HBA Lecture Notes in Mathematics
IMSc Lecture Notes in Mathematics

Pietro Corvaja

Integral Points on Algebraic Varieties

An Introduction to Diophantine Geometry

HINDUSTAN
BOOK AGENCY

Springer

HBA Lecture Notes in Mathematics

IMSc Lecture Notes in Mathematics

About the Series

The *IMSc Lecture Notes in Mathematics* series is a subseries of the *HBA Lecture Notes in Mathematics* series. This subseries publishes high-quality lecture notes of the Institute of Mathematical Sciences, Chennai, India. Undergraduate and graduate students of mathematics, research scholars, and teachers would find this book series useful. The volumes are carefully written as teaching aids and highlight characteristic features of the theory. The books in this series are co-published with Hindustan Book Agency, New Delhi, India.

More information about this series at http://www.springer.com/series/15465

Pietro Corvaja

Integral Points on Algebraic Varieties

An Introduction to Diophantine Geometry

HINDUSTAN
BOOK AGENCY

Springer

Pietro Corvaja
Dipartimento di Matematica
Università degli studi di Udine
Udine, Italy

This work is a co-publication with Hindustan Book Agency, New Delhi, licensed for sale in all countries in electronic form only. Sold and distributed in print across the world by Hindustan Book Agency, P-19 Green Park Extension, New Delhi 110016, India. ISBN: 978-93-80250-83-0 © Hindustan Book Agency 2016.

ISSN 2509-8071 (electronic)
HBA Lecture Notes in Mathematics
ISSN 2509-8098 (electronic)
IMSc Lecture Notes in Mathematics
ISBN 978-981-10-2648-5 (eBook)
DOI 10.1007/978-981-10-2648-5

Library of Congress Control Number: 2016952895

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #22-06/08 Gateway East, Singapore 189721, Singapore

Contents

Introduction

This survey is intended to be a concrete introduction to Diophantine geometry; it originates in a three-week course delivered at the Institute for Mathematical Sciences in Chennai during the special year devoted to Number Theory.

The leading theme is represented by the distribution of integral points on algebraic varieties. Roughly speaking, a Diophantine equation should have only finitely many solutions in integers unless there is a geometric reason explaining their abundance. By 'geometric', we mean some property satisfied by the *algebraic variety* formed by the complex solutions to the given equation (or system of equations).

The celebrated Lang-Vojta's conjecture formalizes this principle: it gives geometrical condition on an algebraic variety under which the set of integral points should be degenerate, i.e. contained in a finite union of proper closed subvarieties. Most of this text is devoted to explaining in concrete instances some features of this conjecture, and to proving some particular cases. A nowadays classical theorem of Faltings and Vojta solved the conjecture for varieties which can be embedded into semi-abelian varieties. It contains e.g. the solution to Mordell's conjecture on rational points on compact hyperbolic curves, as well as Siegel's finiteness theorem for integral points on open hyperbolic curves. We have chosen to focus on a recent different method, which relies on the Subspace Theorem in Diophantine approximation, and makes no use of the theory of algebraic groups.

This work is not meant to supersede any previous standard textbook on Diophantine geometry, such as the classical books by Lang [40], Serre [48], Vojta [55] and the more recent ones by Hindry and Silverman [35] and Bombieri and Gubler [8], to which the reader is referred. The main goal of this work is to rapidly introduce the impatient reader to some concrete problems in Diophantine geometry, especially those involving integral points, to present some recent results not available in textbooks and to show some new viewpoints on classical material. At some points, we preferred to replace proofs by a detailed analysis of particular cases, referring to the papers quoted in the references for complete proofs. In some instances, we decided to prove a general result only in special cases, thinking that a simpler proof in a particular but significant case can be more illuminating than the more complicated proof of the most general statement.

Needless to say, we have omitted many (if not most) central topics in Diophantine geometry, such as: local-to-global principles, arithmetic on elliptic curves and abelian varieties, asymptotic estimates (as appearing e.g. in Manin's conjecture). Even the investigation of rational points on algebraic varieties has been almost omitted, in favor of the case of integral points.

In the first chapter, we introduce the general problem of the distribution of integral and rational points on algebraic varieties; Lang-Vojta's conjecture, the central objective of this work, is formulated and discussed. Also, we provide some useful facts on the behaviour of integral points under morphisms.

In the second chapter, we present without proofs the main tools from Diophantine approximation theory, and show some relations among them. In particular, we present different formulations of the Subspace Theorem, which will be the main tool for proving the degeneracy results for integral points appearing in the subsequent chapters.

The third chapter contains a complete proof of Siegel-Mahler theorem on integral points on curves, as well as different approaches to a previous result of Thue.

The fourth chapter is devoted to the celebrated Hilbert Irreducibility Theorem; we prove a generalized version of Hilbert Irreducibility Theorem by appealing to Siegel's theorem on curves.

The last chapter is devoted to the analysis of integral points on surfaces. It is perhaps the most original part, containing also very recent results not yet published in any textbook.

Acknowledgments

The author is very grateful to the Institute of Mathematical Sciences in Chennai, and especially to Prof. Balasubramanian and his collaborators, for inviting him on the occasion of the Number Theory Year 2010-11. During a subsequent visit to the Institute, the author had the opportunity of lecturing on Hilbert irreducibility theorem, which constitues the topic of the fourth chapter of this text. Discussions with the audience in Chennai were much stimulating, and its encouragement to write up these notes was crucial.

The author is also pleased to thank Martino Buchini, Jung-Kyu Canci, Umberto Zannier, Michel Waldschmidt and an anonymous referee, who read previous versions of these notes, detected some inaccuracies and suggested many improvements.

About the Author

Pietro Corvaja is Full Professor of Geometry at the Dipartimento Di Mathematica Einformatica at the Università degli studi di Udine, Italy. His research topics include arithmetic geometry, Diophantine approximation and the theory of transcendental numbers.

Chapter 1
Integral points on algebraic varieties

1.1 Introducing the problem

Our main concern will be the investigation of the solutions in integers to systems of algebraic equations. Namely, given polynomials $f_1(X_1,\dots,X_N),\dots,f_k(X_1,\dots,X_N) \in \mathbb{Z}[X_1,\dots,X_N]$, we consider the solutions $(x_1,\dots,x_N)\in\mathbb{Z}^N$ to the equations

$$\begin{cases} f_1(x_1,\dots,x_N) = 0 \\ \quad\vdots \qquad\quad \vdots\ \vdots \\ f_k(x_1,\dots,x_N) = 0 \end{cases}$$

The complex solutions to the above system form an affine algebraic variety, defined over the field $\mathbb{Q}$ of rational numbers. Hence the problem is rephrased as studying the integral points on algebraic varieties.

One can consider the analogous question for rational points and can work also on projective varieties. Given *homogeneous* polynomials $f_1(X_0,\dots,X_N),\dots,f_k(X_0,\dots,X_N)\in\mathbb{Z}[X_0,\dots,X_N]$, their common zero set in $\mathbb{P}_N$ is a projective algebraic variety. The solutions $(x_0,\dots,x_N)\in\mathbb{Q}^{N+1}$ to the system $f_i(x_0,\dots,x_N)=0$ $(i=1,\dots,k)$ correspond to rational points $(x_0:\dots:x_N)\in\mathbb{P}_N(\mathbb{Q})$ on such variety.

The aim of this survey is to show relations between the geometry of (complex) algebraic varieties and the distribution of integral or rational points on it. The following examples show that, to achieve this goal, it is necessary to allow extensions of finite degree of the field of definitions and/or of the ring of integers.

(i) Consider the conic $\mathcal{C}\subset\mathbb{P}_2$ of equation (in homogeneous coordinates) $X^2+Y^2=3Z^2$. It admits no rational points, and nevertheless it is isomorphic (as an abstract complex curve) to the projective line $\mathbb{P}_1$, whose rational points are Zariski-dense. If we work over the number field $\mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{3})$, this

P. Corvaja, *Integral Points on Algebraic Varieties*, HBA Lecture Notes in Mathematics, DOI 10.1007/978-981-10-2648-5_1

paradox is solved: both $\mathcal{C}$ and $\mathbb{P}_1$ have a Zariski-dense set of rational points, and the two curves are isomorphic over such number fields.
A simpler example is provided by the conic of equation $X^2 + Y^2 + Z^2 = 0$, which has no real points at all. Again, it has infinitely many points over the number field $\mathbb{Q}(i)$, or $\mathbb{Q}(\sqrt{-2})$.

(ii) Let $\mathcal{C}$ be the affine line of equation $2x + 2y = 1$. Clearly, such an equation admits no integral solution, so $\mathcal{C}$ contains no integral point, although it is isomorphic (even over the rational number field) to the line of equation $x + y = 1$, which contains infinitely many integral points. Of course, both equations have infinitely many solutions over the ring $\mathbb{Z}[1/2]$.

(iii) Consider the hyperbola of equation $xy = 1$ in the affine plane. It contains only two integral points, namely $(1, 1), (-1, -1)$. Nevertheless, it is isomorphic, over the reals (so in particular over the complex numbers) to the hyperbola of equation $x^2 - 2y^2 = 1$, which admits infinitely many integral points (Pell's equation). Extending the ring of integers to $\mathbb{Z}[\sqrt{2}]$, the two curves become isomorphic (and both have infinitely many points with coordinates in such a ring).

Hence, it will be more convenient to complicate a little our setting, allowing arbitrary number fields as fields of definition and searching for solutions in arbitrary rings of S-integers (see below for the definition). Also, it is more convenient to rephrase the notion of integral point on an algebraic variety to a more intrinsic one, recovering in particular cases the naive definition of "point with integral coordinates".

Let κ be a number field. The absolute values of κ are either p-adic (we say also finite, or ultrametric) or archimedean. A place is an equivalence class of absolute values, where two absolute values are called equivalent if they induce the same topology. The finite places correspond to non-zero prime ideals of the ring of integers of κ; the archimedean ones correspond to embeddings $\kappa \hookrightarrow \mathbb{C}$ up to conjugation.

Let ν be a finite place; we denote by $\mathcal{O}_\nu$ the valuation ring at the place ν and by $\mathfrak{m}_\nu$ its maximal ideal:

$$\mathcal{O}_\nu = \{x \in \kappa \, : \, |x|_\nu \leq 1\}, \qquad \mathfrak{m}_\nu = \{x \in \kappa \, : \, |x|_\nu < 1\},$$

and let

$$\kappa(\nu) := \mathcal{O}_\nu / \mathfrak{m}_\nu$$

be the corresponding residue field, which is a finite field. The elements of $\mathcal{O}_\nu$ will be called ν-integers.

For a finite set S of places containing the archimedean ones, we put

$$\mathcal{O}_S = \{x \in \kappa \, : \, |x|_\nu \leq 1, \, \forall \nu \notin S\}.$$

The elements of the ring $\mathcal{O}_S$ will be called S-integers. Note that an S-integer is an element of the number field which is ν-integral for each place ν *outside* S. Whenever S consists precisely of the archimedean absolute values, the ring of S-integers coincides with the ring $\mathcal{O}_\kappa$ of algebraic integers in κ.

The group of S-units will play a prominent role; it is defined to be the group

$$\mathcal{O}_S^* = \{x \in \kappa \,:\, |x|_\nu = 1, \,\forall \nu \notin S\}.$$

For every finite place ν, there is a well defined *reduction map*

$$\mathbb{P}_N(\kappa) \to \mathbb{P}_N(\kappa(\nu)) :$$

given a point $P \in \mathbb{P}_N(\kappa)$ with projective coordinates $(x_0 : \ldots : x_N)$ (where $x_i \in \kappa$ for $i = 0, \ldots, N$), we can choose a non-zero scalar λ such that $\lambda \cdot x_i \in \mathcal{O}_\nu$ for all $i = 0, \ldots, N$ and not all the x_i belong to $\mathfrak{m}_\nu$; the existence of such a λ is guaranteed by the fact that the local ring $\mathcal{O}_\nu$ is a discrete valuation ring, so in particular a principal ideal domain. Let $P_\nu \in \mathbb{P}_N(\kappa(\nu))$ be the point $P_\nu = (\lambda x_0 + \mathfrak{m}_\nu : \ldots : \lambda x_N + \mathfrak{m}_\nu)$; it will be called the reduction modulo ν (or modulo $\mathfrak{m}_\nu$) of the rational point P.

Let now $D \subset \mathbb{P}_N$ be a closed subvariety defined over κ. It is defined by a homogeneous ideal $I_D \subset \kappa[X_0, \ldots, X_N]$; consider its intersection $I_{D,\nu} := I_D \cap \mathcal{O}_\nu[X_0, \ldots, X_N]$ with the ring of polynomials with ν-integral coefficients. One can consider its image in the quotient ring $\mathcal{O}_\nu[X_0, \ldots, X_n]/\mathfrak{m}_\nu = \kappa(\nu)[X_0, \ldots, X_N]$; it is a homogeneous ideal of $\kappa(\nu)[X_0, \ldots, X_N]$, so it corresponds to a closed subvariety D_ν of the projective space $\mathbb{P}_N$ over the finite field $\kappa(\nu)$.

Then it makes sense to check whether a rational point $P \in \mathbb{P}_N(\kappa)$ reduces modulo ν to the closed subvariety D: we will mean that the point P_ν belongs to D_ν.

Let $\tilde{X} \subset \mathbb{P}_N$ be a projective algebraic variety defined over the number field κ and $D \subset \tilde{X}$ be an algebraic subset. We say that a rational point $P \in \tilde{X}(\kappa)$ is integral with respect to D if for no finite place ν of κ the point P reduces to D modulo ν (this in particular implies that P does not lie on D). If S is a finite set of places containing the archimedean ones, we will speak of $(S - D)$ integral points (sometimes omitting the reference to S or D) if the same condition holds for every place ν outside S.

Putting $X := \tilde{X} \setminus D$, we speak of S-integral points of X, and denote its set by $X(\mathcal{O}_S)$.

Whenever $X \subset \mathbb{A}^N \subset \mathbb{P}_N$ is an affine variety, we let $\tilde{X}$ be its completion under the canonical embedding $\mathbb{A}^N \hookrightarrow \mathbb{P}_N$ and put $D = \tilde{X} \setminus X$. Then the $(S - D)$ integral points of $\tilde{X}$ will be the points of X with coordinates in $\mathcal{O}_S$.

Examples

- Let $X = \mathbb{A}^1, \tilde{X} = \mathbb{P}_1$, $D = \{(1 : 0)\}$; the immersion $\mathbb{A}^1 \hookrightarrow \mathbb{P}_1$ is given by $x \mapsto (x : 1)$. A point $x = a/b \in \mathbb{A}^1(\mathbb{Q})$, where a, b are coprime integers, $b \neq 0$, is integral with respect to D if for every prime p, $(a/b : 1) = (a : b) \not\equiv (1 : 0) \pmod{p}$, i.e. no prime number divides b, so $b = \pm 1$, which means that $x \in \mathbb{Z}$.
- Take $X = \mathbb{G}_m = \mathbb{P}_1 \setminus \{0, \infty\}$, so now $D = \{0, \infty\}$. Then a point $(x : 1) \in \mathbb{P}_1(\mathcal{O}_S)$ is integral with respect to D if and only if x is a unit in $\mathcal{O}_S$. So

$\mathbb{G}_m(\mathcal{O}_S) = \mathcal{O}_S^*$. If $\mathcal{O}_S = \mathbb{Z}$ or the ring of integers of an imaginary quadratic field, then $\mathbb{G}_m(\mathcal{O}_S)$ is a finite set; otherwise, it is Zariski-dense.

- Take $\tilde{X} = \mathbb{P}_1 \times \mathbb{P}_1$, and for D the diagonal. A point $P = ((a : b), (c : d)) \in \tilde{X}(\mathbb{Q})$, where $a, b, c, d \in \mathbb{Z}$ and $\gcd(a, b) = \gcd(c, d) = 1$, is D-integral if and only if $ad - bc = \pm 1$. Then $X(\mathbb{Z})$ is in natural bijection with the group $P\mathrm{SL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ and is Zariski-dense in X.
- Take $\tilde{X}$ as above, $D = ((1 : 0), (1 : 0))$; note that D is not a hypersurface. Then a point $P = ((a : b), (c : d))$ as above is D-integral if and only if $\gcd(b, d) = 1$. In the present case too, integral points are Zariski-dense.
- Let $D \subset \mathbb{P}_N$ be a hypersurface defined by the equation $F(X_0, \ldots, X_N) = 0$. Here $F(X_0, \ldots, X_N) \in \mathcal{O}_S[X_0, \ldots, X_N]$ is a polynomial with coprime S-integral coefficients. Then, if we assume for simplicity that $\mathcal{O}_S$ is a principal ideal domain (which can always be achieved after a finite enlargement of S), the $(S - D)$ integral points on $\mathbb{P}_N$ can be written in projective coordinates $(x_0 : \ldots : x_N)$ such that $F(x_0, \ldots, x_N) \in \mathcal{O}_S^\times$.

Our definition depends on the embedding $X \hookrightarrow \mathbb{P}_N$. Actually, given an (abstract) variety $X = \tilde{X} \setminus D$ and a rational point $P \in X(\kappa)$, it is always possible to find an embedding $\tilde{X} \hookrightarrow \mathbb{P}_N$ such that P becomes integral.

It is worthwhile, although unnecessary for the comprehension of the sequel, to look at an alternative definition in terms of schemes. To an algebraic variety X over a number field κ, we can associate an *integral model* over the ring of integers $\mathcal{O}_\kappa$, or more generally over a ring of S-integers $\mathcal{O}_S$: it is a flat scheme $\mathcal{X} \to \mathrm{Spec}(\mathcal{O}_S)$, whose generic fiber is isomorphic to X. Then the S-integral points of X correspond to sections $\mathrm{Spec}(\mathcal{O}_S) \to \mathcal{X}$.

Alternatively, let $\tilde{X}$ be a complete variety, $D \subset \tilde{X}$ a closed subvariety, both defined over the number field κ; let $\tilde{\mathcal{X}}$ be an integral model of $\tilde{X}$, and let $\mathcal{D} \subset \tilde{\mathcal{X}}$ be the closed subscheme corresponding to D. Then the integral points on $X := \tilde{X} \setminus D$ correspond to sections $\mathrm{Spec}(\mathcal{O}_S) \to \tilde{\mathcal{X}}$ *avoiding* the subscheme $\mathcal{D}$. Of course, this integrality notion heavily depends on the chosen integral model for X. In our previous definition, the dependence on the integral model was hidden by the choice of a projective embedding: since the projective space $\mathbb{P}_N$ admits a canonical integral model over $\mathrm{Spec}(\mathcal{O}_S)$ for every ring (of S-integers) $\mathcal{O}_S$, every embedded variety inherits an integral model.

1.2 The conjecture of Lang-Vojta

We recall some facts from (complex) algebraic geometry. Given a smooth complete algebraic variety $\tilde{X}$ and a divisor D on $\tilde{X}$, we associate to it the sequence $h^0(\tilde{X}, nD)$ of the dimensions of the spaces of regular sections of the associated sheaf:

$$h^0(\tilde{X}, nD) = \dim \mathrm{H}^0(\tilde{X}, \mathcal{O}(nD)).$$

Recall that the vector space $\mathrm{H}^0(\tilde{X}, \mathcal{O}(D))$ can be viewed as the space of rational functions f on $\tilde{X}$ whose divisor (f) satisfies $(f) + D \geq 0$; if D is effective, this means that the poles of f are contained in the hypersurface D and their multiplicity is bounded by the corresponding multiplicity in D. We say that a divisor is *big* if it satisfies

$$h^0(\tilde{X}, nD) \gg n^{\dim \tilde{X}}$$

for $n \to \infty$. For instance, whenever D is an ample divisor, $h^0(\tilde{X}, nD) = (D^d/d!)n^d + O(n^{d-1})$, where $d = \dim \tilde{X}$ and the symbol D^d denotes the d-fold intersection product. So, ample divisors are big.

For an effective divisor D, the following are equivalent (see [23], chapter 1):

(i) D is big;
(ii) there exists an integer $n > 0$ such that nD is linearly equivalent to the sum of an ample and an effective divisor.

In the special case of curves, big divisors are simply those with strictly positive degree, which are precisely the ample ones.

Let us recall that the canonical sheaf on a smooth projective variety $\tilde{X}$ of dimension d is the sheaf associated to the canonical line bundle, i.e. the highest external power $\Lambda^d \Omega_{\tilde{X}}$, where $\Omega_{\tilde{X}}$ denotes the cotangent bundle. Given any non-zero rational section of the canonical line bundle, its divisor is a *canonical divisor*. In other words, a divisor K is a canonical divisor if its associated sheaf $\mathcal{O}(K)$ is isomorphic to the canonical sheaf. Hence the canonical divisors form a unique class under the linear equivalence relation.

We can now formulate Vojta's conjecture, which is a generalization of previous conjectures by Bombieri and Lang. Our version below is a particular case of the Main Conjecture in [55]:

Vojta's Conjecture. *Let $\tilde{X}$ be a smooth projective algebraic variety defined over a number field κ; let K be a canonical divisor on $\tilde{X}$ and let D be a reduced effective divisor, with normal crossing singularities (if any). Suppose that $K+D$ is big. Then, for every ring of S-integers $\mathcal{O}_S \subset \kappa$, the S-integral points on $X := \tilde{X} \setminus D$ are not Zariski-dense.*

We shall also say that a variety $X = \tilde{X} \setminus D$, where $\tilde{X}$ is complete and smooth and D is a normal crossing singularity divisor, is of log-general type whenever $K + D$ is ample, K being as above a canonical divisor. It turns out that such a property does not depend on the smooth compactification $\tilde{X}$ of X, provided that the complement $D = \tilde{X} \setminus X$ has only normal crossing singularities.

The particular case where D is empty (i.e. the zero divisor) concerns rational points; in that case Vojta's conjecture asserts that rational points on varieties of general type are not Zariski-dense. In the case of curves, this assertion is Mordell's conjecture, proved by Faltings [29]. In the case of complete surfaces, the conjecture was formulated by Bombieri in 1980, and is still an open problem. A function field analogue of Bombieri's conjecture has been settled by Noguchi [41].

Let us analyze in detail the case of curves. Let $\tilde{\mathcal{C}}$ be a complete curve, and let $D_1, \ldots, D_r$ be distinct points of $\tilde{\mathcal{C}}$, where the integer r might be zero. Put $D = D_1 + \ldots + D_r$, and view D both as a divisor of degree r and a finite set of cardinality r. The complement $\mathcal{C} := \tilde{\mathcal{C}} \setminus D$ is then an affine curve, unless $r = 0$. Consider the set $\mathcal{C}(\mathcal{O}_S)$, which coincides with $\tilde{\mathcal{C}}(\kappa)$ if $r = 0$. Denoting by g the genus of $\tilde{\mathcal{C}}$, every canonical divisor turns out to have degree $2g - 2$, so $K + D$ will be big in all cases but

- $\mathcal{C} = \tilde{\mathcal{C}} \simeq \mathbb{P}_1$
- $\mathcal{C} \simeq \mathbb{A}^1$
- $\mathcal{C} \simeq \mathbb{G}_m$
- $\mathcal{C} = \tilde{\mathcal{C}}$ is an elliptic curve.

In all such cases, $\mathcal{C}(\mathcal{O}_S)$ is infinite, provided we allow a finite extension of the number field κ and possibly of the set of places S. In contrast, $K + D$ is ample, so big, in the following cases:

- $\mathcal{C}$ is rational with at least three points at infinity;
- $\mathcal{C}$ has genus one and is affine;
- $\mathcal{C}$ has genus at least two.

In the first two cases, the finiteness of S-integral points is the famous theorem of Siegel and Mahler. In the last case, as mentioned, the finiteness of rational points was conjectured by Mordell and proved by Faltings. Dimension one, however, is the only dimension in which the conjecture is settled; also, our discussion proves that the formulation is sharp, i.e. the condition on the bigness of $K + D$ cannot be weakened.

Let us analyze more in detail the case where $\mathcal{C}$ is rational with three points at infinity, so we can suppose $\mathcal{C} = \mathbb{P}_1 \setminus \{0, 1, \infty\}$. Its ring of regular functions can be written as

$$\mathcal{O}_S[\mathcal{C}] = \mathcal{O}_S[\mathbb{P}_1 \setminus \{0, 1, \infty\}] = \mathcal{O}_S\left[x, \frac{1}{x}, \frac{1}{1-x}\right].$$

So the integral points correspond to specializations of the variable x to an S-integer u such that its inverse is also S-integer and $(1-u)^{-1}$ is still an S-integer. In other words, u is a unit in $\mathcal{O}_S^*$ and $v := 1 - u$ is a unit. We then obtain the so called *S-unit equation* in two variables

$$u + v = 1.$$

A theorem of Siegel and Mahler asserts that such an equation has only finitely many solutions $(u, v) \in (\mathcal{O}_S^*)^2$. A natural generalization to several variables is provided by Theorem 1.2.4 (see also Theorem 1.2.2).

In higher dimension, the conjecture of Lang-Vojta is largely open. We dispose however of a very general theorem proved by Faltings and Vojta. Before stating it, recall that a semi-abelian variety is a connected commutative algebraic group containing no unipotent subgroups. It can always be realized as an extension of an abelian variety (i.e. an algebraic group which is an irreducible projective variety) by a linear torus (i.e. a power of $\mathbb{G}_m$); in other words, it sits in the middle of an exact sequence

$$0 \to \mathbb{G}_m^n \to G \to A \to 0,$$

where A is an abelian variety.

Theorem 1.2.1 (Faltings-Vojta's Theorem)**.** *Let G be a semi-abelian variety, embedded in a projective space, $Y \subset G$ a closed algebraic subvariety, all defined over a number field κ. Then the Zariski-closure of the set $Y(\mathcal{O}_S)$ of integral points of Y is a finite union of translates of subgroups of G lying in Y.*

In the case $\tilde{\mathcal{C}}$ is a complete curve of genus ≥ 2, one can view $\tilde{\mathcal{C}}$ embedded into its Jacobian G, which is an abelian variety. Since the only translates of subgroups contained in $\tilde{\mathcal{C}}$ are points, the above Theorem 1.2.1 implies finiteness of rational points on $\tilde{\mathcal{C}}$, which constitutes Faltings' theorem.

On the other extreme, consider the case where G is a linear group, so $G = \mathbb{G}_m^n$ is a torus. We then have

Theorem 1.2.2. *Let $Y \subset \mathbb{G}_m^n$ be an algebraic subvariety of a linear torus $\mathbb{G}_m^n$. The Zariski-closure of the set of points of Y whose coordinates are S-units is the union of finitely many translates of subtori contained in Y.*

Let us see some special cases of Vojta's conjecture in dimension two. We consider those affine algebraic surfaces admitting a compactification which is isomorphic to the projective plane $\mathbb{P}_2$. We can then start from the complete surface $\tilde{X} = \mathbb{P}_2$ and remove some curves (i.e. reduced effective divisors) from it in order to satisfy the condition in Vojta's conjecture.

Since the canonical divisor of $\mathbb{P}_2$ is in the class of $-3\cdot$(line), the condition on a curve D on $\mathbb{P}_2$, for the sum $D + K$ being big, becomes: $\deg D \geq 4$. So, Vojta's conjecture asserts the degeneration of integral points on the complement of a curve of degree at least 4, having only normal crossing singularities.

Suppose that $F(X, Y, Z) = 0$ is an equation for the curve D, where $F(X, Y, Z) \in \mathcal{O}_S[X, Y, Z]$ is a homogeneous polynomial without multiple factors. After enlarging if necessary S so to obtain a P.I.D. we can ensure that the coefficients of F generate the unit ideal; also, every point $(x : y : z) \in \mathbb{P}_2(\kappa)$ can be written with coprime coordinates in $\mathcal{O}_S$. Then the integrality condition on the point $(x : y : z)$, written with coprime $\mathcal{O}_S$-integral coordinates, becomes

$$F(x, y, z) \in \mathcal{O}_S^*.$$

Let us consider the very special case of a configuration of four lines in general position on the plane. We can reduce (again after possibly enlarging the field of definition) to the lines $X = 0$, $Y = 0$, $Z = 0$, $X + Y - Z = 0$. The integral points on the complement are parametrized by triples $(x, y, z) \in \mathcal{O}_S^3$ of coprime S-units such that $xyz(x + y - z) \in \mathcal{O}_S^*$; such triples must be taken up to multiplicative constants. Since the elements $x, y, z, (x + y - z)$ are all S-integers and their product is a unit, each factor must be a unit. Then, dividing by the unit z^4 and putting $u := x/z$, $v := y/z$, the integrality condition is expressed by u, v being units and the sum $u+v-1$ being also a unit. Putting $w := 1-u-v$ we obtain the S-unit equation

$$u + v + w = 1. \tag{1.2.3}$$

Recall that Vojta's conjecture would assert the degeneracy of integral points on the complement of the four given lines in the plane; in term of the above equation, this means that the triples $(u, v, w) \in (\mathcal{O}_S^*)^3$ satisfying equation (1.2.3) are not Zariski-dense. This is known, and actually a more precise result has been proved:

Theorem 1.2.4 (S-unit equation Theorem)**.** *Let $\Gamma \subset \mathbb{C}^*$ be a finitely generated multiplicative group. Let $n \geq 2$ be an integer. For all but finitely many solutions $(x_1, \ldots, x_n) \in \Gamma^n$ to the equation*

$$x_1 + \ldots + x_n = 1 \tag{1.2.5}$$

there exists a non-empty subset $I \subset \{1, \ldots, n\}$ such that $\sum_{i \in I} x_i = 0$.

In the situation of our equation $u+v+w = 1$, we obtain that all but finitely many solutions belong to one of the families $(t, -t, 1), (1, t, -t), (t, 1, -t)$ for some unit $t \in \mathcal{O}_S^*$. Geometrically, this means that all but finitely many integral points on the complement of the said configuration of lines belong to one of the three lines of equation $X + Y = 0$, $Y - Z = 0$ or $X - Z = 0$. These lines are characterized by the fact that they cross the configuration of the previous four lines in just two points.

In the general situation of n variables, let us note that the above equation (1.2.5) defines a hypersurface of the torus $\mathbb{G}_m^n$, which is not a subgroup (in the multiplicative sense), nor a translate of a subgroup. Then Theorem 1.2.2 applies; the conclusion of Theorem 1.2.4 is a bit more precise, because it gives a complete description of the possible infinite families of solutions, corresponding to positive dimension subtori contained in Y.

The second natural case to consider is the case of the union of a conic and two lines, in general position. In this case, we do not have just one choice, up to projective automorphisms, but a 1-dimensional moduli space of such configurations.

Up to change of coordinates, we can suppose that D (i.e. the union of a conic and two lines in general position) is given by the equation

$$ZX(Y^2 - X^2 - aXZ - bZ^2) = 0,$$

for scalars $a, b \in \kappa$. So we are looking for points $(X : Y : Z) \in \mathbb{P}_2$ such that $ZX(Y^2 - X^2 - aXZ - bZ^2) \in \mathcal{O}_S^*$. Again, dividing out by Z^4 and putting $u := X/Z, y := Y/Z$ we obtain that the integral points correspond to pairs $(u, y) \in \mathcal{O}_S^* \times \mathcal{O}_S$ such that $y^2 - u^2 - au - b =: v$ is a unit. We then arrive at the equation

$$y^2 = u^2 + au + b + v.$$

Vojta's conjecture would imply the degeneracy of solutions. Consider the very special case where $a = 0$, $b = 1$ and $\mathcal{O}_S \supset \mathbb{Z}[\sqrt{2}, \frac{1}{6}]$. The numbers of the form $\pm 2^{m/2} \cdot 3^n$, with $m, n \in \mathbb{Z}$, are units. In particular, we could have $u = 2^{m/2}, v = 3^n$ for positive m, n. Then Vojta's conjecture implies the following: for every number field κ, all but finitely many solutions $(y, m, n) \in \kappa \times \mathbb{N} \times \mathbb{N}$ to the simple-looking Diophantine equation

$$y^2 = 2^m + 3^n + 1$$

satisfy another non-trivial algebraic equation of the form $f(y, 2^m, 3^n) = 0$, independent of the above one. Here $f(Y, U, V) \in \kappa[Y, U, V]$ is a non-zero polynomial, not multiple of $Y^2 - U^2 - V - 1$. But now, it is easy to see that no infinite degenerate family of solutions can exist for the above equation, so Vojta's conjecture would imply unconditional finiteness. This is however an open problem; a solution in the particular case $\kappa = \mathbb{Q}$ has been recently provided by Leitner using *ad hoc* congruence methods [36].

So, even the simple case of a curve of degree four and three components remains open. Note, however, that its analogues over function fields [20], and in Nevanlinna theory [44] have now been settled.

In the case the curve D has fewer components, the problem becomes even more difficult. No case is known when D is an irreducible curve with normal crossing singularities, although some cases are solved when D is highly singular, after works of Faltings [31] and Zannier [61] (see also [37]).

Let us analyze more in detail the problems arising from the case D is smooth and irreducible. Recall that if such a curve D is defined by the homogenous equation $F(X, Y, Z) = 0$ of degree at least 4, the conclusion of Vojta's conjecture would be the degeneracy of points $(x : y : z) \in \mathbb{P}_2$ with $F(x, y, z) \in \mathcal{O}_S^*$, where the coordinates x, y, z must be chosen in $\mathcal{O}_S$. For instance Vojta's conjecture implies that for every $n \geq 4$ and every ring of S-integers $\mathcal{O}_S$, the triples of S-integers $(x, y, z) \in \mathcal{O}_S^3$ such that

$$x^n + y^n + z^n \in \mathcal{O}_S^*,$$

should not be Zariski-dense. This is still an open problem.

Let us see another explicit example about the complement of a smooth quartic in the plane. Consider the quartic curve

$$D: \; X^4 - 4X^2Y^2 + 4Y^4 + X^3Z + Z^4 = 0.$$

Letting $F(X, Y, Z) = X^4 - 4X^2Y^2 + 4Y^4 + X^3Z + Z^4 = (X^2 - 2Y^2)^2 + X^3Z + Z^4$, the S-integral points on $\mathbb{P}_2 \setminus D$ correspond to the solutions to $F(x, y, z) \in \mathcal{O}_S^*$ where $(x, y, z) \in \mathcal{O}_S^3$. In particular, whenever $F(x, y, z) = 1$, we produce such an integral point, namely $(x : y : z) \in \mathbb{P}_2(\kappa)$. We see at once an infinite family, obtained by taking $z = 0$ and reducing to the Pell's equation

$$x^2 - 2y^2 = \pm 1,$$

which admits infinitely many solutions already in the ring $\mathbb{Z}$ of rational integers. We can explain the geometric reason behind the presence of such an infinite family of solutions: the line of equation $Z = 0$ is a bi-tangent line for the curve D, so its intersection with D consists of just two points; removing these two points, we obtain an affine curve isomorphic to $\mathbb{G}_m$, hence having infinitely many S-integral points on a suitable ring of S-integers. In our case, we obtain infinitely many points already over the integers.

It is well-known that for every smooth quartic D there exist twenty-eight such bi-tangents (up to enlarging the field of definition) and twenty-four more lines which are tangent at an inflexion point; these lines too intersect the curve just at two points; so in general we will have at least fifty-two infinite families of integral solutions to the original equation $F(x, y, z) \in \mathcal{O}_S^*$.

We have seen that the integrality condition with respect to a curve in the projective plane can be expressed by a relation of the form $F(x, y, z) \in \mathcal{O}_S^*$, for a homogeneous polynomial $F(X, Y, Z) \in \mathcal{O}_S[X, Y, Z]$ of a certain degree d. Now, observe that the group $\mathcal{O}_S^*$ is finitely generated, by Dirichlet's theorem, so there exist only finitely many classes modulo perfect d-th powers. This implies that all units become perfect d-th powers in a fixed finite extension of the number field κ. Now, if for some integers $x, y, z \in \mathcal{O}_S$, we have that $F(x, y, z)$ is a unit and a perfect d-th power, we write $F(x, y, z) = u^d$ for some unit $u \in \mathcal{O}_S^*$; dividing x, y, z by u we obtain a solution to the equation $F(x, y, z) = 1$. Now, suppose that the "equation" $F(x, y, z) \in \mathcal{O}_S^*$ has a Zariski-dense set of solutions $(x, y, z) \in \mathcal{O}_S^3$. Then, by our discussion the equation $F(x, y, z) = 1$ will also have a Zariski-dense set of solutions, after enlarging the number field κ if necessary.

So it is reasonable to compare the affine surface $\mathcal{S} \subset \mathbb{A}^3$ of equation

$$\mathcal{S} : \quad F(x, y, z) = 1$$

with the complement $\mathbb{P}_2 \setminus D$, where D is the smooth curve of equation

$$D : F(X, Y, Z) = 0.$$

It turns out that these surfaces are strongly related. First, the surface $\mathcal{S}$ is of log general type if and only if $\mathbb{P}_2 \setminus D$ is so, which occurs if and only if $d = \deg F \geq 4$. For instance, the degeneracy of integral solutions to the equation $x^n + y^n + z^n = 1$ for $n \geq 4$ would follow both from applying Vojta's conjecture to the surface given by the same equation, and by applying the same Vojta's conjecture to the open set of $\mathbb{P}_2$ defined by $X^n + Y^n + Z^n \neq 0$. A second link between the two surfaces is provided by the fact that the map

$$\mathcal{S} \ni (x, y, z) \mapsto (x : y : z) \in \mathbb{P}_2 \setminus D$$

is an étale cover of degree $d = \deg F$. Actually, it is a cyclic cover, since multiplication of (x, y, z) by d-th roots of unity operates on $\mathcal{S}$ without changing the projective class of the point $(x : y : z)$. We shall see in the next paragraph that the Chevalley-Weil theorem provides the geometric formulation and natural generalization for this kind of phenomena.

Another remark about integral points on the complement of a curve D in the plane: we have seen that the problem simplifies if D is sufficiently reducible. For instance, the problem is solved whenever D has at least four components. This fact can be explained geometrically, in view specially of the above general theorem of Faltings-Vojta (Theorem 1.2.1).

Let $F_1, \ldots, F_r \in \mathcal{O}_S[X, Y, Z]$ be pairwise non proportional irreducible forms and let D be the curve of equation $\prod_{i=1}^r F_i(X, Y, Z) = 0$. It has r irreducible components. Letting $d_i = \deg F_i$ and d be a common multiple of the d_i, consider the map $(\mathbb{P}_2 \setminus D) \to \mathbb{G}_m^{r-1}$ sending

$$(\mathbb{P}_2 \setminus D) \ni (x : y : z) \mapsto \left(\frac{F_1^{d/d_1}(x, y, z)}{F_r^{d/d_r}(x, y, z)}, \ldots, \frac{F_{r-1}^{d/d_{r-1}}(x, y, z)}{F_r^{d/d_r}(x, y, z)} \right) \in \mathbb{G}_m^{r-1} .$$

If two of the functions $F_i^{d/d_i}/F_r^{d/d_r}$ are algebraically independent, the image of $\mathbb{P}_2 \setminus D$ is a surface $Y \subset \mathbb{G}_m^{r-1}$; the integral points of $\mathbb{P}_2 \setminus D$ are sent to points with S-unit coordinates, so points of $Y \cap \mathbb{G}_m^{r-1}(\mathcal{O}_S)$. If $r \geq 4$, Y is a proper subvariety of $\mathbb{G}_m^{r-1}$. Hence, if Y is not the translate of a subtorus, which happens only when the homogeneous forms F_i satisfy multiplicative dependence relations, by Theorem 1.2.2 the integral points on Y are degenerate. But then the S-integral points on $\mathbb{P}_2 \setminus D$ will also be degenerate.

However, when $r \leq 3$, and the irreducible components of D are smooth curves intersecting properly, it can be shown that there exists no dominant map $(\mathbb{P}_2 \setminus D) \to Y$ to any proper subvariety Y of a torus, not itself a torus; so Theorem 1.2.2 cannot apply.

Although our main concern will be integral points on affine varieties, let us pursue some speculations also about rational points. As we said, the case of curves is settled by Faltings' theorem, while the case of surfaces remains largely open. For smooth hypersurfaces of $\mathbb{P}_3$, the condition of being of general type amounts to having degree at least five. Those of lower degree are either rational (over $\mathbb{C}$) whenever their degree is $1, 2$ or 3, or K3 surfaces, if their degree is 4. Clearly, rational surfaces have a Zariski-dense set of rational points, provided we enlarge their field of definition so to become rational over the enlarged field; many cases are known of K3 surfaces with a Zariski dense set of rational points. Bombieri's conjecture, i.e. Vojta's conjecture for rational points on complete surfaces, asserts that these are the only cases of smooth surfaces in $\mathbb{P}_3$ admitting a Zariski-dense set of rational points.

One of the most popularly known anecdotes about Ramanujan concerns his remark that the number 1729 is the smallest positive integer which can be written in two different ways as a sum of two cubes:

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

There are infinitely many such numbers, nowadays called “taxicab numbers”: they arise from the solutions in positive integers to the homogeneous Diophantine equation

$$X^3 + Y^3 = Z^3 + W^3$$

which moreover satisfy $(X, Y) \neq (Z, W)$ and $(X, Y) \neq (W, Z)$. Clearly, starting from one solution, we can produce infinitely many others by multiplying X, Y, Z, W by a same number; so we will be interested in *projective solutions* $(X : Y : Z : W) \in \mathbb{P}_3(\mathbb{Q})$. Now, the projective surface defined by the above equation is rational over $\mathbb{Q}$, and it is easy to construct a Zariski-dense set of rational points; also, it is possible to find a Zariski-dense set of such points with positive coordinates. The fact that such a set is Zariski dense implies in particular that it is not contained in the two lines of equation $X - Z = 0 = Y - W$ and $X - W = 0 = Y - Z$, so they really give rise to taxicab numbers.

One can consider the analogue problem for $n = 4$. The K3 surface defined in $\mathbb{P}_3$ by the equation $X^4 + Y^4 = Z^4 + W^4$ is also known to have a Zariski-dense set of rational points [1]; so in particular, infinitely many rational points lie outside the two mentioned “uninteresting” lines. However, for every $n \geq 5$, according to the Bombieri-Vojta conjecture the set of rational points should be degenerate, i.e. the rational points should accumulate on a finite union of curves of geometric genus ≤ 1, apart finitely many exceptions. Moreover, for large values of n, it can be proved theat the only curves of genus ≤ 1 on the corresponding surface are the trivial lines; therefore, there should exist only finitely many ‘taxicab numbers’ of any such exponent n, up to multiplication by n-th powers.

1.3 Behaviour of integral points under morphisms

Let X_1, X_2 be quasi projective algebraic varieties defined over a number field κ, and let $\pi : X_1 \to X_2$ be a morphism defined over κ. We can find projective completions $\tilde{X_1}, \tilde{X_2}$, and divisors D_i on $\tilde{X_i}$ such that $X_i = \tilde{X_i} \setminus D_i$ and the morphism π can be continued to a morphism, still denoted by $\pi : \tilde{X_1} \to \tilde{X_2}$ such that $\pi^{-1}(D_2) = D_1$. We can cover X_1 by a finite family of affine open sets $U_\alpha \subset X_1$ which are isomorphic to closed subsets of an affine space $\mathbb{A}^n$. Let us choose local coordinates such that each S-integral point of X_1 will have

[1] this quartic surface contains eight lines defined over $\mathbb{Q}$. Starting e.g. from the line r of equation $X = Z, Y = W$, we obtain an elliptic fibration as follows: consider the pencil of planes containing r; each plane intersects the surface on the line r and a cubic curve, which is smooth for all but finitely many such planes (precisely, there are nine exceptions); each such plane intersects the line $X = -Z, Y = -W$ at a single point P and the line $X = W, Y = -Z$ at a point Q. These points P and Q, depending on the plane, i.e. on a parameter lying on $\mathbb{P}_1$, provide two sections of this elliptic fibration. Taking Q to be the origin, one can verify that P is not identically torsion with respect to Q; then one obtains infinitely many rational points on all but finitely many fibers. The details are given in [54].

S-integral coordinates. Locally on each U_α the morphism π can be written in polynomial coordinates

$$\pi(t_1, \ldots, t_n) = (p_{1,\alpha}(t_1, \ldots, t_n), \ldots, p_{k,\alpha}(t_1, \ldots, t_n)),$$

where for every $(t_1, \ldots, t_n) \in U_\alpha$, the point $\pi(t_1, \ldots, t_n)$ lies in X_2. The polynomials $p_j(T_1, \ldots, T_n)$ have their coefficients in the number field κ. Due to the fact that the covering $\{U_\alpha\}$ of X_1 is finite, we have only finitely many polynomials to consider, so after enlarging S if necessary, they will all have S-integral coefficients. Then the image of the set of S-integral points on X_1 will be formed by S-integral points on X_2. This in particular implies that if π is dominant and the S-integral points on X_1 are Zariski-dense, the set $X_2(\mathcal{O}_S)$ will also be Zariski-dense, possibly after enlargement of the set S. Or, viewed in the other direction, if $X_2(\mathcal{O}_S)$ is never Zariski-dense, for any ring of S-integers $\mathcal{O}_S$, then $X_1(\mathcal{O}_S)$ too will be always degenerate.

This is consistent with Vojta's conjecture; actually if a smooth variety X_2 is of log-general type and is dominated by a variety X_1 via a generically finite morphism, then the variety X_1 will also be of log-general type.

The above discussion shows that in general, given a generically finite morphism $X_1 \to X_2$, proving degeneracy of integral points on the dominating variety X_1 will be easier than proving it for X_2; actually it can happen that X_2 does not satisfy the hypotheses, nor the conclusion, of Vojta's conjecture, while X_1 does: for instance, every variety dominates a projective space of the same dimension, where the rational points are Zariski-dense.

There exists, however, a case when the Zariski-density of integral points on one variety, over 'sufficiently large' rings of S-integers, is *equivalent* to the Zariski-density of integral points on the other one. It is the case of unramified covers, and is the content of the so-called Chevalley-Weil theorem below, which we formulate in two different ways, restricting for simplicity to the case of curves:

Theorem 1.3.1 (Chevalley-Weil, first version). *Let κ be a number field, $\mathcal{C}_1, \mathcal{C}_2$ be smooth (affine or projective) absolutely irreducible curves defined over κ, $\pi : \mathcal{C}_1 \to \mathcal{C}_2$ an unramified cover. For every ring of S-integers $\mathcal{O}_S \subset \kappa$, there exists a number field κ' containing κ, a finite set of places S' of κ' containing all the places above those of S, such that every S-integral point $p \in \mathcal{C}_2(\mathcal{O}_S)$ admits at least one pre-image $p' \in \pi^{-1}(p)$ in the set $\mathcal{C}_1(\mathcal{O}_{S'})$.*

Here is the alternative formulation:

Theorem 1.3.2 (Chevalley-Weil, second version). *Let κ be a number field, S a finite set of places of κ containing the archimedean ones. Let $\mathcal{C}_1, \mathcal{C}_2$ be two smooth irreducible curves, defined over κ, $\pi : \mathcal{C}_1 \to \mathcal{C}_2$ be an unramified morphism. There exists a finite set of places S' of κ containing S, and finitely many irreducible curves $\mathcal{C}_1^{(1)}, \ldots, \mathcal{C}_1^{(n)}$, and maps $\pi_i : \mathcal{C}_1^{(i)} \to \mathcal{C}_2$, all defined over κ, such that*

(i) *for each* $1 < i < j \leq n$ *there exists an isomorphism* $\psi_{i,j} : \mathcal{C}_1^{(i)} \to \mathcal{C}_1^{(j)}$, *defined over* $\bar{\kappa}$, *with* $\pi_j \circ \psi_{i,j} = \pi_i$.

(ii) *for each* S*-integral point* $p \in \mathcal{C}_2(\mathcal{O}_S)$, *there exists an index* $i \in \{1, \ldots, n\}$ *such that* $\pi_i^{-1}(p)$ *contains an* S'*-integral point.*

We recall that whenever $\mathcal{C}$ is complete, S-integral points are just rational points. So, in that case, Theorems 1.3.1 and 1.3.2 apply to all κ-rational points.

Let us first see concrete instances of Chevalley-Weil theorem, admitting easy proofs.

`Example 1`. Consider the affine curves $\mathcal{C}_1 = \mathcal{C}_2 = \mathbb{G}_m$ and the unramified morphism $x \mapsto x^n$, for some integer $n \geq 1$. We have seen that the integral points on $\mathbb{G}_m$ are the units. So $\mathcal{C}_2(\mathcal{O}_S) = \mathbb{G}_m(\mathcal{O}_S) = \mathcal{O}_S^*$. Now, Dirichlet's finiteness generation theorem asserts that the group of S-units is finitely generated, being the direct product of a finite group and a free abelian group of rank equal to $\sharp(S) - 1$. Then the quotient of $\mathcal{O}_S^*$ modulo its subgroup of n-th powers is finite. Adding to κ the n-th roots of the elements of a complete set of representatives for the quotient defines a finite extension of κ, so a number field κ'. Then each integral point in $\mathcal{C}_2(\mathcal{O}_S)$ will have its pre-images in $\mathcal{C}_1(\kappa')$ (and the integrality is preserved).

`Example 2`. Consider the elliptic curve $\mathcal{C}_2 \subset \mathbb{P}_2$ defined by the homogeneous equation

$$ZY^2 = X(X - Z)(X + 6Z)$$

It has positive rank over $\mathbb{Q}$, since its point $(2 : 4 : 1)$ has infinite order, after taking the point $(0 : 1 : 0)$ as the origin for the group law. Using affine coordinates $x := X/Z, y := Y/Z$, the equation takes the form

$$y^2 = x(x - 1)(x + 6).$$

Suppose now to have a rational point $(x, y) \in \mathbb{Q}^2$ satisfying the above equation, with $y \neq 0$; writing $x = a/b$ for coprime integers a, b, with $b > 0$, we obtain that the rational number

$$\frac{a}{b}\left(\frac{a}{b} - 1\right)\left(\frac{a}{b} + 6\right) = \frac{a(a - b)(a + 6b)}{b^3}$$

must be a square in $\mathbb{Q}$. Clearly, the above fraction is reduced, so both the denominator b^3 and the numerator $a(a - b)(a + 6b)$ must be squares. Now, since a, b are coprime, $a, a - b$ are also coprime; as to a and $a + 6b$, we see immediately that they are either coprime, or their greatest common divisor is $2, 3$ or 6. So, every prime dividing a, with the possible exception of the primes 2 and 3, appears in the factorization of a with even multiplicity. Then a is a square in the number field $\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$, and so is $x = a/b$ (recall that b is a square already in $\mathbb{Q}$, since b^3 is a square).

Let now $\mathcal{C}_1$ be the smooth projective model of the affine algebraic curve defined in $\mathbb{A}^3$ by the system

$$\mathcal{C}_1 : \begin{cases} y^2 = x\,(x-1)\,(x+6) \\ u^2 = x \end{cases}$$

which is naturally endowed with a projection $\pi : \mathcal{C}_1 \to \mathcal{C}_2$, corresponding to the field extension $\mathbb{Q}(\mathcal{C}_2)(\sqrt{x})/\mathbb{Q}(\mathcal{C}_2)$.

The above argument shows that each rational point $P \in \mathcal{C}_2(\mathbb{Q})$ has a pre-image in $\mathcal{C}_1(\bar{\mathbb{Q}})$ which is defined over the number field $\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$, so the conclusion of Theorem 1.3.1 is verified.

Let us now see how to construct the curves $\mathcal{C}_1^{(i)}$ and the map $\pi_i : \mathcal{C}_1^{(i)} \to \mathcal{C}_2$ as in Theorem 1.3.2. The three rational numbers $-1, 2, 3$ generate a multiplicative group of order 8 modulo rational squares; let $\{\epsilon_1, \ldots, \epsilon_8\}$ be representative for the quotient group. Define, for $i = 1, \ldots, 8$, the curve $\mathcal{C}_1^{(i)}$ to be the smooth projective model of the affine curve given by the equation

$$\mathcal{C}_1^{(i)} : \begin{cases} y^2 = x(x-1)(x+6) \\ u^2 = \qquad \epsilon_i x \end{cases}.$$

We call it a twisted form of the curve $\mathcal{C}_1$ defined above; it turns out to be isomorphic to $\mathcal{C}_1$ over the field of algebraic numbers, but not over $\mathbb{Q}$ which is a field of definition for each $\mathcal{C}_1^{(i)}$ and for $\mathcal{C}_1$. We also define $\pi_i : \mathcal{C}_1^{(i)} \to \mathcal{C}_2$ as before, by sending $(u, x, y) \mapsto (x, y)$.

What we proved about the arithmetic of the rational points on $\mathcal{C}_2$ can be rephrased by saying that for each rational point $P \in \mathcal{C}_2$ there exists an index $i \in \{1, \ldots, 8\}$ such that $\pi_i^{-1}(P)$ is formed by rational points of $\mathcal{C}_1$ (now it is meant rational over $\mathbb{Q}$). This is the conclusion of Theorem 1.3.2.

To finish the discussion of this example, let us see that the hypothesis of the Chevalley-Weil theorem is satisfied, namely the covering map $\pi : \mathcal{C}_1 \to \mathcal{C}_2$ between the two complex curves in question is unramified. Since the field extension $\mathbb{C}(\mathcal{C}_1)/\pi^*(\mathbb{C}(\mathcal{C}_2)) = \mathbb{C}(\mathcal{C}_2)(\sqrt{x})/\mathbb{C}(\mathcal{C}_2)$ is obtained by adding the square-root of the rational function x, the possible ramification can arise only over the zeros and poles of x. Proving that in fact there is no ramification amounts to showing that the rational function $x \in \mathbb{C}(\mathcal{C}_2)$ is locally a square everywhere, i.e. all its poles and zeros have even multiplicity. Now, the only pole of x is the point at infinity $(0 : 1 : 0)$, and has multiplicity two, while its only zero is the point $(0 : 0 : 1)$, which is a double-zero.

We now provide an elementary proof of the (first version of) Chevalley-Weil's theorem in the particular case of cyclic covers. In the sequel, we will just need this particular case; actually, we could (but we will not) restrict our attention to the degree two-covers.

We start with some preliminaries on cyclic covers of algebraic curves, which have an independent interest.

Over the complex numbers, we have the following result:

Theorem 1.3.3. *Given a smooth complex projective algebraic curve $\tilde{\mathcal{C}}$ over the field $\mathbb{C}$ of complex numbers, the isomorphism classes of degree two unramified covers $Y \to \tilde{\mathcal{C}}$ are in natural bijection with the following sets:*

(i) $\mathrm{H}^1(\tilde{\mathcal{C}}, \mathbb{Z}/2\mathbb{Z})$*;*
(ii) *the points of* 2*-torsion in the Jacobian of* $\tilde{\mathcal{C}}$*;*
(iii) *the quotient of the multiplicative group* $\{f \in \mathbb{C}(\tilde{\mathcal{C}})^* : \mathrm{ord}_p(f) \equiv 0 \pmod 2 \, \forall p \in \tilde{\mathcal{C}}\}$ *by the group of squares in* $\mathbb{C}(\tilde{\mathcal{C}})^*$*.*

In particular, there are exactly 2^g *isomorphism classes of such covers, where* g *is the genus of the curve.*

Let us rapidly describe such a correspondence. Given a cohomology class in the Čech cohomology group $\mathrm{H}^1(\tilde{\mathcal{C}}, \mathbb{Z}/2\mathbb{Z})$, one can form the topological cover $Y \to \tilde{\mathcal{C}}(\mathbb{C})$ associated to it; it is trivial (i.e. disconnected) if and only if the cohomology class is zero. Now Y can be endowed with a unique complex structure such that the map $Y \to \tilde{\mathcal{C}}$ becomes holomorphic. Being a compact Riemann surface, it is also algebraic and so we obtain a cover in the category of complex algebraic curves.

Starting from a rational function $f \in \mathbb{C}(\tilde{\mathcal{C}})^*$ satisfying the condition

$$\mathrm{ord}_p(f) \equiv 0 \pmod 2 \qquad \forall p \in \tilde{\mathcal{C}},$$

which amounts to saying that f is a square locally everywhere, we can construct the extension $\mathbb{C}(\tilde{\mathcal{C}})(\sqrt{f})/\mathbb{C}(\tilde{\mathcal{C}})$, which is actually a field if and only if f is not (globally) a square. In that case, it corresponds to an irreducible algebraic curve Y endowed with a degree-two morphism $Y \to \tilde{\mathcal{C}}$ (while if f is a square in $\mathbb{C}(\tilde{\mathcal{C}})$, then $\mathbb{C}(\tilde{\mathcal{C}})(\sqrt{f}) \simeq \mathbb{C}(\tilde{\mathcal{C}}) \times \mathbb{C}(\tilde{\mathcal{C}})$).

Finally, a point of 2-torsion in the Jacobian $J(\tilde{\mathcal{C}})$ corresponds to a divisor D on $\tilde{\mathcal{C}}$ of degree 0 such that $2D = (f)$ is principal. Then f is a square locally everywhere, but is not a square globally unless D itself is principal.

We can generalize the above discussion as follows. Let us fix a prime number l. Let $\mathcal{C}$ be a smooth irreducible algebraic curve, defined over a field κ, of characteristic $\neq l$, which contains all the l-th roots of unity. Then every degree l cyclic cover of $\mathcal{C}$ will be of the form $\pi : \mathcal{C}' \to \mathcal{C}$, where the function field $\kappa(\mathcal{C}')$ can be obtained as $\kappa(\mathcal{C})(\sqrt[n]{f})$, for a suitable rational function $f \in k(\mathcal{C})$, not a perfect l-th power in $k(\mathcal{C})$. Such a cover is unramified if and only if all the zeros and poles of f appear with multiplicity divisible by l. Hence the correspondence between the cyclic unramified covers of degree l and the quotient group $\{f \in \kappa(\tilde{\mathcal{C}})^* : \mathrm{ord}_p(f) \equiv 0 \pmod l \, \forall p \in \tilde{\mathcal{C}}\}$ still holds; however, two covers can be "geometrically" isomorphic without being isomorphic over κ. For instance, multiplying f by a non-zero constant which is not a perfect l-th power in κ changes the κ-isomorphism class of the associated cover.

Let us now consider affine curves. Eliminating points from a complete curve "increases" the fundamental group, so we expect the existence of more unramified covers; precisely, given a complete curve $\tilde{\mathcal{C}}$, a finite set $D \subset \tilde{\mathcal{C}}$, all the covers of $\tilde{\mathcal{C}}$ which ramify only over D give rise to unramified covers of $\tilde{\mathcal{C}} \setminus D$.

The natural analogue of Theorem 1.3.3 holds in the affine case too:

Theorem 1.3.4. *Let $\mathcal{C} = \tilde{\mathcal{C}} \setminus D$ be an affine algebraic curve, where $\tilde{\mathcal{C}}$ is smooth and complete and $D \subset \tilde{\mathcal{C}}$ a finite set. There is a natural bijection between the following sets*

(i) *unramified cyclic covers $Y \to \mathcal{C}$;*
(ii) $\mathrm{H}^1(\mathcal{C}, \mathbb{Z}/2\mathbb{Z})$*;*
(iii) *the quotient of the multiplicative group $\{f \in \mathbb{C}(\tilde{\mathcal{C}})^* : \mathrm{ord}_p(f) \equiv 0 \pmod 2 \,\forall p \in \mathcal{C}\}$ by the group of squares in $\mathbb{C}(\tilde{\mathcal{C}})^*$.*

In particular, there exist exactly 2^{g+s-1} such covers, up to isomorphisms, where g is the genus of $\tilde{\mathcal{C}}$ and s is the cardinality of D.

One could even extend the correspondence by mentioning the 2-torsion points in the *generalized Jacobian* of the affine curve $\mathcal{C}$, which turns out to be an extension of the ordinary Jacobian $J(\tilde{\mathcal{C}})$ by a linear torus of dimension $s-1$.

We now proceed towards the proof of the Chevalley-Weil theorem. The first lemma is in a sense the arithmetic analogue of the finiteness of the isomorphism classes of cyclic unramified covers of given degree of a complex algebraic curve.

Lemma 1.3.5. *Let l be a prime number. Let κ be a number field containing the l-th roots of unity, S a finite set of places containing the archimedean ones. There exist only finitely many cyclic extensions of κ of degree l which are unramified outside S.*

Proof. We start by enlarging S to a finite set S' such that the ring of S'-integers is a P.I.D.. We shall prove that there are only finitely many cyclic extensions of given degree of κ unramified outside S', from which the Lemma clearly follows.

By Kummer theory, a degree l cyclic extension of κ will be of the form $\kappa(\sqrt[l]{a})$ where a is an element of κ^*, not a perfect l-th power. After multiplying a by non-zero perfect l-th powers, the field generated by $\sqrt[l]{a}$ does not change; hence we can suppose that a is an S'-integer; we can further suppose that all its divisors which are perfect l-th powers are units. If the field extension $\kappa(\sqrt[l]{a})/\kappa$ is unramified outside S' then a must be a S'-unit. Now, since the group of S'-units is finitely generated, its quotient modulo perfect l-th powers is finite. Hence we deduce the finiteness of such field extensions. □

Lemma 1.3.6. *Let, as before, κ be a number field. Let also $\tilde{\mathcal{C}}$ be a smooth irreducible projective curve defined over κ. Let $f \in \kappa(\mathcal{C})$ be a non-constant rational function having all its zeros and poles in $\tilde{\mathcal{C}}(\kappa)$. There exists a finite set of places S of κ, such that for every (ultrametric) place ν of κ, with $\nu \notin S$, the following holds: for every rational point $p \in \mathcal{C}(\kappa)$ with $\nu(f(p)) \neq 0$ there exists a point $q \in \mathcal{C}(\kappa)$, with $f(q) = 0$ or $f(q) = \infty$ and $p \equiv q \pmod \nu$. Moreover, if f has a zero (resp. a pole) of order h at q and $p \equiv q \pmod{\mathfrak{m}_\nu}^k$, $p \not\equiv q$, $\pmod{\mathfrak{m}_\nu}^{k+1}$, then $\nu(f(p)) = h \cdot k$.*

Proof. We view $\tilde{\mathcal{C}}$ as defined in a projective space by a given system of algebraic equations having integral coefficients in κ. Taking S sufficiently large, we can suppose that the reduction modulo every place ν outside S of such polynomials still defines a smooth irreducible curve over the residue field $\kappa(\nu)$; we denote by $\tilde{\mathcal{C}}_\nu$ this curve, which is defined over $\kappa(\nu)$.

Also, we can write f as the restriction to $\tilde{\mathcal{C}}$ of a given rational function in the coordinates of the ambient space; still after enlarging S, we can suppose that such rational function is well defined and separable modulo every place $\nu \notin S$; we denote by $f_\nu \in \kappa(\nu)(\tilde{\mathcal{C}}_\nu)$ the rational function defined on the reduced curve $\tilde{\mathcal{C}}_\nu$ obtained in this way.

After further enlarging S if necessary, the reductions modulo every place $\nu \notin S$ of the (rational) zeros and poles of f in $\mathcal{C}$ will be all distinct. Then, by Riemann-Hurwitz formula, it follows that f_ν cannot have other zeros nor poles, apart the reduction modulo ν of the zeros or poles of f on $\tilde{\mathcal{C}}$.

The proof is now easy. Whenever, for $p \in \mathcal{C}(\kappa)$, $\nu(f(p)) \neq 0$, the reduction modulo ν of p is a zero or a pole of f_ν, so by our discussion it must be congruent to a rational zero or pole of f.

The last sentence is easily proved by working on local coordinates. □

Proof of Theorem 1.3.2 in the case of cyclic covers. Let us consider first the case of covers of complete curves. Let $\tilde{\mathcal{C}_1} \to \tilde{\mathcal{C}_2}$ be a cyclic cover of degree l, defined over a number field κ. After enlarging the field of definition to a number field $\kappa' \supset \kappa$, we can view the function field extension $\kappa'(\tilde{\mathcal{C}_1})/\kappa'(\tilde{\mathcal{C}_2})$ as $\kappa'(\tilde{\mathcal{C}_2})(\sqrt[l]{f})$, where f is a rational function on $\tilde{\mathcal{C}_2}$ such that all its zeros and poles lie in $\tilde{\mathcal{C}_2}(\kappa')$ and have multiplicity divisible by l. Then define S as in the statement of Lemma 1.3.6. Enlarging κ' we can obtain a new number field, still denoted by κ', containing all the degree l extensions of κ unramified outside S; we can also suppose that it contains all the l-th roots of unity. Let now $p \in \kappa(\tilde{\mathcal{C}_2})$ be a κ-rational point on $\tilde{\mathcal{C}_2}$. Then each of the l pre-images of p in $\tilde{\mathcal{C}_1}$ are defined over $\kappa(\sqrt[l]{f(p)})$. By Lemma 1.3.6, this field is unramified outside S, so is contained in κ'.

The proof in the affine case is almost the same. One must use the hypothesis that the rational points in question are S-integral because there is no control of the multiplicity of the possible zeros and poles of the rational function f which lie at infinity. For this reason, we must consider only points which never reduce to points at infinity, for any ideal of $\mathcal{O}_S$. □

It is clear that our proof is in principle effective, in the sense that it enables to determine the field κ' and the set S' appearing in the statement. A completely explicit bound for the degree and discriminant of the field κ' has been recently provided in [7], actually in the more general case of arbitrary unramified covers, not necessarily cyclic.

Chapter 2
Diophantine approximation

2.1 Diophantine approximation on the line

In this short chapter we present without proof classical material about Diophantine approximation. More details and complete proofs can be found for instance in [50], [51], [8]. We are primarily interested in the rational approximation to algebraic numbers; more precisely, we are interested in estimating the accuracy in the approximation to such numbers with respect to the denominator of the approximant. The following theorem gives the best possible result for an arbitrary irrational number.

Theorem 2.1.1 (Dirichlet). *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be a real irrational number. There exist infinitely many rational numbers a/b (a, b coprime integers, $b > 0$) such that*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$

For instance, one can take for a/b the truncated continued fraction expansion of α.

Some irrational numbers can be approximated to a higher degree; for instance, Liouville's number $\alpha := \sum_{n=1}^{\infty} 10^{-n!}$ has the property that for every positive μ there exist infinitely many rationals a/b (a, b coprime integers, $b > 0$) such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^\mu}.$$

Such numbers are never algebraic; actually, a theorem of Liouville states that:

Theorem 2.1.2 (Liouville). *Let α be a real irrational algebraic number of degree d over $\mathbb{Q}$. There exists a positive number $c(\alpha)$ such that for all rational numbers a/b*

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{c(\alpha)}{b^d}.$$

P. Corvaja, *Integral Points on Algebraic Varieties*, HBA Lecture Notes in
Mathematics, DOI 10.1007/978-981-10-2648-5_2

A deeper theorem, due to Roth (1955) [47], improves on the exponent d:

Theorem 2.1.3 (Roth's Theorem). *Let α be a real algebraic number, $\epsilon > 0$. For all but finitely many rational numbers a/b, the following inequality holds:*

$$\left|\alpha - \frac{a}{b}\right| > \frac{1}{b^{2+\epsilon}}. \tag{2.1.4}$$

In an other formulation: if α is algebraic irrational, there exists a positive real number $c(\alpha, \epsilon)$ such that *for all* rational numbers a/b,

$$\left|\alpha - \frac{a}{b}\right| > \frac{c(\alpha, \epsilon)}{b^{2+\epsilon}}. \tag{2.1.5}$$

Roth's proof is ineffective, in the sense that it does not provide any means of finding the finitely many rational numbers a/b which violate the inequality (2.1.4). Looking at its second formulation, by the ineffective nature of Roth's proof it is not possible to calculate the function $c(\alpha, \epsilon)$.

Roth's theorem is best possible as far as the exponent is concerned in view of the mentioned result of Dirichlet (Theorem 2.1.1). However, one can try to improve on Roth's exponent after restricting the approximations to suitable classes of rational numbers. For instance, one can consider the set of rational numbers which, once written in base ten, have only finitely many digits. These numbers form the ring of S-integers $\mathbb{Z}[\frac{1}{10}] = \mathbb{Z}[\frac{1}{2}, \frac{1}{5}]$.

In that case, Ridout [45] improved Roth's bound by proving that: for every irrational algebraic number α and every positive real $\epsilon > 0$, there are only finitely many pairs of integers $(a, n) \in \mathbb{Z} \times \mathbb{N}$ such that $|\alpha - \frac{a}{10^n}| < 10^{-(1+\epsilon)n}$.

A similar result holds whenever the numerators of the approximations are supposed to be of special type, e.g. products of powers of primes from a fixed finite set. When both numerators and denominators are subject to lie in a finitely generated multiplicative semi-group, then the exponent can be lowered to "ϵ" (see Corollary 2.1.10).

In another direction, one can try to replace the rational number field $\mathbb{Q}$ by an arbitrary number field $\kappa \subset \mathbb{C}$. Of course, the expected exponent should change; for instance, if $\kappa \subset \mathbb{R}$ and has degree $d = [\kappa : \mathbb{Q}]$ over the rational, a variation of Dirichlet's theorem asserts that each real number $\alpha \in \mathbb{R} \setminus \kappa$ can be approximated to a degree $-2d$ with respect to the "height" of the approximant (see below for the precise definition of height).

Still another generalization concerns p-adic approximation: one can fix a p-adic algebraic number $\alpha \in \mathbb{Q}_p$ and study its approximations by rational numbers.

In order to find the most appropriate generalization, containing Roth's and Ridout's theorem and their natural extensions to number fields, we introduce the language of heights and revise the theory of absolute values in a number field.

Let κ be a number field. For every place ν of κ, the corresponding absolute values differ logarithmically by a positive constant: namely, if $|\cdot|_\nu$ and $\|\cdot\|_\nu$

are two equivalent absolute values of κ there exists a positive real number δ such that for every $x \in \kappa$, $|x|_\nu = \|x\|_\nu^\delta$. We are looking for a canonical normalization, which will simplify the notation in the formulation of results from Diophantine approximation. One natural choice would be simply to choose the ν-adic absolute values extending the natural ones already defined in the rational number field $\mathbb{Q}$. However, there is another possibility, which is less canonical since it depends on the number field κ, but has the advantage that by adopting this new convention, the generalization and extensions of Roth's theorem will be easier to state. We proceed to define this second normalization.

Let then ν be a place of κ; the completion κ_ν, which is independent of the chosen normalization for the absolute value, is a finite algebraic extension of the corresponding completion of $\mathbb{Q}$, which is either the real number field $\mathbb{R}$ or a field of p-adic numbers $\mathbb{Q}_p$. If ν is ultrametric, we let p be the characteristic of the residue field $\kappa(\nu)$ (so that κ_ν contains $\mathbb{Q}_p$) and normalize the absolute value $|\cdot|_\nu$ on κ so that on $\mathbb{Q}$ it becomes

$$|x|_\nu = |x|_p^{\frac{[\kappa_\nu:\mathbb{Q}_p]}{[\kappa:\mathbb{Q}]}} \qquad \forall x \in \mathbb{Q}.$$

Since the absolute value is determined by the place up to renormalization, the above relation defines the absolute value on the whole of κ. In other words, there is an embedding $j_\nu : \kappa \hookrightarrow \mathbb{C}_p$ such that for all $x \in \kappa$, $|x|_\nu = |j_\nu(x)|_p^{\frac{[\kappa_\nu:\mathbb{Q}_p]}{[\kappa:\mathbb{Q}]}}$.

If, on the contrary, ν is archimedean, then it corresponds to an embedding $j_\nu : \kappa \hookrightarrow \mathbb{C}$; we then normalize the absolute value $|\cdot|_\nu$ by putting

$$|x|_\nu = |j_\nu(x)|^{\frac{[\kappa_\nu:\mathbb{R}]}{[\kappa:\mathbb{Q}]}},$$

where the symbol $|\cdot|$ on the right-hand side stands for the usual complex absolute value.

With this choice of the normalizations the absolute logarithmic Weil height reads

$$h(x) = \sum_\nu \log^+ |x|_\nu \qquad \forall x \in \kappa,$$

where the sum runs over the places of κ and $\log^+ = \max(0, \log)$. We also put

$$H(x) = \exp(h(x))$$

and call it the height of the algebraic number x. It turns out to be independent of the number field κ containing x.

Also, the product formula can be written 'without weights', as

$$\prod_\nu |x|_\nu = 1 \qquad \forall x \in \kappa^*.$$

We can now formulate the first extension of Roth's theorem: we study the degree of approximation of algebraic numbers by elements of a given number field κ. The result is the following

Theorem 2.1.6. *Let κ be a number field, ν be a place of κ and $\alpha \in \kappa_\nu$ be an element of the topological closure of κ, algebraic over κ but not lying in κ. Let $\| \cdot \|_\nu$ denote the absolute value normalized with respect to κ and extended to κ_ν. Then for every positive real number $\epsilon > 0$ there exists a number $c(\alpha, \nu, \epsilon)$ such that for all $\beta \in \kappa$*

$$|\alpha - \beta|_\nu > c(\alpha, \nu, \epsilon) \cdot H(\beta)^{-2-\epsilon}.$$

Let us consider the particular case where ν is archimedean and $\kappa \subset \kappa_\nu = \mathbb{R}$. While generic real numbers can be approximated by a sequence of rationals with an error bounded by Dirchlet's Theorem, we expect that using as approximants elements of κ instead of only rational numbers the degree of approximability of any real number will increase. Since κ is a vector space of dimension $[\kappa : \mathbb{Q}]$ over $\mathbb{Q}$, it should be possible to make the error in the approximation as little as the height of the approximant to the power $-2[\kappa : \mathbb{Q}]$. Actually this is true, and can be proved via the classical pigeon-hole principle. However, in Theorem 2.1.6 above the usual exponent 2 appears; taking into consideration our normalization, the same inequality written with respect to the usual real absolute value would show precisely the exponent $-2[\kappa : \mathbb{Q}]$; so Theorem 2.1.6 states that for algebraic numbers no improvement on Dirichlet's exponent can be obtained.

The most general version of Roth's Theorem, encompassing both Ridout's theorem and the above Theorem 2.1.6, was formulated by Lang in [40]:

Theorem 2.1.7. *Let κ be a number field; let S be a finite set of places of κ. Let, for every $\nu \in S$, $| \cdot |_\nu$ be the extension of the ν-adic absolute value to κ_ν, normalized with respect to κ and let $\alpha_\nu \in \kappa_\nu$ be an algebraic number. For every $\epsilon > 0$ there exists a number $c = c(S, (\alpha_\nu)_{\nu \in S}, \epsilon)$ such that for all $\beta \in \kappa$ with $\beta \neq \alpha_\nu$ for every $\nu \in S$,*

$$\prod_{\nu \in S} |\alpha_\nu - \beta|_\nu > c \cdot H(\beta)^{-2-\epsilon}.$$

Notice that interesting cases arise when some, or even all, the α_ν lie in κ. Indeed, another equivalent formulation of the general Roth's Theorem 2.1.7 involves only κ-rational points. It appears e.g. in [10] and reads as follows:

Theorem 2.1.8. *Let κ be a number field, $d \geq 1$ an integer, $\alpha_1, \dots, \alpha_d$ be pairwise distinct elements of κ. Let $S_1, \dots, S_d$ be pairwise disjoint finite sets of absolute values. Finally, let $\epsilon > 0$ be a positive real number. Then for all but finitely many elements $\beta \in \kappa$,*

$$\prod_{h=1}^{d} \prod_{\nu \in S_h} |\alpha_h - \beta|_\nu > H(\beta)^{-2-\epsilon}. \tag{2.1.9}$$

The above theorem can be further generalized, by allowing also points at infinity as target of the approximation. This will be useful in order to deduce the mentioned theorem of Ridout. Precisely, for $\alpha = \infty$ and any absolute value

ν, let us define the ν-adic distance from α to $\beta \in \kappa$, provided $\beta \neq 0$, by putting

$$|\alpha - \beta|_\nu = |\infty - \beta|_\nu := |\beta|_\nu^{-1}.$$

Then the condition that a rational number $\beta \in \mathbb{Q}$ be of the form $\beta = a/b$ where b is a product of primes from a fixed set T can be expressed by the inequality $\prod_{\nu \in T} |\beta - \infty|_\nu \leq |b|^{-1}$; if $|\beta| \leq 1$ we also have $H(\beta) = |b|$ so the arithmetic condition that β lies in a fixed ring of S integers is equivalent to the inequality

$$\prod_{\nu \in T} \min(1, |\beta - \infty|_\nu) \leq H(\beta)^{-1},$$

where $T \subset S$ is the set of ultrametric places in S.

Actually, the generalization of Theorem 2.1.8 with one point α allowed to be at infinity follows formally from the present version of Theorem 2.1.8 itself: observe that applying projective transformations $\varPhi : \mathbb{P}_1 \to \mathbb{P}_1$ of the form

$$\varPhi(x) = \frac{ax + b}{cx + d},$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\kappa)$ one can send the given set of target points $\{\alpha_\nu\}_{\nu \in S} \subset \mathbb{P}_1(\kappa) = \kappa \cup \{\infty\}$ to a subset of $\kappa = \mathbb{P}_1(\kappa) \setminus \{\infty\}$.

For instance, in the special case in which the set of $\{\alpha_\nu, \nu \in S\}$ consists of the three rational points $0, 1, \infty \in \mathbb{P}_1(\kappa)$, the above Theorem 2.1.8 implies:

Corollary 2.1.10. *Let $\varGamma \subset \kappa^*$ be a finitely generated multiplicative group. Let T be a finite set of places of κ and $\epsilon > 0$ a positive real number. Then for all but finitely many $\gamma \in \varGamma$*

$$\prod_{\nu \in T} |\gamma - 1|_\nu > H(\gamma)^{-\epsilon}. \tag{2.1.11}$$

Before giving its proof (assuming Theorem 2.1.8) we remark that a stronger and fully effective estimate can be obtained via the theory of linear forms in logarithms (Baker's method), which replaces the right-hand side term in (2.1.11) by a (negative) power of the *logarithmic* height $h(\gamma) = \log H(\gamma)$ of the approximant.

Proof. Let us deduce Corollary 2.1.10 from Theorem 2.1.8. Let S be a finite set of places of κ such that $\varGamma \subset \mathcal{O}_S^*$ and $T \subset S$. For every solution $\gamma \in \varGamma$ to (2.1.11), let T_0 be the set of places ν for which $|\gamma|_\nu < \frac{1}{2}$ and T_∞ the set of places ν such that $|\gamma|_\nu > 2$. Let $T_1 \subset T$ be the set of places ν such that $|\gamma - 1|_\nu < \frac{1}{2}$. Note that $T_0, T_1, T_\infty \subset S$. Then

$$\prod_{\nu \in T} |\gamma - 1|_\nu \geq \left(\prod_{\nu \in T_1} |\gamma - 1|_\nu \right) \cdot \frac{1}{2^{\sharp(T)}}. \tag{2.1.12}$$

We have also the following estimates

$$\prod_{\nu\in T_0}|\gamma|_\nu=\prod_{\nu\in T_0\cap T_1}|\gamma_\nu|\cdot\prod_{\nu\in T_0\setminus T_1}|\gamma|_\nu\geq 2^{-\sharp(T_0)}\prod_{\nu\in T_0\setminus T_1}|\gamma|_\nu \tag{2.1.13}$$

and

$$\prod_{\nu\in T_\infty}|\gamma|_\nu^{-1}=\prod_{\nu\in T_\infty\cap T_1}|\gamma|_\nu^{-1}\cdot\prod_{\nu\in T_\infty\setminus T_1}|\gamma|_\nu^{-1}\geq 2^{-\sharp(T_\infty)}\prod_{\nu\in T_\infty\setminus T_1}|\gamma|_\nu^{-1}. \tag{2.1.14}$$

Also, in view of the fact that γ is a S-unit and of the definition of T_0, T_∞, we have

$$\prod_{\nu\in T_0}|\gamma|_\nu=\prod_{\nu\in T_\infty}|\gamma|_\nu^{-1}=H(\gamma)^{-1}.$$

From inequalities (2.1.13), (2.1.14) and the above identity we obtain

$$\prod_{\nu\in T_0\setminus T_1}|\gamma|_\nu\ll H(\gamma)^{-1},\qquad \prod_{\nu\in T_\infty\setminus T_1}|\gamma|_\nu^{-1}\ll H(\gamma)^{-1} \tag{2.1.15}$$

where the implied constant only depends on $\sharp(S)$.

Consider the projective transformation $x\mapsto\Phi(x)=\frac{x}{x+1}$, which sends $0,1,\infty$ to $0,1/2,1$ respectively. It satisfies, for every valuation ν,

$$\frac{1}{2}|x-0|_\nu\leq|\Phi(x)-0|_\nu\leq 2|x-0|_\nu\qquad\text{if }|x|_\nu\leq\frac{1}{2}$$

$$\frac{1}{2}|x-1|_\nu\leq|\Phi(x)-\frac{1}{2}|_\nu\leq 2|x-1|_\nu\qquad\text{if }|x-1|_\nu\leq\frac{1}{2}$$

and

$$\frac{1}{2}|x|_\nu^{-1}\leq|\Phi(x)-1|_\nu\leq 2|x|_\nu^{-1}\qquad\text{if }|x|_\nu\geq 2.$$

Then we have

$$\prod_{\nu\in T_0\setminus T_1}|\gamma|_\nu\cdot\prod_{\nu\in T_\infty\setminus T_1}|\gamma|_\nu^{-1}\cdot\prod_{\nu\in T_1}|\gamma-1|_\nu\gg\prod_{\nu\in T_0\setminus T_1}|\Phi(\gamma)|_\nu$$
$$\cdot\prod_{\nu\in T_\infty\setminus T_1}|\Phi(\gamma)-1|_\nu\cdot\prod_{\nu\in T_1}\left|\Phi(\gamma)-\frac{1}{2}\right|_\nu.$$

In view of (2.1.15) and the above inequality we can then write

$$\prod_{\nu\in T_0\setminus T_1}|\Phi(\gamma)|_\nu\cdot\prod_{\nu\in T_\infty\setminus T_1}|\Phi(\gamma)-1|_\nu\cdot\prod_{\nu\in T_1}\left|\Phi(\gamma)-\frac{1}{2}\right|_\nu\ll H(\gamma)^{-2}\prod_{\nu\in T_1}|\gamma-1|_\nu.$$

We now apply Theorem 2.1.8, taking for $d=3$, $\alpha_1=0,\alpha_2=\frac{1}{2}$, $\alpha_3=1$; and $S_1=T_0\setminus T_1$, $S_2=T_\infty\setminus T_1$, $S_3=T_1$; the inequality (2.1.9) of Theorem 2.1.8, together with the above estimates, gives the desired conclusion of Corollary 2.1.10. □

In the rational case, we state the following corollary, whose deduction is left to the reader.

Corollary 2.1.16 (Theorem of Ridout). *Let $\{p_1, \ldots, p_l\}, \{q_1, \ldots, q_m\}$ be two set of prime numbers; let λ, μ be real numbers in the closed interval $[0,1]$. Let us consider the set $\mathcal{B}$ of rational numbers β of the form $\beta = p/q$ where*

$$\begin{aligned} p &= p_1^{a_1} \cdots p_l^{a_l} \cdot p^* \\ q &= q_1^{b_1} \cdots q_m^{b_m} \cdot q^* \end{aligned}$$

where $a_1, \ldots, a_l, b_1, \ldots, b_m$ are integers with $a_i \geq 0, b_j \geq 0$ and p^*, q^* satisfy

$$\begin{aligned} p^* &\leq p^{1-\lambda} \\ q^* &\leq q^{1-\mu} \end{aligned}$$

Let $\alpha \in \mathbb{R}$ be a real algebraic number and let $\epsilon > 0$ be a positive real number. Then for all but finitely many $\beta \in \mathcal{B}$,

$$|\alpha - \beta| > H(\beta)^{-2+\lambda+\mu-\epsilon}.$$

We end this section by providing yet another version of Roth's theorem; we shall present it as a lower bound for *homogeneous* linear form.

Theorem 2.1.17 (Homogeneous Roth's Theorem). *Let κ be a number field, S be a finite set of absolute values of κ. For each $\nu \in S$, let $L_{1,\nu}(X,Y), L_{2,\nu}(X,Y)$ be linearly independent linear forms with coefficients in κ. Finally, let $\epsilon > 0$ be a positive real number. For all but finitely many $(x : y) \in \mathbb{P}_1(\kappa)$ the following inequality holds:*

$$\prod_{\nu \in S} \frac{|L_{1,\nu}(x,y)|_\nu}{\max(|x|_\nu, |y|_\nu)} \cdot \frac{|L_{2,\nu}(x,y)|_\nu}{\max(|x|_\nu, |y|_\nu)} > H(x/y)^{-\epsilon}. \qquad (2.1.18)$$

Note that, due to the appearance of the denominator $\max(|x|_\nu, |y|_\nu)$, the left hand-side term is invariant by multiplication of x and y by a non-zero constant, so it only depends on the projective class $(x : y)$ of (x, y). This is consistent with the right-hand side term, which only depends on the ratio x/y.

2.2 Higher dimensional Diophantine approximation

In higher dimension, we shall be interested in approximating hyperplanes defined by linear forms with algebraic coefficients by rational points. We shall adopt the language and notation of projective geometry for simplicity, as in the homogeneous version of Roth's Theorem given in Theorem 2.1.17.

The main result of this section is the so-called Subspace Theorem, first proved, in a particular case, by W. M. Schmidt in the seventies. Here we formulate the generalization provided by H.-P. Schlickewei, which is the natural extension of Roth's theorem to higher dimension.

We need an extension to higher dimension of the notion of height, already introduced for algebraic numbers.

Let κ be a number field, $\mathbf{x} = (x_0, \dots, x_N) \in \kappa^{N+1} \setminus \{0\}$ a non-zero vector. For every place ν of κ, its ν-adic norm $\|\mathbf{x}\|_\nu$ is defined to be

$$\|\mathbf{x}\|_\nu = \max(|x_0|_\nu, \dots, |x_N|_\nu).$$

Let us define the height of the associated projective point, still denoted by $\mathbf{x} = (x_0 : \dots : x_N) \in \mathbb{P}_N(\kappa)$, to be

$$H(\mathbf{x}) = \prod_\nu \|\mathbf{x}\|_\nu,$$

where the product runs over all the valuations of κ.

With these conventions, Schmidt's Subspace Theorem reads:

Theorem 2.2.1 (Subspace Theorem). *Let $N \geq 1$ be a positive integer, κ be a number field and S a finite set of places of κ. Let, for every $\nu \in S$, $L_{0,\nu}(X_0, \dots, X_N), \dots, L_{N,\nu}(X_0, \dots, X_N)$ be linearly independent linear forms with algebraic coefficients in κ_ν. Then for each $\epsilon > 0$ the solutions $\mathbf{x} = (x_0 : \dots : x_N) \in \mathbb{P}_N(\kappa)$ to the inequality*

$$\prod_{\nu \in S} \prod_{i=0}^{N} \frac{|L_{i,\nu}(\mathbf{x})|_\nu}{\|\mathbf{x}\|_\nu} < H(\mathbf{x})^{-N-1-\epsilon} \tag{2.2.2}$$

lie in the union of finitely many hyperplanes of $\mathbb{P}_N$, defined over κ.

For $N = 1$, the conclusion provides the finiteness of the solutions to the inequality (2.2.2); so we recover Roth's Theorem. In higher dimension, however, the finiteness conclusion does not hold: for instance, when the point $\mathbf{x}$ lies in the hyperplane defined by the vanishing of one linear form, the left-hand side term in (2.2.2) vanishes, so the inequality is satisfied. It is worth noticing, however, that the exceptional hyperplanes containing the infinite families of solutions are not necessarily the zero sets of the involved linear forms, as the following example shows:

`Example`. Let α be a real irrational algebraic number, with $0 < \alpha < 1$; consider a "good" rational approximation $p/q \in \mathbb{Q}$ to α. By this we mean that p, q are coprime integers, $q > 0$, and

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2};$$

we know from Dirichlet's Theorem that there exist infinitely many of them. Since $\alpha < 1$, for infinitely many good approximations p/q one has $\max(|p|, |q|) = |q|$, so we can write the above inequality as

$$\left|\alpha - \frac{p}{q}\right| < \max(|p|, |q|)^{-2}.$$

For each such pair (p,q) we have the upper bound

$$\frac{|q\alpha - p|}{\max(|p|,|q|)} \le \frac{|q\alpha - p|}{|q|} < \max(|p|,|q|)^{-2}. \tag{2.2.3}$$

Now take $N=2$, $\kappa=\mathbb{Q}$ and S consisting of the archimedean absolute value of $\mathbb{Q}$ and define the three linear forms $L_i(X_0,X_1,X_2)$ $(i=0,1,2)$ as follows:

$$L_0(X_0,X_1,X_2)=X_0-\alpha X_2, \quad L_1(X_0,X_1,X_2)=X_1-\alpha X_2, \quad L_2(X_0,X_1,X_2)=X_2.$$

Now, with each good approximation p/q to the number α as above we associate the point $(x_0:x_1:x_2)=(p:p:q)$. Then the double product in (2.2.2) becomes

$$\prod_{\nu\in S}\prod_{i=0}^{N}\frac{|L_{i,\nu}(\mathbf{x})|_\nu}{\|\mathbf{x}\|_\nu} = \left(\frac{|p-q\alpha|}{\max(|p|,|q|)}\right)^2 \cdot \frac{|q|}{\max(|p|,|q|)}.$$

By the above inequality (2.2.3) and the trivial estimate $|q|\le\max(|p|,|q|)$, we have the upper bound

$$\prod_{\nu\in S}\prod_{i=0}^{N}\frac{|L_{i,\nu}(\mathbf{x})|_\nu}{\|\mathbf{x}\|_\nu} < \max(|p|,|q|)^{-4},$$

which means that inequality (2.2.2), with e.g. $\epsilon=1/2$, admits infinitely many solutions $(x_0:x_1:x_2)=(p:p:q)$ on the projective line of equation $X_0=X_1$. So, the degeneracy conclusion of Theorem 2.2.1 cannot be replaced by a finiteness one, even after assuming $L_{i,\nu}(\mathbf{x})\neq 0$ for all i,ν.

It will prove useful to have an 'affine version' of the Subspace Theorem, of which Theorem 2.2.1 represents the projective, or homogeneous, formulation. Here is such an affine version, which can be formally deduced from Theorem 2.2.1:

Theorem 2.2.4. *Let κ be a number field, S a finite set of places containing the archimedean ones, $N\ge 2$ an integer. Let, for each $\nu\in S$, $L_{\nu,1}(X_1,\ldots,X_N),\ldots,L_{\nu,N}(X_1,\ldots,X_N)$ be linearly independent linear forms with algebraic coefficients in κ_ν. Then the solutions $(x_1,\ldots,x_N)\in\mathcal{O}_S^N$ to the inequality*

$$\prod_{\nu\in S}\prod_{i=1}^{N}|L_{\nu,i}(\mathbf{x})|_\nu < H(\mathbf{x})^{-\epsilon}$$

lie in the union of finitely many proper linear subspaces of κ^N.

The Subspace Theorem, like Roth's theorem, is ineffective; however, the number of the higher dimensional components of the Zariski-closure of the set of solutions to (2.2.2) can be bounded (see [28]).

The Subspace Theorem, as we said, is a Diophantine approximation statement in higher dimension; the 1-dimensional case of it reduces precisely to

Roth's Theorem. However, there are problems in Diophantine approximation on the line which can be solved only by going to higher dimension, and then applying the Subspace Theorem. Let us see a simple example. We have seen that Ridout's theorem improves on Roth's estimate for the rational approximation to (real) algebraic numbers by rational number whose denominator is a product of powers of fixed set of primes. For instance, we have the bound

$$\left|\alpha - \frac{p}{2^n}\right| \gg 2^{-(1+\epsilon)n},$$

where Roth's exponent $2+\epsilon$ is replaced by $1+\epsilon$. We obtained this estimate after interpreting the special form of the approximant $p/2^n$ as being a rational number close to infinity in the 2-adic absolute value. If we change slightly the denominator, by replacing 2^n by 2^n+1, Ridout's Theorem does not apply anymore. However, by using the Subspace Theorem, we can indeed recover Ridout's $1+\epsilon$ exponent. Let us see how, following an idea introduced in [14] (see also [21], page 165). Define the three linear forms $L_0(X_0, X_1, X_2), L_1(X_0, X_1, X_2)$ and $L_2(X_0, X_1, X_2)$ by putting

$$L_0(X_0, X_1, X_2) = X_0, \quad L_1(X_0, X_1, X_2) = X_1, \quad L_2(X_0, X_1, X_2) \\ = \alpha(X_0 + X_1) - X_2.$$

Then every solution $p/(2^n+1)$ to the inequality

$$|\alpha - p/(2^n+1)| < 2^{-(1+\epsilon)n}$$

gives rise to the point $\mathbf{x} := (1 : 2^n : p) \in \mathbb{P}_2(\mathbb{Q})$ satisfying

$$\left(\prod_{i=0}^{2} \frac{|L_i(\mathbf{x})|}{\|\mathbf{x}\|}\right) \cdot \left(\prod_{i=0}^{2} \frac{|L_i(\mathbf{x})|_2}{\|\mathbf{x}\|_2}\right) < H(\mathbf{x})^{-3-\epsilon}.$$

Hence by the Subspace Theorem 2.2.1, applied with $N=2$, the points $(1, 2^n, p)$ would satisfy one of finitely many linear dependence relations; but from this fact and the starting inequality $|\alpha - p/(2^n+1)| < 2^{-(1+\epsilon)n}$, it is easy to deduce finiteness.

This example can be naturally generalized to produce the following statement:

Theorem 2.2.5. *Let $u : \mathbb{N} \to \mathbb{Q}$ be a sequence defined by*

$$u(n) = \sum_{i=1}^{h} a_i b_i^n,$$

where $h \geq 1$ is a natural number, $a_1, \ldots, a_h$ are rational numbers and $b_1, \ldots, b_h$ are positive integers. Let α be a real irrational algebraic number. Then for every $\epsilon > 0$ there exist only finitely many pairs of rational numbers of the form

$p/u(n)$, where $p \in \mathbb{Z}$, $n \in \mathbb{N}$, such that

$$\left| \alpha - \frac{p}{u(n)} \right| < \max(|p|, |u(n)|)^{-1-\epsilon}.$$

This result is proved in [14]. Note that the exponent $-1-\epsilon$ is Ridout's exponent, as it would be in the case the power sum $u(n)$ consisted in a single exponential function $n \mapsto b^n$. If we suppose also that the numerator p in the displayed inequality if of the form $p = v(m)$ for some power sum $m \mapsto v(m)$, then the exponent can be reduced to $-\epsilon$, still using the Subspace Theorem. Whenever both $u(n)$ and $v(m)$ are geometric progressions (i.e. $u(n) = ab^n, v(m) = a'b'^m$, then the theory of linear forms in logarithms applies and one can even obtain an effective result.

2.3 Approximation to higher degree hypersurfaces

We have seen that Schmdit's Subspace Theorem can be viewed as a statement about approximating hyperplanes, defined over a number field, by rational points.

It is then natural to consider the case where the targets are no more linear sub-spaces, but arbitrary (projective) hypersurfaces. Note that in dimension one (in the setting of Roth's Theorem) there is no such distinction, since the (geometrically) irreducible components of any hypersurfaces are single points, i.e. hyperplanes.

In this direction we do not dispose neither of a good generlization of Dirichlet's Theorem, nor of Roth's Theorem.

Suppose we want to investigate the rational approximation of a single hypersurface; to simplify matters we suppose that such a hypersurface is defined over $\mathbb{Q}$, by the vanishing of a homogeneous form $F(X_0, \ldots, X_N) \in \mathbb{Q}[X_0, \ldots, X_n]$. Set $d = \deg F$. An analogue of Liouville's Theorem is represented by the estimate

$$\frac{|F(\mathbf{x})|}{\|\mathbf{x}\|^d} \geq c \cdot \|\mathbf{x}\|^{-d},$$

where $c > 0$ is a constant depending on F, holding for all rational points $\mathbf{x} = (x_0 : \ldots : x_N) \in \mathbb{P}_N(\mathbb{Q})$ such that $F(\mathbf{x}) \neq 0$. Note that the left-hand side only depends on the projective class of $\mathbf{x}$, so it can be considered as a measure of the distance between the projective point $\mathbf{x}$ and the projective hypersurface $F(X_0, \ldots, X_N) = 0$.

Quoting W. Schmidt [49]: 'Any improvement of this inequality, even though perhaps it may apply only to special cases of non-linear hypersurfaces, would be of great interest and would shed light on certain diophantine equations...".

Note, however, that whenever the homogeneous form $F(X_0, \ldots, X_N)$ has irrational algebraic coefficients in a number field κ, the Liouville's inequality is changed into

$$\frac{|F(\mathbf{x})|}{\|\mathbf{x}\|^d} \geq c \cdot \|\mathbf{x}\|^{-d[\kappa:\mathbb{Q}]} \tag{2.3.1}$$

(here the absolute values are normalized with respect to $\mathbb{Q}$, since $\mathbf{x}$ is still supposed to lie in $\mathbb{P}_N(\mathbb{Q})$).

Of course, one can also consider the affine version, where the involved polynomials are no more supposed to be homogeneous. In that case the 'Liouville's inequality' is expressed as

$$|f(\mathbf{x})| > c(f) \cdot \|\mathbf{x}\|^{-d([\kappa:\mathbb{Q}]-1)}, \tag{2.3.2}$$

for every polynomial $f(X_1, \ldots, X_N) \in \kappa[X_1, \ldots, X_N]$ of total degree d and every integral point $\mathbf{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$.

Improvements on 'Liouville's inequality' (2.3.1) have been obtained in [26], [17], [27]. Their proofs all involve an application of the Subspace Theorem.

To give an example of such improvements on Liouville's inequality in the non-linear case, we quote the corollary to the main theorem in [17], *Addendum*, which reads as follows

Theorem 2.3.3. *Let $f(X_1, \ldots, X_n) \in \bar{\mathbb{Q}}[X_1, \ldots, X_n]$ be a polynomial in n variables with algebraic coefficients of degree d. For every $\epsilon > 0$ there exists a number $c > 0$ such that for all $\mathbf{x} \in \mathbb{Z}^n$ with $f(\mathbf{x}) \neq 0$,*

$$|f(\mathbf{x})| > c \cdot \|\mathbf{x}\|^{-d(n-1)-\epsilon} \tag{2.3.4}$$

We note at once that whenever the degree of the number field κ generated by the coefficients of the polynomial f satisfies $[\kappa : \mathbb{Q}] \geq n$, the above estimate cannot be deduced from Liouville's bound (2.3.2).

The inequality (2.3.4) can be improved after assuming that the approximant lie in a fixed algebraic sub-variety of $\mathbb{A}^n$. Also, it can be extended to number fields and arbitrary set of places. The most general known results can be found in [27], where the estimates are formulated in projective version.

Chapter 3
The theorems of Thue and Siegel

3.1 Thue's equation

One of the first finiteness results on Diophantine equations was proved by Axel Thue in 1909 [58]. It constitutes the starting point of the modern theories of Diophantine equations and Diophantine approximation.

Theorem 3.1.1 (Thue, 1909). *Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a homogeneous irreducible polynomial of degree ≥ 3. Let $c \in \mathbb{Z}$ be a non-zero integer. The diophantine equation*

$$F(x,y) = c \tag{3.1.2}$$

has only finitely many solutions in integers $(x,y) \in \mathbb{Z}^2$.

We provide two proofs of this theorem, the second of which uses Siegel's theorem for open sets of $\mathbb{P}_1$, i.e. Corollary 3.2.4 from next section.

Proof. Our first proof follows Thue's original path. Let us suppose by contradiction that $n \mapsto (x_n, y_n)$ is an infinite sequence of integral solutions to (3.1.2), with $|y_n| \to \infty$ (it is clear that there are only finitely many solutions for each given y). We factor the form $F(X,Y)$ in $\bar{\mathbb{Q}}[X,Y]$ by writing

$$F(X,Y) = \prod_{i=1}^{d} (\beta_i X - \alpha_i Y),$$

where $d = \deg F$ and $(\alpha_i, \beta_i) \in \bar{\mathbb{Q}}^2$ are such that $F(\alpha_i, \beta_i) = 0$. Since $F(X,Y)$ is irreducible (over the rationals), the determinants $\alpha_i \beta_j - \beta_i \alpha_j$ do not vanish for any $i \neq j$. Also $\beta_1, \ldots, \beta_d$ are all non-zero. From the equation (3.1.2) we obtain, by taking absolute values,

$$\prod_{i=1}^{d} \left| \beta_i \frac{x_n}{y_n} - \alpha_i \right| = \frac{|c|}{|y_n|^d} \to 0.$$

P. Corvaja, *Integral Points on Algebraic Varieties*, HBA Lecture Notes in Mathematics, DOI 10.1007/978-981-10-2648-5_3

Then, up to extracting a subsequence from the sequence $n \mapsto y_n$ and reordering indices, we can suppose that the sequence of rational numbers $n \mapsto (x_n/y_n)$ tends to α_1/β_1. From the above relation we also obtain the inequality

$$\left|\frac{x_n}{y_n} - \frac{\alpha_1}{\beta_1}\right| \leq \frac{c_1}{|y_n|^d},$$

holding for all large n in an infinite subsequence, where c_1 is any number larger than $|c\beta_1^{d-1}| \max_i(|\alpha_1\beta_i - \alpha_i\beta_1|^{1-d})$. The above inequality contradicts Roth's Theorem, since $d > 2$, finishing the proof. □

As promised, we give a second proof of Thue's theorem.

Proof. Consider the algebraic curve $\mathcal{C} \subset \mathbb{A}^2$ defined by Thue's equation $F(X,Y) = c$. Let $U \subset \mathbb{P}_1$ be the open set $F(X,Y) \neq 0$. Then U is the complement of $d \geq 3$ points in $\mathbb{P}_1$. The map $\mathcal{C} \to U$ sending $\mathcal{C} \ni (x,y) \mapsto (x:y) \in U$ is a (unramified) cover of U, so if $\mathcal{C}$ had infinitely many integral points the same would be true of U, by Chevalley-Weil. An application of Theorem 3.2.4 gives the desired finiteness. □

Some remarks are in order:

(1) Thue did not use Roth's Theorem, which was not yet known at the time, but he used instead a weaker version that he proved in the same article; it is the lower bound

$$\left|\alpha - \frac{p}{q}\right| > \max(|p|,|q|)^{-\frac{d}{2}-1-\epsilon},$$

where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $\epsilon > 0$, holding for all but finitely many rational numbers p/q.

(2) The same proof, using Roth's Theorem, applies without changes to prove the finiteness of integral solutions to equations of the form

$$F(x,y) = g(x,y)$$

where $F(X,Y)$ is an irreducible form and the total degree of the polynomial $g(X,Y)$ satisfies $\deg g < \deg F - 2$.

(3) All curves defined by a Thue's equation of the form (3.1.2) have d (distinct) points at infinity; if $d \geq 3$, and only in this case, they have non-zero genus, in other words they are not rational (see below). In contrast, when $d = 2$, the conic of equation $F(X,Y) = 0$ has two points at infinity, and has genus zero. The example of Pell's equation $x^2 - ay^2 = 1$, where $a > 0$ is a positive non-square integer, shows that the assumption that $d \geq 3$ cannot be omitted.

(4) Replacing Roth's Theorem by its generalized version, e.g. Theorem 2.1.8, one can deduce in the same way the more general

Theorem 3.1.3 (Thue-Mahler Theorem)**.** *Let κ be a number field, $\mathcal{O}_S \subset \kappa$ a ring of S-integers, $F(X,Y) \in \mathcal{O}_S[X,Y]$ be a binary homogeneous form with*

S-integral coefficients. Suppose that $F(X,Y)$ has at least three pairwise non-proportional linear factors in $\bar{\kappa}[X,Y]$. Then there are only finitely many pairs $(x,y) \in \mathcal{O}_S^2$, up to multiplicative constants, such that

$$F(x,y) \in \mathcal{O}_S^*. \tag{3.1.4}$$

Let us sketch an independent proof of the Thue-Mahler Theorem, which does not use directly Diophantine approximations methods, but rather the S-unit equation theorem in two variables.

It runs as follows: after factoring

$$F(X,Y) = \prod_{i=1}^{k} (\beta_i X - \alpha_i Y)^{e_i} \tag{3.1.5}$$

where $\beta_i X - \alpha_i Y$ for $i = 1, \ldots, k$ are the distinct prime divisors of $F(X,Y)$ in $\bar{\mathbb{Q}}[X,Y]$, we can suppose, after enlarging κ and S if necessary, that the β_i, α_i belong to κ and the determinants $\beta_i\alpha_j - \beta_j\alpha_i$ are S-units. Then for every coprime S-integers x, y, the values $\beta_i x - \alpha_i y$, for $i = 1, \ldots, k$, are pairwise coprime; if (x,y) is a solution to (3.1.4), the product of the $\beta_i x - \alpha_i y$ is a unit, so each term is a unit. Let us write

$$u_i = \beta_i x - \alpha_i y,$$

for $i = 1, \ldots, k$; since by our hypothesis $k \geq 3$, we can consider the first three terms u_1, u_2, u_3. Eliminating x and y from the relations above we obtain a linear relation of the form $a_1u_1 + a_2u_2 + a_3u_3 = 0$, for some non-zero constant coefficients a_1, a_2, a_3, holding for all the solutions (x,y). An application of the S-unit equation theorem (Theorem 3.2.1) gives the desired result. □

It is worthwhile to look for a geometric interpretation of the last proof; it will turn out that this is precisely the second proof of Thue's theorem given above.

We can view the solutions (x,y) to (3.1.4) as integral points on $\mathbb{A}^2$, which moreover are integral with respect to the curve of equation $F(x,y) = 0$ in $\mathbb{A}^2$. The latter is a union of k lines intersecting at the origin. Viewing the point $(x,y) \in \mathbb{A}^2$ as a point $(x : y : 1) \in \mathbb{P}_2$, it becomes integral also with respect to the line at infinity. Hence we are considering integral points in $\mathbb{P}_2$ with respect to a configuration of $k+1$ lines, the first k passing through a single point and the last one, the line at infinity, being in general position with respect to the previous k. This variety is isomorphic to the product $\mathbb{A}^1 \times (\mathbb{P}_1 \setminus \{k \text{ points}\})$, the projection on the last factor being given by $(x : y : 1) \mapsto (x : y)$. Hence its points are degenerate and moreover they lie on finitely many lines $x = \lambda_i y$; this gives the required finiteness statement.

3.2 Hyperelliptic curves and sums of two units

The aim of this section is proving the following two theorems and showing their interdependence.

Theorem 3.2.1 (S-unit Equation Theorem in two variables)**.** *Let $\varGamma \subset \bar{\mathbb{Q}}^*$ be a finitely generated multiplicative group. Then the equation*

$$u + v = 1$$

has only finitely many solutions $(u, v) \in \varGamma \times \varGamma$.

This theorem is indeed equivalent to Siegel's Theorem 3.3.1 for the particular curve $\mathcal{C} = \mathbb{P}_1 \setminus \{0, 1, \infty\}$, as explained in §1.2. The following result is Siegel's theorem in the case of the so-called hyperelliptic curves, where the points (or the point) at infinity are fixed by the hyperelliptic involution.

Theorem 3.2.2. *Let $\mathcal{O}_S$ be a ring of S-integers in a number field κ; let $f(X) \in \mathcal{O}_S[X]$ be a polynomial with at least three simple roots in $\bar{\kappa}$. Then the equation*

$$y^2 = f(x) \tag{3.2.3}$$

has only finitely many solutions $(x, y) \in \mathcal{O}_S \times \kappa$.

In other words, there exist only finitely many $x \in \mathcal{O}_S$ such that the value $f(x)$ is a square in κ. Note that if $f(X)$ has two roots, the conclusion does not hold in general, as the example of the polynomial $f(X) = 2X^2 + 1$ shows already for $\kappa = \mathbb{Q}$ and $\mathcal{O}_S = \mathbb{Z}$. Also, if $f(X)$ has two simple roots, and no other root in $\bar{\kappa}$, then the curve of equation $y^2 = f(x)$ is rational, isomorphic to $\mathbb{G}_m$ over a suitable extension of the number field κ. Hence it contains infinitely many integral points, over a suitable extension of the ring of integers $\mathcal{O}_S$.

Let us prove Theorem 3.2.1 by using Corollary 2.1.10. First we can find a number field κ and a ring of S-integers $\mathcal{O}_S \subset \kappa$ such that $\varGamma \subset \mathcal{O}_S^*$. Suppose by contradiction that there exist infinitely many solutions (u, v) to the equation $u + v = 1$ of the Theorem. By symmetry, we can suppose that for all our solutions $H(v) \geq H(u)$. Now, for each solution (u, v), let $T = T(u, v)$ be the set of places $\nu \in S$ such that $|v|_\nu < 1$. Since S is finite, there are only finitely many possibilities for the subset T. So, after extracting a suitable infinite subsequence, we can and shall suppose that T is fixed. Putting $\gamma := -u/v$ we obtain $\gamma - 1 = -v^{-1}$ so

$$\prod_{\nu \in T} |\gamma - 1|_\nu = \prod_{\nu \in T} \frac{1}{|v|_\nu} = \prod_{\nu \in S} \max(1, |v^{-1}|_\nu) = H(v^{-1})^{-1} = H(v)^{-1},$$

where the last equality follows from the product formula. Since $H(\gamma) \leq H(u) \cdot H(v) \leq H(v)^2$, we obtain

$$\prod_{\nu \in T} |\gamma - 1|_\nu \leq H(\gamma)^{-1/2}.$$

Hence Corollary 2.1.10, applied with any number $\epsilon < 1/2$, gives the desired contradiction, finishing the proof. Note that by inserting on T also the places for which u is small, we could have ended with the inequality $\prod_{\nu \in T} |\gamma - 1|_\nu \ll H(\gamma)^{-1}$, so a much weaker result than Corollary 2.1.10 would suffice.

Let us now prove Theorem 3.2.2 by using Theorem 3.2.1. Of course, if we prove finiteness of solutions of (3.2.3) for x in a ring larger than $\mathcal{O}_S$, our theorem will be proved. Hence we can enlarge the number field κ so that the roots of $f(X)$ become rational and we also enlarge the ring of S-integers $\mathcal{O}_S$ so that it becomes a Principal Ideal Domain. Now equation (3.2.3) can be written as

$$y^2 = a \cdot (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)g(x)$$

where $a, \alpha_1, \alpha_2, \alpha_3 \in \kappa$, $a \neq 0$, the α_i are pairwise distinct and the polynomial $g(X) \in \kappa[X]$ does not vanish at α_i for any $i = 1, 2, 3$. Since the two polynomials $h(X) := a(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ and $g(X)$ are coprime, in the ring $\kappa[X]$, they generate the unit ideal; in other words, there exist polynomials $\varphi(X), \psi(X) \in \kappa[x]$ such that

$$\varphi(X)h(X) + \psi(X)g(X) = 1.$$

Up to enlarging if necessary the ring of S-integers $\mathcal{O}_S$, we can suppose that $a \in \mathcal{O}_S^*$ and that all the coefficients of all the four polynomials $h(X), g(X), \varphi(X), \psi(X)$ are S-integers. Now, for every $x \in \mathcal{O}_S$, from the above identity it follows that the two S-integers $h(x), g(x)$ generate the unit ideal $(1) = \mathcal{O}_S$, so they must be coprime. Hence, due to unique factorization in $\mathcal{O}_S$, whenever the product $f(x) = h(x)g(x)$ is a square in κ, both factors should be squares, up to units. Since the quotient of the group of units modulo squares is finite, we obtain from the infinitude of the set of solutions to (3.2.3) that for at least one unit $\gamma \in \mathcal{O}_S^*$ the equation

$$y^2 = \gamma(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

has infinitely many solutions $(x, y) \in \mathcal{O}_S \times \kappa$. We observe that $x - \alpha_i, x - \alpha_j$ are essentially coprime for $i \neq j$, actually they are coprime whenever the discriminant $((\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1))^2$ is a unit, which we can suppose to hold after enlarging S; so, by repeating the previous argument, we deduce that there exist units $\gamma_1, \gamma_2, \gamma_3$ such that for infinitely many $x \in \mathcal{O}_S$ and each $i = 1, 2, 3$, the elements $\gamma_i(x - \alpha_i)$ are squares in κ. After enlarging κ we can suppose that the γ_i are also squares, so that for infinitely many $x \in \mathcal{O}_S$ there exist $y_1, y_2, y_3 \in \kappa$ such that we can write

$$y_i^2 = x - \alpha_i \qquad \text{for } i = 1, 2, 3.$$

Eliminating x from the first two relations (i.e. those corresponding to $i = 1, 2$) we obtain

$$y_1^2 - y_2^2 = (y_1 - y_2)(y_1 + y_2) = \alpha_2 - \alpha_1$$

Recall that $\alpha_2 - \alpha_1$ is a unit, since the discriminant of $h(X)$ was supposed to be a unit; then $y_1 - y_2$ (and also $y_1 + y_2$) must be a unit. Then, using the same relations for the other pairs of distinct indices i, j in $\{1, 2, 3\}$, we obtain that $y_1 - y_3$ and $y_2 - y_3$ are also unit. Writing

$$\begin{cases} y_1 - y_2 = u_3 \\ y_2 - y_3 = u_1 \\ y_3 - y_1 = u_2 \end{cases}$$

for suitable units u_1, u_2, u_3, we obtain the homogeneous S-unit equation

$$u_1 + u_2 + u_3 = 0.$$

Putting $u := -u_1/u_3$, $v := -u_2/u_3$, we get the relation $u+v = 1$ and Theorem 3.2.1 gives the finiteness of the ratios $u_1/u_3, u_2/u_3$. This in turn gives the finiteness of the triples (y_1, y_2, y_3) up to multiplicative constants and from this and the relation $y_1^2 - y_2^2 = \alpha_2 - \alpha_1$ it is easy to deduce the finiteness of the solutions x.

The above proof might seem complicated and unnatural, but it can be enlightened using a geometric view-point. Let $\mathcal{C}$ be the affine curve defined by our equation (3.2.3). The main point of the proof is the observation that the three rational functions $x - \alpha_i$, for $i = 1, 2, 3$, take perfect square values at integral points (x, y) (after a fixed enlargement of the ring $\mathcal{O}_S$). This is of course connected with the Chevalley-Weil theorem: the three functions in question are locally a square everywhere, so the function field extension $\kappa(\mathcal{C})(\sqrt{x - \alpha_i})/\kappa(\mathcal{C})$ is unramified over $\mathcal{C}$ (it might ramify at infinity, depending on the parity of $\deg f$). Hence, by Chevalley-Weil, each integral point on $\mathcal{C}$ lifts to an integral point on $\mathcal{C}'$, where $\mathcal{C}'$ is the affine curve corresponding to the integral closure of the ring $\kappa[\mathcal{C}][\sqrt{x - \alpha_1}, \sqrt{x - \alpha_2}, \sqrt{x - \alpha_3}]$. Now, letting y_i be square roots of $x - \alpha_i$ in $\kappa[\mathcal{C}']$, we have that the regular functions $u_3 := y_1 - y_2, u_1 := y_2 - y_3, u_2 := y_3 - y_2$ have all their zeros and poles at infinity, so they send $\mathcal{C}' \to \mathbb{G}_m$. So we obtain the morphism $\mathcal{C}' \to \mathbb{G}_m^2$ by sending $\mathcal{C}' \ni p \mapsto (\frac{-u_1(p)}{u_3(p)}, \frac{-u_2(p)}{u_3(p)})$ whose image is the line $u + v = 1$ inside the torus $\mathbb{G}_m^2$; this closed set of the torus is isomorphic to $\mathbb{P}_1 \setminus \{0, 1, \infty\}$, so it contains only finitely many integral points and the proof is finished.

It could be proved that for a general affine hyperelliptic curve $\mathcal{C}$ defined by an equation (3.2.3) there exists no non-constant morphism $\mathcal{C} \to \mathbb{G}_m^2$, and, when such a morphism does exist, its image is a translate of a subtorus; so Theorem 3.2.1 or its generalization Theorem 1.2.2 cannot be used directly. However, the two-variables S-unit equation theorem can be used, and has been used in the above proof, after taking an unramified cover $\mathcal{C}' \to \mathcal{C}$ of the original curve, since the curve $\mathcal{C}'$ does admit such a non-trivial morphism to $\mathbb{G}_m^2$.

We end by showing that Theorem 3.2.1 immediately implies Siegel's theorem in the rational case:

Corollary 3.2.4. *Let $X \subset \mathbb{P}_1$ be an algebraic open set with $\mathbb{P}_1 \setminus X$ consisting of at least three points. Then $X(\mathcal{O}_S)$ is finite, for every ring of S-integers $\mathcal{O}_S$.*

Proof. We just repeat the argument given in the introduction. We can suppose, up to enlarging the field of definition κ, that three of the points of the complement of X in $\mathbb{P}_1$ are $0, 1, \infty$. Then the algebra $\kappa[X]$ contains the functions $x, 1/x, 1/(x-1)$. Hence for every integral point $p \in X(\mathcal{O}_S)$ we obtain a solution $(u, v) = (x(P), 1 - x(P))$ to the S-equation $u + v = 1$ of Theorem 3.2.1. □

3.3 Siegel's Theorem on curves

As mentioned, a general theorem of Siegel-Mahler, which we give here in the most general formulation provided by Lang [39], asserts the finiteness of S-integral points on a large class of curves, namely all those satisfying the assumption of log-general type appearing in Vojta's conjecture:

Theorem 3.3.1 (Siegel's Theorem on curves)**.** *Let $\mathcal{C}$ be an affine curve defined over a number field. Suppose either that it has genus > 0 or that it has at least three points at infinity. Then for each ring of S-integers $\mathcal{O}_S$, the set $\mathcal{C}(\mathcal{O}_S)$ is finite.*

Note that we do not assume the curve is smooth; however, the theorem in the possibly singular case would follow easily from the particular case of smooth curves.

In the sequel, we shall suppose that $\mathcal{C}$ is smooth affine and define $\tilde{\mathcal{C}}$ to be its smooth compactification; let g be the genus of $\tilde{\mathcal{C}}$. We denote by D the complement: $D = \tilde{\mathcal{C}} \setminus \mathcal{C}$.

So Siegel's theorem asserts that whenever $\deg D \geq 3$ or $g \geq 1$, then the set $\mathcal{C}(\mathcal{O}_S)$ is finite. On the other hand, we have already observed in Chapter 1 that if $g = 0$ and $\deg D = 1$ or 2 the corresponding curve, which is either $\mathbb{G}_a = \mathbb{A}^1$ or $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$ has infinitely many integral points (over a suitable ring of S-integers). Hence Siegel's theorem provides a complete classification of the algebraic curves admitting infinitely many integral points.

Let us analyze this classification in view of the Chevalley-Weil theorem. Recall that given two (smooth, affine) curves $\mathcal{C}_1, \mathcal{C}_2$ admitting a dominant morphism $\pi : \mathcal{C}_1 \to \mathcal{C}_2$, if $\mathcal{C}_1(\mathcal{O}_S)$ is infinite, also $\mathcal{C}_2(\mathcal{O}_S)$ will be infinite. On the other hand, if $\pi : \mathcal{C}_1 \to \mathcal{C}_2$ is an unramified cover, then the two finiteness properties are equivalent; more precisely, if $\mathcal{C}_2(\mathcal{O}_S)$ is finite for every ring of S-integers $\mathcal{O}_S$, the same is true of $\mathcal{C}_1(\mathcal{O}_S)$. Let us write, as usual, $\mathcal{C}_i = \tilde{\mathcal{C}}_i \setminus D_i$ and denote by g_i the genus of $\tilde{\mathcal{C}}_i$ and by $s_i = \deg D_i$. The inequalities $g_1 \geq g_2$ and $s_1 \geq s_2$ hold for every dominant morphism $\pi : \mathcal{C}_1 \to \mathcal{C}_2$; moreover, for unramified morphism the equality holds if either $\deg \pi = 1$ (which is certainly the case if $\mathcal{C}_1 = \mathbb{A}^1$) or $\mathcal{C}_2 = \mathbb{G}_m$ (in which case necessarily $\mathcal{C}_1 = \mathbb{G}_m$). Hence, Siegel's finiteness theorem can be stated as follows:

Theorem 3.3.2 (Siegel's Theorem - alternate version)**.** *Let $\mathcal{C}$ be a smooth affine curve defined over a number field κ. The following are equivalent:*

(i) *the set $\mathcal{C}(\mathcal{O}_S)$ is finite for every ring of S-integers;*
(ii) *there exists an unramified cover $\mathcal{C}' \to \mathcal{C}$ of $\mathcal{C}$ such that the genus of $\mathcal{C}'$ is strictly larger than the genus of $\mathcal{C}$;*

(iii) *for every integer g, there exists an unramified cover $\mathcal{C}' \to \mathcal{C}$ of $\mathcal{C}$ such that the genus of $\mathcal{C}'$ is larger than g;*
(iv) *there exists an unramified cover $\mathcal{C}' \to \mathcal{C}$ of $\mathcal{C}$ such that $\mathcal{C}'$ has strictly more points at infinity than $\mathcal{C}$;*
(v) *for every integer N there exists an unramified cover $\mathcal{C}' \to \mathcal{C}$ of $\mathcal{C}$ such that $\mathcal{C}'$ has at least N points at infinity;*
(vi) *the fundamental group of the topological space $\mathcal{C}(\mathbb{C})$ is not abelian.*

By Chevalley-Weil Theorem and topological classification of algebraic curves, this means that an apparently weaker statement than Siegel's, namely the finiteness of integral points on curves of sufficiently large genus (say genus > 100) would imply via Chevalley-Weil theorem the full statement in Theorem 3.3.1. The same could be said about the requirement on the number of points at infinity: the finiteness of integral points on all the curves with at least, say, one hundred points at infinity, over every ring of S-integers, would imply the finiteness of integral points on curves with at least three points at infinity, as well as on those which have positive genus and at least one point at infinity (i.e. are affine).

Siegel's proofs. We give a sketch of a proof of Siegels' Theorem similar to the original one (but we should mention that Siegel did not treat arbitrary S-integers in his 1929 paper [52]; the generalization to arbitrary S-integers is due to Mahler and Lang, see [39]). Actually, Siegel provided two different proofs; we recommend the paper [63], which we are following now, for a careful discussion of the different tools needed in the various approaches.

Let us suppose that an affine curve $\mathcal{C}$ (say embedded in $\mathbb{A}^N$) of genus $>$ 0 admits infinitely many S-integral points. Then we can extract an infinite sequence $P_1, P_2, \ldots$ in $\mathcal{C}(\mathcal{O}_S)$ converging in the projective completion $\tilde{\mathcal{C}}$ for every place $\nu \in S$ (recall that $\tilde{\mathcal{C}}(\kappa_\nu)$ is compact).

For each point $P \in \mathbb{A}^N(\kappa)$ and each place $\nu \in S$, denote by $|P|_\nu$ the sup-norm of P. Then the height of an S-integer point $P \in \mathbb{A}^N(\mathcal{O}_S)$ is

$$H(P) = \prod_{\nu \in S} \max\{1, |P|_\nu\},$$

so $H(P) \le \max\{1, |P|_{\nu_0}\}^{\sharp(S)}$ where ν_0 is such that $|P|_{\nu_0} \ge |P|_\nu$ for any other place ν. We can suppose that for our points in the sequence $P_1, P_2, \ldots$ the place ν_0 is one and the same. Let $Q = \lim_{n \to \infty} P_n$, the limit being taken in the ν_0-adic sense. Then for a suitable local parameter $t \in \kappa(\mathcal{C})$ at Q and a positive real number δ, we shall have

$$|t(P_n)| =: \mathrm{dist}(P_n, Q) \ll |P_n|^{-\delta} \ll H(P_n)^{-\delta/\sharp(S)}. \tag{3.3.3}$$

If $\delta > 2\sharp(S)$, a direct application of Roth's Theorem would be sufficient to conclude. If, however, that $\delta < 2\sharp(S)$, inequality 3.3.3 would not suffice. Siegel's trick to overcome this difficulty consists in taking an unramified covering $\tilde{\mathcal{C}'} \to \tilde{\mathcal{C}}$ of $\mathcal{C}$. By Chevalley-Weil theorem, the integral points P_n lift to integral points $P'_n \in \mathcal{C}'_i(\mathcal{O}_S)$, in one of the finitely many twists of $\mathcal{C}'_i$ of $\mathcal{C}'$. We can suppose, since we may dispose of infinitely many integral points, that all of them lift to integral points on a same curve $\mathcal{C}'$. The rate of convergence at infinity of the P'_n is the same, since the given covering is unramified (even at infinity). On the other hand, the height of the new points P'_n is smaller then that of the P_n by a factor equal to the degree of the cover. Working with a cover of degree $> 2\sharp(S)/\delta$ one is in the situation of applying Roth's theorem and we may conclude.

In connection with Siegels' Theorem, we end this section by showing that the results about Thue-Mahler and hyperelliptic equations fit into this frame.

Let us start by proving that the algebraic curve defined by Thue's equation (3.1.2) is non-rational, as soon as the hypotheses appearing in the statement of Thue's Theorem are satisfied: this is the content of the following

Theorem 3.3.4. *Given a homogeneous form $F(X,Y) \in \mathbb{C}[X,Y]$ of degree $\deg F = d \geq 3$, with no repeated linear factors, for every non-zero complex number $c \in \mathbb{C}^*$ the equation*

$$F(x(t), y(t)) = c$$

has no solutions $(x(t), y(t)) \in \mathbb{C}(t)^2$ in non-constant rational functions.

Proof. Homogenizing, we are reduced to showing that the homogeneous equation

$$F(X,Y) = cZ^d$$

has no non-constant solutions in *coprime polynomials* $x(t), y(t), z(t) \in \mathbb{C}[t]$. Factoring the homogeneous form as in (3.1.5) and dividing all factors by $y(t)$ we obtain

$$\prod_{i=1}^{d} \left(\frac{x(t)}{y(t)} - \frac{\alpha_i}{\beta_i} \right) = C \left(\frac{z(t)}{y(t)} \right)^d ,$$

where $C = \frac{c}{\beta_1 \cdots \beta_d}$. Here we are assuming that all β_i are non-zero, but the proof would not be really different if (at most) one β_i vanishes. As mentioned, the points $\gamma_i := \alpha_i/\beta_i$, $i = 1, \dots, d$, are pairwise distinct. Each time the rational function $f(t) := x(t)/y(t)$ takes one of these values, the function $z(t)/y(t)$ takes the value zero. Since $\deg(z(t)/y(t)) \leq \deg f$, the cardinality of the set $f^{-1}(\{\gamma_1, \dots, \gamma_d\})$ cannot exceed $\deg f$; on the other hand, the pre-image of a set of cardinality d has at least $d \deg(f) - R$ points, where R is the degree of the ramification divisor of f; the latter is equal to $2\deg(f) - 2$ by Riemann-Hurwitz formula or direct computation. Hence $(d-3)\deg f + 2 \leq 0$ from which it follows that $d \leq 2$, finishing the proof. □

It is also easy to see that the number of points at infinity is precisely d; so the curves defined by Thue's equations have two good reasons for the set of their integral points to be finite.

We now consider the geometry of the algebraic curve defined by the hyperelliptic equation

$$y^2 = f(x), \tag{3.3.5}$$

where $f(X) \in \mathbb{C}[X]$ is a polynomial with no repeated factors. The above equation defines a smooth affine curve in the plane $\mathbb{A}^2$; however, whenever $\deg f \geq 4$ its natural completion in $\mathbb{P}_2$ turns out to be singular at its only point at infinity; its desingularization has two points at infinity. Let us denote by $\tilde{\mathcal{C}}$ this smooth projective model.

Theorem 3.3.6. *Let $f(X) \in \mathbb{C}[X]$ be, as before, a non-constant polynomial without repeated roots and let $\tilde{\mathcal{C}}$ be a smooth complete model of the affine curve defined by the above equation* (3.3.5)*. If $\deg f \geq 3$, then $\tilde{\mathcal{C}}$ is non-rational.*

Proof. One could apply the well-known genus formula to prove that the genus of $\tilde{\mathcal{C}}$ is $\frac{d}{2} - 1$ if $d = \deg f$ is even, $\frac{d-1}{2}$ if d is odd: hence it is > 0 whenever $d \geq 3$. Nevertheless, we prefer a proof which is closer in spirit to our proof of the finiteness of integral solutions. We exibit a non-zero class in $\mathrm{H}^1(\tilde{\mathcal{C}}, \{\pm 1\})$, recalling that this group is isomorphic to the quotient

$$\{f \in \mathbb{C}(\tilde{\mathcal{C}})^* \,:\, \mathrm{ord}_p(f) \equiv 0 \pmod 2 \quad \forall p \in \tilde{\mathcal{C}}\}/\{f^2 \,:\, f \in \mathbb{C}(\tilde{\mathcal{C}})^*\}.$$

In fact, supposing for simplicity $d \equiv 0 \pmod 2$, $d \geq 4$, and writing $f(X) = a(X - \alpha_1)\cdots(X - \alpha_d)$, for complex numbers $\alpha_1, \ldots, \alpha_d, a \in \mathbb{C}$, $a \neq 0$, we see at once that each rational function $x - \alpha_i$ has a double zero at $(\alpha_i, 0)$. It has a simple pole at each of the two points at infinity; so the product $f = (x-\alpha_1)(x-\alpha_2)$ is a square locally everywhere. Let us show that it is not globally a square in $\mathbb{C}(\tilde{\mathcal{C}})$; if it were so, we would have $\mathbb{C}(\tilde{\mathcal{C}}) = \mathbb{C}(x)(\sqrt{f})$; however, this extension is unramified over $x = \alpha_3$, while the extension $\mathbb{C}(\tilde{\mathcal{C}})/\mathbb{C}(x)$ does ramify over $x = \alpha_3$. □

3.4 A Subspace Theorem approach to Siegel's Theorem

The aim of this section is to provide a complete proof of Siegel's Theorem on curves assuming the Subspace Theorem (in the version given in Theorem 2.2.1).

Let us go back to the proof of Thue's theorem. Recall that the equation under examination was

$$F(x, y) = c,$$

where $F(X, Y) = \prod_{i=1}^{d}(\beta_i X - \alpha_i Y)$, $d \geq 3$, the linear factors are pairwise coprime and $c \neq 0$. Letting $\mathcal{C}$ be the algebraic curve defined by the above equation, the main point of the proof consisted in considering one of the rational functions $\beta_i x - \alpha_i y$ on $\mathcal{C}$, viewed as a morphism $\mathcal{C} \to \mathbb{A}^1$. We can extend it to the complete curve $\tilde{\mathcal{C}}$ (defined by the homogeneous equation $F(X, Y) = cZ^d$) by sending $\tilde{\mathcal{C}} \ni (X : Y : Z) \mapsto (\beta_i X - \alpha_i Y : Z) \in \mathbb{P}_1$. Then we applied Roth's theorem, i.e. a result on Diophantine approximation on the line. The choice of such a rational functions was dictated by the fact that it is regular on $\mathcal{C}$ (i.e. its poles lie at infinity) and vanishes at sufficiently high degree on an accumulation point for an infinite sequence of integral points on $\mathcal{C}$ (supposed to exist).

This strategy does not work in general: for instance, if a curve $\mathcal{C}$ has only one point at infinity, such a point will be an accumulation point for every infinite sequence of integral points on $\mathcal{C}$, and there exist no non-constant regular function on $\mathcal{C}$ vanishing at infinity. Even if there are more points at infinity, it may be that no function with the desired property exists. Let us see a concrete example:

`Example`. Consider the algebraic curve of equation

$$\mathcal{C} : x^3 - 2y^3 = x + y + 1. \tag{3.4.1}$$

Its genus is one, and moreover it has three points at infinity, so by Siegel's theorem it should have only finitely many integral points. Each sequence (x_n, y_n), $n \in \mathbb{N}$ in $\mathcal{C}(\mathbb{Z})$ should converge to the point $A := (\sqrt[3]{2} : 1 : 0) \in \mathbb{P}_2$ (considering the natural compactification $\tilde{\mathcal{C}}$ of $\mathcal{C}$ given by the equation $X^3 - 2Y^3 = Z^2(X + Y) + Z^3$). The other two points at infinity are $B := (\zeta\sqrt[3]{2} : 1 : 0)$ and $\bar{B} = (\bar{\zeta}\sqrt[3]{2} : 1 : 0)$, where ζ is a primitive third root of unity. Every regular function $f \in \kappa[\mathcal{C}]$ is a polynomial function of $x = X/Z$, $y = Y/Z$. If $\kappa = \mathbb{Q}$, then, since $A, B, \bar{B}$ are Galois-conjugated over $\mathbb{Q}$, such a function must have poles at each of the three points or be constant. However, working over the cubic field $\kappa = \mathbb{Q}(\sqrt[3]{2})$ we can find a function having a zero at A, for instance the function $x + \sqrt[3]{2}y$. Now from the equation (3.4.1) we deduce that

$$(x - \sqrt[3]{2}y) = \frac{x + y + 1}{x^2 + \sqrt[3]{4}xy + y^2}.$$

When the pair (x, y) tends to infinity (i.e. to A) on the curve $\mathcal{C}$ the asymptotic estimations $|x + y + 1| \gg \max(|x|, |y|) = |x|$ and $|x^2 + \sqrt[3]{4}xy + y^2| \ll \max(|x|, |y|) = x^2$ hold. Hence the left hand side tends to zero asymptotically as x^{-1}, not faster; dividing by y one obtains $|x/y - \sqrt[3]{2}| \ll H(x/y)^{-2}$ which is not sufficient to deduce a contradiction via Roth's theorem.

We can, however, try to consider more functions $f_1, \ldots, f_r \in \mathbb{Q}(\sqrt[3]{2})[\mathcal{C}]$, giving rise to a morphism $\mathcal{C} \to \mathbb{A}^r$, and then try to apply Diophantine approximation results in the larger space $\mathbb{A}^r$, like the Subspace Theorem.

Let us now give the details, following [15]. Precisely, we want to prove the following

Theorem 3.4.2. *Let $\mathcal{C}$ be a smooth affine curve with $r \geq 3$ points at infinity, defined over a number field κ. Then for every ring of S-integers $\mathcal{O}_S \subset \kappa$, the set $\mathcal{C}(\mathcal{O}_S)$ is finite.*

The full Siegel's theorem then follows by applying Chevalley-Weil theorem.

Proof. Let $Q_1, \ldots, Q_r$ be the points (valuations) at infinity of the curve $\mathcal{C}$. They are defined over a finite extension of κ. For a large integer N put

$$V_N = \mathrm{H}^0(\tilde{\mathcal{C}}, N(Q_1 + \ldots + Q_r)) = \{f \in \bar{\kappa}[\mathcal{C}] : (f) \geq -N(Q_1 + \ldots + Q_r)\}.$$

Let $f_1, \dots, f_d$, where $d = h^0(N(Q_1 + \ldots + Q_r)) = rN + O(1)$, be a basis of V_N. Since the divisor $Q_1 + \ldots + Q_r$ is defined over κ, we can choose $f_1, \dots, f_d$ defined over κ, i.e. with $f_i \in V_N \cap \kappa[\mathcal{C}]$ for $i = 1, \dots, d$.

As in the previous sketch of the proof, if $\mathcal{C}(\mathcal{O}_S)$ is infinite, we can find a sequence $P_1, P_2, \ldots$ of integral points in $\mathcal{C}(\mathcal{O}_S)$ such that for each place $\nu \in S$ the sequence converges to a point $R_\nu \in \tilde{\mathcal{C}}(\kappa_\nu)$. We let S' to be the set of places for which the limit R_ν lies at infinity.

After multiplying the f_j by a suitable constant, we can suppose that $f_j(P_n) \in \mathcal{O}_S$ for all j, n.

For every $\nu \in S$, consider the filtration $V = W_{\nu,1} \supset W_{\nu,2} \supset \ldots$ defined as

$$W_j = W_{\nu,j} = \{f \in V_N \,:\, \mathrm{ord}_{R_\nu} f \geq j - 1 - N\}.$$

We have $\dim(W_j/W_{j+1}) \leq 1$ for each j; in particular $\dim W_j \geq d - j + 1$.

Now, for each $\nu \in S'$, choose a basis of V_N containing a basis of each subspace $W_{\nu,j}$ (for each j such that $W_{\nu,j} \neq \{0\}$). These functions can be expressed as linear combinations of the basis $(f_1, \dots, f_d)$, i.e. as values of linear forms $L_{\nu,j}(f_1, \dots, f_d)$, where $L_{\mu,j}(X_1, \dots, X_d)$ has its coefficients in $\bar{\kappa}$. Clearly

$$\mathrm{ord}_{R_\nu} L_{\nu,j}(f_1, \dots, f_d) \geq j - N + 1.$$

For $\nu \in S \setminus S'$ we just put $L_{\nu,j}(f_1, \dots, f_d) = f_j$.

For each $\nu \in S'$ choose a local parameter $t_\nu \in \kappa(\mathcal{C})$ at R_ν. The above displayed inequality implies that

$$|L_{\nu,j}(f_1(P_n), \dots, f_d(P_n))|_\nu \ll |t_\nu(P_n)|_\nu^{j-1+N}.$$

Now, observe that we dispose of $d = rN + O(1)$ rational functions $L_{\nu,j}(f_1, \dots, f_d)$, of which at most N have poles and approximately $(r-1)N$ have zeros at R_ν. Estimating the order of the product $\prod_j L_{\nu,j}(f_1, \dots, f_d)$ we have that this order is positive, and actually $> (r-2)N + O(1)$ for large N (a stronger asymptotic estimates in fact holds, but we do not need it).

Put $\mathbf{x} = (f_1(P_n), \dots, f_d(P_n)) \in \mathcal{O}_S^d$ and let as before $|\mathbf{x}|_\nu$ be its sup-norm in the ν-adic absolute value. Observing that for $\nu \notin S'$ the absolute values of $f_j(P_n)$ are uniformly bounded, we can deduce that

$$\prod_{\nu \in S} \prod_{j=1}^{d} \frac{|L_{\nu,j}(\mathbf{x})|_\nu}{|\mathbf{x}|_\nu} \ll \prod_{\nu \in S'} \left(|t_\nu(P_n)|\right)^{(r-2)N}.$$

On the other hand, the height is easily estimated by $H(\mathbf{x}) \ll \prod_{\nu \in S'} \left(|t_\nu(P_n)|\right)^N$. Finally we obtain

$$\prod_{\nu \in S} \prod_{j=1}^{d} \frac{|L_{\nu,j}(\mathbf{x})|_\nu}{|\mathbf{x}|_\nu} \ll H(\mathbf{x})^{2-r}.$$

The Subspace Theorem then implies that infinitely many vectors $\mathbf{x}$ lie on a hyperplane; this is impossible, since the functions $f_1, \dots, f_d$ are linearly independent, so every non-trivial linear combination of $f_1, \ldots, f_d$ can have only finitely many zeros.

Another approach to Siegel's theorem on integral points involving nonstandard analysis has been proposed by Robinson and Roquette [46]. Their proof implicitly uses Mordell-Weil theorem on the Jacobian of the curve, although it does not mention explicitly Jacobians.

Finally, Gasbarri [33] gave a different proof of Siegel's theorem, which uses ideas coming from the proof of Thue-Siegel-Dyson-Gelfond theorem on Diophantine approximation. Basically, he reproves this approximation theorem for integral points lying on a curve, and deduces a finiteness statement whenever there are three points at infinity. □

Chapter 4
Hilbert Irreducibility Theorem

4.1 Hilbert Irreducibility Theorem

In this section we shall be interested in discussing proofs, generalizations and geometric formulations of the so-called Hilbert Irreducibility Theorem (HIT in the sequel).

Here is the original statement, proved by Hilbert in 1894:

Theorem 4.1.1 (Hilbert Irreducibility Theorem). *Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a polynomial, of degree ≥ 1 in Y, irreducible in the ring $\mathbb{Q}[X,Y]$. Then there exist infinitely many integers $n \in \mathbb{Z}$ such that the specialized polynomial $F(n,Y) \in \mathbb{Z}[Y]$ is irreducible in the ring $\mathbb{Q}[Y]$.*

In the case when $\deg_Y F \geq 2$, the only interesting one, as a corollary we obtain that:

Under the above hypothesis on the polynomial $F(X,Y)$, for infinitely many $n \in \mathbb{Z}$ the specialized polynomial $F(n,Y)$ has no rational root.

Consider the plane algebraic curve of equation $\mathcal{C} : F(x,y) = 0$; it is endowed with a map $\mathcal{C} \to \mathbb{A}^1$ defined by the x function: $\mathcal{C} \ni (x,y) \mapsto x \in \mathbb{A}^1$. The above weak conclusion of HIT asserts that the map $x : \mathcal{C}(\mathbb{Z}) \to \mathbb{Z}$ is not surjective. The full HIT predicts that for infinitely many points $n \in \mathbb{Z} = \mathbb{A}^1(\mathbb{Z})$, the preimage $x^{-1}(n)$ is irreducible, i.e. forms a single orbit for the natural action of the Galois group.

A natural generalization to several variables and arbitrary number fields reads as follows:

Theorem 4.1.2. *Let κ be a number field, $d \geq 1$ a positive integer, $F(X_1,\ldots,X_d,Y) \in k[X_1,\ldots,X_d,Y]$ an irreducible polynomial of degree ≥ 1 in Y. Then for a Zariski-dense set of rational points $(a_1,\ldots,a_d) \in \ \kappa^d$ the specialized polynomial $F(a_1,\ldots,a_d,Y) \in \kappa[Y]$ is irreducible.*

P. Corvaja, *Integral Points on Algebraic Varieties*, HBA Lecture Notes in Mathematics, DOI 10.1007/978-981-10-2648-5_4

We provide an equivalent geometric formulation:

Theorem 4.1.3. *Let V be an irreducible affine algebraic variety of dimension $d \geq 1$, $\pi : V \to \mathbb{A}^d$ a dominant morphism, all defined over a number field κ; there exists a Zariski-dense subset of rational points $(a_1, \dots, a_d) \in \mathbb{A}^d(\kappa) = \kappa^d$ such that each of their fibre $\pi^{-1}(a_1, \dots, a_d)$ is irreducible.*

By irreducible, we mean of course irreducible over κ; it will be a finite set of points of $V(\bar{\kappa})$, all conjugate over κ to a single point.

The link between Theorems 4.1.2 and 4.1.3 is clear: a polynomial $F(X_1, \dots, X_d, Y) \in \kappa[X_1, \dots, X_d, Y]$ defines the affine variety in $\mathbb{A}^{d+1}$ of equation $F = 0$, which is naturally endowed with a dominant morphism to the affine space $\mathbb{A}^d$ (projection on the first d coordinates). If the polynomial F is monic in Y, such a projection is also a finite map; we then speak of ramified covering of the affine space.

Remark. Since the affine spaces are simply connected, each covering of degree > 1 of $\mathbb{A}^d$ must ramify somewhere, actually over a codimension one subvariety.

Hilbert Irreducibility Theorem (H.I.T.) is in a sense a converse to the Chevalley-Weil Theorem discussed in the previous section. While the Chevalley-Weil theorem applies in the situation where an unramified covering of algebraic varieties is given (and it predicts a sort of surjectivity over the set of rational points) H.I.T. holds for certain coverings of rational varieties, which do ramify. A weak conclusion of H.I.T. is the non-surjectivity of the set-theoretic map between the sets of rational points.

We shall see in a moment that actually this seemingly weaker statement asserting non-surjectivity over rational points is in fact equivalent to the full H.I.T. provided one admits coverings by possibly reducible varieties. The following statement will be regarded as the general Hilbert Irreducibility Theorem, and will be proved to be equivalent to Theorem 4.1.2:

Theorem 4.1.4. *Let κ be a number field, X be an algebraic variety defined over κ of dimension d and $\pi : X \dashrightarrow \mathbb{A}^d$ a dominant rational map, also defined over κ. Suppose that π admits no section $\theta : \mathbb{A}^d \dashrightarrow X$. Then the set $\mathbb{A}^d(\kappa) = \kappa^d$ is not contained in the image $\pi(X(\kappa))$ of the rational points of X. Moreover, the set $\mathbb{A}^d(\kappa) \setminus \pi(X(\kappa))$ is Zariski-dense on $\mathbb{A}^d$.*

Remarks. (1) If X is irreducible, then the rational map π admits no section if and only if it has degree > 1; in general, the existence of a section is equivalent to the existence of an irreducible component of X where the restriction of π is a birational isomorphism to $\mathbb{A}^d$. (2) Due to the birational invariance of the above statement, the affine space $\mathbb{A}^d$ could be replaced by any κ-rational variety.

Following Serre [48] we call *thin* the sets of rational points which are images of morphisms admitting no section. Precisely:

Definition. Let Y be an algebraic variety defined over a field κ. A subset $A \subset Y(\kappa)$ is said to be *thin* with respect to κ if there exists an algebraic variety X with $\dim X \leq \dim Y$ and a rational map $\pi : X \dashrightarrow Y$ defined over κ such that π admits no sections and A is contained in the image $\pi(X(\kappa))$ of the rational points of X.

We can always decompose the variety X as $X = X' \cup X''$, for two closed subvarieties X', X'', where X' is of pure dimension $d = \dim X = \dim Y$ or is empty and every component of X'' (which might also be empty) has dimension $< d$. Now a rational map $\pi : X \to Y$ admits a section if and only if it is of degree one when restricted to a suitable irreducible component of X'. Also, note that the image of X'' is contained in a hypersurface of $\mathbb{A}^d$.

Hence thin sets in $\mathbb{A}^d$ according to Serre's definition above are union of sets of two kinds: (1) sets of rational points contained in a proper closed subvariety; (2) images of rational points of a variety of pure dimension d under a map admitting no rational section. Again, type (2) sets could be alternatively defined as finite union of images of rational dominant maps of degree > 1 defined on an *irreducible variety* of the same dimension.

We shall prove that those of type (1) are in fact contained in sets of type (2). This is the content of the following lemma (compare with [12], Lemma 5.2)

Lemma 4.1.5. *Let $Y \subset \mathbb{A}^d$ be a proper closed subvariety defined over a field κ. There exists an irreducible algebraic variety X of dimension d and a finite map $\pi : X \to \mathbb{A}^d$ of degree > 1 such that $Y(\kappa) \subset \pi(X(\kappa))$.*

Proof. Let $P(X_1, \ldots, X_d) \in k[X_1, \ldots, X_d]$ be a non-zero squarefree polynomial vanishing identically on Y. Let $X \subset \mathbb{A}^{d+1}$ to be the variety defined by the equation $Y^2 = P(X_1, \ldots, X_d)$. Then X is irreducible (since P is square-free, in particular not a square); projection $\pi : X \to \mathbb{A}^d$ onto the x-coordinates provides a finite map such that $Y(\kappa) \subset \pi(X(\kappa))$. □

In view of the above lemma, we could rephrase the definition of thin set by saying that a subset $Z \subset \mathbb{A}^d(k)$ is thin with respect to κ if it is contained in the image $\pi(X(\kappa))$ where X is a union of irreducible varieties each of dimension d and $\pi : X \to \mathbb{A}^d$ is dominant of degree > 1 on each component of X.

In view of the above consideration, Theorem 4.1.4 becomes equivalent to the statement where "variety of dimension d" is replaced by "variety of pure dimension d". Also, it is equivalent to the following statement: *the set $\mathbb{A}^d(\kappa)$ is not thin.* To justify that this last statement does imply also the last sentence of Theorem 4.1.4, namely that $\mathbb{A}^d(\kappa) \setminus \pi(X(\kappa))$ is Zariski-dense, note that if it were not, up to adding a type (1) subset to $\pi(X(\kappa))$ (which is possible by Lemma 4.1.5), we would obtain the emptiness of $\mathbb{A}^d(\kappa) \setminus \pi(X(\kappa))$, contrary to the fact that $\mathbb{A}^d(\kappa)$ is not thin.

Finally, it remains to us to prove Theorem 4.1.4 in some of its equivalent formulations discussed above and to prove that it formally implies the apparently stronger Theorem 4.1.3.

Proof of Theorem 4.1.4. We start by proving its 1-dimensional analogue:

Theorem 4.1.6. *Let $\mathcal{C}$ be an algebraic curve defined over a number field κ, $\pi : \mathcal{C} \dashrightarrow \mathbb{A}^1$ be a rational dominant map admitting no section. Then $\mathbb{A}^1(\kappa) \not\subset \pi(\mathcal{C}(\kappa))$.*

Proof. We easily reduce to the case where $\mathcal{C}$ is smooth and $\pi : \mathcal{C} \to \mathbb{A}^1$ is a finite morphism; this might affect the set $\pi(\mathcal{C}(\kappa))$ only by a finite set. Then decompose $\mathcal{C}$ into the union $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_r$ of its irreducible components. We know by hypothesis that the restriction $\pi_{|\mathcal{C}_i}$ has degree > 1 for each $i = 1, \ldots, r$ and we have to prove that $\mathbb{A}^1(\kappa) \not\subset \bigcup_{i=1}^r \pi(\mathcal{C}_i(\kappa))$. Let us choose a finite set S of places of κ containing the archimedean ones. Since the ring extension $\kappa[\mathcal{C}]/\pi^*\kappa[\mathbb{A}^1]$ is integral, after enlarging if necessary the set S, we can suppose that the ring extension $\mathcal{O}_S[\mathcal{C}]/\pi^*\mathcal{O}_S[\mathbb{A}^1]$ is also integral. By this we mean that the each component $\mathcal{C}_i$ is defined by an equation $P_i(X,Y) = 0$, where $P_i(X,Y) \in \mathcal{O}_S[X,Y]$ has S-integral coefficients, is monic in Y and the map $\pi : \mathcal{C} \to \mathbb{A}^1$ is the projection on the X-coordinate. Clearly, it suffices to prove that $\mathbb{A}^1(\mathcal{O}_S) \not\subset \pi(\mathcal{C}(\kappa))$, but in view of the integrality of the ring extension $\mathcal{O}_S[\mathcal{C}]/\pi^*\mathcal{O}_S[\mathbb{A}^1]$, each κ-rational pre-image of an S-integer is necessarily an S-integer point of $\mathcal{C}$. If $\mathcal{C}(\mathcal{O}_S)$ is finite, we are done, since $\mathbb{A}^1(\mathcal{O}_S) = \mathcal{O}_S$ is an infinite set. Otherwise, consider the different components $\mathcal{C}_i$ of $\mathcal{C}$ endowed with maps $\pi_i : \mathcal{C}_i \to \mathbb{A}^1$, for $i = 1, \ldots, r$. By hypothesis, for each $i \in \{1, \ldots, r\}$, the map $\pi_i : \mathcal{C}_i \to \mathbb{A}^1$ has degree > 1. Now, consider a non-constant polynomial $p(t) \in \mathcal{O}_S[t]$, which will be chosen later; it defines a finite morphism $p : \mathbb{A}^1 \to \mathbb{A}^1$. We can construct for each $i \in \{1, \ldots, r\}$ the *fiber product* $\mathcal{C}_i' \to \mathbb{A}^1$ of $\pi_i : \mathcal{C}_i \to \mathbb{A}^1$ and $p : \mathbb{A}^1 \to \mathbb{A}^1$, namely the curve

$$\mathcal{C}_i' := \{(\alpha, \beta) \in \mathcal{C}_i \times \mathbb{A}^1 \; : \; \pi_i(\alpha) = p(\beta)\},$$

endowed with its natural projection on $\mathbb{A}^1$, sending $(\alpha, \beta) \mapsto \beta$. Let us choose the polynomial $p(t)$ in such a way that each corresponding curve $\mathcal{C}_i'$ is irreducible and has positive genus. It suffices for this to choose $p(t) = t^3 + c$, where $c \in \mathcal{O}_S$ is chosen outside the zero branch locus of any of the π_i. Hence we have a choice working for all components $\mathcal{C}_i$. Now, the points of $\mathbb{A}^1$ which are both of the form $p(\beta)$ for $\beta \in \mathcal{O}_S$ and $\pi_i(\alpha)$, for $\alpha \in \mathcal{C}_i(\mathcal{O}_S)$, are images of S-integral points of $\mathcal{C}_i'$, by our construction of $\mathcal{C}_i'$. However, by Siegel's Theorem all the curves $\mathcal{C}_i'$ have only finitely many S-integral points; hence only finitely many of the points of the set $p(\mathcal{O}_S) \subset \mathbb{A}^1(\mathcal{O}_S)$ can be images of S-integral points of $\mathcal{C}$, so infinitely many of them lie outside $\pi(\mathcal{C}(\mathcal{O}_S))$. □

End of the proof of Theorem 4.1.4. Let us assume that $\pi : X \dashrightarrow \mathbb{A}^d$ is as above; again, one easily reduces to the case where $\pi : X \to \mathbb{A}^d$ is actually a morphism. Suppose by contradiction that $\mathbb{A}^d(\kappa) \setminus \pi(X(\kappa))$ is not Zariski-dense, so it is contained in a hypersurface $Z \subset \mathbb{A}^d$. Let us choose a line $l \subset \mathbb{A}^d$, defined over κ such that: (1) $l \not\subset Z$; (2) the pre-image $\pi^{-1}(l)$ is a curve; (3) $\mathcal{C}$ and $\pi_{|\mathcal{C}} : \mathcal{C} \to l$ admits no section. The existence of such a line can be proved by standard application of Bertini's theorem. Then Theorem 4.1.6 provides the desired contradiction. □

Proof of Theorem 4.1.3. As promised, we now prove Theorem 4.1.3, by deducing it from Theorem 4.1.4. Recall that we are given an irreducible affine variety V of dimension d and a dominant rational map $\pi : V \dashrightarrow \mathbb{A}^d$ of degree > 1. We want to prove that for a Zariski-dense set of rational points in $\mathbb{A}^d(\kappa)$, each pre-image is irreducible over κ. Again, it is easy to reduce to the case of dimension 1 and of a finite morphism $\pi : V \to \mathbb{A}^1$ (here V is an irreducible curve). We note at once that if the degree of π is two or three, then Theorem 4.1.4 immediately implies our conclusion: actually, if the pre-image of a point, which consists of two or three algebraic points, contains no rational point, it means that such pre-image is made of Galois conjugate elements (in other words: if a polynomial in one variable of degree two or three has no roots, then it is irreducible). To explain the strategy of our proof, let us consider the case of a map $\pi : V \to \mathbb{A}^1$ of degree four. Then, for a point $\alpha \in \mathbb{A}^1(\kappa)$, having a rational pre-image is not equivalent to having a reducible pre-image: it may be that the pre-image is made of two Galois orbits of quadratic points. Let us define the *fibered square* $V \times_\pi V$ of V with respect to π as

$$V \times_\pi V := \{(x, y) \in V \times V \, : \, \pi(x) = \pi(y)\};$$

it is a curve, endowed with a natural projection to $\mathbb{A}^1$; let us also define its symmetric fibered square as the quotient of the variety $V \times_\pi V$ by the natural involution interchanging x and y, and denote it by $V^{(2)}$; it is a reducible curve, contains canonically V via the diagonal embedding $V \hookrightarrow V \times_\pi V$. The reducible curve $V^{(2)}$ is still endowed with a natural projection to $\mathbb{A}^1$, which we denote by π_2. If π has degree 4, which we are assuming, then $\deg(\pi_2) = 4 + 6 = 10$. Now, for a point $\alpha \in \mathbb{A}^1(\kappa)$, the existence of a rational point in the pre-image $\pi_2^{-1}(\alpha)$ is equivalent to the reducibility of the pre-image $\pi^{-1}(\alpha) \subset V(\bar{\kappa})$. So, Theorem 4.1.4 implies the conclusion of Theorem 4.1.3 in this case.

The general case is analogous: if n denotes the degree of the map π, it suffices to consider the union of the curves $V^{(i)}$, where each $V^{(i)}$ is the i-th fold symmetric fiber product of V with itself (with respect to π), for $i = 1, \dots, [n/2]$. □

4.2 Universal Hilbert Sequences

Let us consider the simplest case treated by Hilbert himself, namely that of a polynomial $P(X, Y) \in \mathbb{Z}[X, Y]$, irreducible of degree ≥ 1 in Y. By Hilbert Irreducibility Theorem 4.1.1, there exists an infinite sequence $x_0 < x_1 < x_2, < \dots$ of integers such that the polynomial $P(x_n, Y)$ is irreducible in $\mathbb{Q}[Y]$ for every n. One can ask whether there exists a single sequence working for all irreducible polynomials: of course, we must neglect a finite set depending on the given polynomial, namely the precise question is: *does there exist a sequence $x_0 < x_1 < x_2, < \dots$ of integers such that for every irreducible polynomial $P(X, Y) \in \mathbb{Z}[X, Y]$ of positive degree in Y there exists an index $n_0(P)$ such that for every $n > n_0(P)$ the specialized polynomial $P(x_n, Y)$ is irreducible in $\mathbb{Q}[Y]$?* A positive answer to this question can be given via a diagonalization argument, starting from the original result of Hilbert. It is however tempting to search for explicit sequences with the above property. They are commonly called *Universal Hilbert Sequences*. The first examples, to our knowledge, have been provided by Sprindzuk [53]; other examples have been constructed by Bilu [5] and Dèbes and Zannier [24].

We shall content to show one example, drawn from the paper [14], which classifies Universal Hilbert Sequences among power sums. By a power sum we mean in this context a function $\mathbb{N} \to \mathbb{Q}$ of the form

$$n \mapsto u(n) = b_1 a_1^n + \ldots + b_k a_k^n,$$

where $k \in \mathbb{N}$ and $a_1, \ldots, a_k$ are natural number and $b_1, \ldots, b_k$ are rational numbers. Theorem 4 of [14] reads as follows:

Theorem 4.2.1. *Let $u : \mathbb{N} \to \mathbb{Q}$ be a power sum as above. The following are equivalent:*

(1) the sequence $u(0), u(1), \ldots$ is a Universal Hilbert Sequence;

(2) there exist no integer $d \geq 2$, polynomial $P(X) \in \mathbb{Q}[X]$ of degree d and power sum $v : \mathbb{N} \to \mathbb{Q}$ such that identically $u(nd) = P(v(n))$.

As an example, the sequence $n \mapsto 2^n + 3^n$ is a U.H.S.. Clearly, it is not the case for the sequence $n \mapsto u(n) := 2^n$, or any other geometric progression; actually for the last sequence u, note that putting $P(X) = X^2$ one has $u(2n) = P(u(n))$, so condition (2) is not satisfied.

We now give a sketch of the proof that the sequence $u(n) := 2^n + 3^n$ is a U.H.S.; the general proof of Theorem 4.2.1 is obtained by following the same path.

As in the deduction of Theorem 4.1.3 from Theorem 4.1.4, we reduce to proving the following:

Proposition 4.2.2. *Let $P(X,Y) \in \mathbb{Z}[X,Y]$ be an irreducible polynomial of degree $d \geq 2$ in Y. Then the equation $P(2^n + 3^n, y) = 0$ has only finitely many solutions $(n, y) \in \mathbb{N} \times \mathbb{Z}$.*

Proof. Suppose by contradiction that the equation $P(2^n + 3^n, y) = 0$ has infinitely many integral solutions. Then by Siegel's finiteness theorem on integral points (Theorem 3.3.1), the curve of equation $P(X,Y) = 0$ must have genus zero and only one or two points at infinity. In algebraic language, there exist two non-constant rational functions $f(t), g(t)$ such that $P(f(t), g(t)) \equiv 0$, and such that for infinitely many $n \in \mathbb{N}$, $2^n + 3^n = f(t_n)$ for a suitable $t_n \in \mathbb{Q}$. Moreover, the degree of $f(t)$ equals $d = \deg_Y P$ and $f(t), g(t)$ can have only one or two poles (all together). In the first case, after a change of variables, we obtain that $f(t), g(t) \in \mathbb{Q}[t]$ are polynomials. We then have, again by our assumptions on the infinitude of the integral solutions to the original equation, that the equation $2^n + 3^n = f(t)$ has infinitely many solutions $(n, t) \in \mathbb{N} \times \mathbb{Q}$. After a translation of the form $t \mapsto t + c$, we can suppose that the polynomial $f(t) \in \mathbb{Q}[t]$ is of the form $f(t) = at^d + a_2 t^{d-2} + \ldots + a_d$. Since the denominators of t must be bounded, we can suppose after another change of variable that t is in fact an integer, so the equation $2^n + 3^n = f(t)$ has infinitely many integral solutions, where $f(t)$ has degree d and no term of degree $d-1$. In particular, for infinitely many pairs $(n, t) \in \mathbb{N} \times \mathbb{Z}$ we shall have

$$|2^n + 3^n - at^d| \ll |t|^{d-2}.$$

Working on each arithmetic progression modulo d and writing $n = md + r$, we can say that for at least one value of $r \in \{0, \dots, d-1\}$ and a positive real number c_1, the Diophantine inequality

$$|2^r 2^{md} + 3^r 3^{md} - at^d| < c_1 |t|^{d-2}$$

has infinitely many integral solutions $(m, t) \in \mathbb{N} \times \mathbb{Z}$. □

Now we can rewrite the above inequality as

$$\left| \frac{2^r 2^{md} + 3^r 3^{md}}{t^d} - a \right| < c_1 |t|^{-2},$$

so

$$\left| \frac{3^{r/d} 3^m \sqrt[d]{1 + 2^r 2^{md} 3^{-r} 3^{-md}}}{t} - a^{1/d} \right| < c_2 |t|^{-2},$$

for a suitable constant c_2. Here $3^{r/d}$ and $a^{1/d}$ denote suitable real d-th roots of 3^r and a. Now let us express by Taylor development $\sqrt[d]{1+u}$ as $1 + \delta_1 u + \delta_2 u^2 + O(u^3)$ where δ_1, δ_2 are the rational numbers $\delta_1 = \binom{1/d}{1} = \frac{1}{d}, \delta_2 = \binom{1/d}{2} = \frac{1-d}{2d^2}$. Putting $\alpha_i = \delta_i \cdot \frac{2^{ri}}{3^{ri}}$ for $i = 1, 2$ and noting that $\frac{2^{6m}}{3^{6m}} \ll t^{-2}$ (since t tends to infinity as 3^m), we obtain from the above displayed inequality that

$$\left| \left(\frac{3^{r/d} 3^m}{t} \right) \left(1 + \alpha_1 \frac{2^{md}}{3^{md}} + \alpha_2 \frac{4^{md}}{9^{md}} \right) - a^{1/d} \right| < c_2 \frac{1}{t^2}.$$

Observe that the term $\frac{3^{r/d} 3^m}{t}$ converges to a non-zero limit for $m \to \infty$; so after multiplying both sides by $9^{md} \cdot \frac{t}{3^{r/d} 3^m}$ we obtain we obtain that the inequality

$$|9^{md} + \alpha_1 6^{md} + \alpha_2 4^{md} - a^{1/d} 3^{-r/d} t 3^m| < c_3 9^{(d-1)m} \tag{4.2.3}$$

holds for infinitely many positive integers m. Note that the left-hand side is a linear combination, with algebraic coefficients, of S-units and an S-integer: namely, it is the value of a homogeneous linear form at the point

$$\mathbf{x} = (9^{md}, 6^{md}, 4^{md}, t3^m) \in \mathcal{O}_S^{*\,3} \times \mathcal{O}_S,$$

where $\mathcal{O}_S = \mathbb{Z}[1/6]$. We now proceed to apply the Subspace Theorem, with $\kappa = \mathbb{Q}$, $N = 4$, S consisting of the archimedean absolute value and the 2-adic and 3-adic ones. Let us define the following linear forms: for the archimedean place, denoted by ∞, put $L_{\infty,1}(X_1, \dots, X_4) = X_1 + \alpha_1 X_2 + \alpha_2 X_3 - a^{1/d} 3^{-r/d} X_4$, then complete to a basis by putting $L_{\infty,i}(X_1, \dots, X_4) = X_i$ for $i = 2, 3, 4$. For each p-adic place ($p = 2, 3$), put $L_{p,i} = X_i$. The double product appearing in the statement of the Subspace Theorem becomes

$$\prod_{i=1}^{4} \prod_{\nu \in \{\infty, 2, 3\}} |L_{i,\nu}(\mathbf{x})|_\nu \le 9^{-md} \cdot t \cdot c_3 9^{(d-1)m} \le c_4 3^{-m}.$$

Since the height of the point $\mathbf{x}$ is $\ll 9^{md}$, the Subspace Theorem 2.2.4, applied with any $\epsilon < 1/(2d)$, implies that all but finitely many solutions to the inequality (4.2.3) satisfy finitely many linear dependence relations with integral coefficients. But now, this would yield that a relation like $t = b_1 3^m + b_2 2^{md} 3^{(1-d)m} + b_3 4^{md} 3^{-(2d-1)m}$, for suitable rational numbers b_1, b_2, b_3, would hold infinitely often; this is impossible: by integrality considerations, b_2, b_3 would vanish, and we would have $t = b_1 3^m$; however, an equation like

$$P(2^r 2^{md} + 3^r 3^{md}, 3^{md}) = 0$$

can have only finitely many solutions $m \in \mathbb{N}$.

The case where the rational functions f and g parametrizing the curve $P(X, Y) = 0$ have two poles is similar; details can be found in [14], [60] and [6].

4.3 Hilbert Irreducibility over algebraic groups

In this section, where we give no proofs at all, we shall connect Hilbert irreducibility theory with algebraic groups. Let us start from the original version given by Hilbert himself. Recall that it can be rephrased by saying that given a curve $\mathcal{C}$ and a morphism $\pi : \mathcal{C} \to \mathbb{A}^1$ from the curve to the line, the set $\mathbb{N}$ of natural numbers cannot be contained in the image $\pi(\mathcal{C}(\mathbb{Q}))$ of the rational points on $\mathcal{C}$ (unless the map $\pi : \mathcal{C} \to \mathbb{A}^1$ admits a section).

Now, observe that the line $\mathbb{A}^1$ is the underling algebraic variety of the additive group $\mathbb{G}_a$ and that the set $\mathbb{N}$ of natural numbers is a Zariski-dense sub-semigroup. It is then natural to try to ask the following: *given an algebraic group G defined over a number field κ, a variety V of the same dimension as G and a dominant map $\pi : V \to G$ admitting no section, and given a Zariski-dense sub-semigroup $\Gamma \subset G(\kappa)$, the set Γ cannot be contained in the image $\pi(V(\kappa))$ of the rational points of V.*

Actually, the above statement does not hold, as shown by the simple example below:

Example. Choose $\kappa = \mathbb{Q}$ and $G = V = \mathbb{G}_m$ to be the multiplicative group, and $\pi : \mathbb{G}_m \to \mathbb{G}_m$ be the degree-2 isogeny: $\pi(x) = x^2$. Letting $\Gamma = \{4^n : n \in \mathbb{N}\}$, say, we have that Γ is entirely contained into $\pi(\mathbb{G}_m(\kappa))$.

More generally, whenever V is itself an algebraic group and $\pi : V \to G$ an isogeny, one can construct a counterexample by choosing first a Zariski-dense subgroup in $V(\kappa)$ taking for Γ its image. Starting with the group $\mathbb{G}_a$ this will not be possible, since the latter is simply connected.

It is then natural to ask if such counterexamples are in a sense the only possible ones. In the case of linear algebraic groups, this is the content of the following result, proved in [12]:

Theorem 4.3.1. *Let G be a connected linear algebraic group defined over a number field κ; let V be an algebraic variety with* $\dim V = \dim G$ *and* $\pi : V \dashrightarrow$

G a rational dominant map, all defined over κ. Let $\Gamma \subset G(\kappa)$ be a Zariski-dense sub-semigroup. If $\Gamma \subset \pi(V(\kappa))$ then there exists an algebraic group G', an isogeny $p : G' \to G$ and a rational map $\theta : G' \dashrightarrow V$, all defined over κ, such that $\pi \circ \theta = p$.

Let us see that a particular but significant case is connected with Theorem 4.2.1: consider the case where $G = \mathbb{G}_m^2$ is the two-dimensional torus, Γ is the semigroup generated by the pair $(2, 3) \in \mathbb{G}_m^2$; it is Zariski-dense, since the two numbers 2 and 3 are multiplicatively independent. Take any irreducible polynomial $P(X, Y) \in \mathbb{Q}[X, Y]$ of degree ≥ 2 in Y. Then the surface $V \subset \mathbb{G}_m^2 \times \mathbb{A}^1$ defined by the equation $P(X_1 + X_2, Y) = 0$, provided with the projection $\pi : (X_1, X_2, Y) \mapsto (X_1, X_2)$, gives an example of a ramified covering of $\mathbb{G}_m^2$ admitting no section. Theorem 4.2.1 assures that only finitely many points of Γ have a rational pre-image in V, so in particular $\pi(V(\mathbb{Q}))$ does not contain Γ.

More generally, one can consider Diophantine equations involving linear recurrent sequences. We recall that a linear recurrent sequence is a sequence $u : \mathbb{N} \to \kappa$ which can be expressed in the form

$$u(n) = \sum_{i=1}^{h} p_i(n)\alpha_i^n,$$

where $p_1(T), \dots, p_h(T)$ are polynomial in $\bar{\kappa}[T]$ and $\alpha_1, \dots, \alpha_h \in \bar{\kappa}^*$, called *roots* of the recurrence, are non-zero scalars.

Consider the simple-looking Diophantine equation like $u(n) = y^2$, to be solved in $(n, y) \in \mathbb{N} \times \kappa$, which consists in finding perfect squares (in a given number field) in a linear recurrent sequence. We shall show how this equation can be viewed as a problem on integral points on covers of algebraic groups. Namely, let d be the multiplicative rank of the group generated by the roots, which we suppose for simplicity to be torsion-free (we can however always reduce to this case); let $\beta_1, \dots, \beta_d$ be a basis for this multiplicative group. Put $G = \mathbb{G}_a \times \mathbb{G}_m^d$ and let Γ be the cyclic group generated by $\gamma := (1, \beta_1, \dots, \beta_d)$. For simplicity, we suppose that each α_i, so each β_i, is κ-rational (so the same holds for the polynomials p_i); in that case Γ consists of κ-rational points of G and the sequence u can be expressed as $u(n) = f(\gamma^n)$, where $f \in \kappa[G]$ is a regular function on G. Now, let $V \subset \mathbb{G}_m^d \times \mathbb{A}^1$ be defined by the equation $Y^2 = f(X_1, \dots, X_d)$. Projection $\pi : V \to \mathbb{G}_m^2$ onto the X coordinates provides a dominant map without sections, unless the given linear recurrent sequence is identically a square (i.e. a square in the ring of linear recurrent sequences). One can then conjecture finiteness of integral solutions to the original equation, which would follow (via an elementary reasoning) from the degeneracy of integral points on V.

A theorem of Zannier [59] (previously a conjecture of Pisot) proves that the sequence cannot take *always* perfect square values in a given number field, thus proving that the projection $\pi(V(\kappa))$ cannot contain Γ; this is exactly the content of Theorem 4.3.1 in that case. More generally, Ferretti and Zannier [32] proved Theorem 4.3.1 for variety V and map $\pi : V \to \mathbb{G}_a \times \mathbb{G}_m^d$, at least whenever Γ is cyclic. The extension to arbitrary linear algebraic groups, provided in Theorem 4.3.1, is based on that result, and carried out in [12].

As mentioned, at least when G is a torus, and $\pi : V \to G$ is a finite map, admitting ramification (which prevents V to be a torus itself) one could conjecture that in fact $V(\mathcal{O}_S)$ is degenerate. This would follow from Vojta's conjecture, and would e.g. imply the finiteness of the solutions to equations of the form $y^d = 2^a + 3^b + 1$, which we already mentioned (and will be reconsidered again in the next chapter). For $d = 2$ and $\kappa = \mathbb{Q}$, the above equation has been solved completely by Leitner [36], using *ad hoc* methods.

Of course, it is worthwhile to consider also the case of non-linear algebraic groups. Whenever G is a simple abelian variety, and V is an irreducible algebraic variety provided with a dominant morphism $V \to G$, then either V is itself is an abelian variety (which happens if and only if the morphism is unramified), or V is of general type. In the second case its integral (i.e. rational) points should be degenerate. This particular case of Lang-Vojta conjecture, however, is far from being proved at present. A weaker statement, suggested by Serre, is that whenever $G(\kappa)$ is Zariski-dense, $\pi(V(\kappa))$ should not coincide with $G(\kappa)$, or even should be sparse in some sense. Partial results in this direction are the object of the paper [62].

Chapter 5
Integral points on surfaces

Let us now consider two-dimensional problems, i.e. problems reducing to the distribution of integral points on surfaces.

Let us start with the question of the density of rational points: given a smooth *projective* surface $\tilde{X}$ defined over a number field, we would like to decide whether there exists a number field κ, containing a field of definition for $\tilde{X}$, such that the set $\tilde{X}(\kappa)$ of κ-rational points of $\tilde{X}$ is Zariski-dense. Unlike the case of curves, this problem is by far still open.

It is natural to see what would result assuming Vojta's conjecture, which in our case boils down to Bombieri's conjecture. We recall the (classical) birational classification of algebraic surfaces (see e.g. [3]).

- Rational surfaces. These are the surfaces birationally isomorphic to the plane; it is the case of all smooth hypersurfaces of degree ≤ 3 in projective 3-space.
- Ruled surfaces, i.e. surfaces birationally isomorphic to a product $\tilde{\mathcal{C}} \times \mathbb{P}_1$, where $\mathcal{C}$ is a curve (if $\mathcal{C}$ is the line, then the resulting surface will be rational).
- Elliptic surfaces. They can be thought of as elliptic curves over a 1-dimensional function field; in other words they are surfaces admitting a dominant map $\tilde{X} \dashrightarrow \tilde{\mathcal{C}}$ whose generic fibre has genus one. Unlike other authors, we do not exclude that they are also ruled or rational, K3,....
- Abelian surfaces, i.e. abelian varieties of dimension two.
- K3 surfaces. These are (smooth projective) surfaces which are simply connected and whose canonical bundle is trivial. Being simply connected, they admit no non-zero regular 1-forms, so their cotangent bundle is certainly not trivial, unlike what happens for abelian surfaces. They might admit a fibration to $\mathbb{P}_1$, with elliptic generic fiber, so they can be elliptic in our sense. All smooth quartics in $\mathbb{P}_3$ are K3 surfaces, as well as the smooth hypersurfaces of multi-degree $(2,2,2)$ in $\mathbb{P}_1^3$.
- Kummer, bielliptic and Enriques surfaces. They are obtained as quotients of abelian or $K3$ surfaces. For instance, a Kummer surface is the desingularization of a quotient of the form $A/\pm\mathrm{Id}$, where A is an abelian surface and $-\mathrm{Id}$ is the involution of A sending $P \mapsto -P$.

P. Corvaja, *Integral Points on Algebraic Varieties*, HBA Lecture Notes in
Mathematics, DOI 10.1007/978-981-10-2648-5_5

- Surfaces of general type: all the remaining ones. They are characterised by having a canonical divisor which is big. It is the case for all smooth hypersurfaces of $\mathbb{P}_3$ of degree ≥ 5.

According to the Bombieri-Lang-Vojta conjecture, the latter should have only degenerate sets of integral points. For instance, every smooth surface in $\mathbb{P}_3$ of degree ≥ 5 should have only degenerate rational points.

Concerning the other classes: the rational surfaces have a Zariski-dense set of rational points over a suitable number field. The same is true of abelian surfaces and *a fortiori* holds for their quotients. One can conjecture the same conclusion for general K3 surfaces, but this is established only in particular cases.

Whenever a surface $\tilde{X}$ admits a dominant map $\tilde{X} \dashrightarrow \tilde{\mathcal{C}}$ to a curve of genus ≥ 2, then by Faltings' theorem its rational points are contained in finitely many fibers of such a map (plus possible indetermination points), so they are not Zariski dense. This excludes ruled surfaces, apart those having a rational base (rational surfaces) or an elliptic base; for these, the rational points are Zariski dense, over a suitable number field.

We shall concentrate now on *integral points*, so our geometric datum will be a pair $(\tilde{X}, D)$, where $\tilde{X}$ is smooth projective and $D \subset \tilde{X}$ is a divisor. We shall be interested in S-integral points with respect to D. As usual, such a set will be denoted by $X(\mathcal{O}_S)$, where $X = \tilde{X} \setminus D$ is the corresponding quasi-projective surface.

We recall from §1.2 a general result of Vojta: *let A be a semi-abelian variety, $X \subset A$ a closed irreducible subvariety, both defined over a ring of S-integers of a number field. If X is not a translate of a subgroup of A, then the set $X(\mathcal{O}_S)$ of its integral points is not Zariski-dense.*

Such a theorem applies also to varieties which cannot be embedded into semi-abelian varieties, but admit morphisms to a semi-abelian variety, whose image is not a (translate of a) subgroup: an example in the compact case has been shown above, where a morphism from a surface $\tilde{X}$ to a curve $\tilde{\mathcal{C}}$ of genus ≥ 2 can be prolonged to a morphism $\tilde{X} \to \tilde{\mathcal{C}} \hookrightarrow J(\tilde{\mathcal{C}})$ to the Jacobian of that curve.

Hence, given an algebraic variety X, realized as $\tilde{X} \setminus D$, for a smooth complete variety $\tilde{X}$ and a hypersurface D, it is natural to look at all possible morphisms $X \to A$ to semi-abelian varieties A. These morphisms are in some sense classified by the so-called generalized Albanese variety, which is constructed by integrating logarithmic 1-forms: it is an extension of the ordinary Albanese variety of $\tilde{X}$ by a torus, which depends on the divisor at infinity D. It has the property that every morphism $X \to A'$, where A' is any semi-abelian variety, factors through the generalized Albanese of X. By removing a 'sufficiently big' divisor D, the dimension of the toric part increases and eventually one manages to embed the resulting variety into a semi-abelian one (actually even in a torus). From the algebraic point of view, this operation corresponds to producing many never vanishing regular functions on X, whose values at S-integral points will be S-units. However, if the divisor at infinity is 'too small', it may be that the generalized Albanese variety has dimension $\leq \dim X$; in that case Vojta's theorem will not be applicable. One such case occurs whenever X is simply connected (by this we mean that the topological space $X(\mathbb{C})$ is simply connected): in that case the generalized Albanese variety reduces to one point, and every map to a semi-abelian variety will be constant. Also, whenever X is rational the compact factor of its generalized Albanese, i.e. the ordinary Albanese variety of $\tilde{X}$, vanishes, so Vojta's theorem applies if and only if the S-unit equation theorem can be applied.

It is then particularly interesting to study the distribution of integral points on rational surfaces, also in view of the fact that the rational points on such surfaces are Zariski-dense (up to enlarging the base field).

In next paragraph, we present some recent results which in particular can be applied to prove degeneracy of integral points on some surfaces to which methods based on semi-abelian varieties cannot be used.

5.1 The Subspace Theorem approach

Let, as before, $\tilde{X}$ be a smooth projective surface defined over a number field κ, $D = D_1 \cup \ldots \cup D_r$ be a finite union of curves on $\tilde{X}$. We try to prove, under suitable conditions on D, that the integral points on $X = \tilde{X} \setminus D$ are not Zariski-dense. Let us try to repeat the argument, based on the Subspace Theorem, that we used for curves in §3.4. Letting $V_N = \mathrm{H}^0(\tilde{X}, ND)$ be the space of regular functions on X having poles of degree at most N at infinity, we look for the subspaces $W_{i,j} := H^0(\tilde{X}, ND - jD_i)$ of those functions which moreover have a zero of order at least $j - N$ at D_i (or a pole of order $\leq N - j$ if $j \leq N$). Unlike the case of curves, the cost of each vanishing condition on D_i depends on the curve D_i and also on j; there is no uniform upper bound for the codimension of $W_{i,j}$ in $W_{i,j-1}$. We can see this fact already from a simple example in $\mathbb{P}_2$: take $r = 2, D_1$ the line at infinity and D_2 another curve. Take $j = N + 1$, so $W_{2,j-1}$ is the space of polynomials of degree $\leq N$ while $W_{2,j}$ is the subspace of those polynomials vanishing on the curve D_2. Letting d be the degree of D_2 and $f(x, y) = 0$ an affine equation for D_2, we have that each polynomial in $W_{2,j}$ is of the form $f(x, y)g(x, y)$ for a polynomial $g(x, y)$ of degree $\leq N - d$. Hence the codimension of $W_{2,j}$ in $W_{2,j-1}$ is equal to $\binom{N+2}{2} - \binom{N+2-d}{2}$, provided $d \leq N$. At the next step, we will have to calculate the codimension of $W_{2,j+1}$ in $W_{2,j}$; this will be equal to $\binom{N+2-d}{2} - \binom{N+2-2d}{2}$.

In general, we dispose of an upper bound for such codimension, in terms of intersection indices of D with the D_i. The general estimate is the following:

Lemma 5.1.1. *Let $\tilde{X}$ be a smooth complete surface, D a divisor on $\tilde{X}$, $\mathcal{C}$ an irreducible curve on $\tilde{X}$. Then* $\dim(\mathrm{H}^0(\tilde{X}, D)/\mathrm{H}^0(\tilde{X}, D - \mathcal{C})) \leq \max\{0, 1 + (D.\mathcal{C})\}$.

Proof. The proof is obtained via standard cohomological methods: consider the short exact sequence of sheaves on $\tilde{X}$:

$$0 \to \mathcal{O}_{\tilde{X}}(D - \mathcal{C}) \to \mathcal{O}_{\tilde{X}}(D) \to \mathcal{O}_{\tilde{X}}(D)_{|\mathcal{C}} \to 0.$$

The long-exact on cohomology gives an embedding

$$H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D))/H^0(\tilde{X}, \mathcal{O}_{\tilde{X}}(D-\mathcal{C})) \hookrightarrow H^0(\mathcal{C}, \mathcal{O}_{\tilde{X}}(D)_{|\mathcal{C}}).$$

The last vector space is the space of sections of a line bundle of degree $D \cdot \mathcal{C}$ on the curve $\mathcal{C}$, hence its dimension is bounded as in the Lemma. □

As a consequence, we do not obtain any degeneracy result for integral points simply assuming to have a large number of curves at infinity (such a result would be trivially false, anyway), but we must assume some inequalities on the intersection matrix.

The main result in [16] (see also [19]) reads as follows:

Theorem 5.1.2. *Let $\tilde{X}$ be a smooth projective surface, $D_1, \ldots, D_r$ be irreducible curves, no three of them intersecting. Assume there exist positive integers $p_1, \ldots, p_r$ such that*

- *the divisor $D = p_1 D_1 + \ldots + p_r D_r$ is big and numerically effective;*
- *for each $i = 1, \ldots, r$, letting ξ being the minimal (real) solution to the equation*
$$D_i^2 \xi^2 - 2(D.D_i)\xi + D^2 = 0,$$
the inequality
$$2\xi D^2 > (D.D_i)\xi^2 + 3p_i D^2 \qquad (5.1.3)$$
holds.

Then the set $X(\mathcal{O}_S)$ of S-integral points on $X := \tilde{X} \setminus |D|$ is not Zariski-dense.

One can moreover prove that the Zariski closure of the set $X(\mathcal{O}_S)$ consists of a finite set depending on the number field κ and on S plus a finite union of curves from a set which only depends on X. We postpone to the end of this paragraph a sketch of the proof of Theorem 5.1.2; full details are given in [16]; see also Theorem 5.2, Corollaries 5.6 and 5.7 in [6] and the subsequent proofs provided therein.

The numerical condition on the intersection products might look cumbersome, but some concrete examples show that the above statement is in a sense optimal. In fact, Levin [37] deduced from it the following nice corollary, (see also Theorem 5.8 of [6]):

Corollary 5.1.4. *Let $\tilde{X}$ be a smooth projective surface, $D_1, \ldots, D_4$ be irreducible curves, no three of which intersect. Suppose that each curve D_i is a big divisor. Put $X = \tilde{X} \setminus (D_1 \cup \ldots \cup D_4)$. Then $X(\mathcal{O}_S)$ is not Zariski-dense.*

The example of three lines in general position on the plane, whose complement is isomorphic to $\mathbb{G}_m^2$, shows that the requirement of having at least four big curves at infinity cannot be weakened. Also, the example of the four divisors in $\mathbb{P}_1 \times \mathbb{P}_1$ provided by two horizontal and two vertical lines, whose complement is again $\mathbb{G}_m^2$, shows that one cannot remove completely the ampleness hypothesis.

Another corollary is the following (see [16], Theorem 1):

Corollary 5.1.5. *Let $\tilde{X}$ be as before, $D_1, \dots, D_5$ be five curves, no three of them intersecting. Put $X = \tilde{X} \setminus (D_1 \cup \ldots \cup D_5)$. Suppose that $D_i^2 = 0$ for $i = 1, \dots, 5$ and for suitable positive integers $p_1, \dots, p_5, c$, $p_i p_j (D_i . D_j) = c$ for all $i \neq j$. Then $X(\mathcal{O}_S)$ is not Zariski-dense.*

Again, easy counterexamples are constructed with only four divisors as above.

A typical example of a rational surface is provided by cubic surfaces in $\mathbb{P}_3$; the theory of smooth cubic surfaces is classical; in particular, it is well-known that each smooth cubic surface contains exactly twenty-seven lines (over an algebraically closed field), and that each such line is contained in a hyperplane section consisting of three lines. The canonical divisors of such surfaces are equivalent to the opposite of a hyperplane section. Hence, after Vojta's conjecture one should obtain degeneracy of integral points on any open set obtained by removing two hyperplanes sections (not sharing components).

One corollary of Theorem 5.1.2 provides exactly this conclusion, but demands that such hyperplane sections be completely reduced:

Corollary 5.1.6. *Let $\tilde{X}$ be a smooth cubic surface in $\mathbb{P}_3$ and let $D_1, \dots, D_6$ be six lines lying in two planes, no three of them intersecting. Put $X = \tilde{X} \setminus (D_1 \cup \ldots \cup D_6)$. Then $X(\mathcal{O}_S)$ is not Zariski-dense.*

This is Theorem 1 in [22]. Again, the number of lines to be removed cannot be lowered, and the requirement that they lie in two planes cannot be omitted. Other corollaries of Theorem 5.1.2 will be given in the following paragraph.

As promised, we give a sketch of the proof of Theorem 5.1.2, following closely §3 of [16].

First remark that the theorem would follow if we prove that for each infinite set of integral points there exists a curve containing infinitely many of them. This equivalence is obtained by numbering all the curves on the surface which are defined over the given number field. Secondly, we reduce to the case where all the divisors D_i are defined over a the fixed given field, denoted by κ.

Let $\{P_i\}_{i \in \mathbb{N}}$ be an infinite sequence of pairwise distinct integral points on X. By the above observation, we may suppose that for each place $\nu \in S$, the sequence converges to a point $P_\nu \in \tilde{X}(\kappa_\nu)$.

For a positive integer N, which will be taken to be sufficiently large at the end of the proof, we denote by V_N the vector space

$$V_N = \mathrm{H}^0(\tilde{X}, ND) = \{\varphi \in \kappa(\tilde{X}) \, : \, \mathrm{div}(\varphi) + ND \geq 0\}.$$

It is a finite dimensional sub-vector space of the ring $\kappa[X]$ of regular functions on $X = \tilde{X} \setminus D$. By the asymptotic Riemann-Roch theorem, its dimension satisfies

$$d = d_N := \dim V_N = \frac{D^2}{2} N^2 + O(N)$$

for $N \to \infty$. (Note that $D^2 > 0$ by the assumption that D is big and nef). Let $\varphi_1, \ldots, \varphi_d$ be any base of V_N. After multiplying by a suitable non-zero scalar, we may suppose that each $\varphi_j(P_i)$ lies in the ring $\mathcal{O}_S$.

Our aim is to construct, for each place $\nu \in S$, independent linear forms $L_{1,\nu}, \ldots, L_{d,\nu}$ in $\varphi_1, \ldots, \varphi_d$, which will be ν-adically 'as small as possible' when calculated on the sequence of integral points $P_1, P_2, \ldots$. More precisely, we would like to have the bound

$$\prod_{j=1}^{d} |L_{j,\nu}(P_i)|_\nu \ll \left(\max_j(|\varphi_j(P_i)|_\nu)\right)^{-\mu_\nu} \tag{5.1.7}$$

for suitable $\mu_\nu > 0$, and where the implied constant does not depend on i. (Here we denote by $L_{j,\nu}$ the linear form calculated on $\varphi_1, \ldots, \varphi_d$, so that it becomes a function on X and it makes sense to calculate it on P_i.) The application of the Subspace Theorem will provide the conclusion. In order to have small values of the left-hand side in (5.1.7) we try to construct regular functions $L_{j,\nu}$ such that their product has a zero at the ν-adic limit point P_ν of the sequence P_i.

To reach this goal, we distinguish three cases:

(i) P_ν does not belong to the support of D (i.e. $P_\nu \in X(\kappa_\nu)$);
(ii) P_ν lies in exactly one component D_ν of D;
(iii) P_ν lies at the intersections of two components D_ν, D_ν^* of D.

In case (i) we simply take $L_{j,\nu} = \varphi_j$ for each $j = 1, \ldots, d$. Since both sides in (5.1.7) are uniformely bounded (i.e. bounded independently of i) the inequality holds e.g. for $\mu_\nu = 1$ (thanks to the constant implicit in the symbol $\ll$).

We now consider case (ii), where $P_i \to P_\nu \in D_\nu$ and the limit P_ν does not belong to any other component of D. Consider the filtration $W_1 = V_N \supset W_2 \ldots$, where

$$W_{j,\nu} = W_j := \{\varphi \in V_N \,|\, \mathrm{ord}_{D_\nu}\varphi \geq j - 1 - Np_\nu\}.$$

(Here p_ν is the weight p_i relative to the unique index $i \in \{1, \ldots, r\}$ such that $D_\nu = D_i$.) We can certainly find a basis $L_{1,\nu}, \ldots, L_{d,\nu}$ of V_N (whose elements can be expressed as linear forms in $\varphi_1, \ldots, \varphi_d$) containing a basis for each sub-space W_j; simply take a basis of the smallest nonzero W_j and complete it successively to bases of the previous spaces of the filtration. this basis contains exactly $\dim(W_j/W_{j+1})$ elements in the set $W_j \setminus W_{j+1}$, for each index j such that W_j is nonzero. Also the order at D_ν of every such element is precisely $j - 1 - Np_\nu$. Hence we have

$$\mathrm{ord}_{D_\nu}\left(\prod_{i=1}^{d} L_{i,\nu}\right) = \sum_{i=1}^{d} \mathrm{ord}_{D_\nu}(L_{i,\nu}) = \sum_{j\geq 1}(j - 1 - Np_\nu)\dim(W_j/W_{j+1}).$$

In order to prove that the product on the left-hand side vanishes at D_ν, we need a lower bound for the sum on the right-hand side. Since $\sum_j \dim(W_j/W_{j+1} = \dim V_N = d$, we have $\sum_j(-1 - Np_\nu)\dim(W_j/W_{j+1}) = (-1 - Np_\nu)d$, independently of the filtration. On the contrary, to estimate $\sum_j j\dim(W_j/W_{j+1})$, we need some estimates on the relative dimensions $\dim(W_j/W_{j+1})$. Taking into accounts that the total sum $\sum_j \dim(W_j/W_{j+1})$ must give the fixed value d (independent of the filtration), it turns out that what we need is an *upper* bound for the dimension $\dim(W_j/W_{j+1})$ (basically, we need the existence of 'large' W_j for large values of the index j; in other words, we need to prove that one can construct 'many' regular functions with high vanishing order at D_ν. We shall use for this scope Lemma 5.1.1 which gives the upper bound

$$\dim(W_j/W_{j+1}) \leq 1 + N(D.D_\nu) - jD_\nu^2.$$

Now, by a simple combinatorial lemma (see Lemma 3.1 in [16]), it turns out that the worst situation would occur when the relative dimensions $\dim(W_j/W_{j+1})$ coincide with the above upper bound; so in any case

$$\sum_j j \dim(W_j/W_{j+1}) \geq \sum_j j(1 + N(D.D\nu) - jD_\nu^2) = \sum_j jU_j,$$

where the sum runs over those positive integers j such that $U_j := 1+N(D.D\nu) - jD_\nu^2 \geq 0$. Now let $\xi = \xi_\nu$ be the minimal positive solution to the equation

$$D_\nu^2\xi^2 - 2(D.D_\nu)\xi + D^2 = 0.$$

So $\xi_\nu = \xi_i$ whenever $D_i = D_\nu$. The solutions to the above quadratic equation are shown to be indeed real by an easy application of Hodge Index Theorem (see Lemma 2.4 in [16]) and at least one of them is positive, so ξ_ν is well defined. By the assumption 5.1.3 and little calculations left to the reader, we can find a real number λ with $0 < \lambda < \xi$ and

$$\frac{\lambda^2(D.D_\nu)}{2} - \frac{\lambda^3 D_\nu^2}{3} - \frac{D^2 p_\nu}{2} > 0. \tag{5.1.8}$$

From the definition of ξ and the inequality $\lambda < \xi$ it follows that

$$(D.D_\nu)\lambda - \frac{D_\nu^2\lambda^2}{2} < \frac{D^2}{2}.$$

Put $R = [\lambda N]$ (integral part) and recall that $U_j = 1 + N(D.D\nu) - jD_\nu^2$. Then

$$\sum_{j=1}^{R} U_j = RN(D.D_\nu) - \frac{R^2 D_\nu^2}{2} + O(R+N) \leq N^2\left((D.D_\nu)\lambda - \frac{D_\nu^2\lambda^2}{2}\right) + O(N).$$

By the above inequality, the number between parenthesis is $< D^2/2$ and by the mentioned asymptotic Riemann-Roch theorem $d = d_N = N^2(D^2/2) + O(N)$; so for large N we shall have

$$\sum_{j=1}^{R} U_j \leq d.$$

We then estimate $\sum_j j\dim(W_j/W_{j+1})$ as

$$\sum_j j\dim(W_j/W_{j+1}) \geq \sum_{j=1}^{R} jU_j = \sum_{j=1}^{[\lambda N]} j(1+N(D.D_\nu)-jD_\nu^2).$$

The right-hand side is $N^3\left(\frac{\lambda^2(D.D_\nu)}{2}-\frac{\lambda^3 D_\nu^2}{3}+O(1/N)\right)$. Finally the quantity $\sum_{j\geq 1}\mathrm{ord}_{D_\nu}(L_{j,\nu}) = \sum_{j\geq 1}(j-1-Np_\nu)\dim(W_j/W_{j+1})$ that we want to estimate satisfies the lower bound

$$\begin{aligned}\sum_{j\geq 1}\mathrm{ord}_{D_\nu}(L_{j,\nu}) &= \sum_{j\geq 1} j\dim(W_j/W_{j+1}) - (1+Np_\nu)d \\ &\geq N^3\left(\frac{\lambda^2(D.D_\nu)}{2}-\frac{\lambda^3 D_\nu^2}{3}-\frac{D^2}{2}\right)+O(N^2)\end{aligned}$$

By (5.1.8) it is strictly positive for large values of N. Now, take a local equation $t_\nu = 0$ for D_ν at P_ν and write each function $L_{j,\nu}$ as

$$L_{j,\nu} = t_\nu^{\mathrm{ord}_{D_\nu}(L_{j,\nu})}\rho_{j,\nu}$$

for some rational function ρ_ν, regular at P_ν. In particular, the values $\rho_{j,\nu}(P_i)$ are well-defined for large i and uniformly bounded as i varies. So for each j we have $|L_{j,\nu}(P_i)| \ll t_\nu^{\mathrm{ord}_{D_\nu}(L_{j,\nu})}(P_i)|_\nu$, so

$$\prod_{j=1}^{d}|L_{j,\nu}(P_i)|_\nu \ll |t_\nu(P_i)|_\nu^{\sum_{j=1}^{d}\mathrm{ord}_{D_\nu}(L_{j,\nu})}.$$

By a similar argument, taking into account that φ_j has a pole of order at most Np_ν at D_ν, and no other poles at divisors containing p_ν, we can bound

$$\max_j(\varphi_j(P_i)) \leq t_\nu(P_i)|_\nu^{-Np_\nu}.$$

Hence we obtain relation (5.1.7) for some positive μ_ν independent of P_i.

Let us now consider case (iii), where the sequence P_i converges ν-adically to a point $P_\nu \in D_\nu \cap D_\nu^*$. By assumption, P_ν does not belong to any other divisor D_i. Let us consider *two* filtrations W_j, W_j^* in V_N as before, one for each of the divisors D_ν, D_ν^*. By an elementary fact from linear algebra (see e.g. Lemma 3.2 in [16]) we can choose a basis $L_{1,\nu},\ldots,L_{d,\nu}$ adapted to both filtrations, i.e. containing bases for all the subspaces W_j and W_j^* (however, this would be in general impossible for three filtrations). Let t_ν, t_ν^* be two regular functions at P_ν providing local equations for D_ν, D_ν^* respectively. Then each rational function $L_{j,\nu}$ can be written as

$$L_{j,\nu} = t_\nu^{\mathrm{ord}_{D_\nu}(L_{j,\nu})} t_\nu^{*\,\mathrm{ord}_{D_\nu^*}(L_{j,\nu})}\rho_{j,\nu},$$

where $\rho_{j,\nu}$ is regular at P_ν. By the above calculations, we have that both $\sum_j \mathrm{ord}_{D_\nu}(L_{j,\nu})$ and $\sum_j \mathrm{ord}_{D_\nu^*}(L_{j,\nu})$ can be made strictly positive for large values of N. Hence the relation (5.1.7) holds also in this last case.

We can now apply the Subspace Theorem 2.2.1. We take $\mathbf{x} \in \mathbb{P}_{d-1}(\kappa)$ to be the point $x = (\varphi_1(P_i) : \ldots : \varphi_d(P_i))$. For each $\nu \in S$, the ν-adic term appearing on the left-hand side of (2.2.2) is bounded as

$$\prod_{j=1}^{d} \frac{L_{j,\nu}}{\|\mathbf{x}\|} \leq \|\mathbf{x}\|_\nu^{-d-\mu_n},$$

so, putting $\mu = \min_{\nu \in S}(\mu_\nu)$, the double product on the left side of (2.2.2) is bounded as

$$\prod_{\nu \in S} \prod_{j=1}^{d} \frac{|L_{j,\nu}(\mathbf{x})|_\nu}{\|\mathbf{x}\|} \leq \left(\prod_{\nu \in S} \|\mathbf{x}\|_\nu \right)^{-d-\mu}.$$

Since the values $\varphi_i(P)$ are all S-integers, the term $\left(\prod_{\nu\in S} \|\mathbf{x}\|_\nu\right)$ represents the height of the projective point x. Hence the above inequality implies (2.2.2), so the conclusion of the Subspace Theorem holds. In particular, there will be a hyperplane in $\mathbb{P}_{d-1}$ containing infinitely many points $(\varphi_1(P_i) : \ldots : \varphi_d(P_i))$. This implies that a nonzero regular function on X vanishes on infinitely many integral points of the sequence P_i, so these points lie on an algebraic curve on X. As remarked, this concludes the proof.

5.2 Divisibility problems

Siegel's finiteness theorem in the case of rational curves can be restated as follows:

Theorem 5.2.1. *If $f(X), g(X)$ are coprime polynomials with S-integral coefficients such that for infinitely many S-integers $x \in \mathcal{O}_S$, $f(x)$ divides $g(x)$ in the ring of S-integers, then the polynomial $f(X)$ has at most one (complex) root.*

Proof. Let us factor $f(X)$ over $\bar{\mathbb{Q}}[X]$ as $f(X) = a \cdot (X - \alpha_1) \cdots (X - \alpha_d)$, where $d = \deg(F)$, $a \in \bar{\mathbb{Q}}^*$, $\alpha_1, \ldots, \alpha_d \in \bar{\mathbb{Q}}$. Suppose that $\alpha_1 \neq \alpha_2$; we shall deduce from Siegel's theorem that only finitely many $x \in \mathcal{O}_S$ satisfiy $f(x)|g(x)$. Enlarging S we can suppose that $a, \alpha_1, \alpha_2 \in \mathcal{O}_S$. Let us write, for $i = 1, 2$, the polynomial $g(X)$ as $g(X) = (X - \alpha_i)h_i(X) + r_i$, for some S-integer r_i, which must be non-zero since $f(X), g(X)$ are supposed to be coprime. Then for every $x \in \mathcal{O}_S$ such that $f(x)|g(x)$ we have that $(x - \alpha_i)|g(x)$ for $i = 1, 2$, and so $(x - \alpha_i)|r_i$; after further enlarging $\mathcal{O}_S$, we can suppose that r_1, r_2 are units, so $x - \alpha_i$ must be units; since their difference is the non-zero constant $\alpha_2 - \alpha_1$, only finitely many possibilities for x can occur. □

We shall see that some extension of this fact to two variables polynomials is possible, and leads to questions on integral points on surfaces, more precisely on rational surfaces.

First consider the S-unit equation theorem in three variables, providing the degeneracy of the solutions in S-units to the equation $x+y+z=1$. One can rephrase the statement as follows: the pairs of S-integers $(x,y)\in\mathbb{A}^2(\mathcal{O}_S)$ such that $x|1, y|1, (x+y-1)|1$ are not Zariski-dense on the plane.

We are then considering *three* polynomials $f_i(X,Y)\in\mathcal{O}_S[X,Y]$, for $i=1,2,3$, (in the above examples the polynomials $X, Y, X+Y-1$) and three more polynomials $g_i(X,Y)\in\mathcal{O}_S[X,Y]$ (in our example all the three are equal to the constant 1) and we look for the points $(x,y)\in\mathcal{O}_S^2$ such that

$$f_i(x,y)|g_i(x,y) \qquad \text{for } i=1,2,3. \tag{5.2.2}$$

This corresponds to the system of Diophantine equations $f_i(x,y)\cdot z_i = g(x,y)$ in the unknowns (x,y,z_1,z_2,z_3), to be solved over the ring $\mathcal{O}_S$; the complex solutions define a rational affine surface. Under natural conditions on the polynomials f_i, g_i we can prove the degeneracy of integral points on such a surface, i.e. the degeneracy of the set of solutions to the divisibility problem 5.2.2. This is the content of the following result from [22]:

Theorem 5.2.3. *Let $f_i(X,Y), g_i(X,Y)\in\mathcal{O}_S[X,Y]$, $i=1,2,3$, be two triple of non-zero polynomials satisfying $\deg f_i\geq\deg g_i$; suppose also they satisfy the generic position assumption below. Then the solutions $(x,y)\in\mathcal{O}_S^2$ to the divisibility problem 5.2.2 are not Zariski-dense in the plane.*

Note that in particular it applies whenever $\deg f_i=\deg g_i=1$, thus providing, in the case $f_1=X, f_2=Y, f_3=X+Y-1$, a stronger statement than the S-unit equation theorem.

The mentioned generic position conditions are the following:

- for each $1\leq i<j\leq 3$ the curves of equation $f_i=0$ and $f_j=0$ have no common points at infinity (after embedding $\mathbb{A}^2\hookrightarrow\mathbb{P}_2$ in the usual way).
- there exist no common zero to the three polynomials f_1, f_2, f_3;
- for each i such that g_i is non constant the two affine curves $f_i=0$ and $g_i=0$ intersect transversely;
- for $1\leq i<j\leq 3$ and $h\in\{i,j\}$, the three curves $f_i=0, f_j=0$ and $g_h=0$ have no point in common.

The mentioned case where $\deg f_i=\deg g_i=1$ is of particular geometric interest, since it corresponds to a simply connected smooth surface. It is the first example of a smooth simply connected variety for which the degeneracy of integral points (over arbitrary ring of S-integers) could be proved (note that no example can exist in dimension one). Such a surface could be intrinsically defined as follows: starting from the affine plane, take three lines in general position L_1, L_2, L_3 and three points $P_i\in L_i$, $i=1,2,3$, outside the intersections of the lines. Then let $\tilde{X}$ be the surface obtained by blowing up the three points P_1, P_2, P_3 and X the open subset obtained by removing the strict transforms of the lines L_1, L_2, L_3. Integral points on X correspond bijectively with solutions to the divisibility problem $f_i(x,y)|g_i(x,y)$. Once reformulated in this way, the proof of Theorem 5.2.3 is an application of Theorem 5.1.2.

Other results on degeneracy of solutions to divisibility problems can be deduced form the Main Theorem of [18]. They concern problems of the form

$$f(u,v)|g(u,v), \tag{5.2.4}$$

where $f(x,y), g(x,y) \in \mathcal{O}_S[x,y]$ are coprime polynomials. They correspond to integral points on surfaces in the following way: consider the projective plane $\mathbb{P}_2$, with projective coordinates $(X_1 : X_2 : X_3)$. Consider the three lines $D_i^* : X_i = 0$, for $i = 1,2,3$. Letting $F(X,Y,Z), G(X,Y,Z)$ be the homogeneous forms associated to the polynomials $f(x,y), g(x,y)$, we let $P_1,\ldots,P_k$ be the points defined by $F = G = 0$. Define $\tilde{X}$ as the blow-up of the plane over $P_1,\ldots,P_k$ and D_4 the strict transform of the plane curve $F = 0$ (which can be supposed to be irreducible) and, for $i = 1,2,3$, let D_i be the pull-back of D_i^*. Then, at least whenever the mentioned curves on the plane intersect transversely, the divisibility problem (5.2.4) is equivalent to finding integral points on $X := \tilde{X} \setminus (D_1 \cup \ldots \cup D_4)$.

The proof of the Main Theorem in [18] does not use explicitly any geometry on surfaces, in particular it does not use Riemann-Roch theorem; however, it does make use of Schmidt's Subspace Theorem, which is applied to very explicit linear forms. The main difference from the proof of Theorem 5.1.2 is that in [18] one uses a suitably chosen non-complete linear system instead of our space V_N, and in that case this fact constitutes an advantage. Instead of just proving the degeneracy of solutions to (5.2.4), by the methods of [18] one finds a strong upper bound for the 'g.c.d.' of the values of $f(u,v)$ and $g(u,v)$ at S-unit points, proving in particular that this g.c.d. is asymptotically negligible with respect to the height of $f(u,v)$.

A concrete example of a problem which can be reduced to a divisibility one arises in the work [9] by Canci, about rational periodic points for endomorphisms of the line. There Canci considers the families of pairs (f,P) formed by a degree-two morphism $f : \mathbb{P}_1 \to \mathbb{P}_1$ and a point $P \in \mathbb{P}_1$, periodic for the iteration of f, of fixed order n. The group PGL_2 acts by conjugation on such pairs, and the quotient space turns out to be a quasi-projective surface (a quadratic rational function is defined by five parameters, while the group PGL_3 has dimension three).

Let us consider the pairs (f,P) defined over a number field κ, where $f : \mathbb{P}_1 \to \mathbb{P}_1$ is a quadratic endomorphism having bad reduction only over a fixed set of places S of κ; this means that the degree of the reduction of f modulo every place outside S remains equal to 2. Such pairs are parametrized by S-integral points on an open surface X_n. Theorems 1.2 and 1.4 from [9] read as

Theorem 5.2.5. *Let κ be a number field, S a finite set of places containing the archimedean ones. Let $n \geq 4$ be an integer. Then up to conjugation by elements of $\mathrm{PGL}_2(\kappa)$, there are only finitely many rational functions of degree two, defined over κ, with good reduction outside S, admitting a periodic point of order n. For $n = 3$, all but finitely many such functions are of the form $f(z) = (z-1)(uz+1)/uz^2$, for a unit $u \in \mathcal{O}_S^*$.*

The theorem can be viewed as a finiteness (or degeneration) statement about integral points of the corresponding moduli space X_n.

The proof for $n \geq 4$ consists essentially in producing a morphism $X_n \to \mathbb{P}_1 \setminus \{0, 1, \infty\}$ and then applying Siegel's theorem (so working in dimension one). In the case $n = 3$, on the contrary, such a method cannot work, since the corresponding (rational) surface does not admit such morphisms. Then the proof proceeds by exploiting some divisibility conditions, which can be interpreted as integrality with respect to blown-up divisors, and eventually applying the main theorem of [18].

5.3 Constructing integral points on surfaces

We have seen in Chapter 1.2 that whenever a curve $\tilde{\mathcal{C}} \setminus D$ does not satisfy the hypothesis of Vojta's conjecture, namely when $\deg(D + K_{\tilde{\mathcal{C}}}) \leq 0$, such a curve admits a Zariski-dense set of integral points, provided we allow finite degree extensions of the ring of integers.

The situation is much more complicated and mysterious for surfaces, even for rational ones. However, a good description is possible for complements of curves with normal crossing singularities on the plane. Namely, we have:

Theorem 5.3.1. *Let $D \subset \mathbb{P}_2$ be a curve with normal crossing singularities (if any) satisfying $\deg D \leq 3$, defined over a number field κ. Let $X = \mathbb{P}_2 \setminus D$ be its complement. Then there exists a finite extension of κ and a finite set of places S such that the set $X(\mathcal{O}_S)$ of S-integral points is Zariski-dense in X.*

The crucial case, arising when D is a smooth cubic, has been proved by Beukers [4].

We first give the proof in the easy cases when $\deg D \leq 2$ or D is a singular cubic.

We have already seen the case when D is a configuration of lines (necessarily on general position, due to our assumption on normal crossing singularities). Suppose now that D is the union of a smooth conic and a non-tangent line. Up to projective automorphisms, we can suppose that the line is the one at infinity and that in affine coordinates (x, y) the conic has equation $xy = 1$. Then the integral points correspond to pairs of S-integers $(x, y) \in \mathcal{O}_S^2$ such that $u := xy - 1$ is a unit. These can be obtained by letting u run over the units and factoring $u + 1$ into a product in all possible ways. Clearly, we obtain a Zariski-dense set. Note that this case also covers the case of a single conic, since adding an extra component at infinity can only diminish the set of integral points.

We now treat the case of an irreducible singular curve; we only consider nodal curves, since we assume that the singularities are of normal crossing type. Let D be such a cubic and L_1, L_2 be the principal tangents at its singular point O, i.e. the only lines intersecting D only at O (with multiplicity three). We prove a stronger statement, namely that integral points on the complement of $D+L_1+L_2$ are Zariski-dense. In fact, consider the pencil Λ of lines passing through O: each such line L, if it is different from both L_1, L_2, intersects D at a second point $p(L)$. Then the surface $X := \mathbb{P}_2 \setminus (D+L_1+L_2)$ is endowed with a map $X \to \Lambda \setminus \{L_1, L_2\}$ whose fibers are isomorphic to the complement of two points in $\mathbb{P}_1$. Notice that these missing points are also ordered (e.g. the first is O, the second $p(L)$), so we obtain a principal $\mathbb{G}_m$-bundle with basis $\Lambda \setminus \{L_1, L_2\} \simeq \mathbb{G}_m$. To show that this principle bundle is rivial, it suffices to exhibit a regular section[1]. To do this, just take another nodal curve with the same principle tangents at the nodal point[2] and to each line in Λ associate the intersection with the second nodal curve, which will be always distinct from the intersections with the first one. We have then proved that $X \simeq \mathbb{G}_m^2$, so in particular $X(\mathcal{O}_S)$ is Zariski-dense for a suitable ring of integers $\mathcal{O}_S$.

The much more sophisticated case of the complement of a smooth cubic is treated by constructing infinitely many affine curves on the complement of D, each admitting infinitely many integral points. We have seen that a genus zero curve with at most two points at infinity contains infinitely many S-integral points, *provided we allow a finite extension of the ring of S-integers.* The problem is that we need to work with infinitely many curves, since we want to produce a set of integral points which is dense on the plane, and we allow only finitely many finite extensions of the ring of integers. Hence we need a criterion for the infinitude of integral points on curves over a *fixed* ring of S-integers.

The sought criterion follows from the following two lemmas. The first one is a reformulation of (a generalization of) well known facts in the theory of Pell's equation:

Lemma 5.3.2. *Let κ be a number field, $\mathcal{O}_S \subset \kappa$ be a ring of S-integers; let $\tilde{\mathcal{C}} \subset \mathbb{P}_2$ be a smooth conic defined over $\mathbb{P}_2$. Let $L \subset \mathbb{P}_2$ be a line defined over κ, not tangent to $\mathcal{C}$. Suppose that either (i) $L \cap \mathcal{C}$ consists of two conjugated quadratic points P, P' and one place of S splits in the corresponding quadratic extension of κ, or (ii) the group of units $\mathcal{O}_S^*$ is infinite. Then the group $G \subset \mathrm{PGL}_3(\mathcal{O}_S)$ of projective transformations*

$$G := \{g \in \mathrm{PGL}_3(\mathcal{O}_S) \,:\, g(L) = L, g(\mathcal{C}) = \mathcal{C}\}$$

is infinite.

Proof. Since the group $\mathrm{PGL}_3(\mathcal{O}_S)$ acts transitively on the lines of $\mathbb{P}_2$ defined over κ, we can suppose that L is the line at infinity $Z=0$. Then, in affine coordinates for the complement $\mathbb{P}_2 \setminus L$, the equation for $\mathcal{C} = \tilde{\mathcal{C}} \setminus (L \cap \tilde{\mathcal{C}})$ takes the form:

$$\mathcal{C}: \quad ux^2 + vxy + wy^2 + ax + by = c,$$

[1] or to invoke the triviality of the Picard group of $\mathbb{G}_m \simeq \mathbb{A}^1 \setminus \{0\}$

[2] if e.g. the first cubic curve is defined by the affine equation $y^2 = x^3 + x^2$, one can take for the second one that of equation $y^2 = 2x^3 + x^2$

for suitable S-integers u, v, w, a, b, c. Let $q(x, y) := ux^2 + vxy + wy^2$ be the quadratic form appearing in the equation above. Note that the two points of $L \cap \mathcal{C}$ are $(\xi : 1 : 0)$ where ξ satisfies $u\xi^2 + v\xi + w = 0$. It is well known that the corresponding orthogonal group $\mathrm{SO}(q, \mathcal{O}_S) \subset \mathrm{SL}_2(\mathcal{O}_S)$, namely the group of matrices $T \in \mathrm{SL}_2(\mathcal{O}_S)$ preserving the quadratic form q, is infinite and contains elements of infinite order (in the classical case of the form $x^2 - dy^2$ over the integers, d being positive and non-square, this is the infinitude of the solutions to Pell's equation). Here we use the fact that $\mathcal{O}_S^*$ is infinite or becomes infinite after extending κ by adding the roots of the polynomial $u\xi^2 + v\xi + w$.

If $a = b = 0$ we have finished. Otherwise, we must operate a change of variables, translating the centre of symmetry of the conic to the origin, but this translation might carry integral points of the plane to rational non-integral ones. Precisely, the baricenter of the affine conic $\mathcal{C}$ defined above is the point (α, β) satisfying the equation

$$A \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix},$$

where $A = \begin{pmatrix} 2u & v \\ v & 2w \end{pmatrix}$. The determinant of A being $\det(A) = 4uw - v^2 \neq 0$, the solution (α, β) is defined in the group $(4uw - v^2)^{-1} \cdot \mathcal{O}_S$. Now take for T an element of infinite order in $\mathrm{SO}(q, \mathcal{O}_S)$; let $m \geq 1$ be an integer such that $T^m \equiv I \pmod{(4uw - v^2) \cdot \mathcal{O}_S}$. Then the affine transformation of the plane

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \alpha \\ \beta \end{pmatrix} + T^m \cdot \begin{pmatrix} x - \alpha \\ y - \beta \end{pmatrix} = T^m \cdot \begin{pmatrix} x \\ y \end{pmatrix} + (I - T^m) \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

is defined over $\mathcal{O}_S$ and preserves the conic $\mathcal{C}$. □

From the lemma we deduce the

Corollary 5.3.3. *Let $\tilde{\mathcal{C}}$ be a smooth projective conic and L a line, not tangent to $\tilde{\mathcal{C}}$, both defined over the number field κ. Let $\mathcal{O}_S \subset \kappa$ be a ring of S-integers. Suppose that (i) or (ii) of the lemma above are satisfied and that $\mathcal{C} = \tilde{\mathcal{C}} \setminus (\tilde{\mathcal{C}} \cap L)$ contains one integral point. Then $\mathcal{C}(\mathcal{O}_S)$ is infinite.*

Proof. The deduction is obtained after noticing that the infinite group defined in the above lemma acts freely on $\mathcal{C}(\mathcal{O}_S)$. □

We now state and prove the crucial case of Beukers' Theorem 5.3.1:

Theorem 5.3.4. *Let $D \subset \mathbb{P}_2$ be a smooth cubic defined over a number field κ, containing a κ-rational flexus O. Let S be a finite set of places of κ, containing the archimedean ones and the places of bad reduction for D and such that $\mathcal{O}_S^*$ is infinite. Then $(\mathbb{P}_2 \setminus D)(\mathcal{O}_S)$ is infinite.*

Proof. Due to the presence of a rational flexus and our hypothesis on good reduction, we can write the equation for D in 'almost Weierstrass form':

$$X^3 + ZG(X, Y, Z) = 0 \tag{5.3.5}$$

where $G(X,Y,Z) \in \mathcal{O}_S[X,Y,Z]$ is a quadratic form. Here the rational point O takes coordinates $(0:1:0)$ and the line at infinity takes the equation $Z=0$. Also, the curve D is invariant under the involution $\Phi : \mathbb{P}_2 \to \mathbb{P}_2$ defined by $\Phi(X:Y:Z) = (X:-Y:Z)$.

Consider the set of conics which are also invariant under such an involution: they form the disjoint union of two linear systems, a three-dimensional one and a one-dimensional one, corresponding to the quadratic forms Q satisfying $Q(X,Y,Z) = Q(X,-Y,Z)$ (resp. $Q(X,Y,Z) = -Q(X,-Y,Z)$). Let us denote by Λ the three-dimensional linear system of invariant conics arising in the first case.

We have the following

Claim. For each (complex) point $P \in D$, not fixed by Φ, passes exactly one conic $\tilde{\mathcal{C}}_P$, belonging to the set Λ, with $\tilde{\mathcal{C}}_P \cap D = \{P, \Phi(P)\}$. Such a conic is smooth if P is not a flexus.

The Claim is proved by dimension counting: since the intersection product $\tilde{\mathcal{C}} \cdot D$ must be equal to 6, the intersection multiplicities at $P, \Phi(P)$ must be both equal to 3, and this condition will be also sufficient for the set theoretic intersection being $\{P, \Phi(P)\}$ (we have used the fact that by symmetry the two local intersection products at P and at $\Phi(P)$ must be equal). Now, if we impose the three conditions that the intersection product at P be at least 3: $(\tilde{\mathcal{C}} \cdot D)_P \geq 3$, we obtain at least one solution $\tilde{\mathcal{C}}$ in Λ, since the latter has dimension three. As we remarked, by symmetry we shall automatically have also $(\tilde{\mathcal{C}} \cdot D)_{\Phi(P)} \geq 3$. This guarantees the existence of a solution. If we had two solutions, we would have a pencil of solutions, and a suitable member of that pencil would have intersection ≥ 4 at P and $\Phi(P)$, which is impossible.

The last assertion is also clear: if $\tilde{\mathcal{C}}$ were singular, it would be the union of the two tangent lines at P and $\Phi(P)$, but then $P, \Phi(P)$ would be flexi.

Let us consider, for each point of the form $A_u := (u:1:0)$, $u \in \kappa$, the 'vertical' line L_u joining A_u to $O = (0:1:0)$. It intersects D at two more distinct points $P_u, \Phi(P_u)$, apart for at most three exceptions, when such line is tangent.

Let $\tilde{\mathcal{C}}_u$ be the conic arising from the previous claim, namely intersecting D only at the two points $P_u, \Phi(P_u)$. Put $\mathcal{C}_u := \tilde{\mathcal{C}}_u \setminus \{P_u, \Phi(P_u)\} = \tilde{\mathcal{C}}_U \setminus (L_u \cap \tilde{\mathcal{C}}_u)$. By Corollary 5.3.3, if we find one integral point on $\mathcal{C}_u$, we can deduce that there are infinitely many integral points on $\mathcal{C}_u$; these points will be integral points of the plane with respect to D, since $\tilde{\mathcal{C}}_u \cap D = \tilde{\mathcal{C}}_u \cap L_u = \{P_u \Phi(P_u)\}$. If we can ensure that $\mathcal{C}_u(\mathcal{O}_S)$ is infinite for infinitely many values of u, we will have proved that the integral points on $\mathbb{P}_2 \setminus D$ form a dense set in the plane.

The idea to perform this last step is to choose u in such a way that the intersections $\mathcal{C}_u \cap H$ be a pair of integral points on $H \setminus \{O\} = H \setminus (H \cap D)$. Note that the 1-dimensional family of conics $\tilde{\mathcal{C}}_u$ is not a linear system, so in general the condition of passing through a fixed point will not be a linear one; in particular, given a rational point $P \in \mathbb{P}_2(\kappa)$, it is not always true that a conic of the form $\tilde{\mathcal{C}}_u$ defined over κ and passing through P exists. However, we shall prove that this holds whenever P lies on the line at infinity H.

For this purpose, observe that the pencil of cubics containing D and $3L_u$ consists of the cubics intersecting D with multiplicity ≥ 3 at the points $P_u, \Phi(P_u), O$; this pencil contains the sum of the conic $\tilde{\mathcal{C}}_u$ and the line H. In algebraic terms, if $Q_u(X,Y,Z) = 0$ is an equation for $\tilde{\mathcal{C}}_u$, Q being a quadratic form, then for a suitable scalar λ_u:

$$Z \cdot Q_u(X,Y,Z) = X^3 + ZG(X,Y,Z) + \lambda_u(X - uZ)^3$$

(recall that the equation of the cubic has the form (5.3.5), the line H has equation $Z = 0$ while the line L_u has equation $X - uZ = 0$). Now, comparing the term X^3 on the two sides of the above displayed equality, we obtain that λ_u must be equal to -1 for every u. Hence the quadratic form Q_u appearing in the equation of the conic $\tilde{\mathcal{C}}_u$ is given by

$$Q_u(X,Y,Z) = G(X,Y,Z) + 3uX^2 - Z(3u^2X - u^3Z) \tag{5.3.6}$$

Let now $P = (\alpha : \beta : 0)$ be a point at infinity. The condition that $\tilde{\mathcal{C}}_u$ passes through P amounts to $Q(\alpha, \beta, 0) = 0$, i.e. in view of (5.3.6), $G(\alpha, \beta, 0) + 3u\alpha^2 = 0$; then u must be taken to be equal to $-G(\alpha, \beta, 0)/3\alpha^2$, which is rational if α, β are rational, i.e. if P is rational. Now, we choose P to be integral with respect to D, which amounts to taking $P = (1 : \beta : 0)$, with $\beta \in \mathcal{O}_S$; the corresponding conic $\tilde{\mathcal{C}}_u = \tilde{\mathcal{C}}_{-G(1,\beta,0)/3}$ will be defined over κ and it will have an integral point, namely P, so infinitely many integral points, concluding the proof. □

It is worth noticing that a cubic curve in the plane lies in the anticanonical class, which is ample (the projective plane is a Del Pezzo surface). A natural generalization to Beukers' theorem has been provided by Hassett and Tschinkel [34]: they proved that given a smooth anti-canonical curve on a smooth Del Pezzo surface, the integral points on its complement are potentially dense. Their proof is inspired by Beukers'. Other results in this direction are provided in [22].

5.4 Higher dimensional results

Little is known about the degeneracy of integral points on varieties of dimension larger than two. The general mentioned theorem of Faltings and Vojta still applies, so whenever a variety admits a non-trivial morphism to a semi-abelian variety one can prove degeneracy of integral points, apart when the image of such morphism is itself a semi-abelian variety. This idea has been exploited by Noguchi and Winkelmann [43], who proved the following

Theorem 5.4.1. *Let $\tilde{X}$ be a smooth projective variety defined over a number field κ. Let $q(\tilde{X})$ be its irregularity*[3] *and $\rho(\tilde{X})$ be the rank of its Néron-Severy*

[3] We recall that the irregularity $q(\tilde{X})$ of an algebraic variety is the dimension of its Albanese variety.

group. Let $D_1, \ldots, D_l$ be hypersurfaces of $\tilde{X}$ in general position. Put $X := \tilde{X} \setminus (D_1 \cup \ldots \cup D_l)$. If

$$l > \dim \tilde{X} + \rho(\tilde{X}) - q(\tilde{X}),$$

then the set $X(\mathcal{O}_S)$ is not Zariski-dense in $\tilde{X}$, for any ring of S-integers $\mathcal{O}_S \subset \kappa$.

If $q > m$ the image of $\tilde{X}$ on its Albanese variety is a proper subvariety, which cannot be a translate of an abelian subvariety; one can then apply Falting's theorem. In general, after removing $\dim(\tilde{X}) + \rho - q + 1$ hypersurfaces in general position, one is lead to a situation where Vojta's theorem on semi-abelian varieties can be applied.

The method discussed in this chapter, which is based on the Subspace Theorem, also admits an extension to higher dimension; this is the content of Aaron Levin's thesis, reproduced in [37]. In [13] these methods are applied to the three-dimensional case. P. Autissier in [1], [2] further developed the method, introducing interesting technical improvements.

For instance, Levin's Theorem 5.1.4 on a surface minus four ample curves admits the following generalization to the three-dimensional case:

Theorem 5.4.2. *Let $\tilde{X}$ be a smooth threefold defined over a number field. Let $D_1, \ldots, D_6$ be ample hypersurfaces in general position. The integral points on the affine surface $X := \tilde{X} \setminus (D_1 \cup \ldots \cup D_6)$ are never Zariski-dense.*

This theorem is proved, among other results of the same flavour, by Autissier in [2]. We note that, on every threefold $\tilde{X}$, the sum $K_{\tilde{X}} + D_1 + \ldots + D_5$ of the canonical divisor $K_{\tilde{X}}$ plus *five* ample hypersurfaces is big: hence, after Vojta's conjecture it is likely that the minimal number of hypersurfaces to remove in Autissier's theorem could be lowered to five, but it seems that such an improvement will require essentially new techniques.

References

1. P. Autissier, Géométrie, points entiers et courbes entières, *Annales Sci. E.N.S.* **42** (2009), 221-239.
2. P. Autissier, Sur la non-densité des points entiers, *Duke Math. Journal*, **158** (2011), 13-27.
3. A. Beauville, Surfaces algébriques complexes, *Astérisque* **54** (1978).
4. F. Beukers, Ternary Form Equations, *J. Numb. Theory* **54** (1995), 113-133.
5. Yu. Bilu, A note on universal Hilbert sets. *J. reine angew. Math.* **479** (1996), 195-203.
6. Yu. Bilu, The Many Faces of the Subspace Theorem (after Adamczewski, Bugeaud, Corvaja, Zannier). Séminaire Bourbaki, exposé 967 Novembre 2006, *Astérisque* **317** (2007), 1-38.
7. Yu. Bilu, M. Strambi, A. Surroca, Quantitative Chevalley-Weil Theorem for Curves, to appear in *Monatshefte f. Math.*
8. E. Bombieri, W. Gubler, Heights in Diophantine Geometry, Cambridge University Press, 2006
9. J.K. Canci, Rational periodic points for quadratic maps, *Ann. Inst. Fourier (Grenoble)* **60** (2010), no. 3, 953-985.
10. P. Corvaja, Autour du Théorème de Roth. *Monatshefte f. Math.* **124** (1997), 147-175.
11. P. Corvaja, Problems and results on integral points on rational surfaces. Diophantine Geometry, U. Zannier ed., 123-141, CRM Series, 4, Ed. Norm., Pisa, (2007).
12. P. Corvaja, Rational fixed points for linear group actions. *Ann. Sc. Norm. Super. Pisa Cl. Sci.* **(5)** (2007), no. 4, 561-597.
13. P. Corvaja, A. Levin, U. Zannier, Integral points on threefolds and other varieties, *Tohoku Math. Journal* **(2) 61** (2009), 589-601.
14. P. Corvaja, U. Zannier, Diophantine equations with power sums and universal Hilbert sets, *Indag. Math. N. S.* **9** (1998), 317-332.
15. P. Corvaja, U. Zannier, A subspace theorem approach to integral points on curves. *C. R. Math. Acad. Sci. Paris* **334** (2002), no. 4, 267-271.
16. P. Corvaja, U. Zannier, On integral points on surfaces. *Ann. of Math.* (2) **160** (2004), no. 2, 705-726.
17. P. Corvaja, U. Zannier, On a general Thue's equation. *Amer. J. Math.* **126** (2004), no. 5, 1033-1055, *Addendum* ibidem **128** (2006), no 4, 1057-1066.
18. P. Corvaja, U. Zannier, A lower bound for the height of a rational function at S-unit points. *Monatsh. Math.* **144** (2005), no. 3, 203-224
19. P. Corvaja, U. Zannier, On the integral points on certain surfaces. *Int. Math. Res. Not.* **2006**, 20 pp. (2006).
20. P. Corvaja, U. Zannier, Some cases of Vojta's conjecture for integral points over function fields. *J. Alg. Geom.* **17** n.2 (2008), 295-333.
21. P. Corvaja, U. Zannier, Applications of the Subspace Theorem to certain Diophantine Problems, in H.-P. Schlickewei, K. Schmidt, R. Tichy (eds) *Diophantine Approximation - Festschrift for Wolfgang Schmidt*, Springer Verlag 2008.

P. Corvaja, *Integral Points on Algebraic Varieties*, HBA Lecture Notes in
Mathematics, DOI 10.1007/978-981-10-2648-5

22. P. Corvaja, U. Zannier, Integral points, divisibility between values of polynomials and entire curves on surfaces, *Advances in Math.* **225** (2010), 1095-1118.
23. O. Debarre, Higher Dimensional Algebraic Geometry, Springer Verlag 2001.
24. P. Dèbes, U. Zannier, Universal Hilbert subsets. *Math. Proc. Cambridge Philos. Soc.* **124** (1998), no. 1, 127-134.
25. R. Dvornicich, U. Zannier, Cyclotomic Diophantine problems (Hilbert irreducibility and invariant sets for polynomial maps), *Duke Math. J.* **139** (2007), no. 3, 527-554.
26. J.-H. Evertse, R. G. Ferretti, Diophantine inequalities on projective varieties, *Int. Math. Res. Notes* **2002**, 1295-1330.
27. J.-H. Evertse, R. G. Ferretti, A generalization of the Subspace Theorem with polynomials of higher degree, in *Diophantine Approximation*, Developments in Mathematics **16**, Springer Verlag 2008.
28. J.H. Everste, H. P. Schlickewei, A quantitative version of the absolute subspace theorem, *J. Reine Angew. Math.* **548** (2002), 21-127.
29. G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), no. 3, 349-366.
30. G. Faltings, Diophantine approximation on abelian varieties, *Ann. Math.* **133** (1991), 549-576.
31. G. Faltings, A new application of diophantine approximation, in A panorama of number theory, or the view from Baker's garden (ed. G. Wüstholz), pp. 231-246, Cambridge University Press, 2002.
32. A. Ferretti, U. Zannier, Equations in the Hadamard ring of rational functions, *Ann. Sc. Norm. Super. Pisa Cl. Sci.* **(6)** (2007), 457-475.
33. C. Gasbarri, Dyson's theorem for curves, *J. Number Theory*, **129** (2009), 36-58.
34. B. Hassett, Y. Tschinkel, Density of integral points on algebraic varieties, in: Rational points on algebraic varieties, 169-197, Progress in Math. **199**, Birkhäuser, 2001.
35. M. Hindry, J. Silverman, Diophantine Geometry: an introduction, Graduate Texts in Mathematics 201, Springer Verlag, 2000.
36. D. Leitner, Two exponential Diophantine equations. *J. Théorie Nombres Bordeaux* **23** (2011), no. 2, 479-487.
37. A. Levin, Generalizations of Siegel's and Picard's theorems *Annals of Math.* **70** (2009), 609-655.
38. A. Levin, One-parameter families of unit equations, *Math. Res. Letters* **13** (2006), 935-945
39. S. Lang, On Integral Points on Curves. *Publications Mathématiques I.H.E.S.* **6** (1960), 27-43.
40. S. Lang, Fundamentals of Diophantine Geometry, Spinger Verlag 1983.
41. J. Noguchi, A higher dimensional analogue of Mordell's conjecture over function fields, *Math. Annalen* **258** (1981), 207-212.
42. J. Noguchi, Some results in the analogue of Nevanlinna theory and diophantine approximation, *Diophantine Geometry*, U. Zannier ed., 123-141, CRM Series, 4, Ed. Norm., Pisa, (2007).
43. J. Noguchi, J. Winkelmann, Holomorphic curves and integral points off divisors, *Math. Z.* **239** (2002), 593-610.
44. J. Noguchi, J. Winkelmann, K. Yamanoi, Degeneracy of holomorphic curves into algebraic varieties, *Journal Math. Pures Appl.* **88** (2007), 293-306.
45. D. Ridout, The p-adic generalization of the Thue-Siegel-Roth theorem, *Mathematika* **5** (1958), 40-48.
46. A. Robinson, P. Roquette, On the finiteness theorem of Siegel and Mahler concerning Diophantine equations, *J. Number Theory* **7** (1975), 121-176.
47. K. Roth, Rational approximations to algebraic numbers, *Mathematika* **2** (1955), 1-10.
48. J.-P. Serre, Lectures on the Mordell-Weil Theorem, Aspects of Mathematics E 15, Viehweg Verlag, 1989.
49. W. M. Schmidt, Approximation to Algebraic Numbers, *Monographie de L'Enseignement Amthématiques* **19**, Genève 1972.

50. W. M. Schmidt, Diophantine Approximation, Lecture Notes in Mathematics **785**, Springer Verlag 1980.
51. W. M. Schmidt, Diophantine Approximations and Diophantine Equations, Lecture Notes in Mathematics **1467**, Springer Verlag 1991.
52. C. L. Siegel, Ueber einige Anwendungen diophantischer Approximationen, *Abh. Pr. Akad. Wiss.* **1** (1929) (Ges. Abh., I, 209-266).
53. V. G. Sprindzhuk, Diophantine equations with prime unknowns. (Russian) Analytic number theory, mathematical analysis and their applications. *Trudy Mat. Inst. Steklov.* **158** (1981), 180-196.
54. H.P.F. Swinnerton-Dyer, $A^4+B^4=C^4+D^4$ Revisited, *J. London Math. Soc.*, **43** (1968), 149-151.
55. P. Vojta, Diophantine Approximations and Value Distribution Theory, Lecture Notes in Mathematics **1239**, Springer Verlag, 1987.
56. P. Vojta, Integral points on subvarieties of semiabelian varieties, I, II, *Invent. Math.* **126** (1996), 133-181.
57. P. Vojta, Diophantine Approximation and Nevanlinna Theory, in Arithmetic Geometry, P. Corvaja and C. Gasbarri eds, Cetraro, Italy 2007, Lecture Notes in Mathematics **2009**, 2011.
58. A. Thue, Ueber Annäherungswerte algebraischer Zahlen, *J. reine ang. Math.* **135** (1909), 284-305.
59. U. Zannier, A proof of Pisot's d-th root conjecture, *Annals of Math.* **151** (2000), 375-383.
60. U. Zannier, Some Applications of Diophantine Approximation to Diophantine Equations (with special emphasis on Schmidt's Subspace theorem), Forum Editrice, Udine 2003
61. U. Zannier, On the integral points on the complement of ramification-divisors. *J. Inst. Math. Jussieu* **4** (2005), no. 2, 317-330.
62. U. Zannier, Hilbert Irreducibility Theorem above algebraic groups, *Duke Math. J.* **153** (2010), no. 2, 397-425
63. U. Zannier, Roth theorem, integral points and certain ramified covers of $\mathbb{P}_1$. In *Analytic Number Theory - Essays in honor of Klaus Roth*, Cambridge University Press 2008.
64. U. Zannier, Lecture Notes on Diophantine Analysis, Edizioni della Normale, 2009.