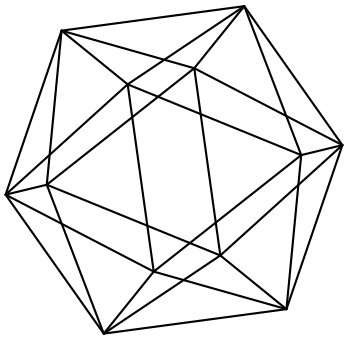
Max-Planck-Institut für Mathematik
Bonn

Counting number fields in fibers

by

Yuri Bilu
(with an appendix by Jean Gillibert)



Max-Planck-Institut für Mathematik
Preprint Series 2016 (35)

Counting number fields in fibers

Yuri Bilu
(with an appendix by Jean Gillibert)

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Institut de Mathématiques de Bordeaux
Université de Bordeaux
351, cours de la Libération
33405 Talence
France

Institut de Mathématiques de Toulouse
Université Paul Sabatier
118 route de Narbonne
31062 Toulouse Cedex 9
France

MPIM 16-35

Counting Number Fields in Fibers

Yuri Bilu*
(with an appendix by Jean Gillibert§)

August 20, 2016

Abstract

Let X be a projective curve over $\mathbb{Q}$ and $t \in \mathbb{Q}(X)$ a non-constant rational function of degree $n \geq 2$. For every $\tau \in \mathbb{Z}$ pick $P_\tau \in X(\bar{\mathbb{Q}})$ such that $t(P_\tau) = \tau$. Dvornicich and Zannier proved that, for large N, the field $\mathbb{Q}(P_1, \dots, P_N)$ is of degree at least $e^{cN/\log N}$ over $\mathbb{Q}$, where $c > 0$ depends only on X and t. In this paper we extend this result, replacing $\mathbb{Q}$ by an arbitrary number field.

Contents

1 Introduction

Everywhere in this paper "curve" means "smooth geometrically irreducible projective algebraic curve".

Let X be a curve over $\mathbb{Q}$ and $t \in \mathbb{Q}(X)$ a non-constant rational function of degree $n \geq 2$. According to the Hilbert Irreducibility Theorem, for infinitely many (in fact, "overwhelmingly many") $\tau \in \mathbb{Z}$ the fiber $t^{-1}(\tau) \subset X(\bar{\mathbb{Q}})$ is $\mathbb{Q}$-irreducible; that is, the Galois group $G_{\mathbb{Q}} = G_{\bar{\mathbb{Q}}/\mathbb{Q}}$ acts on $t^{-1}(\tau)$ transitively. This can also be re-phrased as follows: for every $\tau \in \mathbb{Z}$ pick $P_\tau \in t^{-1}(\tau)$; then

*Institut de Mathématiques de Bordeaux; yuri@math.u-bordeaux.fr
§Institut de Mathématiques de Toulouse

for infinitely many $\tau \in \mathbb{Z}$ we have $[\mathbb{Q}(P_\tau) : \mathbb{Q}] = n$. See Subsection 4 for a precise statement.

Hilbert's Irreducibility Theorem, however, does not answer the following natural question: among the field $\mathbb{Q}(P_\tau)$, are there "many" distinct? This question is addressed in the article of Dvornicich and Zannier [7], where the following theorem is proved (see [7, Theorem 2(a)]).

Theorem 1.1 *In the above set-up, there exist real numbers $c > 0$, depending on n and on the genus $\mathbf{g} = \mathbf{g}(X)$ and $N_0 > 1$, depending on X and t, such that, for every integer $N \geq N_0$ the number field $\mathbb{Q}(P_1, \ldots, P_N)$ is of degree at least $e^{cN/\log N}$ over $\mathbb{Q}$.*

One may note that the statement holds true independently of the choice of the points P_τ.

An immediate consequence is the following result.

Corollary 1.2 *In the above set-up, there exist real numbers $c = c(\mathbf{g}, n) > 0$ and $N_0 = N_0(X, t) > 1$ such that, for every integer $N \geq N_0$, among the number fields $\mathbb{Q}(P_1), \ldots, \mathbb{Q}(P_N)$ there are at least $cN/\log N$ distinct.*

Theorem 1.1 is best possible, as obvious examples show. Say, if X is (the projectivization of) the plane curve $t = u^2$ and t is the coordinate function, then the field

$$\mathbb{Q}(P_1, \ldots, P_N) = \mathbb{Q}(\sqrt{1}, \sqrt{2}, \ldots, \sqrt{N}) = \mathbb{Q}(\sqrt{p} : p \leq N)$$

is of degree $2^{\pi(N)} \leq e^{cN/\log N}$. On the contrary, Corollary 1.2 is not best possible and was recently refined in [4]. See the introduction of [4] for a brief discussion.

The purpose of the present aarticle is extending Theorem 1.1 from the base field $\mathbb{Q}$ to an arbitrary number field. Such an extension is required for certain applications; see, for instance, [2]. Our principal result is the following theorem.

Theorem 1.3 *Let K be a number field of degree d over $\mathbb{Q}$. Further, let X be a curve over K of genus $\mathbf{g}$ and $t \in K(X)$ a non-constant rational function of degree $n \geq 2$. There exist real numbers $c = c(K, \mathbf{g}, n) > 0$ and $B_0 = B_0(K, X, t) > 1$ such that the following holds. Pick $P_\tau \in t^{-1}(\tau)$ for every $\tau \in \mathcal{O}_K$. Then for every $B \geq B_0$ the number field*

$$K(P_\tau : \ \tau \in \mathcal{O}_K, \ \mathrm{H}(\tau) \leq B)$$

is of degree at least $e^{cB^d/\log B}$ over K.

Here $\mathrm{H}(\cdot)$ is the standard absolute height function, see Section 2.

Again, we have the following immediate consequence.

Corollary 1.4 *In the set-up of Theorem 1.3 there exist $c = c(K, \mathbf{g}, n) > 0$ and $B_0 = B_0(K, X, t) > 1$ such that the following holds. Pick $P_\tau \in t^{-1}(\tau)$ for every $\tau \in \mathcal{O}_K$. Then for every $B \geq B_0$, among the number fields*

$$K(P_\tau) \qquad (\tau \in \mathcal{O}_K, \quad \mathrm{H}(\tau) \leq B)$$

there are at least $cB^d/\log B$ distinct fields.

In Sections 2–7 we obtain various auxiliary results. Theorem 1.3 is proved in Section 8. In the Appendix, Jean Gillibert suggests a more canonical approach to the results of Section 7.

Acknowledgments A substantial part of this article was written during my stay the Max-Planck-Institut für Mathematik in Bonn. I thank this institute for the financial support and stimulating working conditions.

This article belongs to a joint project with Jean Gillibert. I thank him for allowing me to publish this part of this project as a separate article, for adding a beautiful appendix, and for many stimulating discussions.

2 Preliminaries

2.1 Number Fields, Heights and Sizes

Given a number field K, we denote by M_K, M_K^∞ and M_K^0 the sets of all, infinite and finite places of K, respectively. To every place $v \in M_K$ we associate the absolute value $|\cdot|_v$ normalized to extend a standard absolute value on $\mathbb{Q}$: if $v \mid \infty$ then $|2016|_v = 2016$, and if $v \mid p < \infty$ then $|p|_v = p^{-1}$. We also associate, to every finite place $v \in M_K^0$, the additive valuation $v(\cdot)$ normalized so that $v(K^\times) = \mathbb{Z}$; equivalently, $v(\mathcal{N}v) = [K_v : \mathbb{Q}_v]$, where $\mathcal{N}v$ denotes the absolute norm of the prime ideal of v. By convention, we set $\mathcal{N}v = 1$ for $v \in M_K^\infty$.

We denote by $\mathrm{H}(\alpha)$ the multiplicative absolute height of an algebraic number α: if K is a number field containing α then

$$\mathrm{H}(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{[K_v:\mathbb{Q}_v]/[K:\mathbb{Q}]}.$$

We will also widely use the "old-fashioned" notion of the *size* $\overline{|\alpha|}$ of an algebraic number α. If α belongs to a number field K then we set

$$\overline{|\alpha|} = \max\{|\alpha|_v : v \in M_K^\infty\}.$$

Together with this "upper size" one can also define the "lower size"

$$\underline{|\alpha|} = \min\{|\alpha|_v : v \in M_K^\infty\}.$$

We have clearly

$$\begin{aligned}
&\underline{|\alpha|} = \overline{|\alpha^{-1}|}^{-1} && (\alpha \in K \smallsetminus \{0\}),\\
&\underline{|\alpha|} \le \mathrm{H}(\alpha) \le \overline{|\alpha|} && (\alpha \in \mathcal{O}_K \smallsetminus \{0\}), \qquad (1)\\
&\overline{|\alpha+\beta|} \le \overline{|\alpha|} + \overline{|\beta|}, \qquad \overline{|\alpha\beta|} \le \overline{|\alpha|} \cdot \overline{|\beta|} && (\alpha, \beta \in K).
\end{aligned}$$

2.2 Algebraic Curves

Unless the contrary is stated explicitly, everywhere in this note "curve" means "smooth geometrically irreducible projective algebraic curve".

Let X be a curve over a field K of characteristic 0. We fix an algebraic closure $\bar{K}$ of K and we denote by G_K the absolute Galois group of K, that is, the Galois group of $\bar{K}/K$.

We call a *K-place* of the field $K(X)$ a class of non-trivial valuations on $K(X)$ whose restriction to K is trivial. We have a bijective correspondence given by

$$P \leftrightarrow \text{the class of } v_P(\cdot)$$

between the set $X(\bar{K})$ of $\bar{K}$-points of X, and the set of $\bar{K}$-places of $\bar{K}(X)$. (Here $v_P(\cdot)$ is, of course, the order of vanishing at P.) In the sequel we tacitly identify the two sets and may speak on a $\bar{K}$-point P on X as a $\bar{K}$-place P of $\bar{K}(X)$, and vice versa.

More generally, there is a bijection between the sets of places of $K(X)$ and the set $X(\bar{K})/G_K$ of G_K-orbits of $\bar{K}$-points, and we again identify two sets. If $P \in X(\bar{K})$ then the residue field of the place P^{G_K} is isomorphic to $K(P)$.

Let $t \in K(X)$ be a K-rational function. For any point P of X there is a well-defined "value" $t(P) \in K(P) \cup \{\infty\}$. It may be defined as the only element τ of $K(P) \cup \{\infty\}$ such that $v_P(t-\tau) > 0$.

Here and everywhere else throughout the article we use the standard convention $t - \infty = t^{-1}$.

Now let $t, u \in K(X)$ be non-constant K-rational functions. We say that a point $P \in X(\bar{K})$ is *(t,u)-regular* if the following two conditions are satisfied.

R1. For any point $P' \neq P$ we have $(t(P'), u(P')) \neq (t(P), u(P))$.

R2. We have
$$\min\{v_P(t - t(P)), v_P(u - u(P))\} = 1.$$

If one of these conditions is not satisfied then we call P a (t,u)-singular point.

The following properties will be used in the article without special reference.

Proposition 2.1 *Let X be a curve over a field K of characteristic 0 and $t, u \in K(X)$ non-constant rational function on X.*

1. *If there is at least one (t,u)-regular $\bar{K}$-point then $K(X) = K(t,u)$.*

   From now on assume that $K(X) = K(t,u)$.

2. *If $P \in X(\bar{K})$ is (t,u)-regular then $K(P) = K(t(P), u(P))$*

3. *Assume that $K(X) = K(t,u)$ and let $F(T,U) \in K[T,U]$ be the irreducible polynomial satisfying $F(t,u) = 0$. Then for a point $P \in X(\bar{K})$ with*

$$t(P) = \tau \neq \infty, \qquad u(P) = \omega \neq \infty$$

the following properties are equivalent.

- *The point P is (t,u)-singular.*
- *We have $F'_T(\tau,\omega) = F'_U(\tau,\omega) = 0$.*

4. *There exist at most finitely many (t,u)-singular points $P \in X(\bar{K})$.*

All this is well-known, but we include the proof for completeness.

Proof of Proposition 2.1 Since X is geometrically irreducible, the constant subfield of $K(X)$ is K. Hence in item 1 it suffices to show that $\bar{K}(X) = \bar{K}(t,u)$ if there is at least one (u,t)-non-singular point $P \in X(\bar{K})$.

Thus, assume that $\bar{K}(t,u)$ is a proper subfield of $\bar{K}(X)$, of degree $m > 1$. Then there are two possibilities for our point P:

- the place P of $\bar{K}(X)$ is totally ramified over $\bar{K}(t,u)$, in which case both $v_P(t - t(P))$ and $v_P(u - u(P))$ are divisible by m, contradicting condition R2;
- the restriction of P to the field $\bar{K}(t,u)$ coincides with the restriction of a different place P', in which case $t(P) = t(P')$ and $u(P) = u(P')$, contradicting condition R1.

This proves item 1.

Now assume that $K(t(P), u(P))$ is a proper subfield of $K(P)$. Pick $\sigma \in G_{K(t(P),u(P))} \setminus G_{K(P)}$. Then we have $P \neq P^\sigma$, but $t(P) = t(P^\sigma)$ and $u(P) = u(P^\sigma)$, contradicting condition R1. This proves item 2.

Item 3 can be found in any "old-fashioned" course of the theory of plane algebraic curves; for instance, see Theorem 5.8 in [11, Chapter IV]. Finally, item 4 follows from item 3. □

3 Lemmas on Ideals

In this subsection K is a number field of degree $d = [K : \mathbb{Q}]$ and $\mathcal{N} = \mathcal{N}_{K/\mathbb{Q}}$ is the $K/\mathbb{Q}$-norm. The index $K/\mathbb{Q}$ will be omitted when this does not cause confusion.

Lemma 3.1 (a "reduced" generator of a principal ideal) *There exists a positive number κ (depending only of K) such that the following holds. Let $\mathfrak{a}$ be a principal fractional ideal of K. Then $\mathfrak{a}$ has a generator α satisfying*

$$\kappa^{-1}(\mathcal{N}\mathfrak{a})^{1/d} \leq \underline{|\alpha|} \leq \overline{|\alpha|} \leq \kappa(\mathcal{N}\mathfrak{a})^{1/d}. \tag{2}$$

Proof This property is well-known and widely used in the Diophantine Analysis, but we include a quick proof for the reader's convenience. To simplify the notation, we denote by S the set of infinite places M_K^∞. Let $\mathrm{Log} : K^\times \to \mathbb{R}^S$ be the "logarithmic map" $\alpha \mapsto (\log|\alpha|_v)_{v\in S}$ and let $\varsigma : \mathbb{R}^S \to \mathbb{R}$ be the linear functional $\mathbf{x} = (x_v)_{v\in S} \mapsto \sum_{v\in S}(d_v/d)x_v$, where $d_v = [K_v : \mathbb{Q}_v]$ is the local degree of v (equal to 1 or 2 depending on whether v is real or complex). Then for $\alpha \in K^\times$ we have $\varsigma(\mathrm{Log}\,\alpha) = d^{-1}\log|\mathcal{N}\alpha|$. In addition to this, we denote by $\mathbf{1}$ the vector $(1)_{v\in S} \in \mathbb{R}^S$ (every component is 1); note that $\varsigma(\mathbf{1}) = 1$.

According to the Dirichlet Unit Theorem, the image $\mathrm{Log}\,\mathcal{O}_K^\times$ of the unit group forms a lattice in $\ker\varsigma$. Hence there exists $\lambda > 0$ such that for any $\mathbf{x} \in \ker\varsigma$ there exits $\mathbf{x}' \in \ker\varsigma$ satisfying $\mathbf{x} \equiv \mathbf{x}' \bmod \mathrm{Log}\,\mathcal{O}_K^\times$ and $\|\mathbf{x}'\|_\infty \le \lambda$, where $\|\cdot\|_\infty$ stands for the sup-norm. More generally, for an arbitrary $\mathbf{x} \in \mathbb{R}^S$, we find, by applying the previous sentence to the vector $\mathbf{x} - \nu(\mathbf{x})\mathbf{1} \in \ker\varsigma$, a vector $\mathbf{x}' \in \mathbb{R}^S$ satisfying $\mathbf{x} \equiv \mathbf{x}' \bmod \mathrm{Log}\,\mathcal{O}_K^\times$ and $\|\mathbf{x}' - \nu(\mathbf{x})\mathbf{1}\|_\infty \le \lambda$. In particular, for $\beta \in K^\times$ we can find $\alpha \in K^\times$ such that $\beta/\alpha \in \mathcal{O}_K^\times$ and

$$e^{-\lambda}|\mathcal{N}\beta|^{1/d} \le |\alpha|_v \le e^{\lambda}|\mathcal{N}\beta|^{1/d}$$

for all $v \in S$. Taking β as a generator of the principal ideal $\mathfrak{a}$, we find thereby another generator α satisfying (2) with $\kappa = e^\lambda$. □

Lemma 3.2 (a "reduced" $\mathbb{Z}$-basis of an ideal) *There exists a positive number κ (depending only of K) such that the following holds. Let $\mathfrak{a}$ be a fractional ideal of K. Then $\mathfrak{a}$ has a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_d$ satisfying*

$$\kappa^{-1}(\mathcal{N}\mathfrak{a})^{1/d} \le \underline{|\alpha_i|} \le \overline{|\alpha_i|} \le \kappa(\mathcal{N}\mathfrak{a})^{1/d}. \qquad (i = 1, \dots, d). \tag{3}$$

Proof There exists a real number λ, depending only on K, such that the following holds: every ideal class of K has an ideal $\mathfrak{b}$ satisfying $\lambda^{-d} \le \mathcal{N}\mathfrak{b} \le \lambda^d$ and having a $\mathbb{Z}$-basis $\beta_1, \dots, \beta_d$ such that

$$\lambda^{-1} \le \underline{|\beta_i|} \le \overline{|\beta_i|} \le \lambda. \qquad (i = 1, \dots, d).$$

In particular, such $\mathfrak{b}$ can be found in the class of our ideal $\mathfrak{a}$. Lemma 3.1 implies that the principal ideal $\mathfrak{a}\mathfrak{b}^{-1}$ has a generator γ satisfying

$$(\kappa')^{-1}(\mathcal{N}(\mathfrak{a}\mathfrak{b}^{-1}))^{1/d} \le \underline{|\gamma|} \le \overline{|\gamma|} \le \kappa'(\mathcal{N}(\mathfrak{a}\mathfrak{b}^{-1}))^{1/d},$$

where κ' depends only on K. Setting $\alpha_i = \beta_i\gamma$, we obtain a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_d$ of $\mathfrak{a}$ satisfying (3) with $\kappa = \kappa'\lambda^2$. □

Given a K-prime $\mathfrak{p}$, an element $\pi \in K$ is called $\mathfrak{p}$-*primitive* if $v_\mathfrak{p}(\pi) = 1$, where $v_\mathfrak{p}$ is the place associated to $\mathfrak{p}$. Since a $\mathbb{Z}$-basis of $\mathfrak{p}$ has at least one primitive element, Lemma 3.2 has the following consequence.

Corollary 3.3 (a "reduced" primitive element) *There exists a positive number κ (depending only of K) such that the following holds. For every K-prime $\mathfrak{p}$ there exists a $\mathfrak{p}$-primitive $\pi \in \mathcal{O}_K$ satisfying*

$$\kappa^{-1}(\mathcal{N}\mathfrak{p})^{1/d} \le \underline{|\pi|} \le \overline{|\pi|} \le \kappa(\mathcal{N}\mathfrak{p})^{1/d}.$$

Another application of Lemma 3.2 is locating "reduced" elements in residue classes.

Corollary 3.4 (a "reduced" element in a residue class) *There exists a real $\kappa \geq 1$ (depending only of K) such that the following holds. Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_K$. Then for every $\alpha \in \mathcal{O}_K$ there exists $\beta \in \mathcal{O}_K$ such that $\alpha \equiv \beta \bmod \mathfrak{a}$ and $\overline{|\beta|} \leq \kappa(\mathcal{N}\mathfrak{a})^{1/d}$.*

Proof It is a standard lattice argument. We identify K with its image (under the diagonal embedding) in $V = \mathbb{R}^{s_1} \times \mathbb{C}^{s_2}$, where s_1 and $2s_2$ are the numbers of real and complex embeddings of K. Then $\mathfrak{a}$ becomes a lattice in V, and every element of V is congruent modulo $\mathfrak{a}$ to an element of its fundamental domain. According to Lemma 3.2, the lattice $\mathfrak{a}$ has a basis $\alpha_1, \ldots, \alpha_d$ satisfying $\overline{|\alpha_i|} \leq \kappa'(\mathcal{N}\mathfrak{a})^{1/d}$, where κ' depends only on K. Every element of the fundamental domain spanned by this basis is of size at most $d\kappa'(\mathcal{N}\mathfrak{a})^{1/d}$. This proves the corollary with $\kappa = d\kappa'$. □

Remark 3.5 Lower estimates for the "lower size" obtained in (2), (3) etc. will not be used elsewhere in this article; we include them only for completeness. Moreover, the proof of Corollary 3.4 can be easily modified to obtain a lower estimate as well. We do not do it because we will not need this lower estimate.

4 Thin Subsets and Hilbert's Irreducibility Theorem

In this section we recall basic definitions and facts about thin sets, and state Hilbert's Irreducibility Theorem.

Let K be a field of characteristic 0. We call $\mathcal{U} \subset K$ a *basic thin subset* of K if there exists a (smooth geometrically irreducible) curve Y defined over K and a non-constant rational function $u \in K(X)$ of degree at least 2 such that $\mathcal{U} \subset u(Y(K))$. A *thin subset* of K is a union of finitely many basic thin subsets. Thin subsets form an ideal in the algebra of subsets of K. Serre in [12, Section 9.1] gives a differently looking, but equivalent definition of thin sets.

Any finite set is thin, and if K is algebraically closed then any subset of K is thin.

Remark 4.1 If L is an extension of K then any thin subset of K is also thin as a subset of L. The converse is true when L is finitely generated over K [3, Proposition 2.1] but not in general; for instance, any number field K is a thin subset of its algebraic closure $\bar{K}$ but is not a thin subset of itself by the Hilbert Irreducibility Theorem quoted below.

Using elementary Galois theory one easily proves the following (see [12, Section 9.2])

Proposition 4.2 *Let X be a curve over K and $t \in K(X)$ a non-constant rational function. Then the set of $\tau \in K$ such that the fiber $t^{-1}(\tau)$ is reducible over K is thin.*

Hilbert's Irreducibility Theorem asserts that when K is a number field then its ring of integers $\mathcal{O}_K$ is not a thin subset of K. In fact, one has the following counting result (see [12], Theorem on page 134).

Theorem 4.3 *Let K be a number field of degree d over $\mathbb{Q}$ and $\mathfrak{V} \subset \mathcal{O}_K$ a thin subset of K. Then for $B \geq 1$ the set $\mathfrak{V}$ has $O(B^{d/2})$ elements α with $\overline{|\alpha|} \leq B$, the implicit constant depending on K and on $\mathfrak{V}$.*

Combining this with Proposition 4.2, we obtain the following "quantitative" version of Hilbert's Irreducibility Theorem.

Corollary 4.4 *Let K be a number field of degree d over the rationals, X a curve over K and $t \in K(X)$ a non-constant rational function. Then for $B \geq 1$ there exist at most $O(B^{d/2})$ elements $\tau \in \mathcal{O}_K$ with $\overline{|\alpha|} \leq B$ such that the fiber $t^{-1}(\tau)$ is reducible over K. Here the implicit constant depends only on K, X and t.*

5 Local Behavior of Functions on a Curve

In this section we compare the behavior of two distinct functions in a neighborhood of a point on an algebraic curve. Our main tool will be the Puiseux expansion.

Unless the contrary is stated explicitly, in this section X is a (smooth projective) curve over a number field K and $t, u \in K(X)$ non-constant K-rational functions. Further, let $A \in X(K)$ be a K-rational point. For $v \in M_K$ we want to compare t and u in a v-adic neighborhood of A.

Theorem 5.1 *Assume that A is a (t,u)-regular point of X (as defined in Subsection 2.2). There exists a finite subset $S \subset M_K$ (depending on X, t, u and A) such that for $v \in M_K \smallsetminus S$ the following holds. Assume that $P \in X(K_v)$ satisfies*

$$|t(P) - t(A)|_v < 1, \qquad |u(P) - u(A)|_v < 1.$$

Then

$$|t(P) - t(A)|_v^{1/v_A(t)} = |u(P) - u(A)|_v^{1/v_A(u)}$$

Remark 5.2 The (t,u)-regularity hypothesis can be relaxed: in fact, it suffices to assume that our point A satisfies only condition R1 in the definition of (t,u)-regularity in Subsection 2.2, while condition R2 may be be suppressed. But the present form of the theorem is sufficient for us, and assuming R2 slightly simplifies the proof.

5.1 Puiseux Expansion

Let us briefly recall the notion of the Puiseux expansion. Let K be a field, X a smooth projective curve over K and $A \in X(K)$ a K-rational point. Further, let $t \in K(X)$ be a non-constant K-rational function with $v_A(t) = 1$. Then one can realize the completion of $K(X)$ with respect to the valuation $v_A(\cdot)$ as the field of formal power series $K((t))$. In particular, we view $K(X)$ as a subfield of $K((t))$, the function $t \in K(X)$ being identified with $t \in K((t))$.

If $u \in K(X)$ is another K-rational function on X, then its image in $K((t))$ is a certain power series $\sum_{k=\nu}^{\infty} a_k t^k$ with $\nu = v_A(u)$ and $a_\nu \neq 0$. We call this series the *Puiseux expansion of u at A in t*.

Now assume that K is a number field. Then the coefficients a_k of the Puiseux expansion satisfy the classical *Eisenstein Theorem*, which says, informally, that for all $v \in M_K$ the v-adic norm of the coefficients grows at most exponentially in k, and for all but finitely many v they are bounded by 1. In symbols: for every $v \in M_K$ there exists $C_v \geq 1$, such that $C_v = 1$ for almost all v, and

$$|a_k|_v \leq C_v^{k-\nu+1} \qquad (k \geq \nu,\ v \in M_K).$$

We will only need the following weaker result.

Proposition 5.3 (Eisenstein) *There exists a finite set $S \subset M_K$ (containing all the infinite places) such that for every $v \in M_K \smallsetminus S$ the coefficients a_k are v-adic integers.*

We want to show now that for all but finitely many v the Puiseux expansion indeed expresses u in terms of t in a suitable v-adic "neighborhood" of the point A.

Proposition 5.4 *In the set-up of this subsection, assume that A is a (t,u)-regular point of X. Then there exists a finite set $S \subset M_K$ (which contains all the infinite places and might be different from the set S of Proposition 5.3) such that for every $v \in M_K \smallsetminus S$ the coefficients a_k are v-adic integers and the following holds. Assume that $P \in X(K_v)$ satisfies $|t(P)|_v < 1$ and $|u(P) - u(A)|_v < 1$. Then the series $\sum_{k=\nu}^{\infty} a_k t(P)^k$ converges v-adically to $u(P)$.*

Proof We may assume without loss of generality that[1] $u(A) = 0$. Then

$$\nu = v_A(u) \geq 1.$$

Let $F(T,U) \in K[T,U]$ be the K-irreducible polynomial such that $F(t,u) = 0$; in particular,

$$F(0,0) = F(t(A), u(A)) = 0. \tag{4}$$

[1] This is obvious if $u(A) \neq \infty$ (just replace u by $u - u(A)$), but requires some explanation in the case when A is a pole of u. In this latter case the set S should be extended to make the leading coefficient of the Puiseux expansion for u an S-unit. Then for $v \notin S$ the coefficients of the series for u are v-adic integers if and only if the same holds for $1/u$. And if, in addition to this, $|t(P)|_v < 1$ and the series for $1/u$ converges v-adically at $t(P)$ to $1/u(P)$, then the series for u converges at $t(P)$ to $u(P)$.

Further, let $A_1 = A, A_2, \ldots, A_s \in X(\bar{K})$ be all points which are zeros of t and which are *not* poles of u. Then $u(A_1), \ldots, u(A_s)$ are the roots of the polynomial $F(0, U)$, of multiplicities $v_{A_1}(t), \ldots, v_{A_s}(t)$, and it has no other roots. Since $A = A_1$ is a (t, u)-regular point, we have $u(A) \neq u(A_i)$ for $i = 2, \ldots, s$. In particular, $0 = u(A)$ is a root of $P(0, U)$ of multiplicity $v_A(t) = 1$. In other words, $F'_U(0, 0) \neq 0$, and we normalize the polynomial F to have

$$F'_U(0, 0) = 1. \tag{5}$$

Now let S be a a finite subset of M_K like in Proposition 5.3. Enlarging it, we may assume that for $v \in M_K \setminus S$ all the coefficients of the polynomial F are v-adic integers.

Now fix $v \in M_K \setminus S$ and let $P \in X(K_v)$ be such that

$$|t(P)|_v < 1, \qquad |u(P)|_v < 1.$$

Set $\tau = t(P)$. Since $|\tau|_v < 1$ and the coefficients of the polynomial F are v-adic integers, (4) and (5) imply that

$$|F(\tau, 0)|_v < 1, \qquad |F'_U(\tau, 0)|_v = 1. \tag{6}$$

Furthermore, since $|\tau|_v < 1$ and the coefficients a_k are v-adic integers, the series $\sum_{k=\nu}^{\infty} a_k \tau^k$ converges in K_v to a sum that we denote by ω. Since $\nu \geq 1$, we have $|\omega|_v < 1$, and since $F(t, \sum_{k=\nu}^{\infty} a_k t^k) = 0$, we have $F(\tau, \omega) = 0$. On the other hand, $F(\tau, u(P)) = F(t(P), u(P)) = 0$ as well.

Thus, both ω and $u(P)$ are roots of the polynomial $F(\tau, U)$. However, Hensel's lemma implies that, in view of (6), this polynomial may have only one root of v-adic norm strictly smaller than 1. Hence $u(P) = \omega$, proving the proposition. □

5.2 Proof of Theorem 5.1

It is an easy consequence of Proposition 5.4. We may assume that

$$t(A) = u(A) = 0$$

and $v_A(t) = 1$. Then $v_A(u) = \nu \geq 1$. Let $\sum_{k=\nu}^{\infty} a_k t^k$ be the Puiseux expansion of u at A, and let S be as in Proposition 5.4. Enlarging S, we may assume that $|a_\nu|_v = 1$ for $v \in M_K \setminus S$.

Now fix $v \in M_K \setminus S$. Then for any $P \in X(K_v)$ satisfying $|t(P)|_v < 1$ and $|u(P)|_v < 1$ we have $u(P) = \sum_{k=\nu}^{\infty} a_k t(P)^k$. Since $|a_\nu|_v = 1$, we obtain $|u(P)|_v = |t(P)|_v^\nu$, whence the result. □

6 Polynomials over Complete Fields

In this section we collect results, mainly well-known, on polynomials over complete field.

6.1 Roots of Polynomials and Power Series

Let K be a field of characteristic 0, complete with respect to a non-archimedean absolute value $|\cdot|$. Let $f(T) \in K[T]$ be a polynomials having a root $\alpha \in K$ of multiplicity e. It is well-known that if $g(T) \in K[T]$ is another polynomial of the same degree, "sufficiently close" to f, then $g(T)$ has e roots in $\bar{K}$ "close" to α; see Proposition 7.1 in [8, Chapter XII] as an example of such a statement.

We need a precise form of this statement. For a polynomial

$$f(T) = a_n T^n + \cdots + a_0 \in K[T]$$

we use notation

$$|f| = \max\{|a_0|, \ldots, |a_n|\}.$$

We extend the absolute value from K to its algebraic closure $\bar{K}$.

Theorem 6.1 *Let $f(T) = a_n T^n + \cdots + a_0 \in K[T]$ be a polynomial of degree n having pairwise distinct roots $\alpha_1, \ldots, \alpha_s \in K$ of multiplicities $e_1, \ldots, e_s$, respectively, and no other roots in $\bar{K}$ (so that $e_1 + \cdots + e_s = n$). Assume that*

$$|f| = |a_n| = 1; \tag{7}$$

$$|\alpha_i - \alpha_j| = 1 \qquad (1 \le i < j \le s); \tag{8}$$

$$\left| \frac{f^{(e_i)}(\alpha_i)}{e_i!} \right| = 1 \qquad (1 \le i \le s). \tag{9}$$

Let $g(T) \in K[T]$ be another polynomial of degree n satisfying $|f - g| < 1$. Then the set of roots of g in $\bar{K}$ splits into disjoint sets $B_1, \ldots, B_s$, such that every B_i has exactly e_i roots counted with multiplicities, and every $\beta \in B_i$ satisfies

$$|\beta - \alpha_i| < 1, \qquad |\beta - \alpha_j| = 1 \quad (i \ne j).$$

The proof relies on the famous theorem of Strassmann on zeros of power series in complete fields. We will use this theorem only for polynomials, but we state it for power series, in its full strength.

Thus, let $f(T) = \sum_{k=0}^{\infty} a_k T^k \in K[[T]]$ be a formal power series over a non-archimedean complete field K, whose coefficients satisfy $|a_k| \to 0$ as $k \to \infty$. Then f defines an analytic function on the closed disc $\mathcal{O} = \{\alpha \in K : |\alpha| \le 1\}$.

Theorem 6.2 (Strassmann) *Set*

$$A = \max\{|a_k| : k = 0, 1, 2, \ldots\}, \qquad \kappa_{\max} = \max\{k : |a_k| = A\}.$$

Then $f(T)$ has at most $\kappa_{\max}$ zeros $\alpha \in K$ with $|\alpha| \le 1$.

The proof is well-known, by induction in $\kappa_{\max}$. If $\kappa_{\max} = 0$ then $f(T)$ clearly does not vanish on $\mathcal{O}$. Now assume that $\alpha \in \mathcal{O}$ is a zero of f. It is easy to see that replacing $f(T)$ by $f(\alpha + T)$ does not alter the value of $\kappa_{\max}$; hence we may assume $\alpha = 0$. It follows that $a_0 = 0$, and we reduce the statement for $f(T)$ to that for $T^{-1} f(T) = a_1 + a_2 T + \ldots$, reducing $\kappa_{\max}$ by 1.

Here is a useful complement to Strassmann's theorem.

Corollary 6.3 *Set* $\kappa_{\min} = \min\{k : |a_k| = A\}$. *Then* $f(T)$ *has at most* $\kappa_{\min}$ *zeros* $\alpha \in K$ *with* $|\alpha| < 1$.

Proof We may assume that the set of zeros $\alpha \in K$ with $|\alpha| < 1$ is non-empty: otherwise there is nothing to prove. Since this set is finite by Theorem 6.2, it has an element θ of maximal absolute value:

$$|\theta| = \max\{|\alpha| : f(\alpha) = 0,\ |\alpha| < 1\}.$$

Then we have to count zeros in $\mathcal{O}$ of the function $f(\theta T)$. Since $|\theta| < 1$, the value of $\kappa_{\max}$ for the series $f(\theta T)$ does not exceed the value of $\kappa_{\min}$ for the series $f(T)$. Hence the result follows by Theorem 6.2. □

Proof of Theorem 6.1 We write $g(T) = b_n T^n + \cdots + b_0$. Extending the field K, we may assume that all the roots of g belong to K as well. Condition (7) implies that all roots of f are of absolute value at most 1. Since $|f - g| < 1$, we have $|g| = |b_n| = 1$, and the roots of g are of absolute value at most 1 as well.

Let us show first of all that for every root β of g there exists a unique root α_i of f such that $|\beta - \alpha_i| < 1$. Indeed, uniqueness follows from (8), and existence from

$$\prod_{i=1}^{s} |\beta - \alpha_i|^{e_i} = |f(\beta)| = |f(\beta) - g(\beta)| \le |f - g| < 1.$$

This already defines the partition $B_1 \cup \ldots \cup B_s$ on the set of roots of g, and we only need to show that each B_i contains exactly e_i roots (counted with multiplicities). Moreover, since $n = e_1 + \cdots + e_s$ is the total number of roots of g, it is sufficient to show that B_i contains *at most* e_i roots.

Thus, fix α_i and omit index i in the sequel. We want to show that g has at most e roots β satisfying $|\beta - \alpha| < 1$. Replacing $f(T)$ and $g(T)$ by $f(\alpha + T)$ and $g(\alpha + T)$, we may assume that $\alpha = 0$. Thus, $f(T) = a_e T^e + \cdots + a_n T^n$ with $|a_e| = 1$ by (9). Then for the coefficients of $g(T)$ we have $|b_k| < 1$ for $k < e$ and $|b_e| = 1$. By Corollary 6.3, the polynomial g has at most e roots β satisfying $|\beta| < 1$. This completes the proof. □

Here is a consequence for number fields.

Corollary 6.4 *Let* K *be a number field and* $f(T) \in K[T]$ *a polynomial of degree* n *having a root* $\alpha \in K$ *of order* e. *Then there exists a finite set* $S \subset M_K$ *(containing all the infinite places), such that for every* $v \in M_K \setminus S$ *the following holds. Let* $g(T) \in K_v[T]$ *be a polynomial of degree* n *satisfying* $|f - g|_v < 1$. *Then* g *has exactly* e *roots* $\beta \in \overline{K_v}$ *satisfying* $|\beta - \alpha|_v < 1$.

Proof If the statement holds true with K replaced by some finite extension, then it is true for K as well. Thus, extending K, we may assume that all roots of f belong to K. And in this case the statement is an immediate consequence of Theorem 6.1. □

6.2 Ramification

Now assume that K is a non-archimedean local field of characteristic 0; we denote by $|\cdot|$ its absolute value and by $\mathcal{O} = \{\alpha \in K : |\alpha| \leq 1\}$ its local ring.

The following property is well-known (at least when the polynomial $f(T)$ is irreducible), but we include the proof for the reader's convenience.

Proposition 6.5 *Let $f(T) \in \mathcal{O}[T]$ be a monic polynomial and $\alpha \in \bar{K}$ a root of f such the field $K(\alpha)$ is ramified over K. Then $|f'(\alpha)| < 1$.*

Proof Note first of all that, since f is monic and has coefficients in $\mathcal{O}$, its root α satisfies $|\alpha| \leq 1$. It follows that $|f'(\alpha)| \leq 1$. We will assume that $|f'(\alpha)| = 1$ and obtain a contradiction.

Let L be the maximal unramified extension of K contained in $K(\alpha)$. Then there exists $\theta \in L$ with $|\theta - \alpha| < 1$. Since $f(\alpha) = 0$ and $|f'(\alpha)| = 1$, we have $|f(\theta)| < 1$ and $|f'(\theta)| = 1$.

The existence part of Hensel's Lemma implies that $f(T)$ has a root $\alpha' \in L$ satisfying $|\alpha' - \theta| < 1$. The uniqueness part of Hensel's lemma implies that $f(T)$ can have at most one root in $K(\alpha)$ with this property. Hence $\alpha = \alpha' \in L$, a contradiction. □

We again have an immediate consequence for the number fields.

Corollary 6.6 *Let K be a number field and $f(T) \in K[T]$. Let $v \in M_K^0$ be such that all the coefficients of f are v-adic integers, and the leading coefficient of f is a v-adic unit. Viewing f as a polynomial over K_v, let $\alpha \in \overline{K_v}$ be its root such that the field $K_v(\alpha)$ is ramified over K_v. Then $|f'(\alpha)|_v < 1$.*

7 Arithmetical vs Geometric Ramification

Let K be a field of characteristic 0 and X a (smooth projective) algebraic curve over K. Further, let $t \in K(X)$ be a non-constant function. For a point $A \in X(\bar{K})$ we define the *ramification index* of t at A by

$$e_A = e_A(t) = v_A(t - t(A));$$

We say that t is *ramified at* A (and call A a *ramification point* of t) if $e_A(t) > 1$. The value $t(A) \in \bar{K} \cup \{\infty\}$ of t at a ramification point will be called a *critical value* of t. (It is also often called a *branch point* of t.) It is well-known that

- a non-constant rational function has at most finitely many ramification points (and critical values);
- if $\bar{K}(t) \neq \bar{K}(X)$ then t has at least 2 distinct critical values (a consequence of the Riemann-Hurwitz formula).

In this section we prove three theorems linking geometric and arithmetical ramification. None of them is really new, but we did not find in the literature what we exactly need.

Theorem 7.1 *Let K be a number field, X a smooth projective algebraic curve over K and $t \in K(X)$ a non-constant K-rational function. Further, let $\alpha \in K \cup \{\infty\}$ be a critical value of t. Then there exists a finite set S of places of M_K such that for every $v \in M_K \setminus S$ the following holds. Let $\tau \in K_v$ be such that $v(\tau - \alpha) = 1$. Then there exists $P \in X(\overline{K_v})$ with $t(P) = \tau$ such that the field $K_v(P)$ is ramified over K_v.*

(Recall that we normalize the discrete valuation $v(\cdot)$ so that $v(K^\times) = \mathbb{Z}$.)

Informally, the theorem says that "geometric ramification enforces arithmetical ramification".

On the contrary, if $t(P)$ is v-adically close to a non-critical value, then $K_v(P)$ does not ramify over K_v.

Theorem 7.2 *Let K be a number field, X a smooth projective algebraic curve over K and $t \in K(X)$ a non-constant K-rational function. Further, let $\alpha \in K \cup \{\infty\}$ be a* ***not*** *a critical value of t. Then there exists a finite set S of places of M_K such that for every $v \in M_K \setminus S$ the following holds: for any $P \in X(\overline{K_v})$ with $|t(P) - \alpha|_v < 1$ the field $K_v(P)$ is unramified over K_v.*

This theorem is easy (it is, basically, an application of Hensel's lemma), but quite useful. In fact, a similar statement is absolutely crucial in [2].

Theorem 7.1 has a partial converse: for almost all v, if $K_v(P)$ ramifies over K_v then $t(P)$ must be v-adically close to a critical value.

Theorem 7.3 *Let K be a number field, X a smooth projective algebraic curve over K and $t \in K(X)$ a non-constant K-rational function. Assume that all the critical values belong to $K \cup \{\infty\}$. Then there exist a finite set $S \subset M_K$ such that for every $v \in M_K \setminus S$ the following holds. Let $P \in X(\overline{K_v})$ be such that $t(P) \in K_v$ and the field $K_v(P)$ ramifies over K_v. Then there exists a unique critical value α such that $|t(P) - \alpha|_v < 1$.*

Remark 7.4 An alternative treatment of the principal results of this section, using the scheme-theoretic language, can be found in the Appendix due to Jean Gillibert.

7.1 Proof of Theorem 7.1

Remark first of all that we may replace K by a finite extension. Indeed, assume that the statement holds true with K replaced by a finite extension K', and let S' be the corresponding finite subset of $M_{K'}$. Then the statement holds over K as well, if we define S as the set of places $v \in M_K$ which extend to some $v' \in S'$ or ramify in K'.

We may assume that $\alpha = 0$. Let $A \in X(\bar{K})$ be a ramification point of t such that $t(A) = 0$. Extending the base field K, we may assume that $A \in X(K)$. Pick a function $u \in K(X)$ with the following properties:

1. $v_A(u) = 1$;
2. for any point $A' \in X(\bar{K})$, distinct from A, we have
$$(t(A'), u(A')) \neq (t(A), u(A));$$
3. u has no poles among the zeros of t.

Observe that properties 1 and 2 above imply that A is a (t, u)-regular point of X, as defined in Subsection 2.2. In particular, we have $K(X) = K(t, u)$.

Let
$$F(T, U) = a_n(T)U^n + \cdots + a_0(T) \in K[T, U] \tag{10}$$
be such a polynomial that $F(t, U)$ is the minimal polynomial of u over $K[t]$. If τ belongs to some extension of K, we set $f_\tau(U) = F(\tau, U)$. Since u has no poles among the zeros of t, the polynomial $f_0(U) \in K[U]$ is of degree $n = \deg_U F$, and $u(A) = 0$ is its root of order $e = e_A(t)$. We normalize F to make f_0 a monic polynomial (having leading coefficient 1).

Now let $S \supseteq M_K^\infty$ be a finite subset of M_K such that for any $v \in M_K \smallsetminus S$ the conclusion of Corollary 6.4 holds for the polynomial f_0 and its root 0, and the conclusion of Theorem 5.1 holds for the functions t, u and the point A. Expanding the set S, we may assume that for $v \in M_K \smallsetminus S$ the coefficients of $F(T, U)$ are v-adic integers.

Now fix $v \in M_K \smallsetminus S$. Since the coefficients of $F(T, U)$ are v-adic integers, for any $\tau \in K_v$ with $|\tau|_v < 1$ we have $|f_\tau - f_0|_v < 1$. Clearly, $\deg f_\tau \leq n$; but, since f_0 is monic and $|f_\tau - f_0|_v < 1$, we have $\deg f_\tau = n$.

Corollary 6.4 implies that f_τ has a root $\omega \in \overline{K_v}$ with the property $|\omega|_v < 1$. Since $F(\tau, \omega) = 0$, there exists a point $P \in X(\overline{K_v})$ such that
$$t(P) = \tau, \qquad u(P) = \omega.$$
For this point we have
$$|t(P) - t(A)|_v = |\tau|_v < 1, \qquad |u(P) - u(A)|_v = |\omega|_v < 1$$
(recall that $t(A) = u(A) = 0$). Applying Theorem 5.1, we find that $|\omega|_v = |\tau|_v^{1/e}$.

Now if $v(\tau) = 1$ then the field $K_v(\omega)$ must have ramification index at least e over K_v. In particular, $K_v(P)$ is ramified over K_v. □

7.2 Proof of Theorem 7.2

As in the proof of Theorem 7.1 we may assume $\alpha = 0$ and we may replace our field K by a suitable finite extension. Thus, we extend K to have all points in the fiber $t^{-1}(0)$ defined over K. Since 0 is not a critical value, $t^{-1}(0)$ consists of n distinct points (where n is the degree of t).

Now let $u \in K[X]$ be such that u takes pairwise distinct finite values at the points from $t^{-1}(0)$. This implies, in particular, that $K(X) = K(t,u)$. We define $F(T,U)$ as in the previous proof. Then the polynomial $f_0(U) = F(0,U) \in K[U]$ is of degree n and has n distinct simple roots in K. In particular, $f_0'(\alpha) \neq 0$ for any root α of f_0.

Further extending the field K, we may assume that all (t,u)-singular points of X are K-rational.

Now let $S \supseteq M_K^\infty$ be a finite subset of M_K such that for $v \in M_K \smallsetminus S$ the coefficients of $F(T,U)$ are v-adic integers, the leading coefficient of f_0 is a v-adic unit, and $|f_0'(\alpha)|_v = 1$ for any root α of f_0.

Fix $v \in M_K \smallsetminus S$ and let $P \in X(\overline{K_v})$ be such that $t(P) = \tau \in K$ and $|\tau|_v < 1$. We may assume P to be (t,u)-regular; otherwise $K_v(P) = K_v$ and there is nothing to prove.

As in the previous proof, the polynomial $f_\tau(U) = F(\tau, U)$ satisfies

$$|f_0 - f_\tau|_v < 1,$$

and its leading coefficient is a v-adic unit. Since P is (t,u)-regular, we have $K_v(P) = K_v(\omega)$, where $\omega = u(P)$. This ω is a root of f_τ, which implies that

$$|f_0(\omega)|_v = |f_0(\omega) - f_\tau(\omega)|_v < 1.$$

Since the leading coefficient of f_0 is a v-adic unit, this means that $|\omega - \alpha|_v < 1$ for some root α of f_0. It follows that $|f_0'(\omega)|_v = 1$, which implies that $|f_\tau'(\omega)|_v = 1$. Corollary 6.6 now implies that $K_v(\omega) = K_v(P)$ is unramified over K_v, as wanted. □

7.3 Proof of Theorem 7.3

Like in the proof of Theorem 7.1, one may replace K by a suitable finite extension. We will profit from it several times in this proof.

Let $u \in K(X)$ be such that $K(t,u) = K(X)$. As in the proof of Theorem 7.1, let $F(T,U) \in K[T,U]$ be such that $F(t,U)$ is the minimal polynomial of u over $K[t]$. We denote by $R(T)$ the U-resultant of the polynomials F and F_U'. We claim the following.

Proposition 7.5 *There exists a finite set $S \subset M_K$ such that for every place $v \in M_K \smallsetminus S$ the following holds. Let $P \in X(\overline{K_v})$ be such that $t(P) = \tau \in K_v$ and the field $K_v(P)$ ramifies over K_v. Then either $|\tau|_v > 1$ or $|R(\tau)|_v < 1$.*

Proof Write $F(T,U)$ as in (10). Then $a_n(T) \mid R[T]$ in the ring $K[T]$. Furthermore, there exist polynomials $G(T,U), H(T,U) \in K[T,U]$ such that

$$G(T,U)F(T,U) + H(T,U)F_U'(T,U) = R(T). \tag{11}$$

Now let $S \supseteq M_K^\infty$ be a finite set of places of K such that for every $v \in M_K \smallsetminus S$ the coefficients of the polynomials F, G and H are v-adic integers, and the leading coefficient of $a_n(T)$ is a v-adic unit.

This implies, in particular, that the coefficients of $R(T)$ are v-adic integers as well, and that

$$a_n(T) \mid R(T) \text{ in } \mathcal{O}_v[T], \tag{12}$$

where $\mathcal{O}_v$ is local ring of K_v.

Extending the base field K, we may assume that all the (t,u)-singular points of X are K-rational.

Fix $v \in M_K \setminus S$ and let P and τ be as in the statement of the proposition. Assume that $|\tau|_v \le 1$ (otherwise there is nothing to prove). Since $K_v(P) \ne K_v$, the point P cannot be (t,u)-singular, and we obtain $K_v(P) = K_v(\omega)$, where $\omega = u(P)$.

Now we have two cases. If $|a_n(\tau)|_v < 1$ then $|R(\tau)|_v < 1$ by (12).

And if $|a_n(\tau)|_v = 1$ then Corollary 6.6 applies to the root ω of the polynomial $f_\tau(U) = F(\tau, U)$. We obtain $|F'_U(\tau,\omega)|_v < 1$. Substituting $T = \tau$ and $U = \omega$ in (11), we obtain $|R(\tau)|_v < 1$. Proposition 7.5 is proved. □

Extending the base field K, we may assume that all roots of $R(T)$ belong to K. Extending it further, we may assume that all the points from the finite set

$$\mathcal{A} = \{P \in X(\bar{K}) : t(P) \text{ is a root of } R(T) \text{ or } \infty\},$$

are K-rational.

Now let $\tilde{u} \in K(X)$ be such that $K(t,\tilde{u}) = K(X)$ and $\tilde{u}$ has pairwise distinct finite values at the points from $\mathcal{A}$. (Existence of such $\tilde{u}$ easily follows from the weak approximation theorem.) We define for $\tilde{u}$ polynomials $\widetilde{F}(T,U)$ and $\widetilde{R}(T)$ in the same way as we defined F and R for u.

Proposition 7.6 *The only common roots of $R(T)$ and $\widetilde{R}(T)$ are the finite critical values of t.*

Proof Let α be a root of $R(T)$ but not a critical value of t. Then the fiber $t^{-1}(\alpha)$ consists of n distinct points. By our choice of $\tilde{u}$, it takes at them n distinct finite values. It follows that the polynomial $\widetilde{F}(\alpha, U)$ is of degree n and has n distinct roots. It particular, $\widetilde{F}'_U(\alpha, U)$ does not vanish at any of these roots. Hence $\widetilde{R}(\alpha) \ne 0$, as wanted. □

Let $\mathcal{C} \subset K \cup \{\infty\}$ be the set of critical values of t.

Proposition 7.7 *There exists a finite set $S \subset M_K$ such that for every place $v \in M_K \setminus S$ the following holds. Let $P \in X(\overline{K_v})$ be such that $t(P) = \tau \in K_v$ and the field $K_v(P)$ ramifies over K_v. Then there exists a unique $\alpha \in \mathcal{C} \cup \{\infty\}$ such that $|\tau - \alpha|_v < 1$.*

Proof Applying Proposition 7.5 to both u and $\tilde{u}$, we find S such that for every $v \in M_K \smallsetminus S$ the following holds. Let P and τ be as in the statement of Proposition 7.7. Then either $|\tau|_v > 1$ or

$$|R(\tau)|_v < 1, \qquad |\widetilde{R}(\tau)|_v < 1. \tag{13}$$

Expanding S, we my assume that that all the finite critical values of t are v-adic integers and $|\alpha - \alpha'|_v = 1$ for any two distinct finite critical values α and α'.

If $|\tau|_v > 1$ then $\alpha = \infty$ is as wanted. From now on assume that $|\tau|_v \le 1$.

Define $D(T) = \gcd\bigl(R(T), \widetilde{R}(T)\bigr)$ in the ring $K[T]$. We normalize $D(T)$ to make it monic. Proposition 7.6 implies that that all roots of $D(T)$ are finite critical values of t. Write

$$D(T) = E(T)R(T) + \widetilde{E}(T)\widetilde{R}(T) \tag{14}$$

with some $E(T), \widetilde{E}(T) \in K[T]$. Further expanding S, we may assume that for $v \in M_K \smallsetminus S$ the coefficients of E, $\widetilde{E}$, R, $\widetilde{R}$ are v-adic integers.

Substituting $T = \tau$ in (14) and using (13), we obtain $|D(\tau)|_v < 1$. Since D is monic, this implies that $|\tau - \alpha|_v < 1$ for some root α of D, which is a critical value of t. And this α is unique because $|\alpha - \alpha'|_v = 1$ for distinct critical values α and α'. □

Now we are ready to complete the proof of Theorem 7.3. If ∞ is a critical value then Proposition 7.7 does the job. Now assume that ∞ is not critical. Applying Theorem 7.2 with $\alpha = \infty$, a suitably expanded S has the following property: if $v \in M_K \smallsetminus S$ and $P \in X(\overline{K_v})$ are such that $t(P) = \tau \in K_v$ and $K_v(P)$ ramifies over K_v, then $|\tau|_v \le 1$. Hence in this case Proposition 7.7 can produce only a finite α, which is a critical value of t. □

7.4 The Critical Polynomial

It would be convenient to have versions of Theorems 7.1 and 7.3 not assuming that the finite critical values belong to K. Let $\Delta(T)$ be the monic separable polynomial whose roots are exactly the finite critical values of t. Then, clearly, $\Delta(T) \in K[T]$.

Theorem 7.8 *There exists a finite set $S \subset M_K$ such that for any $v \in M_K \smallsetminus S$ and $\tau \in K_v$ the following holds.*

1. *Assume that*
   - *either $v\bigl(\Delta(\tau)\bigr) = 1$,*
   - *or ∞ is a critical value and $v(\tau) = -1$.*

   Then v ramifies in $K_v(P)$ for some $P \in X(\overline{K_v})$ with $t(P) = \tau$.

2. *Assume that v ramifies in $K_v(P)$ for some $P \in X(\overline{K_v})$ with $t(P) = \tau$. Then*

   - *either $|\Delta(\tau)|_v < 1$,*
   - *or ∞ is a critical value and $|\tau|_v > 1$.*

Proof If the statement holds true with K replaced by a finite extension K', then it holds over K as well: one only needs to exclude from consideration those finitely many places of K which ramify in K'. This reduces the theorem to the case when all finite critical values belong to K, when it becomes an immediate consequence of Theorems 7.1 and 7.3. □

8 The Argument of Dvornicich and Zannier

In this section we prove the following theorem, which is slightly stronger than Theorem 1.3.

Theorem 8.1 *Let K be a number field of degree d over $\mathbb{Q}$. Further, let X be a curve over K of genus $\mathbf{g}$ and $t \in K(X)$ a non-constant rational function of degree $n \geq 2$. There exist real numbers $c = c(K, \mathbf{g}, n) > 0$ and $B_0 = B_0(K, X, t) > 1$ such that the following holds. Pick $P_\tau \in t^{-1}(\tau)$ for every $\tau \in \mathcal{O}_K$. Then for every $B \geq B_0$ the number field*

$$K(P_\tau : \ \tau \in \mathcal{O}_K, \ \overline{|\tau|} \leq B) \tag{15}$$

is of degree at least $e^{cB^d/\log B}$ over K.

Theorem 1.3 is an immediate consequence because of (1). Another consequence is the following more precise version of Corollary 1.4.

Corollary 8.2 *Let K, X and t be as in Theorem 8.1. Then there exist real numbers $c = c(K, \mathbf{g}, n) > 0$ and $B_0 = B_0(K, X, t) > 1$ such that the following holds. Pick $P_\tau \in t^{-1}(\tau)$ for every $\tau \in \mathcal{O}_K$. Then for every $B \geq B_0$, among the number fields*

$$K(P_\tau) \qquad (\tau \in \mathcal{O}_K, \quad \overline{|\tau|} \leq B)$$

there are at least $cB^d/\log B$ distinct fields.

In the sequel K, X and t as in the statement of Theorem 8.1. Everywhere in this section we adopt the following conventions.

- "Sufficiently large" means "exceeding a certain quantity depending on K, X and t";
- "Almost every" means "outside a finite set depending on K, X and t".

We will adapt the beautiful ramification argument of Dvornicich and Zannier [7], which, as they remark, traces back to the work of Davenport, Lewis and Schinzel [6]. We refer to Section 3 of [4] for a concise exposition of the Dvornicich-Zannier argument over $\mathbb{Q}$.

Let "$\prec$" be a strict order relation on a countable set M. We call it $\mathbb{N}$-*ordering* if $(M, \prec)$ and $(\mathbb{N}, <)$ are isomorphic as ordered sets. We fix an $\mathbb{N}$-ordering "$\prec$" on the set $\mathcal{O}_K$ which makes the size function (non-strictly) increasing: for $\beta, \beta' \in \mathcal{O}_K$ with $\beta \prec \beta'$ we have $\overline{|\beta|} \le \overline{|\beta'|}$.

We say that a place $v \in M_K$ is *primitive* for $\tau \in \mathcal{O}_K$ if v ramifies in the field extension $K\big(t^{-1}(\tau)\big)/K$, but does not ramify in $K\big(t^{-1}(\tau')\big)/K$ for any $\tau' \prec \tau$.

Theorem 8.1 is a consequence of the following two statements.

Proposition 8.3 *Let α be a finite critical value of t. Then almost every $v \in M_K$ having an extension $w \in M_{K(\alpha)}$ of degree $[w : v] = 1$ serves as primitive for some $\tau \in \mathcal{O}_K$ satisfying $\overline{|\tau|} \le \lambda(\mathcal{N}v)^{1/d}$. Here $\lambda \ge 1$ depends only on K.*

Recall that $\mathcal{N}v$ denotes the $K/\mathbb{Q}$-norm of the prime ideal of v, with the convention $\mathcal{N}v = 1$ for an infinite place v.

Proposition 8.4 *Let m be the total number of finite critical values of t. Let ε be a real number satisfying $0 < \varepsilon \le 1$. For every $\tau \in \mathcal{O}_K$ with $\overline{|\tau|} \ge \kappa\varepsilon^{-m-1}$ (where $\kappa \ge 1$ depends only on X and t) there is at most m finite places v of K satisfying $\mathcal{N}v \ge \big(\varepsilon\overline{|\tau|}\big)^d$ and ramified in $K(t^{-1}(\tau))$.*

8.1 Proof of Theorem 8.1

In this subsection we prove Theorem 8.1 assuming validity of Propositions 8.3 and 8.4.

Let α be a finite critical value of t (which exists because $n \ge 2$). Denote by M the set of $v \in M_K$ satisfying the hypothesis of Proposition 8.3. The Tchebotarev Density Theorem implies that that there exists $\delta > 0$ such that

$$\big|\{v \in \mathrm{M} : \mathcal{N}v \le B\}\big| \sim \delta \frac{B}{\log B} \tag{16}$$

as $B \to \infty$. This δ can be estimated from below only in terms of $\mu = [K(\alpha) : K]$; in fact, it is easy to see that

$$\delta \ge \frac{1}{\mu} \ge \frac{1}{m}, \tag{17}$$

where m is the total number of finite critical values.

Now, for a given $B \ge 1$ we define the following three sets:

$$\mathrm{M}(B) = \left\{ v \in \mathrm{M} : \left(\frac{B}{2\lambda}\right)^d \le \mathcal{N}v \le \left(\frac{B}{\lambda}\right)^d \right\},$$

$$\Omega(B) = \{\tau \in \mathcal{O}_K : \tau \text{ has a primitive } v \in M(B)\},$$

$$\Omega'(B) = \{\tau \in \Omega(B) : \text{the fiber } t^{-1}(\tau) \text{ is } K\text{-irreducible}\}.$$

Proposition 8.3 implies that

$$\overline{|\tau|} \le B \text{ for every } \tau \in \Omega(B). \tag{18}$$

If τ admits a primitive v then the field $K\big(t^{-1}(\tau)\big)$ is not contained in the compositum of all the "preceding" fields $K\big(t^{-1}(\tau')\big)$ where $\tau' \prec \tau$. If, in addition to this, the fiber $t^{-1}(\tau)$ is K-irreducible, then the field $K\big(t^{-1}(\tau)\big)$ is the Galois closure (over K) of $K(P_\tau)$, which implies that $K(P_\tau)$ is not contained in the compositum of the "preceding" fields $K(P_{\tau'})$ with $\tau' \prec \tau$. Combining this with (18), we conclude that the degree of the field (15) over K is at least $2^{|\Omega'(B)|}$. We are left with proving that

$$|\Omega'(B)| \ge c\frac{B^d}{\log B}, \tag{19}$$

where $c > 0$ depends on K, $\mathbf{g}$ and n.

Using (16) and (17), we estimate

$$|\mathrm{M}\,(B)| \ge \frac{\delta}{2d\lambda^d}\frac{B^d}{\log B} \ge \frac{1}{2md\lambda^d}\frac{B^d}{\log B}$$

for sufficiently large B. Now Proposition 8.4 applied with $\varepsilon = (2\lambda)^{-1}$ implies that, for sufficiently large B

$$|\Omega(B)| \ge \frac{1}{m}|\mathrm{M}\,(B)| \ge \frac{1}{2m^2d\lambda^d}\frac{B^d}{\log B}.$$

Further, Corollary 4.4 implies that

$$|\Omega'(B)| \ge |\Omega(B)| - O(B^{d/2}) \ge \frac{1}{4m^2d\lambda^d}\frac{B^d}{\log B}.$$

for sufficiently large B.

Finally, the Riemann-Hurwitz formula implies that $m \le 2\mathbf{g} + 2n - 2$. This proves (19) with

$$c = \frac{1}{16(\mathbf{g}+n)^2d\lambda^d},$$

as wanted. □

8.2 Proof of Proposition 8.3

In this subsection we prove Proposition 8.3. Let α, v and w be as in the statement of the proposition. Throwing away finitely many v we may assume that $w(\alpha) \ge 0$. Since $[w : v] = 1$, there exists $\alpha' \in \mathcal{O}_K$ such that $w(\alpha - \alpha') > 0$. Corollaries 3.4 and 3.3 imply that there exist $\gamma', \pi \in \mathcal{O}_K$ such that

$$v(\gamma' - \alpha') > 0, \quad v(\pi) = 1, \quad \overline{|\gamma'|}, \overline{|\pi|} \ll (\mathcal{N}v)^{1/d},$$

where in this proof the constants implied by the $O(\cdot)$-notation and by the Vinogradov $\ll$-notation depend only on K.

Now set

$$\gamma = \begin{cases} \gamma', & w(\gamma' - \alpha) = 1, \\ \gamma' + \pi, & w(\gamma' - \alpha) > 1. \end{cases}$$

Then $w(\gamma - \alpha) = 1$ and $\overline{|\gamma|} \ll (\mathcal{N}v)^{1/d}$.

Theorem 7.1 (applied to the field $K(\alpha)$ instead of K) implies that, unless our w belongs to a finite exceptional set, it ramifies in the field $K\big(\alpha, t^{-1}(\gamma)\big)$. It follows that v ramifies in the latter field as well. This means that v ramifies either in $K(\alpha)$ (which is the case for only finitely many v) or in $K\big(t^{-1}(\gamma)\big)$.

We have proved the following: for almost every $v \in M_K$ satisfying the hypothesis of the proposition, the set

$$\{\gamma \in \mathcal{O}_K : v \text{ ramifies in } K(t^{-1}(\gamma)\}$$

is non-empty and contains an element of size $O\big((\mathcal{N}v)^{1/d}\big)$. Taking as τ the smallest element of this set with respect to the "$\prec$" ordering, we complete the proof. □

8.3 Proof of Proposition 8.4

If $\mathcal{N}v \geq \big(\varepsilon\overline{|\tau|}\big)^d$ and $\overline{|\tau|} \geq \kappa\varepsilon^{-m-1}$ then

$$\mathcal{N}v \geq \kappa^d \varepsilon^{-md} \geq \kappa.$$

Selecting κ sufficiently large, we may assume that the finitely many exceptional places from Theorem 7.8:2 are all of norm smaller than κ. Hence we only have to count $v \in M_K$ satisfying

$$|\Delta(\tau)|_v < 1, \qquad \mathcal{N}v \geq \big(\varepsilon\overline{|\tau|}\big)^d, \tag{20}$$

where $\Delta(T)$ is the "critical polynomial" from Subsection 7.4. Assuming that there is $m+1$ such places, we will show that $\overline{|\tau|} \ll \varepsilon^{-m-1}$, where in this proof the constants implied by the $O(\cdot)$-notation and by the Vinogradov $\ll$-notation depend only on X and t.

Thus, let $v_1, \ldots, v_{m+1}$ be distinct places of K such that every $v = v_i$ satisfies (20). We denote by $\mathcal{N}$ the $K/\mathbb{Q}$-norm. Then $\mathcal{N}v_1 \cdots \mathcal{N}v_{m+1}$ divides the numerator of the rational number $\mathcal{N}\Delta(\tau)$. Since $\deg \Delta = m$, we have $|\mathcal{N}\Delta(\tau)| \ll \overline{|\tau|}^{md}$, and the denominator of this number is $O(1)$. Hence

$$\mathcal{N}v_1 \cdots \mathcal{N}v_{m+1} \ll \overline{|\tau|}^{md}.$$

On the other hand, the left-hand side is bounded from below by $\big(\varepsilon\overline{|\tau|}\big)^{d(m+1)}$. Comparing the lower and the upper bound, we obtain $\overline{|\tau|} \ll \varepsilon^{-m-1}$, as wanted. □

A Appendix (by Jean Gillibert)

The aim of this appendix is to give a scheme-theoretic explanation of the relation between geometric and arithmetic ramification of covers of $\mathbb{P}^1$. More precisely, we shall give alternative statements and proofs for Theorems 7.1, 7.2 and 7.3 of Section 7. We also give both a conceptual and explicit description of the set of "bad" places involved in these statements.

The results that we prove here are essentially due to Beckmann [1]. They have been subsequently generalized by Conrad [5]. However, it may be useful for the reader to have a short proof of the statements we are interested in. As we shall see, the main technical tool is Abhyankar's Lemma.

Let us recall the notation: K is a number field, X is a smooth projective curve over K, and $t : X \to \mathbb{P}^1$ is a non-constant K-morphism. Then t is a finite map, and is étale outside a divisor $D \subset \mathbb{P}^1$, that one calls the branch locus of t.

Let $\mathcal{X} \to \mathbb{P}^1_{\mathcal{O}_K}$ be the normalization of $\mathbb{P}^1_{\mathcal{O}_K}$ in the function field of X (via the map t). The canonical map $\mathcal{X} \to \mathbb{P}^1_{\mathcal{O}_K}$ is a finite flat map with generic fiber t, that we also denote by t by abuse of notation. Let $\mathcal{D} \subset \mathbb{P}^1$ be the branch locus of $t : \mathcal{X} \to \mathbb{P}^1_{\mathcal{O}_K}$. Then, the scheme $\mathbb{P}^1_{\mathcal{O}_K}$ being regular and the scheme $\mathcal{X}$ being normal, the subscheme $\mathcal{D}$ is of pure codimension one, according to the Zariski-Nagata purity Theorem for the branch locus (See [9, exposé X, Theorem. 3.1]). In other terms, $\mathcal{D}$ is a divisor on $\mathbb{P}^1_{\mathcal{O}_K}$.

Let $\overline{D}$ be the scheme-theoretic closure of D in $\mathbb{P}^1_{\mathcal{O}_K}$. This is a horizontal divisor on $\mathbb{P}^1_{\mathcal{O}_K}$, with generic fiber D. Therefore, one can write

$$\mathcal{D} = \overline{D} + V$$

where V is a vertical divisor (hence supported by a finite number of fibers). Let S be the union of the following two finite sets of finite places of K:[2]

(i) the set of places supporting V,

(ii) the set of places above which two branch points of t meet, or above which the field of definition of a branch point is ramified.

By (i), the equality $\mathcal{D} = \overline{D}$ holds true in $\mathbb{P}^1_{\mathcal{O}_{K,S}}$. By (ii), $\overline{D}$ is a geometrically unibranch[3] divisor over $\mathbb{P}^1_{\mathcal{O}_{K,S}}$. In particular, it has strict normal crossings, and disjoint irreducible components.

Remark A.1 If the curve X and the map t are explicitely given (by equations), then it is possible to compute the set S, without computing the integral model $\mathcal{X}$. Indeed, the set of places supporting V is just the set of v for which the field

[2]This set S is similar to that introduced by Beckmann. We note that Conrad considers a smaller set S by allowing two horizontal components of $\mathcal{D}$ to intersect with multiplicity one, but for simplicity we stick to this definition.

[3]Let us recall that a divisor is geometrically unibranch if its irreducible components are disjoint, and if this remains true after any étale base change. For example, the nodal cubic $y^2 = x^2(x+1)$ is an irreducible normal crossing divisor in $\mathbb{P}^2$, but is not geometrically unibranch.

extension $K(X)/K(\mathbb{P}^1)$ corresponding to t is ramified at v, where v is viewed as a valuation on $K(\mathbb{P}^1)$. The other piece of the set S depends only on the knowledge of the set of branch points, and is defined in quite explicit terms.

The reason for which we introduce the set S lies in the following Lemma:

Lemma A.2 *The map $t : \mathcal{X} \to \mathbb{P}^1_{\mathcal{O}_{K,S}}$ is a tame cover with respect to the normal crossing divisor $\mathcal{D}$, in the sense of Grothendieck and Murre [10, Definition 2.2.2]. More precisely:*

1) *t is finite,*

2) *t is étale outside $\mathcal{D}$,*

3) *every irreducible component of $\mathcal{X}$ dominates an irreducible component of $\mathbb{P}^1_{\mathcal{O}_{K,S}}$,*

4) *$\mathcal{X}$ is normal,*

5) *$\mathcal{X}$ is tamely ramified above each $x \in \mathcal{D}$ of codimension 1 in $\mathbb{P}^1_{\mathcal{O}_{K,S}}$.*

Proof As we have seen above, 1) is true by construction of t, and 2) by definition of $\mathcal{D}$. The map t is surjective, hence 3) holds. The scheme $\mathcal{X}$ is normal by construction, so 4) is OK. It just remains to check 5). The local fields of codimension 1 points of $\mathcal{D}$ have characteristic zero, because $\mathcal{D} = \overline{D}$, therefore the tameness assumption is automatically satisfied.

We now recover the nice framework of the theory of tame covers by Grothendieck and Murre. It is certainly possible to transpose these results in the language of log schemes, but we do not need such techniques for our purpose.

We are now ready to state the main result of this appendix.

Theorem A.3 *Let $v \notin S$, and let $P \in X(\bar{K_v})$ which is not a ramification point of t. Then the following holds:*

1) *If the extension $K_v(P)/K_v(t(P))$ is ramified, then there exists a branch point $\alpha \in \mathbb{P}^1(\bar{K_v})$ such that $v(t(P) - \alpha) \geq 1$.*

2) *If there exists a branch point $\alpha \in \mathbb{P}^1(\bar{K_v})$ such that $v(t(P) - \alpha) = 1$, then the extension $K_v(P)/K_v(t(P))$ is ramified.*

3) *More generally, if there exists a branch point $\alpha \in \mathbb{P}^1(\bar{K_v})$ such that $v(t(P) - \alpha)$ is strictly positive and not divisible by any of the (geometric) ramification indices of points in $t^{-1}(\alpha)$, then the extension $K_v(P)/K_v(t(P))$ is ramified.*

In the statement above, we use the standard convention $t(P) - \infty = t(P)^{-1}$, as in the main text of the article. We note that $v(t(P) - \alpha) \geq 1$ means that $t(P)$ and α reduce to the same point in $\mathbb{P}^1(\bar{k_v})$, where k_v denotes the residue field

of K_v. In geometric language, $v(t(P) - \alpha)$ is the intersection number between $t(P)$ and α.

Roughly speaking, Theorem A.3 states that, outside the finite set S, the arithmetic ramification is controlled by the reduction of the geometric ramification. The statement 1) above implies Theorems 7.2 and 7.3, while statement 2) implies (via Hensel's lemma) Theorem 7.1. Our hypotheses are slightly weaker than in Section 7, in particular branch points of t are not assumed to be rational over the base field.

First, we state a version of Abhyankar's Lemma, suitable for our purpose:

Lemma A.4 (Abhyankar's Lemma) *Let Y be a noetherian normal scheme, and let $g : X \to Y$ be a tame cover with respect to a normal crossing divisor $D \subset Y$. Assume furthermore that D is geometrically unibranch. Then for each $y \in \mathrm{Supp}(D)$ there exists an étale neighbourhood $U \to Y$ of y such that $X \times_Y U \to U$ is a finite disjoint union of coverings of the form*

$$\mathrm{Spec}\,(\mathcal{O}_U[T]/(T^e - f)) \longrightarrow U$$

where $f = 0$ is a local equation of D in U, and e is relatively prime to the characteristic of the residue field of y.

Proof This follows from [10, Corollary 2.3.4, ii)]. More precisely, D being geometrically unibranch, the irreducible components of D remain disjoint over any étale neighbourhood of y in Y. Hence the last sentence in the statement of [10, Corollary 2.3.4, ii)] implies that there exists an étale neighbourhood $U \to Y$ of y such that $X \times_Y U \to U$ is a finite disjoint union of Kummer coverings[4] with respect to the divisor $D \times_Y U$. □

Remark A.5 Under the hypoteses of Lemma A.4, X is regular above the points of $\mathrm{Supp}(D)$, according to [10, Proposition 1.8.5, ii)]. In particular, if Y is regular, then X is regular. We note that this is no longer true if D is an arbitrary normal crossing divisor: in this case, one can describe X étale locally as a *generalized* Kummer covering[5] of Y. According to [10, Proposition 1.8.5 iii)], such a covering may be singular above the intersection of two irreducible components of D. See also [5, Lemma 1.4] and the erratum.

Proof of Theorem A.3 1) Let $\mathcal{O}_v$ be the ring of integers of K_v. By projectivity of $\mathcal{X}$ the point P extends into a section $P : \mathrm{Spec}\,(\mathcal{O}_v(P)) \to \mathcal{X}$ where $\mathcal{O}_v(P)$ is the ring of integers of $K_v(P)$. By definition of the branch locus, if $t(P)$ does not meets $\mathcal{D}$ (above v), then $\mathcal{O}_v(P)$ is an étale $\mathcal{O}_v(t(P))$-algebra, that is, $K_v(P)/K_v(t(P))$ is unramified. By construction of S, the divisor $\mathcal{D}$ is the scheme-theoretic closure of D in $\mathbb{P}^1_{\mathcal{O}_{K,S}}$, hence for $v \notin S$ the subschemes $t(P)$ and $\mathcal{D}$ have non-empty intersection above v if and only if there exists a branch point $\alpha \in \mathbb{P}^1(\bar{K_v})$ such that $t(P)$ and α reduce to the same point in $\mathbb{P}^1(\bar{k_v})$.

[4] See [10, Definition 1.2.2] for a definition.

[5] That is, a quotient of a Kummer covering, see [10, Definition 1.3.8].

2) This is a special case of 3).

3) In order to prove the statement, we may assume that $t(P)$ belongs to K_v. Let $\mathcal{O}_v^{\mathrm{sh}}$ be the strict henselization of the ring of integers of K_v with respect to the valuation v. Then the fraction field of $\mathcal{O}_v^{\mathrm{sh}}$ is K_v^{nr}, the maximal unramified extension of K_v.

Let π_v be a uniformizing parameter of $\mathcal{O}_v$, and let k_v be the residue field of $\mathcal{O}_v$. Then π_v is again a uniformizing parameter of $\mathcal{O}_v^{\mathrm{sh}}$, and the residue field of $\mathcal{O}_v^{\mathrm{sh}}$ is $\bar{k_v}$.

Let $\alpha \in \mathbb{P}^1(\bar{K_v})$ be a branch point of t such that $v(t(P) - \alpha) > 0$. Then, by construction of the set S, α belongs to $\mathbb{P}^1(K_v^{\mathrm{nr}})$. Up to composing t by an automorphism of $\mathbb{P}^1$ defined over K_v^{nr}, it is possible to assume that $\alpha = 0$. Let z be the standard coordinate function on $\mathbb{P}^1_{\mathcal{O}_v^{\mathrm{sh}}}$ which vanishes at 0. Let $\bar{0}$ be the closed point of $\mathbb{P}^1_{\mathcal{O}_v^{\mathrm{sh}}}$ defined by $z = 0$ on the special fiber. Then $z = 0$ is a local equation of $\mathcal{D}$ at the point $\bar{0}$ (this follows from the fact that $\mathcal{D}$ is horizontal with disjoint components). Moreover, the ring $\mathcal{O}_v^{\mathrm{sh}}[[z]]$ of formal power series is strictly henselian, because it is complete with respect to the (z, π_v)-adic topology and its residue field is $\bar{k_v}$ which is algebraically closed. We have a natural "localization" map $\mathrm{Spec}\,(\mathcal{O}_v^{\mathrm{sh}}[[z]]) \to \mathbb{P}^1_{\mathcal{O}_v^{\mathrm{sh}}}$ which sends the closed point to $\bar{0}$.

According to Lemma A.2, the map $t : \mathcal{X} \to \mathbb{P}^1_{\mathcal{O}_{K,S}}$ is a tame cover with respect to the normal crossing divisor $\mathcal{D}$. Hence, it follows from [10, Cor. 2.3.6] that the pull-back

$$\mathcal{X} \times_{\mathbb{P}^1} \mathrm{Spec}\,(\mathcal{O}_v^{\mathrm{sh}}[[z]]) \longrightarrow \mathrm{Spec}\,(\mathcal{O}_v^{\mathrm{sh}}[[z]])$$

is a tame cover with respect to the divisor $\{z = 0\}$.

Hence, according to Lemma A.4 (Abhyankar's Lemma), this scheme is a disjoint union of connected Kummer coverings of the form

$$\mathrm{Spec}\,(\mathcal{O}_v^{\mathrm{sh}}[[z]][T]/(T^e - z)) \to \mathrm{Spec}\,(\mathcal{O}_v^{\mathrm{sh}}[[z]])$$

where $e \geq 2$ is the ramification index of some point $\beta \in X$ lying above α. Let us consider the connected cover containing the point P. We may specialize it at the integral section $t(P)$, which gives us the finite cover

$$\mathrm{Spec}\,(\mathcal{O}_v^{\mathrm{sh}}[T]/(T^e - t(P))) \longrightarrow \mathrm{Spec}\,(\mathcal{O}_v^{\mathrm{sh}}).$$

It follows that the field $K_v^{\mathrm{nr}}(P)$ contains at least one root of the polynomial $T^e - t(P)$. Such a field is a ramified extension of K_v^{nr} if and only if e does not divides $v(t(P))$. Hence the result. □

Remark A.6 According to the last part of the proof above, if there exists a branch point α such that $v(t(P)-\alpha) \geq 1$, then there exists a unique ramification point β lying above α which meets P above v. Moreover, if $v(t(P) - \alpha)$ is divisible by the ramification index of β, then the extension $K_v(P)/K_v(t(P))$ is unramified, according to the last sentence of the proof.

Example A.7 Let $\lambda \in \mathbb{Q}$, distinct from 0 and 1, and let E be the elliptic curve defined over $\mathbb{Q}$ by the equation (in Legendre form)

$$y^2 = x(x-1)(x-\lambda).$$

We consider the x-coordinate map $x : E \to \mathbb{P}^1$, which is a degree 2 cover, and whose branch points are 0, 1, λ and ∞. At the function field level, the corresponding extension is

$$\mathbb{Q}\left(\sqrt{x(x-1)(x-\lambda)}\right)/\mathbb{Q}(x).$$

We note that the only prime number which ramifies in this extension is 2. This means that the vertical ramification is supported by 2.

We are now looking for the set of primes above which two branch points meet. We note that the sections 0, 1 and ∞ never meet each other in $\mathbb{P}^1(\mathbb{Z})$. Let $\lambda = \frac{a}{b}$ where a and b are coprime integers. Then λ meets 0 (resp. ∞) above primes dividing a (resp. b). Similarly, λ meets 1 above primes dividing $a-b$. Therefore, the set S is:

$$S = \{2\} \cup \{\text{primes dividing } ab(a-b)\}.$$

In the light of Remark A.6, our Theorem A.3 reads as follows: let $p \notin S$ be a prime number, and let $P \in E(\overline{\mathbb{Q}}_p)$ which is not a ramification point of x. Then the extension

$$\mathbb{Q}_p(P) = \mathbb{Q}_p\left(\sqrt{x(P)(x(P)-1)(x(P)-\lambda)}\right)/\mathbb{Q}_p(x(P))$$

is ramified if and only if there exists a branch point $\alpha \in \{0, 1, \lambda, \infty\}$ such that $v_p(x(P)-\alpha)$ is strictly positive and odd.

References

[1] S. Beckmann, On extensions of number fields obtained by specializing branched coverings, *J. Reine Angew. Math.* **419** (1991), 27–53.

[2] Yu. Bilu, J. Gillibert, Chevalley-Weil Theorem and Subgroups of Class Groups, a manuscript.

[3] Yu. F. Bilu, F. Luca, Divisibility of class numbers: enumerative approach, *J. reine angew. Math.* **578** (2005), 79–91.

[4] Yu. F. Bilu, F. Luca, Diversity in Parametric Families of Number Fields, a manuscript.

[5] B. Conrad, Inertia groups and fibers, *J. Reine Angew. Math.* **522** (2000), 1–26.

[6] H. Davenport, D. Lewis, A. Schinzel, Polynomials of certain special types, *Acta Arith.* **9** (1964), 107–116.

[7] R. Dvornicich, U. Zannier, Fields containing values of algebraic functions, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **21** (1994), 421–443.

[8] S. Lang, *Algebra (Revised Third Edition)*, GTM 211, Springer, 2002.

[9] A. Grothendieck et al., *Revêtements étales et groupe fondamental (SGA 1)*, Lecture Notes in Math. **224**, Springer-Verlag, 1971.

[10] A. Grothendieck, J. P. Murre, *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, Lecture Notes in Math. **208**, Springer-Verlag, 1971.

[11] R. J. Walker, Algebraic Curves, Springer, 1950.

[12] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, 3rd edition, Vieweg & Sohn, Braunschweig, 1997.

[13] S. H. Schanuel, Heights in number fields, *Bull. Soc. Math. France* **107** (1979), 433–449.