Rational points on curves and surfaces and the Brauer–Manin obstruction

Alexander Wang

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2026

Reading Committee:

Bianca Viray, Chair

Max Lieblich

Farbod Shokrieh

Program Authorized to Offer Degree:

Mathematics

University of Washington

Abstract

Rational points on curves and surfaces and the Brauer–Manin obstruction

Alexander Wang

Chair of the Supervisory Committee:
Professor Bianca Viray
Department of Mathematics

A central problem in arithmetic geometry is understanding the existence and structure of rational points on varieties. Over fields with interesting arithmetic, the study of rational points is tied deeply to both the number theoretic properties of the field as well as the geometric properties of the variety. In this thesis, we present two projects involving rational point problems. The first investigates superelliptic curves over Henselian fields and explains the structure of their degree sets, an object which captures a shadow of the arithmetic properties of the curve. The second proves the Hasse principle, a method of establishing the existence of rational points, over even degree extensions of the ground field for a large class of conic bundles over the projective line.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

First and foremost, I'd like to thank my advisor, Bianca Viray, for all of her support throughout my time in graduate school. This dissertation would have been possible without her guidance, feedback, and patience. She has always pushed me to be the best mathematician I can be, and for that I am incredibly grateful. I will miss our meetings and our shared appreciation of dumpling tofu soup.

I thank my parents for their endless support and unconditional love. They have always been my biggest teammates and fans, and I cannot imagine having navigated graduate school without them. I'm especially grateful for my mom's shared experiences as a researcher and an instructor, our phone calls over cooking and commutes, and her timeless advice of "不吃苦中苦，难为人上人". Thank you, Mom and Dad, for everything!

Many faculty members have been incredibly impactful during my time at the University of Washington. Farbod Shokrieh was a wonderful mentor and advocate, and I will miss both our mathematical and non-mathematical discussions. Max Lieblich, Cynthia Vinzant, Jayadev Athreya, and Stefan Steinerberger were also very helpful throughout my graduate career. I'd also like to thank Andy Loveless and Charles Camacho for their role in helping me develop as an instructor. Thanks also goes to Anthony Várilly-Alvarado and Isabel Vogt for their support as I navigated the job market in Fall 2025.

My mathematical journey has been shaped by the work of many wonderful teachers and professors throughout my life. Special thanks goes to Vern Williams and Eugene Huang for setting me on this path. I thank Jonathan Osborne for igniting my passion for mathematics through his multivariable calculus, AMT, and complex analysis classes. I also thank Stephen DeBacker, Sarah Koch, and Jenny Wilson for encouraging and supporting me throughout my

time as an undergraduate at the University of Michigan (Go Blue!). My love for mathematics, as well as my excitement towards teaching, comes from all of you, and I am very grateful.

I am thankful for my academic siblings and the mathematics we have done together. I thank Sam Roven for being a wonderful collaborator and helping me navigate the later years of graduate school. Thanks to Thomas Carr and Carlos Rivera for being excellent role models of arithmetic geometers and helping me learn number theory and algebraic geometry. Alex Galarraga has been an incredible person and mathematician to work with, and I'm grateful to have gone on this journey together. Thanks to Bryan Boehnke for his mathematical feedback and baked goods in our lab meetings. Finally, thanks to Mallory Dolorfino for their friendship, constant encouragement, passing me the puck, and allowing me to use their office to prepare my defense slides.

My time in Seattle was fundamentally shaped by the mathematics graduate student community here at the University of Washington, and I am deeply thankful for the memories we have shared here together in Padelford Hall. I thank Jessie Loucks-Tavitas for being a wonderful TA mentor, a caring and supportive friend, her hilarious sense of humor, and her affinity for crosswords. Thanks to Paige Helms for her thoughtfulness, empathy, and guidance, especially during my time as Graduate Student Representative. Nelson Niu and Natasha Crepeau were both huge inspirations to me in terms of advocacy and activism, and I thank Nelson for our resemblance and his tolerance of my weekly spoiler-tagged messages, and Natasha for her inquisitive responses, her timely use of the spritz bottle, and the memories we shared with Jessie. I thank Charlie Magland for their endless friendshrimp, for being there for me through ups and downs, for our alpaca-filled adventures, and for keeping the office candy drawer well-stocked. I also thank Grace O'Brien for our lengthy office conversations, for hosting game nights, and for our shared passion for Michigan football.

I am so thankful for my graduate cohort, and I wouldn't have wanted to take on this endeavor together with anyone else. Thanks to Haoming Ning and Yirong Yang for always

being supportive of my dream to “回家睡觉”, Tony Zeng for always finding new and innovative ways to mess with me, Garrett Mulcahy for our Costco-and-gossip trips, and Tracy Chin for always reminding me that there’s “a lot of baseball left”. I thank Jackson Morris for always getting my *The Big Lebowski* references, Michael Tang for our shared passion for trivia, and Sean Richardson for being my first-year manifolds partner.

I thank Emma Bishop, Catherine Babecki, Kevin Liu, and Albert Artiles for welcoming me to the department, happy hour escapades, March 32nd plans, and our daily birthday parties. Thanks to Cameron Wright for our time in Park City and our regular geography quizzes, and thanks to Caelan Ritter for teaching me the difference between an hyphen and an endash and how (not) to play against the Scandinavian defense. I’m especially thankful for the friendship of Leo Mayer, Lorenzo Bottiglione, Linhang Huang, Clare Minnerath, Joe Rogge, Isaiah Siegl, Zawad Chowdhury, Dora Kassabova, Maryam Emamjomeh Zadeh, Wolfgang Allred, Jonas Golm, and Jenny Zhan, among countless others.

Thank you to Vikram Mathew and Kaiwen Lu for the time we’ve shared in East Hall. Special thanks go out to Alvand Moini and Ruyan Zhang, who may have known this was my dream since 7th grade. Thanks also to David Chao, Alex Fried, David Hansen, Anoop Kalra, Adit Shah, Jason Stranne, Varun Talwar, and William Xu for their friendship from afar.

Chapter 1

INTRODUCTION

The field of arithmetic geometry lies at the intersection of algebraic geometry and number theory, as solutions to polynomial equations correspond to points of the associated geometric object. While classical algebraic geometers often work over algebraically closed fields, the arithmetic setting prefers (finite extensions of) the rational numbers, where the existence of solutions and structure of solution sets can be very complicated questions to answer. In particular, notions of the integers and prime numbers become involved, opening the door to number-theoretic input. A famous result of Faltings' [Fal83] states that a curve of genus at least 2 has finitely many solutions over a number field; this is a motivating example of the philosophy that geometry controls arithmetic. In this case, the geometric data of the genus of the curve dictates the arithmetic data of the infinitude of rational points. This slogan guides our exploration of arithmetic geometry.

The existence of rational points on varieties over a global field K is a difficult question. A necessary condition for the presence K-points is the existence of K_v-points for every completion K_v (i.e., the variety is **locally soluble**). Finding K_v-points tends to be a more tractable problem, as these fields are complete with respect to an absolute value, allowing for solutions to be constructed from successive approximation. When K_v is archimidean, this is known as Newton's method, and when K_v is nonarchimidean, we can use Hensel's lemma to accomplish the same result. In joint work with Alexander Galarraga [GW25], we study the **degree sets** of superelliptic curves over Henselian fields, a shadow of the arithmetic data describing the field extensions over which a curve possesses points.

Varieties which are locally soluble do not necessarily have global points, and it is a special situation when the existence of local points for every completion guarantees the

existence of global points. The classes of varieties which have this property are said to satisfy the **Hasse principle** (examples include Severi-Brauer varieties and certain torsors over an abelian variety). When the Hasse principle holds, proving the existence of rational points can be reduced to a finite computation, and thus understanding the Hasse principle is of great arithmetic interest. However, even if a variety X is locally soluble, Manin showed that elements of the Brauer group $\mathrm{Br}(X)$ can obstruct the existence of K-points; this is known as the **Brauer–Manin obstruction** [Man71]. In some cases, the Brauer–Manin obstruction fully explains the failure of the Hasse principle, highlighting its importance in the study of rational points. For example, a guiding conjecture of Colliot-Thélène posits that the Brauer–Manin obstruction is the only obstruction to the Hasse principle for geometrically rational varieties [CT92].

Over a fixed field of definition, the Brauer–Manin obstruction has been studied for many classes of varieties; however, investigating how it persists over extensions of the ground field is a relatively new area of research. In joint work with Sam Roven [RW26], we produce one of the first results of this type, establishing the Hasse principle for conic bundles over even degree extensions.

1.1 Organization

This thesis is structured as follows. In Chapter 2, we provide the preliminaries of arithmetic geometry and the theory of rational points on varieties, including a brief discussion of the Brauer–Manin obstruction. In Chapter 3, we discuss results regarding degree sets of superelliptic curves over Henselian fields, in joint work with Alexander Galarraga, and available as an independent paper [GW25]. In Chapter 4, we discuss results regarding the Hasse principle for conic bundles over even degree extensions, in joint work with Sam Roven, and available as an independent paper [RW26].

Chapter 2

GEOMETRY AND ARITHMETIC OF CURVES AND SURFACES

In this chapter, we review the geometry and arithmetic of curves and surfaces. Throughout this text, we say that a **variety** X over a field k is a integral scheme whose structure morphism to $\mathrm{Spec}(k)$ is separated and of finite type. A **nice** variety is a variety which is smooth, projective, and geometrically integral. A **curve** is a variety of dimension 1, and a **surface** is a variety of dimension 2.

2.1 Arithmetic of global and local fields

We begin with a discussion of the fields which appear in our results.

Definition 2.1.1. A **global field** is either:

- a number field (a finite extension of $\mathbb{Q}$), or
- $\mathbb{F}_q(t)$, where $\mathbb{F}_q$ denotes the finite field of q elements.

Definition 2.1.2. Let k be a global field. Then, two absolute values $|\cdot|_1$ and $|\cdot|_2$ on k are equivalent if they define the same topology on k. A **place** of k is an equivalence class of absolute values of k. We write Ω_k to denote the set of places of k.

If a place $v \in \Omega_k$ corresponds to an archimedean absolute value, we say that v is **archimedean**, otherwise we say that v is **nonarchimedean**. For a number field k, the nonarchimedean places of k correspond to the primes of the ring of integers of $\mathcal{O}_k$, while the archimedean places of k correspond to the embeddings of k into $\mathbb{C}$. We can define the **ring of integers** of k, denoted $\mathcal{O}_k$ as the integral closure of $\mathbb{Z}$ in k, if k is a finite extension of $\mathbb{Q}$,

and as the integral closure of $\mathbb{F}_q[t]$ in k, if k is a finite extension of $\mathbb{F}_q(t)$. For a prime $\mathfrak{p}$ of $\mathcal{O}_k$, we can produce a discrete valuation $v_\mathfrak{p}$ on k which induces an absolute value $|x|_\mathfrak{p} = e^{-v_\mathfrak{p}(x)}$. If a place $v \in \Omega_k$ is of this form, we say that v is **finite**, otherwise we say that v is **infinite**. If k is a number field, the finite places are precisely the nonarchimedean places and the infinite places are precisely the archimedean places. However, when k is a global function field, this correspondence can fail.

Definition 2.1.3. A field L is a **local field** if it is the completion of a global field k at a place $v \in \Omega_k$. If v is nonarchimedean, the **ring of integers** of L is the ring

$$\mathcal{O}_L := \{x \in L \mid |x|_v \leq 1\}.$$

In particular, $\mathcal{O}$ is a local ring, with maximal ideal

$$\mathfrak{m}_L := \{x \in L \mid |x|_v < 1\}$$

and **residue field** $\mathcal{O}_L/\mathfrak{m}_L$. A principal generator π for $\mathfrak{m}_L$ is called a **uniformizer** for $\mathcal{O}_L$ (or L).

Alternatively, one may take the intrinsic definition of a local field as a field with a non-trivial absolute value under which it is locally compact [Poo17, Section 1.1.2].

Example 2.1.4. When $k = \mathbb{Q}$, Ostrowski's theorem [Kob84, Theorem I.1] asserts that

$$\Omega_k = \{\text{primes p}\} \cup \{\infty\}$$

where ∞ denotes the standard absolute value. Completing k at a finite place $v = p$ yields the p-adic numbers $\mathbb{Q}_p$, while completing k at $v = \infty$ produces $\mathbb{R}$.

We can package the set of completions of a global field together, which will be a useful tool to keep track of varieties which have points over all completions of a global field.

Definition 2.1.5. Let k be a global field. The **adele ring** of k, denoted $\mathbb{A}_k$, is given by the restricted product

$$\mathbb{A}_k := \prod_{v \in \Omega_k}{}' (k_v, \mathcal{O}_v)$$

where all but finitely many elements of the product lie in $\mathcal{O}_v$.

When v is archimedean, we can take $\mathcal{O}_v = k_v$, since this does not affect the condition that all but finitely many elements of the product must be integral.

2.2 Nonarchimedean local fields and Henselian fields

This section provides many of the basic theory and necessary tools for our analysis in Chapter 3.

Lemma 2.2.1 (Hensel's Lemma, [Neu99, Theorem II.4.6])**.** *Let K be a nonarchimedean local field with ring of integers $\mathcal{O}_K$ and residue field k. Then, if $P \in \mathcal{O}_K[x]$ is a monic polynomial with image $\overline{P} \in k[x]$, then every factorization of $\overline{P}$ in $k[x]$ into coprime polynomials can be lifted uniquely to a factorization of $P \in \mathcal{O}[x]$.*

In particular, if $\overline{P}$ has a simple root in k, then this can be lifted uniquely to a simple root $\alpha \in \mathcal{O}$ of P. Hensel's lemma is very useful in order to solve polynomial equations over local fields, and can be thought of as a p-adic analogue of Newton's method for finding roots over $\mathbb{R}$. As such, we define a class of fields over which Hensel's lemma applies.

Definition 2.2.2. Let K be a field with a valuation v. Then, K is **Henselian** if the valuation ring of K satisfies Hensel's lemma. We say that K is **strictly Henselian** if in addition the residue field of K is separably closed.

In Chapter 3, we will examine extensions of local fields. In particular, the structure of extensions is controlled by the ramification of the uniformizer and the extension of the residue field.

Definition 2.2.3. Let L/K be an extension of local fields, with π_K a uniformizer for $\mathcal{O}_K$ and π_L a uniformizer for $\mathcal{O}_L$. Let ℓ and k be the residue fields of L and K, respectively. Then, for some unit $u \in \mathcal{O}_K^*$ and positive integer e, we have that

$$\pi_L^e = u\pi_K$$

and we say that $e = e_{L/K}$ is the **ramification degree** of L/K. We say that

$$f = f_{L/K} \coloneqq [\ell : k]$$

is the **inertia degree** of L/K.

Theorem 2.2.4 ([Neu99, Proposition II.6.8]). *Let L/K be an extension of Henselian fields. Then, we have that $[L:K] \geq ef$, and furthermore $[L:K] = ef$ if the valuation is discrete and L/K is separable.*

Theorem 2.2.5 ([Neu99, Theorem II.6.2]). *If K is Henselian, and L/K is algebraic, then there is a unique extension of $|\cdot|_K$ to L. If L/K is finite, then the extension is given by*

$$|x|_L = \left(\mathrm{Nm}_{L/K}(x)\right)^{\frac{1}{[L:K]}}$$

and $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

Theorem 2.2.5 shows that we can read off the ramification degree using the valuation (or corresponding absolute value), since we must have that $\nu(\pi_K) = 1$ and $\nu(\pi_L) = \frac{1}{e}$.

Over a Henselian field, we can obtain information about the valuation of the roots of polynomials using Newton polygons, a technique often used in tropical geometry.

Definition 2.2.6. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ over a Henselian field K with valuation ν. The **Newton polygon** of f is the lower convex hull of the points

$$\{(i, \nu(a_i))\}_{i=0}^{n}$$

given as a piecewise linear set in $\mathbb{R}^2$.

Theorem 2.2.7 ([Neu99, Proposition II.6.3]). *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Then, for every segment of the Newton polygon of f of horizontal width w and slope m, f has w corresponding roots of valuation $-m$.*

In Chapter 3, we will use the Newton polygon of $F(x)$ to deduce information regarding the ramification points of the superelliptic curve defined by $y^p = F(x)$.

2.3 Rational points on varieties

For a variety X, we want to be able to understand the points of X, corresponding to solutions of the defining equations of X. However, this depends on the ring in which the coordinates of the points are defined. As such, we would like a definition that is independent of coordinates.

Definition 2.3.1. Let X be a variety. For a scheme S, an **S-valued point** of X is a map $\mathrm{Spec}(S) \to X$. The set of S-points of S is given by

$$X(S) := \mathrm{Hom}(S, X).$$

We motivate this definition with several examples, to illustrate that this definition matches our intuition for a "point" of X.

Example 2.3.2. Let $k = \overline{k}$ be a field. Suppose $R = k[x, y]/f(x, y)$, and let $X = \mathrm{Spec}(R)$. Then, let $\mathrm{Spec}(k) \to X$ be a point. The data of such a map corresponds to a ring map $R \to k$, which is an assignment of x and y to elements of k satisfying $f(x, y) = 0$.

Example 2.3.3. Let L/K be an extension of fields. A K-point $\mathrm{Spec}(K) \to X$ is the choice of an image point $x \in X$ such that $\mathbf{k}(x) \subseteq K$. Composing with the map $\mathrm{Spec}(L) \to \mathrm{Spec}(K)$ induced by inclusion gives an L-point $\mathrm{Spec}(L) \to X$, which is the data of the same point and $\mathbf{k}(x) \subseteq K \subseteq L$.

Example 2.3.3 shows that we can interpret $X(k)$ as the set of points which have residue field contained in k, and are therefore defined over k.

Remark 2.3.4. The assignment $X(S)\colon S \mapsto \mathrm{Hom}(S, X)$ is often called the **functor of points** of X. If X is a scheme over a base scheme T, then the Yoneda lemma tells us that X is determined as a T-scheme up to isomorphism by $X(S)$ for all T-schemes S.

A central question in arithmetic geometry is determining $X(\mathbb{Q})$, the set of rational points of a variety X. More generally, for a global field K, it is a difficult question to determine $X(K)$, or even if $X(K)$ is empty.

Example 2.3.5. Consider $X = V(x^2 + y^2 - 3z^2) \subseteq \mathbb{P}^2$. Clearing denominators, we can search for integer points of X. Then, x^2 and y^2 are both divisible by 3 an even number of times, and since the squares modulo 3 are $\{0, 1\}$, $x^2 + y^2$ must also be divisible by 3 an even number of times. However, $3z^2$ will be divisible by 3 an odd number of times, showing that no integer solutions can exist.

This is an example of a **local obstruction**, as we have shown that $X(\mathbb{Q}) \subseteq X(\mathbb{Q}_3) = \emptyset$, and therefore $X(\mathbb{Q}) = \emptyset$. More generally, for a number field K, we have that $X(K) \subseteq X(K_v)$ for all places $v \in \Omega_K$. If $X(K_v) = \emptyset$ for any place $v \in K_v$, then this is enough to show that $X(K) = \emptyset$.

We can examine the points of X over all completions at once by investigating the **adelic points**, given by the restricted product

$$X(\mathbb{A}_K) = \prod_{v \in \Omega_K}{}' \left(X(K_v), X(\mathcal{O}_v)\right)$$

where all but finitely many entries of the product must lie in $X(\mathcal{O}_v)$. Note that if X is proper, then by the valuative criterion for properness, we have that $X(K_v) = X(\mathcal{O}_v)$, and thus $X(\mathbb{A}_K)$ is simply the product of $X(K_v)$ over all places $v \in \Omega_K$.

In order for $X(K)$ to be nonempty, we must have that $X(\mathbb{A}_K)$ is nonempty. However, the reverse implication does not always hold, and we investigate it further in the work presented in this thesis.

Definition 2.3.6. Let $\mathcal{C}$ be a class of varieties. We say that $\mathcal{C}$ satisfies the **Hasse principle** (or **local-to-global principle**) over K if

$$X(\mathbb{A}_K) \neq \emptyset \implies X(K) \neq \emptyset$$

for all $X \in \mathcal{C}$.

Example 2.3.7. The Hasse-Minkowski Theorem asserts that a quadratic form over a global field K represents 0 over K if and only if it represents 0 over every completion of K, and therefore quadratic forms satisfy the Hasse principle over global fields.

2.4 The Brauer group

In this section, we introduce the Brauer group, a group associated to a variety which captures geometric and arithmetic data.

Definition 2.4.1. A **central simple algebra** over a field K is a finite dimensional K-algebra A such that

- A is simple (i.e. has no nontrivial two-sided ideals), and
- the center of A is isomorphic to K.

We write $\mathrm{CSA}(K)$ for the set of central simple algebras over K.

Example 2.4.2. For $n \in \mathbb{N}$, we have that $M_n(K)$, the set of $n \times n$ matrices over K, form a central simple algebra.

Theorem 2.4.3 (Artin–Wedderburn, [GS17, Theorem 2.1.3])**.** *Let A be a central simple algebra over K. Then, there exists a unique division algebra D/K such that $A \cong M_n(D)$.*

As a simple consequence, we have that $\dim(A)$ is a square for all central simple algebras A, and we say that $\sqrt{\dim_k(A)}$ is the **degree** of A. The Artin–Wedderburn Theorem allows us to better understand the structure of central simple algebras, and also provides the basis for endowing a group structure on the set of central simple algebras.

Definition 2.4.4. Let $A, B \in \mathrm{CSA}(K)$. Then, we say that A and B are **Morita equivalent** if there exist integers m, n such that $M_n(A) \cong M_m(B)$. Equivalently, if $A \cong M_n(D_1)$ and $B \cong M_n(D_2)$ via the Artin–Wedderburn Theorem, then A and B are Morita equivalent if and only if $D_1 \cong D_2$.

Definition 2.4.5. The **Brauer group** of K, denoted $\mathrm{Br}(K)$, is given by

$$\mathrm{Br}(K) := \frac{\mathrm{CSA}(K)}{\text{Morita equivalence}}.$$

In particular, the group structure of $\mathrm{Br}(K)$ is given by tensor product, and $M_n(K)$ represents the identity element.

The assignment K to $\mathrm{Br}(K)$ is functorial, in the sense that for a field extension L/K, we have a map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ mapping $A \mapsto A \otimes_k L$. We say that L **splits** A if $A \otimes_k L \cong M_n(L)$, or equivalently that $A \in \ker(\mathrm{Br}(K) \to \mathrm{Br}(L))$.

Equivalently, we have that $\mathrm{Br}(K) \cong H^2(K, \mathbb{G}_m)$, the second Galois cohomology group of K. Since central simple algebras are separably split, they represent $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-forms of $M_n(K)$, which are classified by $H^1(K, \mathrm{PGL}_n(K))$. Using the exact sequence

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \mathrm{GL}_n(K) \longrightarrow \mathrm{PGL}_n(K) \longrightarrow 0$$

and taking cohomology, we can identify a central simple algebra with its class in $H^1(K, \mathrm{PGL}_n(K)) \to H^2(K, \mathbb{G}_m) = \mathrm{Br}(K)$.

We now discuss quaternion algebras, a specific type of central simple algebra which is particularly amenable to computations.

Definition 2.4.6. For a field K, we can define the quaternion algebra $(a, b)_K$ to be the 4-dimensional K-algebra given by the relations $i^2 = a$, $j^2 = b$, and $ij = -ji$.

To each quaternion algebra, we have an associated conic, given by the correspondence $(a, b)_K \leftrightarrow ax^2 + by^2 = z^2$. This is an example of a **Severi–Brauer variety**, a variety which is geometrically isomorphic to projective space. Such varieties have a close correspondence with elements of the Brauer group.

Lemma 2.4.7 ([GS17, Proposition 1.3.2])**.** *Let $(a, b)_K$ be a quaternion algebra, and let $C : ax^2 + by^2 = z^2 \subseteq \mathbb{P}^2_K$ be the associated conic. Then, $(a, b)_K$ is split if and only if $C(K) \neq \emptyset$.*

Class field theory gives us an understanding of the Brauer groups of local and global fields.

Lemma 2.4.8 ([Poo17, Theorem 1.5.34])**.** *We have that*

- $\mathrm{Br}(\mathbb{C}) = 0$,
- $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$, *generated by the quaternion algebra* $(-1, -1)_{\mathbb{R}}$,

- $\mathrm{Br}(K) = \mathbb{Q}/\mathbb{Z}$, *if* K *is a nonarchimedean local field.*

Lemma 2.4.9 ([GS17, Corollary 6.5.4])**.** *Let* K *be a number field. Then, the sequence*

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \mathrm{Br}(\mathbb{A}_K) = \prod_{v \in \Omega_K} \mathrm{Br}(K_v) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

is exact. The rightmost map is given by choosing a sequence of compatible isomorphisms for each $\mathrm{Br}(K_v)$ *with* $\mathbb{Q}/\mathbb{Z}$*, and summing over these maps.*

We can extend the notion of a Brauer group from fields to schemes using the cohomological definition.

Definition 2.4.10. Let X be a scheme. Then, the Brauer group of X, denoted $\mathrm{Br}(X)$, is given by

$$\mathrm{Br}(X) := H^2_{\text{ét}}(X, \mathbb{G}_m).$$

Note that when $X = \mathrm{Spec}(K)$ for a field K, this agrees with the previous definition. This definition is also functorial, although contravariant for schemes. We highlight some nice properties of Brauer groups of schemes below.

Lemma 2.4.11 ([CTS21, Theorem 3.5.5, Corollary 6.2.11])**.** *The following are properties of the Brauer group of schemes.*

1. *If* X *is a smooth geometrically integral variety over a field* K *with* $\mathrm{char}(K) = 0$*, then the generic point* $\eta\colon \mathrm{Spec}(\mathbf{k}(X)) \to X$ *gives an inclusion* $\mathrm{Br}(X) \to \mathrm{Br}(\mathbf{k}(X))$*.*

2. *If* X *and* Y *are smooth projective varieties which are birationally equivalent, then* $\mathrm{Br}(X) \cong \mathrm{Br}(Y)$*.*

Theorem 2.4.12 ([Poo17, Theorem 6.8.3])**.** *Let* X *be a nice variety over a number field* K *with generic point* $\eta\colon \mathrm{Spec}(\mathbf{k}(X)) \to X$*. Then, there is an exact sequence*

$$0 \longrightarrow \mathrm{Br}(X) \longrightarrow \mathrm{Br}(\mathbf{k}(X)) \longrightarrow \bigoplus_{D \in X^{(1)}} H^1(\mathbf{k}(D), \mathbb{Q}/\mathbb{Z})$$

where the last map is given by a sum of residues at codimension 1 *subschemes.*

We interpret Theorem 2.4.12 as stating that the Brauer classes on X are the Brauer classes on $\mathbf{k}(X)$ which have no residues at any codimension 1 subschemes of X.

2.5 The Brauer–Manin obstruction to the Hasse principle

For a scheme X and a closed point $x \in X(K)$, the map $x\colon \operatorname{Spec}(K) \to X$ induces a functorial map on Brauer groups $x^*\colon \operatorname{Br}(X) \to \operatorname{Br}(K)$. We therefore have, for every field K over which X is defined, a pairing

$$\begin{aligned} \langle -, - \rangle : X(K) \times \operatorname{Br}(X) &\to \operatorname{Br}(K) \\ \langle x, \alpha \rangle &\mapsto x^*\alpha \end{aligned}$$

which is linear in the $\operatorname{Br}(X)$ component. This fits into the following diagram

$$\begin{array}{ccccccccc} & & X(K) \times \operatorname{Br}(X) & \longrightarrow & X(\mathbb{A}_K) \times \operatorname{Br}(X) & & & & \\ & & \downarrow & & \downarrow & \searrow & & & \\ 0 & \longrightarrow & \operatorname{Br}(K) & \longrightarrow & \bigoplus_{v \in \Omega_K} \operatorname{Br}(K_v) & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array}$$

which commutes by the exactness of the bottom row, by Lemma 2.4.9. We then make the following observation: if $X(K) \neq \emptyset$, then for any $\alpha \in \operatorname{Br}(X)$, commutativity of the diagram asserts that the image of $x^*\alpha$ must be $0 \in \mathbb{Q}/\mathbb{Z}$. Thus, given $\alpha \in \operatorname{Br}(X)$, we can define

$$X(\mathbb{A}_K)^\alpha := \left\{ (x_v) \in \mathbb{A}_K \;\middle|\; \sum_{v \in \Omega_K} x_v^*\alpha = 0 \in \mathbb{Q}/\mathbb{Z} \right\}$$

as the set of adelic points orthogonal to α. Then, $X(K) \subseteq X(\mathbb{A}_K)^\alpha$ for all $\alpha \in \operatorname{Br}(X)$, and thus we have that

$$X(K) \subseteq X(\mathbb{A}_K)^{\operatorname{Br}(X)} := \bigcap_{\alpha \in \operatorname{Br}(X)} X(\mathbb{A}_K)^\alpha.$$

Definition 2.5.1. We say that $X(\mathbb{A}_K)^{\operatorname{Br}(X)}$ is the **Brauer–Manin set** of X. If $X(\mathbb{A}_K) \neq \emptyset$ but $X(\mathbb{A}_K)^{\operatorname{Br}(X)} = \emptyset$, then necessarily $X(K) = \emptyset$, and we say that X has a **Brauer–Manin obstruction** to the Hasse principle.

Remark 2.5.2. If X is a scheme over K with structure morphism $\pi\colon X \to \mathrm{Spec}(K)$, then note that for $\alpha \in \mathrm{Br}(K)$, we have that $X(\mathbb{A}_K)^{\pi^*\alpha} = X(\mathbb{A}_K)$. In other words, the Brauer classes coming from the ground field cannot obstruct the Hasse principle. This means that in order to compute a Brauer–Manin obstruction, it suffices to consider $\mathrm{Br}(X)/\mathrm{Br}_0(X)$, where $\mathrm{Br}_0(X)$ denotes the image of $\mathrm{Br}(K)$ inside $\mathrm{Br}(X)$.

Lemma 2.5.3 ([Poo17, Corollary 6.7.8])**.** *Let X be a nice variety over a number field K. Then, the Hochschild–Serre spectral sequence gives an isomorphism*

$$\frac{\mathrm{Br}_1(X)}{\mathrm{Br}_0(X)} \cong H^1(\mathrm{Gal}(k^{\mathrm{sep}}/k), \mathrm{Pic}(\overline{X}))$$

where $\mathrm{Br}_1(X)$ denotes the kernel of the map $\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})$ induced by base change to a separable closure.

When X is a curve or geometrically rational surface, $\mathrm{Br}(X) = \mathrm{Br}_1(X)$, and so Lemma 2.5.3 is very useful for computing the Brauer–Manin obstruction on X. In particular, Châtelet surfaces are geometrically rational, and so Lemma 2.5.3 allows us to compute the Brauer group in Chapter 4.

Chapter 3

DEGREE SETS OF SUPERELLIPTIC CURVES OVER HENSELIAN FIELDS

This chapter represents the work of a long and fruitful collaboration with Alexander Galarraga, available at [GW25] and has been submitted for publication. We maintain that the work is done with equal contribution; however, for the purposes of this thesis, we attribute Section 3.4 and Theorem 3.6.1 to Alexander Galarraga, and Section 3.3 and Section 3.5 to the author.

3.1 Main results

Given a variety V/K over a field K, one would like to determine $V(K)$, the set of K-rational points. If it happens that $V(K)$ is empty, one would then like to determine for which extensions L/K does V acquire points over L. Explicitly, define the degree set of V/K by

$$\mathcal{D}(V/K) \coloneqq \{\deg_K(P) \mid P \in V,\ P \text{ closed}\}$$

where $\deg_K P$ denotes the degree of the residue field $\mathbf{k}(P)$ over K, and the index of V/K by $\operatorname{ind}(V/K) \coloneqq \gcd \mathcal{D}(V)$. We would like to determine the degree set of V/K.

When K is a discretely valued Henselian field, determining the index and the degree set is possible. Gabber, Liu, and Lorenzini have shown that that the index over K depends only on data related to the special fiber [GLL13, Theorem 8.2], and Creutz and Viray showed that the degree set can be computed explicitly from the special fiber of a strict normal crossings model [CV25, Theorem 1.1]. Thus, provided knowledge of the special fiber, one can compute the degree set. For a large class of curves with affine model $f(x, y) = 0$, [Dok21, Theorem 1.1] gives an effective method, and for hyperelliptic curves with potential semistable reduction,

[FN20, Theorem 1.2] describes the special fiber in terms of cluster diagrams. In general, however, the special fiber is difficult to compute.

Creutz and Viray give examples of curves C/K with index 1 having degree set that excludes infinitely many integers. These degree sets do not arise over finite fields or global fields. Indeed, over finitely generated fields, the degree set contains all sufficiently large multiples of the index (e.g. [LL18, Theorem 7.5]). Since $\mathrm{ind}(C/K)$ is the greatest common divisor of the degrees in $\mathcal{D}(C/K)$, we always have a containment $\mathcal{D}(C/K) \subseteq \mathrm{ind}(C/K)\mathbb{N}$. We say that $\mathcal{D}(C/K)$ is **cofinite** if the complement of $\mathcal{D}(C/K)$ in $\mathrm{ind}(C/K)\mathbb{N}$ is finite, and **not cofinite** otherwise. We investigate when this behavior occurs for curves C/K which are **superelliptic** of prime degree (curves with a cyclic cover $C \to \mathbb{P}^1$ of prime degree q). Over fields of characteristic not q, superelliptic curves are birational to an affine plane curve of the form $y^q = F(x)$. When q is 2, the curve is hyperelliptic.

Following [DDMM19], we give an answer in terms of clusters. A **cluster** is a subset of the roots of $F(x)$ contained in an open disk. As the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on the roots of $F(x)$, there is a natural action of $\mathrm{Gal}(\overline{K}/K)$ on clusters (see Definition 3.3.1). Let $\mathcal{O}(\mathfrak{s})$ denote the orbit of a cluster $\mathfrak{s}$ under $\mathrm{Gal}(\overline{K}/K)$, let $c_{\mathfrak{s}}$ be the integer defined in Lemma 3.3.4, and let $\gamma_{\mathfrak{s}} \in K$ be defined as in Lemma 3.4.2. Note that $c_{\mathfrak{s}}$ and $\gamma_{\mathfrak{s}}$ are computable by hand from the roots of $F(x)$, see Example 3.7.1.

Theorem 3.1.1. *Suppose that the residue field of K is algebraically closed and that every root of $F(x)$ is tamely ramified. Then, $\mathcal{D}(C/K)$ is not cofinite if and only if $\nu(F(0)) \not\equiv 0 \pmod{q}$, and for every Galois-invariant cluster $\mathfrak{s}$ of roots of $F(x)$,*

(i) $|\mathfrak{s}| \equiv 0 \pmod{q}$ *and* $c_{\mathfrak{s}} \not\equiv 0 \pmod{q}$, *and*

(ii) if $\gamma_{\mathfrak{s}} \in X_{\mathfrak{s}}$, *then* $\nu(F(\gamma_{\mathfrak{s}})) \not\equiv 0 \pmod{q}$.

When these conditions are satisfied, we have that

$$\mathcal{D}(C/K) \subseteq q\mathbb{N} \cup \bigcup_{\substack{\mathfrak{s} \text{ not Galois} \\ \text{invariant}}} |\mathcal{O}(\mathfrak{s})|\mathbb{N}.$$

The two main tools used in the proof of Theorem 3.1.1 are Lemma 3.3.4 and Lemma 3.5.1. Lemma 3.3.4 provides a formula to compute $\nu(F(x_0))$ as a function of $x_0 \in \overline{K}$ and the nearest cluster, and as such may be of independent interest. Lemma 3.5.1 shows that there is an obstruction to the degree set being cofinite arising from the valuation to points of arbitrary degree.

The results of [CV25] together with Theorem 3.1.1 show that the sizes of the orbits of the clusters must relate to the multiplicities of the components of the special fiber of a regular model with strict normal crossings. Following the construction of [Dok21], for many Galois invariant clusters $\mathfrak{s}$ (specifically, for those that fall in case (*a*) of Lemma 3.4.1), there exists a v-edge $L_{\mathfrak{s}}$, and that $\delta_{L_{\mathfrak{s}}}$ equals 1 if and only if the conditions of Theorem 3.1.1 are not satisfied. When $\delta_{L_{\mathfrak{s}}}$ equals 1, there are intersecting copies of $\mathbb{P}^1$ with coprime multiplicity, and thus [CV25, Theorem 1.1] shows that for some r, $\mathbb{N}_{>r} \subseteq \mathcal{D}(C/K)$. We compute the degrees of all points reducing to the $\mathbb{P}^1$'s arising from $L_{\mathfrak{s}}$ simultaneously in Lemma 3.5.5. When C/K is not Δ_v-regular, the methods of [Dok21] do not give a regular model, see Remark 3.7.2. As in Example 3.7.1, we can often compute the degree set even when C/K is not Δ_v-regular.

Restricting briefly to the case of hyperelliptic curves, [FN20, Theorem 1.2] shows that, if the curve has potential semistable reduction (which is equivalent to every root of $F(x)$ being tamely ramified), the special fiber can be computed from a *cluster diagram* (see [DDMM23] or the overview [BBB+22]) and thus the degree set depends only on the cluster diagram. Using an additional quantity $c_{\mathfrak{s}}$, both $|\mathfrak{s}|$ and $\nu(F(\gamma_{\mathfrak{s}}))$ can be computed from the cluster diagram (see Remark 3.5.4). We do not know how $c_{\mathfrak{s}}$ relates to the cluster diagram.

Theorem 3.1.2. *Let K be a discretely valued Henselian field with algebraically closed residue field of characteristic p. Let q be a prime not equal to p, and let $n_1, \ldots, n_\ell$ be positive integers. Then, there exists a superelliptic curve C/K such that*

$$\mathcal{D}(C/K) = q\mathbb{N} \cup n_1\mathbb{N} \cup \ldots \cup n_\ell\mathbb{N}.$$

As a special case of Theorem 3.1.2, we find that for every pair of odd primes p and q,

there exists a curve C/K such that $\mathcal{D}(C/K) = p\mathbb{N} \cup q\mathbb{N}$. Thus, the density of $\mathcal{D}(C/K)$ in $\mathrm{ind}(C/K)\mathbb{N}$ can be arbitrarily small.

3.2 Generalities on arithmetic over Henselian fields

3.2.1 Notation

Throughout this chapter, let K be a discretely valued Henselian field with value group $\mathbb{Z}$, let ν be the valuation on $\overline{K}$ normalized with respect to K and associated absolute value $|\cdot|$, uniformizer π, and residue characteristic p. A curve is a smooth, projective, geometrically integral, dimension 1 scheme over a field. For a prime $q \neq p$, a superelliptic curve C/K of degree q and genus g is the normalization of the projective closure of an affine variety given by $y^q = F(x)$, where $F(x)$ has no q-th powers. Let $F(x) = a_d \prod_{i=1}(x - \alpha_i)$ be the factorization over $\overline{K}$.

3.2.2 General lemmas

Lemma 3.2.1. *Let p be a prime, let k be a field, and let $a \in k^*$. The polynomial $h(y) = y^p - a$ is either irreducible or $a \in k^{\times p}$.*

Proof. This follows from [Lan02, Chapter VI, Theorem 9.1]. □

Lemma 3.2.2. *For integers a, b, c, and r, let $\rho\colon \frac{1}{r}\mathbb{Z} \to \frac{1}{rb}\mathbb{Z}$ be an affine map defined by*

$$\rho(x) = \frac{a}{b}x + \frac{c}{b}.$$

The image of ρ intersects $\frac{1}{r}\mathbb{Z}$ if and only if $\gcd(a, b)$ divides rc. If this condition holds, then for any open interval I of length greater than $\frac{b+1}{r}$, $\mathrm{im}(\rho)$ restricted to $I \cap \frac{1}{r}\mathbb{Z}$ intersects $\frac{1}{r}\mathbb{Z}$.

Proof. As $\frac{1}{r}\mathbb{Z}$ and $\frac{1}{rb}\mathbb{Z}$ are isomorphic to $\mathbb{Z}$, we construct a map $\varphi\colon \mathbb{Z} \to \mathbb{Z}$ from ρ. Explicitly, let $\theta\colon \mathbb{Z} \to \frac{1}{r}\mathbb{Z}$ be division by r, and let $\psi\colon \frac{1}{rb}\mathbb{Z} \to \mathbb{Z}$ be multiplication by rb. Define φ by $\varphi(x) \coloneqq (\psi \circ \rho \circ \theta)(x) = ax + rc$. Then, $\mathrm{im}(\rho)$ intersects $\frac{1}{r}\mathbb{Z}$ if and only if $\mathrm{im}(\varphi)$ intersects $b\mathbb{Z}$, as $b\mathbb{Z}$ is the image of $\frac{1}{r}\mathbb{Z}$ under ψ. The image of φ intersects $b\mathbb{Z}$ precisely when there is

a solution to $ax \equiv -rc \pmod{b}$, which is solvable if and only if $\gcd(a, b)$ divides rc. For an interval I, if $|I| > \frac{b+1}{r}$, then by the pigeonhole principle, the numerators of $I \cap \frac{1}{r}\mathbb{Z}$ contain a complete set of representatives of congruence classes modulo b. □

3.2.3 Results about Henselian fields

The following is a strengthening of Krasner's lemma, provided that one works with K^t, the tamely ramified closure, rather than $\overline{K}$.

Lemma 3.2.3. *Let B be an open ball in $\overline{K}$ such that $B \cap K^t$ is nonempty. There exists $\beta \in B$ such that for all $\alpha \in B$, $K(\beta) \subseteq K(\alpha)$ and $\deg_K(\beta)$ equals the size of the orbit of B under $\mathrm{Gal}(K^t/K)$.*

Proof. This is the one dimensional case of [Duc13, Theorem 3.5]. □

Lemma 3.2.4. *Assume that the residue field of K is algebraically closed. If r is coprime to the residue characteristic of K, then $K(\sqrt[r]{\pi})$ is the unique extension of K of degree r.*

Proof. This follows from [Lan13, Chapter II, Proposition 12]. □

3.2.4 Structure of degree sets of general schemes over Henselian fields

We establish two lemmas that are crucial to the computation of degree sets. Both follow from a result of Liu and Lorenzini [LL18]. We state them here in the form we require for our argument.

Lemma 3.2.5. *Let X/K be a geometrically integral and smooth scheme of finite type and positive dimension. Let $m \in \mathbb{N}$. If $m \in \mathcal{D}(X/K)$, then $m\mathbb{N} \subseteq \mathcal{D}(X/K)$.*

Proof. Since K is Henselian, K is a large field [Pop10, Theorem 1.1]. If $m \in \mathcal{D}(X/K)$, there exists some extension L/K of degree m such that $X(L)$ is nonempty, and hence contains a smooth point. From [LL18, Proposition 8.3], we find that over any separable extension M/L, X gains infinitely many new points. We can then pick a separable extension M_n/L of

degree n for each $n \in \mathbb{N}$, as for example, if π is a uniformizer for K, then $X^n + \pi X + \pi$ will be an irreducible and separable polynomial. Thus, we find that $m\mathbb{N} \subseteq \mathcal{D}(X/K)$. □

Lemma 3.2.6. *Let X/K be a geometrically integral and smooth scheme of finite type and positive dimension. Let W be a Zariski open subset of X. Then, $\mathcal{D}(W/K) = \mathcal{D}(X/K)$.*

Proof. As W embeds into X, we have that $\mathcal{D}(W/K) \subseteq \mathcal{D}(X/K)$. If $m \in \mathcal{D}(X/K)$, then there exists some L/K of degree m such that $X(L)$ is nonempty. Since K is Henselian, L is also Henselian, and hence is a large field [Pop10, Theorem 1.1], so that $X(L)$ is Zariski dense. Thus, $W(L)$ is nonempty, and hence there exists some point of W having degree dividing m. Applying Lemma 3.2.5, we find that $m \in \mathcal{D}(W/K)$. □

3.3 The valuation of a polynomial

In this section we address the question of determining, for any $x_0 \in \overline{K}$, the valuation of $F(x_0)$ in terms of the valuation of x_0. We give a complete answer in terms of the roots $\{\alpha_i\}$ of the polynomial $F(x)$.

Definition 3.3.1 (see [DDMM19, Definition 1.1])**.** A **cluster** is a nonempty subset $\mathfrak{s} \subseteq \{\alpha_i\}$ of the form $\mathfrak{s} = D \cap \{\alpha_i\}$ for some disk $D_{z,d} = \{x \in \overline{K} \mid |x - z| \leq d\}$ for some $z \in \overline{K}$ and $d \in \mathbb{R}$. Let $\mathcal{O}(\mathfrak{s})$ denote the orbit of $\mathfrak{s}$ as a set under $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, and let $\mathfrak{s}^c$ denote the complement of $\mathfrak{s}$ in $\{\alpha_i\}$.

Lemma 3.3.2. *Let $x_0 \in \overline{K}$, and let $\{\alpha_i\}$ be the roots of $F(x)$. Let $R_{x_0} = \min_i |x_0 - \alpha_i|$ and let S be the set of roots that achieve the minimum. Then, S is a cluster.*

Proof. Choose $z = x_0$ and $d = R_{x_0}$. We then have that $S = D_{z,d} \cap \{\alpha_i\}$. □

Definition 3.3.3. For any cluster $\mathfrak{s}$, let $X_{\mathfrak{s}} \subseteq \overline{K}$ be the set

$$X_{\mathfrak{s}} = \{x \in \overline{K} \mid \forall \alpha \in \mathfrak{s}, |x - \alpha| = R_x, \forall \alpha' \notin \mathfrak{s}, |x - \alpha'| > R_x\}.$$

We think of $X_{\mathfrak{s}}$ as partitioning $\overline{K}$ by the roots of minimal distance. By construction, the collection of $\{X_{\mathfrak{s}}\}$ forms an open cover of $\overline{K}$ as $\mathfrak{s}$ varies over all clusters.

Lemma 3.3.4. *Fix a cluster $\mathfrak{s}$. There exists $c_{\mathfrak{s}} \in \mathbb{Q}$ such that for all $x_0 \in X_{\mathfrak{s}}$ and any $\alpha \in \mathfrak{s}$,*

$$\nu(F(x_0)) = |\mathfrak{s}| \cdot \nu(x_0 - \alpha) + c_{\mathfrak{s}},$$

where $c_{\mathfrak{s}}$ is given by

$$c_{\mathfrak{s}} = \nu(a_d) + \sum_{\beta \in \mathfrak{s}^c} \nu(\alpha - \beta)$$

and all expressions above are independent of the choice of $\alpha \in \mathfrak{s}$.

Note that for any choice of $\alpha \in \mathfrak{s}$, the expression $|\mathfrak{s}|\,\nu(x_0 - \alpha)$ is equivalent to $\sum_{\alpha' \in \mathfrak{s}} \nu(x_0 - \alpha')$, since all roots in $\mathfrak{s}$ are equidistant from x_0. This definition is more symmetric in $\mathfrak{s}$ but less useful computationally.

Remark 3.3.5. By Lemma 3.3.4, $|\mathfrak{s}|$ and $c_{\mathfrak{s}}$ are the coefficients of the piecewise affine linear function given by the slope formula, see [BPR13, Theorem 5.15].

Proof of Lemma 3.3.4. For $\beta \in \mathfrak{s}^c$,

$$R_{x_0} < |x_0 - \beta| = |x_0 - \alpha + \alpha - \beta| \leq \max\{|x_0 - \alpha|, |\alpha - \beta|\} = \max\{R_{x_0}, |\alpha - \beta|\}.$$

We therefore have that $|\alpha - \beta| > R_{x_0}$ and thus by strong triangle inequality, $|x_0 - \beta| = |\alpha - \beta|$ and we have the same equality on valuations. Thus, we have

$$\begin{aligned}\nu(F(x_0)) &= \nu(a_d) + \sum_{\alpha' \in \mathfrak{s}} \nu(x_0 - \alpha') + \sum_{\beta \in \mathfrak{s}^c} \nu(x_0 - \beta) = \nu(a_d) + \sum_{\alpha' \in \mathfrak{s}} \nu(x_0 - \alpha) + \sum_{\beta \in \mathfrak{s}^c} \nu(\alpha - \beta) \\ &= |\mathfrak{s}| \cdot \nu(x_0 - \alpha) + \left(\nu(a_d) + \sum_{\beta \in \mathfrak{s}^c} \nu(\alpha - \beta)\right)\end{aligned}$$

which gives the desired formula for $x_0 \in X_{\mathfrak{s}}$ (note that the choice of α was arbitrary). □

3.4 Properties of clusters

Lemma 3.4.1. *Let $\mathfrak{s}$ be a cluster. Then, at least one of the following is true:*

(a) *there exists some root $\alpha_{\min}$ of $\mathfrak{s}$ such that $\mathfrak{s} = \{\alpha \mid \nu(\alpha) \geq \nu(\alpha_{\min})\}$, or*

(*b*) *all roots of* $\mathfrak{s}$ *are contained in* $B_{|\alpha|}(\alpha)$ *for any* $\alpha \in \mathfrak{s}$*, and further* $X_{\mathfrak{s}} \subseteq B_{|\alpha|}(\alpha)$.

Proof. Let $\alpha_{\min}$ denote a root of $\mathfrak{s}$ of minimal valuation. Suppose that (*a*) does not hold, that is, there exists some $\beta \in \mathfrak{s}^c$ such that $|\beta| \leq |\alpha_{\min}|$. Let $x \in X_{\mathfrak{s}}$. As $\beta \in \mathfrak{s}^c$, by definition of $X_{\mathfrak{s}}$, $|x-\beta| > |x-\alpha_{\min}|$. If $|x| \neq |\alpha_{\min}|$, then $|x-\alpha_{\min}| = \max\{|x|, |\alpha_{\min}|\} \geq \max\{|x|, |\beta|\} \geq |x-\beta|$, a contradiction, and thus $|x| = |\alpha_{\min}|$. As $|\beta| \leq |\alpha_{\min}| = |x|$, the strong triangle inequality gives that $|x-\beta| \leq |x|$, and hence $|x-\alpha_{\min}| < |x-\beta| \leq |x| = |\alpha_{\min}|$, so that $x \in B_{|\alpha_{\min}|}(\alpha_{\min})$. For all $\alpha \in \mathfrak{s}$, by the definition of $X_{\mathfrak{s}}$, $|x-\alpha| = |x-\alpha_{\min}| < |\alpha_{\min}|$. Hence,

$$|\alpha_{\min} - \alpha| = |\alpha_{\min} - x + x - \alpha| \leq \max\{|x-\alpha_{\min}|, |x-\alpha|\} < |\alpha_{\min}|.$$

As all elements of $B_{|\alpha_{\min}|}(\alpha_{\min})$ have the same absolute value and any element of the ball can be chosen as the center, the ball $B_{|\alpha|}(\alpha)$ does not depend on choice of $\alpha \in \mathfrak{s}$. □

Lemma 3.4.2. *Suppose that the residue field of* K *is algebraically closed and that the roots of* $F(x)$ *are tamely ramified. Let* $\mathfrak{s}$ *be a Galois-invariant cluster. There exists* $\gamma_{\mathfrak{s}} \in K$ *and* $\alpha_{\min} \in \mathfrak{s}$ *such that* $\mathfrak{s} = \{\alpha \mid \nu(\alpha - \gamma_{\mathfrak{s}}) \geq \nu(\alpha_{\min} - \gamma_{\mathfrak{s}})\}$.

Proof. If $|\mathfrak{s}| = 1$, then we can take $\gamma_{\mathfrak{s}} = \alpha$ for the unique $\alpha \in \mathfrak{s}$, which is an element of K as $\mathfrak{s}$ is fixed by the Galois action. Now suppose $|\mathfrak{s}| > 1$, and fix some $\alpha \in \mathfrak{s}$. Define

$$\epsilon_{\mathfrak{s}} := \max_{\alpha' \in \mathfrak{s}}\{|\alpha - \alpha'|\} \qquad \delta_{\mathfrak{s}} := \min_{\beta \in \mathfrak{s}^c}\{|\alpha - \beta|\}.$$

For the remainder of the proof, let $\alpha' \in \mathfrak{s}$ be such that $|\alpha - \alpha'| = \epsilon_{\mathfrak{s}}$, and let $\beta \in \mathfrak{s}^c$ be such that $|\alpha - \beta| = \delta_{\mathfrak{s}}$. Let $x \in X_{\mathfrak{s}}$, so that by the definition of $X_{\mathfrak{s}}$,

$$\delta_{\mathfrak{s}} = |\alpha - \beta| = |\alpha - x + x - \beta| \leq \max\{|\alpha - x|, |x - \beta|\} = |x - \beta|,$$
$$\epsilon_{\mathfrak{s}} = |\alpha - \alpha'| = |\alpha - x + x - \alpha'| \leq \max\{R_x, R_x\} < |x - \beta| = \delta_{\mathfrak{s}}.$$

Now, let L/K be the splitting field of $F(x)$. As all roots of $F(x)$ are tamely ramified, by Lemma 3.2.4, there exists $r \in \mathbb{N}$ and a uniformizer τ for L such that $\tau^r = \pi$ and $L = K(\tau)$. Expanding α, α' and β in τ, we have that

$$\alpha = \sum_i b_i \tau^i \qquad \alpha' = \sum_i b_i' \tau^i \qquad \beta = \sum_i c_i \tau^i.$$

Let N be the smallest integer such that $b_N \neq c_N$, so that $\delta_{\mathfrak{s}} = |\alpha - \beta| = |\tau^N|$, and let N' be the smallest integer such that $b_{N'} \neq b'_{N'}$, so that $\epsilon_{\mathfrak{s}} = |\alpha - \alpha'| = |\tau^{N'}|$. We have that $|\tau^{N'}| < |\tau^N|$, so that $N < N'$. Let $\gamma_{\mathfrak{s}} \coloneqq \sum_{-\infty<i}^{N'-1} b_i \tau^i$. Note that by construction of $\gamma_{\mathfrak{s}}$ and definition of β, for all $\beta' \in \mathfrak{s}^c$ and all $\alpha'' \in \mathfrak{s}$,

$$\nu(\beta' - \gamma_{\mathfrak{s}}) \leq \nu(\beta - \gamma_{\mathfrak{s}}) = N\,\nu(\tau) < N'\,\nu(\tau) = \nu(\alpha' - \gamma_{\mathfrak{s}}) \leq \nu(\alpha'' - \gamma_{\mathfrak{s}}). \tag{3.1}$$

Thus, $\gamma_{\mathfrak{s}}$ has the desired property. Finally, we show that $\gamma_{\mathfrak{s}} \in K$. As L/K is tamely ramified and the residue field of K is algebraically closed, $\operatorname{char} K \nmid [L : K]$, and hence L/K is separable and thus Galois. Suppose for the sake of contradiction that $\gamma_{\mathfrak{s}} \notin K$, so that there exists $\sigma \in \operatorname{Gal}(L/K)$ such that $\sigma(\gamma_{\mathfrak{s}}) \neq \gamma_{\mathfrak{s}}$. As the residue field of K is algebraically closed, for all i, $\sigma(b_i) = b_i$. Thus, we see there must exist some minimal $M < N'$ such that $\sigma(\tau^M) \neq \tau^M$ and $b_M \neq 0$. However, this shows that $\sigma(\alpha) \neq \alpha'$, and hence as $\mathfrak{s}$ is Galois invariant, there exists $\alpha_{\min} \in \mathfrak{s}$ such that $|\alpha - \alpha_{\min}| = |\tau^M| > |\tau^{N'}| = |\alpha - \alpha'| = \epsilon_{\mathfrak{s}}$, contradicting the definition of $\epsilon_{\mathfrak{s}}$. □

Remark 3.4.3. For a cluster $\mathfrak{s}$, there must exist some cluster $\mathfrak{s}'$ such that $\gamma_{\mathfrak{s}} \in X_{\mathfrak{s}'}$. From Equation (3.1), for any $\alpha \in \mathfrak{s}$ and $\beta' \in \mathfrak{s}^c$, $|\beta' - \gamma_{\mathfrak{s}}| > |\alpha - \gamma_{\mathfrak{s}}|$, and thus the collection of roots closest to $\gamma_{\mathfrak{s}}$ is a subset of $\mathfrak{s}$, that is, $\mathfrak{s}' \subseteq \mathfrak{s}$. When $\gamma_{\mathfrak{s}}$ is closest to some root α, then by Galois-invariance of the valuation, $\nu(\gamma_{\mathfrak{s}} - \alpha')$ is constant for every conjugate α' of α. We therefore conclude that $\mathfrak{s}' \subseteq \mathfrak{s}$ must be Galois-invariant, and furthermore if $\mathfrak{s}$ contains no Galois-invariant subclusters, then $\gamma_{\mathfrak{s}} \in X_{\mathfrak{s}}$.

Lemma 3.4.4. *Suppose that the residue field of K is algebraically closed and that the roots of $F(x)$ are tamely ramified. Let $\mathfrak{s}$ be a Galois-invariant cluster. Then $c_{\mathfrak{s}} \in \mathbb{Z}$.*

Proof. Note that we can apply a rational change of coordinates: if $\gamma \in K$, consider $F(x+\gamma)$. The set $\mathfrak{s}_\gamma = \{\alpha - \gamma \mid \alpha \in \mathfrak{s}\}$ is a Galois-invariant cluster for $F(x+\gamma)$ and $c_{\mathfrak{s}_\gamma} = c_{\mathfrak{s}}$. By Lemma 3.4.2, we can assume that there exists $\alpha_{\min}$ such that $\mathfrak{s} = \{\alpha \mid \nu(\alpha) \geq \nu(\alpha_{\min})\}$.

As $\nu(a_d) \in \mathbb{Z}$, we must show that $\sum_{\beta \in \mathfrak{s}^c} \nu(\alpha_{\min} - \beta) \in \mathbb{Z}$. Both $\mathfrak{s}$ and the set of roots $\{\alpha_i\}$ are Galois invariant, so $\mathfrak{s}^c$ is as well. For each Galois orbit contained in $\mathfrak{s}^c$, pick some

representative η with minimal polynomial f_η, and let $\mathcal{M} \subseteq \mathfrak{s}^c$ be the set of all η. The sum $\sum_{\beta \in \mathfrak{s}^c} \nu(\alpha_{\min} - \beta)$ equals $\sum_{\eta \in \mathcal{M}} \nu(f_\eta(\alpha_{\min}))$. We show that for all $\eta \in \mathcal{M}$, $\nu(f_\eta(\alpha_{\min})) \in \mathbb{Z}$.

For all $\beta \in \mathfrak{s}^c$, $\nu(\beta) < \nu(\alpha_{\min})$, specifically, we have that for all $\eta \in \mathcal{M}$, $\nu(\eta) < \nu(\alpha_{\min})$. As f_η is irreducible, all roots have the same valuation. Thus, by the strong triangle inequality,

$$\begin{aligned}\nu(f_\eta(\alpha_{\min})) &= \nu\left(\prod_{\beta | f_\eta(\beta)=0} (\alpha_{\min} - \beta)\right) \\ &= \sum_{\beta | f_\eta(\beta)=0} \nu(\alpha_{\min} - \beta) = \sum_{\beta | f_\eta(\beta)=0} \nu(\beta) = (\deg f_\eta) \cdot \nu(\eta).\end{aligned}$$

As f_η is the minimal polynomial of η, a Newton polygon argument shows that the denominator of $\nu(\eta)$ divides $\deg f_\eta$, and hence $\nu(f_\eta(\alpha_{\min})) \in \mathbb{Z}$ as desired. □

Remark 3.4.5. Neither Lemma 3.4.2 nor Lemma 3.4.4 necessarily hold if the roots of $F(x)$ are wildly ramified. Consider $F(x) = (x^3 - 3)(x^2 - 3)$ over $\mathbb{Q}_3$. Let $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ be a root of the second cyclotomic polynomial, $x^2 + x + 1$, so that the roots of $F(x)$ are $\{\sqrt{3}, -\sqrt{3}, \sqrt[3]{3}, \zeta_3\sqrt[3]{3}, \zeta_3^2\sqrt[3]{3}\}$, and let $\mathfrak{s} = \{\sqrt[3]{3}, \zeta_3\sqrt[3]{3}, \zeta_3^2\sqrt[3]{3}\}$. As $\mathfrak{s} = B_{|\sqrt[3]{3}|}(\sqrt[3]{3}) \cap \{\alpha_i\}$, $\mathfrak{s}$ is a Galois-invariant cluster. For all $\gamma \in K$, either $\nu(\gamma) \geq 1$, in which case $\nu(\alpha - \gamma) = \nu(\alpha)$ for all α, or $\nu(\gamma) \leq 0$, in which case $\nu(\alpha - \gamma) = \nu(\gamma)$ for all α. Therefore, no γ can satisfy the conclusions of Lemma 3.4.2 for $\mathfrak{s}$. Further,

$$c_{\mathfrak{s}} = \nu(1) + \nu\left(\sqrt[3]{3} - \sqrt{3}\right) + \nu\left(\sqrt[3]{3} + \sqrt{3}\right) = \frac{2}{3}.$$

Remark 3.4.6. The proof of Lemma 3.4.4 shows that if there exists $\alpha_{\min} \in \mathfrak{s}$ such that $\mathfrak{s} = \{\alpha \mid \nu(\alpha) \geq \nu(\alpha_{\min})\}$, then $c_{\mathfrak{s}}$ is an integer.

3.5 Degree sets of superelliptic curves

We study the degree set of a superelliptic curve C/K via the affine open $U \subseteq C$ such that $U \simeq V(y^q - F(x)) \smallsetminus \{(\alpha_i, 0)\}$. We consider the x-coordinate map $x \colon C \to \mathbb{P}^1$.

3.5.1 Obstructing points of arbitrary degree

We first use the valuation to show that under certain modular arithmetic conditions, we cannot obtain points of arbitrary degree.

Lemma 3.5.1. *Suppose that the residue field of K is algebraically closed and that every root of $F(x)$ is tamely ramified. Fix a Galois-invariant cluster $\mathfrak{s}$. Let $\gamma_{\mathfrak{s}}$ be constructed from $\mathfrak{s}$ as in Lemma 3.4.2. Let r be a natural number not divisible by q. If there exists $P \in U(\overline{K})$ of degree r with $x(P) \in X_{\mathfrak{s}}$, then one of the following holds:*

(i) $|\mathfrak{s}| \not\equiv 0 \pmod{q}$, *or*

(ii) $|\mathfrak{s}| \equiv 0 \pmod{q}$ *and* $c_{\mathfrak{s}} \equiv 0 \pmod{q}$, *or*

(iii) $0 \in X_{\mathfrak{s}}$ *and* $\nu(F(0)) \equiv 0 \pmod{q}$, *or*

(iv) $\gamma_{\mathfrak{s}} \in X_{\mathfrak{s}}$ *and* $\nu(F(\gamma_{\mathfrak{s}})) \equiv 0 \pmod{q}$.

Remark 3.5.2. The quantities appearing in conditions *(i)* and *(ii)* in Lemma 3.5.1 are the coefficients appearing in the slope formula, see Remark 3.3.5.

Proof of Lemma 3.5.1. Let $(x_0, y_0) \in U(\overline{K})$ with $[K(x_0, y_0) : K] = r$. By Lemma 3.2.1, either $K(x_0, y_0)$ is a degree q extension of $K(x_0)$, or $F(x_0) \in K(x_0)^{\times q}$. The first case is not possible by assumption, so we must have that $F(x_0) \in K(x_0)^{\times q}$ and that $K(x_0, y_0) = K(x_0)$. As the residue field of K is algebraically closed, $K(x_0)$ is totally ramified with value group $\frac{1}{r}\mathbb{Z}$, so that $\nu(F(x_0))$ is a multiple of q in $\frac{1}{r}\mathbb{Z}$. As $x_0 \in X_{\mathfrak{s}}$, by Lemma 3.3.4, for any $\alpha \in \mathfrak{s}$,

$$\frac{\nu(F(x_0))}{q} = \frac{|\mathfrak{s}|}{q}\,\nu(x_0 - \alpha) + \frac{c_{\mathfrak{s}}}{q}.$$

We consider the possibilities for $\nu(x_0 - \alpha)$, which by strong triangle inequality, are as follows:

1. $\nu(x_0 - \alpha) = \nu(x_0) \leq v(\alpha)$

2. $\nu(x_0 - \alpha) = \nu(\alpha) < \nu(x_0)$

3. $\nu(x_0 - \alpha) > \nu(\alpha) = \nu(x_0)$.

Case 1: First suppose that $\nu(x_0 - \alpha) = \nu(x_0)$. Then, as $\frac{\nu(F(x_0))}{q} \in \frac{1}{r}\mathbb{Z}$, we have that the map $\frac{1}{r}\mathbb{Z} \to \frac{1}{r}\mathbb{Z}$ given by $x \mapsto \frac{|\mathfrak{s}|}{q}x + \frac{c_\mathfrak{s}}{q}$ satisfies the conditions of Lemma 3.2.2, so that $|\mathfrak{s}| \not\equiv 0 \pmod{q}$ or $|\mathfrak{s}| \equiv 0 \pmod{q}$ and $c_\mathfrak{s} \equiv 0 \pmod{q}$.

Case 2: Now assume that $\nu(x_0 - \alpha) = \nu(\alpha)$ and $\nu(x_0) > \nu(\alpha)$. As case (b) of Lemma 3.4.1 does not hold, case (a) must hold, so there exists $\alpha_{\min}$ such that $\mathfrak{s} = \{\alpha' \mid \nu(\alpha') \geq \nu(\alpha_{\min})\}$. As $\nu(x_0 - \alpha)$ is independent of the choice of $\alpha \in \mathfrak{s}$, all roots of $\mathfrak{s}$ must have the same valuation, which further must be the maximal valuation among all roots of $F(x)$. Thus, for any root α' of $F(x)$, $\nu(x_0) > \nu(\alpha')$. We see that $0 \in X_\mathfrak{s}$ as 0 is closest to the roots of maximal valuation, so

$$\nu(F(x_0)) = \nu(a_d) + \sum_i \nu(x_0 - \alpha_i) = \nu(a_d) + \sum_i \nu(\alpha_i) = \nu(F(0)).$$

Thus, $\nu(F(x_0)) \in \mathbb{Z}$. As $\nu(F(x_0))$ is a multiple of q in $\frac{1}{r}\mathbb{Z}$ and q does not divide r, $\nu(F(x_0)) = \nu(F(0)) = \nu(F(\gamma_\mathfrak{s}))$ is a multiple of q in $\mathbb{Z}$.

Case 3: Finally, suppose that $\nu(x_0 - \alpha) > \nu(\alpha) = \nu(x_0)$. By Lemma 3.4.2, there exists $\gamma_\mathfrak{s} \in K$ and $\alpha_{\min} \in \mathfrak{s}$ such that $\mathfrak{s} = \{\alpha \mid \nu(\alpha - \gamma_\mathfrak{s}) \geq \nu(\alpha_{\min} - \gamma_\mathfrak{s})\}$. Let $G(x) = F(x + \gamma_\mathfrak{s})$, consider the isomorphic curve $y^q = G(x)$, and let $\mathfrak{s}'$ be the $G(x)$-cluster $\{\alpha - \gamma_S \mid \alpha \in \mathfrak{s}\}$.

We show that for all $\alpha \in \mathfrak{s}$, $x_0 - \gamma_\mathfrak{s}$ is not contained in $B_{|\alpha - \gamma_\mathfrak{s}|}(\alpha - \gamma_\mathfrak{s})$. If $|\mathfrak{s}| = 1$, then $\gamma_\mathfrak{s} = \alpha$ and as $P \in U(\overline{K})$, $x(P)$ does not equal α, and hence $x_0 - \gamma_\mathfrak{s} \notin B_0(0)$. Now suppose that $|\mathfrak{s}| > 1$, and let $\alpha' \in \mathfrak{s}$ be such that $|\alpha - \alpha'|$ is maximal as in the proof of Lemma 3.4.2. By construction of $\gamma_\mathfrak{s}$, $|\alpha - \gamma_\mathfrak{s}| = |\alpha - \alpha'|$. As $x_0 \in X_\mathfrak{s}$, we have that

$$\begin{aligned} |x_0 - \gamma_\mathfrak{s} - (\alpha - \gamma_\mathfrak{s})| = |x_0 - \alpha| &= |x_0 - \alpha' + \alpha' - \alpha| \\ &\leq \max\{|x_0 - \alpha'|, |\alpha' - \alpha|\} = \max\{|x_0 - \alpha|, |\alpha - \gamma_\mathfrak{s}|\}. \end{aligned}$$

If $|\alpha - \gamma_\mathfrak{s}| > |x_0 - \alpha|$, then the strong inequality gives a contradiction. Thus, $|\alpha - \gamma_\mathfrak{s}| \leq |x_0 - \alpha|$, and hence $x_0 - \gamma_\mathfrak{s} \notin B_{|\alpha - \gamma_\mathfrak{s}|}(\alpha - \gamma_\mathfrak{s})$ as desired. Then, $\nu((x_0 - \gamma_\mathfrak{s}) - (\alpha - \gamma_\mathfrak{s})) \leq \nu(\alpha - \gamma_\mathfrak{s})$, and hence $x_0 - \gamma_\mathfrak{s}$ must fall in either case 1 or case 2 when considering the $G(x)$-cluster $\mathfrak{s}'$.

As $|\mathfrak{s}'| = |\mathfrak{s}|$ and $c_{\mathfrak{s}'} = c_{\mathfrak{s}}$, in case 1 the congruence conditions hold. Finally, $G(0) = F(\gamma_{\mathfrak{s}})$, and thus in case 2 we have that $\nu(F(\gamma_{\mathfrak{s}})) \in q\mathbb{Z}$. □

Remark 3.5.3. If $\gamma_{\mathfrak{s}} \neq 0$, for all $\alpha \in \mathfrak{s}$, $v(\alpha) = v(\gamma_{\mathfrak{s}})$. If there exist $\alpha, \alpha' \in \mathfrak{s}$ such that $\nu(\alpha_j) \neq \nu(\alpha_{j'})$, then $\gamma_{\mathfrak{s}} = 0$. Thus, for many Galois-invariant $\mathfrak{s}$, $\gamma_{\mathfrak{s}}$ is not contained in $X_{\mathfrak{s}}$.

Remark 3.5.4. Define the **depth** of $\mathfrak{s}$ by $d_{\mathfrak{s}} \coloneqq \min_{\alpha,\alpha'} \nu(\alpha - \alpha')$. When $|\mathfrak{s}| > 1$ and $\gamma_{\mathfrak{s}} \in X_{\mathfrak{s}}$, we have that $\nu(\gamma_{\mathfrak{s}} - \alpha_j) = d_{\mathfrak{s}}$, and hence $\nu(F(\gamma_{\mathfrak{s}})) = |\mathfrak{s}|d_{\mathfrak{s}} + c_{\mathfrak{s}}$.

3.5.2 Constructing points of large degree

We prove a strengthening of the converse of Lemma 3.5.1. Using Hensel's lemma, we show that if there exists a point $P \in U(\overline{K})$ with degree not a multiple of q, then the degree set contains points of all sufficiently large degrees.

Lemma 3.5.5. *Suppose that the residue field of K is algebraically closed and that every root of $F(x)$ is tamely ramified. Fix a Galois-invariant cluster $\mathfrak{s}$. If one of the following holds:*

(i) $|\mathfrak{s}| \not\equiv 0 \pmod{q}$, *or*

(ii) $|\mathfrak{s}| \equiv 0 \pmod{q}$ *and* $c_{\mathfrak{s}} \equiv 0 \pmod{q}$, *or*

(iii) $0 \in X_{\mathfrak{s}}$ *and* $\nu(F(0)) \equiv 0 \pmod{q}$, *or*

(iv) $\gamma_{\mathfrak{s}} \in X_{\mathfrak{s}}$ *and* $\nu(F(\gamma_{\mathfrak{s}})) \equiv 0 \pmod{q}$,

then there exists $r_0 \in \mathbb{N}$ such that for all $r \geq r_0$ with $\gcd(r, q) = 1$, there exists a point $P \in U(\overline{K})$ of degree r with $x(P) \in X_{\mathfrak{s}}$.

Proof. Following the argument in the proof of case 3 of Lemma 3.5.1, without loss of generality we can take $\gamma_{\mathfrak{s}} = 0$, so condition *(iv)* reduces to condition *(iii)*. Suppose that condition *(iii)* holds, so that $0 \in X_{\mathfrak{s}}$ and hence $\mathfrak{s}$ is the set of roots of maximal valuation. We let $r_0 = 1$

and construct points of all degrees $r \geq r_0$. Let N be an integer greater than $\max\{\nu(\alpha)\}$, and let $x_0 = \pi^{N+\frac{1}{r}}$. By construction, $x_0 \in X_{\mathfrak{s}}$, and hence by Lemma 3.3.4, for any $\alpha \in \mathfrak{s}$,

$$\nu(F(x_0)) = |\mathfrak{s}|\,\nu(x_0 - \alpha) + c_{\mathfrak{s}} = |\mathfrak{s}|\,\nu(\alpha) + c_{\mathfrak{s}} = \nu(F(0)) \equiv 0 \pmod{q}.$$

Thus, $(x_0, \sqrt[q]{F(x_0)})$ is a $\overline{K}$-point of degree r over K.

Now suppose that either condition (*i*) or condition (*ii*) holds. As $\gamma_{\mathfrak{s}} = 0$, by Lemma 3.4.2, there exists $\alpha_{\min}$ such that $\mathfrak{s}$ indexes the set $\{\alpha \mid \nu(\alpha) \geq \nu(\alpha_{\min})\}$. Let $N = \nu(\alpha_{\min})$ and let $M = \max_{\beta \in \mathfrak{s}^c}\{\nu(\beta)\}$. Let r_0 be the smallest integer greater than $\frac{q+1}{N-M} + 1$. We construct a point of degree r for all $r \geq r_0$. Consider the affine map $\rho\colon (M, N) \cap \frac{1}{r}\mathbb{Z} \to \frac{1}{rq}\mathbb{Z}$ given by $\rho(x) = \frac{|\mathfrak{s}|}{q}x + \frac{c_{\mathfrak{s}}}{q}$. By Lemma 3.2.2, there exists $\frac{a}{r} \in (M, N)$ such that $\rho\left(\frac{a}{r}\right) \in \frac{1}{r}\mathbb{Z}$. Write $\frac{a}{r} = \frac{su}{st}$ with $\gcd(u, t) = 1$, and let x_0' be a root of $x^t - \pi^u$, so that x_0' has degree t. Let τ be a uniformizer for $K(x_0')$ and let R be an integer larger than $s \cdot \frac{u}{t}$ relatively prime to s. Let ε be a root of $x^s - \tau^R$. A Newton polygon argument shows that the degree of ε over $K(x_0')$ is s and that $\nu(\varepsilon) = \frac{R}{s} > \nu(x_0')$. Let $x_0 = x_0' + \varepsilon$, so that $K(x_0)$ has degree $st = r$ over K, and $\nu(x_0) = \nu(x_0') = \frac{a}{r}$. As $M < \nu(x_0) < N$, $x_0 \in X_{\mathfrak{s}}$, and further

$$\frac{\nu(F(x_0))}{q} = \frac{|\mathfrak{s}|}{q}\,\nu(x_0 - \alpha) + \frac{c_{\mathfrak{s}}}{q} = \frac{|\mathfrak{s}|}{q}\,\nu(x_0) + \frac{c_{\mathfrak{s}}}{q} = \rho\left(\frac{a}{r}\right) \in \frac{1}{r}\mathbb{Z}.$$

Thus, $\nu(F(x_0))$ is a multiple of q in $\frac{1}{r}\mathbb{Z}$, and hence $(x_0, \sqrt[q]{F(x_0)})$ has degree r over K. □

Lemma 3.5.6. *The degree set $\mathcal{D}(C/K)$ contains $q\mathbb{N}$.*

Proof. We show that either $1 \in \mathcal{D}(C/K)$ (and hence equals $\mathbb{N}$) or that $q \in \mathcal{D}(C/K)$, which is sufficient by Lemma 3.2.5. Set $x = 0$ and consider $y^q = F(0)$. By Lemma 3.2.1, either $y^q - F(0)$ is irreducible, or there exists $b \in K$ such that $b^q = F(0)$. If $y^q - F(0)$ is irreducible, $(0, F(0)^{1/q})$ has degree q, otherwise, the point $(0, b)$ has degree 1. □

Lemma 3.5.7. *Suppose F has a separable irreducible factor of degree r. Then, $r\mathbb{N} \subseteq \mathcal{D}(C/K)$.*

Proof. Let α be a separable root of degree r and let ℓ be the multiplicity of α as a root of $F(x)$. Since F is assumed to be free of q-th powers, let i be a lift of $\ell^{-1} \pmod{q}$. Consider

the isomorphic curve given by $y^q = (F(x))^i$. After eliminating q-th powers from $(F(x))^i$, the resulting isomorphic curve is smooth at $(\alpha, 0)$, showing that $\mathcal{D}(C/K)$ contains $\deg \alpha$. □

3.6 Proofs of main theorems

Proof of Theorem 3.1.1. By Lemma 3.2.6, $\mathcal{D}(C/K) = \mathcal{D}(U/K)$. Let $P \in U(\overline{K})$ and consider $x(P)$. As the collection $\{X_{\mathfrak{s}}\}$ covers $\mathbb{A}^1(\overline{K})$, there exists some $\mathfrak{s}$ such that $x(P) \in X_{\mathfrak{s}}$. If $\mathfrak{s}$ is Galois invariant, then Lemma 3.5.1 shows that either q divides the degree of $x(P)$, or that one of the conditions (*i*)-(*iv*) holds. By Lemma 3.5.5, if one of the conditions (*i*)-(*iv*) hold, then the degree set contains $\mathbb{N}_{\geq r_0}$ and is cofinite. Thus, $\mathcal{D}(C/K)$ is not cofinite if and only if the conditions (*i*)-(*iv*) do not hold. If $\mathfrak{s}$ is not Galois invariant, the degree of $x(P)$ is a multiple of $|\mathcal{O}(\mathfrak{s})|$, and $\deg_K(P)$ is a multiple of the degree of $x(P)$, so that $\deg_K(P) \in |\mathcal{O}(\mathfrak{s})|\mathbb{N}$. □

Theorem 3.6.1. *Let D be a positive integer divisible q, and let $\{n_k\} \subseteq \mathbb{N}$ be a finite sequence such that $q\left(\sum_k n_k\right) = D$. Suppose that q is odd, or that the number of times 1 occurs in the sequence $\{n_k\}$ is even. Then, there exists a superelliptic curve C/K with equation $y^q = F(x)$, where $D = \deg F(x)$, such that*

$$\mathcal{D}(C/K) = q\mathbb{N} \cup \bigcup_{n_k > 1} n_k\mathbb{N}.$$

The added condition when q is even is necessary, as when the residue field of K is algebraically closed, [CV25, Lemma 5.8] shows that there does not exist a curve $y^2 = F(x)$ such that $\mathcal{D}(C/K) = 2\mathbb{N}$ with $\deg F(x) \equiv 2 \pmod 4$.

Proof. We begin with the case where q is odd. Define $m_k = \{n_k \mid n_k > 1\}$, and reorder so that both n_k and m_k are weakly increasing. We construct a superelliptic curve C/K with equation $y^q = F(x)$ such that

$$\mathcal{D}(C/K) = q\mathbb{N} \cup \bigcup_{n_k > 1} n_k\mathbb{N} = q\mathbb{N} \cup \bigcup_{k} m_k\mathbb{N}.$$

Define $c \coloneqq D - q\sum_k m_k$ and let a be relatively prime to c, congruent to 1 (mod q), and less than $-c$. As D is a multiple of q, so is c. Define $F(x)$ by

$$F(x) \coloneqq \pi(x^c - \pi^a) \prod_{n_k>1} \prod_{i=1}^{q} (x^{n_k} - \pi) \tag{3.2}$$

and consider the curve C/K defined by $y^q = F(x)$. By Lemma 3.5.6 and Lemma 3.5.7, we have that $q\mathbb{N} \cup \bigcup_{n_k>1} n_k\mathbb{N} \subseteq \mathcal{D}(C/K)$. We show that $\mathcal{D}(C/K) \subseteq q\mathbb{N} \cup \bigcup_{n_k>1} n_k\mathbb{N}$. Let $P \in U(\overline{K})$ and let $\mathfrak{s}$ be such that $x(P) \in X_{\mathfrak{s}}$. By Lemma 3.4.1, $X_{\mathfrak{s}} \subseteq B_{|\alpha|}(\alpha)$ or there exists $\alpha_{\min}$ such that $\mathfrak{s}$ indexes the set $\{\alpha \mid \nu(\alpha) \geq \nu(\alpha_{\min})\}$.

Consider the first case. By construction, the roots of $F(x)$ have valuations $\frac{a}{c}$ or $\frac{1}{n_k}$, and as $x(P) \in B_{|\alpha|}(\alpha)$, $\nu(x(P)) = \frac{a}{c}$ or $\nu(x(P)) = \frac{1}{n_k}$. Let d denote the denominator of $\nu(x(P))$. We have a chain of divisibility conditions: d divides $[K(x(P)) : K]$, which divides $[K(P) : K]$, and as $d = n_k$ or $q \mid c = d$, $[K(P) : K] \in q\mathbb{N} \cup \bigcup_k n_k\mathbb{N}$.

In the second case, there exists $\alpha_{\min}$ such that $\mathfrak{s}$ indexes the set $\{\alpha \mid \nu(\alpha) \geq \nu(\alpha_{\min})\}$. We see that $\mathfrak{s}$ is Galois invariant. Note that $F(x)$ may have wildly ramified roots, so that the assumptions of Lemma 3.5.1 fail. For this specific $\mathfrak{s}$, however, all $P \in U(\overline{K})$ fall into case 1 or case 2, and the proof proceeds as written provided we verify the conclusion of Lemma 3.4.4 (that $c_{\mathfrak{s}}$ is an integer). Let k_0 be the largest index such that $\frac{1}{m_{k_0}} < \nu(\alpha_{\min})$. We compute

$$\begin{aligned} c_{\mathfrak{s}} &= \nu(\pi) + \sum_{\beta \in \mathfrak{s}^c} \nu(\alpha_{\min} - \beta) = 1 + \sum_{\beta \in \mathfrak{s}^c} \nu(\beta) \\ &= 1 + c\left(\frac{a}{c}\right) + qm_1\left(\frac{1}{m_1}\right) + \ldots + qm_{k_0}\left(\frac{1}{m_{k_0}}\right) \in \mathbb{Z}. \end{aligned}$$

As $a \equiv 1 \pmod q$, $c_{\mathfrak{s}} \equiv 2 \pmod q$, and as $q \geq 3$, $c_{\mathfrak{s}} \not\equiv 0 \pmod q$. We compute $|\mathfrak{s}|$. The roots of $F(x)$ have valuations $\frac{a}{c} < \frac{1}{m_1} \leq \frac{1}{m_2} \leq \cdots$. The number of roots of each valuation is a multiple of q, and thus the number of roots α such that $\nu(\alpha_{\min}) \leq \nu(\alpha)$ is a multiple of q. Thus, $|\mathfrak{s}| \equiv 0 \pmod q$. Finally, we check that $\nu(F(0)) \not\equiv 0 \pmod q$, which is necessary for case 2. Let k_1 be the largest index in the sequence $\{m_k\}$. By construction, $\nu(F(0)) = \nu(\pi^{a+1}\pi^{qk_1}) \equiv a + 1 \pmod q$ and as before, $1 + a \not\equiv 0 \pmod q$. As $|\mathfrak{s}| \equiv 0 \pmod q$, $c_{\mathfrak{s}} \not\equiv 0 \pmod q$, and $\nu(F(0)) \not\equiv 0 \pmod q$, we conclude that for all $P \in U(\overline{K})$ such that $x(P) \in X_{\mathfrak{s}}$, $q \mid \deg P$, as in (the contrapositive of) Lemma 3.5.1.

When q is 2, we construct $F(x)$ as in Equation (3.2), with slight modifications. Note that $c_{\mathfrak{s}} \equiv 1 + a \pmod 2$, and thus if we want $2 \nmid c_{\mathfrak{s}}$, we must have $a \equiv 0 \pmod 2$. Thus, choose a such that $a \equiv 2 \pmod 4$ and is smaller than $-cn_k$ for all k. Then, as

$$c = D - 2\sum_{n_k>1} n_k = 2\sum_{n_k=1} n_k$$

and the number of k such that $n_k = 1$ is even by assumption, $c \equiv 0 \pmod 4$, so that $\frac{a}{c}$ (in lowest terms) has even denominator. The rest of the proof is similar to when q is odd. □

Proof of Theorem 3.1.2. If there exists k such that $n_k = 1$, pick a curve C/K with a rational point. Otherwise, the proof is immediate from Theorem 3.6.1. □

3.7 Examples

Our results also provide a method for computing degree sets. Although our lemmas assume algebraically closed residue field, this example is computed over $\mathbb{Q}_7$, as the points constructed of minimal degree (i.e., do not arise from having degree a multiple of a degree already in the degree set) are totally ramified, so the degree set is unchanged over $\mathbb{Q}_7^{\text{unr}}$.

Example 3.7.1. Let $\alpha = 7^{\frac{1}{2}} + 7^{\frac{3}{5}}$, $\beta = 2 \cdot 7^{\frac{1}{2}} + 7^{\frac{3}{5}}$, and $\gamma = 3 \cdot 7^{\frac{1}{2}} + 7^{\frac{3}{5}}$ as elements of $\overline{\mathbb{Q}_7}$, and let $f_1(x)$, $f_2(x)$, and $f_3(x)$ be the minimal polynomials of α, β, and γ respectively over $\mathbb{Q}_7$. Let $F(x) = 7f_1(x)f_2(x)f_3(x)$, and let $C/\mathbb{Q}_7$ be the curve given by $y^3 = F(x)$. Then, we have

$$\mathcal{D}(C/\mathbb{Q}_7) = 3\mathbb{N} \cup 2\left(\{8, 11, 13, 14\} \cup \mathbb{N}_{>15}\right) \cup 10\mathbb{N} \subseteq 3\mathbb{N} \cup 2\mathbb{N}.$$

Proof. Fix a primitive 5th root of unity ζ_5 and let $\mathfrak{s}$ be a cluster for $F(x)$. By Lemma 3.4.1, all roots of $\mathfrak{s}$ are contained in $B_{|\alpha|}(\alpha)$, or there exists $\alpha_{\min}$ such that $\mathfrak{s} = \{\alpha \mid \nu(\alpha) \geq \nu(\alpha_{\min})\}$.

We first consider the case where there exists $\alpha_{\min}$ such that $\mathfrak{s} = \{\alpha \mid \nu(\alpha) \geq \nu(\alpha_{\min})\}$. As all roots of $F(x)$ have the same valuation, $\mathfrak{s}$ must contain all roots of $F(x)$. Then, $|\mathfrak{s}| = 30$ and $c_{\mathfrak{s}} = 1$, and hence we have that

$$\nu(y(P)) = \frac{30}{3}\nu(x(P) - \alpha) + \frac{1}{3}$$

so that by Lemma 3.2.2, 3 divides the denominator of $\nu(y(P))$, and hence $\deg P \in 3\mathbb{N}$. Thus, we can suppose that all roots of $\mathfrak{s}$ are contained in $B_{|\alpha|}(\alpha)$. Each $B_{|\alpha|}(\alpha)$ contains exactly 5 roots of $F(x)$, and as all roots in $B_{|\alpha|}(\alpha)$ are equidistant, either $|\mathfrak{s}| = 5$ or $|\mathfrak{s}| = 1$.

If $|\mathfrak{s}| = 1$, then there exists $\alpha \in \mathfrak{s}$ such that $x(P)$ is closer to α than all Galois conjugates of α, and Krasner's lemma implies that $10 \mid \deg x(P) \mid \deg P$, showing that $\deg P \in 10\mathbb{N}$. As the roots of $F(x)$ have degree 10, by Lemma 3.5.7, $\mathcal{D}(C/K)$ contains $10\mathbb{N}$.

Suppose $|\mathfrak{s}| = 5$. We detail only the case where $\mathfrak{s} = \{7^{\frac{1}{2}} + \zeta_5^i 7^{\frac{3}{5}}\}_{i=1}^5$, as the other cases are similar. We have that $c_{\mathfrak{s}} = \frac{27}{2}$. Fix $\alpha \in \mathfrak{s}$. By Lemma 3.4.1, we have that $X_{\mathfrak{s}} \subseteq B_{|\alpha|}(\alpha)$, and applying Lemma 3.2.3, we find that for all $\eta \in B_{|\alpha|}(\alpha)$, $K(7^{\frac{1}{2}}) \subseteq K(\eta)$, so that if $x(P) \in X_{\mathfrak{s}}$, then $K(7^{\frac{1}{2}}) \subseteq \mathbf{k}(x(P))$. We extend to $K(7^{\frac{1}{2}})$ and renormalize the valuation, remembering that we have divided the degree of our point by 2. Following Lemma 3.5.5 over $K(7^{\frac{1}{2}})$, we have that $\gamma_{\mathfrak{s}} = 7^{\frac{1}{2}}$ and $(M, N) = (1, \frac{6}{5})$. If $\nu(x(P) - \gamma_{\mathfrak{s}}) = \frac{a}{r}$, then

$$\nu(y(P)) = \frac{5}{3} \cdot \frac{a}{r} + \frac{27}{3} = \frac{5a + 27r}{3r}$$

and so 3 divides the denominator of $\nu(y(P))$ unless $5a+27r \equiv 0 \pmod 3$, which occurs if and only if $a \equiv 0 \pmod 3$. We search for $r \in \mathbb{N}$ that produce $\frac{a}{r} \in (1, \frac{6}{5})$ such that $a \equiv 0 \pmod 3$. For r large enough, by Lemma 3.2.2, this condition is always satisfied, and a computer finds the condition is satisfied for 8, 11, 13, 14, and all integers greater than 15. □

Remark 3.7.2. The code of [Dok21] applied to Example 3.7.1 gives the following diagram.

Note that this method is unable to fully compute the special fiber, and thus is insufficient for computing the degree set in this case. Using the main result of [CV25] and the fact that Example 3.7.1 will have the same degree set over $\mathbb{Q}_7^{\text{unr}}$, we see that every component of the special fiber must have multiplicity divisible by 2 or 3.

3.8 Degree sets and maps between curves

In this section, we describe a more general setting in which our ideas can be applied. For a point $P \in C(\overline{K})$, the complete Galois orbit of P is a closed point of C/K. We let $\mathbf{k}(P)$ denote the residue field of this closed point. We make the following observation:

Lemma 3.8.1. *Let X/K and Y/K be curves with a map $X \to Y$. Then, $\mathcal{D}(X/K) \subseteq \mathcal{D}(Y/K)$.*

Proof. Let $P \in X(\overline{K})$ be a point of degree d and let $Q \in Y(\overline{K})$ be the image of P. Let d' be the degree of Q. We have an inclusion of residue fields $\mathbf{k}(Q) \to \mathbf{k}(P)$, which shows that d' divides d. By Lemma 3.2.5, $\mathcal{D}(Y/K)$ contains all multiples of d', and hence contains d. □

A general curve X/K, however, has simple Jacobian, and hence admits no maps $X \to Y$ to a curve Y/K of positive genus. When Y/K has genus 0, $\mathcal{D}(Y/K)$ is either $\mathbb{N}$ or $2\mathbb{N}$. Hence, for a general curve X/K, Lemma 3.8.1 is not very helpful for studying $\mathcal{D}(X/K)$. We thus add structure by studying two maps simultaneously:

Lemma 3.8.2. *Let X/K, Y/K, and Z/K be curves with maps $\varphi : X \to Y$ and $\theta : X \to Z$. Let $P \in X(\overline{K})$. Then, $\operatorname{lcm}\{\deg_K \varphi(P), \deg_K \theta(P)\}$ divides the degree of P over K.*

Proof. We have inclusions of residue fields $\mathbf{k}(\varphi(P)) \to \mathbf{k}(P)$ and $\mathbf{k}(\theta(P)) \to \mathbf{k}(P)$. Thus, $\deg_K P$ is divisible by both $\deg_K \varphi(P)$ and $\deg_K \theta(P)$, and hence is divisible by the least common multiple. □

For a general curve X/K, both Y/K and Z/K must have genus 0. We therefore consider the case where both Y/K and Z/K are $\mathbb{P}^1_K$, and use the structure of $\overline{K}$ to study points on $\mathbb{P}^1_K$. This reduces to the analysis conducted in Section 3.6.

As K is a Henselian discretely valued field, we have a unique extension of the valuation to a map $\nu : \overline{K} \to \mathbb{Q} \cup \{\infty\}$. Thus, ν induces a Galois equivariant map $\nu : \mathbb{A}^1(\overline{K}) \to \mathbb{Q} \cup \{\infty\}$. Fix an affine open $W \subseteq X$ not including poles of φ and θ, so that $\varphi|_W$ and $\theta|_W$ map to $\mathbb{A}^1$. We study the degrees of points $P \in W(\overline{K})$ by studying their image under the compositions

$\nu \circ \varphi|_W$ and $\nu \circ \theta|_W$. By Lemma 3.2.6, $\mathcal{D}(W/K)$ equals $\mathcal{D}(X/K)$, and hence it suffices to only study points in W. Let denom $\left(\frac{a}{b}\right)$ denote the denominator of $\frac{a}{b}$ when written in lowest terms.

Lemma 3.8.3. *Let X/K be a curve with two maps $\varphi, \theta : X \to \mathbb{P}^1$, and let $W \subseteq X$ be an affine open away from the poles of φ and θ. Let $P \in W(\overline{K})$. Define*

$$\Delta_{P,\varphi,\theta} := \operatorname{lcm}\{\operatorname{denom}(\nu(\varphi(P))), \operatorname{denom}(\nu(\theta(P)))\}.$$

Then, $\Delta_{P,\varphi,\theta}$ divides the degree of P over K.

Proof. We first show that $\operatorname{denom}(\nu(\varphi(P)))$ divides $\deg_K \varphi(P)$. As $\varphi(P) \in \mathbb{A}^1(\overline{K})$, there exists some element $\gamma \in \overline{K}$ such that $\varphi(P)$ is the prime ideal $(x - \gamma)$. We have that $\mathbf{k}(\varphi(P)) = K(\gamma)$ and that $\nu(\varphi(P)) = \nu(\gamma)$. As $\nu(\gamma)$ is an element of the value group of $K(\gamma)$, the denominator of $\nu(\gamma)$ divides the ramification degree of $K(\gamma)/K$, which divides the degree of $K(\gamma)/K$, as desired.

The statement is symmetric in φ and θ, and thus $\operatorname{denom}(\nu(\theta(P))$ divides $\deg_K \theta(P)$. Hence, $\operatorname{denom}(\nu(\varphi(P))$ and $\operatorname{denom}(\nu(\theta(P))$ both divide $\operatorname{lcm}\{\deg_K \varphi(P), \deg_K \theta(P)\}$, and hence $\Delta_{P,\varphi,\theta}$ divides $\operatorname{lcm}\{\deg_K \varphi(P), \deg_K \theta(P)\}$ as well. Finally, Lemma 3.8.2 shows that $\Delta_{P,\varphi,\theta} \mid \operatorname{lcm}\{\deg_K \varphi(P), \deg_K \theta(P)\}$, which divides $\deg_K P$. □

Lemma 3.8.4. *Let X/K be a curve with two maps $\varphi, \theta \colon X \to \mathbb{P}^1$, and let $W \subseteq X$ be an affine open away from the poles of φ and θ. Suppose that there exists a finite set $\{r_1, \ldots, r_n\} \subseteq \mathbb{N}$ such that for all $P \in W(\overline{K})$, there exists r_i (depending on P) such that r_i divides $\Delta_{P,\varphi,\theta}$. Then,*

$$\mathcal{D}(X/K) \subseteq \bigcup_i r_i\mathbb{N}.$$

Proof. By Lemma 3.2.6, $\mathcal{D}(X/K) = \mathcal{D}(W/K)$, thus it suffices to bound $\mathcal{D}(W/K)$. For all $P \in W(\overline{K})$, $\Delta_{P,\varphi,\theta}$ divides $\deg_K P$ by Lemma 3.8.3, and thus by hypothesis there exists r_i such that r_i divides $\deg_K P$. Hence, $\deg_K P \in r_i\mathbb{N}$ and the result follows. □

Theorem 3.1.1 can be rephrased to show that if C/K is a superelliptic curve with equation $y^q = F(x)$ such that $F(x)$ has no roots of integer valuation, then in fact $\mathcal{D}(C/K)$ is cofinite if and only if there exists such a set $\{r_1, \ldots, r_n\}$.

In general, it is not resonable to expect one pair of maps to completely explain why the degree set is not cofinite. We can weaken the conditions on Lemma 3.8.4 by letting the pair of maps vary, and show that if C/K is a superelliptic curve with equation $y^q = F(x)$ and the roots of $F(x)$ are tamely ramified, then in fact $\mathcal{D}(C/K)$ is cofinite if and only if there exists a finite collection of maps (θ_i, φ_i) obstructing the degrees of points.

Lemma 3.8.5. *Let X/K be a curve with a finite set of pairs of maps $\{(\varphi_1, \theta_1), \ldots, (\varphi_m, \theta_m)\}$ to $\mathbb{P}^1$, and let $W \subseteq X$ be an affine open away from the poles of $\varphi_1, \theta_1, \ldots, \varphi_m, \theta_m$. Suppose there exists a finite set $\{r_1, \ldots, r_n\} \subseteq \mathbb{N}$ such that for all $P \in W(\overline{K})$, there exists i, j such that r_i divides $\Delta_{P,\varphi_j,\theta_j}$. Then,*

$$\mathcal{D}(X/K) \subseteq \bigcup_i r_i\mathbb{N}.$$

Proof. By Lemma 3.2.6, $\mathcal{D}(X/K) = \mathcal{D}(W/K)$, thus it suffices to bound $\mathcal{D}(W/K)$. By hypothesis, for all $P \in W$, there exists some pair of maps $\varphi_j : W \to \mathbb{P}^1$ and $\theta_j : W \to \mathbb{P}^1$ such that r_i divides $\Delta_{P,\varphi_j,\theta_j}$, and hence we can apply Lemma 3.8.3. The result follows. □

Chapter 4

THE HASSE PRINCIPLE FOR CONIC BUNDLES OVER EVEN DEGREE EXTENSIONS

This chapter represents the work of a collaboration with Sam Roven, available at [RW26]. In particular, many of the results on conic bundles were proven by Roven in his thesis; the extension of the results to general conic bundles, particularly in Lemma 4.2.4, Lemma 4.2.5, Lemma 4.2.6, case *(ii)* of Corollary 4.2.7, and Corollary 4.3.4, were done by the author.

4.1 Main results

Let $X \to \mathbb{P}^1_k$ be a smooth conic bundle over a global field k of characteristic not equal to 2. Over local and global fields, the arithmetic of such conic bundles has been well studied. By the Hasse-Minkowski theorem, conic bundles over $\mathbb{Q}$ with two geometric singular fibers always satisfy the Hasse principle and work of Iskovskikh shows that conic bundles over $\mathbb{Q}$ with three geometric singular fibers always have rational points [Isk96]. However, there exist conic bundles with 4 geometric singular fibers, specifically Châtelet surfaces, that fail the Hasse principle, see [Isk71] for the case over $\mathbb{Q}$ and [Poo09, §5] for a general construction over a number field.

Since conics have numerous quadratic points, for any conic bundle there are numerous quadratic extensions over which they gain global points. However, we show that a much stronger statement holds, namely that for a large class of conic bundles with 4 geometric singular fibers, the Hasse principle holds over **every** even degree extension. The main arithmetic idea in the proof dates back to work of Kanevsky [Kan87].

Theorem 4.1.1. *Let k be a number field, let $X \to \mathbb{P}^1_k$ be a conic bundle with four geometric singular fibers, and assume that either $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \neq 0$ or $X(\mathbb{A}_k) \neq \emptyset$. Then, if L/k is an even*

degree extension, we have

$$X(L) \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset.$$

For arbitrary conic bundles we do not have such unconditional results, however, we can extend our prior results to conic bundles with more geometric singular fibers at the expense of assuming Schinzel's hypothesis as well as restricting to quadratic extensions.

Theorem 4.1.2. *Let k be a number field and let $X \to \mathbb{P}^1_k$ be a conic bundle. Then, there exists an explicit finite set S of quadratic extensions of k such that for every quadratic extension $L/k \notin S$, we have*

$$X(\mathbb{A}_L)^{\mathrm{Br}} \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset.$$

In particular, if X has at most 5 geometric singular fibers, or assuming Schinzel's hypothesis, then X satisfies the Hasse principle over L.

The set S depends only on the closed points $P \in \mathbb{P}^1_k$ over which X has a singular fiber, together with the residues at such P of the generic fiber X_η considered as an element of $\mathrm{Br}(k(t))$.

The proofs of Theorem 4.1.1 and Theorem 4.1.2 consist of two steps. We first show that Brauer classes in the image of the restriction map $\mathrm{Res}_{L/k}\colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)}$ for even degree extensions L/k do not obstruct the existence of rational points. Then, we provide a characterization of when the restriction map is surjective (and therefore the Brauer–Manin set is nonempty) in terms of the singular fibers and the residues of the Brauer class corresponding to the generic fiber at these points. Combining work of Colliot-Thélène and Coray [CTC79], Colliot-Thélène, Sansuc, and Swinnerton-Dyer [CTSSD87], and Colliot-Thélène and Swinnerton-Dyer [CTSD94] show that the Brauer–Manin obstruction is the only obstruction to rational points for conic bundles with five or fewer geometric singular fibers, and if one assumes Schinzel's hypothesis, this can be extended to conic bundles with arbitrarily many geometric singular fibers, see Theorem 4.2.9.

In 2009, Pete Clark coined the notion of a potential Hasse principle failure for smooth, geometrically irreducible varieties over number fields. In particular, given such a variety V/k, we say that it is a *potential Hasse principle failure* (PHPF) if there exists an extension L/k such that V fails the Hasse principle over L. Clark showed the existence of infinitely many curves which were PHPFs. It was also conjectured that for any positive genus curve C/k with no k-rational points, C is a PHPF, see [Cla09, Theorem 1, Conjecture 4]. Theorem 4.1.1 shows that most conic bundles with four geometric singular fibers are not PHPFs, although there do exist cases where new Brauer classes can give a Brauer–Manin obstruction over L. If the conditions of Theorem 4.1.1 are not met, it is possible for there to exist a quadratic extension L/k, where the singular fibers of $X_L \to \mathbb{P}^1_L$ lie over two closed points of degree 2, over which the Hasse principle could possibly fail.

Theorem 4.1.3. *The Châtelet surface $X/\mathbb{Q}$ given by*

$$y^2 - 5z^2 = \frac{3}{5}(5t^4 + 7t^2 + 1)$$

has no $\mathbb{A}_\mathbb{Q}$ points, but fails the Hasse principle over $L = \mathbb{Q}(\sqrt{29})$, i.e. X is a potential Hasse principle failure.

Indeed, we show that for Châtelet surfaces, quadratic extensions not contained in the set S described by Theorem 4.1.2 are the only even degree extensions over which the Hasse principle can fail, and for general conic bundles with four singular fibers, there are only two possible types of behavior (see Corollary 4.3.2). In addition, we trace the failure of the Hasse principle to a parity condition on the number of ramification places of a conic that splits in a fixed quadratic extension (see Theorem 4.4.1).

4.2 Generalities on Brauer groups of conic bundles

4.2.1 Notation

Throughout this chapter, let k be a global field of characteristic not equal to 2. We say that $X \to \mathbb{P}^1_k$ is a conic bundle over $\mathbb{P}^1_k$ if X is smooth and geometrically integral over k and the

morphism to $\mathbb{P}^1_k$ is proper where the generic fiber is a smooth conic. We assume that X is minimal; that is, there does not exist a (-1)-curve on X which can be blown down.

Lemma 4.2.1. *Let k be a local field and let C/k be a smooth conic. If L/k is an even degree extension then $C(L) \neq \emptyset$.*

Proof. From local class field theory, the restriction map factors as

$$\mathrm{Res}_{L/k}\colon \mathrm{Br}\, k \cong \mathbb{Q}/\mathbb{Z} \xrightarrow{[L:k]} \mathbb{Q}/\mathbb{Z} \cong \mathrm{Br}\, L$$

Using the correspondence between smooth conics and quaternion algebras, we can apply this to any element of $\mathrm{Br}\, k[2]$ and obtain the result. □

4.2.2 The Brauer group of a conic bundle

After a change of coordinates, since k is infinite, we may assume that the fiber over the point at infinity, X_∞, is a smooth conic. Let S_k be the finite set of closed points in $\mathbb{A}^1_k$ with geometric singular fiber, where we will write $S = S_k$ when the ground field is unspecified, and let $|S|$ denote the number of such closed points, not counting degree, i.e. if X has four geometric singular fibers and $|S| = 1$, then S contains one closed point of degree 4.

For any point $P \in \mathbb{A}^1_k$, let $\mathbf{k}(P)$ denote its residue field. For $P \in S$, the fiber X_P degenerates to the union of two lines, ℓ_P and ℓ'_P, defined over $\mathbf{k}(P)(\sqrt{\alpha_P})$ for some $\alpha_P \in \mathbf{k}(P)^*$. Since X is assumed to be minimal, if $P \in S$ is a degree 1 point, then α_P cannot be a square in k, as both ℓ and ℓ' would be (-1)-curves defined over k. Note that the generic fiber of $X \to \mathbb{P}^1$ is a Severi-Brauer variety over $k(t)$ and therefore an element of $\mathrm{Br}(k(t))$, and α_P is the residue of this Brauer class at P. The group $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)}$ is then determined by $\mathbf{k}(P)$ and α_P for $P \in S$, as shown in the following lemma.

Lemma 4.2.2. [CTS21, Corollary 11.3.5] *Let $\pi\colon X \to \mathbb{P}^1_k$ be a conic bundle with singular fibers over $S \subseteq \mathbb{P}^1$. Let $V \subseteq \mathbb{F}_2^{|S|}$ be defined by*

$$V = \left\{ \varepsilon = (\varepsilon_P)_{P\in S} \in \mathbb{F}_2^{|S|} \;\middle|\; \prod_{P\in S} \mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P)^{\varepsilon_P} \in k^{\times 2} \right\}.$$

Then, $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)}$ *is isomorphic to* V *modulo the subspace generated by* $(1,\dots,1)$*. The vector* $\varepsilon \in V$ *corresponds to the image of* $\pi^*(A_\varepsilon) \in \mathrm{Br}(X)$*, defined by*

$$A_\varepsilon = \sum_{P\in S} \varepsilon_P \,\mathrm{Cor}_{\mathbf{k}(P)(t)/k(t)}\, \mathcal{A}_P$$

where $\mathcal{A}_P = (\alpha_P, t-\tau_P) \in \mathrm{Br}(\mathbf{k}(P)(t))$ *and* $\tau_P \in \mathbf{k}(P)$ *denotes the image of* t *in* $\mathbf{k}(P) = k[t]/P(t)$*.*

In particular, in order for this quotient to be well-defined, note that $\prod_{P\in S} \mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P) \in k^{\times 2}$ [Sko15, Lemma 2.2]. For a detailed explanation of this construction, see [CTS21, Section 11.3.1].

Corollary 4.2.3. *Let* $\pi\colon X \to \mathbb{P}^1_k$ *be a conic bundle. We have that* $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)}$ *is generated by images of elements of* $\ker(\mathrm{Br}(X)[2] \to \mathrm{Br}(X_\infty))$*.*

Proof. Use the notation of Lemma 4.2.2. For each $P \in S$, we have that $\mathcal{A}_P(\infty) = (1, a_P) = 0 \in \mathrm{Br}(\mathbf{k}(P))$. Since $\mathrm{Cor}_{\mathbf{k}(P)/k}$ is a group homomorphism, we have that each

$$A_\varepsilon \in \ker(\mathrm{Br}(\mathbf{k}(\mathbb{P}^1))[2] \xrightarrow{\infty^*} \mathrm{Br}(k)[2])$$

and so $\pi^*(A_\varepsilon) \in \ker(\mathrm{Br}(X)[2] \to \mathrm{Br}(X_\infty))$. □

Lemma 4.2.4. *Let* L/k *be a finite extension such that* $S_L = S_k$*. For every* $T \subseteq S$*, let* $\beta_T := \prod_{P\in T} \mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P)$*. If* $\beta_T \in k^{\times 2} \Leftrightarrow \beta_T \in L^{\times 2}$ *for all* $T \subseteq S$*, then the map* $\mathrm{Res}_{L/k}\colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)}$ *is an isomorphism.*

Proof. Using [CTS21, Proposition 11.3.4] on both k and L, we have the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Br}(k) & \longrightarrow & \mathrm{Br}(X) & \longrightarrow & \mathbb{F}_2^{|S_k|}/(1,\dots,1) & \longrightarrow & k^\times/k^{\times 2} \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Br}(L) & \longrightarrow & \mathrm{Br}(X_L) & \longrightarrow & \mathbb{F}_2^{|S_L|}/(1,\dots,1) & \longrightarrow & L^\times/L^{\times 2}
\end{array}$$

where the last horizontal map sends $\varepsilon \in \mathbb{F}_2^{|S_k|}/(1,\dots,1)$ to $\prod_{P\in S} \mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P)^{\varepsilon_P}$ and analogously for L, and the vertical maps are induced by $\mathrm{Res}_{L/k}$. In particular, we have that the

map $\mathbb{F}_2^{|S_k|}/(1,\dots,1) \to \mathbb{F}_2^{|S_L|}/(1,\dots,1)$ sends e_P, the basis vector corresponding to P, to the sum $e_{Q_1} + \cdots + e_{Q_n}$, where P splits into $Q_1, \dots, Q_n$ over L. The diagram above induces isomorphisms compatible with restriction

$$\begin{array}{ccc} \frac{\mathrm{Br}(X)}{\mathrm{Br}(k)} & \longrightarrow & \ker\left(\mathbb{F}_2^{|S_k|}/(1,\dots,1) \to k^\times/k^{\times 2}\right) \\ \downarrow & & \downarrow \\ \frac{\mathrm{Br}(X_L)}{\mathrm{Br}(L)} & \longrightarrow & \ker\left(\mathbb{F}_2^{|S_L|}/(1,\dots,1) \to L^\times/L^{\times 2}\right) \end{array}$$

where the vertical maps are given by $\mathrm{Res}_{L/k}$. Since $S = S_L$ and using the explicit description of the map above, the map $\mathbb{F}_2^{|S_k|}/(1,\dots,1) \to \mathbb{F}_2^{|S_L|}/(1,\dots,1)$ is an isomorphism. The condition on β_T precisely implies that the kernels will be equal, and therefore $\mathrm{Res}_{L/k}$ is an isomorphism as desired. □

Lemma 4.2.5. *Let k be a global field of characteristic not equal to 2 and let X/k be a minimal conic bundle with four geometric singular fibers. Then*

$$\frac{\mathrm{Br}(X)}{\mathrm{Br}(k)} \cong \begin{cases} (\mathbb{Z}/2\mathbb{Z})^2 & \text{if } |S| = 4 \text{ and } \alpha_P\alpha_Q \in k^{\times 2} \forall P, Q \in S, P \neq Q \\ (\mathbb{Z}/2\mathbb{Z}) & \text{one of the following three conditions hold} \\ 0 & \text{otherwise} \end{cases}$$

where the conditions are given by

(*i*) $|S| = 2$ *with* $P \in S$ *degree* 2 *and* $\mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P) \in k^{\times 2}$,

(*ii*) $|S| = 3$ *with* $P, Q \in S$ *degree* 1, *and* $\alpha_P\alpha_Q \in k^{\times 2}$,

(*iii*) $|S| = 4$ *with* $\#\{\alpha_P\alpha_Q \in k^{\times 2} \mid P, Q \in S \text{ and } P \neq Q\} = 2$.

Proof. Using the description of $\frac{\mathrm{Br}(X)}{\mathrm{Br}(k)}$ in Lemma 4.2.2, we proceed by cases on the size of S and degrees of points in S. If $|S| = 1$, then $V \cong \mathbb{F}_2$ giving a quotient of 0.

If $|S| = 2$ and contains P of degree 1 and Q of degree 3, in the quotient we can assume $\varepsilon_Q = 0$. The condition then reduces to $\alpha_P^{\varepsilon_P} \in k^{\times 2}$, and since α_P is assumed to not be a square, we must have $\varepsilon_P = 0$ and therefore $\frac{\mathrm{Br}(X)}{\mathrm{Br}(k)} = 0$.

If $|S| = 2$ and contains P, Q both of degree 2, then without loss of generality take $\varepsilon_Q = 0$. We must check if $\mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P)^{\varepsilon_P} \in k^{\times 2}$, and so if $\mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P) \in k^{\times 2}$ then $\varepsilon_P \in \mathbb{F}_2$, otherwise $\varepsilon_P = 0$.

If $|S| = 3$ containing P and Q of degree 1 and R of degree 2, then without loss of generality take $\varepsilon_R = 0$. We then need $\alpha_P^{\varepsilon_P}\alpha_Q^{\varepsilon_Q} \in k^{\times 2}$, and we know $\alpha_P, \alpha_Q \notin k^{\times 2}$. Thus if $\alpha_P\alpha_Q \in k^{\times 2}$ then $(\varepsilon_P, \varepsilon_Q) \in \{(0,0),(1,1)\}$, otherwise $(\varepsilon_P, \varepsilon_Q) = (0,0)$.

If $|S| = 4$, let $S = \{P_i\}_{i=1}^4$ with all $\deg(P_i) = 1$ and $\alpha_{P_i} \notin k^{\times 2}$. We consider the product $\alpha_{P_1}^{\varepsilon_1}\alpha_{P_2}^{\varepsilon_2}\alpha_{P_3}^{\varepsilon_3}\alpha_{P_4}^{\varepsilon_4}$ and note that since $\alpha_{P_1}\alpha_{P_2}\alpha_{P_3}\alpha_{P_4} \in k^{\times 2}$ but no individual $\alpha_{P_i} \in k^{\times 2}$, we cannot have any product of three be a square in k. It remains to consider how many pairs $\alpha_{P_i}\alpha_{P_j}$ for $i \neq j$ are squares in k, and we can check that there must be either 0, 2, or (all) 6 pairs which product to a square. If 0 products are squares, $\varepsilon \in \{(0,\dots,0),(1,\dots,1)\}$ and thus $\frac{\mathrm{Br}(X)}{\mathrm{Br}(k)} = 0$. If 2 products are squares, they must correspond to disjoint pairs $S = \{P_a, P_b\} \sqcup \{P_c, P_d\}$ with $\varepsilon_{P_a} = \varepsilon_{P_b}$ and $\varepsilon_{P_c} = \varepsilon_{P_d}$, and thus after taking the quotient we have $\frac{\mathrm{Br}(X)}{\mathrm{Br}(k)} = \mathbb{Z}/2\mathbb{Z}$. If all 6 products are squares, any ε with a sum congruent to 0 modulo 2 will produce a square, thus after taking the quotient we have $\frac{\mathrm{Br}(X)}{\mathrm{Br}(k)} = (\mathbb{Z}/2\mathbb{Z})^2$. □

In the case where X is a Châtelet surface, all α_{P_i} are equal, so $\frac{\mathrm{Br}(X)}{\mathrm{Br}(k)}$ is $(\mathbb{Z}/2\mathbb{Z})^2$ when $|S| = 4$, $(\mathbb{Z}/2\mathbb{Z})$ when S has at least one point of degree 2, and 0 otherwise.

Lemma 4.2.6. *Let k be a global field of characteristic not equal to 2 and let $X \to \mathbb{P}^1_k$ be a conic bundle with four geometric singular fibers. If $X(k) = \emptyset$ and $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \neq 0$, then $S = \{P_1, P_2\}$ with $\deg(P_i) = 2$ and $\mathrm{Nm}_{\mathbf{k}(P_i)/k}(\alpha_{P_i}) \in k^{\times 2}$ for $i \in \{1,2\}$, and $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} = \mathbb{Z}/2\mathbb{Z}$.*

Proof. This follows from Lemma 4.2.5, however we provide a direct proof. Using the description of $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)}$ in Lemma 4.2.2, we proceed by cases on the size of S and degrees of points in S. If $|S| = 1$, then $V \cong \mathbb{F}_2$ giving a quotient of 0, which violates our assumption that $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \neq 0$. If any of the singular fibers of X lie over a degree 1 point $P \in \mathbb{A}^1_k$, then we can obtain a k-rational point on X by taking the intersection point of the lines ℓ_P and ℓ'_P for such $P \in S$. Thus, if $|S| = 3$ or $|S| = 4$, then at least one $P \in S$ must be degree 1, violating the assumption that $X(k) = \emptyset$. Therefore, if $X(k) = \emptyset$ and $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \neq 0$, we must have $|S| = 2$

consisting of two points of degree 2. If either $\mathrm{Nm}_{\mathbf{k}(P_i)/k}(\alpha_{P_i}) \notin k^{\times 2}$, then $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} = 0$, so both must be non-squares in k. □

Corollary 4.2.7. *Let k be a global field of characteristic not equal to 2 and let $X \to \mathbb{P}^1_k$ be a conic bundle with four geometric singular fibers. If there exists an even degree extension L/k such that $X(L) = \emptyset$ and $\mathrm{Res}_{L/k}\colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)}$ is not surjective, then either*

(i) $|S_k| = 1$ and $|S_L| = 2$ with $P, Q \in S_L$ both degree 2 and interchanged by $\mathrm{Gal}(L/k)$, or

(ii) $|S_k| = |S_L| = 2$ with $P, Q \in S_L$ both degree 2 and fixed by $\mathrm{Gal}(L/k)$, with $\mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P) \notin k^{\times 2}$ and $\mathrm{Nm}_{L\cdot\mathbf{k}(P)/L}(\alpha_P) \in L^{\times 2}$ (equivalently for Q).

Furthermore, in both cases, we must have $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} = 0$.

Proof. Let L/k be an even degree extension such that $X(L) = \emptyset$ and $\mathrm{Res}_{L/k}\colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)}$ is not surjective. In particular, $\frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)} \neq 0$, so by Lemma 4.2.6, we must have that $S_L = \{P, Q\}$ both of degree 2, $\frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)} \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Nm}_{L\cdot\mathbf{k}(P)/L}(\alpha_P) \in L^{\times 2}$. Since S_L is the base change of S_k, either S_k consists of one point of degree 4 split into P and Q over L, which gives case (i). Otherwise, S_k consists of P and Q both degree 2 points over k. If $\mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P) \in k^{\times 2}$, the hypotheses of Lemma 4.2.4 would be satisfied, and thus the restriction map would be an isomorphism. We conclude that $\mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P) \notin k^{\times 2}$, which gives case (ii). Additionally, since $X(k) \subseteq X(L) = \emptyset$, the contrapositive of Lemma 4.2.6 shows that $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} = 0$. □

Remark 4.2.8. If X is a Châtelet surface given by the affine equation $y^2 - az^2 = f(x)$ for a quartic polynomial $f(x)$, then S is geometrically given by the roots of f over a splitting field, $\alpha_P = a$ for all $P \in S$, and the only possible case of Corollary 4.2.7 is (i).

The following theorem is a consequence of work of Colliot-Thélène and Coray, Colliot-Thélène and Swinnerton-Dyer, and Colliot-Thélène, Sansuc, and Swinnerton-Dyer, and is a critical ingredient in our results, as it implies that in order to prove the existence of rational points, it suffices to show that the Brauer–Manin set is nonempty.

Theorem 4.2.9. *Let X/k be a conic bundle with five or fewer geometric singular fibers. Then, $X(k) \neq \emptyset$ if and only if $X(\mathbb{A}_k)^{\mathrm{Br}(X_k)} \neq \emptyset$. Moreover, if one assumes Schinzel's hypothesis, the statement is true for conic bundles with arbitrarily many geometric singular fibers.*

Proof. For Châtelet surfaces, this is proven in [CTSSD87, Theorem B.i.a]. Now assume that X/k is a general a conic bundle with five or fewer geometric singular fibers. Any point of $X(\mathbb{A}_k)^{\mathrm{Br}(X_k)}$ is an adelic 0-cycle of degree 1 orthogonal to the Brauer group, and if there is no Brauer–Manin obstruction to the existence of a 0-cycle of degree 1, then there exists a 0-cycle of degree 1 [CTSD94, Theorem 5.1]. Then, $X(k) \neq \emptyset$ if and only if there exists a zero cycle of degree one over k [CTC79, Corollaire 4]. The case of arbitrarily many geometric singular fibers assuming Schinzel's hypothesis is proven in [CTSD94, Theorem 4.2]. □

4.3 Proofs of main theorems

Theorem 4.3.1. *Let k be a global field of characteristic not equal to 2 and let $X \to \mathbb{P}^1_k$ be a conic bundle with four geometric singular fibers. Then, for any even degree extension L/k*

$$X(\mathbb{A}_L)^{\mathrm{Res}_{L/k}(\mathrm{Br}(X_k))} \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset.$$

In particular, if $\mathrm{Res}_{L/k}\colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)}$ is surjective, then $X(\mathbb{A}_L)^{\mathrm{Br}(X_L)} \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset$.

Proof. We begin by observing that one direction is immediate since $X(\mathbb{A}_L) = \emptyset$ implies that $X(\mathbb{A}_L)^{\mathrm{Res}_{L/k}(\mathrm{Br}(X_k))} = \emptyset$. Now assume that $X(\mathbb{A}_L) \neq \emptyset$ and let Ω_k denote the set of places of k.

We first show that for all $v \in \Omega_k$ and all $w \mid v$, there exists a point $(P_w) \in X(L \otimes_k k_v)$ such that $\sum_{w|v} \mathrm{inv}_w(\mathrm{ev}_{\mathcal{A}}(P_w)) = 0$ for all $\mathcal{A} \in \ker(\mathrm{Br}(X)[2] \to \mathrm{Br}(X_\infty))$. We first consider the case when $X(k_v) \neq \emptyset$. Choose a point $P_v \in X(k_v)$, and for all $w \mid v$, set $P_w = P_v$. Then

$$\begin{aligned}\sum_{w|v} \mathrm{inv}_w(\mathrm{ev}_{\mathcal{A}}(P_w)) &= \sum_{w|v} \mathrm{inv}_w(\mathrm{Res}_{L_w/k_v}(\mathrm{ev}_{\mathcal{A}}(P_v))) = \sum_{w|v} [L_w : k_v]\,\mathrm{inv}_v(\mathrm{ev}_{\mathcal{A}}(P_v)) \\ &= \mathrm{inv}_v(\mathrm{ev}_{\mathcal{A}}(P_v)) \sum_{w|v} [L_w : k_v] = \mathrm{inv}_v(\mathrm{ev}_{\mathcal{A}}(P_v)) \cdot [L : k] = 0 \in \mathbb{Q}/\mathbb{Z}.\end{aligned}$$

Now consider the case where $X(k_v) = \emptyset$. By [CTC79], $X(k_v) \neq \emptyset$ if and only if there exists a 0-cycle of degree 1, hence $X(k_v) = \emptyset$ implies that $X(L_w) = \emptyset$ for all odd degree extensions L_w/k_v. Since $X(L \otimes_k k_v) \neq \emptyset$, L_w/k_v is an even degree extension for all $w \mid v$. Thus, by Lemma 4.2.1, there exists a point $P_w \in X_\infty(L_w)$, and this satisfies $\mathrm{inv}_w(\mathrm{ev}_{\mathcal{A}}(P_w)) = 0$ as $\mathcal{A} \in \ker(\mathrm{Br}(X)[2] \to \mathrm{Br}(X_\infty))$.

Following this construction for each place $v \in \Omega_k$, we produce $(P_w) \in X(\mathbb{A}_L)$ satisfying

$$\sum_{v \in \Omega_k} \sum_{w \mid v} \mathrm{inv}_w(\mathrm{ev}_{\mathcal{A}}(P_w)) = 0.$$

By Corollary 4.2.3, we have that $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)}$ is generated by images of elements of $\ker(\mathrm{Br}(X)[2] \to \mathrm{Br}(X_\infty))$, and therefore we have that $X(\mathbb{A}_L)^{\mathrm{Res}_{L/k}(\mathrm{Br}(X_k))} \neq \emptyset$. □

Proof of Theorem 4.1.1. By work of Colliot-Thélène and Coray, Colliot-Thélène and Swinnerton-Dyer, and Colliot-Thélène, Sansuc, and Swinnerton-Dyer (see Theorem 4.2.9), we have that $X(k) \neq \emptyset$ if and only if $X(\mathbb{A}_k)^{\mathrm{Br}(X)} \neq \emptyset$, so it suffices to show the Brauer–Manin set is nonempty.

Suppose $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} = 0$ and $X(\mathbb{A}_k) \neq \emptyset$. Then, we have that

$$\emptyset \neq X(\mathbb{A}_k) = X(\mathbb{A}_k)^{\mathrm{Br}(X)}$$

and therefore $X(k) \neq \emptyset$ and so $X(L) \neq \emptyset$ for every even degree L/k.

Suppose $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \neq 0$. If $X(L) \neq \emptyset$, we are done, so assume $X(L) = \emptyset$. By Theorem 4.3.1, it suffices to show that $\mathrm{Res}_{L/k} \colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)}$ is surjective. If $\mathrm{Res}_{L/k} \colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)}$ is not surjective, Corollary 4.2.7 shows $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} = 0$, giving a contradiction. □

Corollary 4.3.2. *Let k be a global field of characteristic not equal to 2, let $X \to \mathbb{P}^1_k$ be a conic bundle with four geometric singular fibers. There exists a minimal collection (of size at most three) of quadratic extensions k_i/k such that for all even degree extensions L/k that do not contain any k_i, we have*

$$X(\mathbb{A}_L)^{\mathrm{Br}(X_L)} \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset.$$

Proof. By Theorem 4.3.1, it suffices to show that if L/k is an even degree extension such that $\mathrm{Res}_{L/k}\colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)}$ is not surjective, then L contains one of at most three possible quadratic extensions k_i/k. By Corollary 4.2.7, if the restriction map is not surjective, then there are two cases to consider.

Suppose $|S_k| = 1$ and $|S_L| = 2$, where the two points of L are degree 2 and interchanged by $\mathrm{Gal}(L/k)$. Here, the problematic extensions k_i/k are precisely the extensions for which the singular fibers of $X_{k_i} \to \mathbb{P}^1_{k_i}$ lie over two degree 2 closed points that are interchanged by $\mathrm{Gal}(k_i/k)$. Then, the unique closed point of S_k is of degree 4 and corresponds to either a polynomial of the form $\mathrm{Nm}_{k_0/k}(g(t))$ for k_0/k quadratic and $g(t) \in k_0[t]$ an irreducible quadratic, or of the form $\mathrm{Nm}_{F/k}(\ell(t))$ for F/k biquadratic and $\ell(t) \in F[t]$ linear. Thus, L will contain k_0 in the first case or any of the three quadratic subfields of F in the second case.

Suppose $|S_k| = 2$ and $|S_L| = 2$ with $\mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P) \notin k^{\times 2}$ and $\mathrm{Nm}_{L\cdot\mathbf{k}(P)/L}(\alpha_P) \in L^{\times 2}$ for $P \in S_k = S_L$. Since the points of S_k do not split over L, we must have that $\mathbf{k}(P)$ is linearly disjoint from L, and therefore $\mathrm{Nm}_{L\cdot\mathbf{k}(P)/L}(\alpha_P) = \mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P)$. In order for $\mathrm{Nm}_{L\cdot\mathbf{k}(P)/L}(\alpha_P)$ to be a square in L, the field L must then contain the quadratic field $k(\sqrt{\mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P)})$. □

When X has arbitrarily many singular fibers, we can extend Theorem 4.3.1 at the expense of restricting to quadratic extensions.

Theorem 4.3.3. *Let k be a global field of characteristic not equal to 2 and let $X \to \mathbb{P}^1_k$ be a conic bundle, then for any quadratic extension L/k*

$$X(\mathbb{A}_L)^{\mathrm{Res}_{L/k}(\mathrm{Br}(X_k))} \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset.$$

Proof. Observe that one direction is again immediate, hence we assume that $X(\mathbb{A}_L) \neq \emptyset$. In a similar fashion to the proof of Theorem 4.3.1, we will show that for all $v \in \Omega_k$ there exists a point $(P_w) \in X(L \otimes_k k_v)$ such that $\sum_{w|v} \mathrm{inv}_w(\mathrm{ev}_{\mathcal{A}}(P_w)) = 0$ for all $\mathcal{A} \in \ker(\mathrm{Br}(X)[2] \to \mathrm{Br}(X_\infty))$, and thus $X(\mathbb{A}_L)^{\mathrm{Res}_{L/k}(\mathrm{Br}(X_k))} \neq \emptyset$.

If $X(k_v) \neq \emptyset$ then by an identical argument to the proof of Theorem 4.3.1, there exists a point $(P_w) \in X(\mathbb{A}_L)$ such that $\sum_{w|v} \mathrm{inv}_w(\mathrm{ev}_{\mathcal{A}}(P_w)) = 0$ for all $\mathcal{A} \in \ker(\mathrm{Br}\, X[2] \to \mathrm{Br}\, X_\infty)$.

If $X(k_v) = \emptyset$ and $X(L \otimes_k k_v) \neq \emptyset$, then v is non-split and so L_w/k_v is quadratic. Thus, Lemma 4.2.1 implies the existence of a point $P_w \in X_\infty(L_w)$ which satisfies $\mathrm{inv}_w(\mathrm{ev}_{\mathcal{A}}(P_w)) = 0$ for all $\mathcal{A} \in \ker(\mathrm{Br}(X)[2] \to \mathrm{Br}(X_\infty))$. □

When considering extensions analogous to the extensions k_i of Corollary 4.3.2 for arbitrary conic bundles there are more issues that can arise, but nonetheless, there are still only finitely many. These problematic extensions arise in a similar manner to those of Corollary 4.3.2. Namely, if $S \subseteq \mathbb{P}^1_k$ is the finite set of closed points with geometric singular fiber, then the problematic extensions, k_i/k, are those which either coincide with residue fields $\mathbf{k}(P)$ for $P \in S$, or adjoin square roots of norms of residues $\mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P)$. Over these extensions, $\mathrm{Res}_{k_i/k} \colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_{k_i})}{\mathrm{Br}_0(X_{k_i})}$ could fail to be surjective and new Brauer classes in $\frac{\mathrm{Br}(X_{k_i})}{\mathrm{Br}_0(X_{k_i})}$ could give a Brauer–Manin obstruction to X_{k_i}. For all extensions L/k over which both the points in S remain unchanged and the (products of) norms of residues do not become squares, Lemma 4.2.4 tells us that $\mathrm{Res}_{L/k}$ is an isomorphism, and indeed $X(\mathbb{A}_L)^{\mathrm{Br}(X_L)} \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset$. Since there are only finitely many geometric singular fibers, there are only finitely many problematic extensions of this form, hence we have the following corollary.

Corollary 4.3.4. *Let k be a global field of characteristic not equal to 2, let $X \to \mathbb{P}^1_k$ be a conic bundle, and let L/k be a quadratic extension. For every $T \subseteq S$, let $\beta_T := \prod_{P \in T} \mathrm{Nm}_{\mathbf{k}(P)/k}(\alpha_P)$. Define*

$$M = \left(\bigcup_{P \in S} \{\mathbf{k}(P)\} \right) \cup \left(\bigcup_{T \subseteq S} \left\{ k\left(\sqrt{\beta_T}\right) \right\} \right).$$

Then, if $L \not\subseteq k_i$ for all $k_i \in M$, then

$$X(\mathbb{A}_L)^{\mathrm{Br}(X_L)} \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset.$$

Proof. Since L is disjoint from the fields contained in M, we can apply Lemma 4.2.4 to show that $\mathrm{Res}_{L/k} \colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)}$ is an isomorphism. The result then follows using Theorem 4.3.3. □

Proof of Theorem 4.1.2. This follows from Corollary 4.3.4 and the case of Theorem 4.2.9 using Schinzel's Hypothesis. □

Remark 4.3.5. *Quite generally, if k is a number field and X/k is a smooth, projective, and geometrically rational variety, then $Pic(\overline{X})$ is a Galois lattice split by a finite Galois extension K/k. If E/k is a finite field extension which is linearly disjoint from K/k, then the map $\mathrm{Res}_{E/k}\colon \frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} \to \frac{\mathrm{Br}(X_E)}{\mathrm{Br}_0(X_E)}$ is an isomorphism, and in particular, is surjective. Corollary 4.3.4 is a slight refinement of this result for the case of conic bundles, where the problematic fields are quadratic and made explicit.*

Proof of Theorem 4.1.3. We first show that $X(\mathbb{Q}_p) \neq \emptyset$ if and only if $p = 3$. Note that the fiber at infinity X_∞ is given by $y^2 - 5z^2 = 3w^2$ which has $\mathbb{Q}_p$ points for all $p \neq 3, 5$, and the fiber X_1 over $t = 1$ is given by $y^2 - 5z^2 = \frac{39}{5}$ which has $\mathbb{Q}_5$ points since $-39 \in \mathbb{Q}_5^{\times 2}$. When $p = 3$, note that $5 \notin \mathbb{Q}_3^{\times 2}$, so $\mathbb{Q}_3(\sqrt{5})$ is a quadratic unramified extension of $\mathbb{Q}_3$, and $y^2 - 5z^2$ is a norm from $\mathbb{Q}_3(\sqrt{5})$ and thus has even valuation. Since $5t^4 + 7t^2 + 1$ is irreducible in $\mathbb{F}_3$, the minimum valuation of each term is attained uniquely and thus always has even valuation, and so $\frac{3}{5}(5t^4 + 7t^2 + 1)$ always has odd valuation and cannot be of the form $y^2 - 5z^2$. This shows that $X(\mathbb{A}_\mathbb{Q}) = \emptyset$. Thus, $X(\mathbb{Q}) = \emptyset$, and since $5t^4 + 7t^2 + 1$ is irreducible, by Lemma 4.2.6 we must have $\frac{\mathrm{Br}(X)}{\mathrm{Br}_0(X)} = 0$.

Now consider $L = \mathbb{Q}(\sqrt{29})$. Since $[\mathbb{Q}_3(\sqrt{29}) : \mathbb{Q}_3] = 2$, Lemma 4.2.1 shows $X(\mathbb{Q}_3(\sqrt{29})) \neq \emptyset$ and thus $X(\mathbb{A}_L) \neq \emptyset$. We see that X_L is given by

$$y^2 - 5z^2 = 3\left(t^2 + \frac{1}{10}(7 + \sqrt{29})\right)\left(t^2 + \frac{1}{10}(7 - \sqrt{29})\right)$$

hence by a computation using Lemma 4.2.2 we have $\frac{\mathrm{Br}(X_L)}{\mathrm{Br}_0(X_L)} \cong \mathbb{Z}/2\mathbb{Z} = \langle \mathcal{A} \rangle$, where $\mathcal{A}$ denotes the quaternion algebra $\left(5, t^2 + \frac{1}{10}(7 + \sqrt{29})\right)$.

It remains to show that $X(\mathbb{A}_L)^{\mathrm{Br}(X_L)} = \emptyset$ and we do so by first showing that $\mathrm{ev}_\mathcal{A}\colon X(L_w) \to \mathrm{Br}(L_w)$ is identically zero for all $w \nmid 5$. Begin by observing that for all primes $w \mid p$ where $p \neq 3, 5$, we know that $X_\infty(L_w) \neq \emptyset$, hence $\mathrm{ev}_\mathcal{A}\colon X(L_w) \to \mathrm{Br}(L_w)$ takes the value 0 at such primes, as $\mathcal{A}$ evaluates to $(5, 1) = 0 \in \mathrm{Br}(L_w)$. Since the evaluation map is constant

at all primes w of good reduction [CTS13, Theorem 3.1], it remains to check $\mathrm{ev}_{\mathcal{A}}(X(L_w))$ for primes w lying over $p = 2, 3, 5$, and 29. Now observe that, for $w \mid 2, 3, 29$, we have that $5 \in L_w^{\times 2}$ hence the algebra $\mathcal{A} = \left(5, t^2 + \frac{1}{10}(7 + \sqrt{29})\right)$ is identically zero and $\mathrm{ev}_{\mathcal{A}}(X(L_w)) = 0$. Thus for any $(P_w) \in X(\mathbb{A}_L)$ we have

$$\sum_{w \in \Omega_L} \mathrm{inv}_w\left(\mathrm{ev}_{\mathcal{A}}(P_w)\right) = \sum_{w|5} \mathrm{inv}_w\left(\mathrm{ev}_{\mathcal{A}}(P_w)\right).$$

Let w_1 and w_2 denote the places lying over 5 corresponding to the embeddings in which $\sqrt{29} \equiv 2 \pmod 5$ and $\sqrt{29} \equiv 3 \pmod 5$ respectively and let $P_i = (t_i, y_i, z_i) \in X(L_{w_i})$. We now show that

$$\mathrm{inv}_{w_i}\left(\mathcal{A}(P_i)\right) = \begin{cases} \frac{1}{2} & \text{if } i = 1 \\ 0 & \text{if } i = 2 \end{cases}.$$

Let $\alpha = \frac{1}{10}(7 + \sqrt{29})$ and $\overline{\alpha} = \frac{1}{10}(7 - \sqrt{29})$. Over $\mathbb{Q}_5$, we have

$$X/\mathbb{Q}_5 \colon y^2 - 5z^2 = 3(t^2 + \alpha)(t^2 + \overline{\alpha})$$

hence $\frac{\mathrm{Br}\, X_{\mathbb{Q}_5}}{\mathrm{Br}\, \mathbb{Q}_5}$ is generated by the quaternion algebra $\mathcal{A} = (5, t^2 + \alpha)$. Note that in $\mathrm{Br}\, X$, the quaternion algebra $\mathcal{A}$ is equivalent to the algebra $\mathcal{B} = (5, 3(t^2 + \overline{\alpha}))$. This will be an important tool in the final part of our proof.

First we consider the place w_1 and observe that since $\sqrt{29} \equiv 2 \pmod 5$, we have $w_1(\alpha) = -1$. Moreover, since $\alpha\overline{\alpha} = \frac{1}{5}$, it follows that $w_1(\overline{\alpha}) = 0$. Take $P_1 = (t_1, y_1, z_1)$ and suppose $w_1(t_1) < 0$, and consider the polynomial $P(t) = \frac{3}{5}(5t^4 + 7t^2 + 1)$. We have that $5^{-4w_1(t_1)}P(t) \equiv 3 \pmod 5$ hence $P(t)$ is never a norm from $\mathbb{Q}_5(\sqrt{5})$, so we must have $w_1(t_1) \geq 0$ for all $P_1 \in X(L_{w_1})$. Then, by the strong triangle inequality, $w_1(t_1^2 + \alpha) = w_1(\alpha)$ and since $5\alpha \equiv \frac{1}{2}(7 + \sqrt{29}) \equiv 2 \pmod 5$, it follows that $10(t_1^2 + \alpha) \in \mathbb{Q}_5^{\times 2}$, meaning $\mathrm{ev}_{\mathcal{A}}(P_1) = (5, 10)$ which is a non-split quaternion algebra in $\mathrm{Br}(\mathbb{Q}_5)$. This shows that $\mathrm{inv}_{w_1}\left(\mathrm{ev}_{\mathcal{A}}(P_1)\right) = \frac{1}{2}$.

We now consider the case of w_2 and recall that in this case, $\sqrt{29} \equiv 3 \pmod 5$, hence $w_2(\alpha) = 0$ and $w_2(\overline{\alpha}) = -1$. Take $P_2 = (t_2, y_2, z_2)$ and observe that just as in the previous

case, if $P_2 \in X(L_{w_2})$ we must have $w_2(t_2) \geq 0$. If $w_2(t_2) > 0$ then by the same argument for when $w_1(t_1) \geq 0$, we have that $t_2^2 + \alpha$ is always a square in $\mathbb{Q}_5$, hence $\mathrm{ev}_{\mathcal{A}}(P_2) = 0 \in \mathrm{Br}(\mathbb{Q}_5)$. It remains to consider the case when $w_2(t_2) = 0$ and for this, we consider the algebra $\mathcal{B} = (5, 3(t^2 + \overline{\alpha}))$ and show that $\mathrm{ev}_{\mathcal{B}}(P_2)$ is identically zero in $\mathrm{Br}(\mathbb{Q}_5)$. For such values of t_2 we have $w_2\left(3(t^2 + \overline{\alpha})\right) = w_2(\overline{\alpha})$ hence $5\left(3(t^2 + \overline{\alpha})\right) \equiv 3\overline{\alpha} \pmod 5$, which by Hensel's lemma, is a square in $\mathbb{Q}_5$. It now follows that for all $P_2 \in X(L_{w_2})$ we have $\mathrm{inv}_{w_2}(\mathrm{ev}_{\mathcal{A}}(P_2)) = 0$.

We can now conclude that for any $P_w \in X(\mathbb{A}_L)$ we have

$$\sum_{w \in \Omega_L} \mathrm{inv}_w\left(\mathrm{ev}_{\mathcal{A}}(P_w)\right) = \frac{1}{2}$$

and thus X fails the Hasse principle over L. □

4.4 An additional condition on Châtelet surfaces

We have showed that the failure of the Hasse principle for X over an even degree extension is explained by quadratic extensions associated to the singular fibers of X. In the case of Châtelet surfaces, this can occur for surfaces X/k of the form

$$y^2 - az^2 = c\,\mathrm{Nm}_{F/k}(g(t))$$

where $a, c \notin k^{\times 2}$, $g(t) \in F[t]$ is a monic, irreducible polynomial, and $\mathrm{Nm}_{F/k}$ denotes the usual norm map. In contrast to Theorem 4.1.3, not all such extensions F/k are guaranteed to produce a Brauer–Manin obstruction over F. In order for such an obstruction to exist, the fiber X_∞, the places for which it has no local points, and the places of bad reduction, must satisfy several necessary conditions.

Theorem 4.4.1. *Let k be a number field, let F/k be a quadratic extension, and let X/k be the Châtelet surface given by*

$$y^2 - az^2 = c\,\mathrm{Nm}_{F/k}(g(t))$$

where $a, c \notin k^{\times 2}$ and $g(t) \in F[t]$ is monic irreducible of degree 2. Let Ω_k denote the set of

places of k, let Ω_F denote the set of places of F, and assume $X(\mathbb{A}_k) = \emptyset$. If

$$\sum_{\substack{v \in \Omega_k \\ v \text{ splits in } F}} \text{inv}_v(a, c) = 0 \in \mathbb{Q}/\mathbb{Z}$$

then for all even degree extensions L/k, we have $X(L) \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset$.

Proof. Let $v \in \Omega_k$, let $w \in \Omega_F$ such that $w \mid v$. Let $\mathcal{A} = (a, g(t))$ be a generator of $\frac{\text{Br}(X_F)}{\text{Br}_0(X_F)}$ and let σ denote the generator of $\text{Gal}(F/k)$. If $[F_w : k_v] = 2$ then there exists a point $P_w \in X_\infty(F_w)$ such that $\text{inv}_w(\mathcal{A}(P_w)) = 0$ by Lemma 4.2.1. Now assume that $F_w = k_v$, then there exists a unique place w' such that $w' \neq w$ and $w' \mid v$, hence $F_w = F_{w'} = k_v$. Take $P_v \in X(k_v)$ and set $P_v = P_w = P_{w'} = (t_v, y_v, z_v)$. We then have

$$\begin{aligned} \text{inv}_w(\mathcal{A}(P_v)) + \text{inv}_{w'}(\mathcal{A}(P_v)) &= \text{inv}_w\Big((a, g(t_v)) + (a, \sigma(g)(t_v))\Big) \\ &= \text{inv}_w\Big(a, g(t_v)\sigma(g)(t_v)\Big) \\ &= \text{inv}_v((a, c)). \end{aligned}$$

Now, picking $(P_w) \in X(\mathbb{A}_F)$ as above, we have

$$\sum_{w \in \Omega_F} \text{inv}_w\Big(\mathcal{A}(P_w)\Big) = \sum_{\substack{w \in \Omega_F \\ [F_w : k_v] = 2}} 0 + \sum_{\substack{w \in \Omega_F \\ [F_w : k_v] = 1}} \text{inv}_w\Big(\mathcal{A}(P_w)\Big) = \sum_{\substack{v \in \Omega_k \\ v \text{ splits in } F}} \text{inv}_v(a, c)$$

Now, if

$$\sum_{\substack{v \in \Omega_k \\ v \text{ splits in } F}} \text{inv}_v(a, c) = 0 \in \mathbb{Q}/\mathbb{Z}$$

then $X(\mathbb{A}_F)^{\text{Br}(X_F)} \neq \emptyset$ and it follows that $X(F) \neq \emptyset$. Since F/k is the only even degree extension over which the set S decomposes as two points of degree 2, it follows from Corollary 4.2.7 that if L/k is any even degree extension, then $X(L) \neq \emptyset \Leftrightarrow X(\mathbb{A}_L) \neq \emptyset$. □

BIBLIOGRAPHY

[BBB+22] Alex J. Best, L. Alexander Betts, Matthew Bisatt, Raymond van Bommel, Vladimir Dokchitser, Omri Faraggi, Sabrina Kunzweiler, Céline Maistret, Adam Morgan, Simone Muselli, and Sarah Nowell, *A user's guide to the local arithmetic of hyperelliptic curves*, Bull. Lond. Math. Soc. **54** (2022), no. 3, 825–867. MR4453743 ↑3.1

[BPR13] Matthew Baker, Sam Payne, and Joseph Rabinoff, *On the structure of non-Archimedean analytic curves*, Tropical and non-Archimedean geometry, 2013, pp. 93–121. MR3204269 ↑3.3.5

[Cla09] Pete L. Clark, *On the Hasse principle for Shimura curves*, Israel J. Math. **171** (2009), 349–365. MR2520114 ↑4.1

[CT92] Jean-Louis Colliot-Thélène, *L'arithmétique des variétés rationnelles*, Ann. Fac. Sci. Toulouse Math. (6) **1** (1992), no. 3, 295–336. MR1225663 ↑1

[CTC79] Jean-Louis Colliot-Thélène and Daniel Coray, *L'équivalence rationnelle sur les points fermés des surfaces rationnelles fibrées en coniques*, Compositio Math. **39** (1979), no. 3, 301–332. MR550646 ↑4.1, 4.2.2, 4.3

[CTS13] Jean-Louis Colliot-Thélène and Alexei N. Skorobogatov, *Good reduction of the Brauer-Manin obstruction*, Trans. Amer. Math. Soc. **365** (2013), no. 2, 579–590. MR2995366 ↑4.3

[CTS21] ———, *The Brauer-Grothendieck group*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 71, Springer, Cham, 2021. MR4304038 ↑2.4.11, 4.2.2, 4.2.2

[CTSD94] Jean-Louis Colliot-Thélène and Peter Swinnerton-Dyer, *Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties*, J. Reine Angew. Math. **453** (1994), 49–112. MR1285781 ↑4.1, 4.2.2

[CTSSD87] Jean-Louis Colliot-Thélène, Jean-Jacques Sansuc, and Peter Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces. II*, J. Reine Angew. Math. **374** (1987), 72–168. MR876222 ↑4.1, 4.2.2

[CV25] Brendan Creutz and Bianca Viray, *Degrees of points on varieties over Henselian fields*, Trans. Amer. Math. Soc. **378** (2025), no. 1, 259–278. MR4840304 ↑3.1, 3.1, 3.6, 3.7.2

[DDMM19] Tim Dokchitser, Vladimir Dokchitser, Céline Maistret, and Adam Morgan, *Semistable types of hyperelliptic curves*, Algebraic curves and their applications, 2019, pp. 73–135. MR3916736 ↑3.1, 3.3.1

[DDMM23] ———, *Arithmetic of hyperelliptic curves over local fields*, Math. Ann. **385** (2023), no. 3-4, 1213–1322. MR4566695 ↑3.1

[Dok21] Tim Dokchitser, *Models of curves over discrete valuation rings*, Duke Math. J. **170** (2021), no. 11, 2519–2574. MR4302549 ↑3.1, 3.1, 3.7.2

[Duc13] Antoine Ducros, *Toute forme modérément ramifiée d'un polydisque ouvert est triviale*, Math. Z. **273** (2013), no. 1-2, 331–353. MR3010163 ↑3.2.3

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR718935 ↑1

[FN20] Omri Faraggi and Sarah Nowell, *Models of hyperelliptic curves with tame potentially semistable reduction*, Trans. London Math. Soc. **7** (2020), no. 1, 49–95. MR4201122 ↑3.1, 3.1

[GLL13] Ofer Gabber, Qing Liu, and Dino Lorenzini, *The index of an algebraic variety*, Invent. Math. **192** (2013), no. 3, 567–626. ↑3.1

[GS17] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Second, Cambridge Studies in Advanced Mathematics, vol. 165, Cambridge University Press, Cambridge, 2017. MR3727161 ↑2.4.3, 2.4.7, 2.4.9

[GW25] Alexander Galarraga and Alexander Wang, *Superelliptic degree sets over henselian fields* (2025), available at 2511.15951. ↑1, 1.1, 3

[Isk71] V. A. Iskovskih, *A counterexample to the Hasse principle for systems of two quadratic forms in five variables*, Mat. Zametki **10** (1971), 253–257. MR286743 ↑4.1

[Isk96] V. A. Iskovskikh, *On a rationality criterion for conic bundles*, Mat. Sb. **187** (1996), no. 7, 75–92. MR1404188 ↑4.1

[Kan87] Dimitri Kanevsky, *Application of the conjecture on the Manin obstruction to various Diophantine problems*, 1987, pp. 307–314, 345. Journées arithmétiques de Besançon (Besançon, 1985). MR891437 ↑4.1

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Second, Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR754003 ↑2.1.4

[Lan02] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. ↑3.2.2

[Lan13] ———, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 2013. ↑3.2.3

[LL18] Qing Liu and Dino Lorenzini, *New points on curves*, Acta Arith. **186** (2018), no. 2, 101–141. ↑3.1, 3.2.4, 3.2.4

[Man71] Y. I. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, 1971, pp. 401–411. MR427322 ↑1

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR1697859 ↑2.2.1, 2.2.4, 2.2.5, 2.2.7

[Poo09] Bjorn Poonen, *Existence of rational points on smooth projective varieties*, J. Eur. Math. Soc. (JEMS) **11** (2009), no. 3, 529–543. MR2505440 ↑4.1

[Poo17] ———, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. MR3729254 ↑2.1, 2.4.8, 2.4.12, 2.5.3

[Pop10] Florian Pop, *Henselian implies large*, Ann. of Math. (2) **172** (2010), no. 3, 2183–2195. ↑3.2.4, 3.2.4

[RW26] Sam Roven and Alexander Wang, *On the Hasse Principle for Conic Bundles over Even Degree Extensions*, Res. Number Theory **12** (2026), no. 2, Paper No. 35. MR5049066 ↑1, 1.1, 4

[Sko15] A. Skorobogatov, *Rational points on higher-dimensional varieties* (2015). ↑4.2.2