PACIFIC JOURNAL OF MATHEMATICS
Vol. 173, No. 2, 1996

POLYNOMIALS WITH A GIVEN DISCRIMINANT OVER FIELDS OF ALGEBRAIC FUNCTIONS OF POSITIVE CHARACTERISTIC

ALEXANDRA SHLAPENTOKH

The author extend some results obtained by K. Győry and I. Gaál for number fields and algebraic function fields of characteristic 0, to the fields of algebraic functions of positive characteristic. Though characteristic 0 results in their original form are not true for positive characteristic, one can still effectively classify polynomials with a given discriminant over the fields of algebraic functions of positive characteristic.

§1. Introduction.

This paper extends some results obtained by K. Győry and I. Gaál for number fields and algebraic function fields of characteristic 0, to the fields of algebraic functions of positive characteristic. Though characteristic 0 results in their original form are not true for positive characteristic, one can still effectively classify polynomials with a given discriminant over the fields of algebraic functions of positive characteristic.

Győry defined the following equivalence relation between polynomials over $\mathbb{Z}$:

Difinition 1.1. Let $F(X), F^*(X) \in \mathbb{Z}[X]$, then $F \sim_{\mathbb{Z}} F^*$ if there exists $a \in \mathbb{Z}$ such that $F^*(X) = F(a + X)$.

It is clear that equivalent polynomials have the same discriminant.

One of the main results obtained by Győry is the following theorem:

Theorem 1.2 (Győry). *Let $D \geq 1$ be a fixed number and consider a monic polynomial $F(X) \in \mathbb{Z}[X]$ such that $0 < |D(F)| \leq D$. Then there exist explicitly computable constants $c_1(D)$ and $c_2(D)$, depending only on D, such that* degree$(F) \leq c_1$ *and $F \sim_{\mathbb{Z}} F^*$ with $H(F^*) \leq c_2$, where $H(F^*)$ is the maximal absolute value of all the coefficients of F^*.*

An interesting corollary of this theorem is the fact that up to translation by a rational integer, a number field K of degree n contains only finitely many elements α for which $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is an integral basis of K over $\mathbb{Q}$. (For these and related results of Győry see [7]-[13].) Győry used Minkowski's

inequality to bound the degree of the polynomials by an expression involving the discriminant. Over function fields one cannot hope to bound the degree of the polynomials by the height of the discriminant, since discriminant can be a constant. Therefore, we can expect that the degree of the polynomial will appear in the height bound for F^*.

Results of Györy depended on the following lemma and its p-adic generalization:

Lemma 1.3. *Let K be a number field of degree n_K over $\mathbb{Q}$ and of discriminant D_K over $\mathbb{Q}$. Let $\beta_1, \beta_2, \beta_3$ be algebraic integers such that $\sum \beta_i = 0$, while $\beta_i \neq 0$, and $N_{K/\mathbb{Q}}(\beta_i) \leq G$, where G is a positive constant. Then there exists a unit of K, which will be called ε, such that $H(\varepsilon\beta_i) \leq C(G, n_K, D_K)$, where $H(\varepsilon\beta_i)$ denotes the height of $\varepsilon\beta_i$ (the maximum absolute value of any coefficient of the monic irreducible polynomial of $\varepsilon\beta_i$ over $\mathbb{Z}$) and $C(G, n_K, D_K)$ is an explicitly computable function depending only on the listed arguments.*

The proof of this lemma depends on Baker's method (see [**2**]) and its p-adic analog (see van der Poorten [**15**]). Györy in [**13**] and Gaal in [**6**] have obtained some analogs of Theorem 1.2 for function fields of characteristic 0. They used an analog of the Lemma 1.3 established by Györy in [**13**] and Mason in [**14**] for function field case. To prove our results in the case of the function fields of positive characteristic we shall use Mason's inequality in the case of arbitrary characteristic. As we will see later, in general the results which have been obtained for characteristic 0 will not be true for the case of positive characteristic. In characteristic 0 one could show that every root of a given polynomial was equivalent to an element of a bounded height, because it was possible to bound the height of a root difference by a constant depending on discriminant and the degree of the polynomial. In the case of positive characteristic, we will not be able, in general, to bound the height of the difference of a root pair of a polynomial under consideration using the height of its discriminant and its degree. Nevertheless, we will be able to describe effectively all the possible values of this difference.

§2. Some General Function Field Facts and Definitions.

We will start with defining the objects over which the discussion is carried out. All the fields discussed in the paper will be assumed to be of characteristic $p > 0$.

Definition 2.1. Let R be a field of rational functions over a constant field C_R and let K be a finite extension of R. Then K is called a *field of algebraic functions*. The subfield of K containing all the elements of K which are algebraic over C_R is called the field of constants of K and will be denoted

by C_K.

Lemma 2.2. *Let K be an algebraic function field over a perfect constant field C_K. (A perfect field of positive characteristic p is a field containing all the pth roots of all its elements, so that every finite extension of a perfect field is separable.) Then there exists an element t of K such that $K/C_K(t)$ is separable. (See Eichler* [4, Lemma on p. 143].)

The following sequence of lemmas and definitions 2.3-2.6 establishes the necessary framework and states Mason's fundamental inequality which is the main technical device used in this paper.

Definition 2.3. Let K be an algebraic function field, $\mathfrak{A}$ divisor of K of degree 0, then define the *K-height* of $\mathfrak{A}(H_K(\mathfrak{A}))$ to be

$$H_K(\mathfrak{A}) = \sum_{\text{all } \mathfrak{q}} \max(0, \operatorname{ord}_{\mathfrak{p}} \mathfrak{A}) \operatorname{degree}_K(\mathfrak{q}).$$

($H_K(\mathfrak{A})$ is the degree of zero or pole divisor of $\mathfrak{A}$ in K.)

If $\alpha \in K$ then $H_K(\alpha)$ will be equal to the height of the divisor of $\alpha : \prod_{\text{all } \mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} \alpha}$.

Lemma 2.4. *Let K be an algebraic function field, and let $\alpha, \beta \in K$ be of height less or equal to H_1 and H_2 respectively. Then the heights of $\alpha \pm \beta$, $\alpha \cdot \beta, \alpha/\beta$ are bounded by $H_1 + H_2$, and*

$$\forall m \in \mathbb{Z},\ H_K(\alpha^m) = mH_K(\alpha).$$

Proof. Let $\mathfrak{p}$ be any valuation of K, then

$$\operatorname{ord}_{\mathfrak{p}}(\alpha \pm \beta) \geq \min(\operatorname{ord}_{\mathfrak{p}} \alpha, \operatorname{ord}_{\mathfrak{p}} \beta).$$

Hence,

$$\begin{aligned}
\sum_{\text{all } \mathfrak{p}} \min(\operatorname{ord}_{\mathfrak{p}}(\alpha \pm \beta), 0) \cdot \operatorname{degree}(\mathfrak{p}) &\geq \sum_{\text{all } \mathfrak{p}} \min(\operatorname{ord}_{\mathfrak{p}} \alpha, \operatorname{ord}_{\mathfrak{p}} \beta, 0) \cdot \operatorname{degree}(\mathfrak{p}) \\
&\geq \sum_{\text{all } \mathfrak{p}} \min(\operatorname{ord}_{\mathfrak{p}} \alpha, 0) \cdot \operatorname{degree}(\mathfrak{p}) \\
&\quad + \sum_{\text{all } \mathfrak{p}} \min(\operatorname{ord}_{\mathfrak{p}} \beta, 0) \cdot \operatorname{degree}(\mathfrak{p}) \\
&\geq -H_1 - H_2.
\end{aligned}$$

On the other hand,

$$\begin{aligned}\sum_{\text{all } \mathfrak{p}} \min(\operatorname{ord}_{\mathfrak{p}}(\alpha\beta), 0) \cdot \operatorname{degree}(\mathfrak{p}) &= \sum_{\text{all } \mathfrak{p}} \min(\operatorname{ord}_{\mathfrak{p}} \alpha + \operatorname{ord}_{\mathfrak{p}} \beta, 0) \cdot \operatorname{degree}(\mathfrak{p}) \\ &\geq \sum_{\text{all } \mathfrak{p}} \min(\operatorname{ord}_{\mathfrak{p}} \alpha, 0) \cdot \operatorname{degree}(\mathfrak{p}) \\ &\quad + \sum_{\text{all } \mathfrak{p}} \min(\operatorname{ord}_{\mathfrak{p}} \beta, 0) \cdot \operatorname{degree}(\mathfrak{p}) \\ &\geq -H_1 - H_2.\end{aligned}$$

The assertion concerning the $H(\alpha/\beta)$ follows from the fact that the product formula and the definition of height insure that $H(\alpha) = H(\alpha^{-1})$.

Next note that for any prime $\mathfrak{p}$ of K, $\operatorname{ord}_{\mathfrak{p}} \alpha^m = m \cdot \operatorname{ord}_{\mathfrak{p}} \alpha$ and the assertion concerning the height of a power follows. □

Lemma 2.5 (Fundumental inequality). *Let $\widetilde{M}$ be an algebraic function field of positive characteristic over an algebraically closed field of constants, let V be a fine set of its valuations, let $\gamma_1, \gamma_2, \gamma_3 \in \widetilde{M} \backslash \{0\}$, and assume $\gamma_1 + \gamma_2 + \gamma_3 = 0$, with $\operatorname{ord}_{\mathfrak{p}} \gamma_i = 0$ for all $\mathfrak{p} \notin V$. (Another way to state the preceding condition is to say that γ_i's are V-units.) Then either*

$$H_{\widetilde{M}}\left(\frac{\gamma_1}{\gamma_2}\right) \leq |V| + 2g_{\widetilde{M}} - 2, \tag{2.5.1}$$

where $g_{\widetilde{M}}$ is the genus of the field or for some $x \in \widetilde{M}$, $\gamma_1/\gamma_2 = x^p$. (See Mason [**14**, p. 97].)

Corollary 2.6. *Let $\widetilde{M}$ be an algebraic function field over an algebraically closed field of constants of positive characteristic $p > 0$, let V be a finite set of its valuations, let $\gamma_1, \gamma_2, \gamma_3 \in \widetilde{M} \backslash \{0\}$ and assume $\gamma_1 + \gamma_2 + \gamma_3 = 0$, with $\operatorname{ord}_{\mathfrak{q}} \gamma_i = 0$ for all $\mathfrak{q} \notin V$. Finally suppose $\gamma_1/\gamma_2 = x^{p^r}$, where x is not a pth power in K. Then*

$$H_{\widetilde{M}}(x) \leq |V| + 2g_{\widetilde{M}} - 2.$$

Proof. By assumption we have $\gamma_1 = \gamma_2 x^{p^r}$. Then

$$\gamma_3 = -\gamma_2 - \gamma_1 = \gamma_2(-1 - x)^{p^r}.$$

Therefore, For all $\mathfrak{p} \notin V$, $\operatorname{ord}_{\mathfrak{p}} x = \operatorname{ord}_{\mathfrak{p}}(-1 - x) = \operatorname{ord}_{\mathfrak{p}} 1 = 0$. Thus, if we apply the preceding lemma to $(x + 1) - x - 1$ we will conclude, since by assumption x is not a pth power in K, that $H_{\widetilde{M}}(x) \leq |V| + 2g_{\widetilde{M}} - 2$. □

Lemma 2.7. *Let $M = R(y)$ be an algebraic function field, where $R = C_R(t)$ is a rational function field, M and R have the same constant field, y is*

separable over R and integral over $C_R[t]$. Assume V, a finite set of degree one primes of M, contains all the primes of M extending the infinite valuation of $C_R[t]$, and all primes which are zeros or poles of the discriminant of y. Assume additionally that all the primes of R with factors in V are also of degree 1, and V contains all their factors in M. Moreover assume the following:

1. *There is an algorithm to solve any system of linear equations over C_R or determine that it has no solutions.*

2. *All the primes of V are presented by producing the coefficients of the $\mathfrak{p}$-adic expansions of t and y with respect to some local uniformizing parameters.*

Let $\mathfrak{A}$ be a zero degree divisor of M such that all the primes which are zeros or poles of $\mathfrak{A}$ are contained in V. Then we can effectively determine whether M contains an element α whose divisor is $\mathfrak{A}$. If such an α exists, it can be effectively computed and it is unique up to a constant factor.

(The proof is essentially the same as the proof of the Lemma 1 on page 11 of Mason [**14**].)

The next two lemmas consider the effects of the finite extensions on the degree of the divisors.

Lemma 2.8.

1. *If M/K is a finite separable extension of degree k of algebraic function fields and k_C is the degree of the constant field extension, then a divisor $\mathfrak{A}$ of K of degree d, will have degree $(k/k_C) \cdot d$ as a divisor of M. (See Theorem 4 on page 275 and Theorem 9 on page 279 of Artin* [**1**].)

2. *If $\widetilde{K}/K$ is any separable constant field extension of K, then a divisor of K will have the same degree as a divisor of $\widetilde{K}$. (See Theorem 14 p. 282 and Theorem 17 on page 283 of Artin* [**1**].)

Lemma 2.9. *Let M/K be a finite separable extension of algebraic function fields over constant fields C_M and C_K respectively. Let $\mathfrak{p}$ be a prime of K, $\mathfrak{B}$ a prime of M above $\mathfrak{p}$. Then* $\text{degree}_M(\mathfrak{B}) \leq [M : K] \cdot \text{degree}_K(\mathfrak{p})$.

Proof.

$$e(\mathfrak{B}/\mathfrak{p}) \,\text{degree}_M(\mathfrak{B}) \leq \text{degree}_M(\mathfrak{p}) = [M : K]/[C_M : C_K] \cdot \text{degree}_K(\mathfrak{p}),$$

by the previous lemma. Therefore,

$$\text{degree}_M(\mathfrak{B}) \leq [M : K] \cdot \text{degree}_K(\mathfrak{p}).$$

□

Lemma 2.10. *Let K be an algebraic function field over a perfect field of constants C, let $\widetilde{C}$ be the algebraic closure of C, and let $x \in K$. Then x is a pth power in $\widetilde{C}K$ if and only if x is a pth power in K.*

Proof. Assume the opposite. Then $\widetilde{C}K$ would contain an element inseparable over K which would contradict the assumption that every constant extension of K is separable. □

The following lemma considers the effects of field extensions on the genus.

Lemma 2.11.

1. *Let M be an algebraic function field, and let $\tilde{M}$ be any constant extension of K. Then $g_{\tilde{M}} \leq g_M$. (See Artin Theorem 6 p. 276 and Theorem 21 p. 290 [1].)*

2. *Let M be an algebraic function field and assume $M = R(y)$, where $R = C(t)$ is a rational function field over a constant field C which is also the constant field of M, and y is separable over R. Assume t and y satisfy a polynomial equation $G(t, y) = 0$ of degree n over C. Then the genus g_M of M satisfies the following inequality:*

$$g_M \leq \frac{1}{2}(n-1)(n-2).$$

(*See Artin* [**1**, Theorem 12, p. 311].)

The next two definitions are function field versions of the polynomial height and polynomial equivalence.

Definition 2.12. Let K be an algebraic function field, let $W_K = \{\mathfrak{q}, \ldots, \mathfrak{q}_{w_K}\}$ be a set of prime of K and let O_{K,W_K} be the set of W-integers of K, i.e., the set of all the elements of K having no poles outside W_K. Next let $F, F^* \in O_{K,W_K}[X]$ be such that $F^*(X) = F(X + a)$ for some $a \in O_{K,W_K}$. Then F and F^* will be called O_{K,W_K} -equivalent and this relation will be denoted by

$$F \cong_{K,W_K} F.$$

Definition 2.13. Let K be an algebraic function field, let $F(X) = \sum_{i=0}^{\deg(F)} a_i X^i$ be a polynomial over K. Then define $H_K(F)$ - the K-height of F to be:

$$H_K(F) = \max_i \{H_K(a_i)\}.$$

The next lemma will establish a connection between the height of the polynomial and the height of its roots.

Lemma 2.14. *Let K be an algebraic function field, let $F(X) = a_0 + \ldots + a_{k-1}X^{k-1} + X^k$ be of K-height less or equal to B, a positive constant. Then if M is the splitting field of F, the the M-height of any root is less than $(2Bk!)^2$.*

Proof. First of all we note the following. By Lemma 2.9, $H_M(F) \leq k!H_K(F)$ and for any prime $\mathfrak{p}$ of $M|\operatorname{ord}_{\mathfrak{p}} a_i| \leq Bk!$. Finally, we note that the total number of distinct primes in the pole divisor or zero divisor of any a_i is also bounded by $Bk!$. Next let α be a root of $F(X)$ and assume that for some pole $\mathfrak{p}$ of $\alpha, |\operatorname{ord}_{\mathfrak{p}} \alpha| > 2Bk!$. Then since,

$$\alpha^k = -(a_0 + \ldots + a_{k-1}\alpha^{k-1}),$$

and for $i = 1, \ldots, k-1$,

$$|(i-1)\operatorname{ord}_{\mathfrak{p}} \alpha| + |\operatorname{ord}_{\mathfrak{p}} a_{i-1}| < |\operatorname{ord}_{\mathfrak{p}} a_i \cdot \alpha^i| < |(i+1)\operatorname{ord}_{\mathfrak{p}} \alpha| - |\operatorname{ord}_{\mathfrak{p}} a_{i+1}|,$$

we must conclude that

$$k \cdot \operatorname{ord}_{\mathfrak{p}} \alpha = \min_{0 \leq i \leq k-1} (\operatorname{ord}_{\mathfrak{p}} a_i \alpha^i) = (k-1)\operatorname{ord}_{\mathfrak{p}} \alpha + \operatorname{ord}_{\mathfrak{p}} a_{k-1}.$$

This is impossible, however, and hence $|\operatorname{ord}_{\mathfrak{p}} \alpha| \leq 2Bk!$, so that $H_M(\alpha) \leq (2Bk!)^2$. □

The last proposition in this section deals with the relationship of pth powers of bounded height.

Lemma 2.15. *Let K be a function field of positive characteristic p over perfect field of constants and let $x, y, z \in K$. Assume x, z are not pth powers, y is either a constant or is not a pth power, and for some $l, i, j \in \mathbb{N}$ the following equality holds:*

$$x^{p^l} = y^{p^i} z^{p^j}, \tag{2.15.1}$$

while for some positive constant $B, H_K(x) \leq B, H_K(y) \leq B, H_K(z) \leq B$.

Then $|j - l| < \log_p 2B$.

Proof. First assume y is a constant and $j > l$. Then, using the fact that constant field is perfect, let $w^{p^j} = y^{p^i}$ and conclude that $x = \rho(wz)^{p^{j-l}}$, where ρ is a p^lth root of unity of K. Since the constant field is perfect, $\rho = \tau^{p^{j-l}}$ for some constant $\tau \in K$, and thus x is a pth power. Thus we have a contradiction with our assumption on x and conclude that $l \geq j$. By symmetry, $l \leq j$, and hence, $l = j$.

Next assume y is not a constant and $i > j$ and $l > j$. Then

$$z^{p^j} = \left(x^{p^l} y^{-p^i}\right) = \left(x^{p^{l-\min(l,i)}} \left(y^{-1}\right)^{p^{i-\min(l,i)}}\right)^{p^{\min(l,i)}}.$$

Thus,

$$z = \tau \left(x^{p^{l-\min(l,i)}} \left(y^{-1}\right)^{p^{i-\min(l,i)}}\right)^{p^{\min(l,i)-j}},$$

where τ is a p^jith root of unity of K. Since the field of constants is perfect,

$$\tau = \rho^{p^{\min(l,i)-j}}$$

for some constant ρ and consequently

$$z = \left(\rho x^{p^{l-\min(l,i)}} \left(y^{-1}\right)^{p^{i-\min(l,i)}}\right)^{p^{\min(l,i)-j}}$$

However, $\min(l,i) > j$ and, hence, z is a pth power which contradicts our assumptions. Therefore, by symmetry, we can conclude that out of (i,j,l) at least two indices are equal. If $l = j$, we are done. Suppose not. By symmetric considerations, without loss of generality, assume $i = j$. Then (2.15.1) becomes $x^{p^l} = (yz)^{p^j}$ and $l \geq j$. On the other hand, $x^{p^{l-j}} = \eta yz$, where η is a p^lth root of unity, and therefore $p^{l-j} H_K(x) \leq 2B$. Since the height is always a natural number, $|l - j| \leq \log_p 2B$. □

§3. Main Theorem.

Theorem 3.1. *Let K be an algebraic function field over a perfect field of constants. Let $F(X) \in K[X]$ be a monic polynomial of degree k with a non-zero discriminant $D = D(F)$. Let $\alpha_1 \ldots, \alpha_k$ be the roots of F, let $W_K = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_{W_K}\}$ be the set of poles of coefficients of $F(X)$, let M be any field containing the splitting field of F. Let $d = \max_{1 \leq i \leq w}(\text{degree}_K(\mathfrak{q}_i))$, and without loss of generality let $m = [M : K] \geq k$. Then either*

$$\Delta(F) = \max_{i \neq j} H_M(\alpha_i - \alpha_j) \leq T(H_K(D(F)), g_M, w_K, d, m),$$

where T is an explicitly computable function of the listed arguments or for every pair $i \neq j$

$$(\alpha_i - \alpha_j)^{k(k-1)} = Y_{ij}^{p^{t_{ij}}} D(F),$$

where Y_{ij} is a non-constant unit of the integral closure of O_{K,W_K} in M, and

$$H_M(y) \leq S(H_K(D(F)), g_M, m, w_K, d),$$

where S is an explicitly computable function of the listed arguments.

Proof. We will consider the case of $k = 2$ first. Let

$$F(X) = X^2 + aX + b,$$

and let α_1, α_2 be the roots of the polynomial. Then the discriminant is $(\alpha_1 - \alpha_2)^2$ and the theorem holds for $k = 2$. From now on we will assume $k \geq 3$. Let $\alpha_1, \ldots, \alpha_k$ be all the roots of F, and let $S_K = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s_K}\}$ be the set of valuations of K which are not in W_K and are zeros of $D(F)$. Let C_M be the constant field of M, let $\widetilde{C}_M$ be its algebraic closure, and finally let $\widetilde{M} = \widetilde{C}_M M$.

Let $S_M = \{\mathfrak{B}, \ldots, \mathfrak{B}_{s_M}\}$ and $S_{\widetilde{M}} = \{\widetilde{\mathfrak{B}}_1, \ldots, \widetilde{\mathfrak{B}}_{s_{\widetilde{M}}}\}$ be all the prime ideals lying above the primes of S_K in M and $\widetilde{M}$ respectively and let $W_M = \{\mathfrak{Q}_1, \ldots \mathfrak{Q}_{w_M}\}$ and $W_{\widetilde{M}} = \{\widetilde{\mathfrak{Q}}_1 \ldots, \widetilde{\mathfrak{Q}}_{w_{\widetilde{M}}}\}$ be all the primes lying above the primes of W_K in M and $\widetilde{M}$ respectively. Then

$$w_M \leq [M : K] \cdot w_K \leq m \cdot w_K. \tag{3.1.1}$$

$$s_M \leq [M : K] \cdot s_K \leq m \cdot H_K(D(F)). \tag{3.1.2}$$

Moreover, by Lemma 2.9, $\text{degree}_M(\mathfrak{Q}_i) \leq [M : K] \cdot d \leq md$, and

$$\text{degree}_M(\mathfrak{B}_i) \leq H_M(D(F)) \leq mH_K(D(F)).$$

On the othe hand, by Lemma 2.8, $\text{degree}_{\widetilde{M}} \mathfrak{Q}_i = \text{degree}_M \mathfrak{Q}_i$ and hence $\mathfrak{Q}$ will split in $\widetilde{M}$ into at most md valuations of degree 1. Similarly, $\mathfrak{B}_i$ will split into at most $mH_K(D(F))$ valuations of degree 1. Thus,

$$w_{\widetilde{M}} \leq m^2 w_K d, \tag{3.1.3}$$

$$s_{\widetilde{M}} \leq (mH_K(D(F)))^2. \tag{3.1.4}$$

By the definition of the discriminant of a polynomial, in $\widetilde{M}$, $D(F)$ has the following factorization.

$$D(F) = \prod_{1 \leq i < j \leq k} (\alpha_j - \alpha_i)^2. \tag{3.1.5}$$

Let $1 \leq r < i < j \leq k$ and define $x_{rij}^{p^{t(r,i,j)}} = (\alpha_r - \alpha_j)/(\alpha_r - \alpha_i)$.

Next consider $(\alpha_r - \alpha_i) + (\alpha_i - \alpha_j) + (\alpha_j - \alpha_r) = 0$. Then by Corollary 2.6, we have the following.

$$(\alpha_r - \alpha_i) = (\alpha_r - \alpha_j) x_{rij}^{p^{t(r,i,j)}}, \tag{3.1.6}$$

where either x_{rij} is a constant (in which case x_{rij} is selected so that $t(r,i,,j) = 0$) or it is a non-constant $S_M \cup W_M$ - unit which is not a pth power in $\widetilde{M}$, and in either case

$$\begin{aligned} H_{\widetilde{M}}(x_{rij}) &\leq w_{\widetilde{M}} + s_{\widetilde{M}} + 2g_{\widetilde{M}} - 2 \\ &\leq m^2 w_K d + (mH_K(D(F)))^2 + 2g_{\widetilde{M}} - 2 = T_1, \end{aligned} \tag{3.1.7}$$

where the second inequality follows from Lemma 2.11.

If we let $x_{rii} = 1$ and let $t(1,i,i) = 0$, then (3.1.7) will hold for $1 \leq r < i \leq j \leq k$. Next note that in view of Lemmas 2.8 and 2.10, (3.1.6) is true over M and in (3.1.7), $H_{\widetilde{M}}$ can be replaced by H_M. Further note that

$$(\alpha_1 - \alpha_2)/(\alpha_1 - \alpha_j) = x_{12j}^{p^{t(1,2,j)}},$$

and for $2 \leq i < j \leq k$,

$$(\alpha_1 - \alpha_i)/(\alpha_1 - \alpha_j) = ((\alpha_1 - \alpha_2)/(\alpha_1 - \alpha_j))/((\alpha_1 - \alpha_2)/(\alpha_1 - \alpha_i)),$$

so that

$$x_{12i}^{p^{t(1,2,i)}} x_{1ij}^{p^{t(1,i,j)}} = x_{12j}^{p^{t(1,2,j)}},$$

and, by Lemma 2.15, either x_{12i} or x_{12j} is a constant or

$$|t(1,2,i) - t(1,2,j)| < \log_p 2T_1.$$

Let $t_{12} = \min\{t(1,2,i)\}$, where min is taken over all $2 < i \leq k$ such that x_{12i} is not a constant. Then for all $2 < i \leq k$ such that x_{12i} is not a constant

$$t_{12} \leq t(1,2,i) \leq t_{12} + \log_p 2T_1.$$

Furthermore, for $2 \leq i < j \leq k$ consider

$$\begin{aligned} (\alpha_i - \alpha_j) &= -(\alpha_1 - \alpha_i) + (\alpha_1 - \alpha_j) \\ &= -(\alpha_1 - \alpha_2) x_{12i}^{-p^{t(1,2,i)}} + (\alpha_1 - \alpha_2) x_{12j}^{-p^{t(1,2,j)}} \\ &= (\alpha_1 - \alpha_2)\left(x_{12j}^{-p^{t(1,2,j)-t_{12}}} - x_{12i}^{-p^{t(1,2,i)-t_{12}}}\right)^{p^{t_{12}}} \\ &= (\alpha_1 - \alpha_2)(y_{12ij})^{p^{t_{12}}}, \end{aligned} \tag{3.1.8}$$

where we define $y_{12ij} = \left(x_{12j}^{-p^{t(1,2,j)-t_{12}}} - x_{12i}^{-p^{t(1,2,i)-t_{12}}}\right)$, and note that

$$\begin{aligned} H_M(y_{12ij}) &\leq H_M\left(x_{12i}^{-p^{t(1,2,i)-t_{12}}}\right) + H_M\left(x_{12j}^{-p^{t(1,2,j)-t_{12}}}\right) \\ &\leq 2(2T_1)T_1 = 4T_1^2. \end{aligned} \tag{3.1.9}$$

Since the constant field is perfect the above computation goes through even if one or both of x_{12i} and x_{12j} are constants. Next, note that

$$\begin{aligned}(\alpha_1 - \alpha_j) &= (\alpha_1 - \alpha_2) x_{12j}^{-p^{t(1,2,j)}} \\ &= (\alpha_1 - \alpha_2)\left(x_{12j}^{-p^{(t(1,2,j)-t_{12})}}\right)^{p^{t_{12}}} \\ &= (\alpha_1 - \alpha_2)(y_{121j})^{p^{t_{12}}},\end{aligned}$$

where define $y_{121j} = x_{12j}^{-p^{t(1,2,j)-t_{12}}}$, and conclude that $H_M(y_{121j}) \leq 4T_1^2$. Therefore, $H_M(y_{12ij}) \leq 4T_1^2$ for $1 \leq i < j \leq k$. Finally, let

$$Y_{12} = \prod_{1 \leq i < j \leq k} (y_{12ij}^2) \tag{3.1.10}$$

Then

$$H_M(Y_{12}) \leq k(k-1)(4T_1^2) \leq m(m-1)4T_1^2,$$

and thus in M,

$$D(F) = (\alpha_1 - \alpha_2)^{k(k-1)} Y_{12}^{p^{t_{12}}}. \tag{3.1.11}$$

We now have two cases:

Case 1. Y_{12} is not a unit of O_{M,W_M} or it is a constant.

Case 2. Y_{12} is a non-constant unit of O_{M,W_M}.

We need to consider only the first case. If Y_{12} is not a unit, then it is divisible by at least one prime $\mathfrak{B} \notin W_M$, and so

$$p^{t_{12}} \leq H_M(D(F)) \leq mH_K(D(F)), \tag{3.1.12}$$

and consequently,

$$H_M(Y_{12}^{p^{t_{12}}}) \leq m(m-1)(4T_1^2)mH_K(D(F)) = T_2.$$

In this case, $H_M(\alpha_1 - \alpha_2) \leq (mH_K(D(F)) + T_2) = T_3$.

Similarly, if Y_{12} is a constant then $H_M(\alpha_1 - \alpha_2) = (k(k-1))^{-1} H_M(D(F))$.

Obviously, the same argument can be carried out for any other pair of distinct roots of F to obtain

$$D(F) = (\alpha_i - \alpha_j)^{k(k-1)} Y_{ij}^{p^{t_{ij}}}, \tag{3.1.13}$$

and

$$H_M(Y_{ij}) \leq m(m-1)4T_1. \tag{3.1.14}$$

□

Corollary 3.2. *Let $\alpha_1 \dots, \alpha_k, Y_{ij}$ be as in the theorem, let $\overline{M}$ be the field obtained from M by adjoining all the $(k-1)k$ roots of each Y_{ij}, let $S_{\overline{M}}, W_{\overline{M}}$ be primes in $\overline{M}$ above the primes of S_M and W_M respectively, and let $\theta_i = \sum_{j=1}^{k}(\alpha_i - \alpha_j)$. Then $\theta_i = \delta Y_i^{p^{t_{12}}}$, where $\delta^{k(k-1)} = D(F)$, and Y_i is a sum of k $W_{\overline{M}} \cup S_{\overline{M}}$-units of the height bounded by a constant explicitly computed below.*

Proof. In $\overline{M}$ we have the following equality.

$$(\alpha_1 - \alpha_2) = \delta \vartheta_{12}^{p^{t_{12}}}, \tag{3.2.1}$$

where $\delta^{k(k-1)} = D(F)$, and $(\vartheta_{12}^{p^{t_{12}}})^{k(k-1)} = Y_{12}^{p^{t_{12}}}$. On the other hand, from (3.1.8) we have $(\alpha_i - \alpha_j) = (y_{12ij})^{p^{t_{12}}}(\alpha_1 - \alpha_2)$, and hence

$$(\alpha_i - \alpha_j) = \delta \vartheta_{12}^{p^{t_{12}}} (y_{12ij})^{p^{t_{12}}} = \delta (\vartheta_{ij})^{p^{t_{12}}},$$

where

$$\begin{aligned} H_{\overline{M}}(\vartheta_{ij}) &\le \frac{1}{k(k-1)} H_{\overline{M}}(Y_{12}) + H_{\overline{M}}(y_{12ij}) \\ &\le H_M(Y_{12}) + k(k-1) H_M(y_{12ij}) \\ &\le 4m(m-1)4T_1^2 + 4T_1^2 = T_4. \end{aligned}$$

Next for $i = 1 \dots, k$, let $Y_i = \sum_{j=0}^{k} \vartheta_{ij}$. Then $\theta_i = \delta Y_i^{p^{t_{12}}}$. □

In the following corollaries let $M = R(y)$ be a degree n Galois extention of a rational function field R over a finite field of constants. Assume the minimal polynomial of y over R is given explisitly, so that, using part 2 of Lemma 2.11 we can get an upper bound on g_M. Let K be such that $R \subseteq K \subseteq M$, and let the term "can be described effectively" have the following meaning when applied to the set of all possible values which be taken by an element of $\theta \in M$. There exists a finite set T of primes of M, a finite explicitly given extension $\overline{M}$ of M with $\overline{T}$ being the set of primes of $\overline{M}$ lying over primes of T, such that $\theta = \delta(\sum_{i=1}^{r} w_i)^{p^t}$, where δ, w_i, are elements of $\overline{M}$ and are $\overline{T}$-units whose $\overline{M}$-height is bounded by a constant explicitly computable from the number and degree of primes in T, and n.

(If the constant field of M is finite, then δ and w_i can take finitely many values only and all their possible values can be computed effectively. If the constant field of M is infinite, then w_i and δ can take finitely many values up to multiplication by a constant. If constant field of $\overline{M}$ and the primes of $\overline{T}$ satisfy the conditions of Lemma 2.7, then these finitely many values can be computed effectively.)

Corollary 3.3. *Let D be a zero degree divisor of K, and let W_M be a finite set of valuations of M such that for each prime of W_M all of its conjugates over K are contained in W_M. (In this case W_M contains all the factors of some finite set of primes of K which we will call W_K, and O_{M,W_M} is the integral closure of O_{K,W_K} in M.) Let S_M be the set of all the primes of M which are zeros of D but not in W_M. Finally, assume the height of D is given explicitly. Then if $\alpha \in O_{M,W_M}$ is such that α satisfies a monic polynomial $F(X)$ over O_{K,W_K} splitting in M, having discriminant D and degree k not divisible by the characteristic of the field, then $\alpha = \theta + A$, where $A \in O_{K,W_K}$ and all the possible values of θ_X can be described effectively.*

Proof. Let $\alpha = \alpha_1, \ldots, \alpha_k$ be all the roots of F, as before let $\theta_i = \sum_{i=1}^{r}(\alpha_i - \alpha_j)$. Then, by the previous corollary, θ_i can be described effectively. Next observe that $\alpha_i = k^{-1}\theta_i - k^{-1}\sum_{j=1}^{k}\alpha_j$.

One can rephrase the preceding corollary in terms of the polynomials of K splitting in M to obtain the following result. □

Corollary 3.4. *Let W_K be a finite set of primes of K and let $F(X) \in O_{K,W_K}[X]$ be a splitting in M polynomial with a non-zero discriminant D and degree k not divisible by the characteristic of the field. Let W_M be the primes of M above the primes of W_K, let S_M be all the primes of M dividing D but not in W_M, and assume the height of D is given explicitly. Then $F(X)$ is O_{K,W_K}-equivalent to a polynomial whose coefficients can be described effectively.*

Finally, we can apply Corollary 3.3 in the situation where we are looking for an integral power basis.

Corollary 3.5. *Under the assumptions of Corollary* 3.3, *if M has a power basis $(1, \ldots, \alpha^{n-1})$ over R which is an integral basis for O_M (the ring of integral functions of M) over $C[t]$, then $\alpha = \theta + A$, where A is a polynomial in t, and θ can be described effectively.*

Proof. Since all the elements of $C[t]$ are allowed only the infinite valuation as their pole, if for some $\alpha \in O_M, \{1, \alpha, \ldots, \alpha^{n-1}\}$ is an integral basis of O_M over $C[t]$, then the divisor of the M/R discriminant of α must be of the form $P_\infty^{-a} D_{M/R}$ where $a \in \mathbb{N}$ and $D_{M/R}$ is the discriminant of the extension (see Chevalley [**3**]). The product formula will determine a specific value of a, and, hence, the discriminant of α will be given explicitly. Therefore, the result will follow from the Corollary 3.3. □

The next sequence of corollaries will consider the case when the degree of the polynomial is not prime to the characteristic.

Corollary 3.6. *Suppose all the assumptions of the Corollary* 3.3 *are true but* $k \cong 0 \mod p$. *Next let* $\theta_{ir} = \sum_{j=0}^{k}(\alpha_i - \alpha_j)^r$ *and let* $\omega_i = \sum_{j=1}^{k} \alpha_j^i$. *Then the following statements are true.*

1. *For a fixed* r *all the* θ_{ir} *can be described effectively.*
2. $\omega_i \in K$.
3. *Let* $z \in \mathbb{N}\backslash\{0\}$ *be such that for any* $i = 1, \ldots, z-1$ *either* $\omega_i = 0$ *or* $\binom{z}{i} \cong 0 \mod p$, *then for every* $j = 1, \ldots, k, \theta_{jz} = \omega_z$ *and consequently* ω_z *can be described effectively.*

Proof. The first assertion is proved in the same fashion as the corresponding assertion concerning $\theta_i = \theta_{1i}$. Statement 2 is obvious. To prove 3 consider

$$\theta_{jz} = \sum_{i=1}^{k}(\alpha_j - \alpha_i)^z = \sum_{u=0}^{z} \binom{z}{u} \omega_u \alpha_j^{z-u} = \omega_z.$$

□

We will first consider a special case, where a stronger conclusion can be obtained.

Corollary 3.7. *Under the same assumptions as in the preceding corollary, let*

$$F(X) = a_0 + a_1 X + \ldots + a_{k-1} X^{k-1} + X^k,$$

where $a_i \in O_{K,W_K}$ *and let*

$$i^* = \max\{i \not\cong 0 \mod p,\ i < k, a_i \neq 0\}.$$

Assume, $i^* \not\cong 1 \mod p$. *Then for every* $i = 1, \ldots, k$, *there exist* $a, b \in O_{K,W_K}, \beta_i \in O_{M,W_M}$ *such that all the possible values of* a *and* β_i *can be described effectively and* $a\alpha_i + b = \beta_i$.

Proof. By Lemma 4.1 of the appendix (see Section 4 of the paper), and since $k \cong 0 \mod p$, i^* exists, and

$$k - i^* = r^* = \min\{r \not\cong 0 \mod p,\ \omega_r \neq 0\} \not\cong -1 \mod p.$$

Therefore, $z^* = r^* + 1 \not\cong 0 \mod p$. Moreover, every $z < z^*$ satisfies part 3 of the Corollary 3.6, so that $\forall z = 1, \ldots, z^* - 1$, all the values of ω_z can be described effectively.

In particular, this is true of ω_{r^*}. Next consider,

$$\theta_{iz} = \sum_j (\alpha_i - \alpha_j)^{z^*} = \sum_{u=0}^{z^*} \binom{z^*}{u} \omega_u \alpha_i^{z^*-u} = z^* \omega_{r^*} \alpha_i + \omega_{z^*}.$$

By Corollary 3.6, we are done. □

We consider a general case of a polynomial whose degree is divisible by the characteristic next.

Corollary 3.8. *Under assumptions of Corollary* 3.6, *let a* $\alpha \in O_{M,W_M}$ *be a root of* $F(X) \in O_{K,W_K}[X]$, *and assume* F *splits in* M. *Then there exists* $r \in \mathbb{N}$ *such that* $p^r \leq k$, *there exist* $c_0, \ldots, c_{r+1} \in O_{K,W_K}$, *and there exists* $\beta \in O_{M,W_M}$ *such that* c_i, *for* $i \leq r$, *and* β *can be described effectively and such that*

$$\sum_{i=0}^{r} c_i \alpha^{p^i} + c_{r+1} = \beta.$$

Proof. Define a set of natural numbers Z in the following manner:

$$Z = \left\{ w \in \mathbb{N} \backslash \{0\} \exists\ i < w \text{ such that } \binom{w}{i} \omega_i \neq 0 \right\}.$$

First of all, Z is non-empty. Indeed, let $r = \min\{i | \omega_i \neq 0\}$. By Lemma 4.1 of the appendix, we know that $r \leq k-1$ (otherwise F is inseparable). Then let $w = rp+1$ and observe $\binom{\omega}{\omega-1} \omega_{w-1} = (rp+1)\omega_{rp} = (rp+1)(\omega_r)^p \neq 0$. Next we note that if $z \notin Z$ then by part 3 of Corollary 3.6, all the possible values of ω_z can be described effectively.

Finally, denote by z^* the minimal element of Z, and let $z < z^*$ be such that $\binom{z^*}{z} \omega_z \neq 0$. (Such z exists by definition of Z.) Let $\sum_{i=0}^{[\log_p z^*]} d_i p^i$ be the p-adic representation of z, and let j be the smallest index such that $d_j \neq p-1$. Then if we let $w = (\sum_{i=0}^{\log_p z^*} d_i p^i) + p^j$, in the p-adic representation of w all the p-adic digits will be greater or equal to digits of z, so that $\binom{w}{z} \neq 0$ by Lemma 4.3 of the appendix. Hence, $w \geq z^*$, and $z^* - z \leq p^j$. On the other hand, let $\sum f_i p^i$ be the p-adic representation of z^*. Then, since $\binom{z^*}{z} \omega_z \neq 0$, we must have $f_1 = d_1 = p-1, \ldots, f_{j-1} = d_{j-1} = p-1$. Therefore for such a $z, z - z^* \geq p^j$. Hence $z^* - z = p^j$.

Next consider $\theta_{iz^*} = \sum_{z=0}^{z^*} \binom{z^*}{z} \omega_z \alpha_i^{z^*-z}$. By the argument above,

$$\binom{z^*}{z} \omega_z \alpha_i^{z^*-z} \neq 0 \Longrightarrow \exists\ j, z^* - z = p^j.$$

Therefore,

$$\theta_{iz^*} = \sum_{j=0}^{[\log_p z^*]} \binom{z^*}{p^j} \omega_{z^*-p^j} \alpha_i^{p^j},$$

and $p^j \leq p(k-1)+1 \Longrightarrow p^{j-1} \leq k-1 \Longrightarrow p^{j-1} \leq k/p \Longrightarrow j \leq \log_p k$. □

At this point we note that the obtained results even for the case of the polynomial degree prime to the characteristic of the field are weaker than the corresponding results for the case of characteristic 0. The relative weakness of the main theorem is due to the second case of the theorem. Unfortunately, as the next lemma will show, this case of the theorem does occur.

Lemma 3.9. *Let K, M be as in the main theorem. Then there exists a constant $A > 0$ such that for every $B > 0$ there exists a polynomial F with $H_K(D(F)) < A$ and a pair of roots α_1 and α_2 such that $H_M(\alpha_1 - \alpha_2) > B$.*

Proof. Consider the following equation over K : $F(X) = X^3 + aX + 1 = 0$, where a is a nonconstant element of K. Let $\delta_1, \delta_2, \delta_3$ be the roots of F and observe that $N_{K(\delta_i)/'K}(\delta_i) = -1$, and $Tr_{K(\delta_i)/K}(\delta_i) = 0$. Next let W_K be the set of poles of a in K, let W_M be the set of poles of a in M, let $D = D(\delta_i)^{1/2}$ be a square root of the discriminant of δ_i with respect to K, so that $D^2 \in K$ and let

$$\alpha_1 = (\delta_1 - \delta_2)^{p^r} D, \quad \alpha_2 = (\delta_3 - \delta_1)^{p^r} D, \quad \alpha_3 = (\delta_2 - \delta_3)^{p^r} D.$$

Then $\alpha_i \in O_{M,W_M}$, and

$$\begin{aligned}(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \\ = [(\delta_1 - \delta_2 - \delta_3 + \delta_1)(\delta_1 - \delta_2 - \delta_2 + \delta_3)(\delta_3 - \delta_1 - \delta_2 + \delta_3)]^{p^r} D^3 \\ = (-27\delta_1\delta_2\delta_3)^{p^r} D^3 = 27D^3.\end{aligned}$$

On the other hand,

$$H_M(\alpha_1 - \alpha_2) \geq p^r H_M(\delta_1 - \delta_2) - H_M(D). \tag{3.9.1}$$

Moreover, α is of degree 3 over K. Indeed,

$$\alpha_1 + \alpha_2 + \alpha_3 = 0 \in K$$

$$\alpha_1\alpha_2\alpha_3 = (D(\delta_i)^{1/2})^{p^r} D(\delta_i)^{3/2} = D^{p^r+3} \in K.$$

$$\begin{aligned}
&\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 \\
&\quad = [(\delta_1 - \delta_2)(\delta_3 - \delta_1) + (\delta_3 - \delta_1)(\delta_2 - \delta_3) + (\delta_1 - \delta_2)(\delta_2 - \delta_3)]^{p^r} D^2 \\
&\quad = (\delta_1\delta_3 - \delta_2\delta_3 - \delta_1^2 + \delta_1\delta_2 + \delta_3\delta_2 - \delta_1\delta_2 - \delta_3^2 + \delta_1\delta_3 \\
&\qquad + \delta_1\delta_2 - \delta_2^2 - \delta_1\delta_3 + \delta_2\delta_3)^{p^r} D^2 \\
&\quad = (-\delta_1^2 + \delta_1\delta_2 + \delta_3\delta_2 - \delta_3^2 + \delta_1\delta_3 - \delta_2^2)^{p^r} D^2 \\
&\quad = (a - (\delta_1 + \delta_2 + \delta_3)^2 + 2a)^{p^r} D^2 = 3a^{p^r} D^2.
\end{aligned}$$

Hence, $\alpha_i^3 + 3a^{p^r} D^2 \alpha_i + D^{p^r+1} = 0$, and $D(\alpha_i) = 27^2 D^6$.

We still have to show that $\delta_1 - \delta_2$ is not a constant. Then (3.9.1) will assure that $H_M(\alpha_i - \alpha_j)$ can be made arbitrarily large relative to $D_{K(\alpha_i)/K}(\alpha_i), g_M$, degrees of valuations in W_K and $|W_K|$. First of all, δ_i is not a constant since otherwise a is a constant. Next suppose, $\delta_2 = \delta_1 + c$, where c is a constant. Then

$$\begin{aligned}
&(\delta_1 + c)^3 + a(\delta_1 + c) + 1 = 0. \\
&\delta_1^3 + 3\delta_1^2 c + 3\delta_1 c^2 + c^3 + a\delta_1 + ac + 1 = 0. \\
&3\delta_1^2 + 3\delta_1 c + c^2 + a = 0.
\end{aligned}$$

On the other hand, $a = -(\delta_1^3 + 1)/\delta_1$, so that

$$3\delta_1^3 + 3\delta_1^2 c + c^2\delta_1 - (\delta_1^3 + 1) = 0.$$

Hence, if c is a constant then so is δ_1.

We should also note here, that this example shows that the analog of Theorem 1.2 does not hold for the case of positive characteristic. Indeed, let

$$G_r(X) = X^3 + 3a^{p^r} D^2 X + D^{p^r+1},$$

where a and D are as above. By the above computation, we know that for all r, $D(G_r) = 27^2 D^6$. Let W_K contain all the poles of a and D. Then for any value of r, all the roots of $G_r(X)$ are integral over O_{K,W_K}. Next suppose, $G_r(X) \cong_{K,W_K} G_r^*(X)$, where $H_K(G_r^*)$ is bounded by a constant depending on D, w_K (and possibly some other parameters associated with M or K) only. Let $\alpha_{1r}, \alpha_{2r}, \alpha_{3r}$ and $\beta_{1r}, \beta_{2r}, \beta_{3r}$ be the roots of G_r and G_r^* respectively. Then $\alpha_{ir} = \beta_{ir} + A$, where $A \in O_{K,W_K}$ and in M the height of β_{ir} is again, by Lemma 2.14, bounded by a constant depending on D and w_K only. However, $\alpha_{ir} - \alpha_{jr} = \beta_{ir} - \beta_{jr}$ will under these assumptions still have the height bounded by the above described constant. The last statement can be easily made false by the choice of sufficiently large r. □

Our next lemma provides some insight into the reasons for still weaker results for an arbitrary polynomial in the case of $k \cong 0 \mod p$.

Lemma 3.10. *Let K, M be as in the main theorem again. Then for every map*

$$\mathcal{F}\{H_K(z), z \in K\} \longmapsto \mathbb{N},$$

there exists a polynomial

$$F(X) = X^{p^r} + bX + c,$$

such that

$$\forall a \in K,\ H_K(F(X-a)) > \mathcal{F}(\max(H_M(\alpha_i - \alpha_j))),$$

where $\alpha_1, \ldots, \alpha_{p^r}$ are the roots of F, and M is the splitting field of $F(X)$.

Proof. Let $\alpha_1, \ldots, \alpha_{p^r}$ be all the roofs of $F(X)$. Then for $i \neq j$

$$(\alpha_i - \alpha_j)^{p^r} + b(\alpha_i - \alpha_j) = 0.$$

$$(\alpha_i - \alpha_j)^{p^r - 1} = -b.$$

Therefore, $(\alpha_i - \alpha_j)$ is independent of value of c. Next suppose, there exists $a \in K$ such that

$$H_K(F(X-a)) \leq \mathcal{F}(\max(H_M(\alpha_i - \alpha_j))) - C(b),$$

where $C(b)$ is a constant depending on b only. Then

$$H_K(F(X-a)) = H_K(X^{p^r} + bX - a^{p^r} - ab + c) \leq C(b),$$

and consequently,

$$H_K(a^{p^r} - ab + c) \leq C(b).$$

Let $a^{p^r} - ab + c = z$, where z has a height bounded by $C(b)$. Let $\mathfrak{p}$ be such that

$$0 > \operatorname{ord}_{\mathfrak{p}} b > -p^r + 1,$$

and such that

$$\operatorname{ord}_{\mathfrak{p}} c < -p^r$$

and $\operatorname{ord}_{\mathfrak{p}} c$ is not a multiple of p. Then we would like to consider the five cases which can occur:

1. $\operatorname{ord}_{\mathfrak{p}} a^{p^r} > \operatorname{ord}_{\mathfrak{p}} ab = \operatorname{ord}_{\mathfrak{p}} a + \operatorname{ord}_{\mathfrak{p}} b > -p^r > \operatorname{ord}_{\mathfrak{p}} c$; $(\operatorname{ord}_{\mathfrak{p}} a > 0)$
2. $0 = \operatorname{ord}_{\mathfrak{p}} a^{p^r} > \operatorname{ord}_{\mathfrak{p}} ab = \operatorname{ord}_{\mathfrak{p}} a + \operatorname{ord}_{\mathfrak{p}} b = \operatorname{ord}_{\mathfrak{p}} b > \operatorname{ord}_{\mathfrak{p}} c$; $(\operatorname{ord}_{\mathfrak{p}} a = 0)$
3. $\operatorname{ord}_{\mathfrak{p}} ab = \operatorname{ord}_{\mathfrak{p}} a + \operatorname{ord}_{\mathfrak{p}} b > \operatorname{ord}_{\mathfrak{p}} a^{p^r} > \operatorname{ord}_{\mathfrak{p}} c$; $(\operatorname{ord}_{\mathfrak{p}} a < 0)$
4. $\operatorname{ord}_{\mathfrak{p}} ab = \operatorname{ord}_{\mathfrak{p}} a + \operatorname{ord}_{\mathfrak{p}} b \geq \operatorname{ord}_{\mathfrak{p}} c > \operatorname{ord}_{\mathfrak{p}} a^{p^r}$; $(\operatorname{ord}_{\mathfrak{p}} a < 0)$
5. $\operatorname{ord}_{\mathfrak{p}} c \geq \operatorname{ord}_{\mathfrak{p}} ab = \operatorname{ord}_{\mathfrak{p}} a + \operatorname{ord}_{\mathfrak{p}} b > \operatorname{ord}_{\mathfrak{p}} a^{p^r}$ $(\operatorname{ord}_{\mathfrak{p}} a < 0)$.

In the first three cases,

$$|\operatorname{ord}_{\mathfrak{p}} z| = |\min(\operatorname{ord}_{\mathfrak{p}} a^{p^r}, \operatorname{ord}_{\mathfrak{p}} ab, \operatorname{ord}_{\mathfrak{p}} c)| = |\operatorname{ord}_{\mathfrak{p}} c|.$$

In the last two cases,

$$|\operatorname{ord}_{\mathfrak{p}} z| = |\min(\operatorname{ord}_{\mathfrak{p}} a^{p^r}, \operatorname{ord}_{\mathfrak{p}} ab, \operatorname{ord}_{\mathfrak{p}} c)| = |\operatorname{ord}_{\mathfrak{p}} a^{p^r}| > |\operatorname{ord}_{\mathfrak{p}} c|.$$

Therefore, in either case, assuming $\mathfrak{p}$ is a pole of c whose degree is greater than p^r and is not a multiple of p,

$$C(b) \geq H_K(z) \geq |\operatorname{ord}_{\mathfrak{p}} z| \geq |\operatorname{ord}_{\mathfrak{p}} c|.$$

However, by Approximation Theorem (see, for example, Fried-Jarden [**5**, p. 21]), c can clearly be selected with a pole at $\mathfrak{p}$, whose degree is greater than $\max(C(b), p^r)$ and is not a multiple of p. □

A consequence of the lemma is the fact that even if we have a bound on the height of the root differences, we still could not conclude that the roots were equivalent to an element of bounded height, since these elements would produce a polynomial of a bounded height. Finally, we would like to make the following observation. If we suppose that the infinite valuation corresponding to the pole of t has only one factor in M, then assuming $[M : R]$ is not a multiple of p, the theorem will guarantee that up to polynomial translation we have only finitely many integral power basis. Of course, in this situation one does not need the theorem to reach this conclusion. Since all the functions in the integral closure of the polynomial ring are assumed to have the same valuation as their pole, there can be no cancellations in the product of root differences comprising the discriminant, so we automatically get a height bound on the root differences. On the other hand, the last lemma implies, that if the degree is divisible by the characteristic, even under these very special circumstances we do not get a height bound on roots and cannot conclude that we have finitely many (up to translation) integral power basis.

§4. Appendix.

This appendix contains several technical results used in the proof of the main theorem and its corollaries.

Lemma 4.1. *Let M be a field of characteristic $p > 0, \alpha_1, \ldots, \alpha_k \in M$. For $m = 1, \ldots, k$ define*

$$\omega_m = \sum_{j=1}^{k} \alpha_j^m,$$

and let $a_{k-m} = \sum_{i_1>\ldots>i_m} \alpha_{i_1} \ldots \alpha_{i_m}$, *where* $(i_1, \ldots, i_m)$ *range over all subsets of size* m *of* $\{1, \ldots, k\}$. *Let* $k \cong 0 \mod p$, *let* $a_k = 1$ *and assume* $\omega_m = 0$ *for every* $m = 1, \ldots, r$, *where* $r \leq k$, *and* $m \ncong 0 \mod p$. *Then* $a_{k-r} = 0$.

Conversely, if $k \cong 0 \mod p$ *and* $a_{k-i} = 0$ *for every* $i = 1, \ldots, r$, *where* $r \leq k$ *and* $k - i \ncong 0 \mod p$, *then* $\omega_1 = 0, \ldots, \omega_r = 0$.

Proof. For $0 \leq m \leq k-1$ define $W_{0,i} = 1$,

$$W_{m,i} = \sum_{\substack{i_1>\ldots>i_m \\ i_s \neq i}} \alpha_{i_1} \ldots \alpha_{i_m}.$$

Then we have the following equalities:

$$ma_{k-m} = \sum_{i=1}^{k} \alpha_i W_{m-1,i}; \tag{4.1.1}$$

for every $k \geq i > 0$

$$W_{m,i} = a_{k-m} - \alpha_i W_{m-1,i}. \tag{4.1.2}$$

Therefore

$$\begin{aligned}
\omega_1 \cdot a_{k-m} &= \left(\sum_{i=1}^{k} \alpha_i\right) a_{k-m} = \sum_{i=1}^{k} \alpha_i (W_{m,i} + \alpha_i W_{m-1,i}) \\
&= (m+1) a_{k-m-1} + \sum_{i=1}^{k} \alpha_i^2 (a_{k-(m-1)} - \alpha_i W_{m-2,i}) \\
&= (m+1) a_{k-(m-1)} + \omega_2 a_{k-(m-1)} \\
&\quad - \sum_{i=1}^{k} \alpha_i^3 (a_{k-(m-2)} - \alpha_i W_{m-3,i}) = \cdots .
\end{aligned}$$

It is easy to see by induction that

$$(m+1) a_{k-(m-1)} = \sum_{i=1}^{m+1} (-1)^{i+1} \omega_i a_{k-(m+1-i)}. \tag{4.1.3}$$

Therefore, if $\omega_1 = \ldots = \omega_r = 0$, $ma_{k-m} = 0$ for $m = 1, \ldots, r$. This, in turn implies $a_{k-m} = 0$ for $(m, p) = 1$, and the first assertion of the lemma is true. On the other hand, we can rewrite (4.1.3) in the form:

$$ra_{k-r} = \sum_{i=1}^{r-1} (-1)^{i+1} \omega_i a_{k-(r-i)} + (-1)^{r+1} \omega_r, \tag{4.1.4}$$

and proceed by induction. The second statement of the lemma is true for ω_1. Next assume it holds for $r-1$. Then by induction hypothesis, $\sum_{i=1}^{r-1}(-1)^{i+1}\omega_i a_{k-(r-i)} = 0$ and by assumption, either $a_{k-r} = 0$ or $k - r \cong 0 \mod p$, that is $r \cong 0 \mod p$. In any case the left hand side is 0 and we are done. □

Lemma 4.2. *Let $m \in \mathbb{N}$, assume $m = \sum_{i=0}^{[\log_p m]} a_i p^i$ is the p-adic representation of m with respect to some prime p, and let $m_j = \sum_{i=0}^{j-1} a_i p^i$. Then*

$$[m/p^j] = (m - m_j)/p^j.$$

Proof. Enough to show $m_j < p^j$. Indeed, $m_j \leq \sum_{i=0}^{j-1}(p-1)p^i = (p-1)\frac{p^j-1}{p-1} = p^j - 1 < p^j$. □

Lemma 4.3. *Let $m > t$ be natural numbers and let*

$$m = \sum_{i=0}^{[\log_p m]} a_i p^i, \quad t = \sum_{i=0}^{[\log_p t]} b_i p^i$$

be their p-adic representation with respect to some prime p. Then $\binom{m}{t} \cong 0 \mod p$ *if and only if there exists $i \geq 0$ such that $b_i > a_i$.*

Proof. First assume the existence of i as described above and let i_0 be the smallest such i. Then, since for all $0 \leq i \leq i_0 - 1$ $a_i \geq b_i$, for all $j = 0, \ldots, i_0$, $(m-t)_j = m_j - t_j$. On the other hand,

$$(m-t)_{i_0+1} = m_{i_0} - t_{i_0} + (p + a_{i_0} - b_{i_0})p^{i_0}.$$

We also note that, since in general $[x] + [y] \leq [x+y]$, for all i,

$$[t/p^i] + [(m-t)/p^i] \leq [m/p^i]. \tag{4.3.1}$$

Furthemore,

$$[m/p^{i_0+1}] = (m - m_{i_0+1})/p^{i_0+1} = \left(m - \sum_{0 \leq i \leq i_0} a_i p^i\right)/p^{i_0+1}$$

$$[t/p^{i_0+1}] = (t - t_{i_0+1})/p^{i_0+1} = \left(t - \sum_{0 \leq i \leq i_0} b_i p^i\right)/p^{i_0+1}$$

$$[(m-t)/p^{i_0+1}] = (m - t - (m-t)_{i_0+1})/p^{i_0+1}$$

$$= \left((m-t) - \sum_{0 \leq i < i_0} (a_i - b_i)p^i - (p + a_{i_0} - b_{i_0})p^{i_0}\right)/p^{i_0+1}.$$

Therefore, $[t/p^{i_0+1}]+[(m-t)/p^{i_0+1}] = [m/p^{i_0+1}]-1$, and consequently, taking into account (4.3.1), we conclude that

$$\operatorname{ord}_p \binom{m}{t} = \operatorname{ord}_p \left(\frac{m!}{t!(m-t)!}\right) = \sum_{i\in N}[m/p^i] - \sum_{i\in N}[t/p^i] - \sum_{i\in N}[(m-t)/p^i]$$
$$= \sum_{i\neq i_0+1}[m/p^i] - \sum_{i\neq i_0+1}[p^i] - \sum_{i\neq i_0+1}[(m-t)/p^i] + 1 > 0.$$

Conversely, assume for every i, $a_i \geq b_i$. Then $m - t = \sum(a_i - b_i)p^i$, and for every i, $m_i = t_i + (m-t)_i$. Therefore, for every i

$$[m/p^i] = (m-m_i)/p^i = (t-t_i)/p^i+((m-t)-(m-t)_i)/p^i = [t/p^i]+[(m-t)/p^i],$$

and hence,

$$\operatorname{ord}_p \binom{m}{t} = \operatorname{ord}_p \left(\frac{m!}{t!(m-t)!}\right) = \sum_{i\in N}[m/p^i] - \sum_{i\in N}[t/p^i] - \sum_{i\in N}[(m-t)/p^i] = 0.$$

□

References

[1] E. Artin, *Algebraic Numbers and Algebraic Functions*, Notes on Mathematics and Its Applications, Gordon and Breach Science Publishers, New York, 1986.

[2] A. Baker, *Transcendental Number Theory*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990.

[3] C. Chevalley, *Introduction to the Theory of Algebraic Functions f One Variable*, AMS, 1951.

[4] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*, Academic Press, New York, 1966.

[5] M. Fried and M. Jarden, *Field Arithmetic*, Springer Verlag, New York, 1986.

[6] I. Gaal, *Integral Elements with Given Discriminant over Function Fields*, Acta Math. Hung., **S2** (1988), 133-146.

[7] K. Györy, *Sur le polynômes á coefficients entiers et de discriminant donné*, Acta Arith., **23** (1973), 419-426.

[8] ———, *Sur le polynômes á coefficients entiers et de discriminant donné II*, Publ. Math. Debrecen, **21** (1974), 125-144.

[9] ———, *Sur le polynômes á coefficients entiers et de discriminant donné III*, Publ. Math. Debrecen, **23** (1974), 141-165.

[10] ———, *Polynomials with Given Discriminant*, Coll. Math. Soc. Janos Bolyai, 13, (Debrecen,1974). Topics in Number Theory (Edited by P. Turan), North-Holland Publ. Company (Amsterdam-Oxford - New York, 1976), 65-78.

[11] ———, *On Polynomials with Integer Coefficients and Given Discriminant, IV*, Pubt. Math. Debrecen, **25** (1978), 155-167.

[12] ———, *On Polynomials with Integer Coefficients and Given Discriminant, V, padic Generalization*, Acta Mathematica, **32** (1978), 175-190.

[13] ———, *Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains*, J. Reine. Angew. Math., **346** (1984), 54-100.

[14] R. C. Mason, *Diophantine Equations over Function Fields*, London Mathematical Society Lectllre Notes Series: **96**, Cambridge University Press, Cambridge, 1984.

[15] A. J. van der Poorten, *Linear Forms in Logarithms in the p-adic Case*, Proc. Conf. Transcend. Theory, Cambridge, (1976).

[16] A. Shlapentokh, *Diophantine Relations between the Rings of S-integers of One Variable Functions Fields over Fields of Constants of Positive Characteristic*, Journal of Symbolic Logic, **58** No. 1, (1993) 158-192.

Received June 8, 1993. The research for this paper has been partially supported by NSA Mathematical Sciences Research Program Grant MDA904-92-H-3084.

EAST CAROLINA UNIVERSITY
GREENVILLE, NC 27858