J. Math. Kyoto Univ.
2-3 (1963) 295-322.

Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory

Dedicated to Prof. Y. Akizuki for celebration of his 60-th birthday

By

Kôtaro OKUGAWA

(Received June 8, 1963)

E. R. Kolchin has developed the Picard-Vessiot theory and, more generally, the Galois theory for differential fields of characteristic zero[1]. In these theories, Galois groups are algebraic matric groups or, more generally, algebraic groups; every algebraic group appears as a Galois group, and its structure supplies knowledges about the structure of the differential field-extension. The purpose of the present work is to construct a similar theory of differential fields of an arbitrary characteristic.

By the way, the basic theory of differential fields in the case of characteristic zero is well equipped by Ritt, Kolchin and others, and effectively applied to various problems[2]. But, it may be said that the basic theory in the case of non-zero characteristic is not yet sufficiently made up[3]. Not a few part of difficulties in the latter case are due to the definition of differential fields which is done literally in the same manner as in the former case. If we define them anew by means of Hasse's higher differentiations[4], computations become very troublesome, but we get available results.

1) Kolchin [4-8]. See also Matsumura [9].
2) Ritt [11], Kolchin [4] and [6]. These contain bibliographies on the subject.
3) Kolchin [3], Seidenberg [13], Kaplansky [2] and Okugawa [10].
4) Hasse [1] and Schmidt-Hasse [12].

Thus, we can obtain a generalization of Kolchin's theory of Picard-Vessiot extensions in the case of an arbitrary characteristic.

This paper consists of two characters. Chapter I contains a new definition of differential fields of an arbitrary characteristic and a sketch of various results. In Chapter II, these basic results are applied to develop a theory of Picard-Vessiot extensions of an arbitrary characteristic.

Chapter I. Differential algebra

When we speak of a *ring* in this chapter, it is always supposed tacitly that the ring is commutative and contains a subfield whose unity coincides with that of the ring. All the fields, which appear in this paper, are of an arbitrary fixed characteristic p (zero or non-zero).

1. Differentiations

Let $\delta=\{\delta_\nu\,;\ \nu=0,1,2,\cdots\}$ be an infinite sequence of maps δ_ν of a ring $\boldsymbol{R}$ into itself. We shall call δ a *differentiation* in $\boldsymbol{R}$ if it satisfies the conditions:

(D1) $\delta_0 x = x$, (D2) $\delta_\nu(x+y) = \delta_\nu x+\delta_\nu y$,

(D3) $\delta_\nu(xy) = \sum_{\nu_1+\nu_2=\nu} \delta_{\nu_1}x\cdot\delta_{\nu_2}y$, (D4) $\delta_\lambda(\delta_\mu x) = \binom{\lambda+\mu}{\lambda}\delta_{\lambda+\mu}x$,

whenever $x,\ y\in\boldsymbol{R}$ and $\lambda,\ \mu,\ \nu$ are non-negative integers. From (D1–4), we see:

1° each δ_ν is an endomorphism of the additive group of $\boldsymbol{R}$;

2° δ_1 is a usual derivation in $\boldsymbol{R}$;

3° if n is a positive integer, $x_1,\cdots,x_n,\ x\in\boldsymbol{R}$ and if $\nu,\ \lambda_1,\cdots,\lambda_n$ are non-negative integers, then we have

(D3′) $$\delta_\nu(x_1\cdots x_n) = \sum_{\nu_1+\cdots+\nu_n=\nu} \delta_{\nu_1}x_1\cdot\cdots\cdot\delta_{\nu_n}x_n,$$

(D4′) $$\delta_{\lambda_1}\cdots\delta_{\lambda_n}x = \frac{(\lambda_1+\cdots+\lambda_n)!}{\lambda_1!\cdots\lambda_n!}\delta_{\lambda_1+\cdots+\lambda_n}x;$$

4° as particular cases of (D4′), we get

$$(\mathrm{D4}'')\quad \delta_1^\nu = \nu!\,\delta_\nu\,(\nu\geqslant 0)\,,\qquad (\mathrm{D4}''')\quad \delta_\lambda^\nu = \frac{(\lambda\nu)!}{(\lambda!)^\nu}\delta_{\lambda\nu}\,(\lambda\geqslant 0,\ \nu\geqslant 0)\,,$$

so that

(a) in case $p=0$, δ is determined by δ_1 (cf. Ex. 1.1 below),

(b) in case $p\neq 0$,

$$\delta_1^{c_0}\delta_p^{c_1}\delta_{p^2}^{c_2}\cdots\delta_{p^\alpha}^{c_\alpha} = [\nu!/(p!)^{c_1}(p^2!)^{c_2}\cdots(p^\alpha!)^{c_\alpha}]\,\delta_\nu\,(\nu\geqslant 0)\,,$$

where $\nu=\sum_{e=0}^{\alpha} c_e p^e\ (0\leqslant c_e\leqslant p-1)$ is the p-adic expression of a non-negative integer ν; since the integer in the [ ] is not divisible by p, δ is determined by $\delta_{p^e}\,(0\leqslant e<\infty)$[5];

5° $\delta_\nu c = 0\,(\nu>0)$ for every element c of the prime field in $\boldsymbol{R}$.

We shall have occasions to use the following lemma:

LEMMA 1.1. *Let δ be a differentiation in a ring $\boldsymbol{R}$, $x\in\boldsymbol{R}$, $p\neq 0$, e a positive integer and α an integer >1. Then,*

$$(1.1)\qquad \delta_\lambda(x^{p^e}) = 0 \quad \textit{if}\quad \lambda\not\equiv 0\ (\mathrm{mod.}\ p^e)\,,$$

$$(1.2)\qquad \left.\begin{aligned} \delta_\lambda(x^{p^e}) &= (\delta_\nu x)^{p^e} \\ \delta_\lambda(x^{\alpha p^e}) &= \alpha(x^{\alpha-1}\cdot\delta_\nu x)^{p^e}+[\cdots] \end{aligned}\right\}$$
$$\textit{if}\quad \lambda\equiv 0\ (\mathrm{mod.}\ p^e)\quad \textit{and}\quad \lambda=\nu p^e\,,$$

where the part $[\cdots]$ *contains none of* $\delta_\rho x\ (\rho\geqslant\nu)$.

The proof is easy by virtue of (D3′), taking into account that $\alpha^p\equiv\alpha\ (\mathrm{mod.}\ p)$.

EXAMPLE 1.1. If $\boldsymbol{R}$ is a ring, $p=0$ and D a derivation in $\boldsymbol{R}$, then $\delta=\{\delta_\nu=(1/\nu!)D^\nu;\ \nu\geqslant 0\}$ is a differentiation in $\boldsymbol{R}$.

EXAMPLE 1.2. Let $\boldsymbol{R}$ be a ring and $\boldsymbol{R}_U$ the ring of formal

---

5) If $\lambda=\sum_{k\geqslant 0} a_k p^k$ is the p-adic expression of a non-negative integer λ and if $p^{N(\lambda)}$ is the maximum power of p which divides $\lambda!$, then we see at once that $N(\lambda)=(\lambda-\sum_{k\geqslant 0} a_k)/(p-1)$. From this, it can be proved without difficulty that, when $\lambda_i=\sum_{k\geqslant 0} a_{ik}p^k\ (1\leqslant i\leqslant n)$, $\lambda_1+\cdots+\lambda_n=\sum_{k\geqslant 0} b_k p^k$ are p-adic expressions of a finite number of non-negative integers $\lambda_1,\cdots,\lambda_n$ and their sum, then $(\lambda_1+\cdots+\lambda_n)!/\lambda_1!\cdots\lambda_n!$ is not divisble by p if and only if $\sum_{i=1}^{n} a_{ik}=b_k$ for every k.

power series of m indeterminates $U_1, \cdots, U_m$ over $\boldsymbol{R}$. For every element

$$P=\sum_{\rho_1\geqslant 0,\cdots,\rho_m\geqslant 0} a_{\rho_1\cdots\rho_m} U_1^{\rho_1}\cdots U_m^{\rho_m}\ (a_{\rho_1\cdots\rho_m}\in \boldsymbol{R})$$

of $\boldsymbol{R}_U$, every integer i with $1\leqslant i\leqslant m$ and every non-negative integer ν, put

$$d_{i\nu}P=\sum_{\rho_1\geqslant 0,\cdots,\rho_m\geqslant 0}\binom{\rho_i}{\nu} a_{\rho_1\cdots\rho_m} U_1^{\rho_1}\cdots U_i^{\rho_i-\nu}\cdots U_m^{\rho_m}.$$

Then, every one of the m sequences $d_i=\{d_{i\nu}\,;\,\nu\geqslant 0\}$ $(1\leqslant i\leqslant m)$ is a differentiation in $\boldsymbol{R}_U$. For each i, d_i will be called the *formal differentiation* with respect to U_i. We see at once that $d_{i\lambda}d_{j\mu}=d_{j\mu}d_{i\lambda}$ $(1\leqslant i\leqslant m,\ 1\leqslant j\leqslant m,\ i\neq j,\ \lambda\geqslant 0,\ \mu\geqslant 0)$.

Two differentiations $\delta=\{\delta_\nu\,;\,\nu\geqslant 0\}$, $\delta'=\{\delta'_\nu\,;\,\nu\geqslant 0\}$ in a ring $\boldsymbol{R}$ will be called *commutative* if $\delta_\lambda\delta'_\mu=\delta'_\mu\delta_\lambda$ for every pair λ, μ $(\lambda\geqslant 0,\ \mu\geqslant 0)$.

2. Differential rings and differential fields

The composite notion of a ring (field) $\boldsymbol{R}$ and a finite number of mutually commutative differentiations $\delta_i=\{\delta_{i\nu}\,;\,\nu\geqslant 0\}$ $(1\leqslant i\leqslant m)$ in $\boldsymbol{R}$ is called a *differential ring* (*field* respectively). It is denoted by $(\boldsymbol{R}, \delta_1, \cdots, \delta_m)$: if the associated differentiations are clear, it may be denoted simply by $\boldsymbol{R}$. We shall call the differential ring (field) $\boldsymbol{R}$ *ordinary* or *partial* according as $m=1$ or >1.

If a differential ring (field) $(\boldsymbol{R}, \delta_1, \cdots, \delta_m)$ is given, we regard the set $\Theta=\{\delta_{1\nu_1}\cdots\delta_{m\nu_m}\,;\,\nu_1\geqslant 0, \cdots, \nu_m\geqslant 0\}$ as a domain of operators on $\boldsymbol{R}$; every element $\theta=\delta_{1\nu_1}\cdots\delta_{m\nu_m}$ is called a *differential operator* and $\nu_1+\cdots+\nu_m$ is called the *order* of θ which is denoted by $\operatorname{ord}\theta$. If $x\in\boldsymbol{R}$, $\theta\in\Theta$, then θx and $\operatorname{ord}\theta$ are called a *derivative* of x and the *order* of the derivative θx of x. Notions such as *differential subring* (*subfield*), *differential extension ring* (*field*), *differential ideal*, *differential homomorphism* and so on are defined canonically in view of the domain Θ of differential operators; namely, they are defined as admissible ones under the operator-domain Θ. If an element $c\in\boldsymbol{R}$ is such that $\delta_{i\nu}c=0$ for every pair i, ν $(1\leqslant i\leqslant m,\ \nu>0)$, then c is called a *constant* of $\boldsymbol{R}$. The set of all constants in a differential ring $\boldsymbol{R}$ makes obviously a subring; it is called the *ring of constants* of $\boldsymbol{R}$. If, in particular, $\boldsymbol{R}$ is a differential field, we see that the set of all constants makes a subfield; this is called the *field of constants* of $\boldsymbol{R}$.

Let $\boldsymbol{S}$ be a differential ring (field), $\boldsymbol{R}$ a differential subring (subfield) and $\boldsymbol{m}$ a subset of $\boldsymbol{S}$. The ring (field) which is generated over $\boldsymbol{R}$ by all derivatives of all elements of $\boldsymbol{m}$ is the smallest differential subring (subfield) of $\boldsymbol{S}$ which contains $\boldsymbol{R}$ and $\boldsymbol{m}$; we shall denote it by $\boldsymbol{R}\{\boldsymbol{m}\}$ ($\boldsymbol{R}\langle\boldsymbol{m}\rangle$). The ideal which is generated in $\boldsymbol{S}$ by all derivatives of all elements of $\boldsymbol{m}$ is the smallest differential ideal of $\boldsymbol{S}$ that contains $\boldsymbol{m}$; it is denoted by $((\boldsymbol{m}))$.

PROPOSITION 2.1. *If $\mathfrak{a}$ is a differential ideal of a differential ring $(\boldsymbol{R}, \delta_1, \cdots, \delta_m)$, then the radical ideal $\mathfrak{m}$ of $\mathfrak{a}$ is a differential semiprime ideal*[6] *of $\boldsymbol{R}$.* (Compare this with the result in [3], p. 117.)

In case $p=0$, this is well-known since $\delta_{i\nu}=(1/\nu!)\delta_{i1}{}^{\nu}$ $(1\leqslant i\leqslant m, \nu\geqslant 0)$. In case $p\neq 0$, for every $x\in\mathfrak{m}$, there exists an integer $e>0$ with $x^{p^e}\in\mathfrak{a}$; hence $(\delta_{i\nu}x)^{p^e}=\delta_{i,\nu p^e}(x^{p^e})\in\mathfrak{a}$ by Lem. 1.1., so that $\delta_{i\nu}x\in\mathfrak{m}$ $(1\leqslant i\leqslant m, \nu\geqslant 0)$.

PROPOSITION 2.2. *If $\mathfrak{m}$ is a differential semiprime ideal of a differential ring $(\boldsymbol{R}, \delta_1, \cdots, \delta_m)$ and $\boldsymbol{n}$ a non-empty subset of $\boldsymbol{R}$, then the quotient ideal $\mathfrak{m}:\boldsymbol{n}$ in $\boldsymbol{R}$ is a differential semiprime ideal of $\boldsymbol{R}$.*

If $x\in\mathfrak{m}:\boldsymbol{n}$, then $xz\in\mathfrak{m}$ for every $z\in\boldsymbol{n}$, hence $\delta_{i\nu}x\cdot z+\sum_{\lambda=0}^{\nu-1}\delta_{i\lambda}x\cdot\delta_{i,\nu-\lambda}z=\delta_{i\nu}(xz)\in\mathfrak{m}$. Assuming inductively that $\delta_{i\lambda}x\in\mathfrak{m}:\boldsymbol{n}$ $(0\leqslant\lambda<\nu)$, we get $\delta_{i\nu}x\cdot z^2\in\mathfrak{m}$, and consequently $(\delta_{i\nu}x\cdot z)^2\in\mathfrak{m}$ so that $\delta_{i\nu}x\cdot z\in\mathfrak{m}$. Since this is true for every $z\in\mathfrak{m}$, we have $\delta_{i\nu}x\in\mathfrak{m}:\boldsymbol{n}$.

Let $(\boldsymbol{R}, \delta_1, \cdots, \delta_m)$ be a differential ring and $\mathfrak{a}$ a differential ideal of $\boldsymbol{R}$ not containing 1. Since $\mathfrak{a}$ is an admissible ideal of the ring $\boldsymbol{R}$ under the domain Θ of differential operators, Θ can be regarded canonically as a domain of operators on the quotient ring $\boldsymbol{R}/\mathfrak{a}$. Thus, $\boldsymbol{R}/\mathfrak{a}$ is a differential ring associated with the differentiations $\delta_1, \cdots, \delta_m$. The canonical map of $\boldsymbol{R}$ onto the differential

6) An ideal is called *semiprime* if it coincides with its radical ideal.

ring $\boldsymbol{R}/\mathfrak{a}$ is a differential homomorphism.

Let $(R, \delta_1, \cdots, \delta_m)$ be a differential ring. Now, consider the ring $\boldsymbol{R}_U$ of Ex. 1.2 which is regarded as a differential ring associated with the differentiations $d_1, \cdots, d_m$. If $\theta = \delta_{1\nu_1} \cdots \delta_{m\nu_m}$ is an element of the domain Θ of differential operators of $\boldsymbol{R}$, we denote by U_θ the monomial $U_1^{\nu_1} \cdots U_m^{\nu_m}$. Assigning to every $x \in \boldsymbol{R}$ the element $E(x) = \sum_{\theta \in \Theta} \theta x \cdot U_\theta$ of $\boldsymbol{R}_U$, we get a differential isomorphism E of $\boldsymbol{R}$ into $\boldsymbol{R}_U$, which is called the *Taylor expansion* of $\boldsymbol{R}$.

LEMMA 2.1. *For every choice of non-negative integers $\nu_1, \cdots, \nu_m$, let $\delta_{\nu_1 \cdots \nu_m}$ be a map of a ring $\boldsymbol{R}$ into itself, such that $\delta_{0 \cdots 0}$ is the identity map and the map $x \to E'(x) = \sum_{\nu_1, \cdots, \nu_m} \delta_{\nu_1 \cdots \nu_m} x \cdot U_1^{\nu_1} \cdots U_m^{\nu_m}$ of $\boldsymbol{R}$ into the ring $\boldsymbol{R}_U$ of Ex. 1.2 is a ring-homomorphism with $E'(\delta_{\nu_1 \cdots \nu_m} x) = d_{1\nu_1} \cdots d_{m\nu_m} E'(x)$ $(\nu_1 \geqslant 0, \cdots, \nu_m \geqslant 0)$. Then, putting $\delta_{i\nu_i} = \delta_{0 \cdots \nu_i \cdots 0}$ $(1 \leqslant i \leqslant m, \nu \geqslant 0)$, $\boldsymbol{R}$ becomes a differential ring associated with the differentiations $\delta_i = \{\delta_{i\nu}; \nu \geqslant 0\}$ $(1 \leqslant i \leqslant m)$, where $\delta_{1\nu_1} \cdots \delta_{m\nu_m} = \delta_{\nu_1 \cdots \nu_m}$ and E' is the Taylor expansion of the differential ring $\boldsymbol{R}$.*

PROPOSITION 2.3. *If $(\boldsymbol{R}, \delta_1, \cdots, \delta_m)$ is a differential ring and $\boldsymbol{S}$ the total ring of quotients of $\boldsymbol{R}$, then we can prolong $\delta_1, \cdots, \delta_m$ uniquely to $\boldsymbol{S}$ so that $\boldsymbol{S}$ obtains a structure of a differential extension ring of $\boldsymbol{R}$.*

It is easy to prove this directly, but we get a shorter proof applying Lem. 2.1. We omit the proof here. By the way, If we denote the prolongations by the same symbols $\delta_1, \cdots, \delta_m$ as the given differentiations in $\boldsymbol{R}$ and write each $z \in \boldsymbol{S}$ in the form $z = x/y$ $(x, y \in \boldsymbol{R}$, y being non-zerodivisor in $\boldsymbol{R})$, then $\delta_{i\nu} z$ can be defined by induction on ν, using the equation

$$(2.1) \qquad \delta_{i\nu} x = \delta_{i\nu} z \cdot y + \sum_{\lambda=0}^{\nu-1} \delta_{i\lambda} z \cdot \delta_{i, \nu-\lambda} y \quad (1 \leqslant i \leqslant m, \ \nu \geqslant 0).$$

PROPOSITION 2.4. *Let σ be a differential isomorphism of a differential ring $(\boldsymbol{R}, \delta_1, \cdots, \delta_m)$ onto a differential ring $(\boldsymbol{R}', \delta_1, \cdots, \delta_m)$, each pair of corresponding differentiations being denoted by the same symbols, and $\boldsymbol{S}, \boldsymbol{S}'$ the differential total rings of quotients of $\boldsymbol{R}, \boldsymbol{R}'$ respectively. Then, the prolongation isomorphism of the ring $\boldsymbol{S}$ onto* *the ring* S', *which is uniquely determined, is a differential isomorphism of* S *onto* S'.

The proof is obvious by virtue of the equation (2.1).

PROPOSITION 2.5. *If* $(F, \delta_1, \cdots, \delta_m)$ *is a differential field and* G *a separably algebraic extension field of* F, *then we can prolong* $\delta_1, \cdots, \delta_m$ *uniquely to* G *so that* G *obtains a structure of a differential extension field of* F.

In order to prove this, we may suppose that $[G:F]<\infty$, and consequently, G is generated over F by an element x which is a zero of a polynomial $f(X)=\sum_{k=0}^{n} a_k X^k$ $(a_k \in F, a_n=1)$ irreducible over F. Thus, the proof can be easily done by means of Lem. 2.1. We remark that, in view of the uniqueness, if we denote the prolongations by the same symbols $\delta_1, \cdots, \delta_m$ as the given differentiations in R, then $\delta_{i\nu}x$ can be defined inductively by means of the equation

$$\frac{df}{dX}(x)\cdot\delta_{i\nu}x+\sum_{k=0}^{n}\sum_{\substack{\nu_0+\cdots+\nu_k=\nu \\ \nu_1<\nu,\cdots,\nu_k<\nu}}\delta_{i\nu_0}a_k\cdot\delta_{i\nu_1}x\cdot\cdots\cdot\delta_{i\nu_k}x=0 \qquad (1\leqslant i\leqslant m,\ \nu\geqslant 0), \tag{2.2}$$

so that, for every $y=\sum_{k=0}^{n-1} b_k x^k \in G$ $(b_k \in F)$,

$$\delta_{i\nu}y=\sum_{k=0}^{n-1}\sum_{\nu_0+\cdots+\nu_k=\nu}\delta_{i\nu_0}b_k\cdot\delta_{i\nu_1}x\cdot\cdots\cdot\delta_{i\nu_k}x \quad (1\leqslant i\leqslant m,\ \nu\geqslant 0). \tag{2.3}$$

PROPOSITION 2.6. *Let* σ *be a differential isomorphism of a differential field* $(F, \delta_1, \cdots, \delta_m)$ *onto a differential field* $(F', \delta_1, \cdots, \delta_m)$, *and* G *a separably algebraic differential extension field of* F. *Then, any isomorphism, which is a prolongation of* σ, *of* G *onto a (separably algebraic, and consequently differential) extension field* G' *of* F *is a differential isomorphism.*

The proof is obvious by virtue of the equations (2.2) and (2.3).

3. Differential polynomials

Let $(R, \delta_1, \cdots, \delta_m)$ be a differential ring. If $x_1, \cdots, x_n$ are elements of a differential extension ring of R and θx_j $(\theta \in \Theta, 1\leqslant j\leqslant n)$ satisfy no polynomial relation over R, then $x_1, \cdots, x_n$ are called *differentially independent* over R.

Now, let $X_j(\nu_1, \cdots, \nu_m)$ ($j \in J$ and $\nu_1, \cdots, \nu_m$ being non-negative integers) be a set of indeterminates over $\boldsymbol{R}$ and $\boldsymbol{S}=\boldsymbol{R}[X_j(\nu_1, \cdots, \nu_m)$; $j \in J$, $\nu_1 \geqslant 0, \cdots, \nu_m \geqslant 0]$. Prolong $\delta_{i\nu}(1 \leqslant i \leqslant m, \nu \geqslant 0)$ to $\boldsymbol{S}$ as follows: denoting the prolongations by the same symbols $\delta_{i\nu}$,

1° $\delta_{i\nu} X_j(\nu_1, \cdots, \nu_m) = \binom{\nu+\nu_i}{\nu} X_j(\nu_1, \cdots, \nu+\nu_i, \cdots, \nu_m)$
$(j \in J,\ \nu_1 \geqslant 0, \cdots, \nu_m \geqslant 0)$;

2° for a monomial $M = aY_1 \cdots Y_r$ ($a \in \boldsymbol{R}$ and $Y_1, \cdots, Y_r$ being some of $X_j(\nu_1, \cdots, \nu_m)$ $(j \in J,\ \nu_1 \geqslant 0, \cdots, \nu_m \geqslant 0)$),

$$\delta_{i\nu} M = \sum_{\nu_0+\cdots+\nu_r=\nu} \delta_{i\nu_0} a \cdot \delta_{i\nu_1} Y_1 \cdot \cdots \cdot \delta_{i\nu_r} Y_r ;$$

3° for a finite number of such monomials $M_1, \cdots, M_s$ as in 2°,

$$\delta_{i\nu} (\sum_{k=1}^{s} M_k) = \sum_{k=1}^{s} \delta_{i\nu} M_k .$$

Then, $(\boldsymbol{S}, \delta_1, \cdots, \delta_m)$ becomes a differential extension ring of $\boldsymbol{R}$. Denote $X_j(0, \cdots, 0)$ by X_j, then $X_j(\nu_1, \cdots, \nu_m) = \delta_{1\nu_1} \cdots \delta_{m\nu_m} X_j$ $(j \in J,\ \nu_1 \geqslant 0, \cdots, \nu_m \geqslant 0)$ so that $\boldsymbol{S} = \boldsymbol{R}\{X_j ; j \in J\}$. The $X_j (j \in J)$ are differentially independent over $\boldsymbol{R}$. Elements of $\boldsymbol{S}$ are called *differential polynomials* of $X_j (j \in J)$ over $\boldsymbol{R}$. As a special case, if $\boldsymbol{R}$ is a differential field $\boldsymbol{F}$, we get the differential field of quotients $\boldsymbol{G} = \boldsymbol{F}\langle X_j ; j \in J \rangle$ of $\boldsymbol{S}$.

PROPOSITION 3.1. *If $(\boldsymbol{R}, \delta_1, \cdots, \delta_m)$ is a differential ring and $X_j (j \in J)$ a set of differentially independent elements over $\boldsymbol{R}$, then every constant of $\boldsymbol{S} = \boldsymbol{R}\{X_j ; j \in J\}$ is contained in $\boldsymbol{R}$.*

Proof. In order to prove this, it is enough to consider the special case where $\boldsymbol{R}$ is an ordinary differential ring associated with a single differentiation $\delta = \{\delta_\nu ; \nu \geqslant 0\}$ and a single differentially independent element X over $\boldsymbol{R}$. We shall prove, for each $A \in \boldsymbol{S} = \boldsymbol{R}\{X\}$ with $A \notin \boldsymbol{R}$, the existence of a positive integer μ such that $\delta_\mu A \neq 0$. There are two alternative cases as follows.

Case I: there exist some derivatives of X which are contained in A with exponents not divisible by p. (This case is the only possible one if $p=0$.)

Among such derivatives of X, let $\delta_\nu X$ be the one of the highest order. Write A in the form $A=\sum_{i=0}^{\alpha} A_i(\delta_\nu X)^i$, where A_i are polynomials of $(\delta_\rho X)^p$ $(\rho \geqslant \nu)$ and $\delta_\sigma X$ $(\sigma < \nu)$ over $\boldsymbol{R}$, $\alpha > 0$ and $A_\alpha \neq 0$, and where, furthermore, $\alpha \leqslant p-1$ provided $p \neq 0$. Choose a positive integer μ such that $\binom{\mu+\nu}{\mu}$ is not divisible by p (see footnote 5). Since each term of A_i is of the form

$$a(\delta_{\rho_1}X)^{\beta_1 p^{e_1}} \cdots (\delta_{\rho_r}X)^{\beta_r p^{e_r}} (\delta_{\sigma_1}X)^{f_1} \cdots (\delta_{\sigma_s}X)^{f_s}$$

$$\left(\begin{array}{l} a \in R;\ r,\ s \ \text{ being non-negative integers;} \\ \rho_1 \geqslant \nu,\ \cdots,\ \rho_r \geqslant \nu,\ \ \sigma_1 < \nu,\ \cdots,\ \sigma_s < \nu; \\ \rho_1,\ \cdots,\ \rho_r,\ \sigma_1,\ \cdots,\ \sigma_s \ \text{ being distinct;} \\ \beta_1,\ \cdots,\ \beta_r \ \text{ being positive integers not divisible by } p; \\ e_1,\ \cdots,\ e_r,\ f_1,\ \cdots,\ f_s \ \text{ being positive integers} \end{array}\right)$$

$\delta_\mu(A_i(\delta_\nu X)^i)$ is a sum of parts of the form

$$\sum_{\substack{\lambda_0+\cdots+\lambda_r \\ +\tau_1+\cdots+\tau_s+\omega_1+\cdots+\omega_i=\mu}} \delta_{\lambda_0}a \cdot \delta_{\lambda_1}\{(\delta_{\rho_1}X)^{\beta_1 p^{e_1}}\} \cdots \delta_{\tau_1}\{(\delta_{\sigma_1}X)^{f_1}\} \cdots \delta_{\omega_1}(\delta_\nu X) \cdots \delta_{\omega_i}(\delta_\nu X)\,.$$

Using (1.2) and observing $\delta_\rho X (\rho \geqslant \mu+\nu)$, we get

$$\delta_\mu(A_i(\delta_\nu X)^i) = i\binom{\mu+\nu}{\mu}(\delta_\nu X)^{i-1}(\delta_{\mu+\nu}X)A_i + [\cdots]\,,$$

where the $[\cdots]$ is a polynomial of $(\delta_\rho X)^p$ $(\rho \geqslant \mu+\nu)$ and $\delta_\sigma X$ $(\sigma < \mu+\nu)$ over $\boldsymbol{R}$. Hence,

$$\delta_\mu A = (\partial A/\partial(\delta_\nu X)) \cdot \binom{\mu+\nu}{\mu} \cdot \delta_{\mu+\nu}X + [\cdots] \tag{3.1}$$

(the $[\cdots]$ being as above),

so that $\delta_\mu A \neq 0$.

Case II: every derivative of X is contained in A exclusively with exponents divisible by p. (In this case, we have necessarily $p \neq 0$.)

Let $\delta_{\nu_1}X, \cdots, \delta_{\nu_r}X$ be all the distinct derivatives of X which are actually contained in A. Denote by $e(\nu_1), \cdots, e(\nu_r)$ the positive integers such that A is a polynomial of $(\delta_{\nu_1}X)^{p^{e(\nu_1)}}, \cdots, (\delta_{\nu_r}X)^{p^{e(\nu_r)}}$ over $\boldsymbol{R}$ and each of $e(\nu_1), \cdots, e(\nu_r)$ is taken as large as possible, and put $e=\max(e(\nu_1), \cdots, e(\nu_r))$, $\mu=p^f$, $\lambda=\mu p^e$ and $\mu_i=\lambda/p^{e(\nu_i)}$ $(1 \leqslant i \leqslant r)$, where f is a sufficiently large positive integer such that

$\binom{\mu_i+\nu_i}{\mu_i}$ $(1 \leqslant i \leqslant r)$ are not divisible by p (see footnote 5). For each term

$$M = a(\delta_{\nu_1}X)^{\alpha_1 p^{e(\nu_1)}} \cdots (\delta_{\nu_r}X)^{\alpha_r p^{e(\nu_r)}}$$
$$(a \in \boldsymbol{R}\,;\ \alpha_1, \cdots, \alpha_r \text{ being non-negative integers})$$

of A, let us observe the derivative of X of the highest order in $\delta_\lambda M$. Using (1.2), we get

$$\begin{aligned}\delta_\lambda M &= a\alpha_1 \left\{\binom{\mu_1+\nu_1}{\mu_1}(\delta_{\nu_1}X)^{\alpha_1-1}\delta_{\mu_1+\nu_1}X\right\}^{p^{e(\nu_1)}} (\delta_{\nu_2}X)^{\alpha_2 p^{e(\nu_2)}}\cdots(\delta_{\nu_r}X)^{\alpha_r p^{e(\nu_r)}} \\ &+\cdots \\ &+ a\alpha_r\left\{\binom{\mu_r+\nu_r}{\mu_r}(\delta_{\nu_r}X)^{\alpha_r-1}\delta_{\mu_r+\nu_r}X\right\}^{p^{e(\nu_r)}}(\delta_{\nu_1}X)^{\alpha_1 p^{e(\nu_1)}}\cdots(\delta_{\nu_{r-1}}X)^{\alpha_{r-1}p^{e(\nu_{r-1})}} \\ &+[\cdots] \\ &= \sum_{i=1}^{r}(\partial M/\partial(\delta_{\nu_i}X)^{p^{e(\nu_i)}})\cdot\left\{\binom{\mu_i+\nu_i}{\mu_i}\delta_{\mu_i+\nu_i}X\right\}^{p^{e(\nu_i)}}+[\cdots],\end{aligned}$$

where the $[\cdots]$ contains no derivative of X of order $\geqslant \omega = \max(\mu_1+\nu_1, \cdots, \mu_r+\nu_r)$. Hence,

$$\delta_\lambda A = \sum_{i=1}^{r}(\partial A/\partial(\delta_{\nu_i}X)^{p^{e(\nu_i)}})\cdot\left\{\binom{\mu_i+\nu_i}{\mu_i}\delta_{\mu_i+\nu_i}X\right\}^{p^{e(\nu_i)}}+[\cdots], \tag{3.2}$$

where the $[\cdots]$ is as above and $\partial A/\partial(\delta_{\nu_i}X)^{p^{e(\nu_i)}} \neq 0$ $(1 \leqslant i \leqslant r)$. Suppose that only one of $\mu_1+\nu_1, \cdots, \mu_r+\nu_r$ is equal to ω, then obviously $\delta_\lambda A \neq 0$. On the contrary, suppose that more than one of $\mu_1+\nu_1, \cdots, \mu_r+\nu_r$ are equal to ω; if we had $\delta_\lambda A=0$, we should have $e(\nu_i)=e(\nu_j)$ for at least two distinct values of i, j in order that $\delta_\omega X$ should vanish in $\delta_\lambda A$; this would imply $\mu_i=\mu_j$, contradicting with the inequality $\nu_i \neq \nu_j$.

COROLLARY *If $(\boldsymbol{F}, \delta_1, \cdots, \delta_m)$ is a differential field and X_j $(j \in J)$ a set of differentially independent elements over $\boldsymbol{F}$, then every constant of $\boldsymbol{G}=F\langle X_j\,;\ j \in J\rangle$ is contained in $\boldsymbol{F}$.*

Proof. In order to prove this, it is enough to consider the special case where $(\boldsymbol{F}, \delta)$ is an ordinary differential field and the set X_j consists only of a single element X. Let A/B be an element of $\boldsymbol{G}=\boldsymbol{F}\langle x\rangle$ with $A/B \notin \boldsymbol{F}$, where A, B are elements of $\boldsymbol{F}\{X\}$ and relatively prime as polynomials of derivatives of X over $\boldsymbol{F}$. Assume that A/B is a constant. Then, we get

$$\delta_\mu A\cdot B-A\cdot\delta_\mu B=0 \tag{3.3}$$

for every positive integer μ.

Case I: there exist some derivatives of X which are contained in A or in B with exponents not divisible by p.

Among such derivatives of X, let $\delta_\nu X$ be the one of the highest order and write each of A, B in the form $A=\sum_{i=0}^{\alpha}A_i(\delta_\nu X)^i$, $B=\sum_{j=0}^{\beta}B_j(\delta_\nu X)^j$, where A_i and B_j are polynomials of $(\delta_\rho X)^p$ $(\rho\geqslant\nu)$ and $\delta_\sigma X\,(\sigma<\nu)$ over $\boldsymbol{F}$, at least one of α, β is positive, $A_\alpha\neq 0$ and and $B_\beta\neq 0$, furthermore, $\alpha\leqslant p-1$ and $\beta\leqslant p-1$ provided $p\neq 0$. By (3.1), we get

$$\begin{aligned}&\delta_\mu A\cdot B-A\cdot\delta_\mu B\\&\qquad=\{(\partial A/\partial(\delta_\nu X))B-A(\partial B/\partial(\delta_\nu X))\}\cdot\binom{\mu+\nu}{\mu}\cdot\delta_{\mu+\nu}X+[\cdots]\end{aligned}$$

(the $[\cdots]$ being as in (3.1)).

Since $(\partial A/\partial(\delta_\nu X))B-A(\partial B/\partial(\delta_\nu X))\neq 0$, this contradicts with (3.3) if we take a positive integer μ such that $\binom{\mu+\nu}{\mu}$ is not divisible by p.

Case II: every derivative of X is contained in A and B exclusively with exponents divisible by p. Concerning A and B, determine $\delta_{\nu_1}X$, $\cdots$, $\delta_{\nu_r}X$, $e(\nu_1)$, $\cdots$, $e(\nu_r)$, μ, λ, μ_1, $\cdots$, μ_r as in the proof (Case II) of Prop. 3.1. We get by (3.2)

$$\begin{aligned}&\delta_\lambda A\cdot B-A\cdot\delta_\lambda B\\&=\sum_{i=1}^{r}\{(\partial A/\partial(\delta_{\nu_i}X)^{p^{e(\nu_i)}})B-A(\partial B/\partial(\delta_{\nu_i}X)^{p^{e(\nu_i)}})\}\cdot\binom{\mu_i+\nu_i}{\mu_i}\cdot(\delta_{\mu_i+\nu_i}X)^{p^{e(\nu_i)}}\\&\qquad+[\cdots]\end{aligned}$$

(the $[\cdots]$ being as in (3.2)).

Similarly as in the proof (Case II) of Prop. 3.1, we see that this contradicts with (3.3).

Now, let $(\boldsymbol{F}, \delta_1, \cdots, \delta_m)$ be a differential field, $X_1, \cdots, X_n$ differentially independent over $\boldsymbol{F}$ and $\boldsymbol{R}=\boldsymbol{F}\{X_1, \cdots, X_n\}$ the differential ring of differential polynomials of $X_1, \cdots, X_n$ over $\boldsymbol{F}$.

If we denote by $P(X_1, \cdots, X_n)$, or simply by $P(X)$, an element of $\boldsymbol{R}$, and if $(x_1, \cdots, x_n)$, which may be denoted simply by (x), is a set of n elements of a differential extension field of $\boldsymbol{F}$, then $P(x_1, \cdots, x_n)$, or simply $P(x)$, means the element which is obtained from $P(X_1, \cdots, X_n)$ by the substitution $\delta_{i\nu}X_j \rightarrow \delta_{i\nu}x_j$ $(1 \leqslant i \leqslant m,\ \nu \geqslant 0,\ 1 \leqslant j \leqslant n)$. If $P(x)=0$, (x) is called a *zero* of $P(X)$ or a *solution* of the *differential equation* $P(X)=0$. If $\boldsymbol{m}=\{P_\lambda(X)\,;\ \lambda \in \Lambda\}$ is a subset of $\boldsymbol{R}$ and (x) is a common zero of all $P_\lambda(X)$ $(\lambda \in \Lambda)$, then (x) is called a *zero* of $\boldsymbol{m}$ or a *solution* of the *system* $\{P_\lambda(X)=0\,;\ \lambda \in \Lambda\}$ *of differential equations.* Let $\mathfrak{m}$ be the radical ideal of $((\boldsymbol{m}))$ in $\boldsymbol{R}$, then $\mathfrak{m}$ is a differential semiprime ideal of $\boldsymbol{R}$ (Prop. 2. 1), and the set of zeros of $\boldsymbol{m}$ is identical with that of $\mathfrak{m}$.

Let $\mathfrak{p}$ be a differential pirme ideal of $\boldsymbol{R}$ (not containing 1), and φ the differential homomorphism of $\boldsymbol{R}$ onto the differential quotient ring $\boldsymbol{R}/\mathfrak{p}$. Since we can identify every $a \in \boldsymbol{F}$ with its image $\varphi(a)$, we identify $\boldsymbol{F}$ with a subfield of $\boldsymbol{R}/\mathfrak{p}$. Since $\boldsymbol{R}/\mathfrak{p}$ is a differential integral domain, its field of quotients $\boldsymbol{G}$ is a differential extension field of $\boldsymbol{F}$. If we put $\varphi(X_j)=x_j$ $(1 \leqslant j \leqslant n)$, we get $\boldsymbol{R}/\mathfrak{p}=\boldsymbol{F}\{x_1, \cdots, x_n\}$ and $\boldsymbol{G}=\boldsymbol{F}\langle x_1, \cdots, x_n\rangle$. We see at once that (x) is a zero of $\mathfrak{p}$, and that an element $P(X)$ of $\boldsymbol{R}$ is contained in $\mathfrak{p}$ if $P(x)=0$. A zero (y) of $\mathfrak{p}$ is called a *generic zero* of $\mathfrak{p}$ if every $P(X) \in \boldsymbol{R}$ with $P(y)=0$ is contained in $\mathfrak{p}$; the above-mentioned (x) is a generic zero of $\mathfrak{p}$.

Let $(z_1, \cdots, z_n)$ be a set of n elements of a differential extension field of $\boldsymbol{F}$. If we denote by $\mathfrak{p}_{(z)/F}$ the set of all $P(X) \in \boldsymbol{R}$ with $P(z)=0$, then $\mathfrak{p}_{(z)/F}$ is a differential prime ideal of $\boldsymbol{R}$ not containing 1 and (z) is a generic zero of $\mathfrak{p}_{(z)/F}$; the above-mentioned $\mathfrak{p}$ and (x) are such that $\mathfrak{p}=\mathfrak{p}_{(x)/F}$.

4. Condition (S) and condition (S_0)

Let $(\boldsymbol{F}, \delta_1, \cdots, \delta_m)$ be a differential field and $\boldsymbol{H}$ its differential extension field. If we say that φ is a differential isomorphism *over* $\boldsymbol{F}$ of $\boldsymbol{H}$ into a differential extension field of $\boldsymbol{F}$, we mean that the differential isomorphism φ leaves every element of $\boldsymbol{F}$ invariant.

We say that $\boldsymbol{H}$ *satisfies the condition* (S) *over* $\boldsymbol{F}$, if

$$\text{(S)}\quad \begin{cases} \text{there exists, for every } z \in \boldsymbol{H}-\boldsymbol{F}, \text{ a differential isomorphism } \sigma' \text{ over } \boldsymbol{F} \text{ of } \boldsymbol{H} \\ \text{into a differential extension field of } \boldsymbol{H} \text{ such that } \sigma' z \neq z. \end{cases}$$

In particular, we say that $\boldsymbol{H}$ *satisfies the condition* (S_0) *over* $\boldsymbol{F}$, if

$$(\mathrm{S}_0)\quad \begin{cases} \text{there exists, for ever } z \in \boldsymbol{H}-\boldsymbol{F}, \text{ a differential automorphism} \\ \sigma \text{ over } \boldsymbol{F} \text{ of } \boldsymbol{H} \text{ such that } \sigma z \neq z. \end{cases}$$

Let us consider some results about these conditions, which will be used afterwards.

PROPOSITION 4.1. *Let* $(\boldsymbol{F}, \delta_1, \cdots, \delta_m)$ *be a differential field,* $\boldsymbol{H}$ *its differential extension field which satisfies the condition* (S_0) *over* $\boldsymbol{F}$ *and* $z_1, \cdots, z_r$ *a finite number of elements of* $\boldsymbol{H}$ *which are linearly independent over* $\boldsymbol{F}$. *Then, there exist* r *differential automorphisms* $\sigma_1, \cdots, \sigma_r$ *of* $\boldsymbol{H}$ *over* $\boldsymbol{F}$ *such that* $\det(\sigma_i z_j)_{1\leqslant i\leqslant r,\, 1\leqslant j\leqslant r} \neq 0$.

Proof. We shall prove this by the induction on r. Since the statement is trivial for $r=1$, let r be >1. By the induction assumption, there exist $r-1$ differential automorphisms $\sigma_1, \cdots, \sigma_{r-1}$ of $\boldsymbol{H}$ over $\boldsymbol{F}$ such that $\det(\sigma_i z_j)_{1\leqslant i\leqslant r-1,\, 1\leqslant j\leqslant r-1} \neq 0$. Now, suppose that we have

$$\begin{vmatrix} \sigma_1 z_1 & \cdots & \sigma_1 z_{r-1} & \sigma_1 z_r \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_{r-1} z_1 & \cdots & \sigma_{r-1} z_{r-1} & \sigma_{r-1} z_r \\ \sigma z_1 & \cdots & \sigma z_{r-1} & \sigma z_r \end{vmatrix} = 0$$

for every differential automorphism σ of $\boldsymbol{H}$ over $\boldsymbol{F}$. Choose $r-1$ elements $a_1, \cdots, a_{r-1}$ of $\boldsymbol{H}$ such that $\sum_{j=1}^{r-1} \sigma_i z_j \cdot a_j = \sigma_i z_r$ $(1 \leqslant i \leqslant r-1)$, then we have

$$\sum_{j=1}^{r-1} \sigma z_j \cdot a_j = \sigma z_r \tag{4.1}$$

for every differential automorphism σ of $\boldsymbol{H}$ over $\boldsymbol{F}$, and consequently $\sum_{j=1}^{r-1} \tau\sigma z_j \cdot \tau a_j = \tau\sigma z_r = \sum_{j=1}^{r-1} \tau\sigma z_j \cdot a_j$ i.e. $\sum_{j=1}^{r-1} \tau\sigma z_j \cdot (\tau a_j - a_j) = 0$ for every pair of differential automorphisms σ, τ of $\boldsymbol{H}$ over $\boldsymbol{F}$. Since, for each pair of τ and $i\,(1\leqslant i\leqslant r-1)$, we can take σ so that $\tau\sigma=\sigma_i$, we get $\sum_{j=1}^{r-1}\sigma_i z_j(\tau a_j-a_j)=0$. Hence, $\tau a_j=a_j\,(1\leqslant j\leqslant r-1)$ for every τ, and $a_j\in\boldsymbol{F}\,(1\leqslant j\leqslant r-1)$ dy the condition (S_0). Thus, we get from (4.1) the equality $\sum_{j=1}^{r-1}z_j a_j=z_r$ (a contradiction).

PROPOSITION 4.2. *Let* $(\boldsymbol{F}, \delta_1, \cdots, \delta_m)$ *be a differential field,* $\boldsymbol{H}$ *its differential extension field which satisfies the condition* (S_0) *over* $\boldsymbol{F}$ *and* $x_1, \cdots, x_n$ *a finite number of elements of* $\boldsymbol{H}$ *such that the ring* $\boldsymbol{F}[\theta x_j;\ \theta\in\Theta,\ 1\leqslant j\leqslant n]$ *is of finite type over* $\boldsymbol{F}$. *Let* $X_1, \cdots, X_n$ *be differentially independent over* $\boldsymbol{H}$, *and put* $\boldsymbol{R}=\boldsymbol{F}\{X_1, \cdots, X_n\}$, $\mathfrak{p}=\mathfrak{p}_{(x)/F}$ *and* $\boldsymbol{S}=\boldsymbol{G}\{X_1, \cdots, X_n\}$ *where* $\boldsymbol{G}$ *is an intermediate differential field between* $\boldsymbol{F}$ *and* $\boldsymbol{H}$. *Then,* $\boldsymbol{G}\mathfrak{p}$ *can be represented as an intersection of a finite number of differential prime ideals of* $\boldsymbol{S}$. *If*

$$\boldsymbol{G}\mathfrak{p} = \mathfrak{P}_1\cap\cdots\cap\mathfrak{P}_r \tag{4.2}$$

($\mathfrak{P}_k$ *being differential prime ideals of* $\boldsymbol{S}$)

is such an irredundant representation, we have

$$\mathfrak{P}_k\cap\boldsymbol{R} = \mathfrak{p}, \quad \dim\mathfrak{P}_k = \dim\mathfrak{p} \quad (1\leqslant k\leqslant r)\,, \tag{4.3}$$

where $\dim\mathfrak{p}$ *and* $\dim\mathfrak{P}_k$ *are the transcendence degrees of* $\boldsymbol{R}/\mathfrak{p}$ *over* $\boldsymbol{F}$ *and of* $\boldsymbol{S}/\mathfrak{P}_k$ *over* $\boldsymbol{G}$ *respectively.*

Proof. Since $\boldsymbol{F}[\theta x_j;\ \theta\in\Theta,\ 1\leqslant j\leqslant n]$ is of finite type over $\boldsymbol{F}$, we can choose among $\theta x_j(\theta\in\Theta,\ 1\leqslant j\leqslant n)$ a finite subset $y_1, \cdots, y_l$ such that $\boldsymbol{F}[\theta x_j;\ \theta\in\Theta, 1\leqslant j\leqslant n]=\boldsymbol{F}[y_1, \cdots, y_l]$. Denote by $z_\lambda(\lambda\in\Lambda)$ all of $\theta x_j(\theta\in\Theta, 1\leqslant j\leqslant n)$ other than $y_1, \cdots, y_l$. Furthermore, denote $\theta X_j\,(\theta\in\Theta,\ 1\leqslant j\leqslant n)$ by $Y_1, \cdots, Y_l$, $Z_\lambda(\lambda\in\Lambda)$ correspondingly as we denote $\theta x_j(\theta\in\Theta, 1\leqslant j\leqslant n)$ by $y_1, \cdots, y_l$, $z_\lambda(\lambda\in\Lambda)$, and put $\boldsymbol{R}'=\boldsymbol{F}[Y_1, \cdots, Y_l]$, $\boldsymbol{S}'=\boldsymbol{G}[Y_1, \cdots, Y_l]$ and $\mathfrak{p}'=\mathfrak{p}\cap\boldsymbol{R}'$. If we put $\mathfrak{P}'_\sigma=\mathfrak{p}_{(\sigma y)}/\boldsymbol{G}$ for each differential automorphism σ of $\boldsymbol{H}$ over $\boldsymbol{F}$, we can see by Prop. 4.1 that $\boldsymbol{G}\mathfrak{p}'=\bigcap_\sigma\mathfrak{P}'_\sigma$ so that $\boldsymbol{G}\mathfrak{p}'$ is a semi-prime ideal of $\boldsymbol{S}'$. Therefore, we get an irredundant representation

$$\boldsymbol{G}\mathfrak{p}' = \mathfrak{P}'_1\cap\cdots\cap\mathfrak{P}'_r$$

and can prove without serious difficulties the equalities

$$\mathfrak{P}'_k \cap \boldsymbol{R}' = \mathfrak{p}', \quad \dim \mathfrak{P}'_k = \dim \mathfrak{p}' \qquad (1 \leqslant k \leqslant r).$$

Let $A_\lambda(Y)$ be elements of $\boldsymbol{R}'$ such that $z_\lambda = A_\lambda(y)$ $(\lambda \in \Lambda)$. Then, we see easily that $\mathfrak{p} = (\mathfrak{p}', Z_\lambda - A_\lambda(Y)\,;\ \lambda \in \Lambda)$ in $\boldsymbol{R}$, and that the ideals $\mathfrak{P}_k = (\mathfrak{P}'_k, Z_\lambda - A_\lambda(Y)\,;\ \lambda \in \Lambda)$ are prime ideals of $\boldsymbol{S}$, and that

$$\boldsymbol{G}\mathfrak{p} = \mathfrak{P}_1 \cap \cdots \cap \mathfrak{P}_r \quad \text{(an irredundant representation)},$$
$$\mathfrak{P}_k \cap \boldsymbol{R} = \mathfrak{p}, \quad \dim \mathfrak{P}_k = \dim \mathfrak{p} \qquad (1 \leqslant k \leqslant r).$$

At last, we see by Prop. 2.2 that $\mathfrak{P}_k$ are differential ideals of $\boldsymbol{S}$.

PROPOSITION 4.3. *Let* $(\boldsymbol{F}, \delta_1, \cdots, \delta_m)$ *be a differential field,* $\boldsymbol{H}$ *its differential extension field and* $\boldsymbol{G}$ *an intermediate differential field between* $\boldsymbol{F}$ *and* $\boldsymbol{H}$ *such that* $\boldsymbol{H}$ *satisfies the condition* (S_0) *over* $\boldsymbol{G}$. *If there exist a finite number of elements* $x_1, \cdots, x_n$ *of* $\boldsymbol{H}$ *such that* $\boldsymbol{H} = \boldsymbol{F}\langle x_1, \cdots, x_n\rangle$ *and* $\boldsymbol{F}[\theta x_j\,;\ \theta \in \Theta,\ 1 \leqslant j \leqslant n]$ *is of finite type over* $\boldsymbol{F}$, *then each differential automorphism* σ *of* $\boldsymbol{G}$ *over* $\boldsymbol{F}$ *can be prolonged to a differential isomorphism of* $\boldsymbol{H}$ *into a differential extension field of* $\boldsymbol{H}$.

Proof. Let $X_1, \cdots, X_n$ be differentially independent over $\boldsymbol{H}$, and put $\boldsymbol{S} = \boldsymbol{G}\{X_1, \cdots, X_n\}$, $\boldsymbol{T} = \boldsymbol{H}\{X_1, \cdots, X_n\}$, $\mathfrak{P} = \mathfrak{p}_{(x)/G}$ in $\boldsymbol{S}$ and $\mathfrak{P}^\sigma$ the set of all differential polynomials of $\boldsymbol{S}$ which are obtained from elements of $\mathfrak{P}$ by operating σ on their coefficients. Then, $\mathfrak{P}^\sigma$ is a differential prime ideal $(\not\ni 1)$ of $\boldsymbol{S}$, and, similarly as Prop. 4.2, there exists a differential prime ideal $\mathfrak{P}'(\not\ni 1)$ of $\boldsymbol{T}$ with $\mathfrak{P}' \cap \boldsymbol{S} = \mathfrak{P}^\sigma$. Denote by $(y_1, \cdots, y_n)$ a generic zero of $\mathfrak{P}'$, then (y) is a generic zero of $\mathfrak{P}^\sigma$, and we see that a differential isomorphism of $\boldsymbol{H} = \boldsymbol{G}\langle x_1, \cdots, x_n\rangle$ into $\boldsymbol{H}\langle y_1, \cdots, y_n\rangle$ is determined by $x_i \to y_i$ $(1 \leqslant i \leqslant n)$ such that it prolongs σ.

PROPOSITION 4.4. *Let* $\boldsymbol{F}$ *be a differential field and* $\boldsymbol{G}$ *a separably (and normally) algebraic extension field of* $\boldsymbol{F}$. *Then,* $\boldsymbol{G}$ *can be regarded as a differential extension field of* $\boldsymbol{F}$ *which satisfies the condition* (S) (*the condition* (S_0) *respectively*) *over* $\boldsymbol{F}$.

Proof. For each $z \in \boldsymbol{G} - \boldsymbol{F}$, there exists obviously an isomorphism σ' over $\boldsymbol{F}$ of $\boldsymbol{G}$ onto a separably algebraic extension field $\boldsymbol{G}'$ of $\boldsymbol{G}$ with $\sigma' z \neq z$ (an automorphism σ over $\boldsymbol{F}$ of $\boldsymbol{G}$ with $\sigma z \neq z$).

By Prop. 2.6, σ' is a differential isomorphism over $\boldsymbol{F}$ of the differential structure of $\boldsymbol{G}$ onto that of $\boldsymbol{G}'$ (σ is a differential automorphism over $\boldsymbol{F}$ of the differential structure of $\boldsymbol{G}$).

REMARK. The converse of Prop. 4.4 is partially true. Namely, if $\boldsymbol{G}$ is a differential extension field of $\boldsymbol{F}$ which is algebraic over $\boldsymbol{F}$ and satisfies the condition (S_0) over $\boldsymbol{F}$, then $\boldsymbol{G}$ is separably and normally algebraic over $\boldsymbol{F}$.

5. Linear dependence over constants and linear homogeneous differential equations

If $x_1, \cdots, x_n$ are finite number n of elements of a differential field, and $\theta_1, \cdots, \theta_n$ n differential operators, we denote $\det(\theta_i x_j)_{1\leqq i\leqq n,\, 1\leqq j\leqq n}$ by $W_{\theta_1\cdots\theta_n}(x_1, \cdots, x_n)$.

PROPOSITION 5.1. *Let $x_1, \cdots, x_n$ be n elements of a differential field $\boldsymbol{F}$. Then, $x_1, \cdots, x_n$ are linearly dependent over the field $\boldsymbol{C}$ of constants of $\boldsymbol{F}$, if and only if $W_{\theta_1\cdots\theta_n}(x_1, \cdots, x_n)=0$ for every choice of n differential operators $\theta_1, \cdots, \theta_n$.*

The proof of Prop. 5.1 and the following Cor. are straightfoward.

COROLLARY *Let $x_1, \cdots, x_n$ be elements of a differential field $\boldsymbol{F}$. If there exist $n-1$ differential operators $\theta_1, \cdots, \theta_{n-1}$ such that $W_{\theta_1\cdots\theta_{n-1}}(x_1, \cdots, x_{n-1})\neq 0$ and $W_{\theta_1\cdots\theta_{n-1}\theta}(x_1, \cdots, x_n)=0$ for every differential operator θ, then $x_1, \cdots, x_{n-1}$ are linearly independent over the field $\boldsymbol{C}$ of constants of $\boldsymbol{F}$ and x_n is a linear combination of $x_1, \cdots, x_{n-1}$ over $\boldsymbol{C}$.*

Since $W_{\theta_1\cdots\theta_n}(x_1, \cdots, x_n)$ are polynomials of derivatives of $x_1, \cdots, x_n$ with rational integral coefficients, we can speak without ambiguity of *linear dependence* or *linear independence over constants* as one does in [4].

Let $(\boldsymbol{F}, \delta_1, \cdots, \delta_n)$ be a differential field, X a single differentially independent element over $\boldsymbol{F}$. Linear combinations over $\boldsymbol{F}$ of derivatives of X are called *linear differential forms* of X over $\boldsymbol{F}$. If L is a linear differential form, the equation $L=0$ is called a *linear homogeneous differential equation* of X over $\boldsymbol{F}$.

Herein, we shall consider $\boldsymbol{F}$-modules of linear differential forms of X over $\boldsymbol{F}$. If such a module $\mathfrak{M}$ satisfies the condition $\delta_{i\nu}\mathfrak{M}\subset\mathfrak{M}$ $(1\leqq i\leqq m,\ \nu\geqq 0)$, we shall call $\mathfrak{M}$ a *differential module* of linear differential forms of X over $\boldsymbol{F}$. If $L_\lambda(\lambda\in\Lambda)$ is a set of linear differential forms of X over $\boldsymbol{F}$, the set $\mathfrak{L}$ of all linear combinations over $\boldsymbol{F}$ of all derivatives of $L_\lambda(\lambda\in\Lambda)$ makes the smallest differential module of linear differential forms of X over $\boldsymbol{F}$ which contains $L_\lambda(\lambda\in\Lambda)$. $\mathfrak{L}$ is called the differential module of linear differential forms of X over $\boldsymbol{F}$ which is *generated* by $L_\lambda(\lambda\in\Lambda)$. A solution of the set of linear homogeneous differential equations $L_\lambda=0\,(\lambda\in\Lambda)$ is a zero of $\mathfrak{L}$, and vice versa. Thus, the consideration of a set of linear homogeneous differential equations of X over $\boldsymbol{F}$ can be transfered to that of a differential module of linear differential forms of X over $\boldsymbol{F}$.

Now, arrange all differential operators into a sequence $\{\theta_1,\theta_2,\cdots\}$ and use the notation $\theta_h<\theta_k$ (or $\theta_k>\theta_h$) to mean that θ_h precedes to θ_k in that sequence. If a differential module $\mathfrak{L}$ of linear differential forms of X over $\boldsymbol{F}$ is given, we can divide up the sequence $\{\theta_1,\theta_2,\cdots\}$ into two subsequences $\{\theta'_1,\theta'_2,\cdots\}$, $\{\theta''_1,\theta''_2,\cdots\}$, the latter of which may be finite, in such a manner that $\mathfrak{L}$ has a base $L_{\theta'_i}\,(i\geqq 1)$ of the form

$$L_{\theta'_i}=\theta'_iX-\sum_{j\geqq 1}a_{ij}\cdot\theta''_jX \qquad (i\geqq 1,\ a_{ij}\in\boldsymbol{F};\ a_{ij}=0\ \text{ if }\ \theta''_j>\theta'_i).$$

This base of $\mathfrak{L}$ does depend on the arrangement $\{\theta_1,\theta_2,\cdots\}$, but we see that the number of $\theta''_1,\theta''_2,\cdots$ does not depemd on it. If r is a non-negative integer not larger than that number, it is easy to show that there exist r zeros of $\mathfrak{L}$ which are linearly independent over constants.

Let $\mathfrak{l}=\{L_\lambda=0;\ \lambda\in\Lambda\}$ be a set of linear homogeneous differential equations of X over $\boldsymbol{F}$, and $\mathfrak{L}$ the differential module of linear homogeneous differential forms of X over $\boldsymbol{F}$ which is generated by $\mathfrak{l}$. If the number of $\theta''_1,\theta''_2,\cdots$, which are obtained for $\mathfrak{L}$ in the above-described manner, is finite (say n) then $\mathfrak{l}$ is said to be *of finite type* (or *of type* n).

PROPOSITION 5.2. *Let* $\mathfrak{l}$ *be a set of linear homogeneous differen-*

tial equations of X over $\boldsymbol{F}$. If $\mathfrak{l}$ is of type n, there exist n solutions of $\mathfrak{l}$ which are contained in a differential extension field of $\boldsymbol{F}$ and linearly independent over constants. If $x_1, \cdots, x_n$ are such solutions, every solution of $\mathfrak{l}$, which is contained in a differential extension field of $\boldsymbol{F}\langle x_1, \cdots, x_n\rangle$, is a linear combination of $x_1, \cdots, x_n$ over constants.

Such a set of solutions $x_1, \cdots, x_n$ of $\mathfrak{l}$ will be called a *fundamental system of solutions* of $\mathfrak{l}$.

Chapter II. Picard-Vessiot theory

In this chapter, let $(\boldsymbol{F}, \delta_1, \cdots, \delta_m)$ be a fixed differential field of an arbitrary characteristic p (zero or non-zero) such that the field $\boldsymbol{C}$ of constants of $\boldsymbol{F}$ is algebraically closed. The following discussions are done, in general speaking, in a similar manner as those of [4], so that the proofs of many of the propositions are omitted or outlined.

6. Picard-Vessiot extensions

Let $\boldsymbol{G}$ be a differential extension field of $\boldsymbol{F}$ which satisfies the conditions:

(P1) there exists a set $\mathfrak{l}$ of linear homogeneous differential equations of a differentially independent element X over $\boldsymbol{F}$ which is of type n and has a fundamental system $x_1, \cdots, x_n$ of solutions such that $\boldsymbol{G}=\boldsymbol{F}\langle x_1, \cdots, x_n\rangle$;

(P2) every constant of $\boldsymbol{G}$ is contained in $\boldsymbol{F}$;

(P3) $\boldsymbol{G}$ satisfies the condition (S) over $\boldsymbol{F}$.

Then, $\boldsymbol{G}$ is called a *Picard-Vessiot extension* of $\boldsymbol{F}$. The set $\mathfrak{l}$ in (P1) is called a *defining set of linear homogeneous differential equations* for the Picard-Vessiot extension $\boldsymbol{G}$ of $\boldsymbol{F}$. In case $p=0$, this definition coincides with that in [4].

If σ' is a differential isomorphism over $\boldsymbol{F}$ of $\boldsymbol{G}$ into a differential extension field of $\boldsymbol{G}$, then $\sigma' x_1, \cdots, \sigma' x_n$ is a fundamental system of solutions of $\mathfrak{l}$. Hence, we get by Prop. 5.2

$$\sigma' x_j = \sum_{i=1}^{n} x_i c'_{ij}(\sigma') \qquad (1 \leqslant j \leqslant n),$$

where $c'_{ij}(\sigma')$ are constnts of $\boldsymbol{G}\langle\sigma'\boldsymbol{G}\rangle$ and the matrix $(c'_{ij}(\sigma'))$ is regular.

The following Kolchin's lemma and its corollary hold also true under our definition of differential fields:

LEMMA 6.1. *Let* $\boldsymbol{H}$ *be a differential field,* $\boldsymbol{K}$ *its field of constants, and* $C_1, \cdots, C_n$ *independent indeterminates over* $\boldsymbol{H}$. *If a subset* $\boldsymbol{m}$ *of* $\boldsymbol{H}[C_1, \cdots, C_n]$ *is given, there exists a subset* $\boldsymbol{m}'$ *of* $\boldsymbol{K}[C_1, \cdots, C_n]$ *such that a set* $(c_1, \cdots, c_n)$ *of* n *constants of a differential extension field of* $\boldsymbol{H}$ *is a zero of* $\boldsymbol{m}$ *if and only if it is a zero of* $\boldsymbol{m}'$.

COROLLARY *If* $\boldsymbol{H}, \boldsymbol{K}$ *are as above, and* $c_1, \cdots. c_n$ *any number of constants of a differential extension field of* $\boldsymbol{H}$, *we have*

$$\text{tr. deg.}_{\boldsymbol{H}}(c_1, \cdots, c_n) = \text{tr. deg.}_{\boldsymbol{K}}(c_1, \cdots, c_n).$$

Let $C_{ij}\,(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ be n^2 indeterminates over $\boldsymbol{G}$ and (c'_{ij}) a regular $n \times n$-matrix of constants of a differential extension field of $\boldsymbol{G}$. Then, using Lem. 6.1 and its Cor., we see similarly as in [4] that there exists a semiprime ideal $\mathfrak{g}$ of $\boldsymbol{C}[C_{ij};\ 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n]$ such that a differential isomorphism over $\boldsymbol{F}$ of $\boldsymbol{G}$ into an differential extension field of $\boldsymbol{G}$ can be determined by

$$x_j \to \sum_{i=1}^{n} x_i c'_{ij} \qquad (1 \leqslant j \leqslant n)$$

if and only if (c'_{ij}) is a zero of $\mathfrak{g}$.

If σ is a differential automorphism of $\boldsymbol{G}$ over $\boldsymbol{F}$, we get

$$\sigma x_j = \sum_{i=1}^{n} x_i c_{ij}(\sigma) \qquad (1 \leqslant j \leqslant n),$$

where $(c_{ij}(\sigma))$ is a regular matrix of elements of $\boldsymbol{C}$ and a zero of $\mathfrak{g}$. Conversely, if a regular $n \times n$-matrix (c_{ij}) of elements of $\boldsymbol{C}$ is a zero of $\mathfrak{g}$, a differential automorphism of $\boldsymbol{G}$ over $\boldsymbol{F}$ can be determined by

$$x_j \to \sum_{i=1}^{n} x_i c_{ij} \qquad (1 \leqslant j \leqslant n).$$

The group of all differential automorphisms of $\boldsymbol{G}$ over $\boldsymbol{F}$ is denoted by $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$ and called the *Galois group* of $\boldsymbol{G}$ over $\boldsymbol{F}$. If

$x_1, \cdots, x_n$ of (P1) are fixed, the map $\sigma \to (c_{ij}(\sigma))$ is an isomorphism of $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$ into $GL(n, \boldsymbol{C})$; the image of $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$ is an algebraic matric group and can be identified with $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$.

PROPOSITION 6.1. *If $\boldsymbol{G}$ is a Picard-Vessiot extension of $\boldsymbol{F}$, then $\boldsymbol{G}$ satisfies the condition* (S_0) *over $\boldsymbol{F}$.*

This is clear, following [4], on account of (P3).

PROPOSITION 6.2. *If $\boldsymbol{G}$ is as above, we have*

$$\dim \mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}) = \mathrm{tr.\,deg.}_{\boldsymbol{F}} \boldsymbol{G}\,.$$

The proof is similar to that in [4], by virtue of Prop. 6.1 and Prop. 4.2.

EXAMPLE 6.1. Let $x_1, \cdots, x_n$ be differentially independent over $\boldsymbol{F}$, and $\theta_1, \cdots, \theta_n$ distinct differential operators which are fixed arbitrarily, and put

$$\begin{aligned} u_{\theta i} &= W_{\theta\theta_1\cdots\hat{\theta}_i\cdots\theta_n}(x_1, \cdots, x_n)/W_{\theta_1\cdots\theta_n}(x_1, \cdots, x_n) \quad (\theta \in \Theta,\ 1 \leqslant i \leqslant n)\,, \\ \boldsymbol{F}_u &= \boldsymbol{F}\langle u_{\theta i}\,;\ \theta \in \Theta,\ 1 \leqslant i \leqslant n \rangle\,, \\ \boldsymbol{G} &= \boldsymbol{F}_u\langle x_1, \cdots, x_n \rangle = \boldsymbol{F}\langle x_1, \cdots, x_n \rangle\,. \end{aligned}$$

We shall show that $\boldsymbol{G}$ is a Picard-Vessiot extension of $\boldsymbol{F}_u$ and $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}_u) = GL(n, \boldsymbol{C})$.

By Cor. of Prop. 3.1, every constant of $\boldsymbol{G}$ is contained in $\boldsymbol{F}$, consequently in $\boldsymbol{F}_u$. Let X be a differentially independent element over $\boldsymbol{G}$, and consider linear homogeneous differential equations

$$\begin{aligned} &W_{\theta\theta_1\cdots\theta_n}(X, x_1, \cdots, x_n)/W_{\theta_1\cdots\theta_n}(x_1, \cdots, x_n) = 0 \\ &\text{i.e.}\quad \theta X - \sum_{i=1}^{n}(-1)^{i-1}u_{\theta i}\cdot\theta_i X = 0 \qquad (\theta \in \Theta) \end{aligned}$$

of X over $\boldsymbol{F}_u$. This set of linear homogeneous differential equations is of type n, and $x_1, \cdots, x_n$ is a fundamental system of solutions (Prop. 5.1 and its Cor.). For any regular $n \times n$-matrix (c_{ij}) of elements of $\boldsymbol{C}$, we see at once that $x'_j = \sum_{i=1}^{n} x_i c_{ij}$ $(1 \leqslant j \leqslant n)$ are differentially independent over $\boldsymbol{F}$. Consequently, a differential automorphism of $\boldsymbol{G}$ over $\boldsymbol{F}$ can be determined by $x_j \to x'_j$ $(1 \leqslant j \leqslant n)$; since every $u_{\theta i}$ $(\theta \in \Theta,\ 1 \leqslant i \leqslant n)$ is invariant under this automorphism, so is every element of $\boldsymbol{F}_u$. Thus, $GL(n, \boldsymbol{C})$ is the group of all differential automorphisms of $\boldsymbol{G}$ over $\boldsymbol{F}_u$. Therefore, the above-mentioned semiprime ideal $\mathfrak{g}$ in this case is the zero ideal. Now, it can be easily proved that $\theta_i x_j$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ are algebraically independent over $\boldsymbol{F}_u$. From this and the fact $\mathfrak{g}=(0)$, we can deduce without difficulties that $\boldsymbol{G}$ satisfies the condition (S) over $\boldsymbol{F}_u$.

7. Intermediate differential fields

Let $\boldsymbol{G}$ and $x_1, \cdots, x_n$ be as those at the beginning of the preceding section.

We shall denote by $\mathcal{F}$ the set of all intermediate differential fields over which $\boldsymbol{G}$ satisfies the condition (S), and by $\mathcal{G}$ the set of all algebraic subgroups of $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$.

PROPOSITION 7.1. *If $\boldsymbol{F}_1$ is an element of $\mathcal{F}$, then $\boldsymbol{G}$ is a Picard-Vessiot extension of $\boldsymbol{F}_1$ and $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}_1)$ belongs to $\mathcal{G}$. The map $\boldsymbol{F}_1 \to \mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}_1)$ of $\mathcal{F}$ into $\mathcal{G}$ is bijective.*

Proof. The first half of this is obviously true. Since the set of all elements which are invariant under all elements of $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}_1)$ is $\boldsymbol{F}_1$ (Prop. 6.1), the map $\boldsymbol{F}_1 \to \mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}_1)$ of $\mathcal{F}$ into $\mathcal{G}$ is injective. Let $\mathfrak{G}'$ be an element of $\mathcal{G}$. Then, the set $\boldsymbol{F}'$ of all elements of $\boldsymbol{G}$ which are invariant under all elements of $\mathfrak{G}'$ is clearly an intermediate differential field. If z is an element of $\boldsymbol{G}-\boldsymbol{F}'$, there exists $\sigma \in \mathfrak{G}'$ with $\sigma z \neq z$, so that $\boldsymbol{F}'$ belongs to $\mathcal{F}$. Similarly as in [4], we can prove the equality $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}')=\mathfrak{G}'$.

PROPOSITION 7.2. *Let $\boldsymbol{F}_1$ be an element of $\mathcal{F}$. Then, $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}_1)$ is a normal subgroup of $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$ if and only if $\sigma\boldsymbol{F}_1=\boldsymbol{F}_1$ for every element σ of $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$. If that is so, every element σ of $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$ induces a differential automorphism $\bar{\sigma}$ of $\boldsymbol{F}_1$ over $\boldsymbol{F}$, and the map $\sigma \to \bar{\sigma}$ is a homomorphism of the group $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$ onto the group $\mathfrak{G}(\boldsymbol{F}_1/\boldsymbol{F})$ of all differential automorphisms of $\boldsymbol{F}_1$ over $\boldsymbol{F}$, and the kernel of this homomorphism is $\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}_1)$; moreover, $\boldsymbol{F}_1$ satisfies the condition* (S_0) *over $\boldsymbol{F}$.*

Proof. We prove here only the statement that the homomorphism $\sigma \to \bar{\sigma}$ is onto; the other parts of the proof of Prop. 7.2 are similar to those in [4].

Let τ be an element of $\mathfrak{G}(\boldsymbol{F}_1/\boldsymbol{F})$, and $X_1, \cdots, X_n$ differentially independent over $\boldsymbol{F}_1$, and put $\boldsymbol{R}_1=\boldsymbol{F}_1\{X_1, \cdots, X_n\}$, $\boldsymbol{S}=\boldsymbol{G}\{X_1, \cdots, X_n\}$, $\mathfrak{p}=\mathfrak{p}_{(x)/\boldsymbol{F}_1}$. Denote by $\mathfrak{p}^{\tau}$ the set of all elements of $\boldsymbol{R}_1$ which are obtained from differential polynomials in $\mathfrak{p}$ by operating τ on their coefficients. Then, $\mathfrak{p}^{\tau}$ is a differential prime ideal of $\boldsymbol{R}_1$ not containing 1, and, we can prove similarly as Prop. 4. 2 that the ideal $\boldsymbol{G}\mathfrak{p}^{\tau}$ of $\boldsymbol{S}$ has an irredundant representation as an intersection of differential prime ideals $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ of $\boldsymbol{S}$, so that $\boldsymbol{R}_1\frown\mathfrak{P}_i=\mathfrak{p}^{\tau}$ $(1\leqslant i\leqslant r)$. If $(y_1, \cdots, y_n)$ is a generic zero of $\mathfrak{P}_1$, (y) is also a generic zero of $\mathfrak{p}^{\tau}$. Now, we express every $z\in\boldsymbol{G}$ in the form

$$z = A_1(x)/B_1(x) \quad (A_1(X)\,,\ B_1(X)\in\boldsymbol{R}_1\,;\ B_1(x)\neq 0)\,.$$

Denoting by $A_1^{\tau}(X)$, $B_1^{\tau}(X)$ the differential polynomials which are obtained from $A_1(X)$, $B_1(X)$ respectively by operating τ on their coefficients, put

$$z' = A_1^{\tau}(y)/B_1^{\tau}(y)\,.$$

This z' is well-defined by z, and the map $z\to z'$ determines a differential isomorphism σ' of $\boldsymbol{G}$ into $\boldsymbol{G}\langle y_1, \cdots, y_n\rangle$ which is obviously a prolongation of τ.

On account of the existence of σ', we can see, using Lem. 6. 1, the existence of a differential automorphism σ of $\boldsymbol{G}$ over $\boldsymbol{F}$ which prolongs τ.

8. Primitives and exponentials

Primitives Let x be an element of a differential extension field of $\boldsymbol{F}$, and put $\delta_{i\nu}x=a_{i\nu}$ $(1\leqslant i\leqslant m,\ \nu\geqslant 0)$ and $\theta x=a_{\theta}$ $(\theta\in\Theta)$. If $a_{i\nu}\in\boldsymbol{F}$ $(1\leqslant i\leqslant m,\ \nu>0)$ i.e. $a_{\theta}\in\boldsymbol{F}$ $(\theta\in\Theta,\ \mathrm{ord}\,\theta>0)$, x is called a *primitive* over $\boldsymbol{F}$. If x is a primitive over $\boldsymbol{F}$ and σ' a differential isomorphism over $\boldsymbol{F}$ of $\boldsymbol{F}\langle x\rangle$ into its differential extension field, then $\sigma' x=c'+x$, where c' is a constant of $\boldsymbol{F}\langle x\rangle\langle\sigma'\boldsymbol{F}\langle x\rangle\rangle$.

Let us suppose that x is a primitive over $\boldsymbol{F}$ with $x\notin\boldsymbol{F}$, that every constant of $\boldsymbol{G}=\boldsymbol{F}\langle x\rangle$ is contained in $\boldsymbol{F}$, and that $\boldsymbol{G}$ satisfies the condition (S) over $\boldsymbol{F}$. Then, choosing two integers i_0, ν_0 $(1\leqslant i_0\leqslant m,\ \nu_0>0)$ with $a_{i_0\nu_0}\neq 0$, the set of linear homogeneous differential equations

$$\theta X-(a_\theta/a_{i_0\nu_0})\cdot\delta_{i_0\nu_0}X = 0 \qquad (\theta\in\Theta,\ \mathrm{ord}\,\theta>0)$$

over $\boldsymbol{F}$ has a fundamental system 1, x of solutions, so that $\boldsymbol{G}$ is a Picard-Vessiot extension of $\boldsymbol{F}$. With respect to 1, x, every element σ of the Galois group $\mathfrak{G}=\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$ is identified with an element of $GL(2, \boldsymbol{C})$:

$$\sigma = \begin{pmatrix}1 & c\\ 0 & 1\end{pmatrix} \qquad (c\in\boldsymbol{C}).$$

Hence, $\mathfrak{G}$ is abelian and anticompact (see [4]). The map $\sigma\to c$ is an isomorphism of $\mathfrak{G}$ into the additive group $\boldsymbol{C}^+$ of $\boldsymbol{C}$, the image of $\mathfrak{G}$ being an algebraic subgroup of $\boldsymbol{C}^+$. We have two possible cases:

Case I: suppose $\mathfrak{G}$ is of finite order s. Let its elements be σ_0 (the identity map), $\sigma_1, \cdots, \sigma_{s-1}$ and their images $c_0(=0)$, $c_1, \cdots, c_{s-1}$. Then, x is a root of an algebraic equation $\prod_{i=0}^{s-1}(X+c_i)=a\,(a\in\boldsymbol{F})$ which is irreducible over $\boldsymbol{F}$, and x is separable over $\boldsymbol{F}$. Since $\sigma_i^s=\sigma_0$ i.e. $sc_i=0$ $(1\leqslant i\leqslant s-1)$, Case I can occur only for $p\neq 0$. We can see that s is a power p^e of p, and that there exist e elements $\gamma_1, \cdots, \gamma_e$ of $\boldsymbol{C}$, which are linearly independent over the prime field, such that the additive group $\{c_0, c_1, \cdots, c_{s-1}\}$ is generated by $\gamma_1, \cdots, \gamma_e$. ($\mathfrak{G}$ will be denoted by $\mathfrak{G}_{\gamma_1\cdots\gamma_e}$.)

Case II: suppose $\mathfrak{G}$ infinite. Then, x is transcendental over $\boldsymbol{F}$, and the isomorphism $\sigma\to c$ is onto $\boldsymbol{C}^+$. (In this case $\mathfrak{G}$ is denoted by $\mathfrak{G}_P$.) If $p\neq 0$, for every power p^e of p, $\boldsymbol{C}^+$ contains algebraic subgroups of the form $\mathfrak{G}_{\gamma_1\cdots\gamma_e}$. To such a group $\boldsymbol{G}_{\gamma_1\cdots\gamma_e}$ corresponds the intermediate field

$$\boldsymbol{F}_{\gamma_1\cdots\gamma_e} = \boldsymbol{F}\langle \prod_{\substack{0\leqslant h_1\leqslant p-1\\ \cdots\cdots\\ 0\leqslant h_e\leqslant p-1}} (x+h_1\gamma_1+\cdots+h_e\gamma_e)\rangle\,.$$

Exponentials Let x be a non-zero element of a differential extension field of $\boldsymbol{F}$, and put $(\delta_{i\nu}x)/x=a_{i\nu}$ $(1\leqslant i\leqslant m,\ \nu\geqslant 0)$ and $(\theta x)/x=a_\theta$ $(\theta\in\Theta)$. If $a_{i\nu}\in\boldsymbol{F}$ $(1\leqslant i\leqslant m,\ \nu\geqslant 0)$ i.e. $a_\theta\in\boldsymbol{F}$ $(\theta\in\Theta)$, x is called an *exponential* over $\boldsymbol{F}$. If x is an exponential over $\boldsymbol{F}$

and σ' a differential isomorphism over $\boldsymbol{F}$ of $\boldsymbol{F}\langle x\rangle$ into its differential extension field, then $\sigma' x = c' x$, where c' is a non-zero constant of $\boldsymbol{F}\langle x\rangle\langle\sigma'\boldsymbol{F}\langle x\rangle\rangle$.

Let us suppose that x is an exponential over $\boldsymbol{F}$ with $x\notin\boldsymbol{F}$, that every constant of $\boldsymbol{G}=\boldsymbol{F}\langle x\rangle$ is contained in $\boldsymbol{F}$, and that $\boldsymbol{G}$ satisfies the condition (S) over $\boldsymbol{F}$. Then, the set of linear homogeneous differential equations

$$\theta X - a_\theta X = 0 \qquad (\theta\in\Theta)$$

over $\boldsymbol{F}$ has a fundamental system x of solutions, so that $\boldsymbol{G}$ is a Picard-Vessiot extension of $\boldsymbol{F}$. With respect to x, every element σ of the Galois group $\mathfrak{G}=\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$ is identified with an element of $GL(1, \boldsymbol{C})$:

$$\sigma = c \qquad (c\in\boldsymbol{C})\,.$$

Hence, $\mathfrak{G}$ is abelian and quasicompact (see [4]), and an algebraic subgroup of the multiplicative gronp $\boldsymbol{C}^\times$ of $\boldsymbol{C}$. We have two possible cases:

Case I: suppose $\mathfrak{G}$ of finite order s. Similarly as in [4], we see that $x^s\in\boldsymbol{F}$ where s is not divisible by p, and that $\mathfrak{G}$ consists of all s-th roots of unity. ($\mathfrak{G}$ will be denoted by $\mathfrak{G}_s$.)

Case II: suppose $\mathfrak{G}$ infinite. Then, x is transcendental over $\boldsymbol{F}$ and $\mathfrak{G}=\boldsymbol{C}^\times$. (In this case $\mathfrak{G}$ is denoted by $\mathfrak{G}_E$.) For every positive integer s which is not divisible by p, $\boldsymbol{C}^\times$ contains a unique algebraic subgroup $\mathfrak{G}_s$ of all s-th roots of unity, and the intermediate differential field $\boldsymbol{F}_s=\boldsymbol{F}\langle x^s\rangle$ corresponds to $\mathfrak{G}_s$.

9. Liouvillian extensions

Let $\boldsymbol{H}$ be a differential extension field of $\boldsymbol{F}$. Suppose that $\boldsymbol{H}$ satisfies the following conditions:

(L1) every constant of $\boldsymbol{H}$ is contained in $\boldsymbol{F}$,

(L2) there exist a finite number of elements $y_1, \cdots, y_r$ of $\boldsymbol{H}$ such that $\boldsymbol{H}=\boldsymbol{F}\langle y_1, \cdots, y_r\rangle$,

(L3) if we put $\boldsymbol{F}_0=\boldsymbol{F}$, $\boldsymbol{F}_j=\boldsymbol{F}_{j-1}\langle y_j\rangle$ $(1\leqslant j\leqslant r)$, it holds that, for each j $(1\leqslant j\leqslant r)$, either y_j is a primitive or an exponential

over F_{j-1}, or y_j is separably algebraic and normal[7] over F_{j-1},
(L4) H satisfies the condition (S) over every F_j $(0 \leqslant j \leqslant r)$.

Then, H is called a *Liouvillian extension* of F. In case $p=0$, this is a Liouvillian extension satisfying the normality condition of the remark at p. 38 of [4].

Now, let G be an intermediate differential field between F and H such that G is a Picard-Vessiot extension of F.

LEMMA 9.1. *Let H and G be as above. Then, $G\langle y_1\rangle$ is a Picard-Vessiot extension of $F\langle y_1\rangle$, and G is a Picard-Vessiot extension of $F\langle y_1\rangle \cap G$, and we have*

$$\mathfrak{G}(G\langle y_1\rangle / F\langle y_1\rangle) = \mathfrak{G}(G/F\langle y_1\rangle \cap G)\,.$$

The first two statements are obvious. The last statement can be proved similarly as in [4] (Chap. IV §21).

LEMMA 9.2. *Let H and G be as above. Then, $\mathfrak{G}=\mathfrak{G}(G/F)$ has a normal chain, in which every quotient group is abelian or finite.*

The proof is similar to that in pp. 39–40 of [4].

We shall distinguish, as in [4], ten types of differential extensions of F, namely, extensions by

1° primitives, exponentials, and separably algebraic elements,
2° primitives and exponentials,
3° exponentials and separably algebraic elements,
4° primitives and separably algebraic elements,
5° primitives and separable radicals
6° exponentials, 7° primitives,
8° separably algebraic elements,
9° separable radicals, 10° rational elements;

for each of these types, we do not exclude the possibility of finite repetitions of infinite sequences of extensions.

Let $\mathfrak{G}=\mathfrak{G}(G/F)$ be the Galois group of a Picard-Vessiot extension G of F and $\mathfrak{G}^0$ its component of the identity, and list the properties which they may possess:

7) This means that the separably algebraic extension $F_{j-1}\langle y_j\rangle = F_{j-1}(y_j)$ of F_{j-1} is normal over F_{j-1}.

1°	$\mathfrak{G}^0$ is solvable,	2°	$\mathfrak{G}$ is solvable,
3°	$\mathfrak{G}^0$ is quasicompact,	4°	$\mathfrak{G}^0$ is anticompact,
5°	$\mathfrak{G}$ is solvable and $\mathfrak{G}^0$ is anticompact,		
6°	$\mathfrak{G}$ is solvable and quasicompact,		
7°	$\mathfrak{G}$ is solvable and anticompact,		
8°	$\mathfrak{G}$ is finite,	9°	$\mathfrak{G}$ is solvable and finite,
10°	$\mathfrak{G}=\{\sigma_0\}$ (σ_0 being the identity).		

PROPOSITION 9.1. *Let $\boldsymbol{G}$ be a Picard-Vessiot extension of $\boldsymbol{F}$, $\mathfrak{G}=\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F})$ the Galois group, $\mathfrak{G}^0$ its component of the identity and i a positive integer $\leqslant 10$. If $\mathfrak{G}$ is contained in a Liouvillian extension of $\boldsymbol{F}$ of type i^0, then $\mathfrak{G}$ is of type i^0. Conversely, if $\boldsymbol{G}$ is of type i^0, then $\boldsymbol{G}$ is of type i^0.*

Proof. Suppose that $\boldsymbol{G}$ is contained in a Liouvillian extension $\boldsymbol{H}$ of $\boldsymbol{F}$ of type i^0. Then, we can prove similarly as in [4] (p. 40) that $\mathfrak{G}$ is of type i^0.

Conversely, suppose that $\mathfrak{G}$ is of type i^0, and let us prove that $\boldsymbol{G}$ is of type i^0. Since this is clear in case $8\leqslant i\leqslant 10$, we consider only the cases $1\leqslant i\leqslant 7$ as follows.

$\mathfrak{G}^0$ is a normal algebraic subgroup of $\mathfrak{G}$. Therefore, by Prop. 7.2, it corresponds to the intermediate differential field $\boldsymbol{F}^0$ between $\boldsymbol{F}$ and $\boldsymbol{G}$, such that $\mathfrak{G}^0=\mathfrak{G}(\boldsymbol{G}/\boldsymbol{F}^0)$, $\mathfrak{G}/\mathfrak{G}^0=\mathfrak{G}(\boldsymbol{F}^0/\boldsymbol{F})$ and $\boldsymbol{F}^0$ satisfies the condition (S_0) over $\boldsymbol{F}$. Hence, $\boldsymbol{F}^0$ is a finite algebraic extension of $\boldsymbol{F}$, and, moreover, it is separably and normally algebraic over $\boldsymbol{F}$ (see Rem. at the end of § 4). Since $\mathfrak{G}^0$ is of type 2°, 2°, 6°, 7°, 7°, 6° or 7° according as $\mathfrak{G}$ is of type 1°, 2°, 3°, 4°, 5°, 6° or 7°, we may assume for our purpose that $\mathfrak{G}$ is connected and of type 2°, 6° or 7°.

Case I: $\mathfrak{G}$ is of type 7°. Since $\mathfrak{G}$ can be reduced to special triangular form (see [4] pp. 19–20), the defining set of linear homogeneous differential equations of $\boldsymbol{G}$ over $\boldsymbol{F}$ has a fundamental system $x_1, \cdots, x_n$ of solutions with $\boldsymbol{G}=\boldsymbol{F}\langle x_1, \cdots, x_n\rangle$ such that

$$(9.1)\qquad \sigma x_j=\sum_{i=1}^{j} x_i c_{ij} \qquad (1\leqslant j\leqslant n,\ c_{ij}\in \boldsymbol{C},\ c_{jj}=1)$$

for every $\sigma\in\mathfrak{G}$. Let us prove, by means of (9.1) and the induction on n, that $\boldsymbol{G}$ is of type 7°. Since x_1 is contained in $\boldsymbol{F}$ in any case, the case $n=1$ is trivial. Now, suppose $n>1$; then, we get

$$\sigma(x_j/x_1) = c_{1j}+\sum_{i=2}^{j}(x_i/x_1)\cdot c_{ij} \qquad (2\leqslant j\leqslant n),$$

so that

$$\sigma(\theta(x_j/x_1)) = \sum_{i=2}^{j}\theta(x_i/x_1)\cdot c_{ij} \qquad (2\leqslant j\leqslant n;\ \theta\in\Theta,\ \operatorname{ord}\theta>0,\ \sigma\in\mathfrak{G}).$$

By the induction assumption, $\boldsymbol{F}\langle\theta(x_2/x_1), \cdots, \theta(x_n/x_1)\rangle$ is of type 7° for each $\theta\in\Theta$ with $\operatorname{ord}\theta>0$; hence, $\boldsymbol{F}\langle\theta(x_2/x_1), \cdots, \theta(x_n/x_1);\ \theta\in\Theta, \operatorname{ord}\theta>0\rangle$ is of type 7°, and so is $\boldsymbol{F}\langle x_2/x_1, \cdots, x_n/x_1\rangle = \boldsymbol{F}\langle x_1, \cdots, x_n\rangle=\boldsymbol{G}$.

Case II: $\mathfrak{G}$ is of type 6°. Since $\mathfrak{G}$ can be reduced to diagonal form (see [4] pp. 19–21), the defining set of linear homogeneous differential equations of $\boldsymbol{G}$ over $\boldsymbol{F}$ has a fundamental system $x_1, \cdots, x_n$ of solutions with $\boldsymbol{G}=\boldsymbol{F}\langle x_1, \cdots, x_n\rangle$ such that

$$\sigma x_j = c_j x_j \qquad (1\leqslant j\leqslant n,\ c_j\in\boldsymbol{C})$$

for every $\sigma\in\mathfrak{G}$. Hence, $\sigma(\theta x_j) = c_j(\theta x_j)$ $(1\leqslant j\leqslant n,\ \theta\in\Theta)$, and $\sigma(\theta x_j/x_j)=\theta x_j/x_j$ $(1\leqslant j\leqslant n,\ \theta\in\Theta)$ for every $\sigma\in\mathfrak{G}$, so that $\theta x_j/x_j\in\boldsymbol{F}$ $(1\leqslant j\leqslant n,\ \theta\in\Theta)$. Therefore, $\boldsymbol{G}$ is of type 6° (finite repetitions of extensions by exponentials).

Case III: $\mathfrak{G}$ is of type 2°. Since $\mathfrak{G}$ can be reduced to triangular form (see [4] p. 19), the defining set of linear homogeneous differential equations of $\boldsymbol{G}$ over $\boldsymbol{F}$ has a fundamental system $x_1, \cdots, x_n$ of solutions with $\boldsymbol{G}=\boldsymbol{F}\langle x_1, \cdots, x_n\rangle$ such that

$$\sigma x_j = \sum_{i=1}^{j}x_i c_{ij} \qquad (1\leqslant j\leqslant n,\ c_{ij}\in\boldsymbol{C}) \tag{9.2}$$

for every $\sigma\in\mathfrak{G}$. Let us prove, by means of (9.2) and the induction on n, that $\boldsymbol{G}$ is of type 2°. Similarly as in Case II, x_1 is exponential over $\boldsymbol{F}$. Since the case $n=1$ is trivial, suppose $n>1$. Then, we get

$$\sigma(x_j/x_1) = (c_{1j}/c_{11})+\sum_{i=2}^{j}(x_i/x_1)\cdot(c_{ij}/c_{11}) \qquad (2\leqslant j\leqslant n),$$

so that

$$\sigma(\theta(x_j/x_1))=\sum_{i=2}^{j}\theta(x_i/x_1)\cdot(c_{ij}/c_{11}) \quad (2\leqslant j\leqslant n\,;\ \theta\in\Theta,\ \mathrm{ord}\,\theta>0,\ \sigma\in\mathfrak{G})\,.$$

By the induction assumption, $\boldsymbol{F}\langle\theta(x_2/x_1), \cdots, \theta(x_n/x_1)\rangle$ is of type 2° for each $\theta\in\Theta$ with $\mathrm{ord}\,\theta>0$; hence, $\boldsymbol{F}\langle\theta(x_2/x_1), \cdots, \theta(x_n/x_1)\,;\ \theta\in\Theta, \mathrm{ord}\,\theta>0\rangle$ is of type 2°, and so are $\boldsymbol{F}\langle x_2/x_1, \cdots, x_n/x_1\rangle$ and $\boldsymbol{F}\langle x_1, x_2/x_1, \cdots, x_n/x_1\rangle=\boldsymbol{G}$.

Institute of Mathematics,
Yoshida College,
Kyoto University.

REFERENCES

[0] Borel, A., Groupes linéaires algébriques, Ann. of Math., Vol. 64, 1956, pp. 20–82.
[1] Hasse, H., Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik, Journ. reine angew. Math., Vol. 175, 1936, pp. 50–54.
[2] Kaplansky, I., An introduction to differential algebra, Act. sci. ind., Paris, Hermann, 1957.
[3] Kolchin, E. R., On the basis theorem for differential systems, Trans. Amer. Math. Soc., Vol. 52, 1942, pp. 115–127.
[4] ——————, Algebraic matric groups and the Picard-Vessiot theory of homogeneous ordinary linear differential equations, Ann. Math., Vol. 49, 1948, pp. 1–42.
[4′] ——————, On certain concepts in the theory of algebraic matric groups, Ann. Math., Vol. 49, 1948, pp. 774–789.
[5] ——————, Picard-Vessiot theory of partial differential fields, Proc. Amer. Math. Soc., Vol. 3, 1952, pp. 596–603.
[6] ——————, Galois theory of differential fields, Amer. Journ. Math., Vol. LXXV, 1953, pp. 753–824.
[7] ——————, On the Galois theory of differential fields, Amer. Journ. Math., Vol. LXXVII, 1955, pp. 868–894.
[8] ——————, Abelian extensions of differential fields, Amer. Journ. Math., Vol. LXXXII, 1960, pp. 779–790.
[9] Matsumura, H., Automorphism-groups of differential fields and group-varieties, Mem. Col. Sci., Univ. of Kyoto, Ser. A, Vol. XXVIII, Math., 1953, pp. 283–292.
[10] Okugawa, K., On differential algebra of arbitrary characteristic, Mem. Col. Sci., Univ. of Kyoto, Ser. A, Vol. XXVIII, Math., 1953, pp. 97–107. Concerning an error contained in it, see the description by Kolchin in Math. Review, Vol. 16, 1955, pp. 562–563.
[11] Ritt, J. F., Differential algebra, Amer. Math. Soc. Coloq. Publ., Vol. XXXIII, 1950.
[12] Schmidt, F. K.—H. Hasse, Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten, Journ. reine angew. Math., Vol. 177, 1937, pp. 215–237.
[13] Seidenberg, A., Some basic theorems in differential algebra (Characteristic p, arbitrary), Trans. Amer. Math. Soc., Vol. 73, 1952, pp. 174–190.