Memoirs of the College of Science, University of Kyoto, Series A,
Vol. XXV, Nos. 3 & 4, Article 18, 1949.

Basis-Theorem concerning Differential Polynomials

By

Kôtaro Okugawa

(Received May 18, 1948)

---

1. Differential polynomials. Let x be the independent complex variable and $y_1, \cdots, y_n$ the indeterminate analytic functions of x. We denote by y_{ij} the j th derivative of y_i $(i=1, \cdots, n;\ j=0, 1, 2, \cdots)$. The algebraic properties of the following two kinds of *differential polynomials* of $y_1, \cdots \cdots, y_n$ are important in the theory of systems of ordinary differential equations in the unknown functions $y_1, \cdots, y_n$:

1^0) Let $\mathfrak{F}$ be an arbitrary field which is constituted of functions, meromorphic in a fixed open domain D of the x-plane, and which is closed with respect to the differentiation. Any polynomial of y_{ij} $(i=1, \cdots, n;\ j=0, 1, 2, \cdots)$ with coefficients from $\mathfrak{F}$ is called an *algebraic differential polynomial*. We shall denote by $\mathfrak{P}_0$ the totality of all such polynomials.

2^0) Let $\mathfrak{A}$ be the totality of all functions of $x, y_1, \cdots, y_n$ which are analytic at $(x, y_1, \cdots, y_n) = (0, 0, \cdots, 0)$. Any polynomial of y_{ij} $(i=1, \cdots \cdots, n;\ j=1, 2, \cdots)$ with coefficients in $\mathfrak{A}$ will be called a *differential pseudopolynomial*. The totality of all such polynomials will be denoted by $\mathfrak{P}$.

Both $\mathfrak{P}_0$, $\mathfrak{P}$ are integral domains which are closed with respect to the differentiation.[1]

2. Basis-theorem. One of the first results, concerning these rings $\mathfrak{P}_0$ and $\mathfrak{P}$, is *the basis-theorem of Ritt*.

Let Σ be any subset of $\mathfrak{P}$ $(\mathfrak{P}_0)$. A finite subset Φ of Σ is called a *basis* of Σ if and only if there exists, for every element G of Σ, a positive integer p such that G^p is a linear combination of the elements of Φ and

1. The introductory monograph on these subjects: Ritt, J. F., Differential Equations from the Algebraic Standpoint, Amer. Math. Soc. Colloq. Publ., vol. **14**, New York, 1932. Also see his paper: Ritt, Algebraic aspects of the theory of differential equations, Semicent. Publ., Amer. Math. Soc., vol. **II** (1938). Our paper concerns directly with Ritt, Systems of differential equations, I. Theory of ideals, Amer. Journ. of Math., **60** (1938). 535—548; this paper will be quoted by RII in the following lines.

their derivatives of various orders, where the coefficients of the linear combination are elements of $\mathfrak{P}$ ($\mathfrak{P}_0$) and p may vary in accordance with the element G.

The *basis-theorem* asserts that *any subset of* $\mathfrak{P}$ ($\mathfrak{P}_0$) *has a basis.*

In the algebraic proofs[2] of the theorem, assumption is made of the existence of the "incomplete system", which turns out not to exist, and certain lemmas are established under this assumption and led to a contradiction. In this paper, we shall try a direct proof of the theorem.

In what follows, the descriptions will be limited to $\mathfrak{P}$; but, similar discussions could be done concerning $\mathfrak{P}_0$ and in this case the discussions would be much simpler, because we should not have to deal with elements which are not polynomials (in the ordinary sense) of $y_1, \cdots, y_n$.[3]

3. Reduction of the proof. In order to prove the basis-theorem, looking upon x as another dependent variable, *it is sufficient to prove it in the ring which is the totality of all differential polynomials that do not contain x effectively.*

Let $\mathfrak{A}'$ be the totality of all functions of $y_1, \cdots, y_n$ which are analytic at $(y_1, \cdots, y_n) = (0, \cdots, 0)$. Let $\mathfrak{P}'$ be the totality of all polynomials of y_{ij} $(i = 1, \cdots, n\,;\ j = 1, 2, \cdots)$ with coefficients from $\mathfrak{A}'$, then $\mathfrak{P}'$ is an integral domain which is closed with respect to the differentiation. *We have only to prove the existence of the basis for every subset Σ of $\mathfrak{P}'$.* Let (Σ) be the ideal[4] which is generated by Σ in $\mathfrak{P}'$. We can see that the *existence of the basis* (*in the sense of* § 2) *of the ideal* (Σ) *leads us to that of the set* Σ.

Now, let us fix an *ordering* of the elements of $\mathfrak{P}'$ by means of the method in RII, and call an ideal *regular* if it is *regular* as a subset of $\mathfrak{P}'$ in the sense of RII. Then we see that, *in order to prove the existence of the basis for the ideal, it is sufficient to prove it for the regular ideal of* $\mathfrak{P}'$.

4. Ranking of regular ideals. We can prove that every regular non-zero ideal of $\mathfrak{P}'$ has a *basic set*, i. e., any one of the *ascending sets* of minimal rank in the ideal. Let Σ, Σ' be two regular non-zero ideals of $\mathfrak{P}'$. If a basic set of Σ is *of lower rank* (as an ascending set) than a basic set of Σ', we call Σ *of lower rank* than Σ'. This definition of

2. Raudenbush, H. W., Ideal theory and algebraic differential equations. Trans. Amer. Math. Soc., **36** (1934), 361—368; Ritt, the last paper of the footnote 1.

3. Under the restriction of the space, we shall use the concepts in RII without repeating their definitions; also, we describe only the outlines of our proofs.

4. In this paper, we mean by "ideal" one that is closed with respect to the differentiation.

the rank is independent of the choice of a basic set from a regular ideal. If the *index* of Σ is smaller than that of Σ', then Σ is necessarily of lower rank than Σ'. In this ordering of the regular ideals, the minimal condition is satisfied. Therefore, *in order to prove the existence of the basis for regular ideals, we can rely on the induction with respect to this ranking.* The unit-ideal, which is the regular ideal of the lowest rank, has plainly the basis 1.

Now, let Σ be a regular ideal of $\mathfrak{P}'$ of the index j, and *assume that every regular ideal of lower index or of lower rank than Σ has the basis.* In § 6 we shall prove, under this assumption, that Σ must have the basis. If this would be established, then by induction, the proof of the basis-theorem would be completed. Meanwhile, let $(A) = (A_1, \cdots, A_s)$ be a basic set of Σ, and denote by S_i, I_i *the separant* and *the initial* of A_i $(i = 1, 2, \cdots, s)$. Then, both S_i, I_i are necessarily *reduced with respect to the ascending set* (A).

Under our assumption, we can prove that the ideals (Σ, S_i), (Σ, I_i), which are generated by Σ and S_i, by Σ and I_i respectively, and which are not necessarily regular, must have the bases $(i = 1, \cdots, s)$.

5. A lemma. Applying a lemma of Raudenbush,[5] we can prove:

Lemma. Let Σ be an ideal of $\mathfrak{P}'$, and let G, H two elements of $\mathfrak{P}'$ such that the ideals (Σ, G), (Σ, H) have the bases. And, let their bases be

$$\begin{array}{ll} (1) & B_1, \cdots, B_m, G, \\ (2) & B_1, \cdots, B_m, H, \end{array} \qquad (B_i \in \Sigma \ (i = 1, \cdots, m))$$

respectively (where we can assume that $B_1, \cdots, B_m$ in (1), (2) are common to both sets). Then the set

$$B_1, \cdots, B_m, GH$$

is a basis of the ideal (Σ, GH).

6. The proof of the basis-theorem. Let Σ be a regular non-zero ideal of $\mathfrak{P}'$ of the index j, and let $(A) = (A_1, \cdots, A_s)$ be a basic set of Σ.[6] Put

$$T = S_1 \cdots S_s \; I_1 \cdots I_s,$$

5. See footnote 2. The lemma asserts that, if the product GH of two differential polynomials G, H is a linear combination of a set $P_1, \cdots, P_r$ of differential polynomials and their derivatives, so are the sufficiently large powers of $(dG/dx)\,H$.

6. We can take (A) such that the first $n - j$ elements $A, \cdots, A_{n-j}$ are regular series of the classes $j + 1, \cdots, n$ respectively and that A_i is a polynomial in $y_{j+1}, \cdots, y_{j+i}$ for every $i \, (1 \leqq i \leqq n - j)$.

where S_i, I_i are the separant and the initial of A_i $(i=1, \cdots, s)$. Now, as it was mentioned in § 4, we assume that all regular ideals of the indices $< j$ or of lower ranks than Σ have the bases, and deduce that Σ itself must have the basis.

It was already remarked in § 4 that all ideals (Σ, S_i) and (Σ, I_i) $(i=1, \cdots, s)$ have the bases. Hence, according to the lemma of § 5, the ideal (Σ, T) has the basis. Let

$$B_1, \cdots, B_m, T$$

be a basis of (Σ, T). Then, it can be shown that

$$A_1, \cdots, A_s, \ B_1, \cdots, B_m$$

is a basis of Σ.

(Proof) Let F be any element of Σ. Write F as a polynomial in y_{ij} $(i=1, \cdots, n\,;\ j=1, 2, \cdots)$ with series as its coefficients:

$$F=\sum_{k=1}^{\lambda} G_k Y_k,$$

where Y_k's are distinct monomials of y_{ij} $(i=1, \cdots, n\,;\ j=1, 2, \cdots)$ which are effectively contained in F and coefficients G_k are series. Applying to G_k Späth's theorem and algebraic division by A_i, we arrive at the equalities:

$$G_k = H_{kp} A_p + \cdots + H_{k1} A_1 + G_k' \ (k=1, 2, \cdots, \lambda), \ (p=n-j),$$

where $A_1, \cdots, A_p$ are those elements of the basic set (A) of Σ that are *regular series* of the classes $j+1, \cdots, n$ respectively, and where $H_{kp}, \cdots \cdots, H_{k1}, G_k'$ are series of $\mathfrak{P}'$, and G_k' $(k=1, 2, \cdots, \lambda)$ are polynomials in $y_{j+1}, \cdots, y_n$. Therefore, we have

$$F = H_p A_p + \cdots + H_1 A_1 + F',$$

where $H_1, \cdots, H_p, F'$ are elements of $\mathfrak{P}'$ and F' is a polynomial of $y_{j+1}, \cdots \cdots, y_n$ and y_{ik} $(i=1, 2, \cdots, n\,;\ k=1, 2, \cdots)$ from Σ.

Since F' is an element of (Σ, T), there exists a positive integer q such that

$$(F')^q = \sum_{i,h} P_{ih}\,(d^i B_h/dx^i) + \sum_{k=0}^{r} Q_k\,(d^k T/dx^k) \qquad (1)$$

$$(P_{ih}, Q_k \in \mathfrak{P}').$$

While, let F'' be *the remainder* of F' with respect to the ascending set (A), then

$$T_1F' \equiv F''\,(A),$$

where T_1 is a power product of S_i, I_i $(i=1,\cdots,s)$ and F'' is an element of Σ reduced with respect to the ascending set (A); the congruence means modulo the ideal generated by $A_1,\cdots,A_s$. If F'' were not zero, Σ would have an ascending set of lower rank than the basic set (A); this would be a contradiction. Thus, T_1F' must be a linear combination of the elements of (A) and their derivatives. Hence, for sufficiently large integer t, $(TF')^t$ must be a linear combination of the elements of (A) and their derivatives.

Therefore, by the lemma of Raudenbush, there is a positive integer ν such that

$$(F'T)^\nu, (F'(dT/dx))^\nu, (F'(d^2T/dx^2))^\nu, \cdots, (F'(d^rT/dx^r))^\nu$$

are linear combinations of the elements of (A) and their derivatives.

Now, multiplying (1) by F' and taking the $\{(r+1)(\nu-1)+1\}$ th power of it, we see that $((F')^{q+1})^{(r+1)(\nu-1)+1}$ is a linear combination of the elements of (A) and their derivatives.