LECTURES IN MATHEMATICS

Department of Mathematics
KYOTO UNIVERSITY

16

Differential Algebra of Nonzero Characteristic

BY

Kôtaro OKUGAWA

Published by
KINOKUNIYA CO., Ltd.
Tokyo, Japan

LECTURES IN MATHEMATICS

Department of Mathematics

KYOTO UNIVERSITY

16

Differential Algebra

of

Nonzero Characteristic

By

Kôtaro OKUGAWA

Published by

KINOKUNIYA CO., Ltd.

Printed in Japan

Differential Algebra of Nonzero Characteristic

By

Kôtaro OKUGAWA

Acknowledgment

The author is deeply grateful to Department of Mathematics of Kyoto University which accepted this note to publish in "Lectures in Mathematics, Kyoto University".

Contents

Foreword

The theory of Galois type on differential fields of characteristic zero was established by E. R. Kolchin. Namely, the theory of Picard-Vessiot extensions was developed in [1], [2] and others, and then, more generally, the theory of strongly normal extensions was presented in [3] and others. On the latter theory, some contributions were made by H. Matsumura, C. Chevalley and S. Lang. We can now find a fine treatise on such materials in the book [4] of Kolchin.

Galois groups of Picard-Vessiot extensions are algebraic matric groups, and those of strongly normal extensions are algebraic groups. Since general algebraic groups are well studied also in the case of nonzero characteristic, it is interesting to develop the corresponding theory of Golois type on differential fields of nonzero characteristic. To do this, it seems appropriate to deal with differential fields and rings which are defined by associating a set of mutually commutative iterative higher derivations of infinite rank. From this standpoint, we provided in [5] a method of developing the theory of Picard-Vessiot extensions of arbitrary characteristic. Since then, basic properties of such differential fields and rings of nonzero characteristic have been more elaborately considered by us; recently, we had contributions [7], [8], [10] and [11] of K. Tsuji (née Shikishima). Although complicated calculations and observations are necessary, useful results are obtained, and

the Galois theory of strongly normal extensions of differential field of nonzero characteristic is established.

This note contains, in the case of nonzero characteristic p, detailed descriptions of basic properties of differential fields and rings and of strongly normal extensions of differential fields. In preparing the note, we use freely the notions and results of Chap.0 and Chap.V of [4] and Chap.I of [1], because these chapters deal with basic algebraic notions including that of the algebraic group for arbitrary characteristic and they are very fundamental literatures. Thus materials from these chapters are often introduced as known ones to the reader, although we endeavor to cite the origin of each of them. Generally speaking, we tried to use terminologies and notations of the whole book [4] which is excellent and well-equipped. Our definition of "derivation" in Chap.1 leads to formal difference between each differential algebraic concept of this note and the corresponding one of [4], but a same term or a same notation is used to each pair of corresponding concepts. On the other hand, a number of new differential algebraic concepts and notations must be introduced in this note.

Chap.1 gives fundamental considerations on "derivation". Chap.2 and Chap.3 deal with basic properties of differential fields, differential rings and differential ideals. Chap.4 is devoted maimly to the proof of existence of universal differential extension field of any given differential field. Chap.5

contains the Galois theory of strongly normal extensions of differential fields. This chapter is developed following Chap.VI of [4], although the concern about separability necessitates additional discussions on many steps. In Chap.6, some observations are made on Picard-Vessiot extensions and Liouvillian extensions of differential fields. This shows that the theory of [5] can be rearranged more naturally under the new light of this note.

Theorems are numbered consecutively from beginning to end of each chapter; so are propositions and lemmas. In quoting a result, we indicate not only the chapter but also the section; examples: Th.2 of §1.7; part (a) of Th.10 of §2.6; Cor.2 to Th.1 of §3.1. However, in referring to a result within the same section, we do not mention the section.

We wish to thank heartily E. R. Kolchin, the presence of whose works initiated us into our study and helped us. We express with sincere thanks that many results (§1.8, §2.8, §4.3, §4.8, §5.1, §5.6, §5.7, Examp.3 of §5.8) of this note are originally due to K. Tsuji, and that many helpful criticisms on the preparatory manuscript have been given by our colleagues (of Kyoto Sangyo Univ.) and by our friends.

March 1987

Kôtaro Okugawa

CHAPTER 1

Derivations

1.1. Conventions

The term field is used for commutative field of nonzero characteristic p arbitrarily fixed once for all except for some examples. The term ring is used for commutative unitary ring which contains some field as a unitary subring. If a ring and its subring are considered, the latter is tacitly supposed to be a unitary subring of the former. If a ring-homomorphism is considered, it is also tacitly supposed unitary.

If $\lambda_1, \lambda_2, \ldots$ are to appear as subscripts, superscripts or exponents, we use instead $\lambda(1), \lambda(2), \ldots$ respectively in order to simplify the typewiting. This convention is never applied to the characteristic p, and $p(m)$ denotes always the power p^m for any $m \in \mathbb{Z}$ ($\mathbb{Z}$ being the set of integers).

$\mathbb{N}$ denotes the set of natural number (including 0). Let I be a finite or infinite set. Modifying the notation for the set $\mathbb{N}^I$, we use the notation $\mathbb{N}^{(I)}$ for the set of all families $(\nu) = (\nu(i) \mid i \in I)$ whose components $\nu(i)$ $(i \in I)$ are in $\mathbb{N}$ and zeros except for a finite number. The family (0) means the family (ν) with $\nu(i) = 0$ for all $i \in I$. $\mathbb{N}^{(I)}$ has a canonical structure of an additive semigroup having (0) as the zero element. When the set I is finite, $\mathbb{N}^{(I)}$ coincides with $\mathbb{N}^I$.

1.2. Definitions and elementary properties

Let R be a ring. We mean by a derivation δ of R an iterative higher derivation of infinite rank, that is, an infinite sequence $\delta = (\delta_\nu \mid \nu \in \mathbb{N})$ of mappings δ_ν of R into R which satisfies the following conditions (cf. [5]):

(D1) $\delta_0 = id_R$ (the identity mapping of R),

(D2) $\delta_\nu(x + y) = \delta_\nu x + \delta_\nu y$,

(D3) $\delta_\nu(xy) = \Sigma_{\nu(1)+\nu(2)=\nu} \delta_{\nu(1)}x \cdot \delta_{\nu(2)}y$,

(D4) $\delta_\lambda \delta_\mu x = \binom{\lambda+\mu}{\lambda} \delta_{\lambda+\mu} x$

for all $x,y \in R$ and for all $\lambda,\mu,\nu \in \mathbb{N}$. We say that δ_ν is the member of order ν of δ or the νth member of δ ($\nu \in \mathbb{N}$). Since δ_ν ($\nu \in \mathbb{N}$) are mappings of R into R, we can make product (that is, composite) of any finite number of them; we met already the product of δ_λ and δ_μ in (D4). Multiples of a finite product $\delta_{\lambda(1)}\delta_{\lambda(2)}\cdots\delta_{\lambda(n)}$ of members of δ are meaningful, that is,

(1) $(m\delta_{\lambda(1)}\delta_{\lambda(2)}\cdots\delta_{\lambda(n)})x = m(\delta_{\lambda(1)}\delta_{\lambda(2)}\cdots\delta_{\lambda(n)}x)$

for all $m \in \mathbb{Z}$ and for all $x \in R$; in particular, if $m \equiv 0 \pmod p$, then $m\delta_{\lambda(1)}\delta_{\lambda(2)}\cdots\delta_{\lambda(n)} = 0$ (the zero mapping of R into R). If $m',m'' \in \mathbb{Z}$ and $m' \equiv m'' \pmod p$, we see that

(2) $m'\delta_{\lambda(1)}\delta_{\lambda(2)}\cdots\delta_{\lambda(n)} = m''\delta_{\lambda(1)}\delta_{\lambda(2)}\cdots\delta_{\lambda(n)}$.

We can show by (D1)~(D4) the following basic properties of the derivation δ of R.

1° Every finite product of δ_ν $(\nu \in \mathbb{N})$ is an endomorphism of the additive group R^+ of the ring R.

2° The first member δ_1 of δ is a derivation of rank 1 of R, that is, δ_1 maps R into R and satisfies conditions $\delta_1(x + y) = \delta_1 x + \delta_1 y$, $\delta_1(xy) = \delta_1 x \cdot y + x \cdot \delta_1 y$ for all $x,y \in R$.

3° We have the formula

(D3') $\delta_\nu(x_1 x_2 \cdots x_n) = \Sigma \delta_{\nu(1)} x_1 \cdot \delta_{\nu(2)} x_2 \cdot \cdots \cdot \delta_{\nu(n)} x_n$

for all finite family $(x_1,\ldots,x_n)$ of elements of R and for all $\nu \in \mathbb{N}$, where the summation Σ runs through all the elements $(\nu(1),\ldots,\nu(n)) \in \mathbb{N}^n$ with $\nu(1) + \ldots + \nu(n) = \nu$.

4° For any $\lambda,\mu \in \mathbb{N}$ we get $\delta_\lambda \delta_\mu = \delta_\mu \delta_\lambda$.

5° For any finite product of members of δ, we have

(D4') $\delta_{\lambda(1)} \delta_{\lambda(2)} \cdots \delta_{\lambda(n)}$

$= ((\lambda(1)+\ldots+\lambda(n))!/\lambda(1)!\ldots\lambda(n)!)\delta_{\lambda(1)+\ldots+\lambda(n)}$,

(D4") $\delta_\nu{}^n = ((n\nu)!/(\nu!)^n)\delta_{n\nu}$.

If the p-adic expression of $\nu \in \mathbb{N}$ is $\nu = \Sigma_{\kappa\in\mathbb{N}} c(\kappa)p(\kappa)$, $0 \le c(\kappa) < p$, then we get the formula

(D4"') $\Pi_{\kappa\in\mathbb{N}} \delta_{p(\kappa)}{}^{c(\kappa)} = [\nu!/\Pi_{\kappa\in\mathbb{N}}(p(\kappa)!)^{c(\kappa)}]\delta_\nu$.

Note that both products $\Pi_{\kappa\in\mathbb{N}} \delta_{p(\kappa)}{}^{c(\kappa)}$ and $\Pi_{\kappa\in\mathbb{N}}(p(\kappa)!)^{c(\kappa)}$ are meaningful, since $c(\kappa) = 0$ for all sufficiently large κ and $\delta_{p(\kappa)}{}^0 = id_R$ for all $\kappa \in \mathbb{N}$. For later use, the integer

[ ] of (D4"') is denoted by $[\nu]$.

6° If c is any element of the prime field in R, then $\delta_\nu c = 0$ for all $\nu \in \mathbb{N}-\{0\}$.

It suffices by 1° to prove that $\delta_\nu 1 = 0$ for the unity of R. Using induction on ν, the proof is easy by virtue of 2° and (D3).

An element z of R is called <u>δ-constant</u> if $\delta_\nu z = 0$ for all $\nu \in \mathbb{N}-\{0\}$. In this chapter $R_{c,\delta}$ denotes the set of all δ-constants of R. By 6°, $R_{c,\delta}$ contains the prime field in R.

7° $R_{c,\delta}$ is a subring of R. If R is particularly a field, then $R_{c,\delta}$ is a subfield of R.

The first assertion is obvious by (D2~3). For the second assertion, let R be a field and z a nonzero element of $R_{c,\delta}$. Then it is easy to prove by induction on ν, using 6°, 2° and (D3), that $\delta_\nu(z^{-1}) = 0$ for all $\nu \in \mathbb{N}-\{0\}$.

This subring $R_{c,\delta}$ is called <u>ring of δ-constants</u> of R. It is called <u>field of δ-constants</u> of R if R is a field.

In order to deduce two more properties 8° and 9°, and moreover, also to prepare for later applications, we insert here a useful lemma. We notice beforehand that, if $\lambda \in \mathbb{N}-\{0\}$ has the p-adic expression $\lambda = \Sigma_{\kappa\in\mathbb{N}} a(\kappa)p(\kappa)$, $0 \le a(\kappa) < p$, then

$$N(\lambda) = (\lambda - \Sigma_{\kappa\in\mathbb{N}} a(\kappa))/(p-1)$$

is the largest exponent among the power of p which divide $\lambda!$. In fact, for each $\alpha \in \mathbb{N}-\{0\}$, the number of multiples of $p(\alpha)$ among $1, \ldots, \lambda$ is $\Sigma_{\kappa\geq\alpha} a(\kappa)p(\kappa-\alpha)$, so that

$$N(\lambda) = \Sigma_{\alpha\geq 1}\Sigma_{\kappa\geq\alpha} a(\kappa)p(\kappa-\alpha) = \Sigma_{\kappa\geq 1} a(\kappa)(\Sigma_{\beta=0}^{\kappa-1} p(\beta))$$

$$= \Sigma_{\kappa\geq 1} a(\kappa)(p(\kappa)-1)/(p-1) = (\lambda - \Sigma_{\kappa\geq 1} a(\kappa))/(p-1).$$

Lemma 1 Let the p-adic expressions of finitely many natural numbers $\lambda(1), \ldots, \lambda(n)$ and their sum $\Sigma_{i=1}^{n}\lambda(i)$ be

$$\lambda(i) = \Sigma_{\kappa\in\mathbb{N}} a_i(\kappa)p(\kappa),\ 0 \leq a_i(\kappa) < p \quad (1\leq i\leq n),$$

$$\Sigma_{i=1}^{n}\lambda(i) = \Sigma_{\kappa\in\mathbb{N}} b(\kappa)p(\kappa),\ 0 \leq b(\kappa) < p.$$

Then $(\lambda(1)+\ldots+\lambda(n))!/\lambda(1)!\ldots\lambda(n)! \not\equiv 0 \pmod{p}$ if and only if $\Sigma_{i=1}^{n} a_i(\kappa) = b(\kappa)$ for all $\kappa \in \mathbb{N}$.

Proof. We may suppose that none of $\lambda(1), \ldots, \lambda(n)$ is zero. We use induction on n. The assertion of the lemma is trivially true for $n = 1$. Suppose $n = 2$. By the notice above, the largest exponent among the powers of p which divide $(\lambda(1)+\lambda(2))!/\lambda(1)!\lambda(2)!$ is equal to

$$N(\lambda(1)+\lambda(2)) - N(\lambda(1)) - N(\lambda(2))$$

$$= \Sigma_{\kappa\in\mathbb{N}}(a_1(\kappa) + a_2(\kappa) - b(\kappa))/(p-1).$$

It suffices to show that $\Sigma_{\kappa\in\mathbb{N}}(a_1(\kappa)+a_2(\kappa)-b(\kappa)) > 0$ in case $a_1(\kappa) + a_2(\kappa) \neq b(\kappa)$ for some value of κ.

The last inequality means that carrying occurs at some place in the summation of the p-adic expressions of $\lambda(1)$ and $\lambda(2)$. Suppose that a succession of carryings begins

really at the κth place and ends at the $(\kappa+\nu)$th place (ν being a positive integer), namely that

$$a_1(\kappa) + a_2(\kappa) \geq p,\ b(\kappa) = a_1(\kappa) + a_2(\kappa) - p,$$

$$a_1(\kappa+1) + a_2(\kappa+1) + 1 \geq p,$$

$$b(\kappa+1) = a_1(\kappa+1) + a_2(\kappa+1) + 1 - p,$$

$$\cdots \qquad\qquad \cdots$$

$$a_1(\kappa+\nu-1) + a_2(\kappa+\nu-1) + 1 \geq p,$$

$$b(\kappa+\nu-1) = a_1(\kappa+\nu-1) + a_2(\kappa+\nu-1) + 1 - p,$$

$$a_1(\kappa+\nu) + a_2(\kappa+\nu) + 1 < p,$$

$$b(\kappa+\nu) = a_1(\kappa+\nu) + a_2(\kappa+\nu) + 1.$$

Then $\Sigma_{i=\kappa}^{\kappa+\nu}(a_1(i)+a_2(i)-b(i)) = \nu(p-1) > 0$. On the contrary, if carrying does not occur at the κth place, then $a_1(\kappa) + a_2(\kappa) - b(\kappa) = 0$. Therefore, the assertion of the lemma is valid for $n = 2$. It is now easy to carry out the remaining part of the induction. q.e.d.

We add here two more properties of the derivation δ.

8° The given derivation δ is determined by $\delta_{p(\kappa)}$ ($\kappa \in \mathbb{N}$).

Lem.1 implies that the integer $[\nu]$ of 5° is not divisible by p. Hence we denote by $[\nu]^{-1}$ any one of the integers m with $[\nu]m \equiv 1 \pmod{p}$, these integers being mutually congruent modulo p. Therefore, we get from (D4"') the formula

$$\delta_\nu = [\nu]^{-1} \Pi_{\kappa \in \mathbb{N}} \delta_{p(\kappa)}{}^{c(\kappa)}.$$

9° We see that $\delta_\nu{}^p = 0$ for all $\nu \in \mathbb{N} - \{0\}$.

Set $n = p$ in (D4"), then $(p\nu)!/(\nu!)^p \equiv 0 \pmod p$ by Lem.1 if $\nu \in \mathbb{N}-\{0\}$.

We close this section by adding a lemma which is often useful in later calculations.

Lemma 2 We have the congruence

$$(p(e)\nu(1)+\ldots+p(e)\nu(n))!/(p(e)\nu(1))!\ldots(p(e)\nu(n))!$$

$$\equiv (\nu(1)+\ldots+\nu(n))!/\nu(1)!\ldots\nu(n)! \pmod p$$

for all $e \in \mathbb{N}$ and for all finite family $(\nu(1),\ldots,\nu(n))$ of natural numbers.

Proof. Let $X_1, \ldots, X_n$ be indeterminates over the prime field of characteristic p and ν the sum of $\nu(1), \ldots, \nu(n)$. Expanding both sides of the formula

$$(X_1 + \ldots + X_n)^{p(e)\nu} = (X_1{}^{p(e)} + \ldots + X_n{}^{p(e)})^\nu$$

by the polynomial theorem, we get the congruence of the lemma.

1.3. Examples of derivations

We begin this section with two general definitions.

Definition 1. Let R be a subring of a ring R'. Let $\delta = (\delta_\nu \mid \nu \in \mathbb{N})$ and $\delta' = (\delta'_\nu \mid \nu \in \mathbb{N})$ be derivations of R and R' respectively. If δ_ν is the restriction mapping to R of δ'_ν for all $\nu \in \mathbb{N}$, we call δ restriction derivation

to R of δ', and call δ' extension derivation to R' of δ.

Definition 2. Let R be a ring, and $\delta = (\delta_\nu | \nu \in \mathbb{N})$, $\delta' = (\delta'_\nu | \nu \in \mathbb{N})$ two derivations of R. If $\delta_\lambda \delta'_\mu = \delta'_\mu \delta_\lambda$ for all $\lambda, \mu \in \mathbb{N}$, we say that δ commutes with δ'.

Now we give some simple examples of derivations.

Example 1 Let R be any ring. If we set $\delta_0 = id_R$ and $\delta_\nu = 0$ for all $\nu \in \mathbb{N}-\{0\}$, then $\delta = (\delta_\nu | \nu \in \mathbb{N})$ is trivially a derivation of R. It is called trivial derivation of R. Then the ring of δ-constants of R is the whole ring R.

Example 2 Let R be a ring, $\delta = (\delta_\nu | \nu \in \mathbb{N})$ a derivation of R, $\{U_i | i \in I\}$ a set of indeterminates over R, and $S = R[U_i | i \in I]$ the ring of polynomials in U_i $(i \in I)$ over R. For every $(\rho) = (\rho(i) | i \in I) \in \mathbb{N}^{(I)}$, the product $U^{(\rho)} = \Pi_{i \in I} U_i^{\rho(i)}$ is well defined, and called monomial with coefficient 1 in U_i $(i \in I)$. Every $P \in S$ is uniquely written in the form $P = \Sigma a_{(\rho)} U^{(\rho)}$ with $a_{(\rho)} \in R$, where the summation Σ runs through all $(\rho) \in \mathbb{N}^{(I)}$. If we set $\delta'_\nu P = \Sigma \delta_\nu a_{(\rho)} U^{(\rho)}$ for all $\nu \in \mathbb{N}$, then $\delta' = (\delta'_\nu | \nu \in \mathbb{N})$ is clearly an extension derivation to S of δ. The ring of polynomials $R_{C,\delta}[U_i | i \in I]$ in U_i over $R_{C,\delta}$ is the ring of δ'-constants of S.

Example 3 Let R[[U]] be the ring of formal power series in an indeterminate U over a ring R. Let R[U] be

the ring of polynomials in U over a ring R, canonically identified with a subring of $R[[U]]$. Every $P \in R[[U]]$ is uniquely written in the form $P = \Sigma_{\rho\in\mathbb{N}} a_\rho U^\rho$ with $a_\rho \in R$. P is in $R[U]$ if and only if a_ρ are zeros for all sufficiently large $\rho \in \mathbb{N}$. For every $P = \Sigma_{\rho\in\mathbb{N}} a_\rho U^\rho$ in $R[[U]]$ with $a_\rho \in R$, set

$$d_\nu P = \Sigma_{\rho\in\mathbb{N}} \binom{\rho}{\nu} a_\rho U^{\rho-\nu} \quad (\nu \in \mathbb{N}).$$

We see easily that $d = (d_\nu | \ \nu \in \mathbb{N})$ is a derivation of $R[[U]]$, using the well-known formulas $\binom{\rho+\sigma}{\nu} = \Sigma_{\lambda+\mu=\nu} \binom{\rho}{\lambda}\binom{\sigma}{\mu}$ and $\binom{\rho}{\mu}\binom{\rho-\mu}{\lambda} = \binom{\lambda+\mu}{\lambda}\binom{\rho}{\lambda+\mu}$ for $\rho,\sigma,\tau,\lambda,\mu,\nu \in \mathbb{N}$. If P is particularly in $R[U]$, $d_\nu P$ $(\nu \in \mathbb{N})$ are in $R[U]$, hence restrictions to $R[U]$ of d_ν $(\nu \in \mathbb{N})$ give rise to a derivation of $R[U]$; this derivation is also denoted by d. The derivation d of $R[[U]]$ (respectively $R[U]$) is called <u>formal differentiation</u> of $R[[U]]$ (respectively $R[U]$) relative to U, and often denoted by $d_U = (d_{U\nu} | \ \nu \in \mathbb{N})$. The ring of d-constants of $R[[U]]$ is R, and so is that of $R[U]$. In $R[U]$, d_1 is sometimes denoted by the traditional notation d/dU, that is, $dP/dU = d_1 P$ for every $P \in R[U]$.

<u>Example 4</u> Let R be a ring, $\{U_i | i \in I\}$ with card $I > 1$ a set of indeterminates over R, and $S = R[U_i | \ i \in I]$ the ring of polynomials in U_i $(i \in I)$ over R. For each $j \in I$, let $S_j = R[U_i | \ i \in I, i \neq j]$ the subring of S of polynomials in U_i $(i \in I, i \neq j)$ over R, then S can be regarded as the ring of polynomials in a single indeterminate U_j over

S_j. Applying Examp.3 on S_j, U_j instead of R, U, we get a derivation $\partial_j = (\partial_{j\nu} | \nu \in \mathbb{N})$ which is called formal partial differentiation of S relative to U_j ; this is often denoted by $\partial_{U_j} = (\partial_{U_j\nu} | \nu \in \mathbb{N})$. Derivations ∂_j ($j \in I$) commute mutually, that is, $\partial_{j\lambda}\partial_{k\mu} = \partial_{k\mu}\partial_{j\lambda}$ for all $j,k \in I$ and for all $\lambda,\mu \in \mathbb{N}$. For each $j \in I$, ∂_{j1} is sometimes denoted by $\partial/\partial U_j$; thus $\partial P/\partial U_j = \partial_{j1}P$ for every $P \in S$.

We put here a proposition which states that any derivation δ of a ring R gives rise to an infinite sequence of derivations of R which are defined in a natural manner (cf. [6]).

Proposition 1 Let δ be a derivation of a ring R.

(a) For each $\kappa \in \mathbb{N}$, a derivation $\delta^{(\kappa)} = (\delta_\nu^{(\kappa)} | \nu \in \mathbb{N})$ of R is defined as follows: for every $x \in R$, we set

$$\delta_\nu^{(\kappa)}x = \begin{cases} 0 & (\nu \not\equiv 0 \pmod{p(\kappa)}) \\ \delta_n x & (\nu \equiv 0 \pmod{p(\kappa)} \text{ and } \nu = p(\kappa)n). \end{cases}$$

(b) Derivations $\delta^{(\kappa)}$ ($\kappa \in \mathbb{N}$) commute mutually. For each $\kappa \in \mathbb{N}$, the ring of $\delta^{(\kappa)}$-constants of R coincides with that of δ-constants. If $\kappa(1),\kappa(2) \in \mathbb{N}$, then

$$(\delta^{(\kappa(1))})^{(\kappa(2))} = \delta^{(\kappa(1)+\kappa(2))}.$$

Proof. (a) For each $\delta^{(\kappa)}$ ($\kappa \in \mathbb{N}$), since conditions (D1~3) are clearly satisfied, we verify here only (D4). Let $\lambda,\mu \in \mathbb{N}$ and $x \in R$.

Case I: $\lambda + \mu \not\equiv 0 \pmod{p(\kappa)}$. Since at least one of $\lambda \not\equiv 0$, $\mu \not\equiv 0 \pmod{p(\kappa)}$ takes place, we see that $\delta_\lambda^{(\kappa)} \delta_\mu^{(\kappa)} x = 0 = \binom{\lambda+\mu}{\lambda} \delta_{\lambda+\mu}^{(\kappa)} x$.

Case II: $\lambda + \mu \equiv 0$, $\lambda \not\equiv 0$, $\mu \not\equiv 0 \pmod{p(\kappa)}$ and $\lambda + \mu = p(k)n$. Since $\binom{\lambda+\mu}{\lambda} \equiv 0 \pmod{p}$ by Lem.1 of §1.2, we see that $\binom{\lambda+\mu}{\lambda} \delta_{\lambda+\mu}^{(\kappa)} x = \binom{\lambda+\mu}{\lambda} \delta_n x = 0 = \delta_\lambda^{(\kappa)} \delta_\mu^{(\kappa)} x$.

Case III: $\lambda \equiv 0$, $\mu \equiv 0 \pmod{p(\kappa)}$, $\lambda = p(\kappa)\ell$ and $\mu = p(\kappa)m$. By Lem.2 of §1.2, we see that $\delta_\lambda^{(\kappa)} \delta_\mu^{(\kappa)} x = \delta_\ell \delta_m x = \binom{\ell+m}{\ell} \delta_{\ell+m} x = \binom{\lambda+\mu}{\lambda} \delta_{\lambda+\mu}^{(\kappa)} x$.

Thus (D4) is satisfied in all possible cases.

(b) The first and the second assertions are clear. Set $\kappa = \kappa(1)$ and $\lambda = \kappa(2)$ for simplicity. Let $x \in R$ and $\nu \in \mathbb{N}$.

Case I: $\nu \not\equiv 0 \pmod{p(\lambda)}$. Since also $\nu \not\equiv 0 \pmod{p(\kappa+\lambda)}$, we see that $(\delta^{(\kappa)})_\nu^{(\lambda)} x = 0 = \delta_\nu^{(\kappa+\lambda)} x$.

Case II: $\nu \equiv 0 \pmod{p(\lambda)}$, $\nu = p(\lambda)n$, $\nu \not\equiv 0 \pmod{p(\kappa+\lambda)}$. Since $n \not\equiv 0 \pmod{p(\kappa)}$, we see that $(\delta^{(\kappa)})_\nu^{(\kappa)} x = \delta_n^{(\kappa)} x = 0 = \delta_\nu^{(\kappa+\lambda)} x$.

Case III: $\nu \equiv 0 \pmod{p(\lambda)}$, $\nu = p(\lambda)n$, $\nu \equiv 0 \pmod{p(\kappa+\lambda)}$, $\nu = p(\kappa+\lambda)m$. Since $n = p(\kappa)m$, we see that $(\delta^{(\kappa)})_\nu^{(\lambda)} x = \delta_n^{(\kappa)} x = \delta_m x = \delta_\nu^{(\kappa+\lambda)} x$.

Thus, the last assertion of (b) holds true in all possible cases.

1.4. Derivatives of powers

Let $\delta = (\delta_\nu \mid \nu \in \mathbb{N})$ be a derivation of a ring R. If $x \in R$ and $\nu \in \mathbb{N}$, we say that $\delta_\nu x$ is the *νth δ-derivative* or the *δ-derivative of order ν* of x. We call $\delta_\nu x$ $(\nu \in \mathbb{N})$ *δ-derivatives* of x.

We give in this section some useful formulas on δ-derivatives of powers of x.

Proposition 2 For any $n,\nu \in \mathbb{N}-\{0\}$, we have the formula

$$(1)\quad \begin{cases} \delta_\nu(x^n) = \Sigma_{\nu(1)+\ldots+\nu(n)=\nu} \delta_{\nu(1)}x \cdot \ldots \cdot \delta_{\nu(n)}x \\ = nx^{n-1}\delta_\nu x + \Sigma' \dfrac{n!}{n(1)!\ldots n(r)!}(\delta_{\mu(1)}x)^{n(1)}\ldots(\delta_{\mu(r)}x)^{n(r)}, \end{cases}$$

where the summation Σ' runs through all $r \in \mathbb{N}-\{0\}$, $(\mu(1), \ldots,\mu(r)) \in \mathbb{N}^r$, $(n(1),\ldots,n(r)) \in (\mathbb{N}-\{0\})^r$ that satisfy $\mu(1) <\ldots<\mu(r)<\nu$, $n(1)+\ldots+n(r)=n$, $n(1)\mu(1)+\ldots+n(r)\mu(r)=\nu$.

Proof. It is easy by (D3) to get the formula.

Corollary Let $\nu,e \in \mathbb{N}-\{0\}$, $\alpha \in \mathbb{N}-\{0,1\}$ and $x \in R$.

(a) If $\nu \not\equiv 0 \pmod{p(e)}$, then

$$(2)\quad \delta_\nu(x^{p(e)}) = 0$$

and

$$(3)\quad \delta_\nu(x^{\alpha p(e)}) = 0.$$

(b) If $\nu \equiv 0 \pmod{p(e)}$ and $\nu = p(e)n$, then

$$(4)\quad \delta_\nu(x^{p(e)}) = (\delta_n x)^{p(e)}$$

and

(5) $\delta_\nu(x^{\alpha p(e)}) = \alpha(x^{\alpha-1}\delta_n x)^{p(e)} + \Sigma''(\delta_{n(1)}x\cdot\ldots\cdot\delta_{n(\alpha)}x)^{p(e)}$,

where the summation Σ'' runs through the set of all $(n(1), \ldots, n(\alpha)) \in \mathbb{N}^\alpha$ with $n(1) < n, \ldots, n(\alpha) < n$, $n(1) + \ldots + n(\alpha) = n$.

Proof. (a) Applying (1) on $p(e)$ instead of n, we get (2) by Lem.1 of §1.2. The formula (3) is an immediate consequence of (2).

(b) We get (4) by similar observation as the case of (2). Then, using (4), we see that $\delta_\nu(x^{\alpha p(e)}) = (\delta_n(x^\alpha))^{p(e)}$, so that

$$\delta_\nu(x^{\alpha p(e)}) = (\Sigma_{n(1)+\ldots+n(\alpha)=n}\delta_{n(1)}x\ldots\delta_{n(\alpha)}x)^{p(e)}$$
$$= (\alpha x^{\alpha-1}\delta_n x + \Sigma''\delta_{n(1)}x\ldots\delta_{n(\alpha)}x)^{p(e)}.$$

Since $\alpha^{p(e)} \equiv \alpha \pmod p$, we get the formula (5).

Proposition 3 If δ is a derivation of a perfect field K, then δ is always trivial.

Proof. Let $x \in K$ and $\nu \in \mathbb{N}-\{0\}$. If we take $e \in \mathbb{N}$ such that $\nu \equiv 0 \pmod{p(e)}$ and $\nu \not\equiv 0 \pmod{p(e+1)}$, then we see by (2) that $\delta_\nu x = \delta_\nu((x^{p(-e-1)})^{p(e+1)}) = 0$ since $x^{p(-e-1)} \in K$.

1.5. Taylor expansion

Let $R[[U]]$ be the ring of formal power series in an indeterminate U over a ring R, and d the formal differentiation of $R[[U]]$ relative to U (see Examp.3 of §1.3).

Let a derivation δ of R be given. If we set $E(x) = \Sigma_{\nu\in\mathbb{N}}\delta_\nu x\cdot U^\nu$ for every $x \in R$, a mapping E of R into $R[[U]]$ is defined. It is called Taylor expansion of R relative to δ. We see easily by (D1~4) that E is a ring-isomorphism of R into $R[[U]]$ having the property

(1) $E(\delta_\rho x) = d_\rho E(x)$ $(x \in R, \rho \in \mathbb{N})$.

Lemma 3 Let E' be a mapping of a ring R into the ring $R[[U]]$ of formal power series in an indeterminate U over R. For every $x \in R$, write $E'(x) = \Sigma_{\nu\in\mathbb{N}}\varepsilon_\nu(x)U^\nu$ $(\varepsilon_\nu(x) \in R)$.

(a) The ε_ν $(\nu \in \mathbb{N})$ are mappings of R into R. For these mappings, each one of the conditions

1° $\varepsilon_0(x) = x$,

2° $\varepsilon_\nu(x+y) = \varepsilon_\nu(x) + \varepsilon_\nu(y)$,

3° $\varepsilon_\nu(xy) = \Sigma_{\nu(1)+\nu(2)=\nu}\varepsilon_{\nu(1)}(x)\varepsilon_{\nu(2)}(y)$,

4° $\varepsilon_\lambda(\varepsilon_\mu(x)) = \binom{\lambda+\mu}{\lambda}\varepsilon_{\lambda+\mu}(x)$

for all $x,y \in R$ and for all $\lambda,\mu,\nu \in \mathbb{N}$ is equivalent to the corresponding one of the conditions

1' $\varepsilon_0(x) = x$,

2' $E'(x+y) = E'(x) + E'(y)$,

3' $E'(xy) = E'(x)E'(y)$,

4' $E'(\varepsilon_\rho(x)) = d_\rho E'(x)$

for all $x,y \in R$ and for all $\rho \in \mathbb{N}$.

(b) If all the conditions of (a) are satisfied and if we set $\delta'_\nu = \varepsilon_\nu$ $(\nu \in \mathbb{N})$, $\delta' = (\delta'_\nu \mid \nu \in \mathbb{N})$ is a derivation of R and E' is the Taylor expansion of R relative to δ'.

The proof of the lemma is straightforward.

1.6. Rings of quotients

Let M be a multiplicatively stable subset of a ring R, that is, M is a subset of R which contains the product $s_1 s_2$ for all $s_1, s_2 \in M$, and which contains 1 but not 0. Let $M^{-1}R$ be the ring of quotients of R over M (see §4 of Chap.0 of [4]).

Theorem 1 Let δ be a derivation of R. Then δ has a unique extension derivation $\delta' = (\delta'_\nu \mid \nu \in \mathbb{N})$ to $M^{-1}R$. For every $x = a/s$ $(a \in R, s \in M)$ in $M^{-1}R$, $\delta'_\nu x$ $(\nu \in \mathbb{N})$ are defined inductively by formulas

(1) $\delta'_0 x = x$, $\delta_\nu a = \delta'_\nu x \cdot s + \sum_{\alpha=1}^{\nu} \delta'_{\nu-\alpha} x \cdot \delta_\alpha s$ $(\nu \in \mathbb{N}-\{0\})$.

Proof. For simplicity, R' denotes $M^{-1}R$ in this proof. Let R'[[U]] be the ring of formal power series in an indeterminate U over R', and R[[U]] its subring of all formal power series in U over R. Let d and d' be formal differentiations relative to U of R[[U]] and R'[[U]] respectively. Then d' is an extension derivation to R'[[U]] of d.

In order to prove the uniqueness assertion, suppose that δ has an extension derivation δ' to R'. Let E and E'

be Taylor expansions of R and R' relative to δ and δ' respectively. Then E is the restriction mapping of E' to R. For every $x = a/s$ $(a \in R,\ s \in M)$ of R', we get $E(a) = E'(x)E(s)$. Since $E(s)$ is invertible in $R'[[U]]$, we see that

(2) $\quad E'(x) = E(a)/E(s).$

Starting afresh, let E be the Taylor expansion of R relative to the given derivation δ, then we can define by (2) a mapping E' of R' into $R'[[U]]$. In fact, if $x = a_1/s_1 = a_2/s_2$ $(a_1, a_2 \in R;\ s_1, s_2 \in M)$, there exists $s \in M$ such that $a_1 s_2 s = a_2 s_1 s$, so that $E(a_1)E(s_2)E(s) = E(a_2)E(s_1)E(s)$ and $E(a_1)/E(s_1) = E(a_2)/E(s_2)$. This mapping E' is an extension mapping of E to R' and a ring-homomorphism of R' into $R'[[U]]$. For every $x = a/s$ $(a \in R,\ s \in M)$ of R', write $E'(x)$ in the form $E'(x) = \Sigma_{\nu \in \mathbb{N}} \varepsilon_\nu(x) U^\nu$ $(\varepsilon_\nu(x) \in R')$. Then we can see that conditions 1'~4' of part (a) of Lem.3 of §1.5 are satisfied for R' instead of R. Since conditons 1'~3' are now obvious, we prove by double induction on λ, μ that condition 4° is satisfied. If $\lambda = \mu = 0$, 4° is trivially true. Suppose that at least one of λ, μ is positive. Applying 3° to $a = xs$, we get $\delta_\mu a = \Sigma_{\mu(1)+\mu(2)=\mu} \varepsilon_{\mu(1)}(x) \delta_{\mu(2)} s$. Applying 3° again to this equation, we see that

$$\delta_\lambda \delta_\mu a = \Sigma_{\substack{\lambda(1)+\lambda(2)=\lambda \\ \mu(1)+\mu(2)=\mu}} \varepsilon_{\lambda(1)}(\varepsilon_{\mu(1)}(x)) \delta_{\lambda(2)} \delta_{\mu(2)} s,$$

so that

$$\binom{\lambda+\mu}{\lambda}\delta_{\lambda+\mu}a$$

$$= \varepsilon_\lambda(\varepsilon_\mu(x))s + \Sigma'\binom{\lambda(2)+\mu(2)}{\lambda(2)}\varepsilon_{\lambda(1)}(\varepsilon_{\mu(1)}(x))\delta_{\lambda(2)+\mu(2)}s,$$

where the summation Σ' runs through all those $(\lambda(1),\lambda(2),\mu(1),\mu(2)) \in \mathbb{N}^4$ that satisfy $\lambda(1) + \lambda(2) = \lambda$, $\mu(1) + \mu(2) = \mu$ and at least one of $\lambda(1) < \lambda$, $\mu(1) < \mu$ takes place. Therefore we see by induction assumption that

$$\binom{\lambda+\mu}{\lambda}\delta_{\lambda+\mu}a$$

$$= \varepsilon_\lambda(\varepsilon_\mu(x))s$$

$$+ \Sigma'\binom{\lambda(2)+\mu(2)}{\lambda(2)}\binom{\lambda(1)+\mu(1)}{\lambda(1)}\varepsilon_{\lambda(1)+\mu(1)}(x)\delta_{\lambda(2)+\mu(2)}s.$$

Set $\lambda(1) + \mu(1) = \alpha$, $\lambda(2) + \mu(2) = \beta$, then

$$\binom{\lambda+\mu}{\lambda}\delta_{\lambda+\mu}a = \varepsilon_\lambda(\varepsilon_\mu(x))s + \Sigma''\binom{\alpha}{\lambda(1)}\binom{\beta}{\lambda(2)}\varepsilon_\alpha(x)\delta_\beta s,$$

where the summation Σ'' runs through the set of all $(\alpha,\beta,\lambda(1),\lambda(2)) \in \mathbb{N}^4$ with $\alpha + \beta = \lambda + \mu$, $\lambda(1) + \lambda(2) = \lambda$, $\alpha < \lambda + \mu$. Hence

$$(3)\quad \binom{\lambda+\mu}{\lambda}\delta_{\lambda+\mu}a = \varepsilon_\lambda(\varepsilon_\mu(x))s + \Sigma'''\binom{\lambda+\mu}{\lambda}\varepsilon_\alpha(x)\delta_\beta s,$$

where the summation Σ''' runs through the set of all $(\alpha,\beta) \in \mathbb{N}^2$ with $\alpha + \beta = \lambda + \mu$, $\alpha < \lambda + \mu$. On the other hand, applying 3° to $a = xs$ in another way, we get

$$(4)\quad \delta_{\lambda+\mu}a = \Sigma_{\alpha+\beta=\lambda+\mu}\varepsilon_\alpha(x)\delta_\beta s = \varepsilon_{\lambda+\mu}(x)s + \Sigma'''\varepsilon_\alpha(x)\delta_\beta s.$$

Comparing (3) and (4), we see that $\varepsilon_\lambda(\varepsilon_\mu(x))s = \binom{\lambda+\mu}{\lambda}\varepsilon_{\lambda+\mu}(x)s$. If $\varepsilon_\lambda(\varepsilon_\mu(x)) = b_1/t_1$, $\binom{\lambda+\mu}{\lambda}\varepsilon_{\lambda+\mu}(x) = b_2/t_2$

$(b_1,b_2 \in R;\ t_1,t_2 \in M)$, then there exists $t \in M$ with $b_1t_2st = b_2t_1st$. Since $st \in M$, we conclude that $\varepsilon_\lambda(\varepsilon_\mu(x)) = b_1/t_1 = b_2/t_2 = \binom{\lambda+\mu}{\lambda}\varepsilon_{\lambda+\mu}(x)$.

Therefore, by part (b) of Lem.3 of §1.5, if we set $\delta'_\nu = \varepsilon_\nu$ $(\nu \in \mathbb{N})$, $\delta' = (\delta'_\nu \mid \nu \in \mathbb{N})$ is a derivation of R'; and it is an extension derivation of δ to R'.

The remaining part of the theorem is now clear. q.e.d.

By virtue of the uniqueness statement of Th.1, the extension derivation δ' of δ to $M^{-1}R$ will henceforth be denoted also by the original letter δ.

Corollary 1 Let R and M be as above, and δ, δ' two derivations of R commuting mutually. Then extension derivations of δ and δ' to $M^{-1}R$ commute mutually.

It is straightforward to prove by double induction on λ, μ that $\delta'_\lambda\delta_\mu x = \delta_\mu\delta'_\lambda x$ $(\lambda,\mu \in \mathbb{N};\ x \in M^{-1}R)$.

Corollary 2 Every derivation of an integral domain R has a unique extension derivation to the field of quotients $Q(R)$ of R.

Example 1 Let U be an indeterminate over a field K, $K[U]$ the ring of polynomials in U over K, and d (or d_U) the formal differentiation of $K[U]$ relative to U (see Examp.3 of §1.3). By Cor.2, this derivation d can be uniquely extended to a derivation of the field of quotients $K(U)$ of $K[U]$. The latter derivation is also called formal diffe-

rentiation of $K(U)$ relative to U, and denoted also by d (or d_U). We see that tha field of d-constants of $K(U)$ is K.

In order to show this, let A and B be two relatively prime polynomials of $K[U]$, and suppose that $\gamma = A/B$ is a d-constant. We claim that both A and B do not contain U effectively. Assume the contrary. Then, for some $e \in \mathbb{N}$, $A = \Sigma_{\alpha=0}^{m} a_\alpha U^{\alpha p(e)}$, $B = \Sigma_{\beta=0}^{n} b_\beta U^{\beta p(e)}$ $(a_\alpha, b_\beta \in K)$, at least one of m and n is positive, and there exists either some $a_\alpha \neq 0$ with $\alpha \not\equiv 0 \pmod{p}$ or some $b_\beta \neq 0$ with $\beta \not\equiv 0 \pmod{p}$. Applying $d_{p(e)}$ to $A = \gamma B$, we see by (4) of §1.4 that

$$B\Sigma_{\alpha=0}^{m} a_\alpha (\alpha U^{\alpha-1})^{p(e)} = A\Sigma_{\beta=0}^{n} b_\beta (\beta U^{\beta-1})^{p(e)},$$

and that this equation can not hold. Thus the claim above is verified.

Example 2 Let U_i $(i \in I)$ be a set of indeterminates over a field K, and $K[U_i \mid i \in I]$ the ring of polynomials in U_i $(i \in I)$ over K. Let j be any element of I. Let ∂_j (or ∂_{U_j}) be the formal differentiation of $K[U_i \mid i \in I]$ relative to U_j (see Examp.4 of §1.3). By Cor.2 this derivation ∂_j give rise to a unique extension derivation of the field of quotients $K(U_i \mid i \in I)$ of $K[U_i \mid i \in I]$. The extension derivation is also called formal partial differentiation of $K(U_i \mid i \in I)$ relative to U_j, denoted by ∂_j (or ∂_{U_j}). We can show by using Examp.1 that the field of ∂_j-constants

is $K(U_i \mid i \in I, i \neq j)$.

1.7. Separably algebraic extension fields

Theorem 2 Let H be a separably algebraic extension field of a field K of finite relative degree n. Let x be a primitive element of H over K, and $f(X) = \Sigma_{\rho=0}^{n} a_\rho X^\rho$ ($a_\rho \in K$, $a_n = 1$) the minimal polynomial of x over K. Let δ be a derivation of K.

(a) H has a unique extension derivation $\delta' = (\delta'_\nu \mid \nu \in \mathbb{N})$ of δ.

(b) If we set $f'(X) = df/dX = \Sigma_{\rho=0}^{n} \rho a_\rho X^{\rho-1}$, then $f'(x) \neq 0$ and $\delta'_\nu x$ ($\nu \in \mathbb{N}$) can be defined inductively by formulas

(1) $\delta'_0 x = 0$,

$$f'(x)\delta'_\nu x + \Sigma_{\rho=0}^{n} \Sigma' \delta_{\nu(0)} a_\rho \delta'_{\nu(1)} x \ldots \delta'_{\nu(\rho)} x = 0 \quad (\nu \in \mathbb{N}-\{0\}),$$

where the summation Σ' runs through all those $(\nu(0),\ldots,\nu(\rho)) \in \mathbb{N}^{\rho+1}$ that satisfy $\nu(0)+\ldots+\nu(\rho)=\nu$, $\nu(1) < \nu$, ..., $\nu(\rho) < \nu$. Each $y \in H$ is uniquely written in the form $y = \Sigma_{\sigma=0}^{n-1} b_\sigma x^\sigma$ ($b_\sigma \in K$), and $\delta'_\nu y$ ($\nu \in \mathbb{N}$) are given by formulas

(2) $$\delta'_\nu y = \Sigma_{\sigma=0}^{n-1} \Sigma_{\nu(0)+\ldots+\nu(\sigma)=\nu} \delta_{\nu(0)} b_\sigma \delta'_{\nu(1)} x \ldots \delta'_{\nu(\sigma)} x.$$

Proof. Let $H[[U]]$ be the ring of formal power series in an indeterminate U over H, and $K[[U]]$ its subring of all formal power series in U over K. Let d and d' be formal differentiations of $K[[U]]$ and $H[[U]]$ relative to U respectively. Then d is the restriction derivation of d'.

(a) In order to prove the uniqueness assertion, suppose that δ has an extension derivation δ' to H. Let E and E' be Taylor expansions of K and H relative to δ and δ' respectively. Then E is a restriction mapping of E' to K. Applying E' to $f(x) = 0$ and $y = \Sigma_{\sigma=0}^{n-1} b_\sigma x^\sigma$ (in part (b)), and setting $f^E(X) = \Sigma_{\rho=0}^{n} E(a_\rho) X^\rho$, we get

$$(3) \quad f^E(E'(x)) = \Sigma_{\rho=0}^{n} E(a_\rho) E'(x)^\rho = 0,$$

and

$$(4) \quad E'(y) = \Sigma_{\sigma=0}^{n-1} E(b_\sigma) E'(x)^\sigma.$$

Starting afresh, let E be the Taylor expansion of K relative to the given derivation δ, then we can define a mapping E' of H into $H[[U]]$ by (3) and (4). In fact, if we set $E'(x) = \Sigma_{\nu \in \mathbb{N}} \varepsilon_\nu(x) U^\nu$ ($\varepsilon_\nu(x) \in H$, $\varepsilon_0(x) = x$), (3) is written in the form

$$\Sigma_{\nu \in \mathbb{N}} (\Sigma_{\rho=0}^{n} \Sigma' \delta_{\mu(0)} a_\rho \cdot \varepsilon_{\mu(1)}(x) \cdots \varepsilon_{\mu(\rho)}(x)) U^\nu = 0 \quad (\nu \in \mathbb{N}),$$

where the summation Σ' runs through the set of all those $(\mu(0), \ldots, \mu(\rho)) \in \mathbb{N}^{\rho+1}$ with $\mu(0) + \ldots + \mu(\rho) = \nu$, or equivalently

$$(5) \quad \begin{cases} \varepsilon_0(x) = x, \\ f'(x)\varepsilon_\nu(x) + \Sigma_{\rho=0}^{n} \Sigma'' \delta_{\mu(0)} a_\rho \varepsilon_{\mu(1)}(x) \cdots \varepsilon_{\mu(\rho)}(x) = 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\nu \in \mathbb{N} - \{0\}), \end{cases}$$

where the summation Σ'' runs through the set of all those $(\mu(0), \ldots, \mu(\rho)) \in \mathbb{N}^{\rho+1}$ with $\mu(0) + \ldots + \mu(\rho) = \nu$, $\mu(1) <$

$\nu, \ldots, \mu(\rho) < \nu$. Since $f'(x) \neq 0$, $\varepsilon_\nu(x)$ $(\nu \in \mathbb{N})$ can be defined in H inductively by (5). The mapping E' thus defined by (3) and (4) is clearly an extension mapping of E. If we write $E'(y)$ in the form $E'(y) = \Sigma_{\nu\in\mathbb{N}}\varepsilon_\nu(y)U^\nu$ $(\varepsilon_\nu(y) \in H)$ for all $y \in H$, it is straightforward to prove that E' satisfies the conditions 1'~3' of part (a) of Lem.3 of §1.5 for H instead of R. We prove here that the condition 4' of the lemma is satisfied, namely, that

(6) $E'(\varepsilon_\nu(y)) = d'_\nu E'(y)$ $(y \in H, \nu \in \mathbb{N})$.

In the first place, we prove (6) for $y = x$ by induction on ν. If $\nu = 0$, (6) is trivially true. Suppose $\nu > 0$, then, applying E' to (5) and using induction assumption, we get

(7) $f'^E(E'(x))E'(\varepsilon_\nu(x))$

$$+ \Sigma_{\rho=0}^{n}\Sigma''d_{\mu(0)}E(a_\rho)d'_{\mu(1)}E'(x)\ldots d'_{\mu(\rho)}E'(x) = 0.$$

On the other hand, applying d'_ν to (3), we get

(8) $f'^E(E'(x))d'_\nu E'(x)$

$$+ \Sigma_{\rho=0}^{n}\Sigma''d_{\mu(0)}E(a_\rho)d'_{\mu(1)}E'(x)\ldots d'_{\mu(\rho)}E'(x) = 0.$$

Since $f'(x) \neq 0$ implies $f'^E(E'(x)) \neq 0$, we see by comparing (7) with (8) that $E'(\varepsilon_\nu(x)) = d'_\nu E'(x)$ $(\nu \in \mathbb{N})$.

In the second place, we prove (6) for every $y = \Sigma_{\sigma=0}^{n-1}b_\sigma x^\sigma$ $(b_\sigma \in K)$ of H. Since E' satisfies the conditions 2' and 3', we see by part (a) of Lem.3 of §1.5 that mappings ε_ν $(\nu \in \mathbb{N})$ satisfy the conditions 2° and 3° of

the lemma. Hence, for every $\nu \in \mathbb{N}$, we see that

$$E'(\varepsilon_\nu(y)) = E'(\Sigma_{\sigma=0}^{n-1}\Sigma_{\nu(0)+\ldots+\nu(\sigma)=\nu}\delta_{\nu(0)}b_\sigma\varepsilon_{\nu(1)}(x)\ldots\varepsilon_{\nu(\sigma)}(x))$$
$$= \Sigma_{\sigma=0}^{n-1}\Sigma_{\nu(0)+\ldots+\nu(\sigma)=\nu}d_{\nu(0)}E(b_\sigma)d'_{\nu(1)}E'(x)\ldots d'_{\nu(\sigma)}E'(x)$$
$$= d'_\nu E'(y).$$

Therefore, by part (b) of Lem.3 of §1.5, if we set $\delta'_\nu = \varepsilon_\nu$ $(\nu \in \mathbb{N})$, then $\delta' = (\delta'_\nu \mid \nu \in \mathbb{N})$ is a derivation of H. Since E is the restriction mapping of E', δ is the restriction derivation of δ'. Thus the proof of part (a) is completed.

(b) This part of the theorem is now easily verified.

Remark In the proof above of Th.2, the extension derivation δ' of the given derivation δ seems to depend on the choice of the primitive element x of H over K, but that is not the case. In fact, for each $y \in H$, if $g(Y)$ is the minimal polynomial of y over K and if E' is the Taylor expansion of H relative to an extension derivation of δ, then $E'(y)$ is uniquely determined in $H[[U]]$ by the equation $g^E(E'(y)) = 0$.

For any field K, we denote by K_a and K_s an algebraic closure of K and the separably algebraic closure of K in K_a respectively.

Corollary 1 Let L be any intermediate field between K and K_s. Every derivation of K has a unique extension derivation to L.

The proof is straightforward.

In accordance with the uniqueness assertion of Cor.1, the extension derivation to any intermediate field between K and K_s of a given derivation δ of K is henceforth denoted by the same letter δ.

Corollary 2 Let δ be a derivation of a field K, and C the field of δ-constants of K. Then the field of δ-constants of K_s is the separably algebraic closure C_s of C in K_a.

The proof is straightforward.

Corollary 3 Let δ and δ' be two derivations of a field K which commute mutually. Then extension derivations of δ and δ' to K_s commute mutually.

It is straightforward to prove by double induction on λ, μ that $\delta'_\lambda \delta_\mu x = \delta_\mu \delta'_\lambda x$ $(\lambda, \mu \in \mathbb{N};\ x \in K_s)$.

1.8. Inseparably algebraic extension fields

Let K be a field, K_a an algebraic closure of K, and K_s the separably algebraic closure of K in K_a. Suppose that a derivation δ of K is given. By Cor.1 to Th.2 of §1.7, δ has a unique extension derivation to K_s which we denote also by δ. We inquire in this section how far we can extend this derivation δ to K_a.

Let x be an element of K_a. We say that δ can be extended to x if δ has an extension derivation to some extension field of K_s that contains x. The following two

theorems are due to [8].

Theorem 3 Let K, K_a, K_s and δ be as above. Let x be an element of K_a. Then δ be extended to x if and only if the condition

(1) $\delta_\lambda(x^{p(e)}) = 0 \quad (0 < \lambda < p(e))$

is satisfied for some element $e \in \mathbb{N}$ with $x^{p(e)} \in K_s$. When that is the case, setting $\xi = x^{p(e)}$, the subfield

$$K_{s,x} = K_s((\delta_{\nu p(e)}\xi)^{p(-e)} \mid \nu \in \mathbb{N})$$

of K_a has a unique extension derivation $\delta' = (\delta'_\nu \mid \nu \in \mathbb{N})$ of δ which is defined by the formula

(2) $\delta'_\nu y = (\delta_{\nu p(e)}(y^{p(e)}))^{p(-e)} \quad (\nu \in \mathbb{N},\ y \in K_{s,x})$;

the equality $K_{s,x} = K_s(\delta'_\nu x \mid \nu \in \mathbb{N})$ holds true, and $K_{s,x}$ is the smallest extension field of K_s containing x that has an extension derivation of δ.

Remark 1 By Lem. 1 of §1.2, the condition (1) is equivalent to the condition

(1') $\delta_\lambda(x^{p(e)}) = 0 \quad (\lambda \in \mathbb{N}$ with $\lambda \not\equiv 0 \pmod{p(e)})$.

Proof of Th.3. Suppose that δ can be extended to x. Then x is contained in some extension field L of K_s which has an extension derivation δ' of δ. By (2) and (4) of §1.4, we see for every $e \in \mathbb{N}$ with $x^{p(e)} \in K_s$ that the condition (1') is satisfied, that (setting $\xi = x^{p(e)}$)

(3) $(\delta'_\nu x)^{p(e)} = \delta_{\nu p(e)}(x^{p(e)}) = \delta_{\nu p(e)}\xi \quad (\nu \in \mathbb{N})$,

that the subfield $K_{s,x} = K_s(\delta'_\nu x \mid \nu \in \mathbb{N}) = K_s((\delta_{\nu p(e)}\xi)^{p(-e)} \mid \nu \in \mathbb{N})$ of L has a derivation satisfying (2) which is the restriction of δ' to $K_{s,x}$ and that $K_{s,x} \subset K_a$.

Conversely, suppose that x satisfies the condition (1') for some $e \in \mathbb{N}$ with $x^{p(e)} = \xi \in K_s$. Consider the subfield $K_{s,x} = K_s((\delta_{\nu p(e)}\xi)^{p(-e)} \mid \nu \in \mathbb{N}) = K_s[(\delta_{\nu p(e)}\xi)^{p(-e)} \mid \nu \in \mathbb{N}]$ of K_a, and define mappings δ'_ν $(\nu \in \mathbb{N})$ of $K_{s,x}$ by the formula (2). Then we see easily that δ'_ν $(\nu \in \mathbb{N})$ are extension mapping of δ_ν $(\nu \in \mathbb{N})$ respectively, and, using Lem.2 of §1.2, that $\delta' = (\delta'_\nu x \mid \nu \in \mathbb{N})$ satisfies (D1~4) of §1.2. We see also that $K_{s,x} = K_s(\delta'_\nu x \mid \nu \in \mathbb{N})$ and that $x \in K_{s,x}$.

Remark 2 We can justify by Th.3 that, if an element x of K_a satisfies the condition (1) for some $e \in \mathbb{N}$ with $x^{p(e)} = \xi \in K_s$, then x satisfies the condition (1) for every $d \in \mathbb{N}$ with $x^{p(d)} = \eta \in K_s$, and that formulas $K_{s,x} = K_s((\delta_{\nu p(d)}\eta)^{p(-d)} \mid \nu \in \mathbb{N})$ and $\delta'_\nu y = (\delta_{\nu p(d)}(y^{p(d)}))^{p(-d)}$ $(\nu \in \mathbb{N},\ y \in K_{s,x})$ give the same smallest extension field of K_s containing x which has the same extension derivation $\delta' = (\delta'_\nu \mid \nu \in \mathbb{N})$ of δ.

Theorem 4 Let K, K_a, K_s and δ be as above. Then the set M of all those elements $x \in K_a$ such that δ can be extended to x is an extension field of K_s which has a

unique extension derivation of δ. The field M is the largest extension field of K_s in K_a that has an extension derivation of δ.

Proof. If $x \in M$, x satisfies the condition (1) for some $e \in \mathbb{N}$, hence so does $-x$, and $-x \in M$. If $x_1, x_2 \in M$, we see by Rem.2 that both x_1 and x_2 satisfy the condition (1) for a same $e \in \mathbb{N}$, and that $x_1 + x_2$, $x_1 x_2$ and (in case $x_2 \neq 0$) x_1/x_2 are contained in M. Therefore M is an extension field of K_s. For each $x \in M$, define mappings δ'_ν ($\nu \in \mathbb{N}$) by Th.3 using some $e \in \mathbb{N}$ with $x^{p(e)} \in K_s$ such that the condition (1) is satisfied for e. Then, by Th.3 and Rem.2, mappings δ'_ν ($\nu \in \mathbb{N}$) of M into M are well defined. It is straightforward to show that $\delta' = (\delta'_\nu \mid \nu \in \mathbb{N})$ is an extension derivation to M of δ. The remaining part of the proof of the theorem is now clear. q.e.d.

This derivation of M is henceforth denoted by the same letter δ as the original derivation of K. The field M is called <u>δ-closure</u> of K in K_a and denoted by K_δ.

<u>Corollary</u> Let K, K_a, K_s, δ and K_δ be as above. If we denote by C the field of δ-constants of K, then the fields of δ-constants of K_s and K_δ are the separably algebraic closure C_s and the algebraic closure C_a of C in K_a respectively.

The proof is straightforward by Cor.2 to Th.2 of §1.7 and Th.4.

If K is a perfect field, that is, if $K_s = K_a$, the derivation δ of K is necessarily trivial (see Prop.3 of §1.4) and $K_s = K_\delta = K_a$. On the contrary, consider the case of an imperfect field K, that is, the case that $K_s \neq K_a$. If δ is the trivial derivation of K, it is clear that the trivial derivation of K_a is the unique extension derivation of δ to K_a, so that $K_\delta = K_a$. If δ is a nontrivial derivation of K, then it may happen that $K_s \neq K_\delta \neq K_a$ (see Examp.1 below).

Example 1 Let U be an indeterminate over an imperfect field K_0, $K = K_0(U)$ the field generated by U over K_0, and d the formal differentiation of K relative to U (see Examp.1 of §1.6). Let K_a be an algebraic closure of K, K_s the separably algebraic closure of K in K_a, and K_d the d-closure of K in K_a. Let C denote the field of d-constants K_0 of K. Then fields of d-constants of K_s and K_d are the separably algebraic closure C_s of C in K_a and the algebraic closure C_a of C in K_a respectively, and $C_s \neq C_a$ since C is imperfect.

For each nonconstant $x \in K_a - K_s$, let $e = e(x)$ be the smallest positive integer such that $x^{p(e)} \in K_s$. Setting $\xi = x^{p(e)}$, K_d consists of all elements of K_s and all those x such that

(4) $d_n \xi = 0 \quad (0 < n < p(e))$.

Let $\Sigma_{j=0}^{\alpha} P_j X^j$ $(P_j \in K,\ P_\alpha = 1)$ be the minimal polynomial of

ξ over K. Multiplying it by a polynomial $A_\alpha \in C[U]$ of the smallest possible degree in U, we get a polynomial $f(X) = \Sigma_{j=0}^{\alpha} A_j X^j$, where $A_j = \Sigma_{k=0}^{\beta} a_{jk} U^{p(\varepsilon)k}$, $a_{jk} \in C$ $(0 \le j \le \alpha,$ $0 \le k \le \beta)$ with the largest possible $\varepsilon \in \mathbb{N}$. Then we see necessarily that $f(X) \notin C[U][X^p]$. Now, we can show that the condition (4) is equivalent to the condition

(5) $\varepsilon \ge e$.

Suppose that $\varepsilon \ge e$. Then, for every $n \in \mathbb{N}$ with $0 < n < p(e)$, we get $d_n A_j = 0$ $(0 \le j \le \alpha)$ and

$$0 = (df/dX)(\xi) \cdot d_n \xi + \Sigma_{j=0}^{\alpha} \Sigma' A_j d_{n(1)} \xi \cdots d_{n(j)} \xi,$$

where the summation Σ' runs through all $(n(1),\ldots,n(j)) \in \mathbb{N}^j$ with $n(1) + \ldots n(j) = n$, $n(1) < n$, $\ldots$, $n(j) < n$. Therefore, we see by induction on n that $d_n \xi = 0$ $(0 < n < p(e))$. Conversely, suppose $\varepsilon < e$. Then we see similarly that $d_n A_j = 0$ $(0 < n < p(\varepsilon),\ 0 \le j \le \alpha)$. If we had $d_{p(\varepsilon)} A_j = \Sigma_{k=0}^{\beta} a_{jk} k U^{p(\varepsilon)(k-1)} = 0$ for all j $(0 \le j \le \alpha)$, we should get $a_{jk} = 0$ $(0 \le j \le \alpha,\ 0 \le k \le \beta,\ k \not\equiv 0 \pmod p)$, contradicting the maximality of ε. Hence $d_{p(\varepsilon)} A_j \neq 0$ for some j.

Case: $\varepsilon = 0$. We see that $0 = (df/dX)(\xi) d_1 \xi + \Sigma_{j=0}^{\alpha} d_1 A_j \xi^j$, where $\Sigma_{j=0}^{\alpha} d_1 A_j \xi^j \neq 0$ by virtue of the construction of $f(X)$. Therefore $d_1 \xi \neq 0$, contradicting (4).

Case: $\varepsilon > 0$. For every n $(0 < n < p(\varepsilon))$, since we get

$$0 = (df/dX)(\xi) d_n \xi + \Sigma_{j=0}^{\alpha} \Sigma' A_j d_{n(1)} \xi \cdots d_{n(j)} \xi$$

(the summation Σ' being as above), we see by induction on n

that $d_n\xi = 0$ $(0 < n < p(\varepsilon))$. But, we see that

$$0 = (df/dX)(\xi)d_{p(\varepsilon)}\xi + \Sigma_{j=0}^{\alpha} d_{p(\varepsilon)}A_j\xi^j,$$

so that $d_{p(\varepsilon)}\xi \neq 0$, contradicting (4).

We can conclude that $K_d = K_s(C_a)$. It suffices to show that, if a nonconstant $x \in K_a - K_s$ satisfies the condition (5), x must be separably algebraic over $K_s(C_a)$. Let $f(X)$ be as above, and set $B_j = \Sigma_{k=0}^{\beta} a_{jk}^{p(-\varepsilon)}U^k$ $(\in C_a[U])$. Then we see that

$$0 = f(x^{p(e)}) = \Sigma_{j=0}^{\alpha} B_j^{p(\varepsilon)}x^{p(e)j} = (\Sigma_{j=0}^{\alpha} B_j^{p(\varepsilon-e)}x^j)^{p(e)},$$

so that $g(x) = 0$ on setting $g(X) = \Sigma_{j=0}^{\alpha} B_j^{p(\varepsilon-e)}X^j$. Since $f(X) \notin C[U][X^p]$, we see that $g(X) \notin C_a[U][X^p]$, and that x is separably algebraic over $K_s(C_a)$.

Example 2 Let U and V be two indeterminates over a field K_0. Let $\delta = \partial_U$ and $\delta' = \partial_V$ be formal partial differentiations of $K_0(U,V)$ relative to U and V respectively (see Examp.2 of §1.6), and $K_0(U,V)_\delta$ and $K_0(U,V)_{\delta'}$ the δ-closure and the δ'-closure of $K_0(U,V)$ in $K_0(U,V)_a$ respectively. Then, by Cor. to Th.4, fields of δ-constants of $K_0(U,V)$, $K_0(U,V)_s$ and $K_0(U,V)_\delta$ are $K_0(V)$, $K_0(V)_s$ and $K_0(V)_a$ in $K_0(U,V)_a$ respectively. Similarly, fields of δ'-constants of $K_0(U,V)$, $K_0(U,V)_s$ and $K_0(U,V)_{\delta'}$ are $K_0(U)$, $K_0(U)_s$ and $K_0(U)_a$ respectively. Moreover, we see by Examp. 1 that $K_0(U,V)_\delta = K_0(U,V)_s(K_0(V)_a)$ and $K_0(U,V)_{\delta'} = K_0(U,V)_s(K_0(U)_a)$.

CHAPTER 2

Differential Rings and Differential Fields

2.1. Definitions

A differential ring is a ring R associated with a non-empty set $\Delta = \{\delta_i \mid i \in I\}$ of mutually commutative derivations $\delta_i = (\delta_{i\nu} \mid \nu \in \mathbb{N})$ $(i \in I)$ of R, where the set Δ (correspondingly, the set of indices I) may be finite or infinite. If $i(1)$ and $i(2)$ are distinct elements of I, $\delta_{i(1)}$ and $\delta_{i(2)}$ are regarded as distinct elements of Δ although they may be equal as operators on R. This Δ is called set of derivation operators of the differential ring R. If the set Δ consists of trivial derivations, the notion of differential ring reduces to that of ring. The differential ring R is said to be ordinary or partial according as Δ consists of a single derivation or not. If the ring R is a field, we speak of a differential field.

Remark 1 In literatures on differential algebra, the set of derivation operators is usually finite. We take into consideration also the case of infinite set of derivation operators. The efficacy of this generalization can be seen for example in §2.9.

For every $(\nu) = (\nu(i) \mid i \in I) \in \mathbb{N}^{(I)}$ (see §1.1), the product $\delta_{(\nu)} = \Pi_{i\in I}\delta_{i,\nu(i)}$ is an well-defined endomorphism of the additive group R^+ of the ring R, and called derivative operator of the differential ring R. The well-defined

number $\Sigma_{i\in I}\nu(i)$ is called <u>order</u> of $\delta_{(\nu)}$ and denoted by ord $\delta_{(\nu)}$. If $x \in R$, we say that $\delta_{(\nu)}$ is a <u>derivative</u> of <u>order</u> $\Sigma_{i\in I}\nu(i)$ of x. We denote by Θ the set of all derivative operators $\delta_{(\nu)}$ ($(\nu) \in \mathbb{N}^{(I)}$), and Θ is called <u>set of derivative operators</u> of the differential ring R. If $\theta,\theta' \in \Theta$, the product $\theta\theta'$ is a multiple of an element θ'' of Θ by a natural number denoted by $n(\theta,\theta')$. When $\theta = \delta_{(\lambda)}$, $\theta' = \delta_{(\mu)}$, we see by (D4) of §1.2 that $\theta'' = \delta_{(\lambda)+(\mu)}$, and that $n(\theta,\theta') = \Pi_{i\in I}\binom{\lambda(i)+\mu(i)}{\lambda(i)}$ often denoted by $\binom{(\lambda)+(\mu)}{(\lambda)}$.

For differential rings or fields, notions such as <u>differential subring</u>, <u>differential subfield</u>, <u>differential extension ring</u>, <u>differential extension field</u>, <u>differential ideal</u>, <u>differential homomorphism</u>, <u>differential isomorphism</u> and so on are in any case those that are admissible under the domain of derivative operators Θ. For example, let R, Δ and Θ be as above, and R_1 a subring of the ring R such that $\Theta R_1 = \{\delta_{(\nu)}x_1 \mid x_1 \in R_1, \delta_{(\nu)} \in \Theta\} \subset R_1$, or equivalently, that $\delta_{i\nu}x_1 \in R_1$ ($x_1 \in R_1$, $i \in I$, $\nu \in \mathbb{N}$). Then, each δ_i ($i \in I$) determines its restriction derivation to R_1 denoted also by the same letter δ_i. Thus R_1 can be regarded as a differential ring associated with the same set of derivations Δ. This differential ring R_1 is called differential subring of R, and R is called differential extension ring of R_1. For another example, let R' be a differential ring associated with the set of derivation operators $\Delta' = \{\delta'_i \mid i \in I\}$ which has the same set of indices I as that of Δ. Then R' has

the set of derivative operators $\Theta' = \{\delta'_{(\nu)} \mid (\nu) \in \mathbb{N}^{(I)}\}$. If a ring-homomorphism f of R into R' satisfies the condition that $f(\delta_{(\nu)}x) = \delta'_{(\nu)}f(x)$ $(x \in R, (\nu) \in \mathbb{N}^{(I)})$, or equivalently, that $f(\delta_{i\nu}x) = \delta'_{i\nu}f(x)$ $(x \in R, i \in I, \nu \in \mathbb{N})$, then f is called differential homomorphism of R into R'. If, moreover, the homomorphism f is injective, f is called differential isomorphism of R <u>into</u> R'. In particular, if it is bijective, then f is called differential isomorphism of R <u>onto</u> R', and R is said to be <u>differentially isomorphic</u> to R'.

<u>Remark 2</u> The differential subring R_1 above is associated with the <u>set</u> $\Delta = \{\delta_i \mid i \in I\}$ of derivative operators. But, since δ_i $(i \in I)$ are the restrictions of the original derivations of R, it may happen that $\delta_{i(1)}$ coinsides with $\delta_{i(2)}$ for some pair $(i(1),i(2)) \in I^2$ with $i(1) \neq i(2)$ even if the original derivations of R are distinct.

An element c of the differential ring R is called <u>constant</u> if $\delta_{(\nu)}c = 0$ $(\delta_{(\nu)} \in \Theta$ with ord $\delta_{(\nu)} > 0)$, or equivalently, $\delta_{i\nu}c = 0$ $(i \in I, \nu \in \mathbb{N}-\{0\})$. By 6° of §1.2, every element of the prime field of R is constant.

<u>Proposition 1</u> If R is a differential ring (respectively field), the set of all constants of R is a differential subring (respectively subfield) of R.

This follows from 7° of §1.2.

The set of constants stated in Prop.1 is called <u>ring</u>

(respectively field) of constants of the differential ring (respectively field) R, and denoted by R_c.

Example 1 Let R be any ring. If we associate to it the trivial derivation of R, it is regarded as a differential ring consisting only of constants. This differential ring is essentially the original ring R to which no derivation is associated.

Example 2 Let U be an indeterminate over a ring R_0, $R_U = R_0[[U]]$ the ring of formal power series in U over R_0 and $R = R_0[U]$ the ring of polynomials in U over R_0. If we associate to R_U and R the formal differentiation d relative to U (see Examp.3 of §1.3), R_U and R are regarded as ordinary differential rings, the latter being a differential subring of the former. The ring of constants of either one of R_U and R is R_0.

Example 3 Let $\{U_i \mid i \in I\}$ (card $I > 1$) be a set of indeterminates over a ring R_0, and $R = R_0[U_i \mid i \in I]$ the ring of polynomials in U_i ($i \in I$) over R_0. For every $j \in I$, let ∂_j be the formal differentiation of R relative to U_j (see Examp.4 of §1.3). If we associate to R the set of derivations $\Delta = \{\partial_j \mid j \in I\}$, R is regarded as a partial differential ring. The ring of constants of R is R_0.

Let S be a differential ring (respectively field), and $\{S_j \mid j \in J\}$ a set of differential subrings (respectively subfields) of S. Then the intersection $\cap_{j \in J} S_j$ is a differen-

tial subring (respectively subfield) of S. Let $\Delta = \{\delta_i \mid i \in I\}$ be the set of derivation operators of S, and $\Theta = \{\delta_{(\nu)} \mid (\nu) \in \mathbb{N}^{(I)}\}$ the set of derivative operators of S. If a differential subring (respectively subfield) R of S and a subset Ξ of S are given, and if we set $\Theta\Xi = \{\delta_{(\nu)}\xi \mid \delta_{(\nu)} \in \Theta, \xi \in \Xi\}$, then we see that the ring $R[\Theta\Xi]$ (respectively the field $R(\Theta\Xi)$) generated by $\Theta\Xi$ over R is the smallest differential subring (respectively subfield) of S containing R and Ξ. This is denoted by $R\{\Xi\}$ (respectively by $R\langle\Xi\rangle$), and called differential ring (respectively field) generated by Ξ over the differential ring (respectively field) R. If $S = R\{\Xi\}$ (respectively $S = R\langle\Xi\rangle$) for some finite subset Ξ of S, then S is called finitely generated differential ring (respectively field) over the differential ring (respectively field) R. Let L and M be two differential subfields of a differential field K. Then the smallest differential subfield of K containing both L and M is $L\langle M\rangle = L(M) = M(L) = M\langle L\rangle$. Hence it is denoted by LM and called compositum of the differential fields L and M.

2.2. Differential ring of quotients

Let R be a differential ring associated with the set $\Delta = \{\delta_i \mid i \in I\}$. Let M be a multiplicatively stable subset of R and $M^{-1}R$ the ring of quotients of R over M (see §1.6). By Th.1 of §1.6, every $\delta_i \in \Delta$ has a unique extension derivation to $M^{-1}R$ which is also denoted by δ_i as we remarked

after the proof of that theorem. Extension derivations δ_i ($i \in I$) commute mutually (see Cor.1 to Th.1 of §1.6). The differential ring $M^{-1}R$ associated with the set of these extension derivations $\Delta = \{\delta_i \mid i \in I\}$ is called <u>differential ring of quotients</u> of R over M. It contains R as a differential subring. In particular, if the ring R is an integral domain, we speak of the <u>differential field of quotients</u> $Q(R)$ of R.

<u>Example 1</u> The ring of polynomials $K[U]$ in an indeterminate U over a field K is regarded as an ordinary differential field associated with the formal differentiation d relative to U (see Examp.3 of §1.3). The field of quotients $K(U)$ of $K[U]$ associated with the formal differentiation d relative to U is the differential field of quotients of the differential integral domain $K[U]$. The field of constants of the differential field $K(U)$ is K (see Exam.1 of §1.6).

<u>Example 2</u> The ring of polynoials $K[U_i \mid i \in I]$ in a set of indeterminates U_i ($i \in I$) (card $I > 1$) over a field K is regarded as a partial differential field associated with the set of formal partial differentiations ∂_i relative to U_i ($i \in I$) is regarded as a partial differential ring (see Examp.4 of §1.3). The field of quotients $K(U_i \mid i \in I)$ of $K[U_i \mid i \in I]$ is the differential field of quotients of the differential integral domain $K[U_i \mid i \in I]$. We see easily that the field of constants of the differential field $K(U_i \mid$

$i \in I$) is K (see Examp.2 of §1.6).

2.3. Differential polynomials

Let R be a differential ring with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$, $\delta_i = (\delta_{i\nu} \mid \nu \in \mathbb{N})$ $(i \in I)$, and the set of derivative operators $\Theta = \{\delta_{(\nu)} \mid (\nu) \in \mathbb{N}^{(I)}\}$. Let $\{X_j \mid j \in J\}$ be a nonempty subset of a differential extension ring of R. If there exists no nontrivial polynomial relation over R in the derivatives θX_j $(\theta \in \Theta, j \in J)$ of X_j $(j \in J)$, then X_j $(j \in J)$ are called <u>differential indeterminates</u> over R.

<u>Theorem 1</u> Let R, Δ and Θ be as above. Then, for any nonempty set of indices J, there exists uniquely (up to differential isomorphism over R) a set of differential indeterminates $\{X_j \mid j \in J\}$ over R.

Proof. Let $X_{j,(\rho)}$ $(j \in J, (\rho) \in \mathbb{N}^{(I)})$ be indeterminates over the ring R, and $S = R[X_{j,(\rho)} \mid j \in J, (\rho) \in \mathbb{N}^{(I)}]$ the ring of polynomials in $X_{j,(\rho)}$ $(j \in J, (\rho) \in \mathbb{N}^{(I)})$ over R. We extend each $\delta_{i\nu}$ $(i \in I, \nu \in \mathbb{N})$ to a mapping of S into S as follows. The extension mapping of $\delta_{i\nu}$ to S is denoted also by the same letter $\delta_{i\nu}$:

(i) $\delta_{i\nu} X_{j,(\rho)} = \binom{\nu+\rho(i)}{\nu} X_{j,(\rho')}$,

where $\rho'(k) = \begin{cases} \nu + \rho(i) & (k \in I, k = i) \\ \rho(k) & (k \in I, k \neq i) \end{cases}$ $(j \in J, (\rho) \in \mathbb{N}^{(I)})$.

(ii) Let M be a monomial with coefficient 1 of $X_{j,(\rho)}$

$(j \in J,\ (\rho) \in \mathbb{N}^{(I)})$. If $M = 1$, set $\delta_{i\nu}M = \begin{cases} 1 & (\nu = 0) \\ 0 & (\nu > 0) \end{cases}$. If $M \neq 1$ and $M = Y_1 \cdots Y_r$ ($Y_1, \ldots, Y_r$ being finitely many of $X_{j,(\rho)}$ $(j \in J,\ (\rho) \in \mathbb{N}^{(I)})$), set

$$\delta_{i\nu}M = \Sigma_{\nu(1)+\ldots+\nu(r)=\nu} \delta_{i,\nu(1)}Y_1 \cdots \delta_{i,\nu(r)}Y_r.$$

(iii) For each element $P = \Sigma_M a_M M$ $(a_M \in R)$ where the summation Σ runs through all monomials with coefficient 1 of $X_{j,(\rho)}$ $(j \in J,\ (\rho) \in \mathbb{N}^{(I)})$, set

$$\delta_{i\nu}P = \Sigma_M \Sigma_{\nu(1)+\nu(2)=\nu} \delta_{i,\nu(1)}a_M \delta_{i,\nu(2)}M.$$

This $\delta_{i\nu}P$ is well defined, because the coefficients a_M of P are all zeros except for a finite number.

It is straightforward to show that (i)~(iii) define mutually commutative extension derivations $\delta_i = (\delta_{i\nu} \mid \nu \in \mathbb{N})$ $(i \in I)$ to S of the original derivations δ_i $(i \in I)$ of R, so that S is a differential extension ring of R.

Now, denote $X_{j,(0)}$ by X_j for every $j \in J$, where (0) means the element $(\rho) \in \mathbb{N}^{(I)}$ with $\rho_i = 0$ for all $i \in I$. Then we see that $X_{j,(\rho)} = \delta_{(\rho)}X_j$ $(j \in J,\ (\rho) \in \mathbb{N}^{(I)})$, that $S = R\{X_j \mid j \in J\}$, and that X_j $(j \in J)$ are differential indeterminates over R. The uniqueness assertion of our theorem is obvious. q.e.d.

Elements of S in this proof are called <u>differential polynomials</u> in the differential indeterminates X_j $(j \in J)$ over R, and S is called <u>differential ring of differential</u>

polynomials in X_j $(j \in J)$ over R. If we speak of a differential polynomial ring $R\{X_j \mid j \in J\}$ over a differential ring R, we mean tacitly that the X_j $(j \in J)$ are differential indeterminates over R.

In particular, if R is a differential field, we can consider the differential field of quotients $R\langle X_j \mid j \in J\rangle$ of the differential polynomial ring $R\{X_j \mid j \in J\}$.

Proposition 2 Let R be a differential ring with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$, and $\{X_j \mid j \in J\}$ a set of differential indeterminates over R. Then the ring of constants of the differential polynomial ring $S = R\{X_j \mid j \in J\}$ over R coincides with that of R.

Proof. What we must prove is that each $A \in S-R$ is non-constant. Let an element $A \in S-R$ be given. Then A contains effectively only a finite number of $\delta_{(\nu)}X_j$ $(j \in J, (\nu) \in \mathbb{N}^{(I)})$. Hence we can suppose that I and J are both finite, and consequently, it suffices to prove our proposition in the case that each one of I and J consists of a single element.

Starting afresh, let R be a differential ring associated with a derivation $\delta = (\delta_\nu \mid \nu \in \mathbb{N})$, and S the differential ring of differential polynomials in a single differential indeterminate X over R. Let A be an element of S - R.

Case I: Some derivative of X is contained effectively in A with an exponent not divisible by p. Among such deri-

vatives, let $\delta_\nu X$ be the one of largest order. Write A in the form $A = \Sigma_{h=0}^{\alpha} A_h (\delta_\nu X)^h$, where A_h $(0 \le h \le \alpha)$ are polynomials in $(\delta_\rho X)^p$ $(\rho \ge \nu)$ and $\delta_\sigma X$ $(\sigma < \nu)$ over R, and where $0 < \alpha < p$ with $A_\alpha \neq 0$. Each term of A_h is of the form

$$a(\delta_{\rho(1)}X)^{\beta(1)p(e(1))} \cdots (\delta_{\rho(r)}X)^{\beta(r)p(e(r))} \times (\delta_{\sigma(1)}X)^{f(1)} \cdots (\delta_{\sigma(s)}X)^{f(s)},$$

where $a \in R$ with $a \neq 0$, $r \in \mathbb{N}$, $s \in \mathbb{N}$, $\rho(i) \ge \nu$ $(1 \le i \le r)$, $\sigma(j) < \nu$ $(1 \le j \le s)$, $\beta(i)$ $(1 \le i \le r)$ are positive integers not divisible by p, $e(i) \in \mathbb{N}-\{0\}$ $(1 \le i \le r)$, $f(j) \in \mathbb{N}-\{0\}$ and $\rho(1), \ldots, \rho(r), \sigma(1), \ldots, \sigma(s)$ are distinct. Hence $\delta_\mu(A_h(\delta_\nu X)^h)$ is a sum of expressions of the form

$$\Sigma\left(\begin{array}{l}\delta_{\lambda(0)}a \cdot \delta_{\lambda(1)}\{(\delta_{\rho(1)}X)^{\beta(1)p(e(1))}\}\cdots \\ \quad \times \delta_{\tau(1)}\{(\delta_{\sigma(1)}X)^{f(1)}\}\cdots\delta_{\omega(1)}(\delta_\nu X)\cdots\delta_{\omega(h)}(\delta_\nu X)\end{array}\right),$$

where the summation Σ runs through all those $(\lambda(0),\ldots,\tau(1),\omega(1),\ldots) \in \mathbb{N}^{r+s+h+1}$ that satisfy $\lambda(0) + \ldots + \tau(1) + \ldots + \omega(1) + \ldots = \mu$. Applying (5) of §1.4 and observing derivatives of X of order $\ge \mu+\nu$, we see that

$$\delta_\mu(A_h(\delta_\nu X)^h) = h\binom{\mu+\nu}{\nu}(\delta_\nu X)^{h-1}\delta_{\mu+\nu}X \cdot A_h + [\ \ldots\ ],$$

where $[\ \ldots\ ]$ is a polynomial in $(\delta_\tau X)^p$ $(\tau \ge \mu+\nu)$ and $\delta_\omega X$ $(\omega < \mu+\nu)$ over R. Therefore, we see that

(1) $\quad \delta_\mu A = (\partial A/\partial(\delta_\nu X)) \cdot \binom{\mu+\nu}{\nu}\delta_{\mu+\nu}X + [\ \ldots\ ]$

($[\ \ldots\ ]$ being a similar polynomial as above), so that $\delta_\mu A \neq 0$ for a choice of $\mu \in \mathbb{N}-\{0\}$ satisfying $\binom{\mu+\nu}{\nu} \not\equiv 0 \pmod{p}$

(see Lem.1 of §1.2).

Case II: Every derivative of X contained effectively in A has exponent divisible by p. Let $\delta_{\nu(1)}X, \ldots, \delta_{\nu(r)}X$ be all the distinct derivatives of X which are effectively contained in A. Then A can be written as a polynomial in

$$(\delta_{\nu(1)}X)^{p(e(\nu(1)))}, \ldots, (\delta_{\nu(r)}X)^{p(e(\nu(r)))}$$

over R, taking each one of these $e(\nu(1)), \ldots, e(\nu(r)) \in \mathbb{N}-\{0\}$ as large as possible. Set $e = \max(e(\nu(1)),\ldots,e(\nu(r)))$, $\mu = p(f)$, $\lambda = \mu p(e)$ and $\mu(h) = \lambda/p(e(\nu(h)))$ $(1 \le h \le r)$, where $f \in \mathbb{N}-\{0\}$ is chosen large enough such that $\binom{\mu(h)+\nu(h)}{\nu(h)} \not\equiv 0 \pmod{p}$ $(1 \le h \le r)$. Now, for each term

$$M = a(\delta_{\nu(1)}X)^{\alpha(1)p(e(\nu(1)))}\ldots(\delta_{\nu(r)}X)^{\alpha(r)p(e(\nu(r)))}$$

$$(a \in R,\ a \neq 0,\ \alpha(h) \in \mathbb{N})$$

of A, observe the derivative of X of the largest order which is contained effectively in $\delta_\lambda M$. Applying (5) of §1.4, we get

$$\begin{aligned}
\delta_\lambda M &= a\alpha(1)\left(\begin{array}{l}\{\binom{\mu(1)+\nu(1)}{\nu(1)}(\delta_{\nu(1)}X)^{\alpha(1)-1}\delta_{\mu(1)+\nu(1)}X\}^{p(e(\nu(1)))} \\ \times(\delta_{\nu(2)}X)^{\alpha(2)p(e(\nu(2)))}\ldots(\delta_{\nu(r)}X)^{\alpha(r)p(e(\nu(r)))}\end{array}\right) \\
&\quad + \ldots \\
&\quad + a\alpha(r)\left(\begin{array}{l}\{\binom{\mu(r)+\nu(r)}{\nu(r)}(\delta_{\nu(r)}X)^{\alpha(r)-1}\delta_{\mu(r)+\nu(r)}X\}^{p(e(\nu(r)))} \\ \times(\delta_{\nu(r)}X)^{\alpha(1)p(e(\nu(1)))}\ldots(\delta_{\nu(s)}X)^{\alpha(s)p(e(\nu(s)))}\end{array}\right) \\
&\quad + [\ \ldots\ ],
\end{aligned}$$

where $s = r - 1$ and $[\ \ldots\ ]$ contains no derivative of X of order $\geq \omega = \max(\mu(1)+\nu(1), \ldots, \mu(r)+\nu(r))$. Hence we see that

$$(2)\quad \delta_\lambda A = \Sigma_{h=1}^{r}\Big(\big(\partial A/\partial((\delta_{\nu(h)}X)^{p(e(\nu(h)))})\big) \times\{\binom{\mu(h)+\nu(h)}{\nu(h)}\delta_{\mu(h)+\nu(h)}X\}^{p(e(\nu(h)))}\Big) + [\ \ldots\ ],$$

where $[\ \ldots\ ]$ is a similar polynomial as above. If only one of $\mu(h)+\nu(h)$ $(1 \leq h \leq r)$ is equal to ω, then $\delta_\lambda A \neq 0$. On the contrary, if at least two of $\mu(h)+\nu(h)$ $(1 \leq h \leq r)$ are equal to ω, then we see also $\delta_\lambda A \neq 0$. Because, if we assumed $\delta_\lambda A = 0$, there would exist h, k with $1 \leq h < k \leq r$, $\mu(h)+\nu(h) = \mu(k)+\nu(k) = \omega$, $e(\nu(h)) = e(\nu(k))$, and this would imply that $\mu(h) = \mu(k)$ and $\nu(h) = \nu(k)$ (a contradiction).

Proposition 3 Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$. Let $\{X_j \mid j \in J\}$ be a set of differential indeterminates over K and $L = K\langle X_j \mid j \in J\rangle$ the differential field of quotients of the differential polynomial ring $K\{X_j \mid j \in J\}$. Then the field of constants of L coincides with that of K.

Proof. We must prove that each $T \in L-K$ is nonconstant. By similar consideration as that of the beginning of the proof of Prop.2, we see that it is sufficient to prove the proposition in the case that K is a differential field associated with a single derivation $\delta = (\delta_\nu \mid \nu \in \mathbb{N})$ and L is the dif-

ferential field generated by a single differential indeterminate X over R.

Let A/B $(A,B \in K\{X\}, B \neq 0)$ be an element of L-K. Suppose, as we may, that A and B are relatively prime as polynomials in $\delta_\nu X$ $(\nu \in \mathbb{N})$ over K. Now, assume that A/B is a constant. Then we get

(3) $\delta_\mu A \cdot B - A \cdot \delta_\mu B = 0$ $(\mu \in \mathbb{N})$.

Case I: Some derivative of X is contained effectively in either A or B with an exponent not divisible by p. Among such derivatives of X, let $\delta_\nu X$ be of largest order. Write A and B in the form $A = \Sigma_{h=0}^{\alpha} A_h (\delta_\nu X)^h$ and $B = \Sigma_{k=0}^{\beta} B_k (\delta_\nu X)^k$, where A_h, B_k are polynomials in $(\delta_\rho X)^p$ $(\rho \geq \nu)$ and $\delta_\sigma X$ $(\sigma < \nu)$ over K, and where $\alpha < p$, $\beta < p$, at least one of α, β is positive and $A_\alpha \neq 0$, $B_\beta \neq 0$. Choose $\mu \in \mathbb{N}-\{0\}$ such that $\binom{\mu+\nu}{\nu} \not\equiv 0 \pmod{p}$. Following the calculation by which we derived (1) in the proof of Prop.2, we get

(4) $\delta_\mu A \cdot B - A \cdot \delta_\mu B$

$= \{(\partial A/\partial(\delta_\nu X))B - A(\partial B/\partial(\delta_\nu X))\}\binom{\mu+\nu}{\nu}\delta_{\mu+\nu}X + [\ \ldots\ ]$,

where $[\ \ldots\ ]$ is a polynomial in $(\delta_\tau X)^p$ $(\tau \geq \mu+\nu)$ and $\delta_\omega X$ $(\omega < \mu+\nu)$ over K. Since A and B are relatively prime polynomials, $\{\quad\}$ of (4) can not vanish, contradicting (3).

Case II: Every derivative of X contained effectively

in either A or B has exponent divisible by p. Concerning to A and B, determine $\delta_{\nu(1)}X$, ... ,$\delta_{\nu(r)}X$, $e(\nu(1))$, ... , $e(\nu(r))$, μ, λ, $\mu(1)$, ..., $\mu(r)$ in a similar manner as we did in Case II of the proof of Prop.2. Then, calculating as we did to derive (2) in that proof, we get

$$\delta_\lambda A\cdot B - A\cdot\delta_\lambda B$$

$$= \Sigma_{h=1}^{r} \left(\begin{pmatrix} (\partial A/\partial((\delta_{\nu(h)}X)^{p(e(\nu(h)))}))B \\ - A(\partial B/\partial((\delta_{\nu(h)}X)^{p(e(\nu(h)))})) \end{pmatrix} \times \binom{\mu(h)+\nu(h)}{\mu(h)} (\delta_{\mu(h)+\nu(h)}X)^{p(e(\nu(h)))} \right)$$

$$+ [\ \ldots\ ],$$

where [...] does not contain any derivative of X of order $\geq \omega = \max(\mu(1)+\nu(1), \ldots, \mu(r)+\nu(r))$. Thus we see similarly to the end of Case II of the proof of Prop.2 that the equation above contradicts (3).

2.4. Differential ideals

Let R be a differential ring with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators $\Theta = \{\delta_{(\nu)} \mid (\nu) \in \mathbb{N}^{(I)}\}$. A differential ideal of R is an ideal of the ring R which is stable under the operation of Θ, or equivalently, which is stable under every $\delta_{i\nu}$ ($i \in I$, $\nu \in \mathbb{N}$). The following properties are clear:

(i) If $\mathfrak{a}_1$, ... , $\mathfrak{a}_n$ are finitely many differential ideals of R, the sum ideal $\Sigma_{h=1}^{n}\mathfrak{a}_h$ and the product ideal $\Pi_{h=1}^{n}\mathfrak{a}_h$ are differential ideals of R.

(ii) If $\{\mathfrak{a}_j \mid j \in J\}$ is a set of differential ideals of R, the intersection $\cap_{j\in J}\mathfrak{a}_j$ is a differential ideal of R.

Let a subset Ξ of R be given. The ideal $(\Theta\Xi)$ generated by $\Theta\Xi$ in R is the smallest differential ideal of R containing Ξ, and denoted by $[\Xi]_R$ or simply by $[\Xi]$. This ideal is called differential ideal <u>generated</u> in R by Ξ.

If a differential ideal of R is prime (respectively primary, respectively perfect) as an ideal of the ring R, it is called <u>prime</u> (respectively <u>primary</u>, respectively <u>perfect</u>) <u>differential ideal</u> of R; that is, for example, a differential ideal $\mathfrak{m}$ of R is a perfect differential ideal if and only if, for an element x of R, $x^n \in \mathfrak{m}$ (for some $n \in \mathbb{N}$) implies always $x \in \mathfrak{m}$.

If $\mathfrak{a}$ is an ideal of R, we denote by $\sqrt{\mathfrak{a}}$ the radical ideal in R of $\mathfrak{a}$ (see Vol.I of [13]).

<u>Theorem 2</u> If $\mathfrak{a}$ is a differential ideal of a differential ring R, then its radical ideal $\sqrt{\mathfrak{a}}$ is a perfect differential ideal of R.

Proof. Let $\Delta = \{\delta_i \mid i \in I\}$ be the set of derivation operators of R. Since $\sqrt{\mathfrak{a}}$ is known to be a perfect ideal of R, it suffices to show that $\delta_{i\nu}x \in \sqrt{\mathfrak{a}}$ $(x \in \sqrt{\mathfrak{a}},\ i \in I,\ \nu \in \mathbb{N})$. For each $x \in \sqrt{\mathfrak{a}}$, there exists $e \in \mathbb{N}$ such that $x^{p(e)} \in \mathfrak{a}$. We see by (4) of §1.4 that $(\delta_{i\nu}x)^{p(e)} = \delta_{i,\nu p(e)}(x^{p(e)}) \in \mathfrak{a}$, so that $\delta_{i\nu}x \in \sqrt{\mathfrak{a}}$ $(i \in I,\ \nu \in \mathbb{N})$.

Theorem 3 If $\mathfrak{m}$ is a perfect differential ideal of a differential ring R, and if M is a nonempty subset of R, then the quotient ideal $\mathfrak{m}:M$ is a perfect differential ideal of R.

Proof. Let Δ be as in the proof of Th.2. Since it is known that $\mathfrak{m}:M$ is a perfect ideal of R, we have only to prove by induction on ν that, for each $x \in \mathfrak{m}:M$ and for each $z \in M$,

(1) $\delta_{i\nu}x\cdot z \in \mathfrak{m}$ $(i \in I, \nu \in \mathbb{N})$.

If $\nu = 0$, (1) is trivially true. Suppose $\nu > 0$, then we get

$$\delta_{i\nu}x\cdot z^2 + \Sigma_{\alpha=0}^{\nu-1}\delta_{i\alpha}x\cdot z\cdot\delta_{i,\nu-\alpha}z = \delta_{i\nu}(xz)\cdot z \in \mathfrak{m}$$

$$(i \in I, \nu \in \mathbb{N}).$$

Hence, by induction assumption, we see that $\delta_{i\nu}x\cdot z^2 \in \mathfrak{m}$ and $(\delta_{i\nu}x\cdot z)^2 \in \mathfrak{m}$, so that (1) holds. q.e.d.

In the hypothesis of Th.3, the condition that the differential ideal $\mathfrak{m}$ is perfect can not be dropped as we see in the following example.

Example Let K be a field of characteristic 2, and regard it as a differential field associated with the trivial derivation δ of K. Let $R = K\{X\}$ be the differential polynomial ring in a single differential indeterminate X over K. Consider the differential ideal $\mathfrak{a} = [X^2]$ of R. We see by (2) and (4) of §1.4 that $\mathfrak{a}$ is the ideal gene-

rated by $(\delta_\nu X)^2$ $(\nu \in \mathbb{N})$. Take the set $M = \{X\}$, then X is contained in $\mathfrak{q}:M$, but $\delta_1 X$ is not. Thus $\mathfrak{q}:M$ is not a differential ideal of R.

Starting afresh, let R be a differential ring with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$, and $\mathfrak{q}$ a differential ideal of R with $\mathfrak{q} \neq R$. Denote by $R/\mathfrak{q}$ the residue ring of the ring R modulo the ideal $\mathfrak{q}$, and by ϕ the canonical ring-homomorphism of R onto $R/\mathfrak{q}$. If K_0 denotes a subfield of R, $\phi(K_0)$ is a subfield of $R/\mathfrak{q}$ canonically identified with K_0. Thus $R/\mathfrak{q}$ is a ring in the sense of §1.1. For each $i \in I$ and for each $\nu \in \mathbb{N}$, define a mapping $\delta'_{i\nu}$ of $R/\mathfrak{q}$ into $R/\mathfrak{q}$ by the formula

(2) $\quad \delta'_{i\nu}\phi(x) = \phi(\delta_{i\nu}x) \quad (x \in R)$.

We see easily that these mappings $\delta'_{i\nu}$ $(i \in I, \nu \in \mathbb{N})$ are well defined by (2). Set $\delta'_i = (\delta'_{i\nu} \mid \nu \in \mathbb{N})$ $(i \in I)$, then it is straightforward to show that δ'_i $(i \in I)$ are mutually commutative derivations of $R/\mathfrak{q}$. Since these derivations δ'_i $(i \in I)$ are canonically defined by means of δ_i $(i \in I)$, we denote them henceforth also by the same letters δ_i $(i \in I)$. The differential ring $R/\mathfrak{q}$ associated with the set of these derivations $\Delta = \{\delta_i \mid i \in I\}$ is called <u>differential residue ring</u> of R modulo $\mathfrak{q}$. It turns out that the mapping ϕ is a differential homomorphism of R onto $R/\mathfrak{q}$ called <u>canonical differential homomorphism</u> of R onto $R/\mathfrak{q}$. If $\mathfrak{b}$ is a differential ideal of R containing $\mathfrak{q}$, we see that $\phi(\mathfrak{b})$ is a differen-

tial ideal of $R/\mathfrak{q}$; this is denoted by $\mathfrak{b}/\mathfrak{q}$.

2.5. Differential homomorphisms and differential isomorphisms

Let f be a differential homomorphism of a differential ring R into a differential ring S. We may denote the sets of derivation operators of R and S by one and the same notation $\Delta = \{\delta_i \mid i \in I\}$. Set $R' = f(R)$ and $\mathfrak{q} = \ker f$. Since the homomorphism is unitary (see §1.1), we see that the image of the prime field of R is the prime field of S, that R' is a differential subring of S, and that $\mathfrak{q}$ is a differential ideal of R with $\mathfrak{q} \neq R$. We see also that the image of every differential ideal of R is a differential ideal of R'. We can prove various properties concerning differential homomorphisms and differential isomorphisms. We mention here only two of such properties.

Theorem 4 Let R, S, f, R' and $\mathfrak{q}$ be as above. Let ϕ be the canonical differential homomorphism of R onto the differential residue ring $R/\mathfrak{q}$. We can define the mapping $\overline{f}$: $\phi(x) \mapsto f(x)$ $(x \in R)$ of $R/\mathfrak{q}$ onto R', and this mapping $\overline{f}$ is a differential isomorphism of $R/\mathfrak{q}$ onto R' with $f = \overline{f} \circ \phi$.

The proof is straightforward.

Theorem 5 Let $\mathfrak{b}$ and $\mathfrak{c}$ be two differential ideals of a differential ring R with $\mathfrak{b} \subset \mathfrak{c} \neq R$. Then $\mathfrak{c}/\mathfrak{b}$ is a differential ideal of the differential residue ring $R/\mathfrak{b}$ with

$c/b \neq R/b$ (see the end of §2.4), and the differential residue ring $(R/b)/(c/b)$ is canonically differentially isomorphic to differential residue ring R/c.

The proof is straightforward.

2.6. Contractions and extensions of differential ideals

Let R and S be two differential rings associated with the same set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$. Let a differential homomorphism f of R into S be given. By virtue of the theory of usual rings, we know concepts of contraction and extension of ideals relative to f. That is to say, the contraction of an ideal A of S relative to f is the ideal $A^c = f^{-1}(A)$ of R, and the extension of an ideal $\mathfrak{a}$ of R relative to f is the ideal $\mathfrak{a}^e = (f(\mathfrak{a}))_S$ of S; $\mathfrak{a}^e$ equals the ideal product $Sf(\mathfrak{a})$. Their fundamental properties are well known (see Vol.I of [13]). Hence proofs of the following two theorems require only to show that ideals in quetion are stable under the set of derivative operators Θ, and are straightforward.

Theorem 6 Let R, S, Δ and f be as above.

(a) If A is a differential ideal of S, then A^c is a differential ideal of R.

(b) If $\mathfrak{a}$ is a differential ideal of R, then $\mathfrak{a}^e$ is a differential ideal of S.

Theorem 7 Let R, S, Δ and f be as above.

(a) Let P be a prime differential ideal of S, Q a

primary differential ideal of S, and M a perfect differential ideal of S. Then P^c is a prime differential ideal of R, Q^c a primary differential ideal of R, and M^c a perfect differential ideal of R.

(b) If, in particular, $P = \sqrt{Q}$, then $P^c = \sqrt{Q^c}$.

(c) If M is the radical ideal of a differential ideal A of S, then $M^c = \sqrt{A^c}$.

Remark For extensions of prime, primary and perfect differential ideals of R relative to f, results similar to Th.7 are not obtained in general.

Theorem 8 Let R, S, Δ and f be as above. If M is a perfect differential ideal of S, and if N is a subset of S with $f^{-1}(N) \neq \emptyset$, then

(1) $(M:N)^c \subset M^c : f^{-1}(N)$.

If, moreover, $N \subset f(R)$, the inclusion (1) is replaced by the equality.

By Th.7 and by Th.3 of §2.4, both sides of (1) are perfect differential ideals of R. The proof of Th.8 is straightforward.

In general, (1) is a proper inclusion as we see in the following example.

Example Let K be a differential field associated with a single derivation δ, and X, Y differential indeterminates over K. Set $R = K\{X\}$, $S = K\{X,Y\}$, $M = [X]_S$ and $N = \{0,Y\}$.

If f is the canonical embedding of R into S, then $M{:}N = M$, $(M{:}N)^c = [X]_R$, $f^{-1}(N) = \{0\}$ and $M^c{:}f^{-1}(N) = R$.

Now, return to differential rings R, S with the same set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the differential homomorphism f as in the beginning of this section. Relative to f, let (C) be the set of contractions to R of ideals of S, (E) the set of extensions to S of ideals of R, $(C)_\Delta$ the set of contractions to R of differential ideals of S, and $(E)_\Delta$ the set of extensions to S of differential ideals of R. It is known that the mapping $A^c \mapsto A^{ce}$ (A being ideals of S) of (C) into (E) and the mapping $\mathfrak{a}^e \mapsto \mathfrak{a}^{ec}$ ($\mathfrak{a}$ being ideals of R) of (E) into (C) are bijections, and that either one is the inverse of the other (see Vol.I of [13]).

Theorem 9 Let R, S, Δ and f be as above.

(a) Every differential ideal contained in (C) is an element of $(C)_\Delta$, and every differential ideal contained in (E) is an element of $(E)_\Delta$.

(b) The mapping $A^c \mapsto A^{ce}$ (A being differential ideals of S) of $(C)_\Delta$ into $(E)_\Delta$ and the mapping $\mathfrak{a}^e \mapsto \mathfrak{a}^{ec}$ ($\mathfrak{a}$ being differential ideals of R) of $(E)_\Delta$ into $(C)_\Delta$ are bijections, and either one is the inverse of the other.

Proof. (a) Let $\mathfrak{a}$ be a differential ideal contained in (C). There exists an ideal A of S such that $\mathfrak{a} = A^c$. Since $\mathfrak{a}^{ec} = A^{cec} = A^c = \mathfrak{a}$, and since $\mathfrak{a}^e$ is a differential

ideal of S by Th.6, we see that $\mathfrak{q} \in (C)_\Delta$. The second assertion of part (a) of our theorem is similarly verified.

(b) The assertion is clear, because $A^{cec} = A^c$ for every differential ideal A of S and $\mathfrak{q}^{ece} = \mathfrak{q}^e$ for every differential ideal $\mathfrak{q}$ of R. q.e.d.

In particular, if R is a differential subring of a differential ring S with the set of derivation operators Δ, and if f is the canonical embedding of R into S, we see relative to f that $A^c = A \cap R$ for every ideal A of S, and that $\mathfrak{q}^e = (\mathfrak{q})_S = S\mathfrak{q}$ for every ideal $\mathfrak{q}$ of R. We call $A \cap R$ and $S\mathfrak{q}$ <u>contraction</u> of A to R and <u>extension</u> of $\mathfrak{q}$ to S, respectively, without mentioning f. Correspondingly, we use notations (C), (E), $(C)_\Delta$ and $(E)_\Delta$ without mentioning f. For example, consider the case that R and S are a differential ring R and the differential ring of quotients $M^{-1}R$ of R over a multiplicatively stable subset M of R respectively (see §2.2).

<u>Theorem 10</u> Let R and $M^{-1}R$ be as above.

(a) A differential ideal $\mathfrak{q}$ of R is contained in $(C)_\Delta$ if and only if M is prime to $\mathfrak{q}$, that is, if and only if an element $x \in R$ is contained in $\mathfrak{q}$ whenever $xs \in \mathfrak{q}$ for some $s \in M$.

(b) The set $(E)_\Delta$ consists of all differential ideals of $M^{-1}R$.

(c) The mapping $A \mapsto A^c$ (A being differential ideals of

$M^{-1}R$) of the set of differential ideals of $M^{-1}R$ into $(C)_\Delta$ is a bijection, and $A^{ce} = A$ for every differential ideal A of $M^{-1}R$. This mapping preserves the operation of intersection and that of taking radical ideal; hence, so does the inverse mapping $A^c \mapsto A$.

(d) The mapping $\mathfrak{a} \mapsto \mathfrak{a}^e$ ($\mathfrak{a}$ being differential ideals of R) of the set of differential ideals of R into the set of differential ideals of $M^{-1}R$ is surjective. This mapping preserves the operation of finite intersection and that of taking radical ideal.

(e) For a differential ideal $\mathfrak{a}$ of R, $\mathfrak{a}^e \neq M^{-1}R$ if and only if $\mathfrak{a}$ is disjoint to M.

(f) Let $\mathfrak{q}$ be a primary differential ideal of R that is disjoint to M, and set $\mathfrak{p} = \sqrt{\mathfrak{q}}$. Then we see as follows:

(i) $\mathfrak{p}$ is disjoint to M.

(ii) Both $\mathfrak{p}$ and $\mathfrak{q}$ are contained in $(C)_\Delta$, and they contain the differential ideal $\mathfrak{n} = \{z \in R \mid sz = 0 \text{ for some } s \in M\}$.

(iii) $\mathfrak{q}^e$ is a primary differential ideal of $M^{-1}R$ and $\mathfrak{p}^e = \sqrt{\mathfrak{q}^e}$.

Proof. (a) A differential ideal $\mathfrak{a}$ of R is contained in $(C)_\Delta$ if and only if $\mathfrak{a}^{ec} = \mathfrak{a}$. Since $\mathfrak{a}^{ec} = \{x \in R \mid xs \in \mathfrak{a} \text{ for some } s \in M\}$, the assertion of part (a) of our theorem is true.

(b) It is known that (E) consists of all ideals of

$M^{-1}R$. Therefore, by part (a) of Th.9, the assertion of part (b) of our theorem holds true.

(c) The first half of part (c) of our theorem is obvious by part (b) of Th.9 and by part (b) of our theorem. Let A_j ($j \in J$) be any set of differential ideals of $M^{-1}R$. Then, by (b), there exists a set of differential ideals $\mathfrak{a}_j$ ($j \in J$) of R such that $A_j = \mathfrak{a}_j^e$ ($j \in J$). We see that

$$\cap_{j\in J}A_j = \cap_{j\in J}\mathfrak{a}_j^e \mapsto (\cap_{j\in J}\mathfrak{a}_j^e)^c = \cap_{j\in J}\mathfrak{a}_j^{ec} = \cap_{j\in J}A_j^c.$$

Similarly, for any differential ideal A of $M^{-1}R$, we see that $A = \mathfrak{a}^e$ for some differential ideal $\mathfrak{a}$ of R and that $\sqrt{A} = \sqrt{\mathfrak{a}^e} \mapsto (\sqrt{\mathfrak{a}^e})^c = \sqrt{\mathfrak{a}^{ec}} = \sqrt{A^c}$. The remaining assertion of part (c) of our theorem is obvious.

(d) The first half of part (d) of our theorem is obvious by (b). Let $\mathfrak{a}$ and $\mathfrak{b}$ be two differential ideals of R. Then $\mathfrak{a}^e = \{a/s \mid a \in \mathfrak{a}, s \in M\}$, $\mathfrak{b}^e = \{b/s \mid b \in \mathfrak{b}, s \in M\}$ and $(\mathfrak{a}\cap\mathfrak{b})^e = \{c/s \mid c \in \mathfrak{a}\cap\mathfrak{b}, s \in M\}$. Therefore, it is easy to verify that $(\mathfrak{a}\cap\mathfrak{b})^e = \mathfrak{a}^e\cap\mathfrak{b}^e$. Similarly, we see that $(\sqrt{\mathfrak{a}})^e = \sqrt{\mathfrak{a}^e}$.

Proofs of (e) and (f) are straightforward.

2.7. Separably algebraic extension fields of a differential field

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$, K_a an algebraic closure of the field K, and K_s the separably algebraic closure of K in K_a. We know by §1.7 that each $\delta_i \in \Delta$ can be uniquely extended to a derivation of K_s which is denoted by the same

letter δ_i, and that extension derivations δ_i ($i \in I$) commute mutually. Thus the field K_s with the set of these extension derivations $\Delta = \{\delta_i \mid i \in I\}$ has a unique structure of a differential extension field of K. Moreover, we know also by §1.7 that every intermediate field L between K and K_s is stable under these extension derivations δ_i ($i \in I$), and that L can be uniquely regarded as an intermediate differential field between K and K_s.

Let C and C_s be fields of constants of differential fields K and K_s respectively. We see by Cor.2 to Th.2 of §1.7 that C_s is the separably algebraic closure of C in K_a.

2.8. Inseparably algebraic extension fields of a differential field

Let K be a differential field, K_a an algebraic closure of the field K, and K_s the separably algebraic closure of K in K_a which aquires a uniquely determined structure of a differential extension field of K (see §2.7). We denote by $\Delta = \{\delta_i \mid i \in I\}$ the set of derivation operators of K and K_s. In the present section, we inquire how far we can extend the differential field structure of K_s to K_a.

Let x be an element of K_a. By Th.3 of §1.8 and Rem.1 and Rem.2 to this theorem, we see the following results:

(i) Every $\delta_i \in \Delta$ can be extended to x if and only if the condition

(1) $\delta_{i\lambda}(x^{p(e)}) = 0$ $(i \in I,\ 0 < \lambda < p(e))$

is satisfied for some element $e \in \mathbb{N}$ with $x^{p(e)} \in K_s$. This condition is equivalent to the condition

(1') $\delta_{i\lambda}(x^{p(e)}) = 0$ $(i \in I,\ \lambda \in \mathbb{N}$ with $\lambda \not\equiv 0 \pmod{p(e)})$.

(ii) When (1) is satisfied, setting $\xi = x^{p(e)}$, the subfield $K_{s,x} = K_s((\delta_{i,\nu p(e)}\xi)^{p(-e)} \mid i \in I,\ \nu \in \mathbb{N})$ of K_a has extension derivation $\delta_i' = (\delta_{i\nu}' \mid \nu \in \mathbb{N})$ $(i \in I)$ of $\delta_i = (\delta_{i\nu} \mid \nu \in \mathbb{N})$ $(i \in I)$ respectively. Extension derivations δ_i' $(i \in I)$ are uniquely defined by formulas

(2) $\delta_{i\nu}'y = (\delta_{i,\nu p(e)}(y^{p(e)}))^{p(-e)}$ $(i \in I,\ \nu \in \mathbb{N},\ y \in K_{s,x})$.

The field $K_{s,x}$ and derivations δ_i' $(i \in I)$ are defined independent of $e \in \mathbb{N}$ with $x^{p(e)} \in K_s$.

(iii) If $i,j \in I$ and $i \neq j$, then δ_i' commutes with δ_j'.

(iv) Denoting δ_i' $(i \in I)$ by the same letters δ_i $(i \in I)$ as the given derivations of K, we get $K_{s,x} = K_s(\delta_{i\nu}x \mid i \in I,\ \nu \in \mathbb{N})$, and $K_{s,x}$ aquires the structure of a differential extension field of K. This $K_{s,x}$ is the smallest differential extension field of K containing x.

Now, in a manner similar to the proof of Th.4 of §1.8, we can prove that the set of all those elements of $x \in K_a$ such that every one of the given derivations δ_i $(i \in I)$ of K can be extended to x is the largest differential extension field of K in K_a. This differential extension field of K

is called differential closure of K in K_a, and denoted by K_Δ. Let C, C_s and C_a be fields of constants of K, K_s and K_Δ respectively. It is easy to see that the field of constants of K_Δ is the algebraic closure C_a of C in K_a, and that the field of constants of K_s is the separably algebraic closure C_s of C in C_a.

The results above are due to [8] and [11].

Example Let U be an indeterminate over an imperfect field K_0, and $K = K_0(U)$ the field generated by U over K_0. Consider the ordinary differential field K associated with the formal differentiation d of K relative to U (see Examp.1 of §1.8). The set of derivation operators Δ consists of a single element d. Denote by C the field of constants K_0 of the differential field K. Let K_a be an algebraic closure of K, K_s the separably algebraic closure of K in K_a, and K_Δ the differential closure of K in K_a. We saw in Examp.1 of §1.8 that $K_\Delta = K_s(C_a)$, where C_a denotes the algebraic closure of C in K_a. Since C is supposed to be imperfect, the separably algebraic closure C_s of C in C_a differs from C_a, and $K_\Delta \neq K_s$.

Generalizing the above, associate to the field K the derivation $d^{(\kappa)}$ for any $\kappa \in \mathbb{N}$, constructed from d by Prop.1 of §1.3. Then we get a differential field K with the set of derivation operators Δ consisting of a single element $d^{(\kappa)}$. For this differential field K, the field of constants

is $C = K_0$ as well, but we can prove that $K_\Delta = K_s^{p(-\kappa)}(C_a)$. The proof of the last equality is similar to the proof of the corresponding equality in Examp.1 of §1.8, but it is more complicated.

2.9. The field of constants of a differential field

Theorem 11 If a field K has a differential field structure with the field of constants C. Then K is regular over C, that is, K is separable over C and C is algebraically closed in K.

Proof. Let the set of derivation operators of K be $\Delta = \{\delta_i \mid i \in I\}$.

At first, we prove that C is algebraically closed in K. Let z be an element of K that is algebraic over C.

Case I: z is separably algebraic over C. By induction on ν, we can prove by part (b) of Th.2 of §1.7 that $\delta_{i\nu}z = 0$ $(i \in I, \nu \in \mathbb{N}-\{0\})$, so that $z \in C$.

Case II: z is inseparably algebraic over C. Since C is known by Case I to be separably algebraically closed in K, there exists $e \in \mathbb{N}-\{0\}$ with $z^{p(e)} \in C$. By (4) of §1.4, we see that

$$(\delta_{i\nu}z)^{p(e)} = \delta_{i,\nu p(e)}(z^{p(e)}) = 0 \quad (i \in I, \nu \in \mathbb{N}-\{0\}),$$

so that $z \in C$.

Now, it suffices to show that $C^{p(-1)}$ and K are linearly disjoint over C, or equivalently, that C and K^p are

linearly disjoint over C^p. Assume the contrary, namely, assume that there exists a finite family of elements of C which is linearly independent over C^p, but which is linearly dependent over K^p. Let $(c_1,\ldots,c_n)$ be such a family that consists of least number of elements of C. There exist z_1, $\ldots$, $z_n \in K$, not all zero, satisfying

(1) $\Sigma_{j=1}^{n} c_j z_j^p = 0$.

Suppose, as we may, that $z_n = 1$. Then $z_1, \ldots, z_{n-1}$ are not all contained in C. Therefore, suppose, as we may also, that $z_1 \notin C$, so that there exist $i \in I$ and $\nu \in \mathbb{N}-\{0\}$ with $\delta_{i\nu} z_1 \neq 0$. Take these i and ν, and apply $\delta_{i,\nu p}$ to (1). Then we get

$$0 = \Sigma_{j=1}^{n-1} c_j \delta_{i,\nu p}(z_j^p) = \Sigma_{j=1}^{n-1} c_j (\delta_{i\nu} z_j)^p.$$

This contradicts the minimal property of the family $(c_1,\ldots, c_n)$. q.e.d.

The converse of Th.11 is not true in general. Namely, a field K may be regular over a subfield C although we can never introduce in K any differential field structure for which C is the field of constants.

Example Let π be the prime field of characteristic p, and X an indeterminate over π, and consider the field $K = \pi(X, X^{p(-1)}, X^{p(-2)}, \ldots)$. This field K is clearly regular over π. Since K is a perfect field, there exists no derivation of K other than the trivial one.

The converse of Th.11 is true under some extra condition.

Proposition 4 If a fielf K is separably generated over a subfield C (that is, if K has a finite or infinite separating transcendence basis over C), and if C is algebraically closed in K, then we can introduce in K a differential field structure for which C is the field of constants.

Proof. Let $\{U_j \mid j \in J\}$ be a separating transcendence basis of K over C, and set $K_1 = C(U_j \mid j \in J)$. For each $j \in J$, let ∂_j be the formal differentiation of K_1 relative to U_j. Associating $\Delta = \{\partial_j \mid j \in J\}$ to K_1, K_1 is a differential field with the field of constants C (see Examp.3 of §2.1). Since K is separably algebraic over K_1, K has a unique differential extension field structure of K_1, and it is straightforward to show that the field of constants of K is C (see the end of §2.7).

Proposition 5 Let C be a subfield of a field K. Then K is regular over C if and only if we can introduce in each subfield of K that is finitely generated over C a differential field structure for which C is the field of constants.

The proof is straightforward.

Corollary Let K be a finitely generated extension field of a field C. Then K is regular over C if and only if we can introduce in K a differential field structure for which C is the field of constants. (cf. [6] and [9].)

CHAPTER 3

Differential Ideals

3.1. Perfect and prime differential ideals

Throughout this section, let R be a differential ring with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ.

At first, we give here a lemma and a proposition concerning general differential ideals of R.

Lemma 1 Let $\mathfrak{a}$ be a differential ideal of R, and $s,x \in R$ with $sx \in \mathfrak{a}$. Then, for each $\theta \in \Theta$, there exists $m \in \mathbb{N}$ such that $s^m \cdot \theta x \in \mathfrak{a}$.

Proof. It suffices to suppose that θ is of the form $\theta = \delta_{i(1),\nu(1)} \cdots \delta_{i(r),\nu(r)}$, where $r \in \mathbb{N}-\{0\}$ and $i(1),\ldots,i(r)$ are distinct elements of I and $\nu(1),\ldots,\nu(r) \in \mathbb{N}-\{0\}$.

We begin with the case of $r = 1$ and prove the formula

$$(1) \quad s^{\nu(1)+1}\delta_{i(1),\nu(1)}x \in \mathfrak{a}$$

by induction on $\nu(1)$.

Since $\delta_{i(1),1}s\cdot x + s\cdot\delta_{i(1),1}x = \delta_{i(1),1}(sx) \in \mathfrak{a}$, we get $\delta_{i(1),1}s\cdot sx + s^2\cdot\delta_{i(1),1}x \in \mathfrak{a}$, and consequently, $s^2\delta_{i(1),1}x \in \mathfrak{a}$. Thus the case of $\nu(1) = 1$ of the formula (1) holds true. In case $\nu(1) > 1$, we see that

$$s\cdot\delta_{i(1),\nu(1)}x + \Sigma_{\alpha=1}^{\nu(1)}\delta_{i(1),\alpha}s\cdot\delta_{i(1),\nu(1)-\alpha}x$$

$$= \delta_{i(1),\nu(1)}(sx) \in \mathfrak{a},$$

so that

$$s^{\nu(1)+1}\delta_{i(1),\nu(1)}x + \Sigma_{\alpha=1}^{\nu(1)}\delta_{i(1),\alpha}s\cdot s^{\alpha-1}s^{\nu(1)-\alpha+1}\delta_{i(1),\nu(1)-\alpha}x$$

is contained in $\mathfrak{q}$. Therefore, we get by induction assumption $s^{\nu(1)+1}\delta_{i(1),\nu(1)}x \in \mathfrak{q}$.

Now, the formula

$$(2)\quad s^{(\nu(1)+1)\ldots(\nu(r)+1)}\delta_{i(1),\nu(1)}\cdots\delta_{i(r),\nu(r)}x \in \mathfrak{q} \qquad (r \in \mathbb{N}-\{0\})$$

can be easily proved by (1).

Definition If $\mathfrak{c}$ is an ideal of a ring R_0 and S a nonempty subset of R_0, then $\mathfrak{c}:S^\infty$ denotes the set of all those elements x of R_0 such that $xs \in \mathfrak{c}$ for some power product s of elements of S. This set is clealy an ideal of R_0.

Proposition 1 If $\mathfrak{q}$ is a differential ideal of R, and if S is a nonempty subset of R, then $\mathfrak{q}:S^\infty$ is a differential ideal of R.

Proof. We have only to verify that $\mathfrak{q}:S^\infty$ is stable under the operator domain Θ. Let x be an element of $\mathfrak{q}:S^\infty$, and take a power product s of elements of S with $xs \in \mathfrak{q}$. For any $\theta \in \Theta$, we see by Lem.1 that $s^m\cdot\theta x \in \mathfrak{q}$ for some $m \in \mathbb{N}$, so that $\theta x \in \mathfrak{q}:S^\infty$.

Remark 1 Let M be the set consisting of 1 and all power products of elements of S of Prop.1. If M is a multiplica-

tively stable subset of R in the sense of §1.6, then it is easily verified that $\mathfrak{q}:S^{\infty} = \mathfrak{q}^{ec}$, the contraction and the extension being taken relative to the canonical embedding of R into $M^{-1}R$. Therefore, in this case, the assertion of Prop.1 is a consequence of Th.6 of §2.6.

Lemma 2 Let $\mathfrak{m}$ be a perfect differential ideal of R and $x,y \in R$ with $xy \in \mathfrak{m}$. Then $\theta x \cdot \theta' y \in \mathfrak{m}$ for any two derivative operators $\theta,\theta' \in \Theta$.

Proof. Owing to Lem.1, there exists $m \in \mathbb{N}$ such that $x^m \cdot \theta' y \in \mathfrak{m}$, so that $x \cdot \theta' y \in \mathfrak{m}$. Similarly, we get $\theta x \cdot \theta' y \in \mathfrak{m}$.

Remark 2 The property stated in Lem.2 is not necessarily true for general differential ideals. For example, Let K be a differential field with a single derivation δ, and $K\{X\}$ the differential polynomial ring in a single differential indeterminate X over K; consider the differential ideal $[X^p] = ((\delta_\nu X)^p \mid \nu \in \mathbb{N})$, then $X^p \in [X^p]$, but $X^{p-1}\delta_1 X \notin [X^p]$.

Theorem 1 Let $\mathfrak{q}$ be a differential ideal of R with $\mathfrak{q} \neq R$, and M a multiplicatively stable subset (see §1.6) of R not intersecting $\mathfrak{q}$. Then there exists a prime differential ideal of R containing $\mathfrak{q}$ but not intersecting M.

Proof. Set $\mathfrak{m} = \sqrt{\mathfrak{q}}$ in R. Then $\mathfrak{m}$ is a perfect differential ideal of R not intersecting M (see Th.2 of §2.4). Consider the set of all those perfect differential ideals of R that contain $\mathfrak{q}$ but not intersect M. This set is clearly in-

ductive relative to the inclusion order. Let $\mathfrak{p}$ be a maximal element of the set. We can show that $\mathfrak{p}$ must be a prime ideal of R.

Assume that there exist elements $x,y \in R$ such that $x \notin \mathfrak{p}$, $y \notin \mathfrak{p}$, $xy \in \mathfrak{p}$. By the maximal property of $\mathfrak{p}$, both $\sqrt{[\mathfrak{p},x]}$ and $\sqrt{[\mathfrak{p},y]}$ intersect M. Take $m_1, m_2 \in M$ with $m_1 \in \sqrt{[\mathfrak{p},x]}$, $m_2 \in \sqrt{[\mathfrak{p},y]}$. Then, for some $r,s \in \mathbb{N}-\{0\}$, we get

$$m_1^r = a + \Sigma_{\theta(1)\in\Theta} u_{\theta(1)} \cdot \theta(1)x, \quad m_2^s = b + \Sigma_{\theta(2)\in\Theta} v_{\theta(2)} \cdot \theta(2)y,$$

where $a,b \in \mathfrak{p}$ and where $u_{\theta(1)}, v_{\theta(2)} \in R$ all zeros except a finite number. Hence we see by Lem.2 that $m_1^r m_2^s \in \mathfrak{p}$ (a contradiction).

Corollary 1 Let $\mathfrak{m}$ be a perfect differential ideal of R with $\mathfrak{m} \neq R$.

(a) If an element $u \in R-\mathfrak{m}$ is given, there exists a prime differential ideal of R containing $\mathfrak{m}$ but not containing u.

(b) $\mathfrak{m}$ is the intersection of some family of prime differential ideals of R.

Proof. Part (a) is a particular case of Th.1 where $\mathfrak{a} = \mathfrak{m}$ and $M = \{1, u, u^2, \ldots\}$. Part (b) is an immediate consequence of part (a).

Corollary 2 Let R' be a differential extension ring of R. If a prime differential ideal $\mathfrak{p}$ of R satisfies the condition $(\mathfrak{p})_{R'} \cap R = \mathfrak{p}$, there exists a prime differential ideal $\mathfrak{p}'$ of R' such that $\mathfrak{p}' \cap R = \mathfrak{p}$.

Proof. Set $M = R - \mathfrak{p}$. Then M is a multiplicatively stable subset of R' and $(\mathfrak{p})_{R'} \cap M = \emptyset$. Hence, by Th.1, there exists a prime differential ideal $\mathfrak{p}'$ of R', containing $(\mathfrak{p})_{R'}$ but not intersecting M. We see at once that $\mathfrak{p}' \cap R = \mathfrak{p}$.

3.2. Condition of Noether

Let R be a differential ring with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ. Let $\mathfrak{a}$ be an ideal (respectively, a differential ideal, respectively, perfect differential ideal) of R. If there exists a finite family of elements $a_1, \ldots, a_r$ of $\mathfrak{a}$ such that $\mathfrak{a} = (a_1,\ldots,a_r)$ (respectively, $\mathfrak{a} = [a_1,\ldots,a_r]$, respectively, $\mathfrak{a} = \sqrt{[a_1,\ldots,a_r]}$), the family $a_1, \ldots, a_r$ is called ideal-basis (respectively, differential-ideal-basis, respectively, perfect-differential-ideal-basis) of $\mathfrak{a}$. It is well known that the following conditions 1°, 2°, 3° are mutually equivalent and called condition of Noether for ideals of R:

1° Every ideal of R has an ideal-basis.

2° Every strictly ascending chain of ideals of R is finite.

3° Every nonempty set of ideals of R has a maximal element.

We see that, if the word " ideal" is replaced by "differential ideal" (respectively, "perfect differential ideal") in 1°, 2°, 3°, we obtain also three mutually equivalent conditions. These conditions are called condition of Noether for differential ideals (respectively, perfect differential ideals) of R.

Henceforth in this section, let R be particularly the differential polynomial ring in a set of differential indeterminates $\{X_j \mid j \in J\}$ over a differential field K_0 with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ.

In the theory of differential algebras relative to derivations of rank 1, it is a fundamental fact that, when both I and J are finite, R satisfies the condition of Noether for perfect differential ideals if and only if K_0 is "differentially quasi-perfect", although it does not satisfy the condition of Noether for differential ideals, hence also for ideals (see Cor.2 to Th.1 of Chap.III of [4]). Since we are considering exclusively differential algebras of nonzero characteristic p relative to iterative derivations of rank ∞, R has never such a property.

Example Let m, n be any two positive integers, and consider R in the particular case that $I = \{1, \ldots, m\}$ and $J = \{1, \ldots, n\}$. Then we see by Lem.1 of §1.2 that differential ideals $\mathfrak{p}_h = [\delta_{i1}X_j, \delta_{ip}X_j, \ldots, \delta_{i,p(h)}X_j \mid i \in I, j \in J]$ $(h \in \mathbb{N})$ of R are prime, and that $\mathfrak{p}_h \subset \mathfrak{p}_{h+1}$, $\mathfrak{p}_h \neq \mathfrak{p}_{h+1}$ $(h \in \mathbb{N})$. Thus, for any differential field K_0, R does not satisfy the condition of Noether for perfect differential ideals (hence also for differential ideals and for ideals).

Now, let $\mathfrak{a}$ be a differential ideal of R with $\mathfrak{a} \neq R$, and ϕ the canonical differential homomorphism of R onto

the differential residue ring $R/\mathfrak{q}$. If, among θX_j ($j \in J$, $\theta \in \Theta$), there exist finitely many $\theta_1 X_{j(1)}, \ldots, \theta_n X_{j(n)}$ with $\theta_1, \ldots, \theta_n \in \Theta$ and $j(1), \ldots, j(n) \in J$ such that

$$\phi(\theta X_j) \in \phi(K_0)[\phi(\theta_1 X_{j(1)}), \ldots, \phi(\theta_n X_{j(n)})] \quad (j \in J, \theta \in \Theta),$$

then $R/\mathfrak{q}$ satisfies clearly the condition of Noether for ideals (hence also for differential ideals and for perfect differential ideals). Since there are important differential rings which are differentially isomorphic to such differential residue rings, we shall observe briefly, in the next section, differential rings satisfying the condition of Noether for ideals.

3.3. Differential rings satisfying the condition of Noether for ideals

Let R be a differential ring satisfying the condition of Noether for ideals. It is well known that every differential ideal $\mathfrak{q}$ of R can be represented as finite irredundant intersection of primary ideals of R (these primary ideals belong to distinct prime ideals, and each one of them does not contain the intersection of the others).

Proposition 2 Let $\mathfrak{q}$ be a differential ideal of a differential ring R satisfying the condition of Noether for ideals. If $\mathfrak{q} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ is a decomposition of $\mathfrak{q}$ as finite irredundant intersection of primary components $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ in R, then every isolated primary component is a differential ideal.

Proof. Set $p_1 = \sqrt{q_1}$, ... , $p_r = \sqrt{q_r}$. Let q_α be any isolated primary component of $\mathfrak{a}$. Then p_α does not contain any one of p_β $(1 \leq \beta \leq r, \beta \neq \alpha)$, and we can take elements s_β $(1 \leq \beta \leq r, \beta \neq \alpha)$ such that $s_\beta \in p_\beta$ and $s_\beta \notin p_\alpha$ $(1 \leq \beta \leq r, \beta \neq \alpha)$. Set $s = \Pi_{\beta \neq \alpha} s_\beta$, then $\mathfrak{a}:s^\infty = q_\alpha$. Therefore, by Prop.1 of §3.1, q_α is a differential ideal. q.e.d.

In Prop.2, embedded primary components of $\mathfrak{a}$ may be non-differential ideal as we show in the following example.

Example Let K_0 be a differential field of characteristic 2 with a single trivial derivation δ, and $K_0\{X\}$ the differential polynomial ring in a single differential indeterminate X over K_0. Consider the prime differential ideal $P = (\delta_2 X, \delta_3 X, \ldots)$ of $K_0\{X\}$ and the differential residue ring $R_0 = K_0\{X\}/P = K_0\{x\} = K_0[x, \delta_1 x]$, where x denotes the residue class of X mod P. Then R_0 satisfies obviously the condition of Noether for ideals. Now, the ideal $q_0 = (x, (\delta_1 x)^2)$ of R_0 is a primary nondifferential ideal for the prime differential ideal $p_0 = (x, \delta_1 x)$ of R_0, and the ideal $p_1 = (\delta_1 x)$ of R_0 is a prime differential ideal, and the ideal $\mathfrak{a} = q_0 \cap p_1 = (x\delta_1 x, (\delta_1 x)^2)$ of R_0 is a differential ideal.

Remark 1 Concerning Prop.2, it is not known for us so far whether every differential ideal $\mathfrak{a}$ of R can be written as finite irredundant intersection of primary differential ideals of R. In the preceding example, the ideal $\mathfrak{a} = q_0 \cap p_1$

can be decomposed as an irredundant intersection $\mathfrak{a} = \mathfrak{p}_0^{\,2} \cap \mathfrak{p}_1$ of primary differential ideals.

Corollary If R is as in Prop.2, every perfect differential ideal $\mathfrak{m}$ of R with $\mathfrak{m} \neq R$ admits a unique decomposition as finite irredundant intersection of prime differential ideals of R.

Proof. It is known that $\mathfrak{m}$ can be uniquely written as finite irredundant intersection of prime ideals of R. It is clear by Prop.2 that these prime ideals are prime differential ideals. q.e.d.

The prime differential ideal of R stated in the preceding corollary are called prime differential components of $\mathfrak{m}$ in R.

Remark 2 The set of perfect differential ideals of the differential ring R satisfying the condition of Noether for ideals is a "Noetherian perfect conservative system" in the sense of §§7~9 of Chap.0 of [4]. Therefore, the corollary above is a particular case of Th.1 of §9 loc. cit.

Let R be as above, M a multiplicatively stable subset of R, and $M^{-1}R$ the differential ring of quotients of R over M. Since every ideal of $M^{-1}R$ is the extension of an ideal of R to $M^{-1}R$ (see §10 of Chap.IV of Vol.I of [13]), $M^{-1}R$ satisfies the condition of Noether for ideals.

Proposition 3 Let R, M and $M^{-1}R$ be as above. Let $\mathfrak{m}$

be a perfect differential ideal of R with $\mathfrak{m} \neq R$, and $\mathfrak{m} = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$ the representation as finite irredundant intersection of prime differential ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of R. Renumbering $\mathfrak{p}_j$ $(1 \leq j \leq r)$ if necessary, suppose that $\mathfrak{p}_j \cap M = \emptyset$ $(1 \leq j \leq s)$ and $\mathfrak{p}_j \cap M \neq \emptyset$ $(s+1 \leq j \leq r)$, where s may be 0 or r. If $\mathfrak{m}^e, \mathfrak{p}_1^e, \ldots, \mathfrak{p}_r^e$ be extensions of $\mathfrak{m}, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ to $M^{-1}R$, respectively, then $\mathfrak{p}_1^e, \ldots, \mathfrak{p}_s^e$ are the prime differential components of $\mathfrak{m}^e$ in $M^{-1}R$.

The proof is immediate (see Th.10 of §2.6, and [11] loc. cit.).

3.4. Differential polynomial rings

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ, X_j $(j \in J)$ differential indeterminates over K, and $R = K\{X_j \mid j \in J\}$ the differential polynomial ring in X_j $(j \in J)$ over K. Elements of R are denoted by notations such as $P(X) = P(X_j \mid j \in J)$. Let $(x) = (x_j \mid j \in J)$ be a family of elements of some differential extension field L of K with the same set of indices J as above. Since each element $P(X)$ of R is a polynomial over K in derivatives θX_j $(\theta \in \Theta)$ of X_j $(j \in J)$, if we replace θX_j of $P(X)$ by θx_j for all $j \in J$ and for all $\theta \in \Theta$, we get an element of L which is denoted by $P(x) = P(x_j \mid j \in J)$. The mapping $\phi_{(x)}: P(X) \mapsto P(x)$ ($P(X)$ running through R) is a differential homomorphism of R into L, and it is called substitution of

(x) for (X) :

(1) $\phi_{(x)}(\delta_{(\nu)}(P(X))) = \delta_{(\nu)}(P(x)) = \delta_{(\nu)}(\phi_{(x)}(P(X)))$

$(P(X) \in R,\ (\nu) \in N^{(I)})$.

Let $S = \{P_\sigma(X) \mid \sigma \in \Sigma\}$ be a subset of R. If $P_\sigma(x) = 0$ for all $\sigma \in \Sigma$, (x) is called zero of the system S of differential polynomials, or solutuion of the system $\{P_\sigma(X) = 0 \mid \sigma \in \Sigma\}$ of differential equations, and we say that S vanishes at (x). Any differential equation of the form above is called algebraic differential equation over K.

Theorem 2 Let p be a prime differential ideal of the differential polynomial ring R. Then there exists a zero $(\xi) = (\xi_j \mid j \in J)$ of p such that

(2) $p = \{P(X) \in R \mid P(\xi) = 0\}$,

where ξ_j $(j \in J)$ are taken from some differential extension field of K.

Proof. Let $\bar{R} = R/p$ be the differential residue ring of R modulo p, and ϕ the canonical differential homomorphism of R onto $\bar{R}$. Since ϕ induces a differential isomorphism of K onto $\phi(K)$, we identify each element a of K with the image $\phi(a)$. Then the differential field of quotients $Q(\bar{R})$ of $\bar{R}$ is a differential extension field of K. If we set $\xi_j = \phi(X_j)$ $(j \in J)$, $(\xi) = (\xi_j \mid j \in J)$ satisfies clearly the condition (2). q.e.d.

The zero (ξ) stated in Th.2 is called generic zero of

$\mathfrak{p}$. If (ξ) and (ξ') are two generic zeros of $\mathfrak{p}$, then we get canonically differential isomorphism over K of $K\langle\xi\rangle$ onto $K\langle\xi'\rangle$.

Let $(x) = (x_j \mid j \in J)$ be as above. We use the notstion $\mathfrak{p}_{(x)/K}$ in the sense of $\mathfrak{p}_{(x)/K} = \{P(X) \in R \mid P(x) = 0\}$. This $\mathfrak{p}_{(x)/K}$ is a prime differential ideal of R, and is called <u>defining differential ideal</u> of (x) over K; (x) is a generic zero of $\mathfrak{p}_{(x)/K}$. For example, if $\mathfrak{p}$ and (ξ) are as in Th.2, we see that $\mathfrak{p} = \mathfrak{p}_{(\xi)/K}$.

<u>Theorem 3</u> Let S be a subset of the differential polynomial ring $R = K\{X_j \mid j \in J\}$ over the differential field K, and $(x) = (x_j \mid j \in J)$ a family of elements of some differential extension field of K. Then (x) is a zero of S if and only if it is a zero of $\mathfrak{m} = \sqrt{[S]_R}$.

The proof is straightforward by means of (1).

<u>Theorem 4</u> Let R be as above. If a subset S of R has no zero, then $\sqrt{[S]_R} = R$.

Proof. Set $\mathfrak{m} = \sqrt{[S]_R}$ and assume that $\mathfrak{m} \neq R$. By Cor.1 to Th.1 of §3.1, there exists a prime differential ideal $\mathfrak{p}$ containing $\mathfrak{m}$. Then the generic zero of $\mathfrak{p}$ whose existence is asserted in Th.2 is a zero of S, contradicting the hypothesis.

<u>Corollary</u> (Analogy of the "Nullstellensatz" of Hilbert-Netto) Let R be as above, and let S be a subset of R.

Set $\mathfrak{m} = \sqrt{[S]_R}$, then $\mathfrak{m}$ is the set of all those elements of R that vanish at every zero of S.

Proof. It suffices to suppose that there exists a nonzero element $P(X)$ of R that vanishes at every zero of S and to show that $P(X) \in \mathfrak{m}$.

Take a differential indeterminate Y over R, and set $R' = K\{X_j, Y \mid j \in J\}$. Now, consider the subset

(3) $\{A(X), 1 - YP(X) \mid A \in S\}$

of R'. Since $P(X)$ vanishes at every zero of S, the set (3) has no zero. Therefore, by Th.4, the perfect differential ideal generated in R' by the set (3) must contain 1, and we see that 1 is contained in $[S, 1 - YP]_{R'}$, so that

(4) $1 = \Sigma_{A\in S, \theta\in\Theta} Q_{\theta,A}(X,Y)\theta(A(X))$

$+ \Sigma_{\theta\in\Theta} S_\theta(X,Y)\theta(1 - YP(X))$,

where $Q_{\theta,A}(X,Y)$, $S_\theta(X,Y)$ are suitably chosen in R'. Let K' be the differential field of quotients of R'. For each $(\nu) \in N^{(I)}$, set $T_{(\nu)}(X) = \delta_{(\nu)}(1/P(X)) \in K'$. We see easily that $T_{(\nu)}(X)$ can be written in the form

$$T_{(\nu)}(X) = B_{(\nu)}(X)/P(X)^{e((\nu))}, \quad B_{(\nu)} \in R, \quad e((\nu)) \in N - \{0\}.$$

Since (4) contains effectively only a finite number of terms, regard it as a relation among differential polynomials in Y over K', and substitute $T_{(\nu)}(X)$ in place of $\delta_{(\nu)}Y$ for all $(\nu) \in N^{(I)}$. The result of the substitution in the part

$\theta(1 - YP(X))$ is equal to $\theta(1 - (1/P(X))P(X)) = 0$ for every $\theta \in \Theta$ (see (1)), we get

$$1 = \Sigma_{A\in S,\theta\in\Theta}(D_{\theta,A}(X)/P(X)^{f(\theta,A)})\cdot\theta(A(X)),$$

$$D_{\theta,A}(X) \in R,\ f(\theta,A) \in \mathbb{N}.$$

Therefore, taking a sufficiently large integer s, we see that $P(X)^s \in [S]_R$, so that $P(X) \in \mathfrak{m}$.

3.5. Linear differential polynomials

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ, and $R = K\{X_j \mid j \in J\}$ the differential polynomial ring in differential indeterminates X_j $(j \in J)$ over K. If $A(X)$ is a linear combination of 1 and θX_j $(j \in J, \theta \in \Theta)$ over K, $A(X)$ is called linear differential polynomial in X_j $(j \in J)$ over K, and $A(X) = 0$ is called linear differential equation in X_j $(j \in J)$ over K.

Let a set $S = \{A_\sigma(X) \mid \sigma \in \Sigma\}$ of linear differential polynomials be given, and let $\mathfrak{m}_S$ be the K-submodule of R generated by $\Theta S = \{\theta A_\sigma(X) \mid \sigma \in \Sigma, \theta \in \Theta\}$. This K-submodule $\mathfrak{m}_S$ is called differential K-module generated by S in R. We see that $\Theta\mathfrak{m}_S = \mathfrak{m}_S$ and that $[S] = (\mathfrak{m}_S)$ in R.

Theorem 5 Let K, Δ, Θ, X_j $(j \in J)$, R, S and $\mathfrak{m}_S$ be as above. Then $\sqrt{[S]} = [S] = (\mathfrak{m}_S)$. This ideal is a prime differential ideal of R if $\mathfrak{m}_S$ does not contain 1.

Proof. Suppose that $\mathfrak{m}_S$ does not contain 1. Then there

exists a subset $\mathfrak{D}_1$ of the set $\mathfrak{D} = \{\theta X_j \mid j \in J, \theta \in \Theta\}$ such that no nonzero linear combination over K of 1 and elements of $\mathfrak{D}_1$ is contained in $\mathfrak{m}_S$. Consider the collection of all such subsets as $\mathfrak{D}_1$. It is clearly inductive under the inclusion order. Let $\mathfrak{D}' = \{D'_\tau \mid \tau \in T\}$ be a maximal element of the collection, and $\mathfrak{D}'' = \{D''_\omega \mid \omega \in \Omega\}$ the complement of $\mathfrak{D}'$ in $\mathfrak{D}$. The maximal property of $\mathfrak{D}'$ implies that, for each element D''_ω of $\mathfrak{D}''$, an element $A_\omega = D''_\omega - (a_\omega + \Sigma_{\tau \in T} a_{\omega\tau} D'_\tau)$ of $\mathfrak{m}_S$ with $a_\omega \in K$ and $a_{\omega\tau} \in K$ is uniquely determined, so that $\mathfrak{m}_S$ consists of all the linear combinations of A_ω $(\omega \in \Omega)$ over K. Therefore, the ideal $(\mathfrak{m}_S)$ is generated by A_ω $(\omega \in \Omega)$, and, as we saw already, it is a differential ideal which is equal to $[S]$.

It remains to show that the ideal $(\mathfrak{m}_S)$ is prime. If $P(X)$ is an element of R, it is a polynomial in D'_τ $(\tau \in T)$ and D''_ω $(\omega \in \Omega)$ over K, and we see that $P(X)$ is contained in $(\mathfrak{m}_S)$ if and only if $P(X)$ vanishes by substitution $D''_\omega \mapsto a_\omega + \Sigma_{\tau \in T} a_{\omega\tau} D'_\tau$ $(\omega \in \Omega)$. This shows that $(\mathfrak{m}_S) \neq R$, and that $(\mathfrak{m}_S)$ is a prime ideal of R. q.e.d.

Corollary 1 Under the hypothesis of Th.5, the prime differential ideal $[S]$ is the set of all those elements of R that vanish at every zero of S.

This is an immediate consequence of Cor. to Th.4 of §3.4.

Concerning Th.5, suppose that $1 \notin \mathfrak{m}_S$. Then, by Th.2 of

§3.4, S has a zero (x) in some differential extension field L of K. Suppose as we may that X_j $(j \in J)$ are still differential indeterminates over L. Set $X'_j = X_j - x_j$ $(j \in J)$, then X'_j $(j \in J)$ are differential indeterminates over L. Consider the differential polynomial ring $R' = L\{X'_j \mid j \in J\}$ in X'_j $(j \in J)$ over L. Then S is regarded as a set S' of linear combinations of $\theta X'_j$ $(j \in J, \theta \in \Theta)$ over L and the problem of finding zeros of S in differential extension fields of L is reduced to that of finding zeros of S' in such fields.

According to this observation, let as take up the particular case of the consideration of this section, where S is a set of linear combinations of θX_j $(j \in J, \theta \in \Theta)$. If $A(X)$ is a linear combination of θX_j $(j \in J, \theta \in \Theta)$ over K, it is called <u>linear differential form</u> in X_j $(j \in J)$ over K, and $A(X) = 0$ is called <u>linear homogeneous differential equation</u> in X_j $(j \in J)$ over K.

<u>Corollary 2</u> Let K, Δ, Θ, X_j $(j \in J)$ and R be as above. If S is a set of linear differential forms in X_j $(j \in J)$ over K, and if $\mathfrak{m}_S$ the differential K-module in R generated by S, the ideal $(\mathfrak{m}_S) = [S] = \sqrt{[S]}$ is a prime differential ideal of R. If (ξ) is a generic zero of $[S]$, the differential field $K\langle\xi\rangle$ is purely transcendental over K.

Proof. Since $1 \notin \mathfrak{m}_S$, we see by Th.5 that the first assertion of our corollary holds true. Similarly as in the

proof of Th.5, there exists a maximal subset $D' = \{D'_\tau | \ \tau \in T\}$ of the set $D = \{\theta X_j | \ j \in J, \ \theta \in \Theta\}$ such that no nozero linear combination of elements of D' over K is contained in $\mathfrak{m}_S$. If $D'' = \{D''_\omega | \ \omega \in \Omega\}$ is the complement of D' in D, then, for each element D''_ω of D'', an element $A_\omega = D''_\omega - \Sigma_{\tau \in T} a_{\omega\tau} D'_\tau$ in $\mathfrak{m}_S$ with $a_{\omega\tau} \in K$ is uniquely determined, and $\mathfrak{m}_S$ consists of all the linear combinations of A_ω $(\omega \in \Omega)$ over K. Now, the differential ring $K\{\xi\} = K\{\xi_j | \ j \in J\}$ is canonically identified with the differential residue ring $R/[S]$. If ϕ denotes the canonical differential homomorphism of R onto $R/[S]$, and if we set $\phi(D'_\tau) = \xi'_\tau$ $(\tau \in T)$, $\phi(D''_\omega) = \xi''_\omega$ $(\omega \in \Omega)$, then $\xi'' = \Sigma_{\tau \in T} a_{\omega\tau} \xi'_\tau$ $(\omega \in \Omega)$ and $K\{\xi\} = K[\xi'_\tau, \ \xi''_\omega | \ \tau \in T, \ \omega \in \Omega] = K[\xi'_\tau | \ \tau \in T]$. Since it is easy to show that ξ'_τ $(\tau \in T)$ are algebraically independent over K, the second assertion of our corollary is true. q.e.d.

The choice of the subset D' of D in the proof above is not unique. But, we can prove that the cardinal number of D' is uniquely determined by S. This cardinal number is called <u>order</u> of the set S of linear differential forms.

3.6. Linear dependence over constants

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i | \ i \in I\}$ and the set of derivative operators Θ, and $x_1, \ \ldots, \ x_n$ finitely many elements of K. For any n elements $\theta(1), \ \ldots, \ \theta(n)$ of Θ, we denote by

$$W_{\theta(1),\ldots,\theta(n)}(x_1,\ldots,x_n)$$

the determinant

$$\det(\theta(j)x_h \mid 1 \le j \le n,\ 1 \le h \le n) = \begin{vmatrix} \theta(1)x_1 & \dots & \theta(1)x_n \\ \dots & & \dots \\ \theta(n)x_1 & \dots & \theta(n)x_n \end{vmatrix}$$

Theorem 6 Let K be as above, and $x_1, \dots, x_n$ finitely many elements of K. Then $x_1, \dots, x_n$ are linearly dependent over the field of constants K_c if and only if

(1) $W_{\theta(1),\dots,\theta(n)}(x_1,\dots,x_n) = 0$
for every choice of $\theta(1), \dots, \theta(n)$ in Θ.

Proof. If $x_1, \dots, x_n$ are linearly dependent over K_c, the condition (1) is obviously satisfied. Conversely, we prove by induction on n that (1) implies that $x_1, \dots, x_n$ are linearly dependent over K_c. Case $n = 1$ is trivial. In case $n > 1$, suppose that (1) is satisfied. If

$$W_{\theta(1),\dots,\theta(n-1)}(x_1,\dots,x_{n-1}) = 0$$

for every choice of $\theta(1), \dots, \theta(n-1)$ in Θ, then, by induction assumption, $x_1, \dots, x_{n-1}$ are linearly dependent over K_c, and consequently, so are $x_1, \dots, x_n$. On the contrary, suppose that

(2) $W_{\theta(1),\dots,\theta(n-1)}(x_1,\dots,x_{n-1}) \neq 0$
for some choice of $\theta(1), \dots, \theta(n-1)$ from Θ.

Then there exist elements $a_1, \dots, a_{n-1}$ of K such that

(3) $\Sigma_{h=1}^{n-1}\theta(j)x_h \cdot a_h = \theta(j)x_n \quad (1 \le j \le n-1)$.

Since $W_{\theta(1),\ldots,\theta(n-1),\theta}(x_1,\ldots,x_n) = 0$ for every $\theta \in \Theta$, (3) implies

(4) $\Sigma_{h=1}^{n-1} \theta x_h \cdot a_h = \theta x_n \quad (\theta \in \Theta)$.

Applying δ_{il} to (4), we get

(5) $\Sigma_{h=1}^{n-1} \delta_{il}\theta x_h \cdot a_h + \Sigma_{h=1}^{n-1} \theta x_h \cdot \delta_{il} a_h = \delta_{il}\theta x_n \quad (i \in I)$.

Since each $\delta_{il}\theta$ $(i \in I)$ is a multiple of an element of Θ by a natural number, (4) holds true when θ is replaced by $\delta_{il}\theta$, and this implies $\Sigma_{h=1}^{n-1} \theta x_h \cdot \delta_{il} a_h = 0$ $(i \in I, \theta \in \Theta)$; in particular, we see that

$$\Sigma_{h=1}^{n-1} \theta(j) x_h \cdot \delta_{il} a_h = 0 \quad (i \in I, 1 \leq j \leq n-1),$$

and by (2) that

(6) $\delta_{il} a_h = 0 \quad (i \in I, 1 \leq h \leq n-1)$.

It is now easy to prove by induction on ν that

(7) $\delta_{i\nu} a_h = 0 \quad (i \in I, 1 \leq h \leq n-1, \nu \in \mathbb{N}-\{0\})$.

Having established (7), $a_1, \ldots, a_{n-1}$ are constants, and (4) for $\theta = \delta_{(0)}$ (the identity operator) shows that $x_1, \ldots, x_n$ are linearly dependent over K_c. q.e.d.

In the proof of Th.6, K may be replaced by any differential subfield or extension field containing $x_1, \ldots, x_n$. Therefore, if the condition (1) is satisfied, we say that $x_1, \ldots, x_n$ are <u>linearly dependent over constants</u>. On the contrary, if (1) is not satisfied, we see that $x_1, \ldots, x_n$ are never linearly dependent over the field of constants of

any differential extension field of $K\langle x_1,\ldots,x_n\rangle$, and we say that $x_1, \ldots, x_n$ are <u>linearly independent over constants</u>.

By the proof of Th.6 and the remark above, we get the following corollaries.

<u>Corollary 1</u> Let n elements $x_1, \ldots, x_n$ of a differential field K with the set of derivative operators Θ be given. If there exist elements $\theta(1), \ldots, \theta(n-1)$ of Θ such that $W_{\theta(1),\ldots,\theta(n-1)}(x_1,\ldots,x_{n-1}) \neq 0$ and that $W_{\theta(1),\ldots,\theta(n-1),\theta}(x_1,\ldots,x_n) = 0$ for every $\theta \in \Theta$, then $x_1, \ldots, x_{n-1}$ are linearly independent over constants, and x_n is linearly dependent on $x_1, \ldots, x_{n-1}$ over constants.

<u>Corollary 2</u> If L is a differential extension field of a differential field K, then K and L_c are linearly disjoint over K_c.

Let us show an application of Cor.1. Let K be as above, and $R = K\{X\}$ the differential polynomial ring in a single differential indeterminate X over K. Let S be a set of linear differential forms of R and $\mathfrak{m}_S$ the differential K-module generated by S in R, and suppose that S is of finite order n (see §3.5). There exist n elements $\theta'(1), \ldots, \theta'(n)$ of Θ such that no nonzero linear combination of $\theta'(1)X, \ldots, \theta'(n)X$ over K is contained in $\mathfrak{m}_S$, and that, for each other element θ''_ω $(\omega \in \Omega)$ of Θ, an element $A_\omega(X) = \theta''_\omega X - \Sigma_{h=1}^{n} a_{\omega h}\cdot\theta'(h)X$ of $\mathfrak{m}_S$ with $a_{\omega h} \in K$ is uniquely deter-

mined. Then we obtain the following proposition.

Proposition 4 The set S above has n zeros $x_1,\ldots,x_n$ in some differential extension field of K, which are linearly independent over constants, such that, if x is a zero of S in a differential extension field of $K\langle x_1,\ldots,x_n\rangle$, x is linearly dependent on $x_1, \ldots, x_n$ over constants.

Proof. Let $\mathfrak{m}_S$, $\theta'(1), \ldots, \theta'(n)$ and $A_\omega(X)$ $(\omega \in \Omega)$ be as above. Set $p = (\mathfrak{m}_S)$ in R, then, by Cor.2 to Th.5 of §3.5, p is a prime differential ideal of R, and it is generated by $A_\omega(X)$ $(\omega \in \Omega)$. Now, take n differential indeterminates $X_1, \ldots, X_n$ over K, and set $R_j = K\{X_j\}$ $(1 \leq j \leq n)$, $R' = K\{X_1,\ldots,X_n\}$. For each j $(1 \leq j \leq n)$, a differential isomorphism ϕ_j of R onto R_j over K (that is, $\phi_j(a) = a$ for all $a \in K$) is uniquely determined by $\phi_j(X) = X_j$. Setting $p_j = \phi_j(p)$ $(1 \leq j \leq n)$, consider the ideal $p' = (p_1,\ldots,p_n)$ of R'. Since p' is the differential ideal of R' which is generated by the set of linear differential forms $\cup_{j=1}^{n}\phi_j(S)$, p' is a prime differential ideal of R' by Cor.2 to Th.5 of §3.5. Let $(x_1,\ldots,x_n)$ be a generic zero of p'. Then x_j is a zero of p_j for each j $(1 \leq j \leq n)$, hence of p and of S.

Assume that $W_{\theta'(1),\ldots,\theta'(n)}(x_1,\ldots,x_n) = 0$. Then $W_{\theta'(1),\ldots,\theta'(n)}(X_1,\ldots,X_n) \in p'$, and there exist $P_{\omega j}(X_1,\ldots,X_n) \in R'$ $(\omega \in \Omega, 1 \leq j \leq n)$ such that

(8) $W_{\theta'(1),\ldots,\theta'(n)}(X_1,\ldots,X_n)$

$= \Sigma_{j=1}^{n} \Sigma_{\omega \in \Omega} A_\omega(X_j) P_{\omega j}(X_1, \ldots, X_n)$.

By means of the substitution $\theta''_\omega X_j \mapsto \Sigma_{h=1}^{n} a_{\omega h} \cdot \theta'(h) X_j$ $(1 \leq j \leq n,\ \omega \in \Omega)$, we get $W_{\theta'(1),\ldots,\theta'(n)}(X_1, \ldots, X_n) = 0$ (a contradiction). Therefore, we see that $W_{\theta'(1),\ldots,\theta'(n)}(x_1, \ldots, x_n) \neq 0$.

If x is a zero of S in a differential extension field of $K\langle x_1, \ldots, x_n \rangle$, then

$$\theta''_\omega x_j - \Sigma_h a_{\omega h} \cdot \theta'(h) x_j = A_\omega(x_j) = 0 \quad (1 \leq j \leq n,\ \omega \in \Omega),$$

$$\theta''_\omega x - \Sigma_h a_{\omega h} \cdot \theta'(h) x = A_\omega(x) = 0 \quad (\omega \in \Omega).$$

This implies that $W_{\theta'(1),\ldots,\theta'(n),\theta}(x_1, \ldots, x_n, x) = 0$ for every $\theta \in \Theta$. Hence, by Cor.1 to Th.6, x is linearly dependent on $x_1, \ldots, x_n$ over constants. q.e.d.

This system $(x_1, \ldots, x_n)$ of zeros of S with the property stated in the preceding Prop. is called <u>fundamental system of zeros</u> of S.

3.7. Results about constants

Formulations and discussions of this section are similar to results of Kolchin (cf. [3] and [4]).

Let K be a differential field, and $C_1, \ldots, C_m$ finitely many indeterminates over the field K.

<u>Proposition 5</u> Let K and $C_1, \ldots, C_m$ be as above, and P a linear form (that is, homogeneous polynomial) in $C_1, \ldots, C_m$ over K. Then there exists a finite system of linear

forms $P_1, \ldots, P_r$ in $C_1, \ldots, C_m$ over K_c such that, for every differential extension field L of K, an m-tuple of constants of L is a zero of P if and only if it is a zero of $P_1, \ldots, P_r$.

Proof. Write P in the form $P = \Sigma_{j=1}^{r} a_j P_j$, where $a_1, \ldots, a_r$ are elements of K linearly independent over K_c and $P_1, \ldots, P_r$ are linear forms in $C_1, \ldots, C_m$ over K_c. Let $\gamma_1, \ldots, \gamma_m$ be m constants of L, then, by §3.6, $P(\gamma_1,\ldots,\gamma_m) = 0$ if and only if $P_j(\gamma_1,\ldots,\gamma_m) = 0$ $(1 \leq j \leq r)$.

Proposition 6 Let K and $C_1, \ldots, C_m$ be as above, and $\mathfrak{M}$ a subset of the ring $K[C_1,\ldots,C_m]$. Then there exists a subset $\mathfrak{M}'$ of the ring $K_c[C_1,\ldots,C_m]$ such that, for every differential extension field L of K, an m-tuple of constants of L is a zero of $\mathfrak{M}$ if and only if it is a zero of $\mathfrak{M}'$. Furthermore, $\mathfrak{M}'$ can be taken so as to be a perfect ideal of $K_c[C_1,\ldots,C_m]$.

Proof. Let $\mathfrak{a}$ be the ideal of $K[C_1,\ldots,C_m]$ generated by $\mathfrak{M}$. Then $\mathfrak{a}$ has an ideal-basis $A_1, \ldots, A_r$ (see §3.2). Write A_j in the form $A_j = \Sigma_{h=1}^{s} A_{jh} a_h$ $(1 \leq j \leq r)$, where $a_1, \ldots, a_s$ are elements of K linearly independent over K_c and $A_{jh} \in K_c[C_1,\ldots,C_m]$ $(1 \leq j \leq r, 1 \leq h \leq s)$. Set $\mathfrak{M}' = \{A_{jh} \mid 1 \leq j \leq r, 1 \leq h \leq s\}$. Then, we see similarly as in the proof of Prop.5 that an m-tuple of constants of L is a zero of $\mathfrak{M}$ if and only if it is a zero of $\mathfrak{M}'$. In place of the $\mathfrak{M}'$

above, we may denote by M' the radical of the ideal $(A_{jh} \mid 1 \leq j \leq r, 1 \leq h \leq s)$ of $K_c[C_1,\ldots,C_m]$.

Corollary If L is a differential extension field of a differential field K and $\gamma_1, \ldots, \gamma_m$ finitely many constants of L, then

$$\text{trdeg } K\langle\gamma_1,\ldots,\gamma_m\rangle/K = \text{trdeg } K_c\langle\gamma_1,\ldots,\gamma_m\rangle/K_c.$$

Proposition 7 Let L be a differential extension field of a differential field K. Let H denote the set of all intermediate differential fields between K and $K\langle L_c\rangle$, and D the set of all intermediate fields between K_c and L_c. Then the mapping $D \mapsto K\langle D\rangle$ $(D \in D)$ of D into H and the mapping $H \mapsto H \cap (L_c)$ $(H \in H)$ of H into D are bijective and inverse to each other.

Proof. Let D be any element of D. Since K and L_c are linearly disjoint over K_c by Cor.2 to Th.6 of §3.6, $K\langle D\rangle$ and L_c are also linearly disjoint over D, hence, $K\langle D\rangle \cap (L_c) = D$. Therefore, the former mapping of the assertion of our proposition is injective. To establish the remaining part of our proposition, let H be any element of H. For each element $\eta \in H$ we may write $\eta = \Sigma\kappa_j c_j / \Sigma\kappa_j d_j$, where κ_j are finitely many elements of K linearly independent over K_c, and where $c_j, d_j \in L_c$ with $\Sigma\kappa_j d_j \neq 0$. Since the elements $\eta\kappa_j$ and κ_j of H are linearly dependent over constants, they are also linearly dependent over $H_c = H \cap (L_c)$. Hence, there exist elements $c_j', d_j' \in H \cap (L_c)$ not all zero such that $\Sigma\eta\kappa_j d_j'$

$- \Sigma\kappa_j c_j' = 0$. Now, it is easy to see that $\eta = \Sigma\kappa_j c_j'/\Sigma\kappa_j d_j' \in K\langle H \cap (L_c)\rangle$. This shows that $H = K\langle H \cap (L_c)\rangle$, and the proof of our proposition is completed.

Corollary If L and M are differential extension fields of a differential field K with $L \supset M$, then $K\langle L_c\rangle \cap M = K\langle M_c\rangle$.

3.8. Extensions of the differential field of coefficients

Before we consider the differential case, we must make some preparations in the nondifferential case.

Let K_0 be a field, Y_λ $(\lambda \in \Lambda)$ indeterminates over K_0, and $R_0 = K_0[Y_\lambda | \lambda \in \Lambda]$ the ring of polynomials in Y_λ $(\lambda \in \Lambda)$ over K_0. Let $\mathfrak{p}$ be a prime ideal of R_0. If a family $(y) = (y_\lambda | \lambda \in \Lambda)$ of elements of some extension field of K_0 has the property $\mathfrak{p} = \{P(Y) \in R_0 | P(y) = 0\}$, (y) is called generic zero of $\mathfrak{p}$. For any two generic zeros (y) and (y') of $\mathfrak{p}$, an isomorphism over K_0 of the field $K_0(y) = K_0(y_\lambda | \lambda \in \Lambda)$ onto the field $K_0(y') = K_0(y_\lambda' | \lambda \in \Lambda)$ with $y_\lambda \mapsto y_\lambda'$ $(\lambda \in \Lambda)$ is determined. The transcendence degree of $K_0(y)$ over K_0 is called dimension of $\mathfrak{p}$ and it is denoted by $\dim \mathfrak{p}$. If $K_0(y)$ is separable (respectively regular) over K_0, we say that $\mathfrak{p}$ is separable (respectively regular) over K_0; if that is the case, we say also that $\mathfrak{p}$ is K_0-separable (respectively K_0-regular). Moreover, if $K_0(y)$ is separable (respectively regular) and finitely generated as a field over K_0, $\mathfrak{p}$ is called finitely separable (respectively finitely regular) over

K_0.

More generally, a perfect ideal $\mathfrak{m}$ of R_0 is called K_0-separable if $(R_0/\mathfrak{m})^p$ and K_0 are linearly disjoint over ${K_0}^p$.

Lemma 3 Let K_0 and R_0 be as above, and $\{\mathfrak{m}_\tau \mid \tau \in T\}$ a set of K_0-separable perfect ideals of R_0 totally ordered with respect to inclusion order. Set $\mathfrak{m} = \cup_{\tau \in T} \mathfrak{m}_\tau$, then $\mathfrak{m}$ is also K_0-separable.

Proof. It is obvious that $\mathfrak{m}$ is a perfect ideal of R_0. Let α_γ $(\gamma \in \Gamma)$ be a linear basis of K_0 over ${K_0}^p$. We have only to prove that α_γ $(\gamma \in \Gamma)$ are linearly independent over $(R_0/\mathfrak{m})^p$. Suppose that $\Sigma_{\gamma \in \Gamma} \alpha_\gamma {F_\gamma}^p \in \mathfrak{m}^p$ with $F_\gamma \in R_0$ $(\gamma \in \Gamma)$, then $\Sigma_{\gamma \in \Gamma} \alpha_\gamma {F_\gamma}^p \in {\mathfrak{m}_\tau}^p$ for some $\tau \in T$. Since $\mathfrak{m}_\tau$ is K_0-separable, we see that $F_\gamma \in \mathfrak{m}_\tau \subset \mathfrak{m}$ $(\gamma \in \Gamma)$.

Lemma 4 Let K_0 and R_0 be as above, $\mathfrak{m}$ a K_0-separable perfect ideal of R_0, and M a nonempty subset of R_0. Then $\mathfrak{m}:M$ is also K_0-separable.

Proof. Clearly, $\mathfrak{m}:M$ is a perfect ideal of R_0. Let α_γ $(\gamma \in \Gamma)$ be as in the proof of Lem.3. We have to verify that α_γ $(\gamma \in \Gamma)$ are linearly independent over $(R_0/(\mathfrak{m}:M))^p$. Suppose that $\Sigma_{\gamma \in \Gamma} \alpha_\gamma {F_\gamma}^p \in (\mathfrak{m}:M)^p$ with $F_\gamma \in R_0$ $(\gamma \in \Gamma)$. Then $\Sigma_{\gamma \in \Gamma} \alpha_\gamma {F_\gamma}^p P^p \in \mathfrak{m}^p$ for every $P \in M$. Since $\mathfrak{m}$ is K_0-separable, we see that $F_\gamma P \in \mathfrak{m}$ $(\gamma \in \Gamma, P \in M)$, so that $F_\gamma \in \mathfrak{m}:M$ $(\gamma \in \Gamma)$. q.e.d.

Let K_0, Y_λ $(\lambda \in \Lambda)$ and R_0 be as above, and L_0 an extension field of K_0. Suppose that Y_λ $(\lambda \in \Lambda)$ are still indeterminates over L_0, and let $S_0 = L_0[Y_\lambda \mid \lambda \in \Lambda]$ be the ring of polynomials in Y_λ $(\lambda \in \Lambda)$ over L_0. For any ideal $\mathfrak{a}$ of R_0, $L_0\mathfrak{a}$ denotes the extension ideal $S_0\mathfrak{a}$ of $\mathfrak{a}$ to S_0.

Lemma 5 Let K_0, Y_λ $(\lambda \in \Lambda)$, R_0, L_0 and S_0 be as above, and let $\mathfrak{p}$ be a prime ideal of R_0 that is finitely separable over K_0.

(a) The ideal $L_0\mathfrak{p}$ of S_0 can be written in the form of an irredundant intersection of finitely many prime ideals of S_0:

(1) $L_0\mathfrak{p} = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_t$,

where $\mathfrak{P}_\gamma$ $(1 \leq \gamma \leq t)$ are prime ideals of S_0 and finitely separable over L_0. For $\mathfrak{p}$ and L_0, the $\mathfrak{P}_\gamma$ $(1 \leq \gamma \leq t)$ are uniquely determined up to their numbering. Furthermore, we get

$$\mathfrak{P}_\gamma \cap R_0 = \mathfrak{p}, \quad \dim \mathfrak{P}_\gamma = \dim \mathfrak{p} \quad (1 \leq \gamma \leq t).$$

(b) Every generic zero of each $\mathfrak{P}_\gamma$ is a generic zero of $\mathfrak{p}$.

(c) Each generic zero of $\mathfrak{p}$ is a zero of precisely one of $\mathfrak{P}_\gamma$ $(1 \leq \gamma \leq t)$.

(d) There exists, independent of L_0, an irreducible polynomial T over K_0 such that, for every extension field L_0 of K_0, the number of prime ideals $\mathfrak{P}_\gamma$ in (1) equals the number of irreducible factors into which T splits over L_0.

This lemma is a classical result.

Corollary Let K_0, Y_λ ($\lambda \in \Lambda$), R_0, L_0 and S_0 be as above. If $\mathfrak{p}$ is a prime ideal of R_0 that is finitely regular over K_0, then $L_0\mathfrak{p}$ is a prime ideal of S_0 and finitely regular over L_0.

Proof. The hypothesis implies that T of part (d) of Lem.5 remains irreducible over L_0. q.e.d.

Now, we can consider the differential case. Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ, and X_j ($j \in J$) differential indeterminates over K. Set $R = K\{X_j \mid j \in J\}$. A perfect differential ideal of R is called K-separable if it is K-separable as a perfect ideal of the ring of polynomials in θX_j ($j \in J$, $\theta \in \Theta$) over K. A prime differential ideal of R is called finitely K-separable (respectively K-regular, respectively finitely K-regular) if it is finitely K-separable (respectively K-regular, respectively finitely K-regular) as a prime ideal of the ring of polynomials in θX_j ($j \in J$, $\theta \in \Theta$) over K. Let L be a differential extension field of K. Suppose that X_j ($j \in J$) are still differential indeterminates over L, and set $S = L\{X_j \mid j \in J\}$. For any differential ideal $\mathfrak{q}$ of R, $L\mathfrak{q}$ denotes the extension ideal $S\mathfrak{q}$ that is known to be a differential ideal of S (see Th.6 of §2.6).

Theorem 7 Let K, L, X_j $(j \in J)$, R and S be as above. Let $\mathfrak{p}$ be a prime differential ideal of R that is finitely K-separable.

(a) The differential ideal $L\mathfrak{p}$ of S can be written in the form of an irredundant intersection of finitely many prime differential ideals of S :

$$(2) \quad L\mathfrak{p} = \mathfrak{P}_1 \cap \ldots \cap \mathfrak{P}_t$$

where $\mathfrak{P}_\gamma$ $(1 \leq \gamma \leq t)$ are prime differential ideals of S and finitely separable over L. For $\mathfrak{p}$ and L, the $\mathfrak{P}_\gamma$ $(1 \leq \gamma \leq t)$ are uniquely determined up to their numbering. Furthermore, we get

$$\mathfrak{P}_\gamma \cap R = \mathfrak{p}, \ \dim \mathfrak{P}_\gamma = \dim \mathfrak{p} \quad (1 \leq \gamma \leq t).$$

(b) Every generic zero of each $\mathfrak{P}_\gamma$ is a generic zero of $\mathfrak{p}$.

(c) Each generic zero of $\mathfrak{p}$ is a zero of precisely one of $\mathfrak{P}_\gamma$ $(1 \leq \gamma \leq t)$.

(d) There exists, independent of L, an irreducible differential polynomial T over K such that, for every differential extension field L of K, the number of prime differential ideals $\mathfrak{P}_\gamma$ in (2) equals the number of irreducible factors into which T splits over L.

Proof. Regarding R as the ring of polynomials in the indeterminates θX_j $(j \in J, \ \theta \in \Theta)$ over the field K, we apply Lem.5 to the prime ideal $\mathfrak{p}$ of R. We get the unique de-

composition (2) of $\mathfrak{Lp}$ in the form of an irredundant intersection of prime ideals $\mathfrak{P}_\gamma$ $(1 \leq \gamma \leq t)$ of S, which are finitely separable over L, and for which

$$\mathfrak{P}_\gamma \cap R = \mathfrak{p}, \quad \dim \mathfrak{P}_\gamma = \dim \mathfrak{p} \quad (1 \leq \gamma \leq t).$$

Since $\mathfrak{Lp}$ is a perfect differential ideal of S and

$$\mathfrak{P}_\gamma = \mathfrak{Lp} : (\cap_{1 \leq \gamma' \leq t, \gamma' \neq \gamma} \mathfrak{P}_{\gamma'}) \quad (1 \leq \gamma \leq t),$$

we see by Th.3 of §2.4 that $\mathfrak{P}_\gamma$ $(1 \leq \gamma \leq t)$ are prime differential ideals of S. Thus we have established the assertion (a). The other assertions (b)~(d) are clear by the corresponding assertions of Lem.5. q.e.d.

By Cor. to Lem.5, we get the following corollary to Th.7.

Corollary Let K, X_j $(j \in J)$, R, L and S be as above. If $\mathfrak{p}$ is a prime differential ideal of R and finitely regular over K, then $\mathfrak{Lp}$ is a prime differential ideal of S and finitely regular over L.

Remark 1 We shall have occasion to use this remark afterwards. Let K, X_j $(j \in J)$, R and $\mathfrak{p}$ be as in Th.7, and let τ be a differential automorphism of K. Denote by $\mathfrak{p}^\tau$ the set of all those differential polynomials which are obtained from differential polynomials of $\mathfrak{p}$ by operating τ on the coefficients. Then $\mathfrak{p}^\tau$ is clearly a prime differential ideal of R. Moreover, we can see that $\mathfrak{p}^\tau$ is finitely separable over K. In fact, let $(x) = (x_j \mid j \in J)$ be a generic zero of $\mathfrak{p}$ and $(x') = (x'_j \mid j \in J)$ that of $\mathfrak{p}^\tau$. For each diffe-

rential polynomial $P(X)$ of R, let $P^{\tau}(X)$ be the differential polynomial of R which is obtained from $P(X)$ by operating τ on the coefficients. It is clear $P^{\tau}(x') = 0$ if and only if $P(x) = 0$. For each pair of differential polynomials $A(X)$, $B(X)$ of R with $B(x) \neq 0$, assign $A^{\tau}(x')/B^{\tau}(x')$ to $A(x)/B(x)$. Then a field-isomorphism over K of $K\langle x\rangle$ onto $K\langle x'\rangle$ is defined. Since $K\langle x\rangle$ is finitely separable over K, so is $K\langle x'\rangle$.

Remark 2 In the hypothesis of Th.7, we can not omit the condition that $\mathfrak{p}$ be finitely separable over K (see the following example).

Example Let u_{λ} $(\lambda \in \mathbb{N})$ be indeterminates over the prime field π_2 of characteristic 2, $(K')_a$ an algebraic closure of the field $K' = \pi_2(u_{\lambda} \mid \lambda \in \mathbb{N})$, and δ the trivial derivation of $(K')_a$. Let X be a differential indeterminate over the differential field $(K')_a$ with a single derivation δ, $R' = K'\{X\}$ and $S' = (K')_a\{X\}$. Consider the ideal $\mathfrak{p}'$ of R' which is generated by $(\delta_{2(\lambda)}X)^{3^{\lambda}} - u_{\lambda}$ $(\lambda \in \mathbb{N})$ and $\delta_{\nu}X$ $(\nu \in \mathbb{N}-\{0\}$ with $\nu \neq 2(\lambda)$ for any $\lambda \in \mathbb{N})$. For each $\lambda \in \mathbb{N}$, let $u_{\lambda,1}$, $u_{\lambda,2}$, $\cdots$, $u_{\lambda,3^{\lambda}}$ be all the roots in $(K')_a$ of the equation $U^{3^{\lambda}} - u_{\lambda} = 0$. For each element $(k(0),k(1),\ldots) \in \mathbb{N}^{\mathbb{N}}$ with $1 \leq k(\lambda) \leq 3^{\lambda}$ $(\lambda \in \mathbb{N})$, let $P'_{(k(\lambda))}$ be the ideal of S' which is generated by $\delta_{2(\lambda)}X - u_{\lambda,k(\lambda)}$ $(\lambda \in \mathbb{N})$ and $\delta_{\nu}X$ $(\nu \in \mathbb{N}-\{0\}$ with $\nu \neq 2(\lambda)$ for any $\lambda \in \mathbb{N})$. Then we can see that $\mathfrak{p}'$ is a prime differential ideal of R', that $P'_{(k(\lambda))}$ is a prime

differential ideal of S' for every such element $(k(\lambda))$ of N^N as above, that it is impossible to write $(K')_a\mathfrak{p}'$ in the form of a finite irredundant intersection of prime differential ideals $P'_1, \ldots, P'_t$ of S' with $P'_\gamma \cap R' = \mathfrak{p}'$ $(1 \leq \gamma \leq t)$.

Proposition 8 Let K, L, X_j $(j \in J)$, R and S be as in Th.7. If $\mathfrak{p}$ is a prime differential ideal of R which is K-separable, then $L\mathfrak{p}$ is a perfect differential ideal of S with $L\mathfrak{p} \cap R = \mathfrak{p}$, and it is L-separable. Moreover, if $\mathfrak{p}$ is K-regular, $L\mathfrak{p}$ is a prime differential ideal of S, and it is L-regular.

Proof. $L\mathfrak{p}$ is obviously a differential ideal of S, and it is easy to see that $L\mathfrak{p} \cap R = \mathfrak{p}$. Therefore, our proposition is a direct consequence of results of [4] (see Prop.7 and Cor.1 to Prop.7 of §12 of Chap.0 of [4]).

Lemma 6 Let K, L, X_j $(j \in J)$, R and S be as in Th.7. Let $\mathfrak{p}$ be a prime differential ideal of R that is K-separable. Then the differential ideal $L\mathfrak{p}$ can be written in the form of the intersection of a set of prime differential ideals P of S with $P \cap R = \mathfrak{p}$.

Proof. Take any element A of $S - (R \cup L\mathfrak{p})$, and let M_A be the smallest multiplicatively stable subset of S containing A and $R - \mathfrak{p}$. We show that $M_A \cap L\mathfrak{p} = \emptyset$.

Each element of M_A is written in the form $A^\ell F$ with $\ell \in N$, $F \in R-\mathfrak{p}$. If $A^\ell F$ were contained in $L\mathfrak{p}$ for some such ℓ

and F as above, then AF would be contained in $\mathfrak{Lp}$ by Prop. 8, and we could write $AF = (\Sigma_{h=1}^{n}\alpha_h Q_h)F = \Sigma_{h=1}^{n}\alpha_h P_h$ with $Q_h \in R$, $P_h \in \mathfrak{p}$ and with $\alpha_h \in L$ linearly independent over K; and it would follow that $Q_h F = P_h$, $Q_h \in \mathfrak{p}$ $(1 \leq h \leq n)$ and $A \in \mathfrak{Lp}$ (a contradiction).

Therefore, by Th.1 of §3.1, there exists a prime differential ideal $\mathfrak{P}_A$ of S containing $\mathfrak{Lp}$ but not intersecting M_A. Hence we see that $\mathfrak{P}_A \cap R = \mathfrak{p}$ for any $A \in S-(R \cup \mathfrak{Lp})$ and that $\mathfrak{Lp} = \cap_{A \in S-(R \cup \mathfrak{Lp})} \mathfrak{P}_A$.

Theorem 8 Let K, L, X_j $(j \in J)$, R, S and $\mathfrak{p}$ be as in Th.7. Then there exists a prime differential ideal $\mathfrak{P}$ of S such that $\mathfrak{P}$ is L-separable and $\mathfrak{P} \cap R = \mathfrak{p}$.

Proof. If $\mathfrak{Lp}$ is prime in S, the assertion of our theorem holds true by Prop.8. Therefore, suppose that $\mathfrak{Lp}$ is not prime in S. Then there exist two elements A, B of S such that $A \notin \mathfrak{Lp}$, $B \notin \mathfrak{Lp}$ and $AB \in \mathfrak{Lp}$. Let $\mathfrak{P}_\lambda$ $(\lambda \in \Lambda)$ be all the prime differential ideals of S with $\mathfrak{P}_\lambda \cap R = \mathfrak{p}$. Then, by Lem. 6, we get $\cap_{\lambda \in \Lambda} \mathfrak{P}_\lambda = \mathfrak{Lp}$. Set $\Lambda^A = \{\lambda \in \Lambda \mid A \notin \mathfrak{P}_\lambda\}$, $\Lambda^B = \{\lambda \in \Lambda \mid B \notin \mathfrak{P}_\lambda\}$ and $\Lambda' = \{\lambda \in \Lambda \mid A \in \mathfrak{P}_\lambda, B \in \mathfrak{P}_\lambda\}$. These are disjoint proper subsets of Λ with $\Lambda^A \neq \emptyset$, $\Lambda^B \neq \emptyset$ and $\Lambda^A \cup \Lambda^B \cup \Lambda' = \Lambda$. Consider two perfect differential ideals $\mathfrak{M}^A = \cap_{\lambda \in \Lambda^A} \mathfrak{P}_\lambda$ and $\mathfrak{M}' = \cap_{\lambda \in \Lambda^B \cup \Lambda'} \mathfrak{P}_\lambda$. We see that $\mathfrak{Lp} = \mathfrak{M}^A \cap \mathfrak{M}'$. Since $A \in \mathfrak{P}_\lambda$ $(\lambda \in \Lambda^B \cup \Lambda')$, we get $A \in \mathfrak{M}'$ and $\mathfrak{M}' \not\subset \mathfrak{P}_\lambda$ $(\lambda \in \Lambda^A)$. Therefore, we see that $\mathfrak{Lp}:\mathfrak{M}' = \mathfrak{M}^A$, so that $\mathfrak{M}^A$ is L-separable by Prop.8 and Lem.4. Thus there exists at least one nonempty subset Γ

of Λ such that $M = \cap_{\lambda\in\Gamma} P_\lambda$ is L-separable.

Now, let $\{M\}$ be the set of all such ideals M. We can see that $\{M\}$ is inductive with respect to inclusion order. In fact, let $\{M_\tau \mid \tau \in T\}$ be any totally ordered subset of $\{M\}$. Set $\overline{M} = \cup_{\tau\in T} M_\tau$. Since $\overline{M}\cap R = p$, we see that, for any $A \in S-(R\cup\overline{M})$, there exists a prime differential ideal P'_A of S with $P'_A\cap R = p$ (see the proof of Lem.6), that

$$\overline{M} = \cap_{A\in S-(R\cup\overline{M})} P'_A,$$

that $P'_A \in \{P_\lambda \mid \lambda \in \Lambda\}$, so that $\overline{M}$ is L-separable by Lem.3. Thus $\{M\}$ has a maximal element M^0. This ideal is written in the form $M^0 = \cap_{\lambda\in\Lambda^0} P_\lambda$ for some nonempty subset Λ^0 of Λ. If M^0 were not prime in S, then, discussing for M^0 as we done for Lp in the beginning part of the proof of our theorem, we could see that there would exist in $\{M\}$ an element containing M^0 properly, contradicting the maximal property of M^0. Therefore, M^0 is a prime differential ideal of S with $M^0\cap R = p$ and it is L-separable.

CHAPTER 4

Universal Differential Extension Field

4.1. Definitions

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$, and L a differential extension field of K. A differential extension field V of L is called semiuniversal over L, if, for every $n \in \mathbb{N}-\{0\}$ and every L-separable prime differential ideal $\mathfrak{p}$ of the differential polynomial ring $L\{X_1,\ldots,X_n\}$, there exist elements $x_1, \ldots, x_n$ of V such that $(x) = (x_1,\ldots,x_n)$ is a generic zero of $\mathfrak{p}$.

Let an algebraic closure K_a of the field K be given. Let U be a differential extension field of K, and U_a an algebraic closure of the field U that contains K_a. We say that U is universal over K, if U is the differential closure of itself in U_a (see §2.8) and semiuniversal over every finitely generated differential extension field of K in U.

We add here a proposition which is necessary in this chapter.

Proposition 1 Let K be as above. In a differential extension field of K, let $K\langle\xi_j \mid j \in J\rangle$ and $K\langle\eta_{j'} \mid j' \in J'\rangle$ be two independent differential extension fields of K which are regular over K. Let $X_j, Y_{j'}$ $(j \in J, j' \in J')$ be differential indeterminates over K, and $\mathfrak{p}_{(\xi)/K}$, $\mathfrak{p}_{(\eta)/K}$ defining differential ideals of $(\xi) = (\xi_j \mid j \in J)$, $(\eta) = (\eta_{j'} \mid j' \in J')$

in $K\{X_j \mid j \in J\}$, $K\{Y_{j'} \mid j' \in J'\}$ respectively. Then the differential ideal $(\mathfrak{p}_{(\xi)/K}, \mathfrak{p}_{(\eta)/K})$ generated by $\mathfrak{p}_{(\xi)/K}$ and $\mathfrak{p}_{(\eta)/K}$ in $K\{X_j, Y_{j'} \mid j \in J, j' \in J'\}$ is prime and K-regular, and it has a generic zero $(\xi_j, \eta_{j'} \mid j \in J, j' \in J')$, and

$$\dim(\mathfrak{p}_{(\xi)/K}, \mathfrak{p}_{(\eta)/K}) = \dim \mathfrak{p}_{(\xi)/K} + \dim \mathfrak{p}_{(\eta)/K}.$$

Proof. Our proposition follows from Cor.2 to Prop.7 of §12 of Chap.0 of [4].

4.2. Lemmas

Lemma 1 Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$, K_a an algebraic closure of the field K, and K_Δ the differential closure of K in K_a. If U is a universal differential extension field of K_Δ, then U is a universal differential extension field of K.

Proof. By the hypothesis, U is the differential closure of itself in an algebraic closure U_a of U, where U_a is taken so as to contain K_a. Hence we have only to prove that U is semiuniversal over every finitely generated differential extension field L of K in U. Let $n \in \mathbb{N}-\{0\}$ and $\mathfrak{p}$ an L-separable prime differential ideal of the differential polynomial ring $L\{X_1,\ldots,X_n\}$ over L. The compositum $L\cdot K_\Delta = K_\Delta(L)$ is a finitely generated differential extension field of K_Δ in U. By Th.8 of §3.8 applied to $L\cdot K_\Delta$ and L instead of L and K, there exists a prime differential ideal $\mathfrak{P}$ of the differential polynomial ring $(L\cdot K_\Delta)\{X_1,\ldots,X_n\}$ over $L\cdot K_\Delta$

such that P is $L \cdot K_{\Delta}$-separable and $P \cap (L\{X_1,\ldots,X_n\}) = p$. Therefore, by the hypothesis, P has a generic zero $(x) = (x_1, \ldots,x_n)$ with $x_1,\ldots,x_n \in U$. We see that (x) is a generic zero of p.

Corollary If U is a universal differential extension field of a differential field K, then U is also a universal differential extension field of any differential subfield K' of K.

This corollary can be proved in a similar way to the proof of Lem.1.

Lemma 2 Let H be a differential field, and H_a an algebraic closure of H. Suppose that H is the differential closure of itself in H_a. Then there exists a differential extension field H^* of H that satisfies the following conditions:

1° H^* is the differential closure of itself in an algebraic closure H^*_a of H^*, where H^*_a is taken so as to contain H_a.

2° H^* is semiuniversal over H.

Proof. For each $n \in \mathbb{N}-\{0\}$, let Π_n be the set of all H-separable prime differential ideals of the differential polynomial ring $H\{X_1,\ldots,X_n\}$ over H. Let X_{npj} ($n \in \mathbb{N}-\{0\}$, $p \in \Pi_n$, $j \in \mathbb{N}$ with $1 \leq j \leq n$) be differential indeterminates over H. Then, for each $p \in \Pi_n$, a differential isomorphism ϕ_{np} over H of $H\{X_1,\ldots,X_n\}$ onto $H\{X_{np1},\ldots,X_{npn}\}$ is de-

termined by $\phi_{np}(X_j) = X_{npj}$ $(1 \leq j \leq n)$, and $\phi_{np}(p)$ is an H-separable prime differential ideal of $H\{X_{np1},\ldots,X_{npn}\}$. Let P be the ideal generated by the set $\{\phi_{np}(p) \mid n \in N-\{0\}, p \in \Pi_n\}$ in the differential polynomial ring $R = H\{X_{npj} \mid n \in N-\{0\}, p \in \Pi_n, j \in N$ with $1 \leq j \leq n\}$ over H. We claim that P is a prime differential ideal of R.

Obviously, P is a differential ideal of R. Let A and B be two elements of R with $AB \in P$. If we take a sufficiently large integer s, there exists for every integer k with $1 \leq k \leq s$ a finite set of elements $p(k,1), \ldots, p(k,r_k)$ of Π_k such that A and B are contained in the differential polynomial ring $R' = H\{X_{kp(k,\alpha)j} \mid 1 \leq k \leq s, 1 \leq \alpha \leq r_k, 1 \leq j \leq k\}$ over H and that AB is contained in the ideal $P' = (\phi_{kp(k,\alpha)}(p(k,\alpha)) \mid 1 \leq k \leq s, 1 \leq \alpha \leq r_k)$ of R'. Since H is the differential closure of itself in H_a, H-separable prime differential ideals $\phi_{kp(k,\alpha)}(p(k,\alpha))$ are H-regular. Applying Prop.1 of §4.1 inductively, we see that P' is a prime ideal of R', so that at least one of A and B is contained in P', whence in P.

Let $(x_{npj} \mid n \in N-\{0\}, p \in \Pi_n, 1 \leq j \leq n)$ be a generic zero of P. Then, for each $n \in N-\{0\}$ and each $p \in \Pi_n$, $(x_{np1},\ldots,x_{npn})$ is a generic zero of p. Set $H_1 = H\langle x_{npj} \mid n \in N-0, p \in \Pi_n, 1 \leq j \leq n\rangle$ and take an algebraic closure $(H_1)_a$ such that $(H_1)_a$ contains H_a. If we denote by H* the differential closure $(H_1)_\Delta$ of H_1 in $(H_1)_a$, then H* satisfies conditions 1° and 2° of our lemma.

4.3. The existence theorem

Theorem 1 (The existence theorem) Every differential field K has a universal differential extension field.

Proof. Let $\Delta = \{\delta_i \mid i \in I\}$ be the set of derivation operators of K. By Lem.1 of §4.2, we may suppose that $K = K_\Delta$. Applying Lem.2 of §4.2, we define K_α $(\alpha \in \mathbb{N}-\{0\})$ inductively by $K_1 = K^*$ and $K_{\alpha+1} = (K_\alpha)^*$ $(\alpha \in \mathbb{N}-\{0\})$. We can prove that the differential field $U = \cup_{\alpha\in\mathbb{N}-\{0\}} K_\alpha$ is universal over K.

Clearly, U is the differential closure of itself in its algebraic closure.

Let $L = K\langle a_1,\ldots,a_s\rangle$ be a finitely generated differential extension field of K in U. For a sufficiently large integer t, all the elements $a_1, \ldots, a_s$ are in K_t, whence $L \subset K_t$. Let $n \in \mathbb{N}-\{0\}$ and $\mathfrak{p}$ an L-separable prime differential ideal of the differential polynomial ring $L\{X_1,\ldots,X_n\}$ over L. We may suppose that $X_1, \ldots, X_n$ are differential indeterminates over K_t. By Th.8 of §3.8, there exists a K_t-separable prime differential ideal $\mathfrak{P}$ of $K_t\{X_1,\ldots,X_n\}$ with $\mathfrak{P} \cap L\{X_1,\ldots,X_n\} = \mathfrak{p}$. By Lem.2 of §4.2, $\mathfrak{P}$ has a generic zero $(x) = (x_1,\ldots,x_n)$ with $x_1,\ldots,x_n \in (K_t)^* \subset U$. We see that (x) is a generic zero of $\mathfrak{p}$.

By the above, we have shown that U is a universal differential extension field of K.

4.4. Some properties of the universal differential extension field

Let U be a universal differential extension field of a differential field K with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ.

Theorem 2 Let U be as above, then U is separably algebraically closed.

Proof. Let U_a be an algebraic closure of the field U. Then, by definition, U is the differential closure of itself in U_a. Therefore, by §2.7, every element of U_a which is separably algebraic over U is contained in U.

Theorem 3 Let U be as above. Then the field of constants U_c of U is algebraically closed, and the transcendence degree of U_c over the field of constants K_c of K is infinite.

Proof. Let U_a be as in the proof of Th.2. Then, since $U = U_\Delta$ in U_a, we see by §2.8 that U_c is the algebraic closure of itself in U_a. Thus U_c is algebraically closed.

Let Z be a differential indeterminate over U, and ζ_0 a generic zero of the prime differential ideal $p_0 = (\theta Z \mid \theta \in \Theta$ with ord $\theta > 0)$ of $K\{Z\}$. Since $K\langle\zeta_0\rangle = K(\zeta_0)$ is purely transcendental over K, there exists a generic zero $c_0 \in U$ of p_0. Clearly c_0 is in U_c and transcendental over K_c. Now, assume that we have already shown the existence of n elements

$c_0,\ldots,c_{n-1} \in U_c$ which are independent over K_c. Since the prime differential ideal $p_n = (\theta Z \mid \theta \in \Theta$ with ord $\theta > 0)$ of $K<c_0,\ldots,c_{n-1}>\{Z\}$ is $K<c_0,\ldots,c_{n-1}>$-separable, there exists a generic zero $c_n \in U$ of p_n. It is evident that $c_n \in U_c$ and that $c_0, c_1, \ldots, c_n$ are independent over K_c. Thus we have proved that the transcendence degree of U_c over K_c is infinite.

Theorem 4 Let K be a differential field, and U a universal differential extension field of K. If L is a finitely generated differential extension field of K in U, and if K' is an intermediate differential field between K and L, then U is also universal over K'.

Proof. By virtue of Cor. to Lem.1 of §4.2, it suffices to prove that U is universal over L. But, this is obvious since a finitely generated differential extension field of L is also a finitely generated differential extension field of K.

4.5. Linear homogeneous differential polynomial ideals

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ, and U a universal differential extension field of K.

Let $X_1, \ldots, X_n$ be finitely many differential indeterminates over K, and consider the differential polynomial ring $K\{X_1,\ldots,X_n\}$ over K. The differential ideal of $K\{X_1,\ldots,X_n\}$

generated by a set of linear differential forms in $X_1, \ldots, X_n$ over K is called linear homogeneous differential polynomial ideal of $K\{X_1,\ldots,X_n\}$. By Cor.2 to Th.5 of §3.5, we see that every linear homogeneous differential polynomial ideal $\mathfrak{p}$ of $K\{X_1,\ldots,X_n\}$ is K-regular, so that $\mathfrak{p}$ has a generic zero $(x_1,\ldots,x_n)$ with $x_1,\ldots,x_n \in U$.

The following example is an important particular case of the above.

Example Let X be a differential indeterminate over K, and S a set of linear differential forms in X over K. Suppose that S is of finite order n (see the end of §3.5). By Prop.4 of §3.6 and by the above, we see that there exists a fundamental system of zeros $x_1, \ldots, x_n$ of S with $x_j \in U$ (see the end of §3.6). If $K\langle x_1,\ldots,x_n\rangle_c = K_c$, and if $K\langle x_1, \ldots,x_n\rangle$ is K-separable, we call $K\langle x_1,\ldots,x_n\rangle$ Picard-Vessiot extension of K. We shall see two simple and familiar examples of Picard-Vessiot extensions in the following two sections.

4.6. Primitive elements

Let K, Δ, Θ and U be as in the preceding section. An element x of a differential extension field K is called primitive over K, if θx ($\theta \in \Theta$, ord $\theta > 0$) are all contained in K, equivalently, if $\delta_{i,p(e)}x$ ($i \in I$, $e \in \mathbb{N}$) are all contained in K.

Concerning the notations in the following theorem, see §2.1.

Theorem 5 Let a family $(a_\theta \mid \theta \in \Theta, \text{ord}\,\theta > 0)$ of elements of K be given. Set $a_{\theta'\theta} = n(\theta,\theta')a_{\theta''}$ for each pair θ, θ' of derivative operators with $\text{ord}\,\theta > 0$, $\text{ord}\,\theta' > 0$ and $\theta'\theta = n(\theta,\theta')\theta''$ (θ'' being element of Θ). Then there exists a primitive x over K in U with

(1) $\theta x = a_\theta$ $(\theta \in \Theta, \text{ord}\,\theta > 0)$,

if and only if the condition

(2) $\theta' a_\theta = a_{\theta'\theta}$ $(\theta,\theta' \in \Theta, \text{ord}\,\theta > 0, \text{ord}\,\theta' > 0)$

is satisfied. When that is the case, such a primitive x can be taken so as to be transcendental over K.

Proof. Since the necessity of the condition is obvious, it suffices to show the sufficiency of the condition. Suppose that (2) is satisfied. Let X be a differential indeterminate over K, and consider the ideal $\mathfrak{p} = (\theta X - a_\theta \mid \theta \in \Theta, \text{ord}\,\theta > 0)$ of $K\{X\}$. By (2) and by Th.5 of §3.5, $\mathfrak{p}$ is a prime differential ideal of $K\{X\}$. Moreover, we see that $\mathfrak{p} \cap (K[X]-K) = \emptyset$. Hence, $\mathfrak{p}$ has a generic zero ξ for which $K\langle\xi\rangle = K(\xi)$ is purely transcendental over K (hence, $\mathfrak{p}$ is K-regular), and there exists a generic zero x of $\mathfrak{p}$ in U which is transcendental over K. This x is a primitive over K in U satisfying (1). q.e.d.

Example 1 Let K be any ordinary differential field with a derivation δ, and U a universal differential extension field of K. Take any sequence α_κ $(\kappa \in \mathbb{N})$ of elements of

K_c. Then we can see the existence of a primitive x over K in U such that $\delta_{p(\kappa)}x = \alpha_\kappa$ ($\kappa \in \mathbb{N}$). Clearly $\delta_\nu x = 0$ if $\nu \neq p(\kappa)$ for any $\kappa \in \mathbb{N}$.

Proposition 2 If x is a primitive over K in U satisfying (1), if $K\langle x\rangle_c = K_c$, and if $K\langle x\rangle$ is K-separable, then $K\langle x\rangle$ is a Picard-Vessiot extension of K.

Proof. In case a_θ ($\theta \in \Theta$, ord $\theta > 0$) are all zero, x must be a constant of K, and $K\langle x\rangle = K$ is trivially a Picard-Vessiot extension of K. Therefore, we may suppose that at least one of a_θ ($\theta \in \Theta$, ord $\theta > 0$) is not zero. Let X be a differential indeterminate over K, and S the set of linear differential forms $a_\theta \cdot \theta'X - a_{\theta'} \cdot \theta X$ ($\theta, \theta' \in \Theta$; ord $\theta > 0$, ord $\theta' > 0$) in $K\{X\}$. Then it is easy to see that S is of order 2 and that $(1, x)$ is a fundamental system of zeros of S. Thus $K\langle x\rangle = K(x)$ is a Picard-Vessiot extension of K.

Example 2 In Examp.1 of §2.2, U is a primitive over K, and $K(U)$ is a Picard-Vessiot extension of K. In Examp.2 of §2.2, any linear combination x of a finite number of U_i ($i \in I$) over K is a primitive over K, and $K\langle x\rangle$ is a Picard-Vessiot extension of K. In Examp.1 of this section, if $K = K_c$ and the x is taken so as to be transcendental over K, then $K\langle x\rangle$ is a Picard-Vessiot extension of K.

4.7. Exponential elements

Let K, Δ, Θ and U be as in §4.5. A nonzero element x of a differential extension field of K is called exponen-

tial over K, if $x^{-1}\cdot\theta x$ $(\theta \in \Theta)$ are all contained in K, equivalently, if $x^{-1}\cdot\delta_{i,p(e)}x$ $(i \in I, e \in \mathbb{N})$ are all contained in K.

Theorem 6 Let a family $(a_{(\nu)} \mid (\nu) \in \mathbb{N}^{(I)})$ of elements of K with $a_{(0)} = 1$ be given. Then there exists an exponential x over K in U with

(1) $x^{-1}\cdot\delta_{(\nu)}x = a_{(\nu)}$ $((\nu) \in \mathbb{N}^{(I)})$,

if and only if the condition

(2) $\binom{(\lambda)+(\nu)}{(\lambda)}a_{(\lambda)+(\nu)} = \Sigma_{(\alpha)+(\beta)=(\lambda)}\delta_{(\alpha)}a_{(\nu)}\cdot a_{(\beta)}$

$((\lambda),(\nu) \in \mathbb{N}^{(I)})$

is satisfied. When that is the case, such an exponential x can be taken so as to be transcendental over K.

proof. Suppose that x is an exponential over K in U satisfying (1). For any two elements (λ), (ν) of $\mathbb{N}^{(I)}$, apply $\delta_{(\lambda)}$ to $\delta_{(\nu)}x = a_{(\nu)}x$. Then we get the equations (2). Conversely, suppose that the condition (2) is satisfied. Let X be a differential indeterminate over K, and consider the ideal $\mathfrak{p} = (\delta_{(\nu)}X - a_{(\nu)}X \mid (\nu) \in \mathbb{N}^{(I)})$ of $K\{X\}$. By (2) and by Cor.2 to Th.5 of §3.5, $\mathfrak{p}$ is a prime differential ideal of $K\{X\}$ having a generic zero ξ such that $K\langle\xi\rangle = K(\xi)$ is purely transcendental over K. Hence $\mathfrak{p}$ has in U a generic zero x that is transcendental over K. This x is an exponential over K in U satisfying (1).

Remark Suppose that x is an exponential over K for which $x^{-1}\delta_{(\nu)}x = a_{(\nu)}$ ($(\nu) \in \mathbb{N}^{(I)}$) are all constants of K. Then, by Th.6, the condition $\binom{(\lambda)+(\nu)}{(\lambda)}a_{(\lambda)+(\nu)} = a_{(\nu)}a_{(\lambda)}$ ($(\lambda),(\nu) \in \mathbb{N}^{(I)}$) must be satisfied. Hence we can prove by induction on m that

$$\left(\prod_{i\in I}\frac{(m\nu_i)!}{(\nu_i!)^m}\right)a_{m(\nu)} = a_{(\nu)}{}^m \quad ((\nu) \in \mathbb{N}^{(I)},\ m \in \mathbb{N}-\{0\}).$$

Therefore, we see that $a_{(\nu)}{}^p = 0$ ($(\nu) \in \mathbb{N}^{(I)}-\{(0)\}$), so that x must be constant.

Example 1 Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ such that $K \neq K_c$. Take any nonconstant element u of K and any integer m (> 1) with $m \not\equiv 0 \pmod{p}$. Set $v = u^{1/m} \in K_s$. Then it is easy to prove by induction on ν that $v^{-1}\cdot\delta_{i\nu}v \in K$ ($i \in I$, $\nu \in \mathbb{N}$), so that v is a nonconstant exponential over K.

Proposition 3 If x is an exponential over K in U satisfying (1), if $K\langle x\rangle_c = K_c$, and if $K\langle x\rangle$ is K-separable, then $K\langle x\rangle$ is a Picard-Vessiot extension of K.

Proof. Let X be a differential indeterminate over k, and S the set of linear differential forms $\delta_{(\nu)}X - a_{(\nu)}X$ ($(\nu) \in \mathbb{N}^{(I)}$) in $K\{X\}$. Then we see that S is of order 1 and that x is a fundamental system of zeros of S. Therefore, $K\langle x\rangle = K(x)$ is a Picard-Vessiot extension of K.

Example 2 In Examp.1 of this section, suppose in particu-

lar that Δ consists of a single derivation δ and set $\alpha_\nu = v^{-1}\delta_\nu v$ $(\in K)$ for every $\nu \in \mathbb{N}$. Let U be a universal differential extension field of K. Suppose as we may that $v \in U$. Take $\tau \in \mathbb{N}-\{0\}$ as small as possible such that $\alpha_\tau \neq 0$, then τ must be a certain power $p(\omega)$ $(\omega \in \mathbb{N})$ of p. Let γ be any constant transcendental over K in U, then γv is a transcendental exponential over K. We can see that $K\langle \gamma v \rangle$ is a Picard-Vessiot extension of K when K never contains nonzero element a satisfying $\delta_{p(e+\omega)}a + ma\alpha_{p(\omega)}^{p(e)} = 0$ for any $(e,m) \in \mathbb{N}\times(\mathbb{N}-\{0\})$ with $m \not\equiv 0 \pmod{p}$.

4.8. Weierstrassian elements

In the theory of differential algebra of characteristic zero Weierstrassian elements are very important. To our regret the concept of Weierstrassian element is not so far successfully established. We are interested to nonconstant Weierstrassian elements which are transcendental over the differential field. The observations which was done by us are reported in this section.

Let K be a differential field of characteristic $p \neq 2$ with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ. Let two constants g_2, g_3 of K with $g_2^3 - 27g_3^2 \neq 0$ be given. The definitions of primitive and exponential in §§4.6~4.7 make us to try the following definition.

Let an element x of a differential extension field of

K be called Weierstrassian over K if $y^{-1}\cdot\delta_{i,p(e)}x \in K$ ($i \in I$, $e \in \mathbb{N}$) with nonzero $y = (4x^3 - g_2x - g_3)^{1/2}$. Then we can see by very tedious calculation the followings: If the x above is transcendental over K, it turns out that $\delta_{i\nu}x = 0$ ($i \in I$, $0 < \nu < 3^2$) for $p = 3$ and that $\delta_{i\nu}x = 0$ ($i \in I$, $0 < \nu < 5$) for $p = 5$. According to these calculations we come to the conjecture that, under the definition above, every Weierstrassian element x over K which is transcendental over K must be constant.

Therefore, we adopt here the definition: an element x of a differential extension field of K is called Weierstrassian over K if $(\delta_{i1}x)^2 = a_i^2(4x^3 - g_2x - g_3)$ ($i \in I$) with $a_i \in K$ not all zero. Under this definition we can see as follows.

For the sake of simplicity, we mention only the ordinary differential case where Δ consists of a single derivation $\delta = (\delta_\nu \mid \nu \in \mathbb{N})$ and $(\delta_1x)^2 = a^2(4x^3 - g_2x - g_3)$ with nonzero $a \in K$. The last equation can be written as $y^{-1}\delta_1x = a$ for x transcendental over K. In order that such an element x should exist, the element a of K must satisfy some conditions. For example, let $p = 3$ (hence let $g_2 \neq 0$), then we see by short calculation that $\delta_\nu a = 0$ ($\nu \equiv 2 \pmod 3$).

Let us consider the case where a is a nonzero constant of K. If $p = 3$, there exist transcendental Weierstrassian elements x over K; but, if $p = 5$ and $g_2 \neq 0$, there is no

such element x. (See Examp.1 and Examp.2 below in this section.)

In the case of nonconstant a of K, we can not so far verify the existence of elements x satisfying the definition above which are transcendental over K.

Example 1 (This is due to Tsuji) Let K_0 be a differential field of characteristic 3 with a single derivation $\delta = (\delta_\nu \mid \nu \in \mathbb{N})$, and X a differential indeterminate over K_0. Consider the differential polynomial ring $R = K_0\{X\}$ in X over K_0. Let a, g_2, g_3 be three given constants of K_0 with $a \neq 0$, $g_2 \neq 0$ (hence $g_2^3 - 27g_3^2 \neq 0$), and set $A = (\delta_1 X)^2 - a^2(4X^3 - g_2X - g_3) = (\delta_1 X)^2 - a^2(X^3 - g_2X - g_3)$.

Let $\mathfrak{p}$ (if exits) be a prime differential ideal of R such that $A \in \mathfrak{p}$ and $\mathfrak{p} \cap (K_0[X] - K_0) = \emptyset$. Then, by rather tedious calculations and observations, we see the followings:

(i) $\delta_1 X \notin \mathfrak{p}$.

(ii) Set $B = \delta_2 X + a^2 g_2$, then $\delta_1 A = \delta_1 X \cdot B \in (B) \subset \mathfrak{p}$.

(iii) $\delta_\nu B = \binom{\nu+2}{2} \delta_{2+\nu} X \in \mathfrak{p}$ $(\nu \geq 1)$:

If $\nu = 3n$ $(n \geq 1)$, set $D_n = \delta_\nu B = \delta_{2+3n} X \in \mathfrak{p}$.

If $\nu = 1 + 3n$ or $\nu = 2 + 3n$ $(n \geq 0)$, then $\delta_\nu B = 0$.

(iv) $\delta_2 A = \delta_2 X \cdot B \in (B) \subset \mathfrak{p}$

(v) If $\nu = 3n$ $(n \geq 1)$, set

$$C_n = \delta_\nu A = -\delta_{1+3n} X \cdot \delta_1 X + \Sigma' \delta_{1+3\alpha} X \cdot \delta_{1+3\beta} X - a^2 (\delta_n X)^3 + a^2 g_2 \delta_{3n} X \in \mathfrak{p},$$

where the summation Σ' runs through all pairs $(\alpha,\beta) \in \mathbb{N}^2$ with $\alpha + \beta = n$, $\alpha < n$, $\beta < n$. If $\nu = 1 + 3n$ $(n \geq 1)$, then $\delta_{1+3n}A = (1+3n)\delta_{1+3n}A = \delta_{3n}\delta_1 A = \delta_{3n}(\delta_1 X \cdot B) \in (B, D_m | m \geq 1) \subset \mathfrak{p}$. If $\nu = 2 + 3n$ $(n \geq 1)$, we get similarly $\delta_{2+3n}A \in (B, D_m | m \geq 1) \subset \mathfrak{p}$.

(vi) Set $\mathfrak{a} = (A, B, C_n, D_n | n \geq 1) \subset \mathfrak{p}$.

(vii) $\mathfrak{a}$ is a differential ideal of R and $\mathfrak{a} \cap (K_0[X]-K_0) = \emptyset$.

(viii) $A \in \mathfrak{a}:(\delta_1 X)^\infty \subset \mathfrak{p}:(\delta_1 X)^\infty = \mathfrak{p}$ (see §3.1).

(ix) Set $\mathfrak{p}_0 = \mathfrak{a}:(\delta_1 X)^\infty$. Then $\mathfrak{p}_0$ is the smallest prime differential ideal of R that contains A and that is disjoint to $K_0[X]-K_0$.

By the above, we have established the existence of the $\mathfrak{p}_0$. Let $R/\mathfrak{p}_0$ be the differential residue ring of R modulo $\mathfrak{p}_0$, and x the residue class of X. Then we see that $R/\mathfrak{p}_0 = K_0\{x\}$ by means of the usual identification of elements of K_0 with their residue classes. Consider the differential field $N = K_0\langle x \rangle$. We see that x is transcendental over K_0 with

$$(\delta_1 x)^2 = a^2(4x^3 - g_2 x - g_3).$$

We get also $\delta_2 x = -a^2 g_2$ and $\delta_{2+3\nu}x = 0$ $(\nu \geq 1)$. Set $\eta_\nu = \delta_{3\nu}x$, $\eta'_\nu = \delta_{1+3\nu}x$ $(\nu \geq 1)$. Then

$$\eta'_\nu \delta_1 x = \Sigma' \eta'_\alpha \eta'_\beta - a^2(\delta_\nu x)^3 + a^2 g_2 \eta_\nu \quad (\nu \geq 1).$$

We see that η_ν $(\nu \geq 1)$ are algebraically independent over $K_0(x, \delta_1 x)$, that $N = K_0(x, \delta_1 x, \eta_\nu | \nu \geq 1)$, and that N is K_0-separable. Let U be a universal differential extension field

of K_0. Then we can regard x, and hence $\delta_1 x$, η_ν, η'_ν $(\nu \geq 1)$ as elements of U.

Moreover, we see that

(1) $\delta_{3m}\eta_\nu = \binom{m+\nu}{m}\eta_{m+\nu}$, $\delta_{1+3m}\eta_\nu = \binom{m+\nu}{m}\eta'_{m+\nu}$, $\delta_{2+3m}\eta_\nu = 0$ $(\nu \geq 1, m \geq 0)$,

that η'_ν $(\nu \geq 1)$ are algebraically independent over $K_0(x, \delta_1 x)$, and that

(2) $\delta_{3m}\eta'_\nu = \binom{m+\nu}{m}\eta'_{m+\nu}$, $\delta_{1+3m}\eta'_\nu = \delta_{2+3m}\eta'_\nu = 0$ $(\nu \geq 1, m \geq 0)$.

Example 2 Let K_0 be a differential field of characteristic 5 with a single derivation $\delta = (\delta_\nu \mid \nu \in \mathbb{N})$, and X a differential polynomial ring $R = K_0\{X\}$ in X over K_0. Let a, g_2, g_3 be three constants of K_0 with $a \neq 0$, $g_2^3 - 27g_3^2 \neq 0$, and set $A = (\delta_1 X)^2 - a^2(4X^3 - g_2 X - g_3) = (\delta_1 X)^2 + a^2(X^3 + g_2 X + g_3)$. Assume that there exists a prime differential ideal $\mathfrak{p}$ of R such that $A \in \mathfrak{p}$ and $\mathfrak{p} \cap (K_0[X] - K_0) = \emptyset$. Then, we see that $\delta_1 A = -\delta_1 X \cdot B$ with $B = \delta_2 X + 2a^2X^2 - a^2 g_2 \in \mathfrak{p}$, that $\delta_1 B = 3(\delta_1 X - 2a^2 X \delta_1 X) \in \mathfrak{p}$, and that $\delta_3 B = -a^2 X \delta_3 X - a^2 \delta_1 X \delta_2 X \in \mathfrak{p}$. From these results we can deduce that $a^4 g_2 \delta_1 X \in \mathfrak{p}$, and this contradicts the assumption provided $g_2 \neq 0$. On the other hand, in case $g_2 = 0$ (whence $g_3 \neq 0$), it is not so far known because of the amount of the necessary calculations whether any prime differential ideal $\mathfrak{p}$ as above exists or not.

CHAPTER 5

Strongly Normal Extensions

5.1. Some properties of differential closure

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$, K_a an algebraic closure of K, and K_Δ the differential closure in K_a of K (see §2.8). In this section, we show some properties (due to Tsuji [11]) of K_Δ which are very useful for discussions from §5.6 forward.

Let K_i be the purely inseparably algebraic closure in K_a of K and set $K_\infty = K_\Delta \cap K_i$. We see immediately that K_∞ is a differential extension field of K which is purely inseparably algebraic over K.

Proposition 1 K_Δ is separably algebraic over K_∞.

Proof. Let x be any element of K_Δ. Since x is algeraic over K_∞, we write the minimal polynomial $f(X)$ of x over K_∞ in the form $f(X) = X^{mp(e)} + a_{m-1}X^{(m-1)p(e)} + \ldots + a_0$ $(a_\alpha \in K_\infty)$ with $e \in \mathbb{N}$ as large as possible. Set $b_\alpha = a_\alpha^{p(-e)} \in K_\infty^{p(-e)}$ $(0 \leq \alpha < m)$ and $g(X) = X^m + b_{m-1}X^{m-1} + \ldots + b_0$. Then $g(X)$ is a separable polynomial over $K_\infty^{p(-e)}$ and $g(x) = 0$.

Assume, for some α $(0 \leq \alpha < m)$, that $b_\alpha \notin K_\Delta$, so that there exists a pair $(i,\nu) \in I \times \mathbb{N}$ with $\nu \not\equiv 0 \pmod{p(e)}$ and $\delta_{i\nu}a_\alpha \neq 0$ (see §2.8). Fix such an element $i \in I$, and set $n = \min(\nu \in \mathbb{N} \mid \nu \not\equiv 0 \pmod{p(e)}, \delta_{i\nu}a_\alpha \neq 0$ for some α with $0 \leq \alpha < m)$. Applying δ_{in} to $0 = f(x) = x^{mp(e)} + \ldots + a_0$, we get

$$0 = \Sigma_{\alpha=0}^{m-1}\Sigma_{\lambda+\mu=n}\delta_{i\lambda}a_{\alpha}\cdot\delta_{i\mu}(x^{\alpha p(e)}) = \Sigma_{\alpha=0}^{m-1}\delta_{in}a_{\alpha}\cdot x^{\alpha p(e)}.$$

This is a contradiction since at least one of $\delta_{in}a_{\alpha}$ $(0 \leq \alpha < m)$ is nonzero.

Therefore, we conclude that $b_{\alpha} \in K_{\Delta}$ for all α $(0 \leq \alpha < m)$, that $b_{\alpha} \in K_{\Delta} \cap K_{\infty}^{p(-e)} \subset K_{\Delta} \cap K_{i} = K_{\infty}$, so that x is separably algebraic over K_{∞}. q.e.d.

For simplicity, let U be a universal differential extension field of K_{Δ} (whence of K), and denote by L in Th.1~Th.3 below a differential subfield of U.

We know that any extension field of K_{a} is regular over K_{a}. Correspondingly we have the following theorem.

Theorem 1 Any differential extension field L of K_{Δ} is regular over K_{Δ}.

Proof. Since K_{Δ} is clearly algebraically closed in L (see §2.8), it suffices to show that L^{p} and K_{Δ} are linearly disjoint over K_{Δ}^{p}. Let $\alpha_{1}, \ldots, \alpha_{n}$ be finitely many elements of L such that $\alpha_{1}^{p}, \ldots, \alpha_{n}^{p}$ are linearly dependent over K_{Δ}. Then we can see by induction on n that $\alpha_{1}^{p}, \ldots, \alpha_{n}^{p}$ are linearly dependent over K_{Δ}^{p}.

We may suppose that $n > 1$, that any $n - 1$ of $\alpha_{1}^{p}, \ldots, \alpha_{n}^{p}$ are linearly independent over K_{Δ}, and that

$$(1) \quad \alpha_{n}^{p} = x_{1}\alpha_{1}^{p} + \ldots + x_{n-1}\alpha_{n-1}^{p}$$

with nonzero $x_{1},\ldots,x_{n-1} \in K_{\Delta}$. Set $y_{j} = x_{j}^{p(-1)} \in K_{a}$ $(1 \leq j \leq n-1)$, and assume that at least one of them, say y_{1}, is not

contained in K_Δ. Then, by §2.8, there exists a pair $(i,\nu) \in I\times\mathbb{N}$ such that $\nu \not\equiv 0 \pmod p$ and $\delta_{i\nu}x_1 \neq 0$. Applying $\delta_{i\nu}$ to (1), we get $0 = \delta_{i\nu}x_1\cdot\alpha_1^p + \ldots + \delta_{i\nu}x_{n-1}\cdot\alpha_{n-1}^p$ (a contradiction). q.e.d.

We know that if L' is a subfield of an extension field of K_i, then the compositum $L'K_i$ is separable over K_i. Correspondingly we have the following theorem.

Theorem 2 For any differential field L (in U), the compositum LK_∞ is a differential extension field of K_∞ which is separable over K_∞.

Proof. Since LK_∞ is clearly a differential extension field of K_∞, we have only to prove that LK_∞ is separable over K_∞. Set $K_0 = K_\Delta \cap (LK_\infty)$. Then, K_Δ is separably algebraic over K_0 (see Prop.1), and K_0 is algebraically closed in LK_∞ (see §2.8); hence LK_∞ and K_Δ are linearly disjoint over K_0 (see Chap.I of [12]). Since LK_Δ is regular over K_Δ (see Th.1), we see (by Chap.I of [12]) that LK_∞ is regular over K_0, so that LK_∞ is separable over K_∞ because K_0 is separably algebraic over K_∞.

Theorem 3 Let σ be a differential isomorphism of K into U, and L a differential extension field of K with $L \subset K_\Delta$. Then σ can be extended to a differential isomorphism of L into U.

Proof. Since L is an algebraic extension field of K,

σ can be extended to a field-isomorphism σ_1 of L into $(\sigma K)_a$ $(\subset U_a)$. We must prove that, for every element x of L, $\sigma_1 x \in U$ and $\delta_{i\nu}\sigma_1 x = \sigma_1 \delta_{i\nu} x$ $(i \in I, \nu \in \mathbb{N})$.

Case I: x is separably algebraic over K. Let $f(X) = \Sigma_{\alpha=0}^{n} a_\alpha X^\alpha$ $(a_\alpha \in K, a_n = 1)$ be the minimal polynomial of x over K, and set $f^\sigma(X) = \Sigma_{\alpha=0}^{n} (\sigma a_\alpha) X^\alpha$. Then $f^\sigma(X)$ is the minimal polynomial of $\sigma_1 x$ over σK, and $\sigma_1 x$ is separably algebraic over the differential subfield σK of U. It is straightforward to show that $\sigma_1 x \in U$ and that $\delta_{i\nu}\sigma_1 x = \sigma_1 \delta_{i\nu} x$ $(i \in I, \nu \in \mathbb{N})$ by (1) of §1.7.

Case II: x is inseparably algebraic over K. Let H be separably algebraic closure of K in L, and σ_2 the restriction of σ_1 to H. Then, by Case I, σ_2 is a differential isomorphism of H into U that extends σ. Let y be any element of L. Since L is purely inseparably algebraic over H, there exists $e \in \mathbb{N}$ which has the property that $y^{p(e)} \in H$ and that $\delta_{i\nu}(y^{p(e)}) = 0$ for all $i \in I$ and for all $\nu \in \mathbb{N}$ with $\nu \not\equiv 0 \pmod{p(e)}$. Therefore

$$(\sigma_1 y)^{p(e)} = \sigma_2(y^{p(e)}) \in \sigma_2 H = \sigma_1 H \subset (\sigma K)_a \subset U_a$$

and $\delta_{i\nu}((\sigma_1 y)^{p(e)}) = \delta_{i\nu}(\sigma_2(y^{p(e)})) = \sigma_2 \delta_{i\nu}(y^{p(e)}) = 0$ for all $i \in I$ and for all $\nu \in \mathbb{N}$ with $\nu \not\equiv 0 \pmod{p(e)}$. Hence, by §2.8, we see that $\sigma_1 y \in U_\Delta = U$ and that

$$\delta_{i\nu}\sigma_1 y = (\delta_{i,\nu p(e)}((\sigma_1 y)^{p(e)}))^{p(-e)}$$
$$= (\delta_{i,\nu p(e)}(\sigma_2(y^{p(e)})))^{p(-e)} = (\sigma_2 \delta_{i,\nu p(e)}(y^{p(e)}))^{p(-e)}$$

$= (\sigma_1 \delta_{i,\nu p(e)} (y^{p(e)})^{p(-e)} = \sigma_1 (\delta_{i,\nu p(e)} (y^{p(e)})^{p(-e)}$

$= \sigma_1 \delta_{i\nu} y \quad (i \in I, \nu \in \mathbb{N})$.

5.2. Conventions

Henceforth, in the general discussion of this chapter, we fix a differential field K and a differential extension field N of K with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ. We suppose always that the field N is finitely separable over K; elements $\xi_1, \ldots, \xi_n$ of N are taken once for all such that $N = K(\xi_1, \ldots, \xi_n)$ (hence $N = K\langle \xi_1, \ldots, \xi_n \rangle$), that $\{\xi_1, \ldots, \xi_{n-1}\}$ is a separating transcendence basis of N over K, and that ξ_n is separably algebraic over $K(\xi_1, \ldots, \xi_{n-1})$. N_a denotes a fixed algebraic closure of N, and N_Δ the differential closure in N_a of N. Let U be a fixed universal differential extension field of N_Δ, hence of N and of K (see §4.2 Lem.1 and Cor. to this lemma). We set $C = N_c$ (the field of constants of N) throughout this chapter. In §5.6, we consider the case where a certain extra conditions are satisfied by N.

L and M denote tacitly various differential extension fields of K over which U is universal.

5.3. Differential isomorphisms

By a differential isomorphism of M we mean always a differential isomorphism of M into U. Exceptionally by mentioning expressly, we deal with differential isomorphism whose image is not necessarily contained in U.

Lemma 1 If M is separably algebraic over L, then every field-isomorphism over L of M into U is a differential isomorphism.

Proof. Let ϕ be a field-isomorphism of M into U over L. It suffices to prove by induction on ν that, for every $x \in M$,

(*) $\phi(\delta_{i\nu}x) = \delta_{i\nu}(\phi x)$ $(i \in I, \nu \in \mathbb{N})$.

In case $\nu = 0$, (*) holds trivially. Suppose $\nu > 0$, and let $f(X) = \Sigma_{k=0}^{m} a_k X^k$ $(a_k \in L, a_m = 1)$ be the minimal polynomial of x over L (hence of ϕx). Then it is straightforward to show (*) by the induction assumption (see (1) of §1.7).

Proposition 2 If M is separably algebraic over L with $M \neq L$, then, for each $x \in M-L$, there exists a differential isomorphism ϕ of M over L such that $\phi x \neq x$.

Proof. There exists a conjugate x' in U of x over L and a field-isomorphism ψ of $L(x) = L\langle x\rangle$ over L onto $L(x') = L\langle x'\rangle$ such that $x' \neq x$ and $\psi x = x'$. By Lem.1, ψ is a differential isomorphism of $L\langle x\rangle$ over L onto $L\langle x'\rangle$.

Since $L \subset M \subset L_s \subset L_\Delta$, we see by Th.3 of §5.1 that ψ can be extended to a differential isomorphism ϕ of M. q.e.d.

Owing to K. Nishioka's suggestion, the hypothesis of the following proposition has been made weaker than that of our original proposition.

Proposition 3 Let ψ be a differential isomorphism of L over K. If L is a finitely generated differential extension field of K and if M is a finitely generated differential extension field of L and separable over L, then ψ can be extended to a differential isomorphism of M.

Proof. Let $\eta_1, \ldots, \eta_m$ be elements of M such that $M = L\langle\eta_1,\ldots,\eta_m\rangle$. Let $\mathfrak{p}$ denote the defining differential ideal of $(\eta) = (\eta_1,\ldots,\eta_m)$ in the differential polynomial ring $L\{Y_1,\ldots,Y_m\}$, and $\mathfrak{p}^\psi$ the prime differential ideal in the differential polynomial ring $(\psi L)\{Y_1,\ldots,Y_m\}$ which consists of all those differential polynomials of $\mathfrak{p}$ by applying ψ to the coefficients. Since $\mathfrak{p}$ is L-separable, $\mathfrak{p}^\psi$ is (ψL)-separable. Let $\zeta_1, \ldots, \zeta_\ell$ be elements of L such that $L = K\langle\zeta_1,\ldots,\zeta_\ell\rangle$. Since $\psi L = K\langle\psi\zeta_1,\ldots,\psi\zeta_\ell\rangle \subset U$, U is a universal differential extension field of ψL by Th.4 of §4.4, and $\mathfrak{p}^\psi$ has a generic zero $(\eta') = (\eta'_1,\ldots,\eta'_m)$ with $\eta'_j \in U$. Thus, we can define a mapping ϕ:

$$M = L\langle\eta_1,\ldots,\eta_m\rangle \to (\psi L)\langle\eta'_1,\ldots,\eta'_m\rangle$$

by the formula $\phi(A(\eta)/B(\eta)) = A^\psi(\eta')/B^\psi(\eta')$, where $A(Y), B(Y) \in L\{Y_1,\ldots,Y_m\}$ with $B(\eta) \neq 0$ and $A^\psi(Y)$, $B^\psi(Y)$ denote differential polynomials obtained from $A(Y)$, $B(Y)$ respectively by applying ψ to the coefficients. It is clear that ϕ is a field-isomorphism of M extending ψ. Now, for any two elements $A(Y), B(Y) \in L\{Y\}$ as above and for any $(i,\nu) \in I\times\mathbb{N}$, we can prove by induction on ν that there exists

$C_{i\nu}(Y) \in L\{Y\}$ such that $\delta_{i\nu}(A(Y)/B(Y)) = C_{i\nu}(Y)/B(Y)^{\nu+1}$. To do this, we use the formula

$$\delta_{i\nu}A(Y) = \delta_{i\nu}(A(Y)/B(Y))\cdot B(Y) + \Sigma_{\lambda=0}^{\nu-1}\delta_{i\nu}(A(Y)/B(Y))\cdot\delta_{i,\nu-\lambda}B(Y) \qquad (i \in I,\ \nu \in \mathbb{N}-\{0\}).$$

By means of this formula, we see easily that

$$\delta_{i\nu}\phi(A(\eta)/B(\eta)) = \phi(\delta_{i\nu}(A(\eta)/B(\eta))) \quad (i \in I,\ \nu \in \mathbb{N}).$$

Thus we conclude that ϕ is a differential isomorphism of M which extends ψ.

5.4. Specializations of differential isomorphisms

This section and the next one are formal reproduction of the corresponding part of Kolchin [4], but they contain some new results (properties of K^0 of §5.4 and part (b) of Prop. 6 of §5.5).

Let $(x_j \mid j \in J)$ and $(x'_j \mid j \in J)$ be two families of elements of U with the same set of indices J. If there exists a differential homomorphism ϕ over K of $K\{x_j \mid j \in J\}$ onto $K\{x'_j \mid j \in J\}$ with $\phi(x_j) = x'_j$ $(j \in J)$, $(x'_j \mid j \in J)$ is called differential specialization of $(x_j \mid j \in J)$ over K.

Lemma 2 Let $(\sigma_\lambda \mid \lambda \in \Lambda)$ and $(\sigma'_\lambda \mid \lambda \in \Lambda)$ be two families of differential isomorphisms of M, both having the same set of indices Λ. Then, the following three conditions are mutually equivalent:

1° The family $(\sigma'_\lambda x \mid \lambda \in \Lambda, x \in M)$ is a differential specialization of the family $(\sigma_\lambda x \mid \lambda \in \Lambda, x \in M)$ over M.

2° The family $(\sigma'_\lambda x \mid \lambda \in \Lambda, x \in M)$ is a specialization of the family $(\sigma_\lambda x \mid \lambda \in \Lambda, x \in M)$ over the field M.

3° The field-isomorphisms $\sigma'_\lambda \sigma_\lambda^{-1}$: $\sigma_\lambda M \xrightarrow{\sim} \sigma'_\lambda M$ $(\lambda \in \Lambda)$ and id_M are compatible, that is, there exists a ring-homomorphism of $M[\cup_{\lambda\in\Lambda}\sigma_\lambda M]$ onto $M[\cup_{\lambda\in\Lambda}\sigma'_\lambda M]$ extending id_M and all $\sigma'_\lambda \sigma_\lambda^{-1}$ $(\lambda \in \Lambda)$.

Proof. Clearly, 1° implies 2°, and 2° implies 3°. Let 3° be satisfied, and let ϕ be a ring-homomorphism of $M[\cup_{\lambda\in\Lambda}\sigma_\lambda M]$ onto $M[\cup_{\lambda\in\Lambda}\sigma'_\lambda M]$ extending id_M and all $\sigma'_\lambda \sigma_\lambda^{-1}$ $(\lambda \in \Lambda)$. Suppose that $A(\sigma_\lambda x \mid \lambda \in \Lambda, x \in M) = 0$ for an element $A(X_{\lambda,x} \mid \lambda \in \Lambda, x \in M)$ of the differential polynomial ring $M\{X_{\lambda,x} \mid \lambda \in \Lambda, x \in M\}$. Then $0 = \phi(A(\sigma_\lambda x \mid \lambda \in \Lambda, x \in M)) = A(\sigma'_\lambda x \mid \lambda \in \Lambda, x \in M)$. Therefore 1° is satisfied. q.e.d.

If $(\sigma_\lambda \mid \lambda \in \Lambda)$ and $(\sigma'_\lambda \mid \lambda \in \Lambda)$ satisfy the conditions of Lem.2, $(\sigma'_\lambda \mid \lambda \in \Lambda)$ is called <u>specialization</u> of $(\sigma_\lambda \mid \lambda \in \Lambda)$. This binary relation in the set of all families of differential isomorphisms of M is reflexive and transitive. We say that $(\sigma'_\lambda \mid \lambda \in \Lambda)$ is <u>generic specialization</u> of $(\sigma_\lambda \mid \lambda \in \Lambda)$ if and only if the former is a specialization of the latter such that the latter is also a specialization of the former.

Let σ, σ' be two differential isomorphisms of M, and σ' a specialization of σ. If $M \supset L$, and if σ is a differential isomorphism of M over L, then so is σ. Also, if

σ is a differential automorphism of M, then $\sigma' = \sigma$.

Lemma 3 Let $M \supset L$, and let $(\eta_j \mid j \in J)$ be a family of elements of M such that $M = L\langle \eta_j \mid j \in J \rangle$. Let $(\sigma_\lambda \mid \lambda \in \Lambda)$ and $(\sigma'_\lambda \mid \lambda \in \Lambda)$ be two families of differential isomorphisms of M over L with the same set of indices Λ. Then, $(\sigma'_\lambda \mid \lambda \in \Lambda)$ is a specialization of $(\sigma_\lambda \mid \lambda \in \Lambda)$ if and only if $(\sigma'_\lambda \eta_j \mid \lambda \in \Lambda, j \in J)$ is a differential specialization of $(\sigma_\lambda \eta_j \mid \lambda \in \Lambda, j \in J)$ over M.

This lemma is obvious.

Lemma 4 If σ' is a specialization of a differential isomorphism σ of N over K, then

$$\mathrm{trdeg}(N \cdot \sigma' N)/N \leq \mathrm{trdeg}(N \cdot \sigma N)/N,$$

and the equality holds if and only if σ' is a generic specialization of σ.

Proof. Let $\mathfrak{p}$ and $\mathfrak{p}'$ be the defining differential ideals in the differential polynomial ring $N\{X_1, \ldots, X_n\}$ of $(\sigma\xi_1, \ldots, \sigma\xi_n)$ and $(\sigma'\xi_1, \ldots, \sigma'\xi_n)$ respectively. Since $\mathfrak{p}' \supset \mathfrak{p}$ by the hypothesis, we see the inequality of the lemma. By Lem. 2 and Lem.3, the specialization σ' of σ is generic if and only if $\mathfrak{p}' = \mathfrak{p}$, and this equality takes place if and only if $\mathrm{trdeg}(N \cdot \sigma' N)/N = \mathrm{trdeg}(N \cdot \sigma N)/N$. q.e.d.

Definition Let $M \supset L$. A differential isomorphism σ of M over L is called isolated over L if there does not exist any differential isomorphism of M over L of which σ is

a nongeneric specialization.

Theorem 4 (a) If σ is a differential isomorphism of N over K, then

$$\operatorname{trdeg}(N\cdot\sigma N)/N \leq \operatorname{trdeg} N/K,$$

and the equality holds if and only if σ is isolated over K.

(b) There exist finitely many isolated differential isomorphisms $\sigma_1, \ldots, \sigma_t$ of N over K such that every differential isomorphism of N over K is a specialization of one and only one of $\sigma_1, \ldots, \sigma_t$. If N is regular over K, then $t = 1$.

Proof. Let $\mathfrak{p}$ be the defining differential ideal of $(\xi_1,\ldots,\xi_n)$ in the differential polynomial ring $K\{X_1,\ldots,X_n\}$, then $\operatorname{trdeg} N/K = \dim \mathfrak{p}$. By Th.7 of §3.8 and Cor. to this theorem, $N\mathfrak{p}$ is a perfect differential ideal of the differential polynomial ring $N\{X_1,\ldots,X_n\}$ with a finite number of finitely N-separable prime differential components $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ (t being 1 if N is K-regular), with $\dim \mathfrak{P}_k = \dim \mathfrak{p}$ $(1 \leq k \leq t)$, every generic zero of each $\mathfrak{P}_k$ $(1 \leq k \leq t)$ is a generic zero of $\mathfrak{p}$, and each generic zero of $\mathfrak{p}$ is a zero of one and only one of $\mathfrak{P}_k$ $(1 \leq k \leq t)$. Let $(\xi_{k1},\ldots,\xi_{kn})$ be a generic zero of $\mathfrak{P}_k$ $(1 \leq k \leq t)$ with $\xi_{kj} \in U$ $(1 \leq j \leq n)$. Then, for each k $(1 \leq k \leq t)$, there exists a differential isomorphism σ_k of $N = K\langle\xi_1,\ldots,\xi_n\rangle$ onto $K\langle\xi_{k1},\ldots,\xi_{kn}\rangle$ over K with $\sigma_k\xi_j = \xi_{kj}$ $(1 \leq j \leq n)$, and $\operatorname{trdeg}(N\cdot\sigma_k N)/N = \operatorname{trdeg}$

N/K. If σ is any differential isomorphism of N over K, then $(\sigma\xi_1,\ldots,\sigma\xi_n)$ is a generic zero of $\mathfrak{p}$ and hence is a zero of a unique $\mathfrak{P}_k$. By Lem.3, σ is a specialization of a unique σ_k. We see that each σ_k $(1 \leq k \leq t)$ is isolated over K, that $\mathrm{trdeg}(N\cdot\sigma N)/N \leq \mathrm{trdeg}\ N/K$, and that the equality takes place if and only if σ is isolated over K (see Lem.4).

Corollary Let σ be a differential isomorphism of N over K. Then, σ is isolated over K if and only if N and σN are algebraically disjoint over K.

Proof. By (a) of Th.4, σ is isolated over K if and only if $\mathrm{trdeg}(N\cdot\sigma N)/N = \mathrm{trdeg}(\sigma N)/K$, that is, if and only if N and σN are algebraically disjoint over K. q.e.d.

Let K^0 denote the algebraic closure of K in N. Since K^0 is separably algebraic over K, K^0 is a differential subfield of N. We claim that K^0 is of finite degree over K, and that N is finitely regular over K^0. If an element κ of K^0 is of degree ℓ over K, it is also of degree ℓ over $K(\xi_1,\ldots,\xi_{n-1})$, hence $[N:K(\xi_1,\ldots,\xi_{n-1})] \geq [K^0(\xi_1,\ldots,\xi_{n-1}):K(\xi_1,\ldots,\xi_{n-1})] = [K^0:K]$. Since $\xi_1, \ldots, \xi_{n-1}$ are algebraically independent over K^0 and ξ_n is separably algebraic over $K^0(\xi_1,\ldots,\xi_{n-1})$, N is finitely regular over K^0. Thus the claim is established.

Proposition 4 Let σ and σ' be differential isomorphisms of N over K such that σ is isolated over K and

$\sigma' K^0 \subset N$ (whence $\sigma' K^0 = K^0$). Then we see as follows:

(a) $N \cap \sigma N = K^0 \cap \sigma K^0$.

(b) σ' is a specialization of σ if and only if σ and σ' coincide on K^0. When this is the case, N and σN are linearly disjoint over K^0.

Proof. (a) Since σ is isolated over K, N and σN are algebraically disjoint over K (see Cor. to Th.4), whence $N \cap \sigma N \subset K^0$. Similarly $N \cap \sigma N \subset \sigma K^0$. Therefore, $N \cap \sigma N = K^0 \cap \sigma K^0$.

(b) Suppose that σ' is a specialization of σ. Then there exists a surjective differential homomorphism $\phi: N\{\sigma K^0\} \to N\{\sigma' K^0\}$ over N with $\phi \sigma \kappa = \sigma' \kappa$ for all $\kappa \in K^0$. Since every element of the differential field σK^0 is algebraic over N, it follows that $N\{\sigma K^0\} = N \cdot \sigma K^0$. Therefore, ϕ is actually a differential isomorphism of $N \cdot \sigma K^0$ onto N over N, whence $\sigma K^0 \subset N$, and, σ and σ' coincide on K^0. Conversely, suppose that σ and σ' coincide on K^0. Then $\sigma K^0 = \sigma' K^0 = K^0$ and $\sigma' \sigma^{-1}$ is a differential isomorphism of σN onto $\sigma' N$ over K^0. Since N and σN are algebraically disjoint over K (whence over K^0), and since N is K^0-regular, N and σN are linearly disjoint over K^0 (see Chap.I of [12]). Therefore, $\sigma' \sigma^{-1}$ can be extended to a surjective ring-homomorphism $N[\sigma N] \to N[\sigma' N]$ over N, hence σ' is a specialization of σ (see Lem.2).

Corollary (a) If $\sigma_1, \ldots, \sigma_t$ are differential isomorphism of N over K having the property stated in part (b)

of Th.4, then the differential field of invariants of σ_1, ... , σ_t is K.

(b) If σ is an isolated differential isomorphism of N over K of which id_N is a specialization, then the differential field of invariants of σ is K^0, and a differential isomorphism σ' of N over K is a specialization of σ if and only if σ' leaves invariant every element of K^0.

Proof. (a) Let $\xi \in N$ be an invariant of σ_1, ... , σ_t. Then $\xi \in K^0$ by part (a) of Prop.4. Since, by Prop.3 of §5.3, every differential isomorphism ψ of K^0 over K can be extended to a differential isomorphism of N, every such ψ leaves ξ invariant (see part (b) of Th.4). Therefore, we conclude by Prop.2 of §5.3 that $\xi \in K$.

(b) This is obvious from part (b) of Prop.4.

5.5. Strong differential isomorphisms

A differential isomorphism σ of N is called strong if it satisfies the following two conditions:

1° σ leaves invariant every element of C.

2° $\sigma N \subset N \cdot U_C$ and $N \subset \sigma N \cdot U_C$ (or, equivalently, $N \cdot U_C = \sigma N \cdot U_C$).

Clearly, every differential automorphism of N over C is strong.

For any differential isomorphism σ of N, let $C(\sigma)$ denote the field of constants of $N \cdot \sigma N$. Under the condition 1°, the first inclusion in 2° is equivalent to the inclusion

$N \cdot \sigma N \subset N \cdot U_C$ which, by Prop.7 of §3.7, is equivalent to the condition $N \cdot \sigma N = N \cdot C(\sigma)$. Similarly, the second inclusion in 2° is equivalent to the condition $N \cdot \sigma N = \sigma N \cdot C(\sigma)$. Therefore, the differential isomorphism σ of N over C is strong if and only if

$$N \cdot C(\sigma) = N \cdot \sigma N = \sigma N \cdot C(\sigma).$$

Proposition 5 If σ is a strong differential isomorphism of N, then

$$\mathrm{trdeg}(N \cdot \sigma N)/N = \mathrm{trdeg}\ C(\sigma)/C.$$

Proof. Since $N \cdot \sigma N = N \cdot C(\sigma)$, this proposition is a consequence of Cor. to Prop.6 of §3.7.

Proposition 6 Let σ be a strong differential isomorphism of N over K. Then we see the followings:

(a) $C(\sigma)$ is a finitely generated extension field of C.

(b) If σ is isolated over K, $C(\sigma)$ is separable over C.

Proof. (a) By Prop.5, $\mathrm{trdeg}(N \cdot \sigma N)/N = \mathrm{trdeg}\ C(\sigma)/C$. Let this transcendence degree be r, and $\gamma_1, \ldots, \gamma_r$ r elements of $C(\sigma)$ which are algebraically independent over C. Then, by Prop.6 of §3.7, these $\gamma_1, \ldots, \gamma_r$ are algebraically independent over N, whence $N \cdot \sigma N$ is algebraic of finite degree, say ℓ, over $N(\gamma_1, \ldots, \gamma_r)$. Hence, every element of $C(\sigma)$ is algebraic of degree $\leq \ell$ over $N(\gamma_1, \ldots, \gamma_r)$, and, again by Prop.6 of §3.7, over $C(\gamma_1, \ldots, \gamma_r)$. Therefore, we see that

$C(\sigma)$ is algebraic of finite degree over $C(\gamma_1,\ldots,\gamma_r)$, so that $C(\sigma)$ is finitely generated over C.

(b) By Cor. to Th.4 of §5.4, the hypothesis implies that N and σN are algebraically disjoint over K. Since $\{\sigma\xi_1, \ldots,\sigma\xi_{n-1}\}$ is a separating transcendence basis of σN over K, and since $\sigma\xi_1, \ldots ,\sigma\xi_{n-1}$ are algebraically independent over N, $N\cdot C(\sigma) = N\cdot\sigma N = N(\sigma\xi_1,\ldots,\sigma\xi_{n-1},\sigma\xi_n)$ is separable over N. Let $\{\gamma_1',\ldots,\gamma_s'\}$ be a finite set of elements of $C(\sigma)$ with $C(\sigma) = C(\gamma_1',\ldots,\gamma_s')$. Since $N\cdot C(\sigma) = N(\gamma_1',\ldots,\gamma_s')$ is separable over N, a separating transcendence basis of $N\cdot C(\sigma)$ over N can be chosen from among the $\gamma_1', \ldots , \gamma_s'$, whence $r \leq s$. We may suppose that $\gamma_1', \ldots , \gamma_r'$ be a separating transcendence basis of $N\cdot C(\sigma)$ over N. Then we see by Prop.6 of §3.7 that every element of $C(\sigma)$ is separably algebraic over $C(\gamma_1',\ldots,\gamma_r')$, so that $C(\sigma)$ is separable over C.

Theorem 5 Each strong differential isomorphism of N can be extended to a unique differential automorphism of $N\cdot U_c$ over U_c. Conversely, the restriction to N of each differential automorphism of $N\cdot U_c$ over U_c is a strong differential isomorphism of N.

Proof. N and U_c are linearly disjoint over C. If σ is any differential isomorphism of N over C, σN and U_c are linearly disjoint over C. Hence σ can be extended to a unique differential isomorphism σ^* of $N\cdot U_c$ onto $\sigma N\cdot U_c$

over U_c. When σ is strong, $\sigma N \cdot U_c = N \cdot U_c$ and σ^* is a differential automorphism of $N \cdot U_c$. The converse is clear. q.e.d.

By virtue of Th.5, the set of all strong differential isomorphisms of N is identified with the set of all differential automorphisms of $N \cdot U_c$ over U_c. Since the latter set has a natural group structure, this identification makes the set of all stromg differential isomorphisms of N a group. If $L \subset N$, the set of all strong differential isomorphisms of N over L is a subgroup of this group, canonically identified with the group of all differential automorphisms of $N \cdot U_c$ over $L \cdot U_c$.

Proposition 7 If σ and τ are strong differential isomorphisms of N, then $C(\sigma) \cdot C(\sigma\tau) = C(\sigma) \cdot C(\tau) = C(\sigma\tau) \cdot C(\tau)$ and $C(\sigma^{-1}) = C(\sigma)$.

Proof. We see that

$$N \cdot C(\sigma) = N \cdot \sigma N = \sigma(\sigma^{-1} N \cdot N) = \sigma(\sigma^{-1} N \cdot C(\sigma^{-1})) = N \cdot C(\sigma^{-1}),$$

hence, by Prop.7 of §3.7, that $C(\sigma) = C(\sigma^{-1})$. Similarly,

$$N \cdot C(\sigma) \cdot C(\sigma\tau) = N \cdot \sigma N \cdot \sigma\tau N = N \cdot \sigma(N \cdot \tau N) = N \cdot \sigma(N \cdot C(\tau))$$

$$= N \cdot \sigma N \cdot C(\tau) = N \cdot C(\sigma) \cdot C(\tau),$$

whence $C(\sigma) \cdot C(\sigma\tau) = C(\sigma) \cdot C(\tau)$. Finally, replacing σ, τ in this equation by τ^{-1}, σ^{-1} respectively, we find that

$$C(\tau^{-1}) \cdot C(\tau^{-1}\sigma^{-1}) = C(\tau^{-1}) \cdot C(\sigma^{-1}),$$

so that $C(\tau) \cdot C(\sigma\tau) = C(\tau) \cdot C(\sigma)$.

Proposition 8 Every specialization σ' of a strong dif-

feretial isomorphism σ of N is strong.

Proof. It suffices to show that $\sigma'\alpha \in N\cdot U_c$ and $\alpha \in \sigma'N\cdot U_c$ for each $\alpha \in N$. Let $\{\beta_\lambda \mid \lambda \in \Lambda\}$ be a linear basis of the field N over C. Since $\sigma\alpha \in N\cdot U_c$, we can write it in the form $\sigma\alpha = \Sigma_{\lambda\in\Lambda'} a_\lambda\beta_\lambda / \Sigma_{\lambda\in\Lambda'} b_\lambda\beta_\lambda$, where $a_\lambda, b_\lambda \in U_c$ with b_λ not all zero and where Λ' is a finite subset of Λ. Therefore, $(\beta_\lambda\cdot\sigma\alpha, \beta_\lambda \mid \lambda \in \Lambda')$ is linearly dependent over U_c. By Th.6 of §3.6, we see that $(\beta_\lambda\cdot\sigma'\alpha, \beta_\lambda \mid \lambda \in \Lambda')$ is linearly dependent over U_c, so that there exist $a'_\lambda, b'_\lambda \in U_c$ not all zero with $\Sigma_{\lambda\in\Lambda'} b'_\lambda\beta_\lambda\cdot\sigma'\alpha - \Sigma_{\lambda\in\Lambda'} a'_\lambda\beta_\lambda = 0$. Since $\Sigma_{\lambda\in\Lambda'} b'_\lambda\beta_\lambda$ can not be zero, $\sigma'\alpha = \Sigma_{\lambda\in\Lambda'} a'_\lambda\beta_\lambda / \Sigma_{\lambda\in\Lambda'} b'_\lambda\beta_\lambda \in N\cdot U_c$. Similarly $\alpha \in \sigma'N\cdot U_c$. q.e.d.

If σ' is a generic specialization of a strong differential isomorphism σ of N, there exists a unique differential isomorphism of $N\cdot\sigma N$ onto $N\cdot\sigma'N$ over N that maps $\sigma\alpha$ onto $\sigma'\alpha$ for every $\alpha \in N$. Restricting this, we get a field-isomorphism $C(\sigma) \underset{\sim}{\to} C(\sigma')$ over C which we call the isomorphism <u>induced</u> by the generic specialization and which is denoted by $S_{\sigma',\sigma}$.

<u>Proposition 9</u> Let σ be a strong differential isomorphism of N.

(a) If σ' is a generic specialization of σ, and σ'' is a generic specialization of σ' (whence of σ), then $S_{\sigma'',\sigma'}\circ S_{\sigma',\sigma} = S_{\sigma'',\sigma}$.

(b) If S is any field-isomorphism over C of $C(\sigma)$

onto a subfield C' of U_C, then there exists a unique generic specialization σ' of σ such that $C(\sigma') = C'$ and $S = S_{\sigma',\sigma}$.

Proof. (a) By hypothesis, there exist differential isomorphisms $N\cdot\sigma N \underset{\rightarrow}{\sim} N\cdot\sigma'N$, $N\cdot\sigma'N \underset{\rightarrow}{\sim} N\cdot\sigma''N$ and $N\cdot\sigma N \underset{\rightarrow}{\sim} N\cdot\sigma''N$, and the composite of the former two isomorphisms is the last one. This implies the conclusion of (a).

(b) $C(\sigma)$ and N are linearly disjoint over C, and so are C' and N. Therefore, S can be extended to a field-isomorphism T over N of $N\cdot C(\sigma)$ onto $N\cdot C'$, and T is a differential isomorphism. If we define a mapping σ' of N into U by the formula $\sigma'\alpha = T(\sigma\alpha)$ $(\alpha \in N)$, then σ' is a differential isomorphism of N over C. We see that T is a differential isomorphism $N\cdot\sigma N \underset{\rightarrow}{\sim} N\cdot\sigma'N$, so that σ' is a generic specialization of σ, $C' = C(\sigma')$ and $S = S_{\sigma',\sigma}$. The uniqueness is clear.

Proposition 10 Let σ, σ', τ, τ' be strong differential isomorphisms of N.

(a) If (σ', τ') is a specialization of (σ, τ), then $(\sigma'^{-1}, \sigma'^{-1}\tau')$ is a specialization of $(\sigma^{-1}, \sigma^{-1}\tau)$.

(b) Suppose that σ' and τ' are generic specializations of σ and τ respectively. If (σ', τ') is a specialization of (σ, τ), then the induced isomorphisms $S_{\sigma',\sigma}$ and $S_{\tau',\tau}$ are compatible, and conversely.

(c) Suppose that σ' and τ' are generic specializa-

tions of σ and τ respectively, and let ϕ: $C' \to C''$ be a homomorphism between subrings of U_C. If ϕ and the induced isomorphisms $S_{\sigma',\sigma}$ and $S_{\tau',\tau}$ are compatible, then σ'^{-1} is a generic specialization of σ^{-1} and $\sigma'^{-1}\tau'$ is a specialization of $\sigma^{-1}\tau$; when the latter specialization is generic, then ϕ and the induced isomorphisms $S_{\sigma'^{-1},\sigma^{-1}}$ and $S_{\sigma'^{-1}\tau',\sigma^{-1}\tau}$ are compatible.

Proof. (a) By hypothesis, there exists a ring-homomorphism f: $N[\sigma N, \tau N] \to N[\sigma' N, \tau' N]$ such that $f(\alpha) = \alpha$, $f(\sigma\alpha) = \sigma'\alpha$, $f(\tau\alpha) = \tau'\alpha$ $(\alpha \in N)$. Define a mapping g of $N[\sigma^{-1}N, \sigma^{-1}\tau N]$ by the formula $g(x) = \sigma'^{-1}(f(\sigma x))$ $(x \in N[\sigma^{-1}N, \sigma^{-1}\tau N])$, then g is a ring-homomorphism

$$N[\sigma^{-1}N, \sigma^{-1}\tau N] \to N[\sigma'^{-1}N, \sigma'^{-1}\tau' N]$$

with $g(\alpha) = \alpha$, $g(\sigma^{-1}\alpha) = \sigma'^{-1}\alpha$, $g(\sigma^{-1}\tau\alpha) = \sigma'^{-1}\tau'\alpha$ $(\alpha \in N)$. Therefore, $(\sigma'^{-1}, \sigma'^{-1}\tau')$ is a specialization of $(\sigma^{-1}, \sigma^{-1}\tau)$.

(b) Suppose that (σ', τ') is a specialization of (σ,τ). Then the homomorphism f above maps $N[\sigma N]$ and $N[\tau N]$ isomorphically onto $N[\sigma' N]$ and $N[\tau' N]$ respectively, and hence can be extended to a ring-homomorphism $N[N\cdot\sigma N, N\cdot\tau N] \to N[N\cdot\sigma' N, N\cdot\tau' N]$. This homomorphism is an extension of $S_{\sigma',\sigma}$ and $S_{\tau',\tau}$. Conversely, suppose that the induced isomorphisms $S_{\sigma',\sigma}$ and $S_{\tau',\tau}$ are compatible, namely there exists a ring-homomorphism $C[C(\sigma),C(\tau)] \to C[C(\sigma'),C(\tau')]$ which extends them. Since N and U_C are linearly disjoint over C, this

homomorphism can be extended to a ring-homomorphism f: $N[C(\sigma), C(\tau)] \to N[C(\sigma'),C(\tau')]$ over N. Since f maps $N[C(\sigma)]$ and $N[C(\tau)]$ isomorphically onto $N[C(\sigma')]$ and $N[C(\tau')]$ respectively, f can be extended to a ring-homomorphism g: $N[N\cdot\sigma N, N\cdot\tau N] \to N[N\cdot\sigma' N, N\cdot\tau' N]$ with $g(\alpha) = \alpha$, $g(\sigma\alpha) = \sigma'\alpha$, $g(\tau\alpha) = \tau'\alpha$ $(\alpha \in N)$. The restriction homomorphism h: $N[\sigma N,\tau N] \to N[\sigma' N,\tau' N]$ satisfies $h(\sigma\alpha) = \sigma'\alpha$ and $h(\tau\alpha) = \tau'\alpha$ $(\alpha \in N)$. Therefore, (σ',τ') is a specialization of (σ,τ).

(c) By hypothesis, there exists a ring-homomorphism $N_c[C',C(\sigma),C(\tau)] \to N_c[C'',C(\sigma'),C(\tau')]$ which extends ϕ, $S_{\sigma',\sigma}$ and $S_{\tau',\tau}$. We see by (b) that (σ',τ') is a specialization of (σ,τ), hence by (a) that $(\sigma'^{-1},\sigma'^{-1}\tau')$ is a specialization of $(\sigma^{-1},\sigma^{-1}\tau)$, so that σ'^{-1} and $\sigma'^{-1}\tau'$ are specializations of σ^{-1} and $\sigma^{-1}\tau$ respectively. Since σ' is a generic specialization of σ, we see by (a) that σ'^{-1} is a generic specialization of σ^{-1}. To prove the last assertion of (c), suppose that $\sigma'^{-1}\tau'$ is also a generic specialization of $\sigma^{-1}\tau$. Define a mapping k of $N[C',\sigma^{-1}N,\sigma^{-1}\tau N]$ by the formula $k(x) = \sigma'^{-1}(h(\sigma x))$ $(x \in N[C',\sigma^{-1}N,\sigma^{-1}\tau N])$, where h is the ring-homomorphism $N[C',\sigma N,\tau N] \to N[C'',\sigma' N,\tau' N]$ over N obtained in the manner similar to the proof of (b) and extending ϕ. Then, k is a ring-homomorphism $N[C',\sigma^{-1}N,\sigma^{-1}\tau N] \to N[C'',\sigma'^{-1}N,\sigma'^{-1}\tau' N]$ over N extending ϕ such that $k(\sigma^{-1}\alpha) = \sigma'^{-1}\alpha$, $k(\sigma^{-1}\tau\alpha) = \sigma'^{-1}\tau'\alpha$ $(\alpha \in N)$, and that k maps $N[\sigma^{-1}N]$ and $N[\sigma^{-1}\tau N]$ isomorphically onto $N[\sigma'^{-1}N]$ and

$N[\sigma'^{-1}\tau'N]$ respectively. This k can be extended to a ring-homomorphism $N[C',N\cdot\sigma^{-1}N,N\cdot\sigma^{-1}\tau N] \to N[C'',N\cdot\sigma'^{-1}N,N\cdot\sigma'^{-1}\tau'N]$, which is a common extension of ϕ, $S_{\sigma'^{-1},\sigma^{-1}}$ and $S_{\sigma'^{-1}\tau',\sigma^{-1}\tau}$

Corollary (a) If σ' is a specialization of the strong differential isomorphism σ of N, then σ'^{-1} is a specialization of σ^{-1}. When the former specialization is generic, then so is the latter, and $S_{\sigma',\sigma} = S_{\sigma'^{-1},\sigma^{-1}}$.

(b) If σ' and τ' are generic specializations of the strong differential isomorphisms σ and τ of N respectively such that $S_{\sigma',\sigma}$ and $S_{\tau',\tau}$ are compatible, then $\sigma'\tau'$ is a specialization of $\sigma\tau$. When the last specialization is generic, and $\phi: C' \to C''$ is a homomorphism between subrings of U_C such that ϕ, $S_{\sigma',\sigma}$ and $S_{\tau',\tau}$ are compatible, then ϕ and $S_{\sigma'\tau',\sigma\tau}$ are compatible.

Proof. (a) This follows from Prop.8, parts (a) and (c) of Prop.10 and Prop.7.

(b) By part (a) of this corollary, we may replace σ, σ' by σ^{-1}, σ'^{-1} in part (c) of Prop.10.

5.6. Strongly normal extensions and Galois groups

We call N strongly normal extension of K if every differential isomorphism of N over K is strong. (See Examp.1 of §5.8 below.)

Proposition 11 If N is strongly normal over K, then $C = K_C$.

Proof. By the hypothesis and 1° of §5.5, elements of C are invariant under every differential isomorphism of N over K. We see by part (a) of Cor. to Prop.4 of §5.4 that $C \subset K$.

Proposition 12 Suppose that $C = K_c$, and let $\sigma_1, \ldots, \sigma_t$ be differential isomorphisms of N over K having the property described in part (b) of Th.4 of §5.4. If $\sigma_k N \subset N \cdot U_c$ $(1 \leq k \leq t)$, then N is strongly normal over K.

Proof. Let σ be any one of $\sigma_1, \ldots, \sigma_t$. We get $\sigma N \subset N \cdot C(\sigma)$ by the beginning part of the proof of Prop.8 of §5.5. By Cor. to Th.4 of §5.4, N and σN are algebraically disjoint over K; hence $\xi_1, \ldots, \xi_{n-1}$ are algebraically independent over σN, and ξ_n is separably algebraic over $(\sigma N)(\xi_1, \ldots, \xi_{n-1})$. Therefore, $N \cdot \sigma N = (\sigma N)(\xi_1, \ldots, \xi_n)$ is finitely separable over σN, and we see by Prop.3 of §5.3 that the differential isomorphism $\sigma^{-1}: \sigma N \underset{\rightarrow}{\sim} N$ can be extended to a differential isomorphism ϕ of $N \cdot \sigma N$ into U. Let τ denote the restriction of ϕ to N, then τ is a differential isomorphism of N over K. Thus we get a differential isomorphism $\phi: N \cdot \sigma N \underset{\rightarrow}{\sim} \tau N \cdot N$ over K with $\phi N = \tau N$, $\phi(\sigma N) = N$ and $\phi(C(\sigma)) = C(\tau)$. Since τ is a specialization of one of $\sigma_1, \ldots, \sigma_t$, we get $\tau N \subset N \cdot C(\tau)$ similarly as in the beginning of this proof; hence

$$N = \phi^{-1}(\tau N) \subset \phi^{-1}(N \cdot C(\tau)) = \phi^{-1} N \cdot \phi^{-1}(C(\tau)) = \sigma N \cdot C(\sigma).$$

Therefore, we see that every one of $\sigma_1, \ldots, \sigma_t$ is strong, and by Prop.8 of §5.5 that every differential isomorphism of

N over K is strong.

Proposition 13 Suppose that N is strongly normal over K. If σ is a differential isomorphism of N over K, $C(\sigma)$ is a finitely generated extension field of K_c. Moreover, if σ is isolated over K, $C(\sigma)$ is finitely separable over K_c.

Proof. Since $C = K_c$ by Prop.11, this follows immediately from Prop.6 of §5.5.

Theorem 6 Let N be strongly normal over K, and G the set of all differential isomorphisms of N over K. For two elements $\sigma,\sigma' \in G$, let $\sigma \to \sigma'$ mean that σ' is a specialization of σ; when $\sigma \leftrightarrow \sigma'$ (that is, when σ' is a generic specialization of σ), let $S_{\sigma',\sigma}$ denote the induced isomorphism $C(\sigma) \xrightarrow{\sim} C(\sigma')$. These data define on G a pre-C-set structure relative to the universal field U_c in the sense of Chap.V of [4]. This pre-C-set structure of G and the group structure of G introduced in §5.5, define on G a C-group structure. The dimension of the C-group G equals the transcendence degree of N over K.

Proof. It is necessary to verify the axioms of §§2~3 of Chap.V of [4]. For any $\sigma \in G$, $C(\sigma)$ is by Prop.13 a finitely generated extension field of C in U_c. The relation $\sigma \to \sigma'$ is reflexive and transitive by §5.4. For each pair $\sigma,\sigma' \in G$ with $\sigma \leftrightarrow \sigma'$, associate the field-isomorphism $S_{\sigma',\sigma}$ over C. By Lem.4 of §5.4, Prop.5 of §5.5, part (b) of Th.4 of

§5.4 and part (b) of Prop.6 of §5.5, axiom AS1 holds true. Axiom AS2 follows from Prop.9 of §5.5. Therefore, G has a pre-C-set structure relative to the universal field U_c.

Axiom AG1 follows from Prop.7 of §5.5. By part (c) of Prop.10 of §5.5 and part (a), (b) of Cor. to that proposition, axioms AG2 (a) and (c) are established. Axioms AG2 (b) and (d) will be verified in the next paragraph. To prove axiom AG3, suppose that σ is an isolated differential isomorphism of N over K with $\sigma \to id_N$; we must show that $C(\sigma)$ is C-regular. But, N is regular over K^0 (see §5.4), and so is σN over σK^0. Moreover, we see, by part (b) of Prop. 4 of §5.4 applied to σ and id_N, that $\sigma K^0 = K^0$ and that N and σN are linearly disjoint over K^0. Therefore, $N \cdot \sigma N = N \cdot C(\sigma)$ is N-regular (see Chap.I of [12]). Then we see that $C(\sigma)$ is C-regular, because N and $C(\sigma)$ are linearly disjoit over C (see also Chap.I of [12]).

Now, to prove axioms AG2 (b) and (d), let $\sigma,\tau,\sigma',\tau' \in G$ with $\sigma \to \sigma'$ and $\tau \to \tau'$. Let $\mathfrak{p}$ respectively $\mathfrak{q}$ denote the defining differential ideals of $\sigma^{-1}\xi_1, \ldots, \sigma^{-1}\xi_n$ respectively $\tau\xi_1, \ldots, \tau\xi_n$ in the differential polynomial rings $N\{Y_1,\ldots,Y_n\}$ respectively $N\{Z_1,\ldots,Z_n\}$ over N. Then, by Th.7 of §3.8 and by Th.1 of §5.1, $N_\Delta\mathfrak{p}$ and $N_\Delta\mathfrak{q}$ have finitely N_Δ-regular components, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ respectively. Each differential ideal $\mathfrak{r}_{\alpha\beta} = (\mathfrak{p}_\alpha, \mathfrak{q}_\beta)$ $(1 \le \alpha \le r, 1 \le \beta \le s)$ of the differential polynomial ring $N_\Delta\{Y_1, \ldots,Y_n,Z_1,\ldots,Z_n\}$ is prime and N_Δ-regular (see Prop.1 of

§4.1), and therefore has a generic zero $(\eta_1^{(\alpha,\beta)},\ldots,\eta_n^{(\alpha,\beta)}, \zeta_1^{(\alpha,\beta)},\ldots,\zeta_n^{(\alpha,\beta)})$ with $\eta_j^{(\alpha,\beta)},\zeta_j^{(\alpha,\beta)} \in U$, where $(\eta_1^{(\alpha,\beta)}, \ldots,\eta_n^{(\alpha,\beta)})$ is a generic zero of $r_{\alpha\beta}\cap N_\Delta\{Y_1,\ldots,Y_n\} = p_\alpha$ and of $p_\alpha\cap N\{Y_1,\ldots,Y_n\} = p$, hence $(\eta_1^{(\alpha,\beta)},\ldots,\eta_n^{(\alpha,\beta)})$ is a generic differential specialization of $(\sigma^{-1}\xi_1,\ldots,\sigma^{-1}\xi_n)$ over N and over K. Therefore, there exists a strong differential isomorphism $\sigma_{\alpha\beta}^{-1}$ of N over K with $\sigma_{\alpha\beta}^{-1}\xi_j = \eta_j^{(\alpha,\beta)}$ $(1 \le j \le n)$. By Lem.3 of §5.4, we see that $\sigma^{-1} \leftrightarrow \sigma_{\alpha\beta}^{-1}$. Similarly, there exists a strong differential isomorphism $\tau_{\alpha\beta}$ of N over K such that $\tau_{\alpha\beta}\xi_j = \zeta_j^{(\alpha,\beta)}$ $(1 \le j \le n)$ and $\tau \leftrightarrow \tau_{\alpha\beta}$. By hypothesis, we see that $\sigma^{-1} \to (\sigma')^{-1}$ (see part (a) of Cor. to Prop.10 of §5.5), so that $((\sigma')^{-1}\xi_1,\ldots,(\sigma')^{-1}\xi_n)$ is a zero of p and hence of some p_α, and similarly, that $(\tau'\xi_1,\ldots,\tau'\xi_n)$ is a zero of some q_β. Thus, for some pair (α,β), $((\sigma')^{-1}\xi_1,\ldots,(\sigma')^{-1}\xi_n,\tau'\xi_1,\ldots,\tau'\xi_n)$ is a zero of $r_{\alpha\beta}$, that is, a differential specialization of $(\sigma_{\alpha\beta}^{-1}\xi_1,\ldots, \sigma_{\alpha\beta}^{-1}\xi_n,\tau_{\alpha\beta}\xi_1,\ldots,\tau_{\alpha\beta}\xi_n)$ over N_Δ and hence over N. By Lem.3 of §5.4, $(\tau',(\sigma')^{-1})$ is a specialization of $(\tau_{\alpha\beta},\sigma_{\alpha\beta}^{-1})$. Therefore, by Prop.10 of §5.5, $((\tau')^{-1},(\tau')^{-1}(\sigma')^{-1})$ is a specialization of $(\tau_{\alpha\beta}^{-1},\tau_{\alpha\beta}^{-1}\sigma_{\alpha\beta}^{-1})$, and $\sigma_{\alpha\beta}\tau_{\alpha\beta} \to \sigma'\tau'$. Moreover, $\sigma_{\alpha\beta}$ and $\tau_{\alpha\beta}$ are quasi-independent over C in the sense of [4]; and, if $\sigma_{\alpha\beta}\tau_{\alpha\beta} \leftrightarrow \sigma'\tau'$ and $\tau_{\alpha\beta} \leftrightarrow \tau'$, then the induced isomorphism $C(\sigma_{\alpha\beta}\tau_{\alpha\beta}) \xrightarrow{\sim} C(\sigma'\tau')$ and $C(\tau_{\alpha\beta}) \xrightarrow{\sim} C(\tau')$ are compatible. This proves axiom AG2 (b), and also (d) because $\sigma^{-1} \to (\sigma')^{-1}$ whenever $\sigma \to \sigma'$. Thus G is established as a C-group.

Finally, let σ be a C-generic element of the C-component G^0 containing id_N of G, namely, an isolated differential isomorphism of N over K with $\sigma \to id_N$. Since N and $C(\sigma)$ are linearly disjoint over C (see Cor.2 to Th.6 of §3.6), and N and σN are algebraically disjoint over K (see Cor. to Th.4 of §5.4),

$$\text{trdeg } C(\sigma)/C = \text{trdeg}(N\cdot C(\sigma))/N$$

$$= \text{trdeg}(N\cdot\sigma N)/N = \text{trdeg } N/K.$$

This completes the proof of the theorem. q.e.d.

By this theorem, the set of strong differential isomorphisms over K of the strongly normal extension N of K has a natural structure of C-group relative to the universal field U_C. This C-group is called Galois group of N over K, and denoted by G(N/K), and its component of the identity by $G^0(N/K)$.

Proposition 14 Let N be strongly normal over K. Let C' be an extension field of C in U_C such that U is universal over $(NC')_\Delta$. Then NC' is a strongly normal extension of KC' with field of constants C', and the C'-group G(NC'/KC') is the induced C'-group of the C-group G(N/K), both these groups being identified with each other by means of their canonical identification with the group of differential automorphisms of $N\cdot U_C$ over $K\cdot U_C$.

Remark We can see that there exist fields C' satisfying

the hypothesis of Prop.14. Since the field of constants of N_Δ is an algebraic closure C_a of C (see the end of §2.8), we get $N \cdot C_a \subset N_\Delta$ and $(N \cdot C_a)_\Delta = N_\Delta$. Hence U is universal over $(N \cdot C_a)_\Delta$. Moreover, let $\gamma_1, \ldots, \gamma_r$ be finitely many elements of U_c, and C' any subfield of $C_a(\gamma_1, \ldots, \gamma_r)$. Then $NC' \subset (N \cdot C_a)(\gamma_1, \ldots, \gamma_r) \subset (N \cdot C_a)_\Delta(\gamma_1, \ldots, \gamma_r) = N_\Delta(\gamma_1, \ldots, \gamma_r)$. Therefore, by Th.4 of §4.4, we see that U is universal over NC'.

Proof of Prop.14. We see by Prop.6 of §3.7 that N and KC' are linearly disjoint over K. Hence NC' is finitely separable over KC'. To prove that NC' is strongly normal over KC', let σ be any differential isomorphism of NC' over KC' into U. Since the restriction of σ to N is strong, $\sigma(NC') = \sigma N \cdot \sigma C' \subset N \cdot U_c \cdot \sigma C' \subset NC' \cdot U_c$, and similarly $NC' \subset \sigma(NC') \cdot U_c$. Therefore, NC' is strongly normal over KC'. Hence we see by Prop.11 that $(NC')_c = (KC')_c$ and by Prop.7 of §3.7 that $(NC')_c = C'$.

Identify σ with the differential automorphism of $NC' \cdot U_c = N \cdot U_c$ over $KC' \cdot U_c = K \cdot U_c$ that extends σ, and hence also with the strong differential isomorphism of N over K to which σ restricts. If we denote by $C'(\sigma)$ the field of constants of $NC' \cdot \sigma(NC')$, we find that $N \cdot C'(\sigma) = NC' \cdot C'(\sigma) = NC' \cdot \sigma(NC') = N \cdot \sigma N \cdot C' = N \cdot C(\sigma) \cdot C'$, whence $C'(\sigma) = C(\sigma) \cdot C'$ by Prop.7 of §3.7. If σ' is a specialization of σ in $G(NC'/KC')$, then $(\sigma'\alpha \mid \alpha \in N)$ is a differential specialization of

$(\sigma\alpha \mid \alpha \in N)$ over NC', hence over N, and σ' is a specialization of σ in $G(N/K)$. When the specialization in $G(NC'/KC')$ is generic, there exists a differential isomorphism $NC'\cdot\sigma N \xrightarrow{\sim} NC'\cdot\sigma' N$ over NC' mapping $\sigma\alpha$ onto $\sigma'\alpha$ for every $\alpha \in N$, and this restricts to a differential isomorphism $N\cdot\sigma N \xrightarrow{\sim} N\cdot\sigma' N$ over N, and the specialization in $G(N/K)$ is generic. The induced isomorphism $S_{\sigma',\sigma}^{C'}: C'(\sigma) \xrightarrow{\sim} C'(\sigma')$ is a restriction of the former of two differential isomorphisms above, and the induced isomorphism $S_{\sigma',\sigma}^{C}: C(\sigma) \xrightarrow{\sim} C(\sigma')$ is a restriction of the latter, and hence $S_{\sigma',\sigma}^{C'}$ is an extension of $S_{\sigma',\sigma}^{C}$. This shows that the identification mapping $G(NC'/KC') \to G(N/K)$ is a (C',C)-homomorphism in the sense of §5 of Chap.V of [4].

Now, let H be any C'-group relative to the universal field U_C and $f: H \to G(N/K)$ a (C',C)-homomorphism. To complete the proof of the proposition, we must show that f is a C'-homomorphism of H into $G(NC'/KC')$. For any $y \in H$, $C'(y) \supset C(f(y))$ because f is a (C',C)-homomorphism, hence $C'(y) \supset C(f(y))C' = C'(f(y))$ by the above. If $y \leftrightarrow y'$ in H, then $f(y) \leftrightarrow f(y')$ in $G(N/K)$ and $S_{y',y}^{C'}$ extends $S_{f(y'),f(y)}^{C}$ and hence $S_{f(y'),f(y)}^{C}$ and $id_{C'}$ are bicompatible. Since N and $C[C(f(y)),C']$ are linearly disjoint over C, as are N and $C[C(f(y')),C']$, it follows that id_N, $S_{f(y'),f(y)}^{C}$, $id_{C'}$ are bicompatible, and hence that there exists a differential isomorphism $N\cdot C(f(y))\cdot C' \xrightarrow{\sim} N\cdot C(f(y'))\cdot C'$ over NC' extending $S_{f(y'),f(y)}^{C}$, that is, a differential iso-

morphism $NC'\cdot f(y)(NC') \simeq NC'\cdot f(y')(NC')$ over NC' that maps $f(y)\alpha$ onto $f(y')\alpha$ for every $\alpha \in N$. Therefore, $f(y) \leftrightarrow f(y')$ in $G(NC'/KC')$ and $S^{C'}_{y',y}$ extends $S^{C'}_{f(y'),f(y)}$. It follows that f is a C'-homomorphism.

5.7. The fundamental theorems

The conventions stated in §5.2 still work in this section. If $L \subset M$, we denote by $G(M/L)$ the set of all differential isomorphisms over L of M into U although $G(M/L)$ has not necessarily a group structure. Moreover, N is always supposed strongly normal over K.

Lemma 5 Let $N \supset M$ and let L be purely inseparably algebraic over M. Then, U is also a universal differential extension field of NL, and $G(NL/L)$ is canonically identified with $G(N/M)$.

Proof. Since $NL \subset N_\Delta$, we see by Cor. to Lem.1 of §4.2 that U is a universal differential extension field of NL, and by Th.3 of §5.1 that each differential isomorphism σ in $G(N/M)$ can be extended to a differential isomorphism σ' in $G(NL/M)$. This σ' is uniquely determined by σ because NL is purely inseparably algebraic over N. It is now clear that $G(NL/M)$ can be identified with $G(NL/L)$. q.e.d.

We use in this section the notation $M_\infty = M_\Delta \cap M_i$ introduced in §5.1.

Lemma 6 If $N \supset M$, then $N\cdot M_\infty$ is strongly normal over

M_∞, and the Galois group $G(NM_\infty/M_\infty)$ is identified with $G(N/M)$ which is a C-closed subgroup of the Galois group $G(N/M)$.

Proof. It is clear by Lem.5 that U is a universal differential extension field of NM_∞ and that $G(NM_\infty/M_\infty) = G(N/M)$. By Th.2 of §5.1, NM_∞ is finitely separable over M_∞. Let σ be any element of $G(NM_\infty/M_\infty)$. Since $\sigma \in G(N/M) \subset G(N/K)$, we see by Th.5 of §5.5 that σ can be uniquely extended to a differential automorphism of $N \cdot U_C$ over U_C, hence that σ leaves invariant every constant of NM_∞, and that

$$\sigma(NM_\infty) = \sigma N \cdot M_\infty \subset NU_C M_\infty = (NM_\infty)U_C ,$$

$$NM_\infty \subset (\sigma N)U_C M_\infty = \sigma(NM_\infty)U_C .$$

Therefore, NM_∞ is strongly normal over M_∞.

Since $M_C = C$, we see that $(M_\Delta)_C = C_a$ and $C_i \subset M^{p(-\infty)}$, so that $C_i \subset (M_\Delta \cap M^{p(-\infty)})_C = (M_\infty)_C$. Conversely, let $\gamma \in (M_\infty)_C$. Then, there exists $e \in \mathbb{N}$ with $\gamma^{p(e)} \in M$, whence $\gamma^{p(e)} \in M_C = C$ and $(M_\infty)_C \subset C_i$. Thus we get $(M_\infty)_C = C_i$. Therefore, by Th.6 of §5.6, $G(NM_\infty/M_\infty)$ is a C_i-group, and it is now clear that $G(N/M)$ is a C-closed subgroup of the C-group $G(N/K)$ (see Chap.V of [4]).

Lemma 7 Let H be a C-subgroup of $G(N/M)$. Let L and L' be the fields of invariants in N and $N \cdot C_s$ of H respectively. Then

(a) L' and N are linearly disjoint over L.

(b) $L' = L \cdot C_s$.

Proof. (a) Let $y_1, \ldots, y_{s+1}$ be finitely many elements of L' that are linearly dependent over N. We have to show that they are linearly dependent over L. For this object, suppose as we may that any s of $y_1, \ldots, y_{s+1}$ are linearly independent over N. There exist nonzero elements $\alpha_1, \ldots, \alpha_s$ of N such that $y_{s+1} = \Sigma_{k=1}^{s} \alpha_k y_k$.

Case I: $\sigma\alpha_k = \alpha_k$ $(1 \leq k \leq s)$ for every $\sigma \in H_{C_s}$ (the set of all elements of H that are rational over C_s). Set $H' = \{\tau \in G(N/K) \mid \tau\alpha_k = \alpha_k (1 \leq k \leq s)\} = G(N/K<\alpha_1, \ldots, \alpha_s>)$. We see by Lem.6 that H' is a C-closed subgroup of $G(N/K)$. Since $H_{C_s} \subset H'$ and since H_{C_s} is dense in H (see Chap.V of [4]), we conclude that $H \subset H'$, that $\sigma\alpha_k = \alpha_k$ $(1 \leq k \leq s)$ for every $\sigma \in H$, so that $\alpha_k \in L$ $(1 \leq k \leq s)$.

Case II: There exist $\sigma_0 \in H_{C_s}$ and $k(0)$ $(1 \leq k(0) \leq s)$ such that $\sigma_0\alpha_{k(0)} \neq \alpha_{k(0)}$. Suppose $k(0) = 1$ as we may. Since $y_{s+1} = \sigma_0 y_{s+1} = \Sigma_{k=1}^{s} \sigma_0\alpha_k y_k$ (whence $\Sigma_{k=1}^{s} (\sigma_0\alpha_k - \alpha_k) y_k = 0$), ans since $\sigma_0\alpha_1 - \alpha_1 \neq 0$, we get

(1) $\Sigma_{k=1}^{s} \beta_k y_k = 0$

with $\beta_k = (\sigma_0\alpha_k - \alpha_k)/(\sigma_0\alpha_1 - \alpha_1) \in N \cdot \sigma_0 N = N \cdot C(\sigma_0)$ $(1 \leq k \leq s)$. Now, $C(\sigma_0) \subset C_s$, and there exists $\gamma \in C_s$ such that $C(\sigma_0) = C(\gamma)$. Let $\gamma_1, \ldots, \gamma_t$ $(t=[C(\sigma_0):C])$ be all the conjugates in U of γ over C. For each h $(1 \leq h \leq t)$, a field-isomorphism ϕ_h of $C(\sigma_0)$ over C is determined with $\phi_h(\gamma) = \gamma_h$, and there exists a unique $\sigma_h \in G(N/K)$ with $\sigma_0 \leftrightarrow \sigma_h$

such that $C(\sigma_h) = C(\gamma_h)$ and $\phi_h = S_{\sigma_h,\sigma_0}^{C}$. We see by Prop.14 of §5.7 that $\sigma_h \in G(NC_s/KC_s)$, so that $\sigma_h y_k = y_k$ $(1 \leq h \leq t, 1 \leq k \leq s)$.

Since N and U_c are linearly disjoint over C, $N \cdot C(\sigma_0)$ is finitely separably algebraic over N with $[N \cdot C(\sigma_0) : N] = t$, and $N \cdot C(\sigma_h)$ $(1 \leq h \leq t)$ are all the conjugates of $N \cdot C(\sigma_0)$ over N, and, for each element ω of $N \cdot C(\sigma_0)$, $\sigma_h \omega$ $(1 \leq h \leq t)$ are all the conjugates of ω over N. Now, we see by the above the existence of an element α of $N \cdot C(\sigma_0)$ such that

(2) $\Sigma_{h=1}^{t} \sigma_h \alpha \neq 0$.

Multiplying (1) by such an element α and applying σ_h, we get $\Sigma_{k=1}^{s} \sigma_h(\alpha\beta_k) y_k = 0$ $(1 \leq h \leq t)$ and

$$\Sigma_{k=1}^{s} (\Sigma_{h=1}^{t} \sigma_h(\alpha\beta_k)) y_k = 0$$

with $\Sigma_{h=1}^{t} \sigma_h(\alpha\beta_k) \in N$ $(1 \leq k \leq s)$; and this implies by (2) that $y_1, \ldots, y_s$ are linearly dependent over N. This contradiction shows that Case II never takes place.

(b) Let $(c_\lambda \mid \lambda \in \Lambda)$ be a family of elements of C_s that makes a linear basis of $N \cdot C_s$ over N. Let y be any element of L', and write y in the form $y = \Sigma_{\lambda \in \Lambda} \nu_\lambda c_\lambda$ with $\nu_\lambda \in N$. Then y and c_λ $(\lambda \in \Lambda)$ are linearly dependent over N; hence, by part (a), they are linearly dependent over L. Thus we see $L' \subset L \cdot C_s$.

Theorem 7 (a) Suppose $M \subset N$. Then $G(N/M)$ is a C-closed subgroup of $G(N/K)$. If L is the field of invariants

in N of $G(N/M)$, L is the purely inseparably algebraic closure in N of M and $G(N/M) = G(N/L)$.

(b) Suppose H a C-closed subgroup of $G(N/K)$. If L is the field of invariants in N of H, then L is purely inseparably algebraically closed in N and $H = G(N/L)$.

Remark In order that Th.7 should have the usual formulation of the fundamental theorem of Galois theory, some extra condition is necessary as we see in Examp.2 of §5.8 below. The condition $C = C_i$ in Cor. to Th.7 is such a condition.

Proof of Th.7. (a) We see by Lem.6 that NM_∞ is strongly normal over M_∞, that $G(NM_\infty/M_\infty) = G(N/M)$, that this is a C-closed subgroup of $G(N/K)$, and by part (a) of Cor. to Prop.4 of §5.4 that M_∞ is the field of invariants of $G(NM_\infty/M_\infty)$. Therefore, we see that $L \subset N \cap M_\infty \subset N \cap M_i$, that $L \supset N \cap M_i$, so that $L = N \cap M_i$, namely that L is the purely inseparably algebraic closure in N of M, and that $G(N/M) = G(N/L)$.

(b) It is clear that L is purely inseparably closed in N.

Case I: $C = C_s$. Since $H \subset G(N/L)$, it suffices to show that the assumption $H \neq G(N/L)$ leads to a contradiction. Let us fix C-generic elements $\sigma_1, \ldots, \sigma_r$ of the C-components of H. By the assumption above, there exists $\tau \in G(N/L)-H$ such that τ is not a specialization of any one of $\sigma_1, \ldots, \sigma_r$. For each k $(1 \leq k \leq r)$, there exists an element $F_k(X) = F_k(X_1,\ldots,X_n)$ of the differential polynomial ring $N\{X_1,\ldots,$

$X_n\}$ over N such that $F_k(\sigma_k\xi) = 0$ and $F_k(\tau\xi) \neq 0$. The product $\Pi_{k=1}^{r} F_k(X)$ is a differential polynomial of $N\{X_1,\ldots,X_n\}$ that vanishes at $(\sigma\xi)$ for every $\sigma \in H$, but that does not vanish at $(\tau\xi)$. Among such differential polynomials, let $F(X)$ have the least number of terms; suppose as we may that one of the coefficients of $F(X)$ is 1. Let $\rho \in H_C$ and denote by $F^\rho(X)$ the polynomial of $N\{X_1,\ldots,X_n\}$ obtained from $F(X)$ by applying ρ to the coefficients. Then $F^\rho(\sigma\xi) = \rho F(\rho^{-1}\sigma\xi) = 0$ $(\sigma \in H)$; hence $F - F^\rho$ vanishes at $(\sigma\xi)$ for every $\sigma \in H$ and has less number of terms than F. Therefore, if $\alpha \in N$, $F - \alpha(F - F^\rho)$ vanishes at $(\sigma\xi)$ for every $\sigma \in H$, but it does not vanish at $(\tau\xi)$. If $F - F^\rho$ were not zero, we could choose α such that $F - \alpha(F - F^\rho)$ had less number of terms than F. Thus we have established that $F - F^\rho = 0$ for every $\rho \in H_C$. Let $a_1, \ldots, a_s$ be the coefficients of F, and set $H' = G(N/K\langle a_1,\ldots,a_s\rangle)$. Then $H' \supset H_C$ and H' is a C-closed subgroup of $G(N/K)$ (see (a)). Since $C = C_s$ and since H_C is dense in H by Chap.V of [4], we get $H' \supset H$. Therefore, $F = F^\sigma$ for every $\sigma \in H$, and $a_k \in L$ $(1 \leq k \leq s)$, and $F = F^\omega$ for every $\omega \in G(N/L)$. This implies that $F(\tau\xi) = F^\tau(\tau\xi) = \tau F(\xi) = 0$ contradicting the above.

Case II: C is not necessarily equal to C_s. H is a C-closed subgroup of $G(N/K)$, that is, a subgroup which is a C_i-subset of $G(N/K)$. Hence H is a C_a-subset of the C_a-group $G(NC_a/KC_a) = G(N/K)$ (see Prop.14 of §5.6). Since $C_a = (C_a)_s$,

if we denote by L' the field of invariants in NC_a of H, we see by Case I that $H = G(NC_a/L')$.

We claim here that NC_a is separable over L'. Let $y_1, \dots, y_{s+1}$ be elements of L' which are linearly dependent over $(NC_a)^p$. We have to show that they are linearly dependent over $(L')^p$. We suppose, as we may, that any s of them are linearly independent over $(NC_a)^p$, and that

$$(3) \quad y_{s+1} = \Sigma_{k=1}^{s} \alpha_k^p y_k$$

with nonzero $\alpha_1, \dots, \alpha_s \in NC_a$. For any $\tau \in H_{C_a}$, regarded as an element of $G(NC_a/KC_a)$, we see that $C_a(\tau) \subset C_a$ whence $\tau(NC_a) \subset N \cdot C_a(\tau) \cdot C_a = NC_a$, so that τ is a differential automorphism of NC_a over KC_a. Applying τ to (3), we get $y_{s+1} = \Sigma_{k=1}^{s} (\tau\alpha_k)^p y_k$ and $\Sigma_{k=1}^{s} (\tau\alpha_k - \alpha_k)^p y_k = 0$. Since $\tau\alpha_k - \alpha_k \in NC_a$ $(1 \le k \le s)$, we see by the above that $\tau\alpha_k = \alpha_k$ $(1 \le k \le s)$. The set $\{\sigma \in G(NC_a/KC_a) \mid \sigma\alpha_k = \alpha_k \ (1 \le k \le s)\}$ is C_a-closed, and H_{C_a} is dense in H. Therefore, we conclude that $\sigma\alpha_k = \alpha_k$ $(1 \le k \le s)$ for every $\sigma \in H$, and that $\alpha_k \in L'$ and $\alpha_k^p \in (L')^p$ $(1 \le k \le s)$. Thus the claim is verified.

Regarding H as a C_i-closed subgroup of the C_i-group $G(NC_i/KC_i)$ (see Prop.14 of §5.6), let L^* denote the field of invariants in NC_i of H. Since $(C_i)_s = C_a$, we see by Lem.7 that L' and NC_i are linearly disjoint over L^* and that $L' = L^* C_a$. There are finitely many elements $z_1, \dots, z_r$ of NC_i with $NC_i = L^*(z_1, \dots, z_r)$ and $NC_a = L'(z_1, \dots, z_r)$.

Since we have already proved that NC_a is separable over L', we may suppose that $\{z_1,\dots,z_s\}$ with $s \leq r$ is a separating transcendence basis of NC_a over L'. Then $z_1, \dots, z_s$ are algebraically independent over L^* and make a separating transcendence basis of NC_i over L^*. Therefore, NC_i is strongly normal over L^*, and we see by Prop.14 of §5.6 that

(4) $G(NC_i/L^*) = G((NC_i)C_a/L^*C_a) = G(NC_a/L') = H.$

Now, by Lem.6, NL_∞ is strongly normal over L_∞; hence L_∞ is the field of invariants in NL_∞ of $G(NL_\infty/L_\infty)$. Regarding H as a C_i-subgroup of $G(N/L) = G(NL_\infty/L_\infty)$, let M be the field of invariants in NL_∞ of H. We get $M \supset L_\infty$. Conversely, for each $x \in M$, we can take $e \in \mathbb{N}$ such that $x^{p(e)} \in N$, and $\sigma(x^{p(e)}) = x^{p(e)}$ for every $\sigma \in H$, whence $x^{p(e)} \in L$ and $x \in L_\Delta \cap L_i = L_\infty$. Therefore, $M = L_\infty$ and $L^* \subset L_\infty$. Hence, L^* is purely inseparably algebraic over LC_i, and we see by Lem.5 and (4) that $G(N/L) = G(NC_i/LC_i) = G(NC_i/L^*) = H$.

Corollary Suppose that C is perfect.

(a) If $M \subset N$, and if L is the field of invariants in N of $G(N/M)$ (that is, if L is the purely inseparably algebraic closure in N of M), then N is finitely separable over L (whence N is strongly normal over L), and $G(N/L)$ is a C-subgroup of $G(N/K)$.

(b) If H is a C-subgroup of $G(N/K)$, and if L is the field of invariants in N of H, then L is purely inseparably algebraically closed in N, and N is strongly normal over

L, and $H = G(N/L)$.

Proof. (a) By part (a) of Th.7, we see that a differential subfield L of N is the field of invariants in N of $G(N/M)$ if and only if L is the purely inseparably algebraic closure in N of M, and that $G(N/M)$ is a C-closed subgroup of $G(N/K)$. Since $C = C_i$, applying the proof of part (b) of Th.7 to $G(N/M)$ instead of H, we see that N is finitely separable over L and that $G(N/M) = G(N/L)$.

(b) Since $C = C_i$, we can apply the proof of part (b) of Th.7 to the C-subgroup H of $G(N/K)$ and the field of invariants L in N of H. Then, similarly as in the proof of part (a) of the present corollary, N is strongly normal over L and $H = G(N/L)$.

Theorem 8 If $L \subset N$ and N is separable over L, equivalently, if N is strongly normal over L, then the following four conditions (i)~(iv) are mutually equivalent:

(i) L is strongly normal over K.

(ii) For each $\alpha \in L-K$, there exists strong differential isomorphism τ of L over K such that $\tau\alpha \neq \alpha$.

(iii) $G(N/L)$ is a normal subgroup of $G(N/K)$.

(iv) The inclusion $\sigma L \subset LU_C$ takes place for every $\sigma \in G(N/K)$.

Suppose that these conditions are satisfied. Then, if ι denotes the canonical imbedding homomorphism $G(N/L) \to G(N/K)$, and if ϕ denotes the homomorphism $G(N/K) \to G(L/K)$ defined

by $\phi(\sigma) = \sigma|_L$, for every $\sigma \in G(N/K)$, the sequence

(*) $G(N/L) \xrightarrow{i} G(N/K) \xrightarrow{\phi} G(L/K) \to \{id\}$

is exact and ϕ is a C-homomorphism between C-groups.

Proof. Suppose that the condition (i) is satisfied. Since L is finitely separable over K, the field of invariants in L of G(L/K) is K (see part (a) of Cor. to Prop. 4 of §5.4). Hence the condition (ii) is satisfied.

Now, let the condition (ii) be satisfied, and consider the normalizer $Z = \{\sigma \in G(N/K) \mid \sigma G(N/L) = G(N/L)\sigma\}$ of G(N/L) in G(N/K). Then Z is a C-closed subgroup of G(N/K) containing G(N/L) (see Chap.V of [4]). Let M be the field of invariants in N of Z. Since $\sigma x = x$ for every $(x,\sigma) \in M \times G(N/L)$ and since N is finitely separable over L, every element x of M is contained in L. If M = K, it follows from part (b) of Th.7 that Z = G(N/K), so that the condition (iii) is satisfied. Therefore, for our object, we have only to show that the assumption $M \neq K$ leads to a contradiction. By the assumption we can take $\alpha \in M-K \subset L-K$, and we see by the condition (ii) that there exists a strong differential isomorphism τ of L over K with $\tau\alpha \neq \alpha$. By Prop.3 of §5.3 this τ can be extended to a differential isomorphism σ of N over K. Then, for every $\rho \in G(N/L)$ and for every $\beta \in L$, we get $\sigma\beta = \tau\beta \in LU_C$ (whence $\rho\sigma\beta = \sigma\beta$) and $\sigma^{-1}\rho\sigma\beta = \beta$. Therefore, $\sigma^{-1}\rho\sigma \in G(N/L)$ and $G(N/L)\sigma = \sigma G(N/L)$. It follows that $\sigma \in Z = G(N/M)$ (see part (b) of Th.7), contradicting

the above.

Next, suppose that the condition (iii) is satisfied. Let σ be any element of $G(N/K)$, and β any element of L. Since $\sigma^{-1}\rho\sigma \in G(N/L)$ for every $\rho \in G(N/L)$, we get $\rho\sigma\beta = \sigma\beta$. We see that $\sigma\beta \in N\cdot\sigma N = N\cdot C(\sigma)$ and that $G(N/L) = G(NC(\sigma)/LC(\sigma))$ (see Prop.14 of §5.6), and we conclude that $\sigma\beta \in LC(\sigma)$, so that $\sigma L \subset LC(\sigma) \subset LU_C$. Thus the condition (iv) is satis-

Finally, suppose that the condition (iv) is satisfied. Let τ be any element of $G(L/K)$. Since N is finitely separable over L, we see by Prop.3 of §5.3 that τ can be extended to a differential isomorphism σ of N over K, so by the condition (iv) that $\tau L = \sigma L \subset LU_C$. Therefore, we conclude by Prop.12 of §5.6 that L is strongly normal over K, so that the condition (i) is satisfied.

Thus we have proved that the four conditions (i)~(iv) are mutually equivalent. Now, suppose that these conditions are satisfied, and consider the sequence (*). Clearly, ϕ is a group-homomorphism, and $\ker\phi = \mathrm{im}\,\iota$. Since N is finitely separable over L, each differential isomorphism of L over K can be extended to a differential isomorphism of N over K (see Prop.3 of §5.3). Hence ϕ is a surjective group-homomorphism. It remains to prove that ϕ is a C-homomorphism.

Let $\sigma,\sigma' \in G(N/K)$. It suffices to observe the following three properties 1°~3°:

1° $C(\sigma) = (N\cdot\sigma N)\cap U_C \supset (L\cdot\phi(\sigma)L)\cap U_C = C(\phi(\sigma))$.

2° Suppose $\sigma \to \sigma'$. Since $(\sigma'\alpha \mid \alpha \in N)$ is a differen-

tial specialization of $(\sigma\alpha \mid \alpha \in N)$ over N, we see that $(\phi(\sigma')\beta \mid \beta \in L)$ is a differential specialization of $(\phi(\sigma)\beta \mid \beta \in L)$ over N, hence over L. Therefore we get $\phi(\sigma) \to \phi(\sigma')$.

3° Suppose $\sigma \leftrightarrow \sigma'$. Then we see by 2° that $\phi(\sigma) \leftrightarrow \phi(\sigma')$. The isomorphism $S_{\sigma',\sigma}: C(\sigma) \xrightarrow{\sim} C(\sigma')$ is induced from the differential isomorphism $N \cdot \sigma N \xrightarrow{\sim} N \cdot \sigma' N$ over N which is determined by $\sigma\alpha \mapsto \sigma'\alpha$ $(\alpha \in N)$. Only considering elements α of L, we see that $S_{\phi(\sigma'),\phi(\sigma)}: C(\phi(\sigma)) \xrightarrow{\sim} C(\phi(\sigma'))$ is a restriction of $S_{\sigma',\sigma}$.

5.8. Examples

The conventions of §5.2 are not required in this section.

Example 1 Let K be a differential field and U a universal differential extension field of K. Let S be a set of linear differential forms in a single differential indeterminate X over K. Suppose that S is of finite degree n (see §3.5). Let $(x_1,\ldots,x_n)$ be a fundamental system of zeros of S with $x_j \in U$. Set $N = K\langle x_1,\ldots,x_n\rangle$ and suppose that N is a Picard-Vessiot extension of K (see Examp. of §4.5). Since N is finitely separable over K, we see by Th.4 of §4.4 that U is universal over N. Furthermore, suppose (as we may) that U is universal over N_Δ. If σ is any differential isomorphism into U of N over K, then every σx_j $(1 \le j \le n)$ is a zero in U of S, and we see by Prop.4 of §3.6 that it can be written in the form $\sigma x_j = \sum_{k=1}^{n} c_{kj}(\sigma) x_k$ with $c_{kj}(\sigma) \in U_c$ $(1 \le j \le n,\ 1 \le k \le n)$. Therefore, we conclude by

Prop.12 of §5.6 that N is strongly normal over K. We can see that the Galois group $G(N/K)$ is a liear C-group (see Chap.V of [4]), the element σ of $G(N/K)$ being identified with the element $(c_{kj}(\sigma)) = (c_{kj}(\sigma) \mid 1 \leq k \leq n,\ 1 \leq j \leq n)$ of the general linear group $GL(n)$ relative to the universal field U_C.

Example 2 Let K be a differential field with a single derivation $\delta = (\delta_\nu \mid \nu \in \mathbb{N})$, hence, with the set of derivative operators $\Theta = \{\delta_\nu \mid \nu \in \mathbb{N}\}$, and let U be a universal differential extension field of K. Suppose that δ is trivial in K. Choose a_θ $(\theta \in \Theta,\ \mathrm{ord}\ \theta > 0)$ in K such that at least one of a_θ with $\theta = \delta_{p(\kappa)}$ $(\kappa \in \mathbb{N})$ is not zero, that only a finite number of them are nonzero, and that every a_θ with $\theta \neq \delta_{p(\kappa)}$ for any $\kappa \in \mathbb{N}$ is zero. Then, by Examp. 1 of §4.6, there exists in U a primitive x such that $\theta x = a_\theta$ $(\theta \in \Theta,\ \mathrm{ord}\ \theta > 0)$ and that x is transcendental over K (see Examp.2 of §4.6). If we set $N = K\langle x \rangle$, then $N = K(x)$ and it is not difficult to see that the field of constants C of N coincides with K. Furthermore, suppose (as we may) that U is universal over N_Δ with $\Delta = \{\delta\}$. Then N is a Picard-Vessiot extension of K, whence strongly normal over K. Now, suppose that the field C is imperfect. We can choose $c \in C$ with $c^{p(-1)} \notin C$. Consider the differential subfield $M = K(x^{p(3)} - c^p x^{p(2)})$. We see that $L = K(x^{p(2)} - cx^p)$ is the purely inseparably algebraic closure in N of M, and that N

is not separable over L.

Example 3 In the theory of strongly normal extensions of the differential field of characteristic zero, Weierstrassian extensions are important examples of strongly normal extensions that are not Picard-Vessiot extensions. For differential fields of nonzero characteristic, the existence of Weierstrassian elements that are transcendental over the basic differential field are so far only known in the case of characteristic 3 as we saw in Examp.1 of §4.8. Let K_0, δ, a, g_2, g_3, x, N, η_ν ($\nu \geq 1$), η'_ν ($\nu \geq 1$) and U be as in that example. Set $K = K_0(\eta'_\nu | \nu \geq 1)$. Then, we see that K is a differential extension field of K_0 (see (2) of §4.8), and that x is a transcendental Weierstrassian element over K. Also, we see that $N = K\langle x \rangle = K(x, \delta_1 x)$ and N is finitely separable over K. Now, we add the extra condition that δ is trivial in K_0. Then it is not difficult to see that $N_c = K_c = K_0$. Suppose (as we may) that U is universal over N_Δ with $\Delta = \{\delta\}$. In order to prove that N is strongly normal over K, it suffices to show that $\sigma N \subset NU_c$ for every isolated differential isomorphism σ over K of N into U (see Prop.12 of §5.6). But this is now an open problem for us.

5.9. Differential Galois cohomology

The conventions stated in §5.2 are still applied to this section. Let N be strongly normal over K, and G any C-group having U as its universal field. For each $\sigma \in G(N/K)$,

since σ is identified with a differential automorphism of $N \cdot U_C$ over $K \cdot U_C$ (see Th.5 0f §5.5), we see by one of the defining properties of the pre-C-set structure of G that σ operates on $G_{N \cdot U_C}$.

A mapping $f: G(N/K) \to G$ is called (one-dimensional) cocycle of $G(N/K)$ into G if the following conditions are satisfied. Let σ, σ', τ be elements of $G(N/K)$.

(i) $f(\sigma) \in G_{N \cdot \sigma N} = G_{N \cdot C(\sigma)}$.

(ii) If $\sigma \overset{C}{\to} \sigma'$, then $f(\sigma) \overset{N}{\to} f(\sigma')$ in the induced N-group of the C-group G.

(iii) If $\sigma \overset{C}{\leftrightarrow} \sigma'$ (whence $S_{\sigma', \sigma}: C(\sigma) \overset{\sim}{\to} C(\sigma')$ can be uniquely extended to a field-isomorphism $N \cdot \sigma N \overset{\sim}{\to} N \cdot \sigma' N$ over N), the isomorphism $N \cdot \sigma N \overset{N}{\overset{\sim}{\to}} N \cdot \sigma' N$ is an extension of $S^{N}_{f(\sigma'), f(\sigma)}$.

(iv) $f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau))$.

The set of all such cocycles is denoted by $Z^1(N/K, G)$. If α is any element of G_N, the mapping $G(N/K) \to G$ with $\sigma \mapsto \alpha^{-1} \cdot \sigma\alpha$ is a cocyle of $G(N/K)$ into G. Such a cocycle is called (one-dimensional) coboundary of $G(N/K)$ into G. We denote by $B^1(N/K, G)$ the set of all such coboundaries of $G(N/K)$ into G.

Let f_1, f_2 be elements of $Z^1(N/K, G)$, then f_2 is called cohomologous to f_1 if there exists $\alpha \in G_N$ such that $f_2(\sigma) = \alpha^{-1} \cdot f_1(\sigma) \cdot \sigma\alpha$ for every $\sigma \in G(N/K)$. This relation in $Z^1(N/K, G)$ is an equivalence relation, and the set of all

equivalence classes is denoted by $H^1(N/K,G)$ and called (one-dimensional) cohomology set of $G(N/K)$ into G. If the C-group G is commutative, $Z^1(N/K,G)$ is a subgroup of the commutative group of all mappings of $G(N/K)$ into G, and $B^1(N/K,G)$ is its subgroup, and $H^1(N/K,G) = Z^1(N/K,G)/B^1(N/K,G)$.

Theorem 9 Let W be the locus of $\xi = (\xi_1,\ldots,\xi_n)$ over K with respect to the universal field U, and G a C-group as above. We can consider the K-cohomology of W into G (see §17 of Chap.V of [4]).

(a) For each $f \in Z^1(N/K,G)$, there exists uniquely an element $f_\xi \in Z^1_K(W,G)$ such that $f_\xi(\xi,\sigma\xi) = f(\sigma)$ for all $\sigma \in G(N/K)$.

(b) Let f, f' be two elements of $Z^1(N/K,G)$. Then, f' is cohomologous to f if and only if f'_ξ is K-cohomologous to f_ξ.

This can be proved following the proof of Th.7 of §8 of Chap.VI of [4].

Sketch of the proof. If σ is a C-generic element of a C-component of $G(N/K)$, we see by Cor. to Th.4 of §5.4 that $\dim_K(\xi,\sigma\xi) = 2\cdot\dim_K\xi = \dim(W^2)$, so that $(\xi,\sigma\xi)$ is a K-generic element of a K-component of W^2. Let $\mathfrak{p}$ be the defining differential ideal of ξ in the differential polynomial ring $K\{X_1,\ldots,X_n\}$. Then $N\mathfrak{p}$ can be written as an irredundant intersection $N\mathfrak{p} = P_1\cap\ldots\cap P_t$ of finitely many prime differential ideals $P_1, \ldots, P_t$ of $N\{X_1,\ldots,X_n\}$. Set $\mathfrak{p}_0 =$

$\mathfrak{p}\cap K[X_1,\ldots,X_n]$ and $P_{k0} = P_k\cap N[X_1,\ldots,X_n]$ $(1 \le k \le t)$. Then we see that $N\mathfrak{p}_0 = P_{10}\cap\ldots\cap P_{t0}$. For each k $(1 \le k \le t)$, let $\xi^{(k)}$ be a generic zero of P_k, then there exists a differential isomorphism $\sigma(k)$ over K of $K<\xi>$ onto $K<\xi^{(k)}>$ mapping ξ onto $\xi^{(k)}$. By the proof of part (b) of Th.4 of §5.4, we see that $\sigma(1), \ldots, \sigma(t)$ form a complete set of C-generic elements of the C-components of $G(N/K)$. Also, by Cor. to Th.4 of §5.4, we see that $\sigma(1)\xi, \ldots, \sigma(t)\xi$ form a complete set of N-generic elements of the N-components of W. For each k $(1 \le k \le t)$, applying the result above to the strongly normal extension $N\cdot C(\sigma(k))$ of $K\cdot C(\sigma(k))$, we see that if $\sigma(k,1)\xi, \ldots, \sigma(k,t(k))\xi$ form a complete set of $C(\sigma(k))$-generic elements of the $C(\sigma(k))$-components of $G(N/K)$, then $\sigma(k,1)\xi, \ldots, \sigma(k,t(k))\xi$ form a complete set of $(N\cdot\sigma(k)N)$-generic elements of the $(N\cdot\sigma(k)N)$-components of W. From this, we can deduce for each pair (k,ℓ) $(1 \le k \le t,\ 1 \le \ell \le t(k))$, that $(\sigma(k),\sigma(k,\ell))$ is a C-generic element of a C-component of $G(N/K)^2$, and that $\sigma(k)^{-1}\sigma(k,\ell)$ is a C-generic element of a C-component of $G(N/K)$.

Let f be an element of $Z^1(N/K,G)$. Then, $f(\sigma(k)) \in G_{N\cdot\sigma(k)N} = G_{K(\xi,\sigma(k)\xi)}$, and we see by the discussion following the proof of Prop.15 of §15 of Chap.V of [4] that there exists a unique K-mapping f_ξ of W^2 into G such that $f_\xi(\xi,\sigma(k)\xi) = f(\sigma(k))$ $(1 \le k \le t)$. For any C-generic element σ of a C-component of $G(N/K)$, there exists a unique

k $(1 \leq k \leq t)$ such that $\sigma(k) \leftrightarrow \sigma$, whence there exists a differential isomorphism $K(\xi,\sigma(k)\xi)=N\cdot\sigma(k)N \underset{\rightarrow}{\sim} N\cdot\sigma N=K(\xi,\sigma\xi)$ over K mapping $(\xi,\sigma(k)\xi)$ onto $(\xi,\sigma\xi)$. Therefore we have $f_\xi(\xi,\sigma\xi) = f(\sigma)$. Since we can verify that

$$f_\xi(\xi,\sigma(k)\xi)f_\xi(\sigma(k)\xi,\sigma(k,\ell)\xi) = f_\xi(\xi,\sigma(k,\ell)\xi)$$

for every pair (k,ℓ) $(1 \leq k \leq t,\ 1 \leq \ell \leq t(k))$, we conclude that $f_\xi \in Z^1_K(W,G)$. Starting afresh, let σ be any element of $G(N/K)$. Then, by Prop.24 of §17 of Chap.V of [4], f_ξ is defined at $(\xi,\sigma\xi)$. Now, let τ be a fixed $C(\sigma)$-generic element of $G^0(N/K)$. Then, f_ξ is defined at $(\tau\xi,\sigma\xi)$ and $\tau^{-1}\sigma$ is a C-generic element of a C-component of $G(N/K)$. We see that

$$\begin{aligned} f_\xi(\xi,\sigma\xi) &= f_\xi(\xi,\tau\xi)f_\xi(\tau\xi,\sigma\xi) = f_\xi(\xi,\tau\xi)\cdot\tau(f_\xi(\xi,\tau^{-1}\sigma\xi)) \\ &= f(\tau)\cdot\tau f(\tau^{-1}\sigma) = f(\sigma). \end{aligned}$$

This completes the proof of part (a) of the theorem.

Observe that, for any K-mapping h of W into G, h is defined at ξ and $h(\xi) \in G_N$, and conversely that, for any $\alpha \in G_N$, there exists a K-mapping h of W into G with $h(\xi) = \alpha$. Then we see that, for two elements f, f' of $Z^1(N/K,G)$, there exists $\alpha \in G_N$ such that $f'(\sigma) = \alpha^{-1}\cdot f(\sigma)\cdot\sigma\alpha$ $(\sigma \in G(N/K))$ if and only if there exists a K-mapping h of W into G such that $f'_\xi(\xi,\sigma\xi) = h(\xi)^{-1}\cdot f_\xi(\xi,\sigma\xi)\cdot h(\sigma\xi)$ $(\sigma \in G(N/K))$. This completes the proof of part (b) of the theorem.

Corollary 1 Let the hypothesis and the notations be as in Th.9.

(a) There is a unique mapping $H^1(N/K,G) \to H^1_K(W,G)$ that, for each $f \in Z^1(N/K,G)$, maps the cohomology class of f onto the K-cohomology class of f_ξ. It is an injection which maps $B^1(N/K,G)$ onto $B^1_K(W,G)$. When G is commutative, the mapping above is an injective homomorphism of groups.

(b) The mapping given in part (a) followed by the mapping $H^1_K(W,G) \to H^1(K,G)$ given in Th.12 and Cor.1 of §17 of Chap.V of [4] is an injection $H^1(N/K,G) \to H^1(K,G)$ which is independent of the choice of ξ in the convention stated in §5.2.

Proof. Part (a) is an immediate consequence of Th.9. Part (b) is a result of Cor.3 to Th.12 of §17 of Chap.V of [4].

Corollary 2 Each of the following condition is sufficient for $H^1(N/K,G)$ to be trivial: 1° G is the additive group of U, 2° $G = GL(m)$ with respect to U for a positive integer m, 3° K is algebraically closed. When G is commutative, every element of the commutative group $H^1(N/K,G)$ has finite order.

Proof. This follows from part (b) of Cor.1 above and Th.9 of §12 of Chap.V of [4].

CHAPTER 6

Picard-Vessiot Extensions

6.1. Picard-Vessiot extension whose Galois group is the general linear group

Let K_0 be a differential field associated with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ. Fix any positive integer n, and choose n differential indeterminates $x_1, \ldots, x_n$ over K_0 and n distinct derivative operators $\theta(1), \ldots, \theta(n)$, and set $\Theta' = \Theta - \{\theta(1),\ldots,\theta(n)\}$. Now, set

$$u_{\theta' h} = \frac{W_{\theta',\theta(1),\ldots,\theta(h-1),\theta(h+1),\ldots,\theta(n)}(x_1,\ldots,x_n)}{W_{\theta(1),\ldots,\theta(n)}(x_1,\ldots,x_n)}$$

$$(\theta' \in \Theta',\ 1 \leq h \leq n),$$

$$K = K_0\langle u_{\theta' h} \mid \theta' \in \Theta', 1 \leq h \leq n\rangle$$

and

$$N = K\langle x_1,\ldots,x_n\rangle = K_0\langle x_1,\ldots,x_n\rangle.$$

Let U be a universal differential extension field of N_Δ.

We see by Prop.3 of §2.3 that $N_c = (K_0)_c$, so that $N_c = K_c$. We denote this field by C.

In this section, we prove that N is a Picard-Vessiot extension of K and that $G(N/K)$ can be identified with the general linear group $GL(n)$ relative to the universal field U_c (see Chap.V of [4]).

Let X be a single differential indeterminate over U,

and consider the set of linear differential forms

$$(1)\quad W_{\theta',\theta(1),\ldots,\theta(n)}(X,x_1,\ldots,x_n)/W_{\theta(1),\ldots,\theta(n)}(x_1,\ldots,x_n) \qquad (\theta' \in \Theta').$$

This set can be written in the form

$$(1')\quad \theta'X - \Sigma_{h=1}^{n}(-1)^{h-1}u_{\theta'h}\cdot\theta(h)X \quad (\theta' \in \Theta').$$

Therefore, if we denote by S the set of linear differential forms (1') of $K\{X\}$, S is of order n in the sense of §3.5. We see by Cor.1 to Th.6 of §3.6 that $(x_1,\ldots,x_n)$ is a fundamental system of zeros of S.

Since we get

$$(2)\quad \theta'x_j - \Sigma_{h=1}^{n}(-1)^{h-1}u_{\theta'h}\cdot\theta(h)x_j = 0 \quad (\theta' \in \Theta',\ 1 \le j \le n),$$

it follows that $N = K(\theta(k)x_j \mid 1\le k\le n,\ 1\le j\le n)$. Furthermore, for each (θ',h) $(\theta' \in \Theta',\ 1 \le h \le n)$, each derivative of $u_{\theta'h}$ can be written in the form of a polynomial in $u_{\theta''h'}$ $(\theta'' \in \Theta',\ 1 \le h' \le n)$ over Z (the set of integers); this can be proved by induction on the order of the derivative $\delta_{i\nu}u_{\theta'h}$ $(i \in I,\ \nu \in N)$, making use of (2). Thus $K = K_0(u_{\theta'h} \mid \theta'\in\Theta',\ 1\le h\le n)$. Now, we claim that $\theta(k)x_j$ $(1 \le k \le n,\ 1 \le j \le n)$ are algebraically independent over K.

Assume on the contrary that there exists a nonzero polynomial $A(X_{kj}) = A(X_{kj} \mid 1 \le k \le n,\ 1 \le j \le n)$ in the indeterminates X_{kj} $(1 \le k \le n,\ 1 \le j \le n)$ over $K_0[u_{\theta'h} \mid \theta'\in\Theta',\ 1\le h\le n]$ such that $A(\theta(k)x_j) = 0$. Then, we obtain a relation

$$B(\theta(k)x_j, \theta'x_j \mid 1 \le k \le n,\ \theta' \in \Theta',\ 1 \le j \le n) = 0,$$

where $B(X_{kj}, X_{\theta'j})$ is a nonzero polynomial in the indeterminates X_{kj}, $X_{\theta'j}$ $(1 \le k \le n,\ \theta' \in \Theta',\ 1 \le j \le n)$ over K_0. This is a contradiction since $x_1, \ldots, x_n$ are differential indeterminates over K_0, and the claim above is admitted.

It follows from the claim above and (2) that N is purely transcendental over K, so that N is a Picard-Vessiot extension of K. Therefore, by Examp.1 of §5.8, $G(N/K)$ is identified with a C-subgroup of $GL(n)$.

Let (c_{kj}) be any $n \times n$ nonsingular matrix with $c_{kj} \in U_c$, and set $x'_j = \Sigma_{k=1}^{n} c_{kj}x_k$ $(1 \le j \le n)$. Now, we claim that $x'_1, \ldots, x'_n$ are n differential indeterminates over K_0. Assume on the contrary that there exists a nonzero polynomial $P(X'_{\theta j})$ in the indeterminates $X'_{\theta j}$ $(\theta \in \Theta,\ 1 \le j \le n)$ over U such that all the coefficients of $P(X'_{\theta j})$ are in K_0 and that $P(\theta x'_j) = 0$. Let $X_{\theta k}$ $(\theta \in \Theta,\ 1 \le k \le n)$ be indeterminates over U, then $P(\Sigma_{k=1}^{n} c_{kj}X_{\theta k})$ can be written in the form of a linear combination over U_c of finitely many polynomials $A_1(X_{\theta k}), \ldots, A_r(X_{\theta k})$ in $K_0[X_{\theta k} \mid \theta \in \Theta,\ 1 \le k \le n]$ such that $A_1(\theta x_k), \ldots, A_r(\theta x_k)$ are linearly independent over C. Since we see by §3.6 that $A_1(\theta x_k), \ldots, A_r(\theta x_k)$ must be linearly independent over U_c, $P(\theta x'_j) = 0$ implies $r = 0$ and $P(\Sigma_{k=1}^{n} c_{kj}X_{\theta k}) = 0$ in $U[X_{\theta k} \mid \theta \in \Theta,\ 1 \le k \le n]$. Now, if (γ_{kj}) is the inverse matrix of (c_{kj}), the substitution

$$X_{\theta k} \mapsto \Sigma_{h=1}^{n} \gamma_{hk}X_{\theta h} \quad (\theta \in \Theta,\ 1 \le k \le n)$$

provides us the result $P(X_{\theta j}) = 0$. This is a contradiction, and the claim is verified. Therefore, a differential isomorphism σ over K_0 of N into U is determined by $x_j \mapsto x'_j$ $(1 \leq j \leq n)$. Since each $u_{\theta' h}$ $(\theta' \in \Theta', 1 \leq h \leq n)$ is invariant under σ, so is every element of K. Thus $G(N/K)$ is identified with the whole $GL(n)$.

6.2. Fundamental theorem of Galois theory for Picard-Vessiot extensions

Let N be the Picard-Vessiot extension of the differential field K which was observed in Examp.1 of §5.8. Let C, X, S, $(x_1,\ldots,x_n)$ and U be as in that example. Then the Galois group $G(N/K)$ is a linear C-group, elements of $G(N/K)$ being identified with elements of $GL(n)$. Applying Th.7, Cor. and Th.8 to the Picard-Vessiot extension N of K above, we get at once the following results.

Proposition 1 (a) Let M be an intermediate differential field between K and N. Then $G(N/M)$ is a C-closed subgroup of linear C-group $G(N/K)$. If L is the field of invariants in N of $G(N/M)$, L is the purely inseparably algebraic closure in N of M and $G(N/M) = G(N/L)$.

(b) If H is a C-closed subgroup of $G(N/K)$, and if L is the field of invariants in N of H, then L is purely inseparably algebraically closed in N and $H = G(N/L)$.

Proposition 2 Suppose that C is perfect.

(a) Let M be an intermediate differential field between

K and N. If L is the field of invariants in N of G(N/M) (equivalently, if L is the purely inseparably algebraic closure in N of M), then N is finitely separable over L (whence N is a Picard-Vessiot extension of L), and G(N/L) is a C-subgroup of the linear C-group G(N/K).

(b) If M is a C-subgroup of G(N/K), and if L is the field of invariants in N of H, then L is purely inseparably algebraically closed in N, and N is a Picard-Vessiot extension of L, and H = G(N/L).

Proposition 3 Let L be an intermediate differential field between K and N. If N is separable over L, equivalently, if N is a Picard-Vessiot extension of L, then the following four conditions (i)~(iv) are mutually equivalent:

(i) L is strongly normal over K.

(ii) For each $\alpha \in L-K$, there exists strong differential isomorphism τ of L over K such that $\tau\alpha \neq \alpha$.

(iii) G(N/L) is a normal subgroup of G(N/K).

(iv) The inclusion $\sigma L \subset LU_C$ takes place for every $\sigma \in G(N/K)$.

Suppose that these conditions are satisfied. Then, if ι denotes the canonical imbedding homomorphism $G(N/L) \to G(N/K)$, and if ϕ denotes the homomorphism $G(N/K) \to G(L/K)$ defined by $\phi(\sigma) = \sigma|_L$ for every $\sigma \in G(N/K)$, the sequence

$$G(N/L) \xrightarrow{\iota} G(N/K) \xrightarrow{\phi} G(L/K) \to \{id\}$$

is exact and ϕ is a C-homomorphism of C-groups.

Proposition 4 Let L be an intermediate differential field between K and N such that N is separable over L and that L satisfies the conditions (i)~(iv) of Prop.3. Then the Galois group $G(L/K)$ is a linear C-group.

Proof. By the hypothesis and Prop.3, we have the exact sequence

(1) $G(N/L) \xrightarrow{\iota} G(N/K) \xrightarrow{\phi} G(L/K) \to \{id\}$,

where ι and ϕ are as in Prop.3. On the other hand, since $G(N/K)$ is a linear C-group and $G(N/L)$ is a normal C-subgroup of $G(N/K)$, we see by Chevalley-Kolchin [0] that there exists an exact sequence

(2) $G(N/L) \xrightarrow{\iota} G(N/K) \xrightarrow{\rho} A \to \{id\}$,

where ρ is a group-homomorphism of $G(N/K)$ onto an algebraic subgroup A of $GL(m)$ with respect to the universal field U_C for some $m \in \mathbb{N}-\{0\}$.

For $\lambda, \lambda' \in A$, the extension field $C(\lambda)$ of C in U_C and the relation $\lambda \to \lambda'$ are introduced, and so is the field-isomorphism $S_{\lambda',\lambda}: C(\lambda) \xrightarrow{\sim} C(\lambda')$ when $\lambda \leftrightarrow \lambda'$ (i.e. when $\lambda \to \lambda'$ and $\lambda' \to \lambda$). They are defined by virtue of the C-group structure as follows.

Since we can take $\sigma \in G(N/K)$ such that $\rho(\sigma) = \lambda$, and since $\phi(\sigma)$ is uniquely determined in $G(L/K)$ by λ, set $C(\lambda) = C(\phi(\sigma))$. If $\rho(\sigma) = \lambda$, $\rho(\sigma') = \lambda'$ with $\sigma,\sigma' \in G(N/K)$, we mean by $\lambda \to \lambda'$ that $\phi(\sigma) \to \phi(\sigma')$ takes place. Then, if

$\lambda \leftrightarrow \lambda'$, equivalently, if $\phi(\sigma) \leftrightarrow \phi(\sigma')$, we denote by $S_{\lambda',\lambda}$ the field-isomorphism $S_{\phi(\sigma'),\phi(\sigma)}$.

A bijection γ: $G(L/K) \to A$ can be well-defined by the formula $\phi(\sigma) \mapsto \rho(\sigma)$ $(\sigma \in G(N/K))$.

Now, it is straightforward to prove that the data above satisfy axioms AS1, AS2, AG1, AG2 and AG3 of Chap.V of [4] (i.e. that A is a C-group), and that both γ and γ^{-1} are C-homomorphisms (i.e. that γ is a C-isomorphism of the C-group $G(L/K)$ onto the C-group A).

Proposition 5 Suppose that C is perfect. Let L be as in Prop.4. Then L is finitely purely inseparably algebraic over a Picard-Vessiot extension of K.

Proof. We consider the strongly normal extension L of K. By the proof of Prop.4, there exists an injective C-homomorphism γ of $G(L/K)$ into $GL(m)$ with respect to the universal field U_C for some $m \in \mathbb{N}-\{0\}$. This γ is a one-dimensional cocycle of $G(L/K)$ into $GL(m)$ with respect to the universal field U. We see by Cor.2 to Th.9 of §5.9 that there exists $\alpha \in GL(m)_L$ such that $\gamma(\alpha) = \alpha^{-1} \cdot \sigma\alpha$ for all $\sigma \in G(L/K)$.

If $\alpha = (\alpha_{jj'} \mid 1 \leq j \leq m, 1 \leq j' \leq m)$ with $\alpha_{jj'} \in L$, set $\theta\alpha = (\theta\alpha_{jj'} \mid 1 \leq j \leq m, 1 \leq j' \leq m)$ for every $\theta \in \Theta$. Then we claim at first that all the coefficients of the matrix $\theta\alpha \cdot \alpha^{-1}$ are contained in K for every $\theta \in \Theta$. In fact, for all $\sigma \in G(L/K)$,

$$\sigma(\theta\alpha\cdot\alpha^{-1}) = \theta(\sigma\alpha)\cdot(\sigma\alpha)^{-1} = \theta(\alpha\cdot\gamma(\sigma))\cdot(\alpha\cdot\gamma(\sigma))^{-1}$$

$$= (\theta\alpha)\cdot\gamma(\sigma)\cdot\gamma(\alpha)^{-1}\cdot\alpha^{-1} = \theta\alpha\cdot\alpha^{-1} \quad (\theta \in \Theta),$$

hence the claim is verified.

Set $K\langle\alpha\rangle = K\langle\alpha_{jj'} \mid 1\le j\le m,\ 1\le j'\le m\rangle$. Now, we claim that $K\langle\alpha\rangle$ is a Picard-Vessiot extension of K.

By the preceding claim, we see that $K\langle\alpha\rangle = K(\alpha_{jj'} \mid 1\le j\le m, 1\le j'\le m)$, that $K\langle\alpha\rangle$ is finitely K-separable, and that $K\langle\alpha\rangle_c = C$. Take a maximal set $\{x_1,\dots,x_\ell\}$ among the $\alpha_{jj'}$ $(1 \le j \le m,\ 1 \le j' \le m)$ that is linearly independent over constants. For each $\sigma \in G(L/K)$, since the coefficients $\sigma\alpha_{jj'}$ of $\sigma\alpha = \alpha\cdot\gamma(\alpha)$ are linear combinations over U_c of the coefficients of α, we have $\sigma x_k = \Sigma_{h=1}^{\ell} x_h d_{hk}(\sigma)$ $(1 \le k \le \ell)$ with $d_{hk}(\sigma) \in U_c$. Set $d(\sigma) = (d_{hk}(\sigma) \mid 1 \le h \le \ell,\ 1 \le k \le \ell)$. Then, for any $\theta(1),\dots,\theta(\ell) \in \Theta$, we get

$$\sigma W_{\theta(1),\dots,\theta(\ell)}(x_1,\dots,x_\ell) = W_{\theta(1),\dots,\theta(\ell)}(x_1,\dots,x_\ell)\cdot d(\sigma).$$

Since there exist $\theta'(1),\dots,\theta'(\ell) \in \Theta$ such that

$$W_{\theta'(1),\dots,\theta'(\ell)}(x_1,\dots,x_\ell) \neq 0,$$

we see that $d(\sigma)$ is nonsingular, so that

$$\sigma(W_{\theta(1),\dots,\theta(\ell)}(x_1,\dots,x_\ell)\cdot W_{\theta'(1),\dots,\theta'(\ell)}(x_1,\dots,x_\ell)^{-1})$$

$$= W_{\theta(1),\dots,\theta(\ell)}(x_1,\dots,x_\ell)\cdot W_{\theta'(1),\dots,\theta'(\ell)}(x_1,\dots,x_\ell)^{-1}$$

for all $\sigma \in G(L/K)$. Therefore, all the coefficients of

$$W_{\theta(1),\dots,\theta(\ell)}(x_1,\dots,x_\ell)\cdot W_{\theta'(1),\dots,\theta'(\ell)}(x_1,\dots,x_\ell)^{-1}$$

are contained in K, and if X is a differential indeterminate over L, then

$$W_{\theta,\theta(1),\ldots,\theta(\ell)}(X,x_1,\ldots,x_\ell)\cdot W_{\theta'(1),\ldots,\theta'(\ell)}(x_1,\ldots,x_\ell)^{-1} \in K\{X\}$$

for all choice of θ, $\theta(1)$, ... , $\theta(\ell)$ from Θ. The set of linear differential forms

$$(3)\quad W_{\theta,\theta'(1),\ldots,\theta'(\ell)}(X,x_1,\ldots,x_\ell)\cdot W_{\theta'(1),\ldots,\theta'(\ell)}(x_1,\ldots,x_\ell)^{-1} \qquad (\theta \in \Theta)$$

in X over K is of order ℓ in the sense of §3.5, and x_1, ... , x_ℓ form a fundamental system of zeros of (3). Since $K(x_1,\ldots,x_\ell) = K(\alpha_{jj'} \mid 1\leq j\leq m,\ 1\leq j'\leq m) = K\langle\alpha\rangle$, $K\langle\alpha\rangle$ is a Picard-Vessiot extension of K.

If $\sigma \in G(L/K\langle\alpha\rangle)$, then $\sigma\alpha = \alpha$ and $\gamma(\sigma) = \alpha^{-1}\cdot\sigma\alpha$ is the unit matrix. Since γ is injective, we see that $G(L/K\langle\alpha\rangle) = \{id_L\}$, and by part (b) of Cor. to Th.7 of §5.7 that L is finitely purely inseparably algebraic over $K\langle\alpha\rangle$.

Remark So far we do not know any example of L of Prop. 5 that is not a Picard-Vessiot extension of K. (Cf. §6.3 and §6.4.)

6.3. Picard-Vessiot extension by a primitive

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ, and N a Picard-Vessiot extension by a nonconstant primiti-

ve x over K. Then $N = K\langle x\rangle = K(x)$. Set $C = N_c$ $(=K_c)$ and and $a_\theta = \theta x$ with $a_\theta \in K$ $(\theta \in \Theta, \text{ord}\,\theta > 0)$. Let N_a be an algebraic closure of N, and N_Δ the differential closure in N_a of N, and U a universal differential extension field of N_Δ.

If σ is any element of $G(N/K)$, we see that $\theta(\sigma x - x) = \sigma(\theta x) - \theta x = \sigma a_\theta - a_\theta = 0$ for every $\theta \in \Theta$ with ord $\theta > 0$, so that $\sigma x - x$ is contained in $C(\sigma) = (N \cdot \sigma N)_c$. Set $c(\sigma) = \sigma x - x$ for every element $\sigma \in G(N/K)$. We see that $(1, x)$ is a fundamental system of zeros of defining system of linear differential forms, that $\sigma 1 = 1$, $\sigma x = c(\sigma) + x$ for every $\sigma \in G(N/K)$, and that $c(\sigma'\sigma) = c(\sigma) + c(\sigma')$ for every pair σ, σ' in $G(N/K)$. Set

$$G'(N/K) = \left\{ \begin{pmatrix} 1 & c(\sigma) \\ 0 & 1 \end{pmatrix} \;\middle|\; \sigma \in G(N/K) \right\}.$$

Then, $G'(N/K)$ is a C-subgroup of the general linear group $GL(2)$ relative to the universal field U_c, and $G(N/K)$ is C-isomorphic to $G'(N/K)$ (see Examp.1 of §5.8). $G'(N/K)$ is abelian and unipotent. We can easily see that the additive group U_c is canonically a C-group. Set $G''(N/K) = \{c(\sigma) \mid \sigma \in G(N/K)\}$. Then, $G''(N/K)$ is a C-subgroup of the additive C-group U_c and $G(N/K)$ is C-isomorphic to $G''(N/K)$.

Consider further under the extra condition that C is algebraically closed.

At first, let the x above be algebraic over K. Then,

for every $\sigma \in G(N/K)$, we see that $K(x,\sigma x) = N\cdot\sigma N = N\cdot C(\sigma) = K(x)\cdot C(\sigma)$, and this implies that $C(\sigma) = C$. On the other hand, $G''(N/K)$ is finite and of order p^e for some $e \in \mathbb{N}$. Therefore, there exist e elements $\sigma_1, \ldots, \sigma_e$ of $G(N/K)$ such that $c(\sigma_1), \ldots, c(\sigma_e)$ are contained in C and linearly independent over the prime field and that $G(N/K) = \{\sigma_1^{h(1)}\cdot\ldots\cdot\sigma_e^{h(e)} \mid 0\leq h(1)<p,\ldots,0\leq h(e)<p\}$. Since $\Pi_{\sigma\in G(N/K)}(x + c(\sigma))$ is invariant under every element of $G(N/K)$, it is an element a of K. We see that

$$\Pi_{\sigma\in G(N/K)}(X + c(\sigma)) - a$$

is the minimal polynomial of x over K, because every isomorphism over K of N into U is a differential isomorphism.

Next, let the x above be transcendental over K. Then, we see by Th.6 of §5.6 that $G''(N/K)$ coincides with U_C, so that

$$G'(N/K) = \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \;\middle|\; c \in U_C \right\}.$$

Whether x is algebraic or not over K, Prop.2 and Prop.3 of §6.2 provide the following results.

Let H be a proper C-subgroup of $G(N/K)$, and let L be the corresponding intermediate differential field between K and N. Then, N is a Picard-Vessiot extension of L with the Galois group $H = G(N/L)$ that is of order p^d for some $d \in \mathbb{N}$, and there exist d elements $\sigma_1', \ldots, \sigma_d'$ of H such that $c(\sigma_1'), \ldots, c(\sigma_d')$ $(\in C)$ are linearly independent over the

prime field, that $H = \{(\sigma'_1)^{h(1)} \cdot \ldots \cdot (\sigma'_d)^{h(d)} \mid 0 \le h(1) < p,\ 0 \le h(d) < p\}$. We claim that $L = K(\Pi_{\sigma' \in H}(x + c(\sigma')))$ and that L is a Picard-Vessiot extension by a primitive over K.

If $c_1, \ldots, c_r$ are finitely many elements of C and linearly independent over the prime field, we can prove by induction on r that

$$\Pi_{\substack{0 \le h_1 < p \\ \cdots \\ 0 \le h_r < p}} (X + h_1 c_1 + \ldots + h_r c_r) = X^{p(r)} + \gamma_1 X^{p(r-1)} + \ldots + \gamma_{r-1} X^p + \gamma_r X$$

for some $\gamma_1, \ldots, \gamma_r \in C$ with $\gamma_r \neq 0$. Therefore,

$$\Pi_{\sigma' \in H}(x + c(\sigma')) = x^{p(r)} + \gamma'_1 x^{p(r-1)} + \ldots + \gamma'_{r-1} x^p + \gamma'_r x$$

for some $\gamma'_1, \ldots, \gamma'_r \in C$ with $\gamma'_r \neq 0$, and it is an element of L which is primitive over K. Now, it is easy to verify the claim.

6.4. Picard-Vessiot extension by an exponential

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ, and N a Picard-Vessiot extension by a nonconstant exponential x over K. Then $N = K\langle x \rangle = K(x)$. Let N_a be an algebraic closure of N, and N_Δ the differential closure in N_a of N. Let U be a universal differential extension field of N_Δ. Set $C = N_c$ $(= K_c)$ and $a_{(\nu)} = \delta_{(\nu)} x/x$ $((\nu) \in \mathbb{N}^{(I)})$.

If σ is any element of $G(N/K)$, we can prove by induction on ν that $\delta_{i\nu}(\sigma x/x) = 0$ $(i \in I,\ \nu \in \mathbb{N} - \{0\})$, so that

$\sigma x/x$ is contained in $C(\sigma) = (N \cdot \sigma N)_C$. Set $\sigma x/x = c(\sigma)$ for every element $\sigma \in G(N/K)$. Set $G'(N/K) = \{c(\sigma) \mid \sigma \in G(N/K)\}$. Then, $G'(N/K)$ is a C-subgroup of the general linear group $GL(1)$ relative to the universal field U_C, and $G(N/K)$ is C-isomorphic to $G'(N/K)$ (see Examp.1 of §5.8). $G'(N/K)$ is abelian and semisimple.

At first, let x be algebraic over K. Then $G(N/K)$ is a finite group of order s (say). Since every element c of $G'(N/K)$ satisfies the equation $c^s = 1$, $G'(N/K)$ consists of all the s-th roots of 1. Hence $s \not\equiv 0 \pmod{p}$, and $G(N/K)$ is a cyclic group. There exists an element σ of $G(N/K)$ such that $G(N/K)$ is generated by σ. Since $\sigma(x^s) = (c(\sigma)x)^s = x^s$, x^s is invariant under every element of $G(N/K)$. Hence $x^s \in K$ and N has the relative degree s over K.

Next, let x be transcendental over K. Since we have $\dim G(N/K) = \mathrm{trdeg}\ N/K = 1$ by Th.6 of §5.6, $G'(N/K)$ coincides with $GL(1)$.

Consider further under the extra condition that C is algebraically closed.

Whether x is algebraic or not over K, Prop.2 and Prop.3 of §6.2 provide the following results.

Let H be a proper C-subgroup of $G(N/K)$, and let L be the corresponding intermediate differential field between K and N. Then N is a Picard-Vessiot extension of L with the Galois group $H = G(N/L)$ that is a finite cyclic group of

order t (say) with $t \not\equiv 0 \pmod{p}$. It is easy to see that $L = K\langle x^t \rangle = K(x^t)$, that x^t is an exponential over K, and that L is a Picard-Vessiot extension by an exponential over K.

6.5. Liouvillian extensions

Let K be a differential field with the set of derivation operators $\Delta = \{\delta_i \mid i \in I\}$ and the set of derivative operators Θ, and U a universal differential extension field of K. Set $C = K_C$. Let L be a differential subfield of U such that U is also universal over L_Δ. Then, L is called Liouvillian extension of K if it has the following two properties:

(i) $L_C = K_C$.

(ii) There exists a finite ascending chain of intermediate differential fields $K = K_0, K_1, \ldots, K_{r-1}, K_r = L$ such that, for each j $(1 \leq j \leq r)$, K_j is a Picard-Vessiot extension by a primitive y_j over K_{j-1}, a Picard-Vessiot extension by an exponential y_j over K_{j-1}, or a separably normally algebraic extension by an element y_j over K_{j-1}.

It is well-known that, if M_1, M_2, M_3 are three fields with $M_1 \subset M_2 \subset M_3$ such that M_2 is M_1-separable and that M_3 is M_2-separable, then M_3 is M_1-separable. Therefore, the Liouvillian extension L of K is separable over every K_j $(0 \leq j \leq r)$.

Let L be a Liouvillian extension of K having the properties (i) and (ii) above. Then we have $L_C = C$. Henceforth in this section, suppose that C is algebraically clo-

sed. Let N be an intermediate differential field between K and L such that L is N-separable and that N is a Picard-Vessiot extension of K. Let the order of the defining system of linear differential forms be n, and $x_1, \ldots, x_n$ a fundamental system of zeros of the defining system with $N = K\langle x_1, \ldots, x_n \rangle$.

Since $N\langle y_1 \rangle \subset L$, $N\langle y_1 \rangle$ is a Picard-Vessiot extension of $K\langle y_1 \rangle$. On the other hand, since $K\langle y_1 \rangle \cap N$ is purely inseparably algebraically closed in $K\langle y_1 \rangle$, we see by Prop.2 of §6.2, that $K\langle y_1 \rangle$ is separable over $K\langle y_1 \rangle \cap N$, so that L is separable over $K\langle y_1 \rangle \cap N$ because L is $K\langle y_1 \rangle$-separable. Therefore, N is separable over $K\langle y_1 \rangle \cap N$, and it is a Picard-Vessiot extension of $K\langle y_1 \rangle \cap N$.

Then we can prove the following two lemmas.

Lemma 1 $G(N\langle y_1 \rangle / K\langle y_1 \rangle)$ is canonically identified with $G(N/(K\langle y_1 \rangle \cap N))$.

Proof. If σ is any element of $G(N\langle y_1 \rangle / K\langle y_1 \rangle)$, the restriction $\sigma|_N$ is a differential isomorphism of N over K. Hence, $G(N\langle y_1 \rangle / K\langle y_1 \rangle)$ is regarded as a C-subgroup of $G(N/K)$, and we see by Cor. to Th.7 of §5.7 that there exists an intermediate differential field M between K and N which is purely inseparably algebraically closed in N such that $G(N\langle y_1 \rangle / K\langle y_1 \rangle) = G(N/M)$. It remains to show that $M = K\langle y_1 \rangle \cap N$. Since every element of $K\langle y_1 \rangle \cap N$ is invariant under each $\sigma \in G(N\langle y_1 \rangle / K\langle y_1 \rangle)$, we see $K\langle y_1 \rangle \cap N \subset M$. Conversely, every element

of M is invariant under each $\sigma \in G(N\langle y_1\rangle/K\langle y_1\rangle)$, hence, $M \subset K\langle y_1\rangle$ and $M \subset K\langle y_1\rangle \cap N$.

Lemma 2 $G(N/K)$ has a normal chain of C-subgroups, each of whose factor groups is either abelian or finite.

Proof. Let us use induction on the r above. In case $r = 0$ the assertion is trivially true. In case $r > 0$, $N\langle y_1\rangle$ is a Picard-Vessiot extension of $K\langle y_1\rangle$, and we see by Lem.1 that $G(N\langle y_1\rangle/K\langle y_1\rangle) = G(N/(K\langle y_1\rangle \cap N))$. By induction assumption, $G(N/(K\langle y_1\rangle \cap N))$ has a normal sequence of C-subgroups each of whose factor group is either abelian or finite.

Case I: y_1 is primitive or exponential over K. Let σ be any element of $G(N/K)$. Since we see by §6.3 or by §6.4 that $K\langle y_1\rangle \cap N$ is a Picard-Vessiot extension by a primitive or by an exponential over K, we have $\sigma(K\langle y_1\rangle \cap N) \subset (K\langle y_1\rangle \cap N)\cdot U_c$. Therefore, by Prop.3 of §6.2, $G(N/(K\langle y_1\rangle \cap N))$ is a normal subgroup of $G(N/K)$ with

$$G((K\langle y_1\rangle \cap N)/K) \simeq G(N/K)/G(N/(K\langle y_1\rangle \cap N))$$

and this factor group is abelian.

Case II: $K\langle y_1\rangle$ is separably normally algebraic over K. Let σ be any element of $G(N/K)$. Then, for any element z of $K\langle y_1\rangle \cap N$, σz is contained in $K\langle y_1\rangle \cap (NU_c)$, and σz can be written in the form

$$\sigma z = \Sigma_{\alpha=1}^{s} \eta_\alpha \gamma_\alpha / \Sigma_{\alpha=1}^{s} \eta_\alpha \gamma'_\alpha$$

with $\eta_\alpha \in N$ $(1 \leq \alpha \leq s)$ linearly independent over U_c and

with γ_α, $\gamma'_\alpha \in U_C$. Therefore, η_α , $\eta_\alpha \cdot \sigma z$ $(1 \leq \alpha \leq s)$ are linearly dependent over constants, and there exist elements c_α , c'_α $(1 \leq \alpha \leq s)$ not all zero of C such that

$$\sigma z = \Sigma_{\alpha=1}^{s} \eta_\alpha c_\alpha / \Sigma_{\alpha=1}^{s} \eta_\alpha c'_\alpha ,$$

so that $\sigma z \in K\langle y_1 \rangle \cap N$. This implies that $G(N/(K\langle y_1 \rangle \cap N))$ is a normal subgroup of $G(N/K)$ with the finite factor group

$$G(N/K)/G(N/(K\langle y_1 \rangle \cap N)) \simeq G((K\langle y_1 \rangle \cap N)/K).$$

Thus, in either case, $G(N/K)$ has a normal sequence of C-subgroups each of whose factor groups is abelian or finite. q.e.d.

Similarly as in Kolchin [1], distinguish ten types of extensions in a sequence of differential fields from K to the Liouvillian extension L, namely, extensions by

1° primitives, exponentials and separably normally algebraic elements (y_j being called <u>separably normally algebraic</u> over K_{j-1} if $K_j = K_{j-1}\langle y_j \rangle$ is a separably normally algebraic extension field of K_{j-1}),

2° primitives and exponentials,

3° exponentials and separably normally algebraic elements,

4° primitives and separably normally algebraic elements,

5° primitives and separable radicals (y_j being called <u>separable radical</u> over K_{j-1} if $y_j^\rho \in K_{j-1}$ for some $\rho \in \mathbb{N}$ with $\rho \not\equiv 0 \pmod p$),

6° exponentials, 7° primitives,

8° separably normally algebraic elements,

9° separable radicals,

10° rational elements (whence $L = K$).

On the other hand, let N be a Picard-Vessiot extension of K, $G(N/K)$ the Galois group of N over K, and $G^0(N/K)$ the component of the identity of $G(N/K)$. Similarly as in [1], list ten types of properties which they may possess:

1° $G^0(N/K)$ is solvable,

2° $G(N/K)$ is solvable,

3° $G^0(N/K)$ is solvable and *-semisimple ($G^0(N/K)$ being called *-semisimple if it has a normal chain of C-subgroups each of whose factor groups is either semisimple or finite),

4° $G^0(N/K)$ is solvable and unipotent,

5° $G(N/K)$ is solvable and $G^0(N/K)$ is unipotent,

6° $G(N/K)$ is solvable and semisimple,

7° $G(N/K)$ is solvable and unipotent,

8° $G(N/K)$ is finite,

9° $G(N/K)$ is solvable and finite,

10° $G(N/K) = \{id_N\}$.

Now we can prove the following theorem.

Theorem Let K, Δ and Θ be as above. Let N be a Picard-Vessiot extension of K, and U a universal differential extension field of N_Δ. Set $C = N_C$ ($= K_C$) and suppose that $C = C_a$. Let ν be a positive integer ≤ 10.

(a) If N is contained in a Liouvillian extension L of K (relative to the universal differential extension field U) of type $\nu°$, and if L is N-separable, then $G(N/K)$ is of type $\underline{\nu}°$.

(b) If $G(N/K)$ is of type $\underline{\nu}°$, then N is contained in a Liouvillian extension L of K (relative to the universal differential extension field U) of type $\nu°$.

Proof. (a) Suppose that L has the property (ii). By the proof of Lem.2 and the results of §6.3 and §6.4, we see that the factor group

$$G(N/K)/G(N/(K\langle y_1\rangle \cap N)) \simeq G((K\langle y_1\rangle \cap N)/K)$$

has the following properties:

(1) If y_1 is primitive over K, the factor group is abelian and unipotent.

(2) If y_1 is exponential over K, the factor group is abelian and semisimple.

(3) If y_1 is separably normally algebraic over K, the factor group is finite. If, in addition, y_1 is a separable radical over K, the factor group is finite and abelian (even cyclic).

Therefore, owing to Th.1~Th.3 of §8 of Chap.I of [1] and to the proof of Lem.2 above, we can prove that $G(N/K)$ is of type $\underline{\nu}°$ if L is of type $\nu°$ ($\nu \neq 3$). We have only to show here that $G(N/K)$ is of type $\underline{3}°$ provided L is of type $3°$.

Suppose that L is of type 3°. Then, we see by the proof of Lem.2 that G(N/K) has a normal chain of C-subgroups

$$(4)\quad G(N/K) = G_0,\ G_1,\ \cdots,\ G_r = \{id_N\}$$

each of whose factor groups is semisimple or finite. Consider the normal chain of C-subgroups

$$(5)\quad G(N/K) = G'_0,\ G^0(N/K) = G'_1,\ G'_2 = \{id_N\},$$

and apply to (4) and (5) Zassenhaus' proof of the theorem of Schreier. Thus, if we set

$$\left.\begin{aligned} G_{hj} &= G_h\cdot(G_{h-1}\cap G'_j) \quad (1 \le h \le r,\ 0 \le j \le 2) \\ G'_{jh} &= G'_j\cdot(G_h\cap G'_{j-1}) \quad (0 \le h \le r,\ 1 \le j \le 2) \end{aligned}\right\},$$

we obtain two normal chains of C-subgroups

$$(6)\quad G(N/K) = G_0 = G_{10},\ G_{11},\ G_{12} = G_1 = G_{20},\ G_{21},\ G_{22} = G_2 = G_{30},\ \cdots,\ G_{r-1,2} = G_{r-1} = G_{r0},\ G_{r1},\ G_{r2} = G_r = \{id_N\},$$

$$(7)\quad G(N/K) = G'_0 = G'_{10},\ G'_{11},\ \cdots,\ G'_{1r} = G'_1 = G^0(N/K) = G'_{20},\ G'_{21},\ \cdots,\ G'_{2,r-1},\ G'_{2r} = G'_2 = \{id_N\},$$

which are refinements of (4) and (5) respectively. We know that

$$G'_{2,h-1}/G'_{2h} \simeq G_{h1}/G_{h2} \quad (1 \le h \le r).$$

Since $G_{h0}/G_{h2} = G_{h-1}/G_h$ is semisimple or finite, so is its subgroup G_{h1}/G_{h2}. Therefore, G(N/K) is of type 3°.

(b) The assertion is trivially true for $\nu = 10$. For

$8 \leq \nu \leq 9$, let $G(N/K)$ consists of $\sigma_0 = id_N$, σ_1, ... , σ_{s-1}. Then the elementary symmetric expressions of $\sigma_j x$ $(0 \leq j \leq s-1)$ are contained in K for each element x of N. Hence, N is finitely separably normally algebraic over K because $C(\sigma_j) = C$ $(0 \leq j \leq s-1)$, and the assertion is true for $8 \leq \nu \leq 9$. Now, suppose that $1 \leq \nu \leq 7$. Since $G^0(N/K)$ is a normal C-subgroup of $G(N/K)$ of finite index, we see by Th.8 of §5.7 that there corresponds an intermediate differential field K' between K and N such that K' is purely inseparably algebraically closed in N, that N is a Picard-Vessiot extension of K', that $G^0(N/K) = G(N/K')$, that K' is a strongly normal extension of K, and that $G(N/K)/G^0(N/K) \simeq G(K'/K)$. Hence K' is finitely separably normally algebraic over K. If we regard $G^0(N/K)$ as the Galois group of N over K', then $G(N/K')$ is of type $\underline{2}°$, $\underline{2}°$, *-$\underline{6}°$, $\underline{7}°$, $\underline{7}°$, $\underline{6}°$ or $\underline{7}°$ according as $G(N/K)$ is of type $\underline{1}°$, $\underline{2}°$, $\underline{3}°$, $\underline{4}°$, $\underline{5}°$, $\underline{6}°$ or $\underline{7}°$, where the type *-$\underline{6}°$ means that $G(N/K')$ is solvable and *-semisimple. Moreover, if $G(N/K)$ is of type $\underline{2}°$, $\underline{5}°$, $\underline{6}°$ or $\underline{7}°$, then K' is an extension of K by separable radicals. Therefore, for our object, we need only to prove that if $G(N/K)$ is of type $\underline{2}°$, *-$\underline{6}°$, $\underline{6}°$ or $\underline{7}°$ and if $G(N/K)$ is connected except for type $\underline{7}°$, then N is contained in a Liouvillian extension (in N) of type 2°, 6°, 6° or 7° respectively over K.

Case I: $G(N/K)$ is of type $\underline{7}°$. By Th.2 of §7 of [1],

$G(N/K)$ is reducible to special triangular form. Hence, we can choose a fundamental system $x_1, \ldots, x_n$ of zeros of the defining system of linear differential forms so as to have $N = K\langle x_1,\ldots,x_n\rangle$ and

(8) $\sigma x_j = \sum_{h=1}^{j} x_h c_{hj}(\sigma)$ $(1 \leq j \leq n,\ c_{hj}(\sigma) \in C(\sigma),\ c_{jj} = 1)$

for each $\sigma \in G(N/K)$. We claim that N is of type 7° over K.

Since $\sigma x_1 = x_1$ for every $\sigma \in G(N/K)$, x_1 is contained in K.

If $n = 1$, then $N = K\langle x_1\rangle = K$, and the claim is trivially true.

Suppose $n > 1$. Then, (8) implies that

$$\sigma(x_j/x_1) = c_{1j}(\sigma) + \sum_{h=2}^{j}(x_h/x_1)c_{hj}(\sigma) \quad (2 \leq j \leq n,\ \sigma \in G(N/K)),$$

so that

$$\sigma(\theta(x_j/x_1)) = \sum_{h=2}^{j}\theta(x_h/x_1)c_{hj}(\sigma)$$
$$(2 \leq j \leq n;\ \theta \in \Theta,\ \mathrm{ord}\,\theta > 0;\ \sigma \in G(N/K)).$$

Therefore, making an appropriate induction assumption, and taking into consideration the fact that N is a finitely generated extension field of K, we see that if we set

$$M = K\langle \theta(x_2/x_1),\ldots,\theta(x_n/x_1) \mid \theta\in\Theta,\ \mathrm{ord}\theta>0 \rangle,$$

M is contained in a Liouvillian extension (in N) of type 7° over K and that N is M-separable. Since $x_2/x_1, \ldots, x_n/x_1$ are primitive over M, $N = K\langle x_2/x_1,\ldots,x_n/x_1\rangle = M(x_2/x_1,\ldots,$

x_n/x_1). If N is algebraic over M, then N is a Liouvillian extension of type 7° over K. On the contrary if N is not algebraic over M, we can suppose that $x_2/x_1, \ldots, x_s/x_1$ for some s with $2 \leq s \leq n$ is a separating transcendence basis of N over M. Then $M\langle x_2/x_1,\ldots,x_s/x_1\rangle = M(x_2/x_1,\ldots, x_s/x_1)$ is contained in a Liouvillian extension (in N) of type 7° over K, whence we can conclude as above that N is a Liouvillian extension of type 7° over K.

Case II: $G(N/K)$ is of type 6°. By Th.1 and Th.3 of §7 of [1], $G(N/K)$ is reducible to diagonal form. Hence, we can choose a fundamental system $x_1, \ldots, x_n$ of zeros of the defining system of linear differential forms so as to have $N = K\langle x_1,\ldots,x_n\rangle$ and

(9) $\sigma x_j = x_j \cdot c_j(\sigma)$ $(1 \leq j \leq n;\ c_j(\sigma) \in C(\sigma))$

for every $\sigma \in G(N/K)$. This implies that $\sigma(\theta x_j) = \theta x_j \cdot c_j(\sigma)$ $(1 \leq j \leq n;\ \theta \in \Theta;\ \sigma \in G(N/K))$, that $\sigma(\theta x_j/x_j) = \theta x_j/x_j$ $(1 \leq j \leq n;\ \theta \in \Theta;\ \sigma \in G(N/K))$, and that $\theta x_j/x_j \in K$ $(1 \leq j \leq n;\ \theta \in \Theta)$. Since $x_1, \ldots, x_n$ are exponential over K, we see by similar discussions as in Case I that $N = K(x_1,\ldots,x_n)$ is a Liouvillian extension of type 6° over K.

Case III: $G(N/K)$ is of type 2°. By Th.1 of §7 of [1], $G(N/K)$ is reducible to triangular form. Hence, we can choose a fundamental system $x_1, \ldots, x_n$ of zeros of the defining system of linear differential forms so as to have $N = K\langle x_1,\ldots, x_n\rangle$ and

(10) $\sigma x_j = \Sigma_{h=1}^{j} x_h \cdot c_{hj}(\sigma)$ $(1 \le j \le n;\ c_{hj}(\sigma) \in C(\sigma))$

foe each $\sigma \in G(N/K)$. We claim that N is contained in a Liouvillian extension of type 2° over K.

Since $\sigma x_1 = x_1 \cdot c_{11}(\sigma)$ $(\sigma \in G(N/K))$, x_1 is exponential over K as we saw in Case II.

If $n = 1$, then $N = K\langle x_1 \rangle$ is clearly a Liouvillian extension of type 2° over K.

Suppose $n > 1$. Then, (10) implies that

$$\sigma(x_j/x_1) = c_{1j}(\sigma)/c_{11}(\sigma) + \Sigma_{h=2}^{j}(x_h/x_1)\cdot(c_{hj}(\sigma)/c_{11}(\sigma))$$
$$(2 \le j \le n;\ \sigma \in G(N/K)),$$

so that

$$\sigma(\theta(x_j/x_1)) = \Sigma_{h=2}^{j}\theta(x_h/x_1)\cdot(c_{hj}(\sigma)/c_{11}(\sigma))$$
$$(2 \le j \le n;\ \theta \in \Theta,\ \mathrm{ord}\,\theta > 0;\ \sigma \in G(N/K)).$$

Therefore, making an appropriate induction assumption, and taking into consideration the fact that N is finitely generated extension field of K, we see that if we set

$$M = K\langle \theta(x_2/x_1), \ldots, \theta(x_n/x_1) \mid \theta \in \Theta,\ \mathrm{ord}\,\theta > 0 \rangle$$

M is contained in a Liouvillian extension (in N) of type 2° over K, and N is M-separable. Since $x_2/x_1, \ldots, x_n/x_1$ are primitive over M, and since x_1 is exponential over M, $N = K\langle x_1, x_2/x_1, \ldots, x_n/x_1 \rangle = M(x_1, x_2/x_1, \ldots, x_n/x_1)$. Then, by similar discussions as in Case I, we see that N is a Liouvillian extension of type 2° over K.

Case IV: $G(N/K)$ is of type *-$\underline{6}$°. $G(N/K)$ has a normal chain of C-subgroups

(11) $G(N/K) = G_0, G_1, \cdots, G_{s-1}, G_s = \{id_N\}$,

each of whose factor groups is semisimple or finite. Let the ascending chain of the corresponding intermediate fields between K and N be

(12) $K = M_0, M_1, \cdots, M_{s-1}, M_s = N$.

Then N is a Picard-Vessiot extension of M_j for each j $(0 \leq j \leq s)$. If the factor group G_{j-1}/G_j is finite for some j $(1 \leq j \leq s)$, then M_j is a strongly normal extension and an extension by radicals over M_{j-1} with $G(M_j/M_{j-1}) \simeq G_{j-1}/G_j$ solvable, and we see that a refinement $M_{j-1} = M_{j-1,0}, M_{j-1,1}, \cdots, M_{j-1,t-1}, M_{j-1,t} = M_j$ and a corresponding refinement $G_{j-1} = G_{j-1,0}, G_{j-1,1}, \cdots, G_{j-1,t-1}, G_{j-1,t} = G_j$ exists such that $M_{j-1,h}$ is an extension by a radical of prime degree over $M_{j-1,h-1}$ (whence $M_{j-1,h}$ is a strongly normal extension of $M_{j-1,h-1}$) with $G(M_{j-1,h}/M_{j-1,h-1}) \simeq G_{j-1,h-1}/G_{j-1,h}$ cyclic (whence semisimple) for each h $(1 \leq h \leq t)$. This implies by Th.3 of §8 of [1] that $G(N/K)$ is of type $\underline{6}$°. Thus Case IV is reduced to Case II.

Kôtaro Okugawa
28 Okazaki-Tokusei-cho
Sakyo-ku, Kyoto
606, Japan

BIBLIOGRAPHY

[0] Chevalley, C. and E. Kolchin: Two proofs of a theorem on algebraic groups, Proc. Amer. Math. Soc., Vol.2, pp.126~134.

[1] Kolchin, E. R.: Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations, Ann. Math., Vol.49 (1948), pp.1~42.

[2] _____: Picard-Vessiot theory of partial differential fields, Proc. Amer. Math. Soc., Vol.3 (1952), pp.596~603.

[3] _____: Galois theory of differential fields, Amer. J. Math., Vol.LXXV (1953), pp.753~824.

[4] _____: Differential algebra and algebraic groups, Acad. Press, 1973. (This book contains a complete bibliography on the subject.)

[5] Okugawa, K.: Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory, J. Math. Kyoto Univ., Vol.2 (1963), pp.295~322.

[6] _____: Two topics concerning differential algebras of nonzero characteristic, Acta Hum. Sci., Univ. Sangio Kyotiensis, Vol.XI, Nat. Sci. Ser. (1982), pp.1~8.

[7] Shikishima, K.: Universal extension of a differential field of positive characteristic, Acta Hum. Sci., Univ. Sangio Kyotiensis, Vol.VII, Nat. Sci. Ser. (1978), pp.32~41.

[8] _____: Maximal differential field and its applications, Acta Hum. Sci., Univ. Sangio Kyotiensis, Vol.IX,

Nat. Sci. Ser. (1980), pp.1~10.

[9] Suzuki, S.: Some types of derivations and their applications to field theory, J. Math. Kyoto Univ., Vol.21 (1981), pp.375~382.

[10] Tsuji, K.: Galois theory of differential fields of positive characteristic (in preparation).

[11] _____: Differential closue of a differential field of positive characteristic, J. Math. Kyoto Univ., Vol.26 (1986), pp.711~715.

[12] Weil, A.: Foundations of algebraic geometry, Revised and enlarged edition, Amer. Math. Soc. Coloq. Publ., Vol.XXIX, 1962.

[13] Zariski, O. and P. Samuel: Commutative algebra, I and II, D. Van Nostrand, 1958~60.

Index of Notations

Index of Terminologies

LECTURES IN MATHEMATICS, KYOTO UNIVERSITY

No. 12	Brauer, R.—Theory of Group Characters	$ 10.50
No. 13	Lê Dũng Tráng—Geometry of Tangents on Singular Spaces and Chern Classes	o/s
No. 14.	Hirai, T. and Schiffman G. (Eds.)—Lectures on Harmonic Analysis on Lie Groups and Related Topics	$ 36.40
No. 15.	Matsuda, M.—Lectures on Algebraic Solutions of Hypergeometric Differential Equations	$ 17.00

Printed by Tokyo Press Co., Ltd., Tokyo, Japan

Printed in Japan