

CHAPTER III

ON THE BASIS THEOREM OF DIFFERENTIAL ALGEBRA

The present chapter consists of two principal parts. The first part contains some preliminary lemmas about forms and systems of forms which play a central role in differential algebra and in particular, these results are necessary for the investigation of the second part. The second part is devoted to proving a very important theorem of differential algebra, the basis theorem which states that if \mathcal{F} is a differential field of characteristic zero and y_1, y_2, \dots, y_n are n indeterminates, then $\mathcal{F}\{y_1, y_2, \dots, y_n\}$ is a Noetherian perfect differential ring.

Throughout this chapter, the differential ring \mathcal{R} will denote $\mathcal{F}\{y_1, y_2, \dots, y_n\}$.

1. SYSTEMS OF FORMS AND SOME PRELIMINARY PROPERTIES.

The materials of this part are based on reference [2].

In the preceding chapter we have already studied elements of the differential ring $\mathcal{F}\{y_1, y_2, \dots, y_n\}$ which we called forms. A form, let us recall, is a polynomial in y_1, y_2, \dots, y_n and any number of their derivatives with coefficients in \mathcal{F} , that is a finite sum

$$\sum a_{i_1 \dots i_n j_1 \dots j_n} (D^{i_1} y_1)^{j_1} \dots (D^{i_n} y_n)^{j_n}$$

where the i_m, j_r are non-negative integers, $a_{i_1 \dots i_n j_1 \dots j_n} \in \mathcal{F}$ and $D^{i_m} y_m$ is the i_m th derivative of y_m , $m = 1, 2, \dots, n$ ($D^0 y_i = y_i$).

From now on, capital letters denote forms.

Notation The derivative of y_1 will be indicated by means of a second subscript. Thus

$$y_{1j} = D^j y_1.$$

We write $y_1 = y_{10} = D^0 y_1$.

The j th derivative of a form A , denoted by $A^{(j)}$ is the form obtained by differentiating A j -times.

Definition 3-1 A form A in \mathcal{R} is said to be of order m with respect to y_1 , denoted by $\text{ord } A = m$ in y_1 if A involves y_1 or some of its derivatives and m is the greatest positive integer such that y_{1m} is present in a term of A with a coefficient distinct from zero.

If y_1 does not appear in A , the order of A with respect to y_1 will be taken as zero.

Definition 3-2 A form A in \mathcal{R} is said to be of class p , denoted by $\text{class } A = p$ if p is the largest integer such that y_{pj} appears in A for some non-negative integer j with non-zero coefficient.

We see that if A is an element in \mathcal{F} , A is of class zero.

Definition 3-3 Let A_1 and A_2 be two forms. The form A_2 is said to be of higher rank than A_1 in y_p , or more briefly, higher than A_1 in y_p if either

- i) A_2 is of higher order than A_1 in y_p
- or
- ii) A_1 and A_2 are of the same order, say q in y_p and the exponent (degree) of y_{pq} in A_2 is greater than that of y_{pq} in A_1 or we say that A_2 is greater degree than A_1 in y_{pq} .

Two forms for which no difference in rank is created by the preceding, will be said to be of the same rank in y_p .

All forms of class zero are of the same rank.

Definition 3-4 Let A_1 and A_2 be two forms. A_2 is said to be of higher rank than A_1 , or more briefly, higher than A_1 , if either

i) A_2 is of higher class than A_1

or

ii) A_1 and A_2 are of the same class, say $p > 0$, and A_2 is higher than A_1 in y_p .

Two forms for which no difference in rank is established by the foregoing definition, will be said to be of the same rank.

In order to understand definitions above easily, observe the following example:

Example 3-1 Let $R = \mathcal{F}\{y_1, y_2, y_3, y_4\}$ where \mathcal{F} is a differential field.

$$\text{Let } A_1 = a_0 y_{11} + a_1 y_{22} + a_2 y_{13} y_{24} + a_3 y_{23} y_{35}$$

$$A_2 = b_0 y_{12} + b_1 y_{11} y_{24}^2 + b_3 y_{32}$$

$$A_3 = c_0 y_1 + c_1 y_{22} + c_2 y_{33} + c_4 y_{44}$$

where a_i, b_j, c_k are all non-zero elements in \mathcal{F} .

$$\text{ord } A_1 = \begin{cases} 3 & \text{in } y_1 \\ 4 & \text{in } y_2 \\ 5 & \text{in } y_3 \\ 0 & \text{in } y_4 \end{cases}$$

$$\text{class } A_1 = 3$$



$$\text{ord } A_2 = \begin{cases} 2 & \text{in } y_1 \\ 4 & \text{in } y_2 \\ 2 & \text{in } y_3 \\ 0 & \text{in } y_4 \end{cases}$$

$$\text{class } A_2 = 3$$

$$\text{class } A_3 = 4.$$

A_1 is higher than A_2 in y_1 , by definition 3-3 (i)

A_2 is higher than A_1 in y_2 , by definition 3-3 (ii), since A_1 and A_2 are of the same order 4 in y_2 but the degree of y_{24} in $A_2 = 2$, which is greater than the degree of $y_{24} = 1$ in A_1 .

A_1 is higher than A_2 in y_3 , by definition (i).

A_1 is higher than A_2 , by definition 3-4 (ii) because A_1 and A_2 are of the same class 3 but A_1 is higher than A_2 in y_3 .

A_3 is higher than both A_1 and A_2 , by definition 3-4 (i), since $\text{class } A_3 = 4 > \text{class } A_1 = \text{class } A_2 = 3$.

Lemma 3-1 If A_2 is higher than A_1 and A_3 is higher than A_2 , then A_3 is higher than A_1 .

Proof Suppose first that A_2 is higher than A_1 due to condition (i) and that A_3 is higher than A_2 due to condition (i), then it is clear from the definition that A_3 is higher than A_1 by condition (i).

Suppose now that A_2 is higher than A_1 by (i) and that A_3 is higher than A_2 by (ii). Since A_3 and A_2 are of the same class and A_2 is of higher class than A_1 then A_3 is of higher class than A_1 . Thus A_3 is higher than A_1 by (i).

Now suppose that A_2 is higher than A_1 by (ii), while A_3 is higher than A_2 by (i). A_2 and A_1 are of the same class but A_3 is of higher class than A_2 , therefore A_3 is of higher class than A_1 and hence A_3 is higher than A_1 by (i).

Finally, if A_2 is higher than A_1 by (ii) and A_3 is higher than A_2 by (ii) then A_1 , A_2 and A_3 are of the same class, say p . But A_2 is of higher order than A_1 in y_p and A_3 is of higher order than A_2 in y_p . This implies that A_3 is of higher order than A_1 in y_p . Thus A_3 is higher than A_1 by condition (ii).

Lemma 3-2 If $A_1, A_2, \dots, A_q, \dots$

is an infinite sequence of forms such that, for every q , A_{q+1} is not higher than A_q , then there exists a positive integer r such that for $q > r$, A_q has the same rank as A_r .

Proof A_{q+1} is not higher than A_q , in other words A_q is higher than A_{q+1} or A_q and A_{q+1} have the same rank. If A_q is higher than A_{q+1} , there are 3 possible cases as follows:

- i) A_q is of higher class than A_{q+1}
- ii) A_q and A_{q+1} are of the same class $m > 0$, but A_q is of higher order than A_{q+1} in y_m
- iii) A_q and A_{q+1} are of the same class $m > 0$ and the same order in y_m , say t , but A_q is of higher degree than A_{q+1} in y_{mt} .

We first consider the case (i). Since A_{q+1} is not higher than A_q , we see that the classes of the A_q form a non-increasing set of non-negative integers; it is then clear that there exists a positive integer n_0 such that for $q > n_0$ A_q have the same class as A_{n_0} , say p . If $p = 0$ we are done. If $p > 0$ we are in case (ii). The set of the orders of the A_q for $q > n_0$ form a non-increasing set of non-negative integers and again there exists a positive integer $m \geq n_0$ such that for $q > m$ the forms A_q have the same class and the same order in y_p , say s .

Finally we have case (iii), and by the same reasoning as above there exists a positive integer $r \geq m \geq n_0$ such that for $q > r$ the form A_q will eventually have a common degree in y_{ps} . Thus for $q > r$ A_q have the same rank as A_r . This proves the Lemma.

The following corollary yields a more general result than that of above lemma which is restricted to sequences $\{A_q\}$. But the corollary allows the set of forms to be uncountable.

Corollary Every finite or infinite set of forms contains a form which is not of higher than any other form of the set.

Proof If the set of forms is finite, the corollary is trivial. Assume that there is an infinite set of forms containing no form which is not higher than any other form of the set. Thus if we pick a form in this set, it is higher than some other forms of the set. At this point we shall construct a sequence of forms by the following method.

To start with, we pick A_1 , it is then clear from assumption that A_1 is higher than another form of this set. We pick A_2 such that A_1 is higher than A_2 and then A_3 such that A_2 is higher than A_3 . By this process of construction we have an infinite sequence of forms

$$A_1, A_2, \dots, A_q, \dots$$

such that for every q , A_q is higher than A_{q+1} . This contradiction of the preceding lemma proves the corollary.

Definition 3-5 If A_1 is of class $p > 0$, A_2 will be said to be reduced with respect to A_1 if A_2 is of lower rank than A_1 in y_p .

Example 3-2 Let A_1 and A_2 be the first two forms given in Example 3-1. A_2 is reduced with respect to A_1 , since A_1 is of class 3 and $\text{ord } A_1 = 5$ in $y_3 > \text{ord } A_2 = 2$ in y_3 , that is, A_2 is of lower rank than A_1 in y_3 .

Definition 3-6 The system

$$(1) \quad A_1, A_2, \dots, A_r$$

will be called an ascending set if either

$$i) \quad r = 1 \text{ and } A_1 \neq 0$$

or

$$ii) \quad r > 1, A_1 \text{ is of class greater than } 0, \text{ and for } j > i, A_j \text{ is of higher class than } A_i \text{ and is reduced with respect to } A_i.$$

Remark It follows directly from the definition above that

$$i) \quad r \leq n = \text{the number of indeterminates}$$

$$ii) \quad \text{every non-zero form of } \mathcal{R} \text{ is an ascending set.}$$

Example 3-3 Let $\mathcal{R} = \mathcal{F}\{y_1, y_2, y_3, y_4, y_5, y_6\}$

$$A_1 = a_1 y_{19}$$

$$A_2 = b_1 y_{18} + b_2 y_{27}^2$$

$$A_3 = c_1 y_{16} + c_2 y_{26} y_{37}^2$$

$$A_4 = d_1 y_{14} y_{25} y_{37} y_{43}^3$$

$$A_5 = f_1 y_{17} y_{26} + f_2 y_{36} y_{43}^2 y_{51}$$

where a_1, b_j, c_k, d_1, f_m are all non-zero elements in \mathcal{F} . The system

$$A_1, A_2, A_3, A_4, A_5$$

forms an ascending set. From this example we see easily that the class of A_i is an increasing set of positive integers and if A_i is of class p_i , then

$$\text{ord } A_j \text{ in } y_{p_i} < \text{ord } A_i \text{ in } y_{p_i} \quad \text{for } j > i$$

Definition 3-7 The ascending set (1) will be said to be of higher rank, or more briefly, higher than the ascending set

$$(2) \quad B_1, B_2, \dots, B_s$$

if either

- i) there is a positive integer j , exceeding neither r nor s , such that A_i and B_i are of the same rank for $i < j$ and A_j is higher than B_j

or

- ii) $s > r$ and A_i and B_i are of the same rank for $i \leq r$.

If $j = 1$ in (i), this is taken to mean that A_1 is higher than B_1 .

Two ascending sets for which no difference in rank is established by the preceding definition will be said to be of the same rank. For such sets, $r = s$ and A_i and B_i are of the same rank for every i .

Example 3-4 R is a differential ring as in example 3-3. If $B = ay_{11}$ where $a \neq 0$ in F , then B is an ascending set and the ascending set in Example 3-3 is higher than the ascending set B by (i). Moreover, let

$$B_1 = a'_1 y_{19}$$

$$B_2 = b'_1 y_{16}^2 + b'_2 y_{15} y_{27}^2$$

$$B_3 = c'_1 y_{16} + c'_2 y_{27} y_{37}^2$$

$$B_4 = d'_1 y_{14}^3 + d'_2 y_{26} y_{43}^3 y_{36}^2$$

$$B_5 = f'_1 y_{11} y_{22} y_{33} + f'_2 y_{51} y_{42} y_{36}$$

$$B_6 = h'_1 y_{18} y_{32} + h'_2 y_{43} y_5^2 + h'_3 y_{62}$$

The system

$$B_1, B_2, B_3, B_4, B_5, B_6$$

forms an ascending set and the ascending set in Example 3-3 is higher than this ascending set, by (ii) since the number of forms in this ascending set = 6 > the number of forms in the ascending set in Example 3-3 = 5 and A_i and B_i are of the same rank for $i \leq 5$. If we delete in turn the form B_6 , we then have that the system

B_1, B_2, B_3, B_4, B_5

again forms an ascending set and this ascending set is of the same rank as the ascending set in Example 3-3.

Lemma 3-3 Let Φ_1, Φ_2 and Φ_3 be ascending sets such that Φ_1 is higher than Φ_2 and Φ_2 is higher than Φ_3 . Then Φ_1 is higher than Φ_3 .

Proof Let Φ_1 and Φ_2 be represented by (1) and (2) respectively, and let Φ_3 be

$$C_1, C_2, \dots, C_t.$$

Suppose first that Φ_1 is higher than Φ_2 and Φ_2 is higher than Φ_3 by (i). Since Φ_2 is higher than Φ_3 by (i), there exists a positive integer $j, j \leq s$ and $j \leq t$, such that B_i and C_i are of the same rank for $i < j$ and B_j is higher than C_j . Φ_1 is higher than Φ_2 by (i) also implies that there exists a positive integer $k, k \leq r$ and $k \leq s$, such that A_i and B_i are of the same rank for $i < k$ and A_k is higher than B_k .

If $k < j$, A_i, B_i and C_i are of the same rank for $i < k$. B_k and C_k are of the same rank and A_k is higher than B_k , hence A_k is higher than C_k . Thus Φ_1 is higher than Φ_3 by (i).

If $k > j$, A_j and B_j are of the same rank but B_j is higher than C_j , this implies that A_j is higher than C_j and A_i and C_i are of the same rank for $i < j$, hence Φ_1 is higher than Φ_3 by (i).

If $k = j$, then A_j is higher than B_j and B_j is higher than C_j implying that A_j is higher than C_j by lemma 3-1 and A_i, B_i and C_i are of the same rank for $i < j$. We have again that Φ_1 is higher than Φ_3 by (i).

Suppose now that Φ_1 is higher than Φ_2 by (i), while Φ_2 is higher than Φ_3 by (ii). Φ_1 is higher than Φ_2 implies that there exists a positive integer $j, j \leq r$ and $j \leq s$ such that A_i and B_i are of the same rank for $i < j$ and A_j is higher than B_j , while Φ_2 is higher than Φ_3 by (ii)

implies that $t > s$ and B_i and C_i are of the same rank for $i \leq s$. Therefore A_i , B_i and C_i are of the same rank for $i < j$ as well as B_j and C_j being of the same rank, but A_j is higher than B_j . Then A_j is higher than C_j . Thus Φ_1 is higher than Φ_3 by (i).

The next step we let Φ_1 be higher than Φ_2 by (ii) and Φ_2 be higher than Φ_3 by (i). Let j be the positive integer, $j \leq s$, $j \leq t$, such that B_i and C_i are of the same rank for $i < j$ and B_j is higher than C_j . Since Φ_1 is higher than Φ_2 by (ii), we have $s > r$ and A_i and B_i are of the same rank for $i \leq r$. If $j > r$, then $t > r$ and A_i are of the same rank as C_i for all $i \leq r$. This implies that Φ_1 is higher than Φ_3 by (ii). If $j \leq r$, then A_j is higher than C_j and A_i and C_i are of the same rank for $i < j$. Thus Φ_1 is higher than Φ_3 by (i).

Finally if Φ_1 is higher than Φ_2 by (ii) while Φ_2 is higher than Φ_3 by (ii), then $t > r$ and A_i is of the same rank as C_i for $i \leq r$, whence Φ_1 is higher than Φ_3 by (ii).

We shall need the following fact:

Lemma 3-4 Let

$$\Phi_1, \Phi_2, \dots, \Phi_q, \dots$$

be an infinite sequence of ascending sets such that Φ_{q+1} is not higher than Φ_q for any q . Then there exists a subscript r such that, for $q > r$, Φ_q has the same rank as Φ_r .

Proof To begin with, consider the first forms of the Φ_q 's for any q . By virtue of the lemma 3-2, there exists a positive integer m such that, for $q > m$, they are all of the same rank as the first form of the Φ_m . For the case in which Φ_q with $q > m$ has only one form, we are done.

We now suppose that s is the least positive integer such that $s \geq m$ and Φ_s has at least two forms. We are immediately confronted with the question: Is it possible that there exists a positive integer $\ell > s$ such that Φ_ℓ has one form? A short word about this, there is no positive integer $\ell > s$ such that Φ_ℓ has one form, since if Φ_ℓ has one form, it then follows from definition 3-7 (ii) that Φ_ℓ is higher than Φ_s , contrary to the hypothesis that Φ_ℓ is not higher than Φ_s . Thus Φ_q has at least two forms for $q \geq s$. However, by the same reasoning the second forms of Φ_q 's will eventually be of the same rank. Continuing in this manner, since the Φ_q 's are ascending sets and no Φ_q can have more than n forms where n is the number of indeterminates, we have that there exists a positive integer r such that all the Φ_q with $q > r$ have the same number of forms, corresponding forms being of the same rank. This completes the proof of lemma.

As a consequence of this result we have

Corollary Every finite or infinite set of ascending sets contains an ascending set whose rank is not higher than that of any other ascending set in the set.

The proof of this corollary is the same as the proof of the corollary of lemma 3-2.

Definition 3-8 Let Σ be any finite or infinite system of forms, not all zero. An ascending set Φ of Σ is said to be a basic set of Σ if Φ has the least rank among all ascending sets of Σ .

Remark The definition above is well-defined, since every non-zero form of Σ is an ascending set and by the corollary of lemma 3-4, among all ascending sets, there exist certain ones which have least rank.

At this point, we now introduce a method for constructing a basic set from any given system of forms Σ . It is easy in case Σ is finite. Suppose that Σ is infinite. Of the non-zero forms in Σ , by the corollary of lemma 3-2, there exists a form of least rank, say A_1 .

If A_1 is of class zero, then it is a basic set of Σ . Let A_1 be of class greater than zero. If Σ has no non-zero forms reduced with respect to A_1 , then A_1 is a basic set. Assume such reduced forms exist; they are all of higher class than A_1 , otherwise there is at least one form B which is of lower class than A_1 or the class of B equals the class of A_1 . If B is lower class than A_1 , then B is of lower rank than A_1 by definition 3-4 (i). Consider the case that the class of B equals the class of A_1 . Since B is reduced with respect to A_1 , therefore B is of lower rank than A_1 . In either case B is of lower rank than A_1 which contradicts the minimality of the rank of A_1 .

Let A_2 be the least rank which is reduced with respect to A_1 . Unless Σ contains non-zero forms reduced with respect to A_1 and A_2 , we claim that the ascending set A_1, A_2 will be a basic set of Σ . To prove this, assume that there exists an ascending set Φ of Σ such that Φ is lower than the ascending set A_1, A_2 . If Φ is lower than the ascending set A_1, A_2 by definition 3-7 (i), then the first form of Φ is the same rank as A_1 since the first form of Φ is not of lower rank than A_1 because of the minimality of the rank of A_1 and is not of higher rank than A_1 because of the assumption. Now it is necessary that the second form of Φ is lower than A_2 . Since the second form of Φ is reduced with respect to the first form of Φ , it is also reduced with respect to A_1 , contrary to the least rank of A_2 of forms which are reduced with respect to A_1 . If Φ is lower than the ascending set A_1, A_2 by definition 3-7 (ii), then the number of forms of Φ is greater than 2 and the first and the second form of Φ are of the same rank as A_1 and A_2 respectively. Since Φ is an ascending set, the third form of Φ is reduced

with respect to the first and the second form of Φ , hence it is also reduced with respect to A_1 and A_2 , contrary to the assumption that Σ contains no non-zero forms reduced with respect to A_1 and A_2 . This proves the claim. If such reduced forms exist; let A_3 be one of them of least rank. Continuing this process at most n steps we arrive at an ascending set which is a basic set of Σ .

Definition 3-9 If A_1 , in (1), is of class greater than zero, a form K will be said to be reduced with respect to the ascending set (1) if K is reduced with respect to every A_i , $i = 1, 2, \dots, r$.

From now on, the first form A_1 in the ascending set (1) considered is assumed to be a form of class greater than zero.

Lemma 3-5 Let Σ be a system of forms for which the ascending set (1) is a basic set. Then no non-zero form of Σ can be reduced with respect to (1).

Proof Suppose that there is a form K reduced with respect to (1). Then K has to be higher than A_1 , otherwise K would be an ascending set lower than (1). Similarly K must be higher than A_2 , otherwise A_1, K would be an ascending set lower than (1). By the same reasoning K is higher than A_3, A_4, \dots, A_r . This leads us to the conclusion that K is of higher class than A_j , $j = 1, 2, \dots, r$ and then

$$A_1, A_2, \dots, A_r, K$$

is an ascending set lower than (1). This is a contradiction since the ascending set (1) is a basic set of Σ .

Summarizing the preceeding lemma, we may now assert:

Corollary Let Σ be a system of forms for which the ascending set (1) is a basic set. If a non-zero form, reduced with respect to (1), is adjoined to Σ , then the basic sets of the resulting system are lower than (1).

Definition 3-10 If a form G is of class $p > 0$, and of order m in y_p

- a) The form $\frac{\partial G}{\partial y_{pm}}$, the partial derivative of G with respect to y_{pm} will be called the separant of G .
- b) The coefficient of the highest power of y_{pm} in G will be called the initial of G .

Remark It is clear from the definition above that the separant and initial of G are both lower than G .

Using the above lemmas we arrive at the following result which is necessary for the proof of the basis theorem.

Theorem 3-1 Let G be any form, S_i and T_i be respectively the separant and initial of A_i in (1), $i = 1, 2, \dots, r$. Then there exist non-negative integers $s_i, t_i, i = 1, 2, \dots, r$, such that when a suitable linear combination of the A_i and a certain number of their derivatives with forms for coefficients is subtracted from

$$s_1^1 S_1^2 \dots s_r^r T_1^1 T_2^2 \dots T_r^r G,$$

the remainder, R , is reduced with respect to (1).

Proof For the case G is reduced with respect to (1) there is nothing to prove, merely put $s_i, t_i = 0$ for every $i = 1, 2, \dots, r$ and all coefficients of the A_i and their derivatives can be taken to be zero.

So we may assume that G is not reduced with respect to (1).

Let A_i be of class p_i and of order m_i in y_{p_i} , $i = 1, 2, \dots, r$.

Let j be the largest value of i such that G is not reduced with respect to A_i

Let G be of order h in y_{p_j} .

Since G is not reduced with respect to A_j , then $h \geq m_j$. We suppose first that $h > m_j$, set $k_1 = h - m_j$, therefore $k_1 > 0$. Claim that $A_j^{(k_1)}$, the k_1 th derivative of A_j , will be of order h in y_{p_j} and also linear in $y_{p_j}^h$ with S_j as the coefficient of $y_{p_j}^h$. To prove this,

we write

$$A_j = \square + \sum_{k=1}^m \Delta_k y_{p_j}^k,$$

where \square and Δ_k are forms not involving y_{p_j} , $k = 1, 2, \dots, m$.

We now investigate S_j , the separant of $A_j = \frac{\partial A_j}{\partial y_{p_j}^{m_j}}$, that is,

$$S_j = \sum_{k=1}^m \Delta_k \cdot k y_{p_j}^{k-1}.$$

Consider $A_j^{(1)}$ the first derivative of A_j

$$A_j^{(1)} = D \square + \sum_{k=1}^m (D \Delta_k \cdot y_{p_j}^k + \Delta_k \cdot k y_{p_j}^{k-1} \cdot y_{p_j}^{m_j+1}).$$

Thus $A_j^{(1)}$ will be of order m_j+1 in y_{p_j} with $\sum_{k=1}^m \Delta_k \cdot k y_{p_j}^{k-1} = S_j$ as the

coefficient of $y_{p_j}^{m_j+1}$. We rewrite

$$A_j^{(1)} = \square + \sum_{k=1}^m k \cdot \Delta_k y_{p_j}^{k-1} \cdot y_{p_j}^{m_j+1}$$

where $\begin{array}{|c|c|} \hline \square & \square \\ \hline \end{array} = D \square + \sum_{k=1}^m D \Delta_k \cdot y_{p_j m_j}^k$.

It is clear that $\begin{array}{|c|c|} \hline \square & \square \\ \hline \end{array}$ does not involve $y_{p_j m_j+1}$.

Differentiate $A_j^{(1)}$ again, we have

$$(2) \quad A_j^{(2)} = D \begin{array}{|c|c|} \hline \square & \square \\ \hline \end{array} + \sum_{k=1}^m (D(k \Delta_k y_{p_j m_j}^{k-1}) \cdot y_{p_j m_j+1} + k \Delta_k y_{p_j m_j}^{k-1} y_{p_j m_j+2})$$

Hence $A_j^{(2)}$ will be of order $m_j + 2$ in y_{p_j} with S_j as the coefficient of $y_{p_j m_j+2}$.

Continuing in this way, $A_j^{(k_1)}$ will eventually be of order $m_j + k_1 = h$ in y_{p_j} and linear in $y_{p_j h}$ with S_j as the coefficient of $y_{p_j h}$.

In other words,

$$A_j^{(k_1)} = \diamond + S_j y_{p_j h}$$

where \diamond is a form not involving $y_{p_j h}$ which proves the claim.

We now take $y_{p_j h}$ as an indeterminate and $A_j^{(k_1)}$ as a polynomial in $y_{p_j h}$ of degree one with coefficients in the ring \mathcal{R} , it then follows from theorem 1-5 that there exists a non-negative integer v_1 such that

$$(3) \quad S_j^{v_1} G = C_1 A_j^{(k_1)} + D_1$$

where $D_1 = 0$ or D_1 does not involve $y_{p_j h}$. For uniqueness, we take v_1 as small as possible.

If $D_1 = 0$, the theorem is proven for the case $h > m_j$.

For the case D_1 does not involve $y_{p_j h}$. We shall prove that D_1 is of order less than h in y_{p_j} . Suppose that D_1 is of order k in y_{p_j} with $k > h$.

Since $A_j^{(k_1)}$ and $S_j^{v_1}G$ are of order h in y_{p_j} , therefore they do not involve $y_{p_j}^k$. Hence $y_{p_j}^k$ must appear in C_1 , this implies that D_1 must contain terms involving $y_{p_j}^h$ and $y_{p_j}^k$. This is a contradiction since $y_{p_j}^h$ does not appear in D_1 . This proves our statement.

Now let m be an arbitrary integer with $p_j < m \leq n$ where n is the number of indeterminates. Claim further that D_1 is not of higher rank than G in y_m . To prove this claim, it is only necessary to mention the case in which y_m is actually present in G and let G be of order ℓ in y_m (If y_m is not present in G , then y_m will not be present in D_1 , thus D_1 and G are of the same rank in y_m). By the same proof as above we have that the order of D_1 in y_m can not exceed ℓ . What we must prove now is that D_1 is not of greater degree than G in y_m . To prove this, assume that D_1 is of greater degree than G in y_m . Then C_1 must involve y_m in the same degree as D_1 , say q . This implies that $C_1 A_j^{(k_1)}$ has to contain terms involving $y_{p_j}^h y_m^q$. Since D_1 does not involve $y_{p_j}^h$ and S_j is free of y_m , $S_j^{v_1}G - D_1$ does not involve $y_{p_j}^h \cdot y_m^q$. This contradiction proves our claim.

If D_1 is still of order greater than m_j in y_{p_j} , we take

$$k_2 = \text{ord } D_1 \text{ in } y_{p_j} - m_j,$$

then $k_2 > 0$ and by the same reasoning as above, there exists a non-negative integer v_2 such that

$$(4) \quad S_j^{v_2} D_1 = C_2 A_j^{(k_2)} + D_2$$

with D_2 of lower order than D_1 in y_{p_j} and not of higher rank than D_1 (or G) in any y_m with $m > p_j$. In order to have a unique procedure, we take v_2 as

small as possible. If the order of D_2 in y_{p_j} is greater than m_j , we continue as before obtaining

$$S_j^{v_3 D_2} = C_{3A_j}^{(k_3)} + D_3$$

$$S_j^{v_4 D_3} = C_{4A_j}^{(k_4)} + D_4$$

.

.

.

$$S_j^{v_{u-1} D_{u-2}} = C_{u-1A_j}^{(k_{u-1})} + D_{u-1}$$

$$S_j^{v_u D_{u-1}} = C_{uA_j}^{(k_u)} + D_u.$$

where $k_i = \text{ord } D_{i-1} \text{ in } y_{p_j} - m_j$, $i = 2, 3, \dots, u$

We eventually arrive at D_u , of order not greater than m_j in y_{p_j} .

Multiplying (3) through by $S_j^{v_2}$ yields

$$S_j^{v_2} S_j^{v_1 G} = S_j^{v_2} C_{1A_j}^{(k_1)} + S_j^{v_2} D_1.$$

Substituting for $S_j^{v_2} D_1$ from (4) in this relation, gives

$$S_j^{v_2} S_j^{v_1 G} = S_j^{v_2} C_{1A_j}^{(k_1)} + C_{2A_j}^{(k_2)} + D_2.$$

Let us multiply this equation by $S_j^{v_3}$ and we substitute for $S_j^{v_3} D_2$ in the result, we have

$$S_j^{v_3} S_j^{v_2} S_j^{v_1 G} = S_j^{v_3} S_j^{v_2} C_{1A_j}^{(k_1)} + S_j^{v_3} C_{2A_j}^{(k_2)} + C_{3A_j}^{(k_3)} + D_3$$

Repeating this type of computation finally yields

$$S_j^{v_u} S_j^{v_{u-1}} \dots S_j^{v_1} G = S_j^{v_u} \dots S_j^{v_2} C_1^{(k_1)} + S_j^{v_u} \dots S_j^{v_3} C_2^{(k_2)} + \dots + C_u^{(k_u)} + D_u.$$

Setting $s_j = v_1 + v_2 + \dots + v_u$

$$F_i = S_j^{v_u} S_j^{v_{u-1}} \dots S_j^{v_{i+1}} C_i^{(k_i)}, \quad i = 1, 2, \dots, u-1.$$

$$F_u = C_u.$$

We have

$$(5) \quad S_j^{s_j} G = F_1^{(k_1)} + F_2^{(k_2)} + \dots + F_u^{(k_u)} + D_u.$$

Furthermore, D_u is not of higher rank than $D_{u-1}, D_{u-2}, \dots, D_1$ and G in y_m whenever $n \geq m > p_j$.

If D_u is of order less than m_j in y_{p_j} , then D_u is reduced with respect to A_j . Moreover, we claim that D_u is reduced with respect to A_i for $i > j$. To see this, G is reduced with respect to A_i for $i > j$ by assumption, and hence the order of G in y_{p_i} is less than the order of A_i in y_{p_i} for $i > j$. Since A_1, A_2, \dots, A_r is an ascending set, therefore $p_i > p_j$ for $i > j$. We already know that for $p_i > p_j$

Ord D_u in $y_{p_i} \leq \text{ord } G \text{ in } y_{p_i} < \text{ord } A_i \text{ in } y_{p_i}$, that is, D_u is reduced with respect to A_i with $i > j$, this proves the claim (We will be back where we started and treat the ascending set A_1, A_2, \dots, A_{j-1} and D_u in place of G .) If D_u is of order m_j in y_{p_j} , (We start proving the theorem for the case in which $h = m_j$ from now on.) we now consider D_u and A_j as polynomials in y_{p_j, m_j} with T_j as the coefficient of the highest power of y_{p_j, m_j} in A_j and then use theorem 1-5 again, we find, there is a non-negative integer t_j such that

$$(6) \quad T_j^{t_j} D_u = H A_j + K,$$

where $K = 0$ or K is of lower degree than A_j in $y_{p_j m_j}$. For uniqueness, we take t_j as small as possible. We thus limit ourselves to the case in which $K \neq 0$, otherwise we are done. If $K \neq 0$, then K is reduced with respect to A_j . By the same proof as above, we can guarantee that K is also reduced with respect to A_{j+1}, \dots, A_r . It is possible in this case that K is reduced with respect to A_1, A_2, \dots, A_r . If this occurs, the proof stops here. Suppose that K is not reduced with respect to A_1, A_2, \dots, A_{j-1} . Let g be the largest value i , $1 \leq i \leq j$ such that K is not reduced with respect to A_i and we will then be back to starting point again and treat K as G was treated, we find, there exists a non-negative integer s_g such that

$$(7) \quad S_g^s K = E_1 A_g^{(k'_1)} + E_2 A_g^{(k'_2)} + \dots + E_w A_g^{(k'_w)} + D_w$$

where D_w is of order not greater than m_g in y_{p_g} and furthermore, if $m > p_g$, D_w is not of higher rank than K in y_m .

Suppose that D_w is of order less than m_g in y_{p_g} , by the same proof as above D_w is reduced with respect to A_g, A_{g+1}, \dots, A_r . We shall then be back where we started again.

Suppose that D_w is of order m_g in y_g , we take a non-negative integer t_g as small as possible such that

$$(8) \quad T_g^{t_g} D_w = H' A_g + K'$$

where K' is reduced with respect to A_g, A_{g+1}, \dots, A_r .

Substituting $T_g^{t_g} D_w$ in $T_g^{t_g} \times (7)$ yields the result

$$T_g^{t_g} S_g^s K = T_g^{t_g} (E_1 A_g^{(k'_1)} + \dots + E_w A_g^{(k'_w)}) + H' A_g + K'.$$

Substituting this in $T_g^{s_g} \times (6)$, we obtain

$$T_g^{s_g} E_{T_j}^{t_j} D_u = T_g^{s_g} E_{HA_j} + T_g^{s_g} (E_1 A_g^{(k_1)} + \dots + E_w A_g^{(k'_w)}) + H' A_g + K'.$$

We now arrive at the final stage, substituting this in $T_g^{s_g} E_{T_j}^{t_j} \times (5)$, gives us

$$\begin{aligned} S_g^{s_j} E_{T_j}^{t_j} E_{T_j}^{t_j} G - T_g^{s_g} E_{T_j}^{t_j} (F_1 A_j^{(k_1)} + \dots + F_u A_j^{(k_u)}) - T_g^{s_g} E_{HA_j} \\ - T_g^{s_g} (E_1 A_g^{(k_1)} + \dots + E_w A_g^{(k'_w)}) - H' A_g = K'. \end{aligned}$$

Thus when such a linear combination of A_j , A_g and their derivatives is subtracted from $S_g^{s_j} E_{T_j}^{t_j} E_{T_j}^{t_j} G$, the result is reduced with respect to A_g, A_{g+1}, \dots, A_r .

Continuing in this way, we reach a form R required in the statement of the theorem. This completes the proof of theorem.

Remark Our procedure determines a unique R . We call this R the remainder of G with respect to the ascending set (1).

2. THE BASIS THEOREM

Before proving the basis theorem, it will be convenient to establish the following lemmas:

Lemma 3-6 If the perfect differential ideal $\langle \sigma \rangle$ has a finite basis, then it has a finite basis consisting of elements of σ .

Proof Let a_1, a_2, \dots, a_s be the elements of a finite basis of $\langle \sigma \rangle$. According to theorem 2-3, each a_m , $m = 1, 2, \dots, s$ as an element of $\langle \sigma \rangle$ has a power in $[\sigma]$. Let t_m be a positive integer such that $a_m^{t_m}$ belongs to $[\sigma]$, $m = 1, 2, \dots, s$. Being an element of $[\sigma]$, $a_m^{t_m}$ is equal to

a linear combination of a finite number of elements of σ and a finite number of derivatives of elements of σ with elements in \mathcal{R} as coefficients, that is a finite sum of the form

$$a_m^t = \sum_{i,j,k} b_i D^j y_k$$

where i, j, k are non-negative integers, $y_k \in \sigma$ and $b_i \in \mathcal{R}$, $m = 1, 2, \dots, s$. Let σ_m be the set consisting of all y_k in the expression of a_m^t , hence σ_m is a finite subset of σ . It is clear that a_m^t is in $\langle \sigma_m \rangle$. Since $\langle \sigma_m \rangle$ is a perfect differential ideal, a_m is also in $\langle \sigma_m \rangle$ for all $m = 1, 2, \dots, s$. This implies that $a_m \in \langle \sigma_1, \sigma_2, \dots, \sigma_n \rangle$ for all $m = 1, 2, \dots, s$. Since $\langle a_1, a_2, \dots, a_n \rangle = \langle \sigma \rangle$, then $\langle \sigma_1, \sigma_2, \dots, \sigma_n \rangle = \langle \sigma \rangle$. This proves the lemma.

Lemma 3-7 Let Σ be perfect differential ideal without a finite basis. Let F_1, F_2, \dots, F_s be forms and Λ the system obtained by multiplying each form of Σ by some product of non-negative powers of F_1, F_2, \dots, F_s . Assume that $\langle \Lambda \rangle$ has a finite basis then, $\langle \Sigma, F_1 F_2 \dots F_s \rangle$ has no finite basis.

Proof Suppose that $\langle \Sigma, F_1 F_2 \dots F_s \rangle$ has a finite basis, it then follows from the preceding lemma that $\langle \Sigma, F_1 F_2 \dots F_s \rangle$ can be represented as $\langle H_1, H_2, \dots, H_t; F_1 F_2 \dots F_s \rangle$ where H_1, H_2, \dots, H_t are forms of Σ . By hypothesis, $\langle \Lambda \rangle$ has a finite basis, so we use the preceding lemma again to conclude that $\langle \Lambda \rangle$ has a finite basis consisting of elements of Λ . Since Λ is composed of elements of the form $F_1^{g_{\alpha 1}} F_2^{g_{\alpha 2}} \dots F_s^{g_{\alpha s}} K_\alpha$ where $g_{\alpha i}$ are non-negative integers, $i = 1, 2, \dots, s$ and K_α is in Σ , we may write

$$\langle \Lambda \rangle = \langle F_1^{g_{11}} \dots F_s^{g_{1s}} K_1, F_1^{g_{21}} \dots F_s^{g_{2s}} K_2, \dots, F_1^{g_{m1}} \dots F_s^{g_{ms}} K_m \rangle.$$

Let Π be the set of H 's and K 's above. It is obvious that

$$\langle \Pi, F_1 F_2 \dots F_s \rangle = \langle \Sigma, F_1 F_2 \dots F_s \rangle.$$

Each $F_1^{g_{i1}} \dots F_s^{g_{is}} K_i$ is in $\langle \Pi \rangle$, $i = 1, 2, \dots, m$ since $\langle \Pi \rangle$ is an ideal, thus we get $\Lambda \subseteq \langle \Pi \rangle$.

Since Σ has no finite basis, there exists a form L of Σ not in $\langle \Pi \rangle$. Some $F_1^{g_1} \dots F_s^{g_s} L$ is in $\langle \Lambda \rangle$ and hence in $\langle \Pi \rangle$. Consequently, if g is the maximum of g_1, g_2, \dots, g_s , $F_1^{g_1} F_2^{g_2} \dots F_s^{g_s} L^g$ is also in $\langle \Pi \rangle$ and thus $F_1 F_2 \dots F_s L$ is in $\langle \Pi \rangle$ since $\langle \Pi \rangle$ is perfect differential ideal. L is in $\langle \Sigma, F_1 F_2 \dots F_s \rangle = \langle \Pi, F_1 F_2 \dots F_s \rangle$, as well as being in $\langle \Pi, L \rangle$. By virtue of theorem 2-4, L is in $\langle \Pi, F_1 F_2 \dots F_s L \rangle$ which is $\langle \Pi \rangle$ since $F_1 F_2 \dots F_s L$ is in $\langle \Pi \rangle$. This contradiction proves the lemma.

Lemma 3-8 Let Σ and $\langle \Sigma, F_1 F_2 \dots F_s \rangle$ be perfect differential ideals having no finite basis. Then at least one of the perfect differential ideals $\langle \Sigma, F_1 \rangle, \langle \Sigma, F_2 \rangle, \dots, \langle \Sigma, F_s \rangle$ has no finite basis.

Proof Assume that all $\langle \Sigma, F_1 \rangle, \langle \Sigma, F_2 \rangle, \dots, \langle \Sigma, F_s \rangle$ have a finite basis. We know that $\langle \Sigma, F_i \rangle = \langle \Phi_i, F_i \rangle$ where each Φ_i is a finite subset of Σ , $i = 1, 2, \dots, s$, due to lemma 3-6, also

$$\langle \Sigma, F_i \rangle = \langle \Phi_1, \Phi_2, \dots, \Phi_s, F_i \rangle.$$

We write this out explicitly

$$\begin{aligned} \langle \Sigma, F_1 \rangle &= \langle \phi_1, \phi_2, \dots, \phi_s, F_1 \rangle \\ \langle \Sigma, F_2 \rangle &= \langle \phi_1, \phi_2, \dots, \phi_s, F_2 \rangle \\ &\cdot \\ &\cdot \\ &\cdot \\ \langle \Sigma, F_s \rangle &= \langle \phi_1, \phi_2, \dots, \phi_s, F_s \rangle . \end{aligned}$$

By virtue of theorem 2-4

$$\bigcap_{i=1}^s \langle \Sigma, F_i \rangle = \langle \Sigma, F_1 F_2 \dots F_s \rangle$$

and hence equals $\langle \phi_1, \phi_2, \dots, \phi_s, F_1 F_2 \dots F_s \rangle$. This means that $\langle \Sigma, F_1 F_2 \dots F_s \rangle$ has a finite basis, contrary to the hypothesis.

We now have all the necessary information to prove the basis theorem.

The basis theorem The differential ring $\mathcal{F}\{y_1, y_2, \dots, y_n\}$ where \mathcal{F} is a differential field of characteristic zero is Noetherian perfect differential ring.

Proof We suppose the theorem is false. Then there exist perfect differential ideals of $\mathcal{F}\{y_1, y_2, \dots, y_n\}$ not having a finite basis. We construct a basic set for each. According to the corollary of lemma 3-4, there is a perfect differential ideal Σ without a finite basis whose basic sets are not of higher rank than the basic sets of any other perfect differential ideal without a finite basis. Let ϕ be the ascending set (1), a basic set of Σ . Then $A_1 \neq 0$ is not an element of \mathcal{F} , because \mathcal{F} is a differential field and if $0 \neq A_1 \in \mathcal{F}$,

then A_1^{-1} , the inverse of A_1 under multiplication, exists implying that $A^{-1}A = \text{identity of } \mathcal{F}$ is also in Σ . Thus Σ has the identity as a finite basis.

Consider $\Sigma - \Phi$, the set consisting of all elements of Σ not in Φ . By theorem 3-1, to each form G_α in $\Sigma - \Phi$, where α ranges over some index set, there corresponds a remainder R_α which is reduced with respect to (1).

Let $S_1^{s_{\alpha 1}} S_2^{s_{\alpha 2}} \dots S_r^{s_{\alpha r}} T_1^{t_{\alpha 1}} T_2^{t_{\alpha 2}} \dots T_r^{t_{\alpha r}} G_\alpha$ correspond to R_α where S_i and T_i are separate and initial of A_i , $i = 1, 2, \dots, r$, respectively.

Let Ω be the system composed of A_1, A_2, \dots, A_r and the remainders R_α of forms of $\Sigma - \Phi$.

Let Λ be the system composed of A_1, A_2, \dots, A_r and $S_1^{s_{\alpha 1}} \dots S_r^{s_{\alpha r}} T_1^{t_{\alpha 1}} \dots T_r^{t_{\alpha r}} G_\alpha$ where $G_\alpha \in \Sigma - \Phi$.

We claim that $\langle \Omega \rangle$ has a finite basis. To prove this, assume that $\langle \Omega \rangle$ has no finite basis, therefore Ω contains some non-zero R_α not in (1). There are three cases:

Case 1 R_α is of class greater than that of A_r . Since R_α is reduced with respect to (1), then

$$A_1, A_2, \dots, A_r, R_\alpha$$

forms an ascending set which is of lower rank than (1), by definition 3-7(ii),

This is a contradiction.

Case 2 R_α is of the same class as A_i , for some i . Form the ascending set

$$A_1, A_2, \dots, A_{i-1}, R_\alpha.$$

By definition 3-7 (i), this ascending set is lower than (1), contrary to the the least rank of (1).

Case 3 Class $A_i < \text{class } R_\alpha < \text{class } A_{i+1}$, for some i . Form the ascending set

$$A_1, A_2, \dots, A_i, R_\alpha .$$

This ascending set is lower than (1) by definition 3-7 (i) which is a contradiction.

Case 4 Class $R_\alpha < \text{class } A_1$,

then the ascending set R_α is lower than (1) which is a contradiction.

In either case $\langle \Omega \rangle$ has a basic set of lower rank than (1). This contradiction proves the claim.

It is clear that $\langle \Omega \rangle = \langle \Lambda \rangle$. So $\langle \Lambda \rangle$ also has a finite basis. By lemma 3-7, $\langle \Sigma, S_1 S_2 \dots S_r T_1 T_2 \dots T_r \rangle$ has no finite basis and it then follows from the preceding lemma that at least one of the perfect differential ideals

$$\langle \Sigma, S_1 \rangle, \dots, \langle \Sigma, S_r \rangle, \langle \Sigma, T_1 \rangle, \dots, \langle \Sigma, T_r \rangle$$

has no finite basis.

We now claim that S_i and T_i for every $i = 1, 2, \dots, r$ are reduced with respect to (1).

Let A_j be of class p_j . What we have to prove is that S_i is lower than A_j in y_{p_j} , $j = 1, 2, \dots, r$, $i = 1, 2, \dots, r$.

If $j > i$, it is clear that the class of S_i is less than that of A_j . Then S_i is lower than A_j in y_{p_j} .

If $i > j$, then A_i is reduced with respect to A_j since (1) is an ascending set, that is

$$\text{ord } A_i \text{ in } y_{p_j} < \text{ord } A_j \text{ in } y_{p_j} .$$

Since $\text{ord } S_i \text{ in } y_{p_j} \leq \text{ord } A_i \text{ in } y_{p_j}$.

This implies that S_i is of lower order than A_j in y_{p_j} , hence S_i is reduced with respect to A_j .

If $i = j$, then it follows directly from the definition of separant that S_i is of lower than A_i , thus S_i is reduced with respect to A_i .

In either case S_i is reduced with respect to (1), for every $i = 1, 2, \dots, r$. By the same reasoning T_i is reduced with respect to (1) for every $i = 1, 2, \dots, r$.

By the corollary of lemma 3-5, $\langle \Sigma, S_i \rangle$ and $\langle \Sigma, T_i \rangle$ are lower than (1) for all $i = 1, 2, \dots, r$. Thus one of $\langle \Sigma, S_i \rangle$, $\langle \Sigma, T_i \rangle$, $i = 1, 2, \dots, r$ which has no finite basis is lower than the basic set (1) of Σ , contrary to the assumption that the basic set (1) of Σ which is not of higher rank than the basic sets of any other perfect differential ideals without a finite basis. This completes the proof of the basis theorem.

Remark The basis theorem is not true if \mathcal{F} is of non-zero characteristic

Let p be a prime number and $\mathcal{F} = \mathbb{Z}_p$, a field of characteristic p . In the differential ring $\mathcal{R} = \mathbb{Z}_p \{y\}$, let Σ be the system of forms

$$y^p, y_1^p, y_2^p, \dots$$

Form $\langle \Sigma \rangle$, a perfect differential ideal in \mathcal{R} generated by Σ .

Suppose that the basis theorem is true, then there exists a finite set of forms in Σ , say y^P, y_1^P, \dots, y_n^P such that

$$\langle \Sigma \rangle = \langle y^P, y_1^P, \dots, y_n^P \rangle .$$

Since y_{n+1}^P is in Σ , therefore $y_{n+1}^P \in \langle y^P, y_1^P, \dots, y_n^P \rangle$, contrary to the fact that y_{n+1}^P is not in $\langle y^P, y_1^P, \dots, y_n^P \rangle$.

With the two equivalent corollaries below, we achieve the objective of this chapter.

Corollary Every system Σ of forms has a finite subset F_1, F_2, \dots, F_s such that, for each form $A \in \Sigma$ there is a positive integer t such that $A^t \in [F_1, F_2, \dots, F_s]$.

Proof As a consequence of the basis theorem, the perfect differential ideal $\langle \Sigma \rangle$ has a finite basis, that is, there are forms F_1, F_2, \dots, F_s in Σ such that

$$\langle \Sigma \rangle = \langle F_1, F_2, \dots, F_s \rangle .$$

Let A be an arbitrary form of Σ , it then follows from theorem 2-3 that there is a positive integer t such that $A^t \in [F_1, F_2, \dots, F_s]$.

Corollary Every system Σ of forms has a finite subset F_1, F_2, \dots, F_s such that Σ is contained in the perfect differential ideal generated by F_1, F_2, \dots, F_s :

$$\Sigma \subseteq \langle F_1, F_2, \dots, F_s \rangle .$$