

## Hironaka's Additive Group Scheme, II

By

Tadao ODA <sup>\*)</sup>, <sup>\*\*)</sup>

### Introduction

In connection with resolution of singularities of algebraic varieties in positive characteristics, Hironaka [H] introduced certain subgroup schemes, now called *Hironaka subgroup schemes*, in a vector group scheme over a field  $k$  of positive characteristic  $p$ . Oda [O<sub>1</sub>] then reduced their study to linear algebra as follows: Hironaka subgroup schemes of exponent  $\leq e$  in an  $(n+1)$ -dimensional vector group scheme over  $k$  are in one-to-one correspondence with a proper  $k$ -subspace  $V$  of  $k \otimes_{k^q} T$  for a fixed  $(n+1)$ -dimensional  $k^q$ -vector space  $T$  (with  $q = p^e$ ) satisfying the condition

$$\mathcal{N}_e \mathcal{D}_e(V) = V$$

(cf. [O<sub>1</sub>, Theorem 2.6]). This condition, however, is sometimes rather inconvenient to deal with.

The purpose of this paper is to give alternative characterizations, independent of the exponent, of Hironaka subgroup schemes (Theorem 2.2). Some of our characterizations have close connection with the one given by Russel [R].

As a by-product, we get in Theorem 3.1 a *versal family* of Hironaka subgroup schemes, which provides us not only with an efficient tool for computation but also with insight when we study the effect of permissible blowing-ups on tangent cones, as we see in Theorem 4.1 and in [O<sub>3</sub>], [O<sub>4</sub>].

In Section 1, we collect together notations and results on differential operators of the perfect closure  $F^{-\infty}(k)$  of the ground field  $k$  into itself over  $k$  necessary for our later formulations. We also correct here one of the two errors in [O<sub>2</sub>].

---

Received November 24, 1982.

<sup>\*)</sup> Mathematical Institute, Tôhoku University, Sendai 980, Japan.

<sup>\*\*)</sup> Partly supported by the Grants-in-Aid for Scientific as well as Co-operative Research, the Ministry of Education, Science and Culture, Japan.

In Section 2, we state and prove Theorem 2.2 giving alternative characterizations of Hironaka subgroup schemes, some of which were announced in [O<sub>2</sub>, Theorem]. We also correct in Corollary 2.3 the other error in [O<sub>2</sub>].

In Section 3, we construct a versal family of Hironaka subgroup schemes as we announced in [O<sub>2</sub>] under different notations. The family, combined with results in Section 1, will turn out to be useful in computing interesting examples of Hironaka subgroup schemes. For lack of space here, however, we postpone the computation until a later paper.

Instead, we apply the versal family to obtain Proposition 3.2, which enables us to prove Theorem 4.1 on the *transformation homomorphism* basic in studying the effect of permissible blowing-ups on the tangent cone. As we see in [O<sub>3</sub>], [O<sub>4</sub>], the results in Section 4 naturally lead us to introduce *higher order Hironaka subgroup schemes* essential in studying the “infinitely very near” situation (the terminology due to Giraud [G]) in resolution of singularities.

Thanks are due to Hironaka and Giraud for stimulating discussions.

### §1. Differential Operators on the Perfect Closure

Let  $k$  be a field of positive characteristic  $p$ . On a fixed algebraic closure of  $k$ , let  $F$  be the  $p$ -th power Frobenius map. For each nonnegative integer  $e$ , the subfield  $F^{-e}(k)$  of the algebraic closure consists of the  $p^e$ -th roots of elements of  $k$  and

$$F^{-\infty}(k) := \bigcup_{e \geq 0} F^{-e}(k)$$

is the *perfect closure* of  $k$ .

In this section, we collect together notations and results on differential operators of  $F^{-\infty}(k)$  into itself over  $k$  necessary for our new formulation later, independent of the exponent, of the theory of Hironaka subgroup schemes.

Let  $\Delta$  be the diagonal ideal of  $F^{-\infty}(k) \otimes_k F^{-\infty}(k)$ , i.e., the kernel of the multiplication map  $F^{-\infty}(k) \otimes_k F^{-\infty}(k) \rightarrow F^{-\infty}(k)$ . Consider the *decreasing filtration*  $\{\Delta^{(r)}\}$  of the ring  $F^{-\infty}(k) \otimes_k F^{-\infty}(k)$  by ideals parametrized by *non-negative rational numbers  $r$  with  $p$ -power denominators* as follows:

$$\Delta^{(r)} := \bigcup_{e \geq 0} \{ \Delta \cap (F^{-e}(k) \otimes_k F^{-e}(k)) \}^{m_e},$$

where  $m_e$  is the smallest integer  $\geq rp^e$  for each  $e$ . We have

$$\Delta^{(r)} \cdot \Delta^{(r')} \subset \Delta^{(r+r')}, \quad \bigcap_{r \geq 0} \Delta^{(r)} = \{0\}.$$

Further, we let

$$\Delta^{(r+0)} := \cup_{r' > r} \Delta^{(r')} \subset \Delta^{(r)}$$

so that in particular  $\Delta^{(0+0)} = \Delta$  and  $\Delta^{(r+0)} \cdot \Delta^{(r')} \subset \Delta^{(r+r'+0)}$  for nonnegative rational numbers  $r, r'$  with  $p$ -power denominators.

Let  $\mathcal{D} := \text{Diff}(F^{-\infty}(k)/k)$  be the ring of differential operators of  $F^{-\infty}(k)$  into itself over  $k$ . As is well-known,  $D$  in  $\mathcal{D}$  can be identified with a  $(1 \otimes F^{-\infty}(k))$ -linear functional  $\eta_D$  on  $F^{-\infty}(k) \otimes_k F^{-\infty}(k)$  by

$$D: F^{-\infty}(k) \xrightarrow{i} F^{-\infty}(k) \otimes_k F^{-\infty}(k) \xrightarrow{\eta_D} F^{-\infty}(k),$$

where  $i$  is defined by  $i(\beta) = \beta \otimes 1$  for  $\beta$  in  $F^{-\infty}(k)$ . We have an increasing filtration  $\{\mathcal{D}^{(r)}\}$  of  $\mathcal{D}$  by (left)  $F^{-\infty}(k)$ -subspaces parametrized by nonnegative rational numbers  $r$  with  $p$ -power denominators, if we let

$$\mathcal{D}^{(r)} := \{D \in \mathcal{D}; \eta_D(\Delta^{(r)}) = 0\}.$$

If we further let

$$\mathcal{D}^{(r+0)} := \cap_{r' > r} \mathcal{D}^{(r')} = \{D \in \mathcal{D}; \eta_D(\Delta^{(r+0)}) = 0\} \supset \mathcal{D}^{(r)},$$

then we have

$$\mathcal{D}^{(r+0)} \cdot \mathcal{D}^{(r'+0)} \subset \mathcal{D}^{(r+r'+0)} \quad \text{and} \quad \mathcal{D}^{(r+0)} \cdot \mathcal{D}^{(r')} \subset \mathcal{D}^{(r+r')}$$

for nonnegative rational numbers  $r, r'$  with  $p$ -power denominators.

For each nonnegative integer  $e$ , the  $(1 \otimes F^{-\infty}(k))$ -linear injection  $F^{-e}(k) \otimes_k F^{-\infty}(k) \hookrightarrow F^{-\infty}(k) \otimes_k F^{-\infty}(k)$  induces the  $F^{-\infty}(k)$ -linear surjective restriction map

$$\mathcal{D} \longrightarrow F^{-\infty}(k) \otimes_{F^{-e}(k)} \text{Diff}(F^{-e}(k)/k),$$

which sends  $\mathcal{D}^{(r)}$  (resp.  $\mathcal{D}^{(r+0)}$ ), for each  $r$ , onto the  $F^{-\infty}(k)$ -subspace of differential operators over  $k$  from  $F^{-e}(k)$  to  $F^{-\infty}(k)$  of order  $< rp^e$  (resp.  $\leq rp^e$ ). In particular, we have the  $F^{-\infty}(k)$ -linear surjective restriction map

$$\mathcal{D}^{(1)} \longrightarrow F^{-\infty}(k) \otimes_{F^{-e}(k)} \text{Diff}_{p^{e-1}}(F^{-e}(k)/k),$$

which will play a key role in the theory of Hironaka subgroup schemes.

**Correction.** The definition of  $\text{Diff}(k_{\infty}/k)$  in [O<sub>2</sub>, p. 126, line 5 from below through p. 127, line 5 from above] is completely wrong. It should be modified as above, where  $k_{\infty}$  coincides with  $F^{-\infty}(k)$  in our present notation.

**Lemma 1.1.** *Let  $\mathcal{D}$  act on  $F^{-\infty}(k) \otimes_k F^{-\infty}(k)$  through the first factor.*

Then for nonnegative rational numbers  $r, s$  with  $p$ -power denominators, we have

$$\mathcal{D}^{(s+0)} \cdot \Delta^{(r)} \subset \Delta^{(r-s)}, \mathcal{D}^{(s+0)} \cdot \Delta^{(r+0)} \subset \Delta^{(r-s+0)} \quad \text{and} \quad \mathcal{D}^{(s)} \cdot \Delta^{(r)} \subset \Delta^{(r-s+0)},$$

where we let  $\Delta^{(r')} = F^{-\infty}(k) \otimes_k F^{-\infty}(k)$  if  $r' \leq 0$ .

The proof of the above lemma is obvious.

Here is a more down-to-earth description for what we had so far, which we also use later: Let  $\mathcal{Q}'$  be the set of rational numbers  $r$  with  $p$ -power denominators with  $0 \leq r < 1$ , i.e.,  $r = l/p^e$  for an integer  $l$  with  $0 \leq l < p^e$  and a nonnegative integer  $e$ . Fix a  $p$ -basis  $\{a_\gamma\}_{\gamma \in \Gamma}$  of  $k$  over  $F(k)$ . Thus the monomials in finite numbers of  $a_\gamma$ 's with individual exponents less than  $p$  form an  $F(k)$ -linear basis of  $k$ . Let  $\Lambda$  be the set of such  $\lambda = (\lambda_\gamma)_{\gamma \in \Gamma}$  that  $\lambda_\gamma \in \mathcal{Q}'$  for all  $\gamma \in \Gamma$  and that  $\lambda_\gamma = 0$  for all but a finite number of  $\gamma$ 's. Then  $|\lambda| := \sum_{\gamma \in \Gamma} \lambda_\gamma$  is a well-defined nonnegative rational number with  $p$ -power denominator.

If  $r = l/p^e$  for an integer  $l$  with  $0 \leq l < p^e$ , then  $(a_\gamma)^r := (F^{-e}(a_\gamma))^l$  is a well-defined element of  $F^{-e}(k) \subset F^{-\infty}(k)$ . Thus for  $\lambda = (\lambda_\gamma)_{\gamma \in \Gamma}$  in  $\Lambda$ , we have a well-defined element

$$a^\lambda := \prod_{\gamma \in \Gamma} (a_\gamma)^{\lambda_\gamma} \in F^{-\infty}(k).$$

We see that  $\{a^\lambda; \lambda \in \Lambda\}$  form a  $k$ -linear basis of  $F^{-\infty}(k)$ , while  $\{a^\lambda; \lambda = (\lambda_\gamma)_{\gamma \in \Gamma} \in \Lambda, \lambda_\gamma p^e \in \mathbf{Z} \text{ for all } \gamma \in \Gamma\}$  form a  $k$ -linear basis of  $F^{-e}(k)$ .

Again for  $\lambda = (\lambda_\gamma)_{\gamma \in \Gamma}$  with  $\lambda_\gamma = l_\gamma/p^e$  and  $0 \leq l_\gamma < p^e$ , consider the element

$$(\delta a)^\lambda := \prod_{\gamma \in \Gamma} (F^{-e}(a_\gamma) \otimes 1 - 1 \otimes F^{-e}(a_\gamma))^{l_\gamma} \in F^{-\infty}(k) \otimes_k F^{-\infty}(k).$$

Note that the right hand side is independent of the expression for  $\lambda_\gamma$ 's as fractions. For  $\lambda = (\lambda_\gamma)_{\gamma \in \Gamma}$  and  $\mu = (\mu_\gamma)_{\gamma \in \Gamma}$ , we have  $(\delta a)^\lambda \cdot (\delta a)^\mu = (\delta a)^{\lambda + \mu}$ , where  $\lambda + \mu := (\lambda_\gamma + \mu_\gamma)_{\gamma \in \Gamma}$ .  $\{(\delta a)^\lambda; \lambda \in \Lambda\}$  form an  $(F^{-\infty}(k) \otimes 1)$ - as well as  $(1 \otimes F^{-\infty}(k))$ -linear basis of  $F^{-\infty}(k) \otimes_k F^{-\infty}(k)$ , while for each nonnegative rational number  $r$  with  $p$ -power denominator,

$$\{(\delta a)^\lambda; \lambda \in \Lambda, |\lambda| \geq r\} \quad (\text{resp. } \{(\delta a)^\lambda; \lambda \in \Lambda, |\lambda| > r\})$$

form an  $(F^{-\infty}(k) \otimes 1)$ - as well as  $(1 \otimes F^{-\infty}(k))$ -linear basis of  $\Delta^{(r)}$  (resp.  $\Delta^{(r+0)}$ ).

For any element  $\beta \in F^{-\infty}(k)$ , we have its *Taylor expansions* in  $F^{-\infty}(k) \otimes_k F^{-\infty}(k)$  given by

$$\begin{aligned} \beta \otimes 1 &= \sum_{\lambda \in \Lambda} (1 \otimes \partial_\lambda \beta) \cdot (\delta a)^\lambda \\ 1 \otimes \beta &= \sum_{\lambda \in \Lambda} (\partial_\lambda \beta \otimes 1) \cdot (-\delta a)^\lambda, \end{aligned}$$

where  $(-\delta a)^\lambda := \prod_{\gamma \in \Gamma} (1 \otimes F^{-e}(a_\gamma) - F^{-e}(a_\gamma) \otimes 1)^{l_\gamma}$  for  $\lambda = (\lambda_\gamma)_{\gamma \in \Gamma} \in \Lambda$  with  $\lambda_\gamma = l_\gamma/p^e$ . The operator  $\partial_\lambda$  sending  $\beta \in F^{-\infty}(k)$  to  $\partial_\lambda \beta \in F^{-\infty}(k)$  is an element of  $\mathcal{D}(|\lambda|+0)$ . For each nonnegative rational number  $r$  with  $p$ -power denominator, each  $D$  in  $\mathcal{D}^{(r)}$  (resp.  $\mathcal{D}^{(r+0)}$ ) is expressed uniquely as a possibly infinite  $F^{-\infty}(k)$ -linear combination of  $\partial_\lambda$ 's with  $|\lambda| < r$  (resp.  $|\lambda| \leq r$ ). The infinite linear combination makes sense, since for  $\beta \in F^{-\infty}(k)$ , we have  $\partial_\lambda \beta = 0$  for all but a finite number of  $\lambda$ 's.

*Leibnitz's rule* holds:

$$\partial_\lambda(\beta\beta') = \sum_{\mu+\nu=\lambda} \partial_\mu(\beta) \cdot \partial_\nu(\beta')$$

for  $\beta$  and  $\beta'$  in  $F^{-\infty}(k)$ , where  $\mu$  and  $\nu$  run through  $\Lambda$  satisfying  $\mu + \nu = \lambda$ .

Let  $\lambda = (\lambda_\gamma)_{\gamma \in \Gamma}$  and  $\mu = (\mu_\gamma)_{\gamma \in \Gamma}$  be in  $\Lambda$ . Take the  $p$ -adic expansions

$$\lambda_\gamma = \sum_{i>0} \lambda_\gamma(i) p^{-i}, \quad \mu_\gamma = \sum_{i>0} \mu_\gamma(i) p^{-i}$$

with integers  $0 \leq \lambda_\gamma(i) \leq p-1$  and  $0 \leq \mu_\gamma(i) \leq p-1$  for all  $\gamma \in \Gamma$  and  $i > 0$ . Define, as an element of the prime field in  $k$ , the *generalized multi-binomial coefficient* by

$$\binom{\lambda}{\mu} := \begin{cases} \prod_{\gamma \in \Gamma, i>0} \binom{\lambda_\gamma(i)}{\mu_\gamma(i)} & \text{if } 0 \leq \mu_\gamma(i) \leq \lambda_\gamma(i) \text{ for all } \gamma \in \Gamma \text{ and all } i > 0, \\ 0 & \text{otherwise,} \end{cases}$$

where the right hand side is the product of the usual binomial coefficients regarded modulo  $p$  as an element of  $k$ . By definition,  $\binom{\lambda}{\mu} \neq 0$  implies that  $\lambda - \mu := (\lambda_\gamma - \mu_\gamma)_{\gamma \in \Gamma}$  is in  $\Lambda$  and  $\binom{\lambda}{\mu} = \binom{\lambda}{\lambda - \mu}$ . The proof of the following is immediate:

**Lemma 1.2.** *For  $\lambda$  and  $\mu$  in  $\Lambda$ , we have*

$$\partial_{\lambda \circ \hat{\mu}} = \binom{\lambda + \mu}{\mu} \partial_{\lambda + \mu}, \quad (\partial_\mu \otimes 1)(\delta a)^\lambda = \binom{\lambda}{\mu} (\delta a)^{\lambda - \mu}.$$

**§2. Alternative Characterizations of Hironaka Subgroup Schemes**

Let  $S = k[x_0, \dots, x_n]$  be a polynomial ring over a field  $k$  of positive characteristic  $p$ . For each nonnegative integer  $v$ , let  $S_v$  be the  $k$ -subspace of  $S$  consisting of homogeneous polynomials of degree  $v$ . Hence  $S = \bigoplus_{v \geq 0} S_v$  is a graded  $k$ -algebra in the usual manner. For each nonnegative integer  $e$ , let  $L_e$  be the  $k$ -subspace of  $S_{p^e}$  consisting of the *additive forms*

$$a_0x_0^{p^e} + a_1x_1^{p^e} + \cdots + a_nx_n^{p^e} \quad (a_0, \dots, a_n \in k).$$

Then  $L = \bigoplus_{e \geq 0} L_e$  is naturally a graded left  $k[F]$ -module with  $F$  acting on  $L$  as the  $p$ -th power map, where  $k[F]$  is the twisted polynomial ring in  $F$  over  $k$  satisfying  $Fa = a^pF$  for each  $a$  in  $k$ . We define  $aF^e$  in  $k[F]$  to be of degree  $e$ . We have  $L = k[F] \otimes_k L_0$ , hence  $L$  is  $k[F]$ -free.

To a homogeneous prime ideal  $\mathfrak{p}$  of  $S$  with  $\mathfrak{p} \neq S_+ := \bigoplus_{v>0} S_v$ , Hironaka [H] associated a subgroup scheme  $B(\mathfrak{p})$  defined over  $k$ , the *Hironaka subgroup scheme*, in the vector group scheme  $\text{Spec}(S)$  over  $k$ , which is homogeneous, i.e., stable under the scalar multiplication action of the multiplicative group scheme  $G_m$ . It can be described uniquely in terms of the graded  $k[F]$ -submodule  $L^{B(\mathfrak{p})}$  of  $L$  consisting of the  $B(\mathfrak{p})$ -invariant additive forms with respect to the translation action of  $B(\mathfrak{p})$  on  $L$  (cf. [O<sub>1</sub>] and [O<sub>4</sub>] for details). By the Jacobian criterion, [O<sub>1</sub>, Proposition 2.2, (ii)] then showed that

$$L_e^{B(\mathfrak{p})} = \{h \in L_e; Dh \in \mathfrak{p} \cap L_e \quad \text{for all } D \in \text{Diff}_{p^{e-1}}(k/F^e(k))\}$$

for each nonnegative integer  $e$ , where  $\text{Diff}_{p^{e-1}}(k/F^e(k))$  is the set of differential operators of  $k$  into itself of order  $\leq p^e - 1$  (hence necessarily over the subfield  $F^e(k)$  consisting of the  $p^e$ -th powers of elements of  $k$ ) acting on the coefficients of elements of  $L_e$ .

A graded  $k[F]$ -submodule  $Q$  of  $L$  is said to be of *exponent* not greater than  $e$  (denoted  $\text{exponent}(Q) \leq e$ ) if  $Q$  is generated as a  $k[F]$ -module by  $Q_0 + Q_1 + \cdots + Q_e$ , i.e.,  $kF^{j-e}Q_e = Q_j$  for all  $j \geq e$ . We also call  $\text{exponent}(L^{B(\mathfrak{p})})$  the exponent of the Hironaka subgroup scheme  $B(\mathfrak{p})$ . The *dimension* of  $B(\mathfrak{p})$  equals the rank of  $L/L^{B(\mathfrak{p})}$  as a module over  $k[F]$ .

Graded  $k[F]$ -submodules of  $L$  which can be of the form  $L^{B(\mathfrak{p})}$  for some  $\mathfrak{p}$  were characterized, and then classified in low dimensions, in [O<sub>1</sub>] and [M]. The characterization, however, is inconvenient in that it can simultaneously deal only with those of  $\text{exponent} \leq e$  for a fixed integer  $e$ . Here is a simple observation, which enables us to give more convenient alternative characterizations: The  $p^e$ -th power Frobenius map  $F^e$  on the ring  $F^{-\infty}(k) \otimes_k S$  induces an isomorphism

$$F^e: F^{-e}(k) \otimes_k L_0 \xrightarrow{\sim} L_e = k \otimes_{F^e(k)} F^e(L_0)$$

for each nonnegative integer  $e$ .

**Lemma 2.1.** *For a graded  $k[F]$ -submodule  $Q$  of  $L$ , the following are equivalent:*

- (1) *There exists a homogeneous prime ideal  $\mathfrak{p}$  of  $S$  such that  $Q = \mathfrak{p} \cap L$ .*
- (2)  *$\text{rad}_L(Q) := \{h \in L; F^i h \in Q \text{ for some } i\}$  coincides with  $Q$ .*
- (3) *There exists an  $F^{-\infty}(k)$ -subspace  $W$  of  $F^{-\infty}(k) \otimes_k L_0$  such that  $Q_e = \{F^e z; z \in W \cap (F^{-e}(k) \otimes_k L_0)\}$  for each nonnegative integer  $e$ .*

Moreover, for a given  $Q$  satisfying the equivalent conditions,  $W$  in (3) is uniquely determined by  $Q$  as

$$W = \bigcup_{e \geq 0} F^{-e}(Q_e),$$

and the radical in  $S$  of the  $S$ -ideal  $SQ$  generated by  $Q$  is the smallest homogeneous prime ideal  $\mathfrak{p}$  satisfying the property of (1).

We have  $\text{exponent}(Q) \leq e$  if and only if the corresponding  $W$  is defined over  $F^{-e}(k)$ , i.e., generated over  $F^{-\infty}(k)$  by  $W \cap (F^{-e}(k) \otimes_k L_0)$ .

*Proof.* The equivalence (1) $\Leftrightarrow$ (2) and next to the last statement were already proved in [ $O_1$ , Lemma 2.3]. Given a graded  $k[F]$ -submodule  $Q$ , it is easy to see that  $F^{-e}(Q_e)$  is an increasing sequence whose union  $W$  is an  $F^{-\infty}(k)$ -subspace of  $F^{-\infty}(k) \otimes_k L_0$ . Moreover,  $W \cap (F^{-e}(k) \otimes_k L_0)$  consists of  $z$  in  $F^{-i}(Q_i)$ , for some  $i$ , such that  $F^e(z) \in L_e$ . Thus  $F^{e+i}(z)$  is in  $F^e(Q_i) \subset Q_{e+i}$ , and  $F^e(z)$  is in  $\text{rad}_L(Q)_e$ . q. e. d.

**Definition.** For a  $k$ -vector space  $L_0$ , let  $\mathcal{D} = \text{Diff}(F^{-\infty}(k)/k)$  act on  $F^{-\infty}(k) \otimes_k L_0$  through the first factor  $F^{-\infty}(k)$ . Then for an  $F^{-\infty}(k)$ -subspace  $W$  of  $F^{-\infty}(k) \otimes_k L_0$ , we define  $F^{-\infty}(k)$ -subspaces  $\mathcal{D}'(W)$  and  $\mathcal{N}'(W)$  of  $F^{-\infty}(k) \otimes_k L_0$  by

$$\begin{aligned} \mathcal{D}'(W) &:= \{(D \otimes 1)w; D \in \mathcal{D}^{(1)}, w \in W\}, \\ \mathcal{N}'(W) &:= \{z \in F^{-\infty}(k) \otimes_k L_0; (D \otimes 1)z \in W \text{ for all } D \in \mathcal{D}^{(1)}\}, \end{aligned}$$

where  $\mathcal{D}^{(1)}$  is as in Section 1.

We then have the following, a part of which was announced in [ $O_2$ , Theorem] under different notations, and some of which have close connection with the formulation given by Russel [R].

**Theorem 2.2.** *Let  $L_0$  be a finite dimensional  $k$ -vector space. For an  $F^{-\infty}(k)$ -subspace  $V$  of  $F^{-\infty}(k) \otimes_k L_0$ , the following are equivalent:*

- (1)  $\mathcal{N}'(\mathcal{D}'(V)) = V$ .
- (2) *There exists a unique  $F^{-\infty}(k)$ -subspace  $U$  of  $F^{-\infty}(k) \otimes_k L_0$  satisfying  $\mathcal{D}'(\mathcal{N}'(U)) = U$  such that  $V = \mathcal{N}'(U)$ .*

(2') There exists an  $F^{-\infty}(k)$ -subspace  $U$  of  $F^{-\infty}(k) \otimes_k L_0$  such that  $V = \mathcal{N}'(U)$ .

(3) For the dual  $k$ -vector space  $L_0^*$  of  $L_0$ , there exists an  $F^{-\infty}(k)$ -subspace  $V'$  of  $F^{-\infty}(k) \otimes_k L_0^*$  such that  $V = (\mathcal{D}'(V'))^\perp$ , the perpendicular with respect to the canonical pairing  $(F^{-\infty}(k) \otimes_k L_0) \times (F^{-\infty}(k) \otimes_k L_0^*) \rightarrow F^{-\infty}(k)$  induced by the dual pairing for  $L_0$  and  $L_0^*$ .

(3') For the dual  $k$ -vector space  $L_0^*$  of  $L_0$ , there exists an  $F^{-\infty}(k)$ -subspace  $V'$  of  $F^{-\infty}(k) \otimes_k L_0^*$  such that, with respect to the canonical pairing  $\langle \cdot, \cdot \rangle : (F^{-\infty}(k) \otimes_k L_0) \times (F^{-\infty}(k) \otimes_k L_0^*) \rightarrow F^{-\infty}(k) \otimes_k F^{-\infty}(k)$  induced by the dual pairing for  $L_0$  and  $L_0^*$ , we have

$$V = \{v \in F^{-\infty}(k) \otimes_k L_0; \langle v, v' \rangle \in \Delta^{(1)} \text{ for all } v' \in V'\}.$$

(4) There exists an  $F^{-\infty}(k)$ -subspace  $U$  of  $F^{-\infty}(k) \otimes_k L_0$  such that, via the map  $i : F^{-\infty}(k) \otimes_k L_0 \rightarrow F^{-\infty}(k) \otimes_k F^{-\infty}(k) \otimes_k L_0$  defined by  $i(\beta \otimes y) := \beta \otimes 1 \otimes y$  for  $\beta \in F^{-\infty}(k)$  and  $y \in L_0$ , we have

$$V = \{v \in F^{-\infty}(k) \otimes_k L_0; i(v) \in \Delta^{(1)} \otimes L_0 + F^{-\infty}(k) \otimes U\}.$$

(4') There exists a  $k$ -linear map  $\psi : L_0 \rightarrow E$  to an  $F^{-\infty}(k)$ -vector space  $E$  such that

$$V = (1 \otimes \psi)^{-1}(\Delta^{(1)} \cdot (F^{-\infty}(k) \otimes_k E)),$$

where  $1 \otimes \psi : F^{-\infty}(k) \otimes_k L_0 \rightarrow F^{-\infty}(k) \otimes_k E$  is the scalar extension and  $\Delta^{(1)} \cdot (F^{-\infty}(k) \otimes_k E)$  is the multiple by the ideal  $\Delta^{(1)}$  for the  $(F^{-\infty}(k) \otimes_k F^{-\infty}(k))$ -module structure of  $F^{-\infty}(k) \otimes_k E$ .

*Proof.* The equivalences (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (2') can be proved exactly as in [O<sub>1</sub>, Theorem 2.6 and Lemma 2.9].

(4) $\Leftrightarrow$ (4') is obvious, if we let  $E = (F^{-\infty}(k) \otimes_k L_0)/U$ .

To deal with (2'), (3), (3'), (4) simultaneously, let  $U$  be an  $F^{-\infty}(k)$ -subspace in  $F^{-\infty}(k) \otimes_k L_0$  and let  $V' = U^\perp$  in  $F^{-\infty}(k) \otimes_k L_0^*$  with respect to the pairing in (3). Fix a  $k$ -basis  $\{y_j\}$  of  $L_0$  and the dual basis  $\{y'_j\}$  of  $L_0^*$ . For  $v = \sum_j \beta_j \otimes y_j$  in  $F^{-\infty}(k) \otimes_k L_0$  and  $v' = \sum_j \beta'_j \otimes y'_j$  in  $F^{-\infty}(k) \otimes_k L_0^*$ , we see that  $[v, v'] := \sum_j \beta_j \beta'_j$  is the pairing in (3), while  $\langle v, v' \rangle = \sum_j \beta_j \otimes \beta'_j$  is the one in (3'). By the Taylor expansion in Section 1, we see that

$$\langle v, v' \rangle = \sum_\lambda (1 \otimes \sum_j (\partial_\lambda \beta_j) \beta'_j) (\delta a)^\lambda = \sum_\lambda (1 \otimes [(\partial_\lambda \otimes 1)v, v']) (\delta a)^\lambda.$$

Now,  $v$  is in  $\mathcal{N}'(U)$  if and only if  $(\partial_\lambda \otimes 1)v \in U$  for all  $\lambda \in \Lambda$  with  $|\lambda| < 1$ , i.e.,  $[(\partial_\lambda \otimes 1)v, v'] = 0$  for all  $v' \in V'$  and all  $\lambda \in \Lambda$  with  $|\lambda| < 1$ . Equivalently,



$\langle v, v' \rangle \in \Delta^{(1)}$  for all  $v' \in V'$ , and we get (2') $\Leftrightarrow$ (3').

Since  $\langle v, v' \rangle = \sum_{\lambda} (\sum_j \beta_j (\partial_{\lambda} \beta'_j) \otimes 1) (-\delta a)^{\lambda} = \sum_{\lambda} ([v, (\partial_{\lambda} \otimes 1)v'] \otimes 1) (-\delta a)^{\lambda}$  again by the Taylor expansion, we similarly get (3) $\Leftrightarrow$ (3').

We have  $i(v) = \sum_j \beta_j \otimes 1 \otimes y_j = \sum_{\lambda, j} (1 \otimes \partial_{\lambda} \beta_j \otimes 1) ((\delta a)^{\lambda} \otimes y_j)$ . Since  $\{(\delta a)^{\lambda} \otimes y_j\}_{\lambda, j}$  form a  $(1 \otimes F^{-\infty}(k) \otimes 1)$ -linear basis of  $F^{-\infty}(k) \otimes_k F^{-\infty}(k) \otimes_k L_0$ , we see that  $i(v)$  is in  $\Delta^{(1)} \otimes L_0 + F^{-\infty}(k) \otimes U$  if and only if  $0 = \sum_{|\lambda| < 1} (\delta a)^{\lambda} \sum_j (1 \otimes \beta'_j \partial_{\lambda} \beta_j) = \sum_{|\lambda| < 1} (\delta a)^{\lambda} (1 \otimes [(\partial_{\lambda} \otimes 1)v, v'])$  for all  $v' \in V'$ , i.e.,  $\langle v, v' \rangle \in \Delta^{(1)}$  for all  $v' \in V'$ . We thus get (3') $\Leftrightarrow$ (4).

**Corollary 2.3.** *Let  $S$  be a polynomial ring over  $k$  and let  $L_0$  be the  $k$ -subspace of the linear forms in  $S$ . The Hironaka subgroup schemes  $B$  in  $\text{Spec}(S)$  are in one-to-one correspondence with the proper  $F^{-\infty}(k)$ -subspaces  $V$  of  $F^{-\infty}(k) \otimes_k L_0$  satisfying the equivalent conditions (1) through (4') of Theorem 2.2. The correspondence is given as follows:*

$$L^B = \bigoplus_{e \geq 0} F^e(V \cap (F^{-e}(k) \otimes_k L_0)), \quad V = \bigcup_{e \geq 0} F^{-e}(L_e^B), \quad B = \text{Spec}(S/SL^B),$$

where  $SL^B$  is the  $S$ -ideal generated by  $L^B$ .

Moreover,  $\text{exponent}(B) \leq e$  if and only if the corresponding  $V$  is defined over  $F^{-e}(k)$ . The dimension of  $B$  equals the codimension of  $V$  in  $F^{-\infty}(k) \otimes_k L_0$ .

**Correction.** In [O<sub>2</sub>, Corollary 1], we erroneously took the radical in  $S$  of the correct ideal  $SL^B$ .

*Proof.* The Hironaka subgroup schemes  $B$  are in one-to-one correspondence with the graded  $k[F]$ -submodules  $L^B$  of  $L$  such that  $L_e^B = \{h \in L_e; \text{Diff}_{p^{e-1}}(k/F^e(k))h \subset \mathfrak{p} \cap L_e\}$  for all  $e$ , for a homogeneous prime ideal  $\mathfrak{p} \neq S_+$  of  $S$ , as we recalled at the beginning of this section. Then  $Q := \mathfrak{p} \cap L$  satisfies  $\text{rad}_L(Q) = Q$ , hence let  $U := \bigcup_{e \geq 0} F^{-e}(Q_e)$  as in Lemma 2.1.  $L^B$  also satisfies  $\text{rad}_L(L^B) = L^B$  by [O<sub>1</sub>, Proposition 2.12, (4)]. Hence let  $V := \bigcup_{e \geq 0} F^{-e}(L_e^B)$  again as in Lemma 2.1. The isomorphism  $F^e: F^{-e}(k) \xrightarrow{\sim} k$  induces one  $\text{Diff}(k/F^e(k)) \xrightarrow{\sim} \text{Diff}(F^{-e}(k)/k)$  sending  $D$  to  $F^{-e} \circ D \circ F^e$ . Since we have a surjective restriction map  $\mathcal{D}^{(1)} \rightarrow F^{-\infty}(k) \otimes_{F^{-e}(k)} \text{Diff}_{p^{e-1}}(F^{-e}(k)/k)$  as we saw in Section 1, we easily get  $V = \mathcal{N}'(U)$ . The rest is obvious. q. e. d.

### §3. A Versal Family of Hironaka Subgroup Schemes

In this section, we use the characterizations in the previous section to construct a versal family of Hironaka subgroup schemes, as we announced in [O<sub>2</sub>]

under different notations. Using the versal family, not only can we derive some of the results in [O<sub>1</sub>] and [M] in a more transparent manner, but also get consequences in the next section which turn out to be useful in resolution of singularities, as we see in Section 4 and in [O<sub>3</sub>], [O<sub>4</sub>].

Fix, once for all, a countably infinite dimensional  $k$ -vector space  $E_0$  and let  $E := F^{-\infty}(k) \otimes_k E_0$ , a countably infinite dimensional  $F^{-\infty}(k)$ -vector space. An  $F^{-\infty}(k)$ -subspace  $E$  of  $E$  is said to be *defined over a subfield*  $k' \supset k$  of  $F^{-\infty}(k)$ , if  $E$  is generated over  $F^{-\infty}(k)$  by  $E \cap (k' \otimes_k E_0)$ . Similarly, a  $k$ -linear map  $\phi$  from a  $k$ -vector space  $L_0$  to  $E$  is said to be defined over  $k'$  if the image  $\phi(L_0)$  is contained in  $k' \otimes_k E_0$ .

Regard  $F^{-\infty}(k) \otimes_k E$  as an  $(F^{-\infty}(k) \otimes_k F^{-\infty}(k))$ -module and consider its  $(F^{-\infty}(k) \otimes 1)$ -subspaces

$$E^{(r)} := \Delta^{(r)} \cdot (F^{-\infty}(k) \otimes_k E)$$

$$E^{(r+0)} := \Delta^{(r+0)} \cdot (F^{-\infty}(k) \otimes_k E)$$

for each nonnegative rational number  $r$  with  $p$ -power denominator, where the right hand sides are the multiples by the ideals  $\Delta^{(r)}$  and  $\Delta^{(r+0)}$  of Section 1 for the  $(F^{-\infty}(k) \otimes_k F^{-\infty}(k))$ -module structure.

Consider the action of  $\mathcal{D} = \text{Diff}(F^{-\infty}(k)/k)$  on  $F^{-\infty}(k) \otimes_k E$  always through the first factor. Then by what we saw in Section 1, we have  $\mathcal{D}^{(s+0)} \cdot E^{(r)} \subset E^{(r-s)}$ ,  $\mathcal{D}^{(s+0)} \cdot E^{(r+0)} \subset E^{(r-s+0)}$  and  $\mathcal{D}^{(s)} \cdot E^{(r)} \subset E^{(r-s+0)}$  for nonnegative rational numbers  $r, s$  with  $p$ -power denominators, where we let  $E^{(r')} = F^{-\infty}(k) \otimes_k E$  if  $r' \leq 0$ .

**Definition.** For a  $k$ -vector space  $L_0$  and a  $k$ -linear map  $\phi: L_0 \rightarrow E$ , we denote

$$\Phi^{(r)}(L_0, \phi) := (1 \otimes \phi)^{-1}(E^{(r)})$$

$$\Phi^{(r+0)}(L_0, \phi) := (1 \otimes \phi)^{-1}(E^{(r+0)})$$

for each nonnegative rational number  $r$  with  $p$ -power denominator, where  $1 \otimes \phi: F^{-\infty}(k) \otimes_k L_0 \rightarrow F^{-\infty}(k) \otimes_k E$  is the scalar extension of  $\phi$ .

If we consider the action of  $\mathcal{D}$  on  $F^{-\infty}(k) \otimes_k L_0$  through the first factor, we then have  $\mathcal{D}^{(s+0)} \cdot \Phi^{(r)}(L_0, \phi) \subset \Phi^{(r-s)}(L_0, \phi)$ ,  $\mathcal{D}^{(s+0)} \cdot \Phi^{(r+0)}(L_0, \phi) \subset \Phi^{(r-s+0)}(L_0, \phi)$  and  $\mathcal{D}^{(s)} \cdot \Phi^{(r)}(L_0, \phi) \subset \Phi^{(r-s+0)}(L_0, \phi)$  for nonnegative rational numbers  $r, s$  with  $p$ -power denominators, where we let  $\Phi^{(r')}(L_0, \phi) = F^{-\infty}(k) \otimes_k L_0$  if  $r' \leq 0$ . We have

$$\bigcap_r \Phi^{(r)}(L_0, \phi) = F^{-\infty}(k) \otimes_k \ker(\phi).$$

If  $\phi$  is defined over  $F^{-e}(k)$ , i.e.,  $\phi(L_0) \subset F^{-e}(k) \otimes_k E_0$ , then  $\Phi^{(r)}(L_0, \phi) \neq \Phi^{(r+0)}(L_0, \phi)$  holds only if  $rp^e$  is an integer. If  $\phi$  is defined over a subfield  $k' \supset k$  of  $F^{-\infty}(k)$ , then so are  $\Phi^{(r)}(L_0, \phi)$ .

*Remark.* As a generalization of the proof of (2') $\Leftrightarrow$ (4') in Theorem 2.2, we can similarly show the following which will also be used in Section 4: For a nonzero  $k$ -linear map  $\phi: L_0 \rightarrow E$  from a finite dimensional  $k$ -vector space  $L_0$ , we have

$$\begin{aligned} \Phi^{(r)}(L_0, \phi) &= \{v \in F^{-\sigma}(k) \otimes_k L_0; \mathcal{D}^{(r)}v \subset \Phi^{(0+0)}(L_0, \phi)\} \\ \Phi^{(r+0)}(L_0, \phi) &= \{v \in F^{-\sigma}(k) \otimes_k L_0; \mathcal{D}^{(r+0)}v \subset \Phi^{(0+0)}(L_0, \phi)\} \end{aligned}$$

for each positive rational number  $r$  with  $p$ -power denominator, and

$$F^{-\infty}(k) \otimes_k \ker(\phi) = \{v \in F^{-\infty}(k) \otimes_k L_0; \mathcal{D}v \subset \Phi^{(0+0)}(L_0, \phi)\}.$$

With these preparations, we have the following:

**Theorem 3.1.** (*A versal family of Hironaka subgroup schemes*). Let  $S$  be a polynomial ring over  $k$  and let  $L_0$  be the  $k$ -subspace of the linear forms.

(i) We have a natural surjective map

$$\text{Proj}(S) \rightarrow \{\text{nonzero } k\text{-linear maps } \phi: L_0 \rightarrow E\} / \text{Aut}_{F^{-\infty}(k)}(E)$$

which sends a homogeneous prime ideal  $\mathfrak{p} \neq S_+$  to a nonzero  $k$ -linear map  $\phi: L_0 \rightarrow E$ , determined up to  $F^{-\infty}(k)$ -linear automorphisms of  $E$ , such that

$$\Phi^{(0+0)}(L_0, \phi) = \bigcup_{e \geq 0} F^{-e}(\mathfrak{p} \cap L_e).$$

(ii) Let  $\mathfrak{p}$  and  $\phi$  correspond to each other as in (i). Then the Hironaka subgroup scheme in  $\text{Spec}(S)$  associated to  $\mathfrak{p}$  is  $B(\mathfrak{p}) = \text{Spec}(S/SN)$ , where  $N$  is the graded  $k[F]$ -submodule of  $L$  determined by

$$N = \bigoplus_{e \geq 0} F^e(\Phi^{(1)}(L_0, \phi) \cap (F^{-e}(k) \otimes_k L_0)).$$

(iii)  $\text{exponent}(B(\mathfrak{p})) \leq e$  if and only if the corresponding  $\phi$  can be chosen to be defined over  $F^{-e}(k)$ . The dimension of  $B(\mathfrak{p})$  equals the codimension of  $\Phi^{(1)}(L_0, \phi)$  in  $F^{-\infty}(k) \otimes_k L_0$ .

*Proof.* For  $\mathfrak{p}$  in  $\text{Proj}(S)$ , let  $Q := \mathfrak{p} \cap L$ ,  $U := \bigcup_{e \geq 0} F^{-e}(Q_e)$  and  $V := \bigcup_{e \geq 0} F^{-e}(L_e^{\mathfrak{p}})$  as in the proof of Corollary 2.3. Hence  $V = \mathcal{N}'(U)$ . Let  $E := (F^{-\infty}(k) \otimes_k L_0) / U$  be the quotient  $F^{-\infty}(k)$ -vector space, and let  $\psi: L_0 \rightarrow E$  be the  $k$ -linear map sending  $y \in L_0$  to the image of  $1 \otimes y$  in  $E$ . Then for the scalar

extension  $1 \otimes \psi: F^{-\infty}(k) \otimes_k L_0 \rightarrow F^{-\infty}(k) \otimes_k E$ , we have  $U = (1 \otimes \psi)^{-1}(\Delta \cdot (F^{-\infty}(k) \otimes_k E))$ . By Theorem 2.2, we get  $V = \mathcal{N}'(U) = (1 \otimes \psi)^{-1}(\Delta^{(1)} \cdot (F^{-\infty}(k) \otimes_k E))$ .

$E$  can be embedded  $F^{-\infty}(k)$ -linearly into  $E$ , uniquely up to  $F^{-\infty}(k)$ -linear automorphisms of  $E$ , since  $E$  is finite dimensional, while  $E$  is countably infinite dimensional. Let  $\phi: L_0 \rightarrow E \hookrightarrow E$  be the composite of  $\psi$  with the embedding. We easily see that  $U = \Phi^{(0+0)}(L_0, \phi)$  and  $V = \Phi^{(1)}(L_0, \phi)$ . The rest of the proof is obvious.

*Remark.* (I) If we are interested only in the smallest ambient vector group schemes  $\text{Spec}(S)$  containing given Hironaka subgroup schemes, then we may obviously restrict our attention in Theorem 3.1 to injective  $k$ -linear maps  $\phi: L_0 \hookrightarrow E$ , i.e.,  $L_0$  as nonzero finite dimensional  $k$ -subspaces of  $E$ .

(II) Theorem 3.1 is sometimes convenient, as we see below. It is, however, inconvenient in dealing with different homogeneous prime ideals  $\mathfrak{p}$  giving rise to the same Hironaka subgroup scheme as well as in comparing different Hironaka subgroup schemes. Theorem 2.2, (2) shows, for instance, that there exists the smallest homogeneous prime ideal  $\mathfrak{p}^{(0)} \neq S_+$  which gives rise to a given Hironaka subgroup scheme  $B$ . Namely,  $\mathfrak{p}^{(0)}$  is the intersection with  $S$  of the ideal in  $F^{-\infty}(k) \otimes_k S$  generated by the linear forms in  $\mathcal{D}'(V)$ , where  $B = \text{Spec}(S/SN)$  and  $N = \bigoplus_{e \geq 0} F^e(V \cap (F^{-e}(k) \otimes_k L_0))$ .

(III) Hironaka [H] gave a very handy necessary condition which  $L^B$  for a Hironaka subgroup scheme  $B$  satisfies, i.e.,

$$(*) \quad F^j(L_i) \cap \text{Diff}_{p^j-1}(k/F^j(k))(L_{i+j})^B = F^j(L_i^B)$$

for all  $i, j \geq 0$  (see  $[O_1]$ ). [H],  $[O_1]$  and [M] then used (\*) to classify Hironaka subgroup schemes in low dimensions. In our present formulation, (\*) takes the following form: For a nonzero  $k$ -linear map  $\phi: L_0 \rightarrow E$ , we have

$$(**) \quad (F^{-e}(k) \otimes_k L_0) \cap \mathcal{D}^{(1/p^e)} \cdot \Phi^{(1)}(L_0, \phi) \subset \Phi^{(1)}(L_0, \phi)$$

for all  $e \geq 0$ . The proof of (\*\*) can be carried out easily as follows: We saw that  $\mathcal{D}^{(1/p^e)} \cdot \Phi^{(1)}(L_0, \phi) \subset \Phi^{(1-1/p^e+0)}(L_0, \phi)$ . Moreover,  $(F^{-e}(k) \otimes_k E) \cap E^{(1-1/p^e+0)} \subset E^{(1)}$ , since the left hand side has a  $(1 \otimes F^{-\infty}(k))$ -linear basis consisting of  $(\delta a)^\lambda (1 \otimes \varepsilon_j)$  for an  $F^{-\infty}(k)$ -linear basis  $\{\varepsilon_j\}$  of  $E$  and  $\lambda = (\lambda_\gamma)_{\gamma \in \Gamma} \in A$  with  $\lambda_\gamma p^e \in \mathbf{Z}$  and  $|\lambda| > 1 - 1/p^e$ , hence necessarily  $|\lambda| \geq 1$ .

The following will play an important role in proving Theorem 4.1 in the next section.

**Proposition 3.2.** *If a Hironaka subgroup scheme  $B$  of  $\text{Spec}(S)$  is not a*

vector subgroup scheme and if it arises from a nonzero  $k$ -linear map  $\phi: L_0 \rightarrow E$  as in Theorem 3.1, then  $\Phi^{(1)}(L_0, \phi)$  strictly contains  $\Phi^{(1+0)}(L_0, \phi)$ .

*Proof.* Since  $B$  is not a vector subgroup scheme, i.e.,  $\text{exponent}(B) \neq 0$ , we have  $\Phi^{(1)}(L_0, \phi) \not\cong F^{-\infty}(k) \otimes_k \ker(\phi)$ . Thus there exists  $v$  in  $\Phi^{(1)}(L_0, \phi)$  not in  $F^{-\infty}(k) \otimes_k \ker(\phi)$  such that its image  $z$  in  $F^{-\infty}(k) \otimes_k E$  is of the form

$$z = (1 \otimes \phi)(v) = \sum_{\lambda', j'} (c_{\lambda', j'} \otimes 1) (\delta a)^{\lambda'} (1 \otimes \varepsilon_{j'}),$$

where  $\{\varepsilon_{j'}\}$  is an  $F^{-\infty}(k)$ -linear basis of  $E$  and  $\lambda'$  runs through the elements of  $\Lambda$  with  $|\lambda'| \geq 1$ . Here  $c_{\lambda', j'}$  are elements of  $F^{-\infty}(k)$  not all zero by the choice of  $v$ . There exists  $j \geq 0$  and  $\lambda \in \Lambda$  with the smallest possible  $|\lambda| (\geq 1)$  such that  $c_{\lambda, j} \neq 0$ . We claim that there exists  $\mu \in \Lambda$  such that the generalized binomial coefficient  $\binom{\lambda}{\mu}$  does not vanish and that  $|\mu| = 1$ . Then it will follow that  $\lambda - \mu$  is in  $\Lambda$  and that  $(\partial_{\lambda - \mu} \otimes 1)z = (1 \otimes \phi)((\partial_{\lambda - \mu} \otimes 1)v)$  has the nonzero term  $(c_{\lambda, j} \otimes 1)(\partial_{\lambda - \mu} \otimes 1)((\delta a)^{\lambda} (1 \otimes \varepsilon_j)) = \binom{\lambda}{\mu} (c_{\lambda, j} \otimes 1) (\delta a)^{\mu} (1 \otimes \varepsilon_j)$ , hence it is in  $E^{(1)}$  but not in  $E^{(1+0)}$ . Thus  $(\partial_{\lambda - \mu} \otimes 1)v$  will be in  $\Phi^{(1)}(L_0, \phi)$  but not in  $\Phi^{(1+0)}(L_0, \phi)$ .

Let  $\lambda = (\lambda_\gamma)_{\gamma \in \Gamma}$  and consider the  $p$ -adic expansions

$$\lambda_\gamma = \sum_{i > 0} \lambda_\gamma(i) p^{-i}.$$

By what we saw in Section 1, the above claim amounts to choosing  $\mu = (\mu_\gamma)_{\gamma \in \Gamma}$  in  $\Lambda$  with the  $p$ -adic expansions

$$\mu_\gamma = \sum_{i > 0} \mu_\gamma(i) p^{-i}$$

such that  $0 \leq \mu_\gamma(i) \leq \lambda_\gamma(i)$  for all  $\gamma \in \Gamma$  and all  $i > 0$  and that  $|\mu| = 1$ . For each positive integer  $i$ , let

$$\lambda(i) := \sum_{\gamma \in \Gamma} \lambda_\gamma(i) p^{-i},$$

thus  $|\lambda| = \sum_{i > 0} \lambda(i)$ , which is not less than 1 by assumption. Hence there exists a positive integer  $i'$  such that  $\lambda(1) + \lambda(2) + \dots + \lambda(i' - 1) < 1$  but that  $\lambda(1) + \dots + \lambda(i') \geq 1$ . Then we can obviously choose  $\mu_\gamma(i)$  for  $\gamma \in \Gamma$  and  $i \leq i'$  in such a way that  $0 \leq \mu_\gamma(i) \leq \lambda_\gamma(i)$  for  $\gamma \in \Gamma$  and  $i \leq i'$  and that  $\sum_{\gamma \in \Gamma} \sum_{i \leq i'} \mu_\gamma(i) p^{-i} = 1$ . If we let  $\mu_\gamma(i) = 0$  for all  $\gamma \in \Gamma$  and all  $i > i'$ , then we are done.

*Remark.* The same proof applies to the following more general result: For a nonzero  $k$ -linear map  $\phi: L_0 \rightarrow E$  from a finite dimensional  $k$ -vector space  $L_0$ , let  $r$  be a positive integer such that  $\Phi^{(r)}(L_0, \phi) \not\cong F^{-\infty}(k) \otimes_k \ker(\phi)$ . Then

$$\Phi^{(r)}(L_0, \phi) \not\cong \Phi^{(r+0)}(L_0, \phi).$$

§4. The Basic Transformation Homomorphism

For a homogeneous prime ideal  $\mathfrak{p} \neq S_+$  of  $S$ , consider the localization  $R = S_{\mathfrak{p}}$ , its maximal ideal  $M = \mathfrak{p}S_{\mathfrak{p}}$  and the residue field  $K = R/M$ , which is the field of fractions of the domain  $S/\mathfrak{p}$ . Let  $B(\mathfrak{p})$  be the Hironaka subgroup scheme of  $\text{Spec}(S)$  associated to  $\mathfrak{p}$  and let  $S^{B(\mathfrak{p})}$  be the subring of the invariants in  $S$  with respect to the translation action of  $B(\mathfrak{p})$ . By the very definition of  $B(\mathfrak{p})$ , we see that a homogeneous element  $f \in S_{\nu}$  of degree  $\nu$  is in  $S_{\nu}^{B(\mathfrak{p})}$  if and only if  $f$ , regarded as an element of  $R$ , belongs to  $M^{\nu}$ . Moreover,  $S_{\nu} \cap M^{\nu+1} = \{0\}$  by the Jacobian criterion (cf. [O<sub>1</sub>, Proposition 2.2, (i)]). Thus sending  $f$  in  $S_{\nu}^{B(\mathfrak{p})}$  to its coset in  $M^{\nu}$  mod.  $M^{\nu+1}$ , we have

$$\rho : S^{B(\mathfrak{p})} \hookrightarrow \text{gr}_M(R) := \bigoplus_{\nu \geq 0} M^{\nu}/M^{\nu+1}$$

the basic transformation homomorphism, which is a degree-preserving injective ring homomorphism from the graded  $k$ -algebra to the graded  $K$ -algebra.

To study the effect of permissible blowing-ups on the Hironaka subgroup scheme and the ridge of a tangent cone (cf. [O<sub>3</sub>] and [O<sub>4</sub>]), we need to investigate the restriction of  $\rho$  to the graded  $k[F]$ -submodule  $L^{B(\mathfrak{p})}$  of the additive forms in  $S^{B(\mathfrak{p})}$ :

$$\rho : L^{B(\mathfrak{p})} = \bigoplus_{e \geq 0} L_e^{B(\mathfrak{p})} \hookrightarrow \bigoplus_{e \geq 0} \text{gr}_M^{p^e}(R).$$

As an important application of Proposition 3.2, we get the following, whose proof will be carried out in this section in several steps:

**Theorem 4.1.** *In the above notations, suppose the Hironaka subgroup scheme  $B(\mathfrak{p})$  is not a vector subgroup scheme. Then there exists an integer  $e \geq 1$  and an element  $h$  in  $L_e^{B(\mathfrak{p})}$  such that  $\rho(h)$  is not an additive form in the new polynomial ring  $\text{gr}_M(R)$  over  $K$ , i.e.,  $\rho(h)$  is not in  $KF^e(\text{gr}_M^1(R))$ .*

As before, we denote by  $F$  the  $p$ -th power Frobenius map and consider the obvious multiplication map

$$\theta_e : k \otimes_{F^e(k)} F^e(R) \longrightarrow kF^e(R) \subset R$$

for each nonnegative integer  $e$ . By the Jacobian criterion (cf. [O<sub>1</sub>, the proof of Proposition 2.2]), we see that

$$\begin{aligned} M^{p^e} &= \{z \in R; \text{Diff}_{p^e-1}(R/F^e(R))z \subset M\} \\ RF^e(M) + M^{1+p^e} &= \{z \in R; \text{Diff}_{p^e}(R/F^e(R))z \subset M\} \end{aligned}$$

$$RF^e(M) = \{z \in R; \text{Diff}(R/F^e(R))z \subset M\},$$

where  $\text{Diff}(R/F^e(R))$  (resp.  $\text{Diff}_{p^{e-1}}(R/F^e(R))$ , resp.  $\text{Diff}_{p^e}(R/F^e(R))$ ) is the set of the differential operators of  $R$  into itself over the subring  $F^e(R)$  (resp. those of order  $\leq p^e - 1$ , resp.  $\leq p^e$ ).

**Lemma 4.2.** *Let the set  $\text{Diff}(k/F^e(k))$  of differential operators of  $k$  into itself over  $F^e(k)$  act on  $k \otimes_{F^e(k)} F^e(R)$  through the first factor  $k$ . Then we have:*

$$\begin{aligned} \theta_e^{-1}(M) &= \text{the radical of the ideal } k \otimes_{F^e(k)} F^e(M) \\ \theta_e^{-1}(M^{p^e}) &= \{y \in k \otimes_{F^e(k)} F^e(R); \text{Diff}_{p^{e-1}}(k/F^e(k))y \subset \theta_e^{-1}(M)\}, \\ \theta_e^{-1}(RF^e(M) + M^{1+p^e}) &= \{y \in k \otimes_{F^e(k)} F^e(R); \text{Diff}_{p^e}(k/F^e(k))y \subset \theta_e^{-1}(M)\}, \\ \theta_e^{-1}(RF^e(M)) &= k \otimes_{F^e(k)} F^e(M) = \{y \in k \otimes_{F^e(k)} F^e(R); \text{Diff}(k/F^e(k))y \subset \theta_e^{-1}(M)\}. \end{aligned}$$

*Proof.* The case  $e=0$  being trivial, we may assume  $e \geq 1$ . The first assertion is obvious, since  $\theta_e(k \otimes_{F^e(k)} F^e(M)) \subset kF^e(M) \subset RF^e(M)$  and since  $M$  is the radical of the ideal  $RF^e(M)$  in  $R$ . Fix a  $p$ -basis of  $k$  over  $F(k)$ , and regard it also as a  $p$ -basis of  $kF^e(R)$  over  $F(k)F^e(R)$ . We can obviously extend it to a  $p$ -basis of  $R$  over  $F(R)$ . As in Section 1, differential operators of  $k$  (resp.  $R$ ) into itself over  $F^e(k)$  (resp.  $F^e(R)$ ) can be expressed as infinite  $k$ - (resp.  $R$ -) linear combinations of the Taylor coefficient operators with respect to a  $p$ -basis of  $k$  over  $F(k)$  (resp.  $R$  over  $F(R)$ ). Hence we have an order-preserving inclusion  $\text{Diff}(k/F^e(k)) \hookrightarrow \text{Diff}(R/F^e(R))$ . In an obvious sense,  $\theta_e$  is compatible with the action of  $\text{Diff}(k/F^e(k))$  on  $k \otimes_{F^e(k)} F^e(R)$  through the first factor and that of  $\text{Diff}(R/F^e(R))$  on  $R$ , with respect to the above inclusion. Hence we are done.

q. e. d.

The  $k$ -linear injections  $L_0 \hookrightarrow S \hookrightarrow R$  induce a  $k$ -linear map

$$\chi_e: L_e = k \otimes_{F^e(k)} F^e(L_0) \hookrightarrow k \otimes_{F^e(k)} F^e(R)$$

compatible with the  $\text{Diff}(k/F^e(k))$ -actions through the first factors  $k$ . The composite

$$L_e \xrightarrow{\chi_e} k \otimes_{F^e(k)} F^e(R) \xrightarrow{\theta_e} R$$

is the canonical inclusion  $L_e \subset S \subset R$ .

**Proposition 4.3.** *(The Jacobian criteria). In the above notations, we have:*

$$\begin{aligned} \mathfrak{p} \cap L_e &= L_e \cap M = \chi_e^{-1}(\theta_e^{-1}(M)), \\ L_e^{B(\mathfrak{p})} &= L_e \cap M^{p^e} = \{v \in L_e; \text{Diff}_{p^{e-1}}(k/F^e(k))v \subset \mathfrak{p} \cap L_e\}, \\ L_e^{B(\mathfrak{p})} \cap \rho^{-1}(KF^e(\text{gr}_M^1(R))) &= L_e \cap (RF^e(M) + M^{1+p^e}) \\ &= \{v \in L_e; \text{Diff}_{p^e}(k/F^e(k))v \subset \mathfrak{p} \cap L_e\}, \end{aligned}$$

$$kF^e(\mathfrak{p} \cap L_e) = L_e \cap RF^e(M) = \{v \in L_e; \text{Diff}(k/F^e(k))v \subset \mathfrak{p} \cap L_e\}.$$

*Proof.* The first assertion is obvious, since we have  $k$ -linear injections  $L_e/(\mathfrak{p} \cap L_e) \hookrightarrow (k \otimes_{F^e(k)} F^e(R))/\theta_e^{-1}(M) \simeq kF^e(K) \hookrightarrow K = R/M$ . The second assertion is the one already obtained in  $[O_1, \text{Proposition 2.2, (ii)}]$ , as we recalled in Section 2. The third and the fourth assertions follow from Lemma 4.2, since  $\chi_e$  is compatible with the  $\text{Diff}(k/F^e(k))$ -actions, since

$$KF^e(\text{gr}_M^1(R)) = (RF^e(M) + M^{1+p^e})/M^{1+p^e}$$

and since  $L_e \cap M^{1+p^e} = \{0\}$  by  $[O_1, \text{Proposition 2.2, (i)}]$ . q. e. d.

*Proof of Theorem 4.1.* The  $p^e$ -th power Frobenius map on  $F^{-\infty}(k) \otimes_k S$  induces an isomorphism

$$F^e: F^{-e}(k) \otimes_k L_0 \xrightarrow{\sim} L_e = k \otimes_{F^e(k)} F^e(L_0)$$

as we observed in Section 2. Let  $\phi: L_0 \rightarrow E$  be the nonzero  $k$ -linear map associated to  $\mathfrak{p}$  as in Theorem 3.1, which is determined uniquely up to  $F^{-\infty}(k)$ -linear automorphisms of  $E$ . Then by Theorem 3.1, we have

$$\begin{aligned} (F^{-e}(k) \otimes_k L_0) \cap \Phi^{(0+0)}(L_0, \phi) &= F^{-e}(\mathfrak{p} \cap L_e) \\ (F^{-e}(k) \otimes_k L_0) \cap \Phi^{(1)}(L_0, \phi) &= F^{-e}(L_e^{B(\mathfrak{p})}). \end{aligned}$$

As we pointed out immediately before Theorem 3.1, we can imitate the proof of  $(2') \Leftrightarrow (4')$  in Theorem 2.2 to show that

$$\Phi^{(1+0)}(L_0, \phi) = \{w \in F^{-\infty}(k) \otimes_k L_0; \mathcal{D}^{(1+0)} \cdot w \subset \Phi^{(0+0)}(L_0, \phi)\}.$$

As in Section 1, we have the  $F^{-\infty}(k)$ -linear surjective restriction map

$$\mathcal{D}^{(1+0)} \longrightarrow F^{-\infty}(k) \otimes_{F^{-e}(k)} \text{Diff}_{p^e}(F^{-e}(k)/k),$$

while the isomorphism  $F^e: F^{-e}(k) \simeq k$  induces one  $\text{Diff}(k/F^e(k)) \simeq \text{Diff}(F^{-e}(k)/k)$  as in the proof of Corollary 2.3. Thus by Proposition 4.3, we get

$$(F^{-e}(k) \otimes_k L_0) \cap \Phi^{(1+0)}(L_0, \phi) = F^{-e}(L_e^{B(\mathfrak{p})}) \cap \rho^{-1}(KF^e(\text{gr}_M^1(R))).$$

In view of Proposition 3.2 and Lemma 2.1, we are done.

*Remark.* The above proof of Theorem 4.1 naturally leads us to introduce the higher order Hironaka subgroup schemes  $B(\mathfrak{p}; r) \subset B(\mathfrak{p}; r+0)$  of  $\text{Spec}(S)$  defined over  $k$  for nonnegative rational numbers  $r$  with  $p$ -power denominators by  $\Phi^{(r)}(L_0, \phi) = \bigcup_{e \geq 0} F^{-e}(L_e^{B(\mathfrak{p}; r)})$  and  $\Phi^{(r+0)}(L_0, \phi) = \bigcup_{e \geq 0} F^{-e}(L_e^{B(\mathfrak{p}; r+0)})$ . We have  $B(\mathfrak{p}, 0) = \{0\}$  and  $B(\mathfrak{p}, 1) = B(\mathfrak{p})$ , the original Hironaka subgroup scheme. Their significance in resolution of singularities is investigated in  $[O_3], [O_4]$ .



## References

- [G] J. Giraud, Contact maximal en caractéristique positive, *Ann. Sci. Ecole Norm. Sup.*, (4) **8** (1975), 201–234.
- [H] H. Hironaka, Additive groups associated with points of a projective space, *Ann. of Math.*, **92** (1970), 327–334.
- [M] H. Mizutani, Hironaka's additive group schemes, *Nagoya Math. J.*, **52** (1973), 85–95.
- [O<sub>1</sub>] T. Oda, Hironaka's additive group scheme, in *Number Theory, Algebraic Geometry and Commutative Algebra in honor of Y. Akizuki* (Y. Kusunoki et al., eds.), Kinokuniya, Tokyo, 1973, 181–219.
- [O<sub>2</sub>] ———, A versal family of Hironaka's additive group schemes, *Proc. Japan Acad.*, **58** (A) (1982), 126–128.
- [O<sub>3</sub>] ———, Hironaka group schemes and resolution of singularities, to appear in *Proc. Japan-France Conference in Algebraic Geometry, Tokyo and Kyoto, 1982*, to be published in *Lecture Notes in Math.* **1016**, Springer-Verlag.
- [O<sub>4</sub>] ———, Hironaka subgroup schemes and permissible blowing-ups, to appear.
- [R] P. Russel, On Hironaka's additive groups associated with points in projective space, *Math. Ann.*, **224** (1976), 97–109.

