ABHYANKAR, S.
Math. Annalen 153, 81—96 (1964)

Uniformization in p-Cyclic Extensions of Algebraic Surfaces over Ground Fields of Characteristic p*

By

SHREERAM ABHYANKAR in Baltimore, Maryland/USA

§ 1. Introduction

In the paper "Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$", Annals of Math., vol. 63 (1956), which will be cited as U, we proved that any valuation of a two dimensional algebraic function field L over an algebraically closed ground field k of characteristic $p \neq 0$ can be uniformized (and hence L/k has a nonsingular projective model)[1]. The delicate part of this proof was Theorem 4 of U which asserted the following.

Theorem (1.1). *Let K be a two dimensional algebraic function field over an algebraically closed ground field k of characteristic $p \neq 0$, let K^* be a Galois extension of K of degree p, and let w be a rational nondiscrete valuation of K/k having only one extension w^* to K^*. Assume that w can be uniformized. Then w^* can be uniformized.*

The proof of (1.1) given in U was rather complicated. In the present paper (which is meant to replace §§ 7, 8, 9 of U) we give a simplified version of this proof[2]. As in U, the main part of the proof of (1.1) consists of reducing the multiplicity of a p-fold singularity; this part is formulated as Theorem (2.2) in § 2 and its proof is given in § 5. In § 3 we deduce (1.1) from (2.2). For the purpose of (1.1) we need to prove (2.2) only for rational nondiscrete valuations (which was the only case considered in U). Owing to the simplification in the proof we have been able to prove (2.2) for irrational valuations as well. We have included this because it might throw some light on the problem of "resolution of embedded surface". As in U, along with (2.2) we consider the "pure inseparable case"; this is stated as Theorem (2.1) in § 2 and its proof is given in § 4.

Given a local domain (R, M) and a valuation w of a field containing R, we say that w has center in R if $R_w \supset R$ and $M_w \cap R = M$ where R_w is the valuation ring of w and M_w is the maximal ideal in R_w.

* This work was supported by the National Science Foundation under NSF-G 25225.

[1] This was generalized to perfect k in the subsequent paper "On the field of definition of a nonsingular birational transform of an algebraic surface", Annals of Math., vol. 65 (1957), pp. 268—281. Erratum: on page 279 line 21 of this paper, replace "*any finite algebraic*" by "*any*".

[2] For corrections to § 1 to § 6 of U see Annals of Math., vol. 78 (1963) pp. 202—203. Although §§ 7, 8, 9 of U contain many misprints we need not give errata to them.

Let (R, M) be a local ring. For any $r \in R$ we set:

$$\operatorname{ord}_R r = \max q \quad \text{such that} \quad r \in M^q .$$

For any polynomial $f(Z) = \sum_i r_i Z^i$ in an indeterminate Z with coefficients r_i in R we set:

$$\operatorname{ord}_R f(Z) = \min_i \, (i + \operatorname{ord}_R r_i) .$$

Let R be an integral domain, let x and y be nonzero elements in R, and let $f(Z) \in R[Z]$ be monic of degree n in Z. An element $f'(Z) \in R[Z]$ is said to be an *$[R, x, y]$-translate* of $f(Z)$ if there exist elements r and t in R where t equals a unit in R times a monomial in (x, y), i.e., $t = \delta x^u y^v$ where u and v are nonnegative integers and δ is a unit in R, such that

$$f'(Z) = t^{-n} f(tZ + r) .$$

Note that $f'(Z)$ is then monic of degree n in Z.

Let p be a prime number. For an integer a we write $a \equiv 0(p)$ to mean a is divisible by p, and we write $a \not\equiv 0(p)$ to mean a is not divisible by p. For integers a and b we write $(a, b) \equiv 0(p)$ to mean $a \equiv 0(p)$ and $b \equiv 0(p)$, and we write $(a, b) \not\equiv 0(p)$ to mean either $a \not\equiv 0(p)$ or $b \not\equiv 0(p)$.

From § 7 of U we take over Lemmas 12, 13, 14 and Proposition 5. For convenience we restate the last proposition thus.

(1.2). *Let R be a two dimensional local integral domain such that the completion $\overline{R}$ of R is also an integral domain. Let K and $\overline{K}$ be the quotient fields of R and $\overline{R}$ respectively. Let w be a real nondiscrete valuation of K having center in R. Then w has a unique extension $\overline{w}$ to $\overline{K}$ having center in $\overline{R}$. Furthermore $\overline{w}$ has the same residue field and the same value group as w. In particular $\overline{w}$ is real.*

In Proposition 5 of U we have proved this under the assumption that R is algebraic (which is the only case needed for the proof of (1.1)). This assumption was used only in Lemma 14 of U which asserted that: if $\overline{v}$ is any nonreal valuation of $\overline{K}$ having center in $\overline{R}$ then $\overline{v}$ is discrete of rank two. By a result which we have proved elsewhere[3]) it follows that Lemma 14 of U holds without assuming R to be algebraic. From (1.2) we deduce

(1.3). *Let (R, M) be a two dimensional regular local ring with quotient field K. Let (x, y) be a basis of M and let w be a valuation of K having center in R. Assume that there exist elements $r_1, r_2, \ldots$ in R and positive integers $q(1), q(2), \ldots$ such that $w\left(y - \sum_{i=1}^{n} r_i x^i\right) > q(n)\, w(x)$ for every positive integer n and $q(n) \to \infty$ as $n \to \infty$. Then w is discrete (of rank one or two).*

Proof. Let $\overline{R}$ be the completion of R and let $\overline{K}$ be the quotient field of $\overline{R}$. Let

$$z = y - \sum_{i=1}^{\infty} r_i x^i, \quad z_n = y - \sum_{i=1}^{n} r_i x^i, \quad z_n' = \sum_{i=n+1}^{\infty} r_i x^i$$

[3]) See Theorem 1 on p. 330 of "On the valuations centered in a local domain", Am. J. Math., vol. 78 (1956).

where z and z'_n are regarded as elements in $\overline{R}$. Then $z \neq 0$ and $z = z_n - z'_n$ for every positive integer n. Suppose if possible that w is not discrete. Then w is real nondiscrete[3]) and hence by (1.2) w has a unique extension $\overline{w}$ to $\overline{K}$ having center in $\overline{R}$, and $\overline{w}$ has the same value group as w. By assumption $\overline{w}(z_n) > q(n)\,\overline{w}(x)$; also x^{n+1} divides z'_n in $\overline{R}$ and hence $\overline{w}(z'_n) \geqq \overline{w}(x^{n+1}) > n\,\overline{w}(x)$. Since $z = z_n - z'_n$ we get that $\overline{w}(z) > \min(n, q(n))\,\overline{w}(x)$ for every positive integer n. This is a contradiction because $\overline{w}$ is real and $\min(n, q(n)) \to \infty$ as $n \to \infty$.

§ 2. Quadratic transforms

Let (R, M) be a two dimensional regular local ring with quotient field K. Assume that K is of characteristic $p \neq 0$, R/M is algebraically closed, and R contains a subfield k which maps (isomorphically) onto R/M under the natural homomorphism of R onto R/M. Let w be a *real nondiscrete valuation* of K having center in R. It follows that the residue field of w coincides with the residue field of R, i.e., k maps (isomorphically) onto R_w/M_w under the natural homomorphism of R_w onto R_w/M_w[3]). Let (x, y) be a basis of M.

A basis (x_0, y_0) of M is said to be canonically obtained from (x, y) if $(x_0, y_0) = (x, y)$ or (y, x).

Let (R_1, M_1) be the immediate quadratic transform of R along w[4]). If $w(y) \geqq w(x)$ then let $x' = x$ and $y' = (y/x) - \alpha$ where α is the unique element in k such that $w(y') > 0$; if $w(x) \geqq w(y)$ then let $y'' = y$ and $x'' = (x/y) - \beta$ where β is the unique element in k such that $w(x'') > 0$. In the first case (x', y') s a basis of M_1 and in the second case (x'', y'') is a basis of M_1. A basis (x_1, y_1) of M_1 is said to be canonically obtained from (x, y) if $(x_1, y_1) = (x', y')$ or (y', x') in the first case and $(x_1, y_1) = (x'', y'')$ or (y'', x'') in the second case.

If $(R_0, M_0) = (R, M)$ and (R_i, M_i) is the immediate quadratic transform of (R_{i-1}, M_{i-1}) along w for $i = 1, \ldots, n$ then we say that (R_n, M_n) is the n^{th} quadratic transform of R along w. If $(x_0, y_0) = (x, y)$ or (y, x) and (x_i, y_i) is a basis of M_i which is canonically obtained from (x_{i-1}, y_{i-1}) for $i = 1, \ldots, n$ then we say that the basis (x_n, y_n) of M_n is canonically obtained from (x, y). Note that if $f_{-1}(Z)$ is a monic polynomial in Z with coefficients in R and $f_i(Z)$ is an $[R_i, x_i, y_i]$-translate of $f_{i-1}(Z)$ for $i = 0, 1, \ldots, n$ then $f_n(Z)$ is an $[R_n, x_n, y_n]$-translate of $f_{-1}(Z)$.

A local ring R^* is said to be a quadratic transform of R along w if R^* is an n^{th} quadratic transform of R along w for some nonnegative integer n.

Given a monic polynomial $f(Z)$ of degree p in Z with coefficients in R, we say that the system $\{f, R, x, y\}$ can be *resolved* (relative to w) if there exists a quadratic tranform (R^*, M^*) of R along w, a basis (x^*, y^*) of M^* which is canonically obtained from (x, y), and an $[R^*, x^*, y^*]$-translate $f^*(Z)$ of $f(Z)$ such that $0 < \operatorname{ord}_{R^*} f^*(Z) < p$. From the above observation about translates we get the following: Let (R^*, M^*) be a quadratic transform of R along w, let (x^*, y^*) be a basis of M^* which is canonically obtained from (x, y), and let $f^*(Z)$ be an $[R^*, x^*, y^*]$-translate of $f(Z)$; if the system $\{f^*, R^*, x^*, y^*\}$ can

[4]) For the definition and properties of quadratic transforms see § 2 of the paper cited in Footnote 3.

be resolved then the system $\{f, R, x, y\}$ can be resolved. This remark will tacitly be used in § 4 and § 5.

With this terminology, Theorems 5 und 6 of § 7 of U can be stated as follows.

Theorem (2.1). *Let $f(Z) = Z^p + F$ where $F \in R$ is such that the completion of R does not contain $F^{1/p}$. Then $\{f, R, x, y\}$ can be resolved.*

Theorem (2.2). *Let $f(Z) = Z^p + (x^u y^v)^{p-1}\delta Z + F$ where δ is a unit in R, u and v are nonnegative integers, and $F \in R$. Then $\{f, R, x, y\}$ can be resolved*[5]).

The following lemmas will be used in the proofs of the above theorems which will be given in § 4 and § 5 respectively.

(2.3). *Let R_1 be the immediate quadratic transform of R along w. If $w(y) \geqq w(x)$ and $F \in M^q$ then $F \in x^q R_1$.*

Proof. $F \in M^q$ implies that $F = \sum_{i+j=q} F_{ij} x^i y^j$ with $F_{ij} \in R$. Since $w(y) \geqq w(x)$ we have that $y/x \in R_1$. Hence $F = x^q F^*$ where $F^* = \sum F_{ij}(y/x)^j \in R_1$.

(2.4). *Suppose $w(y) \geqq w(x)$. Let $y_1 = (y/x) - \alpha_1$ with $\alpha_1 \in k$ such that $w(y_1) > 0$. Suppose $w(y_1) \geqq w(x)$. Let $y_2 = (y_1/x) - \alpha_2$ with $\alpha_2 \in k$ such that $w(y_2) > 0$. So on. This cannot happen indefinitely, i.e., for some n we must have $w(y_n) < w(x_n)$.*

Proof. Otherwise there would exist elements $\alpha_1, \alpha_2, \ldots$ in k such that $w\left(y - \sum_{i=1}^{n} \alpha_i x^i\right) > n\, w(x)$ for every positive integer n, and by (1.3) this would imply that w is discrete.

(2.5). *Let R_1 be the immediate quadratic transform of R along w. Assume that $w(y) \geqq w(x)$. Let $x_1 = x$ and $y_1 = (y/x) - \alpha$ with $\alpha \in k$ such that $w(y_1) > 0$. For $0 \neq F' \in R$ let q be the greatest integer such that $qp \leqq \operatorname{ord}_R F'$. Let $F_1 = x_1^{-qp} F' \in R_1$. Let*

$$F' = \sum F'(i,j)\, x^i y^j \quad \textit{and} \quad F_1 = \sum F_1(i,j)\, x_1^i y_1^j$$

be the expansions of F' and F_1 in the completions $k[[x, y]]$ and $k[[x_1, y_1]]$ of R and R_1 respectively (where $F'(i,j)$ and $F_1(i,j)$ are elements in k). Assume that there exist integers a, b such that: $F'(a,b) \neq 0$, and $F'(i,j) = 0$ for all $(i,j) \equiv 0(p)$ with $i + j \leqq a + b$. Then there exist integers a_1, b_1 such that: $a_1 < p$, $b_1 \leqq a + b$, $(a_1, b_1) \not\equiv 0(p)$, $F_1(a_1, b_1) \neq 0$, and $F_1(i,j) = 0$ for all $i < a_1$. If $F'(i,j) = 0$ for all $i < a$ then we can choose a_1, b_1 so that furthermore $b_1 \leqq b$.

Proof. Let $d = \operatorname{ord}_R F'$. Let $a_1 = d - qp$. Then $a_1 < p$. Since $F'(a,b) \neq 0$ we get $d \leqq a + b$. Let b_1 be the greatest integer such that $F'(d - b_1, b_1) \neq 0$. Then $b_1 \leqq d \leqq a + b$. Since $F'(i,j) = 0$ for all $(i,j) \equiv 0(p)$ with $i + j \leqq a + b$, we must have $(d - b_1, b_1) \not\equiv 0(p)$. Hence $(a_1, b_1) \not\equiv 0(p)$. If $F'(i,j) = 0$ for all $i < a$, then $a \leqq d - b_1$, i.e., $a + b_1 \leqq d$, and hence $a + b_1 \leqq a + b$, i.e., $b_1 \leqq b$. Let

$$F = F' - \sum_{i+j=d} F'(i,j)\, x^i y^j\,.$$

[5]) In Theorem 6 of U we proved (2.2) only when w is rational. This is the only case needed in the proof of (1.1).

Then

$$F_1 = x_1^{-qp} F' = x_1^{-qp} F + x_1^{a_1} \sum_{i+j=d} F'(i,j)\,(y_1+\alpha)^j\,.$$

Now $F \in M^{d+1}$ and hence by (2.3)

$$x_1^{-qp} F \in x_1^{a_1+1} R_1\,.$$

Therefore

$$\sum_{i \leqq a_1} F_1(i,j)\, x_1^i y_1^j = x_1^{a_1} \sum_{i+j=d} F'(i,j)\,(y_1+\alpha)^j\,.$$

Consequently $F_1(i,j) = 0$ for all $i < a_1$, and

$$F_1(a_1, b_1) = F'(d-b_1, b_1) \neq 0\,.$$

§ 3. Proof of Theorem (1.1)

Using (2.2) we shall now prove (1.1). By definition, w can be uniformized means there exists a projective model of K/k on which the center of w is at a simple point. Let R'' be the quotient ring of this point. Since K^* is a Galois extension of K of degree p, there exists a primitive element z' of K^* over K such that the minimal monic polynomial $f'(Z)$ of z' over K is of the form

$$f'(Z) = Z^p + G'^{\,p-1} Z + F'\,, \quad 0 \neq G' \in K, \quad F' \in K\,.$$

Upon multiplying z' by a suitable element in R'' we can arrange that G' and F' are in R''. By Proposition 3 of U, there exists a quadratic transform (R', M') of R'' along w and a basis (x', y') of M' such that G' equals a unit in R' times a monomial in (x', y')[6]. By (2.2) there exists a quadratic transform (R, M) of R' along w, a basis (x^*, y^*) of M which is canonically obtained from (x', y'), and elements r and t in R where t equals a unit in R times a monomial in (x^*, y^*), such that $0 < \operatorname{ord}_R f^*(Z) < p$ where $f^*(Z) = t^{-p} f'(tZ + r) \in R[Z]$. Let $z^* = (z' - r)/t$. Then z^* is a primitive element of K^* over K, $f^*(Z)$ is the minimal monic polynomial of z^* over K, and

$$f^*(Z) = Z^p + G^{p-1} Z + F^*$$

where $F^* \in R$, and G equals a unit in R times a monomial in (x^*, y^*). Since w^* is the only extension of w to K^*, there is only one local ring (R^*, M^*) in K^* lying above R. Let $(\overline{R}^*, \overline{M}^*)$ and $(\overline{R}, \overline{M})$ be the completions of R^* and R respectively and let E^* and E be the quotient fields of $\overline{R}^*$ and $\overline{R}$ respectively, where we are regarding E and K^* to be subfields of E^*. Since there is only one local ring in K^* lying above R, by Proposition 1 of U it follows that $f^*(Z)$ is irreducible in $\overline{R}[Z]$. If G were a unit in R then $f^*(Z)$ would factor modulo M into coprime factors and then by Hensel's lemma $f^*(Z)$ would factor in $\overline{R}[Z]$. Therefore G is a nonunit in R and hence $\operatorname{ord}_R(Z^p + G^{p-1}Z) \geqq p$. Let $n = \operatorname{ord}_R f^*(Z)$. Since $0 < n < p$, we must have $\operatorname{ord}_R F^* = n$. Let $A^*(X, Y)$ be the form of degree n in indeterminates X, Y with coefficients in k such that $F^* - A^*(x^*, y^*) \in M^{n+1}$. Take $\delta \in k$ such that $A^*(1, \delta) \neq 0$. Let $x = x^*$, $y = y^* - \delta x^*$, $A(X, Y) = A^*(X, Y + \delta X)$. Then (x, y) is a basis of M, $A(X, Y)$ is a form of degree n in X, Y with coefficients in k, $A(x, y) = A^*(x^*, y^*)$, and $A(X, 0) \neq 0$.

[6] Also see Theorem 2 of the paper cited in Footnote 3.

Now $\overline{R} = k[[x, y]]$ and $E = k((x, y))$. By a theorem of CHEVALLEY[7]), $k((x, y))$ and $k(x, y)^{1/p}$ are linearly disjoint over $k(x, y)$. Since K is a subfield of E, we get that K and $k(x, y)^{1/p}$ are linearly disjoint over $k(x, y)$, and hence K is separable over $k(x, y)$. Therefore K^* is separable over $k(x, y)$, i.e. (x, y) is a separating transcendence basis of K^*/k, and hence (dx, dy) is a K^*-basis of the vector space W of all simple differentials of K^*/k. In particular $dz^* = \alpha\, dx + \beta\, dy$ with α and β in K^*. Take $\gamma \in k$ such that $\alpha + \gamma \neq 0$. Let $z = z^* + \gamma x$. Then $dz = (\alpha + \gamma)\, dx + \beta\, dy$ and hence (dy, dz) is a K^*-basis of W. Therefore (y, z) is a separating transcendence basis of K^*/k. Also z is a primitive element of K^* over K. Let $f(Z) = f^*(Z - \gamma x)$. Then $f(Z)$ is the minimal monic polynomial of z over K and

$$f(Z) = Z^p + G^{p-1} Z + F$$

where $F - A(x, y) \in M^{n+1}$ and hence

$$\operatorname{ord}_R f(Z) = \operatorname{ord}_R F = n\,.$$

Since $A(X, 0) \neq 0$ and $f(z) = 0$ we get

$$x^n \in R^* \cap (y, z)\,\overline{R}^* = (y, z)\, R^*\,.$$

Now $(x, y)\, R^*$ is primary for M^* and hence (y, z) is primary for M^*.

Let (S, N) be the quotient ring of $k[y, z]$ with respect to the maximal ideal generated by y and z. Then S is the quotient ring of a simple point on a projective model of $k(y, z)/k$ and the restriction of w^* to $k(y, z)$ has center in S. Now NR^* is primary for M^* ad hence by ZARISKI's "Main Theorem" R^* is a local ring in K^* lying above S[8]). Consequently the completion $\overline{S} = k[[y, z]]$ of S can be regarded as a subring of $\overline{R}^*$. Let

$$G^{p-1} = \Sigma\, G(i, j)\, x^i y^j \quad \text{and} \quad F = \Sigma\, F(i, j)\, x^i y^j$$

be the respective expansions of G^{p-1} and F in $k[[x, y]]$ where $G(i, j)$ and $F(i, j)$ are elements in k. Let

$$B(X, Y, Z) = Z^p + (\Sigma G(i, j)\, X^i Y^j)\, Z + \Sigma F(i, j)\, X^i Y^j \in k[[X, Y, Z]]\,.$$

Then

$$B(X, 0, 0) - \lambda X^n \in X^{n+1}\, k[[X]] \quad \text{where} \quad 0 \neq \lambda \in k\,.$$

Therefore by the Weierstrass preparation theorem

$$B(X, Y, Z) = C(X, Y, Z)\, D(X, Y, Z)$$

where $C(X, Y, Z)$ and $D(X, Y, Z)$ are elements in $k[[X, Y, Z]]$ such that $C(X, Y, Z)$ is a monic polynomial of degree n in X with coefficients in $k[[Y, Z]]$ and $D(0, 0, 0) \neq 0$. Then

$$0 = f(z) = B(x, y, z) = C(x, y, z)\, D(x, y, z)$$

and $D(x, y, z)$ is a unit in $\overline{R}^*$. Therefore $C(x, y, z) = 0$. Consequently $[k((y, z))\,(x) : k((y, z))] \leqq n$. Let H be the integral closure of $k[[y, z]]$ in

[7]) See Proposition 1.5 in: C. CHEVALLEY, "Some properties of ideals in rings of power series", Trans. Am. Math. Soc., vol. 55 (1944), pp. 68—84.

[8]) See the proof of Proposition 1 of the paper cited in Footnote 1.

$k((y, z))(x)$. Then H is a complete local ring and it is a subspace of $\overline{R}^*$. Also $x \in H$ and $y \in H$. Therefore $\overline{R} = k[[x, y]] \subset H$ and $z \in H$. Consequently $k((x, y))(z) \subset k((y, z))(x)$. Now z is a primitive element of K^* over K and hence z is a primitive element of E^* over E by Proposition 1 of U. Therefore $k((x, y))(z) = E^*$ and hence $k((y, z))(x) = E^*$. Consequently $d(R^* : S) = [E^* : k((y, z))] \leqq n < p$. Therefore w^* can be uniformized by Corollary 2 on p. 510 of U[9]).

§ 4. Proof of Theorem (2.1)

Let

$$F = \Sigma F(i, j)\, x^i y^j, \quad F(i, j) \in k,$$

be the expansion of F in the completion $k[[x, y]]$ of R.

By assumption $F \notin k[[x^p, y^p]]$. Let d be the smallest integer such that $f(a, b) \neq 0$ for some $(a, b) \not\equiv 0(p)$ with $a + b = d$. Let q be the greatest integer such that $qp \leqq d$. Let

$$r = \sum_{i+j \leqq q} F(ip, jp)^{1/p} x^i y^j \in R\,,$$

let $F' = F - r^p$, and let $\Sigma F'(i, j)\, x^i y^j$ be the expansion of F' in $k[[x, y]]$. Then $F'(a, b) \neq 0$, $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq a + b$, and q is the greatest integer such that $qp \leqq \mathrm{ord}_R F'$. Relabel x and y so that $w(y) \geqq w(x)$. Let $x_1 = x$ and $y_1 = (y/x) - \alpha$ with $\alpha \in k$ such that $w(y_1) > 0$. Let R_1 be the immediate quadratic transform of R along w. Let $F_1 = x_1^{-qp} F'$ and let $\Sigma F_1(i,j)\, x_1^i y_1^j$ be the expansion of F_1 in $k[[x_1, y_1]]$. By (2.5) there exist integers a_1, b_1 such that: $a_1 < p$, $(a_1, b_1) \not\equiv 0(p)$, $F_1(a_1, b_1) \neq 0$, and $F_1(i, j) = 0$ for all $i < a_1$. Now

$$f_1(Z) = x_1^{-qp} f(x_1^q Z - r) = Z^p + F_1$$

is an $[R_1, x_1, y_1]$-translate of $f(Z)$ and hence it is enough to show that $\{f_1, R_1, x_1, y_1\}$ can be resolved. Upon replacing $\{f, R, x, y\}$ by $\{f_1, R_1, x_1, y_1\}$ it thus suffices to prove the following.

(4.1). *Assume that there exist integers a, b such that: $a < p$, $(a, b) \not\equiv 0(p)$, $F(a, b) \neq 0$, and $F(i, j) = 0$ for all $i < a$. Then $\{f, R, x, y\}$ can be resolved.*

Proof. Let q' be the greatest integer such that $q'p \leqq a + b$. Let

$$r = \sum_{i+j \leqq q'} F(ip, jp)^{1/p} x^i y^j \in R\,,$$

let $F' = F - r^p$, and let $\Sigma F'(i, j)\, x^i y^j$ be the expansion of F' in $k[[x, y]]$. Then $F'(a, b) = F(a, b) \neq 0$, $F'(i, j) = 0$ for all $i < a$, and $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq a + b$. Since $a + b \geqq 0$, we have $F'(0, 0) = 0$, i.e., $\mathrm{ord}_R F' > 0$.

We shall prove (4.1) by induction on b. If $b = 0$ then $0 < \mathrm{ord}_R F' \leqq a + b = a < p$ and we are done. Now let $b > 0$ and assume that (4.1) is true for all values of b smaller than the given one. Let R_1 be the immediate quadratic transform of R along w.

[9]) This is the only place in the proof of (1.1) where we are using the assumption that w is rational.

(I). *Suppose* $w(y) < w(x)$. Let $y_1 = y$ and $x_1 = x/y$. If $\operatorname{ord}_R F' < p$ then we are done. Now assume that $F' \in M^p$. Let

$$f_1(Z) = y_1^{-p} f(y_1 Z - r) = Z^p + F_1 .$$

Then $F_1 = y_1^{-p} F' \in R_1$. Let $\Sigma F_1(i,j)\, x_1^i y_1^j$ be the expansion of F_1 in $k[[x_1, y_1]]$. Let $b_1 = a + b - p$. Then $b_1 < b$ and $(a, b_1) \not\equiv 0(p)$. Computing in $k[[x_1, y_1]]$ we get

$$F_1 = y_1^{-p} \sum_{i+j\geqq p,\, i\geqq a} F'(i,j)\, x^i y^j = \sum_{i+j\geqq p,\, i\geqq a} F'(i,j)\, x_1^i y_1^{i+j-p} .$$

Therefore $F_1(a, b_1) = F'(a,b) \neq 0$, and $F_1(i,j) = 0$ for all $i < a$. Since $b_1 < b$, $\{f_1, R_1, x_1, y_1\}$ can be resolved by the induction hypothesis.

(II.) *Suppose* $w(y) \geqq w(x)$. Let $x_1 = x$ and $y_1 = (y/x) - \alpha$ with $\alpha \in k$ such that $w(y_1) > 0$. Let q be the greatest integer such that $qp \leqq \operatorname{ord}_R F'$. Let

$$f_1(Z) = x_1^{-qp} f(x_1^q Z - r) = Z^p + F_1$$

where $F_1 = x_1^{-qp} F' \in R_1$. Let $\Sigma F_1(i,j)\, x_1^i y_1^j$ be the expansion of F_1 in $k[[x_1, y_1]]$. By (2.5) there exist integers a_1, b_1 such that: $a_1 < p$, $b_1 \leqq b$, $(a_1, b_1) \not\equiv 0(p)$, $F_1(a_1, b_1) \neq 0$, and $F_1(i,j) = 0$ for all $i < a_1$. If $b_1 < b$ then $\{f_1, R_1, x_1, y_1\}$ can be resolved by the induction hypothesis. So now assume that $b_1 = b$.

If $w(y_1) < w(x_1)$ then $\{f_1, R_1, x_1, y_1\}$ can be resolved as in (I) with f_1, R_1, x_1, y_1, a_1 replacing f, R, x, y, a. If $w(y_1) \geqq w(x_1)$ then proceed as in (II) with f_1, R_1, x_1, y_1, a_1 replacing f, R, x, y, a. By (2.4) this cannot happen indefinitely.

§ 5. Proof of Theorem (2.2)

Recall that now

$$f(Z) = Z^p + (x^u y^v)^{p-1}\, \delta\, Z + F$$

where u and v are nonnegative integers, δ is a unit in R, and $F \in R$. Let

$$F = \Sigma F(i,j)\, x^i y^j, \quad F(i,j) \in k ,$$

be the expansion of F in the completion $k[[x, y]]$ of R. Consider the following conditions.

A_n'. There exist integers a, b such that: $a + b < np$, $F(a,b) \neq 0$, and $F(i,j) = 0$ for all $(i,j) \equiv 0(p)$ with $i + j \leqq a + b$.

B_n'. $\max(u, v) \leqq n$.

C_n'. $u > 0$ and there exist integers a, b such that: $a < p$, $b < np$, $(a, b) \not\equiv$ $\not\equiv 0(p)$, $F(a,b) \neq 0$, and $F(i,j) = 0$ for all $i < a$.

Let A_n (resp.: B_n, C_n) be the statement that $\{f, R, x, y\}$ can be resolved if condition A_n' (resp.: B_n', C_n') is satisfied. In (5.5, 5.6, 5.7) we shall respectively prove that for all $n \geqq 0$: $A_n \Rightarrow B_n$, $B_n \Rightarrow C_{n+1}$, $C_{n+1} \Rightarrow A_{n+1}$. Since A_0' is never satisfied, it would follow that B_n is true for all $n \geqq 0$. Then upon taking $n \geqq \max(u, v)$, by B_n it would follow that $\{f, R, x, y\}$ can always be resolved. The special considerations needed in the proof of (5.5) when w is irrational are made in (5.2′, 5.4′, 5.4″, 5.4‴); the proof of (2.2) when w is rational does not depend on (5.2′, 5.4′, 5.4″, 5.4‴).

In (5.1, 5.2, 5.2′, 5.3) we shall consider the existence of suitable $[R, x, y]$-translates of $f(Z)$, and there for any $G \in R$ by $G(i, j)$ we shall denote the coefficient of $x^i y^j$ in the expansion of G in $k[[x, y]]$.

(5.1). *Assume that* $u > 0$. *For* $r \in R$ *whose existence is asserted below let* $F' = f(r)$.

(5.1.1). *Given* n *there exists* $r \in R$ *such that*: $F'(0, j) = F(0, j)$ *for all* $j \not\equiv 0(p)$, *and* $F'(0, jp) = 0$ *for all* $j \leqq n$.

(5.1.2). *Given* n *there exists* $r \in R$ *such that*: $F'(i, j) = F(i, j)$ *for all* $i < p$, *and* $F'(ip, jp) = 0$ *whenever* $0 < i < u$ *and* $j \leqq n$.

(5.1.3). *There exists* $r \in R$ *such that*: $F'(i, j) = F(i, j)$ *for all* $i < p$, *and* $F'(ip, jp) = 0$ *whenever* $i + j < u + v$ *and* $i > 0$.

(5.1.4). *There exists* $r \in R$ *such that*: $F'(i, j) = F(i, j)$ *for all* $i < p$, *and* $F'(ip, jp) = 0$ *whenever* $i + j \leqq \max(u, v)$ *and* $i > 0$.

(5.1.5). *There exists* $r \in R$ *such that*: $F'(0, j) = F(0, j)$ *for all* $j \not\equiv 0(p)$, *and* $F'(ip, jp) = 0$ *whenever* $i + j \leqq \max(u, v)$.

Proof of (5.1.1). Take $r = -\sum_{j \leqq n} F(0, jp)^{i/p} y^j$.

Proof of (5.1.2). By induction on m $(0 \leqq m < u)$ we shall find $r_m \in R$ such that for $F_m = f(r_m)$ we have: $F_m(i, j) = F(i, j)$ for all $i < p$, and $F_m(ip, jp) = 0$ whenever $0 < i \leqq m$ and $j \leqq n$; it will then suffice to take $r = r_{u-1}$. For $m = 0$ take $r_0 = 0$. Let $m > 0$ and suppose we have found r_{m-1}. Take

$$r_m = r_{m-1} - \sum_{j \leqq n} F_{m-1}(mp, jp)^{1/p} x^m y^j \, .$$

Proof of (5.1.3). By induction on m $(0 \leqq m < u + v)$ we shall find $r_m \in R$ such that for $F_m = f(r_m)$ we have: $F_m(i, j) = F(i, j)$ for all $i < p$, and $F_m(ip, jp) = 0$ whenever $i + j \leqq m$ and $i > 0$; it will then suffice to take $r = r_{u+v-1}$. For $m = 0$ take $r_0 = 0$. Let $m > 0$ and suppose we have found r_{m-1}. Take

$$r_m = r_{m-1} - \sum_{i+j=m,\, i>0} F_{m-1}(ip, jp)^{1/p} x^i y^j \, .$$

Proof of (5.1.4). If $v \neq 0$ then $\max(u, v) < u + v$ and we can apply (5.1.3). Now suppose $v = 0$. Then $\max(u, v) = u$. Taking $n = u$ in (5.1.2) we find $s \in R$ such that for $F^* = f(s)$ we have: $F^*(i, j) = F(i, j)$ for all $i < p$, and $F^*(ip, jp) = 0$ whenever $0 < i < u$ and $j \leqq u$. Since k is algebraically closed, there exists $\alpha \in k$ such that: $\alpha^p + \delta\alpha + F^*(up, 0) \in M$. Take $r = s + \alpha x^u$.

Proof of (5.1.5). Taking $n = \max(u, v)$ in (5.1.1) we find $s \in R$ such that for $F^* = f(s)$ we have: $F^*(0, j) = F(0, j)$ for all $j \not\equiv 0(p)$, and $F^*(0, jp) = 0$ for all $j \leqq \max(u, v)$. Let $f^*(Z) = f(Z + s)$. Then

$$f^*(Z) = Z^p + (x^u y^v)^{p-1} \delta Z + F^* \, .$$

Hence by (5.1.4) there exists $t \in R$ such that for $F' = f^*(t)$ we have: $F'(i, j) = F^*(i, j)$ for all $i < p$, and $F'(ip, jp) = 0$ whenever $i + j \leqq \max(u, v)$ and $i > 0$. Take $r = s + t$ and note that $F' = f^*(t) = f(r)$.

(5.2). *Assume that* $u > 0$ *and there exist integers* a, b *such that*: $a < p$, $(a, b) \not\equiv 0(p)$, $F(a, b) \neq 0$, *and* $F(i, j) = 0$ *for all* $i < a$. *Then there exists* $r \in R$ *such* *that for $F' = f(r)$ we have: $F'(a, b) \neq 0$, $F'(i, j) = 0$ for all $i < a$, and $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq p \max(u, v)$.*

Proof. If $a \neq 0$ then apply (5.1.4), and if $a = 0$ then apply (5.1.5).

(5.2'). *Assume that* $\min(u, v) > 0$ *and there exist integers a, b such that: $a < p$, $b < 2p$, $(a, b) \not\equiv 0(p)$, $F(a, b) \neq 0$, and $F(i, j) = 0$ for all $i < a$. Then there exists $r \in R$ such that for $F' = f(r)$ we have: $F'(a, b) \neq 0$, $F'(i, j) = 0$ for all $i < a$, and $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq a + b$.*

Proof. By (5.2) there exists $s \in R$ such that for $F^* = f(s)$ we have: $F^*(a, b) \neq 0$, $F^*(i, j) = 0$ for all $i < a$, and $F^*(ip, jp) = 0$ whenever $i + j \leqq \max(u, v)$.

By assumption $a + b < 3p$; hence if $\max(u, v) \geqq 2$ then we may take $r = s$. Again by assumption $\max(u, v) \geqq 1$; also if $a = 0$ then $a + b < 2p$; hence if $a = 0$ then we may again take $r = s$.

We are now left with the case when $a \neq 0$ and $\max(u, v) = \min(u, v) = 1$, i.e., when $a > 0$ and $u = v = 1$. Let $f^*(Z) = f(Z + s)$. Then

$$f^*(Z) = Z^p + (xy)^{p-1}\delta Z + F^* .$$

Let $\bar{\delta}$ be the unique element in k such that $\delta - \bar{\delta} \in M$. Since k is algebraically closed, there exists $\alpha \in k$ such that

$$1^0). \qquad \alpha^p + \bar{\delta}\alpha + F^*(p, p) = 0.$$

Let $r = s + t$ where

$$2^0). \qquad t = \alpha xy - F^*(2p, 0)^{1/p} x^2 .$$

Then

$$3^0). \qquad F' = f(r) = f^*(t) = t^p + (xy)^{p-1}\delta t + F^* .$$

By 2^0) and 3^0) we get

$$F' \equiv F^* \bmod x^p R$$

i.e.,

$$F'(i, j) = F^*(i, j) \quad \text{for all} \quad i < p .$$

In particular $F'(a, b) = F^*(a, b) \neq 0$, and $F'(i, j) = F^*(i, j) = 0$ for all $i < a$. Since $a > 0$ we get that $F'(0, 0) = F'(0, p) = F'(0, 2p) = 0$. By 1^0), 2^0) and 3^0) we get

$$F' \equiv F^* - F^*(p, p)x^p y^p - F^*(2p, 0)x^{2p} - F^*(2p, 0)^{1/p}\bar{\delta} x^{p+1}y^{p-1} \bmod M^{2p+1}.$$

Therefore $F'(p, p) = F'(2p, 0) = 0$, and $F'(p, 0) = F^*(p, 0) = 0$. Thus $F'(ip, jp) = 0$ whenever $i + j \leqq 2p$. Since $a + b < 3p$, we conclude that $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq a + b$.

(5.3). *There exists $r \in R$ such that for $F' = f(r)$ we have: $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq p \max(u, v)$.*

Proof. If $\max(u, v) = 0$ then we can take $r \in k$ such that: $r^p + \delta r + F \in M$. If $\max(u, v) > 0$ then upon relabelling x and y we may assume that $u > 0$, and then we can apply (5.1.5).

(5.4). *If $u = v = 0$ then $\{f, R, x, y\}$ can be resolved.*

Proof. By (5.3), $f(Z)$ always has an $[R, x, y]$-translate

$$f'(Z) = Z^p + (x^u y^v)^{p-1}\delta Z + F' \quad \text{with} \quad F' \in M .$$

If $u = v = 0$ then $0 < \operatorname{ord}_R f'(Z) < p$ and hence $\{f, R, x, y\}$ can be resolved.

(5.4′). *Assume that $w(x)$ and $w(y)$ are rationally independent and $u + v = 1$. Then $\{f, R, x, y\}$ can be resolved.*

Proof. Upon relabelling x and y we may assume that

$$f(Z) = Z^p + y^{p-1}\delta Z + F .$$

By (5.3), $f(Z)$ has an $[R, x, y]$-translate

$$f'(Z) = Z^p + y^{p-1}\delta Z + F' \quad \text{with} \quad F' \in M .$$

Let R_1 be the immediate quadratic transform of R along w.

(I). *Suppose* $w(y) < w(x)$. Let $x_1 = y$, $y_1 = x/y$. If $F' \notin M^p$ then $0 < < \operatorname{ord}_R f'(Z) < p$ and we are done. Now assume that $F' \in M^p$. Let $f_1(Z) = x_1^{-p} f'(x_1 Z)$. Then

$$f_1(Z) = Z^p + \delta Z + F_1 \quad \text{with} \quad F_1 \in R_1 .$$

Now $\{f_1, R_1, x_1, y_1\}$ can be resolved by (5.4).

(II). *Suppose* $w(y) > w(x)$. Let $x_1 = x$, $y_1 = y/x$. Then $w(x_1)$ and $w(y_1)$ are rationally independent. If $F' \notin M^p$ then $0 < \operatorname{ord}_R f'(Z) < p$ and we are done. Now assume that $F' \in M^p$. Let $f_1(Z) = x_1^{-p} f'(x_1 Z)$. Then

$$f_1(Z) = Z^p + y_1^{p-1}\delta Z + F_1 \quad \text{with} \quad F_1 \in R_1 .$$

If $w(y_1) < w(x_1)$ then $\{f_1, R_1, x_1, y_1\}$ can be resolved as in (I). If $w(y_1) > w(x_1)$ then proceed as in (II). This cannot happen indefinitely; namely, (II) can recur at most d times where d is the greatest integer such that $d \leqq w(y)/w(x)$.

(5.4″). *Assume that $w(x)$ and $w(y)$ are rationally independent*, $\min(u, v) > 0$, *and there exist integers a, b such that: $a < p$, $b < 2p$, $(a, b) \not\equiv 0(p)$, $F(a, b) \neq 0$, and $F(i, j) = 0$ for all $i < a$. Then $\{f, R, x, y\}$ can be resolved.*

Proof. We shall prove this by induction on b. By (5.2′), $f(Z)$ has an $[R,x,y]$-translate

$$f'(Z) = Z^p + (x^u y^v)^{p-1}\delta Z + F'$$

such that for the expansion $\sum F'(i, j) x^i y^j$ of F' in $k[[x, y]]$ we have: $F'(a,b) \neq 0$, $F'(i, j) = 0$ for all $i < a$, and $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq a + b$. If $b = 0$ then $0 < \operatorname{ord}_R f'(Z) \leqq a + b < p$ and hence $\{f, R, x, y\}$ can be resolved. Now let $b > 0$ and assume that (5.4″) is true for all values of b smaller than the given one. Let R_1 be the immediate quadratic transform of R along w.

(I). *Suppose* $w(y) < w(x)$. Let $y_1 = y$, $x_1 = x/y$. Then $w(x_1)$ and $w(y_1)$ are rationally independent. If $F' \notin M^p$ then $0 < \operatorname{ord}_R f'(Z) < p$ and we are done. Now assume that $F' \in M^p$. Then $a + b \geqq p$. Let $b_1 = a + b - p$. Then $(a, b_1) \not\equiv \not\equiv 0(p)$ and $b_1 < b$. Let $f_1(Z) = y_1^{-p} f'(y_1 Z)$. Then

$$f_1(Z) = Z^p + (x_1^{u_1} y_1^{v_1})^{p-1}\delta Z + F_1 \quad \text{with} \quad F_1 \in R_1 ,$$

where $u_1 = u > 0$, $v_1 = u + v - 1 > 0$. Let $\sum F_1(i, j) x_1^i y_1^j$ be the expansion of F_1 in $k[[x_1, y_1]]$. Computing in $k[[x_1, y_1]]$ we get

$$F_1 = y_1^{-p} F' = \sum_{i+j \geqq p,\ i \geqq a} F'(i, j) x_1^i y_1^{i+j-p} .$$

Therefore $F_1(a, b_1) = F'(a, b) \neq 0$, and $F_1(i, j) = 0$ for all $i < a$. Since $b_1 < b$, $\{f_1, R_1, x_1, y_1\}$ can be resolved by the induction hypothesis.

(II). *Suppose* $w(y) > w(x)$. Let $x_1 = x$, $y_1 = y/x$. Then $w(x_1)$ and $w(y_1)$ are rationally independent. Let q be the greatest integer such that $qp \leqq \operatorname{ord}_R F'$. Then $q \leqq a + b < 3p$ and hence $q \leqq 2$. Let $f_1(Z) = x_1^{-qp} f'(x_1^q Z)$. Then

$$f_1(Z) = Z^p + (x_1^{u_1} y_1^{v_1})^{p-1} \delta Z + F_1$$

where $F_1 = x_1^{-qp} F' \in R_1$, $u_1 = u + v - q \geqq 0$, $v_1 = v > 0$. If $u_1 = 0$ then $v_1 = 1$ and hence $\{f_1, R_1, x_1, y_1\}$ can be resolved by (5.4′). Now assume that $u_1 > 0$, i.e., $\min(u_1, v_1) > 0$. Let $\sum F_1(i, j) x_1^i y_1^j$ be the expansion of F_1 in $k[[x_1, y_1]]$. By (2.5) there exist integers a_1, b_1 such that: $a_1 < p$, $b_1 \leqq b$, $(a_1, b_1) \not\equiv 0(p)$, $F_1(a_1, b_1) \neq 0$, and $F_1(i, j) = 0$ for all $i < a_1$. If $b_1 < b$ then $\{f_1, R_1, x_1, y_1\}$ can be resolved by the induction hypothesis. So now assume that $b_1 = b$.

If $w(y_1) < w(x_1)$ then $\{f_1, R_1, x_1, y_1\}$ can be resolved as in (I). If $w(y_1) > w(x_1)$ then proceed as in (II). This cannot happen indefinitely; namely, (II) can recur at most d times where d is the greatest integer such that $d \leqq w(y)/w(x)$.

(5.4‴). *Let* $n > 0$ *be given. Suppose that* A_n *is true and also suppose that:* (D) *if* $\min(u, v) < \max(u, v) = n$ *then* $\{f, R, x, y\}$ *can be resolved. Now assume that:* $w(x)$ *and* $w(y)$ *are rationally independent;* $u = v = n$; *and* $1 < w(y)/w(x) < 2$ *or* $1 < w(x)/w(y) < 2$. *Then* $\{f, R, x, y\}$ *can be resolved.*

Proof. Upon relabelling x and y we may assume that $1 < w(y)/w(x) < 2$. Let (R_i, M_i) be the i^{th} quadratic transform of R along w. Let $x_1 = x$, $y_1 = y/x$, $y_2 = y_1$, $x_2 = x_1/y_1$. Then (x_i, y_i) is a basis of M_i which is canonically obtained from (x, y) for $i = 1, 2$; also $w(x_2)$ and $w(y_2)$ are rationally independent.

By (5.3), $f(Z)$ has an $[R, x, y]$-translate

$$f^*(Z) = Z^p + (x^n y^n)^{p-1} \delta Z + F^* \quad \text{with} \quad F^* \in R\,,$$

such that for the expansion $\sum F^*(i, j) x^i y^j$ of F^* in $k[[x, y]]$ we have: $F^*(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq np$. For a moment suppose that $\operatorname{ord}_R F^* \geqq (n + 1)p$. Let $f'(Z) = x_1^{-(n+1)p} f^*(x_1^{n+1} Z)$. Then

$$f'(Z) = Z^p + (x_1^{u'} y_1^{v'})^{p-1} \delta Z + F' \quad \text{with} \quad F' \in R_1\,,$$

where $u' = n - 1 \geqq 0$ and $v' = n$. In particular $\min(u', v') < \max(u, v) = n$ and hence $\{f', R_1, x_1, y_1\}$ can be resolved by (D). Now assume that $\operatorname{ord}_R F^* < (n + 1)p$. Take integers a, b such that: $F^*(a, b) \neq 0$, and $F^*(i, j) = 0$ whenever $i + j < a + b$. By the previous conditions on $F^*(i, j)$ we then have: $a + b < (n + 1)p$, $(a, b) \not\equiv 0(p)$, and $F^*(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq a + b$. If $a + b < np$ then $\{f^*, R, x, y\}$ can be resolved by A_n. So also assume that $a + b \geqq np$, i.e., $\operatorname{ord}_R F^* \geqq np$. Let $f_1(Z) = x_1^{-np} f^*(x_1^n Z)$. Then

$$f_1(Z) = Z^p + (x_1^n y_1^n)^{p-1} \delta Z + F_1 \quad \text{with} \quad F_1 \in R_1\,.$$

Let $\sum F_1(i, j) x_1^i y_1^j$ be the expansion of F_1 in $k[[x_1, y_1]]$. Let $a_1 = a + b - np$, $b_1 = b$. Then $a_1 < p$, $b_1 = b \leqq a + b < (n + 1)p$, and $(a_1, b_1) \not\equiv 0(p)$. Computing in $k[[x_1, y_1]]$ we get

$$F_1 = x_1^{-np} F^* = \sum_{i + j \geqq np} F^*(i, j) x_1^{i+j-np} y_1^j\,.$$

Therefore $F_1(a_1, b_1) = F^*(a, b) \neq 0$, and $F_1(i, j) = 0$ for all $i < a_1$.

Since $n > 0$, by (5.2), $f(Z)$ has an $[R_1, x_1, y_1]$-translate

$$f_1^*(Z) = Z^p + (x_1^n y_1^n)^{p-1}\delta Z + F_1^*$$

such that for the expansion $\sum F_1^*(i,j)x_1^i y_1^j$ of F_1^* in $k[[x_1, y_1]]$ we have: $F_1^*(a_1, b_1) \neq 0$, $F_1^*(i,j) = 0$ for all $i < a_1$, and $F_1^*(i,j) = 0$ for all $(i,j) \equiv 0(p)$ with $i + j \leqq np$. For a moment suppose that $\operatorname{ord}_{R_1} F_1^* \geqq (n+1)p$. Let $f''(Z) = y_2^{-(n+1)p} f_1^*(y_2^{n+1}Z)$. Then

$$f''(Z) = Z^p + (x_2^{u''} y_2^{v''})^{p-1}\delta Z + F'' \quad \text{with} \quad F'' \in R_2,$$

where $u'' = n$ and $v'' = n - 1 \geqq 0$. In particular $\min(u'', v'') < \max(u'', v'') = n$ and hence $\{f'', R_2, x_2, y_2\}$ can be resolved by (D). Now assume that $\operatorname{ord}_{R_1} F_1^* < (n+1)p$. If $F_1^*(i,j) \neq 0$ for some i, j with $i + j < np$ then $\{f_1^*, R_1, x_1, y_1\}$ can be resolved by A_n. So also assume that $F_1^*(i,j) = 0$ whenever $i + j < np$, i.e., $\operatorname{ord}_{R_1} F_1^* \geqq np$. Then in particular $a_1 + b_1 \geqq np$. Let $f_2(Z) = y_2^{-np} f_1^*(y_2^n Z)$. Then

$$f_2(Z) = Z^p + (x_2^n y_2^n)^{p-1}\delta Z + F_2 \quad \text{with} \quad F_2 \in R_2.$$

Let $\sum F_2(i,j)x_2^i y_2^j$ be the expansion of F_2 in $k[[x_2, y_2]]$. Let $a_2 = a_1$, $b_2 = a_1 + b_1 - np$. Then $a_2 < p$, $b_2 < p + (n+1)p - np = 2p$, and $(a_2, b_2) \not\equiv 0(p)$. Computing in $k[[x_2, y_2]]$ we get

$$F_2 = y_2^{-np} F_1^* = \sum_{i+j \geqq np,\, i \geqq a_1} F_1^*(i,j) x_2^i y_2^{i+j-np}.$$

Therefore $F_2(a_2, b_2) = F_1^*(a_1, b_1) \neq 0$, and $F_2(i,j) = 0$ for all $i < a_2$. Consequently $\{f_2, R_2, x_2, y_2\}$ can be resolved by (5.4'').

(5.5). *For any* $n \geqq 0 : A_n \Rightarrow B_n$.

Proof. We make induction on n. B_0 is true by (5.4) and hence (5.5) is trivial for $n = 0$. Now let $n > 0$ and assume that $A_{n-1} \Rightarrow B_{n-1}$. Note that for all $m \leqq n : A'_m \Rightarrow A'_n$ and hence $A_n \Rightarrow A_m$. In particular, now $A_n \Rightarrow A_{n-1} \Rightarrow B_{n-1}$.

Thus we may assume that A_n and B_{n-1} are true. We are given that $\max(u, v) \leqq n$, $(n > 0)$. We want to prove that $\{f, R, x, y\}$ can be resolved.

Let (R_i, M_i) be the i^{th} quadratic transform of R along w. We define $x_0, y_0, x_1, y_1, \ldots$ as follows. Let $x_0 = x$, $y_0 = y$. Suppose we have defined $x_0, y_0, \ldots, x_i, y_i$, $(i \geqq 0)$. If $w(y_i) \geqq w(x_i)$ then let $x_{i+1} = x_i$, $y_{i+1} = (y_i/x_i) - \alpha_i$ with $\alpha_i \in k$ such that $w(y_i) > 0$; if $w(y_i) < w(x_i)$ then let $x_{i+1} = y_i$, $y_{i+1} = x_i/y_i$. Then (x_i, y_i) is a basis of M_i which is canonically obtained from (x, y) for all $i \geqq 0$. Next we define integers $u_0, v_0, u_1, v_1, \ldots$ by the following recurrence equations where we take $u_0 = u$, $v_0 = v$.

1⁰). $$u_{i+1} = u_i + v_i - n.$$

2⁰). $$v_{i+1} = \begin{cases} 0 & \text{if} \quad w(y_i) = w(x_i) \\ v_i & \text{if} \quad w(y_i) > w(x_i) \\ u_i & \text{if} \quad w(y_i) < w(x_i). \end{cases}$$

For a moment suppose that $\max(u_i, v_i) = n$ for all $i \geqq 0$. Then by 1⁰) and 2⁰) we get that $\min(u_i, v_i) \geqq 0$ for all $i \geqq 0$. Let if possible $j \geqq 0$ be such that $\min(u_j, v_j) < n$. Then $u_{j+1} < n$ by 1⁰); hence $v_{j+1} = n$ because $\max(u_{j+1},$

$v_{j+1}) = n$. Thus $\min(u_j, v_j) < n$ implies that $u_{j+1} = \min(u_{j+1}, v_{j+1}) < n = v_{j+1}$, and this in turn implies that $u_{j+2} = \min(u_{j+2}, v_{j+2}) < n = v_{j+2}$, and so on. In other words we now have $u_e < v_e = n$ for all $e > j$. Consequently by 2⁰), $w(y_e) > w(x_e)$ for all $e > j$. Whence from the definition of x_{i+1}, y_{i+1} we get that for all $e > j: w(y_e) > w(x_e)$, $x_{e+1} = x_e$, $y_{e+1} = y_e/x_e$. By (2.4) this contradicts the fact that w is real nondiscrete[10]). Thus we have proved

(I). If $\max(u_i, v_i) = n$ for all $i \geqq 0$ then $u_i = v_i = n$ for all $i \geqq 0$.

If $w(x_i)$ and $w(y_i)$ are rationally dependent for some $i \geqq 0$, then for some $j \geqq i$ we must have $w(y_j) = w(x_j)$ and hence $v_{j+1} = 0$ by 2⁰). Therefore by (I) we get

(II). If $\max(u_i, v_i) = n$ for all $i \geqq 0$ then $w(x_i)$ and $w(y_i)$ are rationally independent for all $i \geqq 0$.

Having made these two observations we proceed to prove that $\{f, R, x, y\}$ can be resolved.

If $\max(u, v) < n$ then we are done by B_{n-1}. Now assume that $\max(u,v) = n$. By (5.3), $f(Z)$ has an $[R, x, y]$-translate

$$f'(Z) = Z^p + (x^u y^v)^{p-1}\delta Z + F'$$

such that for the expansion $\sum F'(i,j)x^i y^j$ of F' in $k[[x, y]]$ we have: $F'(i,j) = 0$ for all $(i,j) \equiv 0(p)$ with $i + j \leqq np$. If $F'(a, b) \neq 0$ for some a, b with $a + b < np$ then $\{f', R, x, y\}$ can be resolved by A_n. Now assume that $F'(a, b) = 0$ whenever $a + b < np$, i.e., $\operatorname{ord}_R F' \geqq np$. Let $f_1(Z) = x_1^{-np} f'(x_1^n Z)$. Then

$$f_1(Z) = Z^p + (x_1^{u_1} y_1^{v_1})^{p-1}\delta_1 Z + F_1$$

where $F_1 \in R_1$, δ_1 is a unit in R_1, $\max(u_1, v_1) \leqq n$, and $\min(u_1, v_1) \geqq 0$. If $\max(u_1, v_1) < n$ then we are done by B_{n-1}. Now suppose that $\max(u_1, v_1) = n$. Thus either $\{f, R, x, y\}$ can be resolved, or $f(Z)$ has an $[R_1, x_1, y_1]$-translate

$$f_1(Z) = Z^p + (x_1^{u_1} y_1^{v_1})^{p-1}\delta_1 Z + F_1$$

where $F_1 \in R_1$, δ_1 is a unit in R_1, $\max(u_1, v_1) = n$, and $\min(u_1, v_1) \geqq 0$.

Upon replacing f, R, x, y by f_1, R_1, x_1, y_1 in the above argument we deduce that either $\{f_1, R_1, x_1, y_1\}$ can be resolved or $f_1(Z)$ has an $[R_2, x_2, y_2]$-translate

$$f_2(Z) = Z^p + (x_2^{u_2} y_2^{v_2})^{p-1}\delta_2 Z + F_2$$

where $F_2 \in R_2$, δ_2 is a unit in R_2, $\max(u_2, v_2) = n$, and $\min(u_2, v_2) \geqq 0$.

Repeating this procedure we conclude the following:

(III). Either $\{f, R, x, y\}$ can be resolved or for all $i \geqq 0$ we have: $\max(u_i, v_i) = n$, $\min(u_i, v_i) \geqq 0$, and $f(Z)$ has an $[R_i, x_i, y_i]$-translate

$$f_i(Z) = Z^p + (x_i^{u_i} y_i^{v_i})^{p-1}\delta_i Z + F_i$$

where $F_i \in R_i$ and δ_i is a unit in R_i.

In view of (I) and (II), by (III) we get (IV) and (V):

(IV). If $\min(u, v) < \max(u, v) = n$ then $\{f, R, x, y\}$ can be resolved[11]).

[10]) Actually it even contradicts the fact that w is real.

[11]) We are assuming A_n and B_{n-1}.

(V). Either $\{f, R, x, y\}$ can be resolved or 3^0): for all $i \geqq 0$ we have that $w(x_i)$ and $w(y_i)$ are rationally independent and $f(Z)$ has an $[R_i, x_i, y_i]$-translate

$$f_i(Z) = Z^p + (x_i^n y_i^n)^{p-1} \delta_i Z + F_i$$

where $F_i \in R_i$ and δ_i is a unit in R_i[12]).

We may now assume that 3^0) prevails. If $w(y) > w(x)$ then let d be the greatest integer such that $d + 1 \leqq w(y)/w(x)$, and if $w(y) < w(x)$ then let d be the greatest integer such that $d + 1 \leqq w(x)/w(y)$. Then $d \geqq 0$, and either $1 < w(y_d)/w(x_d) < 2$ or $1 < w(x_d)/w(y_d) < 2$. Therefore in view of (IV), $\{f_d, R_d, x_d, y_d\}$ can be resolved by (5.4‴).

(5.6). *For any* $n \geqq 0 : B_n \Rightarrow C_{n+1}$.

Proof. We are assuming B_n. We are given that C'_{n+1} is satisfied. By induction on b we shall show that $\{f, R, x, y\}$ can be resolved. By (5.2), $f(Z)$ has an $[R, x, y]$-translate

$$f'(Z) = Z^p + (x^u y^v)^{p-1} \delta Z + F'$$

such that for the expansion $\sum F'(i, j) x^i y^j$ of F' in $k[[x, y]]$ we have: $F'(a, b) \neq 0$, $F'(i, j) = 0$ for all $i < a$, and $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq p \max(u, v)$. If $b = 0$ then $0 < \operatorname{ord}_R f'(Z) \leqq a + b = a < p$ and hence $\{f, R, x, y\}$ can be resolved. Now let $b > 0$ and assume that $\{f, R, x, y\}$ can be resolved for all values of b smaller than the given one. Let R_1 be the immediate quadratic transform of R along w.

(I). *Suppose* $w(y) < w(x)$. Let $y_1 = y$ and $x_1 = x/y$. If $F' \notin M^p$ then $0 < \operatorname{ord}_R f'(Z) < p$ and we are done. Now assume that $F' \in M^p$. Then $a + b \geqq p$. Let $b_1 = a + b - p$. Then $b_1 < b$ and $(a, b_1) \not\equiv 0(p)$. Let $f_1(Z) = y_1^{-p} f'(y_1 Z)$. Then

$$f_1(Z) = Z^p + (x_1^u y_1^{u+v-1})^{p-1} \delta Z + F_1 \quad \text{with} \quad F_1 \in R_1 .$$

Let $\sum F_1(i, j) x_1^i y_1^j$ be the expansion of F_1 in $k[[x_1, y_1]]$. Computing in $k[[x_1, y_1]]$ we get

$$F_1 = y_1^{-p} F' = \sum_{i+j \geqq p,\, i \geqq a} F'(i, j) x_1^i y_1^{i+j-p} .$$

Therefore $F_1(a, b_1) = F'(a, b) \neq 0$, and $F_1(i, j) = 0$ for all $i < a$. Since $b_1 < b$, $\{f_1, R_1, x_1, y_1\}$ can be resolved by the induction hypothesis.

(II). *Suppose* $w(y) \geqq w(x)$. Let $x_1 = x$ and $y_1 = (y/x) - \alpha$ with $\alpha \in k$ such that $w(y_1) > 0$. Let q be the greatest integer such that $qp \leqq \operatorname{ord}_R F'$. Then $qp \leqq a + b < p + (n + 1)p = (n + 2)p$ and hence $q \leqq n + 1$. If $\max(u, v) \leqq n$ then we are done by B_n. So assume that $\max(u, v) \geqq n + 1$. Now $a + b < (n + 2)p$, and $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq (n + 1)p$. Therefore $F'(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq a + b$. Let $f_1(Z) = x_1^{-qp} f'(x_1^q Z)$. Then

$$f_1(Z) = Z^p + (x_1^{u_1} y_1^{v_1})^{p-1} \delta_1 Z + F_1$$

where $F_1 = x_1^{-qp} F' \in R_1$, δ_1 is a unit in R_1, $u_1 = u + v - q \geqq 0$, and $0 \leqq v_1 \leqq v$. Let $\sum F_1(i, j) x_1^i y_1^j$ be the expansion of F_1 in $k[[x_1, y_1]]$. By (2.5) there exist integers a_1, b_1 such that: $a_1 < p$, $b_1 \leqq b$, $(a_1, b_1) \not\equiv 0(p)$, $F_1(a_1, b_1) \neq 0$, and

[12]) **This completes the proof of (5.5) when w is rational.**

$F_1(i, j) = 0$ for all $i < a_1$. If $\max(u_1, v_1) \leqq n$ then $\{f_1, R_1, x_1, y_1\}$ can be resolved by B_n. So assume that $\max(u_1, v_1) \geqq n + 1$. If $v \leqq n$ then $v_1 \leqq v \leqq n$ and hence $u_1 \geqq n + 1 > 0$; if $v > n$ then $u_1 = u + v - q \geqq 1 + (n + 1) - (n + 1) = 1$. Thus in either case $u_1 > 0$. If $b_1 < b$ then $\{f_1, R_1, x_1, y_1\}$ can be resolved by the induction hypothesis. So now assume that $b_1 = b$.

If $w(y_1) < w(x_1)$ then $\{f_1, R_1, x_1, y_1\}$ can be resolved as in (I). If $w(y_1) \geqq w(x_1)$ then proceed as in (II). By (2.4) this cannot happen indefinitely.

(5.7). *For any* $n > 0 : C_n \Rightarrow A_n$.

Proof. We make induction on n. Since A_1 is obviously true, (5.7) is trivial for $n = 1$. Now let $n > 1$ and assume that $C_{n-1} \Rightarrow A_{n-1}$. For all $m \leqq n : C'_m \Rightarrow C'_n$ and hence $C_n \Rightarrow C_m$. In particular $C_n \Rightarrow C_{n-1}$. Also by (5.5), $A_{n-1} \Rightarrow B_{n-1}$.

Thus we may assume B_{n-1} and C_n, $(n > 1)$. We are given that A'_n is satisfied, i.e., there exist integers a, b such that: $a + b < np$, $F(a, b) \neq 0$, and $F(i, j) = 0$ for all $(i, j) \equiv 0(p)$ with $i + j \leqq a + b$. We want to show that $\{f, R, x, y\}$ can be resolved. Upon relabelling x and y, we may assume that $w(y) \geqq w(x)$. Let $x_1 = x$ and $y_1 = (y/x) - \alpha$ with $\alpha \in k$ such that $w(y_1) > 0$. Let R_1 be the immediate quadratic transform of R along w. If $\max(u, v) < n$ then we are done by B_{n-1}. Now assume that $\max(u, v) \geqq n$. Let q be the greatest integer such that $qp \leqq \operatorname{ord}_R F$. Then $qp \leqq a + b < np$ and hence $q \leqq n - 1$. Let $f_1(Z) = x_1^{-qp} f(x_1^q Z)$. Then

$$f_1(Z) = Z^p + (x_1^{u_1} y_1^{v_1})^{p-1} \delta_1 Z + F_1$$

where $F_1 = x_1^{-qp} F$, δ_1 is a unit in R_1, $u_1 = u + v - q \geqq \max(u, v) - (n - 1) \geqq n - (n - 1) = 1$, and $v_1 \geqq 0$. Let $\sum F_1(i, j) x_1^i y_1^j$ be the expansion of F_1 in $k[[x_1, y_1]]$. By (2.5) there exist integers a_1, b_1 such that: $a_1 < p$, $b_1 \leqq a + b < np$, $(a_1, b_1) \not\equiv 0(p)$, $F_1(a_1, b_1) \neq 0$, and $F_1(i, j) = 0$ for all $i < a_1$. Therefore $\{f_1, R_1, x_1, y_1\}$ can be resolved by C_n.

(Received December 31, 1962)