cdots, y_q$, but does in $y_1, \cdots, y_q, y_j$ for each $j > q$. In Ritt's terminology $y_1 \cdots, y_q$ is a complete set of arbitrary unknowns for Π. It is natural to call q the *dimension* of Π (in symbols, dim Π).

Suppose henceforth that $\mathcal{F}$ is ordinary. It is easy to see that the degree of transcendency of $\mathcal{F}\langle\eta_1, \cdots, \eta_n\rangle$ over $\mathcal{F}\langle\eta_1, \cdots, \eta_q\rangle$ (both these differential fields being considered as fields) is finite. We denote the degree of transcendency of any field $\mathcal{K}$ over a subfield $\mathcal{G}$ by $\partial^0\mathcal{K}/\mathcal{G}$. It will be seen that it is natural to call the integer $\partial^0\mathcal{F}\langle\eta_1, \cdots, \eta_n\rangle/\mathcal{F}\langle\eta_1, \cdots, \eta_q\rangle$ the *order* of Π with respect to $y_1, \cdots, y_q$ (when the set of arbitrary unknowns is understood, for example when $q=0$, we use the notation: ord Π).

Presented to the Society, November 2, 1946; received by the editors October 10, 1946.

[1] Kolchin, *Extensions of differential fields*, I, Ann. of Math. vol. 43 (1942) pp. 724–729. We shall refer to this paper as *Extensions* I.

[2] The subject matter treated here, together with some of the material from *Extensions* I, is roughly parallel to the contents of §§24–31, 75 of Ritt, *Differential equations from the algebraic standpoint*, Amer. Math. Soc. Colloquium Publications, vol. 14, New York, 1932.

[3] Kolchin, *Extensions of differential fields*, II, Ann. of Math. vol. 45 (1944) pp. 358–361. We shall refer to this paper as *Extensions* II.

If $\mathcal{J}\langle\eta_1, \cdots, \eta_q\rangle$ contains a nonconstant (which is the case either when $\mathcal{J}$ does or when $q>0$) then by Extensions I there is an ω such that $\mathcal{J}\langle\eta_1, \cdots, \eta_q, \omega\rangle=\mathcal{J}\langle\eta_1, \cdots, \eta_n\rangle$. Let $A=A(\eta_1, \cdots, \eta_q, w)$ be an irreducible differential polynomial in $\mathcal{J}\langle\eta_1, \cdots, \eta_q\rangle\{w\}$, with solution $w=\omega$, of lowest possible order. Since ω and its first ord Π derivatives must be algebraically dependent over $\mathcal{J}\langle\eta_1, \cdots, \eta_q\rangle$, the order of A is not greater than ord Π. On the other hand, if the order of A is p then the pth derivative (and consequently all the derivatives) of ω is algebraically dependent over $\mathcal{J}\langle\eta_1, \cdots, \eta_q\rangle$ on ω and its first $p-1$ derivatives, so that ord $\Pi=\partial^0\mathcal{J}\langle\eta_1 \cdots, \eta_n\rangle/\mathcal{J}\langle\eta_1, \cdots, \eta_q\rangle$ $=\partial^0\mathcal{J}\langle\eta_1, \cdots, \eta_q, \omega\rangle/\mathcal{J}\langle\eta_1, \cdots, \eta_q\rangle\leqq p$. Therefore the order of A in w is $p=$ord Π. $A(y_1, \cdots, y_q, w)$ is called a *resolvent* of Π. (Actually, this is a slight generalization of Ritt's resolvent, which must be in $\mathcal{J}\{y_1, \cdots, y_q, w\}$ instead of merely in $\mathcal{J}\langle y_1, \cdots, y_q\rangle\{w\}$.)

Let $\mathcal{G}$ be a differential extension field of $\mathcal{J}$, let $\{\Pi\}=\Pi_1\cap \cdots \cap\Pi_r$ be the decomposition into prime components (that is, prime differential ideals none of which contains another) of the perfect differential ideal generated by Π in $\mathcal{G}\{y_1, \cdots, y_n\}$, and let $A_1(y_1, \cdots, y_q, w) \cdots A_s(y_1, \cdots, y_q, w)$ be the complete factorization of $A(y_1, \cdots, y_q, w)$ in $\mathcal{G}\langle y_1, \cdots, y_q\rangle\{w\}$. Each $A_i(y_1, \cdots, y_q, w)$ is of order p in w, for a factor of $A(y_1, \cdots, y_q, w)$ of order less than p would be a common factor of the coefficients in $A(y_1, \cdots, y_q, w)$ when $A(y_1, \cdots, y_q, w)$ is considered as a polynomial in w_p, the pth derivative of w. We shall now establish Ritt's result that $r=s$ and each $A_i(y_1, \cdots, y_q, w)$ is a resolvent of one Π_j. This result implies that Π decomposes if and only if $A(y_1, \cdots, y_q, w)$ factors, and that each prime component in the decomposition has the same order as Π has.

Let $\eta_1', \cdots, \eta_n'$ be a generic solution of Π_1. Then (by *Extensions* I, §1) $\eta_1', \cdots, \eta_n'$ is a generic solution of Π, so that $\eta_1'\rightarrow\eta_1, \cdots, \eta_n'\rightarrow\eta_n$ generates an isomorphism of $\mathcal{J}\langle\eta_1', \cdots, \eta_n'\rangle$ onto $\mathcal{J}\langle\eta_1, \cdots, \eta_n\rangle$. Therefore if we let ω' be the same differential rational function over $\mathcal{J}$ of $\eta_1', \cdots, \eta_n'$ that ω is of $\eta_1, \cdots, \eta_n$, we shall have

$$\mathcal{J}\langle\eta_1', \cdots, \eta_q', \omega'\rangle = \mathcal{J}\langle\eta_1', \cdots, \eta_n'\rangle.$$

Now ω' is a solution of $A'=A(\eta_1', \cdots, \eta_q', w)$, and therefore of some $A_i'=A_i(\eta_1', \cdots, \eta_q', w)$, say of A_1'. Furthermore, ω' is not a solution of two different A_i''s, for ω' does not annul the separant $\partial A'/\partial w_p=\partial(A_1' \cdots A_s')/\partial w_p$. Let ω'' be a generic solution of the prime component of $\{A_1'\}$ in $\mathcal{G}\langle\eta_1', \cdots, \eta_q'\rangle\{w\}$ not containing the separant $\partial A_1'/\partial w_p$. Then ω'' is a generic solution of the prime component of $\{A'\}$ in $\mathcal{J}\langle\eta_1', \cdots, \eta_q'\rangle\{w\}$ not containing the separant $\partial A'/\partial w_p$, so that $\omega''\rightarrow\omega'$ generates an isomorphism of $\mathcal{J}\langle\eta_1', \cdots, \eta_q', \omega''\rangle$ onto $\mathcal{J}\langle\eta_1', \cdots, \eta_q', \omega'\rangle$, and a homomorphism of $\mathcal{G}\langle\eta_1', \cdots, \eta_q'\rangle\{\omega''\}$ onto $\mathcal{G}\langle\eta_1', \cdots, \eta_q'\rangle\{\omega'\}$. Therefore, if for each $i>q$ we let η_i'' be the same differential rational function over $\mathcal{J}\langle\eta_1', \cdots, \eta_q'\rangle$ of ω'' as η_i' is of ω', then $\eta_1', \cdots, \eta_q', \eta_{q+1}'', \cdots, \eta_n''$ is a generic solution of Π and a solution of some Π_i. Since $\eta_1', \cdots, \eta_n'$ must be a solution of the same Π_i, and since one Π_i does not contain another, $\eta_1', \cdots, \eta_q', \eta_{q+1}'', \cdots, \eta_n''$ is a solution of Π_1, and indeed a generic one.

Therefore $\eta_{q+1}''\rightarrow\eta_{q+1}', \cdots, \eta_n''\rightarrow\eta_n'$ generates an isomorphism of $\mathcal{G}\langle\eta_1', \cdots, \eta_q', \eta_{q+1}'', \cdots, \eta_n''\rangle$ onto $\mathcal{G}\langle\eta_1', \cdots, \eta_n'\rangle$, A_1' is an irreducible differential polynomial in $\mathcal{G}\langle\eta_1', \cdots, \eta_q'\rangle\{w\}$, with solution $w=\omega'$, of minimal degree, and $A_1(y_1, \cdots, y_q, w)$ is a resolvent of Π_1. In the same way, every Π_i has an $A_j(y_1, \cdots, y_q, w)$ as a resolvent, so that $r\leqq s$. To show that there is no $A_j(y_1, \cdots, y_q, w)$ left over, for any j let ω_j be a generic solution of the prime component of $\{A_j'\}$ in $\mathcal{G}\langle\eta_1', \cdots, \eta_n'\rangle\{w\}$ not containing $\partial A_j'/\partial w_p$. For each $i>q$ let η_{ji} be the same differential rational function over $\mathcal{J}\langle\eta_1', \cdots, \eta_q'\rangle$ of ω_j as η_i' is of ω'. Then $\eta_1', \cdots, \eta_q', \eta_{j,q+1}, \cdots, \eta_{jn}$ is a generic solution of Π and therefore a solution of some Π_i, say Π_{i_0}. Therefore ω_j is a solution of the A_k' for which $A_k(y_1, \cdots, y_q, w)$ is a resolvent of Π_{i_0}. This implies that $A_k(y_1, \cdots, y_q, w)$ is divisible by $A_j(y_1, \cdots, y_q, w)$, so that $k=j$ and $A_j(y_1, \cdots, y_q, w)$ is a resolvent of a Π_i.

If $q=0$ and $\mathcal{J}$ consists solely of constants it is still true that each prime component of $\{\Pi\}$ has the same order as Π. To see this introduce a new unknown u and let $\mathcal{J}'=\mathcal{J}\langle u\rangle$, $\mathcal{G}'=\mathcal{G}\langle u\rangle$. The perfect differential ideal generated by Π in $\mathcal{J}'\{y_1, \cdots, y_n\}$ is clearly prime and has the same order as Π has. The prime components of the perfect differential ideal generated by Π in $\mathcal{G}'\{y_1, \cdots, y_n\}$ are the perfect differential ideals generated by $\Pi_1, \cdots, \Pi_r$, and have the same order. Therefore ord $\Pi_i=$ ord Π for each i.

2. **Corrections to Extensions II.** We refer now to the proof on page 359 of *Extensions* II. The derivation of the equation $\omega K(z)-H(z)=\alpha A(z)$ is incorrect, for it rests on the unjustified assumption (see lines 18 and 17 from the bottom) that $\partial A(z)/\partial y_p\in\mathcal{G}\{z\}$. To save the proof we delete in toto lines 22–4 from the bottom ("Denote the $\cdots A(z)$:"), and replace them by the following considerations.

Let $\omega=H(y)/K(y)$ be any coefficient in $A(z)$ not merely an element of $\mathcal{J}$, with $H(y)$, $K(y)$ free of common divisor. Clearly $\omega K(z)-H(z)\in\Sigma$.

Denote the lowest common denominator of the coefficients in $A(z)$ by $D(y)$, and let $B(y, z)=D(y)A(z)$. Then $B(y, z)\in\mathcal{F}\{y, z\}$, and $B(y, y)=0$. Since $A(z)$ is irreducible and one of the coefficients in $A(z)$ is unity, the irreducible factors of $B(y, z)$ are distinct and all have the same order in z as $A(z)$ has.

Denoting the order of $B(y, z)$ in y by p, let $B_1(y, z)$ be an irreducible factor of $B(y, z)$ of order p in y. Let Λ_1 be the prime component of $\{B_1(y, z)\}$ which contains neither of the separants of $B_1(y, z)$. No other irreducible factor of $B(y, z)$ is in Λ_1, for such a factor would have the same order in z as $B_1(y, z)$ and would be divisible by $B_1(y, z)$. Let y, ζ_1 be a generic solution of Λ_1. $B(y, z)\in\Lambda_1$ but the separant of $B(y, z)$ with respect to z is not in Λ_1 (for otherwise the separant of $B_1(y, z)$ would be in Λ_1). Therefore ζ_1 is a nonsingular solution of $A(z)$, a solution of Σ, and a solution of $\omega K(z)-H(z)$. Thus $H(y)K(z)-K(y)H(z)$ vanishes for the generic solution y, ζ_1 of Λ_1, and is in Λ_1. With order in y clearly not greater than p, $H(y)K(z)-K(y)H(z)$ must be divisible by $B_1(y, z)$.

Similarly, $H(y)K(z)-K(y)H(z)$ is divisible by all the irreducible factors $B_1(y, z), \cdots, B_s(y, z)$ of $B(y, z)$ which have order p in y. Since all these $B_i(y, z)$'s are distinct we may write

$$H(y)K(z) - K(y)H(z) = L(y, z)B_1(y, z) \cdots B_s(y, z),$$

where $L(y, z)\in\mathcal{F}\{y, z\}$. Moreover, if we denote the degree of $B(y, z)$ in y_p (the pth derivative of y) by d, we see that the degree of $H(y)K(z)-K(y)H(z)$ in y_p is not greater than d, that of $B_1(y, z) \cdots B_s(y, z)$ is d, so that $L(y, z)$ is of degree 0 in y_p, that is, of order not greater than $p-1$ in y.

Let $B_{s+1}(y, z)$ be an irreducible factor of $B(y, z)$ of order $p-1$ in y, let Λ_{s+1} be the prime component of $\{B_{s+1}(y, z)\}$ not containing the separants of $B_{s+1}(y, z)$, and let y, ζ_{s+1} be a generic solution of Λ_{s+1}. As with y, ζ_1 before, we see that y, ζ_{s+1} is a solution of $H(y)K(z)-K(y)H(z)$. But y, ζ_{s+1} is not a solution of any $B_i(y, z)$ with $i\leqq s$, for no such $B_i(y, z)$ is in Λ_{s+1}. Hence y, ζ_{s+1} is a solution of $L(y, z)$, and $L(y, z)\in\Lambda_{s+1}$. This implies, since the order of $L(y, z)$ in y is not greater than $p-1$, that $L(y, z)$ is divisible by $B_{s+1}(y, z)$.

Similarly, $L(y, z)$ is divisible by all the irreducible factors $B_{s+1}(y, z), \cdots, B_t(y, z)$ of order $p-1$ in y, so that

$$H(y)K(z) - K(y)H(z) = M(y, z)B_1(y, z) \cdots B_t(y, z),$$

where $M(y, z)\in\mathcal{F}\{y, z\}$. Moreover, if we denote the degree of $B(y, z)$ in y_p, y_{p-1} by e, we see that the degree of $H(y)K(z)-K(y)H(z)$ in y_p, y_{p-1} is not greater than e, that of $B_1(y, z) \cdots B_t(y, z)$ is e, so that $M(y, z)$ is of degree 0 in y_p, y_{p-1}, that is, of order not greater than $p-2$ in y.

Continuing in this way we finally arrive at an equation

$$H(y)K(z) - K(y)H(z) = P(z)B_1(y, z) \cdots B_w(y, z),$$

where $B_1(y, z), \cdots, B_w(y, z)$ are all the irreducible factors of $B(y, z)$. Since $H(z)$, $K(z)$ have no common divisor, $H(y)K(z)-K(y)H(z)$ has no factor free of y that is not also free of z. Therefore $P(z)\in\mathcal{J}$, and $H(y)K(z)-K(y)H(z)=aB(y, z)$, where $a\in\mathcal{J}$. The desired equation $\omega K(z)-H(z)=\alpha A(z)$ immediately follows.

The rest of the proof of the theorem as given in *Extensions* II is apparently correct.

Of the two examples given in *Extensions* II, the proof for Example 2 is incorrect, and I do not yet know whether that example is valid.

COLUMBIA UNIVERSITY