An algorithm on polynomials in one indeterminate with coefficients in a two dimensional regular local domain.

By SHREERAM SHANKAR ABHYANKAR (a Lafayette USA) (*)

In memory of Guido Castelnuovo in the recurrence of the first centenary of his birth.

Summary. - *See the first three paragraphs of the Introduction.*

§ 1. - Introduction.

We shall use the terminology of [10: § 1, 2.1, 2.2, and 3.1 to 3.5]. Also, for a nonzero polynomial $f(Z)=\sum_i f_i Z^i$ in an indeterminate Z with coefficients f_i in a regular local domain R we define: $\mathrm{ord}_R f(Z) = \min(i + \mathrm{ord}_R f_i)$ where the minimum is taken over all i for which $f_i \neq 0$.

Let R be a two dimensional regular local domain with maximal ideal M such that R/M is algebraically closed. In [10] we have given an algorithm dealing with a nonconstant monic polynomial $f(Z)$ in Z with coefficients in R when the degree of $f(Z)$ in Z is a power of the characteristic of R/M. In turn, using the results of [10], here we shall develop an algorithm dealing with an arbitrary nonconstant polynomial $f(Z)$ in Z with coefficients in R. The main result of this paper can be stated thus:

THEOREM 1.1 - *Let R be a two dimensional regular local domain with maximal ideal M such that R/M is algebraically closed. Let (x, y) be a basis of M and let J be a coefficient set for R. For every nonnegative integer i let (R_i, x_i, y_i) be a canonical i^{th} quadratic transform of (R, x, y, J) such that $R_i \subset R_{i+1}$ for all i. Let I be the set of all nonnegative integers i such that $x_{i+1} \neq x_i$, let I^* be the set of all nonnegative integers i such that $x_{i+2} \neq x_{i+1} = x_i$, and let I' be the set of all nonnegative integers i such that $x_{i+1} = x_i$ and $x_i/y_i \in R_{i+1}$. Assume that if I^* and I' are infinite sets and characteristic of $R/M = p \neq 0 =$ characteristic of R then R contains a primitive p^{th} root of 1 and a $(p-1)^{th}$ root of p. Let R_i^* be the completion of R_i. Let $f(Z)$ be a monic*

(*) This work was supported by the National Science Foundation under NSF-GP-4248-50-395 at Purdue University.

polynomial of degree $n > 0$ *in* Z *with coefficients in* R. *If* I *is a finite set then let* j *be any given nonnegative integer such that* $i \notin I$ *for all* $i \geq j$, *and for each* $i \geq j$ *let* r_{i+1} *be the unique element in* J *such that* $y_i = x_i(y_{i+1} + r_{i+1})$ *and let* $y_i^* = y_i - (r_{i+1}x_i + r_{i+2}x_i^2 + \ldots) \in R_i^*$; *and if* I *is an infinite set then let* j *be any given nonnegative integer and for each* $i \geq j$ *let* $y_i^* = y_i$. *Then there exists* $i \geq j$ *such that either*: Z^n *is an* R_k^**-translate of* $f(Z)$ *for all* $k \geq i$; *or*: *there exist nonnegative integers* d *and* e *and an* R_i^**-translate* $F(Z)$ *of* $f(Z)$ *such that upon letting* $g(Z) = F(x_i^d y_i^{*e} Z)/(x_i^d y_i^{*e})^n$ *we have that* $g(Z) \in R_i^*[Z]$, $0 < \operatorname{ord}_{R_i^*} g(Z) < n$, *and if* I *is an infinite set and* $e \neq 0$ *then* $M \subset y_i R_i$.

The significance of the conditions on I, I^*, and I' is explained by the following lemma.

LEMMA 1.2 - *Let* R *be a two dimensional regular local domain with maximal ideal* M. *Let* (x, y) *be a basis of* M *and let* J *be a coefficient set for* R. *Let* w *be a valuation of the quotient field of* R *such that* w *dominates* R *and* w *is residually algebraic over* R. *Let* R_i *be the* i^{th} *quadratic transform of* R *along* w *and let* (x_i, y_i) *be a basis of the maximal ideal* M_i *in* R_i *such that* $x_0 = x$ *and* $y_0 = y$, *and for all* $i \geq 0$ *we have that*: *if* $w(x_i) = w(y_i)$ *then* $x_{i+1} = x_i$ *and* $y_{i+1} - (y_i/x_i) \in R_i$; *if* $w(x_i) < w(y_i)$ *then* $x_{i+1} = x_i$ *and* $y_{i+1} = y_i/x_i$; *and if* $w(x_i) > w(y_i)$ *then* $x_{i+1} = x_i/y_i$ *and* $y_{i+1} = y_i$; (*note that these conditions are satisfied in case* R/M *is algebraically closed and* (R_i, x_i, y_i) *is the canonical* i^{th} *quadratic transform of* (R, x, y, J) *along* w *for all* $i \geq 0$). *Let* I *be the set of all nonnegative iutegers* i *such that* $x_{i+1} \neq x_i$, *let* I^* *be the set of all nonnegative integers* i *such that* $x_{i+2} \neq x_{i+1} = x_i$, *and let* I' *be the set of all nonnegative integers* i *such that* $x_{i+1} = x_i$ *and* $x_i/y_i \in R_{i+1}$. *Then we have the following*: (1) *If* I *is a finite set then* w *is either discrete or nonreal.* (2) *If* I *is a finite set then* I^* *is a finite set.* (3) *If* I *is an infinite set and* I^* *is a finite set then* w *is nonreal and* I' *is a finite set.* (4) I^* *is a finite set if and only if* w *is either discrete or nonreal.* (5) I' *is a finite set if and only if there exists a nonnegative integer* j *such that* $w(x_i) \neq w(y_i)$ *for all* $i \geq j$. (6) I' *is a finite set if and only if there exists a nonnegative integer* j *such that* $w(x_i)$ *and* $w(y_i)$ *are rationally independent for all* $i \geq j$. (7) *If* w *is irrational then there exists a nonnegative integer* j *such that* $(w(x_i), w(y_i))$ *is a free basis* (*as a module over the ring of integers*) *of the value group of* w *for all* $i \geq j$. (8) I^* *is an infinite set and* I' *is a finite set if and only if* w *is irrational.* (9) I^* *is an infinite set and* I' *is an infinite set if and only if* w *is rational nondiscrete.* (10) *If* I *is an infinite set and* I' *is a finite set then there exists a positive integer* j *such that* $M \subset y_i R_i$ *for all* $i \geq j$.

PROOF. - To prove (1) assume that I is a finite set; then there exists a nonnegative integer j such that for all $i \geq j$ we have that $x_{i+1} = x_i$ and hence $w(x_i) \leq w(y_i)$; now for each $i \geq 0$ we have that $\min(w(x_i), w(y_i)) \leq w(z)$

for all $z \in M_i$, and by [2: Lemma 12] we know that $\bigcup_{i=j}^{\infty} M_i = M_w$; therefore $0 < w(x_j) \leq w(z)$ for all $z \in M_w$ and hence w is either discrete or nonreal, (2) is obvious. If I is an infinite set and I^* is a finite set then there exists a nonnegative integer j such that $x_i \neq x_{i+1} = x_i/y_i$ and $y_{i+1} = y_i$ for all $i \geq j$, and hence w is nonreal and I' is a finite set; this proves (3). If I^* is a finite set then by (1) and (3) we get that w is either discrete or nonreal; conversely assume that w is either discrete or nonreal; then by [2: Theorem 1] there exists $0 \neq z' \in M_w$ such that $w(z') \leq w(z)$ for all $z \in M_w$; by [2: Lemma 12] we know that $\bigcup_{i=0}^{\infty} M_i = M_w$ and hence there exists a nonnegative integer j such that $z' \in M_i$ for all $i \geq j$; now for each $i \geq 0$ we have that $\min(w(x_i), w(y_i)) \leq w(z)$ for all $z \in M_i$, and hence $\min(w(x_i), w(y_i)) = w(z')$ for all $i \geq j$; consequently if $w(x_i) = w(z')$ for some $i \geq j$ then $x_{k+1} = x_k$ for all $k \geq i$ and hence I^* is a finite set; and if $w(x_i) \neq w(z')$ for all $i \geq j$ then $x_{i+1} \neq x_i$ for all $i \geq j$ and hence again I^* is a finite set; this proves (4). Clearly I' is the set of all nonnegative integers i such that $w(x_i) = w(y_i)$, and hence we get (5) and (6). (7) follows from [10: Lemma 3.11]. (8) follows from (4), (6), and (7). (9) follows from (4) and (8). To prove (10) assume that I is an infinite set and I' is a finite set; then there exists a positive integer j such that $x_j \neq x_{j-1}$ and $w(x_i) \neq w(y_i)$ for all $i \geq j$; it follows that $x_{j-1} \in y_i R_i$ and $y_{j-1} \in y_i R_i$ for all $i \geq j$, and hence $M \subset y_i R_i$ for all $i \geq j$.

Note that, using completions, a different proof of a special case of Lemma 1.2(1) was given in [1: page 513], [6: (1.3)], and [7: (1.3)]. In [2: Lemma 12] we have proved the following.

LEMMA 1.3 - *Let R be a two dimensional regular local domain with quotient field K. For each nonnegative integer i let R_i be a two dimensional regular local domain such that R_i is an i^{th} quadratic transform of R and $R_i \subset R_{i+1}$ for all $i \geq 0$. Then $\bigcup_{i=0}^{\infty} R_i$ is the valuation ring of a valuation w of K such that w dominates R_i and w is residually algebraic over R_i for all i. If w' is any valuation of K such that w' dominates R_i for all i then $\bigcup_{i=0}^{\infty} R_i = R_{w'}$.*

In view of the above two lemmas, Theorem 1.1 reduces to the following.

THEOREM 1.4 - *Let R be a two dimensional regular local domain with maximal ideal M such that R/M is algebraically closed. Let (x, y) be a basis of M, let J be a coefficient set for R, let w be a valuation of the quotient field of R such that w dominates R and w is residually algebraic over R, let (R_i, x_i, y_i) be the canonical i^{th} quadratic transform of (R, x, y, J) along w, and let R_i^* be the completion of R_i. Let $f(Z)$ be a monic polynomial of degree $n > 0$ in Z with coefficients in R. Then we have the following.*

(1) *Assume that* w *is rational nondiscrete. Also assume that if characteristic of* $R/M = p \neq 0 =$ *characteristic of* R *then* R *contains a primitive* p^{th} *root of* 1 *and a* $(p-1)^{th}$ *root of* p. *Then there exists a nonnegative integer* i *such that either*: Z^n *is an* R_k^**-translate of* $f(Z)$ *for all* $k \geq i$; *or*: *there exist nonnegative integers* d *and* e *and an* R_i^**-translate* $F(Z)$ *of* $f(Z)$ *such that upon letting* $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ *we have that* $M \subset \operatorname{rad}_{R_i} y_i^e R_i$, $g(Z) \in R_i^*[Z]$, *and* $0 < \operatorname{ord}_{R_i^*} g(Z) < n$.

(2) *Assume that* $w(x_i) \neq w(y_i)$ *for all* $i \geq 0$. *Then either*: Z^n *is an* R_k^**-translate of* $f(Z)$ *for all* $k \geq 0$; *or*: *there exist nonnegative integers* i, d, e *and an* R_i^**-translate* $F(Z)$ *of* $f(Z)$ *such that upon letting* $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ *we have that* $g(Z) \in R_i^*[Z]$ *and* $0 < \operatorname{ord}_{R_i^*} g(Z) < n$.

(3) *Assume that* $x_i = x$ *for all* $i \geq 0$. *For each* $i \geq 0$ *let* r_{i+1} *be the unique element in* J *such that* $y_i = x(y_{i+1} + r_{i+1})$. *Then either*: Z^n *is an* R_k^**-translate of* $f(Z)$ *for all* $k \geq 0$; *or*: *there exist nonnegative integers* i, d, e *and an* R_i^**-translate* $F(Z)$ *of* $f(Z)$ *such that upon letting* $y^* = y_i - (r_{i+1}x + r_{i+2}x^2 + \dots) \in R_i^*$ *and* $g(Z) = F(x^d y^{*e} Z)/(x^d z^{*e})^n$ *we have that* $g(Z) \in R_i^*[Z]$ *and* $0 < \operatorname{ord}_{R_i^*} g(Z) < n$.

In Theorem 2.10(1) of § 2 we shall prove Theorem 1.4(1), and in Theorem 3.8 of § 3 we shall prove Theorems 1.4(2) and 1.4(3). § 2 and § 3 are completely independent of each other. Except for a few definitions, § 3 does not depend on [10]. The proof of Theorems 1.4(2) and 1.4(3) given in § 3 is quite easy and, except for the fact that the use of derivatives is replaced by the use of the notion of nonsplitting polynomials, it is in the same general line of thought as [1: § 1] and Zariski's proof of uniformization of nonrational valuations in zero characteristic given in his papers [13], [14], [15]. On the other hand, in § 2 the results of [10] play a major role. The technique used in § 2 to deduce Theorem 1.4(1) from the results of [10] was inspired by Zariski's recent theory of equisingularity in zero characteristic (see [16], [17], [18], [19]); I had the good fortune of attending the course on that theory given by Zariski at Harvard in the fall of 1963; the considerations of § 2 may also throw some light on the yet undeveloped theory of equisingularity in nonzero characteristic. In the setup of Zariski's recent simple proof of resolution of singularities of embedded surfaces in zero characteristic outlined in [16], the case of a simple point of the discriminant locus is easier than the case of an ordinary double point of the discriminant locus; it can be seen that the case of a simple point of the discriminant locus essentially corresponds to the case of a rational valuation and the case of an ordinary double point of the discriminant locus essentially corresponds to the case of a nonrational valuation; so it is not surprising that if in § 2 we were to restrict our attention to zero characteristic then the resulting proof would be quite similar to ZARISKI'S treatment of the case of a simple point of the discriminant locus outlined in [16]; the difficulty in § 2 arises for nonzero characteristic and that is where the results of [10] come into play. Thus this paper is inspired by both the older (for nonrational valuations) and the newer (for rational valuations) work of ZARISKI on singularities.

I conclude this introduction by fondly expressing my perpetual gratitude to my guru Professor OSCAR ZARISKI. I do so by dedicating this paper to my paramguru (guru's guru) the late Professor GUIDO CASTELNUOVO on the occasion of the centenary of his birth.

§ 2. - Rational nondiscrete valuations.

DEFINITION 2.1 - Let $f(Z)$ be a monic polynomial of degree $n > 0$ in Z with coefficients in a field K. Take elements $z_1, \dots, z_n$ in an overfield of K such that $f(Z) = (Z - z_1) \dots (Z - z_n)$, and let $L = K(z_1, \dots, z_n)$. $f(Z)$ is said to be *separable* over K if L is separable over K; note that this condition depends only on $f(Z)$ and K and not on the elements $z_1, \dots, z_n$; also note that this condition is equivalent to saying that either K is of characteristic zero, or K is of characteristic $p \neq 0$ and $f'(Z) \notin K[Z^p]$ for every nonconstant monic irreducible factor $f'(Z)$ of $f(Z)$ in $K[Z]$. Let $y_1, \dots, y_m$ be the distinct elements amongst the elements $z_1, \dots, z_n$. We define

$$D_K(f(Z)) = \operatorname{Norm}_{L/K} \prod_{i \neq j} (y_i - y_j)$$

where the product is over $m(m-1)$ terms (by convention the product over an empty family is 1) and where for any $x \in L$, as usual, $\operatorname{Norm}_{L/K} x$ denotes the norm of x relative to the field extension L of K. Note that: (1) $0 \neq D_K(f(Z)) \in K$; (2) $D_K(f(Z)) = \prod_{i \neq j} (y_i - y_j)^d$ where $d = [L : K]$; (3) $D_K(f(Z))$ depends only on K and $f(Z)$ and not on $z_1, \dots, z_n$; and (4) if R is any normal domain with quotient field K such that $f(Z) \in R[Z]$ then $D_K(f(Z)) \in R$. Let $g(Z)$ be another monic polynomial of positive degree in Z with coefficients in K. We define

$$D(g(Z), f(Z)) = \prod_{i=1}^{n} g(z_i).$$

Note that: (5) $D(g(Z), f(Z)) \in K$; (6) $D(g(Z), f(Z))$ depends only on $g(Z)$ and $f(Z)$ and not on K and $z_1, \dots, z_n$; and (7) if R is any subring of K such that $g(Z) \in R[Z]$ and $f(Z) \in R[Z]$ then $D(g(Z)), f(Z)) \in R$.

LEMMA 2.2 - *Let R be a normal quasilocal domain with quotient field K, let $x \in R$ such that xR is a prime ideal in R and S is a one dimensional* *regular local domain where* $S = R_{xR}$, *let* L *be a finite normal extension of* K *such that integral closure* T *of* S *in* L *is quasilocal (by [20: § 7 and § 8 it follows that* T *is then a one dimensional regular local domain), let* $X \in L$ *such that* $X^q = x$ *where* q *is a positive integer, let* L' *be a subfield of* L *containing* K, *let* $d = [L' : K]$, *let* $z \in L'$ *such that* $z = sX^b + s'$ *where* b *is a nonnegative integer,* $s \in R$ *such that* $s \notin xR$, *and* $s' \in L$ *such that* s' *is integral over* R *and* $\operatorname{ord}_T s' > \operatorname{ord}_T X^b$, *and let* $y = \operatorname{Norm}_{L'/K} z$. *Then we have the following*: (1) $bd \equiv 0(q)$, $\operatorname{ord}_S y = bd/q$, $y/x^{bd/q} \in R$, *and* $y/x^{bd/q} \notin xR$. (2) s *is a unit in* R *if and only if* $y/x^{bd/q}$ *is a unit in* R. (3) y *is an* R*-monomial in* x *if and only if* s *is a unit in* R.

PROOF. - Clearly s is a unit in S and hence $\operatorname{ord}_T s = 0$; since $\operatorname{ord}_T s' > \operatorname{ord}_T X^b$ we get that $\operatorname{ord}_T z = \operatorname{ord}_T X^b$. Now $y = G_1(z) \dots G_d(z)$ where $G_1, \dots, G_d$ are K-automorphisms of L; for any K-automorphism G of L we clearly have $G(T) = T$ and hence $\operatorname{ord}_T G(u) = \operatorname{ord}_T u$ for all $u \in L$; in particular $\operatorname{ord}_T G_i(z) = \operatorname{ord}_T z$ for $1 \leq i \leq d$ and hence $\operatorname{ord}_T y = d \operatorname{ord}_T z = d \operatorname{ord}_T X^b = (bd/q) \operatorname{ord}_T x$; since x and y are in K we therefore get that $\operatorname{ord}_S y = (bd/q) \operatorname{ord}_S x$; since $\operatorname{ord}_S x = 1$ we conclude that $\operatorname{ord}_S y = bd/q$ and hence $bd \equiv 0(q)$. Now z is integral over R and $z \neq 0$, and hence $0 \neq y \in R$. Let a be the greatest integer such that $y/x^a \in R$; then $y/x^a \notin xR$ and hence y/x^a is a unit in S; consequently $\operatorname{ord}_S y = a$ and hence $a = bd/q$. Therefore $y/x^{bd/q} \in R$ and $y/x^{bd/q} \notin xR$. Since $\operatorname{ord}_S y = bd/q$ and $y/x^{bd/q} \in R$ it follows that y is an R-monomial in x if and only if $y/x^{bd/q}$ is a unit in R. Therefore it now suffices to show that s is a unit in R if and only if $y/x^{bd/q}$ is a unit in R. Let $m = [L : L']$, $n = [L : K]$, and $y' = \operatorname{Norm}_{L/K} z$. Then $n = md$ and $y' = y^m$, and hence $y'/x^{bn/q} = (y/x^{bd/q})^m$. Since $X^q = x$ and $\operatorname{ord}_S x = 1$ we get that $Z^q - x$ is the minimal monic polynomial of X over K; consequently $[L : K(X)] = n/q$ and $\operatorname{Norm}_{K(X)/K} X = (-1)^{q+1} x$, and hence $\operatorname{Norm}_{L/K} X^b = ((\operatorname{Norm}_{K(X)/K} X)^{n/q})^b = (-1)^{(q+1)(bn/q)} x^{bn/q}$. Let $t = s'/X^b$ and $u = \operatorname{Norm}_{L/K}(s + t)$. Then $s + t = z/X^b$ and hence $u = (\operatorname{Norm}_{L/K} z)/(\operatorname{Norm}_{L/K} X^b)$; consequently $u = (-1)^{(q+1)(bn/q)}(y/x^{bd/q})^m \in R$, and hence u is a unit in R if and only if $y/x^{bd/q}$ is a unit in R. Therefore $u \in R$, and it suffices to show that u is a unit in R if and only if s is a unit in R. Now $u = H_1(s + t) \dots H_n(s + t)$ where $H_1, \dots, H_n$ are K-automorphisms of L. Since $\operatorname{ord}_T s' > \operatorname{ord}_T X^b$ we get that $t \in Q$ where Q is the maximal ideal in T. Since $H_i(Q) = Q$ and $s \in R$ we get that $H_i(s + t) = s + H_i(t) \equiv s \mod Q$ for $1 \leq i \leq n$. Therefore $u \equiv s^n \mod Q$, i.e., $u - s^n \in Q$. Now $u \in R$, $s \in R$, and $Q \cap R = (Q \cap S) \cap R = (xS) \cap R = xR$. Therefore $u - s^n \in xR$ and hence in particular $u - s^n$ is a nonunit in R. Since R is quasilocal, we conclude that u is a unit in R if and only if s^n is a unit in R, i.e., if and only if s is a unit in R.

LEMMA 2.3 - *Let* R *be a normal quasilocal domain with maximal ideal* M *and quotient field* K, *let* $x \in R$ *such that* xR *is a prime ideal in* R *and* S

is a one dimensional regular local domain where $S = R_{xR}$, let L be a finite normal extension of K such that the integral closure T of S in L is quasilocal (by [20: § 7 and § 8] it follows that T is then a one dimensional regular local domain), let $X \in L$ such that $X^q = x$ where q is a positive integer such that q is not divisible by the characteristic of R/M and K contains a primitive q^{th} root W of 1, let $g(Z)$ be a monic polynomial of degree $d > 1$ in Z with coefficients in R such that $g(Z)$ is irreducible in $K[Z]$ and $D_K(g(Z))$ is an R-monomial in x, let $f(Z) = g(Z)^e$ where e is a positive integer, and let $n = de$. Assume that there exist elements z, r, s, s' in L and a positive integer b such that $f(z)=0$, $z-r=sX^b+s'$, $r \in R$, $s \in R$, $s \notin xR$, s' is integral over R, $\operatorname{ord}_T s' > \operatorname{ord}_T X^b$, and $b \not\equiv 0(q)$. Let $a = bn/q$. Then a is a positive integer with $a \not\equiv 0(n)$, and for any $r^* \in R$ with $\operatorname{ord}_S r^* \geq a/n$ we have that $f(r + r^*)/x^a$ is a unit in R.

PROOF. - Now $[K(z) : K] = d$ and hence by Lemma 2.2(1) we get that $bd \equiv 0(q)$ and hence $bn \equiv 0(q)$; since $a = bn/q$ and $b \not\equiv 0(q)$ we conclude that a is a positive integer and $a \not\equiv 0(n)$. Upon letting $h(Z) = Z^q - x$ we get that $h(Z) \in K[Z]$ and $h(X) = 0 = h(WX)$; since $\operatorname{ord}_S x = 1$ we get that $h(Z)$ is irreducible in $K[Z]$; therefore there exists a K-automorphism G of L such that $G(X) = WX$. Let $z_1 = G(z)$. Since $g(z) = 0$ we get that $g(z_1) = 0$. Since q is not divisible by the characteristic of R/M and $b \not\equiv 0(q)$ we get that $1-W^b$ is a unit in R and hence $(1 - W^b)s \in R$ and $(1 - W^b)s \notin xR$; in particular $(1-W^b)s$ is a unit in S and hence $\operatorname{ord}_T X^b = \operatorname{ord}_T(1-W^b)sX^b$. Clearly $G(T) = T$ and hence $\operatorname{ord}_T G(s') = \operatorname{ord}_T s'$; consequently $\operatorname{ord}_T(s' - G(s')) > \operatorname{ord}_T X^b$. Now $z - z_1 = (1 - W^b)sX^b + (s' - G(s'))$ and hence $\operatorname{ord}_T(z - z_1) = \operatorname{ord}_T X^b$. Therefore $z \neq z_1$. Since L is a normal extension of K, there exist distinct elements $z_2, \ldots, z_m$ in L such that $d \equiv 0(m)$, $z \neq z_i \neq z_1$ for $2 \leq i \leq m$, and $g(Z) = ((Z - z)(Z - z_1) \ldots (Z - z_m))^{d/m}$. Let $L' = K(z, z_1, \ldots, z_m)$. Let $y = \operatorname{Norm}_{L'/K}(z - z_1)$. Let $y' = \operatorname{Norm}_{L'/K} z'$ where

$$z' = [\prod_{i=2}^{m} (z - z_i)] [\prod_{i=1}^{m} (z_i - z)] [\prod_{i=1}^{m} \prod_{1 \leq j \leq m,\, j \neq i} (z_i - z_j)].$$

Then $0 \neq y \in R$ and $0 \neq y' \in R$. Also $yy' = D_K(g(Z))$ and hence by assumption there exists a nonnegative integer c^* such that yy'/x^{c^*} is a unit in R. Then $\operatorname{ord}_S yy' = c^*$. Let c and c' be the greatest integers such that $y/x^c \in R$ and $y'/x^{c'} \in R$. Then $y/x^c \notin xR$ and $y'/x^{c'} \notin xR$. Therefore y/x^c and $y'/x^{c'}$ are units in S and hence $\operatorname{ord}_S y = c$ and $\operatorname{ord}_S y' = c'$. Therefore $\operatorname{ord}_S yy' = c + c'$ and hence $c + c' = c^*$. Consequently $(y/x^c)(y'/x^{c'}) = yy'/x^{c^*}$; since y/x^c and $y'/x^{c'}$ are in R and yy'/x^{c^*} is a unit in R, we conclude that y/x^c and $y'/x^{c'}$ are units in R and hence y and y' are R-monomials in x. Thus $z - z_1 = (1-W^b)sX^b + (s' - G(s'))$, $(1-W^b)s \in R$, $(1-W^b)s \notin xR$, $s' - G(s')$ is integral over R, $\operatorname{ord}_T(s' - G(s')) > \operatorname{ord}_T X^b$, $y = \operatorname{Norm}_{L'/K}(z - z_1)$, and y is an R-monomial in x; therefore by Lemma 2.2(3) we get that $(1 - W^b)s$ is a unit in R; since $1 - W^b$ is a unit in R we conclude that s is a unit in R. Given any $r^* \in R$

with $\mathrm{ord}_S r^* \geq a/n$ let $y^* = \mathrm{Norm}_{K(z)/K}(z - r - r^*)$. Since $a \not\equiv 0(n)$ we get that $\mathrm{ord}_S r^* > a/n = (a/n)\,\mathrm{ord}_S x$ and hence $\mathrm{ord}_T r^* > (a/n)\,\mathrm{ord}_T x = (a/n)(q/b)\,\mathrm{ord}_T X^b = \mathrm{ord}_T X^b$. Consequently $\mathrm{ord}_T(s' - r^*) > \mathrm{ord}_T X^b$ and also $s' - r^*$ is integral over R; since $z - r - r^* = sX^b + (s' - r^*)$ and s is a unit in R, by Lemma 2.2(2) we get that $y^*/x^{db/q}$ is a unit in R; since $(-1)^n y^{*e}/x^a = (-1)^n (y^*/x^{db/q})^e$ we conclude that $(-1)^n y^{*e}/x^a$ is a unit in R. Let $g'(Z) = g(Z + r + r^*)$. Then $g'(Z)$ is the minimal monic polynomial of $z - r - r^*$ over K and hence $y^* = (-1)^d g'(0)$. Now $f(r + r^*) = g(r + r^*)^e$ and $g(r + r^*) = g'(0)$. Therefore $f(r + r^*) = (-1)^n y^{*e}$ and hence $f(r + r^*)/x^a$ is a unit in R.

Lemma 2.4 - *Let R be a normal local domain with maximal ideal M and quotient field K, let p be the characteristic of R/M, let $0 \neq x \in R$ such that xR is a prime ideal in R, let $S = R_{xR}$, let X be an element in an overfield of K such that $X^q = x$ where q is a positive integer such that $q \not\equiv 0(p)$ and K contains a primitive q^{th} root of 1, let $K' = K(X)$, let R' be the integral closure of R in K', and let S' be the integral closure of S in K'. Then: S and S' are one dimensional regular local domains; XR' is a prime ideal in R'; $S' = R'_{XR'}$; for any $0 \neq y \in R$ if b is the greatest integer such that $y/x^b \in R$ then $b = \mathrm{ord}_S y$; for any $0 \neq y \in R'$ if b is the greatest integer such that $y/X^b \in R'$ then $\mathrm{ord}_{S'} y = b$; and if R/xR is a regular local domain then so is R'/XR'. Furthermore we have the following.*

(1) *Let $g(Z)$ be a monic polynomial of degree $d > 1$ in Z with coefficients in R such that $g(Z)$ is irreducible in $K[Z]$, $g(z) = 0$ for some $z \in K'$, and $D_K(g(Z))$ is an R-monomial in x. Let $f(Z) = g(Z)^e$ where e is a positive integer and let $n = de$. Then there exists $r \in R$ and a positive integer a with $a \not\equiv 0(n)$ such that for any $r^* \in R$ with $\mathrm{ord}_S r^* \geq a/n$ we have that $f(r + r^*)/x^a$ is a unit in R.*

(2) *Assume that $p \neq 0$. Let L be a normal extension of K such that L is a p-extension of K', let $g(Z)$ be a monic polynomial of degree $d > 0$ in Z with coefficients in R such that $g(Z)$ is irreducible in $K[Z]$, and let $f'(Z)$ be a monic polynomial of degree $m > 0$ in Z with coefficients in R' such that $f'(Z)$ is irreducible in $K'[Z]$, $f'(Z)$ divides $g(Z)$ in $K'[Z]$, and $f'(z) = 0$ for some $z \in L$. Then m is the highest power of p which divides d, and if $g(Z) \notin K[Z^m]$ then $f'(Z) \neq Z^m + f'(0)$. Let $f(Z) = g(Z)^e$ where e is a positive integer and let $n = de$. Assume that $m > 1$, $p \in xR$, S' is totally ramified in L, R/xR is a regular local domain, $D_K(g(Z))$ is an R-monomial in x, and there exist nonnegative integers a' and c' and $r' \in R'$ such that $\mathrm{ord}_{S'} f'(r') = a'$, $\mathrm{ord}_{R'/X} f(r')/X^{a'} = c'$, $(a', c') \not\equiv 0(m)$, and $c' \leq m/p$. Then there exist nonnegative integers a and c and $r \in R$ such that $(a, c) \not\equiv 0(n)$ and $c \leq n/p$ and such that for any $r^* \in R$ with $\mathrm{ord}_S r^* \geq a/n$ we have that $\mathrm{ord}_S f(r + r^*) = a$ and $\mathrm{ord}_{R/x} f(r + r^*)/x^a = c$.*

Proof. - Clearly S is a one dimensional regular local domain with maximal ideal xS and hence xR is a minimal prime ideal in R; for any

$0 \neq y \in R$ if b is the greatest integer such that $y/x^b \in R$ then $y/x^b \notin xR$ and hence y/x^b is a unit in S and hence $\mathrm{ord}_S y = b$. Since $\mathrm{ord}_S x = 1$, $K' = K(X)$, $X^q = x$, $q \not\equiv 0(p)$, and K contains a primitive q^{th} root of 1, we deduce that $[K' : K] = q$, K' is a separable normal extension of K, S' is a one dimensional regular local domain with maximal ideal XR', and $h'(S') = h'(S)$ where h' is the canonical epimorphism of S' onto S'/XS'. Since S' is a one dimensional regular local domain with maximal ideal XS' upon letting $P = (XS') \cap R'$ we get that P is a minimal prime ideal in R', $S' = R'_P$, $PS' = XS'$, $P \cap R = xR$, and P is the only minimal prime ideal in R' whose intersection with R is xR (for instance see [4: Lemma 1.9 and 1.28]). If P' is any minimal prime ideal in R' such that $X \in P'$ then $x \in P' \cap R$ and by [4: Proposition 1.24B] we know that $P' \cap R$ is a minimal prime a ideal in R; consequently $P' \cap R = xR$ and hence $P' = P$. Thus P is the only minimal prime ideal in R' containing X; since $XR'_P = PR'_P$ and R' is a normal noetherian domain, by [20: Theorem 15 on page 223 and Theorem 14 on page 277] we conclude that $XR' = P$. Therefore XR' is a minimal prime ideal in R', $S' = R'_{XR'}$, and $(XR') \cap R = xR$; for any $0 \neq y \in R'$ if b is the greatest integer such that $y/X^b \in R'$ then $y/X^b \notin XR'$ and hence y/X^b is a unit in S' and hence $\mathrm{ord}_{S'} y = b$. In particular $h'(S')$ is the quotient field of $h'(R')$ in $h'(S')$, and $h'(R')$ is integral over $h'(R)$. Let h be the canonical epimorphism of R' onto R'/XR'. Since $h'(S') = h'(S)$ and $h'(S)$ is the quotient field of $h'(R)$ in $h'(S)$ it follows that if R/xR is normal then $h'(R') = h'(R)$, i.e., $h(R') = h(R)$. Therefore, if R/xR is a regular local domain then $h(R') = h(R)$ and $h(R')$ is a regular local domain. Since $K' = K(X)$, $X^q = x$, $q = [K' : K]$, and $q \not\equiv 0(p)$, by [8: Theorem 7] we get that $1, X, \ldots, X^{q-1}$ is a free R-basis of R'. We shall now prove (1) and (2) separately.

PROOF OF (1) – Now $z \in R'$ and $z \notin K$. Therefore $z = r + r_1 X + \ldots + r_{q-1} X^{q-1}$ where $r, r_1, \ldots, r_{q-1}$ are elements in R such that $r_i \neq 0$ for some i. Let b' the greatest integer such that $r_i/x^{b'} \in R$ for $1 \leq i \leq q-1$. Let j be the smallest integer such that $1 \leq j \leq q-1$ and $r_j/x^{b'} \notin xR$. Let $s = r_j/x^{b'}$, $s' = z - r - r_j X^j$, and $b = j + qb'$. Then $z - r = sX^b + s'$, $s \in R$, $s \notin xR$, $s' \in R'$, $\mathrm{ord}_{S'} s' > \mathrm{ord}_{S'} X^b$, and b is a positive integer such that $b \not\equiv 0(q)$. Therefore upon letting $a = bn/q$, by Lemma 2.3 we get that a is a positive integer with $a \not\equiv 0(n)$, and $f(r + r^*)/x^a$ is a unit in R for all $r^* \in R$ with $\mathrm{ord}_S r^* \geq a/n$.

PROOF OF (2) – Since L is a p-extension of K' we get that m is a power of p. Let F_i be the coefficient of Z^{m-i} in $f'(Z)$ for $1 \leq i \leq m$. Let $L' = K(F_1, \ldots, F_m)$, $[K' : L'] = u$, and $[L' : K] = v$. Since $[K' : K] = q$, $K' = K(X)$, $X^q = x$, $q \not\equiv 0(p)$, and K contains a primitive q^{th} root of 1, we deduce that $q = uv$, $\mathrm{ord}_{S'} y \equiv 0(u)$ for all $0 \neq y \in L'$, $L' = K(X^u)$, K contains a primitive v^{th} root W of 1, L' is a separable normal extension of K, and the group of all K-automorphisms of L' is a cyclic group of order v and it has a generator G such that $G(X^u) = WX^u$. Now $g(Z)$ and $f'(Z)$ are the minimal monic polynomials of z

over K and L' respectively, and hence $g(Z) = f'(Z)f^*(Z)$ where $f^*(Z) = Z^{d-m} + F_1^* Z^{d-m-1} + \dots + F_{d-m}^*$ with $F_1^*, \dots, F_{d-m}^*$ in L'. Upon applying G^i to the coefficients of $g(Z)$, $f'(Z)$, and $f^*(Z)$ we get that $g(Z) = f_i(Z)f_i^*(Z)$ where $f_i(Z) = Z^m + G^i(F_1)Z^{m-1} + \dots + G^i(F_m)$ and $f_i^*(Z) = Z^{d-m} + G^i(F_1^*)Z^{d-m-1} + \dots + G^i(F_{d-m}^*)$. Hence in particular $f_i(Z)$ divides $g(Z)$ in $L'[Z]$. Since $f'(Z)$ is irreducible in $L'[Z]$ and $L' = K(F_1, \dots, F_m)$ we get that $f_i(Z)$ is irreducible in $L'[Z]$ for $1 \leq i \leq v$, $f_v(Z) = f'(Z)$, and $f_i(Z) \neq f_{i'}(Z)$ for $1 \leq i < i' \leq v$. Therefore upon letting $g'(Z) = f_1(Z) \dots f_v(Z)$ we get that $g'(Z)$ divides $g(Z)$ in $L'[Z]$ and $g'(z) = 0$. Let $g_k(Z)$ and $f_{ik}(Z)$ be the polynomials obtained by applying G^k to the coefficients of $g'(Z)$ and $f_i(Z)$ respectively; then $g_k(Z) = f_{1k}(Z) \dots f_{vk}(Z)$; now $f_{1k}(Z), \dots, f_{vk}(Z)$ is a permutation of $f_1(Z), \dots, f_v(Z)$ and hence $g_k(Z) = g'(Z)$; this being so for $1 \leq k \leq v$ we get that $g'(Z) \in K[Z]$. Therefore $g(Z) = g'(Z)$; hence $d = mv$, m is the highest power of p which divides d, and if $g(Z) \notin K[Z^m]$ then $f'(Z) \neq Z^m + f'(0)$. Henceforth let the remaining assumptions be in force. Let T be the integral closure of S' in L. Then T is the integral closure of S in L, and T is a one dimensional regular local domain. Now $r' = r + r_1 X + \dots + r_{q-1}X^{q-1}$ where $r, r_1, \dots, r_{q-1}$ are elements in R. If $r' \neq r$ then let b' be the greatest integer such that $r_i/x^{b'} \in R$ for $1 \leq i \leq q-1$ and let j be the smallest integer such that $1 \leq j \leq q-1$ and $r_j/x^{b'} \notin xR$. We shall now divide the argument into two cases.

Case when $r' \neq r$ *and* $\operatorname{ord}_T(z - r') > \operatorname{ord}_T X^{j+qb'}$. Let $b = j + qb'$, $s = r_j/x^{b'}$, and $s' = z - r - sX^b$. Then b is a positive integer such that $b \not\equiv 0(q)$, $s \in R$, $s \notin xR$, $r' - r - sX^b \in X^{b+1}R'$, $s' \in L$, s' is integral over R, and $z - r = sX^b + s'$. Since $s' = (z - r') + (r' - r - sX^b)$, $\operatorname{ord}_T(z - r') > \operatorname{ord}_T X^b$, and $r' - r - sX^b \in X^{b+1}R'$, we get that $\operatorname{ord}_T s' > \operatorname{ord}_T X^b$. Therefore upon taking $a = bn/q$ and $c = 0$, by Lemma 2.3 we get that a and c are nonnegative integers such that $(a, c) \not\equiv 0(n)$ and $c \leq n/p$ and such that for any $r^* \in R$ with $\operatorname{ord}_S r^* \geq a/n$ we have that $f(r + r^*)/x^a$ is a unit in R and hence $\operatorname{ord}_S f(r + r^*) = a$ and $\operatorname{ord}_{R/x} f(r + r^*)/x^a = c$.

Case when either $r' = r$, *or* $r' \neq r$ *and* $\operatorname{ord}_T(z - r') \leq \operatorname{ord}_T X^{j+qb'}$. If $r' = r$ then let b'' be any positive integer such that $\operatorname{ord}_T(z - r') \leq \operatorname{ord}_T X^{b''}$, and if $r' \neq r$ then let $b'' = j + qb'$. Then in both the cases b'' is a positive integer such that $\operatorname{ord}_T(z - r') \leq \operatorname{ord}_T X^{b''}$ and $r - r' \in X^{b''}R'$. Let $A(Z) = f'(Z + r') = Z^m + A_1 Z^{m-1} + \dots + A_m$ with $A_1, \dots, A_m$ in K'. Then $A(Z)$ is the minimal monic polynomial of $z - r'$ over K' and hence $A(0) = (-1)^m H_1(z - r') \dots H_m(z - r')$ where $H_1, \dots, H_m$ are K'-automorphisms of L; now $H_i(T) = T$ and hence $\operatorname{ord}_T H_i(z - r') = \operatorname{ord}_T(z - r')$ for $1 \leq i \leq m$; consequently $\operatorname{ord}_T A(0) = \operatorname{ord}_T(z - r')^m$; since $A(0) = f'(r')$ and $\operatorname{ord}_{S'} f'(r') = a' = \operatorname{ord}_{S'} X^{a'}$ we get that $\operatorname{ord}_{S'} A(0) = a'$ and $\operatorname{ord}_T(z - r') = (a'/m) \operatorname{ord}_T X$; since $\operatorname{ord}_T(z - r') \leq \operatorname{ord}_T X^{b''}$ we get that $b'' \geq a'/m$; since $r - r' \in X^{b''}R'$ we conclude that: 1) $r - r' \in X^b R'$ where b is the smallest integer such that $b \geq a'/m$. Since $A(Z)$ is the minimal monic polynomial of $z - r'$ over K', $\operatorname{ord}_{S'} A(0) = a'$, and S' is totally ramified in L, by [10: Lemma 2.5] we get that: 2) $\operatorname{ord}_{S'} A_i \geq ia'/m$ for $1 \leq i \leq m$, and if

$a' \equiv 0(m)$ then $\mathrm{ord}_{S'}A_i > ia'/m$ for $1 \leq i < m$. By 1) and 2) we get that $\mathrm{ord}_{S'}(A(r-r') - A(0)) > a'$; since $A(r-r') = f'(r)$ and $\mathrm{ord}_{S'}A(0) = a'$ we get that $\mathrm{ord}_{S'}f'(r) = a'$; since $f'(r) \in L'$ we conclude that $a' \equiv 0(u)$. Let $a = eva'/q$ and $c = evc'$. Then a and c are nonnegative integers such that $(a, c) \equiv\mid\equiv 0(n)$ and $c \leq n/p$. Let r^* be any given element in R such that $\mathrm{ord}_S r^* \geq a/n$. Then $\mathrm{ord}_S r^* \geq (a/n)\ \mathrm{ord}_S X^q$ and hence $\mathrm{ord}_{S'}r^* \geq (a/n)\ \mathrm{ord}_{S'}X^q = a'/m$. Consequently by 1) we get that $r + r^* - r' \in X^b R'$ where b is the smallest integer such that $b \geq a'/m$. Therefore by 2) we get that $\mathrm{ord}_{S'}(A(r + r^* - r') - A(0)) > a'$. Since $A(r + r^* - r') = f'(r + r^*)$ and $A(0) = f'(r')$ we get that $f'(r + r^*) - f'(r') \in X^{a'+1}R'$. Since $\mathrm{ord}_{S'}f'(r') = a'$ we deduce that $\mathrm{ord}_{S'}f'(r+r^*) = a'$ and $\mathrm{ord}_{h(R')}h(f'(r+r^*)/X^{a'}) = \mathrm{ord}_{h(R')}(f'(r')/X^{a'}) = c'$. Let $t' = f'(r + r^*)/X^{a'}$. Then $t' \in R'$ and $\mathrm{ord}_{h(R')}h(t') = c'$. Now $f'(r + r^*) \in L'$; also $a' \equiv 0(u)$ and hence $X^{a'} \in L'$. Therefore $t' \in L'$. Since K' is a finite normal extension of K there exists a K-automorphism G_i of K' such that $G_i(y) = G^i(y)$ for all $y \in L'$. Since $h(R') = h(R)$ there exists $t \in R$ such that $t' - t \in XR'$. Now $G_i(t) = t$ and $G_i(XR') = XR'$. Therefore $G^i(t') - t' = G_i(t' - t) - (t' - t) \in XR'$. This being so for $1 \leq i \leq v$ we get that $t^* - t'^v \in XR'$ where $t^* = G^1(t')\dots G^v(t')$. Therefore $\mathrm{ord}_{h(R')}h(t^*) = vc'$. Now $t^* = \mathrm{Norm}_{L'|K}t' \in R' \cap K = R$, $h(R') = h(R)$, and $(XR') \cap R = xR$. Therefore $\mathrm{ord}_{R/x}t^* = \mathrm{ord}_{h(R')}h(t^*) = vc' = c/e$. Now $g(r + r^*) = f_1(r + r^*) \dots f_v(r + r^*)$, $f_i(r + r^*) = G^i(f'(r + r^*)) = G^i(X^{a'})G^i(t')$ for $1 \leq i \leq v$, $G^1(X^{a'}) \dots G^v(X^{a'}) = (-1)^{(a'/u)(v+1)}X^{a'v}$, and $a'v = aq/e$. Therefore $g(r + r^*) = (-1)^{(a'/u)(v+1)}t^* x^{a/e}$ and hence $\mathrm{ord}_S g(r + r^*) = a/e$ and $\mathrm{ord}_{R/x}g(r + r^*)/x^{a/e} = c/e$. Since $f(r + r^*) = g(r + r^*)^e$ we conclude that $\mathrm{ord}_S f(r + r^*) = a$ and $\mathrm{ord}_{R/x}f(r + r^*)/x^a = c$.

LEMMA 2.5 - *Let R be a quasilocal domain with quotient field K. Let $0 \neq x \in R$ such that R/xR is a regular local domain and S is a one dimensional regular local domain where $S = R_{xR}$ (note that for any $0 \neq y \in R$ if b is the greatest integer such that $y/x^b \in R$ then $\mathrm{ord}_S y = b$). Let L be a finite normal extension of K such that S does not split in L. Let v be a positive integer and for $i = 1, \dots, v$ let $g_i(Z)$ be a monic polynomial of degree $d(i) > 1$ in Z with coefficients in R such that $g_i(Z)$ is irreducible in $K[Z]$ and $g_i(z_i) = 0$ for some $z_i \in L$, let $f_i(Z) = g_i(Z)^{e(i)}$ where $e(i)$ is a positive integer, and let $n(i) = d(i)e(i)$. Let $f(Z) = f_1(Z) \dots f_v(Z)$ and $n = n(1) + \dots + n(v)$. Assume that for $i = 1, \dots, v$ there exist nonnegative integers $a(i)$ and $c(i)$ and $r_i \in R$ such that $(a(i), c(i)) \equiv\mid\equiv 0(n(i))$ and $c(i) < n(i)$ and such that for any $r_i^* \in R$ with $\mathrm{ord}_S r_i^* \geq a(i)/n(i)$ we have that $\mathrm{ord}_S f(r_i + r_i^*) = a(i)$ and $\mathrm{ord}_{R/x}f(r_i + r_i^*)/x^{a(i)} = c(i)$. Also assume that $D(g_i(Z), g_j(Z))$ is an R-monomial in x whenever $1 \leq i \leq v$, $1 \leq j \leq v$, and $i \neq j$. Then there exists $r \in R$ such that upon letting $F(Z) = f(Z + r) = Z^n + F_1 Z^{n-1} + \dots + F_n$ with $F_1, \dots, F_n$ in R we have that either: (1) there exists an integer u such that $0 < u < n$, F_u is an R-monomial in x, $\mathrm{ord}_S F_j \geq (j/u)\ \mathrm{ord}_S F_u$ for $1 \leq j \leq u$, and $\mathrm{ord}_S F_j > (j/u)\ \mathrm{ord}_S F_u$ for $u < j \leq n$; or: (2) there exist nonnegative integers a and c such that $(a, c) \equiv\mid\equiv 0(n)$, $c \leq c(1) + \dots + c(v)$, $\mathrm{ord}_S F_n = a$, $\mathrm{ord}_{R/x}F_n/x^a = c$, and $\mathrm{ord}_S F_j \geq ja/n$ for $1 \leq j \leq n$.*

PROOF. - Upon replacing $1, \dots, v$ by a suitable permutation of $1, \dots, v$ we may assume that $a(1)/n(1) \geq a(i)/n(i)$ for $1 < i \leq v$. Let $r = r_1$ and $F(Z) = f(Z + r) = Z^n + F_1Z^{n-1} + \dots + F_n$ with $F_1, \dots, F_n$ in R. For $1 \leq i \leq v$ let $g_i'(Z) = g_i(Z + r)$, $f_i'(Z) = g_i'(Z)^{e(i)}$, $y_i = z_i - r$, $s_i = r_i - r$, and $b(i) = \text{ord}_S f_i'(0)$. Then $F(Z) = f_1'(Z) \dots f_v'(Z)$, and for $1 \leq i \leq v$ we have that $g_i'(Z)$ is a monic polynomial of degree $d(i)$ in Z with coefficients in R, $g_i'(Z)$ is irreducible in $K[Z]$, $y_i \in L$, $g_i'(y_i) = 0$, $s_i \in R$, and: 1) $\text{ord}_S f_i'(s_i + s_i^*) = a(i)$ and $\text{ord}_{R/x} f_i'(s_i + s_i^*)/x^{a(i)} = c(i)$ for all $s_i^* \in R$ with $\text{ord}_S s_i^* \geq a(i)/n(i)$. In particular $s_1 = 0$ and hence: 2) $\text{ord}_S f_1'(0) = a(1) = b(1)$. For $1 < i \leq v$ we have that $D(f_i'(Z), f_1'(Z)) = D(f_i(Z), f_1(Z)) = (D(g_i(Z), g_1(Z)))^{e(i)e(1)}$ and hence $D(f_i'(Z), f_1'(Z))$ is an R-monomial in x. Let T be the integral closure of S in L. Then T is a one dimensional regular local domain and for any K-automorphism G of L we have that $G(T) = T$ and hence $\text{ord}_S G(y) = \text{ord}_S y$ for all $y \in L$. Since L is a finite normal extension of K there exist K-automorphisms G_{ij} of L such that upon letting $y_{ij} = G_{ij}(y_i)$ we have that $g_i'(Z) = (Z - y_{i1}) \dots (Z - y_{id(i)})$ for $1 \leq i \leq v$. Now $\text{ord}_S y_{ij} = \text{ord}_S y_i$ for $1 \leq i \leq v$ and $1 \leq j \leq d(i)$, and

$$f_i'(Z) = \prod_{j=1}^{d(i)} (Z - y_{ij})^{e(i)} = Z^{n(i)} + \sum_{j=1}^{n(i)} f_{ij}' Z^{n(i)-j}$$

where $f_{ij}' \in R$ for $1 \leq i \leq v$ and $1 \leq j \leq n(i)$. Therefore: 3) $\text{ord}_T y_{ij} = \text{ord}_T y_i = (b(i)/n(i))\text{ord}_T x$ for $1 \leq i \leq v$ and $1 \leq j \leq d(i)$, and: 4) $\text{ord}_S f_{ij}' \geq jb(i)/n(i)$ for $1 \leq i \leq v$ and $1 \leq j \leq n(i)$.

Let i be any integer such that $1 \leq i \leq v$ and $b(i)/n(i) < a(1)/n(1)$. Then by 2) and 3) we get that $b(1) = a(1)$, $i \neq 1$, $b(i)/n(i) < b(1)/n(1)$, and $\text{ord}_T y_{1j} = (b(1)/n(1))\text{ord}_T x$ for $1 \leq j \leq d(1)$; since $\text{ord}_S f_i'(0) = b(i)$ and

$$f_i'(y_{1j}) = y_{1j}^{n(i)} + \sum_{k=1}^{n(i)} f_{ik}' y_{1j}^{n(i)-k} \quad \text{for } 1 \leq j \leq d(1),$$

by 4) we get that $\text{ord}_T f_i'(y_{1j}) = \text{ord}_T f_i'(0) = \text{ord}_T x^{b(i)}$ and $\text{ord}_T(f_i'(y_{1j}) - f_i'(0)) > \text{ord}_T x^{b(i)}$ for $1 \leq j \leq d(1)$. Therefore $f_i'(y_{1j})/x^{b(i)} \in T$, $f_i'(0)/x^{b(i)} \in T$, and $f_i'(y_{1j})/x^{b(i)} \equiv f_i'(0)/x^{b(i)}$ mod Q for $1 \leq j \leq d(1)$ where Q is the maximal ideal in T, and hence

$$\prod_{j=1}^{d(1)} (f_i'(y_{1j})/x^{b(i)})^{e(1)} \equiv (f_i'(0)/x^{b(i)})^{n(1)} \text{ mod } Q.$$

Now

$$\prod_{j=1}^{d(1)} f_i'(y_{1j})^{e(1)} = D(f_i'(Z), f_1'(Z)) = tx^{b'}$$

where t is a unit in R and b' is a nonnegative integer, and hence

$$tx^{b'-b(i)n(1)} \equiv (f_i'(0)/x^{b(i)})^{n(1)} \text{ mod } Q.$$

Since $tx^{b'-b(i)n(1)}$ and $(f'_i(0)/x^{b(i)})^{n(1)}$ are in K and $K \cap Q = xS$ we get that

5) $$tx^{b'-b(i)n(1)} - (f'_i(0)/x^{b(i)})^{n(1)} \in xS.$$

Since $f'_i(0) \in R$ and $\text{ord}_S f'_i(0) = b(i)$ we get that $f'_i(0)/x^{b(i)} \in R$ and $f'_i(0)/x^{b(i)}$ is a unit in S; consequently by 5) we get that $tx^{b'-b(i)n(1)}$ is a unit in S; since t is a unit in R we must the have $b' - b(i)n(1) = 0$ and hence by 5) we get that $t - (f'_i(0)/x^{b(i)})^{n(1)} \in (xS) \cap R = xR$; since t is a unit in R we conclude that $f'_i(0)/x^{b(i)}$ is a unit in R. Thus we have shown that: 6) if i is any integer such that $1 \leq i \leq v$ and $b(i)/n(i) < a(1)/n(1)$ then $f'_i(0)/x^{b(i)}$ is a unit in R.

Next, let i be any integer such that $1 \leq i \leq v$ and $b(i)/n(i) \geq a(1)/n(1)$. Since $a(1)/n(1) \geq a(i)/n(i)$ we get that $b(i) \geq a(i)$ and hence by 4) we get that $\text{ord}_S f'_{ij} \geq ja(i)/n(i)$ for $1 \leq j \leq n(i)$; upon taking $s_i^* = 0$ in 1) we get that $\text{ord}_S f'_i(s_i) = a(i)$; now

$$f'_i(s_i) = s_i^{n(i)} + \sum_{j=1}^{n(i)} f'_{ij} s^{n(i)-j}$$

and hence we must have $\text{ord}_S s_i \geq a(i)/n(i)$; therefore upon taking $s_i^* = -s_i$ in 1) we get that $\text{ord}_S f'_i(0) = a(i)$ and $\text{ord}_{R/x} f'(0)/x^{a(i)} = c(i)$; since $b(i)/n(i) \geq$ $\geq a(1)/n(1) \geq a(i)/n(i)$ and $b(i) = \text{ord}_S f'_i(0) = a(i)$ we also get that $a(i)/n(i) = a(1)/n(1)$. Thus we have shown that: 7) if i is any integer such that $1 \leq i \leq v$ and $b(i)/n(i) \geq a(1)/n(1)$ then $\text{ord}_S f'_i(0) = a(i)$, $\text{ord}_{R/x} f'_i(0)/x^{a(i)} = c(i)$, $b(i) = a(i)$, and $a(i)/n(i) = a(1)/n(1)$.

We shall show that if $b(i)/n(i) < a(1)/n(1)$ for some i with $1 \leq i \leq v$ then condition (1) holds, and if $b(i)/n(i) \geq a(1)/n(1)$ for all i with $1 \leq i \leq v$ then condition (2) holds, and this will complete the proof.

First suppose that $b(i)/n(i) < a(1)/n(1)$ for some i with $1 \leq i \leq v$. Let $a' = \min(b(1)/n(1), \ldots, b(v)/n(v))$, let V be a set of all integers i such that $1 \leq i \leq v$ and $b(i)/n(i) = a'$, and let V' be the set of all integers i such that $1 \leq i \leq v$ and $i \notin V$. Then $V \neq \emptyset$ and by 2) we also have that $1 \in V'$ and hence $V' \neq \emptyset$. Let

$$u = \sum_{i \in V} n(i) \quad \text{and} \quad a = \sum_{i \in V} b(i).$$

Then $0 < u < n$ and $a = ua'$. Let

$$A(Z) = \prod_{i \in V} f'_i(Z) = Z^u + \sum_{j=1}^{u} A_j Z^{u-j},$$

$$B(Z) = \prod_{i \in V'} f'_i(Z) = Z^{n-u} + \sum_{j=1}^{n-u} B_j Z^{n-u-j}$$

with $A_1, \ldots, A_u, B_1, \ldots, B_{n-u}$ in R. Now

$$A_u = A(0) = \prod_{i \in V} f_i'(0) \quad \text{and} \quad ua' = \sum_{i \in V} b(i)$$

and by 6) we know that $f_i'(0)/x^{b(i)}$ is a unit in R for all $i \in V$, and hence: 8) $\mathrm{ord}_S A_u = ua'$ and $A_u/x^{ua'}$ is a unit in R. Since $b(i)/n(i) = a'$ for $i \in V$ and $b(i)/n(i) > a'$ for $i \in V'$, by 3) we get that $\mathrm{ord}_T y_{ij} = a' \, \mathrm{ord}_T x$ for $i \in V$ and $1 \leq j \leq d(i)$, and $\mathrm{ord}_T y_{ij} > a' \, \mathrm{ord}_T x$ for $i \in V'$ and $1 \leq j \leq d(i)$; since

$$A(Z) = \prod_{i \in V} \prod_{j=1}^{d(i)} (Z - y_{ij})^{e(i)} \quad \text{and} \quad B(Z) = \prod_{i \in V'} \prod_{j=1}^{d(i)} (Z - y_{ij})^{e(i)}$$

we deduce that: 9) $\mathrm{ord}_S A_j \geq ja'$ for $1 \leq j \leq u$, and $\mathrm{ord}_S B_j > ja'$ for $1 \leq j \leq n-u$. Now $F(Z) = A(Z)B(Z)$ and hence upon letting $A_0 = 1$ we get that

10) $$F_j = \begin{cases} A_j + \sum_{k=1}^{\min(j, n-u)} B_k A_{j-k} & \text{for } 1 \leq j \leq u \\ \sum_{k=0}^{\min(u, n-j)} B_{j-u+k} A_{u-k} & \text{for } u < j \leq n. \end{cases}$$

By 8), 9), and 10) we deduce that $\mathrm{ord}_S F_u = ua'$, $F_u/x^{ua'}$ is a unit in R, $\mathrm{ord}_S F_j \geq (j/u) \, \mathrm{ord}_S F_u$ for $1 \leq j \leq u$, and $\mathrm{ord}_S F_j > (j/u) \, \mathrm{ord}_S F_u$ for $u < j \leq n$.

Finally, suppose that $b(i)/n(i) \geq a(1)/n(1)$ for $1 \leq i \leq v$. Then by 7) we get that $\mathrm{ord}_S f_i'(0) = a(i)$, $\mathrm{ord}_{R/x} f_i'(0)/x^{a(i)} = c(i)$, and $b(i)/n(i) = a(i)/n(i) = a(1)/n(1)$ for $1 \leq i \leq v$. Let $a = a(1) + \ldots + a(v)$ and $c = c(1) + \ldots + c(v)$. Since $F_n = F(0) = f_1'(0) \ldots f_v'(0)$ we get that $\mathrm{ord}_S F_n = a$ and $\mathrm{ord}_{R/x} F_n/x^a = c$. Clearly $b(i)/n(i) = a(i)/n(i) = a/n$ for $1 \leq i \leq v$ and hence by 3) we get that $\mathrm{ord}_T y_{ij} = (a/n) \, \mathrm{ord}_T x$ for $1 \leq i \leq v$ and $1 \leq j \leq d(i)$; since

$$F(Z) = \prod_{i=1}^{v} \prod_{j=1}^{d(i)} (Z - y_{ij})^{e(i)}$$

we deduce that $\mathrm{ord}_S F_j \geq ja/n$ for $1 \leq j \leq n$. Since $c(i) < n(i)$ for $1 \leq i \leq v$ we get that $c < n$. If $c \neq 0$ then clearly $(a, c) \not\equiv 0(n)$; if $c = 0$ then $c(1) = 0$ and hence $a(1) \not\equiv 0(n(1))$, and hence $a \not\equiv 0(n)$ because $a/n = a(1)/n(1)$. Thus in both the cases $(a, c) \not\equiv 0(n)$.

LEMMA 2.6 - *Let R be a two dimensional regular local domain with quotient field K and maximal ideal M such that R/M is algebraically closed. Let (x, y) be a basis of M and let J be a coefficient set for R. Let w be a real valuation of K such that w dominates R and w is residually algebraic over R. Let (R_k, x_k, y_k) be the canonical k^{th} quadratic transform of (R, x, y, J) along w.*

Let $F(Z)$ be a monic polynomial of degree $n > 0$ in Z with coefficients in R. Assume that $F(Z)$ is of prenonsplitting-type relative to ord_{xR} *and there exist nonnegative integers a and c such that* $\mathrm{ord}_{xR}F(0) = a$, $\mathrm{ord}_{R|x}F(0)/x^a = c$, $(a, c) \equiv|\equiv 0(n)$, *and* $c \leq n/2$. *Then there exist nonnegative integers k, d, e and an R_k-translate $F'(Z)$ of $F(Z)$ such that upon letting* $f(Z) = F'(x_k^d y_k^e Z)/(x_k^d y_k^e)^n$ *we have that* $k \leq n/2$, $M \subset \mathrm{rad}_{R_k} y_k^e R_k$, $f(Z) \in R_k[Z]$, *and* $0 < \mathrm{ord}_{R_k} f(Z) < n$.

PROOF. - Let d' be the greatest integer such that $nd' \leq a$ and let $a' = a - nd'$. Since $(a, c) \equiv|\equiv 0(n)$ we get that $(a', c) \equiv|\equiv 0(n)$ and $n > 1$.

We claim the following: (1) Let t be any nonnegative integer such that $w(y_u) < w(x_u)$ for $0 \leq u < t$; then either: (1_t) there exist nonnegative integers k and e such that upon letting $f(Z) = F(x_k^{d'} y_k^e Z)/(x_k^{d'} y_k^e)^n$ we have that $0 \leq k \leq t$, $k \leq n/2$, $M \subset \mathrm{rad}_{R_k} y_k^e$, $f(Z) \in R_k[Z]$, and $0 < \mathrm{ord}_{R_k} f(Z) < n$; or: (2_t) $t \leq (n/2) - 1$, $a' > 0$, and there exist nonnegative integers e' and c' such that upon letting $g(Z) = F(x_t^{d'} y_t^{e'} Z)/(x_t^{d'} y_t^{e'})^n$ we have that $c' \leq c - t$, $M \subset \mathrm{rad}_{R_t} y_t^{e'}$, $g(Z) \in R_t[Z]$, $\mathrm{ord}_{x_t R_t} g(0) = a'$, $\mathrm{ord}_{R_t|x_t} g(0)/x_t^{a'} = c'$, $\mathrm{ord}_{R_t} g(Z) \geq n$, and $g(Z)$ is of prenonsplitting-type relative to $\mathrm{ord}_{x_t R_t}$. We shall prove this by induction on t. First suppose that $t = 0$ and let $f(Z) = F(x^{d'} Z)/x^{nd'}$; then $f(Z) \in R[Z]$, $\mathrm{ord}_{xR} f(0) = a'$, $\mathrm{ord}_{R|x} f(0)/x^{a'} = c$, and $f(Z)$ is of prenonsplitting-type relative to ord_{xR}; since $(a', c) \equiv|\equiv 0(n)$ and $\mathrm{ord}_R f(0)/x^{a'} = c < n$ we get that $\mathrm{ord}_R f(Z) > 0$, and if $\mathrm{ord}_R f(Z) \geq n$ then $a' > 0$; therefore if $\mathrm{ord}_R f(Z) < n$ then (1_0) holds, and if $\mathrm{ord}_R f(Z) \geq n$ then (2_0) holds. Now suppose that $t > 0$ and assume that (1) is true for all values of t smaller than the given one. If (1_{t-1}) holds then clearly (1_t) holds. So now suppose that (1_{t-1}) does not hold. Then by the induction hypothesis (2_{t-1}) holds. Let $e = 1 + d' + e'$ and $f(Z) = F(x_t^{d'} y_t^e Z)/(x_t^{d'} y_t^e)^n$. Now $f(Z) = g(y_t Z)/y_t^n$, $y_{t-1} = y_t$, $x_{t-1} = x_t y_t$, $\mathrm{ord}_{y_t R_t} = \mathrm{ord}_{R_{t-1}}$, and $\mathrm{ord}_{x_t R_t} = \mathrm{ord}_{x_{t-1} R_{t-1}}$. Therefore $M \subset \mathrm{rad}_{R_t} y_t^e$, $f(Z) \in R_t[Z]$, $f(Z)$ is of prenonsplitting-type relative to $\mathrm{ord}_{x_t R_t}$, and $\mathrm{ord}_{R_t} f(0) \geq$ $\geq \mathrm{ord}_{x_t R_t} f(0) = a' > 0$. Hence if $\mathrm{ord}_{R_t} f(Z) < n$ then (1_t) holds. So now assume that $\mathrm{ord}_{R_t} f(Z) \geq n$. Since $\mathrm{ord}_{x_{t-1} R_{t-1}} g(0) = a'$ and $\mathrm{ord}_{R_{t-1}|x_{t-1}} g(0)/x_{t-1}^{a'} = c'$ we get that $g(0)/x_{t-1}^{a'} = s x_{t-1} + s' y_{t-1}^{c'}$ where $s \in R_{t-1}$ and s' is a unit in R_{t-1}. Since $\mathrm{ord}_{R_{t-1}} g(0) \geq n$ we get that $c' \geq \mathrm{ord}_{R_{t-1}} g(0)/x_{t-1}^{a'} \geq n - a'$; consequently $a' + c' \geq n$ and $\mathrm{ord}_{R_{t-1}} s \geq n - 1 - a'$, and hence $s'' \in R_t$ where $s'' = s/y_t^{n-1-a'}$. Now $f(0)/x_t^{a'} = g(0)/(x_{t-1}^{a'} y_t^{n-a'}) = s'' x_t + s' y_t^{c''}$ where $c'' = a' + c' - n$, and hence $\mathrm{ord}_{R_t|x_t} f(0)/x_t^{a'} = c''$. Since $a' < n$ and $c' \leq c - (t-1)$ we get that $c'' \leq c - t$. Now $a' + c'' \geq \mathrm{ord}_{R_t} f(0) \geq n$ and hence $c'' \geq 1$. Since $1 \leq c'' \leq c - t$ and $c \leq n/2$ we get that $t \leq (n/2) - 1$. Therefore (2_t) holds. This completes the induction.

We shall now prove the assertion of the lemma. Since w is real, there exists a nonnegative integer t such that $w(y_u) < w(x_u)$ for $0 \leq u < t$ and $w(y_t) \geq w(x_t)$. If (1_t) holds then we have nothing to show. So now assume that

(1_t) does not hold. Then by (1) we know that (2_t) holds. Let $k = t+1$. Then $k \leq n/2$, $x_t = x_k$, and $y_k = (y_t/x_t) - s^*$ with $s^* \in J$. Let $y' = y_t - s^* x_t$. Then $y' = x_k y_k$ and $(x_t, y')R_t = M'$ where M' is the maximal ideal in R_t. Let $e = e'$ and $V = 1$ if $s^* = 0$, and $e = 0$ and $V = (y_k + s^*)^{e'}$ if $s^* \neq 0$. Then $M \subset \operatorname{rad}_{R_k} y_k^e$, and V is a unit in R_k. Let $g'(Z) = g(x_k Z)/x_k^n$. Since $\operatorname{ord}_{R_t} g(Z) \geq n$ we get that $g'(Z) \in R_k[Z]$. Now $g(Z) = Z^n + g_1 Z^{n-1} + \ldots + g_n$ with $g_1, \ldots, g_n$ in R_t. Since $\operatorname{ord}_{R_t} g(Z) \geq n$ we get that

$$g_i = \sum_{j=0}^{i} g_{ij} x_t^{i-j} y'^j \quad \text{with } g_{ij} \in R_t \text{ for } 1 \leq i \leq n,\ 0 \leq j \leq i.$$

Since R_t/M' is algebraically closed, there exists $r \in R_t$ such that $r' \in M'$ where

$$r' = r^n + \sum_{i=1}^{n} g_{i0} r^{n-i}.$$

Let $d = 1 + d' + e'$ and $F'(Z) = F(Z + V x_k^d y_k^e r)$. Then $F'(Z)$ is an R_k-translate of $F(Z)$. Let $f(Z) = F'(x_k^d y_k^e Z)/(x_k^d y_k^e)^n$. Then $f(Z) = V^n g'((Z/V) + r)$; consequently $f(Z) \in R_k[Z]$, and $f(0) = V^n g'(r) = V^n g(r x_k)/x_k^n$, and hence $\operatorname{ord}_{R_k} f(0) = \operatorname{ord}_{R_k} g(r x_k)/x_k^n$. Now

$$g(r x_k) = g(r x_t) = r^n x_t^n + \sum_{i=1}^{n} \sum_{j=0}^{i} g_{ij} r^{n-i} x_t^{n-j} y'^j = x_k^n (r' + r'')$$

where

$$r'' = \sum_{i=1}^{n} \sum_{j=1}^{i} g_{ij} r^{n-i} y_k^j.$$

Since $r' \in M'$ we get that $\operatorname{ord}_{R_k} r' > 0$; also clearly $\operatorname{ord}_{R_k} r'' > 0$; therefore $\operatorname{ord}_{R_k} g(r x_k)/x_k^n > 0$ and hence $\operatorname{ord}_{R_k} f(0) > 0$. Since $\operatorname{ord}_{x_t R_t} g(0) = a'$ and $\operatorname{ord}_{R_t/x_t} g(0)/x_t^{a'} = c'$, we get that

$$g(0)/x_t^{a'} = h x_t + h' y'^{c'} \text{ where } h \in R_t,\ h' \in R_t,\ h' \notin M'.$$

Let i be any integer such that $1 \leq i < n$; since $g(Z)$ is of prenonsplitting-type relative to $\operatorname{ord}_{x_t R_t}$ we get that $\operatorname{ord}_{x_t R_t} g_i \geq ia'/n$ and hence $\operatorname{ord}_{x_t R_t} g_i r^{n-i} x_t^{n-i} \geq$ $\geq (n-i) + (ia'/n)$; since $a' < n$ and $i < n$ we get that $(n-i)(1-(a'/n)) > 0$ and hence $n - i > a' - (ia'/n)$; consequently $(n-i) + (ia'/n) > a'$ and hence $\operatorname{ord}_{x_t R_t} g_i r^{n-i} x_t^{n-i} > a'$. Thus $\operatorname{ord}_{x_t R_t} g_i r^{n-i} x_t^{n-i} > a'$ for $1 \leq i < n$; also $\operatorname{ord}_{x_t R_t} r^n x_t^n \geq$ $\geq n > a'$; now

$$g(r x_t) - g(0) = r^n x_t^n + \sum_{i=1}^{n-1} g_i r^{n-i} x_t^{n-i}$$

and hence $h'' \in R_t$ where $h'' = (g(rx_t) - g(0))/x_t^{1+a'}$; consequently

$$g(rx_t)/x_t^{a'} = (h + h'')x_t + h'y'^{c'}, \; h + h'' \in R_t, \; h' \in R_t, \; h' \notin M'.$$

Therefore $\text{ord}_{x_t R_t} g(rx_t) = a'$ and $\text{ord}_{R_t/x_t} g(rx_t)/x_t^{a'} = c'$. Consequently $g(rx_t) \neq 0$ and upon letting $m = \text{ord}_{R_t} g(rx_t)/x_t^{a'}$ we get that $m \leq c' \leq c - t \leq (n/2) - t \leq n/2$. Since $\text{ord}_{R_t} g(rx_t)/x_t^{a'} = m$ we can write

$$g(rx_t)/x_t^{a'} = \sum_{j=0}^{m} G_j x_t^{m-j} y'^j + \sum_{j=0}^{m+1} G'_j x_t^{m+1-j} y'^j$$

where $G'_j \in R_t$, $G_j \in J$, and $G_j \neq 0$ for some j. Let b be the smallest integer such that $G_b \neq 0$ and let

$$G = \sum_{j=b}^{m} G_j y_k^{j-b} \quad \text{and} \quad G' = \sum_{j=0}^{m+1} G'_j y_k^j.$$

Then $0 \leq b \leq m$, $G' \in R_k$, G is a unit in R_k, and $g(rx_k)/x_k^{a'} = x_k^m(G'x_k + Gy_k^b)$. Consequently $\text{ord}_{x_k R_k} g(rx_k) = m + a'$ and $\text{ord}_{R_k} g(rx_k)/x_k^{m+a'} \leq \text{ord}_{R_k/x_k} g(rx_k)/x_k^{m+a'} = b \leq m$ and hence $\text{ord}_{R_k} g(rx_k)/x_k^n \leq 2m + a' - n$. Since $a' < n$ and $m \leq n/2$ we conclude that $\text{ord}_{R_k} g(rx_k)/x_k^n < n$ and hence $\text{ord}_{R_k} f(0) < n$. Therefore $0 < \text{ord}_{R_k} f(Z) < n$.

LEMMA 2.7 - *Let R be a two dimensional regular local domain with maximal ideal M and let (x, y) be a basis of M. Let $F(Z) = Z^n + F_1 Z^{n-1} + \ldots + F_n$ with $n > 0$ and $F_1, \ldots, F_n$ in R. Assume that there exists an integer u with $0 < u < n$ such that F_u is an R-monomial in x, $\text{ord}_{xR} F_j \geq (j/u)\, \text{ord}_{xR} F_u$ for $1 \leq j \leq u$, and $\text{ord}_{xR} F_j > (j/u)\, \text{ord}_{xR} F_u$ for $u < j \leq n$. Let d be the greatest integer such that $du \leq \text{ord}_{xR} F_u$, and let $f(Z) = f(x^d Z)/x^{nd}$. Then $f(Z) \in R[Z]$ and $0 < \text{ord}_R f(Z) < n$.*

PROOF. - Obvious.

LEMMA 2.8 - *Let w be a valuation of a field K such that R_w/M_w is algebraically closed and let p be the characteristic of R_w/M_w. Let L be a finite normal extension of K such that w does not split in L. If $p = 0$ then let $p' = 1$, and if $p \neq 0$ then let p' be the highest power of p which divides $[L:K]$. Let $q = [L:K]/p'$. Then there exists a unique subfield K' of L such that $K \subset K'$ and $[K':K] = q$. Furthermore K' is a separable normal extension of K and the group of all K-automorphisms of K' is abelian. If w is rational then the group of all K-automorphisms of K' is cyclic.*

PROOF. - Let L' be the maximal separable extension of K in L and let G be the group of all K-automorphisms of L'. Since R_w/M_w is algebraically closed and w does not split in L', by a result of KRULL (see [11] or [21: § 12 of Chapter VI]) there exists a normal subgroup G' of G such that the order of G' is p' and G/G' is isomorphic to a factor group of the value group of w' where w' is the valuation of L' such that $R_{w'}$ is the integral closure of R_w in L' (in [21], G' is called the large ramification group of w' over w). Our assertion follows by taking K' to be the fixed field of G' and noting the following: 1) if $p \neq 0$ and H' is a normal subgroup of a finite group H such that the order of H' is the highest power p^e of p which divides the order of H then H' is the only subgroup of H of order p^e (for instance see [22: Theorem 3 on page 106]); 2) any finite factor group of any subgroup of the additive group of all rational numbers is cyclic (for instance see [3: Proposition 1]).

THEOREM 2.9 - *Let R be a two dimensional regular local domain with maximal ideal M and quotient field K such that R/M is algebraically closed. Let p be the characteristic of R/M. Assume that if $p \neq 0 =$ characteristic of R then K contains a primitive p^{th} root of 1 and a $(p-1)^{th}$ root of p. Let (x, y) be a basis of M and let J be a coefficient set for R. Let w be a rational nondiscrete valuation of K dominating R (by [2: Theorem 1] we know that w is then residually algebraic over R). Let (R_k, x_k, y_k) be the canonical k^{tk} quadratic transform of (R, x, y, J) along w, and let S_k be the quotient ring of R_k with respect to x_kR_k. Let I be the set of all positive integers k for which there exists an integer j with $0 \leq j < k$ such that $w(x_j) = w(y_j)$ and $w(x_i) \leq w(y_i)$ whenever $j < i < k$ (note that I is then an infinite set). For any $t \in I$ let $I(t)$ be the set of all $k \in I$ such that $k \geq t$ (note that for any $t \in I$ and any integer $k \geq t$ we have that x_t is an R_k-monomial in x_k if and only if $k \in I$). Let L be a finite normal extension of K such that w does not split in L. If $p = 0$ then let $p' = 1$, and if $p \neq 0$ then let p' be the highest power of p which divides $[L:K]$. Let $q = [L:K]/p'$. Assume that K contains a primitive q^{th} root of 1. Then we have the following.*

(1) *There exists $t \in I$ such that S_k is totally ramified in L for all $k \in I(t)$.*

(2) *Let K' be as in Lemma 2.8, and let R'_k and S'_k be the integral closures of R_k and S_k in K' respectively. Then the integral closure of R_w in K' is the valuation ring $R_{w'}$ of a rational nondiscrete valuation w' of K', and for all $k \geq 0$ we have that R'_k is a two dimensional local domain, J is a coefficient set for R'_k, R'_k/M'_k is algebraically closed where M'_k is the maximal ideal in R'_k, w' dominates R'_k, and w' is residually algebraic over R'_k. Furthermore there exists $t \in I$ and elements X_k, x'_k, y'_k in R'_k for all $k \in I(t)$ such that $x'_t = X_t$ and $y'_t = y_t$ and such that for all $k \in I(t)$ we have the following: $p \in x_kR_k$, $K' = K(X_k)$, X_k^q/x_k is a unit in R_k, x'_k/X_k is a unit in R'_k, R'_k is regular, $(x'_k, y'_k)R'_k = M'_k = (X_k, y_k)R'_k$, S'_k is the quotient ring of R'_k with respect to $x'_kR'_k$, S_k and S'_k are totally ramified in L, (R'_k, x'_k, y'_k) is a canonical quadratic transform of (R'_t, x'_t, y'_t, J) along w', and X_t is an R'_k-monomial in x'_k.*

(3) *Let $g(Z)$ be a monic polynomial of degree $d>1$ in Z with coefficients in R such that $g(Z)$ is irreducible in $K[Z]$ and $g(z)=0$ for some $z\in L$. Let $f(Z)=g(Z)^e$ where e is a positive integer and let $n=de$. Then $d\equiv 0(p)$ if and only if $p\neq 0$ and $z\notin K'$ where K' is as in Lemma 2·8. Assume that either R is a spot over a pseudogeometric domain, or $d\not\equiv 0(p)$, or the following condition holds: $0\neq p=$ characteristic of R, $d\equiv 0(p)$, and $g(Z)\notin K[Z^m]$ where m is the highest power of p which divides d. Then there exists $t'\in I$ such that for each $k\in I(t')$ there exists $r_k\in R_k$ and nonnegative integers $a(k)$ and $c(k)$ such that $(a(k), c(k))\not\equiv 0(n)$, $c(k)=0$ if $d\not\equiv 0(p)$, $c(k)\leq n/p$ if $d\equiv 0(p)$, and $\operatorname{ord}_{S_k} f(r_k+r_k^*)=a(k)$ and $\operatorname{ord}_{R_k/x_k} f(r_k+r_k^*)/x_k^{a(k)}=c(k)$ for all $r_k^*\in R_k$ with $\operatorname{ord}_{S_k} r_k^*\geq a(k)/n$.*

(4) *Let $f(Z)$ be a monic polynomial of degree $n>0$ in Z with coefficients in R such that $f(Z)=(Z-z_1)\ldots(Z-z_n)$ for some $z_1,\ldots,z_n$ in L. Assume that either R is a spot over a pseudogeometric domain, or $p=0$, or the following condition holds: $0\neq p=$ characteristic of R and if $g(Z)$ is any nonconstant monic irreducible factor of $f(Z)$ in $K[Z]$ such that the degree d of $g(Z)$ is divisible by p then $g(Z)\notin K[Z^m]$ where m is the highest power of p which divides d (note this condition is satisfied if $0\neq p=$ characteristic of R and $f(Z)$ is separable over K). Then either: 1) Z^n is an R-translate of $f(Z)$; or: 2) there exists $t'\in I$, an $R_{t'}$-translate $F(Z)=Z^n+F_1Z^{n-1}+\ldots+F_n$ of $f(Z)$ with $F_1,\ldots,F_n$ in $R_{t'}$, and an integer u with $0<u<n$ such that for all $k\in I(t')$ we have that F_u is an R_k-monomial in x_k, $\operatorname{ord}_{x_kR_k}F_j\geq(j/u)\operatorname{ord}_{x_kR_k}F_u$ for $1\leq j\leq u$, and $\operatorname{ord}_{x_kR_k}F_j>(j/u)\operatorname{ord}_{x_kR_k}F_u$ for $u<j\leq n$; or: 3) there exists $t'\in I$ such that for each $k\in I(t')$ there exists an R_k-translate $F^{(k)}(Z)$ of $f(Z)$ and nonnegative integers $a(k)$ and $c(k)$ such that $F^{(k)}(Z)$ is of prenonsplitting-type relative to $\operatorname{ord}_{x_kR_k}$, $\operatorname{ord}_{x_kR_k}F^{(k)}(0)=a(k)$, $\operatorname{ord}_{R_k/x_k}F^{(k)}(0)/x_k^{a(k)}=c(k)$, $(a(k), c(k))\not\equiv 0(n)$, $c(k)=0$ if the degree of every nonconstant monic irreducible factor of $f(Z)$ in $K[Z]$ is nondivisible by p, and $c(k)\leq n/p$ if the degree of some nonconstant monic irreducible factor of $f(Z)$ in $K[Z]$ is divisible by p (note that in both the cases $c(k)\leq n/2$). Furthermore, if Z^n is not an R-translate of $f(Z)$ then: 4) there exist nonnegative integers i, d, e and an R_i-translate $F(Z)$ of $f(Z)$ such that upon letting $f'(Z)=F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ we have that $M\subset\operatorname{rad}_{R_i} y_i^e R_i$, $f'(Z)\in R_i[Z]$, and $0<\operatorname{ord}_{R_i}f'(Z)<n$.*

PROOF OF (1) AND (2) - Let K' be as in Lemma 2.8 and let R_k' and S_k' be the integral closures of R_k and S_k in K' respectively. By Lemma 2.8, K' is a separable normal extension of K, $[K':K]=q$, and the group of all K-automorphisms of K' is cyclic. Since R/M is algebraically closed and w does not split in L, we get that the integral closure of R_w in K' is the valuation ring $R_{w'}$ of a rational nondiscrete valuation w' of K' and $h(R_{w'})=$ $=h(R_w)$ where h is the canonical epimorphism of $R_{w'}$ onto $R_{w'}/M_{w'}$, and for all $k\geq 0$ we have that R_k' is a two dimensional local domain, J is a coefficient set for R'_k, R'_k/M'_k is algebraically closed where M'_k is the maximal ideal in R'_k, w' dominates R'_k, and w' is residually algebraic over R'_k. Since K contains a primitive q^{th} root of 1, we can find $0 \neq X \in K'$ such that $K'=K(X)$ and $X^q \in R$. By [10: Lemmas 3.7 and 3.12] there exists $u \in I$ such that for all $k \in I(u)$ we have that $p \in x_k R_k$ and $X^q/x_k^{d(k)}$ is a unit in R_k for some nonnegative integer $d(k)$; upon letting $Y_k = X^{q/e(k)}/x_k^{d(k)/e(k)}$ where $e(k)$ is the greatest common divisor of q and $d(k)$ we get that $Y_k \in L$ and $Y_k^{e(k)}$ is a unit in R_w; now $e(k) \not\equiv 0(p)$ and hence by [8: Proposition 22] we deduce that $Y_k \in K$; since $[K':K] = q$, $K' = K(X)$, and $X^q \in K$, we must have $e(k) = 1$; therefore there exist integers $m(k)$ and $m'(k)$ such that $m(k)d(k) + m'(k)q = 1$; upon letting $X_k = X^{m(k)} x_k^{m'(k)}$ we get that $K' = K(X_k)$ and X_k^q/x_k is a unit in R_k and hence by [8: Theorem 6] we get that R'_k is regular and $(X_k, y_k)R'_k = M'_k$; since X_k^q/x_k is a unit in R_k we deduce that S_k is totally ramified in K' and S'_k is the quotient ring of R'_k with respect to $X_k R'_k$. Let (R''_i, x''_i, y''_i) be the canonical i^{th} quadratic transform of (R'_u, X_u, y_u, J) along w'. By [2: Theorem 3], for each $k \in I(u)$ there exists a nonnegative integer $i(k)$ such that $R''_{i(k)} = R'_k$ for all $k \in I(u)$, and $i(k) < i(k')$ for all k and k' in $I(u)$ with $k < k'$. By [10: Theorem 4.23] there exists a nonnegative integer i^* such that S''_i is totally ramified in L for all $i \geq i^*$ where S''_i is the quotient ring of R''_i with respect to $x''_i R''_i$. We can take $t \in I(u)$ such that $i(t) \geq i^*$. Then $S''_{i(k)}$ is totally ramified in L for all $k \in I(t)$. Now X_u^q/x_u is a unit in R_u, X_t^q/x_t a unit in R_t, and x_u is an R_t–monomial in x_t; consequently X_u^q is an R'_t–monomial in X_t and hence X_u/X_t^c is a unit in R'_t for some positive integer c; since $(R'_t, x''_{i(t)}, y''_{i(t)})$ is a canonical quadratic transform of (R'_u, X_u, y_u, J), there exists a positive integer a and a nonnegative integer b such that $X_u/(x''^{a}_{i(t)} y''^{b}_{i(t)})$ is a unit in R'_t; therefore $X_t/x''_{i(t)}$ must be a unit in R'_t. For each $k \in I(t)$ there exists a unique basis (x'_k, y'_k) of M'_k such that (R'_k, x'_k, y'_k) is a canonical quadratic transform of (R'_t, X_t, y_t, J); note that then $x'_t = X_t$ and $y'_t = y_t$. Let k be any element in $I(t)$; now X_t^q/x_t is a unit in R_t, X_k^q/x_k is a unit in R_k, and x_t is an R_k–monomial in x_k; consequently X_t^q is an R'_k–monomial in X_k and hence $X_t/X_k^{c(k)}$ is a unit in R'_k for some positive integer $c(k)$; since (R'_k, x'_k, y'_k) is a canonical quadratic transform of (R'_t, X_t, y_t, J), there exists a positive integer $a(k)$ and a nonnegative integer $b(k)$ such that $X_t/(x'^{a(k)}_k y'^{b(k)}_k)$ is a unit in R'_k; it follows that $b(k) = 0$, X_t is an R'_k–monomial in x'_k, and x'_k/X_k is a unit in R'_k; now $(R'_k, x''_{i(k)}, y''_{i(k)})$ is a canonical quadratic transform of $(R'_t, x''_{i(t)}, y''_{i(t)}, J)$ and hence there exists a positive integer $a'(k)$ and a nonnegative integer $b'(k)$ such that $x''_{i(t)}/(x''^{a'(k)}_{i(k)} y''^{b'(k)}_{i(k)})$ is a unit in R'_k; since $X_t/x''_{i(t)}$ is a unit in R'_t we conclude that $x'_k/x''_{i(k)}$ is a unit in R'_k; since $x'_k/x''_{i(k)}$ and x'_k/X_k are units in R'_k we get that $S''_{i(k)} = S'_k =$ the quotient ring of R'_k with respect to $x'_k R'_k$. Since S_k and $S''_{i(k)}$ are totally ramified in K' and L respectively, we conclude that S_k and S'_k are totally ramified in L.

PROOF OF (3) - Let K', R'_k, S'_k, w', t, X_k, x'_k, y'_k be as in (2). By [10: Lemma 3.7] there exists $t'' \in I(t)$ such that $D_K(g(Z))$ is an R_k-monomial in x_k for all $k \in I(t'')$. Let $m = [L : K'(z)]$ and let $f'(Z)$ be the minimal monic polynomial of z over K'. First suppose that $m = 1$; then $z \in K'$ and hence $d \not\equiv 0(p)$; upon taking $t' = t''$, by Lemma 2.4(1) we get that for each $k \in I(t')$ there exists $r_k \in R_k$ and a positive integer $a(k)$ with $a(k) \not\equiv 0(n)$ such that for all $r_k^* \in R_k$ with $\text{ord}_{S_k} r_k^* \geq a(k)/n$ we have that $f(r_k + r_k^*)/x_k^{a(k)}$ is a unit in R_k and hence $\text{ord}_{S_k} f(r_k + r_k^*) = a(k)$ and $\text{ord}_{R_k/x_k} f(r_k + r_k^*)/x_k^{a(k)} = c(k)$ where $c(k) = 0$. So now assume that $m > 1$. Then $p \neq 0$, $z \notin K'$, $f'(Z)$ is a monic polynomial of degree m in Z with coefficients in R'_0, $f'(Z)$ divides $g(Z)$ in $K'[Z]$, and by the first part of Lemma 2.4(2) we get that m is the highest power of p which divides d, and if $g(Z) \notin K[Z^m]$ then $f'(Z) \neq Z^m + f'(0)$. Hence by assumption, either: R is a spot over a pseudogeometric domain, or: R is of characteristic p and $f'(Z) \neq Z^m + f'(0)$. Therefore upon taking K', w', $f'(Z)$, R'_t, x'_t, y'_t, $\{X_t\}$ respectively for K, w, $f(Z)$, R, x, y, X in [10: Theorem 5.5] we can find $t' \in I(t'')$ such that for each $k \in I(t')$ there exists $r'_k \in R'_k$ and nonnegative $a'(k)$, $b'(k)$, $c'(k)$ such that $\text{ord}_{S'_k} f'(r'_k) = a'(k)$, $\text{ord}_{y'_k R'_k} f'(r'_k) \geq b'(k)$, $\text{ord}_{R'_k/x'_k} f'(r'_k)/(x'^{a'(k)}_k y'^{b'(k)}_k) = c'(k)$, $(a'(k),\ b'(k) + c'(k)) \not\equiv 0(m)$, $c'(k) \leq m/p$, and $X_t \in \text{rad}_{R'_k} y'^{b'(k)}_k$; now X_t is an R'_k-monomial in x'_k and hence we must have $b'(k) = 0$; therefore by Lemma 2.4(2) there exists $r_k \in R_k$ and nonnegative integers $a(k)$ and $c(k)$ such that $(a(k),\ c(k)) \not\equiv 0(n)$ and $c(k) \leq n/p$, and $\text{ord}_{S_k} f(r_k + r_k^*) = a(k)$ and $\text{ord}_{R_k/x_k} f(r_k + r_k^*)/x_k^{a(k)} = c(k)$ for all $r_k^* \in R_k$ with $\text{ord}_{S_k} r_k^* \geq a(k)/n$.

PROOF OF (4) - By Lemmas 2.6 and 2.7 it follows that if either 2) or 3) holds then 4) holds. Therefore it suffices to show that either 1) or 2) or 3) holds. Let $g_1(Z), \ldots, g_v(Z)$ be the distinct nonconstant monic irreducible factors of $f(Z)$ in $K[Z]$. Then $g_1(Z), \ldots, g_v(Z)$ are in $R[Z]$ and there exist positive integers $e(1), \ldots, e(v)$ such that $f(Z) = f_1(Z) \ldots f_v(Z)$ where $f_i(Z) = g_i(Z)^{e(i)}$ for $1 \leq i \leq v$. Let $d(i)$ be the degree of $g_i(Z)$ in Z and let $n(i) = d(i)e(i)$ for $1 \leq i \leq v$. Then $n = n(1) + \ldots + n(v)$. We can relabel the elements $z_1, \ldots, z_n$ so that $g_i(z_i) = 0$ for $1 \leq i \leq v$. For a moment suppose that $d(i) = 1$ for some i; let $F(Z) = f(Z + z_i)$; then $F(Z)$ is an R-translate of $f(Z)$ and $F(Z) = Z^n + F_1 Z^{n-1} + \ldots + F_n$ where $F_1, \ldots, F_n$ are elements in R such that $F_n = 0$; let V be the set of all integers j with $1 \leq j \leq n$ such that $F_j \neq 0$; if V is empty then $F(Z) = Z^n$ and we have nothing to show; so now suppose that V is nonempty; by [10: Lemma 3.7] there exists $t' \in I$ such that F_j is an $R_{t'}$-monomial in $x_{t'}$ for all $j \in V$; let u be the greatest integer in V such that $(1/u)\ \text{ord}_{S_{t'}} F_u = \min_{j \in V} (1/j)\ \text{ord}_{S_{t'}} F_j$; then $0 < u < n$ and for all $k \in I(t')$ we have that F_u is an R_k-monomial in x_k, $\text{ord}_{S_k} F_j \geq (j/u)\ \text{ord}_{S_k} F_u$ for $1 \leq j \leq u$, and $\text{ord}_{S_k} F_j > (j/u)\ \text{ord}_{S_k} F_u$ for $u < j \leq n$. So henceforth we may assume that $d(i) > 1$ for $1 \leq i \leq v$. Now $0 \neq D(g_i(Z),\ g_j(Z)) \in R$ whenever $1 \leq i \leq v$, $1 \leq j \leq v$, and $i \neq j$, and hence by [10: Lemma 3.7] there exists $t'' \in I$ such that $D(g_i(Z), g_j(Z))$ is an R_k-monomial in x_k whenever $k \in I(t'')$, $1 \leq i \leq v$, $1 \leq j \leq v$, and $i \neq j$. By (1) there exists $t \in I(t'')$ such that S_k is totally ramified in L for all $k \in I(t)$. For $1 \leq i \leq v$, by (3) there exists $t_i \in I$ such that for each $k \in I(t_i)$ there exists $r_{ik} \in R_k$ and nonnegative integers $a(i, k)$ and $c(i, k)$ such that: $(a(i, k), c(i, k)) \not\equiv 0(n(i))$, $c(i, k) = 0$ if $d(i) \not\equiv 0(p)$, $c(i, k) \leq n(i)/p$ if $d(i) \equiv 0(p)$, and $\mathrm{ord}_{S_k} f_i(r_{ik} + r^*_{ik}) = a(i, k)$ and $\mathrm{ord}_{R_k/x_k} f_i(r_{ik} + r^*_{ik})/x_k^{a(i,k)} = c(i, k)$ for all $r^*_{ik} \in R_k$ with $\mathrm{ord}_{S_k} r^*_{ik} \geq a(i, k)/n(i)$. First suppose that there exists $T \in I$, an R_T-translate $F(Z) = Z^n + F_1 Z^{n-1} + \ldots + F_n$ of $f(Z)$ with $F_1, \ldots, F_n$ in R_T, and an integer u with $0 < u < n$ such that F_u is an R_T-monomial in x_T, $\mathrm{ord}_{S_T} F_j \geq (j/u)\, \mathrm{ord}_{S_T} F_u$ for $1 \leq j \leq u$, and $\mathrm{ord}_{S_T} F_j > (j/u)\, \mathrm{ord}_{S_T} F_u$ for $u < j \leq n$; then for all $k \in I(T)$ we have that F_u is an R_k-monomial in x_k, $\mathrm{ord}_{S_k} F_j \geq (j/u)\, \mathrm{ord}_{S_k} F_u$ for $1 \leq j \leq u$, and $\mathrm{ord}_{S_k} F_j > (j/u)\, \mathrm{ord}_{S_k} F_u$ for $u < j \leq n$; and hence it suffices to take $t' = T$. So henceforth we may also assume that if k is any element in I, $F(Z) = Z^n + F_1 Z^{n-1} + \ldots + F_n$ is any R_k-translate of $f(Z)$ with $F_1, \ldots, F_n$ in R_k, and u is any integer with $0 < u < n$ such that F_u is an R_k-monomial in x_k and $\mathrm{ord}_{S_k} F_j \geq (j/u)\, \mathrm{ord}_{S_k} F_u$ for $1 \leq j \leq u$, then $\mathrm{ord}_{S_k} F_j \leq (j/u)\, \mathrm{ord}_{S_k} F_u$ for some j with $u < j \leq n$. Let $t' = \max(t, t_1, \ldots, t_v)$. For any $k \in I(t')$, by Lemma 2.5 there exists an R_k-translate $F^{(k)}(Z)$ of $f(Z)$ and nonnegative integers $a(k)$ and $c(k)$ such that $F^{(k)}(Z)$ is of prenonsplitting-type relative to ord_{S_k}, $(a(k), c(k)) \not\equiv 0(n)$, $c(k) \leq c(1, k) + \ldots + c(v, k)$, $\mathrm{ord}_{S_k} F^{(k)}(0) = a(k)$, and $\mathrm{ord}_{R_k/x_k} F^{(k)}(0)/x_k^{a(k)} = c(k)$; it follows that $c(k) = 0$ if $d(i) \not\equiv 0(p)$ for $1 \leq i \leq v$, i.e., if the degree of every nonconstant monic irreducible factor of $f(Z)$ in $K[Z]$ is nondivisible by p, and $c(k) \leq n/p$ if $d(i) \equiv 0(p)$ for some i, i.e., if the degree of some nonconstant monic irreducible factor of $f(Z)$ in $K[Z]$ is divisible by p.

THEOREM 2.10 - *Let R be a two dimensional regular local domain with maximal ideal M such that R/M is algebraically closed. Let p be the characteristic of R/M. Assume that if $p \neq 0 =$ characteristic of R then R contains a primitive p^{th} root of 1 and a $(p-1)^{th}$ root of p. Let (x, y) be a basis of M and let J be a coefficient set for R. Let w be a rational nondiscrete valuation of K dominating R (by [2: Theorem 1] we know that w is then residually algebraic over R). Let (R_i, x_i, y_i) be the canonical i^{th} quadratic transform of (R, x, y, J) along w. Let R^*_i be the completion R_i. Let $f(Z)$ be a monic polynomial of degree $n > 0$ in Z with coefficients in R. Then we have the following.*

(1) *There exists a nonnegative integer i such that either: Z^n is an R^*_k-translate of $f(Z)$ for all $k \geq i$; or: there exist nonnegative integers d and e and an R^*_i-translate $F(Z)$ of $f(Z)$ such that upon letting $g(Z) = F(x_i^d y_i^e)/(x_i^d y_i^e)^n$ we have that $M \subset \mathrm{rad}_{R_i} y_i^e R_i$, $g(Z) \in R^*_i[Z]$, and $0 < \mathrm{ord}_{R^*_i} g(Z) < n$.*

(2) *Let I be the set of all positive integers k for which there exists an integer j with $0 \leq j < k$ such that $w(x_j) = w(y_j)$ and $w(x_i) \leq w(y_i)$ whenever*

$j < i < k$ (note that I is then an infinite set). For any $t \in I$ let $I(t)$ be the set of all $k \in I$ such that $k \geq t$ (note that for any $t \in I$ and any integer $k \geq t$ we have that x_t is an R_k-monomial in x_k if and only if $k \in I$). Then either: 1) there exists a nonnegative integer i such that Z^n is an R_k^*-translate of $f(Z)$ for all $k \geq i$; or: 2) there exists $t \in I$ and an integer u with $0 < u < n$ such that for each $k \in I(t)$ there exists an R_k^*-translate $F^{(k)}(Z) = Z^n + F_1^{(k)} Z^{n-1} + \ldots + F_n^{(k)}$ of $f(Z)$ with $F_1^{(k)}, \ldots, F_n^{(k)}$ in R_k^* such that $F_u^{(k)}$ is an R_k^*-monomial in x_k, $\operatorname{ord}_{x_k R_k^*} F_j^{(k)} \geq \geq (j/u) \operatorname{ord}_{x_k R_k^*} F_u^{(k)}$ for $1 \leq j \leq u$, and $\operatorname{ord}_{x_k R_k^*} F_j^{(k)} > (j/u) \operatorname{ord}_{x_k R_k^*} F_u^{(k)}$ for $u < j \leq n$; or: 3) there exists $t \in I$ such that for each $k \in I(t)$ there exists an R_k^*-translate $F^{(k)}(Z)$ of $f(Z)$ and nonnegative integers $a(k)$ and $c(k)$ such that $F^{(k)}(Z)$ is of prenonsplitting-type relative to $\operatorname{ord}_{x_k R_k^*}$, $\operatorname{ord}_{x_k R_k^*} F^{(k)}(0) = a(k)$, $\operatorname{ord}_{R_k^*/x_k} F^{(k)}(0)/x_k^{a(k)} = c(k)$, $(a(k), c(k)) \not\equiv 0(n)$, $c(k) = 0$ if $p = 0$, and $c(k) \leq n/p$ if $p \neq 0$ (note that in both the cases $c(k) \leq n/2$).

PROOF. - Let $R'' = R_0^*$ and let K'' be the quotient field of R''. By [5: Proposition 1], for each nonnegative integer i there exists a unique two dimensional regular local domain R_i'' such that R_i'' is an i^{th} quadratic transform of R'' and $K \cap R_i'' = R_i$. For each $i \geq 0$ let M_i and M_i'' be the maximal ideals in R_i and R_i'' respectively, and let $R_i''^*$ be the completion of R_i''. Then by [5: Proposition 1], for each $i \geq 0$ we have that $R_i'' \subset R_{i+1}''$, $K \cap M_i'' = M_i$, $M_i R_i'' = M_i''$, and there exists an isomorphism h_i'' of $R_i''^*$ onto R_i^* such that $h_i''(s) = s$ for all $s \in R_i$. By Lemma 1.3, $\bigcup_{i=0}^{\infty} R_i''$ is the valuation ring $R_{w''}$ of a valuation w'' of K'' such that w'' dominates R_i'' and w'' is residually algebraic over R_i'' for all $i \geq 0$. It follows that (R_i'', x_i, y_i) is the canonical i^{th} quadratic transform of (R'', x, y, J) along w'' for all $i \geq 0$. Since w is rational nondiscrete, by Lemma 1.2(9) we deduce that w'' is rational nondiscrete. We can take a finite normal extension L of K'' such that $f(Z) = (Z - z_1) \ldots (Z - z_n)$ for some $z_1, \ldots, z_n$ in L. Let L' be the maximal separable extension of K'' in L. We can take a valuation W of L' such that $K'' \cap R_W = R_{w''}$. Let K' be the splitting field of W over w''. Then $K' \cap R_W$ is the valuation ring $R_{w'}$ of a rational nondiscrete valuation w' of K' such that $K'' \cap R_{w'} = R_{w''}$. By [4: Proposition 1.46] we get that w' does not split in L'. Since L is a purely inseparable exension of L' we deduce that w' does not split in L. By [9: Lemma 14] there exists a nonnegative integer b such that upon letting $T' =$ the integral closure of R_b'' in L', $P' = M_W \cap T'$, and $Q = T'_{P'}$ we have that K' is the splitting field of Q over R_b''. Therefore upon letting $T =$ the integral closure of R_b'' in K', $P = M_{w'} \cap T$, $R' = T_P$, and $M' = PR'$, by [4: § 3 and Theorem 1.47] we get that R' is a two dimensional local domain with quotient field K', M' is the maximal ideal in R', R'/M' is algebraically closed, w' dominates R', w' is residually algebraic over R', R' dominates R_b'', $M_b'' R' = M'$, and $H(R') = H(R_b'')$ where H is the canonical epimorphism of R' onto R'/M'. In particular

$(x_b, y_b)R' = M'$ and hence R' is regular. For each $i \geq b$ let R'_i be the $(i-b)^{th}$ quadratic transform of R' along w', let M'_i be the maximal ideal in R'_i, and let R'^*_i be the completion of R'_i. Since $K'' \cap R_{w'} = R_{w''}$, it follows that (R'_i, x_i, y_i) is the canonical $(i-b)^{th}$ quadratic transform of (R', x_b, y_b, J) along w' for all $i \geq b$. Now R'_i is the quotient ring of $R'_{i-1}[x_i, y_i]$ with respect to $(R'_{i-1}[x_i, y_i]) \cap M_{w'}$ for all $i > b$; therefore R'_i is the quotient ring of $R'[x_{b+1}, y_{b+1}, \ldots, x_i, y_i]$ with respect to $(R'[x_{b+1}, y_{b+1}, \ldots, x_i, y_i]) \cap M_{w'}$ for all $i > b$; clearly $R'[x_{b+1}, y_{b+1}, \ldots, x_i, y_i] = R'[x_i, y_i]$ and hence R'_i is the quotient ring of $R'[x_i, y_i]$ with respect to $(R'[x_i, y_i]) \cap M_{w'}$ for all $i > b$. Similarly R''_i is the quotient ring of $R''_b[x_i, y_i]$ with respect to $(R''_b[x_i, y_i]) \cap M_{w''}$ for all $i > b$. Now $M_{w''} = K'' \cap M_{w'}$ and hence we deduce that R'_i dominates R''_i for all by $i \geq b$. Also then for each $i \geq b$ we clearly have that $M''_i R'_i = M'_i$ and $H_i(R'_i) = H_i(R''_i)$ where H_i is the canonical epimorphism of R'_i onto R'_i/M'_i. Therefore for each $i \geq b$, by [5: Lemma 2] there exists an isomorphism h'_i of R'^*_i onto R''^*_i such that $h'_i(s) = s$ for all $s \in R''_i$. Thus for each $i \geq b$, upon letting $h_i(s) = h''_i(h'_i(s))$ for all $s \in R'^*_i$, we get an isomorphism h_i of R'^*_i onto R^*_i such that $h_i(s) = s$ for all $s \in R_i$. If Z^n is an R'-translate of $f(Z)$ then $Z^n = f(Z + r')$ for some $r' \in R'$, and hence for each $k \geq b$ we get that $f(Z + h_k(r'))$ is an R^*_k-translate of $f(Z)$ and $Z^n = f(Z + h_k(r'))$. Therefore we have nothing to show if Z^n is an R'-translate of $f(Z)$. Henceforth assume that Z^n is not an R'-translate of $f(Z)$. Since R'' is complete and R''/M'' is an algebraically closed field of characteristic p where M'' is the maximal ideal in R'', for any positive integer q with $q \not\equiv 0(p)$, by HENSEL's lemma we get that $Z^q - 1 = (Z - s_1) \ldots (Z - s_q)$ with $s_1, \ldots, s_q$ in R''; consequently R'' contains a primitive q^{th} root of 1 and hence so does R'. Again since R'' is complete, by [12: (32.1)] we know that R'' is pseudogeometric. Clearly R' is a spot over R''. Therefore by Theorem 2.9(4) there exist nonnegative integers i, d, e with $i \geq b$ and an element r in R'_i such that upon letting $f'(Z) = f(x_i^d y_i^e Z + r)/(x_i^d y_i^e)^n$ we have that $M' \subset \mathrm{rad}_{R'_i} y_i^e R'_i$, $f'(Z) \in R'_i[Z]$, and $0 < \mathrm{ord}_{R'_i} f'(Z) < n$; let $F(Z) = f(Z + h_i(r))$ and $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$; then $M \subset \mathrm{rad}_{R_i} y_i^e R_i$, $F(Z)$ is an R^*_i-translate of $f(Z)$, $g(Z) \in R^*_i[Z]$, and $0 < \mathrm{ord}_{R^*_i} g(Z) < n$. This completes the proof of (1). To prove (2) let I' be the set of all integers $k > b$ for which there exists an integer j with $b \leq j < k$ such that $w'(x_j) = w'(y_j)$ and $w'(x_i) \leq w'(y_i)$ whenever $j < i < k$. It follows that $I' \subset I$, and if t and k are any integers such that $t \in I'$ and $k \in I(t)$ then $k \in I'$. Therefore by Theorem 2.9(4) we get that: either 2′) there exists $t \in I$ with $t \geq b$ and an integer u with $0 < u < n$ such that for each $k \in I(t)$ there exists $r_k \in R'_k$ such that upon letting $F'^{(k)}(Z) = f(Z + r_k) = Z^n + F_1'^{(k)} Z^{n-1} + \ldots + F_n'^{(k)}$ with $F_1'^{(k)}, \ldots, F_n'^{(k)}$ in R'_k we have that $F_u'^{(k)}$ is an R'_k-monomial in x_k, $\mathrm{ord}_{x_k R'_k} F_j'^{(k)} \geq (j/u)\, \mathrm{ord}_{x_k R'_k} F_u'^{(k)}$ for $1 \leq j \leq u$, and $\mathrm{ord}_{x_k R'_k} F_j'^{(k)} > (j/u)\, \mathrm{ord}_{x_k R'_k} F_u'^{(k)}$ for $u < j \leq n$; or 3′) there exists $t \in I$ with $t \geq b$ such that for each $k \in I(t)$ there exists $r_k \in R'_k$ and nonnegative integers

$a(k)$ and $c(k)$ such that upon letting $F'^{(k)}(Z) = f(Z + r_k)$ we have that $F'^{(k)}(Z)$ is of prenonsplitting-type relative to $\operatorname{ord}_{x_k R'_k}$, $\operatorname{ord}_{x_k R'_k} F'^{(k)}(0) = a(k)$, $\operatorname{ord}_{R'_k/x_k} F'^{(k)}(0)/x_k^{a(k)} = c(k)$, $(a(k), c(k)) \equiv\mid\equiv 0(n)$, $c(k) = 0$ if $p = 0$, and $c(k) \leq n/p$ if $p \neq 0$. If 2′) holds then upon letting $F^{(k)}(Z) = f(Z + h_k(r_k)) = Z^n + F_1^{(k)} Z^{n-1} + \ldots + F_n^{(k)}$ with $F_1^{(k)}, \ldots, F_n^{(k)}$ in R_k^* we get that $F^{(k)}(Z)$ is an R_k^*-translate of $f(Z)$, $F_u^{(k)}$ is an R_k^*-monomial in x_k, $\operatorname{ord}_{x_k R_k^*} F_j^{(k)} \geq (j/u) \operatorname{ord}_{x_k R_k^*} F_u^{(k)}$ for $1 \leq j \leq u$, and $\operatorname{ord}_{x_k R_k^*} F_j^{(k)} > (j/u) \operatorname{ord}_{x_k R_k^*} F_u^{(k)}$ for $u < j \leq n$. If 3′) holds then upon letting $F^{(k)}(Z) = f(Z + h_k(r_k))$ we get that $F^{(k)}(Z)$ is an R_k^*-translate of $f(Z)$, $F^{(k)}(Z)$ is of prenonsplitting-type relative to $\operatorname{ord}_{x_k R_k^*}$, $\operatorname{ord}_{x_k R_k^*} F^{(k)}(0) = a(k)$, and $\operatorname{ord}_{R_k^*/x_k} F^{(k)}(0)/x_k^{a(k)} = c(k)$. This completes the proof of (2).

§ 3 - Nonrational valuations.

DEFINITION 3.1 - By N we denote the set of all nonnegative integers, and by N^q we denote the set of all q-tuples $b = (b(1), \ldots, b(q))$ of nonnegative integers. Let R be a q dimensional regular local domain, let $(X_1, \ldots, X_q)$ be a basis of the maximal ideal in R, let J be a coefficient set for R, and let $y \in R$; then there exists a unique $y(b) \in J$ for all $b \in N^q$ such that $y = \Sigma y(b) X_1^{b(1)} \ldots X_q^{b(q)}$ in the completion of R where the sum is over N^q; the expression $\Sigma y(b) X_1^{b(1)} \ldots X_q^{b(q)}$ is called the expansion of y in $J[[X_1, \ldots, X_q]]$.

LEMMA 3.2 - *Let $e_1, \ldots, e_q$ be a finite number of positive elements in an ordered abelian group G. Let v be the map of N^q into G given by taking $v(b) = b(1)e_1 + \ldots + b(q)e_q$ for all $b \in N^q$. Then we have the following.*

(1) *Let V be any nonempty subset of N^q. Then there exists $a \in V$ such that $v(a) \leq v(b)$ for all $b \in V$; (note that if $e_1, \ldots, e_q$ are rationally independent then a is uniquely determined by V, and moreover $v(a) < v(b)$ for all $b \in V$ with $b \neq a$).*

(2) *Assume that $v(N^q)$ is an infinite set, and for $1 \leq j \leq q$ and $1 \leq k \leq q$ there exists a positive integer $m(j, k)$ such that $m(j, k) e_k \geq e_j$. Then there exists a unique one-to-one order-preserving map of N onto $v(N^q)$.*

(3) *Assume that $e_1, \ldots, e_q$ are rationally independent, and for $1 \leq j \leq q$ and $1 \leq k \leq q$ there exists a positive integer $m(j, k)$ such that $m(j, k) e_k \geq e_j$. Then there exists a unique one-to-one map u of N onto N^q such that $v(u(j)) < v(u(k))$ for all j and k in N with $j < k$.*

PROOF OF (1) - We make induction on q. The assertion being trivial for $q = 1$, let $q > 1$ and assume that the assertion is true for all values of q smaller than the given one. Relabel $e_1, \ldots, e_q$ so that $e_i \leq e_q$ for $1 \leq i \leq q$.

Fix $d \in V$ and let $n = d(1) + \ldots + d(q)$. Let V' be the set of all $b \in V$ such that $v(b) \leq v(d)$. For every nonnegative integer j let V_j be the set of all $b \in V'$ such that $b(q) = j$. Let W be the set of all nonnegative integers j such that $j \leq n$ and V_j is nonempty. Then W is a finite nonempty set and $V' = \bigcup_{j \in W} V_j$. For each $j \in W$, by the induction hypothesis, there exists $a_j \in V_j$ such that $a_j(1)e_1 + \ldots + a_j(q-1)e_{q-1} \leq b(1)e_1 + \ldots + b(q-1)e_{q-1}$ for all $b \in V_j$. For each $j \in W$, we then have that $v(a_j) \leq v(b)$ for all $b \in V_j$. Clearly there exists $k \in W$ such that $v(a_k) \leq v(a_j)$ for all $j \in W$. Let $a = a_k$. Then $a \in V$ and $v(a) \leq v(b)$ for all $b \in V'$, and hence $v(a) \leq v(b)$ for all $b \in V$.

PROOF OF (2) – The uniqueness follows from the fact that the identity map of N onto itself is the only one-to-one order-preserving map of N onto itself. To prove the existence, relabel $e_1, \ldots, e_q$ so that $e_1 \leq e_i \leq e_q$ for $1 \leq i \leq q$. By assumption there exists a positive integer m such that $e_q \leq me_1$. For any a and b in N^q with $v(b) \leq v(a)$ we have that $e_1(b(1) + \ldots + b(q)) \leq v(b) \leq v(a) \leq$ $\leq e_q(a(1) + \ldots + a(q)) \leq me_1(a(1) + \ldots + a(q))$ and hence $b(1) + \ldots + b(q) \leq$ $\leq m(a(1) \ldots + a(q))$. Consequently, for any $a \in N^q$ upon letting M_a be the set of all $b \in N^q$ with $v(b) < v(a)$ we get that M_a is a finite set. Therefore, for any $a' \in v(N^q)$ upon letting $M'_{a'}$ be the set of all $b' \in v(N^q)$ with $b' < a'$ we get that $M'_{a'}$ is a finite set; let $p(a')$ be the number of elements in $M'_{a'}$. Then p is a one-to-one order-preserving map of $v(N^q)$ onto N. Therefore p^{-1} is a one-to-one order-preserving map of N onto $v(N^q)$.

PROOF OF (3) – Now $v(a) \neq v(b)$ for all a and b in N^q with $a \neq b$, and hence our assertion follows from (2).

LEMMA 3.3 – *Let w be a valuation of a field K and let $X_1, \ldots, X_q$ be a finite number of nonzero elements in M_w. Then we have the following.*

(1) *Given any nonempty subset V of N^q there exists $a \in V$ such that $w(X_1^{a(1)} \ldots X_q^{a(q)}) \leq w(X_1^{b(1)} \ldots X_q^{b(q)})$ for all $b \in V$; (note that if $w(X_1), \ldots, w(X_q)$ are rationally independent then a is uniquely determined by V, and moreover $w(X_1^{a(1)} \ldots X_q^{a(q)}) < w(X_1^{b(1)} \ldots X_q^{b(q)})$ for all $b \in V$ with $b \neq a$).*

(2) *Let V be the set of all elements v in the value group of w such that $v = w(X_1^{b(1)} \ldots X_q^{b(q)})$ for some $b \in N^q$. Assume that V is an infinite set, and for $1 \leq j \leq q$ and $1 \leq k \leq q$ there exists a positive integer $m(j, k)$ such that $w(X_k^{m(j,k)}) \geq w(X_j)$. Then there exists a unique one-to-one order-preserving map of N onto V.*

(3) *Let V be the set of all $X \in K$ such that $X = X_1^{b(1)} \ldots X_q^{b(q)}$ for some $b \in N^q$. Assume that $w(X_1), \ldots, w(X_q)$ are rationally independent, and for $1 \leq j \leq q$ and $1 \leq k \leq q$ there exists a positive integer $m(j, k)$ such that $w(X_k^{m(j,k)}) \geq w(X_j)$. Then there exists a unique one-to-one map H of N onto V such that $w(H(j)) < w(H(k))$ for all j and k in N with $j < k$.*

PROOF. - Follows from Lemma 3.2 by taking $e_1 = w(X_1), \ldots, e_q = w(X\ )$.

LEMMA 3.4 - *Let R be a local domain such that the completion R^* of R is a domain. Let $X_1, \ldots, X_q$ be a finite number of nonzero nonunits in R. Let w be a valuation of the quotient field K of R such that w dominates R and $w(X_1), \ldots, w(X_q)$ are rationally independent. Let $y \in R$, let V be a nonempty subset of N^q, and for each $b \in V$ let $y(b)$ be a unit in R such that $y = \sum_{b\in V} y(b) X_1^{b(1)} \ldots X_q^{b(q)}$ in R^*. Let $a \in V$ be as in Lemma 3.3(1). Then $w(y) = w(X_1^{a(1)} \ldots X_q^{a(q)})$.*

PROOF. - We make induction on q. If $q = 1$ then $y/X_1^{a(1)}$ is a unit in R and hence $w(y) = w(X_1^{a(1)})$. Now let $q > 1$ and assume that the assertion is true for all values of q smaller than the given one. By [1: Lemma 13] there exists a valuation w^* of the quotient field of R^* such that w^* dominates R^* and $R_w = K \cap R_{w^*}$. Then $w^*(X_1), \ldots, w^*(X_q)$ are rationally independent. Relabel $X_1, \ldots, X_q$ so that $w^*(X_i) \leq w^*(X_q)$ for $1 \leq i \leq q$. Let $n = a(1) + \ldots + a(q)$. For every nonnegative integer j let V_j be the set of all $b \in V$ such that $b(q) = j$. Let W be the set of all nonnegative integers j such that $j \leq n$ and V_j is nonempty. Then W is a finite nonempty set. For each $j \in W$, by Lemma 3.3(1) there exists a unique $a_j \in V_j$ such that $w^*(X_1^{a_j(1)} \ldots X_q^{a_j(q)}) < w^*(X_1^{b(1)} \ldots X_q^{b(q)})$ for all $b \in V_j$ with $b \neq a_j$. Clearly there exists a unique $k \in W$ such that $a = a_k$. For each $j \in W$, upon letting

$$y_j = \sum_{b \in V_j} y(b) X_1^{b(1)} \ldots X_q^{b(q)} \in R^*,$$

by the induction hypothesis we get that $w^*(y_j) = w^*(X_1^{a_j(1)} \ldots X_q^{a_j(q)})$. Consequently $w^*(y_k) = w^*(X_1^{a(1)} \ldots X_q^{a(q)}) < w^*(y_j)$ for all $j \in W$ with $j \neq k$. Therefore upon letting $y' = \sum_{j \in W} y_j \in R^*$ we get that $w^*(y') = w^*(X_1^{a(1)} \ldots X_q^{a(q)})$. Clearly $(y - y')/X_q^{n+1} \in R^*$ and hence $w^*(y - y') > w^*(X_q^n) \geq w^*(X_1^{a(1)} \ldots X_q^{a(q)})$. Therefore $w^*(y) = w^*(X_1^{a(1)} \ldots X_q^{a(q)})$ and hence $w(y) = w(X_1^{a(1)} \ldots X_q^{a(q)})$.

LEMMA 3.5 - *Let R be a q dimensional regular local domain with maximal ideal M, let $(X_1, \ldots, X_q)$ be a basis of M, let J be a coefficient set for R, and let w be a valuation of the quotient field K of R such that w dominates R and $w(X_1), \ldots, w(X_q)$ are rationally independent. For any $0 \neq y \in R$ let $\Sigma y(b) X_1^{b(1)} \ldots X_q^{b(q)}$ be the expansion of y in $J[[X_1, \ldots, X_q]]$, let V be the set of all $b \in N^q$ such that $y(b) \neq 0$, and let $a \in V$ be as in Lemma 3.3(1); then $w(y) = w(X_1^{a(1)} \ldots X_q^{a(q)})$. Moreover, w is residually rational over R and $(w(X_1), \ldots, w(X_q))$ is a free basis (as a module over the ring of integers) of the value group of w.*

Proof. – By Lemma 3.4 we get that $w(y) = w(X_1^{a(1)} \dots X_q^{a(q)})$. Given any $0 \neq x \in K$ there exist nonzero elements y' and y'' in R such that $x = y'/y''$. Let $\Sigma y'(b) X_1^{b(1)} \dots X_q^{b(q)}$ and $\Sigma y''(b) X_1^{b(1)} \dots X_q^{b(q)}$ be the expansions of y' and y'' in $J[[X_1, \dots, X_q]]$ respectively. By Lemma 3.3(1) there exist unique elements a' and a'' in N^q such that $y'(a') \neq 0 \neq y''(a'')$, $w(X_1^{a'(1)} \dots X_q^{a'(q)}) < w(X_1^{b(1)} \dots X_q^{b(q)})$ for all $b \in N^q$ with $y'(b) \neq 0$ and $b \neq a'$, and $w(X_1^{a''(1)} \dots X_q^{a''(q)}) < w(X_1^{b(1)} \dots X_q^{b(q)})$ for all $b \in N^q$ with $y''(b) \neq 0$ and $b \neq a''$. By Lemma 3.4 we get that $w(y') = w(X_1^{a'(1)} \dots X_q^{a'(q)})$ and $w(y'') = w(X_1^{a''(1)} \dots X_q^{a''(q)})$. Therefore $w(x) = w(X_1^{a'(1)-a''(1)} \dots X_q^{a'(q)-a''(q)})$. This shows that $(w(X_1), \dots, w(X_q))$ is a free basis of the value group of w. Now suppose that x is a unit in R_w. Then $a'' = a'$. Let $z = X_1^{a'(1)} \dots X_q^{a'(q)}$, $z' = y' - y'(a')z$, and $z'' = y'' - y''(a')z$. Then $w(y'') = w(z)$ and by Lemma 3.4 we get that $w(z') > w(z) < w(z'')$. Now $y'(a')/y''(a')$ is a unit in R; also $x - (y'(a')/y''(a')) = (y''(a')z' - y'(a')z'')/(y''(a')y'')$ and hence $w(x - (y'(a')/y''(a'))) > 0$. This show that w is residually rational over R.

Lemma 3.6 – *Let R be a q dimensional regular local domain with maximal ideal M such that R/M is algebraically closed. Let $(X_1, \dots, X_q)$ be a basis of M, let J be a coefficient set for R, and let w be a valuation of the quotient field K of R such that w dominates R and $w(X_1), \dots, w(X_q)$ are rationally independent. Let $f(Z)$ be a monic polynomial of degree $n > 0$ in Z with coefficients in R. Then we have the following.*

(1) *Assume that $f(Z)$ is of prenonsplitting-type relative to w and let $0 \neq X \in K$ such that $w(f(0)) \geq w(X^n)$. Then there exists $r \in J$ such that $w(f(rX)) > w(X^n)$. Furthermore, if $w(f(0)) = w(X^n)$ then $r \neq 0$.*

(2) *Assume that w is real, every R-translate of $f(Z)$ is of prenonsplitting-type relative to w, and for each $r \in R$ we have that either $f(r) = 0$ or $w(f(r)) = w((X_1^{a(1)} \dots X_q^{a(q)})^n)$ for some $a \in N^q$. Then $f(Z) = (Z - z)^n$ for some $z \in R^*$ where R^* is the completion of R.*

(3) *Assume that R is complete, every R-translate of $f(Z)$ is of prenonsplitting-type relative to w, and for each $r \in R$ we have that either $f(r) = 0$ or $w(f(r)) = w((X_1^{a(1)} \dots X_q^{a(q)})^n)$ for some $a \in N^q$. Then $f(z) = 0$ for some $z \in R$.*

(4) *Assume that R is complete, Z^n is not an R-translate of $f(Z)$, and every R-translate of $f(Z)$ is of prenonsplitting-type relative to w. Then $n > 1$, $f(z) \neq 0$ for all $z \in R$, and there exists an R-translate $F(Z)$ of $f(Z)$ such that $w(F(0)) = w(X_1^{a(1)} \dots X_q^{a(q)})$ for some $a \in N^q$ with $a \not\equiv 0(n)$.*

Proof of (1) – Let $g(Z) = f(XZ)/X^n$. Then $g(Z)$ is a monic polynomial of degree n in Z with coefficients in R_w. By Lemma 3.5, w is residually rational over R and hence R_w/M_w is algebraically closed and J is a coefficient set for R_w. Therefore there exists $r \in J$ such that $g(r) \in M_w$. Since $f(rX)/X^n = g(r)$

we get that $w(f(rX)) > w(X^n)$. If $w(f(0)) = w(X^n)$ then $g(0) = f(0)/X^n \notin M_w$ and hence $r \neq 0$.

PROOF OF (2) - Let V be the set of all monomials $X_1^{b(1)} \dots X_q^{b(q)}$ with $b \in N^q$. Since w is real, by Lemma 3.3(3) there exists a unique one-to-one map H of N onto V such that $w(H(j)) < w(H(k))$ for all j and k in N with $j < k$. Since R/M is algebraically closed there exists $r_0 \in J$ such that $f(r_0) \in M$; by assumption either $f(r_0) = 0$ or $w(f(r_0)) = w(X^n)$ for some $X \in V$; since $f(r_0) \in M$ and $H(0) = 1$ we get that $w(f(r_0 H(0))) \geq w(H(1)^n)$. For $k \in N$ with $k \neq 0$ suppose we have defined $r_j \in J$ for $0 < j < k$ such that $w(f(r_0 H(0) + \dots + r_j H(j))) \geq w(H(j+1)^n)$ for $0 < j < k$; let $F(Z) = f(Z + r_0 H(0) + \dots + r_{k-1} H(k-1))$; then $F(0) = f(r_0 H(0) + \dots + r_{k-1} H(k-1))$ and hence $w(F(0)) \geq w(H(k)^n)$; since $F(Z)$ is an R-translate of $f(Z)$, by assumption we know that $F(Z)$ is of prenonsplitting-type relative to w and hence by (1) there exists $r_k \in J$ such that $w(F(r_k H(k))) > w(H(k)^n)$; then $w(f(r_0 H(0) + \dots + r_k H(k))) > w(H(k)^n)$, and by assumption either $f(r_0 H(0) + \dots + r_k H(k)) = 0$ or $w(f(r_0 H(0) + \dots + r_k H(k))) = w(X'^n)$ for some $X' \in V$; therefore we must have $w(r_0 H(0) + \dots + r_k H(k)) \geq w(H(k+1)^n)$. Thus by induction we have defined $r_k \in J$ for all $k \in N$ such that upon letting $z_k = r_0 H(0) + \dots + r_k H(k)$ we have that $w(f(z_k)) \geq w(H(k+1)^n)$ for all $k \in N$. For each $u \in N$ there exists $v(u) \in N$ such that $H(k) \in M^{*u}$ for all $k \in N$ with $k \geq v(u)$ where M^* is the maximal ideal in R^*. Therefore there exists a unique $z \in R^*$ such that $z - z_k \in M^{*u}$ for all k and u in N with $k \geq v(u)$. By [1: Lemma 13] there exists a valuation w^* of the quotient field of R^* such that w^* dominates R^* and $R_w = K \cap R_{w^*}$. Since $R_w = K \cap R_{w^*}$ we get that $w^*(f(z_k)) \geq w^*(H(k+1)^n)$ for all $k \in N$, and hence $w^*(f(z_k)) \geq w^*(H(k))$ for all $k \in N$. Since w is real and $R_w = K \cap R_{w^*}$, for each $j \in N$ there exists $p(j) \in N$ such that $w^*(y) \geq w^*(H(j))$ for all $y \in M^{*p(j)}$; hence for each $j \in N$ there exists $c(j) \in N$ such that $w^*(z - z_k) \geq w^*(H(j))$ for all $k \in N$ with $k \geq c(j)$. Now $f(z) - f(z_k) \in (z - z_k)R^*$ for all $k \in N$, and hence $w^*(f(z) - f(z_k)) \geq w^*(H(j))$ for all k and j in N with $k \geq c(j)$. Also note that $w^*(X_1), \dots, w^*(X_q)$ are rationally independent. Suppose if possible $f(z) \neq 0$. Then by Lemma 3.5 there exists $t \in N$ such that $w^*(f(z)) = w^*(H(t))$. Let $a = 1 + t + c(t+1)$. Then $w^*(f(z) - f(z_a)) \geq w^*(H(t+1))$ and $w^*(f(z_a)) \geq w^*(H(t+1))$, and hence $w^*(f(z)) \geq w^*(H(t+1))$. This is a contradiction because $w^*(f(z)) = w^*(H(t))$. Therefore $f(z) = 0$. Let $g(Z) = f(Z + z) = Z^n + g_1 Z^{n-1} + \dots + g_n$ with $g_i \in R^*$. Then $g_n = g(0) = f(z) = 0$. Suppose if possible that $g_i \neq 0$ for some i, and let e be the smallest integer such that $g_e \neq 0$; by Lemma 3.5 there exists $t'' \in N$ such that $w^*(g_e) = w^*(H(t''))$; let t' be the element in N such that $H(t') = X_1 H(t'')^n$ and let $d = c(t')$; then $w^*(z - z_d) > w^*(g_e^n)$; let $G(Z) = f(Z + z_d) = Z^n + G_1 Z^{n-1} + \dots + G_n$ with $G_i \in R$; then $G(Z)$ is an R-translate of $f(Z)$ and hence $G(Z)$ is of prenonsplitting-type relative to w; consequently $w(G_i^n) \geq w(G_n^i)$ for all i and hence in particular

$w^*(G_e^n) \geq w^*(G_n^e)$; now $G(Z) = g(Z + z_d - z)$ and hence $G_e = g_e + t^*(z_d - z)^e$ with $t^* \in R^*$; consequently $w^*(G_e^n) = w^*(g_e^n) < w^*(z - z_d)$; also $G_n = G(0) = g(z_d - z) \in (z_d - z)R^*$ and hence $w^*(G_n^e) \geq w^*(G_n) \geq w^*(z_d - z)$; thus $w^*(G_e^n) < w^*(G_n^e)$ which is a contradiction. Therefore $g_i = 0$ for all i, i.e., $f(Z) = (Z - z)^n$.

PROOF OF (3) - There exist integers $0 = d(0) < d(1) < \dots < d(e) = q$ such that upon relabelling $X_1, \dots, X_q$ suitably, for $1 \leq i \leq e$ and $d(i-1) < j \leq d(i)$ we have that for $d(i-1) < k \leq d(i)$: $w(X_k^{m(j,k)}) \geq w(X_j)$ for some positive integer $m(j, k)$, and for $d(i) < k \leq q$: $w(X_k) \geq w(X_j^m)$ for every positive integer m. For $0 < i \leq e$ let V_i be the set of all monomials $X_{d(i-1)+1}^{b(1)} \dots X_{d(i)}^{b(d(i)-d(i-1))}$ with $b \in N^{d(i)-d(i-1)}$, and let $V_0 = \{1\}$. For $0 \leq i < e$ let W_i be the set of all monomials $X_{d(i)+1}^{b(1)} \dots X_q^{b(q-d(i))}$ with $b \in N^{q-d(i)}$, and let $W_e = \{1\}$. By induction on i we shall show that for any integer i with $0 \leq i \leq e$ we have the following: (3_i) given any $s \in R$ and $Y \in W_i$ such that $w(f(s)) \geq w(Y^n)$, there exists $z \in R$ such that $w(f(s + zY)) > w(T^n Y^n)$ for all $T \in V_i$. To prove (3_0) let $s \in R$ and $Y \in W_0$ be given such that $w(f(s)) \geq w(Y^n)$; upon letting $F(Z) = f(Z+s)$ we get that $w(F(0)) \geq w(Y^n)$; since $F(Z)$ is an R-translate of $f(Z)$, by assumption we know that $F(Z)$ is of prenonsplitting-type relative to w and hence by (1) there exists $z \in R$ such that $w(F(zY)) > w(Y^n)$; clearly then $w(f(s + zY)) > w(T^n Y^n)$ for all $T \in V_0$. Now let $0 < i \leq e$ and assume that (3_{i-1}) holds. To prove (3_i) let $s \in R$ and $Y \in W_i$ be given such that $w(f(s)) \geq w(Y^n)$. By Lemma 3.3(3) there exists a unique one-to-one map H of N onto V_i such that $w(H(j)) < w(H(k))$ for all j and k in N with $j < k$; note that $H(0) = 1$. For $k \in N$ suppose we have defined $r_j \in R$ for $0 \leq j < k$ such that $w(f(s + (r_0 H(0) + \dots + r_j H(j))Y)) \geq w(H(j + 1)^n Y^n)$ for $0 \leq j < k$; then $H(k)Y \in W_{i-1}$ and $w(f(s + (r_0 H(0) + \dots + r_{k-1} H(k-1))Y)) \geq w(H(k)^n Y^n)$, and hence by (3_{i-1}) there exists $r_k \in R$ such that $w(f(s + (r_0 H(0) + \dots + r_k H(k))Y)) > w(T'^n H(k)^n Y^n)$ for all $T' \in V_{i-1}$; we claim that $w(f(s + (r_0 H(0) + \dots + r_k H(k))Y)) \geq w(H(k + 1)^n Y^n)$; this being obvious in case $f(s + (r_0 H(0) + \dots + r_k H(k))Y) = 0$, now suppose that $f(s + (r_0 H(0) + \dots + r_k H(k))Y) \neq 0$; then by assumption there exists $X' \in W_0$ such that $w(f(s + (r_0 H(0) + \dots + r_k H(k))Y)) = w(X'^n)$; then $w(X') > w(T' H(k) Y)$ for all $T' \in V_{i-1}$ and hence we must have $w(X') \geq w(H(k + 1)Y)$; consequently $w(f(s + (r_0 H(0) + \dots + r_k H(k))Y)) \geq w(H(k + 1)^n Y^n)$. Thus by induction we have defined $r_k \in R$ for all $k \in N$ such that upon letting $z_k = r_0 H(0) + \dots + r_k H(k)$ we have that $w(f(s + z_k Y)) \geq w(H(k+1)^n Y^n)$ for all $k \in N$. Let $M' = (X_{d(i-1)+1}, \dots, X_{d(i)})R$. Then for each $u \in N$ there exists $v(u) \in N$ such that $H(k) \in M'^u$ for all $k \in N$ with $k \geq v(u)$. Consequently there exists a unique $z \in R$ such that $z - z_k \in M'^u$ for all k and u in N with $k \geq v(u)$. Clearly for each $j \in N$ there exists $p(j) \in N$ such that $w(y) \geq w(H(j)^n)$ for all $y \in M'^{p(j)}$. Therefore for each $j \in N$ there exists $c(j) \in N$ such that $w(z - z_k) \geq w(H(j)^n)$ for all $k \in N$ with $k \geq c(j)$. Let $f'(Z) = f(Z + s)$. Then $w(f'(0)) \geq w(Y^n)$; since $f'(Z)$ is an R-translate of $f(Z)$, by assumption we know that $f'(Z)$ is of prenonsplitting-type relative to w and hence upon letting $g(Z) = f'(YZ)/Y^n$ we get that $g(Z)$ is a monic polynomial of degree n in Z with coefficients in R_w. Now $g(z) - g(z_k) \in (z - z_k)R_w$ for all $k \in N$, and hence $w(g(z) - g(z_k)) \geq w(H(j)^n)$ for all k and j in N with $k \geq c(j)$. Also $g(z_k) = f(s + z_k Y)/Y^n$ and $w(f(s + z_k Y)) \geq w(H(k+1)^n Y^n)$ for all $k \in N$, and hence $w(g(z_k)) \geq w(H(j)^n)$ for all k and j in N with $k \geq j$. Therefore $w(g(z)) \geq w(H(j)^n)$ for all $j \in N$. Now $f(s + zY)/Y^n = g(z)$ and hence $w(f(s + zY) \geq$ $\geq w(H(j)^n Y^n)$ for all $j \in N$, i.e., $w(f(s + zY)) \geq w(T^n Y^n)$ for all $T \in V_i$. This completes the induction on i and hence in particular (3_e) is established. Upon taking $s = 0$ and $Y = 1$, by (3_e) we find $z \in R$ such that $w(f(z)) \geq w(T^n)$ for all $T \in V_e$. Suppose if possible that $f(z) \neq 0$; then by assumption there exists $X^* \in W_0$ such that $w(f(z)) = w(X^{*e})$; then $w(X^*) \geq w(T)$ for all $T \in V_e$ which is a contradiction. Therefore $f(z) = 0$.

PROOF OF (4) - Since Z^n is not an R-translate of $f(Z)$ we get that $n > 1$. Suppose if possible that $f(z) = 0$ for some $z \in R$ and let $g(Z) = f(Z + z)$; then $g(Z)$ is an R-translate of $f(Z)$ and hence $g(Z) \neq Z^n$; since $g(Z)$ is a monic polynomial of degree n in Z with coefficients in R, $n > 1$, $g(0) = 0$, and $g(Z) \neq Z^n$, we get that $g(Z)$ is not of prenonsplitting-type relative to w; this is a contradiction. Therefore $f(z) \neq 0$ for all $z \in R$. Consequently by (3) there exists $r \in R$ such that for all $a \in N^q$ with $a \equiv 0(n)$ we have that $w(f(r)) \neq$ $\neq w(X_1^{a(1)} \dots X_q^{a(q)})$. Let $F(Z) = f(Z + r)$. Then $F(Z)$ is an R-translate of $f(Z)$, $F(0) = f(r) \neq 0$, and by Lemma 3.5 there exists $a \in N^q$ such that $w(F(0)) =$ $= w(X_1^{a(1)} \dots X_q^{a(q)})$. It follows that $a \not\equiv 0(n)$.

LEMMA 3.7 - *Let R be a two dimensional regular local domain with maximal ideal M. Let (x, y) be a basis of M and let J be a coefficient set for R. Let w be a valuation of the quotient field K of R such that w dominates R, and $w(x)$ and $w(y)$ are rationally independent; (by Lemma 3.5 we know that w is then residually rational over R). Let R_i be the i^{th} quadratic transform of R along w and let M_i be the maximal ideal in R_i. Let $x_0 = x$ and $y_0 = y$. Since $w(x_0)$ and $w(y_0)$ are rationally independent, there exists a unique basis (x_i, y_i) of M_i for all $i > 0$ such that $w(x_i)$ and $w(y_i)$ are rationally independent for all $i > 0$, and such that for all $i > 0$ we have that: if $w(x_{i-1}) < w(y_{i-1})$ then $x_i = x_{i-1}$ and $y_i = y_{i-1}/x_{i-1}$, and if $w(x_{i-1}) > w(y_{i-1})$ then $x_i = x_{i-1}/y_{i-1}$ and $y_i = y_{i-1}$. (Note that if R/M is algebraically closed then (R_i, x_i, y_i) is the canonical i^{th} quadratic transform of (R, x, y, J) along w for all $i \geq 0$). We have the following.*

(1) *Given $(a, b) \in N^2$ let $(a(0), b(0)) = (a, b)$ and define $(a(i), b(i)) \in N^2$ for all $i > 0$ by the following recurrence equations: if $w(x_{i-1}) < w(y_{i-1})$ then $a(i) = a(i-1) + b(i-1)$ and $b(i) = b(i-1)$, and if $w(x_{i-1}) > w(y_{i-1})$ then $a(i) = a(i-1)$ and $b(i) = a(i-1) + b(i-1)$. Then $x^a y^b = x_i^{a(i)} y_i^{b(i)}$ for all $i \geq 0$;*

and if v is a positive integer such that $(a, b) \equiv|\equiv 0(v)$ then $(a(i), b(i)) \equiv|\equiv 0(v)$ for all $i \geq 0$. Given any positive integer u let $a'(i)$, $a''(i)$, $b'(i)$, $b''(i)$ be the unique nonnegative integers such that $a(i) = a'(i) + ua''(i)$, $a'(i) < u$, $b(i) = b'(i) + ub''(i)$, and $b'(i) < u$; then given any nonnegative integer j there exists an integer i such that $j \leq i < j + u$ and $a'(i) + b'(i) < u$.

(2) *Given any finite number of nonzero elements $G_1, \ldots, G_n$ in R_w there exists a nonnegative integer j such that $G_1, \ldots, G_n$ are R_i–monomials in (x_i, y_i) for all $i \geq j$.*

(3) *Let $F(Z)$ be a monic polynomial of degree $n > 0$ in Z with coefficients in R such that $F(Z) \neq Z^n$ and $F(Z)$ is not of prenonsplitting-type relative to w. Then $n > 1$ and there exist nonnegative integers i, d, e such that for $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ we have that $g(Z) \in R_i[Z]$ and $0 < \mathrm{ord}_{R_i} g(Z) < n$.*

(4) *Let $F(Z)$ be a monic polynomial of degree $n > 0$ in Z such that $F(Z)$ is of prenonsplitting-type relative to w and $w(F(0)) = w(x^a y^b)$ for some $(a, b) \in N^2$ with $(a, b) \equiv|\equiv 0(n)$. Then $n > 1$ and there exist nonnegative integers i, d, e such that for $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ we have that $g(Z) \in R_i[Z]$ and $0 < \mathrm{ord}_{R_i} g(Z) < n$.*

(5) *Assume that R is complete and R/M is algebraically closed. Let $f(Z)$ be a monic polynomial of degree $n > 0$ in Z with coefficients in R such that Z^n is not an R-translate of $f(Z)$. Then $n > 1$ and there exist nonnegative integers i, d, e and an R-translate $F(Z)$ of $f(Z)$ such that for $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ we have that $g(Z) \in R_i[Z]$ and $0 < \mathrm{ord}_{R_i} g(Z) < n$.*

PROOF OF (1) – By induction on i it follows that $x^a y^b = x_i^{a(i)} y_i^{b(i)}$ for all $i \geq 0$, and if v is a positive integer such that $(a, b) \equiv|\equiv 0(v)$ then $(a(i), b(i)) \equiv|\equiv 0(v)$ for all $i \geq 0$. For any $i > 0$ for which $a'(i-1) + b'(i-1) \geq u$ we get that: if $w(x_{i-1}) < w(y_{i-1})$ then $a'(i) = a'(i-1) + b'(i-1) - u$ and $b'(i) = b'(i-1)$ and hence $a'(i) + b'(i) < a'(i-1) + b'(i-1)$, and if $w(x_{i-1}) > w(y_{i-1})$ then $a'(i) = a'(i-1)$ and $b'(i) = a'(i-1) + b'(i-1) - u$ and hence again $a'(i) + b'(i) < a'(i-1) + b'(i-1)$. Therefore given any nonnegative integer j there exists an integer i such that $j \leq i < j + u$ and $a'(i) + b'(i) < u$.

PROOF OF (2) – In view of Lemma 1.3 it suffices to show that given $0 \neq G \in R$ there exists a nonnegative integer j such that G is an R_i–monomial in (x_i, y_i) for all $i \geq j$. By Lemma 3.5 there exists $(a, b) \in N^2$ such that $G/(x^a y^b)$ is a unit in R_w. By Lemma 1.3 there exists a nonnegative integer j such that $G/(x^a y^b)$ is a unit in R_i for all $i \geq j$. By (1) we know that $x^a y^b$ is an R_i–monomial in (x_i, y_i) for all $i \geq 0$, and hence G is an R_i–monomial in (x_i, y_i) for all $i \geq j$.

PROOF OF (3) – Now $n > 1$, $F(Z) = Z^n + F_1 Z^{n-1} + \ldots + F_n$ with $F_1, \ldots, F_n$ in R, and $w(F_k^n) < w(F_n^k)$ for some k with $1 \leq k < n$. Let u be the greatest integer such that $w(F_u^{n!/u}) \leq w(F_m^{n!/m})$ for all m with $1 \leq m \leq n$. Then $1 \leq u < n$, $F_u \neq 0$, and $F_m^u/F_u^m \in R_w$ for $1 \leq m \leq n$. By Lemma 3.5 there exists $(a, b) \in N^2$ such that $F_u/(x^a y^b)$ is a unit in R_w. Then $F_m^u/(x^a y^b)^m \in R_w$ for $1 \leq m \leq n$. Let $a(i)$, $b(i)$, $a'(i)$, $a''(i)$, $b'(i)$, $b''(i)$ be as in (1). By Lemma 1.3 there exists a nonnegative integer j such that for all $i \geq j$ we have that $F_u/(x^a y^b)$ is a unit in R_i and $F_m^u/(x^a y^b)^m \in R_i$ for $1 \leq m \leq n$. By (1) there exists an integer i with $j \leq i < j + u$ such that $a'(i) + b'(i) < u$. Let $d = a''(i)$ and $e = b''(i)$. Then $x^a y^b = (x_i^d y_i^e)^u (x_i^{a'(i)} y_i^{b'(i)})$ and hence $F_u/(x_i^d y_i^e)^u \in R_i$ and $\operatorname{ord}_{R_i} F_u/(x_i^d y_i^e)^u < u$. Also, for $1 \leq m \leq n$ we get that $(F_m/(x_i^d y_i^e)^m)^u \in R_i$ and $F_m/(x_i^d y_i^e)^m \in K$; since R_i is normal we deduce that $F_m/(x_i^d y_i^e)^m \in R_i$ for $1 \leq m \leq n$. Therefore for $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ we have that $g(Z) \in R_i[Z]$ and $0 < \operatorname{ord}_{R_i} g(Z) < n$.

PROOF OF (4) – Since $(a, b) \not\equiv 0(n)$ we get that $n > 1$. Take $u = n$ and let $a(i)$, $b(i)$, $a'(i)$, $a''(i)$, $b'(i)$, $b''(i)$ be the nonnegative integers defined in (1); then by taking $v = n$ in (1) we get that $(a'(i), b'(i)) \not\equiv 0(n)$ for all $i \geq 0$ and hence $a'(i) + b'(i) > 0$ for all $i \geq 0$. Now $F(Z) = Z^n + F_1 Z^{n-1} + \ldots + F_n$ where $F_1, \ldots, F_n$ are elements in R such that $F_n/(x^a y^b)$ is a unit in R_w and $F_m^n/(x^a y^b)^m \in R_w$ for $1 \leq m \leq n$. By Lemma 1.3 there exists a nonnegative integer j such that for all $i \geq j$ we have that $F_n/(x^a y^b)$ is a unit in R_i and $F_m^n/(x^a y^b)^m \in R_i$ for $1 \leq m \leq n$. By (1) there exists an integer i with $j \leq i < j + n$ such that $a'(i) + b'(i) < n$. Let $d = a''(i)$ and $e = b''(i)$. Then $x^a y^b = (x_i^d y_i^e)^n (x_i^{a'(i)} y_i^{b'(i)})$ and hence $F_n/(x_i^d y_i^e)^n \in R_i$ and $0 < \operatorname{ord}_{R_i} F_n/(x_i^d y_i^e)^n < n$. Also, for $1 \leq m \leq n$ we get that $(F_m/(x_i^d y_i^e)^m)^n \in R_i$ and $F_m/(x_i^d y_i^e)^m \in K$; since R_i is normal we deduce that $F_m/(x_i^d y_i^e)^m \in R_i$ for $1 \leq m \leq n$. Therefore for $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ we have that $g(Z) \in R_i[Z]$ and $0 < \operatorname{ord}_{R_i} g(Z) < n$.

PROOF OF (5) – Follows from (3), (4), and Lemma 3.6(4).

THEOREM 3.8 – *Let R be a two dimensional regular local domain with maximal ideal M such that R/M is algebraically closed. Let (x, y) be a basis of M and let J be a coefficient set for R. Let w be a valuation of the quotient field K of R such that w dominates R and w is residually algebraic over R. Let (R_i, x_i, y_i) be the canonical i^{th} quadratic transform of (R, x, y, J) along w. Let R_i^* be the completion of R_i. Let $F(Z)$ be a monic polynomial of degree $n > 0$ in Z with coefficients in R. Then we have the following.*

(1) *Assume that $w(x_i) \neq w(y_i)$ for all $i \geq 0$. Then either: Z^n is an R_k^*-translate of $f(Z)$ for all $k \geq 0$; or: there exist nonnegative integers i, d, e and an R_i^*-translate $F(Z)$ of $f(Z)$ such that upon letting $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ we have that $g(Z) \in R_i^*[Z]$ and $0 < \operatorname{ord}_{R_i^*} g(Z) < n$.*

(2) *Assume that $x_i = x$ for all $i \geq 0$. For each $i \geq 0$ let r_{i+1} be the unique element in J such that $y_i = x(y_{i+1} + r_{i+1})$. Then either: Z^n is an*

R_k^*-translate of $f(Z)$ for all $k \geq 0$; or: there exist nonnegative integers i, d, e and an R_i^*-translate $F(Z)$ of $f(Z)$ such that upon letting $y^* = y_i - (r_{i+1}x + r_{i+2}x^2 + ...) \in R_i^*$ and $g(Z) = F(x^d y^{*e} Z)/(x^d y^{*e})^n$ we have that $g(Z) \in R_i^*[Z]$ and $0 < \mathrm{ord}_{R_i^*} g(Z) < n$.

PROOF. - By [5: Proposition 1], for each $i \geq 0$ there exists a unique two dimensional regular local domain R_i' such that R_i' is an i^{th} quadratic transform of R_0^* and $K \cap R_i' = R_i$. For each $i \geq 0$ let $R_i'^*$ be the completion of R_i', and let M_i, M_i', M_i^*, $M_i'^*$ be the maximal ideals in R_i, R_i', R_i^*, $R_i'^*$ respectively. Then for each $i \geq 0$, by [5: Proposition 1] we get that $R_i' \subset R_{i+1}'$, $K \cap M_i' = M_i$, $M_i R_i' = M_i'$, and there exists an isomorphism h_i of $R_i'^*$ onto R_i^* such that $h_i(s) = s$ for all $s \in R_i$. By Lemma 1.3, $\bigcup_{i=0}^{\infty} R_i'$ is the valuation ring $R_{w'}$ of a valuation w' of the quotient field of R_0^* such that w' dominates R_i' and w' is residually algebraic over R_i' for all $i \geq 0$. It follows that (R_i', x_i, y_i) is the canonical i^{th} quadratic transform of (R_0^*, x, y, J) along w' for all $i \geq 0$. If Z^n is an R_0^*-translate of $f(Z)$ then $Z^n = f(Z + r)$ for some $r \in R_0^*$ and hence for each $k \geq 0$ we get that $f(Z + h_k(r))$ is an R_k^*-translate of $f(Z)$ and $Z^n = f(Z + h_k(r))$. So henceforth we may assume that Z^n is not an R_0^*-translate of $f(Z)$.

To prove (1) assume that $w(x_i) \neq w(y_i)$ for all $i \geq 0$. Then for each $i \geq 0$ we have that either $x_{i+1} = x_i$ and $y_{i+1} = y_i/x_i$, or $x_{i+1} = x_i/y_i$ and $y_{i+1} = y_i$. Therefore $w'(x)$ and $w'(y)$ are rationally independent and hence by Lemma 3.7(5) there exists $s \in R_0^*$ and nonnegative integers i, d, e such that upon letting $F'(Z) = F(Z + s)$ and $g'(Z) = F'(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$ we have that $g'(Z) \in R_i'[Z]$ and $0 < \mathrm{ord}_{R_i'} g'(Z) < n$. Let $F(Z) = F(Z + h_i(s))$ and $g(Z) = F(x_i^d y_i^e Z)/(x_i^d y_i^e)^n$. Then $F(Z)$ is an R_i^*-translate of $f(Z)$, $g(Z) \in R_i^*[Z]$, and $0 < \mathrm{ord}_{R_i^*} g(Z) < n$.

To prove (2) assume that $x_i = x$ for all $i \geq 0$, and for each $i \geq 0$ let r_{i+1} be the unique element in J such that $y_i = x(y_{i+1} + r_{i+1})$. Let $y_i^* = y_i - (r_{i+1}x + r_{i+2}x^2 + ...) \in R_i^*$ for all $i \geq 0$. Then $M_i^* = (x, y_i^*)R_i^*$ for all $i \geq 0$. Now $y_j x^j = y - (r_1 x + r_2 x^2 + ... + r_j x^j)$ for all $j \geq 0$. Consequently $y_i^* x^i = y - (r_1 x + r_2 x^2 + ...) \in R_i^*$ for all $i \geq 0$ and hence $y_i^* x^i - y_j x^j \in M_i^{*j}$ for all $i \geq 0$ and $j \geq 0$. In particular $y_0^* - y_j x^j \in M_0^{*j}$ for all $j \geq 0$; also $M_0^{*j} \subset M_i'^j \subset M_i'^{*j} = h_i^{-1}(M_i^{*j})$ and $h_i(y_j x^j) = y_j x^j$ for all $i \geq 0$ and $j \geq 0$; consequently $h_i(y_0^*) - y_j x^j \in M_i^{*j}$ for all $i \geq 0$ and $j \geq 0$, and hence $h_i(y_0^*) = y_i^* x^i$ for all $i \geq 0$. Therefore $y_0^* x^{-i} \in R_i'$ and $h_i(y_0^* x^{-i}) = y_i^*$ for all $i \geq 0$. It follows that $w(x)$ and $w(y_0^*)$ are rationally independent and $(R_i', x, y_0^* x^{-i})$ is the canonical i^{th} quadratic transform of (R_0^*, x, y_0^*, J) along w' for all $i \geq 0$. Therefore by Lemma 3.7(5) there exists $s \in R_0^*$ and nonnegative integers i, d, e such that upon letting $F'(Z) = F(Z + s)$ and $g'(Z) = F'(x^d (y_0^* x^{-i})^e Z)/(x^d (y_0^* x^{-i})^e)^n$ we have that $g'(Z) \in R'_i[Z]$ and $0 < \mathrm{ord}_{R'_i} g'(Z) < n$. Let $y^* = y_i^*$, $F(Z) = F(Z + h_i(s))$, and $g(Z) = F(x^d y^{*e} Z)/(x^d y^{*e})^n$. Then $F(Z)$ is an R_i^*-translate of $f(Z)$, $g(Z) \in R_i^*[Z]$, and $0 < \mathrm{ord}_{R_i^*} g(Z) < n$.

BIBLIOGRAPHY

[1] S. ABHYANKAR, *Local uniformization on algebraic surfaces over ground fields of characteristic* $p \neq 0$, Annals of Mathematics, vol. 63 (1956), pp. 491-526.

[2] — —, *On the valuations centered in a local domain*, American Journal of Mathematics, vol. 78 (1956), pp. 321-348.

[3] — —, *Simultaneous resolution for algebraic surfaces*, American Jourmal of Mathematics, vol. 78 (1956), pp. 761-790.

[4] — —, *Ramification theoretic methods in algebraic geometry*, Princeton University Press, Princeton, 1959.

[5] — —, *Tame coverings and fundamental groups of algebraic varieties*, Part II: *Branch curves with higher singularities*, American Journal of Mathematics, vol. 82 (1960), pp. 120-178.

[6] — —, *Uniformization in p-cyclic extensions of algebraic surfaces over ground fields of characteristic p*, Mathematische Annalen, vol. 153 (1964), pp. 81-96.

[7] — —, *Reduction to multiplicity less than p in a p-cyclic extension of a two dimensional regular local ring (p = characteristic of the residue field)*, Mathematische Annalen, vol. 154 (1964), pp. 28-55.

[8] — —, *Uniformization of Jungian local domains*, Mathematische Annalen, vol. 159 (1965), pp. 1-43. Correction, Mathematische Annalen, vol. 160 (1965), pp. 319-320.

[9] — —, *Uniformization in a p-cyclic extension of a two dimensional regular local domain of residue field characteristic p*, forthcoming.

[10] — —, *Nonsplitting of valuations in extensions of two dimensional regular local domains*, forthcoming.

[11] W. KRULL, *Allgemeine Bewertungstheorie*, Journal für die reine und angewandte Mathematik, vol. 167 (1931), pp. 160-196.

[12] M. NAGATA, *Local Rings*, Interscience, New York, 1962.

[13] O. ZARISKI; *The reduction of singularities of an algebraic surface*, Annals of Mathematics, vol. 40 (1939), pp. 639-689.

[14] — —, *Local uniformization on algebraic varieties*, Annals of Mathematics, vol. 41 (1940), pp. 852-896.

[15] — —, *Reduction of singularities of algebraic three dimensional varieties*, Annals of Mathematics, vol. 45 (1944), pp. 472-542.

[16] — —, *La resoluzione delle singolarità delle superficie algebriche immerse*, Accademia Nazionale dei Lincei, Rendiconti della Classe di Scienze fisiche, matematiche e naturali, Serie 8, vol. 31 (1962), pp. 97-102 and 177-180.

[17] — —, *Equisingular points on algebraic varieties*, Seminari dell'Istituto Nazionale di Alta Matematica 1962-1963, pp. 164-177.

[18] — —, *Studies in equisingularity*, Part I, American Journal of Mathematics, forthcoming.

[19] — —, *Studies in equisingularity*, Part II, American Journal of Mathematics, forthcoming.

[20] O. ZARISKI and P. SAMUEL, *Commutative Algebra*, vol. I, Van Nostrand, Princeton, 1958.

[21] — —, *Commutative Algebra*, vol. II, Van Nostrand, Princeton, 1960.

[22] H. ZASSENHAUS, *The theory of groups*, Chelsea Publishing Company, New York, 1959.