ETH Zürich

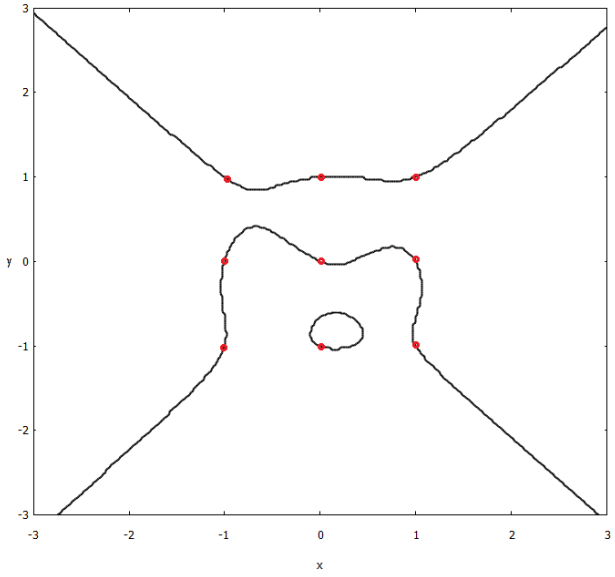
Bachelor thesis

A theorem of Runge

On the finiteness of integral points of certain irreducible rational curves

Author:
Raphael Steiner

Supervisor:
PD Dr. Clemens Fuchs



August 28, 2012

Contents

1 Introduction

In 1887 Carl Runge proved the theorem stating that there are only finitely many integral zeros of an irreducible integer polynomial in 2 variables such that its polynomial of highest degree factors into 2 non-constant relatively prime polynomials. A later result by Siegel showed that if an affine curve has infinitely many integral points, then it must have genus 0 and at most 2 points at infinity. But Siegel's proof was ineffective in comparison to Runge's proof which was effective, when applied.
This bachelor thesis gives a proof of the finiteness in a slightly more general setting than Runge's original theorem and a bound in some simple cases.

1.1 Notation

$\mathbb{N} = \{1, 2, 3, \dots\}$ the set of natural numbers or positive integers.
$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ the set of non-negative integers.
$\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$ the set of integers.
$\mathbb{Q}$ the set of rational numbers.
$\mathbb{R}$ the set of real numbers.
$\mathbb{C}$ the set of complex numbers.
$\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$ usually embedded in $\mathbb{C}$ in the standard way.
$\mathcal{P}(A)$ the set of all subsets of a set A.
$Q(B)$ the fraction/quotient field of an integer domain B.
$B^\times$ the group of units of an integer domain B.
$\langle B \rangle$ the ideal generated by the elements of B.
$r(\mathfrak{a})$ the radical ideal of an ideal $\mathfrak{a}$.

Rings shall always assumed to be unitary commutative rings.

2 Preliminaries

In this chapter a short overview of some results from commutative algebra, especially discrete valuations, and topological results are given, which are needed in later chapters.

2.1 Noetherian Rings

Definition 2.1. A partially ordered set $(A, \leq)$ satisfies the ascending chain condition iff every countable chain $a_1 \leq a_2 \leq a_3 \leq \cdots$ is eventually constant, that is $\exists N \in \mathbb{N} : \forall n \geq N : a_n = a_N$.

Definition 2.2. A ring A is called noetherian iff $(\{I \subseteq A | I \text{ is an ideal of } A\}, \subseteq)$ satisfies the ascending chain condition.

Proposition 2.3. *The following assertions are equivalent:*

1. *The ring A is noetherian.*

2. *Every ideal of A is finitely generated.*

Proof. See page 75 of [AM94]. □

Theorem 2.4 (Hilbert Basis theorem)**.** *If a ring A is noetherian, then the ring of polynomials $A[X]$ is also noetherian.*

Proof. See page 81 of [AM94]. □

Example. The polynomial ring $K[X_1, \ldots, X_n]$ over a field K is a noetherian unique factorization domain.

2.2 Dimension of a ring

Definition 2.5. The Krull dimension of a ring A, generally referred to as the dimension of the ring A, is defined as: $\dim(A) = \sup\{n \in \mathbb{N}_0 | \exists\ \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n : \forall i = 0, \ldots, n : \mathfrak{p}_i \subseteq A \text{ prime ideal}\}$

Definition 2.6. The height of a prime $\mathfrak{p}$ is defined as: $\text{height}(\mathfrak{p}) = \sup\{n \in \mathbb{N}_0 | \exists\ \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p} : \forall i = 0, \ldots, n : \mathfrak{p}_i \subseteq A \text{ prime ideal}\}$

Definition 2.7. A noetherian local ring A of dimension d is called regular iff $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$, where $\mathfrak{m}$ is its maximal ideal and $k = A/\mathfrak{m}$ is the residue field.

Theorem 2.8. *Let k be a field and let B be an integral domain which is finitely generated as a k-algebra. Then:*

1. *The dimension of B is equal to the transcendence degree of the quotient field $Q(B)$ of B over k.*

2. *For any prime ideal $\mathfrak{p} \subseteq B$: $\text{height}\,\mathfrak{p} + \dim B/\mathfrak{p} = \dim B$.*

Proof. See chapter 5, paragraph 14 of [M70]. □

2.3 Discrete valuation rings

Definition 2.9. Let K be a field. A discrete valuation of K is a surjective map $\nu : K^\times \to \mathbb{Z}$ such that:

1. $\nu(xy) = \nu(x) + \nu(y)$,

2. $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$,

this is usually extended to K by setting $\nu(0) = +\infty$. The ring $R = \{x \in K | \nu(x) \geq 0\}$ is called the valuation ring of ν. If k is a subfield of K such that $\nu(k^\times) = \{0\}$, we say that ν is a discrete valuation of K/k.

Definition 2.10. An integral domain R is called a discrete valuation ring iff there exists a discrete valuation ν of its field of fractions such that R is the valuation ring of ν.

A discrete valuation ring is a local ring with maximal ideal $\mathfrak{m} = \{x \in R | \nu(x) > 0\}$, since all the elements with $\nu(x) = 0$ are units. $R/\mathfrak{m}$ is called the residue field of ν. Moreover two elements x, y satisfy $x|y$ iff $\nu(x) \leq \nu(y)$. It follows that all non-zero ideals are of the form $\{x \in R | \nu(x) \geq k\}$ for some $k \in \mathbb{N}_0$ and hence noetherian. Also, since the valuation is surjective, there exists an element $x \in R$ such that $\nu(x) = 1$, and all non-zero ideals are of the form $(x^k) = (x)^k$, which is prime iff $k = 1$ and thus of dimension 1. Such an x is called a local parameter.

Example. Let K be a field. All discrete valuations of $K(X)/K$ are given by ν_f, where $f \in K[X]$ is irreducible and $\nu_f(g) = \max\{k \in \mathbb{N}_0 |\ f^k | g\}$ ($K[X]$ is factorial) for $g \in K[X] \backslash \{0\}$ extended to $K(X)$, and $\nu_\infty(\frac{g}{h}) = \deg(h) - \deg(g)$ for $g, h \neq 0$.

Proof. Let ν be a discrete valuation of $K(X)/K$, R the corresponding valuation ring and $\mathfrak{m}$ its maximal ideal. If $\nu(X) \geq 0$, then $K[X] \subseteq R$ and $\mathfrak{m} \cap K[X]$ is prime and thus of the form (f), where f irreducible in $K[X]$. Then $K[X]_{(f)} \subseteq R$, so $\nu_f(g) \geq 0 \Rightarrow \nu(g) \geq 0$ and $\nu_f(g) > 0 \Rightarrow \nu(g) > 0$, further if $\nu_f(g) < 0$, then $\nu_f(g^{-1}) > 0$ so $\nu(g^{-1}) > 0$ and $\nu(g) < 0$, which implies $K[X]_{(f)} = R$ and thus $\nu = \nu_f$, because the maximal ideals coincide. If $\nu(X) < 0$, then $\nu(\frac{1}{X}) > 0$ and $K[\frac{1}{X}] \subseteq R$ and $\mathfrak{m} \cap K[\frac{1}{X}] = (\frac{1}{X})$. So again $K[\frac{1}{X}]_{(\frac{1}{X})} \subseteq R$ and $\nu_\infty(g) \geq 0 \Rightarrow \nu(g) \geq 0$ and $\nu = \nu_\infty$. For further details see page 9 of [I93]. □

Proposition 2.11. *Let $\nu_1, \ldots, \nu_n$ be different discrete valuations of K/k, then there exist elements $x_1, \ldots, x_n \in K$ such that $\nu_i(x_j) = \delta_{ij}$, where δ_{ij} is the Kronecker delta.*

Proof. See page 5 of [I93] or page 12 of [S08]. □

Theorem 2.12. *Let R be a noetherian local domain of dimension 1, $\mathfrak{m}$ its maximal ideal and $k = R/\mathfrak{m}$ its residue field. Then the following are equivalent:*

1. *R is a discrete valuation ring.*
2. *R is integrally closed.*
3. *$\mathfrak{m}$ is a principal ideal.*
4. *$\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, i.e. R is regular.*
5. *Every non-zero ideal of R is a power of $\mathfrak{m}$.*
6. *$\exists x \in R:$ every non-zero ideal is of the form (x^k) for some $k \in \mathbb{N}_0$.*

Proof. See page 94 of [AM94]. □

Proposition 2.13. *Let R be a discrete valuation ring with valuation ν, $\mathfrak{m}$ its maximal ideal, t a local parameter and k a subfield of R, such that the composition $k \xrightarrow{\text{id}} R \xrightarrow{\pi} R/\mathfrak{m}$ is an isomorphism of k. Then:*

1. *For any $z \in R$ there is a unique $\lambda \in k$ such that $z - \lambda \in \mathfrak{m}$.*

2. *For any $z \in R$ and $n \in \mathbb{N}_0$ there are unique $\lambda_0, \ldots, \lambda_n \in k$ and $z_n \in R$ such that $z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1}$.*

3. *There is a monomorphism $l : Q(R) \to k((t))$ such that the valuations ν and ν_t agree, where $\nu_t(\sum_{n \geq m} \lambda_n t^n) = \min\{n \geq m | \lambda_n \neq 0\}$.*

Proof. Let $z \in R$ and $\lambda = \pi(z) \in k$, then $\pi(z - \lambda) = 0$ and hence $z - \lambda \in \mathfrak{m}$. Let also $z - \lambda' \in \mathfrak{m}$, then $\lambda' - \lambda \in \mathfrak{m}$ and hence $\lambda' - \lambda = \pi(\lambda' - \lambda) = 0$. Now $x \in \mathfrak{m} \Leftrightarrow t | x$ so *2.* follows immediately by induction. Now the uniqueness in *2.* implies the homomorphism condition of the induced map $l : R \to k[[t]]$, which is injective, because for a non-zero element z, $z \in \mathfrak{m}^n \backslash \mathfrak{m}^{n+1}$, where $n = \nu(z)$ and so $\lambda_{n+1}(z) \neq 0$. This morphism extends to $l : Q(R) \hookrightarrow k((t))$. Now it's clear that the valuations agree on R respectively on $\mathrm{Im}(R)$. For an element $z \in Q(R) \backslash R$ write $z = t^k z'$ with $k = \nu(z) < 0$ and hence $z' \in R$ a unit. Now $l(z) = l(t^k z') = l(t^{-k})^{-1} l(z') = t^k l(z')$ and thus the valuations agree. □

2.4 Topology

Definition 2.14. A non-empty topological space X is called irreducible iff any two non-empty open sets have non-empty intersection or equivalently X cannot be written as a union of two proper closed subsets. A subset Y of X is called irreducible iff Y is an irreducible topological space with the induced topology.

Proposition 2.15. *A non-empty open subset U of an irreducible topological space X is irreducible and dense.*

Proof. $\overline{U} \cup U^c = X$, now $U^c \neq X$, so $\overline{U} = X$. Let W, V be non-empty open subsets of X, then $\emptyset \neq W \cap V \cap U = (W \cap U) \cap (V \cap U)$. □

Proposition 2.16. *The closure of an irreducible subset Y is again irreducible.*

Proof. Let W, Z be closed in $\overline{Y}$ such that $\overline{Y} = W \cup Z$, then $W \cap Y$ and $Z \cap Y$ are closed in Y and $(W \cap Y) \cup (Z \cap Y) = Y$, so $W \cap Y = Y$ or $Z \cap Y = Y$ without loss of generality the former, thus $Y \subseteq W$ and, since W is closed, $\overline{Y} \subseteq W$. □

Definition 2.17. The dimension of a topological space is defined as $\dim(X) = \sup\{n \in \mathbb{N}_0 | \exists Y_0 \subsetneq Y_1 \subsetneq \cdots \subsetneq Y_n : \forall i = 0, \ldots, n : Y_i \text{ is a closed irreducible subset of } X\}$.

Definition 2.18. A topological space X is called noetherian iff $(\{Y \subseteq X | Y \text{ is closed}\}, \supseteq)$ satisfies the ascending chain condition.

Proposition 2.19. *A subset Y of an noetherian topological space X is again noetherian with the induced topology.*

Proof. Let $V_i \subseteq X$ be closed subsets such that $V_1 \cap Y \supseteq V_2 \cap Y \supseteq \cdots$ is a decreasing sequence of closed subsets of Y, then $V_1 \supseteq V_1 \cap V_2 \supseteq V_1 \cap V_2 \cap V_3 \supseteq \cdots$ is a decreasing sequence of closed subsets of X, thus eventually constant, and $Y \cap \bigcap_{i=1}^{n} V_n = V_n \cap Y$. □

Proposition 2.20. *In a noetherian topological space every non-empty closed subset Y is a finite union $Y = Y_1 \cup \cdots \cup Y_n$ of closed irreducible subsets Y_i. If one requires $Y_j \not\supseteq Y_i$ for $j \neq i$, then they are uniquely determined and are called the irreducible components of Y.*

Proof. See page 5 of [H77] □

3 Some Algebraic Geometry

This chapter follows more or less the structure of [H77], chapter 1, but over an arbitrary field as in [G12]. Most proofs of the former also apply to the more general setting, if not proofs are given.

3.1 Varieties

3.1.1 Affine varieties

Let K/k be a field extension, where K is algebraically closed, and let $A = k[X_1, \ldots, X_n]$ be the polynomial ring in n variables. There are natural maps I, V:

$$\begin{aligned} I : \mathcal{P}(K^n) &\to \mathcal{P}(A) \\ X &\mapsto \{f \in A | \forall (x_1, \ldots, x_n) \in X : f(x_1, \ldots, x_n) = 0\} \end{aligned}$$

$$\begin{aligned} V : \mathcal{P}(A) &\to \mathcal{P}(K^n) \\ B &\mapsto \{(x_1, \ldots, x_n) \in K^n | \forall f \in B : f(x_1, \ldots, x_n) = 0\} \end{aligned}$$

Proposition 3.1. *The following holds:*

1. $V(B) \cup V(B') = V(B \cdot B'), \quad \forall B, B' \subseteq A.$
2. $\bigcap_{j \in J} V(B_j) = V\left(\bigcup_{j \in J} B_j\right), \quad \forall B_j \subseteq A.$
3. $V(\emptyset) = K^n.$
4. $V(\{1\}) = \emptyset.$
5. $V(B) = V(\langle B \rangle) = V(r(\langle B \rangle)), \quad \forall B \subseteq A.$
6. $I(X)$ *is a radical ideal in* $A, \quad \forall X \subseteq K^n.$

1. through *4.* imply that we can equip K^n with the topology, where the closed sets are exactly the sets of the form $V(B)$ for some $B \subseteq A$. This topology shall be referred to as the *Zariski topology induced by* k. *5.* and *6.* imply that we can restrict the domain of V and the co-domain of I to ideals of A or even radical ideals of A.

Proposition 3.2. *The pair (V, I) forms a Galois connection that is:*

1. $B_1 \subseteq B_2 \Rightarrow V(B_1) \supseteq V(B_2), \quad \forall B_1, B_2 \subseteq A.$
2. $X_1 \subseteq X_2 \Rightarrow I(X_1) \supseteq I(X_2), \quad \forall X_1, X_2 \subseteq K^n.$
3. $B \subseteq I(V(B)), \quad \forall B \subseteq A.$
4. $X \subseteq V(I(X)), \quad \forall X \subseteq K^n.$

Proposition 3.3. *It follows that:*

1. $I \circ V \circ I = I.$
2. $V \circ I \circ V = V.$
3. *The restricted maps*

$$\mathcal{R}_k := \{B \subseteq A | \exists X \subseteq K^n : B = I(X)\} \underset{I}{\overset{V}{\rightleftharpoons}} \{X \subseteq K^n | \exists B \subseteq A : X = V(B)\} =: \mathcal{A}_k$$

are inverse to each other.

Definition 3.4. The elements of $\mathcal{A}_k$ shall be called affine k-algebraic sets.

Proposition 3.5. $V(I(X)) = \overline{X}, \quad \forall X \subseteq K^n$, *where* $\overline{X}$ *denotes the closure of* X *in the Zariski topology induced by* k.

Theorem 3.6 (Hilbert's Nullstellensatz)**.** *Let* $\mathfrak{a} \subseteq A$ *be an ideal, then* $I(V(\mathfrak{a})) = r(\mathfrak{a})$.

Proof. We shall use weak form of Hilbert's Nullstellensatz, which states that if k and E are fields and E is a finitely generated k-algebra, then E is an algebraic extension of k. A proof can be found on page 82 of [AM94]. Thus if one is given a proper ideal $\mathfrak{a}$, then $V(\mathfrak{a})$ is non-empty, because the extension of $\mathfrak{a}$ to $K[X_1, \ldots, X_n]$ is again proper: extend $k_1 = 1$ to a basis (k_i) of K/k, let $\sum_j f_j a_j \in \mathfrak{a}^e$, $f_j \in K[X_1, \ldots, X_n]$ and $a_j \in \mathfrak{a}$, where each $f_j = \sum_i k_i f_{ij}$, $f_{ij} \in k[X_1, \ldots, X_n]$, then $\sum_j f_j a_j \in k[X_1, \ldots, X_n]$ iff $\sum_j f_{ij} a_j = 0$ for all $i \neq 1$, thus $\mathfrak{a}^{ec} = \mathfrak{a}$. So one can take a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}^e$. Then $K[X_1, \ldots, X_n] / \mathfrak{m}$ is an algebraic extension of K, thus is isomorphic to K, and the image of $X_1, \ldots, X_n$ defines a point, which is a common vanishing point of all elements of $\mathfrak{m} \supseteq \mathfrak{a}$. Now we are going to use Rabinowitsch's trick. Suppose $f \in I(V(\mathfrak{a}))$, by introducing a new variable X_0 one sees that the ideal generated by $\mathfrak{a}$ and $1 - X_0 f$ does not have a common vanishing point, so they generate the whole ring. Thus one gets an equation $1 = g_0(1 - X_0 f) + \sum_{i=1}^{k} g_i f_k$ for some $g_i \in k[X_0, \ldots, X_n]$ and $f_i \in \mathfrak{a}$. Setting $X_0 = \frac{1}{f}$ and clearing denominators one gets $f \in r(\mathfrak{a})$. The reverse inclusion is trivial. □

Corollary 3.7. *There is a one-to-one correspondence between affine* k*-algebraic sets of* K^n *and radical ideals in* A.

Definition 3.8. An affine k-algebraic set X is called an affine k-variety iff X is irreducible in the Zariski topology induced by k.

Proposition 3.9. *There is a one-to-one correspondence between affine k-varieties of K^n and prime ideals in A.*

Definition 3.10. An affine k-algebraic set X is called an affine variety, if it is absolutely irreducible, that is X is irreducible in the Zariski topology induced by K, in other words X is an affine K-variety. Note that in this case X is necessarily an affine k-variety.

Definition 3.11. Let X be an affine k-variety. We define the affine coordinate ring to be $A[X] := A \,/\, I(X)$, which is an integral domain. By $A(X)$ we denote the quotient field of $A[X]$ and also we define $X(L) := X \cap L^n$, where L is a subfield of K, to be the points on X with coordinates in L.

3.1.2 Projective varieties

Definition 3.12. The n-dimensional projective space over a field K is defined as: $\mathbb{P}^n(K) := (K^{n+1} \backslash \{0\}) \,/\, K^\times$, where the quotient has to be understood as $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$, $\lambda \in K^\times$. By $(a_0 : \cdots : a_n)$ we denote the class of $(a_0, \ldots, a_n)$.

Every homogeneous polynomial f in $S = k[X_0, \ldots, X_n]$ defines a function $f : \mathbb{P}^n(K) \to \{0, 1\}$, where $f(a_0 : \cdots : a_n) = 0 \Leftrightarrow f(a_0, \ldots, a_n) = 0$. Let $S^h = \bigcup_{d \in \mathbb{N}_0} S_d$ denote the homogeneous elements of S. Then one has again maps:

$$
\begin{aligned}
I : \mathcal{P}(\mathbb{P}^n(K)) &\to \mathcal{P}(S^h) \\
X &\mapsto \{f \in S^h | \forall (x_0 : \cdots : x_n) \in X : f(x_1 : \cdots : x_n) = 0\} \\
V : \mathcal{P}(S^h) &\to \mathcal{P}(\mathbb{P}^n(K)) \\
B &\mapsto \{(x_0 : \cdots : x_n) \in \mathbb{P}^n(K) | \forall f \in B : f(x_0 : \cdots : x_n) = 0\}
\end{aligned}
$$

Proposition 3.13. *The following holds:*

1. $V(B) \cup V(B') = V(B \cdot B'), \quad \forall B, B' \subseteq S^h.$
2. $\bigcap_{j \in J} V(B_j) = V\left(\bigcup_{j \in J} B_j\right), \quad \forall B_j \subseteq S^h.$
3. $V(\emptyset) = \mathbb{P}^n(K).$
4. $V(\{1\}) = \emptyset.$

So we can equip $\mathbb{P}^n(K)$ with the topology, where the closed sets are exactly the sets of the form $V(B)$ for some $B \subseteq S^h$. This topology is referred to as the *Zariski topology induced by* k and the closed sets are called projective k-algebraic sets.

Definition 3.14. An ideal $\mathfrak{a}$ of a graded ring $R = \bigoplus_{d \in \mathbb{Z}} R_d$ is called homogeneous iff $\mathfrak{a} = \bigoplus_{d \in \mathbb{Z}} \mathfrak{a}_d = \bigoplus_{d \in \mathbb{Z}} (\mathfrak{a} \cap R_d)$.

Proposition 3.15. *An ideal is homogeneous iff it can be generated by homogeneous elements. The sum, product, intersection and radical of homogeneous ideals are again homogeneous and a homogeneous ideal* $\mathfrak{a}$ *is prime iff* $f, g \in \mathfrak{a} \Rightarrow f \in \mathfrak{a}$ *or* $g \in \mathfrak{a}$ *for homogeneous elements* f, g.

Let $\mathcal{I}^h$ denote the set of homogeneous ideals of S. The domain of V can be extended to $\mathcal{I}^h$, by setting $V(\mathfrak{a}) = V(\mathfrak{a} \cap S^h)$ and also the co-domain of I can be extended to $\mathcal{I}^h$ by composition of $\langle \cdot \rangle$.

Proposition 3.16. *The following holds:* $V(B) = V(\langle B \rangle), \quad \forall B \subseteq S^h$.

So we can restrict to homogeneous ideals.

Proposition 3.17. *The following holds:*

1. V, I *form a Galois connection.*
2. *For a homogeneous ideal* $\mathfrak{a}$*:* $V(\mathfrak{a}) = \emptyset \Leftrightarrow r(\mathfrak{a}) = S$ *or* $S_+ \left(:= \bigoplus_{d \in \mathbb{N}} S_d\right) \Leftrightarrow \exists d \in \mathbb{N} : S_d \subseteq \mathfrak{a}$.
3. $V(\mathfrak{a}) \neq \emptyset \Rightarrow I(V(\mathfrak{a})) = r(\mathfrak{a}), \quad \forall \mathfrak{a} \in \mathcal{I}^h$.
4. $V(I(X)) = \overline{X}, \quad \forall X \subseteq \mathbb{P}^n(K)$.

Definition 3.18. A projective k-algebraic set X is called a projective k-variety iff X is irreducible in the Zariski topology induced by k.

Proposition 3.19. *There is a one-to-one correspondence between projective* k*-varieties of* $\mathbb{P}^n(K)$ *and homogeneous prime ideals in* S.

Definition 3.20. A projective k-algebraic set X is called a projective variety, if it is absolutely irreducible, that is X is irreducible in the Zariski topology induced by K; in other words X is a projective K-variety. Note that in this case X is necessarily a projective k-variety.

Definition 3.21. Let X be a projective k-variety. We define the homogeneous coordinate ring to be $S[X] := S \,/\, I(X)$, which is a graded integral domain. We also define $X(L) := X \cap \mathbb{P}^n(L)$ for L a subfield of K to be the points on X with coordinates in L, where $\mathbb{P}^n(L)$ is embedded in $\mathbb{P}^n(K)$ in the usual way: $(a_0 : \cdots : a_n) \mapsto (a_0 : \cdots : a_n)$.

Definition 3.22. An affine/projective (k-)variety of dimension 1 is called an affine/projective (k-)curve.

Definition 3.23. An affine/projective K-variety Y is defined over a subfield L of K if one can find a set of generators of $I(X) \subseteq K[X_1, \ldots, X_n]$, respectively $K[X_0, \ldots, X_n]^h$, which are in $L[X_1, \ldots, X_n]$, respectively $L[X_0, \ldots, X_n]^h$.

3.2 Functions, morphisms and rational maps

Definition 3.24. Let X be an affine/projective k-variety, V a non-empty open subset of X. A function $f : V \to K$ is called regular at a point $P \in V$ iff there exists an open neighborhood U of P and polynomials $g, h \in A$, respectively S_d for some $d \in \mathbb{N}_0$, such that h is nowhere zero on U and $f = g/h$ on U. A function is called regular on V iff it is regular at every point in V.

Definition 3.25. A morphism between varieties (of any kind) X, Y is a continuous map $\varphi : X \to Y$ such that for every open subset $V \subseteq Y$ and any regular function $f : V \to K$ $f \circ \varphi : \varphi^{-1}(V) \to K$ is a regular map.

Definition 3.26. Let X be a k-variety. By $\mathcal{O}^k(X)$ we denote the set of all regular functions on X. Given a point P on X, we define the local ring $\mathcal{O}_P^k$ at P on X to be the ring of germs of regular functions on X near P, that is the set of pairs (U, f), where U is an open neighborhood of P and f a regular function on U, and two elements (U, f) and (V, g) are identified iff there is an open neighborhood $W \subseteq U \cap V$ of P such that $f = g$ on W. $\mathcal{O}_P^k$ is a local ring where the maximal ideal is the set of regular functions vanishing at P, because if a regular function is not vanishing at P, then its inverse is a regular function defined if necessary on a smaller neighborhood of P.

Definition 3.27. Let X be a k-variety. The function field $k(X)$ is defined as the set of equivalence classes (U, f), where $U \subseteq X$ is a non-empty open subset and f is a regular function on U, and where we identify two pairs $(U, f), (V, g)$ iff there exists a non-empty open subset $W \subseteq U \cap V$ such that $f = g$ on W. Note that operations can be defined, since X being irreducible implies that any two non-empty open subsets have non-empty intersection.

Theorem 3.28. *Let X be an affine k-variety with affine coordinate ring $A[X]$, then the following holds:*

1. $\mathcal{O}^k(X) \cong A[X]$.
2. *Given a point P and $\mathfrak{m}_p \subseteq A[X]$ the set of all functions vanishing at P we have $\mathcal{O}_P^k \cong A[X]_{\mathfrak{m}_P}$ and if $P \in X(k)$, then $\dim \mathcal{O}_P^k = \dim X$.*
3. *$k(X) \cong A(X)$, the quotient field of $A[X]$. Moreover the transcendence degree of $k(X)$ is equal to $\dim X$.*

If S is a graded ring and $\mathfrak{p}$ a homogeneous ideal, then we define $S_{(\mathfrak{p})}$ to be the set of all elements of degree 0, when localizing at the homogeneous elements of S not in $\mathfrak{p}$ and the grading is extended in the usual way: $\deg(f/g) = \deg(f) - \deg(g)$ for homogeneous elements f, g.

Theorem 3.29. *Let X be a projective k-variety, with homogeneous coordinate ring $S[X]$, then the following holds:*

1. *Given a point P and $\mathfrak{m}_p \subseteq S[X]$ the ideal generated by all the homogeneous polynomials $f \in S[X]$ vanishing at P we have $\mathcal{O}_P^k \cong S[X]_{(\mathfrak{m}_P)}$.*

2. *$k(X) \cong S[X]_{((0))}$.*

Definition 3.30. An open neighborhood of a point P in a variety Y, which is isomorphic to an affine variety, is called an affine neighborhood.

Example. Let Y be a projective variety, P a point in Y and $f \in S^h$ of degree 1 (f defines a hyperplane), such that $f(P) \neq 0$, then $Y \backslash V(f)$ is an affine neighborhood of P.

Proof. Clearly $Y \backslash V(f)$ is an open neighborhood of P. Suppose $Y \subseteq \mathbb{P}^n(K)$, and consider the following map and its inverse:

$$\begin{aligned} \varphi : \mathbb{P}^n(K) \backslash V(f) &\to V(f-1) \subseteq K^{n+1} \\ (a_0 : \cdots : a_n) &\mapsto \left(\frac{a_0}{f(a_0, \ldots, a_n)}, \ldots, \frac{a_n}{f(a_0, \ldots, a_n)} \right) \\ \varphi^{-1} : V(f-1) \subseteq K^{n+1} &\to \mathbb{P}^n(K) \backslash V(f) \\ (a_0, \ldots, a_n) &\mapsto (a_0 : \cdots : a_n) \end{aligned}$$

These are both continuous. Now $Y \backslash V(f)$ is irreducible (non-empty open subset of an irreducible set) and so also its image, thus an affine variety. It is also easily checked, that φ and φ^{-1} restricted to $Y \backslash V(f)$ respectively $\mathrm{Im}(Y \backslash V(f))$ are morphisms. □

If k is infinite and given finitely many points, then there is always a hyperplane avoiding all of these points. $Y \backslash V(X_i)$ is an affine open cover of Y and is called the standard affine cover.

Definition 3.31. Let X, Y be varieties. A rational map $\varphi : X \to Y$ is an equivalence class of pairs (U, φ_U), where U is a non-empty open subset of X, φ_U is a morphism of U to Y and the equivalence is given by $(U, \varphi_U) \cong (V, \varphi_V)$ iff φ_U and φ_V agree on $U \cap V$. A birational map is a rational map, which admits an inverse as a rational map, in this case we say X and Y are birationally equivalent. If a birational map has a representative, such that $U = X$, then it also defines a morphism and is thus called a birational morphism.

The above example defines a birational map. If X and Y are birationally equivalent, then by definition of a function field it is clear, that their function fields are isomorphic.

3.3 Non-singularity

Definition 3.32. Let Y be an affine K-variety defined over k and let $f_1, \ldots, f_t \in k[X_1, \ldots, X_n]$ be a set of generators of $I(Y) \subseteq K[X_1, \ldots, X_n]$. Y is called non-singular at a point $P \in Y(k)$ iff the rank of the matrix $(\frac{\partial f_i}{\partial X_j}(P))_{1 \leq i \leq t, 1 \leq j \leq n}$ is $n - r$ where r is the dimension of Y. This is independent of the choice of the set of generators

Lemma 3.33. *Let A be an integral domain, $\mathfrak{m} \subseteq A$ a maximal ideal and $n \in \mathbb{N}$, then*

$$\mathfrak{m} \Big/ \mathfrak{m}^n \cong \mathfrak{m}A_{\mathfrak{m}} \Big/ (\mathfrak{m}A_{\mathfrak{m}})^n$$

Proof. Consider the map:

$$\begin{array}{rccc} \mathfrak{m} \to & \mathfrak{m}A_{\mathfrak{m}} & \to & \mathfrak{m}A_{\mathfrak{m}} \Big/ (\mathfrak{m}A_{\mathfrak{m}})^n \\ x \mapsto & \dfrac{x}{1} & \mapsto & \overline{\left(\dfrac{x}{1}\right)} \end{array}$$

We shall prove, that the kernel is $\mathfrak{m}^n$ and that the map is surjective. Since $\mathfrak{m}$ is prime $\frac{a}{s} \in \mathfrak{m}A_{\mathfrak{m}}$ iff $a \in \mathfrak{m}$. Also notice that for $s \notin \mathfrak{m}$ one has $(s) + \mathfrak{m}^n = A$, suppose not, then it would be contained in a maximal ideal $\mathfrak{n}$ and one would have $\mathfrak{m} = r(\mathfrak{m}^n) \subseteq r(\mathfrak{n}) = \mathfrak{n}$ and thus $\mathfrak{n} = \mathfrak{m}$ and $s \in \mathfrak{m}$, a contradiction. Let x be in the kernel. Thus $\frac{x}{1} \in (\mathfrak{m}A_{\mathfrak{m}})^n$ and so $sx \in \mathfrak{m}^n$ for some $s \notin \mathfrak{m}$ and we have an equation $sy + m = 1$, where $y \in A$ and $m \in \mathfrak{m}^n$ and thus $\mathfrak{m}^n \ni syx + mx = x$, on the other hand it is clear that $\mathfrak{m}^n$ is contained in the kernel. Now consider an element $\overline{(a/s)}$ in $\mathfrak{m}A_{\mathfrak{m}} \,/\, (\mathfrak{m}A_{\mathfrak{m}})^n$. We need to find an element $y \in \mathfrak{m}$ such that $\frac{y}{1} - \frac{a}{s} \in (\mathfrak{m}A_{\mathfrak{m}})^n$, but we have an equation $sy + m = a$, with $m \in \mathfrak{m}^n$ and $y \in A$, but further $a \in \mathfrak{m}$ and so since $s \notin \mathfrak{m}$ we have $y \in \mathfrak{m}$ and thus y satisfies the condition. □

Theorem 3.34. *Let Y be an affine K-variety defined over k. Then Y is non-singular at a point $P \in Y(k)$ iff $\mathcal{O}_P^k$ is a regular local ring.*

Definition 3.35. Let Y be a K-variety defined over k. Then Y is also a K-variety defined over a field $k \subseteq L \subseteq K$. Y is called non-singular at a point $P \in Y(K)$ iff the local ring $\mathcal{O}_P^L$ at P is a regular local ring for any field $k \subseteq L \subseteq K$ containing P. Note, since $\mathcal{O}_P^L$ depends only on an affine neighborhood of P, the theorem implies it is sufficient that $\mathcal{O}_P^L$ is a regular local ring for a specific field L containing P. Y is called non-singular iff Y is non-singular at every point.

Theorem 3.36. *Let $\mathcal{C}$ be a projective curve over an algebraically closed field K of characteristic 0. Then there is a up to isomorphism unique non-singular projective curve $\mathcal{X}$ and a birational morphism f from $\mathcal{X}$ onto $\mathcal{C}$. Moreover the local rings corresponding to the points of $\mathcal{X}$ are in one-to-one correspondence with the discrete valuation rings of $K(\mathcal{C})/K$ and $f(Q) = P$ iff $\mathcal{O}_{Q,\mathcal{X}}^K$ dominates $\mathcal{O}_{P,\mathcal{C}}^K$, that is $\mathcal{O}_{P,\mathcal{C}}^K \subseteq \mathcal{O}_{Q,\mathcal{X}}^K$ and the contraction of the maximal ideal is again the maximal ideal. We say $\mathcal{X}$ is a non-singular model of $\mathcal{C}$.*

Proof. See chapter 1 paragraph 6 of [H77], or chapter 7 of [F69] for a more constructive proof. □

3.4 Weil-divisors for curves

If we are given a non-singular K-curve Y defined over k, then every local ring $\mathcal{O}_P^L$, $k \subseteq L \subseteq K$, $P \in Y(L)$, is a discrete valuation ring with respect to the valuation ν_P^L with field of fractions $L(Y)$ and residue field L.

Proposition 3.37. *Let Y be as above, $k \subseteq L \subseteq K$ be field and $P \in Y(L)$ a point, then $\nu_P^K|_{L(Y)} = \nu_P^L$ and we write ν_P instead of ν_P^K.*

Proof. It is sufficient to show that a local parameter $\mathcal{O}_P^L$ is also a local parameter in $\mathcal{O}_P^K$. Choose an affine neighborhood of P. Let $\mathfrak{b} = I(Y)$ and $\mathfrak{m}_L, \mathfrak{m}_K$ be the maximal ideal corresponding to P in $L[X_1, \ldots, X_n], K[X_1, \ldots, X_n]$ respectively and $\mathfrak{m}_P^L, \mathfrak{m}_P^K$ the maximal ideal corresponding to P in $\mathcal{O}_P^L, \mathcal{O}_P^K$ respectively. Now since Y is defined over $k \subseteq L$ and $P \in Y(L)$, we can find generators $f_1, \ldots, f_m$ of $\mathfrak{b}$ with coefficients in L and $\mathfrak{m}_L, \mathfrak{m}_K$ are both generated by $X_1 - a_1, \ldots, X_n - a_n$, where $P = (a_1, \ldots, a_n)$. Consider the following commuting diagram:

$$\begin{array}{ccc} \mathfrak{m}_P^L \Big/ \left(\mathfrak{m}_P^L\right)^2 & \xrightarrow{\text{id}} & \mathfrak{m}_P^K \Big/ \left(\mathfrak{m}_P^K\right)^2 \\ \downarrow \wr & & \downarrow \wr \\ \mathfrak{m}_L \Big/ \mathfrak{m}_L^2 + \mathfrak{b} & \xrightarrow{\text{id}} & \mathfrak{m}_K \Big/ \mathfrak{m}_K^2 + \mathfrak{b} \end{array}$$

The isomorphisms are due to Lemma 3.33 and the other maps are given by the identity. We shall prove, that the bottom map is injective. Extend $k_1 = 1$ to a basis (k_α) of K over L. Suppose g is in the kernel, then $g = \sum p_i f_i + \sum q_{i,j}(X_i - a_i)(X_j - a_j)$. Write $p_i = \sum k_\alpha p_i^\alpha$ and $q_{i,j} = \sum k_\alpha q_{i,j}^\alpha$, where $p_i^\alpha, q_{i,j}^\alpha \in L[X_1, \ldots, X_n]$. Then

$$g = \sum_\alpha k_\alpha \left(\sum p_i^\alpha f_i + \sum q_{i,j}^\alpha (X_i - a_i)(X_j - a_j) \right) = \sum p_i^1 f_i + \sum q_{i,j}^1 (X_i - a_i)(X_j - a_j)$$

This means g is already in the ideal $\mathfrak{m}_L^2 + \mathfrak{b}$, hence zero. Now a local parameter of $\mathcal{O}_P^L$ corresponds to a non-zero element in $\mathfrak{m}_P^L \,/\, \left(\mathfrak{m}_P^L\right)^2$ and is therefore non-zero in $\mathfrak{m}_P^K \,/\, \left(\mathfrak{m}_P^K\right)^2$ and thus a local parameter of $\mathcal{O}_P^K$. □

Lemma 3.38. *Given $f \in K(Y)^\times$, then $\nu_P(f) = 0$ for all but finitely many points $P \in Y$.*

Proof. It is enough to look at the affine case, by taking the standard affine cover. Let $f = g/h$ with $g, h \notin I(Y)$. It suffices to show that $V((g) + I(Y))$ and $V((h) + I(Y))$ are both finite. Now $V((g) + I(Y)) \subsetneq Y$, which means that $V((g) + I(Y))$ is a finite union of irreducible closed subsets of dimension 0, which are single points since K is algebraically closed. □

Definition 3.39. A divisor is an element of the free abelian group $\mathrm{Div}(Y)$ generated by the points $P \in Y$, thus of the form $D = \sum_P n_P P$, where $n_p \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many P. The support of such a divisor D is $\mathrm{Supp}(D) = \bigcup_{n_P \neq 0} \{P\}$. The divisor of zeros respectively poles of D is defined as $(D)_0 = \sum_{n_P > 0} n_P P$ respectively $(D)_\infty = \sum_{n_P < 0} -n_P P$, such that $D = (D)_0 - (D)_\infty$.

We can define a partial order on $\mathrm{Div}(Y)$ by $\sum_P n_P P \geq \sum_P n'_P P \Leftrightarrow \forall P \in Y : n_P - n'_P \geq 0$.

Thanks to the Lemma 3.38 one has a morphism of abelian groups:

$$(\cdot) : K(Y)^\times \to \mathrm{Div}(Y)$$
$$f \mapsto \sum_P \nu_P(f)P$$

The points for which $\nu_P(f) > 0$ are called zeros (of order $\nu_P(f)$) of f and the points for which $\nu_P(f) < 0$ are called poles (of order $-\nu_P(f)$) of f. Divisors, which are in the image of $(\cdot)$, are called principal divisors.
There is also a natural map $\deg : \mathrm{Div}(Y) \to \mathbb{Z}$, which maps $\sum_P n_P P$ to $\sum_P n_P$.

If the curve Y over an algebraically closed field K of characteristic 0 is singular, one can still define a divisor properly just by taking the valuations (points) of a non-singular model of Y.

Proposition 3.40. *The Galois group* $\mathrm{Gal}(K/k)$ *acts on* $\mathrm{Div}(Y)$ *with the action* $\sigma(\sum_P n_P P) = \sum_P n_P \sigma(P)$ *for* $\sigma \in \mathrm{Gal}(K/k)$.

Proof. If P is a point on Y, then $\sigma(P)$ is a point on Y, because all the points are given by zeros of polynomials with coefficients in k, and it is clearly an action. □

Definition 3.41. A divisor is defined over k iff it is invariant under the action of $\mathrm{Gal}(K/k)$.

Proposition 3.42. *Every* $\sigma \in \mathrm{Gal}(K/k)$ *induces an isomorphism of local rings* $\sigma : \mathcal{O}_P^K \xrightarrow{\sim} \mathcal{O}_{\sigma(P)}^K$ *and one has* $\nu_P(f) = \nu_{\sigma(P)}(f^\sigma)$.

Proof. If $U = Y \backslash V(f_1, \ldots, f_l)$ is an open neighborhood of P and $f = g/h$ is a regular function on U (by making U smaller if necessary), then $f^\sigma = g^\sigma/h^\sigma$ is regular on $U^\sigma = V(f_1^\sigma, \ldots, f_l^\sigma)^c$ an open neighborhood of $\sigma(P)$, where we denote by g^σ the image of g under the induced morphism $\sigma : K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]$, moreover $\sigma(I(Y)) = I(Y)$, because one can find generators of the ideal in $k[X_1, \ldots, X_n]$, so equivalence classes are preserved. Thus σ induces a morphism $\mathcal{O}_P^K \to \mathcal{O}_{\sigma(P)}^K$ the inverse of which is clearly given by the induced morphism of σ^{-1}. Let t be a local parameter at P and t' a local parameter at $\sigma(P)$, then $\nu_{\sigma(P)}(t^\sigma) = e, \nu_P(t^{\sigma^{-1}}) = e' > 0$. Now $t = (t^\sigma)^{\sigma^{-1}} = u^{\sigma^{-1}}(t'^{\sigma^{-1}})^e = u^{\sigma^{-1}} u'^{e'} t^{ee'}$ for some unit u in $\mathcal{O}_{\sigma(P)}^K$ and a unit u' in $\mathcal{O}_P^K$, further $u^{\sigma^{-1}}$ is also a unit in $\mathcal{O}_P^K$, so we have $1 = ee'$ by taking ν_P, thus $e = e' = 1$ and t^σ is also a local parameter in $\mathcal{O}_{\sigma(P)}^K$. □

Corollary 3.43.

$$\sigma((f)) = \sigma\left(\sum_P \nu_P(f)P\right) = \sum_P \nu_P(f)\sigma(P) = \sum_P \nu_{\sigma^{-1}(P)}(f)P = \sum_P \nu_P(f^\sigma)P = (f^\sigma)$$

.

Note that the restriction of σ to $k(Y)$ is the identity map, hence for $f \in k(Y)$ the divisor (f) is defined over k.

If P is an algebraic point over k we can define $k(P)$ to be the minimal field containing k and P, in the affine case one gets that field just by adjoining the coordinates and in the projective case one first needs to normalize a coordinate to 1 and can then adjoin the coordinates. One can now look at the size of the orbit of P, which is exactly $[k(P) : k]_s$.

Now we consider a field k of characteristic 0 and $K = \overline{k}$ an algebraic closure. Let P be a point of a non-singular curve $\mathcal{C}$ defined over k. L an algebraic extension of k, then $\nu_P(L(\mathcal{C})) = s\mathbb{Z}$ for some $s \in \mathbb{N}_0$. Clearly $s \in \mathbb{N}$, as there is a regular function with coefficients in k, which vanishes on P (P is algebraic over k). So $\frac{1}{s}\nu_P|_{L(\mathcal{C})}$ is a discrete valuation of $L(\mathcal{C})$.

Lemma 3.44. *Assume the assumptions of above. Let P, P' be points on $\mathcal{C}$. Then $\frac{1}{s}\nu_P|_{L(\mathcal{C})} = \frac{1}{s'}\nu_{P'}|_{L(\mathcal{C})}$ iff P and P' are conjugate over L.*

Proof. If they are conjugate over L, then clearly they define the same discrete valuation, because of Proposition 3.42. Now suppose they are equal and reduce to an affine neighborhood of P and P'. Let $P = (a_1, \ldots, a_n), P' = (a'_1, \ldots, a'_n)$ and $Q \in L[X_1, \ldots, X_n]$ a polynomial of degree 1 such that $Q(P)$ is a primitive element of $L(P)/L$ and $Q(P')$ a primitive element of $L(P')/L$. Let f be the minimal polynomial of $Q(P)$ over L, then $(f \circ Q)(P) = 0$ and thus $(f \circ Q)(P') = 0$, which means $Q(P)$ and $Q(P')$ are conjugate. Now let f_i be a polynomial such that $f_i(Q(P)) = a_i$, then $(f_i \circ Q - X_i)(P) = 0$ and thus $(f_i \circ Q - X_i)(P') = 0$. So if $Q(P') = \sigma(Q(P))$, then $a'_i = \sigma(a_i)$ therefore P and P' are conjugate over L. □

Proposition 3.45. *There is a regular function $f \in k(\mathcal{C})$ such that $\nu_P(f) = 1$.*

Proof. Let L be the minimal field containing P. With the use of Proposition 2.11 and Lemma 3.44, there is a $g \in L(\mathcal{C})$ such that $\nu_P(g) = 1$ and $\nu_{\sigma(P)}(g) = 0$ for $\sigma(P) \neq P$. Let f be the product of the conjugates g^σ of g, now since L is minimal, it follows that $\sigma(P) \neq P \Rightarrow g^\sigma \neq g$. Also since k is perfect, $f \in k(\mathcal{C})$ and because of proposition 3.42 it follows $\nu_P(f) = 1$. □

Proposition 3.46. *Let $f \in k(\mathcal{C})\backslash k$ and $P_1, \ldots, P_r \in \mathcal{C}$ be zeros of f such that their discrete valuations do not agree on $k(\mathcal{C})$, then:*

$$\sum_{i=1}^{r} \nu_{P_i}(f) n(P_i) \leq [k(\mathcal{C}) : k(f)],$$

where $n(P_i) = [k_{P_i} : k]$ and k_{P_i} the residue field of $\nu_{P_i}|_{k(\mathcal{C})}$.

Proof. See page 30/45 of [I93] or page 13 of [S08]. □

Corollary 3.47. *Let $f \in k(\mathcal{C})\backslash k$, then:*

$$\deg(f)_0, \deg(f)_\infty \leq [k(\mathcal{C}) : k(f)].$$

Proof. A point P has $[k(P) : k]$ conjugates over k, where $k(P)$ is the minimal field containing P. Also the ring inclusions $\mathcal{O}_P^k \subseteq \mathcal{O}_P^{k(P)} \cap k(\mathcal{C}) \subseteq \mathcal{O}_P^{k(P)}$ factored at their maximal ideal gives $k(P) \subseteq k_P \subseteq k(P)$. Thus the residue field is $k(P)$ and the result follows for $\deg(f)_0$ by Proposition 3.42 and the previous Proposition. Also $\deg(f)_\infty = \deg(\frac{1}{f})_0$ and $k(f) = k(\frac{1}{f})$. So it follows also for $\deg(f)_\infty$. □

Definition 3.48. Given a curve Y over an algebraically closed field K of characteristic 0 and a divisor D one can define a K-vector space $L(D) = \{f \in K(Y)^\times | (f) + D \geq 0\} \cup \{0\}$. Denote by $l(D) = \dim_K(L(D))$ its dimension.

Theorem 3.49 (Riemann's Inequality)**.** *There is a constant g such that $l(D) \geq \deg(D) + 1 - g$ for all divisors D. The smallest such constant is called the genus of $K(Y)$.*

Proof. See page 196 of Fulton, Algebraic Curves [F69]. □

4 Runge's Theorem and Applications

In this section we consider the field extension $\overline{\mathbb{Q}}/\mathbb{Q}$, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

Theorem 4.1. *Let $\mathcal{C}$ be an absolutely irreducible non-singular projective curve defined over $\mathbb{Q}$, and $f \in \mathbb{Q}(\mathcal{C})$ have a pole Q' such that $-\nu_{Q'}(f)[\mathbb{Q}(Q') : \mathbb{Q}] < \deg(f)_\infty$. Then there are only finitely many rational points $P \in \mathcal{C}(\mathbb{Q})$ such that $f(P) \in \mathbb{Z}$.*

Since f is in $\mathbb{Q}(\mathcal{C})$, we have that (f) and a fortiori $(f)_\infty$ is defined over $\mathbb{Q}$ and thus $(f)_\infty$ is of the form $\sum_Q -\nu_Q(f)\sum_{\sigma\in\Sigma_Q}\sigma(Q)$, where Q runs over a system of representatives of poles of the disjoint orbits under the action of the Galois group and Σ_Q is a minimal set such that the set $\{\sigma(Q)|\sigma \in \Sigma_Q\}$ is exactly the orbit of Q. Then Σ_Q has the size $[\mathbb{Q}(Q) : \mathbb{Q}]$. So the condition "There is a pole Q' of (f) such that $-\nu_{Q'}(f)[\mathbb{Q}(Q') : \mathbb{Q}] < \deg(f)_\infty$" is equivalent to "The pole divisor of (f) splits into two positive divisors with disjoint support defined over $\mathbb{Q}$" moreover it is equivalent to "$f \notin \mathbb{Q}$ and every pole Q of (f) satisfies $-\nu_Q(f)[\mathbb{Q}(Q) : \mathbb{Q}] < \deg(f)_\infty$" and one has the following equivalent version:

Theorem 4.2. *Let $\mathcal{C}$ be an absolutely irreducible non-singular projective curve defined over $\mathbb{Q}$, and $f \in \mathbb{Q}(\mathcal{C})\backslash\mathbb{Q}$ be such that the pole divisor splits into two positive divisors with disjoint support defined over $\mathbb{Q}$. Then there are only finitely many rational points $P \in \mathcal{C}(\mathbb{Q})$ such that $f(P) \in \mathbb{Z}$.*

Proof. Let $R \in \overline{\mathbb{Q}}$ be a pole of f, $k = \mathbb{Q}(R)$ be the minimal field containing R and $u \in \mathcal{O}_R^k$ be a local parameter. Let g be a primitive element of $\mathbb{Q}(\mathcal{C})/\mathbb{Q}(f)$, which we can assume to be integral over $\mathbb{Z}[f]$ (Subring of $\mathbb{Q}(f)$ generated by $\mathbb{Z}$ and f). Now denote by n, m the order at R of f, g respectively and $d = [\mathbb{Q}(\mathcal{C}) : \mathbb{Q}(f)]$. By Proposition 2.13 we can develop f, g into Laurent series $\sum_{i\geq n}\lambda_i u^i, \sum_{i\geq m}\mu_i u^i \in k((u))$. We consider all rational functions of the form:

$$F(f, g) = A_0(f) + A_1(f)g + \cdots + A_{d-1}(f)g^{d-1},$$

where all A_i are polynomials in $\mathbb{Q}[X]$ of degree smaller than some constant M. They form a vector space of dimension dM. We now like to impose that $F(f, g)$ is in $\mathcal{O}_R^k$ and moreover $F(f, g)(R) = 0$, this corresponds to $\max\{nM, nM + (d-1)m\}$ linear equations over k or $\max\{nM, nM + (d-1)m\}[k : \mathbb{Q}]$ equations over $\mathbb{Q}$. Since $n[k : \mathbb{Q}] < \deg(f)_\infty \leq d$ holds, for a sufficiently large M $\max\{nM, nM + (d-1)m\}[k : \mathbb{Q}] < dM$ holds and thus there exists a non-trivial solution $G'(X, Y)$, which we then can multiply by some non-zero integer q, such that $G(X, Y) = qG'(X, Y) \in \mathbb{Z}[X, Y]$; put $H_R = G(f, g)$. Consider a point $P \in \mathcal{C}(\mathbb{Q})$ such that $f(P) \in \mathbb{Z}$, then $g(P)$ is integral over $\mathbb{Z}$ and in $\mathbb{Q}$, hence $g(P) \in \mathbb{Z}$. Thus $H_R(P) \in \mathbb{Z}$. H_R is regular at P and thus defines a continuous function on a neighborhood of R in $\mathbb{P}^n(\mathbb{R})$ (standard topology), which means we can find an open neighborhood U_R of R such that $|H_R(Q)| < 1$ for all $Q \in U_R$.
Now complement of the union of the U_R over all poles intersected with the real points of the curve $\mathcal{C}(\mathbb{R})$ is a closed, thus compact, subset of $\mathcal{C}(\mathbb{R})$ on which f is continuous and thus bounded by some constant say B. Now let $P \in \mathcal{C}(\mathbb{Q})$ be a point such that $f(P) \in \mathbb{Z}$, if $P \in U_R$ for some pole R, then $H'_R(P) = 0$, which has only finitely many solutions. If not

then $\mathbb{Z} \ni |f(P)| < B$, each of which has only finitely many solutions. Hence the result follows. □

Note that the proof of the theorem is dependent on the field of definition of the positive divisors, in which $(f)_\infty$ can split, which indicates that the theorem is not geometrical.

Proposition 4.3. *Let $f \in \mathbb{Z}[X,Y]$ be an irreducible polynomial such that its highest homogeneous part is not a constant times a power of an irreducible polynomial over $\mathbb{Q}$, then the equation $f(X,Y) = 0$ has only finitely many solutions in $\mathbb{Z}^2$.*

Proof. First consider the case f is not absolutely irreducible, i.e. f factors in $\overline{\mathbb{Q}}[X,Y]$. Then it already completely factors in some finite extension k of $\mathbb{Q}$. Take a basis $(a_i)_{i=1,\dots,n}$ of $k/\mathbb{Q}$ and an absolutely irreducible factor g and write $g = \sum a_i g_i$ with $g_i \in \mathbb{Q}[X,Y]$. Now an integral zero (x,y) must satisfy $g_i(x,y) = 0$ for all i. This can happen only finitely many times, because the greatest common divisor of the g_i's over $\mathbb{Q}[X,Y]$ is 1 (else f would not be irreducible), so the greatest common divisor over $\overline{\mathbb{Q}}[X,Y]$ must also be 1. This then further implies, that $V(g_1,\dots,g_n)$ cannot have an irreducible component of dimension ≥ 1, suppose it has then $V(g_1,\dots,g_n) \supseteq V(\mathfrak{p}) \Rightarrow (g_1,\dots,g_n) \subseteq r(g_1,\dots,g_n) \subseteq \mathfrak{p}$, for some prime $\mathfrak{p}$ of height ≤ 1. If the height were 0, then $\mathfrak{p} = (0)$ a contradiction, else take an arbitrary element of $\mathfrak{p}$ and factor it in absolutely irreducible factors, then at least one of them, say h, needs to be in $\mathfrak{p}$, then $(0) \subsetneq (h) \subseteq \mathfrak{p}$ is a chain of primes and thus $(h) = \mathfrak{p}$ and $h|g_i$ for all i a contradiction. This now implies that $V(g_1,\dots,g_n)$ contains at most finitely many points.
If f is absolutely irreducible, then the homogenization $f^h(X,Y,Z) = Z^{\deg(f)} f(X/Z, Y/Z)$ gives rise to an absolutely irreducible projective curve $\mathcal{C}$ defined over $\mathbb{Q}$. The highest degree of f factors as $c\prod_{i=1}^r f_i(X,Y)^{e_i}$ where $c \in \mathbb{Q}^\times$, $r, e_i \in \mathbb{N}$, $r > 1$, $f_i(X,Y) \in \mathbb{Z}[X,Y]$ primitive, irreducible and pairwise relatively prime in $\mathbb{Q}[X,Y]$. Now f_i factors as $c_i \prod_{j=1}^{s_i}(k_{ij}X - k'_{ij}Y)$ in $\overline{\mathbb{Q}}[X,Y]$ with not both k_{ij}, k'_{ij} zero for any i,j and $k_{ij}k'_{mn} - k'_{ij}k_{mn} \neq 0$ for $(i,j) \neq (m,n)$. There is an integer k, such that $X - kY \nmid f_i(X,Y)$ (one of $\{0,1,\dots,r\}$ will work). Let $h = (X - kY)/Z \in \mathbb{Q}(\mathcal{C})$. Now the points $(x,y) \in \mathbb{Z}^2$ we are interested in correspond to the points $(x : y : 1)$ and satisfy $h(x : y : 1) \in \mathbb{Z}$. Let $l : \mathcal{X} \to \mathcal{C}$ be a non-singular model. We can look at the poles of h in $\mathcal{X}$. All poles Q must satisfy $Z(l(Q)) = 0$, so $l(Q) = (k'_{ij} : k_{ij} : 0)$ for some i,j. If $l(Q) = (k'_{ij} : k_{ij} : 0)$, then $(X - kY)(l(Q)) \neq 0$ thus the poles are exactly $l^{-1}(\{(k'_{ij} : k_{ij} : 0) | i \in \{1,\dots,r\}, j \in \{1,\dots,s_i\}\})$. Define the divisors

$$D_i = \sum_{\substack{Q \in \mathcal{X} \\ l(Q) \in \{(k'_{mn} : k_{mn} : 0) | m \neq i\}}} -Q.$$

It's clear that $0 > \deg(D_i)$. So by Riemann's inequality we can find a $F_i \in \overline{\mathbb{Q}}(\mathcal{C}) \backslash \overline{\mathbb{Q}}$, such that $(F_i) \geq ND_i$ for some sufficiently large integer N. Consider the conjugate functions F_i^σ, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Similarly to Proposition 3.42 every automorphism of $\overline{\mathbb{Q}}(\mathcal{C})$ gives an automorphism of $\mathcal{X}$ such that the valuations commute with the automorphism: $\nu_Q^\sigma(g) = \nu_Q(g^{\sigma^{-1}})$ is a valuation on $\overline{\mathbb{Q}}(\mathcal{C})$ and so equal to $e\nu_P$ for some $e \in \mathbb{N}$ and a point $P \in \mathcal{X}$ and

thus define $\sigma(Q) = P$ and it follows again that $e = 1$ and $\nu_Q(g) = \nu_{\sigma(Q)}(g^\sigma)$. One can also check that this is an automorphism of $\mathcal{X}$, but that is not needed here. Moreover one has:

$$l(Q) = P \Leftrightarrow \mathcal{O}^{\overline{\mathbb{Q}}}_{Q,\mathcal{X}} \text{ dominates } \mathcal{O}^{\overline{\mathbb{Q}}}_{P,\mathcal{C}} \Leftrightarrow \mathcal{O}^{\overline{\mathbb{Q}}}_{\sigma(Q),\mathcal{X}} \text{ dominates } \mathcal{O}^{\overline{\mathbb{Q}}}_{\sigma(P),\mathcal{C}} \Leftrightarrow l(\sigma(Q)) = \sigma(P).$$

Thus we conclude that $l \circ \sigma = \sigma \circ l$ and further that $(F_i^\sigma) \geq ND_i$, because $l(\mathrm{Supp}(D_i)) = \sigma(l(\mathrm{Supp}(D_i)))$. There are only finitely many conjugates of F_i because all the coefficients of F_i are already in some finite field extension of $\mathbb{Q}$. Then all of the elementary symmetric polynomials e_i^j of the conjugates of F_i satisfy $(e_i^j) \geq N'D_i$ for some maybe larger positive integer N' and they are in $\mathbb{Q}(\mathcal{C})$. Not all can be in $\mathbb{Q}$ or else F_i would be algebraic over $\mathbb{Q}$, which is not possible by definition. Denote by e_i one which is not in $\mathbb{Q}$. All valuations of $\overline{\mathbb{Q}}(h)$ are induced by the valuations of $\overline{\mathbb{Q}}(\mathcal{C})$, which correspond to the points of $\mathcal{X}$. Consider the valuation $\nu_P, P \notin \mathrm{Supp}((h)_\infty)$, then ν_P is not extending the valuation ν_∞ of $\mathbb{Q}(h)$, because $\nu_P(h) \geq 0$ and $\nu_\infty(h) = -1$, and $\nu_P(e_i) \geq 0$. Also the valuations corresponding to the points of $\mathrm{Supp}((h)_\infty)$ are extending the valuation ν_∞. Since $\overline{\mathbb{Q}}(\mathcal{C})/\overline{\mathbb{Q}}(h)$ is a finite extension, it follows that the minimal polynomial of e_i has coefficients in $\overline{\mathbb{Q}}[h]$ (see page 27 of [I93]). Moreover since $\mathcal{C}$ is defined over $\mathbb{Q}$ one can look at the minimal polynomial with a basis of $\overline{\mathbb{Q}}/\mathbb{Q}$ including 1 and take the part with basis element 1, this is an equation, which shows that e_i is integral over $\mathbb{Q}[h]$. Replacing e_i by a non-zero multiple, we can assume that e_i is integral over $\mathbb{Z}[h]$. For every pole $Q \in \mathcal{X}$ of h there is an i such that e_i is regular on Q. So take an open neighborhood U_Q in $\mathcal{X}(\mathbb{C})$ (topology induced by the standard topology of $\mathbb{P}^n(\mathbb{C})$) of Q such that $|e_i(Q) - e_i(Q')| < \frac{1}{2}\ \forall Q' \in U_Q$ and e_i is regular on $l(U_Q)$ except for maybe $l(Q)$. On the complement of the union of the sets $(U_Q)_{Q \text{ pole of } h}$ h is bounded. Let $R = (x : y : 1)$ be a point in $\mathcal{C}$ with $x, y \in \mathbb{Z}$. If $R \in l(U_Q)$ for some Q, then $e_i(S) = e_i(R) \in \mathbb{Z}$ for any point S such that $l(S) = R$, this has only finitely many solutions, else $h(S) = h(R)$ is bounded, which has also only finitely many solutions. □

If one can get a grip at these functions around the poles, one can actually get a bound on the absolute value of the zeros. This has been done with the use of Puiseux series in a paper of Hilliker and Straus [HS83].

The theorem can be used for equations of the form $Y^d = X^d + c$ for $d \geq 2$ and $c \neq 0$, but not $X^3 - 2Y^3 = 1$. So how does it compare to Thue's theorem? Regarding equations of the form $f(X, Y) = c$, where f is homogenous, Thue's theorem needs an irreducible factor of $f(X, Y)$ of degree ≥ 3, whereas Runge's theorem needs $f(X, Y) - c$ to irreducible and $f(X, Y)$ to factor into two non-constant relatively prime polynomials or $f(X, Y)$ needs a factor $g(X, Y)$ such that $g(X, Y)$ factors into two non-constant relatively prime polynomials and $g(X, Y) - k$ must be irreducible for any divisor k of c. So the conditions are fairly different even though close. Also one may not disregard the advantage of Runge's theorem of being effective.

Example. All integer solutions to $X(X-1)(X-2)(3X-4) = Y(Y-1)(Y-2)(3Y-1)$ are exactly those with $X, Y \in \{0, 1, 2\}$.

Proof. First we make the substitution $X-1 \to X$ and $Y-1 \to Y$, in order to keep the coefficients small, so we must find the integer solutions to $F(X,Y) = X(X-1)(X+1)(3X-1) - Y(Y-1)(Y+1)(3Y+2) = 0$. The polynomial of highest degree of $F(X,Y)$ is $3(X^4-Y^4) = 3(X-Y)(X+Y)(X^2+Y^2) = 3(X-Y)(X+Y)(X+iY)(X-iY)$. The question arises whether $F(X,Y)$ is reducible, irreducible over $\mathbb{Q}$ or absolutely irreducible. Suppose either $(X-P(Y))$ or $(Y-P(X))$ is a factor, then clearly $\deg(P)=1$, so suppose $(X-aY-b)$ is a factor, by plugging $aY+b$ in for X and comparing the polynomial of highest degree one finds $a \in \{-1,1,i,-i\}$. If one sets $Y=-1,0,1,-\frac{2}{3}$ one finds:

$$\begin{aligned}
0 &= (-a+b)(-a+b-1)(-a+b+1)(-3a+3b-1),\\
0 &= b(b-1)(b+1)(3b-1),\\
0 &= (a+b)(a+b-1)(a+b+1)(3a+3b-1),\\
0 &= (-\frac{2}{3}a+b)(-\frac{2}{3}a+b-1)(-\frac{2}{3}a+b+1)(-2a+3b-1).
\end{aligned}$$

So $b \in \{-1,0,1,\frac{1}{3}\}$, if $b=-1,0$ then the last equation cannot be satisfied. If $b=1$, then the last equation implies $a=1$, so the third equation is not satisfied. If $b=\frac{1}{3}$, then the first equation cannot be satisfied. So one is left with the case $F(X,Y)$ is the product of two absolutely irreducible factors of degree 2. Again by comparing the polynomial of highest degree one finds, that the polynomial of highest degree of the factors must be one of the pairs $(X^2-Y^2, X^2+Y^2), (X^2+(-1+i)XY-iY^2, X^2+(1-i)XY-iY^2), (X^2+(1+i)XY+iY^2, X^2+(-1-i)XY+iY^2)$. In the latter cases the factors would have to be conjugate, which they are not. Consider the first case:

$$F(X,Y) = (X^2-Y^2+aX+bY+c)(3X^2+3Y^2+dX+eY+f).$$

Looking at the coefficient of X^3 and XY^2, one finds $3a+d=-1$ and $3a-d=0$, so $a=-\frac{1}{6}, d=-\frac{1}{2}$. Further by looking at the coefficient of X^2 and X one finds $ad+3c+f=-3$ and $af+cd=1$, so $3c+f=-3-\frac{1}{12}$ and $3c+f=-6$ a contradiction. So $F(X,Y)$ is absolutely irreducible.

We can define an absolutely irreducible projective curve defined over $\mathbb{Q}$ by the equation $F^h(X,Y,Z) = Z^4F(X/Z,Y/Z)$. We choose the function $h=X/Z$. Now the only interesting poles are those in $\mathbb{R}$, so define:

$$\begin{aligned}
f_1 &= \frac{X-Y}{Z} = \frac{X^3+2Y^3+3X^2Z-3Y^2Z-XZ^2-2YZ^2}{3(X+Y)(X^2+Y^2)},\\
f_2 &= \frac{X+Y}{Z} = \frac{X^3+2Y^3+3X^2Z-3Y^2Z-XZ^2-2YZ^2}{3(X-Y)(X^2+Y^2)}.
\end{aligned}$$

These are the desired functions at the poles $(1:1:0)$ and $(1:-1:0)$. It remains to find positive integers n_1, n_2 such that n_1f_1, n_2f_2 are integral over $\mathbb{Z}[h]$. We have $F(X/Z,Y/Z)=0$ and of course $h=X/Z$ and $Y/Z = h-f_1 = f_2-h$. Thus we find:

$$\begin{aligned}
0 &= 3f_1^4 - 2(6h+1)f_1^3 + 3(6h^2+2h-1)f_1^2 - 2(6h^3+3h^2-3h-1)f_1 + 3h(h^2-1),\\
0 &= 3f_2^4 - 2(6h-1)f_2^3 + 3(6h^2-2h-1)f_2^2 - 2(6h^3-3h^2-3h+1)f_2 - h(h^2-1).
\end{aligned}$$

Thus we can choose $n_1 = n_2 = 3$ (even though in this example $n_1 = n_2 = 1$ is sufficient for the points of interest). Now $3f_1(1:1:0) = \frac{3}{4}$ and $3f_2(1:-1:0) = -\frac{1}{4}$. Lets consider the pole $(1:1:0)$ first:

$$G_1(W,Z) = 12f_1(1:W+1:Z) - 3 = \frac{5W^3 + 12(1-Z)W^2 + 2(3-12Z-4Z^2)W - 12Z^2}{(2+W)(2+2W+W^2)}.$$

So for $|W| < \frac{1}{2}$ we have:

$$|G_1(W,Z)| \leq \frac{5|W|^3 + 12(1+|Z|)|W|^2 + 2(3+12|Z|+4|Z|^2)|W| + 12|Z|^2}{(2-|W|)(2-2|W|-|W|^2)},$$

which is increasing in $|W|, |Z|$ and the value at $|W| = |Z| = \frac{3}{7}$ is smaller than 9. So the first neighborhood $U_1 = \{(1:Y:Z) \in \mathcal{C}(\mathbb{R})|\ |Y-1| < \frac{3}{7}, |Z| < \frac{3}{7}\}$ is found: If (x,y) is an integral solution, then $(x:y:1) \in U_1$ implies $3(x-y) \in \{-1,0,1,2\}$, so $x = y$ and further $x = y \in \{-1,0,1\}$. Similarly for the pole $(1:-1:0)$:

$$G_2(W,Z) = 12f_2(1:W-1:Z) + 1 = \frac{7W^3 - 4(5+3Z)W^2 + 2(9+12Z-4Z^2)W + 4Z^2}{(2-W)(2-2W+W^2)}.$$

For $|W| < \frac{1}{2}$ one has again:

$$|G_2(W,Z)| \leq \frac{7|W|^3 + 4(5+3|Z|)|W|^2 + 2(9+12|Z|+4|Z|^2)|W| + 4|Z|^2}{(2-|W|)(2-2|W|-|W|^2)},$$

which is increasing in $|W|, |Z|$ and the value at $|W| = |Z| = \frac{2}{5}$ is smaller than 10. This defines then the second neighborhood $U_2 = \{(1:Y:Z) \in \mathcal{C}(\mathbb{Q})|\ |Y-1| < \frac{2}{5}, |Z| < \frac{2}{5}\}$: If (x,y) is an integral solution then $(x:y:1) \in U_1$ implies $3(x+y) \in \{-2,-1,0,1,2\}$, so $x = -y$ and further $x = -y \in \{-1,0,1\}$. Now $\mathcal{C}(\mathbb{R})\backslash(U_1 \cup U_2)$ is already closed thus compact set on which h is continuous, because it does not contain its poles (that's why the only interesting poles are those in $\mathbb{R}$). Suppose one has a point $(x:y:1)$ not in U_1 nor in U_2, then either $x = 0$ or $|1/x| \geq \frac{2}{5}$ or $|(y-x)/x| \geq \frac{2}{5}$ and $|(y+x)/x| \geq \frac{3}{7}$. We deal with the last case first, put $w = y/x$ and $|x| \geq 1$, by manipulating the equation one gets:

$$|x| = \frac{\left|1 + 2w^3 + \frac{1}{x}(3-3w^2) - \frac{1}{x^2}(1+2w)\right|}{3|w^4-1|} \leq \frac{5 + 2|w| + 3|w|^2 + 2|w|^3}{3|w^4-1|}.$$

Now if $w \geq 1$, then $w \geq \frac{7}{5}$, if $w \leq -1$ then $w \leq -\frac{10}{7}$. So if $|w| \geq 1$ then $|w| \geq \frac{7}{5}$ and therefore:

$$|x| \leq \frac{5 + 2|w| + 3|w|^2 + 2|w|^3}{3(w^4-1)} \leq \frac{5 + 7w^4}{3(w^4-1)} = \frac{7}{3} + \frac{4}{w^4-1} < 4.$$

If $w < 1$, then $w \leq \frac{3}{5}$, if $w > -1$ then $w \geq -\frac{4}{7}$. So if $|w| < 1$, then $|w| \leq \frac{3}{5}$ and therefore:

$$|x| \leq \frac{5 + 2|w| + 3|w|^2 + 2|w|^3}{3(1-w^4)} < 3.$$

So it remains to check, when $-3 \leq x \leq 3$. Which is done by brute force: y must be a divisor of $x(x-1)(x+1)(3x-1)$ and if $x \in \{-1,0,1\}$ then it is trivial. We conclude that all the integral solutions are exactly those with $x, y \in \{-1,0,1\}$. □

One can easily, but with some work, extend the above demonstration of Runge's method to bound the integer solutions, if the highest degree has only zeros in $\mathbb{Q}$ of multiplicity 1 or in $\mathbb{C}\backslash\mathbb{R}$. The next proposition is certainly related to that case, but another method for finding the functions around the poles is used.

Proposition 4.4. *Let $f \in \mathbb{Q}[X]$ be a polynomial of degree b and leading coefficient l. Suppose f is not a perfect power and a, q are positive integers such that $q|\gcd(a,b)$ and $q > 1$ and l is a q-th power. Then the equation $Y^a = f(X)$ has only finitely many integral solutions $(x,y) \in \mathbb{Z}^2$ and their absolute values are bounded by some effective computable constant.*

Proof. By putting $Z = Y^{\frac{a}{q}}$ it suffices to look at the case $1 < a = q|b$ (since only more solutions may occur).Let $b = dq$, $f(X) = \sum_{i=0}^{dq} a_i X^{qd-i}$ with $a_0 = c^q$, without loss of generality $c = \frac{p}{s}$ with $p, s \in \mathbb{N}$ and $\gcd(p,s) = 1$ (if $2|q$ just replace c by $-c$ and if $2 \nmid q$ multiply the equation by -1), D a common denominator of the coefficients of f and $h = \max\{a_i | i = 0, \ldots, qd\}$. By Taylor's theorem:

$$(1+x)^\alpha = \sum_{i=0}^{n} \binom{\alpha}{i} x^i + r_n(x)$$

with Cauchy's error estimate

$$r_n(x) = (n+1)\binom{\alpha}{n+1}(1+\xi)^{\alpha-n-1}(x-\xi)^n x$$

for some ξ between 0 and x. For $|x| < 1$ we have

$$\left|\frac{x-\xi}{1+\xi}\right| \leq \frac{|x|-|\xi|}{1-|\xi|} = 1 - \frac{1-|x|}{1-|\xi|} \leq 1 - (1-|x|) = |x|$$

and so

$$|r_n(x)| \leq \left|\alpha\left(1-\frac{\alpha}{1}\right)\cdot\cdots\cdot\left(1-\frac{\alpha}{n}\right)\right|(1+\xi)^{\alpha-1}|x|^{n+1}. \tag{1}$$

Going back to the original equation, if $X \neq 0$ we have:

$$\begin{aligned} Y &= cX^d\left(1+\sum_{i=1}^{dq}\frac{f_i}{c^q}X^{-i}\right)^{\frac{1}{q}} = cX^d\sum_{i=0}^{d}\binom{\frac{1}{q}}{i}\left(\sum_{j=1}^{dq}\frac{f_i}{c^q}X^{-j}\right)^i + cX^d r_d \\ &= \underbrace{cX^d + \sum_{i=1}^{d} b_i X^{d-i}}_{g(X)} + \underbrace{\sum_{i=d+1}^{d^2q} b_i X^{d-i}}_{h(X)} + \underbrace{cX^d r_d}_{h'(X)} \end{aligned}$$

with

$$\begin{aligned} |b_m| &\leq c\sum_{i=1}^{d}\left(\left|\binom{\frac{1}{q}}{i}\right|\sum_{\substack{k_1,\ldots,k_i\in\{1,\ldots,dq\}\\ k_1+k_2+\cdots+k_i=m}}\prod_{n=1}^{i}\left|\frac{f_{k_i}}{c^q}\right|\right) \\ &\leq c\sum_{i=1}^{d}\left(1\cdot(dq)^i\cdot\left(\frac{h}{c^q}\right)^i\right) \\ &\leq 2c\left(\frac{dqh}{c^q}\right)^d. \end{aligned} \tag{2}$$

Now for $x, y \in \mathbb{Z}$ we have that $g(X) \in (p^{qd}D^d)^{-1}\mathbb{Z}[X]$ and so if $|h(x)+h'(x)| < (p^{qd}D^d)^{-1}$, we must have $y = g(x)$. For $|x| \geq 1$ we have by (2):

$$|h(x)| \leq 2cd(dq-1)\left(\frac{dqh}{c^q}\right)^d |x|^{-1}. \tag{3}$$

For $|x| > \max\left\{1, \frac{dqh}{c^q}\right\}$ we have:

$$\left|\sum_{i=1}^{dq}\frac{f_i}{c^q}x^{-i}\right| \leq \sum_{i=1}^{dq}\left|\frac{f_i}{c^q}\right|\cdot|x|^{-i} \leq \frac{dqh}{c^q}|x|^{-1} < 1.$$

So we can apply (1) to estimate $|h'(x)|$. For $|x| > \max\left\{1, \frac{2dqh}{c^q}\right\}$ we have

$$\begin{aligned} |h'(x)| &\leq c|x|^d\frac{1}{q}(1+\xi)^{\frac{1-q}{q}}\left|\sum_{i=1}^{dq}\frac{f_i}{c^q}x^{-i}\right|^{d+1} \\ &\leq \frac{2c}{q}\left(\frac{dqh}{c^q}\right)^{d+1}|x|^{-1}. \end{aligned} \tag{4}$$

Now (3) and (4) imply for $|x| > \max\left\{1, \frac{2dqh}{c^q}\right\}$:

$$|h(x)+h'(x)| \leq 2cd\left(\frac{dqh}{c^q}\right)^d(dq+h)|x|^{-1}.$$

That means for $|x| > 2cd\left(dqhD^{q+1}\right)^d(dq+h)$ we have $y = g(x)$. Now $g(X)^q \neq f(X)$, therefore we are now interested in the size of the roots of $t(X) = g(X)^q - f(X)$. First notice that $(p^qD)^{dq}t(X) \in \mathbb{Z}[X]$ and that the coefficients have absolute value of at most $(d+1)^q(2c)^q\left(dqh/c^q\right)^{dq} + h$. Now for a polynomial $\sum_{i=0}^{n}a_iX^i \in \mathbb{Z}[X]$ the absolute values of the roots are bounded by $\max\{|a_i|\}+1$, because for $|x| \geq \max\{|a_i|\}+1$ one has:

$$\left|\sum_{i=0}^{n}a_ix^i\right| \geq |a_n||x|^n - \sum_{i=0}^{n-1}|a_i||x|^i \geq \sum_{i=0}^{n-1}\left(\max\{|a_j|\}-|a_i|\right)|x|^i + 1 > 0.$$

Thus the absolute value of the roots of $t(X)$ are at most $(p^qD)^{dq}((d+1)^q(2c)^q\left(\frac{dqh}{c^q}\right)^{dq}+h)+1$. In conclusion the solutions $(x,y)\in\mathbb{Z}^2$ of $y^a=f(x)$ satisfy:

$$\begin{aligned}|x| &\leq \max\left\{2cd\left(dqhD^{q+1}\right)^d(dq+h),(2c(d+1))^q\left(dqhD^{q+1}\right)^{dq}+h(p^qD)^{dq}+1\right\}\\ &\leq (2c(d+1))^q\left(dqhD^{q+1}\right)^{dq}(dq+h)+h(p^qD)^{dq}+1.\end{aligned}$$

□

In the proof only f being not a perfect q-th power is required. Further note one gets a better bound by choosing q as small as possible.
This idea of using the Taylor expansion around infinity generalizes further into finding an algebraic closure of $\mathbb{C}((X^{-1}))$, which is given by the Puiseux series. This result is known as the Newton-Puiseux theorem.

Corollary 4.5. *Let $q\in\mathbb{N},q>1$, $f(X)\in\mathbb{Q}[X]$ be a non-constant polynomial not a perfect q-th power and $l\in\mathbb{Q}^+$. Then there are only finitely many $x\in\mathbb{Z}$ such that $f(x)$ and $f(x+l)$ are both q-th powers in $\mathbb{Q}$ and they can be effectively found.*

Proof. Let D be a common denominator of $f(X)$ and $f(X+l)$, then for every $x\in\mathbb{Z}$ such that $f(x)=r^q$ and $f(x+l)=s^q$, where $r,s\in\mathbb{Q}$, one has $\mathbb{Z}\ni D^qf(x)^{q-1}f(x+l)=(Dr^{q-1}s)^q$ and so $Dr^{q-1}s\in\mathbb{Z}$. Now $D^qf(X)^{q-1}f(X+l)$ has degree $q\deg(f)$ and leading coefficient $(Dc)^q$, where c is the leading coefficient of $f(X)$. It remains to prove, that $D^qf(X)^{q-1}f(X+l)$ is not a q-th power, because then we can apply the previous proposition. Let $f(X)=cQ(X)^qQ_1(X)^{k_1}\cdot\dots\cdot Q_m(X)^{k_m}$, where $Q_i\in\mathbb{Q}[X]$ are distinct monic irreducible polynomials of degree >0 and $0<k_i<q$ and $Q\in\mathbb{Q}[X]$ monic. Now suppose $D^qf(X)^{q-1}f(X+l)$ is a perfect q-th power. Then $G(X)=\left(Q_1(X)^{k_1}\cdot\dots\cdot Q_m(X)^{k_m}\right)^{q-1}Q_1(X+l)^{k_1}\cdot\dots\cdot Q_m(X+l)^{k_m}$ has to be a q-th power in $\mathbb{Q}[X]$. Now in order to have $q|\nu_{Q_i}(G)$ there must be a $j(i)$ such that $Q_{j(i)}(X+l)=Q_i(X)$ (and $k_{j(i)}=k_i$). Now there exists $u\neq v\in\mathbb{N}_0$ such that

$$\underbrace{j\circ\dots\circ j}_{u-\text{times}}(1)=\underbrace{j\circ\dots\circ j}_{v-\text{times}}(1)=h,$$

then $Q_h(X+(u-v)l)=Q_h(X)$.
For a polynomial $P(X)$ over a field of characteristic 0, $P(X)=P(X+a)$ for some $a\neq 0$ implies that $P(X)$ is constant, because $P(X)-P(0)$ has infinitely many distinct roots $x=0,a,2a,3a,\dots$.
This implies $m=0$. Now if there is a $x\in\mathbb{Z}$ such that $f(x)=r^q,r\in\mathbb{Q}^\times$, then c must be a q-th power in $\mathbb{Q}$ contradicting the assumption. If not, then the only solutions are the integral zeros of distance l. □

Given a polynomial $f(X)$, then there is not necessarily a bound on l, because there are arbitrary large Pythagorean triples: $[a(b^2-c^2)]^2=[a(b^2+c^2)]^2-[2abc]^2=[a(b-c)^2]\cdot[a(b-c)^2+4abc]$, which generate solutions for $f(X)=X$.

5 References

[AM94] Michael Francis Atiyah, Ian G. MacDonald, *Introduction To Commutative Algebra*, Westview Press 1994

[B06] Siegfried Bosch, *Algebra*, Springer Berlin Heidelberg 2006

[F69] William Fulton, *Algebraic Curves*, Benjamin/Cummings Publishing Company 1969

[G12] Steven D. Galbraith, *Mathematics of Public Key Cryptography*, Cambridge University Press 2012

[H77] Robin Hartshorne, *Algebraic Geometry*, Springer 1977

[HS83] David Lee Hilliker, E. G. Straus, *Determination of bounds for the solutions to those binary diophantine equations that satisfy the hypotheses of Runge's theorem*, Transactions of the american mathematical society Volume 280. Number 2. December 1983

[I93] Kenkichi Iwasawa, *Algebraic functions*, American Mathematical Society 1993

[M70] Hideyuki Matsumura, *Commutative Algebra*, Benjamin/Cummings Publishing Co. 1980

[S08] Henning Stichtenoth, *Algebraic Function Fields and Codes*, Springer 2008

[Z09] Umberto Zannier, *Lecture Notes on Diophantine Analysis*, Edizioni della Normale 2009