Università degli studi di Pisa

Dipartimento di Matematica

PhD Thesis

Effective Estimates for Coverings of Curves over Number Fields

Advisors : **Prof. Yuri Bilu, Prof. Roberto Dvornicich** Candidate: **Marco Strambi**

Contents

	Intro	duction	4
	Nota	tion and Conventions	7
1	Gen	eral Lemmas and Useful Tools	10
	1.1	Heights	10
		1.1.1 Estimates for Sums and Products of Polynomials	10
		1.1.2 Bounds for Solutions of Algebraic Equations	13
		1.1.3 Height of sets of places	15
		1.1.4 Height and Discriminants	16
	1.2	Power Series	17
	1.3	Integral Elements	19
	1.4	Local Lemmas	20
	1.5	Miscellaneous Lemmas	22
2	Effe	ctive Riemann Esistence Theorem	23
2	Effe 2.1	ctive Riemann Esistence TheoremIntroduction	23 23
2	Effe 2.1 2.2	ctive Riemann Esistence Theorem Introduction	23 23 25
2	Effe 2.1 2.2 2.3	ctive Riemann Esistence TheoremIntroductionSetup for the Proof of Theorem 2.1.2Function y and Polynomial $f(X, Y)$	 23 23 25 26
2	Effe 2.1 2.2 2.3 2.4	ctive Riemann Esistence TheoremIntroduction	 23 25 26 27
2	Effe 2.1 2.2 2.3 2.4 2.5	ctive Riemann Esistence TheoremIntroductionSetup for the Proof of Theorem 2.1.2Function y and Polynomial $f(X, Y)$ The Discriminant and its Roots, and the Puiseux ExpansionsThe Puiseux Expansions at Infinity	 23 25 26 27 28
2	Effe 2.1 2.2 2.3 2.4 2.5 2.6	ctive Riemann Esistence TheoremIntroductionSetup for the Proof of Theorem 2.1.2Function y and Polynomial $f(X,Y)$ The Discriminant and its Roots, and the Puiseux ExpansionsThe Puiseux Expansions at InfinityThe Indeterminates	 23 25 26 27 28 29
2	Effe 2.1 2.2 2.3 2.4 2.5 2.6 2.7	ctive Riemann Esistence TheoremIntroductionSetup for the Proof of Theorem 2.1.2Function y and Polynomial $f(X, Y)$ The Discriminant and its Roots, and the Puiseux ExpansionsThe Puiseux Expansions at InfinityThe IndeterminatesThe Algebraic Set V	 23 25 26 27 28 29 31
2	Effe 2.1 2.2 2.3 2.4 2.5 2.6 2.7 2.8	ctive Riemann Esistence TheoremIntroduction	 23 25 26 27 28 29 31 32
2	Effe 2.1 2.2 2.3 2.4 2.5 2.6 2.7 2.8 2.9	ctive Riemann Esistence TheoremIntroduction	 23 25 26 27 28 29 31 32 33
2	Effe 2.1 2.2 2.3 2.4 2.5 2.6 2.7 2.8 2.9 2.10	ctive Riemann Esistence TheoremIntroduction	 23 23 25 26 27 28 29 31 32 33 35
2	Effe 2.1 2.2 2.3 2.4 2.5 2.6 2.7 2.8 2.9 2.10 2.11	ctive Riemann Esistence TheoremIntroduction	 23 25 26 27 28 29 31 32 33 35 36
2	Effe 2.1 2.2 2.3 2.4 2.5 2.6 2.7 2.8 2.9 2.10 2.11 2.12	ctive Riemann Esistence TheoremIntroduction	 23 23 25 26 27 28 29 31 32 33 35 36 37

3	Effe	ectivity in the Chevalley-Weil Theorem	38
	3.1	Introduction	38
	3.2	Eisenstein Theorem for Power Series	40
		3.2.1 Eisenstein Theorem	41
		3.2.2 Fields Generated by the Coefficients	43
		3.2.3 The "Essential" Coefficients	45
	3.3	Proximity and Ramification	46
		3.3.1 Proof of Proposition 3.3.3	50
		3.3.2 Proof of Proposition 3.3.4	51
		3.3.3 Proof of Proposition 3.3.5	52
	3.4	A Tower of $\overline{\mathbb{K}}$ -Points	56
	3.5	The Chevalley-Weil Theorem	58
	Bibl	iography	62

Introduction

The purpose of this thesis is to obtain totally explicit versions for two fundamental results about coverings of algebraic curves: the *Riemann Existence Theorem* and the *Chevalley-Weil Theorem*. In the introduction we briefly recall basic facts on these two theorems. The detailed statements, which require certain amount of notation, can be found in the introductions of the corresponding chapters of the thesis.

The Riemann Existence Theorem

The Riemann Existence Theorem asserts that every compact Riemann surface is (analytically isomorphic to) a complex algebraic curve. In other words, the field of meromorphic functions on a compact Riemann surface S is finitely generated and of transcendence degree 1 over \mathbb{C} .

One of the most common ways of defining Riemann surfaces is realizing them as finite ramified coverings of the Riemann sphere $\mathbb{P}^1(\mathbb{C})$. Moreover, even if the covering is purely topological, the \mathbb{C} -analytic structure on the Riemann sphere lifts, in a unique way, to the covering surface. Thus, the Riemann Existence Theorem can be restated as follows.

Theorem A Let M be a finite subset of $\mathbb{P}^1(\mathbb{C})$. Then for any finite covering of $\mathbb{P}^1(\mathbb{C})$ by a closed oriented surface, unramified outside the set M, there exists a complex algebraic curve \mathcal{C} and a rational function $x \in \mathbb{C}(\mathcal{C})$ such that our covering is isomorphic¹ to $\mathcal{C}(\mathbb{C}) \xrightarrow{x} \mathbb{P}^1(\mathbb{C})$, the covering defined by x. Moreover, the couple (\mathcal{C}, x) is unique up to a naturally defined isomorphism².

We refer to [6] for several more precise statements, and for the connection of the Riemann Existence Theorem and the Inverse Galois Problem.

One of the purposes of this thesis is to give an effective description of the curve \mathcal{C} , or, more precisely, of the couple (\mathcal{C}, x) , in terms of the degree of the initial topological covering and the set M of the ramification points, provided the points from that set are defined over the field $\overline{\mathbb{Q}}$ of all algebraic numbers. In this case the curve \mathcal{C} is also defined over $\overline{\mathbb{Q}}$ (this is the "easy"

¹Two coverings $S_1 \xrightarrow{\pi_1} S$ and $S_2 \xrightarrow{\pi_2} S$ of topological spaces are *isomorphic* if there exists a homeomorphism $S_1 \xrightarrow{\varphi} S_2$ such that $\pi_1 = \pi_2 \circ \varphi$.

²If (\mathcal{C}', x') is another such couple, then the field isomorphism $\mathbb{C}(x) \to \mathbb{C}(x')$ given by $x \mapsto x'$, extends to a field isomorphism $\mathbb{C}(\mathcal{C}) \to \mathbb{C}(\mathcal{C}')$.

direction of Belyi's Theorem). We produce a plane model of \mathcal{C} over $\overline{\mathbb{Q}}$, such that one of the coordinates is x, and we give explicit bounds for the degree and the height of the defining equation of this model, and of the degree and discriminant of the number field over which this model is defined.

Notice that we do not produce a new proof of the Riemann Existence Theorem. In fact, we do use both the existence and the uniqueness statements of Theorem A.

The principal motivation of this work lies in the field of effective Diophantine analysis, where the covering technique is widely used. It happens quite often that only the degree of the covering and the ramification points are known, and to work with the covering curve, one needs to have an effective description of it.

In particular, in Chapter 3 we use our explicit version of the Riemann existence theorem to get a user-friendly version of the Chevalley-Weil theorem, see Theorem 3.1.5.

The Chevalley-Weil Theorem

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 B (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 $P \in V(\mathbb{K})$ and $\widetilde{P} \in \widetilde{V}(\overline{\mathbb{K}})$ 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 [17, 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 \tilde{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 all parameters; neither is the version recently suggested by Draziotis and Poulakis [9, 10], who also make some other restrictive assumptions (see Remark 3.1.3 in Chapter 3 for more on this).

In the thesis we obtain 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 [9, 10], and goes back to [1, 2].

For the precise statement of our results see the introduction of Chapter 3.

Plan of the thesis

In Chapter 1 we collect auxiliary facts of diverse nature, which are used throughout the thesis. In Chapter 2 we obtain an explicit version of the Riemann Existence Theorem over a number field. This chapter is based on the article [3], joint with Yu. Bilu. In Chapter 3 we obtain several explicit versions of the Chevalley-Weil Theorem for curves. This chapter is based on the article [4], joint with Yu. Bilu and A. Surroca.

Notation and Conventions

Let f(X) be a polynomial in X over some field (or integral domain), and β is an element of this field (or domain), then we denote by $\operatorname{ord}_{X=\beta}f$ the order of vanishing of f at β . Sometimes we write simply $\operatorname{ord}_{\beta}$ or even ord, when this does not lead to a confusion. We employ the same notation not only to polynomials, but also to formal power series in $X - \beta$.

We denote by α the finite point (α : 1) of the projective line \mathbb{P}^1 , and by ∞ the infinite point (1 : 0).

Let $\underline{\alpha} = (\alpha_1, \ldots, \alpha_N) \in \overline{\mathbb{Q}}^N$ be a point with algebraic coordinates in the affine space of dimension N. Let \mathbb{K} be a number field containing $\alpha_1, \ldots, \alpha_N$ and $M_{\mathbb{K}}$ be the set of its valuations. We assume that every valuation $v \in M_{\mathbb{K}}$ is normalized 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} , (then, in the case of an infinite *v*, the field \mathbb{K}_v is either \mathbb{R} or \mathbb{C}). For $v \in M_{\mathbb{K}}$ we put

$$|\underline{\alpha}|_v = \max\left\{|\alpha_1|_v, \dots, |\alpha_N|_v\right\}$$

Let $\underline{\alpha}$ be a point in $\mathbb{P}^N(\overline{\mathbb{Q}})$ such that the vector $(\alpha_0 : \ldots : \alpha_N)$ is a coordinate vector for $\underline{\alpha}$, we define then the absolute logarithmic projective height (in the sequel simply projective height) of the point $\underline{\alpha}$ as

$$h_{p}(\underline{\alpha}) = \frac{1}{[\mathbb{K}:\mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} [\mathbb{K}_{v}:\mathbb{Q}_{v}] \log \max\{|\alpha_{0}|_{v}, \dots, |\alpha_{N}|_{v}\}.$$
 (1)

Throughout the text, we also denote by h_a the absolute logarithmic affine height (or simply affine height from now on) on the affine space. Thus if $(\alpha_1, \ldots, \alpha_N)$ is a coordinate vector of a point in $\overline{\mathbb{Q}}^N$, we define

$$h_{a}(\alpha_{1},\ldots,\alpha_{N}) = h_{p}(1:\alpha_{1}:\ldots:\alpha_{N}).$$
(2)

or, in an equivalent way

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

where $\log^+ x := \log \max\{1, x\}.$

It is well-known and easy to verify that these definitions are independent of the choice of the field \mathbb{K} .

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

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

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

where $\mathcal{D}_{\mathbb{L}/\mathbb{K}}$ is the discriminant of \mathbb{L} over \mathbb{K} and $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}$ is the norm map. This quantity has the following properties. First, it is additive in towers: if $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ is a tower of number fields, then

$$\partial_{\mathbb{M}/\mathbb{K}} = \partial_{\mathbb{L}/\mathbb{K}} + \partial_{\mathbb{M}/\mathbb{L}}.$$

Second, it does not increase under the base extension: if \mathbb{K}' is a finite extension of \mathbb{K} and $\mathbb{L}' = \mathbb{L}\mathbb{K}'$ then

$$\partial_{\mathbb{L}'/\mathbb{K}'} \leq \partial_{\mathbb{L}/\mathbb{K}}.$$

Combining the two properties above, we obtain the "triangle inequality": if \mathbb{L}_1 and \mathbb{L}_2 are two extensions of \mathbb{K} , then

$$\partial_{\mathbb{L}_1\mathbb{L}_2/\mathbb{K}} \leq \partial_{\mathbb{L}_1/\mathbb{K}} + \partial_{\mathbb{L}_2/\mathbb{K}}.$$

All these properties will be used without special reference.

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

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

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.

Finally, we shall systematically use the following estimates from [19].

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

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

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

See [19], Corollary 1 of Theorem 2 for (4), Theorem 9 for (5), and (6) follows easily from the Corollary of Theorem 6.

Chapter 1

General Lemmas and Useful Tools

In this chapter we develop and collect some results we use sistematically afterwards, covering topics like heights of polynomials, algebraic varieties, formal (Puiseux) power series, ramifications and curves.

1.1 Heights

1.1.1 Estimates for Sums and Products of Polynomials

Recall that, for a polynomial f with algebraic coefficients, we denote by $h_p(f)$ and by $h_a(f)$, respectively, the projective height and the affine height of the vector of its coefficients ordered somehow, and the height $h_a(f_1, \ldots, f_s)$ 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 1.1.1 Let f_1, \ldots, f_s be polynomials in $\mathbb{Q}[X_1, \ldots, X_r]$ and put

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

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

- 1. $h_{a}(\prod_{i=1}^{s} f_{i}) \leq \sum_{i=1}^{s} h_{a}(f_{i}) + \log(r+1) \sum_{i=1}^{s-1} \deg f_{i},$
- 2. $h_{p}(\prod_{i=1}^{s} f_{i}) \ge \sum_{i=1}^{s} h_{p}(f_{i}) \sum_{i=1}^{s} \deg f_{i},$
- 3. $h_a(g(f_1, \ldots, f_s)) \le h_a(g) + (h + \log(s+1) + N\log(r+1)) \deg g.$

Notice that we use the projective height in Part 2, and the affine height in the other parts.

Proof. Part 2 is the famous Gelfond inequality, see, for instance, Proposition B.7.3 in [15]. The rest is an immediate consequence of Lemma 1.2 from [16]. \Box

Remark 1.1.2 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 $t \leq s$, then we may replace $\log(s+1)$ by $\log(t+1)$, and $\deg g$ by the degree with respect to these indeterminates:

 $h_{a}(g(f_{1},\ldots,f_{t},Y_{t+1},\ldots,Y_{s})) \leq h_{a}(g) + (h + \log(t+1) + N\log(t+1)) \deg_{Y_{1},\ldots,Y_{t}} g.$

Remark 1.1.3 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

$$h_{a}(\beta_{1}) + \dots + h_{a}(\beta_{\rho}) \leq h_{p}(f) + \log(\rho + 1)$$

This is a classical result of Mahler, see, for instance, [20, Lemma 3].

Corollary 1.1.4 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. $h_p(f) \le h_p(g) + \deg g$,
- 2. $h_a(f) \le h_p(g) + h_a(a) + \deg g$.

Proof. The first item of the corollary is a direct consequence of Part 2 of Lemma 1.1.1. Then one can remark that $h_p(f) = h_p(f/a)$ as the projective height is indipendend of multiplication by a constant, also that the projective and the affine heights of f/a coincides as one of the coefficients is 1. We have then

$$h_{a}(f) = h_{a}\left(a \cdot \frac{f}{a}\right) \le h_{a}(a) + h_{a}\left(\frac{f}{a}\right) = h_{a}(a) + h_{p}(f) \le h_{a}(a) + h_{p}(g) + \deg g,$$

where the first inequality holds by Part 1 of Lemma 1.1.1.

Corollary 1.1.5 Let α be an algebraic number and $f \in \mathbb{Q}[X,Y]$ be a polynomial with algebraic coefficients, let also $f^{(\alpha)}(X,Y) = f(X + \alpha,Y)$ and $m = \deg_X f$, then

$$h_{a}(f^{(\alpha)}) \le h_{a}(f) + mh_{a}(\alpha) + 2m\log 2.$$

Proof. This is a direct application of item 3 of Lemma 1.1.1, together with Remark 1.1.2. $\hfill \Box$

In one special case item 3 of Lemma 1.1.1 can be refined.

Lemma 1.1.6 Let $(f_{ij})_{ij}$ be an $s \times s$ matrix of polynomials in $\overline{\mathbb{Q}}[X_1, \ldots, X_r]$ of degrees and affine heights bounded by μ and h, respectively. Then

 $h_{a}\left(\det\left(f_{ij}\right)_{ij}\right) \leq s\left(h + \log s + \mu \log(r+1)\right).$

For the proof see [16], end of Section 1.1.1.

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

Lemma 1.1.7 Let $f(X,Y) \in \overline{\mathbb{Q}}[X,Y]$ be of X-degree m and Y-degree n. Then

$$h_{a}(R_{f}) \le (2n-1)h_{a}(f) + (2n-1)\left(\log(2n^{2}) + m\log 2\right),$$
 (1.1)

$$h_p(R_f) \le (2n-1)h_p(f) + (2n-1)\log\left((m+1)(n+1)\sqrt{n}\right),$$
 (1.2)

Proof. Estimate (1.2) is due to Schmidt [20, Lemma 4]. To prove (1.1), we invoke Lemma 1.1.6. 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 $h_a(f) + \log n$, the result follows after an obvious calculation.

Remark 1.1.8 Estimate (1.1) 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) satisfy

$$h_{a}(R_{f}) \leq (2 \deg f - 1)h_{a}(f) + (2 \deg f - 1)\log(2(\deg f)^{2}).$$

Finally, we need one more technical lemma.

Lemma 1.1.9 Let $g(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ be of X-degree m, and fix $\rho \in \overline{\mathbb{Q}}$. Put $f(X, Y) = (X - \rho)^m g((X - \rho)^{-1}, Y).$

Then

$$h_{a}(f) \le h_{a}(g) + mh_{a}(\rho) + 2m\log 2.$$

Proof. The polynomials g(X, Y) and $\tilde{g}(X, Y) = X^m g(X^{-1}, Y)$ have the same coefficients and thereby the same height. Now direct application of Lemma 1.1.1 and Remark 1.1.2 implies the result.

1.1.2 Bounds for Solutions of Algebraic Equations

Let $p_1(\underline{X}), \ldots, p_k(\underline{X})$ be polynomials in $\underline{X} = (X_1, \ldots, X_N)$ with algebraic coefficients. By an *isolated solution* of the system of polynomial equations

$$p_1(\underline{X}) = \ldots = p_k(\underline{X}) = 0. \tag{1.3}$$

we mean a zero-dimensional component of the algebraic set in $\overline{\mathbb{Q}}^N$ defined by (1.3). (Existence of such a component implies that $k \geq N$.) Our aim is to bound the height of an isolated solution in terms of the degrees and the heights of the polynomials p_1, \ldots, p_k .

Such a bound follows from the arithmetical Bézout inequality due to Bost, Gillet and Soulé [5] and Philippon [18]. Krick, Pardo and Sombra [16] did a great job of producing the user-friendly version of this fundamental result. We very briefly recall some facts from [16] which will be used here. For an affine algebraic set $V \subset \mathbb{A}^N$, defined over $\overline{\mathbb{Q}}$, Krick, Pardo and Sombra [16, Section 1.2] define the *height* of V, to be denoted here as $h_{\text{KPS}}(V)$. We do not reproduce here the full definition of this height function, but only list three of its properties. The first two follow immediately from the definition, for the third see [16, end of Section 1.2.3].

(positivity) For any V we have $h_{KPS}(V) \ge 0$.

(additivity) The height function is "additive" in the following sense: for any V_1 and V_2 without common components,

$$h_{KPS}(V_1 \cup V_2) = h_{KPS}(V_1) + h_{KPS}(V_2).$$

(one-point set) If $V = {\underline{\alpha}}$ is a one-point algebraic set, then

$$h_{a}(\underline{\alpha}) \le h_{KPS}(V).$$

In fact, $h_{\text{KPS}}({\underline{\alpha}})$ is defined by (3) with $\log^+|\underline{\alpha}|_v$ replaced, for an archimedean v, by $\log(1 + |\alpha_1|_v^2 + \cdots + |\alpha_N|_v^2)^{1/2}$.

The properties above have the following consequence: for an affine algebraic set ${\cal V}$

$$\sum_{\{\underline{\alpha}\} \text{ component of } V} h_{a}(\underline{\alpha}) \le h_{KPS}(V), \qquad (1.4)$$

where the sum is over the 0-dimensional components of $V(\overline{\mathbb{Q}})$. This will be used later.

We adapt the work of Krick, Pardo and Sombra as follows.

Proposition 1.1.10 Let \mathbb{K} be a number field and let

$$p_1(\underline{X}), \dots, p_k(\underline{X}) \in \mathbb{K}[\underline{X}]$$

be polynomials in $\underline{X} = (X_1, \ldots, X_N)$. Let $\underline{\alpha}$ be an isolated solution of (1.3) and $\mathbb{L} = \mathbb{K}(\underline{\alpha})$ the number field generated by the coordinates of $\underline{\alpha}$. Then $k \geq N$. Further, assume that

$$\deg p_1 \ge \deg p_2 \ge \ldots \ge \deg p_k.$$

and put

$$\nabla = \deg p_1 \cdots \deg p_N, \qquad \Sigma = \sum_{i=1}^N \frac{1}{\deg p_i}, \qquad h = \max\{h_a(p_1), \dots, h_a(p_k)\}.$$

Then

$$[\mathbb{L}:\mathbb{K}] \le \nabla, \tag{1.5}$$

$$[\mathbb{L}:\mathbb{K}]\mathbf{h}_{\mathbf{a}}(\underline{\alpha}) \le \nabla \Sigma h + 2\nabla N \log(N+1), \tag{1.6}$$

$$\partial_{\mathbb{L}/\mathbb{K}} \le 2\nabla\Sigma h + 5\nabla N \log(N+1), \tag{1.7}$$

(we refer to the Notations and Convention Chapter for the definition of $\partial_{\mathbb{L}/\mathbb{K}}$).

The following consequence is immediate.

Corollary 1.1.11 In the set-up of Proposition 1.1.10, denote by V the algebraic subset of $\overline{\mathbb{Q}}^N$ defined by (1.3), and let W be another algebraic subset of $\overline{\mathbb{Q}}^N$ such that the difference set $V \setminus W$ is finite. Then every $\underline{\alpha} \in V \setminus W$ satisfies (1.5), (1.6) and (1.7).

For the proof of Proposition 1.1.10 we shall use the following lemma, due to Silverman [23, Theorem 2].

Lemma 1.1.12 Let \mathbb{K} be a number field and $\underline{\alpha}$ be a point in $\overline{\mathbb{Q}}^N$. Then the relative discriminant $\partial_{\mathbb{L}/\mathbb{K}}$ of the field $\mathbb{L} = \mathbb{K}(\underline{\alpha})$ over \mathbb{K} satisfies the inequality

$$\partial_{\mathbb{L}/\mathbb{K}} \leq 2([\mathbb{L}:\mathbb{K}]-1)h_{a}(\underline{\alpha}) + \log[\mathbb{L}:\mathbb{K}].$$

Proof of Proposition 1.1.10 We denote by V the algebraic set defined by (1.3). Since it has a 0-dimensional component $\underline{\alpha}$, we have $k \geq N$. Among the k polynomials p_1, \ldots, p_k one can select N polynomials q_1, \ldots, q_N such that $\underline{\alpha}$ is an isolated solution of the system $q_1(\underline{X}) = \ldots = q_N(\underline{X}) = 0$. The algebraic set defined by this system has at most deg $q_1 \cdots \text{deg } q_N \leq \nabla$ irreducible (over $\overline{\mathbb{Q}}$) components: this follows from the geometric Bézout inequality. In particular, there is at most ∇ isolated solutions. Since a \mathbb{K} -conjugate of an isolated solution is again an isolated solution, we must have (1.5). Since all conjugates of α have the same height, the left-hand side of (1.4) exceeds $[\mathbb{L} : \mathbb{K}]h_{\mathbf{a}}(\alpha)$.

On the other hand, Krick, Pardo and Sombra proved that

$$h_{\text{KPS}}(V) \le \nabla \Sigma h + 2\nabla N \log(N+1);$$

see Corollary 2.11 from [16], or, more precisely, the displayed inequality just before the beginning of Section 2.2.3 on page 555 of [16]. Together with (1.4) this proves (1.6). Combining it with Lemma 1.1.12, we obtain (1.7). \Box

1.1.3 Height of sets of places

We summarize the properties of this height in the following proposition:

Proposition 1.1.13 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

$$\mathbf{h}(S_{\mathbb{L}}) \le \mathbf{h}(S) \le [\mathbb{L} : \mathbb{K}]\mathbf{h}(S_{\mathbb{L}}).$$

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

$$\begin{split} h\big(\mathrm{Den}_{\mathbb{K}}(\underline{\alpha})\big) &\leq [\mathbb{K}(\underline{\alpha}) : \mathbb{K}]h_{\mathrm{a}}(\underline{\alpha}), \\ h\big(\mathrm{Num}_{\mathbb{K}}(\underline{\alpha})\big) &\leq [\mathbb{K}(\underline{\alpha}) : \mathbb{K}]\big(h_{\mathrm{a}}(\underline{\alpha}) - h_{\mathrm{p}}(\underline{\alpha})\big) \qquad (\underline{\alpha} \neq \underline{0}). \end{split}$$

In particular, for $\alpha \in \overline{\mathbb{K}}^*$ we have $h(\operatorname{Num}_{\mathbb{K}}(\alpha)) \leq [\mathbb{K}(\alpha) : \mathbb{K}]h_a(\alpha)$.

This will be used without special reference.

1.1.4 Height and Discriminants

We need some estimates for the discriminant of a number field in terms of the heights of its generators. Lemma 1.1.12 has the following consequence:

Corollary 1.1.14 Let $f(X) \in \mathbb{K}[X]$ be a polynomial of degree N. Then

$$\sum_{f(\alpha)=0} \partial_{\mathbb{K}(\alpha)/\mathbb{K}} \le 2(N-1)h_{p}(f) + 3N\log N,$$
(1.8)

the sum being over the roots of f.

Proof. Since for any root α we have $[\mathbb{K}(\alpha) : \mathbb{K}] \leq N$, we estimate the left-hand side of (1.8) by Lemma 1.1.12 as

$$2(N-1)\sum_{f(\alpha)=0} \mathbf{h}_{\mathbf{a}}(\alpha) + N\log N.$$

Remark 1.1.3 allows us to bound the sum on the right by $h_p(f) + \log(N+1)$. Now, to complete the proof, just remark that $(N-1)\log(N+1) \le N\log N$. \Box

We shall also need a bound for the discriminant of a different nature, known as the *Dedekind-Hensel inequality* (see [7, 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 1.1.15 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 $\operatorname{Ram}(\mathbb{L}/\mathbb{K})$ be the set of places of \mathbb{K} ramified in \mathbb{L} . Then

$$\partial_{\mathbb{L}/\mathbb{K}} \le \frac{\nu - 1}{\nu} h(\operatorname{Ram}(\mathbb{L}/\mathbb{K})) + 1.26\nu.$$
 (1.9)

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 $\sum_{p \leq \nu} 1 \leq 1.26\nu / \log \nu$, which is (4).

A similar estimate was obtained by Serre [22, Proposition 4]. However, (1.9) is more suitable for our purposes.

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

Lemma 1.1.16 In the set-up of Lemma 1.1.15 we have

$$h(\operatorname{Ram}(\mathbb{L}/\mathbb{K})) \leq \nu \partial_{\mathbb{L}/\mathbb{K}}.$$

1.2 Power Series

In this section \mathbb{K} is a field of characteristic 0 and $f(X, Y) \in \mathbb{K}[[X]][Y]$ is a polynomial in Y with coefficients in the ring $\mathbb{K}[[X]]$ of formal power series. We denote by ord the order of vanishing at 0. By the initial segment of length κ of a power series $y = \sum_{k=0}^{\infty} \gamma_k X^k$ we mean $y = \sum_{k=0}^{\kappa} \gamma_k X^k$.

Lemma 1.2.1 Let $\widetilde{y} = \sum_{k=0}^{\kappa} \gamma_k X^k \in \mathbb{K}[X]$ be a polynomial in X of degree at most κ . Assume that

$$\operatorname{ord} f(X, \widetilde{y}) > 2\kappa, \quad \operatorname{ord} f'_Y(X, \widetilde{y}) = \kappa.$$

Then there exists a unique formal power series $y = \sum_{k=0}^{\infty} \gamma_k X^k$ belonging to $\mathbb{K}[[X]]$ such that f(X, y) = 0, and such that \tilde{y} is the initial segment of y of length κ .

Proof. By Hensel's Lemma, there exists a unique power series y such that f(X, y) = 0 and $\operatorname{ord}(y - \tilde{y}) > \kappa$. The latter inequality implies that \tilde{y} is the initial segment of y of length κ .

Lemma 1.2.2 Let $y_1, y_2 \in \mathbb{K}[[X]]$ be distinct formal power series such that

$$f(X, y_1) = f(X, y_2) = 0.$$

Put $\kappa_j = \operatorname{ord} f'_Y(X, y_j)$. Then there exist $k \leq \min\{\kappa_1, \kappa_2\}$ such that the k-th coefficients of y_1 and y_2 are distinct.

Proof. Let \widetilde{y}_j be the initial segment of y_j of length κ_j . Then

$$\operatorname{ord}(y_j - \widetilde{y}_j) > \kappa_j.$$

Hence

$$f(X, \widetilde{y}_j) = f(X, y_j) + f'_Y(X, y_j)(y_j - \widetilde{y}_j) + \text{terms of order} > 2\kappa_j,$$

Since $f(X, y_j) = 0$ and $\operatorname{ord} f'_Y(X, y_j) = \kappa_i$, the right-hand side is of order $> 2\kappa_j$. Similarly,

$$f'_Y(X, \widetilde{y}_j) = f'_Y(X, y_j) + \text{terms of order} > \kappa_j,$$

which implies that the right-hand side is of order κ_i . We have proved that

$$\operatorname{ord} f(X, \widetilde{y}_j) > 2\kappa_j, \qquad \operatorname{ord} f'_Y(X, \widetilde{y}_j) = \kappa_j$$

Lemma 1.2.1 implies that y_j is the unique power series satisfying $f(X, y_j) = 0$ and having \tilde{y}_j as an initial segment. Since the series y_1 and y_2 are distinct, none of \tilde{y}_j can be an initial segment of the other¹. Whence the result. \Box

Lemma 1.2.3 Suppose \mathbb{K} algebrically closed and let $y_1, \ldots, y_\ell \in \mathbb{K}[[X]]$ be pairwise distinct formal power series such that

$$f(X, y_1) = \ldots = f(X, y_\ell) = 0.$$

Assume that f is monic² in Y and that

$$\sum_{j=1}^{\ell} \operatorname{ord} f'_Y(y_j) = \operatorname{ord} d(X), \qquad (1.10)$$

where d(X) is the Y-discriminant of f. Then f splits into linear factors over the ring $\mathbb{K}[[X]]$:

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

where $y_1, \ldots, y_n \in \mathbb{K}[[X]]$.

Proof. Since f is monic, it splits, by the Puiseux theorem, into linear factors over the ring $\mathbb{K}[[X^{1/e}]]$ for some e:

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

where $y_{\ell+1}, \ldots, y_n \in \mathbb{K}[[X^{1/e}]]$. Further, $d(X) = \prod_{j=1}^n f'_Y(y_j)$, which, together with (1.10) implies that

$$\operatorname{ord} f'_{Y}(y_j) = 0 \qquad (j = \ell + 1, \dots, n).$$
 (1.11)

²that is, f is of the form Y^n + terms of lower degree in Y

¹If, say, \tilde{y}_1 is an initial segment of \tilde{y}_2 then the same argument as above shows that $\operatorname{ord} f'_Y(X, \tilde{y}_2) = \operatorname{ord} f'_Y(X, \tilde{y}_1)$, that is, $\kappa_1 = \kappa_2$, whence $\tilde{y}_1 = \tilde{y}_2$. Lemma 1.2.1 now implies that $y_1 = y_2$, a contradiction.

If we now write $y_j = a_{j0} + a_{j1}X^{1/e} + \dots$, then (1.11) implies that

$$\operatorname{ord} f'_{Y}(X, a_{j0}) = 0$$
 $(j = \ell + 1, \dots, n).$

Lemma 1.2.1 now implies that in each of the rings $\mathbb{K}[[X]]$ and $\mathbb{K}[[X^{1/e}]]$, the polynomial f has exactly one root with initial term a_{j0} . Hence $y_j \in \mathbb{K}[[X]]$ for $j = \ell + 1, \ldots, n$, as wanted.

1.3 Integral Elements

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

Lemma 1.3.1 Let \mathbb{L} be a finite separable extension of \mathbb{K} of degree n and \overline{R} the integral closure of R in \mathbb{L} . Let $\omega_1, \ldots, \omega_n \in \overline{R}$ form a base of \mathbb{L} over \mathbb{K} . We denote by Δ the discriminant of this basis: $\Delta = \left(\det \left[\sigma_i(\omega_j)\right]_{ij}\right)^2$, where $\sigma_1, \ldots, \sigma_n : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ are the distinct embeddings of \mathbb{L} into $\overline{\mathbb{K}}$. Then

$$\bar{R} \subset \Delta^{-1}(R\omega_1 + \dots + R\omega_n).$$

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

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

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

Corollary 1.3.2 Let

$$f(T) = f_0 T^n + f_1 T^{n-1} + \dots + f_n \in R[T]$$

be a K-irreducible polynomial, and $\alpha \in \overline{\mathbb{K}}$ one of its roots. Let \overline{R} be the integral closure of R in the field $\mathbb{K}(\alpha)$. Then $\overline{R} \subset \Delta(f)^{-1}R[\alpha]$. where $\Delta(f)$ is the discriminant of f.

Proof. It is well-known that the quantities

$$\omega_1 = 1,$$

$$\omega_2 = f_0 \alpha,$$

$$\omega_3 = f_0 \alpha^2 + f_1 \alpha,$$

$$\dots$$

$$\omega_n = f_0 \alpha^{n-1} + f_1 \alpha^{n-2} + \dots + f_{n-2} \alpha$$

are integral over R; see, for example, [21, page 183]. Applying Lemma 1.3.1 to the basis $\omega_1, \ldots, \omega_n$, we complete the proof.

1.4 Local Lemmas

In this section \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 unit³.

Lemma 1.4.1 Let $f(X) \in \mathcal{O}_v[X]$ be a *v*-monic polynomial, and let $\eta \in \mathbb{K}$ 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 $|R(f, f')|_v < 1$, where R(f, f') is the resultant of *f* and *f'*.

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 we have $h(X) \in \mathcal{O}_v[X]$, and since $f'(\eta) = g'(\eta)h(\eta)$, we obtain $|f'(\eta)|_v \leq |g'(\eta)|_v < 1$. Since R(f, f')is a linear combination of f and f' with coefficients in $\mathcal{O}_v[X]$, the result follows.

Given a polynomial f(X) over some field of characteristic 0, we define by $\hat{f}(X)$ the radical of f, that is, the separable polynomial, having the same

³We say that α is a *v*-adic unit if $|\alpha|_v = 1$.

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 1.4.2 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.

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 $|\widehat{f}(\xi)|_v < 1$. \Box

Lemma 1.4.3 Let $f(X) \in \mathcal{O}_v[X]$ and $\xi \in \mathcal{O}_v$ satisfy

 $|f(\xi)|_v < 1, \qquad |f'(\xi)|_v = 1.$

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 1.4.4 Let $f(X), g(X) \in \mathcal{O}_v[X]$ and $\alpha, \xi \in \mathcal{O}_v$ satisfy

$$f(X) = (X - \alpha)^m g(X), \qquad 0 < |\xi - \alpha|_v < |g(\alpha)|_v$$

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.

1.5 Miscellaneous Lemmas

Lemma 1.5.1 Let C be a smooth projective curve defined over an algebraically closed field \mathbb{K} of characteristic 0. Let $x \in \mathbb{K}(C)$ have only simple poles, and let $y \in \mathbb{K}(C)$ have a single (possibly, multiple) pole which is a pole of x as well. Then $\mathbb{K}(C) = \mathbb{K}(x, y)$.

Proof. Since x has only simple poles in $\mathbb{K}(\mathcal{C})$, the place at ∞ of the field $\mathbb{K}(x)$ splits completely in $\mathbb{K}(\mathcal{C})$. Let P be the pole of y, and let \tilde{P} be the place of $\mathbb{K}(x, y)$ below P. Then \tilde{P} is above the place at ∞ of $\mathbb{K}(x)$. Hence it also splits completely in $\mathbb{K}(\mathcal{C})$.

Now assume that $\mathbb{K}(x, y)$ is a proper subfield of $\mathbb{K}(\mathcal{C})$. Then there are at least two places of $\mathbb{K}(\mathcal{C})$ above \tilde{P} . In particular, there is a place $P' \neq P$ above \tilde{P} . This P' must be a pole of y, a contradiction. \Box

Lemma 1.5.2 Let \mathbb{K} be an algebraically closed field of characteristic 0 and let V be a non-empty irreducible quasiprojective variety over \mathbb{K} . Let $\{(\mathcal{C}_t, D_t) : t \in V\}$ be an algebraic family of curves supplied with an effective divisor. Also, let s be a positive integer. Assume that there exists $\tau \in V$ such that \mathcal{C}_{τ} is irreducible and dim $\mathcal{L}(D_{\tau}) = s$. Then the set

$$\left\{ t \in V : \begin{array}{l} \text{either } \mathcal{C}_t \text{ is reducible} \\ \text{or } \mathcal{C}_t \text{ is irreducible and } \dim \mathcal{L}(D_t) > s \end{array} \right\}$$

is not Zariski dense in V.

Proof. This is a consequence of the theorems of Bertini and semi-continuity, see, for instance, Theorem 12.8 in [14, Chapter III]. \Box

Lemma 1.5.3 Given a positive integer n and a finite set $M \subset \mathbb{C}$, there exist only finitely many extensions of the rational function field $\mathbb{C}(x)$ of degree n, unramified outside M.

Proof. This is an immediate consequence of the uniqueness statement of Theorem A. \Box

Chapter 2

Effective Riemann Esistence Theorem

2.1 Introduction

To state the main result of this chapter, we recall briefly one of the topological forms of the Riemann Existence Theorem.

Theorem 2.1.1 Let M be a finite subset of $\mathbb{P}^1(\mathbb{C})$. Then for any finite covering of $\mathbb{P}^1(\mathbb{C})$ by a closed oriented surface, unramified outside the set M, there exists a complex algebraic curve \mathcal{C} and a rational function $x \in \mathbb{C}(\mathcal{C})$ such that our covering is isomorphic¹ to $\mathcal{C}(\mathbb{C}) \xrightarrow{x} \mathbb{P}^1(\mathbb{C})$, the covering defined by x. Moreover, the couple (\mathcal{C}, x) is unique up to a naturally defined isomorphism².

As we said in the introduction, the purpose of this chapter is to give an effective description of the couple (\mathcal{C}, x) . We produce a plane model of \mathcal{C} over $\overline{\mathbb{Q}}$, such that one of the coordinates is x, and we give explicit bounds for the degree and the height of the defining equation of this model, and of the degree and discriminant of the number field over which this model is defined.

Our method of proof is as follows. First, we use the existence part of Theorem 2.1.1 to show the existence of \mathcal{C} and x. Next, we define "quasicanonically" a generator y of $\overline{\mathbb{Q}}(\mathcal{C})$ over $\overline{\mathbb{Q}}(x)$, and denote by f(X,Y) the

¹Two coverings $S_1 \xrightarrow{\pi_1} S$ and $S_2 \xrightarrow{\pi_2} S$ of topological spaces are *isomorphic* if there exists a homeomorphism $S_1 \xrightarrow{\varphi} S_2$ such that $\pi_1 = \pi_2 \circ \varphi$.

²If (\mathcal{C}', x') is another such couple, then the field isomorphism $\mathbb{C}(x) \to \mathbb{C}(x')$ given by $x \mapsto x'$, extends to a field isomorphism $\mathbb{C}(\mathcal{C}) \to \mathbb{C}(\mathcal{C}')$.

irreducible polynomial satisfying f(x, y) = 0. Further, we show that the coefficients of this polynomial satisfy certain system of algebraic equations and inequalities, and we use the uniqueness part of Theorem 2.1.1 to show that the set of solutions of the system is finite. (To be more precise, the coefficients of f form only a part of the variables involved in the equations and inequalities.) Using this, we estimate the height of the polynomial, and the degree and discriminant of the number field generated by its coefficients.

Let us state our principal result.

Theorem 2.1.2 Let $S \to \mathbb{P}^1(\mathbb{C})$ be a finite covering of degree $n \ge 2$ by a closed oriented surface S of genus \mathbf{g} , unramified outside a finite set $\mathbf{M} \subset \mathbb{P}^1(\overline{\mathbb{Q}})$. Put³

$$\mathbb{K} = \mathbb{Q}(\mathcal{M}), \qquad h = \max\{h_{\mathbf{a}}(\alpha) : \alpha \in \mathcal{M}\}, \qquad \Lambda = \left(2(\mathbf{g}+1)n^2\right)^{10\mathbf{g}n+12n}.$$

Then there exist a number field \mathbb{L} , containing \mathbb{K} , an algebraic curve \mathcal{C} defined over \mathbb{L} and rational functions $x, y \in \mathbb{L}(\mathcal{C})$ such that $\mathbb{L}(\mathcal{C}) = \mathbb{L}(x, y)$ and the following is true.

- 1. The covering $x : \mathcal{C}(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is isomorphic to the given covering $S \to \mathbb{P}^1(\mathbb{C})$.
- 2. The rational functions $x, y \in \mathbb{L}(\mathcal{C})$ satisfy the equation f(x, y) = 0, where the absolutely irreducible polynomial $f(X, Y) \in \mathbb{L}[X, Y]$ is such that

$$\deg_X f = \mathbf{g} + 1, \qquad \deg_Y f = n, \qquad \mathbf{h}_{\mathbf{a}}(f) \le \Lambda(h+1). \tag{2.1}$$

3. The degree and the discriminant of \mathbb{L} over \mathbb{K} satisfy

$$[\mathbb{L}:\mathbb{K}] \le \Lambda, \qquad \partial_{\mathbb{L}/\mathbb{K}} \le \Lambda(h+1), \tag{2.2}$$

(we recall that $\partial_{\mathbb{L}/\mathbb{K}} = (\log \mathcal{N}_{\mathbb{K}/\mathbb{Q}} \mathcal{D}_{\mathbb{L}/\mathbb{K}})/[\mathbb{L}:\mathbb{Q}]$ and $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}$ is the norm map).

³A pedantic reader may complain that the definition of h below is formally incorrect, because $h_a(\cdot)$ is the affine height, and M is a subset of the projective line. Of course, this can be easily overcome, for instance by writing $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ and defining $h_a(\infty) = 0$.

This argument is inspired by the work of Zverovich [24], who applies a rather similar approach, though he works only in the complex domain. The system of equation considered by Zverovich is simpler than ours, but we could not understand one key point in his proof of the finiteness of the number of solutions.

Our result is sensitive only to the set M of ramification points, and the degree n of the covering. It would be interesting to obtain a more precise result, which depends on the more subtle elements of the "covering data", like the monodromy permutations associated to every ramification point. Probably, the "correct" statement of Theorem 2.1.2 must involve the notion of the Hurwitz space associated to the given topological covering, see [8]. Another interesting problem is to characterize our curve not in terms of the defining equation, but in more invariant terms, for instance, to estimate its Faltings height.

In our result, the quantity Λ depends exponentially on n. This improves on Theorem 3A from [1], where the dependence is doubly exponential. There are strong reasons to believe that the "correct" estimate is polynomial in n. Indeed, this is case for a similar problem over a function field, see the recent work of Edixhoven et al. [13].

2.2 Setup for the Proof of Theorem 2.1.2

Let $S \to \mathbb{P}^1(\mathbb{C})$ be a covering as in the statement of Theorem 2.1.2. According to Theorem A, our covering is isomorphic to $\mathcal{C}(\mathbb{C}) \xrightarrow{x} \mathbb{P}^1(\mathbb{C})$, where \mathcal{C} is a complex algebraic curve and x is a rational function on \mathcal{C} . Since all ramification points of the latter covering are algebraic, the curve \mathcal{C} the function xare definable over $\overline{\mathbb{Q}}$.

We are going to find a field $\mathbb{L} \supset \mathbb{K}$, a function $y \in \mathbb{L}(\mathcal{C})$ such that $\overline{\mathbb{Q}}(\mathcal{C}) = \overline{\mathbb{Q}}(x, y)$, and an absolutely irreducible polynomial $f(X, Y) \in \mathbb{L}[X, Y]$ such that f(x, y) = 0, and such that the degrees $\deg_X f$, $\deg_Y f$, the height $h_a(f)$, as well as the degree $[\mathbb{L} : \mathbb{K}]$ and the relative discriminant of \mathbb{L}/\mathbb{K} satisfy required (in)equalities. To achieve this, we define algebraic sets V and W in a high-dimensional affine space, such that the set $V \setminus W$ contains a point having the coefficients of f as part of its coordinates. We then show that the set $V \setminus W$ is finite (and hence the coefficients of f) using Corollary 1.1.11. As a by-product, we will also bound the degree and the discriminant of the field generated by the coefficients.

We write

$$\mathbf{M} = \{\alpha_1, \ldots, \alpha_\mu\}.$$

For the main part of the proof we shall assume that the curve C is unramified over ∞ (that is, ∞ is not one of the points $\alpha_1, \ldots, \alpha_{\mu}$), and that C has no Weierstrass point above ∞ . In other words, the poles of x are neither ramified nor Weierstrass. The general case easily reduces to this one, see Section 2.12.

Now we start the detailed proof. Since it is going to be long and involved, we divide it into short logically complete steps.

2.3 Function y and Polynomial f(X, Y)

Fix a pole P of x. Since P is not a Weierstrass point of \mathcal{C} , we have

$$\dim \mathcal{L}(mP) = 2, \qquad \dim \mathcal{L}((m-1)P) = 1.$$

with $m = \mathbf{g}(\mathcal{C}) + 1$.

Since x is unramified above the infinity, x^{-1} can serve as a local parameter at P. If y belongs to $\mathcal{L}(mP)$, but not to $\mathcal{L}((m-1)P)$, then y has the Puiseux expansion at P of the form $\sum_{k=-m}^{\infty} c_k x^{-k}$ with $c_{-m} \neq 0$. Since $\dim \mathcal{L}(mP) = 2$, there exists a unique $y \in \mathcal{L}(mP)$ with the properties

$$c_{-m} = 1, \qquad c_0 = 0.$$
 (2.3)

In the sequel, we mean by y the function satisfying these conditions.

The function y has a single pole P which is a pole of x as well. Lemma 1.5.1 implies now that $\overline{\mathbb{Q}}(\mathcal{C}) = \overline{\mathbb{Q}}(x, y)$ (here we use the assumption that x is unramified above ∞). Also, y is integral over the ring $\overline{\mathbb{Q}}[x]$. Hence, there exists a unique absolutely irreducible polynomial $f(X, Y) \in \overline{\mathbb{Q}}[X, Y]$, such that f(x, y) = 0, monic in Y and satisfying

$$\deg_Y f = [\overline{\mathbb{Q}}(\mathcal{C}) : \overline{\mathbb{Q}}(x)] = n.$$

We also have

$$\deg_X f = [\bar{\mathbb{Q}}(\mathcal{C}) : \bar{\mathbb{Q}}(y)] = \deg(y)_{\infty} = m,$$

where $(y)_{\infty} = mP$ is the divisor of poles of y. We write

$$f(X,Y) = Y^{n} + \sum_{j=0}^{n-1} \sum_{i=0}^{m} \theta_{ij} X^{i} Y^{j}.$$
 (2.4)

2.4 The Discriminant and its Roots, and the Puiseux Expansions

Let d(X) be the discriminant of f(X, Y) with respect to Y. Every α_i is a root of d(X). Besides the α_i -s, the polynomial d(X) may have other roots; we denote them $\beta_1, \ldots, \beta_{\nu}$. Thus, we have

$$d(X) = \delta \prod_{i=1}^{\mu} (X - \alpha_i)^{\sigma_i} \prod_{i=1}^{\nu} (X - \beta_i)^{\tau_i}, \qquad (2.5)$$

where $\delta \in \overline{\mathbb{Q}}^*$ and where σ_i and τ_i are positive integers.

Now fix $i \in \{i, \ldots, \nu\}$. Since x is unramified over β_i , the function y has n Puiseux expansions at β_i of the form

$$y_{ij} = \sum_{k=0}^{\infty} \gamma_{ijk} \left(x - \beta_i \right)^k \qquad (j = 1, \dots, n).$$

We put

$$\kappa_{ij} = \operatorname{ord}_{\beta_i} f'_Y(x, y_{ij}).$$

Then

$$\kappa_{i1} + \dots + \kappa_{in} = \tau_i. \tag{2.6}$$

We may assume that $\kappa_{i1} \geq \ldots \geq \kappa_{in}$ and we define ℓ_i from the condition

$$\kappa_{i\ell_i} > 0, \qquad \kappa_{ij} = 0 \quad \text{for } j > \ell_i.$$
 (2.7)

Then (2.6) reads

$$\sum_{j=1}^{\ell_i} \kappa_{ij} = \tau_i, \qquad (2.8)$$

which implies that

$$\sum_{\substack{1 \le i \le \nu \\ 1 \le j \le \ell_i}} (\kappa_{ij} + 1) \le \sum_{\substack{1 \le i \le \nu \\ 1 \le j \le \ell_i}} 2\kappa_{ij} = 2(\tau_1 + \dots + \tau_\nu) \le 2 \deg d(X).$$
(2.9)

This inequality will be used in Section 2.6.

We also let \tilde{y}_{ij} be the initial segment of the series y_{ij} of length κ_{ij} :

$$\widetilde{y}_{ij} = \sum_{k=0}^{\kappa_{ij}} \gamma_{ijk} \left(x - \beta_i \right)^k.$$
(2.10)

Then we have

$$\operatorname{ord}_{\beta_i} f(x, \widetilde{y}_{ij}) > 2\kappa_{ij}, \quad \operatorname{ord}_{\beta_i} f'_Y(x, \widetilde{y}_{ij}) = \kappa_{ij},$$

see the proof of Lemma 1.2.2.

Lemma 1.2.2 also implies that, for every fixed *i*, neither of $\tilde{y}_{i1}, \ldots, \tilde{y}_{in}$ is an initial segment of the other. In other words, for every distinct indices $j_1, j_2 \in \{1, \ldots, n\}$ there is a non-negative integer $\lambda(i, j_1, j_2) \leq \min \{\kappa_{ij_1}, \kappa_{ij_2}\}$ such that

$$\gamma_{ij_1\lambda(i,j_1,j_2)} \neq \gamma_{ij_2\lambda(i,j_1,j_2)}$$

2.5 The Puiseux Expansions at Infinity

We also have the Puiseux expansions of y at infinity:

$$y_{\infty j} = \sum_{k=0}^{\infty} \gamma_{\infty jk} x^{-k} \qquad (j = 2, \dots, n),$$

$$y_{\infty 1} = \sum_{k=-m}^{\infty} \gamma_{\infty 1k} x^{-k}.$$
 (2.11)

We define the polynomials

$$g(T,Y) = T^m f(T^{-1},Y), \qquad h(T,Y) = T^{m(n+1)} f(T^{-1},T^{-m}Y)$$

and put $t = x^{-1}$, so that the expansions (2.11) can be written in powers of t. Now we define the numbers

$$\kappa_{\infty j} = \operatorname{ord}_{t=0} g'_Y(t, y_{\infty j}) \qquad (j = 2, \dots, n),$$

$$\kappa_{\infty 1} = \operatorname{ord}_{t=0} h'_Y(t, t^m y_{\infty 1}).$$

We have $h(T, T^m Y) = T^{mn}g(T, Y)$, whence

$$\kappa_{\infty 1} = mn + \operatorname{ord}_{t=0} g'_Y(t, y_{\infty 1}).$$

Hence the sum $\kappa_{\infty 1} + \kappa_{\infty 2} + \cdots + \kappa_{\infty n}$ is bounded by mn plus the order at T = 0 of the Y-discriminant of g(T, Y). Bounding the latter order by the degree of this discriminant, we obtain

$$\kappa_{\infty 1} + \kappa_{\infty 2} + \dots + \kappa_{\infty n} \le mn + \deg d(X). \tag{2.12}$$

$$\ell_{\infty} = n, \tag{2.13}$$

we re-write (2.12) as

$$\sum_{1 \le j \le \ell_{\infty}} (\kappa_{\infty j} + 1) \le (m+1)n + \deg d(X).$$
(2.14)

This will be used in Section 2.6.

Further, for j = 2, ..., n let $\tilde{y}_{\infty j}$ be the initial segment of the series $y_{\infty j}$ of length $\kappa_{\infty j}$, and let $\tilde{y}_{\infty 1}$ be the initial segment of the series $y_{\infty 1}$ of the length $\kappa_{\infty 1}$:

$$\widetilde{y}_{\infty j} = \sum_{k=0}^{\kappa_{\infty j}} \gamma_{\infty jk} t^k \qquad (j = 2, \dots, n),$$
(2.15)

$$\widetilde{y}_{\infty 1} = \sum_{k=-m}^{\kappa_{\infty 1}-m} \gamma_{\infty 1k} t^k.$$
(2.16)

Then we have

$$\operatorname{ord}_{t=0} g\left(t, \widetilde{y}_{\infty j}\right) > 2\kappa_{\infty j}, \qquad \operatorname{ord}_{t=0} g'_Y\left(t, \widetilde{y}_{\infty j}\right) = \kappa_{\infty j} \qquad (j = 2, \dots, n),$$

$$\operatorname{ord}_{t=0} h\left(t, t^m \widetilde{y}_{\infty 1}\right) > 2\kappa_{\infty 1}, \quad \operatorname{ord}_{t=0} h'_Y\left(t, t^m \widetilde{y}_{\infty 1}\right) = \kappa_{\infty 1}.$$

Identities (2.3) now become

$$\gamma_{\infty 1,-m} = 1, \qquad \gamma_{\infty 10} = 0.$$

As in the finite case, for every distinct $j_1, j_2 \in \{2, \ldots, n\}$ there exists a nonnegative integer $\lambda(\infty, j_1, j_2) \leq \min \{\kappa_{\infty j_1}, \kappa_{\infty j_2}\}$ such that

$$\gamma_{\infty j_1 \lambda(\infty, j_1, j_2)} \neq \gamma_{\infty j_2 \lambda(\infty, j_1, j_2)}.$$

2.6 The Indeterminates

We consider the vector

$$\varphi = \left(\underline{\theta}, \underline{\alpha}, \underline{\beta}, \underline{\gamma}, \delta\right),\,$$

where

• $\underline{\theta} = (\theta_{ij})_{\substack{0 \le i \le m \\ 0 \le j \le n-1}}$ is the vector of coefficients of f, see (2.4);

- $\underline{\alpha} = (\alpha_i)_{1 \le i \le \mu}$ and $\underline{\beta} = (\beta_i)_{1 \le i \le \nu}$ are the vectors of roots of the discriminant d(X), and δ is its leading coefficient, see (2.5);
- $\underline{\gamma} = \left(\underline{\gamma}_{ij}\right)_{\substack{i \in \{1, \dots, \nu, \infty\}\\ 1 \leq j \leq \ell_i}}$, where ℓ_i are defined in (2.7) and (2.13), and $\underline{\gamma}_{ij}$ is the vectors of coefficients of the initial segment \widetilde{y}_{ij} of the Puiseux expansion y_{ij} , that is,

$$\underline{\gamma}_{ij} = (\gamma_{ijk})_{0 \le k \le \kappa_{ij}}, \qquad (i,j) \ne (\infty,1),$$
$$\underline{\gamma}_{\infty 1} = (\gamma_{\infty 1k})_{-m \le k \le \kappa_{\infty 1} - m}$$

see (2.10), (2.15) and (2.16).

We are only interested in the vectors $\underline{\theta}$ and $\underline{\alpha}$, but we cannot study them separately of the other vectors defined above.

Vector φ belongs to the affine space $\overline{\mathbb{Q}}^{\Omega}$ of dimension

$$\Omega := (m+1)n + \mu + \nu + \sum_{\substack{1 \le i \le \nu \\ 1 \le j \le \ell_i}} (\kappa_{ij}+1) + \sum_{1 \le j \le \ell_\infty} (\kappa_{\infty j}+1) + 1$$

$$\leq 2(m+1)n + 4 \deg d(X) + 1$$

$$\leq 10mn + 2n - 8m + 1, \qquad (2.17)$$

where we use (2.9), (2.14) and the estimates $\mu + \nu \leq \deg(d(X)) \leq 2m(n-1)$.

We shall define algebraic sets V and W in $\overline{\mathbb{Q}}^{\Omega}$ such that $\varphi \in V \setminus W$ and $V \setminus W$ is finite. This will allow us to use Corollary 1.1.11 to bound the height of φ . This would imply a bound on the height of $\underline{\theta}$, which is the height of the polynomial f.

To define our algebraic sets, we introduce the vector of indeterminates Φ whose coordinates correspond to the coordinates of φ :

$$\Phi = (\underline{\Theta}, \underline{A}, \underline{B}, \underline{\Gamma}, \Delta) \,,$$

where

$$\underline{\Theta} = (\Theta_{ij})_{\substack{0 \le i \le m \\ 0 \le j \le n-1}}, \quad \underline{\mathbf{A}} = (\mathbf{A}_i)_{1 \le i \le \mu}, \quad \underline{\mathbf{B}} = (\mathbf{B}_i)_{1 \le i \le \nu}, \quad \underline{\Gamma} = \left(\underline{\Gamma}_{ij}\right)_{\substack{i \in \{1, \dots, \nu, \infty\} \\ 1 \le j \le \ell_i}}$$

with

$$\underline{\Gamma}_{ij} = (\Gamma_{ijk})_{0 \le k \le \kappa_{ij}} \qquad \text{for } (i,j) \ne (\infty,1), \qquad \underline{\Gamma}_{\infty 1} = (\Gamma_{\infty 1k})_{-m \le k \le \kappa_{\infty 1} - m}.$$

2.7 The Algebraic Set V

The first series of equations defining the algebraic set V is

$$A_i = \alpha_i \qquad (i = 1, \dots, \mu). \tag{2.18}$$

To write down the rest of the equations defining V we introduce the polynomials F(X, Y), D(X), G(T, Y) and H(T, Y) with coefficients in $\mathbb{Z}[\underline{\Theta}]$, which correspond to the polynomials d(X), g(T, Y) and h(T, Y) from Section 2.4. More specifically, we put

$$F(X,Y) = Y^{n} + \sum_{j=0}^{n-1} \sum_{i=0}^{m} \Theta_{ij} X^{i} Y^{j} \in \mathbb{Z}[\underline{\Theta}][X,Y],$$

we define D(X) as the Y-discriminant of F(X, Y) and we put

$$G(T,Y) = T^m F(T^{-1},Y), \qquad H(T,Y) = T^{m(n+1)} F(T^{-1},T^{-m}Y).$$

The second series of equations comes out from the equality

$$D(X) = \Delta \prod_{i=1}^{\mu} (X - A_i)^{\sigma_i} \prod_{i=1}^{\nu} (X - B_i)^{\tau_i}, \qquad (2.19)$$

where the quantities σ_i and τ_i are defined in (2.5). In order to define the third set of equation we introduce the polynomials

$$\widetilde{Y}_{ij} = \sum_{k=0}^{\kappa_{ij}} \Gamma_{ijk} \left(X - \mathbf{B}_i \right)^k \qquad (1 \le i \le \nu, \quad 1 \le j \le \ell_i),$$
$$\widetilde{Y}_{\infty j} = \sum_{k=0}^{\kappa_{\infty j}} \Gamma_{\infty jk} T^k \qquad (2 \le j \le \ell_\infty)$$

and the Laurent polynomial

$$\widetilde{Y}_{\infty 1} = \sum_{k=-m}^{\kappa_{\infty 1}-m} \Gamma_{\infty 1k} T^k.$$

The equations come out from the relations

$$\operatorname{ord}_{X=B_i} F(X, Y_{i,j}) > 2\kappa_{ij}, \qquad (1 \le i \le \nu, \quad 1 \le j \le \ell_i), \qquad (2.20)$$
$$\operatorname{ord}_{X=B_i} F'_Y(X, \widetilde{Y}_{i,j}) \ge \kappa_{ij}$$

$$\operatorname{ord}_{T=0} G(T, Y_{\infty,j}) > 2\kappa_{\infty j}, \qquad (2 \le j \le \ell_{\infty}), \qquad (2.21)$$
$$\operatorname{ord}_{T=0} G'_{Y}(T, \widetilde{Y}_{\infty,j}) \ge \kappa_{\infty j}$$

$$\operatorname{ord}_{T=0} H(T, T^m \widetilde{Y}_{\infty,1}) > 2\kappa_{\infty 1}, \qquad \operatorname{ord}_{T=0} H'_Y(T, T^m \widetilde{Y}_{\infty,1}) \ge \kappa_{\infty j}.$$
(2.22)

The final two equations are

$$\Gamma_{\infty 1,-m} = 1, \qquad \Gamma_{\infty 10} = 0.$$
 (2.23)

The following statement is immediate in view of the definitions and properties from Sections 2.4 and 2.5.

Proposition 2.7.1 Vector φ belongs to the set V.

2.8 The Algebraic Set W

We write

$$W = W_1 \cup W_2 \cup W_3 \cup W_4 \cup W_5 \cup W_6,$$

where the sets W_1, \ldots, W_6 are defined below.

The set W_1 is defined by $\Delta = 0$. Next, put

$$W_2 = \bigcup_{\substack{1 \le i \le \mu \\ 1 \le j \le \nu}} W_2^{(ij)}, \qquad W_3 = \bigcup_{1 \le i < j \le \nu} W_3^{(ij)},$$

where $W_2^{(ij)}$ is defined by $A_i = B_j$ and $W_3^{(ij)}$ is defined by $B_i = B_j$.

Further, we put

$$W_4 = \bigcup_{\substack{i \in \{1, \dots, \nu, \infty\}\\ 1 \le j \le \ell_i}} W_4^{(ij)},$$

where the set $W_4^{(ij)}$ is defined by the relations

$$\operatorname{ord}_{X=B_i} F'_Y(X, Y_{ij}) > \kappa_{ij}, \qquad \text{when } i \neq \infty,$$

$$(2.24)$$

 $\operatorname{ord}_{T=0}G'_Y(T, \widetilde{Y}_{\infty j}) > \kappa_{\infty j}, \quad \text{when } i = \infty \text{ and } j \neq 1, \quad (2.25)$

$$\operatorname{ord}_{T=0} H'_Y(T, T^m \widetilde{Y}_{\infty 1}) > \kappa_{\infty j}, \qquad \text{when } (i, j) = (\infty, 1).$$
(2.26)

Further, we put

$$W_5 = \left(\bigcup_{\substack{1 \le i \le \nu \\ 1 \le j_1 < j_2 \le \ell_i}} W_5^{(ij_1j_2)}\right) \cup \left(\bigcup_{2 \le j_1 < j_2 \le \ell_\infty} W_5^{(\infty j_1j_2)}\right),$$

where $W_5^{(ij_1j_2)}$ is defined by the equation $\Gamma_{ij_1\lambda(ij_1j_2)} = \Gamma_{ij_2\lambda(ij_1j_2)}$ and $W_5^{(\infty j_1j_2)}$ by the equation $\Gamma_{\infty j_1\lambda(\infty j_1j_2)} = \Gamma_{\infty j_2\lambda(\infty j_1j_2)}$, the numbers $\lambda(i, j_1, j_2)$ being defined at the end of Sections 2.4 and 2.5.

Finally, Lemma 1.5.2 implies that there is a proper Zariski-closed subset W_6 of V such that $\varphi \notin W_6$ and for any $\widehat{\varphi} = \left(\underline{\widehat{\theta}}, \underline{\widehat{\alpha}}, \underline{\widehat{\beta}}, \underline{\widehat{\gamma}}, \widehat{\delta}\right) \in V \setminus W_6$ the polynomial

$$Y^{n} + \sum_{j=0}^{n-1} \sum_{i=0}^{m} \widehat{\theta}_{ij} X^{i} Y^{j}$$
(2.27)

is irreducible and has the following property. Let \hat{x} and \hat{y} be the coordinate functions on the curve $\hat{\mathcal{C}}$ defined by (2.27). Then the effective divisor $(\hat{y})_{\infty}$ satisfies dim $\mathcal{L}((\hat{y})_{\infty}) = 2$.

The following statement is again immediate.

Proposition 2.8.1 The vector φ does not belong to the set W.

2.9 Finiteness of $V \setminus W$

Here we prove that the set $V \setminus W$ is finite. Let $\widehat{\varphi} = \left(\underline{\widehat{\theta}}, \underline{\widehat{\alpha}}, \underline{\widehat{\beta}}, \underline{\widehat{\gamma}}, \widehat{\delta}\right)$ be a point in $V \setminus W$. Then $\underline{\widehat{\alpha}} = \underline{\alpha}$ because of (2.18).

Put

$$\widehat{F}(X,Y) = Y^n + \sum_{j=0}^{n-1} \sum_{i=0}^m \widehat{\theta}_{ij} X^i Y^j.$$

It is a $\overline{\mathbb{Q}}$ -irreducible polynomial (because $\widehat{\varphi} \notin W_6$) and defines an algebraic curve $\widehat{\mathcal{C}}$ together with rational functions $\widehat{x}, \widehat{y} \in \overline{\mathbb{Q}}(\widehat{\mathcal{C}})$ satisfying $\widehat{F}(\widehat{x}, \widehat{y}) = 0$. Notice that this implies that \widehat{y} is integral over $\overline{\mathbb{Q}}[\widehat{x}]$.

Let $\widehat{d}(X)$ be the Y-discriminant of $\widehat{F}(X,Y)$. Then

$$\widehat{d}(X) = \widehat{\delta} \prod_{i=1}^{\mu} (X - \alpha_i)^{\sigma_i} \prod_{i=1}^{\nu} \left(X - \widehat{\beta}_i \right)^{\tau_i}$$

because $\widehat{\varphi}$ satisfies (2.19). Since $\widehat{\varphi} \notin W_2 \cup W_3$, the numbers $\widehat{\beta}_i$ are pairwise distinct and also are distinct from every α_i .

The covering $\widehat{\mathcal{C}} \xrightarrow{\widehat{x}} \mathbb{P}^1$ can be ramified only over the roots of $\widehat{d}(X)$, and, perhaps, over infinity. We want to show that \widehat{x} is unramified over the numbers $\widehat{\beta}_i$ and over infinity.

Fix a root β_i and define

$$\widetilde{\widehat{y}}_{ij}(X) = \sum_{k=0}^{\kappa_{ij}} \widehat{\gamma}_{ijk} (X - \widehat{\beta}_i)^k \qquad (j = 1, \dots, \ell_i).$$
(2.28)

Then

$$\operatorname{ord}_{\widehat{\beta}_i}\widehat{F}(X,\widetilde{\widehat{y}}_{ij}) > 2\kappa_{ij}, \quad \operatorname{ord}_{\widehat{\beta}_i}\widehat{F}'_Y(X,\widetilde{\widehat{y}}_{ij}) = \kappa_{ij},$$

because $\widehat{\varphi}$ satisfies (2.20) and does not satisfy (2.24). Also, none of $\widetilde{\widehat{y}}_{ij}$ is an initial segment of another, because $\widehat{\varphi} \notin W_5$.

Using Lemma 1.2.1, we find ℓ_i pairwise distinct Puiseux expansions

$$\widehat{y}_{i1},\ldots,\widehat{y}_{i\ell_i}\in\mathbb{Q}[[X-\beta_i]]$$

of \widehat{x} at $\widehat{\beta}_i$. satisfying $\operatorname{ord}_{\widehat{\beta}_i} \widehat{F}'_Y(X, \widehat{y}_{ij}) = \kappa_{ij}$. Since

$$\sum_{j=1}^{\ell_i} \operatorname{ord}_{\widehat{\beta}_i} \widehat{F}'_Y(X, \widehat{y}_{ij}) = \sum_{j=1}^{\ell_i} \kappa_{ij} = \tau_i = \operatorname{ord}_{\widehat{\beta}_i} \widehat{d}(X),$$

by (2.8), Lemma 1.2.3 implies that all *n* Puiseux expansions of \hat{x} at $\hat{\beta}_i$ are in $\overline{\mathbb{Q}}[[X - \hat{\beta}_i]]$, which means that \hat{x} is unramified over $\hat{\beta}_i$.

In a similar way we prove that \hat{x} is unramified over infinity (here $\ell_{\infty} = n$ and we do not need Lemma 1.2.3). Moreover, \hat{y} has at infinity n - 1 Puiseux expansions without negative powers and one expansion starting from the term of degree -m. Since \hat{y} is integral over $\overline{\mathbb{Q}}[\hat{x}]$, we have $(\hat{y})_{\infty} = m\hat{P}$, where \hat{P} is a pole of \hat{x} . Since $\hat{\varphi} \notin W_6$, we have dim $\mathcal{L}(m\hat{P}) = 2$.

Thus, each $\widehat{\varphi} \in V \setminus W$ gives rise to a pair $(\widehat{\mathcal{C}}, \widehat{x})$, where $\widehat{\mathcal{C}}$ is an algebraic curve and \widehat{x} an rational function on $\widehat{\mathcal{C}}$ of degree n, unramified outside the points α_i . By Lemma 1.5.3, there is only finitely many possibilities for $(\widehat{\mathcal{C}}, \widehat{x})$. Fix one. Since dim $\mathcal{L}(m\widehat{P}) = 2$, the function \widehat{y} is uniquely defined by the equations (2.23). It follows that the polynomial \widehat{F} is uniquely defined as well. Hence so is $\widehat{\delta}$, and the vector $\widehat{\beta}$ is uniquely defined up to ordering its components. Having this order fixed, we find that $\widehat{\gamma}$ is uniquely defined.

This proves that the set $V \setminus W$ is finite.

2.10 Degrees and Heights of the Equations Defining V

In this section we estimate the degrees and the heights of the equations defining the algebraic set V.

Since $\kappa_{ij} \leq \deg d(X) \leq 2m(n-1)$, equations defined by (2.20) are of degree at most

$$n(2m(n-1)+1) + 1 \le 2mn^2.$$

Here the "1" inside the parentheses is the degree of \widetilde{Y}_{ij} in $\underline{\Gamma}$, and the "1" outside the parentheses is the degree of F (and of F'_Y) in $\underline{\Theta}$.

A straightforward verification shows that the degrees of the other equations are bounded by $2mn^2$ as well.

Now let us estimate the heights of the equations. The heights of the μ equations (2.18) are obviously bounded by $h = \max\{h_a(\alpha_1), \ldots, h_a(\alpha_{\mu})\}$.

Estimating the heights of the remaining equations can be done with Lemma 1.1.1. All of the polynomials occurring below have rational integer coefficients. We call the size of a polynomial p with coefficients in \mathbb{Z} (denoted by ||p||) the sup-norm of the vector of its coefficients. For a non-zero polynomial p we have $h_a(p) \leq \log ||p||$, with equality if the coefficients are co-prime. In particular, $h_a(p) = 0$ if p is of size 1, which is the case for many polynomials below.

The left-hand side of (2.19) is a determinant of order 2n - 1 whose entries are polynomials in n(m + 1) + 1 variables X and Θ , each entry being of degree at most m + 1 and of size at most n. Hence its height can be estimated using Lemma 1.1.6:

$$h_{a}(D) \leq (2n-1) \Big(\log n + \log(2n-1) + (m+1) \log(n(m+1)+2) \Big) \\ \leq 10(mn)^{2}.$$

The right-hand side of (2.19) is a product of at most 2m(n-1) polynomials of degree 1 and size 1 in $\mu + \nu + 1$ variables <u>A</u>, <u>B</u> and X. Lemma 1.1.1 (1) allows us to estimate the height of the right-hand side by the quantity $2m(n-1)\log(\nu + \mu + 1) \leq 5(mn)^2$. We thereby bound the heights of the equations coming from (2.19) by $10(mn)^2$.

Equations (2.23) are, obviously, of height 0. The height of equations coming from (2.20), (2.21) and (2.22) can be estimated using Lemma 1.1.1 (3). For $i \neq \infty$ the polynomial \widetilde{Y}_{ij} is in $\kappa_{ij} + 2 \leq 2mn$ variables $X, B_j, \underline{\Gamma}_{ij}$. It is of degree $\kappa_{ij} + 1 \leq 2mn - 1$ and of size bounded by $2^{\kappa_{ij}} \leq 4^{mn}$. Lemma 1.1.1 (3) together with Remark 1.1.2 bound the height of the polynomials $F(X, \tilde{Y}_{i,j})$ and $F'_Y(X, \tilde{Y}_{i,j})$ are bounded by the quantities

$$(mn \log 4 + \log 2 + 2mn \log(2mn + 1))(m + n)$$

and

 $\log n + (mn\log 4 + \log 2 + 2mn\log(2mn+1))(m+n-1),$

respectively. Both do not exceed $6(mn)^3$, which bounds the heights of equations coming from (2.20). Similarly, one bounds by $12(mn)^3$ the heights of equations coming from (2.21) and (2.22).

We conclude: the algebraic set V is defined by equations of degree bounded by $2mn^2$ and height bounded by $h + 12(mn)^3$.

2.11 The Height of φ and the Field $\mathbb{K}(\varphi)$

Now we may apply Proposition 1.1.10, or, more precisely, Corollary 1.1.11 to bound the height of the vector φ , and the number field generated by its coordinates. Recall that φ belongs to $\overline{\mathbb{Q}}^{\Omega}$, where the dimension Ω satisfies

$$\Omega \le 10mn + 2n - 7,$$

see (2.17). If we define ∇ and Σ as in Proposition 1.1.10, we would have

$$h_{a}(f) \le h_{a}(\varphi) \le \nabla \Sigma (h + 12(mn)^{3}) + 2\nabla \Omega \log(\Omega + 1).$$

Furthermore, the field $\mathbb{L} = \mathbb{K}(\varphi)$ satisfies $[\mathbb{L} : \mathbb{K}] \leq \nabla$ and

$$\partial_{\mathbb{L}/\mathbb{K}} \le 2\nabla\Sigma (h + 12(mn)^3) + 5\nabla\Omega \log(\Omega + 1).$$

Since the degrees of the equations defining V are bounded by $2mn^2$, we have

$$\nabla \le (2mn^2)^{\Omega} \le (2mn^2)^{10mn+2n-7}.$$

Obviously, $\Sigma \leq \Omega \leq 12mn$. After trivial calculations we obtain

$$h_{a}(f) \leq \Lambda'(h+1), \qquad [\mathbb{L}:\mathbb{K}] \leq \Lambda', \qquad \partial_{\mathbb{L}/\mathbb{K}} \leq \Lambda'(h+1)$$
 (2.29)

with $\Lambda' = (2mn^2)^{10mn+2n-3}$. Since $m = \mathbf{g} + 1$, this proves Theorem 2.1.2 in the case when there is no ramified points and no Weierstrass points among the poles of x.

2.12 The General Case

We no longer assume that the set of poles of x has no Weierstrass and no ramified points (called *bad* points in the sequel). Since there exists at most $\mathbf{g}^3 - \mathbf{g}$ Weierstrass points and at most $2\mathbf{g}$ ramified points, there exists $\rho \in \mathbb{Z}$, satisfying

$$|\rho| \le \mathbf{g}^3 + \mathbf{g} \le m^3$$

(recall that $m = \mathbf{g} + 1$) such that the fiber of x above ρ contains no bad points. It follows that the function $\check{x} = (x - \rho)^{-1}$ has no bad points among its poles, and the previous argument applies to it. We find a number field \mathbb{L} , a function $y \in \mathbb{L}(\mathcal{C})$ such that $\mathbb{L}(\mathcal{C}) = \mathbb{L}(\check{x}, y)$ and a polynomial $\check{f}(X, Y) \in \mathbb{L}[X, Y]$ such that $\check{f}(\check{x}, y) = 0$,

$$\deg_X \check{f} = m = \mathbf{g} + 1, \qquad \deg_Y \check{f} = n,$$

and (2.29) holds with f replaced by \check{f} and h replaced by

$$\check{h} := \max \Big\{ \mathrm{h}_{\mathrm{a}} \big((\alpha_1 - \rho)^{-1} \big), \ldots, \mathrm{h}_{\mathrm{a}} \big((\alpha_\mu - \rho)^{-1} \big) \Big\}.$$

Obviously

$$\check{h} \le h + \log\left(2\max\{1, |\rho|\}\right) \le h + 3\log(2m),$$

which proves (2.2) after a short calculation. Further, the polynomial

$$f(X,Y) := (X-\rho)^m \check{f}\big((X-\rho)^{-1},Y\big)$$

satisfies f(x, y) = 0 and

$$h_{a}(f) \le h_{a}(\check{f}) + 3m\log(2m)$$

by Lemma 1.1.9. Again a trivial calculation implies (2.1). Theorem 2.1.2 is completely proved. $\hfill \Box$

Chapter 3

Effectivity in the Chevalley-Weil Theorem

3.1 Introduction

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

Remark 3.1.1 Notice that equations f(X, Y) = 0 and $\tilde{f}(X, \tilde{Y}) = 0$ define affine plane models of our curves C and \tilde{C} ; we do not assume these models non-singular.

We recall that $h_p(\cdot)$ and $h_a(\cdot)$ denote the projective and the affine absolute logarithmic heights, respectively, see the Notations and Conventions Chapter for the definitions. We also recall the normalized logarithmic discriminant $\partial_{\mathbb{L}/\mathbb{K}}$ and the height h(S) of a finite set of places S:

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

see the Notation and Conventions Chapter for the details.

Put

$$\Omega = 160mn^{3} \log n (h_{p}(f) + 2m + 2n),$$

$$\widetilde{\Omega} = 160\widetilde{m}\widetilde{n}^{3} \log \widetilde{n} (h_{p}(\tilde{f}) + 2\widetilde{m} + 2\widetilde{n}),$$

$$\Upsilon = 2\widetilde{n} (\widetilde{m}h_{p}(f) + mh_{p}(\tilde{f})).$$
(3.1)

Theorem 3.1.2 ("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 $P \in \mathcal{C}(\overline{\mathbb{K}})$ and $\widetilde{P} \in \widetilde{\mathcal{C}}(\overline{\mathbb{K}})$ such that $\phi(\widetilde{P}) = P$ we have

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

Remark 3.1.3 Draziotis and Poulakis [10, Theorem 1.1], assume that C is a non-singular plane curve (which is quite restrictive) and that $P \in C(\mathbb{K})$. 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

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

where $N = \deg f$, $\widetilde{N} = \deg \widetilde{f}$, 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 $v \in M_{\mathbb{K}} \setminus S$ and any extension \bar{v} of v to $\bar{\mathbb{K}}$ we have $|x(P)|_{\bar{v}} \leq 1$.

Theorem 3.1.4 ("affine" Chevalley-Weil theorem) In the above setup, 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

$$\partial_{\mathbb{K}(\widetilde{P})/\mathbb{K}(P)} \le \Omega + \widetilde{\Omega} + \Upsilon + \mathbf{h}(S).$$
(3.2)

Again, Draziotis and Poulakis [9, 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 Chapter 2, we obtain versions of Theorems 3.1.2 and 3.1.4, which depend only on the degrees and the ramification points of our curves over \mathbb{P}^1 . For a finite set $A \subset \mathbb{P}^1(\overline{\mathbb{K}})$ we define $h_a(A)$ as the affine height of the vector whose coordinates are the finite elements of A.

Theorem 3.1.5 Let A be a finite subset of $\mathbb{P}^1(\overline{\mathbb{K}})$ such that the covering $\mathcal{C} \xrightarrow{x} \mathbb{P}^1$ is unramified outside A. Put

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

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

$$\partial_{\mathbb{K}(\widetilde{P})/\mathbb{K}(P)} \leq \Lambda(h_{\mathrm{a}}(A)+1).$$

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

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

3.2 Eisenstein Theorem for Power Series

Our main technical tool is the quantitative Eisenstein theorem, based on the work of Dwork, Robba, Schmidt and van der Poorten [11, 12, 20]. Let

$$y = \sum_{k=-k_0}^{\infty} a_k x^{k/e} \tag{3.3}$$

be an algebraic power series with coefficients in $\overline{\mathbb{Q}}$, where we assume $k_0 \geq 0$ and $a_{-k_0} \neq 0$ 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 $|a_k|_v \leq 1$ for all k. We need a quantitative form of this statement, in terms of an algebraic equation f(x, y) = 0 satisfied by y.

3.2.1 Eisenstein Theorem

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

$$d = [\mathbb{K} : \mathbb{Q}], \qquad m = \deg_X f, \qquad n = \deg_Y f. \tag{3.4}$$

Write

$$f(X,Y) = f_0(X)Y^n + f_1(X)Y^{n-1} + \dots$$
(3.5)

and put

$$u = \operatorname{ord}_0 f_0. \tag{3.6}$$

Then, if y 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 $[\mathbb{L} : \mathbb{K}] \le n$.

The following theorem is a combination of the ideas and results from [11, 12, 20].

Theorem 3.2.1 Let \mathbb{K} be a number field and $f(X, Y) \in \mathbb{K}(X, Y)$. We use notation (3.4–3.6). 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,

$$d^{-1} \sum_{v \in M_{\mathbb{K}}} d_v \log A_v \le (2n-1)\mathbf{h}_{\mathbf{p}}(f) + 6n^2 + 2n\log m,$$
(3.7)

$$d^{-1} \sum_{v \in M_{\mathbb{K}}} d_v \log B_v \le h_p(f) + \log(2n).$$
 (3.8)

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

$$h\left(\left\{v \in M^{0}_{\mathbb{K}} : \frac{d_{v} \log A_{v}}{\log \mathcal{N}v} \notin \mathbb{Z}\right\}\right) \leq (2n-1)h_{p}(f) + n(2\log m + 3\log n + 5).$$
(3.9)

Finally, let y be an algebraic power series, written as in (3.3), 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 $k \geq -k_0$ we have

$$|a_k|_w \le B_v A_v^{u+k/e},\tag{3.10}$$

where u is defined in (3.6).

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

$$\mu = \operatorname{ord}_0 R_f(X), \tag{3.11}$$

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

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

Clearly σ_v does not depend on the fixed prolongation. Schmidt [20, Lemma 5] proves that

$$d^{-1} \sum_{v \in M_{\mathbb{K}}} d_v \log(1/\sigma_v) \le (2n-1)h_{\mathbb{P}}(f) + 2n\log\left((m+1)(n+1)\sqrt{n}\right).$$
(3.12)

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

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

$$A_{v} = \begin{cases} 2^{n}/\sigma_{v}, & p(v) = \infty, \\ 1/\sigma_{v}, & n < p(v) < \infty, \\ \left(np(v)^{1/(p(v)-1)}\right)^{n}/\sigma_{v}, & p(v) \le n, \end{cases}$$
$$B_{v} = \begin{cases} 2n|f|_{v}, & p(v) = \infty, \\ |f|_{v}, & p(v) < \infty \end{cases}$$

Notice that $A_v = B_v = 1$ for all but finitely many v.

Inequality (3.10) is established in [2, Section 2.3]. Inequality (3.8) is immediate from the definition of B_v . Further,

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

where we used (4) and (6) for the last estimate. Combining this with (3.12), we obtain

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

which implies (3.7) after a routine calculation.

The definition of B_v implies that $\frac{d_v \log B_v}{\log N_v} \in \mathbb{Z}$. We are left with (3.9). Write the set on the left of (3.9) as $S_1 \cup S_2$, where S_1 consists of v with $p(v) \leq n$, and S_2 of those with p(v) > n. Obviously,

$$h(S_1) \le \sum_{p \le n} \log p \le 1.02n,$$
 (3.13)

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

$$h(S_2) \le h_p(R^*) + \log(1 + \deg R^*) \le (2n-1)h_p(f) + (2n-1)\log((m+1)(n+1)\sqrt{n}) + \log(2mn),$$

where we use the property $h_p(R^*) = h_p(R)$ and Lemma 1.1.7 for the last inequality. Together with (3.13), this implies (3.9) after an easy calculation.

Here is one consequence that we shall use.

Corollary 3.2.2 In the set-up of Theorem 3.2.1, 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 $h(T) \leq (4n-1)h_p(f) + 13n^2 + 4n\log m$.

Proof. For $v \in T$ we have either $\log \mathcal{N}v \leq d_v \log A_v$ or $\log \mathcal{N}v \leq d_v \log B_v$ or $\frac{d_v \log A_v}{\log \mathcal{N}v} \notin \mathbb{Z}$. Partitioning the set into three sets and using (3.7), (3.8) and (3.9), we obtain the result after an easy calculation.

3.2.2 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 3.2.3** In the set-up of Theorem 3.2.1, 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 (3.6) and (3.11). Then

$$\partial_{\mathbb{L}/\mathbb{K}} \le (4n\mu + 4nu\nu + 2\nu) \,\mathrm{h}_{\mathrm{p}}(f) + (\mu + u\nu) \left(12n^2 + 4n\log m\right) + 3\nu\log(2n).$$
(3.14)

Proof. As shown in [2, Lemma 2.4.2], the field \mathbb{L} is generated over K by $a_{-k_0}, \ldots, a_{\kappa}$, where $\kappa \leq e\mu/\nu$ (we recall that in [2] the quantity μ has a slightly different definition and is less than or equal to our μ). Using Theorem 3.2.1 we estimate the height of the vector $\underline{a} = (a_{-k_0}, \ldots, a_{\kappa})$ as follows:

$$\begin{aligned} \mathbf{h}_{\mathbf{a}}(\underline{a}) &\leq d^{-1} \sum_{v \in M_{\mathbb{K}}} d_{v} \log B_{v} + d^{-1} \left(u + \frac{\kappa}{e} \right) \sum_{v \in M_{\mathbb{K}}} d_{v} \log A_{v} \\ &\leq \mathbf{h}_{\mathbf{p}}(f) + \log(2n) + \left(\frac{\mu}{\nu} + u \right) \left((2n-1)\mathbf{h}_{\mathbf{p}}(f) + 6n^{2} + 2n\log m \right) \\ &\leq \left(2n \left(\frac{\mu}{\nu} + u \right) + 1 \right) \mathbf{h}_{\mathbf{p}}(f) + \left(\frac{\mu}{\nu} + u \right) \left(6n^{2} + 2n\log m \right) + \log(2n). \end{aligned}$$

Applying now Lemma 1.1.12, we obtain

$$\partial_{\mathbb{L}/\mathbb{K}} \leq (4n\mu + 4nu\nu + 2\nu) \operatorname{h}_{p}(f) + (\mu + u\nu) \left(12n^{2} + 4n\log m\right) + 2\nu \log(2n) + \log \nu,$$

which is even sharper than (3.14).

Let now $\{y_1, \ldots, y_n\}$ 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 3.2.3.

Corollary 3.2.4 In the previous set-up, the following inequality holds

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

3.2.3 The "Essential" Coefficients

In this subsection the letter q always denotes a prime number. Let us assume now that the series (3.3) 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 exists at least one k such that $q \nmid k$ and $a_k \neq 0$. We denote by $\kappa(q)$ the smallest kwith this property, and we call $a(q) = a_{\kappa(q)}$ the q-essential coefficient of the series (3.3). 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 (3.6) and (3.11).

Proposition 3.2.5 In the above set-up, the following inequality holds:

$$\sum_{q|e} h_{a}(a(q)) \le \log_{2} e\left(u + \frac{\mu}{\nu}\right) \left(2nh_{p}(f) + 6n^{2} + 2n\log m\right).$$
(3.15)

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

$$\sum_{q|e} \frac{1}{q-1} \le \sum_{q|e} 1 \le \log_2 e.$$
(3.16)

Now, Theorem 3.2.1 gives us the explicit bound

$$h_{a}(a(q)) \leq \left(u + \frac{\mu}{\nu(q-1)}\right) \left(2nh_{p}(f) + 6n^{2} + 2n\log m\right)$$

for the height of the q-essential coefficient $h_a(a_{\kappa(q)})$. Summing up over all primes q dividing e, and simplifying by (3.16) we obtain the result. \Box

Corollary 3.2.6 Define y_i as in the previous section and let $a_i(q)$ denote the q-essential coefficient of the series y_i . Then

$$\sum_{i=1}^{n} \sum_{q|e} h_{a}(a_{i}(q)) \leq (u+\mu) \left(2n^{2}h_{p}(f) + 6n^{3} + 2n^{2}\log m\right) \log_{2} n$$

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

3.3 Proximity and Ramification

This section is the technical heart of the chapter. 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 K-irreducible polynomial such that our functions x and y satisfy f(x, y) = 0 (the polynomial f is well-defined up to a constant factor). Since C is absolutely irreducible, so is the polynomial f(X, Y).

Remark 3.3.1 One can say that the plane curve define by the equation f(X, Y) = 0 is a two-dimensional affine model of C. We do not assume this model to be smooth.

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

$$f(X,Y) = f_0(X)Y^n + f_1(X)Y^{n-1} + \dots + f_n(X).$$
(3.17)

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 $e = e_Q$ the ramification index of x at Q (that is, $e = \operatorname{ord}_Q(x - \alpha)$). Fix a primitive e-th root of unity $\zeta = \zeta_e$. Then there exist e equivalent Puiseux expansions of y at Q:

$$y_i^{(Q)} = \sum_{k=-k^{(Q)}}^{\infty} a_k^{(Q)} \zeta^{ik} (x-\alpha)^{k/e} \qquad (i=0,\dots,e-1),$$
(3.18)

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

Let \bar{v} be a valuation of $\bar{\mathbb{K}}$. We say that the series (3.18) 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

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

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

- $|\xi \alpha|_{\bar{v}} < 1;$
- the e series (3.18) ν̄-adically converge at ξ, and one of the sums y_i^(Q)(ξ) 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 $\overline{\mathbb{K}}$ -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 Galoisinvariant 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

the polynomial $f_0(X)$, defined in (3.17), is monic. (3.19)

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

$$\mathbf{h}_{\mathbf{a}}(f) = \mathbf{h}_{\mathbf{p}}(f). \tag{3.20}$$

Now, we define

$$T_1 = \left\{ v \in M^0_{\mathbb{K}} : \text{the prime below } v \text{ is } \leq n \right\},\$$

$$T_2 = \left\{ v \in M^0_{\mathbb{K}} : |f|_v > 1 \right\}.$$

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

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

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 1.4. Since the polynomial $\widehat{R}(X)$ is separable, we have $\Delta \in \mathbb{K}^*$. Now we define the set T_4 as follows:

$$T_4 = \{ v \in M^0_{\mathbb{K}} : |\Delta|_v < 1 \}.$$

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 (3.18), we denote by $a_k^{(Q)}$ the coefficients of these expansions. Now define

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

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, $[\mathbb{K}^{(Q)} : \mathbb{K}(\alpha)] \leq n$. Now we define

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

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 3.2.3. Now put

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

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

$$\ell(P, Q, \bar{v}) = \frac{\log |\xi - \alpha|_{\bar{v}}}{\log |\pi|_{v}},$$
(3.21)

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 3.3.3 Let \mathcal{Q} be the sets defined above. Then for any point $P \in \mathcal{C}(\overline{\mathbb{K}}) \setminus \mathcal{Q}$ 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 3.3.4 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 (3.21).

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

Proposition 3.3.5 Put $T = T_1 \cup T_2 \cup \ldots \cup T_7$. Then $h(T) \le 150mn^3 \log n (h_p(f) + 2m + 2n).$

3.3.1 Proof of Proposition 3.3.3

We fix, once and for all, a finite valuation $v \in M_{\mathbb{K}}$, its extension $\bar{v} \in M_{\overline{\mathbb{K}}}$, and a point $P \in \mathcal{C}(\overline{\mathbb{K}})$ semi-defined over \mathbb{K} and such that $\xi = x(P) \notin \mathcal{A}$. We shall assume that $|\xi|_v \leq 1$, 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 1.4.2 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) = 0is non-singular, which implies that $\mathbb{K}(P) = \mathbb{K}(\xi, \eta) = \mathbb{K}(\eta)$ (recall that $\xi \in \mathbb{K}$). Now Lemma 1.4.1 implies that $|R(\xi)|_v < 1$, which implies that $|\widehat{R}(\xi)|_v < 1$ by Lemma 1.4.2.

Next, since $v \notin T_4$, we have $|\widehat{R}'(\xi)|_v = 1$. Lemma 1.4.3 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 (α, \bar{v}) is well-defined up to the Galois action of $\operatorname{Gal}(\overline{\mathbb{K}}/\mathbb{K})$. 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 $R(\xi) \neq 0$, we have $f_0(\xi) \neq 0$ 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 $R(\xi) \neq 0$). 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 $Q \in Q$. 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 $\ell(P, Q, \bar{v})$.

3.3.2 Proof of Proposition 3.3.4

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,

$$\eta = \sum_{k=-k^{(Q)}}^{\infty} a_k \left(\sqrt[e]{\xi - \alpha}\right)^k.$$
(3.22)

Now 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 (3.21). 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 $\mathbb{K}_{\bar{v}}$ 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 (3.22), 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 3.2.3. 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 $\theta \in \mathbb{K}_v\left(\eta, \sqrt[e]{\xi-\alpha}\right)$. 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 $|a_k|_v \leq 1$

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 $\operatorname{ord}_{\pi}\Pi$ divides e'/q. On the other hand, $\operatorname{ord}_{\Pi}\theta = (\kappa \ell/e) \cdot \operatorname{ord}_{\pi}\Pi \in \mathbb{Z}$, 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. \Box

3.3.3 Proof of Proposition 3.3.5

The proposition is a direct consequence of the estimates

$$h(T_1) \le 1.02n,$$
 (3.23)

$$h(T_2) \le h_p(f), \tag{3.24}$$

$$h(T_3) \le (2n-1)(h_p(f) + m\log 2 + \log(2n^2)),$$
 (3.25)

- $h(T_4) \le 16mn^2 (h_p(f) + 2m + 2\log n),$ (3.26)
- $h(T_5) \le 16mn^2 (h_p(f) + 2m + 2n),$ (3.27)
- $h(T_6) \le 40mn^3 (h_p(f) + 2m + 2n),$ (3.28)

$$h(T_7) \le 18mn^3 \log n (h_p(f) + 2m + 2n).$$
 (3.29)

Remark 3.3.6 Estimates (3.28) and (3.29) can probably be refined, to have the main term of the form $O(mn^2h_p(f))$, which would result in the similar main term in Proposition 3.3.5.

Proof of (3.23) Obviously, $h(T_1) \leq \sum_{p \leq n} \log p$, which is bounded by 1.02*n* according to (5).

Proof of (3.24) Item 2 of Proposition 1.1.13 implies that $h(T_2) \leq h_a(f)$. Since $h_a(f) = h_p(f)$ by (3.20), the result follows.

Proof of (3.25) Item 2 of Proposition 1.1.13 and Lemma 1.1.7 imply that

$$h(T_3) \le h_a(r_0) \le h_a(R) \le (2n-1)h_a(f) + (2n-1)(\log(2n^2) + m\log 2).$$

(3.30)

Again using (3.20) we have the result

Again using (3.20), we have the result.

Proof of (3.26) We have $\deg \widehat{R} \leq \deg R \leq (2n-1)m$. Further, using Corollary 1.1.4 and inequalities (3.30), we find

$$h_{a}(\widehat{R}) \le h_{p}(R) + h_{a}(r_{0}) + \deg R \le (4n-2)h_{a}(f) + (8n-4)(\log n+m).$$

Finally, using Remark 1.1.8 and the previous estimates, we obtain

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

Using (3.20), we obtain the result.

Preparation for the proofs of (3.27–3.29) 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

$$|\mathcal{A}| \le \sum_{\alpha \in \mathcal{A}} \mu_{\alpha} \le \deg R(X) \le m(2n-1), \tag{3.31}$$

$$\sum_{\alpha \in \mathcal{A}} \mathbf{h}_{\mathbf{a}}(\alpha) \leq \sum_{\alpha \in \mathcal{A}} \mu_{\alpha} \mathbf{h}_{\mathbf{a}}(\alpha) \leq \mathbf{h}_{\mathbf{p}}(R) + \log(2mn) \leq (2n-1)\mathbf{h}_{\mathbf{p}}(f) + 3n\log(4mn),$$
(3.32)

where for (3.32) we use Remark 1.1.3 and Lemma 1.1.7. Denoting by u_{α} order of α as the root of $f_0(X)$, we have, obviously,

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

$$\sum_{\alpha \in \mathcal{A}} u_{\alpha} \mathbf{h}_{\mathbf{a}}(\alpha) \leq \mathbf{h}_{\mathbf{p}}(f_0) + \log(m+1) \leq \mathbf{h}_{\mathbf{p}}(f) + \log(m+1).$$

Using the notation

$$f^{(\alpha)}(X,Y) = f(X+\alpha,Y) \tag{3.33}$$

and Corollary 1.1.5, we obtain the following inequalities:

$$\sum_{\alpha \in \mathcal{A}} h_{a}(f^{(\alpha)}) \leq \sum_{\alpha \in \mathcal{A}} \mu_{\alpha} h_{a}(f^{(\alpha)}) \leq 4mnh_{p}(f) + 7m^{2}n + 3nm\log n, \quad (3.34)$$

$$\sum_{\alpha \in \mathcal{A}} u_{\alpha} \mathbf{h}_{\mathbf{a}}(f^{(\alpha)}) \le 2m \mathbf{h}_{\mathbf{p}}(f) + 3m^2.$$
(3.35)

Proof of (3.27) 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 3.2.1 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 3.2.2 implies that

$$h(T_5^{(\alpha)}) \le (4n-1)h_p(f^{(\alpha)}) + 13n^2 + 4n\log m.$$
 (3.36)

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 1.1.13 implies that

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

Using (3.36), we obtain

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

Using (3.31) and (3.34), we obtain (3.27) after an easy calculation.

Proof of (3.28) 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}'_{α} 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 1.1.13 implies that

$$h(T_6) \le \sum_{\alpha \in \mathcal{A}'} h\Big(\operatorname{Ram}\big(\mathbb{K}(\alpha)/\mathbb{K}\big) \Big) + \sum_{\alpha \in \mathcal{A}'} \sum_{Q \in \mathcal{Q}'_{\alpha}} [\mathbb{K}(\alpha) : \mathbb{K}] h\Big(\operatorname{Ram}\big(\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)\big) \Big),$$
(3.37)

where $\operatorname{Ram}(\cdot)$ is defined in Lemma 1.1.15. Lemma 1.1.16 implies that

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

The latter sum can be easily estimated by Corollary 1.1.14 and Lemma 1.1.7:

$$\sum_{\alpha \in \mathcal{A}} \partial_{\mathbb{K}(\alpha)/\mathbb{K}} \le 4mn h_{p}(R) + 6mn \log(2mn) \le 8mn^{2} h_{p}(f) + 18mn^{2} \log(3mn).$$
(3.38)

To estimate the second sum in (3.37), we again use Lemma 1.1.16:

$$\sum_{\alpha \in \mathcal{A}'} \sum_{Q \in \mathcal{Q}'_{\alpha}} [\mathbb{K}(\alpha) : \mathbb{K}] h\Big(\operatorname{Ram}\big(\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)\big) \Big) \leq \\ \leq \sum_{\alpha \in \mathcal{A}'} [\mathbb{K}(\alpha) : \mathbb{K}] \sum_{Q \in \mathcal{Q}'_{\alpha}} \big[\mathbb{K}^{(Q)} : \mathbb{K}(\alpha) \big] \partial_{\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)} = \sum_{\alpha \in \mathcal{A}} \sum_{x(Q) = \alpha} \partial_{\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)}$$

Corollary 3.2.4 implies that

$$\sum_{x(Q)=\alpha} \partial_{\mathbb{K}^{(Q)}/\mathbb{K}(\alpha)} \leq \left(4n^{2}\mu_{\alpha} + 4u_{\alpha}n^{3} + 2n^{2}\right) h_{p}(f^{(\alpha)}) + \left(\mu_{\alpha}n + u_{\alpha}n^{2}\right) \left(12n^{2} + 4n\log m\right) + 3n^{2}\log(2n).$$

Summing up over $\alpha \in \mathcal{A}$ and using (3.31), (3.34) and (3.35), we obtain

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

which, together with (3.38), implies (3.28).

Proof of (3.29) 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}'_{α} from the previous proof, and using item 2 of Proposition 1.1.13, we obtain

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

Corollary 3.2.6 estimates the inner sum by

$$(u_{\alpha} + \mu_{\alpha}) \left(2n^{2} h_{p}(f^{(\alpha)}) + 6n^{3} + 2n^{2} \log m \right) \log_{2} n.$$

Applying inequalities (3.31), (3.34) and (3.35) once again, we obtain

$$h(T_7) \le 12mn^3 \log_2 n h_p(f) + 24mn^3(m+n) \log_2 n.$$

Since $\log_2 n \le 1.5 \log n$, the result follows. This completes the proof of Proposition 3.3.5.

3.4 A Tower of $\overline{\mathbb{K}}$ -Points

In this section we retain the set-up of Section 3.3; 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 $\mathbb{K}(\mathcal{C}) = \mathbb{K}(x, y)$. We 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 (3.17) is monic. We again define the polynomial R(X), the sets $\mathcal{A} \subset \overline{\mathbb{K}}$, $\mathcal{Q} \subset \mathcal{C}(\overline{\mathbb{K}})$ 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 $z \in \mathbb{K}(\widetilde{\mathcal{C}})$ such that $K(\widetilde{\mathcal{C}}) = \mathbb{K}(x, z)$. We let $\tilde{f}(X, Z) \in \mathbb{K}[X, Z]$ be an irreducible polynomial of X-degree \widetilde{m} and Z-degree \widetilde{n} such that $\tilde{f}(x, z) = 0$; we write

$$\tilde{f}(X,Z) = \tilde{f}_0(X)Z^{\tilde{n}} + \tilde{f}_1(X)Z^{\tilde{n}-1} + \dots + \tilde{f}_{\tilde{n}}(X)$$

and assume that the polynomial $\tilde{f}_0(X)$ is monic. We define in the the similar way the polynomial $\tilde{R}(X)$, the sets $\tilde{\mathcal{A}} \subset \bar{\mathbb{K}}$, $\tilde{\mathcal{Q}} \subset \tilde{\mathcal{C}}(\bar{\mathbb{K}})$ and $\tilde{T}_1, \ldots, \tilde{T}_7 \subset M_{\mathbb{K}}$, etc. We also define the notion of proximity on the curve $\tilde{\mathcal{C}}$ exactly in the same way as we did it for \mathcal{C} in Definition 3.3.2, and we have the analogues of Propositions 3.3.3, 3.3.4 and 3.3.5.

In addition to all this, we define one more finite set of places of \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 define put

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

Proposition 3.4.1 Let $P \in \mathcal{C}(\overline{\mathbb{K}})$ be semi-defined over \mathbb{K} (that is, we have $\xi = x(P) \in \mathbb{K}$), and let $\widetilde{P} \in \widetilde{\mathcal{C}}(\overline{\mathbb{K}})$ be a point above P (that is, $\phi(\widetilde{P}) = P$). Let v be a finite place of \mathbb{K} , and \overline{v} an extension of v to $\overline{\mathbb{K}}$. Assume that \widetilde{P} is \overline{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} -close to the $Q \in \mathcal{C}(\bar{\mathbb{K}})$ which lies below \tilde{Q} .

For the proof we shall need a simple lemma.

Lemma 3.4.2 In the above set-up, there is a polynomial $\Phi(X, Z) \in \mathbb{K}[X, Z]$ such that

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

Proof. Since $f_0(x)y$ is integral over $\mathbb{K}[x]$, Corollary 1.3.2 implies that $f_0(x)y \in \widetilde{R}(x)^{-1}\mathbb{K}[x,z]$, whence the result.

Proof of Proposition 3.4.1 We put $\alpha = x(\widetilde{Q})$. By the definition of the set \widetilde{Q} , we have $\alpha \in \widetilde{A}$. Assume that $|\xi|_v \leq 1$ and $v \notin T \cup \widetilde{T} \cup U$. Let \widetilde{e} be the ramification of \widetilde{Q} over \mathbb{P}^1 , and let

$$z_i^{(\widetilde{Q})} = \sum_{k=-k^{(\widetilde{Q})}}^{\infty} a_k^{(\widetilde{Q})} \tilde{\zeta}^{ik} (x-\alpha)^{k/\widetilde{e}} \qquad (i=0,\ldots,\widetilde{e}-1),$$
(3.39)

be the equivalent Puiseux expansions of z at \widetilde{Q} (here $\widetilde{\zeta}$ is a primitive \widetilde{e} -th root of unity). Since \widetilde{P} is \overline{v} -close to \widetilde{Q} , we have $|\xi - \alpha|_{\overline{v}} < 1$ and the \widetilde{e} series (3.39) converge at ξ , with one of the sums being $z(\widetilde{P})$.

Now $\Phi(X, Z)$ be the polynomial from Lemma 3.4.2. Then the \tilde{e} series

$$\frac{\Phi\left(x, z_i^{(Q)}\right)}{f_0(x)\widetilde{R}(x)} \qquad (i = 0, \dots, \widetilde{e} - 1) \tag{3.40}$$

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 (3.40) exactly \tilde{e}/e times.

Write $f_0(X)\widetilde{R}(X) = (X - \alpha)^r g(X)$ with $g(\alpha) \neq 0$. Since

 $v \notin T_2 \cup \widetilde{T}_2 \cup \widetilde{T}_3 \cup \widetilde{T}_4 \cup U,$

we have $|g(\alpha)|_{\bar{v}} = 1$. Now Lemma 1.4.4 implies that the Laurent series at α of the rational function $(f_0(x)\tilde{R}(x))^{-1}$ converges at ξ . Hence all the series (3.40) converge at ξ , and among the sums we find

$$\frac{\Phi\left(x(\widetilde{Q}), z(\widetilde{Q})\right)}{f_0\left(x(\widetilde{Q})\right)\widetilde{R}\left(x(\widetilde{Q})\right)} = y(Q).$$

Hence P is \bar{v} -close to Q.

We shall also need a bound for U similar to that of Proposition 3.3.5.

Proposition 3.4.3 We have $h(U) \leq \Upsilon + \Xi$, where Υ is defined in (3.1) and

$$\Xi = 2m\widetilde{n}(2\widetilde{m} + 3\log\widetilde{n}) + (m + 2\widetilde{m}\widetilde{n})\log(m + 2\widetilde{m}\widetilde{n}).$$
(3.41)

Proof. Item 2 of Proposition 1.1.13 implies that $h(U) \leq h_a(\Theta)$, where Θ is the resultant of $f_0(X)$ and $\widetilde{R}_2(X)$. Expressing Θ as the familiar determinant, we find

$$h_{a}(\Theta) \leq \deg \widetilde{R}_{2}h_{a}(f_{0}) + \deg f_{0}h_{a}(\widetilde{R}_{2}) + (\deg f_{0} + \deg \widetilde{R}_{2})\log(\deg f_{0} + \deg \widetilde{R}_{2}).$$
(3.42)

Since both f_0 and \widetilde{R}_2 are monic polynomials (by the convention (3.19) and the definition of \widetilde{R}_2), we may replace the affine heights by the projective heights. Further, we have the estimates

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

the latter estimate being a consequence of Corollary 1.1.4 and Lemma 1.1.7. Substituting all this to (3.42), we obtain the result.

3.5 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 3.4. Here is our principal result, which will easily imply all the theorems stated in the introduction.

Theorem 3.5.1 Assume that the covering ϕ is unramified outside the poles of x. Let $P \in \mathcal{C}(\overline{\mathbb{K}})$ be semi-defined over \mathbb{K} , and let $\widetilde{P} \in \widetilde{\mathcal{C}}(\overline{\mathbb{K}})$ be a point above P. As usual, 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 $|\xi|_v \leq 1$ and $v \notin T \cup \widetilde{T} \cup U$. Fix an extension \overline{v} of v to $\overline{\mathbb{K}}$, and let \widetilde{w} and w be the restrictions of \overline{v} to $\mathbb{K}(\widetilde{P})$ and $\mathbb{K}(P)$, and \widetilde{e} and e their ramification indexes over v, respectively.

Proposition 3.3.3 implies that \widetilde{P} is \overline{v} -adically close to some $\widetilde{Q} \in \widetilde{Q}$. Proposition 3.3.4 now implies that $\widetilde{e} = e_{\widetilde{Q}}/\gcd(e_{\widetilde{Q}}, \ell)$.

Let Q be the point of \mathcal{C} lying under Q. Put $\alpha = x(Q) = x(Q)$. The rest of the proof splits into two cases. 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 \widetilde{w} is not ramified over v, and, a fortiori, over w.

Now assume that $\alpha \in \mathcal{A}$. Proposition 3.4.1 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. We have then $e = e_Q / \operatorname{gcd}(e_Q, \ell) = \widetilde{e}$ by Proposition 3.3.4. This shows tha \widetilde{w} is unramified over w, completing the proof. \Box

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

Proposition 3.5.2 We have

$$h(T \cup \widetilde{T} \cup U) \le \Omega + \widetilde{\Omega} + \Upsilon.$$
(3.43)

where Ω , $\widetilde{\Omega}$ and Υ are defined in (3.1).

Proof. Combining Propositions 3.3.5 and 3.4.3, we obtain the estimate

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

where Ξ is defined in (3.41). A routine calculation show that $\Xi \leq (\Omega + \widetilde{\Omega})/4$, whence the result.

Now we can prove the theorems from the introduction.

Proof of Theorem 3.1.2 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} that ramify in $\mathbb{K}(\tilde{P})$. Theorem 3.5.1 and estimate (3.43) imply that

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

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

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

Thus,

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

and Lemma 1.1.15 implies that

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

The theorem is proved.

Proof of Theorem 3.1.4 Let S' be set of places of the field $\mathbb{K}(P)$ extending the places from S. The right-hand side of (3.2) will not increase (see item 1 of Proposition 1.1.13) 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 3.5.1 and (3.43), we obtain

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

We again complete the proof, applying Lemma 1.1.15.

To order to prove Theorem 3.1.5, we use the effective Riemann Existence Theorem, proved in Chapter 2, in the following form.

Theorem 3.5.3 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 $A \subset \mathbb{P}^1(\overline{\mathbb{K}})$. Put

$$h = h_{a}(A), \qquad \Lambda' = \left(2(\mathbf{g}+1)n^{2}\right)^{10\mathbf{g}n+12n},$$

where $\mathbf{g} = \mathbf{g}(\mathcal{C})$. Then there exists a rational function $y \in \overline{\mathbb{K}}(\mathcal{C})$ such that $\overline{\mathbb{K}}(\mathcal{C}) = \overline{\mathbb{K}}(x, y)$ and the rational functions $x, y \in \overline{\mathbb{K}}(\mathcal{C})$ satisfy the equation

f(x,y) = 0, where the absolutely irreducible polynomial $f(X,Y) \in \mathbb{L}[X,Y]$ is such that

$$\deg_X f = \mathbf{g} + 1, \qquad \deg_Y f = n, \qquad \mathbf{h}_{\mathbf{p}}(f) \le \Lambda'(h+1). \tag{3.44}$$

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

Proof of Theorem 3.1.5 We shall prove the "projective" case 1 of this theorem. The affine case is proved similarly.

We define Λ' in the same way as Λ' in Theorem 3.5.3, but with n and \mathbf{g} replaced by \tilde{n} and $\tilde{\mathbf{g}}$. We use Theorem 3.5.3 to find functions $y \in \bar{\mathbb{K}}(\mathcal{C})$ and $z \in \bar{\mathbb{K}}(\tilde{\mathcal{C}})$, and polynomials $f(X, Y) \in \bar{\mathbb{K}}[X, Y]$ and $\tilde{f}(X, Z) \in \bar{\mathbb{K}}[X, Z]$. Denoting by \mathbb{L} the field generated by the set A and the coefficients of both the polynomials, we find $\partial_{\mathbb{L}/\mathbb{K}(A)} \leq (\Lambda' + \tilde{\Lambda}')(h+1)$ with $h = h_a(A)$. Using Lemma 1.1.12, we estimate $\partial_{\mathbb{K}(A)/\mathbb{K}} \leq 2(\delta - 1)h + \log \delta$. Hence

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

We define the quantities Ω , $\tilde{\Omega}$ and Υ as in the introduction. Then, applying Theorem 3.1.2, but over field \mathbb{L} rather than \mathbb{K} , we find

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

Hence

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

The last sum is bounded by

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

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

Bibliography

- YU. BILU, Effective Analysis of Integral Points on Algebraic Curves, Ph. D. Thesis, Beer Sheva, 2003.
- [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] YU. BILU, M. STRAMBI, A. SURROCA, Quantitative Chevalley-Weil Theorem for Curves, in preparation.
- [5] J.-B. BOST, H. GILLET, C. SOULÉ, Heights of projective varieties and positive Green forms, J. Amer. Math. Soc. 7 (1994), 903–1027.
- [6] P. DÈBES, Méthodes topologiques et analytiques en théorie inverse de Galois: théorème d'existence de Riemann, in [8], pp. 27–41.
- [7] R. DEDEKIND, Werke I, Vieweg, 1930.
- [8] B. DESCHAMPS (ed.), Arithmétique des revétements algébriques: Proc. colloq. Saint-Étienne, March 24–26, 2000, Séminaires et Congrès 5, SMF, Paris, 2001.
- [9] K. DRAZIOTIS, D. POULAKIS, Explicit Chevalley-Weil Theorem for Affine Plane Curves, *Rocky Mountain J. of Math.* **39** (2009), 49–70.
- [10] K. DRAZIOTIS, D. POULAKIS, An Effective Version of Chevalley-Weil Theorem for Projective Plane Curves, arXiv:0904.3845.
- [11] B. DWORK AND P. ROBBA, On natural radii of p-adic convergence, Trans. Amer. Math. Soc., 256 (1979), 199–213.

- [12] B. M. DWORK AND A. J. VAN DER POORTEN, The Eisenstein constant, Duke Math. J., 65(1) (1992), 23–43.
- [13] B. EDIXHOVEN, R. DE JONG, J. SCHEPERS, Covers of surfaces with fixed branch locus, arXiv:0807.0184v1.
- [14] R. HARTSHORNE, Algebraic Geometry, Graduate Texts in Math. 52, Springer, New York, 1977.
- [15] M. HINDRY, J. H. SILVERMAN, Diophantine Geometry: an Introduction, Graduate Texts in Math. 201, Springer Verlag, 2000.
- [16] T. KRICK, L.M. PARDO, M. SOMBRA, Sharp estimates for the arithmetic Nullstellensatz, *Duke Math. J.* 109 (2001), 521–598.
- [17] S. LANG, Fundamentals of Diophantine Geometry, Springer, New York, 1983.
- [18] P. PHILIPPON, Sur des hauteurs alternatives, I, Math. Ann. 289 (1991), 255–283; II, Ann. Inst. Fourier 44 (1994), 1043–1065; III, J. Math. Pures Appl. 74 (1995), 345–365.
- [19] J. B. ROSSER, L. SCHOENFELD, Lowell Approximate formulas for some functions of prime numbers, *Illinois J. Math.* 6 (1962), 64–94.
- [20] W. M. SCHMIDT, Eisenstein's theorem on power series expansions of algebraic functions. Acta Arith., 56(2) (1990), 161–179.
- [21] W. M. SCHMIDT, Construction and estimates of bases in function fields. J. Number Theory, 39) (1991), 181–224.
- [22] J.-P. SERRE, Quelques applications du théorème de densité de Chebotarev, Publ. Math. IHES 54 (1981), 323–401.
- [23] J. H. SILVERMAN, Lower bounds for height functions. Duke Math. J., 51 (1984), 395–403.
- [24] É. I. ZVEROVICH, An algebraic method for constructing the basic functionals of a Riemann surface given in the form of a finite covering of a sphere (Russian), *Sibirsk. Mat. Zh.* 28 (1987), 32–43, 217. (translated in *Siberian Math. J.* 28 (1987), 889–898).