Quantitative Chevalley-Weil Theorem for Curves

Yuri Bilu (Bordeaux)
Marco Strambi (Pisa and Bordeaux)
Andrea Surroca*(Basel)

Version of August 9, 2009

(version 1)

Abstract

2000 Mathematics Subject Classification. Primary: ; Secondary: .

Contents

1 Introduction **1**

2 Preliminaries **3**

3 Auxiliary Material **4**

4 Power Series **8**

5 Proximity and Ramification **12**

6 A Tower of $\bar{\mathbb{K}}$-Points **19**

7 The Chevalley-Weil Theorem **20**

1 Introduction

The Chevalley-Weil theorem is one of the most basic principles of the Diophantine analysis. Already Diophantus of Alexandria routinely used reasoning of the kind "if a and b are 'almost' co-prime integers and ab is a square, then each of a and b is 'almost' a square". The Chevalley-Weil theorem provides a general set-up for this kind of arguments.

Theorem 1.1 (Chevalley-Weil) *Let $\widetilde{V} \xrightarrow{\phi} V$ be a finite étale covering of normal projective varieties, defined over a number field $\mathbb{K}$. Then there exists a non-zero integer T such that for any $P \in V(K)$ and $\widetilde{P} \in \widetilde{V}(\bar{K})$ such that $\phi(\widetilde{P}) = P$, the relative discriminant of $\mathbb{K}(\widetilde{P})/\mathbb{K}(P)$ divides T.*

There is also a similar statement for coverings of affine varieties and integral points. See [11, Section 2.8] for more details.

The Chevalley-Weil theorem is indispensable in the Diophantine analysis, because it reduces a Diophantine problem on the variety V to that on the covering variety $\widetilde{V}$, which can often be simpler to deal. In particular, the Chevalley-Weil theorem is used, sometimes implicitly, in the proofs of the great finiteness theorems of Mordell-Weil, Siegel and Faltings.

In view of all this, a quantitative version of the Chevalley-Weil theorem, at least in dimension 1, would be useful to have. One such version appears in Chapter 4 of [1], but it is not explicit in

*Supported by the Marie Curie IEF 025499 of the European Community and the Ambizione Fund 121962 of the Swiss National Science Foundation

all parameters; neither is the version recently suggested by Draziotis and Poulakis [5, 6], who also make some other restrictive assumptions (see Remark 1.4 below).

In the present article we present a version of the Chevalley-Weil theorem in dimension 1, which is explicit in all parameters and considerably sharper than the previous versions. Our approach is different from that of [5, 6] and goes back to [1, 2].

To state our principal results, we have to introduce some notation. Let $\mathbb{K}$ be a number field, $\mathcal{C}$ an absolutely irreducible smooth projective curve $\mathcal{C}$ defined over $\mathbb{K}$, and $x \in \mathbb{K}(\mathcal{C})$ a non-constant $\mathbb{K}$-rational function on $\mathcal{C}$. We also fix a covering $\widetilde{\mathcal{C}} \xrightarrow{\phi} \mathcal{C}$ of $\mathcal{C}$ by another smooth irreducible projective curve $\widetilde{\mathcal{C}}$; we assume that both $\widetilde{\mathcal{C}}$ and the covering ϕ are defined over $\mathbb{K}$. We consider $\mathbb{K}(\mathcal{C})$ as a subfield of $\mathbb{K}(\widetilde{\mathcal{C}})$; in particular, we identify the functions $x \in \mathbb{K}(\mathcal{C})$ and $x \circ \phi \in \mathbb{K}(\widetilde{\mathcal{C}})$.

We also fix one more rational function $y \in \mathbb{K}(\mathcal{C})$ such that $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$ (existence of such y follows from the primitive element theorem). Let $f(X,Y) \in \mathbb{K}[X,Y]$ be the $\mathbb{K}$-irreducible polynomial such that $f(x,y) = 0$ (it is well-defined up to a constant factor). Since $\mathcal{C}$ is absolutely irreducible, so is the polynomial $f(X,Y)$. We put $m = \deg_X f$ and $n = \deg_Y f$.

Similarly, we fix a function $\widetilde{y} \in \mathbb{K}(\widetilde{\mathcal{C}})$ such that $K(\widetilde{\mathcal{C}}) = \mathbb{K}(x, \widetilde{y})$. We let $\tilde{f}(X,\widetilde{Y}) \in \mathbb{K}[X,\widetilde{Y}]$ be an irreducible polynomial such that $\tilde{f}(x,\widetilde{y}) = 0$. We put $\widetilde{m} = \deg_X \tilde{f}$ and $\widetilde{n} = \deg_Y \tilde{f}$. We denote by ν the degree of the covering ϕ, so that $\widetilde{n} = n\nu$.

Remark 1.2 Notice that equations $f(X,Y) = 0$ and $\tilde{f}(X,\widetilde{Y}) = 0$ define affine plane models of our curves $\mathcal{C}$ and $\widetilde{\mathcal{C}}$; *we do not assume these models non-singular.*

In the sequel, $\mathrm{h_p}(\cdot)$ and $\mathrm{h_a}(\cdot)$ denote the projective and the affine absolute logarithmic heights, respectively, see Section 2 for the definitions. We also define normalized logarithmic discriminant $\partial_{\mathbb{L}/\mathbb{K}}$ and the height $\mathrm{h}(S)$ of a finite set of places S as

$$\partial_{\mathbb{L}/\mathbb{K}} = \frac{\log \mathcal{N}_{\mathbb{K}/\mathbb{Q}} \mathcal{D}_{\mathbb{L}/\mathbb{K}}}{[\mathbb{L}:\mathbb{Q}]}, \qquad \mathrm{h}(S) = \frac{\sum_{v\in S} \log \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(v)}{[\mathbb{K}:\mathbb{Q}]};$$

see Section 2 for the details.

Put

$$\begin{aligned} \Omega &= 200mn^3 \log n\bigl(\mathrm{h_p}(f) + 2m + 2n\bigr),\\ \widetilde{\Omega} &= 200\widetilde{m}\widetilde{n}^3 \log \widetilde{n}\bigl(\mathrm{h_p}(\tilde{f}) + 2\widetilde{m} + 2\widetilde{n}\bigr),\\ \Upsilon &= 2\widetilde{n}\bigl(\widetilde{m}\mathrm{h_p}(f) + m\mathrm{h_p}(\tilde{f})\bigr). \end{aligned} \tag{1}$$

Theorem 1.3 ("projective" Chevalley-Weil theorem) *In the above set-up, assume that the covering $\widetilde{\mathcal{C}} \xrightarrow{\phi} \mathcal{C}$ is unramified. Then for every $P \in \mathcal{C}(\bar{\mathbb{K}})$ and $\widetilde{P} \in \widetilde{\mathcal{C}}(\bar{\mathbb{K}})$ such that $\phi(\widetilde{P}) = P$ we have*

$$\partial_{\mathbb{K}(\widetilde{P})/\mathbb{K}(P)} \le 2(\Omega + \widetilde{\Omega} + \Upsilon).$$

Remark 1.4 Draziotis and Poulakis [6, Theorem 1.1], assume that $\mathcal{C}$ is a non-singular plane curve (which is quite restrictive) and that $P \in \mathcal{C}(\mathbb{K})$. Their set-up is slightly different, and the two estimates cannot be compared directly. But it would be safe to say that their estimate is not sharper than

$$\partial_{\mathbb{K}(\widetilde{P})/\mathbb{K}(P)} \le cm^3 N^{30} \widetilde{N}^{13} \left(\mathrm{h_p}(f) + \mathrm{h_p}(\tilde{f})\right) + C,$$

where $N = \deg f$, $\widetilde{N} = \deg \tilde{f}$, the constant c is absolute and C depends of N, $\widetilde{N}$ and the degree $[\mathbb{K}:\mathbb{Q}]$.

Now let S be a finite set of places of $\mathbb{K}$, including all the archimedean places. A point $P \in \mathcal{C}(\bar{\mathbb{K}})$ will be called *S-integral* if for any $v \in M_{\mathbb{K}} \smallsetminus S$ and any extension $\bar{v}$ of v to $\bar{\mathbb{K}}$ we have $|x(P)|_{\bar{v}} \le 1$.

Theorem 1.5 ("affine" Chevalley-Weil theorem) *In the above set-up, assume that the covering $\widetilde{\mathcal{C}} \xrightarrow{\phi} \mathcal{C}$ is unramified outside the poles of x. Then for every S-integral point $P \in \mathcal{C}(\bar{\mathbb{K}})$ and $\widetilde{P} \in \widetilde{\mathcal{C}}(\bar{\mathbb{K}})$ such that $\phi(\widetilde{P}) = P$ we have*

$$\partial_{\mathbb{K}(\widetilde{P})/\mathbb{K}(P)} \le \Omega + \widetilde{\Omega} + \Upsilon + \mathrm{h}(S). \tag{2}$$

Again, Draziotis and Poulakis [5, Theorem 1.1] obtain a less sharp result under more restrictive assumptions.

It might be also useful to have a statement free of the defining equations of the curves $\mathcal{C}$ and $\widetilde{\mathcal{C}}$. Using the result of [3], we obtain versions of Theorems 1.3 and 1.5, which depend only on the degrees and the ramification points of our curves over $\mathbb{P}^1$. For a finite set $A \subset \mathbb{P}^1(\bar{\mathbb{K}})$ we define $\mathrm{h}_{\mathrm{a}}(A)$ as the affine height of the vector whose coordinates are the finite elements of A.

Theorem 1.6 *Let A be a finite subset of $\mathbb{P}^1(\bar{\mathbb{K}})$ such that the covering $\mathcal{C} \xrightarrow{x} \mathbb{P}^1$ is unramified outside A. Put*

$$\delta = [\mathbb{K}(A) : \mathbb{K}], \qquad \widetilde{\mathbf{g}} = \mathbf{g}(\widetilde{\mathcal{C}}), \qquad \Lambda = \big((\widetilde{\mathbf{g}}+1)\widetilde{n}\big)^{25(\widetilde{\mathbf{g}}+1)\widetilde{n}} + 2(\delta - 1).$$

1. *Assume that the covering $\phi : \widetilde{\mathcal{C}} \to \mathcal{C}$ is unramified. Then for every $P \in \mathcal{C}(\bar{\mathbb{K}})$ and $\widetilde{P} \in \widetilde{\mathcal{C}}(\bar{\mathbb{K}})$ such that $\phi(\widetilde{P}) = P$ we have*

$$\partial_{\mathbb{K}(\widetilde{P})/\mathbb{K}(P)} \le \Lambda\big(\mathrm{h}_{\mathrm{a}}(A) + 1\big).$$

2. *Assume that the covering $\phi : \widetilde{\mathcal{C}} \to \mathcal{C}$ is unramified outside the poles of x, and let S be as above. Then for every S-integral point $P \in \mathcal{C}(\bar{\mathbb{K}})$ and $\widetilde{P} \in \widetilde{\mathcal{C}}(\bar{\mathbb{K}})$ such that $\phi(\widetilde{P}) = P$ we have*

$$\partial_{\mathbb{K}(\widetilde{P})/\mathbb{K}(P)} \le \mathrm{h}(S) + \Lambda\big(\mathrm{h}_{\mathrm{a}}(A) + 1\big).$$

2 Preliminaries

Let $\mathbb{K}$ be any number field and let $M_{\mathbb{K}} = M_{\mathbb{K}}^0 \cup M_{\mathbb{K}}^\infty$ be the set of its places, with $M_{\mathbb{K}}^0$ and $M_{\mathbb{K}}^\infty$ denoting the sets of finite and infinite places, respectively. For every place $v \in M_{\mathbb{K}}$ we normalize the corresponding valuation $|\cdot|$ so that its restriction to $\mathbb{Q}$ is the standard infinite or p-adic valuation. Also, we let $\mathbb{K}_v$ be the v-adic completion of $\mathbb{K}$, (in particular, $\mathbb{K}_v$ is $\mathbb{R}$ or $\mathbb{C}$ when v is infinite).

Heights For a vector $\underline{\alpha} = (\alpha_1, \ldots, \alpha_N) \in \bar{\mathbb{Q}}^N$ we define, as usual, the *absolute logarithmic projective height* and *absolute logarithmic affine height* (in the sequel simply *projective* and *affine heights*) by[1]

$$\mathrm{h}_{\mathrm{p}}(\underline{\alpha}) = \frac{1}{[\mathbb{K}:\mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} [\mathbb{K}_v : \mathbb{Q}_v] \log \|\underline{\alpha}\|_v, \qquad \mathrm{h}_{\mathrm{a}}(\underline{\alpha}) = \frac{1}{[\mathbb{K}:\mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} [\mathbb{K}_v : \mathbb{Q}_v] \log^+ \|\underline{\alpha}\|_v, \quad (3)$$

where $\mathbb{K}$ is any number field containing the coordinates of $\underline{\alpha}$,

$$\|\underline{\alpha}\|_v = \max\{|\alpha_0|_v, \ldots, |\alpha_N|_v\}$$

and $\log^+ = \max\{\log, 0\}$. With our choice of normalizations, the right-hand sides in (3) are independent of the choice of the field $\mathbb{K}$. For a polynomial f with algebraic coefficients we denote by $\mathrm{h}_{\mathrm{p}}(f)$ and by $\mathrm{h}_{\mathrm{a}}(f)$ the projective height and the affine height of the vector of its coefficients respectively, ordered somehow.

Logarithmic discriminant Given an extension $\mathbb{L}/\mathbb{K}$ of number fields, we denote by $\partial_{\mathbb{L}/\mathbb{K}}$ the *normalized logarithmic relative discriminant*:

$$\partial_{\mathbb{L}/\mathbb{K}} = \frac{\log \mathcal{N}_{\mathbb{K}/\mathbb{Q}} \mathcal{D}_{\mathbb{L}/\mathbb{K}}}{[\mathbb{L}:\mathbb{Q}]},$$

where $\mathcal{D}_{\mathbb{L}/\mathbb{K}}$ is the usual relative discriminant and $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}$ is the norm map. The properties of this quantity are summarized in the following proposition.

[1] In the definition of the projective height we assume that at least one coordinate of $\underline{\alpha}$ is non-zero.

Proposition 2.1 *1. (additivity in towers) If $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ is a tower of number fields, then $\partial_{\mathbb{M}/\mathbb{K}} = \partial_{\mathbb{L}/\mathbb{K}} + \partial_{\mathbb{M}/\mathbb{L}}$.*

2. (base extension) If $\mathbb{K}'$ is a finite extension of $\mathbb{K}$ and $\mathbb{L}' = \mathbb{L}\mathbb{K}'$ then $\partial_{\mathbb{L}'/\mathbb{K}'} \le \partial_{\mathbb{L}/\mathbb{K}}$.

3. (triangle inequality) If $\mathbb{L}_1$ and $\mathbb{L}_2$ are two extensions of $\mathbb{K}$, then $\partial_{\mathbb{L}_1\mathbb{L}_2/\mathbb{K}} \le \partial_{\mathbb{L}_1/\mathbb{K}} + \partial_{\mathbb{L}_2/\mathbb{K}}$.

These properties will be used without special reference.

Height of a set of places Given a number field $\mathbb{K}$ and finite set of places $S \subset M_{\mathbb{K}}$, we define the *absolute logarithmic height* of this set as

$$\mathrm{h}(S) = \frac{\sum_{v\in S} \log \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(v)}{[\mathbb{K}:\mathbb{Q}]},$$

where the norm $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(v)$ of the place v is the norm of the corresponding prime ideal if v is finite, and is set to be 1 when v is infinite. The properties of this height are summarized in the following proposition.

Proposition 2.2 *1. (field extension) If $\mathbb{L}$ is an extension of $\mathbb{K}$ and $S_{\mathbb{L}}$ is the set of extensions of the places from S to $\mathbb{L}$, then $\mathrm{h}(S_{\mathbb{L}}) \le \mathrm{h}(S) \le [\mathbb{L}:\mathbb{K}]\mathrm{h}(S_{\mathbb{L}})$.*

2. (denominators and numerators) For $\underline{\alpha} \in \bar{\mathbb{K}}^N$ let the sets $\mathrm{Den}_{\mathbb{K}}(\underline{\alpha})$ and $\mathrm{Num}_{\mathbb{K}}(\underline{\alpha})$ consist of all $v \in M_{\mathbb{K}}$ having an extension $\bar{v}$ to $\bar{\mathbb{K}}$ such that $\|\underline{\alpha}\|_{\bar{v}} > 1$, respectively, $\|\underline{\alpha}\|_{\bar{v}} < 1$. Then

$$\mathrm{h}\big(\mathrm{Den}_{\mathbb{K}}(\underline{\alpha})\big) \le [\mathbb{K}(\underline{\alpha}):\mathbb{K}]\mathrm{h_a}(\underline{\alpha}),$$
$$\mathrm{h}\big(\mathrm{Num}_{\mathbb{K}}(\underline{\alpha})\big) \le [\mathbb{K}(\underline{\alpha}):\mathbb{K}]\big(\mathrm{h_a}(\underline{\alpha}) - \mathrm{h_p}(\underline{\alpha})\big) \qquad (\underline{\alpha} \ne \underline{0}).$$

In particular, for $\alpha \in \bar{\mathbb{K}}^*$ we have $\mathrm{h}\big(\mathrm{Num}_{\mathbb{K}}(\alpha)\big) \le [\mathbb{K}(\alpha):\mathbb{K}]\mathrm{h_a}(\alpha)$.

This will also be used without special reference.

Sums over primes We shall systematically use the following estimates from [12].

$$\sum_{p\le x} 1 \le 1.26\frac{x}{\log x}, \tag{4}$$

$$\sum_{p\le x} \log p \le 1.02x, \tag{5}$$

$$\sum_{p\le x} \frac{\log p}{p-1} \le 2\log x. \tag{6}$$

See [12], Corollary 1 of Theorem 2 for (4), Theorem 9 for (5), and (6) follows easily from the Corollary of Theorem 6.

3 Auxiliary Material

In this section we collect miscellaneous facts, mostly elementary and/or well-known, to be used in the article.

3.1 Integral Elements

In this subsection R is an integrally closed integral domain and $\mathbb{K}$ its quotient field.

Lemma 3.1 *Let $\mathbb{L}$ be a finite separable extension of $\mathbb{K}$ of degree n and $\bar{R}$ the integral closure of R in $\mathbb{L}$. Let $\omega_1, \ldots, \omega_n \in \bar{R}$ form a base of $\mathbb{L}$ over $\mathbb{K}$. We denote by Δ the discriminant of this basis: $\Delta = \Big(\det\,[\sigma_i(\omega_j)]_{ij}\Big)^2$, where $\sigma_1, \ldots, \sigma_n : \mathbb{L} \hookrightarrow \bar{\mathbb{K}}$ are the distinct embeddings of $\mathbb{L}$ into $\bar{\mathbb{K}}$. Then $\bar{R} \subset \Delta^{-1}(R\omega_1 + \cdots + R\omega_n)$.*

Proof This is standard. Write $\beta \in \bar{R}$ as $\beta = a_1\omega_1 + \cdots + a_n\omega_n$ with $a_i \in \mathbb{K}$. Solving the system of linear equations

$$\sigma_i(\beta) = a_1\sigma_i(\omega_1) + \cdots + a_n\sigma_i(\omega_n) \qquad (i = 1, \ldots, n)$$

using the Kramer rule, we find that the numbers Δa_i are integral over R. Since R is integrally closed, we have $\Delta a_i \in R$. $\square$

Corollary 3.2 *Let $f(T) = f_0T^n + f_1T^{n-1} + \cdots + f_n \in R[T]$ be a $\mathbb{K}$-irreducible polynomial, and $\alpha \in \bar{\mathbb{K}}$ one of its roots. Let $\bar{R}$ be the integral closure of R in $\mathbb{K}(\alpha)$. Then $\bar{R} \subset \Delta(f)^{-1}R[\alpha]$. where $\Delta(f)$ is the discriminant of f.*

Proof It is well-known that the quantities

$$\omega_1 = 1, \quad \omega_2 = f_0\alpha, \quad \omega_3 = f_0\alpha^2 + f_1\alpha, \quad \ldots \qquad \omega_n = f_0\alpha^{n-1} + f_1\alpha^{n-2} + \cdots + f_{n-2}\alpha$$

are integral over R; see, for example, [14, page 183]. Applying Lemma 3.1 to the basis $\omega_1, \ldots, \omega_n$, we complete the proof. $\square$

3.2 Local Lemmas

In this subsection $\mathbb{K}$ is a field of characteristic 0 supplied with a discrete valuation v. We denote by $\mathcal{O}_v$ the local ring of v. We say that a polynomial $F(X) \in \mathbb{K}[X]$ is *v-monic* if its leading coefficient is a v-adic unit[2].

Lemma 3.3 *Let $F(X) \in \mathcal{O}_v[X]$ be a v-monic polynomial, and let $\eta \in \bar{\mathbb{K}}$ be a root of F. (We do not assume F to be the minimal polynomial of η over $\mathbb{K}$, because we do not assume it $\mathbb{K}$-irreducible.) Assume that v ramifies in the field $\mathbb{K}(\eta)$. Then $|F'(\eta)|_v < 1$ (for any extension of v to $\mathbb{K}(\eta)$).*

Proof We may assume that $\mathbb{K}$ is v-complete, and we let $\mathfrak{d} = \mathfrak{d}_{\mathbb{K}(\eta)/\mathbb{K}}$ be the different of the extension $\mathbb{K}(\eta)/\mathbb{K}$. Since v ramifies in $\mathbb{K}(\eta)$, the different is a non-trivial ideal of $\mathcal{O}_v$.

Since η is a root of a v-monic polynomial, it is integral over $\mathcal{O}_v$. Let $G(X) \in \mathcal{O}_v[X]$ be the minimal polynomial of η. Then the different $\mathfrak{d}$ divides $G'(\eta)$, which implies that $|G'(\eta)|_v < 1$.

Write $F(X) = G(X)H(X)$. By the Gauss lemma, $H(X) \in \mathcal{O}_v[X]$. Since $F'(\eta) = G'(\eta)H(\eta)$, we obtain $|F'(\eta)|_v \le |G'(\eta)|_v < 1$, as wanted. $\square$

Given a polynomial $F(X)$ over some field of characteristic 0, we define by $\widehat{F}(X)$ the *radical* of F, that is, the separable polynomial, having the same roots and the same leading coefficient as F:

$$\widehat{F}(X) = f_0 \prod_{F(\alpha)=0} (X - \alpha),$$

where f_0 is the leading coefficient of F and the product runs over the **distinct** roots of F (in an algebraic closure of the base field).

Lemma 3.4 *Assume that $F(X) \in \mathcal{O}_v[X]$. Then the radical $\widehat{F}(X)$ is in $\mathcal{O}_v[X]$ as well. Also, if $|F(\xi)|_v < 1$ for some $\xi \in \mathcal{O}_v$, then we have $|\widehat{F}(\xi)|_v < 1$ as well.*

[2] We say that α is a v-adic unit if $|\alpha|_v = 1$.

Proof Let $F(X) = P_1(X)^{\alpha_1} \cdots P_k(X)^{\alpha_k}$ be the irreducible factorization of F in $\mathbb{K}[X]$. The Gauss Lemma implies that we can choose $P_i(X) \in \mathcal{O}_v[X]$ for $i = 1, \ldots, k$. Since the characteristic of $\mathbb{K}$ is 0, every P_i is separable. Obviously, the leading coefficient of the separable polynomial $P_1(X) \cdots P_k(X)$ divides that of $F(X)$ in the ring $\mathcal{O}_v$. Hence $\widehat{F}(X) = \gamma P_1(X) \cdots P_k(X)$ with some $\gamma \in \mathcal{O}_v$, which proves the first part of the lemma. The second part is obvious: if $|F(\xi)|_v < 1$ then $|P_i(\xi)|_v < 1$ for some i, which implies $|\widehat{F}(\xi)|_v < 1$. □

Lemma 3.5 *Let $F(X) \in \mathcal{O}_v[X]$ and $\xi \in \mathcal{O}_v$ satisfy $|F(\xi)|_v < 1$ and $|F'(\xi)|_v = 1$. Let $\bar{v}$ be an extension of v to $\bar{\mathbb{K}}$. Then there exists exactly one root $\alpha \in \bar{\mathbb{K}}$ of F such that $|\xi - \alpha|_{\bar{v}} < 1$.*

Proof This is a consequence of Hensel's lemma. Extending $\mathbb{K}$, we may assume that it contains all the roots of F. Hensel's lemma implies that there is exactly one root α in the v-adic completion of $\mathbb{K}$ with the required property. This root must belong to $\mathbb{K}$. □

Lemma 3.6 *Let $F(X), G(X) \in \mathcal{O}_v[X]$ and $\alpha, \xi \in \mathcal{O}_v$ satisfy*

$$F(X) = (X - \alpha)^m G(X), \qquad G(\alpha) \neq 0, \qquad |\xi - \alpha|_v < |G(\alpha)|_v$$

with some non-negative integer m. Expand the rational function $F(X)^{-1}$ into the Laurent series at α. Then this series converges at $X = \xi$.

Proof Substituting $X \mapsto \alpha + X$, we may assume $\alpha = 0$, in which case the statement becomes obvious. □

3.3 Heights

Recall that, for a polynomial f with algebraic coefficients, we denote by $\mathrm{h_p}(f)$ and by $\mathrm{h_a}(f)$, respectively, the projective height and the affine height of the vector of its coefficients ordered somehow. More generally, the height $\mathrm{h_a}(f_1, \ldots, f_s)$ of a finite system of polynomials is, by definition, the affine height of the vector formed of all the non-zero coefficients of all these polynomials.

Lemma 3.7 *Let $f_1, \ldots, f_s$ be polynomials in $\bar{\mathbb{Q}}[X_1, \ldots, X_r]$ and put*

$$N = \max\{\deg f_1, \ldots, \deg f_s\}, \qquad h = \mathrm{h_a}(f_1, \ldots, f_s).$$

Let also g be a polynomial in $\bar{\mathbb{Q}}[Y_1, \ldots, Y_s]$. Then

1. $\mathrm{h_a}\left(\prod_{i=1}^s f_i\right) \le \sum_{i=1}^s \mathrm{h_a}\left(f_i\right) + \log(r+1) \sum_{i=1}^{s-1} \deg f_i$,
2. $\mathrm{h_p}\left(\prod_{i=1}^s f_i\right) \ge \sum_{i=1}^s \mathrm{h_p}\left(f_i\right) - \sum_{i=1}^s \deg f_i$,
3. $\mathrm{h_a}\big(g\left(f_1, \ldots, f_s\right)\big) \le \mathrm{h_a}(g) + \big(h + \log(s+1) + N\log(r+1)\big) \deg g$.

Notice that we use the projective height in item 2, and the affine height in the other items.

Proof Item 2 is the famous Gelfond inequality, see, for instance, Proposition B.7.3 in [9]. The rest is an immediate consequence of Lemma 1.2 from [10]. □

Remark 3.8 If in item 3 we make substitution $Y_i = f_i$ only for a part of the indeterminates Y_i, say, for t of them, where $t \le s$, then we may replace $\log(s+1)$ by $\log(t+1)$, and $\deg g$ by the degree with respect to these indeterminates:

$$\mathrm{h_a}\big(g\left(f_1, \ldots, f_t, Y_{t+1}, \ldots, Y_s\right)\big) \le \mathrm{h_a}(g) + \big(h + \log(t+1) + N\log(r+1)\big) \deg_{Y_1, \ldots, Y_t} g.$$

Remark 3.9 When all the f_i are just linear polynomials in one variable, item 2 can be refined as follows: let $F(X)$ be a polynomial of degree ρ, and $\beta_1, \ldots, \beta_\rho$ are its roots (counted with multiplicities); then

$$\mathrm{h_a}(\beta_1) + \cdots + \mathrm{h_a}(\beta_\rho) \leq \mathrm{h_p}(F) + \log(\rho + 1).$$

This is a classical result of Mahler, see, for instance, [13, Lemma 3].

Corollary 3.10 *Let f and g be polynomials with algebraic coefficients such that f divides g. Let also a be a non-zero coefficient of f. Then*

1. $\mathrm{h_p}(f) \leq \mathrm{h_p}(g) + \deg g$,
2. $\mathrm{h_a}(f) \leq \mathrm{h_p}(g) + \mathrm{h_a}(a) + \deg g$.

Proof Item 1 is a direct consequence of item 2 of Lemma 3.7. For item 2 remark that one of the coefficients of f/a is 1, which implies that

$$\mathrm{h_a}(f/a) = \mathrm{h_p}(f/a) = \mathrm{h_p}(f) \leq \mathrm{h_p}(g) + \deg g.$$

Since $\mathrm{h_a}(f) \leq \mathrm{h_a}(a) + \mathrm{h_a}(f/a)$, the result follows. □

Corollary 3.11 *Let α be an algebraic number and $f \in \bar{\mathbb{Q}}[X, Y]$ be a polynomial with algebraic coefficients, let also $f^{(\alpha)}(X, Y) = f(X + \alpha, Y)$ then*

$$\mathrm{h_a}(f^{(\alpha)}) \leq \mathrm{h_a}(f) + m\mathrm{h_a}(\alpha) + 2m \log 2,$$

where $m = \deg_X f$.

Proof This is a direct application of item 3 of Lemma 3.7, together with Remark 3.8. □

In one special case item 3 of Lemma 3.7 can be refined.

Lemma 3.12 *Let*

$$F_{ij}(X) \in \bar{\mathbb{Q}}[X] \qquad (i, j = 1, \ldots, s)$$

be polynomials of degree bounded by μ and of affine height bounded by h; then

$$\mathrm{h_a}\left(\det(F_{ij})\right) \leq sh + s(\log s + \mu \log 2).$$

For the proof see [10], end of Section 1.1.1.

We also need an estimate for both the affine and the projective height of the Y-resultant $R_f(X)$ of a polynomial $f(X, Y) \in \bar{\mathbb{Q}}[X, Y]$ and its Y-derivative f'_Y, in terms of the affine (respectively, projective) height of f.

Lemma 3.13 *Let $f(X, Y) \in \bar{\mathbb{Q}}[X, Y]$ be of X-degree m and Y-degree n. Then*

$$\mathrm{h_a}(R_f) \leq (2n-1)\mathrm{h_a}(f) + (2n-1)\left(\log(2n^2) + m \log 2\right), \tag{7}$$

$$\mathrm{h_p}(R_f) \leq (2n-1)\mathrm{h_p}(f) + (2n-1)\log\left((m+1)(n+1)\sqrt{n}\right), \tag{8}$$

Proof Estimate (8) is due to Schmidt [13, Lemma 4]. To prove (7), we invoke Lemma 3.12. Since $R_f(X)$ can be presented as a determinant of dimension $2n-1$, whose entries are polynomials of degree at most m and of affine height at most $\mathrm{h_a}(f) + \log n$, the result follows after an obvious calculation. □

Remark 3.14 Estimate (7) holds true also when $m = 0$. We obtain the following statement: the resultant R_f of a polynomial $f(X)$ and its derivative $f'(X)$ satisfies

$$\mathrm{h_a}(R_f) \leq (2\deg f - 1)\mathrm{h_a}(f) + (2\deg f - 1)\log\left(2(\deg f)^2\right).$$

3.4 Discriminants

We need some estimates for the discriminant of a number field in terms of the heights of its generators. In this subsection $\mathbb{K}$ is a number field, $d = [\mathbb{K} : \mathbb{Q}]$ and $\mathcal{N}(\cdot) = \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\cdot)$. The following result is due to Silverman [16, Theorem 2].

Lemma 3.15 *Let $\underline{a} = (a_1, \ldots, a_k)$ be a point in $\bar{\mathbb{Q}}^k$. Put $\nu = [\mathbb{K}(\underline{a}) : \mathbb{K}]$. Then*

$$\partial_{\mathbb{K}(\underline{a})/\mathbb{K}} \le 2(\nu - 1)\mathrm{h_a}(\underline{a}) + \log \nu. \qquad \square$$

This has the following consequence.

Corollary 3.16 *Let $F(X) \in \mathbb{K}[X]$ be a polynomial of degree N. Then*

$$\sum_{F(\alpha)=0} \partial_{\mathbb{K}(\alpha)/\mathbb{K}} \le 2(N-1)\mathrm{h_p}(F) + 3N \log N, \tag{9}$$

the sum being over the roots of F.

Proof Since for any root α we have $[\mathbb{K}(\alpha) : \mathbb{K}] \le N$, we estimate the left-hand side of (9) as

$$2(N-1) \sum_{F(\alpha)=0} \mathrm{h_a}(\alpha) + N \log N$$

Remark 3.9 allows us to bound the sum on the right by $\mathrm{h_p}(F) + \log(N + 1)$. Now, to complete the proof, just remark that $(N - 1)\log(N + 1) \le N \log N$. $\square$

We shall also need a bound for the discriminant of a different nature, known as the *Dedekind-Hensel inequality* (see [4, page 397] for historical comments and further references). This inequality gives an estimate of the relative discriminant of a number field extension in terms of the ramified places.

Lemma 3.17 *Let $\mathbb{K}$ be a number field of degree d over $\mathbb{Q}$, and $\mathbb{L}$ an extension of $\mathbb{K}$ of finite degree ν, and let $\mathrm{Ram}(\mathbb{L}/\mathbb{K})$ be the set of places of $\mathbb{K}$ ramified in $\mathbb{L}$. Then*

$$\partial_{\mathbb{L}/\mathbb{K}} \le \frac{\nu - 1}{\nu}\mathrm{h}\big(\mathrm{Ram}(\mathbb{L}/\mathbb{K})\big) + 1.26\nu. \tag{10}$$

This is Proposition 4.2.1 from [2] (though the notation in [2] is different, and the quantity estimated therein is $\nu\partial\mathbb{L}/\mathbb{K}$ in our notation), the only difference being that the error term is now explicit. The proof is the same as in [2], but in the very last line one should use the estimate $\sum_{p \le \nu} 1 \le 1.26\nu/\log \nu$, which is (4).

A similar estimate was obtained by Serre [15, Proposition 4]. However, (10) is more suitable for our purposes.

It is useful to have an opposite estimate as well. The following is obvious.

Lemma 3.18 *In the set-up of Lemma 3.17 we have $\mathrm{h}\big(\mathrm{Ram}(\mathbb{L}/\mathbb{K})\big) \le \nu\partial_{\mathbb{L}/\mathbb{K}}$.*

4 Power Series

Our main technical tool in the quantitative Eisenstein theorem, based on the work of Dwork, Robba, Schmidt and van der Poorten [7, 8, 13]. Let

$$y = \sum_{k=-k_0}^{\infty} a_k x^{k/e} \tag{11}$$

be an algebraic power series with coefficients in $\bar{\mathbb{Q}}$, where we assume $k_0 \ge 0$ and $a_{-k_0} \ne 0$ when $k_0 > 0$. The classical Eisenstein theorem tells that the coefficients of this series belong to some number field, that for every valuation v of this field $|a_k|_v$ grows at most exponentially in k, and for all but finitely many v we have $|a_k|_v \le 1$ for all k. We need a quantitative form of this statement, in terms of an algebraic equation $f(x, y) = 0$ satisfied by y.

4.1 Eisenstein Theorem

Thus, let $f(X,Y) \in \mathbb{K}(X,Y)$ be a polynomial over a number field $\mathbb{K}$. We put

$$d = [\mathbb{K} : \mathbb{Q}], \qquad m = \deg_X f, \qquad n = \deg_Y f. \tag{12}$$

Write

$$f(X,Y) = f_0(X)Y^n + f_1(X)Y^{n-1} + \dots \tag{13}$$

and put

$$u = \mathrm{ord}_0 f_0. \tag{14}$$

If the series y, written as (11), satisfies the equation $f(x,y) = 0$, then

$$k_0/e \le u \le m.$$

Also, if $\mathbb{L}$ is the extension of $\mathbb{K}$ generated by all the coefficients a_k of the series y, then it is well-known that

$$[\mathbb{L} : \mathbb{K}] \le n.$$

Finally, for $v \in M_{\mathbb{K}}$ we denote by d_v its local degree over $\mathbb{Q}$, and by $\mathcal{N}v$ its absolute norm:

$$d_v = [\mathbb{K}_v : \mathbb{Q}_v], \qquad \mathcal{N}v = \mathcal{N}_{\mathbb{K}/\mathbb{Q}}(v). \tag{15}$$

With this notation, the height $\mathrm{h}(S)$ of a finite set of places $S \subset M_{\mathbb{K}}$ is given by $d^{-1}\sum_{v\in S} d_v \log \mathcal{N}v$.

The following theorem is a combination of the ideas and results from [7, 8, 13].

Theorem 4.1 *Let $\mathbb{K}$ be a number field and $f(X,Y) \in \mathbb{K}(X,Y)$. We use notation (12–15). For every $v \in M_{\mathbb{K}}$ there exist real numbers $A_v, B_v \ge 1$, with $A_v = B_v = 1$ for all but finitely many v, such that the following holds. First of all,*

$$d^{-1} \sum_{v\in M_{\mathbb{K}}} d_v \log A_v \le (2n-1)\mathrm{h_p}(f) + 6n^2 + 2n\log m, \tag{16}$$

$$d^{-1} \sum_{v\in M_{\mathbb{K}}} d_v \log B_v \le \mathrm{h_p}(f) + \log(2n). \tag{17}$$

Further, for any non-archimedean valuation v of $\mathbb{K}$ we have $\frac{d_v \log B_v}{\log \mathcal{N}v} \in \mathbb{Z}$ and

$$\mathrm{h}\left(\left\{v \in M_{\mathbb{K}}^0 : \frac{d_v \log A_v}{\log \mathcal{N}v} \notin \mathbb{Z}\right\}\right) \le (2n-1)\mathrm{h_p}(f) + n(2\log m + 3\log n + 5). \tag{18}$$

Finally, let y be an algebraic power series, written as in (11), and satisfying $f(x,y) = 0$. Let $\mathbb{L}$ be the number field generated over $\mathbb{K}$ by the coefficients of y. Then for any valuation $w|v$ of $M_{\mathbb{L}}$ and for all $k \ge -k_0$ we have

$$|a_k|_w \le B_v A_v^{u+k/e}, \tag{19}$$

where u is defined in (14).

Proof This is, essentially, [2, Theorem 2.1], with the error terms made explicit. (Warning: we denote by B_v the quantity denoted in [2] by A'_v.) Below we briefly review the proof from [2], indicating the changes needed to get explicit error terms.

Denote by $R_f(X)$ the Y-resultant of f and f'_Y, and put

$$\mu = \mathrm{ord}_0 R_f(X), \tag{20}$$

(notice that μ has a slightly different meaning in [2]). We may normalize the polynomial f to have $f_0(X) = X^u f_0^*(X)$ with $f_0^*(0) = 1$. We also write $R_f(X) = AX^\mu R^*(X)$ with $R^*(0) = 1$.

Let $\alpha_1,\dots,\alpha_t$ be the roots of $R^*(X)$. For every valuation v in $\mathbb{K}$ fix an extension to $\mathbb{K}(\alpha_1,\dots,\alpha_t)$ and put

$$\sigma_v=\min(1,|\alpha_1|_v,\dots,|\alpha_t|_v).$$

Clearly σ_v does not depend on the fixed prolongation. Schmidt [13, Lemma 5] proves that

$$d^{-1}\sum_{v\in M_{\mathbb{K}}} d_v\log(1/\sigma_v)\le(2n-1)\mathrm{h}_{\mathrm{p}}(f)+2n\log\left((m+1)(n+1)\sqrt{n}\right). \tag{21}$$

(Notice that Schmidt uses a different normalization of valuations).

For every valuation v of $\mathbb{K}$ we define real numbers $A_v,B_v\ge 1$ as follows:

$$A_v=\begin{cases}2^n/\sigma_v, & p(v)=\infty,\\ 1/\sigma_v, & n<p(v)<\infty,\\ \left(np(v)^{1/(p(v)-1)}\right)^n/\sigma_v, & p(v)\le n,\end{cases}\qquad B_v=\begin{cases}2n|f|_v, & p(v)=\infty,\\ |f|_v, & p(v)<\infty,\end{cases}$$

where $p(v)$ is the underlying prime. Notice that $A_v=B_v=1$ for all but finitely many v.

Inequality (19) is established in [2, Section 2.3]. Inequality (17) is immediate from the definition of B_v. Further,

$$\begin{aligned}d^{-1}\sum_{p(v)\le n} d_v\log\left(np(v)^{1/(p(v)-1)}\right)^n&=d^{-1}n\sum_{p\le n}\sum_{p(v)=p}d_v\left(\log n+\frac{\log p}{p-1}\right)\\&=n\sum_{p\le n}\left(\log n+\frac{\log p}{p-1}\right)\\&\le 1.26n^2+2n\log n,\end{aligned}$$

where we used (4) and (6) for the last estimate. Combining this with (21), we obtain

$$d^{-1}\sum_{v\in M_{\mathbb{K}}} d_v\log A_v\le(2n-1)\mathrm{h}_{\mathrm{p}}(f)+n\log 2+1.26n^2+2n\log n+2n\log\left((m+1)(n+1)\sqrt{n}\right),$$

which implies (16) after a routine calculation.

The definition of B_v implies that $\frac{d_v\log B_v}{\log\mathcal{N}v}\in\mathbb{Z}$. We are left with (18). Write the set on the left of (18) as $S_1\cup S_2$, where S_1 consists of v with $p(v)\le n$, and S_2 of those with $p(v)>n$. Obviously,

$$\mathrm{h}(S_1)\le\sum_{p\le n}\log p\le 1.02n, \tag{22}$$

where we use (5). For S_2 we have the estimate (see [2], second displayed equation on page 134)

$$\begin{aligned}\mathrm{h}(S_2)&\le\mathrm{h}_{\mathrm{p}}(R^*)+\log(1+\deg R^*)\\&\le(2n-1)\mathrm{h}_{\mathrm{p}}(f)+(2n-1)\log\left((m+1)(n+1)\sqrt{n}\right)+\log(2mn),\end{aligned}$$

where we use the property $\mathrm{h}_{\mathrm{p}}(R^*)=\mathrm{h}_{\mathrm{p}}(R)$ and Lemma 3.13 for the last inequality. Together with (22), this implies (18) after an easy calculation. □

Here is one consequence that we shall use.

Corollary 4.2 *In the set-up of Theorem 4.1, let T be the subset of $v\in M_K$ such that one of the inequalities $A_v>1$ or $B_v>1$ holds. Then $\mathrm{h}(T)\le(4n-1)\mathrm{h}_{\mathrm{p}}(f)+13n^2+4n\log m$.*

Proof For $v\in T$ we have either $\log\mathcal{N}v\le d_v\log A_v$ or $\log\mathcal{N}v\le d_v\log B_v$ or $\frac{d_v\log A_v}{\log\mathcal{N}v}\notin\mathbb{Z}$. Partitioning the set into three sets and using (16), (17) and (18), we obtain the result after an easy calculation. □

4.2 Fields Generated by the Coefficients

We also need to bound the discriminant of the number field, generated by the coefficients of an algebraic power series. Such a bound is obtained in [2, Lemma 2.4.2]. Here we obtain a similar statement, explicit in all parameters.

Proposition 4.3 *In the set-up of Theorem 4.1, let $\mathbb{L}$ be the number field generated by the coefficients of the series y. Put $\nu = [\mathbb{L} : \mathbb{K}]$, and define u and μ as in (14) and (20). Then*

$$\partial_{\mathbb{L}/\mathbb{K}} \le (4n\mu + 4nu\nu + 2\nu)\,\mathrm{h_p}(f) + (\mu + u\nu)\left(12n^2 + 4n\log m\right) + 3\nu\log(2n). \tag{23}$$

Proof As we have seen in [2, Lemma 2.4.2], the field $\mathbb{L}$ is generated over K by $a_{-k_0}, \dots, a_\kappa$, where $\kappa \le e\mu/\nu$ (we recall that in [2] the quantity μ has a slightly different definition and, is less than or equal to our μ). Using Theorem 4.1 we estimate the height of the vector $\underline{a} = (a_{-k_0}, \dots, a_\kappa)$ as follows:

$$\begin{aligned}
\mathrm{h_a}(\underline{a}) &\le d^{-1}\sum_{v\in M_{\mathbb{K}}} d_v \log B_v + d^{-1}\left(u + \frac{\kappa}{e}\right)\sum_{v\in M_{\mathbb{K}}} d_v\log A_v\\
&\le \mathrm{h_p}(f) + \log(2n) + \left(\frac{\mu}{\nu} + u\right)\left((2n-1)\mathrm{h_p}(f) + 6n^2 + 2n\log m\right)\\
&\le \left(2n\left(\frac{\mu}{\nu} + u\right) + 1\right)\mathrm{h_p}(f) + \left(\frac{\mu}{\nu} + u\right)\left(6n^2 + 2n\log m\right) + \log(2n).
\end{aligned}$$

Applying now Lemma 3.15, we obtain

$$\partial_{\mathbb{L}/\mathbb{K}} \le (4n\mu + 4nu\nu + 2\nu)\,\mathrm{h_p}(f) + (\mu + u\nu)\left(12n^2 + 4n\log m\right) + 2\nu\log(2n) + \log\nu,$$

which is even sharper than (23). □

Let now $\{y_1, \dots, y_n\}$ be the set of all power series roots of f at 0, that is,

$$f(x, Y) = f_0(x)(Y - y_1)\cdots(Y - y_n),$$

and let $\mathbb{L}_i$ be the field generated by the coefficients of y_i. Summing up and estimating each degree $[\mathbb{L}_i : \mathbb{Q}]$ by n, we obtain the following consequence of Proposition 4.3.

Corollary 4.4 *In the previous set-up, the following inequality holds*

$$\sum_{i=1}^n \partial_{\mathbb{L}_i/\mathbb{K}} \le \left(4n^2\mu + 4n^3u + 2n^2\right)\mathrm{h_p}(f) + \left(\mu n + un^2\right)\left(12n^2 + 4n\log m\right) + 3n^2\log(2n).$$

4.3 The "Essential" Coefficients

In this subsection the letter q always denotes a prime number. Let us assume now that the series (11) has exact ramification e; that is, it cannot be written as a series in $x^{1/e'}$ with $e' < e$. Then for every q dividing e there exist at least one k such that $q \nmid k$ and $a_k \ne 0$. We denote by $\kappa(q)$ the smallest k with this property, and we call $a(q) = a_{\kappa(q)}$ the *q-essential* coefficient of the series (11). We want to estimate the height of the q-essential coefficients. We again put $\nu = [\mathbb{L} : \mathbb{K}]$, and define u and μ as in (14) and (20).

Proposition 4.5 *In the above set-up, the following inequality holds:*

$$\sum_{q|e} \mathrm{h_a}(a(q)) \le \log_2 e\left(u + \frac{\mu}{\nu}\right)\left(2n\mathrm{h_p}(f) + 6n^2 + 2n\log m\right). \tag{24}$$

Proof We can bound the number $\kappa(q)$ by

$$\kappa(q) \le \frac{e\mu}{\nu(q-1)} - 1$$

by [2, Lemma 2.4.4]. We shall use the trivial bounds

$$\sum_{q|e} \frac{1}{q-1} \le \sum_{q|e} 1 \le \log_2 e. \tag{25}$$

Now, Theorem 4.1 gives us the explicit bound

$$\mathrm{h_a}(a(q)) \le \left(u + \frac{\mu}{\nu(q-1)}\right)\left(2n\mathrm{h_p}(f) + 6n^2 + 2n\log m\right)$$

for the height of the q-essential coefficient $\mathrm{h_a}(a_{\kappa(q)})$. Summing up over all primes q dividing e, and simplifying by (25) we obtain the result. □

Corollary 4.6 *Define y_i as in the previous section and let $a_i(q)$ denote the q-essential coefficient of the series y_i. Then*

$$\sum_{i=1}^{n}\sum_{q|e} \mathrm{h_a}(a_i(q)) \le (u+\mu)\left(2n^2\mathrm{h_p}(f) + 6n^3 + 2n^2\log m\right)\log_2 n.$$

Proof Let e_i be the ramification of the series y_i. Summing up and using $\log_2 e_i \le \log_2 n$ and $1/\nu \le 1$, we obtain the result. □

5 Proximity and Ramification

This section is the technical heart of the article. We consider a covering $\mathcal{C} \to \mathbb{P}^1$, a point Q on $\mathcal{C}$ and a non-archimedean place v, and show, that in a certain v-adic neighborhood of Q, the v-ramification is the same and is determined by the ramification of Q over $\mathbb{P}^1$. Roughly speaking, "geometric ramification defines arithmetic ramification". It is not difficult to make a qualitative statement of this kind, but it is a rather delicate task to make everything explicit.

Thus, in this section we fix, once and for all:

- a number field $\mathbb{K}$;
- an absolutely irreducible smooth projective curve $\mathcal{C}$ defined over $\mathbb{K}$;
- a non-constant rational function $x \in \mathbb{K}(\mathcal{C})$;
- one more rational function $y \in \mathbb{K}(\mathcal{C})$ such that $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$ (existence of such y follows from the primitive element theorem).

Let $f(X, Y) \in \mathbb{K}[X, Y]$ be the $\mathbb{K}$-irreducible polynomial such that $f(x, y) = 0$ (it is well-defined up to a constant factor). Since $\mathcal{C}$ is absolutely irreducible, so is the polynomial $f(X, Y)$.

We put $m = \deg_X f$, $n = \deg_Y f$, and write

$$f(X, Y) = f_0(X)Y^n + f_1(X)Y^{n-1} + \cdots + f_n(X). \tag{26}$$

Let $Q \in \mathcal{C}(\bar{\mathbb{K}})$ be a $\bar{\mathbb{K}}$-point of $\mathcal{C}$, which is not a pole of x. We let $\alpha = x(Q)$ and we denote by e_Q the ramification index of x at Q (that is, $e = \mathrm{ord}_Q(x - \alpha)$). When it does not cause a confusion (in particular, everywhere in this section) we write e instead of e_Q. Fix a primitive e-th root of unity $\zeta = \zeta_e$. Then there exist e equivalent Puiseux expansions of y at Q:

$$y_i^{(Q)} = \sum_{k=-k^{(Q)}}^{\infty} a_k^{(Q)} \zeta^{ik} (x-\alpha)^{k/e} \qquad (i = 0, \ldots, e-1), \tag{27}$$

where $k^{(Q)} = \max\{0, -\mathrm{ord}_Q(y)\}$.

Let $\bar{v}$ be a valuation of $\bar{\mathbb{K}}$. We say that the series (27) converge $\bar{v}$-adically at $\xi \in \bar{\mathbb{K}}$, if, for a fixed e-th root $\sqrt[e]{\xi - \alpha}$, the e numerical series

$$\sum_{k=-k^{(Q)}}^{\infty} a_k^{(Q)} \left(\zeta^i \sqrt[e]{\xi - \alpha}\right)^k \qquad (i = 0, \ldots, e-1)$$

converge in the $\bar{v}$-adic topology. We denote by $y_i^{(Q)}(\xi)$, with $i = 0, \ldots, e-1$, the corresponding sums. While the individual sums depend on the particular choice of the root $\sqrt[e]{\xi - \alpha}$, the very fact of convergence, as well as the set $\left\{y_0^{(Q)}(\xi), \ldots, y_{e-1}^{(Q)}(\xi)\right\}$ of the sums, are independent of the choice of the root.

Now we are ready to introduce the principal notion of this section, that of proximity of a point to a different point with respect to a given valuation $\bar{v} \in M_{\bar{\mathbb{K}}}$.

Definition 5.1 *Let $P \in \mathcal{C}(\bar{\mathbb{K}})$ be a $\bar{\mathbb{K}}$-point of $\mathcal{C}$, not a pole of x, and put $\xi = x(P)$. We say that P is $\bar{v}$-**adically close** to Q if the following conditions are satisfied:*

- $|\xi - \alpha|_{\bar{v}} < 1$;
- *the e series (27) $\bar{v}$-adically converge at ξ, and one of the sums $y_i^{(Q)}(\xi)$ is equal to $y(P)$.*

An important warning: the notion of proximity just introduced is not symmetric in P and Q: the proximity of P to Q does not imply, in general, the proximity of Q to P. Intuitively, one should think of Q as a "constant" point, and of P as a "variable" point.

To state the main results of this section, we have to define a finite set $\mathcal{Q}$ of $\bar{\mathbb{K}}$-points of the curve $\mathcal{C}$, and certain finite sets of non-archimedean places of the field $\mathbb{K}$. Let $R(X) = R_f(X) \in \mathbb{K}[X]$ be the Y-resultant of $f(X,Y)$ and $f'_Y(X,Y)$, and let $\mathcal{A}$ be the set of the roots of $R(X)$:

$$\mathcal{A} = \{\alpha \in \bar{\mathbb{K}} : R(\alpha) = 0\}.$$

We define $\mathcal{Q}$ as follows:

$$\mathcal{Q} = \left\{Q \in \mathcal{C}(\bar{\mathbb{K}}) : x(Q) \in \mathcal{A}\right\}.$$

It is important to notice that $\mathcal{Q}$ contains all the finite ramification points of x (and may contain some other points as well). Also, the set $\mathcal{Q}$ is Galois-invariant over $\mathbb{K}$: every point belongs to it together with its Galois orbit over $\mathbb{K}$.

Now let us define the finite sets of valuations of $\mathbb{K}$ mentioned above. First of all we assume (as we may, without loss of generality) that

$$\text{the polynomial } f_0(X)\text{, defined in (26), is monic.} \tag{28}$$

In particular, f has a coefficient equal to 1, which implies equality of the affine and the projective heights of f:

$$\mathrm{h_a}(f) = \mathrm{h_p}(f). \tag{29}$$

Now, we define

$$T_1 = \left\{v \in M_{\mathbb{K}}^0 : \text{the prime below } v \text{ is } \le n\right\},$$
$$T_2 = \left\{v \in M_{\mathbb{K}}^0 : |f|_v > 1\right\}.$$

Further, let r_0 be the leading coefficient of $R(X)$. We define

$$T_3 = \left\{v \in M_{\mathbb{K}}^0 : |r_0|_v < 1\right\}.$$

Next, we let Δ be the resultant of $\widehat{R}(X)$ and $\widehat{R}'(X)$, where $\widehat{R}$ is the radical of R, see Subsection 3.2. Since the polynomial $\widehat{R}(X)$ is separable, we have $\Delta \in \mathbb{K}^*$. Now we define the set T_4 as follows:

$$T_4 = \left\{v \in M_{\mathbb{K}}^0 : |\Delta|_v < 1\right\}.$$

Now fix $Q \in \mathcal{C}(\bar{\mathbb{K}})$ and define three sets $T_5^{(Q)}$, $T_6^{(Q)}$ and $T_7^{(Q)}$, using the Puiseux expansions of y at $Q \in \mathcal{Q}$. As in (27), we denote by $a_k^{(Q)}$ the coefficients of these expansions. Now define

$$T_5^{(Q)} = \left\{v \in M_{\mathbb{K}}^0 : \left|a_k^{(Q)}\right|_{\bar{v}} > 1 \text{ for some } k \text{ and some } \bar{v} \text{ extending } v\right\}, \qquad T_5 = \bigcup_{Q \in \mathcal{Q}} T_5^{(Q)}.$$

The Eisenstein theorem implies that the set $T_5^{(Q)}$ is finite. Further, the coefficients $a_k^{(Q)}$ generate a finite extension $\mathbb{K}^{(Q)}$ of $\mathbb{K}(\alpha)$ (where, as above, $\alpha = x(Q)$); more precisely, $[\mathbb{K}^{(Q)} : \mathbb{K}(\alpha)] \le n$. Now we define

$$T_6^{(Q)} = \left\{v \in M_{\mathbb{K}}^0 : v \text{ ramifies in } \mathbb{K}^{(Q)}\right\}, \qquad T_6 = \bigcup_{Q \in \mathcal{Q}} T_6^{(Q)}.$$

Finally, for any prime divisor q of $e = e_Q$ let $a^{(Q)}(q)$ be the *q-essential coefficient* of the series $y^{(Q)}$, as defined Subsection 4.3. Now put

$$T_7^{(Q)} = \left\{v \in M_{\mathbb{K}}^0 : \left|a^{(Q)}(q)\right|_{\bar{v}} < 1 \text{ for some } q|e_Q \text{ and some } \bar{v} \text{ extending } v\right\}, \qquad T_7 = \bigcup_{Q \in \mathcal{Q}} T_7^{(Q)}.$$

Finally, for $P, Q \in \mathcal{C}(\bar{\mathbb{K}})$ and a finite valuation $\bar{v} \in M_{\bar{\mathbb{K}}}$ we let v be the restriction of $\bar{v}$ to $\mathbb{K}$ and π a primitive element of the local ring $\mathcal{O}_v$, and define

$$\ell(P, Q, \bar{v}) = \frac{\log|\xi - \alpha|_{\bar{v}}}{\log|\pi|_v}, \tag{30}$$

where, as above, $\xi = x(P)$ and $\alpha = x(Q)$.

Now we are ready to state the principal results of this section. Call a point $P \in \mathcal{C}(\bar{\mathbb{K}})$ *semi-defined over* $\mathbb{K}$ if $\xi = x(P) \in \mathbb{K}$.

Proposition 5.2 *Let $\mathcal{Q}$ be the set defined above. Then for any point $P \in \mathcal{C}(\bar{\mathbb{K}}) \smallsetminus \mathcal{Q}$ semi-defined over $\mathbb{K}$, and for any finite valuation $v \in M_{\mathbb{K}}$, at least one of the following conditions is satisfied (we again put $\xi = x(P)$).*

- $|\xi|_v > 1$.
- $v \in T_2 \cup T_3 \cup T_4 \cup T_5$.
- *v is not ramified in the field $\mathbb{K}(P)$.*
- *For any $\bar{v} \in M_{\bar{\mathbb{K}}}$, extending v, our point P is $\bar{v}$-adically close to some $Q \in \mathcal{Q}$, which is well-defined when $\bar{v}$ is fixed. Moreover, the integers e_Q and $\ell(P, Q, \bar{v})$ are independent of the particular choice of $\bar{v}$.*

Proposition 5.3 *Assume that $P \in \mathcal{C}(\bar{\mathbb{K}})$ is semi-defined over $\mathbb{K}$, and let P be $\bar{v}$-adically close to some $Q \in \mathcal{C}(\bar{\mathbb{K}})$ for some finite valuation $\bar{v} \in M_{\bar{\mathbb{K}}}$. Let v and w be the restrictions of $\bar{v}$ to $\mathbb{K}$ and $\mathbb{K}(P)$, respectively. Assume that v does not belong to $T_1 \cup T_5^{(Q)} \cup T_6^{(Q)} \cup T_7^{(Q)}$. Then the ramification index of w over v is equal to $e_Q/(\gcd(e_Q, \ell)$, where $\ell = \ell(P, Q, \bar{v})$ is defined in (30).*

(Intuitively, the last condition means that the arithmetic ramification comes from the geometric ramification.)

Proposition 5.4 *Put $T = T_1 \cup T_2 \cup \ldots \cup T_7$. Then*

$$\mathrm{h}(T) \le 150mn^3 \log n\bigl(\mathrm{h}_{\mathrm{p}}(f) + 2m + 2n\bigr).$$

5.1 Proof of Proposition 5.2

We fix, once and for all, a finite valuation $v \in M_{\mathbb{K}}$, its extension $\bar{v} \in M_{\bar{\mathbb{K}}}$, and a point $P \in \mathcal{C}(\bar{\mathbb{K}})$ semi-defined over $\mathbb{K}$ and such that $\xi = x(P) \notin \mathcal{A}$. We assume that $|\xi|_v \le 1$, that $v \notin T_2 \cup \ldots \cup T_5$ and that v is ramified in $\mathbb{K}(P)$, and we shall prove that P is $\bar{v}$-adically close to a unique $Q \in \mathcal{Q}$, and that the numbers e_Q and $\ell(P, Q, \bar{v})$ are independent of the selected $\bar{v}$.

Since $v \notin T_2 \cup T_3$, the polynomial $R(X)$ belongs to $\mathcal{O}_v[X]$ and is v-monic. Lemma 3.4 implies that so is its radical $\widehat{R}(X)$. Also, every root α of R is a v-adic integer.

Put $\eta = y(P)$. Since $\xi \notin \mathcal{A}$, the point (ξ, η) of the plane curve $f(X, Y) = 0$ is non-singular, which implies that $\mathbb{K}(P) = \mathbb{K}(\xi, \eta) = \mathbb{K}(\eta)$ (recall that $\xi \in \mathbb{K}$). Now Lemma 3.3 implies that $|f'_Y(\xi, \eta)|_{\bar{v}} < 1$. It follows that $|R(\xi)|_v < 1$, which implies that $|\widehat{R}(\xi)|_v < 1$ by Lemma 3.4.

Next, since $v \notin T_4$, we have $|\widehat{R}'(\xi)|_v = 1$. Lemma 3.5 implies now that there exists a unique $\alpha \in \mathcal{A}$ such that $|\xi - \alpha|_{\bar{v}} < 1$. The uniqueness of α implies that the couple $(\alpha, \bar{v})$ is well-defined up to the Galois action of $\mathrm{Gal}(\bar{\mathbb{K}}/\mathbb{K})$. Hence, while α depends on the choice of $\bar{v}$, the quantity $|\xi - \alpha|_{\bar{v}}$ is independent of $\bar{v}$.

Fix this α from now on. There is $\sum_{x(Q)=\alpha} e_Q = n$ Puiseux expansions of y at the points Q above α, and they satisfy

$$f(x, Y) = f_0(x) \prod_{x(Q)=\alpha} \prod_{i=0}^{e_Q-1} \left(Y - y_i^{(Q)}\right).$$

Since $v \notin T_5$, each of the series $y_i^{(Q)}$ has v-adic convergence radius at least 1. Since $|\xi - \alpha|_{\bar{v}} < 1$, all them $\bar{v}$-adically converge at ξ. Moreover, the convergence is absolute, because $\bar{v}$ is non-archimedean. Hence

$$f(\xi, Y) = f_0(\xi) \prod_{x(Q)=\alpha} \prod_{i=0}^{e_Q-1} \left(Y - y_i^{(Q)}(\xi)\right).$$

Since $R(\xi) \ne 0$, we have $f_0(\xi) \ne 0$ as well. Hence we have on the left and on the right polynomials of degree n in Y, the polynomial on the left having $\eta = y(P)$ as a simple root (here we again use that $R(\xi) \ne 0$). Hence exactly one of the sums $y_i^{(Q)}(\xi)$ is equal to η. We have proved that P is $\bar{v}$-adically close to exactly one $Q \in \mathcal{Q}$.

The uniqueness of Q implies that e_Q is independent of the particular choice of $\bar{v}$. Indeed, if we select a different $\bar{v}$, then Q will be replaced by a conjugate over $\mathbb{K}$, and conjugate points have the same ramification. Also, as we have seen above $|\xi - \alpha|_{\bar{v}}$ is independent of the choice of $\bar{v}$ as well; hence so is $\ell(P, Q, \bar{v})$. $\square$

5.2 Proof of Proposition 5.3

We may assume, by re-defining the root $\sqrt[e]{\xi - \alpha}$ that $\eta = y(P)$ is the sum of $y_0^{(Q)}$ at ξ. In the sequel we omit reference to Q (when it does not lead to confusion) and write e for e_Q, a_k for $a_k^{(Q)}$, etc. Thus, we have, in the sense of $\bar{v}$-adic convergence,

$$\eta = \sum_{k=-k^{(Q)}}^{\infty} a_k \left(\sqrt[e]{\xi - \alpha}\right)^k. \tag{31}$$

We have to show that the ramification index of any extension of v to $\mathbb{K}(P)$ is $e' = e/\gcd(e, \ell)$, where ℓ is defined in (30). Since $v \notin T_6$, it is unramified in the field, generated over $\mathbb{K}$ by α and the coefficients a_k. Hence we may extend $\mathbb{K}$ and assume that all of the latter belong to it.

Let $\mathbb{K}_v$ be a v-adic completion of $\mathbb{K}$. We consider $\bar{\mathbb{K}}_{\bar{v}}$ as its algebraic closure, and the fields $\mathbb{K}_v(P) = \mathbb{K}_v(\eta)$ and $\mathbb{K}_v\left(\sqrt[e]{\xi - \alpha}\right)$ as subfields of the latter. According to (31), we have $\mathbb{K}_v(\eta) \subset \mathbb{K}_v\left(\sqrt[e]{\xi - \alpha}\right)$. The latter field has ramification e' over $\mathbb{K}_v$: see, for instance, Proposition 3.3 from [2]. (Here and below we use the fact that all our ramifications are tame, which follows from the assumption $v \notin T_1$.) If the ramification of $\mathbb{K}_v(\eta)$ is not e', then it must divide e'/q, where q is a prime divisor of e'. We want to show that this is impossible.

Let $\kappa = \kappa^{(Q)}(q)$ be as defined in Subsection 4.3. Then the q-essential coefficient $a^{(Q)}(q)$ is equal to a_κ. Put

$$\theta = \eta - \sum_{k=k^{(Q)}}^{\kappa-1} a_k \left(\sqrt[e]{\xi-\alpha}\right)^k = a_\kappa \left(\sqrt[e]{\xi-\alpha}\right)^\kappa + \sum_{k=\kappa+1}^{\infty} a_k \left(\sqrt[e]{\xi-\alpha}\right)^k$$

By the definition of κ, we have $\theta \in \mathbb{K}_v\left(\eta, \sqrt[e/q]{\xi-\alpha}\right)$. The ramification of $\mathbb{K}_v\left(\sqrt[e/q]{\xi-\alpha}\right)/\mathbb{K}_v$ is $(e/q)/\gcd(e/q,\ell) = e'/q$ (since q divides e', it cannot divide $\ell' = \ell/\gcd(e,\ell)$, and we have $\gcd(e/q,\ell) = \gcd(e,\ell)$). Hence the ramification of $\mathbb{K}_v(\theta)/\mathbb{K}_v$ divides e'/q. But, since $v \notin T_5 \cup T_7$, we have $|a_k|_v \le 1$ for all k and $|a_\kappa|_v = 1$, which implies that $|\theta|_v = \left|\left(\sqrt[e]{\xi-\alpha}\right)^\kappa\right|_v$. If π and Π are primitive elements of the local fields $\mathbb{K}_v$ and $\mathbb{K}_v(\theta)$, respectively, then $\mathrm{ord}_\pi\Pi$ divides e'/q. On the other hand, $\mathrm{ord}_\Pi\theta = (\kappa\ell/e)\cdot \mathrm{ord}_\pi\Pi \in \mathbb{Z}$, which implies that $(\kappa\ell/e)\cdot(e'/q) = \kappa\ell'/q \in \mathbb{Z}$. But q does not divide any of the numbers κ and ℓ', a contradiction. $\square$

5.3 Proof of Proposition 5.4

The proposition is a direct consequence of the estimates

$$\mathrm{h}(T_1) \le 1.02n, \tag{32}$$
$$\mathrm{h}(T_2) \le \mathrm{h_p}(f), \tag{33}$$
$$\mathrm{h}(T_3) \le (2n-1)\big(\mathrm{h_p}(f) + m\log 2 + \log(2n^2)\big), \tag{34}$$
$$\mathrm{h}(T_4) \le 16mn^2\big(\mathrm{h_p}(f) + 2m + 2\log n\big), \tag{35}$$
$$\mathrm{h}(T_5) \le 16mn^2\big(\mathrm{h_p}(f) + 2m + 2n\big), \tag{36}$$
$$\mathrm{h}(T_6) \le 40mn^3\big(\mathrm{h_p}(f) + 2m + 2n\big), \tag{37}$$
$$\mathrm{h}(T_7) \le 18mn^3\log n\big(\mathrm{h_p}(f) + 2m + 2n\big). \tag{38}$$

Remark 5.5 Estimates (37) and (38) can probably be refined, to have the main term of the form $O(mn^2\mathrm{h_p}(f))$, which would result in the similar main term in Proposition 5.4.

Proof of (32) Obviously, $\mathrm{h}(T_1) \le \sum_{p\le n}\log p$, which is bounded by $1.02n$ according to (5). $\square$

Proof of (33) Item 2 of Proposition 2.2 implies that $\mathrm{h}(T_2) \le \mathrm{h_a}(f)$. Since $\mathrm{h_a}(f) = \mathrm{h_p}(f)$ by (29), the result follows. $\square$

Proof of (34) Item 2 of Proposition 2.2 and Lemma 3.13 imply that

$$\mathrm{h}(T_3) \le \mathrm{h_a}(r_0) \le \mathrm{h_a}(R) \le (2n-1)\mathrm{h_a}(f) + (2n-1)\left(\log(2n^2) + m\log 2\right). \tag{39}$$

Again using (29), we have the result. $\square$

Proof of (35) We have $\deg\widehat{R} \le \deg R \le (2n-1)m$. Further, using Corollary 3.10 and inequalities (39), we find

$$\mathrm{h_a}(\widehat{R}) \le \mathrm{h_p}(R) + \mathrm{h_a}(r_0) + \deg R \le (4n-2)\mathrm{h_a}(f) + (8n-4)\left(\log n + m\right).$$

Finally, using Remark 3.14 and the previous estimates, we obtain

$$\mathrm{h}(T_4) \le \mathrm{h_a}(\Delta) \le (2\deg\widehat{R} - 1)\left(\mathrm{h_a}(\widehat{R}) + \log(2(\deg\widehat{R})^2)\right) \le 16mn^2\mathrm{h_a}(f) + 32mn^2\left(\log n + m\right).$$

Using (29), we obtain the result. $\square$

Preparation for the proofs of (36–38) Recall that we denote by $R(X)$ the Y-resultant of $f(X,Y)$ and $f'_Y(X,Y)$ and by $\mathcal{A}$ the set of the roots of $R(X)$. If we denote by μ_α the order of α as the root of $R(X)$, then we have

$$|\mathcal{A}| \le \sum_{\alpha\in\mathcal{A}} \mu_\alpha \le \deg R(X) \le m(2n-1), \tag{40}$$

$$\sum_{\alpha\in\mathcal{A}} \mathrm{h_a}(\alpha) \le \sum_{\alpha\in\mathcal{A}} \mu_\alpha \mathrm{h_a}(\alpha) \le \mathrm{h_p}(R) + \log(2mn) \le (2n-1)\mathrm{h_p}(f) + 3n\log(4mn), \tag{41}$$

where for (41) we use Remark 3.9 and Lemma 3.13. Denoting by u_α order of α as the root of $f_0(X)$, we have, obviously,

$$\sum_{\alpha\in\mathcal{A}} u_\alpha \le m,$$

$$\sum_{\alpha\in\mathcal{A}} u_\alpha \mathrm{h_a}(\alpha) \le \mathrm{h_p}(f_0) + \log(m+1) \le \mathrm{h_p}(f) + \log(m+1).$$

Using the notation

$$f^{(\alpha)}(X,Y) = f(X+\alpha, Y) \tag{42}$$

and Corollary 3.11, we obtain the following inequalities:

$$\sum_{\alpha\in\mathcal{A}} \mathrm{h_a}(f^{(\alpha)}) \le \sum_{\alpha\in\mathcal{A}} \mu_\alpha \mathrm{h_a}(f^{(\alpha)}) \le 4mn\mathrm{h_p}(f) + 7m^2n + 3nm\log n, \tag{43}$$

$$\sum_{\alpha\in\mathcal{A}} u_\alpha \mathrm{h_a}(f^{(\alpha)}) \le 2m\mathrm{h_p}(f) + 3m^2. \tag{44}$$

Proof of (36) For $\alpha \in \mathcal{A}$ and $v \in M_{\mathbb{K}(\alpha)}$ let $A_v(\alpha)$ and $B_v(\alpha)$ be the quantities of Theorem 4.1 but for the polynomial $f^{(\alpha)}$ instead of f. Put

$$T_5^{(\alpha)} = \left\{ v \in M_{\mathbb{K}(\alpha)} : A_v^{(\alpha)} > 1 \text{ or } B_v^{(\alpha)} > 1 \right\},$$

Corollary 4.2 implies that

$$\mathrm{h}\bigl(T_5^{(\alpha)}\bigr) \le (4n-1)\mathrm{h_p}(f^{(\alpha)}) + 13n^2 + 4n\log m. \tag{45}$$

Now let $\mathcal{A}'$ be a maximal selection of $\alpha \in \mathcal{A}$ pairwise non-conjugate over $\mathbb{K}$. Then every place from T_5 extends to some place from $T_5^{(\alpha)}$ for some $\alpha \in \mathcal{A}'$. Item 1 of Proposition 2.2 implies that

$$\mathrm{h}(T_5) \le \sum_{\alpha\in\mathcal{A}'} [\mathbb{K}(\alpha):\mathbb{K}]\mathrm{h}\bigl(T_5^{(\alpha)}\bigr).$$

Using (45), we obtain

$$\begin{aligned}\mathrm{h}(T_5) &\le (4n-1)\sum_{\alpha\in\mathcal{A}'} [\mathbb{K}(\alpha):\mathbb{K}]\mathrm{h_p}(f^{(\alpha)}) + (13n^2 + 4n\log m)\sum_{\alpha\in\mathcal{A}'} [\mathbb{K}(\alpha):\mathbb{K}] \\ &= (4n-1)\sum_{\alpha\in\mathcal{A}} \mathrm{h_p}(f^{(\alpha)}) + (13n^2 + 4n\log m)|\mathcal{A}|.\end{aligned}$$

Using (40) and (43), we obtain (36) after an easy calculation. □

Proof of (37) We again let $\mathcal{A}'$ be a maximal selection of $\alpha \in \mathcal{A}$ pairwise non-conjugate over $\mathbb{K}$, and for any $\alpha \in \mathcal{A}$ we let $\mathcal{Q}'_\alpha$ be a maximal selection of points Q with $x(Q) = \alpha$, pairwise non-conjugate over $\mathbb{K}(\alpha)$. A place $v \in M_K$ belongs to T_6 in one of the following cases: either v ramifies in $\mathbb{K}(\alpha)$ for some $\alpha \in \mathcal{A}'$, or an extension of v to some $\mathbb{K}(\alpha)$ ramifies in $\mathbb{K}^{(Q)}$ for some $Q \in \mathcal{Q}'_\alpha$. Item 1 of Proposition 2.2 implies that

$$\mathrm{h}(T_6) \le \sum_{\alpha\in\mathcal{A}'} \mathrm{h}\Big(\mathrm{Ram}\big(\mathbb{K}(\alpha)/\mathbb{K}\big)\Big) + \sum_{\alpha\in\mathcal{A}'}\sum_{Q\in\mathcal{Q}'_\alpha} [\mathbb{K}(\alpha):\mathbb{K}]\mathrm{h}\Big(\mathrm{Ram}\big(\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)\big)\Big), \tag{46}$$

where $\mathrm{Ram}(\cdot)$ is defined in Lemma 3.17. Lemma 3.18 implies that

$$\sum_{\alpha\in\mathcal{A}'} \mathrm{h}\Big(\mathrm{Ram}\big(\mathbb{K}(\alpha)/\mathbb{K}\big)\Big) \le \sum_{\alpha\in\mathcal{A}'}[\mathbb{K}(\alpha):\mathbb{K}]\partial_{\mathbb{K}(\alpha)/\mathbb{K}} = \sum_{\alpha\in\mathcal{A}}\partial_{\mathbb{K}(\alpha)/\mathbb{K}}.$$

The latter sum can be easily estimated by Corollary 3.16 and Lemma 3.13:

$$\sum_{\alpha\in\mathcal{A}}\partial_{\mathbb{K}(\alpha)/\mathbb{K}} \le 4mn\mathrm{h}_{\mathrm{p}}(R) + 6mn\log(2mn) \le 8mn^2\mathrm{h}_{\mathrm{p}}(f) + 18mn^2\log(3mn). \tag{47}$$

To estimate the second sum in (46), we again use Lemma 3.18:

$$\begin{aligned}\sum_{\alpha\in\mathcal{A}'}\sum_{Q\in\mathcal{Q}'_\alpha} [\mathbb{K}(\alpha):\mathbb{K}]\mathrm{h}\Big(\mathrm{Ram}\big(\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)\big)\Big) &\le \sum_{\alpha\in\mathcal{A}'}[\mathbb{K}(\alpha):\mathbb{K}]\sum_{Q\in\mathcal{Q}'_\alpha}\big[\mathbb{K}^{(Q)}:\mathbb{K}(\alpha)\big]\partial_{\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)}\\ &= \sum_{\alpha\in\mathcal{A}}\sum_{x(Q)=\alpha}\partial_{\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)}\end{aligned}$$

Corollary 4.4 implies that

$$\begin{aligned}\sum_{x(Q)=\alpha}\partial_{\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)} \le \quad & \left(4n^2\mu_\alpha + 4u_\alpha n^3 + 2n^2\right)\mathrm{h}_{\mathrm{p}}(f^{(\alpha)}) +\\ &+ \left(\mu_\alpha n + u_\alpha n^2\right)\left(12n^2 + 4n\log m\right) + 3n^2\log(2n).\end{aligned}$$

Summing up over $\alpha \in \mathcal{A}$ and using (40), (43) and (44), we obtain

$$\sum_{\alpha\in\mathcal{A}}\sum_{x(Q)=\alpha}\partial_{\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)} \le 32mn^3\mathrm{h}_{\mathrm{p}}(f) + 60mn^3(m+n),$$

which, together with (47), implies (37). ☐

Proof of (38) For $Q \in \mathcal{Q}$ denote by Σ_Q the sum of the heights of all the essential coefficients of the Puiseux expansion at Q. Keeping the notation $\mathcal{A}'$ and $\mathcal{Q}'_\alpha$ from the previous proof, and using item 2 of Proposition 2.2, we obtain

$$\mathrm{h}(T_7) \le \sum_{\alpha\in\mathcal{A}'}[\mathbb{K}(\alpha):\mathbb{K}]\sum_{Q\in\mathcal{Q}'_\alpha}\big[\mathbb{K}^{(Q)}:\mathbb{K}(\alpha)\big]\Sigma_Q = \sum_{\alpha\in\mathcal{A}}\sum_{x(Q)=\alpha}\Sigma_Q.$$

Corollary 4.6 estimates the inner sum by

$$(u_\alpha + \mu_\alpha)\Big(2n^2\mathrm{h}_{\mathrm{p}}(f^{(\alpha)}) + 6n^3 + 2n^2\log m\Big)\log_2 n.$$

Applying inequalities (40), (43) and (44) once again, we obtain

$$\mathrm{h}(T_7) \le 12mn^3\log_2 n\,\mathrm{h}_{\mathrm{p}}(f) + 24mn^3(m+n)\log_2 n.$$

Since $\log_2 n \le 1.5\log n$, the result follows. This completes the proof of Proposition 5.4. ☐

6 A Tower of $\bar{\mathbb{K}}$-Points

In this section we retain the set-up of Section 5; that is, we fix a number field $\mathbb{K}$, a curve $\mathcal{C}$ defined over $\mathbb{K}$ and rational functions $x, y \in \mathbb{K}(\mathcal{C})$ such that $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$. Again, let $f(X, Y) \in \mathbb{K}[X, Y]$ be the $\mathbb{K}$-irreducible polynomial of X-degree m and Y-degree n such that $f(x, y) = 0$, and we again assume that $f_0(X)$ in (26) is monic. We again define the polynomial $R(X)$, the sets $\mathcal{A} \subset \bar{\mathbb{K}}$, $\mathcal{Q} \subset \mathcal{C}(\bar{\mathbb{K}})$ and $T_1, \ldots, T_7 \subset M_{\mathbb{K}}$, etc.

We also fix a covering $\widetilde{\mathcal{C}} \stackrel{\phi}{\to} \mathcal{C}$ of $\mathcal{C}$ by another smooth irreducible projective curve $\widetilde{\mathcal{C}}$; we assume that both $\widetilde{\mathcal{C}}$ and the covering ϕ are defined over $\mathbb{K}$. We consider $\mathbb{K}(\mathcal{C})$ as a subfield of $\mathbb{K}(\widetilde{\mathcal{C}})$; in particular, we identify the functions $x \in \mathbb{K}(\mathcal{C})$ and $x \circ \phi \in \mathbb{K}(\widetilde{\mathcal{C}})$. We fix a function $\widetilde{y} \in \mathbb{K}(\widetilde{\mathcal{C}})$ such that $K(\widetilde{\mathcal{C}}) = \mathbb{K}(x, \widetilde{y})$. We let $\tilde{f}(X, \widetilde{Y}) \in \mathbb{K}[X, \widetilde{Y}]$ be an irreducible polynomial of X-degree $\widetilde{m}$ and $\widetilde{Y}$-degree $\widetilde{n}$ such that $\tilde{f}(x, \widetilde{y}) = 0$; we write

$$\tilde{f}(X, \widetilde{Y}) = \tilde{f}_0(X)\widetilde{Y}^{\widetilde{n}} + \tilde{f}_1(X)\widetilde{Y}^{\widetilde{n}-1} + \cdots + \tilde{f}_{\widetilde{n}}(X)$$

and assume that the polynomial $\tilde{f}_0(X)$ is monic. We define in the similar way the polynomial $\widetilde{R}(X)$, the sets $\widetilde{\mathcal{A}} \subset \bar{\mathbb{K}}$, $\widetilde{\mathcal{Q}} \subset \widetilde{\mathcal{C}}(\bar{\mathbb{K}})$ and $\widetilde{T}_1, \ldots, \widetilde{T}_7 \subset M_{\mathbb{K}}$, etc. We also define the notion of proximity on the curve $\widetilde{\mathcal{C}}$ exactly in the same way as we did it for $\mathcal{C}$ in Definition 5.1, and we have the analogues of Propositions 5.2, 5.3 and 5.4.

In addition to all this, we define one more finite set of places of the field $\mathbb{K}$ as follows. Write $\widetilde{R}(X) = \widetilde{R}_1(X)\widetilde{R}_2(X)$, where the polynomials $\widetilde{R}_1(X), \widetilde{R}_2(X) \in \mathbb{K}(X)$ are uniquely defined by the following conditions:

- the roots of $\widetilde{R}_1(X)$ are contained in the set of the roots of $f_0(X)$;
- the polynomial $\widetilde{R}_2(X)$ has no common roots with $f_0(X)$ and is monic.

Now let Θ be the resultant of $f_0(X)$ and $\widetilde{R}_2(X)$. Then $\Theta \neq 0$ by the definition of $\widetilde{R}_2(X)$, and we put

$$U = \{v \in M_{\mathbb{K}} : |\Theta|_v < 1\}.$$

Proposition 6.1 *Let $P \in \mathcal{C}(\bar{\mathbb{K}})$ be semi-defined over $\mathbb{K}$ (that is, $\xi = x(P) \in \mathbb{K}$), and let $\widetilde{P} \in \widetilde{\mathcal{C}}(\bar{\mathbb{K}})$ be a point above P (that is, $\phi(\widetilde{P}) = P$). Let v be a finite place of $\mathbb{K}$, and $\bar{v}$ an extension of v to $\bar{\mathbb{K}}$. Assume that $\widetilde{P}$ is $\bar{v}$-close to some $\widetilde{Q} \in \widetilde{\mathcal{Q}}$. Then we have one of the following options.*

- $|\xi|_v > 1$.
- $v \in T \cup \widetilde{T} \cup U$.
- *P is $\bar{v}$-adically close to the $Q \in \mathcal{C}(\bar{\mathbb{K}})$ which lies below $\widetilde{Q}$.*

For the proof we shall need a simple lemma.

Lemma 6.2 *In the above set-up, there exists a polynomial $\Phi(X, \widetilde{Y}) \in \mathbb{K}[X, \widetilde{Y}]$ such that*

$$y = \frac{\Phi(x, \widetilde{y})}{f_0(x)\widetilde{R}(x)}$$

Proof Since $f_0(x)y$ is integral over $\mathbb{K}[x]$, Corollary 3.2 implies that $f_0(x)y \in \widetilde{R}(x)^{-1}\mathbb{K}[x, \widetilde{y}]$, whence the result. □

Proof of Proposition 6.1 We put $\alpha = x(\widetilde{Q})$. By the definition of the set $\widetilde{\mathcal{Q}}$, we have $\alpha \in \widetilde{\mathcal{A}}$. Assume that $|\xi|_v \le 1$ and $v \notin T \cup \widetilde{T} \cup U$. Let $\widetilde{e}$ be the ramification of $\widetilde{Q}$ over $\mathbb{P}^1$, and let

$$\widetilde{y}_i^{(\widetilde{Q})} = \sum_{k=-k^{(\widetilde{Q})}}^{\infty} a_k^{(\widetilde{Q})} \widetilde{\zeta}^{ik} (x-\alpha)^{k/\widetilde{e}} \qquad (i = 0, \ldots, \widetilde{e}-1), \tag{48}$$

be the equivalent Puiseux expansions of $\widetilde{y}$ at $\widetilde{Q}$ (here $\widetilde{\zeta}$ is a primitive $\widetilde{e}$-th root of unity). Since $\widetilde{P}$ is $\bar{v}$-close to $\widetilde{Q}$, we have $|\xi - \alpha|_{\bar{v}} < 1$ and the $\widetilde{e}$ series (48) converge at ξ, with one of the sums being $\widetilde{y}(\widetilde{P})$.

Now let $\Phi(X, \widetilde{Y})$ be the polynomial from Lemma 6.2. Then the $\widetilde{e}$ series

$$\frac{\Phi\bigl(x, \widetilde{y}_i^{(\widetilde{Q})}\bigr)}{f_0(x)\widetilde{R}(x)} \qquad (i = 0, \ldots, \widetilde{e}-1) \tag{49}$$

contain all the equivalent Puiseux series of y at $Q = \phi(\widetilde{Q})$. More precisely, if the ramification of Q over $\mathbb{P}^1$ is e, then every of the latter series occurs in (49) exactly $\widetilde{e}/e$ times.

Write $f_0(X)\widetilde{R}(X) = (X-\alpha)^r g(X)$ with $g(\alpha) \ne 0$. The assumption $v \notin T_2 \cup \widetilde{T}_2 \cup \widetilde{T}_3 \cup \widetilde{T}_4 \cup U$ implies that $|g(\alpha)|_{\bar{v}} = 1$. Now Lemma 3.6 implies that the Laurent series at α of the rational function $\bigl(f_0(x)\widetilde{R}(x)\bigr)^{-1}$ converges at ξ. Hence all the series (49) converge at ξ, and among the sums we find

$$\frac{\Phi\bigl(x(\widetilde{P}), \widetilde{y}(\widetilde{P})\bigr)}{f_0\bigl(x(\widetilde{P})\bigr)\widetilde{R}\bigl(x(\widetilde{P})\bigr)} = y(P).$$

Hence P is $\bar{v}$-close to Q. □

We shall also need a bound for U similar to that of Proposition 5.4.

Proposition 6.3 *We have* $\mathrm{h}(U) \le \Upsilon + \Xi$, *where* Υ *is defined in (1) and*

$$\Xi = 2m\widetilde{n}(2\widetilde{m} + 3\log\widetilde{n}) + (m + 2\widetilde{m}\widetilde{n})\log(m + 2\widetilde{m}\widetilde{n}). \tag{50}$$

Proof Item 2 of Proposition 2.2 implies that $\mathrm{h}(U) \le \mathrm{h_a}(\Theta)$, where Θ is the resultant of $f_0(X)$ and $\widetilde{R}_2(X)$. Expressing Θ as the familiar determinant, we find

$$\mathrm{h_a}(\Theta) \le \deg \widetilde{R}_2 \mathrm{h_a}(f_0) + \deg f_0 \mathrm{h_a}(\widetilde{R}_2) + (\deg f_0 + \deg \widetilde{R}_2)\log(\deg f_0 + \deg \widetilde{R}_2). \tag{51}$$

Since both f_0 and $\widetilde{R}_2$ are monic polynomials (by the convention (28) and the definition of $\widetilde{R}_2$), we may replace the affine heights by the projective heights. Further, we have the estimates

$$\deg f_0 \le m, \qquad \deg \widetilde{R}_2 \le \widetilde{m}(2\widetilde{n}-1), \qquad \mathrm{h_p}(f_0) \le \mathrm{h_p}(f),$$
$$\mathrm{h_p}(\widetilde{R}_2) \le (2\widetilde{n}-1)\mathrm{h_p}(\tilde{f}) + (2\widetilde{n}-1)\left(2\widetilde{m} + \log\bigl((\widetilde{n}+1)\sqrt{\widetilde{n}}\bigr)\right),$$

the latter estimate being a consequence of Corollary 3.10 and Lemma 3.13. Substituting all this to (51), we obtain the result. □

7 The Chevalley-Weil Theorem

Now we may to gather the fruits of our hard work. In this section we retain the set-up of Section 6. Here is our principal result, which will easily imply all the theorems stated in the introduction.

Theorem 7.1 *Assume that the covering ϕ is unramified outside the poles of x. Let $P \in \mathcal{C}(\bar{\mathbb{K}})$ be semi-defined over $\mathbb{K}$, and let $\widetilde{P} \in \widetilde{\mathcal{C}}(\bar{\mathbb{K}})$ be a point above P. As before, we put $\xi = x(P) = x(\widetilde{P})$. Then for every non-archimedean $v \in M_{\mathbb{K}}$ we have one of the following options.*

- $|\xi|_v > 1$.
- $v \in T \cup \widetilde{T} \cup U$.
- *Any extension of* v *to* $\mathbb{K}(P)$ *is unramified in* $\mathbb{K}(\widetilde{P})$.

Proof Let $v \in M_{\mathbb{K}}$ be a non-archimedean valuation such that $|\xi|_v \le 1$ and $v \notin T \cup \widetilde{T} \cup U$. Fix an extension $\bar{v}$ of v to $\bar{\mathbb{K}}$, and let $\widetilde{w}$ and w be the restrictions of $\bar{v}$ to $\mathbb{K}(\widetilde{P})$ and $\mathbb{K}(P)$, and $\widetilde{e}$ and e their ramification indexes over v, respectively.

If $\widetilde{P} \in \widetilde{\mathcal{Q}}$ then v is unramified in $K(\widetilde{P})$ because[3] $v \notin \widetilde{T}_1 \cup \widetilde{T}_6$. From now on, we assume that $\widetilde{P} \notin \widetilde{\mathcal{Q}}$. Proposition 5.2 implies that $\widetilde{P}$ is $\bar{v}$-adically close to some $\widetilde{Q} \in \widetilde{\mathcal{Q}}$, and Proposition 5.3 implies that $\widetilde{e} = e_{\widetilde{Q}}/\gcd(e_{\widetilde{Q}}, \ell)$. Let Q be the point of $\mathcal{C}$ lying under $\widetilde{Q}$. Put $\alpha = x(\widetilde{Q}) = x(Q)$. If $\alpha \notin \mathcal{A}$ then the covering $\mathcal{C} \mapsto \mathbb{P}^1$ does not ramify at Q. Since ϕ is unramified outside the poles of x, the covering $\widetilde{\mathcal{C}} \mapsto \mathbb{P}^1$ does not ramify at $\widetilde{Q}$, that is, $e_{\widetilde{Q}} = 1$. Hence $\widetilde{e} = 1$, which means that v is not ramified in $\mathbb{K}(\widetilde{P})$.

Now assume that $\alpha \in \mathcal{A}$. Proposition 6.1 implies that P is $\bar{v}$-adically close to Q. Now notice that $e_Q = e_{\widetilde{Q}}$, again because ϕ is unramified. Also, $\ell(P, Q, \bar{v})) = \ell(\widetilde{P}, \widetilde{Q}, \bar{v}) = \ell$, just by the definition of this quantity. Again using Proposition 5.3, we obtain that $e = e_Q/\gcd(e_Q, \ell) = \widetilde{e}$. This shows tha $\widetilde{w}$ is unramified over w, completing the proof. $\square$

We also need an estimate for $\mathrm{h}(T \cup \widetilde{T} \cup U)$.

Proposition 7.2 *We have*

$$\mathrm{h}(T \cup \widetilde{T} \cup U) \le \Omega + \widetilde{\Omega} + \Upsilon. \tag{52}$$

where Ω, $\widetilde{\Omega}$ *and* Υ *are defined in (1).*

Proof Combining Propositions 5.4 and 6.3, we obtain the estimate

$$\mathrm{h}(T \cup \widetilde{T} \cup U) \le \frac{3}{4}(\Omega + \widetilde{\Omega}) + \Upsilon + \Xi,$$

where Ξ is defined in (50). A routine calculation show that $\Xi \le (\Omega + \widetilde{\Omega})/4$, whence the result. $\square$

Now we can prove the theorems from the introduction.

Proof of Theorem 1.3 We may replace $\mathbb{K}$ by $\mathbb{K}(P)$ and assume that $P \in \mathcal{C}(\mathbb{K})$. Put $\xi = x(P)$ and let R be the set of places of $\mathbb{K}$ having an extension to $\mathbb{K}(P)$ that ramifies in $\mathbb{K}(\widetilde{P})$. Theorem 7.1 and estimate (52) imply that

$$\mathrm{h}\big(\{v \in R : |\xi|_v \le 1\}\big) \le \Omega + \widetilde{\Omega} + \Upsilon.$$

Replacing x by x^{-1} and the polynomials f, $\tilde{f}$ by $X^m f(X^{-1}, Y)$ and $X^{\widetilde{m}} \tilde{f}(X^{-1}, Y)$, respectively, we obtain the estimate

$$\mathrm{h}\big(\{v \in R : |\xi|_v \ge 1\}\big) \le \Omega + \widetilde{\Omega} + \Upsilon.$$

Thus,

$$\mathrm{h}(R) \le 2(\Omega + \widetilde{\Omega} + \Upsilon),$$

and Lemma 3.17 implies that

$$\partial_{K(\widetilde{P})/\mathbb{K}} \le 2\frac{\nu - 1}{\nu}(\Omega + \widetilde{\Omega} + \Upsilon) + 1.26\nu \le 2(\Omega + \widetilde{\Omega} + \Upsilon).$$

The theorem is proved. $\square$

[3]The field $\mathbb{K}(\widetilde{P})$ coincides with the field $\mathbb{K}^{(\widetilde{P})}$, generated by the coefficients of the Puiseux series at $\widetilde{P}$, if x is unramified at $\widetilde{P}$; if there is ramification e, we have $\mathbb{K}(\widetilde{P}, \zeta_e) = \mathbb{K}^{(\widetilde{P})}(\zeta_e)$. Hence any $v \notin \widetilde{T}_1 \cup \widetilde{T}_6$ is unramified at any $\widetilde{P} \in \widetilde{\mathcal{Q}}$.

Proof of Theorem 1.5 Let S' be set of places of the field $\mathbb{K}(P)$ extending the places from S. The right-hand side of (2) will not increase (see item 1 of Proposition 2.2) if we replace $\mathbb{K}$ by $\mathbb{K}(P)$ and S by S'. Thus, we may assume that $P \in \mathcal{C}(\mathbb{K})$. Again using Theorem 7.1 and (52), we obtain

$$\mathrm{h}(R \smallsetminus S) \le \Omega + \widetilde{\Omega} + \Upsilon.$$

We again complete the proof, applying Lemma 3.17. □

To prove Theorem 1.6, we need the following result from [3].

Theorem 7.3 *Let $x : \mathcal{C} \to \mathbb{P}^1$ be a finite covering of degree $n \ge 2$, defined over $\mathbb{K}$ and unramified outside a finite set $A \subset \mathbb{P}^1(\bar{\mathbb{K}})$. Put $h = \mathrm{h}_{\mathrm{a}}(A)$ and $\Lambda' = \left(2(\mathbf{g}+1)n^2\right)^{10\mathbf{g}n+12n}$, where $\mathbf{g} = \mathbf{g}(\mathcal{C})$. Then there exists a rational function $y \in \bar{\mathbb{K}}(\mathcal{C})$ such that $\bar{\mathbb{K}}(\mathcal{C}) = \bar{\mathbb{K}}(x,y)$ and the rational functions $x, y \in \bar{\mathbb{K}}(\mathcal{C})$ satisfy the equation $f(x,y) = 0$, where $f(X,Y) \in \bar{\mathbb{K}}[X,Y]$ is an absolutely irreducible polynomial satisfying*

$$\deg_X f = \mathbf{g}+1, \qquad \deg_Y f = n, \qquad \mathrm{h}_{\mathrm{p}}(f) \le \Lambda'(h+1). \tag{53}$$

Moreover, the number field $\mathbb{L}$, generated over $\mathbb{K}$ by the set A and by the coefficients of f satisfies $\partial_{\mathbb{L}/\mathbb{K}(A)} \le \Lambda'(h+1)$.

Proof of Theorem 1.6 We shall prove the "projective" case (that is, item 1) of this theorem. The "affine" case is proved similarly.

We define $\widetilde{\Lambda}'$ in the same way as Λ' in Theorem 7.3, but with n and $\mathbf{g}$ replaced by $\widetilde{n}$ and $\widetilde{\mathbf{g}}$. We use Theorem 7.3 to find functions $y \in \bar{\mathbb{K}}(\mathcal{C})$ and $\widetilde{y} \in \bar{\mathbb{K}}(\widetilde{\mathcal{C}})$, and polynomials $f(X,Y) \in \bar{\mathbb{K}}[X,Y]$ and $\tilde{f}(X,\widetilde{Y}) \in \bar{\mathbb{K}}[X,\widetilde{Y}]$. Denoting by $\mathbb{L}$ the field generated by the set A and the coefficients of both the polynomials, we find $\partial_{\mathbb{L}/\mathbb{K}(A)} \le (\Lambda' + \widetilde{\Lambda}')(h+1)$ with $h = \mathrm{h}_{\mathrm{a}}(A)$. Using Lemma 3.15, we estimate $\partial_{\mathbb{K}(A)/\mathbb{K}} \le 2(\delta-1)h + \log\delta$. Hence

$$\partial_{\mathbb{L}/\mathbb{K}} \le \left(\Lambda' + \widetilde{\Lambda}' + 2(\delta-1)\right)(h+1).$$

We define the quantities Ω, $\widetilde{\Omega}$ and Υ as in the introduction. Then, applying Theorem 1.3, but over the field $\mathbb{L}$ rather than $\mathbb{K}$, we find $\partial_{\mathbb{L}(\widetilde{P})/\mathbb{L}(P)} \le 2(\Omega + \widetilde{\Omega} + \Upsilon)$. We have

$$\partial_{\mathbb{K}(\widetilde{P})/\mathbb{K}(P)} \le \partial_{\mathbb{L}(\widetilde{P})/\mathbb{K}(P)} = \partial_{\mathbb{L}(\widetilde{P})/\mathbb{L}(P)} + \partial_{\mathbb{L}(P)/\mathbb{K}(P)} \le \partial_{\mathbb{L}(\widetilde{P})/\mathbb{L}(P)} + \partial_{\mathbb{L}/\mathbb{K}}.$$

The last sum is bounded by

$$2(\Omega + \widetilde{\Omega} + \Upsilon) + \left(\Lambda' + \widetilde{\Lambda}' + 2(\delta-1)\right)(h+1),$$

which, obviously, does not exceed $\Lambda(h+1)$, as wanted. □

References

[1] Yu. Bilu, *Effective Analysis of Integral Points on Algebraic Curves*, Ph. D. Thesis, Beer Sheva, 1993.

[2] Yu. Bilu, Quantitative Siegel's Theorem for Galois Coverings, *Compositio Math.*, **106(2)** (1997), 125–158.

[3] Yu. Bilu, M. Strambi, Quantitative Riemann Existence Theorem over a Number Field, *Acta Arith.*, to appear.

[4] R. Dedekind, *Werke* I, Vieweg, 1930.

[5] K. Draziotis, D. Poulakis, Explicit Chevalley-Weil Theorem for Affine Plane Curves, *Rocky Mountain J. of Math.* **39** (2009), 49–70.

[6] K. Draziotis, D. Poulakis, An Effective Version of Chevalley-Weil Theorem for Projective Plane Curves, arXiv:0904.3845.

[7] B. Dwork and P. Robba, On natural radii of p-adic convergence, *Trans. Amer. Math. Soc.* **256** (1979), 199–213.

[8] B. M. Dwork and A. J. van der Poorten, The Eisenstein Constant, *Duke Math. J.* **65(1)** (1992), 23–43.

[9] M. Hindry, J. H. Silverman, Diophantine Geometry: an Introduction, Graduate Texts in Math. **201**, Springer Verlag, 2000.

[10] T. Krick, L.M. Pardo, M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, *Duke Math. J.* **109** (2001), 521–598.

[11] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.

[12] J. B. Rosser, L. Schoenfeld, Lowell Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

[13] W. M. Schmidt, Eisenstein's theorem on power series expansions of algebraic functions. *Acta Arith.* **56(2)** (1990), 161–179.

[14] W. M. Schmidt, Construction and estimates of bases in function fields. *J. Number Theory* **39)** (1991), 181–224.

[15] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev, *Publ. Math. IHES* **54** (1981), 323–401.

[16] J. H. Silverman, Lower bounds for height functions. *Duke Math. J.* **51** (1984), 395–403.