

# Effective Analysis of Integral Points on Algebraic Curves

*Thesis submitted in partial fulfillment  
of the requirements for the degree of  
DOCTOR OF PHILOSOPHY*

*by*  
Yuri Bilu

*Submitted to the Senate of Ben-Gurion University  
of the Negev*

November 1993

*BEER-SHEVA*

# Effective Analysis of Integral Points on Algebraic Curves

*Thesis submitted in partial fulfillment  
of the requirements for the degree of  
DOCTOR OF PHILOSOPHY*

*by*  
Yuri Bilu

*Submitted to the Senate of Ben-Gurion University  
of the Negev*

*Approved by the advisor \_\_\_\_\_*

*Approved by the Chairman  
of the Research Studies Committee \_\_\_\_\_*

May 1994

*BEER-SHEVA*

This work was carried out under the supervision of  
Professor Daniel Berend

at the Department of Mathematics and Computer Science  
Faculty of Natural Sciences

Effective Analysis  
of  
Integral Points  
on  
Algebraic Curves

*Thesis submitted in partial fulfillment  
of the requirements for the degree of  
DOCTOR OF PHILOSOPHY*

*by*  
Yuri Bilu

*Submitted to the Senate of Ben-Gurion University  
of the Negev*

May 1994

*BEER-SHEVA*

## Acknowledgements

It was Professor V.G. Sprindžuk who taught me Diophantine approximations and Diophantine equations. His remarkable lectures and books, and, especially, personal contact with such a brilliant mathematician stimulated my interest in Diophantine equations and enriched my knowledge on the subject. His premature passing was a great loss for his students and colleagues, as well as for all mathematical community.

My first steps in mathematics were made under the supervision of Professor V.I. Bernik. Though his interests belong to another area of number theory, I had a great pleasure to be in contact with him as a mathematician and a man.

However, this thesis was prepared at the Department of Mathematics and Computer Science of the Ben-Gurion University of the Negev. I am grateful to this department for financial support and very stimulating atmosphere, in which I spent three remarkable years. My special thanks are to my advisors in Israel, Professor Daniel Berend and Professor Miriam Cohen, for having been a great help throughout in matters both mathematical and nonmathematical. Their guidance far exceeded the limits of official advisorship.

Various topics concerning this thesis were discussed with Professors E. Bombieri, D. Bertrand, R. Livne and E. de Shalit. Professor H. P. Schlickewei and the referee of my article [Bi94] drew my attention to the paper [Schm91], which is extensively used in the thesis. I had a useful correspondence with Professor Y. Ihara. I would also like to thank Professors A. Baker, K. Györy, W. Schmidt and R. Tijdeman for their encouraging letters, and Professors G. Freiman, S. Gelbart, M. Lin and R. Sen for moral support during my first years in Israel.

Finally, I am greatly indebted to my family for their constant support and encouragement.

# Contents

<b>Introduction</b>	<b>4</b>
<b>Notations</b>	<b>9</b>
<b>1 Main theorem about integral points</b>	<b>12</b>
1 Introduction. . . . .	12
2 Puiseux expansions. . . . .	14
3 Comparison of heights. . . . .	21
4 Siegel's construction of convenient units of algebraic number fields. . . . .	25
5 Lower bounds for linear forms in logarithms. . . . .	30
6 Proof of Theorem 1A. . . . .	33
7 Proof of Theorem 1B. . . . .	36
<b>2 Bounds for isolated solutions of systems of algebraic equations</b>	<b>37</b>
1 Introduction . . . . .	37
2 A projection. . . . .	38
3 A construction of a small point in general position. . . . .	39
4 A bound for the number of components. . . . .	40
5 Proof of Theorem 2B. . . . .	41
<b>3 An effective version of Riemann existence theorem</b>	<b>43</b>
1 Introduction . . . . .	43
2 Some properties of algebraic power series. . . . .	44
3 Proof of Theorem 3A. . . . .	47
4 Proof of Theorem 3B. . . . .	54
<b>4 An effective Chevalley-Weil theorem for curves</b>	<b>55</b>
1 Introduction. . . . .	55
2 Upper bounds for local and global discriminants. . . . .	57
3 A neighbourhood of a fixed point. . . . .	58
4 Proof of Theorem 4A. . . . .	61
5 Proof of Theorem 4B. . . . .	64

<b>5</b>	<b>A generalization of the Main Theorem and applications</b>	<b>69</b>
1	A generalization of Theorem 1B. . . . .	69
2	Curves of genus 0. . . . .	71
3	Curves of genus 1. . . . .	72
4	Hyperelliptic curves. . . . .	72
5	The Thue equation. . . . .	74
6	Strongly ramified coverings. . . . .	76
7	Galois coverings. . . . .	77
8	The results of H. Kleiman. . . . .	78

# Introduction

Let  $C$  be an algebraic curve defined over the field of all algebraic numbers  $\bar{\mathbf{Q}}$ ,  $x \in \bar{\mathbf{Q}}(C)$  non-constant, and  $\Sigma = \text{supp}(x)_\infty$  the set of poles of  $x$ . Let  $\mathbf{K}$  be an algebraic number field such that both  $C$  and  $x$  are defined over  $\mathbf{K}$ , and  $S$  a finite set of valuations of  $\mathbf{K}$ , containing the set  $S_\infty$  of Archimedean valuations. (Such  $\mathbf{K}$  and  $S$  will be called *suitable*.) The main object studied in this thesis is *the set of  $S$ -integral points*

$$C(x, \mathbf{K}, S) = \{P \in C(\mathbf{K}) \mid |x(P)|_v \leq 1 \text{ for } v \notin S\}.$$

The classical theorem of Siegel [Sie29] (see [La83, Ch.8] for a modern proof) states that  $C(x, \mathbf{K}, S)$  is finite provided  $|\Sigma| \geq 3$  or  $\mathbf{g}(C) \geq 1$ . In the case  $\mathbf{g}(C) \geq 2$  it is covered by Mordell's conjecture, proved by G. Faltings [Fa83], which asserts that  $C(\mathbf{K})$  is finite provided  $\mathbf{g}(C) \geq 2$ . Unfortunately, existing proofs of Siegel's theorem and Mordell's conjecture are non-effective, i.e. no explicit bound is given for the heights of the points from  $C(x, \mathbf{K}, S)$  (or  $C(\mathbf{K})$ ).

Very roughly speaking, Siegel's argument may be divided into two steps: (i) *reduction to Diophantine approximations*, and (ii) *application of Diophantine approximations*. Though S. Lang [La83] uses in the reduction step the non-effective Mordell-Weil theorem, this step can be also carried out effectively. But for the second step one needs a very strong result from Diophantine approximations (a generalized Thue-Siegel theorem in the original Siegel's argument, or Roth's theorem in modern expositions), for which no effective version is available.

A.O.Gelfond noticed in [Ge52] that certain Diophantine equations can be reduced to a Diophantine inequality of a weaker (than Thue-Siegel theorem) type. This inequality is a non-trivial lower bound for a linear form in logarithms of algebraic numbers, i.e. the following statement:

$$0 < \left| \alpha_1^{b_1} \dots \alpha_n^{b_n} - 1 \right|_v < e^{-\varepsilon B} \implies B = \max(b_1, \dots, b_n) \leq c(\varepsilon, \alpha_1, \dots, \alpha_n, v) \quad (1)$$

(here  $\alpha_i \in \bar{\mathbf{Q}}$ ,  $b_i \in \mathbf{Z}$ ,  $\varepsilon > 0$ , and  $v$  is a valuation of  $\mathbf{Q}(\alpha_1, \dots, \alpha_n)$ ). (1) easily follows from the results of Thue-Siegel type [Ge52, Th.1.3.3] but, of course, with a non-effective  $c(\varepsilon, \alpha_1, \dots, \alpha_n, v)$ . However, Gelfond had an effective proof of (1) for  $n = 2$ , and conjectured that, using similar approach, one can prove (1) effectively for an arbitrary  $n$ .

Indeed, in 1966 A.Baker [Ba66] obtained effective lower bounds for linear forms in any number of logarithms. This enabled him to realize Gelfond's idea of effective solution of Diophantine equations. See [Ba68], [Ba68a], [Ba68b], [Ba69].

The investigations of A. Baker were supplemented and generalized by other authors. We refer to [ShvPTSc77], [Sp80], [Sp82], [Fe82], [ShT86], [EGShT88], [EG88]

for historical surveys and extensive bibliography. However, mainly studied were equations of two classical types. The first one is *Thue equation*

$$f(x, y) = A, \quad (2)$$

$f$  being a form having three distinct linear factors, and  $A \neq 0$ . The second is the *superelliptic equation*

$$y^m = f(x), \quad (3)$$

where  $f(x) = a \prod_{i=1}^{\nu} (x - \alpha_i)^{r_i}$  and the  $\nu$ -tuple  $\left( \frac{m}{(m, r_1)}, \dots, \frac{m}{(m, r_{\nu})} \right)$  is not of the type  $(n, 1, \dots, 1)$  or  $(2, 2, 1, \dots, 1)$  (in particular,  $\nu \geq 2$ ).

As was noticed already by Siegel, the case  $\mathbf{g}(C) = 0$ ,  $|\Sigma| \geq 3$  can be reduced to (2). The case  $\mathbf{g}(C) = 1$  was considered by A. Baker and J. Coates [BaC70] by reduction to (3). Thus, for curves of genus 0 and 1 Siegel's theorem is effective. The case  $\mathbf{g}(C) \geq 2$  still remains open (except for particular cases discussed below).

V.G. Sprindžuk posed the problem of extending the method of Gelfond–Baker to classes of Diophantine equations more general than (2) and (3). An attempt of such an extension was made by H. Kleiman [Kl76], who considered a general equation  $f(x, y) = 0$ , but made some strong assumptions about the polynomial  $f$ .

Another result of this type is Theorem 5F of this thesis (Section 5.6), originally proved in [Bi88], [Bi88a]. Let  $C$  and  $x$  be as above, and consider the covering  $x : C \rightarrow \mathbf{P}^1$ . For any  $\alpha \in \mathbf{P}^1$  denote  $e_{\alpha} = \text{g.c.d.}(e_1, \dots, e_s)$ , where  $e_1, \dots, e_s$  are the ramification indices above  $\alpha$ . (Obviously,  $e_{\alpha} = 1$  for all but finitely many  $\alpha$ ).

**Theorem 5F.** *Assume that*

$$\sum_{\alpha \neq \infty} (1 - e_{\alpha}^{-1}) > 1$$

(the sum ranging over the finite part of  $\mathbf{P}^1$ ). Then for any suitable  $\mathbf{K}, S$

$$\max_{P \in C(x, \mathbf{K}, S)} h_x(P) \leq c(C, x, \mathbf{K}, S), \quad (4)$$

$c$  being effective.

It is clear that Theorem 5F covers equation (3). It also generalizes the above-mentioned results of Kleiman (see Section 5.8).

A simple calculation with Hurwitz formula shows that Theorem 5F yields the following *Effective Siegel theorem for Galois coverings of the line*.

**Theorem 5G** ([Bi88a] and Section 5.7). *Let  $\mathbf{g}(C) \geq 1$  and  $x : C \rightarrow \mathbf{P}^1$  be a Galois covering. Then for any suitable  $\mathbf{K}, S$  (4) is valid with an effective  $c$ .*

To describe the main results of the thesis we need some more notations.

Consider the group of  $\Sigma$ -units, i.e. functions  $z \in \bar{\mathbf{Q}}(C)$  that  $\text{supp}(z) \subseteq \Sigma$ . This group is isomorphic to  $\bar{\mathbf{Q}}^* \oplus \mathbf{Z}^\rho$ , where  $\rho = \rho(\Sigma)$  satisfies  $0 \leq \rho(\Sigma) \leq |\Sigma| - 1$ .

In Chapter 1 we prove

**Theorem 1B.** *If*

$$\rho(\Sigma) \geq 2$$

*then for any suitable  $\mathbf{K}, S$*

$$\max_{P \in C(x, \mathbf{K}, S)} h_x(P) \leq c(C, x, \mathbf{K}, S, \Lambda),$$

*$c$  being effective.*

Here  $\Lambda$  is a parameter characterising  $\Sigma$ , to be defined in Section 1.1. It can be easily estimated in practical cases. Actually we get an explicit value for  $c$  provided  $C$  is a non-singular model of a plane curve  $f(x, y) = 0$ .

The sketch of the proof is as follows. Fix  $Q \in C(x, \mathbf{K}, S)$ . Then for some  $v \in S$  and  $P \in \Sigma$  the point  $Q$  is “close” to  $P$  in  $v$ -metric. We have  $\rho(\Sigma \setminus \{P\}) \geq 1$ , hence there exists a non-constant  $\Sigma \setminus \{P\}$ -unit  $z$ . Since  $x(Q)$  is  $S$ -integer,  $z(Q)$  should be an  $S$ -unit (in a finite extension of  $\mathbf{K}$ ).

Since  $Q$  is “close” to  $P$ , the difference  $|(z(P))^{-1} z(Q) - 1|_v$  is small. Since  $z(Q)$  is an  $S$ -unit, we get an inequality of the type (1). Now the theory of linear forms in logarithms completes the proof.

Thus, as in Siegel’s argument, we have a reduction step, which is described above, and a Diophantine approximation step – the use of linear forms in logarithms.

In previous proofs of effective theorems by the method of Gelfond-Baker the problem is reduced to linear  $S$ -unit equations, and the latter are then analysed by means of linear forms in logarithms; see, for instance, [Sp82], [ShT86], [Schm92]. The new feature of the proposed argument is that the problem is reduced directly to linear forms in logarithms, without intermediate use of  $S$ -unit equations. This way possesses a double advantage: the proof becomes more direct, and the result – more general. Indeed, it does not seem that the proof of Theorem 1B can be carried out via linear  $S$ -unit equations.

One more comment is needed here. There exist various ways to express exactly the phrase “ $P$  is close to  $Q$ ”. For example, the formalism of Weil functions may be used, as in [Bo83]. However, we prefer the “old-fashioned” technique of Puiseux expansions, because it allows to carry out all the calculations in a very explicit form. Fortunately, recently W.M. Schmidt [Schm91] obtained very precise estimates for Puiseux expansions of Riemann-Roch bases, which essentially improve the previous results of J. Coates [Co70].

P. Vojta [Vo87, §2.4] applied a similar approach to the study of integral points on varieties of arbitrary dimension. He proves that under some conditions, similar to

our condition  $\rho(\Sigma) \geq 2$ , the set of integral points is not dense in the Zariski topology. However, Vojta reduces the problem to the non-effective Roth-Schmidt theorem and therefore his results are also non-effective.

Theorem 1B immediately yields effective theorems for Thue equations (2) and for curves of genus 0 (see Chapter 5). A natural question arises: is it possible to deduce other effective theorems, obtained by the Gelfond-Baker method, from a single general principle?

Let us say that an effective Diophantine theorem is *absolute* if it has the following form:

*Assume that  $C$  and  $x$  satisfy some condition. Then for any suitable  $\mathbf{K}$ ,  $S$  we have an effective upper bound for  $S$ -integral points.*

In other words, the only assumption made about  $\mathbf{K}$  and  $S$  is that they are suitable. All effective theorems mentioned above (Thue and superelliptic equations, curves of genus 0 and 1, Theorems 5F, 5G and 1B) are absolute. A typical example of a non-absolute theorem is Runge theorem [Bo83, Section V]. In Chapter 5 we prove Theorem 5A, which covers most of the known absolute effective Diophantine theorems. But, in order to formulate it in the most flexible form, we need some preliminary work, which is done in Chapters 2 – 4.

In Chapter 2 we prove an effective upper bound for the height of an isolated solution of a system of polynomial equations. We need such bound in Chapter 3. The argument is almost straightforward, but we were unable to find a suitable reference.

In Chapter 3 we prove a kind of an effective version of the Riemann existence theorem. It is known that there exist finitely many finite algebraic coverings of the projective line with given degree and ramification points. In Chapter 3 we give effective upper bounds for the height and degree of a defining polynomial of the covering curve in terms of the degree of the covering and the heights of ramification points (which are assumed to be defined over  $\bar{\mathbf{Q}}$ ). This result seems to be of independent interest.

In Chapter 4 we prove an effective version of Chevalley-Weil theorem for the case of curves. Using the result of Chapter 3, it may be represented in the following form.

**Theorem 4B (i).** *Let  $\varphi : \tilde{C} \rightarrow C$  be a finite covering of algebraic curves, unramified over  $C \setminus \Sigma$ ,  $Q \in C(x, \mathbf{K}, S)$  and  $\tilde{Q} \in \varphi^{-1}(Q)$ . Then  $\tilde{Q} \in \tilde{C}(\tilde{\mathbf{K}})$ , where*

$$N_{\tilde{\mathbf{K}}/\mathbf{K}} D_{\tilde{\mathbf{K}}/\mathbf{K}} \leq c(C, x, \mathbf{K}, S, \deg \varphi),$$

*$c$  being effective.*

Actually, we give an expression for  $c$ , explicite almost in all parametres.

Chapter 5 starts from already mentioned

**Theorem 5A.** *Let  $\varphi : \tilde{C} \rightarrow C$  be a finite covering of algebraic curves, unramified over  $C \setminus \Sigma$ . Assume that  $\rho(\tilde{\Sigma}) \geq 2$ , where  $\tilde{\Sigma} = \varphi^{-1}(\Sigma)$ . Then for any  $Q \in C(x, \mathbf{K}, S)$*

$$h_x(Q) \leq c(C, x, \mathbf{K}, S, \tilde{\Lambda}, \deg \varphi),$$

*c being effective.*

(Here  $\tilde{\Lambda}$  is defined for  $\tilde{\Sigma}$  as  $\Lambda$  for  $\Sigma$ .)

This theorem is proved in Section 5.1. The rest of Chapter 5 consists of various applications of Theorem 5A. We show that it covers most of classical absolute Diophantine theorems: curves of genus 0 and 1, hyperelliptic curves (provided  $\Sigma$  contains a fiber of the canonical double covering), Thue equation, etc. It also provides alternative proofs for Theorems 5F and 5G, formulated above, and for the results of H. Kleiman. As one more possible application of Theorems 1B and 5A, which is not reflected in the thesis, we may mention modular curves (in view of Manin–Drinfeld Theorem). See [Bi94, §7], where some results of D. Kubert and S. Lang [KuLa81, Ch.8] are generalized.

It would be interesting to find such a generalization of Theorem 5A, which covers also certain polynomial–exponential Diophantine equation, (e.g. Catalan type equations), equations containing products of consecutive integers, etc. The result of B. Brindza, K. Györy and R. Tijdeman [BrGyT86] gives hope that for Catalan equation such a generalization exists.

# Notations

We use the standard notations  $\mathbf{Z}$ ,  $\mathbf{Q}$ ,  $\mathbf{R}$  and  $\mathbf{C}$  for the ring of integers, and the fields of rational, real and complex numbers, respectively.

All fields are assumed to be of characteristic zero, unless contrary is stated explicitly. The algebraic closure of the field  $k$  is denoted by  $\bar{k}$ . In particular,  $\bar{\mathbf{Q}}$  is the field of all algebraic numbers.

Boldface letters  $\mathbf{K}$ ,  $\mathbf{L}$ ,  $\mathbf{M}$  usually denote algebraic number fields (i.e. finite extensions of  $\mathbf{Q}$ ). Given an algebraic number field  $\mathbf{K}$  fix once and for all an embedding  $\mathbf{K} \hookrightarrow \bar{\mathbf{Q}}$ . Denote:

- $d_{\mathbf{K}}$  =  $[\mathbf{K} : \mathbf{Q}]$ ;
- $D_{\mathbf{K}}$  – the absolute discriminant of  $\mathbf{K}$ ;
- $R_{\mathbf{K}}$  – the regulator of  $\mathbf{K}$ ;
- $h_{\mathbf{K}}$  – the class number;
- $\mathcal{R}_{\mathbf{K}}$  – the ring of integers;
- $\mathcal{R}_{\mathbf{K}}(S)$  – the ring of  $S$ -integers  
(here  $S$  is a finite set of valuations of  $\mathbf{K}$ , including all Archimedean valuations, and  $\alpha \in \mathbf{K}$  is  $S$ -integer if  $|\alpha|_v \leq 1$  for all  $v \notin S$ );
- $N_{\mathbf{K}}$  – the *absolute norm* map  
(in particular, if  $I$  is a fractional ideal of  $\mathbf{K}$ , then  $N_{\mathbf{K}}(I)$  is well-defined as a non-negative rational number).

For a finite extension  $\mathbf{L}/\mathbf{K}$  denote

- $d_{\mathbf{L}/\mathbf{K}}$  =  $[\mathbf{L} : \mathbf{K}]$ ;
- $D_{\mathbf{L}/\mathbf{K}}$  – the relative discriminant (which is an ideal of  $\mathbf{K}$ );
- $N_{\mathbf{L}/\mathbf{K}}$  – the relative norm map.

Valuations are assumed to be normalized so that their restrictions to  $\mathbf{Q}$  coincide with standard infinite or  $p$ -adic valuations. For a valuation  $v$  of  $\mathbf{K}$  denote:

- $p(v)$  – the prime below  $v$ ;
- $N_{\mathbf{K}}(v)$  – the norm of the corresponding prime ideal;
- $\mathbf{K}_v$  – the  $v$ -adic completion of  $\mathbf{K}$ ;
- $d_{\mathbf{K}}(v)$  =  $[\mathbf{K}_v : \mathbf{Q}_v]$ ;
- $e_{\mathbf{K}}(v)$  – the ramification index of  $v$  over  $\mathbf{Q}$ ;
- $f_{\mathbf{K}}(v)$  =  $\frac{d_{\mathbf{K}}(v)}{e_{\mathbf{K}}(v)} = \frac{\ln N_{\mathbf{K}}(v)}{\ln p(v)}$ .

$d_{\mathbf{L}/\mathbf{K}}(v)$ ,  $e_{\mathbf{L}/\mathbf{K}}(v)$  and  $f_{\mathbf{L}/\mathbf{K}}(v)$  are defined similarly.

A  $\mathbf{K}$ -system  $\{a(v)\}$  is a function on the set of valuations of  $\mathbf{K}$  with the following properties:

$$a(v) \geq 0 \quad \text{for all } v;$$

$$a(v) = 0 \quad \text{for all but finitely many } v;$$

$$\frac{e_{\mathbf{K}}(v) a(v)}{\ln p(v)} \in \mathbf{Z} \quad \text{for non-Archimedean } v.$$

Compare this with the  $K$ -system in [Schm91, p.187] and the  $M_K$ -divisor in [La83]. Denote

$$\text{nor}\{a(v)\} = \frac{1}{d_{\mathbf{K}}} \sum_v d_{\mathbf{K}}(v) a(v).$$

If  $\{a(v)\}$  is a  $\mathbf{K}$ -system and  $\mathbf{L}$  an extension of  $\mathbf{K}$ , then we have a well-defined  $\mathbf{L}$ -system, which is also defined by  $\{a(v)\}$ .

$\mathbf{P}^m$  denotes the  $m$ -dimensional projective space. The point  $(1 : \alpha)$  of  $\mathbf{P}^1$  is frequently denoted by  $\alpha$ , and the point  $(0 : 1)$  – by  $\infty$ .

For  $\alpha = (\alpha_0 : \dots : \alpha_m) \in \mathbf{P}^m(\bar{\mathbf{Q}})$  denote by  $h(\alpha)$  its absolute logarithmic height:

$$h(\alpha) = \frac{1}{d_{\mathbf{K}}} \sum_v d_{\mathbf{K}}(v) \max_{0 \leq i \leq m} \ln |\alpha_i|_v,$$

where  $\mathbf{K} = \mathbf{Q}(\alpha_0, \dots, \alpha_m)$ , and the sum is over the valuations of  $\mathbf{K}$ . If  $\alpha = (\alpha_1, \dots, \alpha_m)$  is a point in affine space, then  $h(\alpha) = h(1 : \alpha_1 : \dots : \alpha_m)$ . In particular, for  $\alpha \in \bar{\mathbf{Q}}$  we have

$$h(\alpha) = \frac{1}{d_{\mathbf{K}}} \sum_v d_{\mathbf{K}}(v) \max(0, \ln |\alpha|_v),$$

where  $\mathbf{K} = \mathbf{Q}(\alpha)$ . We have also  $h(\infty) = 0$ .

Although we denote affine and projective heights with the same letter  $h$ , this does not lead to confusion because it is always clear from the context what height is in mind.

If  $C$  is a projective curve over  $\bar{\mathbf{Q}}$  and  $x \in \bar{\mathbf{Q}}(C)$  then we also consider  $x$  as a finite ramified covering  $x : C \rightarrow \mathbf{P}^1$ . Then, as usual, we have the Weil height  $h_x : C(\bar{\mathbf{Q}}) \rightarrow \mathbf{R}_{\geq 0}$  defined by  $h_x(P) = h(x(P))$ .

We denote also by  $(x)$  the principal divisor, by  $(x)_0$  and  $(x)_\infty$  – the divisors of zeros and poles, and by  $\text{supp}(x)_0$ ,  $\text{supp}(x)_\infty$  – the supports of these divisors, i.e. the sets of zeros and poles of  $x$ .

Let  $f$  be a polynomial with algebraic coefficients and  $(\alpha_1, \dots, \alpha_m)$  be the vector of its non-zero coefficients ordered somehow. Denote

$$\begin{aligned} |f|_v &= \max_v |\alpha_i|_v, \\ h(f) &= h(\alpha_1 : \dots : \alpha_m) \end{aligned}$$

(so that  $h(\alpha f) = h(f)$  for  $\alpha \neq 0$ ).

We define  $\exp_k(x)$  by  $\exp_1(x) = \exp x$  and  $\exp_{k+1}(x) = \exp(\exp_k(x))$ .

More specific notations are introduced in appropriate places. A list of such notations is provided below (together with pages they are introduced).

$C(x, \mathbf{K}, S)$	p. 3	$h(D)$	p. 14
$l(z)$	p. 11	$\mathbf{K}_D$	p. 14
$\rho(\Sigma)$	p. 11	$L(z)$	p. 14
$\lambda_r(\Sigma)$	p. 11	$h(z)$	p. 14
$x_\alpha$	p. 13	$\mathbf{K}_z$	p. 14
$e_P$	p. 13	$d_r(\Sigma)$	p. 18
$x_P$	p. 13	$R_{\mathbf{K}}(S), R(S)$	p. 25
$z^{(P)}, z^{(P,i)}$	p. 13	$(n, h)$ – closed set	p. 38
$\varepsilon_P$	p. 13	$(n, h)$ – system	p. 38
$l(D), L(D)$	p. 14	Ram $(\mathbf{L}/\mathbf{K})$	p. 58
$\mathcal{L}(D)$	p. 14		

# Chapter 1

## Main theorem about integral points

### 1 Introduction.

Let  $C$  be an irreducible non-singular projective curve over  $\bar{\mathbf{Q}}$ , and  $\Sigma$  a finite subset of  $C(\bar{\mathbf{Q}})$ . For  $z \in \bar{\mathbf{Q}}(C)$  denote

$$l(z) = \sum_{P \in C(\bar{\mathbf{Q}})} |\text{Ord}_P(z)|. \quad (1)$$

A function  $z \in \bar{\mathbf{Q}}(C)$  is a  $\Sigma$ -unit if  $\text{Supp}(z) \subseteq \Sigma$ . Denote by  $U_\Sigma$  the group of  $\Sigma$ -units of the field  $\bar{\mathbf{Q}}(C)$ . Then  $U_\Sigma \cong \bar{\mathbf{Q}}^* \oplus \mathbf{Z}^\rho$ , where  $\rho = \rho(\Sigma)$  satisfies

$$0 \leq \rho(\Sigma) \leq |\Sigma| - 1. \quad (2)$$

Denote

$$\lambda_1(\Sigma) = \begin{cases} \min \{l(z) \mid z \in U_\Sigma \setminus \bar{\mathbf{Q}}^*\}, & \rho(\Sigma) \geq 1 \\ \infty, & \rho(\Sigma) = 0 \end{cases} \quad (3)$$

$$\lambda_r(\Sigma) = \max_{\substack{\Sigma' \subset \Sigma \\ |\Sigma'| = |\Sigma| - r + 1}} \lambda_1(\Sigma'). \quad (4)$$

In particular,

$$\lambda_r(\Sigma) < \infty \Leftrightarrow r \leq \rho(\Sigma). \quad (5)$$

Choose  $x \in \bar{\mathbf{Q}}(C)$  such that  $\Sigma \subseteq \text{supp}(x)_\infty$ , and  $y \in \bar{\mathbf{Q}}(C)$  such that  $\bar{\mathbf{Q}}(C) = \bar{\mathbf{Q}}(x, y)$ . Assume that  $x$  and  $y$  satisfy an irreducible (over  $\bar{\mathbf{Q}}$ ) algebraic equation

$$f(x, y) = 0. \quad (6)$$

Denote:

$$m = \deg_X f(X, Y), \quad n = \deg_Y f(X, Y), \quad (7)$$

$$N = \max(2, \deg f), \quad (8)$$

$$h = \max(1, h(f)). \quad (9)$$

Let  $\mathbf{K}$  be an algebraic number field such that  $C$ ,  $x$  and  $y$  are defined over  $\mathbf{K}$ . In particular, we may assume that  $f(X, Y) \in \mathbf{K}[X, Y]$ . Let  $S$  be a finite set of valuations of  $\mathbf{K}$ , including the subset  $S_\infty$  of all Archimedean valuations. Denote:

$$\begin{aligned} d &= d_{\mathbf{K}}; & d' &= \max(d, 2); \\ D &= D_{\mathbf{K}}; & D' &= \max(D, e); \\ \mathcal{D} &= \sqrt{D} (\ln D')^d \prod_{v \in S \setminus S_\infty} \ln N_{\mathbf{K}}(v); \\ \sigma &= |S|; \\ p &= \max\left(\max_{v \in S \setminus S_\infty} p(v), e^e\right); \\ \eta &= \max(\ln h, p^{d'} (\ln \ln p)^3). \end{aligned}$$

Finally, denote by  $\mathbf{K}(\Sigma)$  the composite of the fields  $\mathbf{K}(P)$ , where  $P \in \Sigma$ .

We prove in this chapter the following

**Theorem 1A.** *Let  $\rho(\Sigma) \geq 2$ , and assume that  $\Sigma \subseteq C(\mathbf{K})$ . Put  $\Lambda = \max(N, \lambda_2(\Sigma))$ . Then for any  $Q \in C(x, \mathbf{K}, S)$*

$$h_x(Q) \leq c_{11}(\sigma) \Lambda^{37} (h + \mathcal{D}) \eta \mathcal{D}^2, \quad (10)$$

where  $c_{11}(\sigma) = 2^{91\sigma+111} \sigma^{19\sigma+24}$ , and

$$h_x(Q) \leq c_{12}(\sigma) \Lambda^{37} p^{d'} (\ln \ln p)^3 (h + \mathcal{D}) \mathcal{D}^2, \quad (11)$$

$c_{12}(\sigma)$  being effectively computable.

**Remark.** The right-hand side of (10) is non-linear in  $h$  (for large  $h$  we have  $\eta = \ln h$ ), but has a better dependence on  $\sigma$  than the right-hand side of (11). However, the right-hand side of (11) is linear in  $h$ . We do not calculate explicitly  $c_{12}(\sigma)$ , but it should be roughly of the same order of magnitude as  $\sigma^{c\sigma^2}$  (see Remark after Proposition 5.3).

From Theorem 1A we deduce easily the following theorem, which is the main result of this chapter.

**Theorem 1B.** *Let  $\rho = \rho(\Sigma) \geq 2$ , and denote  $\Lambda = \lambda_2(\Sigma)$ . Let  $\varepsilon > 0$ . Then for any  $Q \in C(x, \mathbf{K}, S)$*

$$h_x(Q) \leq c(N, d, \varepsilon) \Lambda^{37} \left( \sigma^{20\sigma} D^{\frac{3}{2}} p^d \prod_{v \in S \setminus S_\infty} \ln^3 N_{\mathbf{K}}(v) \right)^{\nu+\varepsilon} e^{(4N)^{16+|\Sigma|-\rho} dh}, \quad (12)$$

where  $\nu = n(n-1) \dots (n - |\Sigma| + \rho - 1)$ .

Among the parameters appearing in (10)–(12), the only "unusual" is  $\Lambda$ . Using [Ma88, Th.A], we may prove that  $\Lambda \leq e^{c(N)dh}$  with an effective  $c(N)$  (this yields, by the way, that the condition  $\rho(\Sigma) \geq 2$  can be effectively verified). The proof consists of long, but more or less straightforward, calculations and is omitted here. However, as will be seen in Chapter 5, in practical cases  $\Lambda$  can be easily estimated in terms of  $N$ , and hence Theorems 1A and 1B are sufficient for most applications.

## 2 Puiseux expansions.

**Proposition 1** [Sil84, Th.2]. *Let  $\alpha = (\alpha_0 : \dots : \alpha_\mu) \in \mathbf{P}^\mu(\bar{\mathbf{Q}})$ , and  $[\mathbf{K}(\alpha) : \mathbf{K}] = \delta$ . Then*

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{K}(\alpha)/\mathbf{K}} \leq 2\delta(\delta-1)h(\alpha) + \delta \ln \delta.$$

For  $\alpha \in \bar{\mathbf{Q}} \cup \{\infty\}$  denote

$$x_\alpha = \begin{cases} x - \alpha, & \alpha \in \bar{\mathbf{Q}} \\ \frac{1}{x}, & \alpha = \infty. \end{cases}$$

For  $P \in C$  denote

$$\begin{aligned} e_P &= \text{Ord}_P x_\alpha, \\ x_P &= x_\alpha^{\frac{1}{e_P}}, \end{aligned}$$

where  $\alpha = x(P)$ . For any  $z \in \bar{\mathbf{Q}}(C)$  fix once and for all one of the  $e_P$  equivalent [Schm91, p.185] Puiseux expansions of  $z$  at  $P$  (with respect to  $x$ ), which we denote by

$$z^{(P)} = \sum_{s=\text{Ord}_P(z)}^{\infty} \gamma_s(P) x_P^s.$$

We also fix a primitive root of unity of order  $e_P$ , and denote it by  $\varepsilon_P$ . Then all  $e_P$  equivalent Puiseux expansions of  $z$  at  $P$  are

$$z^{(P,i)} = \sum_{s=\text{Ord}_P(z)}^{\infty} \gamma_s(P) (\varepsilon_P^i x_P)^s \quad (0 \leq i \leq e_P - 1)$$

(in particular,  $z^{(P)} = z^{(P,0)}$ ).

Let  $D = \sum_{P \in C} m(P)P$  be a divisor on  $C$ , i.e.  $m(P) \in \mathbf{Z}$  and  $m(P) = 0$  for all but finitely many  $P$ . Denote

$$\begin{aligned} l(D) &= \sum_{P \in C} |m(P)|, \\ L(D) &= \max(l(D), N), \\ \mathcal{L}(D) &= \{z \in \bar{\mathbf{Q}}(C) \mid (z) + D \geq 0\}. \end{aligned}$$

Assume that  $\text{supp}D \subseteq C(\bar{\mathbf{Q}})$ . Then we may define  $h(D) = \max_{P \in \text{supp}D} h_x(P)$ . Denote by  $\mathbf{K}_D$  the *field of definition* of  $D$  over  $\mathbf{K}$  (i.e.  $\mathbf{K}_D = \bar{\mathbf{K}}^{G_D}$ , where  $G_D$  is the subgroup of  $\text{Gal}(\bar{\mathbf{K}}/\mathbf{K})$ , consisting of the automorphisms preserving the divisor  $D$ ).

The following proposition is a non-complete summary of Theorems A2, B2 and C2 from [Schm91].

**Proposition 2.** *Let  $D$  be a divisor on  $C$  with  $\text{supp}D \subseteq C(\bar{\mathbf{Q}})$ . Then there exist  $g_1, \dots, g_n \in \mathbf{K}_D(C)$  and  $\pi_1, \dots, \pi_n \in \mathbf{Z}$  with the following properties :*

(i) *For any  $P \in C(\bar{\mathbf{Q}})$  the coefficients  $\gamma_{is}(P)$  of the Puiseux expansions*

$$g_i^{(P)} = \sum_{s=\text{Ord}_P(g_i)}^{\infty} \gamma_{is}(P)x_P^s$$

*belong to a finite extension  $\mathbf{K}_P$  of  $\mathbf{K}_D(\alpha)$  (where  $\alpha = x(P)$ ), satisfying  $[\mathbf{K}_P : \mathbf{K}_D(\alpha)] \leq n$ .*

(ii) *For any  $P \in C(\bar{\mathbf{Q}})$  there exist  $\mathbf{K}_D(\alpha)$ -systems  $\{c_P(v)\}, \{c_P^{(i)}(v)\}$  such that*

$$\ln |\gamma_{is}(P)|_v \leq sc_P(v) + c_P^{(i)}(v)$$

*and we have*

$$\text{nor}\{c_P(v)\} \leq 9L^5(h + h(\alpha) + h(D) + 12 \ln L)$$

$$\text{nor}\{c_P^{(i)}(v)\} \leq 370L^{11}(h + h(\alpha) + h(D) + 12 \ln L),$$

*where  $L = L(D)$ .*

(iii) *The set  $\{x^k g_i \mid 0 \leq k \leq \pi_i, \pi_i \geq 0\}$  forms a basis of the space  $\mathcal{L}(D)$ .*

Let  $z \in \bar{\mathbf{Q}}(C)$ . Denote by  $\mathbf{K}_z$  the field of definition of the principal divisor  $(z)$ , and put

$$h(z) = \max_{P \in \text{supp}(z)} h_x(P), \quad L(z) = \max(N, l(z)). \quad (1)$$

**Proposition 3.** *Let  $z \in \bar{\mathbf{Q}}(C)$ . Then there exists a non-zero  $\beta \in \bar{\mathbf{Q}}$  such that, if we replace  $z$  by  $\beta z$ , then :*

(i)  $z \in \mathbf{K}_z(C)$ .

(ii) For any  $P \in C(\bar{\mathbf{Q}})$  the coefficients  $\gamma_s(P)$  of the Puiseux expansions

$$z^{(P)} = \sum_{s=\text{Ord}_P(z)}^{\infty} \gamma_s(P)x_P^s \quad (2)$$

belong to a finite extension  $\mathbf{K}_P$  of  $\mathbf{K}_z(\alpha)$  ( where  $\alpha = x(P)$ ), satisfying

$$[\mathbf{K}_P : \mathbf{K}_z(\alpha)] \leq n, \quad (3)$$

$$\frac{1}{d_{\mathbf{K}_z}} \ln N_{\mathbf{K}_z} D_{\mathbf{K}_P/\mathbf{K}_z} \leq 747L^{13}d^2(\alpha)(h + h(\alpha) + h(z) + 12 \ln L), \quad (4)$$

where  $d(\alpha) = [\mathbf{K}_z(\alpha) : \mathbf{K}_z]$ ,  $L = L(z)$ .

(iii) For any  $P \in C(\bar{\mathbf{Q}})$  there exist  $\mathbf{K}_z(\alpha)$ -systems  $\{c_P(v)\}$ ,  $\{c'_P(v)\}$  such that

$$\ln |\gamma_s(P)|_v \leq sc_P(v) + c'_P(v) \quad (5)$$

and we have

$$\text{nor}\{c_P(v)\} \leq 9L^5(h + h(\alpha) + h(z) + 12 \ln L)$$

$$\text{nor}\{c'_P(v)\} \leq 370L^{11}(h + h(\alpha) + h(z) + 12 \ln L).$$

**Proof.** Apply Proposition 2 to the principal divisor  $(z)$ . Then one of the numbers  $\pi_i$  should be 0, and the others are negative. Hence one of  $g_i$  is equal to  $\beta z$  for some non-zero  $\beta \in \bar{\mathbf{Q}}$ . This proves everything except (4).

Now prove (4). As can be easily deduced from [Co70, Lemma 3],  $\mathbf{K}_P$  is generated over  $\mathbf{K}_z(\alpha)$  by  $\gamma_s(P)$  ( $s \leq \kappa$ ), where  $\kappa = (2n - 2)\frac{1}{2}l(z)(n + 1)e_P \leq L^4$ . Therefore by Proposition 1

$$\frac{1}{d_{\mathbf{K}_z}} N_{\mathbf{K}_z} D_{\mathbf{K}_P/\mathbf{K}_z} \leq 2n^2 d^2(\alpha)(\tilde{h} + 1),$$

where

$$\tilde{h} = h\left(1 : \alpha : \gamma_{\text{Ord}_P(z)} : \dots : \gamma_{\kappa}\right) \leq 373L^{11}(h + h(\alpha) + h(z) + 12 \ln L).$$

Hence we have (4), which completes the proof.

In this chapter we need only the simplest assertion (iii) of the following proposition, but we formulate it in all generality for the purposes of Chapter 2.

**Proposition 4.**

(i) Let  $F_1, \dots, F_\mu \in \bar{\mathbf{Q}}[X_1, \dots, X_\nu]$  and  $F = F_1 \cdot \dots \cdot F_\mu$ . Then

$$h(F) \geq h(F_1) + \dots + h(F_\mu) - \nu \deg F.$$

(ii) Let  $F, G \in \bar{\mathbf{Q}}[X_1, \dots, X_\nu]$  and  $G|F$ . Then

$$h(G) \leq h(F) + \nu \deg F.$$

(iii) Let  $F \in \bar{\mathbf{Q}}[X]$  and  $\alpha \in \bar{\mathbf{Q}}$  a root of  $F$ . Then

$$h(\alpha) \leq h(F) + \deg F.$$

(All assertions are valid provided  $F \neq 0$ .)

**Proof.** (i) follows from the corresponding local estimates

$$|F|_v \geq (c(v))^{-1} |F_1|_v \dots |F_\mu|_v, \quad (6)$$

$$\text{where } c(v) = \begin{cases} e^{\nu \deg F}, & \text{if } v \text{ is Archimedean} \\ 1, & \text{if } v \text{ is non-Archimedean.} \end{cases}$$

The non-Archimedean case is well known as Gauss lemma (and the inequality in (6) should be replaced by an equality). For the Archimedean case see [Ge52, Lemma 3.4.2].

(ii) follows from (i), and (iii) – from (ii), if we take  $G(X) = X - \alpha$ .

We want to apply Proposition 3 to the case  $z = y$ .

Clearly,  $h(y)$  is the maximal height of roots of the polynomial  $f(X, 0)\hat{f}(X, 0)$ , where  $\hat{f}(X, Y) = Y^n f(X, Y^{-1})$ . By Proposition 4,  $h(y) \leq h + m$ , and, obviously,  $l(y) = 2m$ ,  $\mathbf{K}_y = \mathbf{K}$ .

**Proposition 5.** For any  $P \in C(\bar{\mathbf{Q}})$  the coefficients  $\beta_s(P)$  of the Puiseux expansion

$$y^{(P)} = \sum_{s=\text{Ord}_P(y)}^{\infty} \beta_s(P) x_P^s \quad (8)$$

belong to a finite extension  $\mathbf{K}_P$  of  $\mathbf{K}(\alpha)$  (where  $\alpha = x(P)$ ), satisfying

$$[\mathbf{K}_P : \mathbf{K}(\alpha)] \leq n, \quad (9)$$

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{K}_P/\mathbf{K}} \leq 2^{24} N^{13} d^2(\alpha)(h + h(\alpha) + 5N). \quad (10)$$

There exist  $\mathbf{K}(\alpha)$ -systems  $\{b_P(v)\}, \{b'_P(v)\}$  such that for any valuation  $v$  of  $\mathbf{K}_P$

$$\ln |\beta_s(P)|_v \leq sb_P(v) + b'_P(v) \quad (11)$$

and we have

$$\text{nor}\{b_P(v)\} \leq 576N^5(h + h(\alpha) + 5N), \quad (12)$$

$$\text{nor}\{b'_P(v)\} \leq 2^{22}N^{11}(h + h(\alpha) + 5N). \quad (13)$$

**Proof.** We cannot apply directly Proposition 3 because of the constant multiple  $\beta$  occuring in its assertion. But in the case  $z = y$  we have  $\beta \in \mathbf{K}$ , and hence we obtain (9) and (10) immediately. We also have  $\mathbf{K}(\alpha)$ -systems  $\{b_P(v)\}, \{b''_P(v)\}$  such that

$$\ln |\beta\beta_s(P)|_v \leq sb_P(v) + b''_P(v)$$

and we have

$$\text{nor}\{b_P(v)\} \leq 576N^5(h + h(\alpha) + 5N)$$

$$\text{nor}\{b''_P(v)\} \leq 370 \cdot 2^{12}N^{11}(h + h(\alpha) + 5N).$$

Since  $|\text{supp}(y)| \leq 2m$ , there exists  $\mu \in \mathbf{Z}$  such that  $|\mu| \leq m$  and

$$\text{supp}(x_\mu)_0 \cap \text{supp}(y) = \emptyset.$$

Choosing  $P \in \text{supp}(x_\mu)_0$ , we obtain

$$h(\beta y(\mu)) = h(\beta\beta_0(P)) \leq \text{nor}\{b''_P(v)\} \leq 370 \cdot 2^{12}N^{11}(h + \ln \mu + 5N).$$

On the other hand, from Proposition 4 (iii) it follows that

$$h(y(\mu)) \leq h(g) + \deg g \leq h + n \ln \mu + \ln(m + 1) + n \leq h + 2N^2,$$

where  $g(Y) = f(\mu, Y)$ . Hence

$$h(\beta) \leq 371 \cdot 2^{12}N^{11}(h + \ln \mu + 5N) \leq 371 \cdot 2^{12}N^{11}(h + 6N).$$

Therefore we have (11)–(13) with

$$\beta'(v) = \beta''(v) + \ln \max(1, |\beta|_v).$$

The proposition is proved.

**Remark.** A more direct proof with a better quantitative result follows from [Schm90, Th.2].

If  $\mathbf{K}_P$  is the field defined in Proposition 5, then clearly  $\mathbf{K}(P) \subseteq \mathbf{K}_P(\varepsilon_P)$ , and we get

**Proposition 6.** *For any  $P \in C(\bar{\mathbf{Q}})$  we have*

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{K}(P)/\mathbf{K}} \leq 2^{24} N^{14} d^2(\alpha)(h + h(\alpha) + 6N).$$

For  $0 \leq r < |\Sigma|$  denote

$$d_r(\Sigma) = \max \{ [\mathbf{K}(\Sigma') : \mathbf{K}] \mid \Sigma' \subseteq \Sigma, |\Sigma'| = |\Sigma| - r \}.$$

In particular,  $d_0(\Sigma) = [\mathbf{K}(\Sigma) : \mathbf{K}]$ .

**Proposition 7.** *For  $0 \leq r < |\Sigma|$  we have*

$$d_r(\Sigma) \leq n(n-1) \dots (n - |\Sigma| + r + 1) \leq n^{|\Sigma| - r}. \quad (14)$$

Further

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{K}(\Sigma)/\mathbf{K}} \leq |\Sigma| d_1(\Sigma) 2^{24} N^{14} (h + 6N) \leq 2^{24} N^{14 + |\Sigma|} (h + 6N). \quad (15)$$

**Proof.** Let  $M$  be a finite subset of  $C(\bar{\mathbf{K}})$ , defined over  $\mathbf{K}$  (i.e.  $\sigma M = M$  for any  $\sigma \in \text{Gal}(\bar{\mathbf{K}}/\mathbf{K})$ ). Then, clearly, for any subset  $M' \subseteq M$  we have

$$[\mathbf{K}(M') : \mathbf{K}] \leq \mu(\mu - 1) \dots (\mu - \mu' + 1),$$

where  $\mu = |M|$ ,  $\mu' = |M'|$ . This proves (14) because the set  $\text{supp}(x)_{\infty}$  is defined over  $\mathbf{K}$ .

Further, let  $\Sigma = \{P_1, \dots, P_{|\Sigma|}\}$ . Denote  $\mathbf{K}_0 = \mathbf{K}$ ,  $\mathbf{K}_i = \mathbf{K}(P_1, \dots, P_i)$ , so that  $\mathbf{K}_{|\Sigma|} = \mathbf{K}(\Sigma)$ . Then for  $0 \leq i < |\Sigma|$

$$\delta_i = [\mathbf{K}_i : \mathbf{K}] \cdot [\mathbf{K}(\Sigma) : \mathbf{K}_{i+1}] \leq d_1(\Sigma).$$

Hence by Proposition 6

$$\begin{aligned} \frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{K}(\Sigma)/\mathbf{K}} &= \sum_{i=0}^{|\Sigma|-1} \frac{\delta_i}{d_{\mathbf{K}_i}} \ln N_{\mathbf{K}_i} D_{\mathbf{K}_{i+1}/\mathbf{K}_i} \leq \\ &\leq |\Sigma| d_1(\Sigma) 2^{24} N^{14} (h + 6N), \end{aligned}$$

which proves the first inequality in (15). The second follows immediately from (14).

We also apply Proposition 3 to the case when  $z$  is a  $\Sigma$ -unit. In this case  $\mathbf{K}_z \subseteq \mathbf{K}(\Sigma)$ , and we get

**Proposition 8.** *Let  $z$  be a  $\Sigma$ -unit. Then there exists a non-zero  $\beta \in \bar{\mathbf{Q}}$  such that, if we replace  $z$  by  $\beta z$ , then :*

- (i)  $z \in \mathbf{K}(\Sigma)(C)$ .
- (ii) For any  $P \in \text{supp}(x)_\infty$ , there exist  $\mathbf{K}(\Sigma)$ -systems  $\{c_P(v)\}, \{c'_P(v)\}$  such that for any valuation  $v$  of  $\mathbf{K}_P$  the coefficients  $\gamma_s(P)$  of the Puiseux expansion (2) satisfy (5), and we have

$$\text{nor}\{c_P(v)\} \leq 9L^5(h + 12 \ln L), \quad (16)$$

$$\text{nor}\{c'_P(v)\} \leq 370L^{11}(h + 12 \ln L). \quad (17)$$

We conclude this section with a general remark. Though it is almost obvious, we include it because it is used further in the thesis several times.

**Proposition 9.** Let  $\alpha \in \bar{\mathbf{Q}} \cup \{\infty\}$ ,  $Q \in C(\bar{\mathbf{Q}}) \setminus \text{supp}(x)_\infty$  and  $v$  a valuation of  $\bar{\mathbf{Q}}$ . Assume that the series

$$y^{(P)}(Q) = \sum_{s=\text{Ord}_P(y)}^{\infty} \beta_s(P) (x_P(Q))^s \quad (P \in \text{supp}(x_\alpha)_0)$$

converge absolutely with respect to the  $v$ -metric. Then one of the sums  $y^{(P)}(Q)$  equals  $y(Q)$  for an appropriate choice of the value of the root  $x_P(Q) = (x_\alpha(Q))^{\frac{1}{e_P}}$ . (In particular,  $y(Q) \neq \infty$ .)

Moreover, fix this  $P$  and assume further that  $x(Q)$  is not a root of  $\Delta(X)$  (the discriminant of  $f(X, Y)$  with respect to  $Y$ ). Let  $z \in \bar{\mathbf{Q}}(C)$ , and suppose that

$$\text{supp}(z)_\infty \cap \text{supp}(x_\beta)_0 = \emptyset,$$

where  $\beta = x(Q)$ . Assume that the series

$$z^{(P)}(Q) = \sum_{s=\text{Ord}_P(z)}^{\infty} \gamma_s(P) (x_P(Q))^s$$

converges in the  $v$ -metric. Then the sum  $z^{(P)}(Q)$  is equal to  $z(Q)$  for an appropriate choice of the value of  $x_P(Q)$  (possibly other than before).

**Proof.** We write

$$f(X, Y) = a(X)Y^n + \text{terms of lower degree in } Y,$$

$$g(X, Y) = Y^n f(X, Y^{-1}) = a(X) + \text{terms containing } Y.$$

Then in the field of fractional power series in  $x_\alpha$  [Wa50, §4.3] the polynomial  $f(x, Y)$  splits as

$$f(x, Y) = a(x) \prod_{P \in \text{supp}(x_\alpha)_0} \prod_{i=0}^{e_P-1} (Y - y^{(P,i)}).$$

From the absolute convergence we conclude that

$$f(x(Q), Y) = a(x(Q)) \prod_{P \in \text{supp}(x_\alpha)_0} \prod_{i=0}^{e_P-1} (Y - y^{(P,i)}(Q)).$$

It is impossible that  $a(x(Q)) = 0$ , as otherwise  $f(x(Q), Y) \equiv 0$ , which contradicts the irreducibility of  $f(X, Y)$ . Hence  $y(Q) \neq \infty$ , because else  $y^{-1}(Q) = 0$  is the root of  $g(x(Q), Y)$ , and this yields that  $a(x(Q)) = 0$ . Since  $f(x(Q), y(Q)) = 0$ ,  $y(Q)$  equals one of the  $y^{(P,i)}(Q)$ , which proves of the first part.

Since  $\bar{\mathbf{Q}}(C) = \bar{\mathbf{Q}}(x, y)$ , we have  $z = \frac{p(x, y)}{q(x)}$ , where  $p(X, Y)$  and  $q(X)$  are polynomials. Moreover, we may suppose that each root of  $q(X)$  is either a root of  $\Delta(X)$ , or equal to  $x(P')$  for some  $P' \in \text{supp}(z)_\infty$  [Schm91, Th.A1]. In particular,  $q(x(Q)) \neq 0$ .

Now, for some  $j \in \{0, \dots, e_P - 1\}$  we have  $z^{(P,j)} = \frac{p(x, y^{(P,i)})}{q(x)}$ . Hence

$$z^{(P,j)}(Q) = \frac{p(x(Q), y^{(P,i)}(Q))}{q(x(Q))} = \frac{p(x(Q), y(Q))}{q(x(Q))} = z(Q),$$

q.e.d.

### 3 Comparison of heights.

Let  $x, y, m, n$  be as in Section 1.1. Then we have the "quasi-equivalence of heights": for any  $P \in C(\bar{\mathbf{Q}})$  and  $\varepsilon > 0$

$$\left| \frac{h_x(P)}{n} - \frac{h_y(P)}{m} \right| \leq \varepsilon h_x(P) + c(\varepsilon, N, h). \quad (1)$$

In this section we establish weaker inequalities, but in a more explicit form. Of course, it is not very difficult to prove (1) and even

$$\left| \frac{h_x(P)}{n} - \frac{h_y(P)}{m} \right| \leq c(N) \left( \sqrt{h_x(P)} + \sqrt{h} \right)$$

with explicit constants (using, for example, the methods of [Sp82, Ch.9] and [Sp83]). However, for our purposes the trivial estimations of this section will be sufficient.

**Proposition 1.** For any  $P \in C(\bar{\mathbf{Q}})$

$$h_y(P) \leq m h_x(P) + h + n + \ln(m + 1), \quad (2)$$

$$h_x(P) \leq nh_y(P) + h + m + \ln(n + 1). \quad (3)$$

**Proof.** Replacing  $x$  by  $x^{-1}$  and/or  $y$  by  $y^{-1}$  if necessary, we may assume that  $P$  is not a pole of  $x$  or  $y$ . Denote  $g(Y) = f(x(P), Y)$ . Then  $g(Y) \not\equiv 0$  since  $f$  is irreducible over  $\bar{\mathbf{Q}}$ , and we have

$$\deg g \leq n,$$

$$h(g) \leq h + mh_x(P) + \ln(m + 1).$$

Since  $g(y(P)) = 0$ , Proposition 2.4 gives

$$h_y(P) = h(y(P)) \leq h(g) + \deg g \leq h + mh_x(P) + n + \ln(m + 1),$$

which proves (2). By symmetry, (3) follows as well.

**Proposition 2.** Let  $A = [a_{ij}]_{\substack{1 \leq i \leq \mu \\ 1 \leq j \leq \nu}}$  be a matrix with entries in  $\mathbf{K}$ , and denote

$$h(A) = h(\dots : a_{ij} : \dots).$$

Assume that the set of solutions  $b = (b_1, \dots, b_\nu)^t \in \mathbf{K}^\nu$  of the system of linear equations

$$Ab = 0$$

forms an  $r$ -dimensional subspace of  $\mathbf{K}^\nu$ . Then there exists a basis  $b^{(1)}, \dots, b^{(r)}$  of this subspace, satisfying

$$h(b^{(i)}) = h(b_1^{(i)} : \dots : b_\nu^{(i)}) \leq (\nu - 1)h(A) + \ln(\nu - 1)! \quad (1 \leq i \leq r).$$

**Proof.** Without loss of generality  $\mu = \text{rank} A = \nu - r$ , and  $\det B \neq 0$ , where  $B = [a_{ij}]_{1 \leq i, j \leq \mu}$ . Let  $B_j^{(i)}$  be the matrix obtained from  $B$  by replacing its  $j$ -th column by the  $(\mu + i)$ -th column of  $A$ . Define

$$b_j^{(i)} = \begin{cases} \det B_j^{(i)}, & 1 \leq j \leq \mu \\ \det B, & j = \mu + i \quad (1 \leq i \leq r) \\ 0, & \text{otherwise.} \end{cases}$$

Then  $b^{(i)} = (b_1^{(i)}, \dots, b_\nu^{(i)})$  are as desired.

**Proposition 3.** Let  $\delta_1, \delta_2, \mu_1, \mu_2$  be non-negative integers,

$$z_i = \sum_{s=-\delta_i}^{\infty} \gamma_{is} t^s \quad (i = 1, 2)$$

power series with coefficients in a field  $k$  of characteristic 0, and  $v$  a valuation of  $k$ . Let  $\kappa \geq \delta = \mu_1\delta_1 + \mu_2\delta_2$ , and assume that

$$\ln |\gamma_{is}|_v \leq \hat{c}_i(v) \quad (i = 1, 2, -\delta_i \leq s \leq \kappa),$$

where  $\hat{c}_1(v), \hat{c}_2(v) \geq 0$ . Put  $z = z_1^{\mu_1} z_2^{\mu_2} = \sum_{s=-\delta}^{\infty} \gamma_s t^s$ . Then

$$\ln |\gamma_s|_v \leq \hat{c}(v) + \ln \max \left( 1, \left| \binom{\delta + \mu - 1}{\mu - 1} \right|_v \right) \quad (-\delta \leq s \leq 0), \quad (4)$$

where  $\mu = \mu_1 + \mu_2$ ,  $\hat{c}(v) = \mu_1 \hat{c}_1(v) + \mu_2 \hat{c}_2(v)$ .

**Proof.** We say that  $z = \sum_{s=-\delta}^{\infty} \gamma_s t^s$  is dominated by  $\hat{z} = \sum_{s=-\delta}^{\infty} \hat{\gamma}_s t^s$ , if  $\hat{\gamma}_s \in \mathbf{R}_{\geq 0}$ , and  $|\gamma_s|_v \leq \hat{\gamma}_s$ . Domination is preserved by addition and multiplication of power series.

Clearly,  $\gamma_{-\delta}, \dots, \gamma_0$  depend only on  $\gamma_{is}$ , where  $i = 1, 2$ , and  $-\delta_i \leq s \leq \delta - \delta_i$ . Hence we may replace each  $z_i$  by  $\sum_{s=-\delta_i}^{\delta - \delta_i} \gamma_{is} t^s$ . Therefore we may assume that  $z_i$  is

dominated by  $e^{\hat{c}_i(v)} \sum_{s=-\delta_i}^{\infty} t^s$ , and hence  $z$  is dominated by

$$e^{\hat{c}(v)} \prod_{i=1}^{\mu} \sum_{s=-\delta_i}^{\infty} t^s = e^{\hat{c}(v)} t^{-\delta} (1-t)^{-\mu} = e^{\hat{c}(v)} \sum_{s=-\delta}^{\infty} \binom{s + \delta + \mu - 1}{\mu - 1} t^s,$$

which implies (4) immediately.

**Proposition 4.** Let  $z_1, z_2 \in \bar{\mathbf{Q}}(C)$  be integral over  $\bar{\mathbf{Q}}[x]$ , and  $\kappa \geq \frac{1}{2}l(z_1)l(z_2)$ . For each  $P \in \text{supp}(x)_{\infty}$  denote  $\delta_i(P) = -\min(0, \text{Ord}_P(z_i))$ , and let

$$z_i^{(P)} = \sum_{s=-\delta_i(P)}^{\infty} \gamma_{is}(P) x_P^s \quad (i = 1, 2)$$

be the Puiseux expansions. Finally, assume that

$$\hat{c}(v) \geq \max(0, \max \{ |\gamma_{is}(P)|_v \mid i = 1, 2; P \in \text{supp}(x)_{\infty}; -\delta_i(P) \leq s \leq \kappa \})$$

Then  $z_1, z_2$  satisfy an irreducible equation  $g(z_1, z_2) = 0$ , where

$$\deg_{Z_1} g(Z_1, Z_2) \leq \frac{1}{2}l(Z_2), \quad (5)$$

$$\deg_{Z_2} g(Z_1, Z_2) \leq \frac{1}{2}l(Z_1), \quad (6)$$

$$h(g) \leq 3\kappa^2 \text{ nor } \{\hat{c}(v)\} + 3\kappa^2. \quad (7)$$

**Proof.** Put  $\lambda_1 = \frac{1}{2}l(z_2)$ ,  $\lambda_2 = \frac{1}{2}l(z_1)$ . If  $g(z_1, z_2) = 0$  is the irreducible equation satisfied by  $z_1, z_2$ , then

$$\deg_{Z_1} g(Z_1, Z_2) = [\bar{\mathbf{Q}}(z_1, z_2) : \bar{\mathbf{Q}}(z_2)] \leq [\bar{\mathbf{Q}}(C) : \bar{\mathbf{Q}}(z_2)] = \lambda_1,$$

and similarly

$$\deg_{Z_2} g(Z_1, Z_2) \leq \lambda_2.$$

This proves (5), (6). Now put  $g(Z_1, Z_2) = \sum_{\mu_1=0}^{\lambda_1} \sum_{\mu_2=0}^{\lambda_2} b_{\mu_1\mu_2} Z_1^{\mu_1} Z_2^{\mu_2}$ . Then the vector  $b = (b_{00}, \dots, b_{\lambda_1\lambda_2})$  is determined up to a constant multiple by the system of linear equations

$$\text{Ord}_P \left( \sum_{\mu_1=0}^{\lambda_1} \sum_{\mu_2=0}^{\lambda_2} b_{\mu_1\mu_2} z_1^{\mu_1} z_2^{\mu_2} \right) \geq 0 \quad (P \in \text{supp}(x)_\infty).$$

As follows from the obvious inequality  $\lambda_1\delta_1(P) + \lambda_2\delta_2(P) \leq \kappa$  and Proposition 3, the matrix  $A$  of this system satisfies

$$h(A) \leq (\lambda_1 + \lambda_2) \text{ nor } \{\hat{c}(v)\} + \ln \begin{pmatrix} \kappa + \lambda_1 + \lambda_2 - 1 \\ \lambda_1 + \lambda_2 - 1 \end{pmatrix}.$$

Denote  $\nu = (\lambda_1 + 1)(\lambda_2 + 1)$ . Then by Proposition 2

$$h(g) = h(b_{00}, \dots, b_{\lambda_1\lambda_2}) \leq (\nu - 1)h(A) + \ln(\nu - 1)! \leq 3\kappa^2 \text{ nor } \{\hat{c}(v)\} + 3\kappa^2,$$

q.e.d.

**Proposition 5.** Let  $z$  be  $\Sigma$ -unit, and  $\beta \in \bar{\mathbf{Q}} \setminus \{0\}$  be as in Proposition 2.8. Then if we replace  $z$  by  $\beta z$ , we obtain

$$h_z(Q) \leq \frac{1}{2}l(z)h_x(Q) + 1113 L^{17}(h + 14 \ln L), \quad (8)$$

$$h_x(Q) \leq nh_z(Q) + 1113 L^{17}(h + 14 \ln L) \quad (9)$$

for any  $Q \in C(\bar{\mathbf{Q}})$ , where  $L = L(z)$  is defined in (2.1). Moreover, there is a  $\mathbf{K}(\Sigma)$ -system  $\{q(v)\}$  such that for any  $Q \notin \text{supp}(x)$

$$|\ln |z(Q)|_v| \leq q(v) + \frac{1}{2}l(z) \ln \max(1, |x(Q)|_v) \quad (10)$$

and we have

$$\text{nor}\{q(v)\} \leq 2226L^{17}(h + 15 \ln L). \quad (11)$$

**Proof.** Apply the previous proposition to  $z_1 = x$ ,  $z_2 = z$ . We have

$$\kappa = \frac{1}{2}l(x)l(z) \leq nL,$$

and we may put

$$\hat{c}(v) = \max_{P \in \text{supp}(x)_\infty} c'_P(v) + \kappa c_P(v),$$

where  $\{c'_P(v)\}$ ,  $\{c_P(v)\}$  are from Proposition 2.8. We get an irreducible equation  $g(x, z) = 0$  such that

$$\begin{aligned} \deg_X g(X, Z) &\leq \lambda = \frac{1}{2}l(z), \\ \deg_Z g(X, Z) &\leq n, \\ h(g) &\leq 3n^2L^2 \text{ nor } \{\hat{c}(v)\} + 3n^2L^2 \leq 1112L^{16}(h + 13 \ln L). \end{aligned}$$

By Proposition 1 we obtain (8) and (9). To prove (10) and (11) note that

$$g(X, Z) = \theta_1 Z^{\lambda_1} + Zg_1(X, Z) + \theta_0,$$

where  $\deg_Z g_1(X, Z) \leq n - 2$ . Define

$$q_i(v) = \ln |\theta_i^{-1} g|_v + \ln \max(1, |\lambda + 1|_v) \quad (i = 0, 1).$$

Then

$$\ln |Z(Q)|_v \leq \lambda \ln \max(1, |x(Q)|_v) + q_1(v),$$

$$\ln |Z(Q)|_v \geq -\lambda \ln \max(1, |x(Q)|_v) + q_0(v)$$

provided  $Q \notin \text{supp}(x)$ , and therefore

$$\text{nor}\{q_i(v)\} \leq h(g) + \ln |\lambda + 1|.$$

This implies (10) and (11) with  $q(v) = \max(q_0(v), q_1(v))$ .

## 4 Siegel's construction of convenient units of algebraic number fields.

Propositions 2 and 6 of this section go back to Siegel's paper [Sie69].

**Proposition 1.** *Let  $\Gamma$  be a lattice in  $\mathbf{R}^{\sigma-1}$ . Then there exist linearly independent  $x^{(i)} = (x_1^{(i)}, \dots, x_{\sigma-1}^{(i)}) \in \Gamma$  ( $1 \leq i \leq \sigma - 1$ ) such that*

$$\prod_{i=1}^{\sigma-1} \sum_{j=1}^{\sigma-1} |x_j^{(i)}| \leq (\sigma - 1)! \det \Gamma.$$

**Proof.** Apply Minkowski's inequality on successive minima to the body

$$B = \left\{ x = (x_1, \dots, x_{\sigma-1}) \in \mathbf{R}^{\sigma-1} \quad : \quad |x_1| + \dots + |x_{\sigma-1}| \leq 1 \right\}.$$

Let now  $S = (v_1, \dots, v_\sigma)$  be a finite set of valuations of an algebraic number field  $\mathbf{K}$ . Let  $\eta_1, \dots, \eta_{\sigma-1}$  be a fundamental system of  $S$ -units. The  $S$ -regulator is defined by

$$R(S) = R_{\mathbf{K}}(S) = |\det A|,$$

where

$$A = [a_{ij}]_{1 \leq i, j \leq \sigma-1}, \quad a_{ij} = d(v_i) \ln |\eta_j|_{v_i}. \quad (1)$$

Here  $d(v) = d_{\mathbf{K}}(v)$ .  $R_{\mathbf{K}}(S)$  is well-defined and coincides with the standard regulator  $R_{\mathbf{K}}$  when  $S = S_\infty$

Applying Proposition 1 to the lattice, generated by the columns of the matrix  $A$ , we obtain

**Proposition 2.** *There exist independent  $S$ -units  $\theta_1, \dots, \theta_{\sigma-1}$  satisfying*

$$\prod_{i=1}^{\sigma-1} \sum_{\substack{v \in S \\ v \neq v_\sigma}} d(v) |\ln |\theta_i|_v| \leq (\sigma-1)! R(S). \quad (2)$$

For an  $S$ -unit  $\theta$  we have  $\sum_{v \in S} d(v) \ln |\theta|_v = 0$ . Hence

$$d(v_\sigma) |\ln |\theta|_{v_\sigma}| \leq \sum_{\substack{v \in S \\ v \neq v_\sigma}} d(v) |\ln |\theta|_v|.$$

Therefore

$$h(\theta) = \frac{1}{2d} \sum_{v \in S} d(v) |\ln |\theta|_v| \leq \frac{1}{d} \sum_{\substack{v \in S \\ v \neq v_\sigma}} d(v) |\ln |\theta|_v|$$

(here  $d = d_{\mathbf{K}}$ ). We get

**Proposition 3.** *The units  $\theta_1, \dots, \theta_{\sigma-1}$ , defined in Proposition 2, satisfy*

$$\prod_{i=1}^{\sigma-1} h(\theta_i) \leq \frac{(\sigma-1)!}{d^{\sigma-1}} R(S).$$

Denote by  $U$  the multiplicative group generated by  $\theta_1, \dots, \theta_{\sigma-1}$ .

**Proposition 4** [Do79]. *Let  $\alpha \in \mathbf{K} \setminus \{0\}$ . Then either  $\alpha$  is a root of unity, or*

$$h(\alpha) \geq \frac{1}{d\xi},$$

where

$$\xi = \xi(d) = 2400 \ln^3 d', \quad d' = \max(d, 2). \quad (3)$$

**Proposition 5.** *Let  $h_i = \max(h(\theta_i), 1)$ . Then*

$$h_1 \cdot \dots \cdot h_{\sigma-1} \leq \xi^{\sigma-1}(\sigma-1)! R(S).$$

In particular,

$$h_i \leq \xi^{\sigma-1}(\sigma-1)! R(S) \quad (1 \leq i \leq \sigma-1).$$

**Proof.** Immediately from Propositions 3 and 4.

**Proposition 6.** *For any  $\alpha \in \mathbf{K}$  there exists  $\theta \in U$  such that  $\beta = \alpha\theta^{-1}$  satisfies*

$$\frac{1}{d} \sum_{\substack{v \in S \\ v \neq v_\sigma}} d(v) |\ln |\beta|_v| \leq \xi^{\sigma-1} \sigma! R(S).$$

**Proof.** Denote

$$b_{ij} = d(v_i) \ln |\theta_j|_{v_i}, \quad B = [b_{ij}]_{1 \leq i, j \leq \sigma-1}, \quad (4)$$

$$c_i = d(v_i) \ln |\alpha|_{v_i}, \quad c = (c_1, \dots, c_{\sigma-1})^t, \quad (5)$$

$$x = (x_1, \dots, x_{\sigma-1})^t = B^{-1}c. \quad (6)$$

For each  $x_i$  let  $y_i$  be the nearest integer. Take  $\theta = \theta_1^{y_1} \cdot \dots \cdot \theta_{\sigma-1}^{y_{\sigma-1}}$ . Then  $\beta = \alpha\theta^{-1}$  satisfies

$$\begin{aligned} \frac{1}{d} \sum_{\substack{v \in S \\ v \neq v_\sigma}} d(v) |\ln |\beta|_v| &\leq \frac{1}{d} \sum_{i=1}^{\sigma-1} \sum_{\substack{v \in S \\ v \neq v_\sigma}} |x_i - y_i| d(v) |\ln |\theta_i|_v| \leq \frac{1}{2d} \sum_{i=1}^{\sigma-1} \sum_{\substack{v \in S \\ v \neq v_\sigma}} d(v) |\ln |\theta_i|_v| \leq \\ &\leq \frac{1}{2d} \sum_{i=1}^{\sigma-1} \sum_{v \in S} d(v) |\ln |\theta_i|_v| \leq (h_1 + \dots + h_{\sigma-1}) \leq \xi^{\sigma-1} \sigma! R(S), \end{aligned}$$

q.e.d.

**Proposition 7.** *Let  $\theta = \theta_1^{y_1} \cdot \dots \cdot \theta_{\sigma-1}^{y_{\sigma-1}}$ . Denote  $Y = \max(|y_1|, \dots, |y_{\sigma-1}|)$ . Then*

$$h(\theta) \leq Y \xi^{\sigma-1} \sigma! R(S) \quad (7)$$

and

$$Y \leq 2d\xi\sigma! h(\theta). \quad (8)$$

**Proof.** We have

$$h(\theta) \leq Y(h_1 + \dots + h_{\sigma-1}) \leq Y\xi^{\sigma-1}\sigma! R(S).$$

To prove (8) we use the notations (4)–(6) with  $\theta$  instead of  $\alpha$ . Denote by  $B_j$  the matrix obtained from  $B$  upon replacing its  $j$ -th column by  $c$ . Note that

$$\sum_{i=1}^{\sigma-1} |b_{ij}| \geq \frac{1}{2} \sum_{i=1}^{\sigma} |b_{ij}| = dh(\theta_j) \geq \frac{1}{\xi}.$$

Hence by (1)

$$|\det B_j| \leq \sum_{i=1}^{\sigma-1} |c_i| \frac{\prod_{k=1}^{\sigma-1} \sum_{i=1}^{\sigma-1} |b_{ik}|}{\sum_{i=1}^{\sigma-1} |b_{ij}|} \leq 2d\xi h(\theta)(\sigma-1)! R(S).$$

On the other hand, we have clearly

$$|\det B| \geq R(S).$$

Hence

$$|y_i| = \frac{|\det B_j|}{|\det B|} \leq 2d\xi(\sigma-1)! h(\theta),$$

which proves (8).

We conclude this section by evaluating  $R(S)$  in terms of more traditional parameters of the field  $\mathbf{K}$ . We write  $D, R, h, \mathcal{R}, Nv$  instead of  $D_{\mathbf{K}}, R_{\mathbf{K}}, h_{\mathbf{K}}, \mathcal{R}_{\mathbf{K}}, N_{\mathbf{K}}(v)$ . By  $h(S) = h_{\mathbf{K}}(S)$  we denote the class number of the ring  $\mathcal{R}(S) = \mathcal{R}_{\mathbf{K}}(S)$  of  $S$ -integers.

**Proposition 8.** *Assume that  $S \supseteq S_{\infty}$ . Then*

$$R(S) = R \frac{h}{h(S)} \prod_{v \in S \setminus S_{\infty}} \ln Nv.$$

**Proof.** Denote by  $\text{Div}_S$  the subgroup of the divisor group of the field  $\mathbf{K}$ , generated by the non-Archimedean points from  $S$ ; by  $\text{Prin}_S$  the subgroup of  $\text{Div}_S$ , consisting of principal divisors, and let  $\text{Cl}_S = \text{Div}_S / \text{Prin}_S$ . Denote also by  $\text{Cl}$  and  $\text{Cl}(S)$  the class groups of the rings  $\mathcal{R}$  and  $\mathcal{R}(S)$  respectively. Then we have an obvious exact sequence

$$0 \longrightarrow \text{Cl}_S \longrightarrow \text{Cl} \longrightarrow \text{Cl}(S) \longrightarrow 0,$$

which implies  $h_S = \frac{h}{h(S)}$ , where  $h_S = [\text{Div}_S : \text{Prin}_S]$ .

Now let  $S \setminus S_\infty = \{v_1, \dots, v_\rho\}$ , and  $S_\infty = \{v_{\rho+1}, \dots, v_\sigma\}$ . Define

$$\varphi : \text{Div}_S \longrightarrow \mathbf{R}^\rho$$

by

$$\varphi \left( \sum_{i=1}^{\rho} n_i v_i \right) = (n_1 \ln Nv_1, \dots, n_\rho \ln Nv_\rho).$$

Then  $\varphi(\text{Div}_S)$  is a lattice in  $\mathbf{R}^\rho$  with discriminant  $\prod_{i=1}^{\rho} \ln Nv_i$  and  $\varphi(\text{Prin}_S)$  is a sublattice of index  $h_S$ . Note that for any  $S$ -unit  $\eta$ , the image of the principal divisor  $(\eta)$  is

$$\left( -d(v_1) \ln |\eta|_{v_1}, \dots, -d(v_\rho) \ln |\eta|_{v_\rho} \right)^t.$$

Now let  $\eta_{\rho+1}, \dots, \eta_{\sigma-1}$  be a fundamental system of  $S_\infty$ -units, and complete it to a fundamental system  $\eta_1, \dots, \eta_{\sigma-1}$  of  $S$ -units. Then the matrix  $A$  defined in (1) will be of the form

$$A = \begin{pmatrix} A' & 0 \\ * & A'' \end{pmatrix},$$

where  $A''$  is a  $(\sigma - \rho - 1) \times (\sigma - \rho - 1)$ -matrix with  $\det A'' = R$ , and the columns of the  $\rho \times \rho$ -matrix  $A'$  form a basis of the lattice  $\varphi(\text{Prin}_S)$ . Hence

$$|\det A'| = h_S \prod_{i=1}^{\rho} \ln Nv_i = \frac{h}{h(S)} \prod_{v \in S \setminus S_\infty} \ln Nv.$$

Finally

$$R(S) = |\det A| = R \frac{h}{h(S)} \prod_{v \in S \setminus S_\infty} \ln Nv,$$

q.e.d.

**Proposition 9** [Lav70]. *Let  $\mathbf{K} \neq \mathbf{Q}$ . Then*

$$hR \leq c\sqrt{D}(\ln D)^{d-1},$$

where

$$c = \frac{\sqrt{e} \left(1 + \frac{1}{\ln D}\right)^{d+1} d}{(2\sqrt{\pi})^d} \leq \frac{5d}{1.45^d} \leq 5. \quad (9)$$

**Corollary 10.** *Let  $\mathbf{K} \neq \mathbf{Q}$ . Then*

$$R(S) \leq 5\sqrt{D}(\ln D)^{d-1} \prod_{v \in S \setminus S_\infty} \ln Nv. \quad (10)$$

## 5 Lower bounds for linear forms in logarithms.

After the first results of A. Baker [Ba66] considerable progress was made in estimating linear forms in logarithms. See [Fe74], [Ba77], [vP77], [Fe82] for historical surveys, and [PW88], [Wü88], [BaWü93], [Yu90] for further results. Recently a new method was proposed by E. Bombieri [Bo93].

In this section  $\mathbf{K}$  is an algebraic number field, and we fix an embedding  $\mathbf{K} \hookrightarrow \mathbf{C}$ . We denote by  $\log z$  any value of the logarithm, and by  $\ln z$  its principal value, i.e.

$$-\pi < \operatorname{Im} \ln z \leq \pi.$$

Let  $\alpha_1, \dots, \alpha_{\sigma-1}$ ,  $\alpha \in \mathbf{K}^*$ ,  $b_1, \dots, b_{\sigma-1} \in \mathbf{Z}$ . Denote:

$$\begin{aligned} d &= d_{\mathbf{K}}; \\ h_i &= \max(h(\alpha_i), 1) \quad (1 \leq i \leq \sigma - 1); \\ A' &= \max(h_1, \dots, h_{\sigma-1}, e); \\ A &= \max(A', h(\alpha)); \\ B &= \max(b_1, \dots, b_{\sigma-1}). \end{aligned}$$

Let  $\log \alpha_1, \dots, \log \alpha_{\sigma-1}$ ,  $\log \alpha$  be arbitrary but fixed non-zero values of logarithms, and  $V_1, \dots, V_{\sigma-1}$  and  $V$  any positive real numbers satisfying

$$V_i \geq \max \left\{ h_i, \frac{|\log \alpha_i|}{d}, \frac{\sigma}{d} \right\} \quad (1)$$

$$V \geq \max \left\{ V_1, \dots, V_{\sigma-1}, \frac{|\log \alpha|}{d}, A \right\} \quad (2)$$

Denote

$$\Lambda = b_1 \log \alpha_1 + \dots + b_{\sigma-1} \log \alpha_{\sigma-1} + \log \alpha.$$

**Proposition 1** [PW88, Th.2.1]. *Let  $\Lambda \neq 0$ . Then*

$$|\Lambda| \geq \exp(-c_{51}(\sigma)d^{\sigma+2}V_1 \dots V_{\sigma-1}V(\ln B + 1 + \ln dV)(1 + \ln d)),$$

where  $c_{51}(\sigma) \leq 2^{8\sigma+51}\sigma^{2\sigma}$ .

**Remark.** A better value for  $c_{51}(\sigma)$  can be found in [BGMMS90]. I was informed by Prof. R. Steiner that a better result is proved in [BaWü93], but this paper is not available for me at the present moment.

**Proposition 2.** *Let  $v$  be an Archimedean valuation of  $\mathbf{K}$ , and  $0 < \varepsilon \leq 1$ . Suppose that*

$$0 < \lambda = \left| \alpha_1^{b_1} \cdot \dots \cdot \alpha_{\sigma}^{b_{\sigma}} \alpha - 1 \right|_v < e^{-\varepsilon B} \quad (3)$$

and that  $\sigma \geq \frac{d}{2}$ . Then

$$B \leq c_{52}(\sigma) \frac{1}{\varepsilon} \left( \ln \frac{1}{\varepsilon} \right) h_1 \dots h_\sigma A \ln A \quad (4)$$

with

$$c_{52}(\sigma) = 2^{11\sigma+94} \sigma^{4\sigma+6}. \quad (5)$$

**Proof.** We follow [PW88, pp.285–286]. As proved there, the inequality  $\lambda < \frac{1}{3}$  yields that there exists  $\kappa \in \mathbf{Z}$  such that

$$|b_1 \ln \alpha_1 + \dots + b_{\sigma-1} \ln \alpha_{\sigma-1} + \ln \alpha - 2\pi i \kappa| < \frac{3}{2} \lambda.$$

Comparing the imaginary parts we get  $|\kappa| < \frac{\sigma-1}{2} B + 1$  (recall that  $\ln$  denotes the principal value of the logarithm). Clearly,

$$\frac{|\ln \alpha_i|}{d} \leq \frac{|\ln |\alpha_i||}{d} + \frac{\pi}{d} \leq h_i + \frac{\pi}{d}.$$

Hence, if we define

$$V_i = \frac{2\sigma + \pi}{d} h_i \quad (1 \leq i \leq \sigma - 1), \quad (6)$$

$$V_\sigma = \frac{2\sigma + \pi}{d}, \quad V = \frac{2\sigma + \pi}{d} A, \quad (7)$$

we see that (1) is valid with  $\sigma$  replaced by  $\sigma + 1$ . Hence by Proposition 1 (with  $\sigma + 1$  instead of  $\sigma$ )

$$\varepsilon B \leq c_{51}(\sigma+1) \cdot d^2 (1 + \ln d) (2\sigma + \pi)^{\sigma+1} h_1 \dots h_{\sigma-1} A \left( \ln \left( 1 + \frac{\sigma}{2} B \right) + 1 + \ln(2\sigma + \pi) A \right), \quad (8)$$

which implies (3) after routine computations.

Note that the argument in [PW88, pp.285–286] is slightly inaccurate. Namely, the choice  $V_j = 7 \log A_j$  is incorrect, because the inequality  $V_j \geq \frac{n}{D}$  may fail.

**Proposition 3.** *Under the assumptions of Proposition 2 we have also*

$$B \leq c_{53}(\sigma) \frac{1}{\varepsilon} \left( \ln \frac{1}{\varepsilon} \right) h_1 \dots h_{\sigma-1} \cdot A \ln A', \quad (9)$$

$c_{53}$  being effectively computable.

**Proof.** Similar to the proof of Theorem 1.3 in [PW88, pp.286]. One should only pay attention on the dependence of the constants on  $\varepsilon$ .

**Remark.** We do not present here a numerical value for  $c_{53}$  because it is essentially worse than  $c_{52}$  (something like  $\sigma^{c\sigma^2}$ ; see [PW88, pp.283–284]). If someone is interested in a “good” dependence on  $\sigma$  rather than on  $A$ , he should use Proposition 2; otherwise – Proposition 3. Unfortunately, in the Archimedean case there is still no version of Propositions 2 and 3 “good” both in  $A$  and in  $\sigma$ . I am thankful to Prof. R. Steiner for a useful correspondence on this matter.

In the non-Archimedean case the situation is better due to results of Kunrui Yu. Let  $v$  be a non-Archimedean valuation of  $\mathbf{K}$ , and  $p = \max(p(v), e^e)$ . Let  $V_1, \dots, V_{\sigma-1}, V'$  and  $V$  satisfy

$$V_i \geq \max\left(h_i, \frac{|\ln \alpha_i|}{2\pi d}, \ln p\right) \quad (1 \leq i \leq \sigma - 1), \quad (10)$$

$$V' \geq \max(V_1, \dots, V_{\sigma-1}), \quad (11)$$

$$V \geq \max\left(V', \frac{|\ln \alpha|}{2\pi d}, A\right). \quad (12)$$

Denote

$$\Phi = 7 \cdot 10^5 \left( \frac{10\sigma d}{\sqrt{\ln p}} \right)^{2\sigma} p^{d'} V_1 \cdots V_{\sigma-1} \cdot V \ln(24\sigma d(V' + 1)),$$

where  $d' = \max(d, 2)$ .

**Proposition 4** [Yu90, p.16]. *Let  $0 < \delta \leq 1$ . Then*

$$\lambda = |\alpha_1^{b_1} \cdots \alpha_{\sigma-1}^{b_{\sigma-1}} \cdot \alpha - 1|_v > \exp\left(-\frac{\ln p}{e_v} \max\left(\Phi \ln \frac{\Phi}{\delta A}, \delta B\right)\right) \quad (13)$$

(provided  $\lambda \neq 0$ ).

**Proposition 5.** *Under the assumptions of Proposition 2 but with a non-Archimedean  $v$  we have*

$$B \leq c_{52}(\sigma) \frac{1}{\varepsilon} \left( \ln \frac{1}{\varepsilon} \right) p^{d'} (\ln \ln p) h_1 \cdots h_\sigma \cdot A \ln^2 A', \quad (14)$$

where  $c_{52}$  is from (6).

**Proof.** In Proposition 4 take  $\delta = \min\left(1, \frac{e_v}{2 \ln p} \varepsilon\right)$ . Then

$$B \leq \frac{\ln p}{\varepsilon e_v} \Phi \ln \frac{2\Phi \ln p}{\varepsilon e_v A}.$$

Putting  $V_i = h_i \ln p$ ,  $V' = A' \ln p$  and  $V = A \ln p$ , we obtain (14).

## 6 Proof of Theorem 1A.

Set

$$b(v) = \max_{P \in \Sigma} e_P b_P(v),$$

where  $\{b_P(v)\}$  are from Proposition 2.5. Then

$$\text{nor}\{b(v)\} \leq 576N^6(h + 5N). \quad (1)$$

Fix  $Q \in C(x, \mathbf{K}, S)$ . Let  $w \in S$  be defined from

$$|x(Q)|_w = \max_{v \in S} |x(Q)|_v.$$

Fix a prolongation of  $w$  on  $\bar{\mathbf{Q}}$ , and denote it also by  $w$ . We have

$$h_x(Q) \leq \frac{\sigma}{d} \ln |x(Q)|_w. \quad (2)$$

Without loss of generality

$$\ln |x(Q)|_w > b(w), \quad (3)$$

as otherwise

$$h_x(Q) \leq \sigma \text{nor}\{b(v)\} \leq 576\sigma N^6(h + 5N), \quad (4)$$

which is much better than (1.10) and (1.11).

We use the notation (2.8). By (3), the series

$$y^{(P)}(Q) = \sum_{s=\text{Ord}_P(y)}^{\infty} \beta_s(P) (x(Q))^{-\frac{s}{e_P}} \quad (P \in \text{supp}(x)_{\infty}) \quad (5)$$

converge in  $w$ -metric. By Proposition 2.9 one of the sums  $y^{(P)}(Q)$  should be equal to  $y(Q)$  for an appropriate choice of the value of the root  $(x(Q))^{\frac{1}{e_P}}$ . Fix this  $P$  up to the end of the proof.

We have  $\rho(\Sigma \setminus \{P\}) \geq 1$ , hence there exists a  $\Sigma \setminus \{P\}$ -unit  $z$  satisfying  $L(z) \leq \Lambda$ . We replace  $z$  by  $\beta z$  as in Proposition 2.8, and assume further that (i), (ii) of this proposition are valid. Since  $\mathbf{K} = \mathbf{K}(\Sigma)$ , we have  $z \in \mathbf{K}(C)$ .

Let  $\{c_P(v)\}, \{c'_P(v)\}$  be as in (ii) of Proposition 2.8, where  $P$  is the fixed one. We may assume that

$$\ln |x(Q)|_w > e_P(c_P(w) + 1) \quad (6)$$

since otherwise we again have a much better bound for  $h_x(Q)$  than (1.10) and (1.11). Hence the series

$$z^{(P,i)}(Q) = \sum_{s=0}^{\infty} \gamma_s(P) (x(Q))^{-\frac{s}{e_P}} \quad (7)$$

converges in  $w$ -metric. We may suppose that  $x(Q)$  is not a root of  $\Delta(x)$ , the discriminant of  $f(X, Y)$  with respect to  $Y$ , as otherwise we again have a very good upper

bound for  $h_x(Q)$ . Hence by Proposition 2.9, for an appropriate choice of  $(x(Q))^{\frac{1}{e_P}}$  (possibly other than before) we have

$$z(Q) = \sum_{s=0}^{\infty} \gamma_s(P) (x(Q))^{-\frac{s}{e_P}}. \quad (8)$$

Note that since  $P \notin \text{supp}(z)$ , we start the summation from  $\text{Ord}_P(z) = 0$ . We have  $\gamma = \gamma_0(P) \neq 0$ , and

$$h(\gamma) \leq \text{nor}\{c'_P(v)\} \leq 370\Lambda^{11}(h + 12 \ln \Lambda). \quad (9)$$

Denote  $\mu = \gamma^{-1}z(Q)$ . Let  $\theta_1, \dots, \theta_{\sigma-1}$  be the independent  $S$ -units, defined in Section 4, and  $U$  – the multiplicative group generated by  $\theta_1, \dots, \theta_{\sigma-1}$ . By Proposition 4.6 there exists  $\theta \in U$  such that  $\mu_0 = \mu\theta^{-1}$  satisfies

$$\frac{1}{d} \sum_{\substack{v \in S \\ v \neq v_0}} d(v) |\ln |\mu_0|_v| \leq \xi^{\sigma-1} \sigma! R(S), \quad (10)$$

where  $v_0$  is a fixed valuation from  $S$ ,  $\xi$  is from (4.3), and  $R(S) = R_{\mathbf{K}}(S)$  is the  $S$ -regulator, defined in Section 4.

On the other hand, by (3.10) and (3.11) we have

$$\begin{aligned} \frac{1}{d} \sum_{v \notin S} d(v) |\ln |\mu_0|_v| &= \frac{1}{d} \sum_{v \notin S} d(v) |\ln |\mu|_v| \leq h(\gamma) + \frac{1}{d} \sum_{v \notin S} d(v) |\ln |z(Q)|_v| \leq \\ &\leq h(\gamma) + \text{nor}\{q(v)\} \leq 2227\Lambda^{17}(h + 15 \ln \Lambda). \end{aligned} \quad (11)$$

By the Product formula

$$\frac{d(v_0)}{d} |\ln |\mu_0|_{v_0}| \leq \frac{1}{d} \sum_{v \neq v_0} d(v) |\ln |\mu_0|_v|. \quad (12)$$

Combining (10)-(12), we get

$$\begin{aligned} h(\mu_0) &= \frac{1}{2d} \sum_v d(v) |\ln |\mu_0|_v| \leq \frac{1}{d} \sum_{v \neq v_0} d(v) |\ln |\mu_0|_v| \leq \\ &\leq \xi^{\sigma-1} \sigma! R(S) + 2227\Lambda^{17}(h + 15 \ln \Lambda). \end{aligned} \quad (13)$$

We have also

$$|h(\theta) - h_z(Q)| \leq h(\gamma) + h(\mu_0). \quad (14)$$

Write  $\theta = \theta_1^{b_1} \dots \theta_{\sigma-1}^{b_{\sigma-1}}$ , and let  $B = \max\{|b_1|, \dots, |b_{\sigma-1}|\}$ . Then, combining (9), (13), (14), (3.8), (3.9) and Proposition 4.7, we get

$$B \leq T(h_x(Q) + W), \quad (15)$$

$$h_x(Q) \leq T(B + W)R(S), \quad (16)$$

where  $T = 2^{16\sigma}\sigma^{4\sigma}\Lambda^{18}$  and  $W = h + R(S)$ .

On the other hand, (6), (9), (2.17) and (2) imply that

$$\begin{aligned} \left| \mu_0 \theta_1^{b_1} \cdots \theta_{\sigma-1}^{b_{\sigma-1}} - 1 \right|_w &= \left| \gamma^{-1} \sum_{s=1}^{\infty} \gamma_s(P) (x(Q))^{-\frac{s}{e_P}} \right|_w \leq \\ &\leq \frac{|\gamma^{-1}|_w e^{c'_P(w)+c_P(w)} |X(Q)|_w^{-\frac{1}{e_P}}}{1 - e^{c_P(w)} |X(Q)|_w^{-\frac{1}{e_P}}} \leq \\ &\leq \frac{e^{2d \text{nor}\{c'_P(v)\} + d \text{nor}\{c_P(v)\}}}{1 - e^{-1}} |X(Q)|_w^{-\frac{1}{e_P}} \leq \\ &\leq \exp \left( 741\Lambda^{11}d(h + 13 \ln \Lambda) - \frac{\ln |x(Q)|_w}{e_P} \right) \leq \\ &\leq \exp \left( d \left( 741\Lambda^{11}(h + 13 \ln \Lambda) - \frac{h_x(Q)}{\sigma n} \right) \right) \leq \\ &\leq \exp \left( d \left( W' - \frac{B}{T\sigma n} \right) \right), \end{aligned}$$

where  $W' = 742\Lambda^{11}(h + 13 \ln \Lambda) + R(S)$ .

If  $B \leq 2T\sigma nW'$ , then  $h_x(Q) \leq 3T^2\sigma nW'R(S)$ . Combining this with (4.10), we get a better result than (1.10) and (1.11). Hence assume that  $B > 2T\sigma nW'$ . Then

$$\left| \mu_0 \theta_1^{b_1} \cdots \theta_{\sigma-1}^{b_{\sigma-1}} - 1 \right|_w < e^{-\frac{dB}{2T\sigma n}}. \quad (17)$$

If the left-hand side of (17) vanishes, then  $z(Q) = \gamma$ , which also implies an inequality better than (1.10) and (1.11). Hence we may assume that the left-hand side of (7) is non-zero. This allows us to use

linear forms in logarithms.

If  $w$  is non-Archimedean, we get by Propositions 5.5, 4.5 and inequality (13), that

$$B \leq c_{61}(\sigma)p^{d'}(\ln \ln p)\Lambda^{19}(h + R(S))R(S) \ln^2(1 + R(S)), \quad (18)$$

where  $c_{61}(\sigma) = 2^{76\sigma+107}\sigma^{15\sigma+19}$ .

If  $w$  is Archimedean, then by Propositions 5.3, 4.5 and inequality (13) we have

$$B \leq c_{62}(\sigma)\Lambda^{19}(h + R(S))R(S) \ln(1 + R(S)), \quad (19)$$

$c_{62}$  being effectively computable.

If  $w$  is Archimedean, we may also use Proposition 5.2, and to get

$$B \leq c_{61}(\sigma)\Lambda^{19}(h + R(S))R(S) \ln(h + R(S)). \quad (20)$$

Now, combining (18) or (20) with (16) and (4.10), we obtain (1.10). Replacing in the previous sentence (20) by (19), we get (1.11). This completes the proof of Theorem 1A.

## 7 Proof of Theorem 1B.

Let  $\Sigma'$  be a  $(|\Sigma| - \rho + 2)$ -element subset of  $\Sigma$ . Then  $\rho(\Sigma') \geq 2$  and  $d_0(\Sigma') = d_{\rho-2}(\Sigma)$ . Now use Theorem 1A with  $\Sigma$ ,  $\mathbf{K}$  and  $S$  replaced by  $\Sigma'$ ,  $\tilde{\mathbf{K}} = \mathbf{K}(\Sigma')$  and  $\tilde{S}$ , respectively. Here  $\tilde{S}$  is the set of valuations of  $\tilde{\mathbf{K}}$  lying above the valuations from  $S$ . By (1.10) we have

$$h_x(Q) \leq c_{11}(\tilde{\sigma})(\max(\Lambda, N))^{37} (h + \tilde{D}) \tilde{D}^2 \tilde{\eta}, \quad (1)$$

where

$$\tilde{\sigma} = |\tilde{S}|, \quad (2)$$

$$\tilde{D} = \sqrt{\tilde{D}} (\ln \tilde{D}')^{\tilde{d}} \prod_{v \in \tilde{S} \setminus \tilde{S}_\infty} \ln N_{\tilde{\mathbf{K}}}(v), \quad (3)$$

$$\tilde{\eta} = \max(\ln h, p^{\tilde{d}'} (\ln \ln p)^3), \quad (4)$$

$$\tilde{d} = d_{\tilde{\mathbf{K}}}, \quad \tilde{d}' = \max(\tilde{d}, 2), \quad (5)$$

$$\tilde{D} = D_{\tilde{\mathbf{K}}}, \quad \tilde{D}' = \max(\tilde{D}, e), \quad (6)$$

and  $\tilde{S}_\infty$  – the set of Archimedean valuations of  $\tilde{\mathbf{K}}$ .

Clearly,  $\tilde{\sigma} \leq \sigma d_0(\Sigma')$ , hence

$$c_{11}(\sigma) \leq c(N) (\sigma^{20\sigma})^{d_0(\Sigma')}. \quad (7)$$

Further,  $\tilde{d} = d d_0(\Sigma')$ , and by Proposition 2.7

$$\tilde{D} \leq \tilde{D}' \leq c(N, d) D^{d_0(\Sigma')} e^{2^{24} N^{14+|\Sigma'|} d h}. \quad (8)$$

Therefore

$$\begin{aligned} \tilde{D} &\leq c(N, d) \left( \sqrt{\tilde{D}} (\ln \tilde{D} + h)^d \prod_{v \in \tilde{S} \setminus \tilde{S}_\infty} \ln N_{\tilde{\mathbf{K}}}(v) \right)^{d_0(\Sigma')} e^{2^{23} N^{14+|\Sigma'|} d h} \leq \\ &\leq c(N, d, \varepsilon) \left( \sqrt{\tilde{D}} \prod_{v \in \tilde{S} \setminus \tilde{S}_\infty} \ln N_{\tilde{\mathbf{K}}}(v) \right)^{d_0(\Sigma')+\varepsilon} e^{2^{24} N^{16+|\Sigma|-\rho} d h}. \end{aligned} \quad (9)$$

Further, we may assume that  $\tilde{\mathbf{K}} \neq \mathbf{Q}$ , because if  $\tilde{\mathbf{K}} = \mathbf{Q}$  then (1.10) holds. Hence  $\tilde{d}' = \tilde{d}$ , and we have

$$\tilde{\eta} \leq \max(\ln h, p^{d d_0(\Sigma)} (\ln \ln p)^3) \leq \max(\ln h, c(N, \varepsilon) p^{d(d_0(\Sigma)+\varepsilon)}). \quad (10)$$

Substituting (7), (9), and (10) in (1), we obtain

$$h_x(Q) \leq c(N, d, \varepsilon) \Lambda^{37} \left( \sigma^{20\sigma} D^{\frac{3}{2}} p^d \prod_{v \in \tilde{S} \setminus \tilde{S}_\infty} \ln^3 N_{\tilde{\mathbf{K}}}(v) \right)^{d_{\rho-2}(\Sigma)+\varepsilon} e^{(4N)^{16+|\Sigma|-\rho} d h}. \quad (11)$$

Since  $d_{\rho-2}(\Sigma) \leq n(n-1) \dots (n-|\Sigma|+\rho-1)$  by Proposition 2.7, the proof is complete.

# Chapter 2

## Bounds for isolated solutions of systems of algebraic equations

### 1 Introduction

Let  $\mathbf{K}$  be an algebraic number field,  $X = (X_1, \dots, X_m)$ ,  $f_1, \dots, f_k \in \mathbf{K}[X]$ ,

$$\max_{1 \leq i \leq k} \deg f_i \leq n, \quad \max_{1 \leq i \leq k} h(f_i) \leq h. \quad (1)$$

**Theorem 2A.** *Let  $A$  be a Zariski-closed subset of  $\bar{\mathbf{Q}}^m$ , defined by*

$$f_i(X) = 0 \quad (1 \leq i \leq k), \quad (2)$$

*and  $B$  – another Zariski-closed subset of  $\bar{\mathbf{Q}}^m$ . Assume that the set  $A \setminus B$  is finite. Then for any  $\alpha \in A \setminus B$  we have*

- (i)  $[\mathbf{K}(\alpha) : \mathbf{K}] \leq n^m$ ;
- (ii)  $h(\alpha) \leq c_{11}(n, m)h + c_{12}(n, m)$ , where  $c_{11}(n, m) = (2n)^{4m^2}$  and  $c_{12}(n, m)$  is effectively computable.

(Here  $h(\alpha)$  is the affine height of  $\alpha$ .)

Instead of Theorem 2A, we shall prove an equivalent Theorem 2B, formulated below.

Let  $X = (X_0, \dots, X_m)$ , and assume that  $f_1, \dots, f_k \in \mathbf{K}[X]$  are homogeneous in  $X$ .

**Theorem 2B.** *Assume that  $\alpha \in \mathbf{P}^m(\bar{\mathbf{Q}})$  is a zero-dimensional component of the Zariski-closed set defined by (2). Then we have (i), (ii) of Theorem 2A (now with projective height instead of affine height).*

By *component* we always mean a  $\bar{\mathbf{Q}}$ -irreducible component.

It is clear that each of the two theorems immediately follows from the other.

It will be convenient to use the following

**Definition 1.** Let  $A \subseteq \mathbf{P}^m$  be a Zariski-closed set, and assume that  $A$  may be defined ( set-theoretically !) by the system of polynomial equations (2), where the polynomials  $f_1, \dots, f_k$  satisfy (1). Then  $A$  is called an  $(n, h)$ -closed set.

The system of polynomial equations (2) is then an  $(n, h)$ -system.

## 2 A projection.

For  $\alpha, \beta \in \mathbf{P}^m$  denote by  $l(\alpha, \beta)$  the line passing through  $\alpha$  and  $\beta$ .

**Proposition 1.** *Let  $A$  be  $(n, h)$ -closed, and  $\beta = (\beta_0 : \dots : \beta_m) \in \mathbf{P}^m(\bar{\mathbf{Q}})$  satisfy  $\beta \notin A$  and  $\beta_m \neq 0$ . Denote*

$$\begin{aligned} \varphi_\beta : \mathbf{P}^m \setminus \{\beta\} &\longrightarrow \mathbf{P}^{m-1}, \\ x &\longrightarrow l(\beta, x) \cap \mathbf{P}^{m-1}, \end{aligned}$$

where we identify  $\mathbf{P}^{m-1}$  with the hyperplane  $X_m = 0$ . Then  $\varphi_\beta(A)$  is  $(n_0, h_0)$ -closed, where

$$\begin{aligned} n_0 &= 2^m n^{2^m - 1}, \\ h_0 &\leq n_0 h + c(n, m)(h(\beta) + 1). \end{aligned}$$

**Proof.** Define  $\psi : \mathbf{P}^m \rightarrow \mathbf{P}^m$  by

$$\psi(x_0 : \dots : x_m) = (\beta_m x_0 - \beta_0 x_m : \dots : \beta_m x_{m-1} - \beta_{m-1} x_m : \beta_m x_m).$$

Then  $\gamma = \psi(\beta) = (0 : \dots : 0 : 1)$ , and  $\varphi_\beta = \psi^{-1} \circ \varphi_\gamma \circ \psi$ .

Clearly,  $B = \psi(A)$  is  $(n, h_1)$ -closed, where

$$h_1 \leq h + c(n, m)(h(\beta) + 1).$$

Let

$$f_i(X) = 0 \quad (i = 1, \dots, k)$$

be an  $(n, h_1)$ -system of polynomial equations, defining  $B$ . Denote  $Y = (Y_0, \dots, Y_{m-1})$ , and  $\delta_{p,q}(X, Y) = X_p Y_q - X_q Y_p$ .

Note that

$$\varphi_\gamma(x_0 : \dots : x_m) = (x_0 : \dots : x_{m-1}).$$

Since  $\gamma \notin B$ , the point  $y = (y_0 : \dots : y_{m-1}) \in \mathbf{P}^{m-1}$  belongs to  $\varphi_\gamma(B)$  if and only if the system of polynomial equations

$$f_i(X) = 0 \quad (i = 1, \dots, k),$$

$$\Delta_{pq}(X, y) = 0 \quad (0 \leq p < q \leq m - 1)$$

has a solution  $x = (x_0 : \dots : x_m)$ .

Let  $g_1(Y), \dots, g_\nu(Y)$  be a resultant system for the polynomials  $f_i(X)$ ,  $\Delta_{pq}(X, Y)$ , as defined in [Schm76, p.179]. Then  $\varphi_\gamma(B)$  is defined by the system of polynomial equations

$$g_i(Y) = 0 \quad (1 \leq i \leq \nu).$$

By Theorems 1A and 1D from [Schm76, ChV] we may assume that the following conditions hold :

$$\begin{aligned} \max_{1 \leq i \leq \nu} \deg g_i &\leq 2^m n^{2^m - 1} = n_0, \\ h_2 = \max_{1 \leq i \leq \nu} h(g_i) &\leq n_0 h_1 + c(n, m) \leq n_0 h + c(n, m)(h(\beta) + 1). \end{aligned}$$

Hence,  $\varphi_\gamma(B)$  is  $(n_0, h_2)$ -closed. Therefore  $\varphi_\beta(A) = \psi^{-1} \circ \varphi_\gamma(B)$  is  $(n_0, h_0)$ -closed, where

$$h_0 \leq h_2 + c(n, m)(h(\beta) + 1) \leq n_0 h + c(n, m)(h(\beta) + 1),$$

q.e.d.

### 3 A construction of a small point in general position.

**Proposition 1.** *Let  $f$  be a non-zero polynomial in  $X_0, \dots, X_m$  over a field of characteristic zero. Denote  $n = \deg f$ . Then there exist  $\beta_0, \dots, \beta_m \in \mathbf{Z} \setminus \{0\}$  such that  $\max_{0 \leq i \leq m} |\beta_i| \leq \frac{n}{2} + 1$  and  $f(\beta_0, \dots, \beta_m) \neq 0$ .*

**Proof.** Simple induction in  $m$ .

**Proposition 2.** *Let  $A$  be a closed set in  $\mathbf{P}^m$  defined by a system of polynomial equations of degree  $\leq n$ . Assume that  $\dim A \leq m - 2$  and let  $\alpha \in A$ . Then there exists  $\beta \in \mathbf{P}^m(\mathbf{Q})$ ,  $\beta \neq \alpha$ , such that  $h(\beta) \leq \ln(n^2 + 1)$  and  $l(\alpha, \beta) \cap A = \{\alpha\}$  (in particular,  $\beta \notin A$ ).*

**Proof.** Among the polynomials of degree  $\leq n$ , defining  $A$ , there are two (say,  $f_1, f_2$ ) such that the algebraic set  $f_1(X) = f_2(X) = 0$  is of dimension  $m - 2$ . Fix a coordinate vector for  $\alpha$  and denote

$$g_i(T_0, T_1, X) = f_i(\alpha T_0 + XT_1) \quad (i = 1, 2).$$

Note that  $g_i \not\equiv 0$ , because  $g_i(0, 1, X) = f_i(X)$ .

Let  $g_i = T_1^{\sigma_i} \tilde{g}_i$ , where  $\tilde{g}_i(1, 0, X) \not\equiv 0$ , and let  $R(X)$  be the resultant of  $\tilde{g}_1, \tilde{g}_2$  with respect to  $(T_0, T_1)$ . We have  $\deg R \leq 2n^2$ .

For any  $x \in \mathbf{P}^m$ , if  $l(\alpha, x) \cap A$  contains a point  $\gamma \neq \alpha$ , then  $R(x) = 0$ . Hence, taking  $\beta \in \mathbf{P}^m(\mathbf{Q})$  which satisfies

$$h(\beta) \leq \ln \left( \frac{\deg R}{2} + 1 \right) \leq \ln(n^2 + 1)$$

and  $R(\beta) \neq 0$  (which is possible by Proposition 1), we obtain  $\beta$  as desired.

## 4 A bound for the number of components.

The *degree*  $\deg V$  of an irreducible projective variety  $V$  of dimension  $d$  is the number  $|L \cap V|$ , where  $L$  is the generic hyperplane of codimension  $d$ . The same definition is valid when  $V$  is reducible, but all its components are of the same dimension.

For any closed set  $A \subseteq \mathbf{P}^m$  denote

$$\delta(A, T) = \sum_V (\deg V) T^{\dim V}, \quad (1)$$

the sum being taken over the set of irreducible components of  $A$ . Note that

$$\delta(\cup A_i, T) = \sum \delta(A_i, T) \quad (2)$$

provided  $A_i$  and  $A_j$  have no common components when  $i \neq j$ .

**Proposition 1** *Let  $A$  be a closed set and  $f(X)$  be a polynomial of degree  $n$ . Then*

$$\delta(A \cap V_f, n) \leq \delta(A, n), \quad (3)$$

where  $V_f$  is defined by  $f(X) = 0$ .

**Proof.** Take first an irreducible  $V$ . Consider two cases:

(i)  $V \subseteq V_f$ . Then

$$\delta(V \cap V_f, n) = \delta(V, n). \quad (4)$$

(ii)  $V \not\subseteq V_f$ . Then all components of  $V \cap V_f$  are of the same dimension, equal to  $\dim V - 1$ . We get

$$\delta(V \cap V_f, n) = \deg(V \cap V_f) n^{\dim V - 1} \leq n \cdot \deg V \cdot n^{\dim V - 1} = \delta(V, n), \quad (5)$$

where the inequality follows from Bezout theorem.

Thus, for irreducible  $V$

$$\delta(V \cap V_f, n) \leq \delta(V, n). \quad (6)$$

In the general case (2) and (6) yield

$$\delta(A \cap V_f, n) = \sum_V \delta(V \cap V_f, n) \leq \sum_V \delta(V, n) = \delta(A, n),$$

where the sum is over the components of  $A$ . This proves the proposition.

Since  $\delta(\mathbf{P}^m, n) = n^m$ , we get immediately the following

**Corollary 2.** *Let  $A$  be defined by a system of polynomial equations of degree  $\leq n$  with coefficients in  $\mathbf{K}$ . Then*

$$\delta(A, n) \leq n^m.$$

*In particular,  $A$  has at most  $n^m$  components, and each component is defined over a field  $\mathbf{L}$  with  $[\mathbf{L} : \mathbf{K}] \leq n^m$ .*

As a particular case of the last statement we get the proof of part (i) of Theorems 2A and 2B.

**Remark.** It is easy to see that if  $V$  is a component of dimension  $d$ , then  $V$  is defined over a field  $\mathbf{L}$  with  $[\mathbf{L} : \mathbf{K}] \leq n^{m-d}$ . We do not need this fact.

## 5 Proof of Theorem 2B.

Part (i) was already proved at the end of the previous section. Now prove (ii). We use induction in  $m$ . Assume that  $c_{12}(n, m - 1)$  is defined for all  $n \in \mathbf{N}$ . Replacing  $f_i$  by  $\frac{f_i}{\text{g.c.d.}(f_1, \dots, f_k)}$  (and  $h$  by  $h + mn$ , by Proposition 1.2.4), we may assume that  $\dim A \leq m - 2$ . Let  $\beta = (\beta_0 : \dots : \beta_m)$  be the point from Proposition 3.2, i.e.,  $h(\beta) \leq \ln(n^2 + 1)$  and  $l(\alpha, \beta) \cap A = \{\alpha\}$ . Without loss of generality  $\beta_m \neq 0$ , and we choose a coordinate vector for  $\beta$  so that  $\beta_m = 1$ .

Let  $\varphi_\beta$  be the map defined in Proposition 2.1. Then  $\gamma = \varphi_\beta(\alpha)$  is a zero-dimensional component of  $B = \varphi_\beta(A)$ . By Proposition 2.1,  $\varphi_\beta(A)$  is  $(n_0, h_0)$ -closed, where

$$\begin{aligned} n_0 &= 2^m n^{2^m - 1}, \\ h_0 &\leq n_0 h + c_{51}(n, m). \end{aligned}$$

By induction

$$\begin{aligned} h(\gamma) &\leq (2n_0)^{4^{(m-1)^2}} h_0 + c_{12}(n_0, m-1) \leq \\ &\leq (2n)^{4^{m^2}-2} h + c_{52}(n, m), \end{aligned}$$

with

$$c_{52}(n, m) = (2n_0)^{4^{(m-1)^2}} \cdot c_{51}(n, m) + c_{12}(n_0, m-1).$$

Note that  $\varphi_\beta(x) = (x_0 - \beta_0 x_m : \dots : x_{m-1} - \beta_{m-1} x_m)$ . We may choose a coordinate vector for  $\alpha$  so that one of the numbers

$$\gamma_i = \alpha_i - \beta_i \alpha_m \quad (0 \leq i \leq m-1)$$

will be 1. Define

$$g_i(Y_0, \dots, Y_{m-1}, X) = f_i(Y_0 + \beta_0 X, \dots, Y_{m-1} + \beta_{m-1} X, X).$$

Since  $\varphi_\beta^{-1}(\gamma)$  consists of only one point  $\alpha$ , for at least one  $i$  we have

$$p_i(X) = g_i(\gamma_0, \dots, \gamma_{m-1}, X) \neq 0.$$

Since one of the  $\gamma_j$ 's is 1, we have

$$\begin{aligned} h(p_i) &\leq nh(\gamma) + h(g_i) + c_{53}(n, m) \leq \\ &\leq nh(\gamma) + h + nh(\beta) + c_{54}(n, m) \leq \\ &\leq nh(\gamma) + h + c_{55}(n, m). \end{aligned}$$

Since  $p_i(\alpha_m) = f_i(\alpha_0, \dots, \alpha_m) = 0$ , we obtain

$$h(1 : \alpha_m) \leq h(p_i) + n \leq nh(\gamma) + h + c_{56}(n, m).$$

Finally,

$$\begin{aligned} h(\alpha) &= h((\gamma_0 + \beta_0 \alpha_m) : \dots : (\gamma_{m-1} + \beta_{m-1} \alpha_m) : \alpha_m) \leq \\ &\leq h(\gamma) + h(\beta) + h(1 : \alpha_m) + c_{57}(n, m) \leq \\ &\leq (n+1)h(\gamma) + h + c_{58}(n, m) \leq \\ &\leq (2n)^{4^{m^2}} h + c_{12}(n, m), \end{aligned}$$

with  $c_{12} = c_{52} + c_{58}$ .

# Chapter 3

## An effective version of Riemann existence theorem

### 1 Introduction

Let  $C$  be a non-singular algebraic curve over  $\bar{\mathbf{Q}}$ , and let  $x \in \bar{\mathbf{Q}}(C)$  be non-constant. We define  $x_\alpha$ ,  $e_P$  and  $x_P$  as in Chapter 1. Define:

$$\begin{aligned} n &= [\bar{\mathbf{Q}}(C) : \bar{\mathbf{Q}}(x)]; \\ M &= \{x(P) \mid P \in C(\bar{\mathbf{Q}}) \text{ and } e_P > 1\}; \\ \mu &= |M|; \quad h = \max_{\alpha \in M} h(\alpha). \end{aligned}$$

Note that

$$\mathbf{g} = \mathbf{g}(C) = 1 + \frac{1}{2} \sum_{P \in M} (e_P - 1) - n \leq \left(\frac{1}{2}\mu - 1\right)(n - 1).$$

Let  $\mathbf{K}$  be an algebraic number field, and suppose that  $M \setminus \{\infty\} \subseteq \mathbf{K}$ .

**Theorem 3A.** *There exists  $y \in \bar{\mathbf{Q}}(C)$  such that  $\bar{\mathbf{Q}}(C) = \bar{\mathbf{Q}}(x, y)$  and  $x, y$  satisfy an absolutely irreducible equation*

$$f(x, y) = 0$$

*with the following properties:*

(i)  $f(X, Y) \in \mathbf{L}(X, Y)$ , where

$$[\mathbf{L} : \mathbf{K}] \leq \exp(n^6 \mu^3), \tag{1}$$

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{L}/\mathbf{K}} \leq c_{11}(n, \mu)h + c(n, \mu), \tag{2}$$

with  $c_{11}(n, \mu) = \exp_2(2n^{11}\mu^5)$ .

- (ii)  $\deg_Y f(X, Y) = n$ .
- (iii)  $\deg_X f(X, Y) \leq \mathbf{g} + 1 \leq \frac{1}{2}n(\mu - 1)$ .
- (iv)  $h(f) \leq c_{11}(n, \mu)h + c(n, \mu)$ .

The proof presented here is influenced by [Zv85], [Zv87]. See also [FrV91] for a much deeper approach, oriented to applications in inverse Galois problem.

Sometimes it is known a priori that  $C$  is defined over a certain algebraic number field  $\mathbf{K}_0$  and  $x \in \mathbf{K}_0(C)$ . In this case we can choose  $y \in \mathbf{K}_0(C)$ .

**Theorem 3B.** *Let  $C$  be defined over an algebraic number field  $\mathbf{K}_0$ , and  $x \in \mathbf{K}_0(C)$ . Then there exists  $y_0 \in \mathbf{K}_0(C)$  such that  $\mathbf{K}_0(C) = \mathbf{K}_0(x, y_0)$  and  $x, y_0$  satisfy an irreducible equation  $f_0(x, y_0) = 0$  with the following properties:*

- (i)  $f_0(X, Y) \in \mathbf{K}_0(X, Y)$ ;
- (ii)  $\deg_Y f_0(X, Y) = n$ ;
- (iii)  $\deg_X f_0(X, Y) \leq n(\mathbf{g} + 1) \leq \frac{1}{2}n^2(\mu - 1)$ ;
- (iv)  $h(f_0) \leq c_{11}(n, \mu)h + c(n, \mu)$ .

I am thankful to S. Brodsky for a useful talk.

## 2 Some properties of algebraic power series.

Let  $f(X, Y) \in k[X, Y]$  be an irreducible polynomial over a field  $k$ ,  $m = \deg_X f(X, Y)$  and  $n = \deg_Y f(X, Y)$ .

**Proposition 1.** *Let*

$$y^{(i)} = \sum_{s=\delta_i}^{\infty} \beta_{is} x_\alpha^{s/e_i} \quad (i = 1, 2)$$

*be two distinct power series, satisfying*

$$f(x, y^{(i)}) = 0 \quad (i = 1, 2).$$

*Then*

$$\text{Ord}_\alpha(y^{(1)} - y^{(2)}) \leq (3n - 4)m.$$

*In other words, there exist  $s_1, s_2$  such that*

$$\frac{s_1}{e_1} = \frac{s_2}{e_2} \leq (3n - 4)m, \quad \beta_{1s_1} \neq \beta_{2s_2}.$$

**Proof.** Let  $y^{(1)}, \dots, y^{(n)}$  be all distinct roots of  $f(x, Y)$  in the field of fractional power series in  $x_\alpha$ , and  $r(X)$  – the resultant of  $f(X, Y)$  and  $\frac{\partial f}{\partial Y}(X, Y)$  with respect to  $Y$ . We have

$$\text{Ord}_\alpha(y^{(i)}) \geq -\text{Ord}_\alpha f_n(x) \quad (1 \leq i \leq n),$$

where we put  $f(X, Y) = f_n(X)Y^n + \dots + f_0(X)$ .

On the other hand,

$$a(X)f(X, Y) + b(X)\frac{\partial f}{\partial Y}(X, Y) = r(X)$$

for some polynomials  $a(X), b(X)$ , whence

$$\text{Ord}_\alpha \frac{\partial f}{\partial Y}(x, y^{(i)}) \leq \text{Ord}_\alpha r(x) \leq \deg r(X) = (2n - 1)m.$$

Since

$$\frac{\partial f}{\partial Y}(x, y^{(1)}) = f_n(x)(y^{(1)} - y^{(2)}) \dots (y^{(1)} - y^{(n)}),$$

we obtain

$$\text{Ord}_\alpha(y^{(1)} - y^{(2)}) \leq (2n - 1)m + (n - 2)\text{Ord}_\alpha f_n(x) - \text{Ord}_\alpha f_n(x) \leq (3n - 4)m,$$

q.e.d.

**Corollary 2.** Let  $C, x, y$  and  $f(X, Y)$  be as in Section 1.1, and

$$y^{(P)} = \sum_{s=-\text{Ord}_P(y)}^{\infty} \beta_s(P)x_P^s$$

the Puiseux expansion of  $y$  at  $P$ . Then for any prime  $q|e_P$  there exists  $s \leq (3n-4)e_{PM}$  such that  $\beta_s \neq 0$  and  $s \not\equiv 0 \pmod{q}$ .

**Proof.** Use Proposition 1 for the series  $y^{(P,0)}$  and  $y^{(P,q)}$ , as defined in Section 1.1.

We say that

$$y_k = \sum_{s=-\delta}^k \beta_s x_\alpha^{\frac{s}{e}}$$

is a *beginning* of an algebraic power series  $y$  if

$$\text{Ord}_\alpha(y - y_k) > \frac{k}{e}. \quad (1)$$

**Proposition 3.** Let

$$k > (3n - 2)me. \quad (2)$$

Then the following conditions are equivalent.

(i)  $y_k$  is a beginning of a power series  $y$ , satisfying  $f(x, y) = 0$ .

(ii)

$$\text{Ord}_\alpha f(x, y_k) > \frac{k}{e} + \text{Ord}_\alpha \frac{\partial f}{\partial Y}(x, y_k). \quad (3)$$

**Proof.** (i)  $\implies$  (ii). As we have already seen in the proof of Proposition 1,

$$\text{Ord}_\alpha(y) \geq -m, \quad (4)$$

$$\text{Ord}_\alpha \left( \frac{\partial f}{\partial Y}(x, y) \right) \leq (2n - 1)m. \quad (5)$$

From (1), (2), (4), (5) and Taylor's formula

$$\frac{\partial f}{\partial Y}(x, y_k) = \frac{\partial f}{\partial Y}(x, y) + \frac{1}{2} \frac{\partial^2 f}{\partial Y^2}(x, y)(y_k - y) + \dots$$

we deduce that

$$\text{Ord}_\alpha \left( \frac{\partial f}{\partial Y}(x, y_k) \right) = \text{Ord}_\alpha \left( \frac{\partial f}{\partial Y}(x, y) \right) \leq (2n - 1)m.$$

Hence by another Taylor's formula

$$0 = f(x, y) = f(x, y_k) + \frac{\partial f}{\partial Y}(x, y_k)(y - y_k) + \dots$$

we get (3).

(ii)  $\implies$  (i). Let  $r(X)$  be as in the proof of Proposition 1. Then

$$\text{Ord}_\alpha f(x, y_k) > (3n - 2)m - (n - 1)m = (2n - 1)m \geq \text{Ord}_\alpha r(x).$$

Hence

$$\text{Ord}_\alpha \left( \frac{\partial f}{\partial Y}(x, y_k) \right) \leq (2n - 1)m. \quad (6)$$

(3) and (6) yield that

$$\text{Ord}_\alpha \left( \frac{\partial f}{\partial Y}(x, y_k) \right) < \frac{1}{2} \text{Ord}_\alpha f(x, y_k).$$

Therefore, by Hensel's lemma [CF67, Ch.II, App.B] there exists a root  $y$  of  $f(x, Y)$  in the field of formal power series  $\bar{\mathbf{Q}} \left( \left( x^{\frac{1}{e}} \right) \right)$  such that

$$\text{Ord}_\alpha(y - y_k) \geq \text{Ord}_\alpha f(x, y_k) - \text{Ord}_\alpha \left( \frac{\partial f}{\partial Y}(x, y_k) \right) > \frac{k}{e},$$

q.e.d.

**Proposition 4.** *Let  $C$  be an algebraic curve defined over a field  $k$  of characteristic 0, and  $x \in k(C)$  be non-constant. Assume that  $y \in \bar{k}(C)$  satisfies the following conditions:*

- (i)  *$y$  has a unique pole  $P$ , and  $P$  is unramified over  $\bar{k}(x)$ ;*
- (ii) *the Puiseux expansion of  $y$  at  $P$  is of the form*

$$y^{(P)} = x_\alpha^{-m} + \sum_{s=-m+1}^{\infty} \beta_s x_\alpha^s,$$

where  $\alpha = x(P)$ .

Let  $y \in K(C)$ , where  $K$  is a finite extension of  $k$ . Then  $k(C) = k(x, y_0)$ , where  $y_0 = \text{Tr}_{K/k}(y)$ .

**Proof.** Clearly,  $k(P) \subseteq K$ . Replacing  $y$  by  $\frac{1}{[K : k(P)]} \text{Tr}_{K/k(P)}(y)$ , we may assume that  $K = k(P) = k(\beta_i \mid i \geq -m + 1)$ . Let

$$\{P_1, \dots, P_s\} = \text{supp}(x_\alpha)_0,$$

and assume that  $P_1 = P$ ,  $P_2, \dots, P_r$  are the points conjugate to  $P$  over  $k$ . Then  $y_0$  has a pole of order  $m$  at each of the points  $P_1, \dots, P_r$  and has pairwise distinct Puiseux expansions at these points, because the coefficients  $\beta_i$  generate  $K$  over  $k$ . Further,  $y_0$  has no poles among  $P_{r+1}, \dots, P_s$ . We see that the Puiseux expansion of  $y_0$  at  $P$  does not coincide with any of expansions at  $P_2, \dots, P_s$ . Hence  $y_0$  generates  $k(C)$  over  $k(x)$ , q.e.d.

### 3 Proof of Theorem 3A.

Without loss of generality, we may assume that  $C$  is unramified over  $\infty$ . Indeed, there exists  $b \in \mathbf{Z}$  such that  $|b| \leq \frac{1}{2}\mu + 1$  and  $b \notin M$ . Replacing  $x$  by  $\frac{1}{x-b}$ , we get the desired situation.

When  $n = 1$  we may take  $y = x$ , and when  $n = 2$  we may take

$$y = \sqrt{\prod_{\alpha \in M} (x - \alpha)}.$$

Hence assume further that  $n \geq 3$ .

Let  $P$  be a fixed pole of  $x$ . Define  $m$  through the conditions

$$\begin{aligned} \dim \mathcal{L}(mP) &= 2, \\ \dim \mathcal{L}((m-1)P) &= 1. \end{aligned} \quad (1)$$

In particular,

$$m \leq \mathbf{g} + 1 \leq \frac{1}{2}n(\mu - 1). \quad (2)$$

There exists a uniquely defined  $y \in \mathbf{Q}(C)$  such that the Puiseux expansion of  $y$  at  $P$  looks as

$$y^{(P)} = x^m + \text{terms of lower degree in } x,$$

and  $y$  has no other poles except  $P$ .

It is clear that  $\bar{\mathbf{Q}}(C) = \bar{\mathbf{Q}}(x, y)$ . Let  $f(x, y) = 0$  be an irreducible algebraic equation for  $x, y$ . Then

$$f(X, Y) = Y^n + f_{n-1}(X)Y^{n-1} + \dots + f_0(X), \quad (3)$$

where  $\deg f_j(X) \leq m$  ( $0 \leq j \leq n-1$ ). So, we have (ii) and (iii), and it remains to prove (i) and (iv).

Denote

$$f(X, Y) = Y^n + \sum_{j=0}^{n-1} \sum_{i=0}^m \theta_{ij} X^i Y^j. \quad (4)$$

Let  $d(X)$  be the discriminant of  $f(X, Y)$  with respect to  $Y$ . Then

$$d(X) = \gamma \prod_{i=1}^{\nu-1} (X - \alpha_i)^{\sigma_i}, \quad (5)$$

where  $\gamma \in \bar{\mathbf{Q}}$ ,  $\sigma_i > 0$ ,

$$\alpha_i \neq \alpha_j \quad (1 \leq i < j \leq \nu - 1), \quad (6)$$

$\nu - 1 \geq \mu$  and  $M = \{\alpha_1, \dots, \alpha_\mu\}$ . Denote also  $\alpha_\nu = \infty$ .

For each  $i = 1, \dots, \nu$  we have  $n$  distinct power series

$$y^{(i,j)} = \sum_{s=-\delta_{ij}}^{\infty} \beta_{ijs} x^{\frac{s}{e_{ij}}} \quad (1 \leq j \leq n), \quad (7)$$

such that

$$f(x, Y) = \prod_{j=1}^n (Y - y^{(i,j)}). \quad (8)$$

Here

$$\delta_{ij} = \begin{cases} m, & i = \nu \text{ and } j = n \\ 0, & \text{otherwise,} \end{cases}$$

and  $e_{ij}$  have minimal possible values. In particular,  $e_{ij} \leq n$ , and  $e_{ij} = 1$  for  $i \geq \mu$ .

Put  $\kappa = (3n - 2)nm$ , and consider

$$\varphi = (\gamma, \theta, \alpha, \beta) \in \bar{\mathbf{Q}} \times \bar{\mathbf{Q}}^{n(m+1)} \times \bar{\mathbf{Q}}^{\nu-1} \times \bar{\mathbf{Q}}^{\nu \cdot n(\kappa+1)+m},$$

defined as follows:

$$\theta = (\dots, \theta_{ij}, \dots)_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n-1}}, \quad (9)$$

$$\alpha = (\alpha_1, \dots, \alpha_{\nu-1}), \quad (10)$$

$$\beta = (\dots, \beta_{ijs}, \dots)_{\substack{1 \leq i \leq \nu \\ 1 \leq j \leq n \\ -\delta_{ij} \leq s \leq \kappa}}. \quad (11)$$

We shall define two Zariski-closed subsets  $V, W$  of  $\bar{\mathbf{Q}}^{m_1}$ , where

$$m_1 = 1 + n(m+1) + \nu - 1 + \nu n(\kappa+1) + m,$$

such that  $\varphi \in V \setminus W$ . Then we shall prove that the set  $V \setminus W$  is finite. This will enable us to estimate  $[\mathbf{L} : \mathbf{K}]$  and  $h(f)$  with the help of Theorem 2.

By  $\Phi = (\Gamma, \Theta, A, B)$  we denote an indeterminant vector such that  $\Gamma$  is a scalar indeterminant, and

$$\Theta = (\dots, \Theta_{ij}, \dots)_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n-1}},$$

$$A = (A_1, \dots, A_{\nu-1}),$$

$$B = (\dots, B_{ijs}, \dots)_{\substack{1 \leq i \leq \nu \\ 1 \leq j \leq n \\ -\delta_{ij} \leq s \leq \kappa}}.$$

We put  $V = V_1 \cap V_2 \cap V_3 \cap V_4$ , and below we describe each of these sets.

$V_1$  is defined by

$$A_i = \alpha_i \quad (1 \leq i \leq \mu). \quad (V_1)$$

$V_2$  is defined by

$$D(X) = \Gamma \prod_{i=1}^{\nu-1} (X - A_i)^{\sigma_i}, \quad (V_2)$$

where  $D(X)$  is the discriminant with respect to  $Y$  of the polynomial

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

Denote

$$Y_{\kappa}^{(i,j)} = \sum_{s=-\delta_{ij}}^{\kappa} B_{ijs} (X - A_i)^{\frac{s}{e_{ij}}} \quad (1 \leq i \leq \nu, 1 \leq j \leq n),$$

where  $e_{ij}$  come from (8), and for  $i = \nu$  one should replace  $X - A_i$  by  $X^{-1}$ . Then  $V_3$  is defined by

$$\text{Ord}_{A_i} [F(X, Y_{\kappa}^{(i,j)})] > \frac{\kappa}{e_{ij}} + \text{Ord}_{A_i} \left[ \frac{\partial F}{\partial Y} (X, Y_{\kappa}^{(i,j)}) \right] \quad (1 \leq i \leq \nu, 1 \leq j \leq n) \quad (V_3)$$

(for  $i = \nu$  replace  $\text{Ord}_{A_i}$  by  $\text{Ord}_\infty$ ).

Finally,  $V_4$  is defined by

$$B_{\nu;n;-m} = 1. \quad (V_4)$$

Now define  $W$ . We put

$$W = W_1 \cup W_2 \cup W_3, \quad (12)$$

where

$$W_1 = \bigcup_{\substack{1 \leq i \leq \nu \\ 1 \leq j_1 < j_2 \leq n}} W_1(i, j_1, j_2), \quad (13)$$

$$W_3 = \bigcup_{1 \leq k \leq m-1} W_3(k). \quad (14)$$

Below we describe each of the sets occurring in (12)–(14).

Let  $1 \leq i \leq \nu$ , and  $1 \leq j_1 < j_2 \leq n$ . Then  $W_1(i, j_1, j_2)$  is defined by

$$\text{Ord}_{A_i} \left( Y_\kappa^{(i,j_1)} - Y_\kappa^{(i,j_2)} \right) > (3n - 4)m \quad (W_1(i, j_1, j_2))$$

(replace  $A_i$  by  $\infty$  for  $i = \nu$ ).

For  $W_2$  we need the following wellknown fact.

*There exist polynomials  $p_1(\Theta), \dots, p_\rho(\Theta)$  with the following property. For any specialization  $\tilde{\theta}$  of  $\Theta$ , the polynomial*

$$\tilde{f}(X, Y) = Y^n + \sum_{j=0}^{n-1} \sum_{i=0}^m \tilde{\theta}_{ij} X^i Y^j \quad (15)$$

*is reducible (over the algebraic closure of the field, generated by its coefficients) if and only if*

$$p_i(\tilde{\theta}) = 0 \quad (1 \leq i \leq \rho). \quad (16)$$

Then  $W_2$  is defined by

$$p_i(\Theta) = 0 \quad (1 \leq i \leq \rho). \quad (W_2)$$

A specialization  $\tilde{\varphi} = (\tilde{\gamma}, \tilde{\theta}, \tilde{\alpha}, \tilde{\beta})$  of  $\Phi$  is called *suitable* if  $\tilde{\varphi} \in (V_2 \cap V_3) \setminus (W_1 \cup W_2)$ . Fix a suitable specialization  $\tilde{\varphi}$  and define  $\tilde{f}$  as in (15). Let

$$\tilde{y}_\kappa^{(i,j)} = \sum_{s=\delta_{ij}}^{\kappa} \tilde{\beta}_{ij} x_{\tilde{\alpha}_i}^{\frac{s}{e_i}} \quad (1 \leq i \leq \nu, 1 \leq j \leq n) \quad (18)$$

(we set  $\tilde{\alpha}_\nu = \infty$ ). Since  $\varphi \in V_3 \setminus W_1$ , and by Proposition 2.3 the expressions  $\tilde{y}_\kappa^{(i,1)}, \dots, \tilde{y}_\kappa^{(i,n)}$  are the beginnings of  $n$  distinct power series  $\tilde{y}^{(i,1)}, \dots, \tilde{y}^{(i,n)}$  satisfying

$$\tilde{f}(x, Y) = \prod_{j=1}^n (Y - \tilde{y}^{(i,j)}) \quad (1 \leq i \leq \nu). \quad (19)$$

Let  $\tilde{y}$  be a root of  $\tilde{f}(x, Y) = 0$ . Denote by  $\tilde{P}^{(i,j)}$  the point of the field  $\bar{\mathbf{Q}}(x, \tilde{y})$ , corresponding to the Puiseux expansion  $\tilde{y}^{(i,j)}$  of  $\tilde{y}$ . Let  $k \in \{1, \dots, m-1\}$ . We say that  $k$  is *essential* for  $\tilde{\varphi}$  if

$$\dim \mathcal{L} \left( k\tilde{P}^{(\nu,n)} \right) > \dim \mathcal{L} \left( (k-1)\tilde{P}^{(\nu,n)} \right). \quad (20)$$

**Proposition.** *Let  $k \in \{1, \dots, m-1\}$ . Then there exist polynomials  $q_{k1}(\tilde{\varphi}), \dots, q_{k\tau_k}(\tilde{\varphi})$  such that  $k$  is essential for a suitable  $\tilde{\varphi}$  if and only if*

$$q_{ki}(\tilde{\varphi}) = 0 \quad (1 \leq i \leq \tau_k). \quad (21)$$

**Proof.** Fix a suitable  $\tilde{\varphi}$ . Let  $z \in \mathcal{L} \left( k\tilde{P}^{(\nu,n)} \right)$ . Then  $z = \frac{p(x, \tilde{y})}{\tilde{d}(x)}$ , where  $\tilde{d}(X)$  is the discriminant of  $\tilde{f}(X, Y)$  with respect to  $Y$ , and  $p$  satisfies

$$\deg_Y p(X, Y) \leq n-1. \quad (22)$$

To estimate  $\deg_X p(X, Y)$  we use the inequality

$$\text{Ord}_{\tilde{P}} \frac{\partial \tilde{f}}{\partial Y}(x, \tilde{y}) \leq (2n-1)me_{\tilde{P}},$$

proved in section 3.2, and the explicite formula

$$p_j(x) = \tilde{d}(x) \text{Tr} \frac{z \sum_{i=j+1}^n \tilde{f}_i(x) \tilde{y}^{i-j-1}}{\frac{\partial \tilde{f}}{\partial Y}(x, \tilde{y})}, \quad (23)$$

which follows easily from [La70, Prop. 3.2]. Here

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

$$p(X, Y) = p_{n-1}(X)Y^{n-1} + \dots + p_0(X)$$

(of course,  $\tilde{f}_n(X) = 1$ ) and  $\text{Tr} : \bar{\mathbf{Q}}(x, \tilde{y}) \rightarrow \bar{\mathbf{Q}}(x)$  is the trace map. We have

$$\begin{aligned} \deg_X p(X, Y) &= \max_{0 \leq j \leq n-1} \deg p_j(X) \leq \deg d(X) + \\ &+ \max_{0 \leq j \leq n-1} \max_{\tilde{P} \in \text{supp}(x)_\infty} \left( -\frac{1}{e_{\tilde{P}}} \text{Ord}_{\tilde{P}} \frac{z \sum_{i=j+1}^n \tilde{f}_i(x) \tilde{y}^{i-j-1}}{\frac{\partial \tilde{f}}{\partial Y}(x, \tilde{y})} \right) \leq \end{aligned}$$

$$\begin{aligned} &\leq \deg \tilde{d}(X) + k + m + (n-1)m + (2n-1)m = \deg \tilde{d}(X) + k + (3n-1)m \leq \\ &\leq \deg \tilde{d}(X) + k(n-1) + \kappa, \end{aligned} \quad (24)$$

where the last inequality follows from  $n \geq 3$ .

Thus,  $k$  is essential for  $\tilde{\varphi}$  if and only if there exists a polynomial  $p(X, Y)$  satisfying (22), (24) and the conditions

$$\text{Ord}_{\alpha_i} p(x, \tilde{y}^{(i,j)}) \geq \text{Ord}_{\alpha_i} \tilde{d}(x) \quad (1 \leq i \leq \nu, 1 \leq j \leq n, (i, j) \neq (\nu, n)), \quad (25)$$

$$\text{Ord}_{\infty} (p(x, \tilde{y}^{(\nu,n)}) - x^k \tilde{d}(x)) \geq 1 - k - \deg \tilde{d}(X). \quad (26)$$

The conditions (25), (26) are equivalent to a (non-homogeneous) system of linear equations for the coefficients of  $p(X, Y)$ . The coefficients of these linear equations are polynomials in  $\tilde{\gamma}$ ,  $\tilde{\alpha}$  and  $\tilde{\beta}$ . For the equations (25) this follows from the inequality

$$\text{Ord}_{\alpha_i} \tilde{d}(x) \leq \deg \tilde{d}(X) \leq (2n-2)m \leq \frac{\kappa}{e_{ij}}. \quad (27)$$

For the equations (26) this follows from (24).

The solvability of this system is equivalent to vanishing of certain determinants, which are polynomials in  $\tilde{\gamma}$ ,  $\tilde{\alpha}$  and  $\tilde{\beta}$ . This proves the Proposition.

Now we define  $W_3(k)$  (where  $0 \leq k \leq m-1$ ) by

$$q_{ki}(\Phi) = 0 \quad (1 \leq i \leq \tau_k). \quad (W_3(k))$$

The next step is to prove that the set  $V \setminus W$  is finite.

So, let  $\tilde{\varphi} \in V \setminus W$ . We define  $\tilde{f}$ ,  $\tilde{y}$ ,  $\tilde{y}^{(i,j)}$ ,  $\tilde{P}^{(i,j)}$  as above. As follows from  $(V_2)$ ,  $\bar{\mathbf{Q}}(x, \tilde{y})$  can be ramified only over  $\tilde{\alpha}_1, \dots, \tilde{\alpha}_{\nu-1}, \tilde{\alpha}_{\nu} = \infty$ . By Corollary 2.2,

$$e_{\tilde{P}^{(i,j)}} = e_{ij} \quad (1 \leq i \leq \nu, 1 \leq j \leq n). \quad (28)$$

But for  $i > \mu$  we have

$$e_{ij} = 1 \quad (1 \leq j \leq n). \quad (29)$$

Hence the field  $\mathcal{K} = \bar{\mathbf{Q}}(x, \tilde{y})$  is ramified only over  $\tilde{\alpha}_1, \dots, \tilde{\alpha}_{\mu}$ , which are equal to  $\alpha_1, \dots, \alpha_{\mu}$  respectively.

Thus, the extension  $\mathcal{K}/\bar{\mathbf{Q}}(x)$  has fixed degree and fixed ramification points  $\alpha_1, \dots, \alpha_{\mu}$ . Hence we have only finitely many possibilities for the field  $\mathcal{K}$ .

Fix one such possibility. Since  $\varphi \notin W_3$ , we have

$$\dim \mathcal{L}(m\tilde{P}^{(\nu,n)}) = 2, \quad (30)$$

$$\dim \mathcal{L} \left( (m-1) \tilde{P}^{(\nu, n)} \right) = 1. \quad (31)$$

Hence  $\tilde{y}$  is defined uniquely by  $(V_4)$ . Therefore  $\tilde{f}$  is defined uniquely. Finally, we have finitely many possibilities for numerating  $\tilde{\alpha}_{\mu+1}, \dots, \tilde{\alpha}_{\nu-1}$  and finitely many possibilities for numerating  $\tilde{y}^{(i,1)}, \dots, \tilde{y}^{(i,n)}$  when  $i$  is fixed.

Thus,  $V \setminus W$  is finite. Obviously  $\varphi \in V_1 \cap V_2 \cap V_4 \setminus (W_2 \cup W_3)$ . Further,  $\varphi \in V_3$  by Proposition 2.3, and  $\varphi \notin W_1$  by Proposition 2.1. Hence  $\varphi \in V \setminus W$ , and we may use Theorem 2A.

Equations  $(V_1)$  form a  $(1, h)$ -system of algebraic equations (see Definition 2.1.2) with coefficients in  $\mathbf{K} \supseteq \mathbf{Q}(\alpha_1, \dots, \alpha_\mu)$ . Equations  $(V_2)$ – $(V_4)$  form a  $(n_1, h_1)$ -system, where

$$h_1 \leq c_1(n, \mu), \quad (32)$$

$$n_1 \leq 2nm \leq 2n(\mathbf{g} + 1) \leq \mu n^2. \quad (33)$$

Denote  $h' = \max(h, h_1)$ . Then  $(V_1)$ – $(V_4)$  is an  $(n_1, h')$ -system of algebraic equations in  $m_1$  indeterminants. We have  $\nu - 1 \leq \deg d(X) \leq (2n - 2)m$ , hence

$$m_1 \leq 6n^3 m^2 \leq \frac{3}{2} n^5 \mu^2. \quad (34)$$

By Theorem 2  $\varphi \in \mathbf{L}^{m_1}$ , where

$$[\mathbf{L} : \mathbf{K}] \leq n_1^{m_1} \leq \exp(n^6 \mu^3), \quad (35)$$

(recall that  $n \geq 3$ ). This proves (1.1). Further,

$$h(\varphi) \leq (2n_1)^{4m_1^2} h' + c(n_1, m_1) \leq \left[ \exp_2(1.2 n^{11} \mu^5) \right] h + c(n, \mu). \quad (36)$$

Hence

$$h(f) = h(\theta) \leq h(\varphi) \leq c_{11}(n, \mu) h + c(n, \mu),$$

which proves (iv). Finally, by Proposition 1.1.2

$$\begin{aligned} \frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{L}/\mathbf{K}} &\leq 2[\mathbf{L} : \mathbf{K}]^2 h(\varphi) + [\mathbf{L} : \mathbf{K}] \ln[\mathbf{L} : \mathbf{K}] \leq \\ &\leq c_{11}(n, \mu) h + c(n, \mu), \end{aligned}$$

which proves (1.2). The proof of Theorem 3A is complete.

## 4 Proof of Theorem 3B.

Let  $\mathbf{K} = \mathbf{K}_0(\alpha \mid \alpha \in M)$ . The divisor

$$(dx) = \sum_{P \in C} (e_P - 1)P - 2(x)_\infty \quad (1)$$

is defined over  $\mathbf{K}_0$ , hence the set  $\text{supp}(dx)$  is also defined over  $\mathbf{K}_0$  (this means that it is preserved by the automorphisms from  $\text{Gal}(\bar{\mathbf{K}}_0/\mathbf{K}_0)$ ). Therefore the set

$$M \cup \{\infty\} = \{x(P) \mid P \in \text{supp}(dx)\} \quad (2)$$

is defined over  $\mathbf{K}_0$ . This yields that

$$[\mathbf{K} : \mathbf{K}_0] \leq \mu!. \quad (3)$$

Let now  $y$ ,  $\kappa$ ,  $\varphi$  and  $\mathbf{L}$  be as in the previous section. Like in the previous section, we may suppose that  $C$  is unramified over  $\infty$ . In this case  $y$  is integral over  $\bar{\mathbf{Q}}[x]$  – this follows immediately from the definition of  $y$ . Hence  $y_0 = \frac{1}{[\mathbf{L} : \mathbf{K}_0]} \text{Tr}_{\mathbf{L}/\mathbf{K}_0}(y)$  is also integral over  $\bar{\mathbf{Q}}[x]$ . For any  $P \in \text{supp}(x)_\infty$  we have clearly  $\text{Ord}_P(y_0) \geq -m$ , hence  $l(y_0) \leq 2mn$ . Therefore the irreducible equation

$$f_0(x, y_0) = 0 \quad (4)$$

satisfies (ii), (iii) of Theorem 3B. Let

$$y_0^{(P)} = \sum_{s=\text{Ord}_P(y_0)}^{\infty} \beta_{0s}(P)x_P^s \quad (P \in \text{supp}(x)_\infty) \quad (5)$$

be the Puiseux expansions of  $y_0$  at the poles of  $x$ , and  $\mathbf{L}_1$  – the field generated by their coefficients. Define  $\mathbf{L}_1$ -system  $\{\hat{b}(v)\}$  by

$$\hat{b}(v) = \max(0, \max\{\ln |\beta_{0s}(P)|_v \mid -\text{Ord}_P(y_0) \leq s \leq \kappa, P \in \text{supp}(x)_\infty\}). \quad (6)$$

Then by (3.35) and (3)

$$\text{nor}\{\hat{b}(v)\} \leq [\mathbf{L} : \mathbf{K}_0] h(\varphi) + c([\mathbf{L} : \mathbf{K}_0]) \leq \left[\exp(n^6 \mu^3)\right] \mu! h(\varphi) + c(n, \mu) \quad (7)$$

(like in the previous section, we suppose that  $n \geq 3$ ).

Since  $\kappa = (3n - 2)nm \geq 2n^2m \geq \frac{1}{2}l(y_0)l(x)$ , we may use Proposition 1.3.4. We get

$$h(f_0) \leq \frac{3}{2}\kappa \text{nor}\{\hat{b}(v)\} + 3\kappa \ln \kappa \leq c_{11}(n, \mu)h + c(n, \mu),$$

as follows from (3.36) and (7).

Finally, by Proposition 2.4  $\mathbf{K}_0(C) = \mathbf{K}_0(x, y_0)$ . Theorem 3B is proved.

# Chapter 4

## An effective Chevalley-Weil theorem for curves

### 1 Introduction.

Let  $C, \tilde{C}$  be non-singular projective curves over  $\bar{\mathbf{Q}}$  of genus  $\mathbf{g} = \mathbf{g}(C)$ , and  $\varphi : \tilde{C} \rightarrow C$  a finite covering of degree  $\nu$ . Choose  $x, y \in \bar{\mathbf{Q}}(C)$  such that  $\bar{\mathbf{Q}}(C) = \bar{\mathbf{Q}}(x, y)$ . Denote  $\tilde{x} = x \circ \varphi \in \bar{\mathbf{Q}}(\tilde{C})$ , and choose  $\tilde{y} \in \bar{\mathbf{Q}}(\tilde{C})$  such that  $\bar{\mathbf{Q}}(\tilde{C}) = \bar{\mathbf{Q}}(\tilde{x}, \tilde{y})$ . Let  $f(x, y) = 0$  and  $\tilde{f}(\tilde{x}, \tilde{y}) = 0$  be the absolutely irreducible algebraic equations for  $x, y$  and  $\tilde{x}, \tilde{y}$  respectively. Denote

$$\begin{aligned} n &= \deg_Y f(X, Y); & \tilde{n} &= \deg_Y \tilde{f}(X, Y) = n\nu; \\ N &= \max(2, \deg f); & \tilde{N} &= \max(N, \deg \tilde{f}); \\ h &= \max(1, h(f)); & \tilde{h} &= \max(h, h(\tilde{f})). \end{aligned}$$

**Theorem 4A.** *Let  $\mathbf{K}$  be an algebraic number field such that  $C, \tilde{C}$  and  $\varphi$  are defined over  $\mathbf{K}$ ,  $x, y \in \mathbf{K}(C)$  and  $\tilde{x}, \tilde{y} \in \mathbf{K}(\tilde{C})$ . ( In particular, we may assume that  $f$  and  $\tilde{f}$  have coefficients in  $\mathbf{K}$ .)*

(i) *Assume that  $\varphi$  is unramified over  $C \setminus \Sigma$ , where  $\Sigma$  is a subset of  $\text{supp}(x)_\infty$ .*

*Then for any  $Q \in C(x, \mathbf{K}, S)$  and  $\tilde{Q} \in \varphi^{-1}(Q)$  we have*

$$\begin{aligned} [\mathbf{K}(\tilde{Q}) : \mathbf{K}] &\leq \nu, & (1) \\ \frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}}(D_{\mathbf{K}(\tilde{Q})/\mathbf{K}}) &\leq \frac{\nu-1}{d_{\mathbf{K}}} \sum_{v \in S \setminus S_\infty} \ln N_{\mathbf{K}}(v) + (4\tilde{N})^{22} \tilde{h} + c(\tilde{N}). & (2) \end{aligned}$$

- (ii) Assume that  $\varphi$  is unramified over  $C$ . Then for any  $Q \in C(x, \mathbf{K})$  and  $\tilde{Q} \in \varphi^{-1}(Q)$  we have (1) and

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}}(D_{\mathbf{K}(\tilde{Q})/\mathbf{K}}) \leq (4\tilde{N})^{22} \tilde{h} + c(\tilde{N}). \quad (3)$$

If only  $C$ ,  $x$  and  $y$  are defined over  $\mathbf{K}$ , we have the following version of Theorem 4A.

**Theorem 4B.** *Let  $C$ ,  $x$  and  $y$  be defined over an algebraic number field  $\mathbf{K}$ .*

- (i) Assume that  $\varphi$  is unramified over  $C \setminus \Sigma$ , where  $\Sigma \subseteq \text{supp}(x)_{\infty}$ . Denote

$$n_1 = \max(2\mathbf{g}, |\Sigma|).$$

Then for any  $Q \in C(x, \mathbf{K}, S)$  and  $\tilde{Q} \in \varphi^{-1}(Q)$  there exists a finite extension  $\tilde{\mathbf{K}}/\mathbf{K}$  with the following properties:

- (a)  $\tilde{C}$  and  $\varphi$  are defined over  $\tilde{\mathbf{K}}$ ;  
(b) we have

$$[\tilde{\mathbf{K}} : \mathbf{K}] \leq n^{|\Sigma|} \exp(10n_1^{12}\nu^6), \quad (4)$$

$$\begin{aligned} \frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}}(D_{\tilde{\mathbf{K}}/\mathbf{K}}) &\leq \left(\exp_2(66n_1^{21}\nu^{11})\right) N^{|\Sigma|+14}h + \\ &+ \frac{\nu-1}{d_{\mathbf{K}}} \sum_{v \in S \setminus S_{\infty}} \ln N_{\mathbf{K}}(v) + c(N, \nu); \end{aligned} \quad (5)$$

- (c)  $\tilde{Q} \in C(\tilde{\mathbf{K}})$ .

- (ii) Assume that  $\varphi$  is unramified over  $C$ . Then for any  $Q \in C(\mathbf{K})$  and  $\tilde{Q} \in \varphi^{-1}(Q)$  there exists a finite extension  $\tilde{\mathbf{K}}/\mathbf{K}$  with the following properties :

- (a)  $\tilde{C}$  and  $\varphi$  are defined over  $\tilde{\mathbf{K}}$ ;  
(b) we have

$$[\tilde{\mathbf{K}} : \mathbf{K}] \leq n \exp(2^{16}\mathbf{g}^{12}\nu^6), \quad (6)$$

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}}(D_{\tilde{\mathbf{K}}/\mathbf{K}}) \leq \left(\exp_2(2^{28}\mathbf{g}^{21}\nu^{11})\right) N^{14}h + c(N); \quad (7)$$

- (c)  $\tilde{Q} \in C(\tilde{\mathbf{K}})$ .

## 2 Upper bounds for local and global discriminants.

In this section  $\mathbf{L}/\mathbf{K}$  is a finite extension of algebraic number fields. The letter  $v$  will always denote a non-Archimedean valuation of the field  $\mathbf{K}$ , and  $w$  – of the field  $\mathbf{L}$ . We denote  $e(w) = e_{\mathbf{L}/\mathbf{K}}(w)$ ,  $f(w) = f_{\mathbf{L}/\mathbf{K}}(w)$ . For any non-Archimedean valuation  $v$  of  $\mathbf{K}$  the function  $|\dots|_v$  is well-defined on the set of fractional ideals of  $\mathbf{K}$ , as well as on the set of fractional ideals of the  $v$ -adic completion  $\mathbf{K}_v$ . In particular, the assertion of [CF67, Ch.1, Prop.4.5(ii)] may be written as

$$\ln |D_{\mathbf{L}/\mathbf{K}}|_v = \sum_{w|v} \ln |D_{\mathbf{L}_w/\mathbf{K}_v}|_v. \quad (1)$$

**Proposition 1.** *Let  $w|v$ . Then*

$$-\ln |D_{\mathbf{L}_w/\mathbf{K}_v}|_v \leq \left( -e(w) \ln |e(w)|_v + (e(w) - 1) \frac{\ln N_{\mathbf{K}}(v)}{d_{\mathbf{K}}(v)} \right) f(w). \quad (2)$$

**Proof.** Without loss of generality we may assume  $f(w) = 1$ . Let  $\Pi$  be a primitive element of  $\mathbf{L}_w$ . Then  $g(\Pi) = 0$  for a polynomial  $g(X) \in \mathbf{K}_v[X]$  of the form

$$g(X) = a_e X^e + a_{e-1} X^{e-1} + \dots + a_0,$$

where  $e = e(w)$  and

$$\begin{aligned} a_e &= 1, \\ |a_i|_v &\leq 1 \quad (1 \leq i \leq e-1), \\ |a_0|_v &= 1. \end{aligned}$$

For  $1 \leq i < j \leq e$  we have

$$|i a_i \Pi^i|_w \neq |j a_j \Pi^j|_w.$$

Hence

$$|g'(\Pi)|_w = \max_{1 \leq i \leq e} |i a_i \Pi^i|_w \geq |e \Pi^{e-1}|_w.$$

Therefore  $\varphi = \mathbf{N}_{\mathbf{L}_w/\mathbf{K}_v}(g'(\Pi))$  satisfies

$$|\varphi|_v \geq |e|_v^e \cdot |\pi|_v^{e-1},$$

where  $\pi = \mathbf{N}_{\mathbf{L}_w/\mathbf{K}_v}(\Pi)$  is a primitive element of  $\mathbf{K}_v$ . Since  $\varphi \in D_{\mathbf{L}_w/\mathbf{K}_v}$ , we get

$$\begin{aligned} -\ln |D_{\mathbf{L}_w/\mathbf{K}_v}|_v &\leq -\ln |\varphi|_v \leq \\ &\leq -e \ln |e|_v - (e-1) \ln |\pi|_v = -e \ln |e|_v + (e-1) \frac{\ln N_{\mathbf{K}}(v)}{d_{\mathbf{K}}(v)}, \end{aligned}$$

q.e.d.

**Remark.** It is well-known that when  $|e|_v = 1$ , the inequality (1) turns to equality .

Denote by  $\text{Ram}(\mathbf{L}/\mathbf{K})$  the set of all non-Archimedean valuations of  $\mathbf{K}$ , ramified in  $\mathbf{L}$ .

**Proposition 2.** *Denote  $\nu = [\mathbf{L} : \mathbf{K}]$ . Then*

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{L}/\mathbf{K}} \leq \frac{\nu - 1}{d_{\mathbf{K}}} \sum_{v \in \text{Ram}(\mathbf{L}/\mathbf{K})} \ln N_{\mathbf{K}}(v) + \nu \ln \nu! .$$

**Proof.** By (1), (2)

$$\begin{aligned} -\ln |D_{\mathbf{L}/\mathbf{K}}|_v &= \frac{\ln N_{\mathbf{K}}(v)}{d_{\mathbf{K}}(v)} \sum_{w|v} (e(w) - 1) f(w) - \sum_{w|v} e(w) f(w) \ln |e(w)|_v \leq \\ &\leq \frac{\nu - 1}{d_{\mathbf{K}}(v)} \ln N_{\mathbf{K}}(v) - \nu \ln |\nu!|_v . \end{aligned}$$

(For the last inequality we used that each of the numbers

$$\prod_{w|v} e(w), \quad \prod_{w|v} e(w)!, \quad \left( \sum_{w|v} e(w) \right)!, \quad \nu!$$

divides the next one.) Hence

$$\begin{aligned} \ln N_{\mathbf{K}} D_{\mathbf{L}/\mathbf{K}} &= \sum_{v \in \text{Ram}(\mathbf{L}/\mathbf{K})} d_{\mathbf{K}}(v) \left( -\ln |D_{\mathbf{L}/\mathbf{K}}|_v \right) \leq \\ &\leq (\nu - 1) \sum_{v \in \text{Ram}(\mathbf{L}/\mathbf{K})} \ln N_{\mathbf{K}}(v) + d_{\mathbf{K}} \nu \ln \nu! , \end{aligned}$$

q.e.d.

### 3 A neighbourhood of a fixed point.

In this section we make some preparations for the proof of Theorem 4A. We use the notations of Section 1.2.

Fix  $P \in C(\bar{\mathbf{Q}})$ , and let  $x(P) = \alpha$ . Then we have the Puiseux expansion

$$y^{(P)} = \sum_{s=\text{Ord}_P(y)}^{\infty} \beta_s(P) x_P^s. \tag{1}$$

Let the field  $\mathbf{K}_P$  and  $\mathbf{K}(\alpha)$ -systems  $\{b_P(v)\}, \{b'_P(v)\}$  be from Proposition 1.2.5. Define the following sets of non-Archimedean valuations of the field  $\mathbf{K}_P$ :

$$T'_1 = \{v \mid b_P(v) + b'_P(v) > 0\}; \quad (2)$$

$$T'_2 = \begin{cases} \{v \mid |\alpha|_v > 1\}, & \alpha \neq \infty, \\ \emptyset, & \alpha = \infty; \end{cases} \quad (3)$$

$$T'_3 = \{v \mid 0 < |\beta_s|_v < 1 \text{ for some } s \leq 3N^3\}; \quad (4)$$

$$T'_4 = \{v \mid v \text{ is ramified over } \mathbf{K}\}. \quad (5)$$

Further, let  $T_i$  include the restrictions to  $\mathbf{K}$  of the valuations from  $T'_i$ :

$$T_i = T_i(P) = \{v|_{\mathbf{K}}, \text{ where } v \in T'_i\} \quad (i = 1, 2, 3, 4). \quad (6)$$

Define also  $T_5(P) = \{v \mid |e_P|_v < 1\}$  and put

$$T(P) = T_1(P) \cup \dots \cup T_5(P).$$

By Proposition 1.2.5

$$\begin{aligned} \frac{1}{d_{\mathbf{K}_P}} \sum_{v \in T'_1 \cup T'_2 \cup T'_3} \ln N_{\mathbf{K}_P}(v) &\leq \text{nor}\{b_P(v)\} + \text{nor}\{b'_P(v)\} + h(\alpha) + \sum_{s=\text{Ord}_P(y)}^{3N^3} h(\beta_s) \leq \\ &\leq 2^{24} N^{14} (h + h(\alpha) + 5N). \end{aligned} \quad (7)$$

Hence by the same proposition

$$\begin{aligned} \frac{1}{d_{\mathbf{K}}} \sum_{v \in T(P)} \ln N_{\mathbf{K}}(v) &\leq [\mathbf{K}_P : \mathbf{K}] \cdot 2^{24} N^{14} (h + h(\alpha) + 5N) + \frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}}(D_{\mathbf{K}_P/\mathbf{K}}) + e_P \leq \\ &\leq 2^{25} N^{15} d^2(\alpha) (h + h(\alpha) + c(N)), \end{aligned} \quad (8)$$

where  $d(\alpha) = [\mathbf{K}(\alpha) : \mathbf{K}]$ .

Fix a valuation  $v$  of  $\mathbf{K}$  and a prolongation of  $v$  on  $\bar{\mathbf{Q}}$ , which we also denote by  $v$ .

**Definition 1.** We say that  $Q \in C(\bar{\mathbf{Q}}) \setminus \text{supp}(x)_{\infty}$  is close to  $P$  in  $v$ -metric, if

(i)  $|x_{\alpha}(Q)|_v < 1$ ;

(ii) the series

$$y^{(P)}(Q) = \sum_{s=\text{Ord}_P(y)}^{\infty} \beta_s(P) (x_P(Q))^s \quad (9)$$

converges in  $v$ -metric;

(iii) for an appropriate choice of the value of the root  $x_P(Q) = (x_{\alpha}(Q))^{\frac{1}{e_P}}$  the sum  $y^{(P)}(Q)$  is equal to  $y(Q)$ .

**Proposition 2.** *Let  $v$  be non-Archimedean and  $v \notin T(P)$ . Suppose that  $Q$  is close to  $P$  in  $v$ -metric, and that*

$$x(Q) \in \mathbf{K} \quad (10),$$

$$\frac{\partial f}{\partial Y}(x(Q), y(Q)) \neq 0. \quad (11)$$

Denote  $\mathbf{L} = \mathbf{K}(x_P(Q))$ . Then for the fixed prolongation of  $v$  we have

$$e_{\mathbf{L}/\mathbf{K}}(v) = e_{\mathbf{K}(Q)/\mathbf{K}}(v). \quad (12)$$

**Remark.** Since  $v \notin T_5(P)$ ,  $v$  is unramified in the extension  $\mathbf{L}(\varepsilon_P)/\mathbf{L}$ . Hence the assertion of Proposition 2 does not depend on the particular choice of the root  $x_P(Q) = (x_\alpha(Q))^{\frac{1}{e_P}}$ . Further in the proof we assume that  $x_P(Q)$  is defined as in Definition 1 (iii).

**Proof.** We denote  $\varepsilon = \varepsilon_P$ ,  $e = e_P$ ,  $\beta_s = \beta_s(P)$ ,  $\lambda = x_P(Q)$ ,  $\mu = y(Q)$ .

Since  $v \notin T_4$ , it is unramified in  $\mathbf{K}_P$ . Hence, replacing  $\mathbf{K}$  by  $\mathbf{K}_P$ , we may assume that  $\alpha$  and the coefficients  $\beta_s$  belong to  $\mathbf{K}$ . Under this additional assumption we shall prove that  $\mathbf{L}_v$  is an unramified extension of  $\mathbf{K}_v(Q)$ , which, of course, implies (12). Note that by (11)  $\mathbf{K}(Q) = \mathbf{K}(x(Q), y(Q)) = \mathbf{K}(\lambda^e, \mu)$ .

By the assumption,  $\mu = \sum_{s=\text{Ord}_P(y)}^{\infty} \beta_s \lambda^s$ . In particular,

$$\mathbf{K}_v(Q) = \mathbf{K}_v(\lambda^e, \mu) \subseteq \mathbf{K}_v(\lambda) = \mathbf{L}_v,$$

and we should prove only that  $\mathbf{L}_v/\mathbf{K}_v(Q)$  is unramified.

Let  $\pi$  be a primitive element of  $\mathbf{K}_v(Q)$ . Then  $\lambda^e = \eta \pi^r$  for some  $v$ -adic unit  $\eta \in \mathbf{K}_v(Q)$  and  $r \in \mathbf{Z}$ . Since  $v \notin T_5$ , the field  $\mathbf{M}_v = \mathbf{K}_v(Q)(\eta^{\frac{1}{e}}, \varepsilon)$  is unramified over  $\mathbf{K}_v(Q)$ . Hence it is sufficient to prove that  $\lambda \in \mathbf{M}_v$ .

Denote  $e_1 = \frac{e}{(e, r)}$ ,  $r_1 = \frac{r}{(r, e)}$ . Let  $a, b \in \mathbf{Z}$  satisfy  $ar_1 + be_1 = 1$ . Then

$$\Pi = \lambda^a \pi^b$$

satisfies

$$\Pi^{e_1} = \pi \eta^{\frac{ae_1}{e}} \varepsilon^i, \quad \Pi^{r_1} = \lambda \eta^{\frac{-be_1}{e}} \varepsilon^j, \quad (13)$$

for some  $i, j \in \mathbf{Z}$ . As follows from (13),  $\Pi$  is a primitive element of the field  $\mathbf{M}_v(\lambda)$ .

Assume now that  $e_1 > 1$ . Then there exists a prime  $q|e_1$ . Denote

$$s_0 = s_0(q) = \min\{s \mid s \not\equiv 0 \pmod{q} \text{ and } \beta_s \neq 0\}.$$

By Corollary 3.2.2  $s_0 \leq 3N^3$ , and we have  $|\beta_{s_0}|_v = 1$  because  $v \notin T_3$ . Therefore for any  $s > s_0$

$$|\beta_{s_0} \lambda^{s_0}|_v > |\beta_s \lambda^s|_v,$$

because  $|\lambda|_v < 1$  and  $v \notin T_1$ . Hence  $\omega = \sum_{s=s_0}^{\infty} \beta_s \lambda^s$  satisfies

$$\text{Ord}_{\Pi}(\omega) = \text{Ord}_{\Pi}(\beta_{s_0} \lambda^{s_0}) = s_0 r_1.$$

On the other hand,

$$\omega = \mu - \sum_{s=\text{Ord}_P(y)}^{s_0-1} \beta_s \lambda^s \in \mathbf{M}_v(\Pi^q),$$

hence  $q|\text{Ord}_{\Pi}(\omega)$ . We see that  $q|s_0 r_1$ , which is a contradiction. Thus  $e_1 = 1$ , and  $\lambda \in \mathbf{M}_v$ . The proof of Proposition 2 is complete.

## 4 Proof of Theorem 4A.

Let  $\Delta(x)$  be the discriminant of  $f(X, Y)$ . We write

$$f(X, Y) = a(X)Y^n + \text{terms of lower degree in } Y, \quad (1)$$

$$\Delta(X) = \gamma X^{\deg \Delta(X)} + \text{terms of lower degree.} \quad (2)$$

Without loss of generality suppose that the leading coefficient of  $a(X)$  is 1, i.e.

$$a(X) = X^{\deg a(X)} + \text{terms of lower degree.} \quad (3)$$

In particular, one of the coefficients of  $f(X, Y)$  is 1. This yields that

$$h(f) = \text{nor} \{ \max(0, \ln |f|_v) \}, \quad (4)$$

$$h(\gamma) \leq (2n - 2)h + C(N). \quad (5)$$

Let now  $M$  be a finite subset of  $\bar{\mathbf{Q}} \cup \{\infty\}$  which will be specialized later. Define

$$T = \left( \bigcup_{x(P) \in M} T(P) \right) \cup \{v \mid |f|_v > 1\} \cup \{v \mid |\gamma|_v \neq 1\}. \quad (6)$$

where the sets  $T(P)$  are defined in the previous section. Then, using (3.8), (4) and (5), we get

$$\begin{aligned} \frac{1}{d_{\mathbf{K}}} \sum_{v \in T \setminus S_{\infty}} \ln \mathbf{N}_{\mathbf{K}}(v) &= \frac{1}{d_{\mathbf{K}}} \sum_{x(P) \in M} \sum_{v \in T(P)} \ln \mathbf{N}_{\mathbf{K}}(v) + h(f) + 2h(\gamma) \leq \\ &\leq 2^{26} N^{15} \left( \max_{\alpha \in M} d^2(\alpha) \right) \left( |M|(h + c(N)) + \sum_{\alpha \in M} h(\alpha) \right). \end{aligned} \quad (7)$$

Replacing  $C$  by  $\tilde{C}$ , we define similarly  $\tilde{X}$ ,  $\tilde{\Delta}(X)$ ,  $\tilde{\gamma}$ , and the sets  $\tilde{T}_i(\tilde{P})$ ,  $\tilde{T}(\tilde{P})$  and  $\tilde{T}$ . In particular, we have

$$\frac{1}{d_{\mathbf{K}}} \sum_{v \in \tilde{T} \setminus S_{\infty}} \ln \mathbf{N}_{\mathbf{K}}(v) \leq 2^{26} \tilde{N}^{15} \left( \max_{\alpha \in M} d^2(\alpha) \right) \left( |M|(\tilde{h} + c(\tilde{N})) + \sum_{\alpha \in M} h(\alpha) \right). \quad (8)$$

Now define  $M$  as the set of the roots of the polynomial  $a(X)\Delta(X)\tilde{a}(X)\tilde{\Delta}(X)$ . Then we have

$$|M| \leq 2N^2 + 2\tilde{N}^2 \leq 4\tilde{N}^2, \quad (9)$$

$$\max_{\alpha \in M} d(\alpha) \leq 2\tilde{N}^2, \quad (10)$$

$$\begin{aligned} \sum_{\alpha \in M} h(\alpha) &\leq h(a(X)\Delta(X)\tilde{a}(X)\tilde{\Delta}(X)) + c(\tilde{N}) \leq \\ &\leq 2Nh + 2\tilde{N}\tilde{h} + c(\tilde{N}) \leq 4\tilde{N}\tilde{h} + c(\tilde{N}), \end{aligned} \quad (11)$$

where (11) follows from Proposition 1.2.4. Substituting this to (7), (8), we get

$$\frac{1}{d_{\mathbf{K}}} \sum_{v \in (T \cup \tilde{T}) \setminus S_{\infty}} \ln \mathbf{N}_{\mathbf{K}}(v) \leq 2^{32} \tilde{N}^{21} \tilde{h} + c(N). \quad (12)$$

**Proposition 1.** *Let  $Q \in C(\mathbf{K}) \setminus \text{supp}(x)_{\infty}$ ,  $\tilde{Q} \in \varphi^{-1}(Q)$ ,  $|x(Q)|_v \leq 1$  and  $v \notin T \cup \tilde{T}$ . Then  $v$  is unramified in  $\mathbf{K}(\tilde{Q})$ .*

**Proof.** If  $\tilde{y}(\tilde{Q}) = \infty$ , then  $\tilde{x}(\tilde{Q})$  is a root of  $\tilde{a}(X)$ . If  $\frac{\partial f}{\partial Y}(\tilde{x}(\tilde{Q}), \tilde{y}(\tilde{Q})) = 0$ , then  $\tilde{x}(\tilde{Q})$  is a root of  $\tilde{\Delta}(x)$ . In the both cases  $\tilde{x}(\tilde{Q}) \in M$ , and the assertion becomes trivial, because  $v \notin \tilde{T}_4(\tilde{Q})$ . Hence we may assume further that

$$\tilde{y}(\tilde{Q}) \neq \infty, \quad \frac{\partial f}{\partial Y}(\tilde{x}(\tilde{Q}), \tilde{y}(\tilde{Q})) \neq 0. \quad (13)$$

Denote  $\beta = x(Q) = \tilde{x}(\tilde{Q})$ . We have  $v \notin T_2(P)$  for any  $P$  such that  $x(P) \in M$ . Hence  $|\alpha|_v \leq 1$  for any  $\alpha \in M$ . Therefore  $|\beta - \alpha|_v \leq 1$  for any  $\alpha \in M$ . Assume first that for any  $\alpha \in M$  we have  $|\beta - \alpha|_v = 1$ . Then

$$|\tilde{a}(\beta)|_v = 1, \quad (14)$$

$$|\tilde{\Delta}(\beta)| = 1, \quad (15)$$

because the leading coefficients of  $\tilde{a}(x)$  is 1, and  $|\tilde{\gamma}|_v = 1$ . Since  $|\tilde{f}|_v \leq 1$ , the conditions (14) and (15) imply that  $v$  is unramified in  $\mathbf{K}(\tilde{Q}) = \mathbf{K}(y(\tilde{Q}))$ .

Assume now that

$$|\beta - \alpha|_v < 1 \quad (16)$$

for some  $\alpha \in M$ . Then by Proposition 1.2.9  $\tilde{Q}$  is close to some  $\tilde{P} \in \text{supp}(x_\alpha)_0$ . By Proposition 3.2

$$e_{\mathbf{K}(\tilde{Q})/\mathbf{K}}(v) = e_{\tilde{\mathbf{L}}/\mathbf{K}}(v), \quad (17)$$

where

$$\tilde{\mathbf{L}} = \mathbf{K} \left( (\beta - \alpha)^{\frac{1}{e_{\tilde{P}}}} \right).$$

On the other hand, it is clear that  $Q$  is close to  $P = \varphi(\tilde{P})$ . (To see this one should consider  $y$  as an element of  $\tilde{\mathbf{Q}}(\tilde{C})$ , and then apply the second part of Proposition 1.2.9.) Hence

$$e_{\mathbf{L}/\mathbf{K}}(v) = e_{\mathbf{K}(Q)/\mathbf{K}}(v) = 1, \quad (18)$$

where

$$\mathbf{L} = \mathbf{K} \left( (\beta - \alpha)^{\frac{1}{e_P}} \right).$$

But  $\tilde{P}$  is unramified over  $P$ , hence

$$e_P = e_{\tilde{P}}, \quad (19)$$

and we get finally

$$e_{\mathbf{K}(\tilde{Q})/\mathbf{K}}(v) = 1, \quad (20)$$

q.e.d.

Now we may complete the proof of Theorem 4. Assume that  $\varphi$  is unramified over  $C \setminus \Sigma$  and  $Q \in C(x, \mathbf{K}, S)$ . Inequality (1.1) is obvious. Further, by Proposition 1

$$\text{Ram}(\mathbf{K}(\tilde{Q})/\mathbf{K}) \subseteq T \cup \tilde{T} \cup S, \quad (21)$$

where  $\text{Ram}$  is defined in Section 2. Then (1.2) follows immediately from (12), (21) and Proposition 2.2.

Assume now that  $\varphi$  is unramified over  $C$  and  $Q \in C(\mathbf{K})$ . Then we should replace the set  $M$  by  $M \cup \{\infty\}$ . For this modified  $M$  we still have (9) – (11), and hence (12) also holds.

We are going to prove that

$$\text{Ram}(\mathbf{K}(\tilde{Q})/\mathbf{K}) \subseteq T \cup \tilde{T}. \quad (22)$$

If  $x(Q) = \infty$  then  $\tilde{x}(\tilde{Q}) = \infty \in M$ , hence

$$\text{Ram}(\mathbf{K}(\tilde{Q})/\mathbf{K}) = \tilde{T}_5(\tilde{Q}) \subseteq \tilde{T}.$$

Let now  $\beta = x(Q) \in \mathbf{K}$ , and  $v \notin T \cup \tilde{T}$ . If  $|\beta|_v \leq 1$ , then  $v$  is unramified in  $\mathbf{K}(\tilde{Q})$  by Proposition 1. If  $|\beta|_v > 1$ , then we may repeat the argument of Proposition 1 with  $\alpha = \infty$ , and prove again that  $v$  is unramified in  $\mathbf{K}(\tilde{Q})$ . This completes the proof of (22). Now (1.3) follows from (12), (22) and Proposition 2.2. The proof of Theorem 4A is complete.

## 5 Proof of Theorem 4B.

The proofs of cases (i) and (ii) are very similar. We shall consider case (i), which is more important for our further purposes, and indicate during the proof the minor changes necessary for the case (ii).

Fix an arbitrary  $P_1 \in \Sigma$  (or  $P_1 \in \text{supp}(x)_\infty$  in the case (ii) ), and put

$$n_1 = \max(|\Sigma|, 2\mathbf{g}).$$

(Note that except the trivial case  $\deg \varphi = 1$ , we have certainly  $n_1 \geq 2$ ; for if  $\mathbf{g} = 0$ , then  $\varphi$  should be ramified and  $|\Sigma| \geq 2$ .) Define the following divisor  $D$  :

$$D = \sum_{P \in \Sigma} P + (n_1 - |\Sigma|) P_1. \quad (1)$$

Then  $\deg D = n_1$ , and  $D$  is defined over the field  $\mathbf{K}_1 = \mathbf{K}(\Sigma)$ , defined in Section 1.1. By Proposition 1.2.7

$$[\mathbf{K}_1 : \mathbf{K}] \leq n^{|\Sigma|}, \quad (2)$$

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{K}_1/\mathbf{K}} \leq 2^{24} N^{|\Sigma|+14} (h + 6N). \quad (3)$$

(In the case (ii)  $D = n_1 P_1$ ,  $\mathbf{K}_1 = \mathbf{K}(P)$ , and we have

$$[\mathbf{K}_1 : \mathbf{K}] \leq n,$$

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\mathbf{K}_1/\mathbf{K}} \leq 2^{24} N^{14} (h + 6N). )$$

Since  $D$  is non-special, the space  $\mathcal{L}(D)$  generates the field  $\bar{\mathbf{Q}}(C)$ . Hence for any basis  $x_1, \dots, x_\mu$  of this space, there exist  $a_2, \dots, a_\mu \in \mathbf{Z}$  such that  $x_1$  and  $y_1 = a_2 x_2 + \dots + a_\mu x_\mu$  generate  $\bar{\mathbf{Q}}(C)$  over  $\bar{\mathbf{Q}}$ , and  $\max_{2 \leq i \leq \mu} |a_i| \leq (n_1 - 1)!$ . (We suppose that  $x_1$  is non-constant.) Indeed, denote by  $\mathcal{K}_1$  the minimal extension of  $\mathcal{K} = \bar{\mathbf{Q}}(C)$ , normal over  $\bar{\mathbf{Q}}(x_1)$ . Consider the polynomial  $\mathcal{G}(A_2, \dots, A_\mu) \in \mathcal{K}_1[A_2, \dots, A_\mu]$ , defined by

$$\mathcal{G}(A_2, \dots, A_\mu) = \prod_{\substack{\sigma \in \text{Gal}(\mathcal{K}_1/\mathcal{K}) \\ \sigma \neq \text{Id}}} \sum_{i=2}^{\mu} A_i (\sigma x_i - x_i). \quad (4)$$

Then

$$\deg \mathcal{G}(A_2, \dots, A_\mu) \leq (n_1 - 1)!,$$

and by Proposition 2.3.1 there exist  $a_2, \dots, a_\mu \in \mathbf{Z}$  such that

$$\max_{2 \leq i \leq \mu} |a_i| \leq \left( \frac{1}{2} (n_1 - 1)! + 1 \right)$$

and  $\mathcal{G}(a_2, \dots, a_\mu) \neq 0$ . These  $a_2, \dots, a_\mu$  are as desired.

As follows from Proposition 1.2.2, the basis  $x_1, \dots, x_\mu$  can be chosen so that the coefficients of the Puiseux expansions

$$x_i^{(P)} = \prod_{s=\text{Ord}_P(x_i)}^{\infty} \alpha_{is}(P) x_P^s \quad (5)$$

satisfy

$$\ln |\alpha_{is}(P)|_v \leq a'(v) + s a(v), \quad (P \in \text{supp}(x)_\infty) \quad (6)$$

where

$$\text{nor}\{a(v)\} \leq 9n_1 L^5 (h + 12 \ln L), \quad (7)$$

$$\text{nor}\{a'(v)\} \leq 370n_1^2 L^{11} (h + 12 \ln L), \quad (8)$$

$$L = \max(N, n_1). \quad (9)$$

If  $y_1$  is defined as above, then the coefficients of its Puiseux expansions

$$y_1^{(P)} = \prod_{s=\text{Ord}_P(y_1)}^{\infty} \beta_{1s}(P) x_P^s \quad (10)$$

satisfy

$$\ln |\beta_{1s}(P)|_v \leq b'(v) + s b(v), \quad (P \in \text{supp}(x)_\infty)$$

where

$$b'(v) = a'(v) + \max(0, n_1 \ln |n_1|_v). \quad (11)$$

Let the pairs  $x, x_1$  and  $x_1, y_1$  satisfy absolutely irreducible algebraic equations

$$g(x, x_1) = 0, \quad (12)$$

$$f_1(x_1, y_1) = 0 \quad (13)$$

respectively. Then

$$\deg_X g(X, X_1) \leq n_1, \quad (14)$$

$$\deg_{X_1} g(X, X_1) \leq n, \quad (15)$$

$$\deg f_1(X_1, Y_1) \leq n_1, \quad (16)$$

and we may suppose that the coefficients of  $g(X, X_1)$  and  $f_1(X_1, Y_1)$  belong to  $\mathbf{K}_1$ . Finally, we use Proposition 1.3.4 in order to estimate  $h(g)$  and  $h(f_1)$ . In the both cases we may put  $\kappa = 2Ln_1$  and  $\hat{c}(v) = b'(v) + \kappa a(v)$ . Then by (1.3.7)

$$\begin{aligned} h(g), h(f_1) &\leq 6L^2 n_1^2 (\text{nor}\{a'(v)\} + n_1 \ln n_1 + 2Ln_1 \text{nor}\{a(v)\}) + 6L^2 n_1^2 \leq \\ &\leq 2223n_1^4 L^{13} (h + 12 \ln L). \end{aligned} \quad (17)$$

We summarize all above in the following

**Proposition 1.** *There exist :*

- (i) a finite extension  $\mathbf{K}_1/\mathbf{K}$  satisfying (2), (3);
- (ii)  $x_1, y_1 \in \mathbf{K}_1(C)$  such that  $\mathbf{K}_1(C) = \mathbf{K}_1(x_1, y_1)$ ;
- (iii) absolutely irreducible polynomials  $f_1(X_1, Y_1)$  and  $g(X, X_1)$  with coefficients in  $\mathbf{K}_1$ , satisfying (12)–(17).

The next step is to find a “small” generator of  $\bar{\mathbf{Q}}(\tilde{C})$  over  $\bar{\mathbf{Q}}(\tilde{x}_1)$ , where  $\tilde{x}_1 = x_1 \circ \varphi$ .

**Proposition 2.** *There exist :*

- (i) a finite extension  $\tilde{\mathbf{K}}_1/\mathbf{K}_1$  satisfying

$$[\tilde{\mathbf{K}}_1 : \mathbf{K}] \leq (\exp(9n_1^{12}\nu^6)) n^{|\Sigma|}, \quad (18)$$

$$\frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\tilde{\mathbf{K}}_1/\mathbf{K}} \leq (\exp_2(65n_1^{21}\nu^{11})) N^{14+|\Sigma|} h + c(N, \nu); \quad (19)$$

- (ii)  $\tilde{y}_1 \in \tilde{\mathbf{K}}_1(C)$  such that  $\tilde{\mathbf{K}}_1(C) = \tilde{\mathbf{K}}_1(\tilde{x}_1, \tilde{y}_1)$  ;

- (iii) an absolutely irreducible polynomial  $\tilde{f}_1(X_1, Y_1)$  with coefficients in  $\tilde{\mathbf{K}}_1$  such that

$$\tilde{f}_1(\tilde{x}_1, \tilde{y}_1) = 0, \quad (20)$$

$$\deg_{X_1} \tilde{f}_1(X_1, Y_1) \leq n_1^3 \nu, \quad (21)$$

$$\deg_{Y_1} \tilde{f}_1(X_1, Y_1) \leq n_1 \nu, \quad (22)$$

$$h(\tilde{f}_1) \leq (\exp_2(65n_1^{21}\nu^{11})) N^{13} h + c(N, \nu). \quad (23)$$

(In the case (ii) of Theorem 4B, we should replace  $|\Sigma|$  by 1 in (18) and by 0 in (19).)

**Proof.** Let  $\Delta_1(X)$  be the discriminant of  $f_1(X, Y)$  with respect to  $Y$ ,

$$M = \{\alpha_1, \dots, \alpha_{\mu-1}, \infty\} = \{\text{the roots of } \Delta_1(X)\} \cup \{\infty\}$$

and  $\mathbf{K}_1(M)$  the splitting field of  $\Delta_1(X)$  over  $\mathbf{K}_1$ . Then we have

$$\mu = |M| \leq \deg \Delta_1(X) + 1 \leq (2n_1 - 2)n_1 + 1, \quad (24)$$

$$[\mathbf{K}_1(M) : \mathbf{K}_1] \leq (\mu - 1)!, \quad (25)$$

$$\begin{aligned} \frac{1}{d_{\mathbf{K}_1}} \ln N_{\mathbf{K}_1} D_{\mathbf{K}_1(M)/\mathbf{K}_1} &\leq ((\mu - 1)!)^2 (h(1 : \alpha_1 : \dots : \alpha_{\mu-1}) + 1) \leq \\ &\leq (\mu - 1)^{2\mu-2} ((\mu - 1) h(\Delta_1) + (\mu - 1)^2 + 1) \leq \\ &\leq \mu^{2\mu} ((2n_1 - 2)h(f_1) + c(n_1)) \leq \\ &\leq (2n_1)^{4n_1^2} L^{13} h + c(N). \end{aligned} \quad (26)$$

The covering  $x_1 : C \rightarrow \mathbf{P}^1$  is unramified over  $\mathbf{P}^1 \setminus M$ . Hence the covering

$$\tilde{x}_1 : \tilde{C} \rightarrow \mathbf{P}^1$$

is also unramified over  $\mathbf{P}^1 \setminus M$ . Its degree  $\tilde{n}_1$  is less or equal to  $\nu n_1$ . Therefore, by Theorem 3A  $\bar{\mathbf{Q}}(\tilde{C}) = \bar{\mathbf{Q}}(\tilde{x}_1, \tilde{y}_1)$ , where  $\tilde{x}_1$  and  $\tilde{y}_1$  satisfy an absolutely irreducible equation  $\tilde{f}_1(\tilde{x}_1, \tilde{y}_1) = 0$  with the following properties. First of all,

$$\tilde{f}_1(X_1, Y_1) \in \tilde{\mathbf{K}}_1(X_1, Y_1),$$

where

$$\begin{aligned} [\tilde{\mathbf{K}}_1 : \mathbf{K}] &\leq n^{|\Sigma|} \cdot (\mu - 1)! \cdot \exp(\tilde{n}_1^6 \mu^3) \leq \\ &\leq n^{|\Sigma|} \exp(9n_1^{12} \nu^6), \end{aligned} \quad (27)$$

$$\begin{aligned} \frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\tilde{\mathbf{K}}_1/\mathbf{K}} &\leq \left( \exp(9n_1^{12} \nu^6) \right) 2^{24} N^{14+|\Sigma|} (h + 6N) + \\ &\quad + \left( \exp(\tilde{n}_1^6 \mu^3) \right) \left( (2n_1)^{4n_1^2} L^{13} h + c(N) \right) + \\ &\quad + \left( \exp_2(2\tilde{n}_1^{11} \mu^5) \right) \max_{\alpha \in M} h(\alpha) + c(\tilde{n}_1, \mu) \leq \\ &\leq \left( \exp_2(65n_1^{21} \nu^{11}) \right) N^{14+|\Sigma|} h + c(N, \nu). \end{aligned} \quad (28)$$

Further,

$$\deg_{Y_1} \tilde{f}(X_1, Y_1) \leq \tilde{n}_1 \leq n_1 \nu, \quad (29)$$

$$\deg_{X_1} \tilde{f}_1(X_1, Y_1) \leq \frac{1}{2} \tilde{n}_1 (\mu - 1) \leq n_1^3 \nu, \quad (30)$$

$$\begin{aligned} h(\tilde{f}) &\leq \left( \exp_2(2\tilde{n}_1^{11} \mu^5) \right) \max_{\alpha \in M} h(\alpha) + c(n_1, \mu) \leq \\ &\leq \left( \exp_2(65n_1^{21} \nu^{11}) \right) N^{13} h + c(N, \nu). \end{aligned} \quad (31)$$

Proposition 2 is proved.

Now we are able to complete the proof of Theorem 4B. Consider first (i). We assume further that

$$g(X, X_1) = X_1^{\deg_{X_1} g(X, X_1)} + \text{the terms of lower degree in } X_1. \quad (32)$$

Define the set  $\tilde{S}_1$  of valuations of  $\tilde{\mathbf{K}}_1$  by

$$\tilde{S}_1 = \{ v \mid v|_{\mathbf{K}} \in S \text{ or } |g|_v > 1 \}. \quad (33)$$

Then

$$\begin{aligned} \frac{1}{d_{\tilde{\mathbf{K}}_1}} \sum_{v \in \tilde{S}_1 \setminus \tilde{S}_\infty} \ln N_{\mathbf{K}_1}(v) &= \frac{1}{d_{\mathbf{K}}} \sum_{v \in S \setminus S_\infty} \ln N_{\mathbf{K}}(v) + h(g) \leq \\ &\leq \frac{1}{d_{\mathbf{K}}} \sum_{v \in S \setminus S_\infty} \ln N_{\mathbf{K}}(v) + 2223n_1^4 L^{13}(h + 12 \ln L). \end{aligned} \quad (34)$$

Now let  $Q \in C(x, \mathbf{K}, S)$ . Then  $Q \in C(x_1, \tilde{\mathbf{K}}_1, \tilde{S}_1)$ . Denote  $\tilde{\mathbf{K}} = \tilde{\mathbf{K}}_1(Q)$ . Then by Theorem 4A (i)

$$[\tilde{\mathbf{K}} : \mathbf{K}] \leq \nu \cdot [\tilde{\mathbf{K}}_1 : \mathbf{K}] \leq n^{|\Sigma|} \exp(10n_1^{12}\nu^6), \quad (35)$$

$$\begin{aligned} \frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\tilde{\mathbf{K}}/\mathbf{K}} &\leq \nu \frac{1}{d_{\mathbf{K}}} \ln N_{\mathbf{K}} D_{\tilde{\mathbf{K}}_1/\mathbf{K}} + \frac{1}{d_{\tilde{\mathbf{K}}_1}} \ln N_{\tilde{\mathbf{K}}_1} D_{\tilde{\mathbf{K}}_1(Q)/\tilde{\mathbf{K}}_1} \leq \\ &\leq \left( \exp_2(65n_1^{21}\nu^{11}) \right) \nu N^{14+|\Sigma|} h + \frac{\nu-1}{d_{\tilde{\mathbf{K}}_1}} \sum_{v \in \tilde{S}_1 \setminus \tilde{S}_\infty} \ln N_{\tilde{\mathbf{K}}_1}(v) + \\ &\quad + (4\tilde{N}_1)^{22} \tilde{h}_1 + c(\tilde{N}_1) \leq \\ &\leq \left( \exp_2(65n_1^{21}\nu^{11}) \right) \nu N^{14+|\Sigma|} h + \frac{\nu-1}{d_{\mathbf{K}}} \sum_{v \in S \setminus S_\infty} \ln N_{\mathbf{K}}(v) + \\ &\quad + 2223n_1^4 L^{13}(h + 12 \ln L) + \\ &\quad + (5n_1^3\nu)^2 \left( \exp_2(65n_1^{21}\nu^{11}) \right) N^{13} h + c(N, \nu) \leq \\ &\leq \left( \exp_2(66n_1^{21}\nu^{11}) \right) N^{14+|\Sigma|} h + \\ &\quad + \frac{\nu-1}{d_{\mathbf{K}}} \sum_{v \in S \setminus S_\infty} \ln N_{\mathbf{K}}(v) + c(N, \nu). \end{aligned} \quad (36)$$

Here

$$\tilde{N}_1 = \max(2, \deg \tilde{f}_1) \leq 5n_1^3\nu, \quad (37)$$

and

$$\tilde{h}_1 = \max(1, h(\tilde{f}_1)). \quad (38)$$

This completes the proof of part (i). The proof of part (ii) is absolutely similar and even simpler, because we need not care about the sets  $S$  and  $S_1$ .

# Chapter 5

## A generalization of the Main Theorem and applications

In this chapter we use the notations of Section 1.1.

### 1 A generalization of Theorem 1B.

**Theorem 5A.** *Assume that there exists a finite covering  $\varphi : \tilde{C} \rightarrow C$ , defined over  $\bar{\mathbf{Q}}$ , unramified over  $C \setminus \Sigma$  and such that*

$$\rho(\tilde{\Sigma}) \geq 2, \quad (1)$$

where  $\tilde{\Sigma} = \varphi^{-1}(\Sigma)$ . Denote  $\tilde{\Lambda} = \max(\lambda_2(\tilde{\Sigma}), N)$ . Then for any  $Q \in C(x, \mathbf{K}, S)$

$$\begin{aligned} h_x(Q) &\leq c(N, d, \nu) \tilde{\Lambda}^{37} \left( \sigma^\sigma D p^d \right)^{c_{11}(n_1, \nu) n^{|\Sigma|}} \times \\ &\quad \times \left( \prod_{v \in S \setminus S_\infty} N_{\mathbf{K}}(v) \right)^{c_{12}(n_1, \nu) n^{|\Sigma|}} e^{c_{13}(n_1, \nu) N^{(\nu+1)|\Sigma|+28} d h}, \end{aligned} \quad (2)$$

where  $n_1 = \max(2g, |\Sigma|)$  and

$$\begin{aligned} c_{11}(n_1, \nu) &= \exp\left(11n_1^{12}\nu^6\right), \\ c_{12}(n_1, \nu) &= \nu^{\nu^{|\Sigma|+1}}, \\ c_{13}(n_1, \nu) &= \exp_2\left(67n_1^{21}\nu^{11}\right). \end{aligned}$$

**Proof.** Fix  $\tilde{Q} \in \varphi^{-1}(Q)$ . Then  $\tilde{Q} \in \tilde{C}(\tilde{\mathbf{K}})$ , where  $\tilde{\mathbf{K}}$  is from Theorem 4B. Since  $\tilde{x}(\tilde{Q}) = x(Q)$  is  $S$ -integer,  $\tilde{Q} \in \tilde{C}(\tilde{x}, \tilde{\mathbf{K}}, \tilde{S})$ , where  $\tilde{x} = x \circ \varphi$  and  $\tilde{S}$  is the set of

valuations of  $\tilde{\mathbf{K}}$  lying above  $S$ . Let  $\tilde{x}_1, \tilde{y}_1$  be from Section 4.5. Then  $\tilde{\mathbf{K}}(\tilde{C}) = \tilde{\mathbf{K}}(\tilde{x}_1, \tilde{y}_1)$ , as follows from the definition of the field  $\tilde{\mathbf{K}}$  in Section 4.5. The same argument as in the beginning of Section 4.5 shows that  $\tilde{\mathbf{K}}(\tilde{C}) = \tilde{\mathbf{K}}(\tilde{x}, \tilde{y})$ , where  $\tilde{y} = a\tilde{x}_1 + b\tilde{y}_1$ , and  $a, b \in \mathbf{Z}$ ,  $\max(|a|, |b|) \leq c(N, \nu)$ . Further, we have  $b \neq 0$ , because  $\tilde{\mathbf{K}}(\tilde{x}, \tilde{x}_1)$  is a proper subfield of  $\tilde{\mathbf{K}}(\tilde{C})$ , except maybe the trivial case  $\deg \varphi = 1$ .

Let  $g(X, X_1)$  and  $\tilde{f}_1(X_1, Y_1)$  be as in Section 4.5. Denote

$$g_1(X_1, Y) = \tilde{f}_1\left(X_1, \frac{1}{b}(Y - aX_1)\right).$$

Then by (4.5.21)–(4.5.23)

$$\deg_{X_1} g_1(X_1, Y) \leq 2n_1^3\nu, \quad \deg_Y g_1(X_1, Y) \leq n_1\nu, \quad (3)$$

$$h(g_1) \leq \left(\exp_2(65n_1^{21}\nu^{11})\right) N^{13}h + c(N, \nu). \quad (4)$$

Let  $\tilde{x}, \tilde{y}$  satisfy an absolutely irreducible equation  $\tilde{f}(\tilde{x}, \tilde{y}) = 0$ . Then  $\tilde{f}(X, Y)$  divides  $R(X, Y)$ , the resultant of  $g(X, X_1)$  and  $g_1(X_1, Y)$  with respect to  $X_1$ . We have

$$\begin{aligned} h(\tilde{f}) &\leq h(R) + \deg R \leq 2\nu n_1^3 h(g) + n h(g_1) + c(N, \nu) \leq \\ &\leq \left(\exp_2(66n_1^{21}\nu^{11})\right) N^{14}h + c(N, \nu), \end{aligned} \quad (5)$$

$$\deg \tilde{f} \leq 3\nu n_1^4 n. \quad (6)$$

Now we may apply Theorem 1B, but we prefer to use a more exact formula (1.6.11). Putting in it  $\varepsilon = 1$ , we get

$$\begin{aligned} h_x(Q) = h_{\tilde{x}}(\tilde{Q}) &\leq c(\tilde{N}, \tilde{d})\tilde{\Lambda}^{37} \left( \tilde{\sigma}^{20\tilde{\sigma}} \tilde{D}^{\frac{3}{2}} p^{\tilde{d}} \prod_{v \in \tilde{S} \setminus \tilde{S}_\infty} \ln^3 N_{\tilde{\mathbf{K}}}(v) \right)^{d_{\rho-2}(\tilde{\Sigma}/\tilde{\mathbf{K}})+1} \times \\ &\times e^{(4\tilde{N})^{14+|\tilde{\Sigma}|} \tilde{d}\tilde{h}}, \end{aligned} \quad (7)$$

where  $\rho = \rho(\tilde{\Sigma})$ ,

$$\tilde{d} = d_{\tilde{\mathbf{K}}} \leq d n^{|\Sigma|} \exp(10n_1^{12}\nu^6); \quad (8)$$

$$\begin{aligned} \tilde{D} = D_{\tilde{\mathbf{K}}} &\leq c(N, \nu, d) e^{(\exp_2(66n_1^{21}\nu^{11})) N^{|\Sigma|+14} d h} \left( \prod_{v \in S \setminus S_\infty} N_{\mathbf{K}}(v) \right)^{\nu-1} \times \\ &\times D^{n^{|\Sigma|} \exp(10n_1^{12}\nu^6)}; \end{aligned} \quad (9)$$

$$\tilde{\sigma} = |\tilde{S}| \leq \sigma n^{|\Sigma|} \exp(10n_1^{12}\nu^6); \quad (10)$$

$$\prod_{v \in \tilde{S} \setminus \tilde{S}_\infty} \ln^3 N_{\tilde{\mathbf{K}}}(v) \leq c(N) \left( \prod_{v \in S \setminus S_\infty} \ln^3 N_{\mathbf{K}}(v) \right)^{n^{|\Sigma|} \exp(10n_1^{12}\nu^6)}; \quad (11)$$

$$\tilde{n} = \deg_Y \tilde{f}(X, Y) = n\nu; \quad (12)$$

$$\tilde{N} = \max(2, \deg \tilde{f}(X, Y)) \leq 4\nu n_1^3 n; \quad (13)$$

$$|\tilde{\Sigma}| \leq \nu |\Sigma|;$$

$$\tilde{h} = \max(1, h(\tilde{f})) \leq \left( \exp_2(66n_1^{21}\nu^{11}) \right) N^{14} h + c(N, \nu). \quad (14)$$

Note also, that, as follows from the definition of the field  $\tilde{\mathbf{K}}$ ,

$$\Sigma \subseteq C(\tilde{\mathbf{K}}).$$

Hence

$$d_{\rho-2}(\tilde{\Sigma}/\tilde{\mathbf{K}}) \leq d_0(\tilde{\Sigma}/\tilde{\mathbf{K}}) = [\tilde{\mathbf{K}}(\tilde{\Sigma}) : \tilde{\mathbf{K}}] \leq \nu^{|\Sigma|}. \quad (15)$$

Substituting (8)–(15) to (7), we get (1) after easy calculations.

## 2 Curves of genus 0.

Assume that  $\mathbf{g}(C) = 0$  and  $|\Sigma| \geq 3$ . Then it is wellknown that the set  $C(x, \mathbf{K}, S)$  is effectively bounded. However, as much as we know, the first explicit bound was computed only recently in [Po93]. In this section we show that such a bound also follows from our Theorem 1B.

**Theorem 5B.** *Assume that  $\mathbf{g}(C) = 0$  and  $|\Sigma| \geq 3$ . Let  $\varepsilon > 0$ . Then for any  $Q \in C(x, \mathbf{K}, S)$  we have*

$$h_x(Q) \leq c(N, d, \varepsilon) \left( \sigma^{20\sigma} D^{\frac{3}{2}} p^d \prod_{v \in S \setminus S_\infty} \ln N_{\mathbf{K}}(v) \right)^{n^3 - 3n^2 + 2n + \varepsilon} e^{(4N)^{17} dh}. \quad (1)$$

**Proof.** Since  $\mathbf{g}(C) = 0$ , we have

$$\begin{aligned} \rho(\Sigma) &= |\Sigma| - 1, \\ \lambda_2(\Sigma) &= 2, \\ \Lambda &= \max(\lambda_2(\Sigma), N) = N, \end{aligned}$$

and we obtain (1) immediately from Theorem 1B.

### 3 Curves of genus 1.

The first effective upper bound for integral points on elliptic curves is due to A. Baker and J. Coates [BaC70], only for the case  $\mathbf{K} = \mathbf{Q}$  and  $S = S_\infty$ . This bound was very large and was sharpened by S.V. Kotov and L.A. Trelina [KTr79], who also restricted themselves only to  $\mathbf{K} = \mathbf{Q}$ , but considered arbitrary  $S$ . In our terms, they proved that, provided  $\mathbf{g}(C) = 1$ , for any  $Q \in C(x, \mathbf{Q}, S)$

$$h_x(Q) \leq c(N)\sigma^{8^4+N^8(\sigma+1)}e^{(8^6+4N^6+N^8)(\sigma+1)h}p^{8^2+N^6}.$$

A rather sharp bound was recently obtained by W. Schmidt [Schm92] for arbitrary  $\mathbf{K}$  and  $S = S_\infty$ . He proved that, provided  $\mathbf{g}(C) = 1$ , for any  $Q \in C(x, \mathbf{K}, S_\infty)$

$$h_x(Q) \leq c(d, N)D^{433N}e^{(4N)^{13}dh}.$$

Our Theorem 5A implies, for arbitrary  $\mathbf{K}$  and  $S$ , a bound of the same type that Schmidt's.

**Theorem 5C.** *Assume that  $\mathbf{g}(C) = 1$ . Then for any  $Q \in C(x, \mathbf{K}, S)$  we have*

$$h_x(Q) \leq c(N, d) \left( \sigma^\sigma D p^d \right)^{c_{31}n} \left( \prod_{v \in S \setminus S_\infty} N_{\mathbf{K}}(v) \right)^{1024n} e^{c_{32}N^{33}dh}, \quad (1)$$

where  $c_{31} = \exp(2 \cdot 10^8)$ ,  $c_{32} = \exp_2(10^{15})$ .

**Proof.** Without loss of generality  $|\Sigma| = 1$ . Let  $\Sigma = \{P\}$ , and assume that  $P$  is the origin of the group law on the elliptic curve  $C$ . Following [La78, Sec.6.3], take in Theorem 5A  $\tilde{C} = C$ , and  $\varphi$  – the multiplication by 2. Then  $\tilde{\Sigma} = \text{Ker } \varphi$ ,  $\rho(\tilde{\Sigma}) = 3$ . Hence we may use Theorem 5A with  $\Lambda = \lambda_2(\tilde{\Sigma}) \leq 4$ ,  $\nu = 4$  and  $n_1 = 2$ . Substituting this data to (1.1), we get (1).

### 4 Hyperelliptic curves.

Let  $C$  be a hyperelliptic curve. Then we have the *canonical double covering*

$$\kappa : C \rightarrow \mathbf{P}^1,$$

ramified at  $2\mathbf{g} + 2$  *Weierstrass points* of  $C$ . Each fiber of  $\kappa$  may be considered as a set or as a divisor; it will be clear from the context in what sense the word “fiber” is used.

J.-P. Serre [Se89] noted that if  $\Sigma$  contains a fiber of  $\kappa$ , then  $C(x, \mathbf{K}, S)$  is effectively bounded. A corresponding explicit bound was obtained by D. Poulakis [Po92] in the case  $S = S_\infty$ . He proved that, if  $C$  is hyperelliptic and  $\Sigma$  contains a fiber of  $\kappa$ , then for any  $Q \in C(x, \mathbf{K}, S_\infty)$

$$h_x(Q) \leq c(N, d) D^{c_{41}(\mathbf{g})N^3 d^2} e^{c_{42}(\mathbf{g})N^{18} d^2 h}, \quad (1)$$

where  $c_{41}, c_{42}$  are of the type  $\mathbf{g}^{c\mathbf{g}}$ . However, one may expect here a bound of the same type, as Schmidt's bound for elliptic curves (see the previous section), i.e. the bound of the type  $c(N, d) D^{c(N)} e^{c(N)dh}$ . We shall see that such a bound follows easily from our Theorem 5A, though we get a worse, than in (1), dependence in  $\mathbf{g}$ .

When  $C$  is defined by a canonical equation  $y^2 = f(x)$ , where  $\deg f = 2\mathbf{g} + 1$  or  $2\mathbf{g} + 2$ , then the canonical covering is given by  $x$ , and  $\text{supp}(x)_\infty$  is exactly a fiber of  $\kappa$ . Of course, in this case effective bounds for integral and  $S$ -integral points were obtained much earlier. See [Ba69], [Sp76], [Tr78], [Sp82], and bibliographies in [Sp82] and [ShT86]. We do not consider this case separately because it is covered by our Theorems 5D and 5F.

**Theorem 5D.** *Assume that  $C$  is hyperelliptic and  $\Sigma$  contains a fiber of  $\kappa$ . Then for any  $Q \in C(x, \mathbf{K}, S)$*

$$h_x(Q) \leq c(N, d) (\sigma^\sigma D p^d)^{c_{43}(\mathbf{g})n^2} \left( \prod_{v \in S \setminus S_\infty} N_{\mathbf{K}}(v) \right)^{c_{44}n^2} e^{c_{45}(\mathbf{g})N^{38}dh},$$

where  $c_{43} = \exp(2 \cdot 10^8 \mathbf{g}^{12})$ ,  $c_{44} = 2^{18}$ ,  $c_{45}(\mathbf{g}) = \exp_2(10^{15} \mathbf{g}^{21})$ .

We need some elementary properties of hyperelliptic curves.

For any (ramified) covering  $C \rightarrow \mathbf{P}^1$  its fibers form a linear system on  $C$ , and we say that the covering is *special* if the corresponding linear system is special.

**Lemma 1.** *Let  $\kappa : C \rightarrow \mathbf{P}^1$  be as above, and  $\varphi : \tilde{C} \rightarrow C$  – an unramified double covering. Then  $\kappa \circ \varphi : \tilde{C} \rightarrow \mathbf{P}^1$  is special.*

**Proof.** If  $\mathbf{g}(C) \geq 3$ , then  $\mathbf{g}(\tilde{C}) = 2\mathbf{g}(C) - 1 \geq 5$ , and  $\kappa \circ \varphi$  is special because its degree is 4. If  $\mathbf{g}(C) = 2$ , then the fibers of  $\kappa \circ \varphi$  belong to the canonical class of  $\tilde{C}$ , which is special.

**Lemma 2.** [Wa50, Th.6.7.1] *Let  $C$  be hyperelliptic, and  $\psi : C \rightarrow \mathbf{P}^1$  be special. Then there exists a ramified covering  $\delta : \mathbf{P}^1 \rightarrow \mathbf{P}^1$  such that  $\psi = \delta \circ \kappa$ .*

**Proof of Theorem 5D.** Without loss of generality assume that  $\Sigma$  is a fiber of  $\kappa$ . It is well known that there exists a double unramified covering  $\varphi_1 : C_1 \rightarrow C$  by another hyperelliptic curve  $C_1$ . By Lemma 1  $\kappa \circ \varphi_1$  is special. Hence by Lemma 2

$\kappa \circ \varphi_1 = \delta \circ \kappa_1$ , where  $\kappa_1 : C_1 \rightarrow \mathbf{P}^1$  is the canonical double covering of  $\mathbf{P}^1$  by  $C_1$ , and  $\delta : \mathbf{P}^1 \rightarrow \mathbf{P}^1$ . This yields that  $\varphi_1^{-1}(\Sigma)$  consists of two fibers of  $\kappa_1$ . Further, consider a double unramified covering  $\varphi_2 : \tilde{C} \rightarrow C_1$ , where  $\tilde{C}$  is one more hyperelliptic curve. Hence  $\tilde{\Sigma} = \varphi^{-1}(\Sigma)$  consists of four fibers of  $\tilde{\kappa}$ , where  $\varphi = \varphi_1 \circ \varphi_2$  and  $\tilde{\kappa} : \tilde{C} \rightarrow \mathbf{P}^1$  is the canonical covering of  $\mathbf{P}^1$  by  $\tilde{C}$ . Since the fibers of  $\tilde{\kappa}$  are linearly equivalent, we have  $\rho(\tilde{\Sigma}) \geq 3$ ,  $\tilde{\Lambda} = \lambda_2(\tilde{\Sigma}) \leq 4$ . Now applying Theorem 5A, we get (1).

## 5 The Thue equation.

By Thue equation we mean the Diophantine equation

$$f(X, Y) = A, \quad (1)$$

where  $A$  and the coefficients of the binary form  $f$  belong to an algebraic number field  $\mathbf{K}$ ,  $A \neq 0$  and  $f$  has at least 3 pairwise distinct linear factors. This equation and its generalizations were effectively studied in numerous papers of A. Baker, J. Coates, J.-H. Evertse, N.I. Feldman, K. Györy, S.V. Kotov, Z.Z. Papp, T. Shorey, V.G. Sprindžuk, R.J. Stroeker, N. Tzanakis, B.M.M. de Weger and many other authors; see [Sp74], [Sp80], [Sp84], [ShT86] and [EG87] for historical accounts and extensive bibliography.

In this section we show that Theorem 1B implies effective bounds for  $S$ -integral solutions of Thue equation. Since we study  $S$ -integral solutions, we do not consider separately Thue–Mahler equation. Of course, such or better bound can also be derived using classical methods; the goal of this section, as well as of Sections 2–4, is not so much to obtain new results, but to show that Theorems 1B and 5A generalize some classical facts.

**Theorem 5E.** *Let  $f(X, Y) \in \mathbf{K}[X, Y]$ , and assume that  $f(X, Y)$  is of the form*

$$f(X, Y) = f_1(X, Y) \prod_{i=1}^3 (\alpha_i X + \beta_i Y + \gamma_i) - A, \quad (2)$$

where  $f_1(X, Y) \in \bar{\mathbf{Q}}[X, Y]$  is an arbitrary polynomial, and

$$A \cdot \begin{vmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{vmatrix} \cdot \begin{vmatrix} \alpha_1 & \beta_1 \\ \alpha_3 & \beta_3 \end{vmatrix} \cdot \begin{vmatrix} \alpha_2 & \beta_2 \\ \alpha_3 & \beta_3 \end{vmatrix} \neq 0. \quad (3)$$

Then each solution  $(X_0, Y_0) \in \mathcal{R}_{\mathbf{K}}(S) \times \mathcal{R}_{\mathbf{K}}(S)$  of

$$f(X, Y) = 0 \quad (4)$$

satisfies

$$h(X_0), h(Y_0) \leq c(N, d) \left( \sigma^{20\sigma} D^{\frac{3}{2}} p^d \prod_{v \in S \setminus S_\infty} \ln^3 N_{\mathbf{K}}(v) \right)^{N!} e^{(14N)^{N+14} dh}. \quad (5)$$

In particular, we have an effective bound for  $S$ -integral solutions of the equation

$$N_{\mathbf{L}/\mathbf{K}}(X + \beta Y + \gamma) = A,$$

where  $\mathbf{L} = \mathbf{K}(\beta)$ ,  $[\mathbf{L} : \mathbf{K}] \geq 3$  and  $A \in \mathbf{K} \setminus 0$ . In the case  $S = S_\infty$ , such a bound follows from a theorem of Sprindžuk [Sp74a], [Sp82, §4.5].

**Proof.** Fix a solution  $(X_0, Y_0)$ . Then for some  $\mathbf{K}$ -irreducible factor  $g(X, Y)$  of  $f(X, Y)$  we have

$$g(X_0, Y_0) = 0.$$

It is wellknown that, if the polynomial  $g(X, Y) \in \mathbf{K}[X, Y]$  is irreducible over  $\mathbf{K}$ , but reducible over  $\bar{\mathbf{Q}}$ , then the solutions  $(X_0, Y_0) \in \mathbf{K} \times \mathbf{K}$  of  $g(X, Y) = 0$  satisfy

$$h(X_0), h(Y_0) \leq c(\deg g)(h(g) + 1) \quad (6)$$

(see [Sp82, §9.6]). Hence we may assume that  $g(X, Y) = 0$  is absolutely irreducible.

Let  $C$  be a non-singular model of the plane curve  $g(X, Y) = 0$ , and  $x, y \in \mathbf{K}(C)$  correspond to the coordinate functions of this plane curve. Denote

$$\Sigma = \text{supp}(x)_\infty \cup \text{supp}(y)_\infty.$$

Clearly,  $z_i = \alpha_i x + \beta_i y + \gamma_i$  are  $\Sigma$ -units. We shall prove that  $z_1$  and  $z_2$  are multiplicatively independent mod  $\bar{\mathbf{Q}}^*$  and hence  $\rho(\Sigma) \geq 2$ .

Indeed, we have  $\alpha_3 x + \beta_3 y + \gamma_3 = \alpha z_1 + \beta z_2 + \gamma$ , where  $\alpha \beta \neq 0$  by (3). Hence we have  $\varphi(z_1, z_2) = 0$ , where

$$\varphi(Z_1, Z_2) = Z_1 Z_2 (\alpha Z_1 + \beta Z_2 + \gamma) \varphi_1(Z_1, Z_2) - A,$$

for some polynomial  $\varphi_1(Z_1, Z_2)$ .

Now suppose that  $z_1, z_2$  are multiplicatively dependent. Then  $\Phi(z_1, z_2) = 0$ , where  $\Phi(Z_1, Z_2)$  is a polynomial of one of the types  $Z_1^{p_1} Z_2^{p_2} - \mu$  or  $Z_1^{p_1} - \mu Z_2^{p_2}$ . Here  $\mu \in \bar{\mathbf{Q}}^*$ ,  $p_1, p_2 \geq 0$  and  $(p_1, p_2) = 1$ .

Clearly,  $\varphi(Z_1, Z_2)$  and  $\Phi(Z_1, Z_2)$  have a common factor. But  $\Phi(Z_1, Z_2)$  is irreducible, hence  $\Phi | \varphi$ . However, if  $\Phi = Z_1^{p_1} - \mu Z_2^{p_2}$  and  $p_1, p_2 > 0$ , then  $\Phi(0, 0) = 0$ , and  $\varphi(0, 0) = -A \neq 0$ . If  $\Phi = Z_1^{p_1} Z_2^{p_2} - \mu$  and  $p_1 > 0$ , then, taking  $\delta_1$  satisfying the equation

$$(-1)^{p_2} (\alpha \delta_1 + \gamma)^{p_2} \delta_1^{p_1} = \beta^{p_2} \mu,$$

and defining

$$\delta_2 = -\beta^{-1}(\alpha\delta_1 + \gamma),$$

we have  $\Phi(\delta_1, \delta_2) = 0$ ,  $\varphi(\delta_1, \delta_2) = -A \neq 0$ . In the both cases we get a contradiction. Hence  $\rho(\Sigma) \geq 2$ , and clearly  $\lambda(\Sigma) \leq c(N)$ .

There exists  $a \in \mathbf{Z}$ ,  $|a| \leq N$  such that  $\text{supp}(x - ay)_\infty = \Sigma$ . By Theorem 1B

$$h(X_0 - aY_0) \leq c(N, d) \left( \sigma^{20\sigma} D^{\frac{3}{2}} p^d \prod_{v \in S \setminus S_\infty} \ln^3 N_{\mathbf{K}}(v) \right)^{N!} e^{(4N)^{N+14} dh'}, \quad (7)$$

where  $h' = h(g) \leq h(f) + N$ . From (4), (7) one easily gets (5).

## 6 Strongly ramified coverings.

The following result is due to the author [Bi88a], where it is proved by another method (for  $S = S_\infty$ ).

**Theorem 5F.** For  $\alpha \in \mathbf{P}^1$  denote

$$e_\alpha = \text{g.c.d.} \{e_P \mid x(P) = \alpha\}. \quad (1)$$

Suppose that

$$\sum_{\alpha \neq \infty} (1 - e_\alpha^{-1}) > 1. \quad (2)$$

Then for any  $Q \in C(x, \mathbf{K}, S)$  we have

$$h_x(Q) \leq c(N, d) \left( \sigma^\sigma D p^d e^{dh} \prod_{v \in S \setminus S_\infty} N_{\mathbf{K}}(v) \right)^{c(N)}. \quad (3)$$

**Proof.** We have two possible cases. Either

(i)  $e_\alpha \geq 3$ ,  $e_\beta \geq 2$  for distinct  $\alpha, \beta \in \bar{\mathbf{Q}}$ , or

(ii)  $e_{\alpha_1} = e_{\alpha_2} = e_{\alpha_3} = 2$  for distinct  $\alpha_1, \alpha_2, \alpha_3 \in \bar{\mathbf{Q}}$ .

In the case (i), put  $p = e_\alpha$ ,  $q = e_\beta$  and denote by  $\varepsilon_p, \varepsilon_q$  primitive roots of unity of degrees  $p$  and  $q$  respectively. Put also

$$\begin{aligned} \gamma &= (\alpha - \beta)^{\frac{1}{q}}, & t &= (x - \beta)^{\frac{1}{q}}, \\ u_i &= (t - \varepsilon_q^i \gamma)^{\frac{1}{p}} & (0 \leq i \leq q-1). \end{aligned}$$

The extension  $\bar{\mathbf{Q}}(C)(t, u_0, u_1)/\bar{\mathbf{Q}}(C)$  corresponds to a covering  $\varphi : \tilde{C} \rightarrow C$  unramified over  $C \setminus \Sigma$ , where  $\Sigma = \Sigma(x)$ . Functions  $u_0, u_1$  satisfy the equation

$$u_0^p - u_1^p = (\varepsilon_q - 1)^\gamma \gamma.$$

By the method of the previous section we can prove that  $z_i = u_0 - \varepsilon_p^i u_1$  ( $i = 0, 1$ ) are  $\tilde{\Sigma}$ -units multiplicatively independent mod  $\bar{\mathbf{Q}}^*$ , where  $\tilde{\Sigma} = \varphi^{-1}(\Sigma)$ .

In the case (ii) denote  $t_i = \sqrt{x - \alpha_i}$  ( $i = 1, 2, 3$ ), and  $z_i = t_i - t_3$  ( $i = 1, 2$ ). Again, the extension  $\bar{\mathbf{Q}}(C)(t_1, t_2, t_3)/\bar{\mathbf{Q}}(C)$  corresponds to a covering  $\varphi : \tilde{C} \rightarrow C$  unramified over  $C \setminus \Sigma$ , and  $z_1, z_2$  are  $\tilde{\Sigma}$ -units. If they are multiplicatively dependent then  $\Phi(z_1, z_2) = 0$ , where  $\Phi(Z_1, Z_2)$  is as in the previous section. The functions  $z_1, z_2$  also satisfy  $g(z_1, z_2) = 0$ , where

$$g(Z_1, Z_2) = Z_1^2 Z_2 - Z_1 Z_2^2 + (\alpha_1 - \alpha_3) Z_2 - (\alpha_2 - \alpha_3) Z_1.$$

If we prove that  $g$  is irreducible, we shall obtain  $\Phi = \lambda g$  ( $\lambda \in \bar{\mathbf{Q}}$ ), which is a contradiction. Hence  $z_1, z_2$  are multiplicatively independent mod  $\bar{\mathbf{Q}}^*$ .

To prove that  $g(Z_1, Z_2)$  is irreducible consider its discriminant with respect to  $Z_1$ :

$$\Delta(Z_2) = Z_2^4 + Z_2^2(-4\alpha_1 + 2\alpha_2 + 2\alpha_3) + (\alpha_2 - \alpha_3)^2.$$

The discriminant of  $\Delta(Z_2)$  is

$$4096(\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 \neq 0.$$

Hence  $\Delta(Z_2)$  is not a square, and therefore  $g(Z_1, Z_2)$  is irreducible.

Thus, in the both cases  $\rho(\tilde{\Sigma}) \geq 2$ . We have also  $\nu \leq \max(8, n^2)$ ,  $\tilde{\Lambda} \leq c(N)$ ,  $n_1 \leq N^2$ . By Theorem 5A we get (3).

## 7 Galois coverings.

**Theorem 5G.** *Assume that  $x : C \rightarrow \mathbf{P}^1$  is a Galois covering, and  $\mathbf{g}(C) \geq 1$ . Then for any  $Q \in C(x, \mathbf{K}, S)$  we have (6.3).*

**Proof.** For any  $\alpha \in \mathbf{P}^1$  and  $P \in \text{supp}(x_\alpha)_0$  we have  $e_P = e_\alpha$ . Hence we may write Hurwitz formula as

$$2\mathbf{g} - 2 + 2n = \sum_{\alpha \in \mathbf{P}^1} \frac{n}{e_\alpha} (e_\alpha - 1).$$

Then

$$\sum_{\alpha \neq \infty} (1 - e_\alpha^{-1}) = 1 + \frac{2\mathbf{g} - 2}{n} + e_\infty^{-1} > 1,$$

and we may apply Theorem 5F.

## 8 The results of H. Kleiman.

Let  $G$  be the monodromy group of the covering  $x : C \rightarrow \mathbf{P}^1$ , i.e.  $G = \text{Gal}(\mathcal{K}/\bar{\mathbf{Q}}(x))$ , where  $\mathcal{K}$  is the smallest extension of  $\bar{\mathbf{Q}}(C)$ , normal over  $\bar{\mathbf{Q}}(x)$ . We use here the standard representations of  $G$  by permutations of the set  $\{1, \dots, n\}$ . A permutation  $\sigma$  is *stabilizing* if  $\sigma(i) = i$  for some  $i \in \{1, \dots, n\}$ .

Let  $\Delta(X)$  be the discriminant of  $f(X, Y)$  with respect to  $Y$ . Although the following assertion is not stated explicitly in [Kl76], it can be easily deduced from the argument on p. 129 of Kleiman's paper.

**Proposition 1.** *If*

- (i) *all stabilizing permutations of  $G$  are even and*
- (ii)  *$\Delta(X)$  has at least 3 distinct roots of odd order,*

*then  $C(x, \mathbf{K}, S)$  is effectively bounded.*

Kleiman proves also

**Proposition 2** [Kl76, Th.4]. *Let  $\mathbf{K}_0$  be the smallest field containing the coefficients of  $f(X, Y)$ . Assume that  $G$  is imprimitive with two sets of imprimitivity, and all  $\mathbf{K}_0$ -irreducible factors of  $\Delta(X)$  are of degree at least 3. Then  $C(x, \mathbf{K}, S)$  is effectively bounded.*

We shall prove that Propositions 1 and 2 follow from Theorem 5F. In particular, we have a bound (6.3) for  $Q \in C(x, \mathbf{K}, S)$ .

**Proof of Proposition 1.** A permutation  $\sigma$  is *of the type*  $(e_1, \dots, e_s)$  if it is a product of  $s$  commuting cycles  $\xi_1, \dots, \xi_s$  of lengths  $e_1, \dots, e_s$ , respectively. Let now  $\alpha \in \mathbf{P}^1$ ,  $\text{supp}(x_\alpha)_0 = \{P_1, \dots, P_s\}$  and  $e_i = e_{P_i}$  ( $1 \leq i \leq s$ ). Then there exists  $\sigma = \sigma_\alpha \in G$  of the type  $(e_1, \dots, e_s)$  [Che48, §41].

The condition (i) implies now that, if  $\sigma_\alpha$  is an odd permutation then all the numbers  $e_i$  are even and thus  $e_\alpha \geq 2$ . (If some  $e_i$  is odd, then  $\sigma_\alpha^{e_i}$  is an odd permutation, stabilizing the elements of the cycle  $\xi_i$ .) The condition (ii) means that for at least three distinct  $\alpha \neq \infty$ , the permutation  $\sigma_\alpha$  is odd. Thus

$$\sum_{\alpha \neq \infty} (1 - e_\alpha^{-1}) \geq \frac{3}{2},$$

i.e. (6.2) holds.

**Proof of Proposition 2.** Let  $I_1$  and  $I_2$  be the imprimitivity sets and

$$H = \{\sigma \in G \mid \sigma I_1 = I_1\}.$$

Then  $[G : H] = 2$ , therefore  $[\mathcal{K}^H : \bar{\mathbf{Q}}(x)] = 2$ , where  $\mathcal{K}$  is defined in the beginning of the section. Since  $H$  contains all stabilizing permutations from  $G$ ,  $\mathcal{K}^H$  is subfield of  $\bar{\mathbf{Q}}(C)$ .

There exists at least one  $\alpha \in \mathbf{P}^1 \setminus \{\infty\}$  ramified in  $\mathcal{K}^H$ . This implies that  $2 \mid e_\alpha$ . Let  $\alpha = \alpha_1, \dots, \alpha_m$  be all conjugates of  $\alpha$  over  $\mathbf{K}_0$ . Then  $e_{\alpha_i} = e_\alpha \geq 2$  for  $1 \leq i \leq m$ . We get

$$\sum_{\alpha \neq \infty} (1 - e_\alpha^{-1}) \geq \frac{m}{2} \geq \frac{3}{2},$$

and (6.2) is again satisfied.

# Bibliography

- [Ba66] **A. Baker**, Linear forms in the logarithms of algebraic numbers I, *Mathematica* **13** (1966), 204–216; II, *ibid.* **14** (1967), 102–107; III, *ibid.* **14** (1967); 220–224; IV, *ibid.* **15** (1968), 204–216.
- [Ba68] **A. Baker**, Contributions to the theory of Diophantine equations. I, II, *Phil. Trans. R. Soc. London Ser.A* **263** (1967–68), 173–208.
- [Ba68a] **A. Baker**, The Diophantine equation  $y^2 = ax^3 + bx^2 + cx + d$ , *J. London Math. Soc.* **43** (1968), 1–9.
- [Ba68b] **A. Baker**, Bounds for the solutions of the hyperelliptic equations, *Proc. Camb. Phil. Soc.*, **65** (1969), 439–444.
- [Ba77] **A. Baker**, The theory of linear forms in logarithms, in *Transcendence Theory: Advances and Applications*, London, Academic Press, 1977, 1–27.
- [BaC70] **A. Baker**, **J. Coates**, Integer points on curves of genus 1, *Proc. Camb. Phil. Soc.* **67** (1970), 592–602.
- [BaWü] **A. Baker**, **G. Wüstholz**, Logarithmic forms and Group Varieties, to appear.
- [BGMMS90] **J. Blass**, **A.M.W. Glass**, **D.K. Manski**, **D.B. Meronk**, **R.P. Steiner**, Constants for lower bounds for linear forms in the logarithms of algebraic numbers I, II, *Acta Arithm.* **55** (1990), 1–22.
- [Bi88] **Yu. Bilu** (Belotserkovski), Effective analysis of a class of Diophantine equations (Russian), *Vestsi Akad. Navuk BSSR, Ser. Fiz.-Math. Navuk*, 1988, no. 3, 111–115
- [Bi88a] **Yu. Bilu** (Belotserkovski), Effective analysis of a new class of Diophantine equations (Russian), *Vestsi Akad. Navuk BSSR, Ser. Fiz.-Math. Navuk*, 1988, no. 6, 34–39, 125

- [Bi91] **Yu. Bilu** (Belotserkovski), Diophantine equations and units of algebraic function fields (Russian), *Vestsi Akad. Navuk BSSR, Ser. Fiz.-Math. Navuk*, 1991, no. 6, 114.
- [Bi94] **Yu. Bilu**, Effective analysis of integer points on algebraic curves, *Israel J. of Math.*, to appear.
- [Bo83] **E. Bombieri**, On Weil's "Théorème de Décomposition", *Amer. J. Math.* **105** (1983), 295–308.
- [Bo93] **E. Bombieri**, Effective Diophantine Approximation on  $\mathbf{G}_m$ , to appear.
- [BrGyT86] **B. Brindza, K. Györy, R. Tijdeman**, On the Catalan equation over algebraic number fields, *J. reine angew. Math.* **367**, 90–102.
- [CF67] **J.W.S. Cassels, A. Fröhlich** (eds.), *Algebraic Number Theory*, Academic Press, 1967.
- [Co70] **J. Coates**, Construction of rational functions on a curve, *Proc. Camb. Phil. Soc.* **68** (1970), 105–123.
- [Che48] **N.G. Chebotarev**, *The Theory of Algebraic Functions* (Russian), Moscow–Leningrad, 1948.
- [Do79] **E. Dobrowolski**, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arithm.* **34** (1979), 391–401.
- [EG88] **J.-H. Evertse, K. Györy**, Decomposable form equations, *New advances in Transcendence Theory*, Cambridge Univ. Press, 1988, 175–202.
- [EGST88] **J.-H. Evertse, K. Györy, C.L. Stewart, R. Tijdeman**,  $S$ -unit equations and their applications, *New advances in Transcendence Theory*, Cambridge Univ. Press, 110–174.
- [Fa83] **G. Faltings**, Endlichkeitssätze für abelche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366; Erratum: **75** (1984), p.381.
- [Fe74] **N.I. Feldman**, Estimates for linear forms in logarithms of algebraic numbers and some of their applications, *Current Problems of Analytic Number Theory*, Nauka i Tehnika, Minsk, 1974, 244–268.
- [Fe82] **N.I. Feldman**, *Seventh Problem of Hilbert* (Russian), Moscow Univ. Press, 1982.

- [FrV91] **M.D. Fried, H. Völklein**, The inverse Galois problem and rational points on moduli spaces, *Math. Ann.* **290** (1991), 771–800.
- [Ge52] **A.O. Gelfond**, *Transcendent and Algebraic Numbers* (Russian), Moscow 1952; English trans.: New York, Dover, 1960.
- [Kl76] **H. Kleiman**, On the Diophantine equation  $f(x, y) = 0$ , *J. reine und angew. Math.* **286/287** (1976), 124–131.
- [KTr79] **S.V. Kotov, L.A. Trellina**,  $S$ -ganze Punkte auf elliptischen Kurven, *J. reine und angew. Math.* **306** (1979), 28–41.
- [KuLa81] **D. Kubert, S. Lang**, *Modular Units*, Springer, 1981.
- [La70] **S. Lang**, *Algebraic Number theory*, Addison - Wesley, 1970.
- [La78] **S. Lang**, *Elliptic Curves: Diophantine Analysis*, Springer, 1978.
- [La83] **S. Lang**, *Fundamentals of Diophantine Geometry*, Springer, 1983.
- [Lav70] **A.F. Lavrik**, A remark on the Siegel-Brauer theorem concerning the parametres of algebraic number fields (Russian), *Mat. Zametki* **8** (1970), 259–263. (English Trans.: *Math. Notes* **8** (1970), 615–617.)
- [Ma88] **D.W. Masser**, Linear relations on algebraic groups, *New advances in Transcendence Theory*, Cambridge Univ. Press, 1988, 248–263.
- [Po92] **D. Poulakis**, Points entiers sur les courbes hyperelliptiques, *Acta Arithm.* **62** (1992), 25–43.
- [Po93] **D. Poulakis**, Points entiers sur les courbes de genre 0, *Colloquium Math.* **66** (1993), 1–7.
- [PW88] **P. Philippon, M. Waldschmidt**, Lower bounds for linear forms in logarithms, *New advances in Transcendence Theory*, Cambridge Univ. Press, 1988, 280–312.
- [Schm76] **W.M. Schmidt**, *Equations over finite fields. An elementary approach*. Lecture Notes in Math. **536**, Springer 1976.
- [Schm90] **W.M. Schmidt**, Eisenstein’s theorem on power series expansions of algebraic functions, *Acta Arithm.* **56** (1990), 161–179.
- [Schm91] **W.M. Schmidt**, Construction and Estimation of Bases in Function Fields, *J. Number Theory* **39** (1991), 181–224.
- [Schm92] **W.M. Schmidt**, Integer points on curves of genus 1, *Compositio Math.* **81** (1992), 33–59.

- [Se89] **J.-P. Serre**, *Lectures on the Mordell–Weil Theorem*, Vieweg, 1989.
- [ShT86] **T.N. Shorey, R. Tijdeman**, *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge, 1986.
- [ShvPTSc77] **T.N. Shorey, A. van der Poorten, R. Tijdeman, A. Schinzel**, Applications of Gelfond–Baker method to Diophantine equations, *Transcendence Theory: Advances and Applications*, Academic Press, 1977, 59–77.
- [Sie29] **C.L. Siegel**, Über einige Anwendungen Diophantischer Approximationen, *Abh. Preuss Akad. Wiss. Phys.-Math. Kl.*, 1929, Nr. 1.
- [Sie69] **C.L. Siegel**, Abschätzung von Einheiten, *Nachr. Akad. Wiss. Göttingen II. Math.-Phys. Kl.*, 1969, Nr. 9, 71–86.
- [Sil84] **J.H. Silverman**, Lower bounds for height functions, *Duke Math. J.* **51** (1984), 395–403.
- [Sp74] **V.G. Sprindžuk**, Effective analysis of Thue and Thue–mahler equations, *Current Problems of Analytic Number Theory*, Nauka i Tehnika, Minsk, 1974, 199–222.
- [Sp74a] **V.G. Sprindžuk**, Representations of numbers by the norm forms with two dominating variables, *J. Number Theory*, **6** (1974), 481–486.
- [Sp76] **V.G. Sprindžuk**, Hyperelliptic Diophantine equation and class numbers (Russian), *Acta Arithm.* **30** (1976), 95–106.
- [Sp80] **V.G. Sprindžuk**, Achievements and problems in Diophantine approximation theory (Russian), *Uspekhi Mat. Nauk* **35** (1980), No. 4, 3–68, 248. (English Transl.: *Russian Math. Surv.* **35**, No. 4, 1–80.)
- [Sp82] **V.G. Sprindžuk**, *Classical Diophantine Equations in Two Unknowns* (Russian), Nauka, Moscow, 1982.
- [Sp83] **V.G. Sprindžuk**, Arithmetic specializations in polynomials, *J. reine und angew. Math.* **340** (1983), 26–52.
- [Tr78] **L.A. Trelina**,  $S$ -integral solutions of Diophantine equations of hyperelliptic type (Russian), *DAN BSSR* **22** (1978), No. 10, 881–884.
- [V87] **P. Vojta**, *Diophantine Approximation and Value Distribution Theory*, Lecture Notes in Math. **1239**, Springer, 1987.
- [vP77] **A.J. van der Poorten**, Linear forms in logarithms in the  $p$ -adic case, *Transcendence Theory: Advances and Applications*, London, Academic Press, 1977, 29–57.

- [Wa50] **R. Walker**, *Algebraic curves*, Princeton, NJ, 1950.
- [Wü88] **G. Wüstholz**, A new approach to Baker's theorem on linear forms in logarithms III, *New advances in Transcendence Theory*, Cambridge Univ. Press, 1988, 399–410.
- [Yu90] **Kunrui Yu**, Linear forms in  $p$ -adic logarithms II, *Compositio Math.* **74** (1990), 15–113.
- [Zv85] **E.I. Zverovich**, On the construction of the algebraic function field, corresponding to a given covering of the sphere (Russian), *DAN BSSR* **29** (1985), No.2, 104–107.
- [Zv87] **E.I. Zverovich**, An algebraic method of the construction of the main functionals of a Riemann surface, defined as a finite covering of the sphere (Russian), *Siberian Math. J.* **28** (1987), No 6, 32–43.