Sums of Squares in Algebraic Function Fields

David Grimm

Sums of Squares in Algebraic Function Fields

Dissertation

zur Erlangung des akademischen Grades
des Doktors der Naturwissenschaften
am Fachbereich Mathematik und Statistik
der Universität Konstanz

vorgelegt von

David Grimm

Tag der mündlichen Prüfung: 21. Juli 2011

Betreuer & Gutachter: PD Dr. Karim Johannes Becher (Universität Konstanz)
zweiter Gutachter: Prof. Dr. Claus Scheiderer (Universität Konstanz)

David Grimm
Egerstr. 14
78532 Tuttlingen
david.m.grimm@gmail.com

Gewidmet meinen Eltern
Rosi und Volker

Acknowledgements

I thank my colleagues...

- ... Karim J. Becher for giving me an interesting research question and for his support and advice;
- ... Julia Hartmann for an inspiring course on the topic covered in [**HH10**] and [**HHK09**];
- ... Kevin Hutchinson and his colleagues University College Dublin for their hospitality during a predoctoral research stay;
- ... David Leep for his encouragement and for inspiring discussions beyond the scope of this thesis;
- ... Claus Scheiderer for carefully reviewing my thesis and spotting non-neglectable mistakes before the final print;
- ... Jan Van Geel for his ideas and for being my go-to-guy for all geometry-related problems;
- ... Adrian Wadsworth for helping me find a more conceptual proof of a main result;
- ... Sophie Beke, Sabine Burgdorf, Christoph Hanselka, Daniel Plaumann, Rainer Sinn, James O'Shea and Sven Wagner for logistical support and/or mathematical discussions.

...my friends and family...

- ... Cristina Radu for being a supportive friend during my year abroad in Ireland;
- ... Eve and Simon for recharging my batteries with good food and diverting evenings; and for her loving and caring support...
- ... Luisa.

...and I acknowledge financial and logistical support by the...

- ... *Deutsche Forschungsgemeinschaft*: project (*Quadratic Forms and Invariants*, BE2614/3);
- ... *Science Foundation of Ireland Research Frontiers Programme* (Grant 05/RFP/MAT0022);
- ... *Zukunftskolleg der Universität Konstanz.*

Konstanz, September 2011 David Grimm

Table of Contents

CHAPTER 1

Introduction

The study of sums of squares in function fields lies at the cross roads of 'real algebraic geometry' and 'arithmetic of fields'. The content of this thesis falls in the second category.
In real algebraic geometry, one considers varieties over real closed fields, such as the real numbers $\mathbb{R}$, seeking to characterize the regular functions that take positive values when evaluated in any real point of the variety (or of some so-called semi-algebraic subset of the variety).
The initial problem that started off this research area was Hilbert's 17th problem, whether the real n-variate polynomials that are nonnegative on $\mathbb{A}^n(\mathbb{R}) = \mathbb{R}^n$ can be written as a sum of squares of polynomial fractions. Artin gave a positive answer to this problem. As a matter of fact, this characterization of sums of squares generalizes to rational functions on smooth integral varieties over $\mathbb{R}$. Pfister [**Pfi67**] found an upper bound on the number of squares needed in a representation, depending on the dimension n of the real variety.

THEOREM 1.1 (Pfister). *Let F be the function field of an n-dimensional integral variety over $\mathbb{R}$. Then every sum of squares in F is a sum of 2^n squares.*

For a field K and $n \in \mathbb{N}$ we denote the nonzero sums of n squares by

$$D_K(n) = \{x \in K^\times \mid \exists\, x_1, \dots, x_n \in K \text{ such that } x = x_1^2 + \dots + x_n^2\}.$$

We also write $K^{\times 2} = D_K(1)$ for the nonzero squares and

$$\sum K^{\times 2} = \bigcup_{n \in \mathbb{N}} D_K(n)$$

for the nonzero sums of squares. Note that $\sum K^{\times 2}$ is a subgroup of $K^\times$ and so is $D_K(2)$, as follows[1] from the identitiy $(x^2+y^2)(u^2+v^2) = (xu - yv)^2 + (xv + yu)^2$.

[1]In fact, Pfister proved that $D_K(2^r)$ is a group for any $r \in \mathbb{N}$.

We denote by

$$p(K) = \inf\{n \in \mathbb{N} \mid D_K(n) = \sum K^{\times 2}\}$$

the *Pythagoras number of* K, and

$$s(K) = \inf\{n \in N \mid -1 \in D_K(n)\}$$

the *level of* K. Fields with Pythagoras number one are called *Pythagorean*. Fields with infinite level, that is, where -1 is not a sum of squares, are called *real*. A field is real if and only if it admits an *ordering*, that is, a total order relation that respects the field operations in the expected manner. Real Pythagorean fields are called *Euclidean* if they allow only one ordering.
In this terminology, Pfister's result states that $p(F) \leq 2^n$ for any function field F of an n-dimensional integral variety over $\mathbb{R}$. For general base fields K, it is not even known for the rational function field in one variable, whether $p(K) < \infty$ implies $p(K(X)) < \infty$. It is natural to investigate whether additional field arithmetic properties of K yield more information on the sum of squares properties of a function field over K, and vice versa. I restricted my research to function fields of integral curves, also called *algebraic function fields*. In this case, (1.1) follows from an earlier result by Witt, see e.g. [**PD01**, 3.4.11].

THEOREM 1.2 (Witt). *We have $p(F) = 2$ for every algebraic function field $F/\mathbb{R}$.*

Note that $p(F) \geq 2$ is generally true for function fields F/K. For rational function fields, this is because $X^2 + 1$ is not a square, and it generalizes to arbitrary algebraic function fields, by [**Lam05**, VIII.5.7]:

THEOREM 1.3 (Diller-Dress). *Let L/K be a finite field extension. If L is Pythagorean then so is K.*

Let me introduce a hierarchy of field arithmetic properties that are all satisfied by $\mathbb{R}$. We call a real field K ...

- ... *hereditarily Pythagorean* if every finite real extension field L of K is Pythagorean.
- ... *hereditarily Euclidean* if every finite real extension field L of K is Euclidean.
- ... *real closed* if every proper finite extension field L of K is nonreal.

In the statements (1.1) and (1.2) one can replace $\mathbb{R}$ by any real closed field, with the same proofs.

It is reasonable to ask whether one can go further down in this hierarchy such that Witt's result still holds. The following is an optimal answer to this question, which is a consequence of work by Elman and Wadsworth [**EW87**, Thm], together with [**Lam05**, 6.8 & 6.11], and of work by Becher and Van Geel [**BG09**, 4.7].

THEOREM 1.4 (Becher-Van Geel, Elman-Wadsworth). *Let K be a field not containing $\sqrt{-1}$. Then the following are equivalent.*

(i) K is hereditarily Euclidean.
(ii) Every algebraic function field over K has Pythagoras number 2.
(iii) The function field F of the affine conic $Y^2 = -(X^2+1)$ over K has Pythagoras number 2.

Note that if K is a nonreal field, then $s(K) \leq p(K) \leq s(K)+1$, which follows by the identity $4x = (x+1)^2 - (x-1)^2$. In particular, function fields F containing $\sqrt{-1}$ have trivially Pythagoras number two. The implication $(iii) \Rightarrow (i)$ of (1.4) raises the question whether the existence of a geometrically integral curve whose function field has Pythagoras number two, already implies that its base field is hereditarily Euclidean or contains $\sqrt{-1}$. The following result (shown in [**Bec78**, Chap. III, Theorem 4]) answers this question in the negative, as there exist hereditarily Pythagorean fields that are not Euclidean, such like $\mathbb{R}((t))$, for example.

THEOREM 1.5 (Becker). *Let K be a field not containing $\sqrt{-1}$. Then K is hereditarily Pythagorean if and only if $p(K(X)) = 2$.*

In the view of (1.4 & 1.5), two follow-up questions come to ones mind.

QUESTION 1.6. *Is there a bound on the Pythagoras number of algebraic function fields over hereditarily Pythagorean fields ?*

QUESTION 1.7. *Does the existence of a geometrically integral curve whose function field has Pythagoras number two already imply that its base field is hereditarily Pythagorean?*

Note that a positive answer to (1.7) would yield, by (1.5), that $p(F) = 2$ implies $p(K(X)) = 2$ for finite extensions $F/K(X)$ not containing $\sqrt{-1}$. This would complement (1.3), as well as a result by Prestel, who showed in [**Pre78**] that there exist quadratic extensions of real fields where the Pythagoras number can drop from arbitrarily large values down to 2. A partial answer to (1.7) is given by following [**BG09**, 3.3], which gives a positive answer for some curves, such as curves containing a smooth rational point.

Theorem 1.8 (Becher, Van Geel). *Let K be a field not containing $\sqrt{-1}$. Let F/K be an algebraic function field that allows a K-valuation whose residue field is an odd degree extension of K. Then $p(K(X)) \leq p(F)$. In particular, if $p(F) = 2$ then K is hereditarily Pythagorean.*

It is a fact well know to algebraic geometers, that an algebraic function field F/K is the function field of a regular projective curve over K, and that K-valuations on F correspond to the closed points on this curve. The following examples of smooth irreducible curves over K have function fields for which the above criterion does not apply.

Example 1.9. Let C be a regular projective conic over a field K not containing $\sqrt{-1}$. That is, the projective curve given by a quadratic form $aX^2 + bY^2 + cZ^2 = 0$ for $a, b, c \in K^\times$. Assume that C contains no rational point. Then Springer's Theorem [**Lam05**, VII.2.7] implies that residue fields of K-valuations on the function field of the conic are even degree extensions of K, since by the correspondence between points and K-valuations, the conic has rational points over every residue field of a K-valuation.

We will show later in this work, that affine curves $1 = aX^n + bY^m$ with $a, b \in K^\times$ and $n, m \in \mathbb{N}$, such that $\mathrm{char}(K)$ does not divide nm, are geometrically integral. We call such curves *Cassels-Catalan curves*, due to the similarity of their defining equation with the equations considered in the Cassels-Catalan Conjecture. In the case $n = m$, their function fields are said to be *of Fermat type*, see [**Sti09**, V.3.4].

Example 1.10. Assume $-1 \notin K^{\times 2}$. Let F/K be an algebraic function field of Fermat type, that is, of a projective curve $Z^n = aX^n + bY^n$ with $a, b \in K^\times$ with $\mathrm{char}(K)$ not dividing n. Suppose furthermore that n is even. Obviously, every closed point $(x : y : z)$ on this curve yields a closed point $(x^{\frac{n}{2}} : y^{\frac{n}{2}} : z^{\frac{n}{2}})$ on the regular conic defined by $Z^2 = aX^2 + bY^2$. If $a, b \in K^\times$ are chosen in such way that the conic has no rational point, it follows by the previous example that the residue field of every K-valuation on F is an even degree extension of K, as this extension contains, as an intermediate extension, the residue field of a K-valuation on the function field of the conic $Z^2 = aX^2 + bY^2$.

The criterion (1.8) does not apply to function fields as in (1.9 & 1.10). Nevertheless, the following two results give positive answers of (1.7) for these kind of function fields.

THEOREM 1.11. *Let K be a field not containing $\sqrt{-1}$. Let F/K be the function field of a Cassels–Catalan curve. Then $p(F) = 2$ implies that K is hereditarily Pythagorean.*

This result will be proven in (4.10). Affine conics are in particular Cassels–Catalan curves. The first part of the following result is therefore just a corollary of (1.11). However, in (4.15), we give a separate, more conceptual proof, which exploits geometric properties particular to conics.

THEOREM 1.12. *Let K be a field not containing $\sqrt{-1}$. Let F/K be a function field of a smooth conic. Then $p(F) = 2$ implies that K is hereditarily Pythagorean. If in addition F is nonreal, then $p(F) = 2$ implies that K is hereditarily Euclidean.*

This result has a converse in [**TY05**, Thm.1, Thm. 2 & Thm. 3] by Tikhonov and Yanchevskiĭ, which is also a partial answer to (1.6).

THEOREM 1.13 (Tikhonov, Yanchevskiĭ). *Let K be hereditarily Pythagorean field and F/K the function field of a conic. If F is real then $p(F) = 2$. In the case where F is nonreal, we have $p(F) = 2$ if K is Euclidean, and $p(F) = 3$ if K is not Euclidean.*

Together, (1.12 & 1.13) generalize Becker's result to real function fields of genus zero. The genus is a birational invariant for algebraic curves, that often serves as a mean of classifying irreducible curves or algebraic function fields. By [**Sti09**, VI.3.4], function fields of Cassels–Catalan curves can have arbitrary genus. This is a good indication that Question (1.7) might have a positive answer in general.

Coming back to Question (1.6), we may consider particular hereditarily Pythagorean base fields. A typical example of a hereditarily Pythagorean field that is not Euclidean is $\mathbb{R}((t_1))\dots((t_n))$ for any positive integer n. By $(i) \Leftrightarrow (iii)$ of (1.4), we know that the function field of the conic $Y^2 + X^2 + 1 = 0$ over $\mathbb{R}((t))$ has Pythagoras number at least three, and in fact exactly three, as its function field is nonreal of level two. Tikhonov gave a first example of a real algebraic function field over $\mathbb{R}((t))$ with Pythagoras number at least three. In (6.9), we will present his example, and show that its Pythagoras number is in fact exactly three, and that, up to multiplication with sums of two squares, there is only one sum of three but not fewer squares. This will be shown using our following two results.

Theorem 1.14. *Let $F/\mathbb{R}((t))$ be an algebraic function field. Then*

$$|\sum F^{\times 2}/D_F(2)| = 2^{\chi(F)}.$$

In particular, $p(F) = 2$ if and only if $\chi(F) = 0$.

Here, $\chi(F)$ denotes a certain geometric invariant of the function field F that will be defined properly when we give a proof (6.4) for (1.14). For now, let me just mention that there exist certain geometric objects related to F, so called regular models for F over $\mathbb{R}[[t]]$, that can be roughly thought of as pairs consisting of an integral smooth projective curve over $\mathbb{R}((t))$ (called the generic fiber) and a projective curve over $\mathbb{R}$ (called the special fiber). In this setup, $\chi(F)$ denotes the number of geometrically irreducible components of the special fiber with only finitely many $\mathbb{R}$-rational points. The question, what the value of $p(F)$ is in the case where $\chi(F) \neq 0$, is left open by (1.14). The following result, proven in (6.7), states that $p(F) = 3$ in this case.

Theorem 1.15. *Let $n \in \mathbb{N}$, and $F/\mathbb{R}((t_1))\dots((t_n))$ be an algebraic function field. Then $2 \leq p(F) \leq 3$.*

We prove these results using different local global principles for quadratic forms for algebraic function fields over complete discrete valued fields. We first derive our own geometric local global principle (5.2) from a recently discovered local-global principle [**HHK09**, 4.2] by Harbater, Hartmann, and Krashen, in order to give a proof (6.4) for (1.14). As another application of our geometric local-global principle, we obtain a short presentation of a proof by Colliot-Thélène, Parimala, and Suresh for their recently discovered valuation theoretic local-global principle [**CTPS**, 3.1]. We use their local global principle, to obtain a proof (6.7) for (1.15).

Finally, we consider function fields F of Fermat type over $\mathbb{R}((t))$, and compute $\chi(F)$ in some cases where this is relatively easily possible. The results in these cases yield that $p(F) = 2$ if F is real, and $p(F) = 3$ if F is nonreal. This observation is consistent with the result (1.13) by Tikhonov and Yanchevskiĭ on the Pythagoras number of function fields of genus zero over hereditarily Pythagorean fields, and it suggest that their result might have a generalization to function fields of Fermat type, at least when the base field is $\mathbb{R}((t))$.

CHAPTER 2

Preliminaries in commutative algebra

In this work, all *rings* are commutative with unit element 1, and ring homomorphisms map the unit on the unit. In the ring with one element, we have $0 = 1$, but we do not consider this ring a domain.

1. Noetherian and local rings

THEOREM 2.1 (Krull's Intersection Theorem). *Let A be a Noetherian domain, and $\mathfrak{a}$ a proper ideal of A. Then $\bigcap_{n\in\mathbb{N}} \mathfrak{a}^n = \{0\}$.*

REFERENCE:. [**Eis95**, 5.4].

The set of prime ideals of A is denoted by $\mathrm{Spec}(A)$, called the (prime-) spectrum of A. For $\mathfrak{p} \in \mathrm{Spec}(A)$, the *height of* $\mathfrak{p}$ is defined as

$$h(\mathfrak{p}) = \sup\{n \in \mathbb{N} \mid \exists \mathfrak{p}_0, \ldots, \mathfrak{p}_n \in \mathrm{Spec}(A) \text{ with } \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}\}.$$

The height of $\mathfrak{p}$ is sometimes also-called the *codimension of* $\mathfrak{p}$. The *Krull dimension* of a ring A is the supremum of the heights of its prime ideals.

THEOREM 2.2 (Krull's Height Theorem). *Let A be a Noetherian ring. Let $\mathfrak{p} \in \mathrm{Spec}(A)$ and $x_1, \ldots, x_r \in \mathfrak{p}$ such that $(x_1, \ldots, x_r) \not\subseteq \mathfrak{q}$ for any $\mathfrak{q} \in \mathrm{Spec}(A)$ with $\mathfrak{q} \subsetneq \mathfrak{p}$. Then $h(\mathfrak{p}) \leq r$.*

REFERENCE:. [**Eis95**, 10.2].

COROLLARY 2.3 (Krull's Principal Ideal Theorem). *Let A be a Noetherian ring, $x \in A$ and $\mathfrak{p} \in \mathrm{Spec}(A)$ minimal prime ideal containing x. Then $h(\mathfrak{p}) \leq 1$.*

It follows that a prime ideal $\mathfrak{p}$ of height r of a Noetherian ring A cannot be generated by less then r elements.

A domain A is called *normal* if it is integrally closed in its field of fractions. Normal Noetherian domains of Krull dimension at most one are called *Dedekind domains.*

Regular local rings. Let A be a local Noetherian ring of Krull dimension n. Its maximal ideal $\mathfrak{m}$ is generated by at least n elements, and if $\mathfrak{m} = (x_1, \dots, x_n)$ for some $x_1, \dots, x_n \in \mathfrak{m}$, then we call A a *regular local ring*.

PROPOSITION 2.4 (Auslander-Buchsbaum). *Every regular local ring is a unique factorization domain.*

REFERENCE:. [**Eis95**, 19.19].

In particular, every regular local ring is a domain (cf. [**Eis95**, 10.10]).

LEMMA 2.5. *Let A be a regular local ring of dimension n and let $x_1, \dots, x_n \in A$ be generators of its maximal ideal. Then, for any $j \in \{1, \dots, n\}$, the ring $A/(x_1, \dots, x_j)$ is regular local of Krull dimension $n - j$ and $A_{(x_1,\dots,x_j)}$ is a regular local ring of Krull dimension j.*

PROOF. $A/(x_1, \dots, x_{\ell-1})$ is a local ring of Krull dimension $n - \ell + 1$, by [**Mat86**, 14.1]. Its maximal ideal is generated by the residues $x_\ell + (x_1, \dots, x_{\ell-1}), \dots, x_n + (x_1, \dots, x_{\ell-1})$. Hence $A/(x_1, \dots, x_{\ell-1})$ is a regular local ring.
$A_{(x_1,\dots,x_j)}$ is obviously a local ring. The height of its maximal ideal coincides with its Krull dimension, but also with the height of the prime ideal $(x_1, \dots, x_j)$ in A. by (2.2), we have $h(x_1, \dots, x_j) \leq j$. On the other hand, we have that $h(x_1, \dots, x_j) \geq j$, since the Krull dimension of $A/(x_1, \dots, x_j)$ is $n-j$, and thus otherwise we would have $h(x_1, \dots, x_n) < n$. □

LEMMA 2.6. *Let $\mathcal{O}$ be a regular local ring with maximal ideal $\mathfrak{m}$ and $\sqrt{-1} \notin \mathcal{O}/\mathfrak{m}$. Then $\mathcal{O}[\sqrt{-1}]$ is a regular local ring with maximal ideal $\mathfrak{m}\mathcal{O}[\sqrt{-1}]$ and $\mathcal{O}[\sqrt{-1}] \cap \mathrm{Quot}(\mathcal{O}) = \mathcal{O}$.*

PROOF. Since $\sqrt{-1} \notin \mathcal{O}/\mathfrak{m}$, the ring $\mathcal{O}[\sqrt{-1}] = \mathcal{O}[X]/(X^2+1)$ is obviously a finite extension of $\mathcal{O}$, whereby $\mathcal{O}[\sqrt{-1}]$ is at least of the same dimension, by a 'Going-Up' result [**Eis95**, 4.15], it is semilocal and its finitely many maximal ideals all lie over $\mathfrak{m}\mathcal{O}[\sqrt{-1}]$. On the other hand, $\mathcal{O}[\sqrt{-1}]/\mathfrak{m}\mathcal{O}[\sqrt{-1}] = \mathcal{O}/\mathfrak{m}[X]/(X^2+1)$ is a field, since $\sqrt{-1} \notin \mathcal{O}/\mathfrak{m}$. Hence $\mathcal{O}[\sqrt{-1}]$ is local and in fact regular local. □

Completions and Hensel's Lemma. Let A be a ring and $\mathfrak{a}$ a proper ideal. Consider for $i \geq 1$, the rings $A/\mathfrak{a}^i$ with the canonical residue maps $\rho_{n,m} : A/\mathfrak{a}^n \to A/\mathfrak{a}^m$ for $m \leq n$, which yield an inverse system of rings. We call the inverse limit

$$\varprojlim_{i\in\mathbb{N},i\geq 1} A/\mathfrak{a}^i = \{(g_i)_{i\geq 1} \mid \rho_{n,m}(g_n) = g_m \text{ for } 1 \leq m \leq n\}$$

the *completion of* A *with respect to* $\mathfrak{a}$, sometimes denoted by $\widehat{A}$ when the ideal $\mathfrak{a}$ is understood.

REMARK 2.7. Let A be ring and $\mathfrak{a}, \mathfrak{b}$ proper ideals such that $\mathfrak{b}^n = \mathfrak{a}$ for some $n \in \mathbb{N}$. Then $\varprojlim A/\mathfrak{a}^i \cong \varprojlim A/\mathfrak{b}^i$. The isomorphism is induced by isomorphisms $A/\mathfrak{a}^i \cong A/\mathfrak{b}^{ni}$ for $i \in \mathbb{N}$.

If the natural homomorphism $A \to \widehat{A}$ is an isomorphism, then we say that A is *complete with respect to* $\mathfrak{a}$.

EXAMPLE 2.8. Let A be a ring, $\mathfrak{a}$ a proper ideal, and $\widehat{A} = \varprojlim A/\mathfrak{a}^i$. The set $\hat{\mathfrak{a}} = \{(g_i)_{i\geq 1} \in \widehat{A} \mid g_1 = 0\}$ is a proper ideal in $\widehat{A}$. Moreover, by the way the inverse system is defined, one sees that

$$\hat{\mathfrak{a}}^n = \{(g_i)_{i\geq 1} \in \widehat{A} \mid g_j = 0 \text{ for all } 1 \leq j \leq n\}$$

for every $n \geq 1$, whereby one can show that $\widehat{A}/\hat{\mathfrak{a}}^i \cong A/\mathfrak{a}^i$ and thus that $\widehat{A}$ is complete with respect to $\hat{\mathfrak{a}}$. In particular, $\widehat{A}/\hat{\mathfrak{a}} \cong A/\mathfrak{a}$.

REMARK 2.9. Note that the natural homomorphism $A \to \widehat{A}$ is injective if and only if $\bigcap \mathfrak{a}^i = \{0\}$. Hence, if A is a Noetherian domain, then we have injectivity by (2.1).

If A is a local ring with maximal ideal $\mathfrak{m}$ and $\widehat{A}$ is the completion of A with respect to $\mathfrak{m}$, then $\widehat{A}$ is a local ring with maximal ideal $\hat{\mathfrak{m}}$, by [**AM69**, 10.16]. If A is Noetherian, then the completion $\widehat{A}$ with respect to any proper ideal is Noetherian, by [**AM69**, 10.26].

PROPOSITION 2.10. *Let* A *be a Noetherian local ring. Then* $\widehat{A}$ *is regular if and only if* A *is regular.*

REFERENCE:. [**AM69**, 11.24].

THEOREM 2.11 (Hensel's Lemma). *Let* A *be a ring that is complete with respect to a proper ideal* $\mathfrak{a}$*, and let* $f \in A[X]$ *be a polynomial in one variable and* $\frac{d}{dX}f \in A[X]$ *its formal derivative. For* $a \in A$ *such that* $f(a) \in \mathfrak{a}$ *and* $\frac{d}{dX}f(a) \in A^\times$*, there exists* $b \in A$ *such that* $f(b) = 0$ *and* $(b - a) \in \mathfrak{a}$*.*

REFERENCE:. This is a special case of [**Eis95**, 7.3].

2. Valuation rings and valuations

A domain $\mathcal{O}$ is called a *valuation ring* if, for every $x \in \mathrm{Quot}(\mathcal{O})$, we have that $x \in \mathcal{O}$ or $\frac{1}{x} \in \mathcal{O}$. If, moreover, $\mathcal{O}$ is a principal ideal domain, then we call $\mathcal{O}$ a *discrete valuation ring*. Valuation rings are local rings.

PROPOSITION 2.12. *Let $\mathcal{O}$ be a ring. The following are equivalent*

(i) $\mathcal{O}$ is a discrete valuation ring,
(ii) $\mathcal{O}$ is a one dimensional regular local ring,
(iii) $\mathcal{O}$ is a local Dedekind domain of Krull dimension one.

REFERENCE:. [**Mat86**][11.2].

Let K be a field and $(\Gamma, +, \leq)$ an ordered abelian group (i.e. endowed with a linear order relation that respects the addition). Let ∞ be an abstract element that is larger than any element in Γ, and extend the addition on $\Gamma \cup \{\infty\}$ consistent with the order relation.
A map $v : K \longrightarrow \Gamma \cup \infty$ is called a *valuation*, if for all $x, y \in K$,

(i) $v(x) = \infty \Leftrightarrow x = 0$
(ii) $v(xy) = v(x) + v(y)$
(iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

As a very useful immediate consequence, we note that

(iv) $v(x) \neq v(y) \Rightarrow v(x + y) = \min\{v(x), v(y)\}$.

We call $\Gamma_v = v(K^\times) \subseteq \Gamma$ the *value group of* v. Every valuation v on K defines a ring $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$. This is a valuation ring and its maximal ideal is $\mathfrak{m}_v = \{x \in K \mid v(x) > 0\}$. Conversely, every valuation ring $\mathcal{O}$ with field of fractions K defines a valuation

$$v : K \to K^\times/\mathcal{O}^\times \cup \{\infty\},$$

where the abelian group $K^\times/\mathcal{O}^\times$ is written additively and endowed with an order structure which is uniquely determined by requiring that $a\mathcal{O}^\times > 0$ iff $a \in \mathfrak{m}$. We call $\kappa_v = \mathcal{O}_v/\mathfrak{m}_v$ the *residue field of* v. In the case where $\mathrm{char}(\kappa_v) = 2$, we call v a *dyadic* valuation, and *nondyadic* otherwise.
We call two valuations v_1 and v_2 on K *equivalent* if there exists an order preserving isomorphism $\gamma : \Gamma_{v_1} \to \Gamma_{v_2}$ such that $\gamma \circ v_1 = v_2$. One can show that this is the same as saying that $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$.
We call an ordered abelian group Γ *discretely ordered of rank* n if it is order-isomorphic to $(\mathbb{Z}^n, \leq_{\mathrm{lex}})$ for some $n \in \mathbb{N}$, where $\leq_{\mathrm{lex}}$ denotes the lexicographic ordering. This is defined by

$$(m_1, \ldots, m_n) \leq_{\mathrm{lex}} (\ell_1, \ldots, \ell_n)$$

if for any $1 \leq i \leq n$ such that $\ell_i < m_i$, there exists $1 \leq j < i \leq n$ such that $m_j < \ell_j$.

We call a valuation v discrete if its value group Γ_v is order-isomorphic to $\mathbb{Z}$ and, identifying Γ_v with $\mathbb{Z}$, we call any $\pi \in K$ with $v(\pi) = 1$, or equivalently, every generator of the maximal ideal $\mathfrak{m}_v$ of $\mathcal{O}_v$, a *uniformizing element for* v. A valuation v on a field K is trivial if $\Gamma_v \cong \{0\}$, that is, if $\mathcal{O}_v = K$. Note that a valuation v is discrete if and only if $\mathcal{O}_v$ is a discrete valuation ring.

NOTATION 2.13. We denote by $\Omega(K)$ the set of equivalence classes of discrete valuations on K.

LEMMA 2.14. *Let $\mathcal{O}$ be a regular local ring of dimension n with maximal ideal $\mathfrak{m}$ and field of fractions K. There exists a valuation v on K with $v(K^\times)$ discretely ordered of rank n, such that $\mathcal{O} \subseteq \mathcal{O}_v$, $\mathfrak{m}_\mathfrak{v} \cap \mathcal{O} = \mathfrak{m}$, and the canonical embedding $\mathcal{O}/\mathfrak{m} \hookrightarrow \mathcal{O}_v/\mathfrak{m}_v$ is an isomorphism.*

PROOF. Write $\mathfrak{m} = (x_1, \dots, x_n)$. We show by induction on n that there exists a discrete valuation v with $\Gamma_v \cong (\mathbb{Z}^n, \leq_{\text{lex}})$ such that $\mathcal{O} \subseteq \mathcal{O}_v$ and such that

$$v(x_i) = e_i = (0, \dots, 0, \underbrace{1}_{i^{\text{th}}}, 0, \dots, 0) \in \mathbb{Z}^n = \Gamma_v,$$

which implies that $\mathfrak{m} = \mathfrak{m}_v \cap \mathcal{O}$, and furthermore, that $\mathcal{O}/\mathfrak{m} \to \mathcal{O}_v/\mathfrak{m}_v$ is surjective.

The case $n = 1$ is clear, since then $\mathcal{O}$ is already a discrete valuation ring. Suppose $n > 1$. The maximal ideal $\mathfrak{m}$ is generated by n elements, i.e. $\mathfrak{m} = (x_1, \dots, x_n)$. The ring $\mathcal{O}/(x_1, \dots, x_{n-1})$ is a regular local ring of Krull dimension 1. Hence, it is a discrete valuation ring, and we denote by v' the induced valuation on its field of fractions with uniformizer x_n. The field $\operatorname{Quot}(\mathcal{O}/(x_1, \dots, x_{n-1}))$ is the residue field of the regular local ring $\mathcal{O}_{(x_1, \dots, x_{n-1})}$, which is of Krull dimension $n-1$. By the induction hypothesis, there exists a discrete valuation w on K with $\Gamma_w \cong (\mathbb{Z}^{n-1}, \leq_{\text{lex}})$ such that $\kappa_w = \operatorname{Quot}(\mathcal{O}/(x_1, \dots, x_{n-1}))$ with $w(x_i) = e_i$ for $1 \leq i \leq n-1$. We define a valuation

$$v : K \to \mathbb{Z}^{n-1} \times \mathbb{Z} \cup \{\infty\}$$

as follows. For $x \in \kappa(X)$, we define the first $n-1$ components to be $w(x) = (w_1(x), \dots, w_{n-1}(x)) \in \mathbb{Z}^{n-1}$. Then we have that $w(y) = 0$ for

$$y = \frac{x}{x_1^{w_1(x)} \cdots x_{n-1}^{w_{n-1}(x)}},$$

and we define the last component of $v(x)$ to be $v'(\overline{y})$, where $\overline{y} \in \kappa_w$ is the residue of $y \in \mathcal{O}_w$. In particular, $v(x_i) = e_i$ for all $1 \leq i \leq n$. We extend the lexicographical order of $\mathbb{Z}^{n-1}$ to $\mathbb{Z}^n$ by including the last component as the smallest in the lexicographic hierarchy. This defines a valuation v whose residue field κ_v is equal to $\kappa_{v'}$, which by assumption, is $\left(\mathcal{O}/(x_1,\ldots,x_{n-1})\right)_{(\overline{x}_n)} / \overline{x}_n \left(\mathcal{O}/(x_1,\ldots,x_{n-1})\right)_{\overline{x}_n} \cong \mathcal{O}/\mathfrak{m}$. □

Approximation and complete discrete valuations. Valuation rings $\mathcal{O}_1 \neq \mathcal{O}_2$ with the same field of fractions K are called *independent* if the only subring of K containing both $\mathcal{O}_1$ and $\mathcal{O}_2$, is K itself (cf. [**End72**, 6.11]).

LEMMA 2.15. *Let $\mathcal{O}$ be a discrete valuation ring with field of fractions K. Let A be a subring of K with $\mathcal{O} \subseteq A$, then either $A = \mathcal{O}$ or $A = K$. in particular, distinct discrete valuation rings with field of fractions K are independent.*

PROOF. Denote by $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$. Suppose A is a subring of K containing $\mathcal{O}$. Then A is necessarily a discrete valuation ring by the defining properties, and it is also easy to see that its maximal ideal $\mathfrak{m}_A$ is contained in $\mathfrak{m}$, whereby it is a prime ideal of $\mathcal{O}$. Since $\mathcal{O}$ is a principal ideal domain, we have $\mathfrak{m}_A = \pi^r\mathcal{O}$ for some $r \in \mathbb{N}$ and a $\pi \in \mathcal{O}$ such that $\pi\mathcal{O} = \mathfrak{m}$. But since $\mathfrak{m}_A$ is a prime ideal, it follows that $r = 1$ and hence $\mathfrak{m}_A = \mathfrak{m}$. Consequently, it follows that $A = \mathcal{O}$. □

PROPOSITION 2.16 (Weak Approximation Theorem). *Let K be a field and let $v_1, \ldots, v_n \in \Omega(K)$ be pairwise distinct. For any $m_1, \ldots, m_n \in \mathbb{Z}$ there exists $x \in K$ such that $v_i(x) = m_i$ for $1 \leq i \leq n$.*

REFERENCE:. [**End72**, 11.17], together with (2.15).

NOTATION 2.17. We call a discrete valued field (K, v) complete if $\mathcal{O}_v$ is a complete ring with respect to $\mathfrak{m}_v$.

REMARK 2.18. Let (K, v) be a discrete valued field with valuation ring $\mathcal{O}_v$. Then its completion $\widehat{\mathcal{O}}_v$ with respect to $\mathfrak{m}_v$ is a discrete valuation ring, as follows from the fact that it is a regular local ring by (2.10). We denote by K^v its field of fraction and call it the completion of v.

LEMMA 2.19. *Let (K, v) be a complete discrete valued field. Then v is the unique discrete valuation on K.*

PROOF. For any discrete valuation w on K, let $\mathcal{O}_w$ denote its valuation ring and $\mathfrak{m}_w$ its maximal ideal. Recall that, for any two distinct discrete valuations w_1 and w_2 on K, one has $\mathcal{O}_{w_1} \not\subseteq \mathcal{O}_{w_2}$ and $\mathcal{O}_{w_2} \not\subseteq \mathcal{O}_{w_1}$.

Now let w be an arbitrary discrete valuation on K. Since $\mathcal{O}_v$ is a complete ring with respect to $\mathfrak{m}_v$, it satisfies (2.11) and thus the elements of $1+\mathfrak{m}_v$ are n^{th} powers for all $n \in \mathbb{N}$ prime to the residue characteristic of v. As w is discrete, this yields that $1+\mathfrak{m}_v \subseteq \mathcal{O}_w^\times \subseteq \mathcal{O}_w$ and thus $\mathfrak{m}_v \subseteq \mathcal{O}_w$. If $\mathfrak{m}_v \subseteq \mathfrak{m}_w$, then $\mathcal{O}_w \subseteq \mathcal{O}_v$. Otherwise there exists $t \in \mathfrak{m}_v \setminus \mathfrak{m}_w$, in particular $w(t) = 0$ and $\mathcal{O}_v = \frac{1}{t}(t\mathcal{O}_v) \subseteq \frac{1}{t}\mathfrak{m}_v \subseteq \mathcal{O}_w$. Hence $w = v$ in either case by (2.15). □

Remark 2.20. There is another notion of completeness ([**EP05**, p. 50]) for valued fields which coincides with our notion in the case where the value group is discrete of rank one. One can replace 'discrete' by 'order-embeddable into $\mathbb{R}$' in the statement of (2.19), see [**EP05**, 2.3.2].

Extending valuations. Let E/K be a field extension. Let v be a valuation on K. A valuation w on E *extends* v if $w|_K = v$. In this situation, $\kappa_v \subseteq \kappa_w$ is a subfield and $\Gamma_v \subseteq \Gamma_w$ is a subgroup. By [**EP05**, 3.1.2], there exists at least on extension w of v.

Proposition 2.21. *Let E/K be a separable quadratic extension and let ι denote the nontrivial automorphism of E/K. Let v denote a discrete valuation on K and w an extension of v to E. Then w and $w \circ \iota$ are the only valuations on E extending v, and one of the following holds.*

a) $w = w \circ \iota$ and $\kappa_w = \kappa_v$ and $|\Gamma_w : \Gamma_v| = 2$,
b) $w = w \circ \iota$ and $[\kappa_w : \kappa_v] = 2$ and $|\Gamma_w = \Gamma_v|$,
c) $w \neq w \circ \iota$ and $\kappa_w = \kappa_v = \kappa_{w\circ\iota}$ and $\Gamma_w = \Gamma_v$.

Moreover, if $E = K[\sqrt{d}]$ for some $d \in \mathcal{O}_v^\times \setminus K^{\times 2}$, then $\kappa_w = \kappa_v[\sqrt{d}]$

Reference:. [**EP05**, 3.2.15 & 3.3.5].

Proposition 2.22. *If (K, v) is a complete discrete valued field and L/K a finite field extension, then v extends uniquely to a valuation w on L, and (L, w) is a complete discrete valued field.*

Reference:. [**Lan02**, XII.2.5].

Proposition 2.23. *Let E/K be a finitely generated field extension of transcendence degree one. Let w be a discrete valuation on E and denote $v = w|_K$. Then one of the following holds*

a) v is trivial and κ_w/K is a finite extension.
b) v is nontrivial and κ_w/κ_v is algebraic.
c) v is nontrivial and κ_w/κ_v is a finitely generated field extension of trenscendence degree one.

Reference:. [**EP05**, 3.4.3].

Sums of squares and valuations. A valuation v on K is called *real* if κ_v is real, and *nonreal* otherwise. Note that only real fields admit real valuations.

LEMMA 2.24. *Let v be a real valuation on K, and $x_1, \dots, x_n \in K$. Then $v(x_1^2 + \cdots + x_n^2) = 2\min\{v(x_i) \mid 1 \leq i \leq n\}$. In particular, for any $\sigma \in \sum K^{\times 2}$ there exists $a \in K^\times$ such that $v(a^2\sigma) = 0$, and for every $\sigma \in \sum K^{\times 2}$ with $v(\sigma) = 0$, we have $\overline{\sigma} \in \sum \kappa_v^{\times 2}$.*

PROOF. Suppose that $v(x_1^2 + \cdots + x_n^2) > 2\min\{v(x_i) \mid 1 \leq i \leq n\}$. Assume, without loss of generality, that $v(x_1) = \min\{v(x_i) \mid 1 \leq i \leq n\}$. Then $0 < v(1 + (\frac{x_2}{x_1})^2 + \cdots + (\frac{x_n}{x_1})^2)$, contradicting the fact that κ_v is real. □

COROLLARY 2.25. *Let v be a real valuation on K. Then $p(K) \geq p(\kappa_v)$.*

PROOF. Let $x_1, \dots, x_n \in \mathcal{O}_v^\times$ such that $\overline{x}_1^2 + \cdots + \overline{x}_n^2 \notin D_{\kappa_v}(n-1)$. Suppose, for the sake of contradiction, that there exist $y_1, \dots, y_{n-1} \in K$ such that $x_1^2 + \cdots + x_n^2 = y_1^2 + \cdots + y_{n-1}^2$. Then $v(y_i) \geq 0$ by (2.24). This yields the contradiction $\overline{x}_1^2 + \cdots + \overline{x}_n^2 = \overline{y}_1^2 + \cdots + \overline{y}_{n-1}^2 \in D_{\kappa_v}(n-1)$. Hence, $x_1^2 + \cdots + x_n^2 \in D_K(n)$. It follows $p(K) \geq p(\kappa_v)$, when choosing $n = p(\kappa_v)$. □

PROPOSITION 2.26. *Let $n \geq 1$ and v be a nonreal nondyadic valuation on K whose value group $v(K^\times)$ is discretely ordered of finite rank. Then $p(K) > s(\kappa_v)$.*

PROOF. Let $s = s(\kappa_v)$. Then there exist $x_0, \dots, x_s \in \mathcal{O}_w^\times$ with $\overline{x}_0^2 + \ldots + \overline{x}_s^2 = 0$. We may assume that $v(x_0^2 + \ldots + x_s^2) \notin 2v(K^\times)$; in fact, if $v(x_0^2 + \ldots + x_s^2) \in 2v(K^\times)$, we simply replace x_s by $(x_s + t)$, where $t \in K$ is such that $v(t)$ is the minimal positive element in $v(K^\times)$. Hence, $v(x_0^2 + \ldots + (x_s + t)^2) = v((x_0^2 + \cdots + x_s^2) + (2x_s t + t^2)) = v(t) \notin 2v(K^\times)$. We claim that $x_0^2 + \ldots + x_s^2$ is not a sum of s squares in K. Suppose on the contrary that $x_0^2 + \ldots + x_s^2 = y_1^2 + \ldots + y_s^2$ for some $y_1, \dots, y_s \in K$ with $v(y_1) \leq v(y_i)$ for $1 \leq i \leq s$. Let $z_i = \dfrac{y_i}{y_1} \in \mathcal{O}_v$ for $2 \leq i \leq s$. Since $v(y_1^2 + \ldots + y_s^2) \notin 2v(K^\times)$, it follows that $v(1 + z_2^2 + \ldots + z_s^2) > 0$. We obtain that $-1 = \overline{z}_2^2 + \ldots + \overline{z}_s^2$ in κ_v, contradicting the fact that $s = s(\kappa_v)$. □

CHAPTER 3

Preliminaries in algebraic geometry

Before we introduce algebraic varieties in the language of schemes, we consider classical algebraic sets in finite dimensional vector spaces, in order to obtain some observations on scalar restriction in the context of varieties. The scalar restriction is treated in a elementary and simplistic language as it is used later in a set-up where the scheme theoretic considerations are not necessary. We also recall the concept of a variety in the language of schemes. In fact, we only define the notion of a prevariety as the missing condition (separability) is either implicit or irrelevant in the statements that we consider. We also give a brief summary on curves over fields and fibered surfaces over one dimensional Dedekind domains. It is in this context of relative curves (or fibered surfaces) that the setup of algebraic geometry in the language of schemes is needed later in the work. In this chapter we formulate several observations tailored for our later use that cannot be found verbatim in the standard literature, and we embed these observations in a quick and self-contained introduction to algebraic geometry. Some facts and definitions however are considered basic, and thus given without proof or reference.

1. Some notes on scalar restriction

Let K be a field and V a K-vector space of dimension $n < \infty$. We call a mapping V to K a *K-polynomial function* if it is given by evaluating a K-polynomial in n variables, after identifying V with K^n via choosing any basis for V. Endowing K with the cofinite topology, that is, the topology where the closed subsets are the finite sets and the set K, we define the *K-topology on V* to be the initial topology of the K-polynomial functions.

A partially defined function $V \dashrightarrow K$ that is defined on a K-open subset of V, is called a *K-rational function on V* if it is (locally) given by a fraction of K-polynomial functions.

If V, W are two finite dimensional K-vector spaces, we call a map $\varphi : V \to W$ a *K-polynomial map* if, for each basis element w_i of a fixed K-basis $w_1, \dots, w_m$ of W, the function $\pi_i \circ \varphi : V \to K$ is a polynomial function, where $\pi_i : W \longrightarrow K$ is the projection

$$(\alpha_1 w_1 + \cdots + \alpha_i w_i + \cdots + \alpha_m w_m) \mapsto \alpha_i.$$

More generally, a partially defined map $\varphi : V \dashrightarrow W$ that is defined on a K-open subset of V is called a *K-rational map* if the corresponding $\varphi \circ \pi_{w_i}$ are K-rational functions.
Note that if V' is a K-linear subspace of V and φ is a K-rational map on V that is defined on some $P \in V'$, then $\varphi|_{V'}$ is a K-rational map.

LEMMA 3.1. *Let L/K be a finite field extension. For every $f \in L(t)$ there exist $g \in L[t]$ and $h \in K[t]$ such that $f = \frac{g}{h}$.*

PROOF. Choosing $\alpha_1, \dots, \alpha_n \in L$ such that $L = K[\alpha_1, \dots, \alpha_n]$, we have that $L(t) = K[\alpha_1, \dots, \alpha_n](t) = K(t)[\alpha_1, \dots, \alpha_n]$. □

PROPOSITION 3.2. *Let L/K be a finite field extension. Then*

$$\mathrm{mult} : L \times L \to L,\ (x, y) \mapsto xy$$

is a K-polynomial map and

$$\mathrm{inv} : L \dashrightarrow L,\ x \mapsto \frac{1}{x}$$

is a K-rational map.

PROOF. We identify L with a K-subalgebra of $\mathrm{End}_K(L)$, via the algebra homomorphism that asigns to $a \in L$ the left-multiplication map $x \mapsto ax$. The multiplication on $\mathrm{End}_K(L)$ is a K-polynomial map

$$\mathrm{End}_K(L) \times \mathrm{End}_K(L) \to \mathrm{End}_K(L),$$

as can be seen by identifying $\mathrm{End}_K(L)$ with a matrix algebra over K. Hence, its restriction $\mathrm{mult} : L \times L \to L$ to L is also a K-polynomial map. The nonempty subset of invertible elements of $\mathrm{End}_K(L)$ is a K-open subset, as it can be defined by the nonvanishing of the determinant function, which is a K-polynomial function. Finally, the inversion map is a K-rational map on $\mathrm{End}_K(L)$ by Cramer's rule, defined on the invertible elements. Hence, its restriction $\mathrm{inv} : L \dashrightarrow L$ to L is also a K-polynomial map. □

LEMMA 3.3. *Let L/K be a finite extension and $f \in L(t)$. Then the L-rational map $f : L \dashrightarrow L$ is a K-rational map, i.e. after fixing a K-basis of L the map is given by $[L : K]$ fractions of polynomials in $[L : K]$ variables over K.*

Proof. First, we show this in the case $f \in L[t]$. Write $s = [L : K]$. Let us fix an arbitrary K-basis $(\ell_1, \dots, \ell_s)$ of L.
Write $f = f_0 + f_1 t + \cdots + f_d t^d$ with $f_0, \dots, f_d \in L$ and $d \in \mathbb{N}$. For $z \in L$ write $z = r_1\ell_1 + \cdots + r_s\ell_s$ with $r_1, \dots r_s \in K$. One has

$$\begin{aligned} f(z) =& f(r_1\ell_1 + \cdots + r_s\ell_s) \\ =& \sum_{i=0}^{d} f_i \cdot (r_1\ell_1 + \cdots + r_s\ell_s)^i \\ =& \sum_{i=0}^{d} \sum_{\mu_1+\cdots+\mu_s=i} \left(\frac{i!}{\mu_1! \cdots \mu_s!}\right) \ell_1^{\mu_1} \cdots \ell_s^{\mu_s} f_i \quad r_1^{\mu_1} \cdots r_s^{\mu_s}. \end{aligned}$$

We can consider this as a polynomial function over L in s variables evaluated at $(r_1, \dots, r_s)$. We can choose $\tilde{f}_1, \dots, \tilde{f}_s \in K[X_1, \dots, X_s]$ such that

$$f(r_1\ell_1 + \cdots + r_s\ell_s) = \tilde{f}_1(r_1, \dots, r_s)\ell_1 + \cdots + \tilde{f}_s(r_1, \dots, r_s)\ell_s.$$

Hence the map $f : L \to L$ is given by the polynomials $\tilde{f}_1, \dots, \tilde{f}_s$ over K.
Now assume that $f \in L(t)$. Let $g, h \in L[t]$ be relatively prime such that $f = \frac{g}{h}$. Then $f : L \dashrightarrow L$ is defined on $L \setminus h^{-1}(\{0\})$ and factors into

$$f : L \xrightarrow{(f,g)} L \times L \overset{\mathrm{id}\times\mathrm{inv}}{\dashrightarrow} L \times L \overset{\mathrm{mult}}{\dashrightarrow} L,$$

where $(g, h) : L \to L \times L, x \mapsto (g(x), h(x))$ and $\mathrm{id} \times \mathrm{inv} : L \times L \dashrightarrow L \times L, (x, y) \mapsto (x, y^{-1})$. Since it is a composition of K-rational maps, we conclude that f is a K-rational map. □

Proposition 3.4. *Let K be an infinite field and L/K a proper finite field extension that is not purely inseparable. Let $f \in L(t)$ be a rational function. If $f(z) \in K$ for every $z \in L$ where f is defined, then $f \in K$.*

Proof. First, we show that $f \in K(t)$. By (3.1) there exists $g \in L[t]$ and $h \in K[t]$ such that $f = \frac{g}{h}$.
Write $g = (g_0, g_1, \dots, g_d) \cdot (1, t, \dots, t^d)^{\mathrm{t}}$ with $g_0, \dots, g_d \in L$ for some $d \in \mathbb{N}$. Evaluation of this polynomial in pairwise distinct elements $\alpha_0, \dots, \alpha_d \in K \setminus h^{-1}(\{0\})$ yields a system of linear equations over k for

the indeterminants $g_0, \dots, g_d$ as presented below.

$$\begin{pmatrix} 1 & \alpha_0 & \cdots & \alpha_0^d \\ 1 & \alpha_1 & \cdots & \alpha_1^d \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^d \end{pmatrix} \cdot \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_d \end{pmatrix} = \begin{pmatrix} f(\alpha_0) \\ f(\alpha_1) \\ \vdots \\ f(\alpha_d) \end{pmatrix} \in K^{d+1}$$

The Vandermonde matrix $(\alpha_i^j)_{0 \le i,j \le d}$ is invertible and defined over K. Therefore $g_0, \dots, g_d \in K$.

Now we are going to show that $\frac{g}{h} \in K$. Let $\beta \in L$ be a separable element over K and let σ be an automorphism of K_{sep}/K such that $\sigma(\beta) \neq \beta$. For any $(r_0, r_1) \in K \times K$ we have $g(r_0 + r_1\beta)\sigma(h(r_0 + r_1\beta)) = \sigma(g(r_0 + r_1\beta))h(r_0 + r_1\beta)$ by the assumption that $f(z) \in K$ for all $z \in L \backslash h^{-1}(\{0\})$. Thus $g(r_0+r_1\beta)h(r_0+r_1\sigma(\beta)) = g(r_0+r_1\sigma(\beta))h(r_0+r_1\beta)$. Since $K \times K$ is Zariski dense in $K_{\mathrm{alg}} \times K_{\mathrm{alg}}$, the polynomial identity $g(X+Y\beta)h(X+Y\sigma(\beta)) = g(X+Y\sigma(\beta))h(X+Y\beta)$ follows. We obtain that $g(X)h(Y) = g(Y)h(X)$ and consequently that $f = \frac{g}{h} \in K$, by showing that $X+Y\sigma(\beta)$ and $X+Y\beta$ are algebraically independent over K. Assume there exists a polynomial $P \in K[T_1, T_2]$ over K such that $P(X + Y\beta, X + Y\sigma(\beta)) = 0$. For any $a, b \in K_{\mathrm{alg}}$ there are $x, y \in K_{\mathrm{alg}}$ such that

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & \beta \\ 1 & \sigma(\beta) \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

as the determinant of the 2×2 matrix does not vanish. Hence $P(a, b) = 0$ for all $(a, b) \in K_{\mathrm{alg}} \times K_{\mathrm{alg}}$ and thus $P(T_1, T_2) = 0$. □

Proposition 3.5. *Let L/K be a finite separable extension of infinite fields. Let $f \in L(t)$ be a nonconstant rational function. Let $W \subseteq L$ be any nonempty K-open subset on which f is defined. Then there exists $\alpha \in W$ such that $f(\alpha)$ is a primitive element of L/K.*

Proof. By (3.3), $f : L \dashrightarrow L$ defines a K-rational map. Note that the K-open subset W is dense in L, and thus irreducible with respect to its subspace topology. As f is continuous with respect to the subspace topology, the topological subspace $f(W) \subseteq L$ is irreducible. Assume that $f(\alpha)$ is not a primitive element of L/K for any $\alpha \in W$. Then the image of f lies in the finite union of the maximal proper subfields of L containing K, i.e. in the union of finitely many vector subspaces of L. None of those maximal proper subfields is contained in the union of the others. Thus the image of f is contained in one maximal proper subfield F of L containing K, as otherwise, we could write the irreducible image of f as the nontrivial finite union of the relatively closed subsets consisting of the intersections of the image of f with each of the maximal proper subfields. By (3.4), we obtain that $f \in F$, i.e. that f is a constant function, contradicting the assumption of the statement. $\square$

2. Schemes

After these explicit first and elementary definitions and observations of the Zariski-topology, polynomial maps, rational functions, and scalar restriction, we will start over and present a more holistic, intrinsic but compatible abstract approach to algebraic geometry.
The underlying object in every setting of geometry is a topological space X, together with some additional structure that depends on the setting. The topological space X is called *irreducible*, if it is not the union of two proper closed subsets. We denote by $\dim(X)$ the *dimension of* X, i.e. the supremum of the lengths of chains of proper closed irreducible subsets of X. For a closed irreducible subset $Y \subset X$, we call the supremum of lenghts of chains of proper closed irreducible subsets of X containing Y, the *codimension* of Y in X. We call a point $P \in X$ a point of codimension n in X, if $\overline{\{P\}}$ is of codimension n in X.

Locally ringed spaces. Let X be a topological space. A *presheaf of rings* $\mathcal{O}_X$ consists of the following data: A commutative ring $\mathcal{O}_X(U)$ for every open subset $U \subseteq X$, with $\mathcal{O}_X(\emptyset) = \{0\}$, and for any two open subsets $V \subseteq U \subseteq X$, a ring homomorphism $\rho_{UV} : \mathcal{O}_X(U) \to \mathcal{O}_X(V)$ (called the *restriction homomorphism from* U *to* V), such that for any triple $W \subseteq V \subseteq U \subseteq X$ of open subsets, we have $\rho_{UW} = \rho_{VW} \circ \rho_{UV}$ and $\rho_{UU} = \mathrm{id}_U$. For $s \in \mathcal{O}_X(U)$, we write $s|_V$ instead of $\rho_{UV}(s)$.

We call a presheaf $\mathcal{O}_X$ a *sheaf* if, for every nonempty open $U \subseteq X$, and every open covering $(U_i)_{i\in I}$ of U together with elements $s_i \in \mathcal{O}_X(U_i)$ such that $s_i|_{V_i \cap V_j} = s_j|_{V_i \cap V_j}$, there exists a unique element $s \in \mathcal{O}_X(U)$ such that $s_i = s|_{V_i}$ for all $i \in I$.

We call a pair $(X, \mathcal{O}_X)$, where X is topological space and $\mathcal{O}_X$ a sheaf of rings on X, a *ringed space*. A *morphims of ringed spaces* $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a continuous map $f : X \to Y$ and for each open $U \subseteq Y$ a ring homomorphism $f^\#_U : \mathcal{O}_Y(U) \to \mathcal{O}_X(f^{-1}(U))$, such that this system of homomorphisms commutes with the respective system of restriction maps. On also calls $f^\#$ a *morphism of sheaves*. An isomorphism $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ of *ringed spaces* is a homeomorphism f, and for each open $U \subseteq Y$, an isomorphism $f^\#_U : \mathcal{O}_Y(U) \to \mathcal{O}_X(f^{-1}(U))$.

Note that in some books, the notion ‘ringed space’ refers to what we will call a ‘locally ringed space’.

Let $(X, \mathcal{O}_X)$ be a ringed space. For any $P \in X$, the system of rings $\mathcal{O}_X(U)$ for neighbourhoods U of P, together with the restriction homomorphisms, is a directed system of rings, and induces the *stalk* $\mathcal{O}_{X,P} = \varinjlim \mathcal{O}_X(U)$. If $\mathcal{O}_{X,P}$ is a local ring for each $P \in X$, we call $(X, \mathcal{O}_X)$ a *locally ringed space.*

A morphism of ringed spaces $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ induces, for every $P \in X$, a homomorphism $f_P^\# : \mathcal{O}_{Y,f(P)} \to \mathcal{O}_{X,P}$ in the obvious way. If $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are locally ringed spaces, then $(f, f^\#)$ is called a *morphism of locally ringed spaces* if ${f_P^\#}^{-1}(\mathfrak{m}_{X,P}) = \mathfrak{m}_{Y,f(P)}$ for every $P \in X$, where $\mathfrak{m}_{X,P}$ and $\mathfrak{m}_{Y,f(P)}$ denote the maximal ideals of $\mathcal{O}_{X,P}$ and $\mathcal{O}_{Y,f(P)}$ respectively.

If $(X, \mathcal{O}_X)$ is a locally ringed space and $P \in X$, we call $\mathcal{O}_{X,P}/\mathfrak{m}_{X,P}$ the *residue field of* $P \in X$.

We call a morphism $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ an *open immersion of locally ringed spaces*, if f is an homeomorphism between X and an open subset of Y, and if $f_P^\#$ is a isomorphism for every $P \in X$.
We call a morphism $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ a *closed immersion of locally ringed spaces*, if f is an homeomorphism between X and a closed subset of Y, and if $f_P^\#$ is surjective for every $P \in X$.
By $\dim(X, \mathcal{O}_X)$ we denote the dimension of the topological space X, i.e. the supremum over the $n \in \mathbb{N}$ such that there exist nonempty closed irreducible subsets $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n \subseteq X$.

Affine schemes. Let A be a ring. The set of proper prime ideals of A is denoted $\operatorname{Spec}(A)$. The Zariski topology on $\operatorname{Spec}(A)$ is given by defining those subsets $V(\mathfrak{a})$, consisting of the prime ideals that contain a given ideal $\mathfrak{a} \subseteq A$, to be closed. A basis for the open sets of $\operatorname{Spec}(A)$ is therefore, for each $f \in A$, the set $D(f)$ of prime ideals not containing f, which is homeomorphic to $\operatorname{Spec}(A_f)$, where A_f denotes the localization of A with respect to the multiplicative set $\{1, f, f^2, \dots\}$. For an arbitrary open subset $U \subseteq \operatorname{Spec}(A)$, we set $\mathcal{O}_{\operatorname{Spec}(A)}(U)$ to be the subring of

$$\prod_{\mathfrak{q} \in U} A_{\mathfrak{q}}$$

consisting of tuples $(\pi_{\mathfrak{q}})_{(\mathfrak{q} \in U)}$ such that, for each $\mathfrak{q} \in U$, there exist $a, f \in A$, $f \notin \mathfrak{q}$, such that $\pi_{\mathfrak{p}} = \frac{a}{f}$ in $A_{\mathfrak{p}}$ for all $\mathfrak{p} \in U \cap D(f)$. The

restriction homomorphisms $\mathcal{O}_{\operatorname{Spec}(A)}(W) \to \mathcal{O}_{\operatorname{Spec}(A)}(U)$ for open $U \subseteq W \subseteq \operatorname{Spec}(A)$ are defined in the obvious manner.
This definition makes $(\operatorname{Spec}(A), \mathcal{O}_{\operatorname{Spec}(A)})$ a locally ringed space, see [**Har83**, II.2.3 (a)]. More precisely, one can show that $\mathcal{O}_{\operatorname{Spec}(A),\mathfrak{p}} \cong A_{\mathfrak{p}}$ for any $\mathfrak{p} \in \operatorname{Spec}(A)$, and moreover that $\mathcal{O}_{\operatorname{Spec}(A)}(D(f)) \cong A_f$ for any $f \in A$, see [**Har83**, II.2.2].
One calls a locally ringed space as just described an *affine scheme*. One often just writes $\operatorname{Spec}(A)$ for the affine scheme $(\operatorname{Spec}(A), \mathcal{O}_{\operatorname{Spec}}(A))$, as the data of the sheaf $\mathcal{O}_{\operatorname{Spec}(A)}$ is completely given by the ring A. The morphisms of locally ringed spaces between two affine schemes $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ are in one-to-one correspondence with the ring homomorphisms $A \to B$, where a ring homomorphism induces the topological map by taking inverse images of prime ideals under the ring homomorphism, and the morphisms on the sheaves are simply the natural continuation of the ring homomorphisms to localizations.

Arbitrary schemes. An arbitrary locally ringed space $(X, \mathcal{O}_X)$ is called a *scheme* if, for each $P \in X$, there exists an open neighbourhood U of P such that $(U, \mathcal{O}_X|_U)$ is isomorphic (as a locally ringed space) to an affine scheme. When the structure sheaf $\mathcal{O}_X$ is understood, we sometimes just write X for the scheme. Typical examples for schemes that are not affine schemes are *projective schemes*, which are defined as follows.

EXAMPLE 3.6. Let $A = \bigoplus_{n\in\mathbb{N}} A_n$ be a graded ring. By $\operatorname{Proj}(A)$, we denote the set of proper homogeneous prime ideals not containing the so-called irrelevant ideal $\bigoplus_{n>0} A_n$. The Zariski topology on $\operatorname{Proj}(A)$ is given by defining those subsets $V_+(\mathfrak{a})$, consisting of homogeneous prime ideal that contain a given homogeneous ideal $\mathfrak{a} \subseteq A$, to be closed. The open subsets of this topology have as a basis the sets $D_+(f)$, consisting of those $\mathfrak{p} \in \operatorname{Proj}(A)$ that do not contain the given homogeneous element $f \in A$. For any $\mathfrak{q} \in \operatorname{Proj}(A)$, we define $A_{\mathfrak{q}}^{(0)}$ to be the formal fractions $\frac{a}{b}$ of homogeneous elements $a, b \in A$ of the same degree, inside the localization of A with respect to the multiplicative set of the homogeneous elements that are not contained in $\mathfrak{q}$. This is obviously a local ring, with the maximal ideal consisting of those fractions of homogeneous elements of same degree whose denominator lies in $\mathfrak{q}$. For any open set $U \subseteq \operatorname{Proj}(A)$, we set $\mathcal{O}_{\operatorname{Proj}(A)}(U)$ to be the subring of $\prod_{\mathfrak{q}\in U} A_{\mathfrak{q}}^{(0)}$ consisting of elements $(\pi_{\mathfrak{q}})_{\mathfrak{q}\in U}$ such that for each $\mathfrak{p} \in U$, there exist homogeneous $a, f \in A$ of the same degree with $f \notin \mathfrak{p}$ such that $\pi_q = \frac{a}{f}$ in $A_{\mathfrak{q}}^{(0)}$ for each $\mathfrak{q} \in U \cap D_+(f)$. This makes $(\mathrm{Proj}(A), \mathcal{O}_{\mathrm{Proj}(A)})$ a locally ringed space. More precisely, [**Eis95**, II.2.5] shows that $\mathcal{O}_{(\mathrm{Proj}(A),\mathfrak{p})} \cong A_{\mathfrak{q}}^{(0)}$ for any $\mathfrak{q} \in \mathrm{Proj}(A)$ and that, for any homogeneous $f \in A$, the open locally ringed subspace $(D_+(f), \mathcal{O}_{\mathrm{Proj}(A)}|_{D_+(f)})$ is isomorphic to the affine scheme

$$(\mathrm{Spec}(A_f^{(0)}), \mathcal{O}_{\mathrm{Spec}(A_f^{(0)})}),$$

where $A_f^{(0)}$ is the subring of A_f consisting of fractions of elements of same degree. This shows that $(\mathrm{Proj}(A), \mathcal{O}_{\mathrm{Proj}(A)})$ is a scheme.

EXAMPLE 3.7. Let A be a ring and $A[x_0, \dots, x_n]$ the polynomial ring endowed with the total degree grading. We call $\mathrm{Proj}(A[x_0, \dots, x_n])$ the projective n-space over A, denoted $\mathbb{P}_A^n$.

A scheme X is called ...

... *irreducible* if its topological space is irreducible.
... *reduced* if for every open subset $U \subseteq X$ the ring $\mathcal{O}_X(U)$ is a reduced ring.
... *integral* if for every nonempty open subset $U \subseteq X$ the ring $\mathcal{O}_X(U)$ is an integral domain.
... *Noetherian* if it is quasicompact and each $P \in X$ has an open neighbourhood that is isomorphic to the spectrum of a Noetherian ring.

In [**Har83**, II.3.1], it is shown that a scheme is integral if and only if it is irreducible and reduced.

Dimension, regularity, and function fields. A scheme X is called *normal at* $P \in X$ if $\mathcal{O}_{X,P}$ is a normal domain. X is called *normal* if it is normal in every point. A Noetherian scheme X is called *regular at the point* $P \in X$, if $\mathcal{O}_{X,P}$ is a regular local ring. It is called *regular* if it is regular in every point of X. If, moreover, X is a Noetherian scheme, then regularity of X is equivalent to regularity in every closed point of X.

If X is a Noetherian scheme and $P \in X$, then the Krull-dimension of $\mathcal{O}_{X,P}$ is finite and coincides with the codimension of $\overline{\{P\}}$ in X. We denote by $X^{(n)}$ the set of points of codimension n in X.

If $P \in X$ is a regular point of codimension one, then $\mathcal{O}_{X,P}$ is a discrete valuation ring. Every irreducible closed subset $Y \subseteq X$ of a scheme X has a unique generic point $\eta \in X$, that is, a point $\eta \in X$ such that $\overline{\{\eta\}} = Y$.

Let X be a nonempty irreducible scheme and $\eta \in X$ its generic point. Then we call $\mathcal{O}_{X,\eta}/\mathfrak{m}_{X,\eta}$ the *function field of* X, denoted $\kappa(X)$. If X is integral and $\operatorname{Spec}(A) \subseteq X$ is a nonempty open affine subscheme, then $\kappa(X) = \operatorname{Quot}(A)$.

Morphisms of schemes. Let X, Y denote two schemes. A morphism $f : X \to Y$ of locally ringed spaces is called a *morphism of schemes*.
If A and B are rings, then the homomorphisms of rings $A \to B$ are in one-to-one correspondence with the morphisms of schemes

$$\operatorname{Spec}(B) \to \operatorname{Spec}(A),$$

see [**Har83**, II.2.3]. The topological map on the spectras is induced by taking preimages of prime ideals under the respective ring homomorphism.

Example 3.8 (open subschemes & open immersions). An open subscheme of a scheme Y is an open subset U together with the restricted sheaf $\mathcal{O}_Y|_U$. We call a morphism $f : X \to Y$ an *open immersion* if it is an open immersion of locally ringed spaces, whereby f induces an isomorphism between X and an open subscheme of Y.

Example 3.9 (closed immersions & closed subschemes). A morphism of schemes $f : X \to Y$ is called a *closed immersion* if it is a closed immersions of locally ringed spaces. A *closed subscheme* of a scheme Y is an equivalence class of closed immersions $f : X \to Y$, where two closed immersions $f : X \to Y$ and $f' : X' \to Y$ are equivalent if there exists an isomorphism of schemes $\iota : X \to X'$ such that $f' \circ \iota = f$. The subscheme is represented by X.

If $Y = \operatorname{Spec}(A)$ is an affine scheme, then there exists a one-to-one correspondence between ideals $\mathfrak{a}$ of A and closed subschemes X of Y, and the closed immersion $X \to Y$ comes (up to an isomorphism) from the ring homomorphism $A \to A/\mathfrak{a}$.
If $Y = \operatorname{Proj}(A)$ for a graded ring A, then every closed subscheme X of the projective scheme Y comes from a homogeneous ideal $\mathfrak{a} \in \operatorname{Proj}(A)$, and the closed immersion $X \to Y$ is given (up to an isomorphism) by the graded ring homomorphism $A \to A/\mathfrak{a}$.
Letting X be a closed subset of a scheme Y, we can endow X with the structure of a reduced subscheme, called the *subscheme with the induced reduced structure* and denoted X_{red}, see [**Har83**, II.3.2.6]. If $Y = \operatorname{Spec}(A)$ and $X = V(\mathfrak{a})$, for some ideal $\mathfrak{a}$ in A, then $X_{\mathrm{red}} = \operatorname{Spec}(A/\sqrt{\mathfrak{a}})$, where $\sqrt{\mathfrak{a}}$ denotes the radical ideal of $\mathfrak{a}$.

REMARK 3.10 (restricting morphisms). Letting $f : X \to Y$ be a morphism of schemes and Z a subscheme (open or closed) of X with a given immersion (open or closed) $\gamma : Z \to X$, we call $f \circ \gamma$ the *restriction of f to Z*, denoted $f|_Z$.

LEMMA 3.11. *Let $f : X \to Y$ be a morphism of schemes. Suppose $U \subseteq Y$ is an open subscheme with $f(X) \subseteq U$. There exists a unique morphism $g : X \to U$ such that $f = \gamma \circ g$, where $\gamma : U \hookrightarrow Y$ is the open immersion corresponding to the open subscheme structure $U \subseteq Y$.*

PROOF. The map $g : X \to U, x \mapsto f(x)$ is a continous map. For any $W \subseteq U$ open, define $g^{\#}_W : \mathcal{O}_U(W) \to \mathcal{O}_X(g^{-1}(W)), r \mapsto f^{\#}_W(r)$. This yields a morphism of locally ringed spaces $(g, g^{\#}) : (X, \mathcal{O}_X) \to (U, \mathcal{O}_U)$. The uniqueness of g is clear. □

NOTATION 3.12. Let $f : X \to Y$ be a morphism and $U \subseteq X$ an open subscheme such that $f(X) \subseteq U$. Then we denote $g : X \to U$ as in (3.11) by $f|^U = g$.

LEMMA 3.13. *Let X be a reduced scheme, $f : X \to Y$ a morphism and $Z \subseteq Y$ a closed reduced subscheme such that $f(X) \subseteq Z$. Let $\gamma : Z \hookrightarrow Y$ be a closed immersion with respect to the subscheme structure of Z in Y. Then there exists a unique morphism $g : X \to Z$, such that $f = \gamma \circ g$.*

PROOF. Let us first assume that $Y = \operatorname{Spec}(A)$ and $X = \operatorname{Spec}(B)$ are affine. Then $Z = \operatorname{Spec}(A/\mathfrak{a})$ for some radical ideal $\mathfrak{a}$ of A. The morphism $f : X \to Y$ corresponds to a ring homomorphism $f^* : A \to B$ such that $\mathfrak{a} \subseteq (f^*)^{-1}(\mathfrak{p})$ for every prime ideal $\mathfrak{p} \in \operatorname{Spec}(B)$. Hence $\mathfrak{a} \subseteq \ker(f^*)$, since $\{0\} \subseteq B$ is the intersection of all prime ideals by assumption that B is reduced. Hence $A \to B$ factors via $g^* : A/\mathfrak{a} \to B$. The canonical ring morphism $\gamma^* : A \to A/\mathfrak{a}$ induces $\gamma : Z \hookrightarrow Y$. The ring homomorphism g^* induces $g : X \to Z_{\text{red}}$.
Now we only assume that Y is affine. Let $X_1 \cup \cdots \cup X_r = X$ be an open affine cover. Then the hypothesis applies to $f|_{X_i}$ for $1 \leq i \leq r$. Let $g_i : X_i \to Z$ the morphisms such that $f|_{X_i} = \gamma \circ g_i$, which exist by the previous consideration. It follows that $\gamma \circ g_i|_{X_i \cap X_j} = \gamma \circ g_j|_{X_i \cap X_j}$ for $\leq i, j \leq r$, and since γ is a closed immersions, i.e. injective as a topological map and such that $\gamma^{\#}$ is a surjective map on the sheafs, it follows that $g_i|_{X_i \cap X_j} = g_j|_{X_j \cap X_i}$ for $1 \leq i, j \leq r$. One can glue the morphisms g_i together to form one morphism $g : X \to Z$, (cf. [**Har83**, p.88]). The uniqueness of g follows from the uniqueness of the restrictions to the affine parts.

Finally, assume that $Y = Y_1 \cup \cdots \cup Y_r$ is an affine open cover of Y. Write $X_i = f^{-1}(Y_i)$ for $1 \leq i \leq r$. Write $Z_i = Y_i \cap Z$. Note that $f|_{X_i}^{Y_i}(X_i) \subset Z_i$. By the previous considerations, there exists, for each $1 \leq i \leq r$, a morphism $g_i : X_i \to Z_i$ such that $f|_{X_i}^{Y_i} = \gamma_i \circ g_i$, where $\gamma_i = \gamma|_{Z_i}^{Y_i}$. Hence $f|_{X_i} = \gamma|_{Z_i} \circ g_i$. Write $\tilde{g}_i$ for $\delta_i \circ g_i$, where $\delta_i : Z_i \hookrightarrow Z$ is the open immersion. Then $f|_{X_i} = \gamma \circ \tilde{g}_i$. By the same arguments, we can show that $\tilde{g}_i|_{X_i \cap X_j} = \tilde{g}_j|_{X_i \cap X_j}$ for $1 \leq i, j \leq r$, and thus we can glue the $\tilde{g}_i$ to form one morphism $g : X \to Z$ such that $f = \gamma \circ g$. □

NOTATION 3.14. Let X be a reduced scheme, $f : X \to Y$ a morphism and $Z \subset Y$ a closed reduced subscheme such that $f(X) \subseteq Z$. Then we denote $g : X \to Z$ as in (3.13) by $f|^Z$.

Finite morphisms. A morphism $f : X \to Y$ of schemes is called *finite* if, for every affine open subscheme Y' of Y, the open subscheme $f^{-1}(Y') \subset X$ is affine and, moreover, $\mathcal{O}_X(f^{-1}(Y'))$ is a finitely generated $\mathcal{O}_Y(Y')$-module, see [**Har83**, p.84]. Equivalently, one could require these conditions for an arbitrary covering of Y by affine open subschemes $(Y_i)_{i \in I}$. With this in mind, one can easily conclude the following facts about finite morphisms.

REMARK 3.15. The composition $f \circ g$ of two finite morphisms f, g is again finite. Conversely, if the composition $f \circ g$ of two morphisms f, g is finite, and moreover f is finite, then so is g.

EXAMPLE 3.16. Every closed immersion $f : X \to Y$ is a finite morphism. This follows from the fact that every closed subscheme of an affine scheme is again affine. Let $\mathrm{Spec}(A) \subset Y$ be an affine open subscheme. Let $X' = f^{-1}(\mathrm{Spec}(A))$. One can restrict the morphism of locally ringed spaces to the open subsets, thereby inducing a closed immersion of schemes $f' : X' \to \mathrm{Spec}(A)$. The equivalence class of this closed immersion is a closed subscheme of $\mathrm{Spec}(A)$. Hence, up to an isomorphism, f' is given by the ring homomorphism $A \to A/\mathfrak{a}$ for some ideal $\mathfrak{a}$ of A, and thus $X \cong \mathrm{Spec}(A/\mathfrak{a})$ is affine.

LEMMA 3.17. *Let $f : X \to Y$ be a finite morphism. Then f is a closed topological map, and $f^{-1}(\{y\})$ is a finite set of closed points for each closed point $y \in Y$.*

PROOF. An affine cover $(Y_i)_{i \in Y}$ of Y yields an affine open cover $(X_i)_{i \in I}$ of X, with $X_i = f^{-1}(Y_i)$. Let V be a closed subset of X. For $i \in I$ set $V_i = V \cap X_i$. To show that f is a closed topological map, it is sufficient to show that $W_i = f|_{X_i}^{Y_i}(V_i)$ is relatively closed in Y_i. Since $f|_{X_i}^{Y_i}$ is a

finite morphism of affine varieties, it corresponds to a finite extension of rings $A_{Y_i} \hookrightarrow A_{X_i}$. By assumption, $V_i = V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of A_{X_i}. We let $\mathfrak{b}$ denote $A_{Y_i} \cap \mathfrak{a}$. We claim that $W_i = V(\mathfrak{b})$ in $\mathrm{Spec}(A_{Y_i})$. It is clear that $W_i \subseteq V(\mathfrak{b})$. The reverse inclusion, $V(\mathfrak{b}) \subset W_i$, follows from a 'lying over and going down' result for integral extensions, see [**Eis95**, 4.4.15].
The second assertion, that $f^{-1}(\{y\})$ is a finite set of closed points for each closed point $y \in Y$, can be shown as follows. Since $y \in Y_i$ for some $i \in I$, we know that $y = \mathfrak{p}$ for some maximal ideal $\mathfrak{p} \subset A_{Y_i}$. Let $\mathfrak{a} = \mathfrak{p}A_{X_i}$. Then $B = A_{X_i}/\mathfrak{a}$ is finite dimensional vector space over $k = A_{Y_i}/\mathfrak{p}$. Let $\mathfrak{m} \subset B$ be a prime ideal such that $\mathfrak{m} \cap k = \{0\}$. Then $B/\mathfrak{m}$ is a finitely generated integral ring extension that is finite dimensional over k, and hence a field, whereby $\mathfrak{m}$ is a maximal ideal. Let $\mathfrak{m}_1, \dots, \mathfrak{m}_n \subset B$ be finitely many such maximal ideals and $\mathfrak{b} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. By the Chinese remainder theorem we have that $B/\mathfrak{b} \cong B\mathfrak{m}_1 \times \cdots \times B/\mathfrak{m}_n$, which is a finite dimensional k-vector space whose dimension is bounded by that of $B/\mathfrak{a}$. Hence n is bounded as well. All this together, shows that $f^{-1}(\{y\})$ is a finite set of closed points. □

Remark 3.18. Let $f : X \to Y$ be a finite morphism. If $Z \subset X$ is a closed subscheme, then $f|_Z$ is finite. If X is reduced and $Z \subset Y$ is a closed reduced subscheme with $f(X) \subseteq Z$, then $f|^Z$ is a finite morphism, as well. Both properties follow from (3.15) and the fact that closed immersions are finite.

Example 3.19. Let A be a ring and $n, d \in \mathbb{N}$. Denote by $N+1$ the number of distinct monomials of degree d in the $n+1$ variables $x_0, \dots, x_n$. Let ι denote a bijection between the set $\{0, \dots, N\}$ and the monomials in $x_0, \dots, x_n$ of total degree d. Consider the graded homomorphism of rings $\iota_d^* : A[y_0, \dots, y_N] \to A[x_0, \dots, x_n]$ defined by $y_i \mapsto \iota(i)$. This graded morphism induces a morphism of schemes $\iota_d : \mathbb{P}^n_A \to \mathbb{P}^N_A$, which is a closed immersion and is called the *d-uple embedding*, (cf. [**Liu06**, 5.1, Exercise 27]). As a closed immersion, it is in particular a finite morphism.

Example 3.20. Let $r \leq n \in \mathbb{N}$ and let $L_0, \dots, L_r \in A[x_0, \dots, x_n]$ be linear homogeneous polynomials. Consider the projection

$$\pi : \mathbb{P}^n_A \setminus V_+(L_0, \dots, L_r) \to \mathbb{P}^r_A$$

defined as follows: $\mathbb{P}^n_A \setminus V_+(L_0, \dots, L_r) = D_+(L_0) \cup \cdots \cup D_+(L_r)$ and $\mathbb{P}^r_A = D_+(y_0) \cup \cdots \cup D_+(y_r)$ for $\mathbb{P}^r_n = \mathrm{Proj}(A[y_0, \dots, y_r])$.

Consider, for $0 \le m \le r$, the ring morphisms

$$\pi_m^* : A\left[\frac{y_0}{y_m}, \dots, \frac{y_r}{y_m}\right] \longrightarrow A\left[\frac{x_0}{L_m}, \dots, \frac{x_n}{L_m}\right]$$
$$\frac{y_i}{y_m} \mapsto \frac{L_i}{L_m}.$$

The induced morphisms of schemes $\pi_m : D_+(L_m) \to D_+(y_m) \hookrightarrow \mathbb{P}_A^r$ coincide on overlaps, i.e. $\pi_m|_{D_+(L_m L_k)} = \pi_k|_{D_+(L_m L_k)}$, whereby one can glue the morphisms together to obtain π. Letting $Z \hookrightarrow \mathbb{P}_A^n$ be closed subscheme that is disjoint from $V_+(L_0, \dots, L_r)$, we have that $\pi|_Z$ is a finite morphism by [**Mum99**, II.7, Prop. 6].

Fibered product and base change. For a fixed scheme S, one can consider the category of schemes over S, that is, the category whose objects are morphisms of schemes $f_X : X \to S$. We sometimes refer to X as a *scheme over* S and keep the so-called *structure morphism* f_X in mind. A morphism in this category is given as follows. Let $f_X : X \to S$ and $f_Y : Y \to S$ be two schemes over S (or S-schemes). A morphism of schemes $g : X \to Y$ is called a *morphism of* S*-schemes*, if $f_X = f_Y \circ g$. If $S = \text{Spec}(A)$ for a ring A, we say A*-scheme* and A*-morphism* instead of Spec(A)-schemes and Spec(A)-morphism.

Let $f_X : X \to S$ and $f_Y : Y \to S$ be two S-schemes. Then there exists a triple consisting of an S-scheme $f_Z : Z \to S$ and two S-morphisms $\pi_X : Z \to X$ and $\pi_Y : Z \to Y$, such that the following holds:
For any other S-scheme $f_{Z'} : Z' \to S$ together with two S-morphisms $\pi'_X : Z' \to X$ and $\pi'_Y : Z' \to Y$, there exists a unique S-morphism $\varphi : Z' \to Z$ such that $\pi_X \circ \varphi = \pi'_X$ and $\pi_Y \circ \varphi = \pi'_Y$.
(Z, π_X, π_Y) is called the *fibered product of* X *and* Y *over* S, denoted by $X \times_S Y$, and π_X and π_Y are referred to as projections.
The triple (Z, π_X, π_Y) is unique up to a unique S-isomorphism that makes the projections and ths structure morphisms to S commute.
The existence and uniqueness of the fibered product is shown (e.g.) in [**Har83**, II.3.3]. In the case where $X = \text{Spec}(R_1)$, $Y = \text{Spec}(R_2)$ and $S = \text{Spec}(A)$ are affine schemes, then $X \times_S Y$ is known to be $\text{Spec}(R_1 \otimes_A R_2)$.

The fibered product $X \times_S Y$ is sometimes referred to as the *base change of the* S*-scheme* X *to the base* Y, denoted X_Y, with the second projection π_Y considered to be the new structure morphism.

EXAMPLE 3.21. Each scheme S has a natural structure homomorphism to $\mathrm{Spec}(\mathbb{Z})$. We define the *projective n-space over S*, denoted $\mathbb{P}^n_S$, to be

$$\mathrm{Proj}(\mathbb{Z}[X_0,\dots,X_n]) \times_{\mathrm{Spec}(\mathbb{Z})} S.$$

The second projection morphism of the fibered product makes this an S-scheme. Note that if $S = \mathrm{Spec}(A)$ for some ring A, then $\mathbb{P}^n_S = \mathrm{Proj}(A[X_0,\dots,X_n]) = \mathbb{P}^n_A$, the projective n-space over A as defined in (3.6).

Let X be an S-scheme and $p \in S$. Denote $\kappa(p) = \mathcal{O}_{S,p}/\mathfrak{m}_{S,p}$. The natural homomorphisms $\mathcal{O}_S(U) \to \mathcal{O}_{S,p} \to \kappa(p)$ for every open neighbourhood $U \subset S$ of p gives rise to a morphism of scheme $\mathrm{Spec}(\kappa(p)) \to S$ (note that together with the zero maps $\mathcal{O}_S(U) \to \{0\}$ for the open non-neighbourhoods U of p, we have a morphism of sheaves). The *fiber of p* is defined to be $X_p = X \times_S \mathrm{Spec}(\kappa(p))$. The local homomorphism $\mathcal{O}_{S,p} \to \mathcal{O}_{\mathrm{Spec}(\kappa_p),(0)} = \kappa(p)$ is obviously surjective and, in addition, it is injective if S is integral and $p \in S$ is the generic point. This shows that if $p \in S$ is a closed point, then $\mathrm{Spec}(\kappa(p)) \to S$ is a closed immersion and, if S is integral and its generic point p is such that $\{p\} \subseteq S$ is open (it is for example the case if S is the spectrum of a discrete valuation ring), then $\mathrm{Spec}(\kappa(p)) \to S$ is an open immersion.
One can show for arbitrary $p \in S$, that the topological space of X_p is homeomorphic to $f^{-1}(\{p\})$. The homeomorphism being the topological map of the projection $X \times_S \kappa(p) \to X$, see [**Liu06**, 3.1.16].
In case $p \in S$ is a closed point, i.e. $\overline{\{p\}} = \{p\}$, then we call X_p *a closed fiber of X/S*, or the *special fiber of X/S* if p is the only closed point in S. If S is irreducible and $p \in S$ the generic point of S, i.e. $\overline{\{p\}} = S$, then we call X_p the *generic fiber of X/S*.

REMARK 3.22. If $p \in S$ is a closed point, then the projection morphism $X_p = X \times_S \mathrm{Spec}(\kappa(p)) \to X$ is a closed immersion, as $\mathrm{Spec}(\kappa(p)) \to S$ is, with closed immersions beeing stable under base change, see [**Liu06**, 3.1.23].

LEMMA 3.23. *Let $f : X \to S$ be a morphism, $p \in S$ a closed point, and let $P \in X_p$. Then $\mathcal{O}_{X,P}/\mathfrak{m}_{X,P} \cong \mathcal{O}_{X_p,P}/\mathfrak{m}_{X_p,P}$.*

PROOF. We have $X_p = X \times_S \mathrm{Spec}(p)$, where $\kappa(p) = \mathcal{O}_{S,p}/\mathfrak{m}_{S,p}$. The closed immersion $\pi_X : X_p \to X$, given by the projection of the fibered product, is considered as a topological embedding. By the property of closed immersions, we have that the local homomorphism $\pi_P^\# : \mathcal{O}_{X,P} \to \mathcal{O}_{X_p,P}$ is surjective. Hence, $\mathcal{O}_{X,P}/\mathfrak{m}_{X,P} \cong \mathcal{O}_{X_p,P}/\mathfrak{m}_{X_p,P}$. □

Further properties of morphisms. We say a morphism $f : X \to Y$ is …

… *locally of finite type* if, for every open affine subscheme Y' of Y, there exists an open affine cover $(X_i)_{i\in I}$ of $f^{-1}(Y')$ such that the $\mathcal{O}_X(X_i)$ are finitely generated $\mathcal{O}_X(Y')$-algebras. If, moreover, the cover can be chosen to be finite, then one calls it *of finite type*, (see [**Har83**, p. 84]).

… *projective* if for some $n \in \mathbb{N}$ there exists a closed immersion $g : X \to \mathbb{P}^n_Y$ such that $f = \pi_Y \circ g$, where $\pi_Y : \mathbb{P}^n_Y \to Y$ is the projection of the fibered product. See [**Har83**, p.103].

Remark 3.24. Projective morphisms are of finite type.
This can be seen as follows: A projective morphism $f : X \to Y$ can be factored via a closed immersion $X \hookrightarrow \mathbb{P}^n_Y$ and the projection $\mathbb{P}^n_Y \to Y$. Following [**Har83**, II, Exercise 3.13], one can show that closed immersions are of finite type, and that compositions of morphisms of finite type are of finite type. The projection $\mathbb{P}^n_Y \to Y$ is of finite type. To see this, let $\operatorname{Spec}(B)$ be any open affine subset of Y. Its inverse image under the projection is $\operatorname{Proj}(\mathbb{Z}[x_0, \ldots, x_n]) \times_{\operatorname{Spec}(\mathbb{Z})} \operatorname{Spec}(B)$. This set can be covered by the finitely many open affine subschemes $U_i = \operatorname{Spec}(B[\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}])$ for $0 \le i \le n$. The rings $\mathcal{O}_{\mathbb{P}^n_Y}(U_i) = B[\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}]$ are finitely generated B-algebras. Thus $f : X \to Y$ is of finite type.

Remark 3.25. If $f : X \to Y$ is a projective morphism and Y is Noetherian, then f is *universally closed*, that is, $\pi_{Y'} : X \times_Y Y' \to Y'$ is a closed topological map for every base change with respect to $Y' \to Y$. In particular f is a closed topological map, since $f = \pi_Y$ for the trivial base change $X = X \times_Y Y$ with respect to $\mathrm{id}_Y : Y \to Y$. This is [**Har83**, II.4.9]. Note that X is automatically Noetherian, as $f : X \to Y$ is of finite type, by (3.24).

We sometimes call a scheme X over an affine scheme $S = \operatorname{Spec}(A)$, for a ring A, a *scheme over* A. If the structure morphism $f : X \to S$ has a certain property $\mathcal{P}$ as the ones listed above, we say X is a scheme of property $\mathcal{P}$ over S (respectively A). If X and Y are two S-schemes, then an S-*morphism* (respectively A-*morphism*) $f : X \to Y$ is a morphism of schemes that commutes with the structure morphisms to S.

Divisors. In the following, we define divisors only for regular Noetherian integral schemes, which makes the objects look simpler than in general, because Weil-divisors are Cartier-divisors in this case, see [**Liu06**, 7.2.16].

Let X be a regular Noetherian integral scheme. Recall that $X^{(1)}$ denotes the set of codimension one points in X. A *divisor on* X is a formal sum

$$D = \sum_{x \in X^{(1)}} n_x[x],$$

where $n_x \in \mathbb{Z}$ is zero for all but finitely many $x \in X^{(1)}$. If $n_x \geq 0$ for all $x \in X^{(1)}$, we call D an *effective divisor.* Let F denote the function field of X. Note that every $x \in X^{(1)}$ defines a discrete valuation $v_x : F \to \mathbb{Z} \cup \{\infty\}$. The set $\mathrm{supp}(D) = \{x \in X^{(1)} \mid n_x \neq 0\}$ is called the *support of the divisor D.*

A divisor $D = \sum_{x \in X^{(1)}} n_x[x]$ on X defines a sheaf $\mathcal{O}_X(D)$ of $\mathcal{O}_X$-modules. For any open subset $U \subset X$ one sets

$$\mathcal{O}_X(D)(U) = \{f \in F \mid \forall x \in U \cap X^{(1)} : v_x(f) \geq -n_x\}.$$

The stalk

$$\mathcal{O}_X(D)_P = \varinjlim_{\text{open } U \ni P} \mathcal{O}_X(D)(U)$$

in $P \in X$ is an $\mathcal{O}_{X,P}$-module.

For $f \in F^\times$, the divisor $\mathrm{div}(f) = \sum_{x \in X^{(1)}} v_x(f)[x]$ is called a *principal divisor on* X. In this case, we have $\mathcal{O}_X(\mathrm{div}(f)) = f^{-1}\mathcal{O}_X$. The following statement says, that locally, every divisor is a principal divisor.

PROPOSITION 3.26. *For every divisor D on X, there exists an open covering $X = \bigcup_{i=1}^m U_i$ and $f_1, \ldots, f_m \in F$, such that $D|_{U_i} = \mathrm{div}(f_i)|_{U_i}$ and $f_i \in f_j\mathcal{O}_{U_i \cap U_j}^\times$ for all i, j. Conversely every covering $(U_i, f_i)_i$, subject to these conditions, yields a divisor D on X. Moreover, any two such coverings $(U_i, f_i)_i$ and $(W_j, g_j)_j$ yield the same divisor if and only if $f_i \in g_j\mathcal{O}_X^\times(U_i \cap W_j)$ for all i, j.*

PROOF. We first show that locally every divisor D is a principal divisor. Let us first consider the case where $D = [x]$ for some $x \in X^{(1)}$. We claim that for every $P \in X$ there exists an open affine neighbourhood U_P of P such that $x = f_P\mathcal{O}_X(U_P) \in \mathrm{Spec}(\mathcal{O}_X(U_P)) = U_P$, i.e. $D|_{U_P} = \mathrm{div}(f_P)|_{U_P}$. Since x is contained in every affine open neighbourhood U of P and since $\mathcal{O}_{X,P}$ is the direct limit over $\mathcal{O}_X(U)$ of all affine open neighbourhoods of P, the prime ideals $\mathfrak{p}_U \subset \mathcal{O}_X(U)$ corresponding to the codimension one point $x \in U$ form a direct system of height one prime ideals whose direct limit $\mathfrak{p}$ is a height one prime ideal in $\mathcal{O}_{X,P}$. As X is regular, $\mathfrak{p} = f_P\mathcal{O}_{X,P}$ is a principal ideal. One can easily verify that there exists an open affine neighbourhood U_P of P such that $f_P \in \mathcal{O}_X(U_P)$ is prime and $f_P\mathcal{O}_X(U_P)\mathfrak{p}_{U_P} = x \in U_P$. Hence we obtain a covering $\{(U_P, f_P) \mid P \in X\}$ with the desired properties. As X is a Noetherian topological space, there exists a finite subcovering. When $D = \sum_{x\in \mathrm{supp}(D)} n_x[x]$ is arbitrary, one first considers for each $x \in \mathrm{supp}(D)$ as above the coverings $\{(U_P^x, f_{x,P}) \mid P \in X\}$, then one considers the covering $\{(W_P, f_P) \mid P \in X\}$, where

$$W_P = \bigcap_{x\in \mathrm{supp}(D)} U_P^x \quad \text{and} \quad f_P = \prod_{x\in \mathrm{supp}(D)} f_{x,P}^{n_x}.$$

Again, since X is Noetherian, we obtain a finite subcover of X. By construction, it is clear that f_P and f_Q differ only by a unit in $\mathcal{O}_X(W_P \cap W_Q)$.

Now suppose conversely that there exists a cover $(U_i, f_i)_i$ of X with $f_i \in F$ such that f_i and f_j differ only by an invertible element in $\mathcal{O}_X(U_i \cap U_j)$. For $x \in X^{(1)}$ we set $n_x = v_x(f_i)$ for any i such that $x \in U_i$. It is easy to verify that n_x is well defined. The divisor $D = \sum_{x\in X^{(1)}} n_x[x]$ is thus well defined, and if any other covering (W_j, g_j) leads to the same definition, then necessarily $v_x(f_i) = v_x(g_j)$ whenever $x \in U_i \cap W_j$. Thus f_i and g_j differ only by a unit in $\mathcal{O}_X(U_i \cap W_j)$, since otherwise, if $f_i = g_j \frac{y}{z}$ for some $y, z \in \mathcal{O}_X(U_i \cap W_j)$ not both units, then there exists a height one prime ideal $\mathfrak{p} \subset \mathcal{O}_X(U_i \cap W_j)$ containing the nonunit by (2.3) and thus $\mathrm{div}(f_i)|_{U_i\cap W_j} \neq \mathrm{div}(g_j)|_{U_i\cap W_j}$. Conversely a covering (W_j, g_j) such that f_i and g_j differ by a unit in $\mathcal{O}_X(U_i \cap W_j)$ obviously defines the same divisor. □

From the above proposition follows in particular that if (U_i, f_i) is a covering of X that defines a divisor D then $\mathcal{O}_X(D)|_{U_i} = f_i^{-1}\mathcal{O}_X|_{U_i}$, and consequently, for any point $P \in U_i$, we have $\mathcal{O}_X(D)_P = f_i^{-1}\mathcal{O}_{X,P}$.

Remark 3.27. Let $g : X \to Y$ be a dominant morphism of integral Noetherian regular schemes. Let D be an divisor on Y. Let $(U_i)_{1\le i\le m}$ be a covering of Y and $f_i \in F$ with $D|_{U_i} = \mathrm{div}(f_i)|_{U_i}$. Then the inverse image of D, denoted g^*D, is given as follows. Set $W_i = g^{-1}(U_i)$. Let $g_i \in K(X)$ denote $g_\eta^\#(f_i)$, where $\eta \in X$ is the generic point. It is clear that for $i \neq j$ we have $g_i\mathcal{O}_X^\times(W_i \cap W_j) = g_j\mathcal{O}_X^\times(W_i \cap W_j)$, since $f_i\mathcal{O}_Y^\times(U_i \cap U_j) = f_j\mathcal{O}_Y^\times(U_i \cap U_j)$. We set

$$g^*D = \sum_{x\in X^{(1)}} m_x[x],$$

where $m_x = v_x(g_i)$ if $x \in W_i$. Note that this definition is independent of the chosen cover (U_i, f_i) of Y that defines D. Note that if D is effective, then so is g^*D, and if $D = (f)$ is a principal divisor, then $g^*D = (g_\eta^\#(f))$ is as well.

We say that an effective divisor D has *normal crossing in a point* $P \in X$ of codimension n if the exist $x_1, \dots, x_n \in \mathfrak{m}_{X,P}$ such that $\mathfrak{m}_{X,P} = (x_1, \dots, x_n)$ and integers $r_1, \dots, r_n \geq 0$ such that $\mathcal{O}_X(-D)_P = x_1^{r_1} \cdots x_n^{r_n} \mathcal{O}_{X,P}$. We say that D has *normal crossing* if it has normal crossing in every point $P \in X$.

COROLLARY 3.28. *Let $f \in F^\times$. Let $D = \sum_{x \in X^{(1)}} n_x[x]$ be an effective divisor on X such that* $\operatorname{supp}(\operatorname{div}(f)) \subset \operatorname{supp}(D)$. *Let $P \in X$ a point of codimension n such that D has normal crossings P. Then there exist $x_1, \dots, x_n \in \mathfrak{m}_{X,P}$ and $\ell_1, \dots, \ell_n \in \mathbb{Z}$ such that $\mathfrak{m}_{X,P} = (x_1, \dots, x_n)$ and $f = u x_1^{\ell_1} \cdots x_n^{\ell_n}$ for some $u \in \mathcal{O}_{X,P}^\times$.*

PROOF. By definition there exist integers $r_1, \dots, r_n \geq 0$ such that $\mathcal{O}_X(-D)_P = x_1^{r_1} \cdots x_n^{r_n} \mathcal{O}_{X,P}$. We can write $f = \frac{f_1}{f_2}$ with $f_1, f_2 \in \mathcal{O}_{X,P}$ relatively prime. (Recall that $\mathcal{O}_{X,P}$ is a factorial ring.) Hence there exists a neighbourhood U of P, where the effective principal divisors $\operatorname{div}(f_1)|_U$ and $\operatorname{div}(f_2)|_U$ have disjoint support and thus $\operatorname{supp}(\operatorname{div}(f_1)|_U) \cup \operatorname{supp}(\operatorname{div}(f_2)|_U) \subset \operatorname{supp}(D|_U)$. In particular, there exists an $m \in \mathbb{N}$ such that $v_x(\frac{1}{f_i}) \geq -mn_x$ for all $x \in U \cap X^{(1)}$ and $i = 1, 2$. In particular $\frac{1}{f_i} \in \mathcal{O}_X(mD)_P = x_1^{-mr_1} \cdots x_n^{-mr_n} \mathcal{O}_{X,P}$ for $i = 1, 2$. Hence $x_1^{mr_1} \cdots x_n^{mr_n} = f_i \gamma_i$ for some $\gamma_i \in \mathcal{O}_{X,P}$ for $i = 1, 2$. Since $\mathcal{O}_{X,P}$ is factorial, unique prime factorization implies that $f_i = u_i x_1^{m_{i,1}} \cdots x_n^{m_{i,n}}$ for some $u_i \in \mathcal{O}_{X,P}^\times$ and $m_{i,j} \in \mathbb{N}$ for $i = 1, 2$, hence $f = u x_1^{\ell_1} \cdots x_n^{\ell_n}$ for some $u \in \mathcal{O}_{X,P}^\times$ and $\ell_1, \dots, \ell_n \in \mathbb{Z}$. □

3. Varieties

We call a scheme X of finite type over a field K a *K-prevariety.* A K-morphism of schemes between abstract K-prevarieties is called a *morphism of K-prevarieties.*

EXAMPLE 3.29. The affine n-space $\mathbb{A}_K^n$ over K, and the projective n-space $\mathbb{P}_K^n$ over K, are K-prevarieties. Moreover the affine K-prevarieties are exatly the closed K-subschemes of some $\mathbb{A}_K^n$, and similarly the projective K-prevarieties are the closed subschemes of some $\mathbb{P}_K^n$.

Let E/K be a field extension. We denote by $V_E = V \times_{\operatorname{Spec}(K)} \operatorname{Spec}(E)$ the base change of V to E. One can show that V_E is an E-prevariety. We denote by $\pi_E : V_E \to V$ the projection of the fibered product. We say that a point $x' \in V_E$ lies over a point $x \in E$ if $\pi(x') = x$.

A K-prevariety V is called *smooth at a point* $x \in V$ if $V_{K_{\mathrm{alg}}}$ is regular at the points $x' \in V_{K_{\mathrm{alg}}}$ lying over x. V is called smooth if it is smooth at all points. If V is smooth at a point $x \in V$, then x is a regular point of V, see [**Liu06**, 3.23]. Conversely, if K is perfect, then V is smooth if and only if it is regular, see [**Liu06**, 4.3.33]. Note that even if K is not perfect, smoothness (or regularity) of V is equivalent to smoothness (or regularity) at all closed points of V.
For $P \in V$, we denote its residue field $\kappa(P) = \mathcal{O}_{V,P}/\mathfrak{m}_{V,P}$ by $K(P)$ If V is irreducible, and $\eta \in V$ its generic point, we denote the function field $\kappa(V) = \mathcal{O}_{V,\eta}/\mathfrak{m}_{V,\eta}$ by $K(V)$.

Lemma 3.30. *Let V be an n-dimensional irreducible algebraic prevariety over K. Then its function field $K(V)/K$ is a finitely generated field extension of transcendence degree n. Moreover, V is geometrically irreducible if and only if K is relatively algebraically closed in $K(V)$.*

Proof. Let $\eta \in V$ denote the generic point. By our definition $K(V) = \mathcal{O}_{V,\eta}/\mathfrak{m}, \eta$. Let $U = \mathrm{Spec}(A)$ be an affine neighbourhood of η, and let $\eta = \mathfrak{p} \in \mathrm{Spec}(A)$, then $\mathfrak{p}$ is the unique minial prime ideal, and hence $\mathfrak{p} = \sqrt{(0)}$. Furthermore, A is a finitely generated K-algebra As $K(V) = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = \mathrm{Quot}(A/\mathfrak{p})$, it is enough to show that the finitely generated K-algebra $A/\mathfrak{p}$ has transcendence n over K. This is the case by [**Eis95**, 8.2, Thm.A], together with the fact that dimensions of V is the Krull dimension of A, which is the same as that of $A/\mathfrak{p}$. Now suppose that $K \hookrightarrow A/\mathfrak{p}$ is not relatively algebraically closed. Then, for some algebraic extension L/K, the ring $A/\mathfrak{p} \otimes_K L = A \otimes_K L/\mathfrak{p} \otimes_K L$ is a direct product of rings, whereby the radical of $\mathfrak{p} \otimes_K L$ is not a prime ideal in $A \otimes_K L$. Hence, the inverse image of the generic point in V under the projection $\pi : V : V_L \to V$ is not a unique (generic) point, whereby V_L is not irredcuible. The same conclusions backwards show that K is not relatively algebraically closed in $A/\mathfrak{p}$, if we assume that V_L is not irreducible. □

Lemma 3.31. *Let V be a K-prevariety, and $P \in V$ a closed point. Then $K(P)$ is a finite field extension of K.*

Proof. We can assume that $V = \mathrm{Spec}(R)$ for a finitely generated K-algebra. The closed point $P \in V$ corresponds to a maximal ideal $\mathfrak{P}$ in R. Then $K(P) = \mathcal{O}_{V,P}/\mathfrak{m}_{V,\mathcal{P}} \cong R/\mathfrak{P}$ as K-algebras. Since $R/\mathfrak{P}$ is a field and a finitely generated K-algebra, it is necessarily a finite field extension of K. □

Rational maps. Let V, W be two integral K-prevarieties. Consider the pairs (U, g), where $U \subset V$ are open nonempty subschemes and $f : U \to W$ morphisms of K-prevarieties. We call two such pairs (U_1, g_1) and (U_2, g_2) equivalent if $f|_{U_1 \cap U_2} = g|U_1 \cap U_2$. We call an equivalence class f a *rational map of K- prevarieties*, and write

$$f : V \dashrightarrow W.$$

We call a rational map $f : V \dashrightarrow W$ of integral K-prevarieties *dominant*, if one (or equivalently any) representative (U, g) of f is a dominant morphism. Letting $f : V \dashrightarrow W$ and $h : W \dashrightarrow X$ be dominant rational maps of K-prevarieties, we have that $h \circ f : V \dashrightarrow X$ is well defined.
We call two integral K-prevarieties V, W *birational* if there exist dominant rational maps $f : V \dashrightarrow W$ and $h : W \dashrightarrow V$, such that $h \circ f = \mathrm{id}_V$ and $f \circ h = \mathrm{id}_W$ as rational maps.
We say that an integral K-prevariety V is ...

- ... *rational*, if it is birational to $\mathbb{A}^n_K$ for some $n \in \mathbb{N}$.
- ... *unirational*, if there exists a dominant rational map $\mathbb{A}^n_K \dashrightarrow V$ of K-prevarieties for some $n \in \mathbb{N}$.
- ... *containing a rational curve*[1] if there exists a nonconstant rational map $\mathbb{A}^1_K \dashrightarrow V$.

Let V be a K-prevariety. We call a point $P \in V$ a rational point if $\mathcal{O}_{V,P}/\mathfrak{m}_{V,P} = K$. Note that rational points are necessarily closed points. We denote by $V(K)$ the set of rational points of V.

REMARK 3.32. Let $f : V \dashrightarrow W$ be a rational map of affine integral K-prevarieties. Suppose V is a closed subscheme of $\mathbb{A}^n_K$, i.e. $V = \mathrm{Spec}(K[x_1, \dots, x_n]/\mathfrak{p})$ for some prime ideal $\mathfrak{p} \subset K[x_1, \dots, x_n]$ and, similarly, suppose that $W = \mathrm{Spec}(K[y_1, \dots, y_m]/\mathfrak{q})$ for some prime ideal $\mathfrak{q} \subset K[y_1, \dots, y_n]$. Then there exist polynomials $g_0, g_1, \dots, g_m \in K[x_1, \dots, x_n]$, with $g_0 \notin \mathfrak{p}$, such that the homomorphism defined by

$$K[y_1, \dots, y_m]/\mathfrak{q} \longrightarrow (K[x_1, \dots, x_n]/\mathfrak{p})_{g_0 + \mathfrak{p}}$$
$$y_i + \mathfrak{q} \mapsto \frac{g_i + \mathfrak{p}}{g_0 + \mathfrak{p}}$$

yields a morphism $g : D(g_0 + \mathfrak{p}) \to W$ whose equivalence class as a rational map is f.

[1]Lüroth' s Theorem [**Har83**, IV.2.5.5] justifies this terminology.

Closed points and geometric points. Let $G = \mathrm{Gal}(K_{\mathrm{alg}}/K)$ denote the group of K-automorphisms on K_{alg}, i.e. the absolute Galois group of K. For any $n \in \mathbb{N}$, we consider the equivalence relation $\sim_G$ on K^n_{alg} given by: $(a_1, \ldots, a_n) \sim_G (b_1, \ldots, b_n)$ if there exists a $\sigma \in G$ such that $b_i = \sigma(a_i)$ for each $1 \le i \le n$. We denote the equivalence class of $(a_1, \ldots, a_n)$ by $(a_1, \ldots, a_n)_{\sim_G}$. Endow $K^n_{\mathrm{alg}}/\sim_G$ with the topology whose closed subsets are generated by the zero loci of n-variate polynomials over K. Then the set of closed points in $\mathbb{A}^n_K$ is homeomorphic to $K^n_{\mathrm{alg}}/\sim_G$ under the obvious identification.

Remark 3.33. In the situation of (3.32), under the above identification of closed points, the partially defined map

$$K^n_{\mathrm{alg}}/\sim_G \dashrightarrow K^m_{\mathrm{alg}}/\sim_G$$
$$(a_1, \ldots, a_n)_{\sim_G} \mapsto (\frac{g_1}{g_0}(a_1, \ldots, a_n), \ldots, \frac{g_m}{g_0}(a_1, \ldots, a_m))_{\sim_G}$$

restricted to the closed points of V where defined, coincides with the restriction of the topological map f to the closed points on V where defined.

Remark 3.34. Let V be an affine K-prevariety, that is, a closed subscheme of $\mathbb{A}^n_K$ for some $n \in \mathbb{N}$. Letting $P \in V$ be a closed point and letting $(a_1, \ldots, a_n)_{\sim_G} \in K^n_{\mathrm{alg}}/\sim_G$ correspond to P, we have that $\mathcal{O}_{V,P}/\mathfrak{m}_{V,P} \cong_K K(a_1, \ldots, a_n)$.

We can define a slightly different equivalence relation on $\left(K^{n+1}_{\mathrm{alg}}\right)_0 = K^{n+1}_{\mathrm{alg}} \setminus \{0, \ldots, 0\}$. We say that $(a_0, \ldots, a_n) \approx_G (b_0, \ldots, b_n)$ if there exists $\sigma \in G$ and $c \in K_{\mathrm{alg}}$ such that $\sigma(a_i) = cb_i$ for each $0 \le i \le n$. We write $(a_0 : \cdots : a_n)_G$ for the equivalence class of $(a_0, \ldots, a_n)$. Endow $\left(K^{n+1}_{\mathrm{alg}}\right)_0/\approx_G$ with the topology whose closed subsets are generated by the zero loci of homogeneous $n+1$-variate polynomials over K. Then the set of closed points in $\mathbb{P}^n_K$ is homeomorphic to $\left(K^{n+1}_{\mathrm{alg}}\right)_0/\approx_G$.

Remark 3.35. Let V be a K-prevariety and L/K an algebraic field extension. The projection morphism $\pi_V : V_L \to V$ maps the closed points of V_L on the closed points of V. If V is affine, there exists a closed immersion $V \hookrightarrow \mathbb{A}^n_K$ for some $n \in \mathbb{N}$. Since $\mathbb{A}^n_L = \mathbb{A}^n_K \times_{\mathrm{Spec} K} \mathrm{Spec}(L)$, we obtain a closed immersion $V_L \hookrightarrow \mathbb{A}^n_L$ that commutes with $V \hookrightarrow \mathbb{A}^n_K$ and the projections $V_L \to V$ and $\mathbb{A}^n_L \to \mathbb{A}^n_K$, by the properties of the fibered product. When we consider these morphisms just as topological maps and the schemes as topological spaces, then $V \subset \mathbb{A}^n_K$ and $V_L \subset \mathbb{A}^n_L$

and the projection $\mathbb{A}^n_L \to \mathbb{A}^n_K$ restricted to the closed points corresponds to

$$\begin{aligned} K^n_{\mathrm{alg}}/\sim_H &\longrightarrow K^n_{\mathrm{alg}}/\sim_G \\ (a_1,\dots,a_n)_{\sim_H} &\mapsto (a_1,\dots,a_n)_{\sim_G}, \end{aligned}$$

where $G = \mathrm{Gal}(K_{\mathrm{alg}}/K)$ denotes the absolute Galois group of K, and the subgroup $H = \mathrm{Gal}(K_{\mathrm{alg}}/L)$ denotes the absolute Galois group of L.

Generic splitting of quadrics and other varieties. We say a K-prevariety V has a property $\mathcal{P}$ *geometrically* if $V_{K_{\mathrm{alg}}}$ has the property $\mathcal{P}$. For example, a K-prevariety is called *geometrically integral* if $V_{K_{\mathrm{alg}}}$ is integral.

PROPOSITION 3.36. *Let L/K be a finite separable extension of infinite fields. Let V be a K-prevariety and suppose that V_L contains an L-rational curve. Then there exists a closed point $P \in V$ such that $K(P) \cong_K L$.*

PROOF. We can assume that V_L is a closed sub-prevariety of $\mathbb{A}^m_L$ for some $m \in \mathbb{N}$.
Let $\varphi : \mathbb{A}^1_L \dashrightarrow V_L$ be a nonconstant rational map. Let G denote the absolute Galois group $\mathrm{Gal}(K_{\mathrm{alg}}/K)$ of K and $H = \mathrm{Gal}(K_{\mathrm{alg}}/L)$ the absolute Galois group of L. By (3.33), φ corresponds to a partially defined map

$$\begin{aligned} K_{\mathrm{alg}}/\sim_H &\dashrightarrow K^m_{\mathrm{alg}}/\sim_H \\ a_\sim &\mapsto (\varphi_1(a),\dots,\varphi_m(a))_{\sim_H} \end{aligned}$$

where $\varphi_1,\dots,\varphi_m$ are fractions of univariate polynomials with coefficients in L. We can assume that $\varphi_1|_L : L \dashrightarrow L$ is nonconstant. By (3.5), there exists $\alpha \in L$ such that $\varphi_1(\alpha)$ is a primitive element of L/K. By (3.35), we have that $(\varphi_1(\alpha),\dots,\varphi_m(\alpha))_{\sim_G} \in V$. Then $K(P) \cong_K K(\varphi_1(\alpha),\dots,\varphi_m(\alpha)) = L$ by (3.34). □

COROLLARY 3.37. *Let L/K be a finite separable extension of infinite fields. Let V be a geometrically integral K-prevariety such that V_L is unirational. Then there exists a regular point $P \in V$ such that $K(P) \cong_K L$.*

PROOF. The subset of regular points $\mathrm{Reg}(V) \subset V$ is an open sub-prevariety by [**Liu06**, 4.2.24 & 4.2.25]. Let $V' \subset \mathrm{Reg}(V)$ be an open affine sub-prevariety of V . Hence $V'_L \subseteq V_L$ is also an open affine sub-prevariety. Let $U \subseteq \mathbb{A}^n_L$ be an open sub-prevariety and $g : U \to V_L$ a dominant morphism. Since $U' = g^{-1}(V'_L)$ is open dense in $\mathbb{A}^r_L$, and $g|_{U'}^{V'_L}$ is a dominant morphism, we may assume that $V \subset \mathbb{A}^m_L$ is affine and regular and that $g : U \to V_L$ is a dominant morphism of L-prevarieties. Let $P_1 \neq P_2 \in U$ be two L-rational points, i.e.

$$\begin{aligned} P_1 &= (x_1 - a_1, \ldots, x_n - a_n) \in \operatorname{Spec}(L[x_1, \ldots, x_n]), \\ P_2 &= (x_1 - b_1, \ldots, x_n - b_n) \in \operatorname{Spec}(L[x_1, \ldots, x_n]). \end{aligned}$$

Let $1 \neq \ell \in L$. Consider the nonconstant morphism $\gamma : \mathbb{A}^1_L \to \mathbb{A}^n_L$ given by $L[x_1, \ldots, x_n] \to L[y], x_i \mapsto c_i y + d_i$, where $c_i, d_i \in L$ are such that $c_i + d_i = a_i$ and $c_i \ell + d_i = b_i$ for $1 \leq i \leq n$.
Let $W = \gamma^{-1}(U)$. Then $g \circ \gamma|_W^U : W \to V_L$ defines a nonconstant rational morphism $\mathbb{A}^1_L \dashrightarrow V_L$. Hence the claim follows from (3.36). □

Let us put (3.37) into context. Let V be either a Severi-Brauer variety or a quadric. The function field $K(V)$ of the respective variety V is a generic splitting field of V, that is, $V_{K(V)}$ is rational, and every extension field L of K, such that V_L is rational, contains the residue field of a K-valuation of $K(V)$ (and vice versa). Employing (3.37), we get the following improvement of this result.[2]

THEOREM 3.38. *Let L/K be a finite separable extension of infinite fields, and V a quadric or a Severi-Brauer variety over K. Then the following are equivalent:*

i) V_L is rational.
ii) V_L contains a rational point.
iii) There exists a K-valuation v on $K(V)$ with residue field $\kappa_v \hookrightarrow L$.
iv) There exists a K-valuation v on $K(V)$ with residue field $\kappa_v \cong L$.

PROOF. The equivalences $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$ are long known, even for more general varieties such as so-called reductive group schemes or so-called twisted flag varieties, cf. [**KR94**] or [**MPW98**], even without the assumption that K is infinite and without placing any restriction on the extension L/K. $(iv) \Rightarrow (iii)$ is obvious, and $(i) \Rightarrow (iv)$ follows from (3.37) as, for any regular point $P \in V$, its residue field $K(P)$ is the residue field of a valuation on $K(V)$, by (2.14), which is a K-valuation by construction. □

[2] A. Wadsworth communicated a crucial idea for proving this result.

4. Curves and fibered surfaces

Algebraic curves. A prevariety C over K whose irreducible components are all of dimension one is called an *algebraic curve over K*.

Note that by the principal ideal theorem (2.3) and the descending chain condition for prime ideals [**Eis95**, 10.3] for Noetherian rings, any $f \in K[X,Y] \setminus K$ defines an affine algebraic curve $\mathrm{Spec}(K[x,y]/(f))$ as a closed subscheme of $\mathbb{A}^2_K$. Similarly, every homogeneous polynomial $f \in K[X,Y,Z] \setminus K$ defines a projective algebraic curve, also denoted by $f = 0$. Such curves are referred to as *plane affine* or *plane projective* curves. They are integral if and only if f is irreducible as a polynomial, and geometrically integral if and only if f is irreducible over K_{alg}.

Example 3.39. Let K be a field with $\mathrm{char}(K) \neq 2$, $a, b \in K^\times$ and $n, m \in \mathbb{N}$. We claim that the Cassels–Catalan curve $C^{n,m}_{a,b}$ defined by the equation $aX^n + bY^m = 1$ is geometrically integral, if nm is relatively prime to $\mathrm{char}(K)$. The curve $aX^n + bY^m = 1$ is isomorphic over K_{alg} to $X^n + Y^m = 1$. By [**Lan02**, Chap. VI, 9.1], we have that $X^n - (1 - Y^m)$ is irreducible as a polynomial in $K_{\mathrm{alg}}(Y)[X]$, since $(1 - Y^m)$ is not a pth power for any prime p dividing n, nor is it a fourth power, by the assumption on $\mathrm{char}(K)$. In particular, $X^n + Y^m - 1$ is an irreducible polynomial in $K_{\mathrm{alg}}[X,Y]$.

Definition 3.40. An *algebraic function field F/K* is a finitely generated field extension of transcendence degree one.

By (3.30), the function field of an irreducible K-curve is an algebraic function field. Conversely, every algebraic function field F/K is the function field of an irreducible K-curve C: Suppose $F = K(a_1, \ldots, a_n)$ is of transcendence degree one over K. Then $C = \mathrm{Spec}(K[a_1, \ldots, a_n])$ is a one dimensional K-scheme, by [**Eis95**, 8.2, Thm.A].
Letting $K[a_1, \ldots, a_n] = K[x_1, \ldots, x_n]/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$, the projective closure of C in $\mathbb{P}^n_K$ is given by a homogenization of $\mathfrak{p}$ in $K[x_0, \ldots, x_n]$. The function field remains the same. Hence, C can be chosen projective and, by the following, even regular.

Theorem 3.41 (Resolution of curve singularities). *Let C be an integral projective curve over K. Then there exists a regular projective curve C' over K and a surjective K-morphism $C' \to C$ that defines a birational map. In particular, every algebraic function field F/K is the function field of an integral regular projective curve.*

Reference:. [**Liu06**, 8.1.26].

REMARK 3.42 (Jacobi criterion for curves). Let $f(X,Y) \in K[X,Y]\backslash K$. Then the affine plane K-curve $\mathrm{Spec}(K[X,Y]/(f))$ is smooth in a closed point $P \in \mathbb{A}^2_K$, if and only if

$$P \notin V(f, \frac{\partial}{\partial X} f, \frac{\partial}{\partial Y} f) \subset \mathbb{A}^2_K.$$

See [**Liu06**, 4.2.19].

EXAMPLE 3.43. The projective curve $aX^n + bY^n = Z^n$ is a smooth curve if $\mathrm{char}(K)$ is relatively prime to n. One can see this using (3.42) on different affine charts that cover the projective curve. We do this for one chart, and leave the two others to the imagination of the reader. The affine chart $aX^n + bY^n = 1$ is smooth, as the system of equations

$$\begin{aligned} aX^n + bY^n - 1 &= 0 \\ \frac{\partial}{\partial X}(aX^n + bY^n - 1) = naX^{n-1} &= 0 \\ \frac{\partial}{\partial Y}(aX^n + bY^n - 1) = nbY^{n-1} &= 0 \end{aligned}$$

has no simultaneous solution in $K \times K/\sim_G$.

LEMMA 3.44. *Let $n \geq 2$ and $X \subseteq \mathbb{P}^n_K$ be a projective curve. Then there exist homogeneous polynomials $h_1, \ldots, h_n \in K[x_0, \ldots, x_n]$ such that $V_+(h_1, \ldots, h_n) \cap X = \emptyset$.*

PROOF. Consider the affine open subspace $D_+(x_0) = \mathbb{A}^n_K \subset \mathbb{P}^n_K$. In this subset, X corresponds to an ideal in $K[x_1, \ldots, x_n]$ generated by some polynomials $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$. As even $X_{K_{\mathrm{alg}}}$ consists of only finitely many irreducible components, which are of dimension one, it is clear that only for finitely many $(b_1, \ldots, b_{n-1}) \in K^{n-1}_{\mathrm{alg}}$ we have $f_i(b_1, \ldots, b_{n-1}, x_n) = 0 \in K[x_n]$ for all $1 \leq i \leq r$. Consider the finite exceptional set

$$\mathcal{E} = \left\{ \begin{matrix} (b_1, \ldots, b_{n-1}) \\ \in K^{n-1}_{\mathrm{alg}} \end{matrix} \,\middle|\, \begin{matrix} \exists\, \sigma_1, \ldots, \sigma_{n-1} \in G = \mathrm{Gal}(K_{\mathrm{alg}}/K) \text{ such that for} \\ 1 \leq i \leq r : \; f_i(\sigma_1(b_1), \ldots, \sigma_{n-1}(b_{n-1}), x_n) = 0 \end{matrix} \right\}$$

For arbitrary $(a_1, \ldots, a_{n-1}) \in K^{n-1}_{\mathrm{alg}} \backslash \mathcal{E}$ one can choose some $a_n \in K_{\mathrm{alg}}$ such that $(\sigma_1(a_1), \ldots, \sigma_{n-1}(a_{n-1}), a_n)_{\sim_G} \notin X$ for all

$$(\sigma_1, \ldots, \sigma_{n-1}) \in G^n$$

For $j \in \{1, \ldots, n\}$ let $g_j(x_j) \in K[x_j]$ denote the minimal polynomial of a_j over K. Consider the homogenizations $\tilde{h}_j(x_0, x_j) = g_j(\frac{x_j}{x_0}) x_0^{\deg(g_j)}$ for $j \in \{1, \ldots, n\}$. Then $V_+(h_1, \ldots, h_n) \cap X = \emptyset$. □

Fibered surfaces. Let A be a one dimensional Dedekind domain. A two dimensional integral scheme $\mathcal{C}$, together with a *flat*(cf. [**Liu06**, Def. 4.3.1] for this notion) projective morphism $f : \mathcal{C} \to \mathrm{Spec}(A)$, is called a *projective* A*-curve* or a *fibered surface over* A. If $\mathcal{C}$ is normal, it is called a *normal fibered surface over* A. By [**Liu06**, 4.3.10], a morphism from a scheme to $\mathrm{Spec}(A)$ flat if and only if it is non-constant; if the morphism is moreover projective an therefore closed, it is thus flat if and only if its generic fiber is nonempty.

PROPOSITION 3.45. *Let A be a one dimensional Dedekind domain and $\mathcal{C}$ a fibered surface over A. For every closed point $\mathfrak{p} \in \mathrm{Spec}(A)$, the closed fiber $\mathcal{C}_{\mathfrak{p}}$ is a projective curve over $A/\mathfrak{p}$, and the generic fiber $\mathcal{C}_{(0)}$ is an integral projective curve over* $\mathrm{Quot}(A)$.

REFERENCE:. See [**Liu06**, 8.3.3].

COROLLARY 3.46. *Let $\mathcal{C}$ a fibered surface over a Dedekind domain A of dimension one.*

(i) Every closed point $P \in \mathcal{C}$ is contained in a closed fiber $\mathcal{C}_{\mathfrak{p}}$ where $(0) \neq \mathfrak{p} \in \mathrm{Spec}(A)$.
(ii) The closed points $P \in \mathcal{C}$ are exactly those with $\mathrm{codim}_{\mathcal{C}}(\overline{\{P\}}) = 2$.
(iii) The nonclosed points $\eta \in \mathcal{C}$ are exatly those with $\mathrm{codim}_{\mathcal{C}}(\overline{\{\eta\}}) = 1$*, or the unique generic point of* $\mathcal{C}$.

PROOF. Recall that the projective structure morphism $\mathcal{C} \to \mathrm{Spec}(A)$ is a closed map by (3.25), whereby we obtain (i).
(ii) : Since $\mathcal{C}$ has dimension 2, it is clear that every point of codimension 2 is a closed point. Otherwise, if $P \in \mathcal{C}$ is a closed point, then it is contained in an irreducible component of the closed fiber $\mathcal{C}_{\mathfrak{p}}$ for some $(0) \neq \mathfrak{p} \in \mathrm{Spec}(A)$, by (i). Since this irreducible component is one-dimensional, by (3.45), and a proper closed subset in the irreducible space $\mathcal{C}$, the codimension of $\mathfrak{P}$ is at least 2, and hence exactly 2.
(iii) is just complementary to (ii). □

Note that the function field of the fibered surface $\mathcal{C}$ over A is the same as the function field of its generic fiber $\mathcal{C}_{(0)}$, and hence is an algebraic function field over $K = \mathrm{Quot}(A)$.
Conversely, suppose that F/K is an algebraic function field, that is, the function field of a curve of an integral projective curve C over K, i.e. a one-dimensional scheme $\mathrm{Proj}(K[x_0, \ldots, x_n]/\mathfrak{p}')$ for some homogeneous prime ideal $\mathfrak{p}' \subset K[x_0, \ldots, x_n]$ not containing the irrelevant

ideal. Its inverse image $\mathfrak{p} \subset A[x_0, \ldots, x_n]$ under the canonical embedding $A[x_0, \ldots, x_n] \hookrightarrow K[x_0, \ldots, x_n]$ of graded rings is a homogeneous prime ideal.
Set $\mathcal{C} = \operatorname{Proj}(A[x_0, \ldots, x_n]/\mathfrak{p})$. This scheme over A has generic fiber $\mathcal{C}_{(0)} = C$, by [**Liu06**, 3.1.9]. It is clear that $\dim(\mathcal{C}) \geq \dim(C) + 1 = 2$. In fact, equality holds (cf. [**Eis95**, 13.8]). Now, for arbitrary $q \in A$ prime, consider the canonical surjective homomorphism of graded rings $A[x_0, \ldots, x_n] \to A/(q)[x_0, \ldots, x_n]$ and let $\mathfrak{a}_q \subset A/(q)[x_0, \ldots, x_n]$ denote the homogeneous ideal given by the image of $\mathfrak{p}$ under this homomorphism.
This describes the closed fiber $\mathcal{C}_{(q)} = \operatorname{Proj}(A/(q)[x_0, \ldots, x_n]/\mathfrak{a}_q)$. Note that $\mathcal{C}_{(q)}$ is nonempty, as the radical of $\mathfrak{a}_q$ does not contain the irrelevant ideal (as neither did $\mathfrak{p}'$).

Remark 3.47. Let A be a one dimensional Dedekind domain, and $K = \operatorname{Quot}(A)$. The algebraic function fields over K coincide with the function fields of fibered surfaces over A.

Recall that the generic fiber $\mathcal{C}_{(0)}$ of a fibered surface $\mathcal{C}$ over A is an open subscheme of $\mathcal{C}$, and that the closed fibers $\mathcal{C}_{\mathfrak{p}}$ for $(0) \neq \mathfrak{p} \in \operatorname{Spec}(A)$ are closed subschemes of $\mathcal{C}$. Set theoretically they are the actual fibers of the set theoretic map $\mathcal{C} \to \operatorname{Spec}(A)$, whereby they are disjoint and their union is $\mathcal{C}$.

Example 3.48. Let $\mathcal{O}$ be a discrete valuation ring with maximal ideal $\mathfrak{m} = (t)$ and residue field k. Then $\mathbb{P}^1_{\mathcal{O}}$ is a fibered surface over $\mathcal{O}$ with special fiber $\mathbb{P}^1_k$. Let $\infty \in \mathbb{P}^1_{\mathcal{O}}$ denote any closed k-rational point. Write $\infty = (x_0) \in \operatorname{Proj}(k[x_0, x_1])$, respectively $\infty = (t, x_0) \in \operatorname{Proj}(\mathcal{O}[x_0, x_1])$.

The following proposition is [**HH10**, 6.6]. We include the original proof with a minor correction.

Proposition 3.49. *Let $\mathcal{O}$ be a discrete valuation ring with maximal ideal $\mathfrak{m}$, and $\mathcal{C}$ a fibered surface over $\mathcal{O}$. Let $\mathcal{S} \subset \mathcal{C}$ be a finite set of closed points. Then there exists a finite $\mathcal{O}$-morphism $f : \mathcal{C} \to \mathbb{P}^1_{\mathcal{O}}$ such that $\mathcal{S} \subseteq f^{-1}(\{\infty\})$.*

Proof. Since $\mathcal{C}$ is projective over $\mathcal{O}$, there exists a closed $\mathcal{O}$-immersion $\mathcal{C} \hookrightarrow \mathbb{P}^n_{\mathcal{O}}$ for some $n \in \mathbb{N}$. We let k denote $\mathcal{O}/\mathfrak{m}$. We show the claim by induction on n.
If $n = 1$, then $\mathcal{C} \cong \mathbb{P}^1_{\mathcal{O}}$. Let $g \in k[y_0, y_1]$ be a homogeneous polynomial such that $g_0(\mathcal{S}) = 0$. Let $g_1 \in k[y_0, y_1]$ be an homogeneous polynomial of the same degree as g_0, say d, such that $V_+(g_0, g_1) = \emptyset$.

Let $G_0, G_1 \in \mathcal{O}[y_0, y_1]$ be homogeneous lifts of g_0, g_1. Let $N+1$ denote the number of distinct monomials of degree d in two variables. Let $\iota_d : \mathbb{P}^1_{\mathcal{O}} \to \mathbb{P}^N_{\mathcal{O}}$ denote the d-uple embedding given by the graded morphism $\iota_d^* : \mathcal{O}[x_0, \dots, x_N] \to \mathcal{O}[y_0, y_1]$, as in (3.19). The $\mathcal{O}$-morphism ι_d is finite, and thus is closed, by (3.17). Let $\mathcal{C}' \subseteq \mathbb{P}^N_{\mathcal{O}}$ denote the closed reduced subscheme given by $\iota_d(\mathcal{C})$ with its induced reduced subscheme structure. By (3.18), $\iota_d|^{\mathcal{C}'}$ is a finite morphism. Let $L_0, L_1 \in \mathcal{O}[x_0, \dots, x_N]$ be homogeneous linear polynomials such that $\iota_d^*(L_0) = G_0$ and $\iota_d^*(L_1) = G_1$, and let $\ell_0, \ell_1 \in k[x_0, \dots, x_n]$ be the reductions of L_0, L_1 with respect to $\mathfrak{m}$, which are homogeneous of the same degree. We see that $V_+(L_0, L_1) \cap \mathcal{C}' = \emptyset$. Letting $\pi : \mathbb{P}^N_{\mathcal{O}} \setminus V_+(L_0, L_1) \to \mathbb{P}^1_{\mathcal{O}}$ be the projection morphism, as in (3.20), we have that $\pi|_{\mathcal{C}'}$ is a finite $\mathcal{O}$-morphism, whereby $V_+(\ell_0) = \pi^{-1}(\{\infty\})$. Hence, $\mathcal{S} \subset V_+(g_0) = (\pi|_{\mathcal{C}'} \circ \iota_d|^{\mathcal{C}'})^{-1}(\{\infty\})$. Note that $(\pi|_{\mathcal{C}'} \circ \iota_d|^{\mathcal{C}'})$ is a finite $\mathcal{O}$-morphism, by (3.15).

Now assume that $n > 1$. By (3.44), there exist homogeneous polynomials $h_1, \dots, h_n \in k[x_0, \dots, x_n]$ such that $V_+(h_1, \dots, h_n) \cap X = \emptyset$, where $X \subset \mathbb{P}^n$ denotes the special fiber of $\mathcal{C}$. In fact, replacing the h_j by appropriate powers, we can assume that $h_1, \dots, h_n$ all have the same degree d. Let $H_1, \dots, H_n \in \mathcal{O}[x_0, \dots, x_n]$ be homogeneous lifts of $h_1, \dots, h_n$. Since the closed points of $V_+(H_1, \dots, H_n) \subset \mathbb{P}^n_{\mathcal{O}}$ are not contained in X, it follows that $V_+(H_1, \dots, H_n) \cap \mathcal{C} = \emptyset$.[3]

Let $N+1$ be as before the number of degree d-monomials in $\mathcal{O}[x_0, \dots, x_n]$ and consider the finite d-uple $\mathcal{O}$-embedding $\iota_d : \mathbb{P}^n_{\mathcal{O}} \hookrightarrow \mathbb{P}^N_{\mathcal{O}}$, as in (3.19), and $\iota_d^* : \mathcal{O}[y_0, \dots, y_N] \to \mathcal{O}[x_0, \dots, x_n]$ the defining morphism of graded algebras. Let $L_1, \dots, L_n \in \mathcal{O}[y_0, \dots, y_N]$ be homogeneous linear polynomials, such that their images under ι_d^* are $H_1, \dots, H_n \in \mathcal{O}[x_0, \dots, x_n]$. Since ι_d is an embedding, it is clear that $V_+(L_1, \dots, L_n) \cap \iota_d(\mathcal{C}) = \emptyset$. Let $\mathcal{C}' \subset \mathbb{P}^N_{\mathcal{O}}$ denote the closed reduced subscheme given by $\iota_d(\mathcal{C})$, with the induced reduced subscheme structure. Then

$$\iota_d|_{\mathcal{C}}^{\mathcal{C}'} : \mathcal{C} \to \mathcal{C}'$$

is a finite $\mathcal{O}$-morphism, by (3.18). Now consider the projection morphism

$$\pi : \mathbb{P}^N_{\mathcal{O}} \setminus V_+(L_1, \dots, L_n) \longrightarrow \mathbb{P}^{n-1}_{\mathcal{O}}.$$

The restriction of $\pi|_{\mathcal{C}'}$ is a finite $\mathcal{O}$-morphism, by (3.20). Let $\mathcal{C}''$ denote the closed reduced subscheme of $\mathbb{P}^{n-1}_{\mathcal{O}}$ given by the closed subset

[3]In the original proof in [**HH10**], the $h_1, \dots, h_n$ were not chosen correctly.

$\pi|_{\mathcal{C}'}(\mathcal{C}')$, together with its induced reduced structure. Then $\pi|_{\mathcal{C}'}^{\mathcal{C}''}$ is a finite morphism, by (3.18). Hence, the map $\psi = \pi|_{\mathcal{C}'}^{\mathcal{C}''} \circ \iota_d|_{\mathcal{C}}^{\mathcal{C}'} : \mathcal{C} \to \mathcal{C}''$ is a finite $\mathcal{O}$-morphism, by (3.15). Since it is the image of a finite morphism mapping from a 2-dimensional scheme, $\mathcal{C}''$ is 2-dimensional. It is obviously projective over $\mathcal{O}$. Moreover, the generic fiber of $\mathcal{C}''$ is nonempty. Hence $\mathcal{C}''$ is a fibered surface over $\mathcal{O}$, embedded as a closed subscheme in $\mathbb{P}^{n-1}_{\mathcal{O}}$. Moreover, $\mathcal{S}'' = \psi(\mathcal{S})$ is a finite set of closed points in $\mathcal{C}''$, by (3.17). By the induction hypothesis, there exists a finite $\mathcal{O}$-morphism $\rho : \mathcal{C}'' \to \mathbb{P}^1_{\mathcal{O}}$ such that $\mathcal{S}'' \subset \psi^{-1}(\{\infty\})$. Hence $f = \rho \circ \psi : \mathcal{C} \to \mathbb{P}^1_{\mathcal{O}}$ is a finite $\mathcal{O}$-morphism, with $\mathcal{S} \subset f^{-1}(\{\infty\})$. □

A regular fibered surface $\mathcal{C}$ over a one dimensional Dedekind domain A is also called an *arithmetic surface over A*.

Desingularization. Let A be a one dimensional Dedekind domain with field of fractions K. Let F be an algebraic function field over K. By (3.41), there exists an regular integral projective K-curve C with $F = K(C)$.
We call a normal fibered surface $\mathcal{C} \to \operatorname{Spec}(A)$ a *model for C over A* if its generic fiber $\mathcal{C}_{(0)}$ is isomorphic to C as abstract K-prevarieties. If moreover $\mathcal{C}$ is regular, i.e. an arithmetic surface, we will call it a *regular model for C over A*.
Instead of a 'model for C', we also speak of a *model for F/K*, if we start with a given algebraic function field F/K.

Note that by [**Liu06**, 8.3.51], in the following theorem, T may in fact be an arbitrary one dimensional Dedekind domain if the generic fiber of $\mathcal{C}$ is assumed to be smooth. This is for example always the case when K is a perfect field.

THEOREM 3.50 (Desingularization). *Let T be a complete discrete valuation ring, and $\mathcal{C}$ a fibered surface over T. Then there exists an arithmetic surface $\mathcal{C}'$ over T and a T-morphism $\mathcal{C}' \to \mathcal{C}$ that restricts to an isomorphism on the generic fibers.*

PROOF. By [**Liu06**, 8.2.39 $(a),(c)$] the scheme $\mathcal{C}$ is *excellent* (cf. [**Liu06**, Def. 8.2.35] for this notion). Hence, by Lipman's desingularization of reduced noetherian two dimensional excellent schemes [**Liu06**, 8.3.44], there exists a desingularization morphism $\mathcal{C}' \to \mathcal{C}$. Moreover, by [**Liu06**, 8.2.39 (d) & 8.3.47 (b)], this desingularization morphism is projective. Since the desingularization morphism is birational, it follows that it is an isomorphism on the generic fibers of $\mathcal{C}'$ and $\mathcal{C}$. □

Corollary 3.51. *Let T be a complete discrete valuation ring with fields of fractions K. Then every algebraic function field F/K has a regular model over T.*

Proof. Let C denote the regular projective curve over K with function field F, as exists by (3.41). It is defined by some homogeneous prime ideal $\mathfrak{p}$ in a polynomial ring $K[X_0, \dots, X_n]$. Let $\mathfrak{P}$ denote its preimage of $\mathfrak{p}$ in the ring $T[X_0, \dots, X_n]$ under the natural homomorphism $T[X_0, \dots, X_n] \to K[X_0, \dots, X_n]$ of graded rings. Let $\mathcal{C} = \mathrm{Proj}(T[X_0, \dots, X_n]/\mathfrak{P})$. This is a fibered surface over T with generic fiber C. By (3.50), we obtain a regular model for F over T. □

The previous desingularization result (3.50) is the arithmetic analog of the well known resolution of singularities for (geometric) surfaces (over fields of arbitrary charateristic). The equally well known 'embedded resolution' result of singularities of curves on regular surfaces also has an arithmetic analog:

Theorem 3.52 (Embedded resolution). *Let T be complete discrete valuation ring, $\mathcal{C}$ an arithmetic surface over T and D an effective divisor on $\mathcal{C}$. Then there exists an arithmetic surface $\mathcal{C}'$ over T and a T-morphism $f : \mathcal{C}' \to \mathcal{C}$ such that f^*D is a divisor with normal crossings on $\mathcal{C}'$, and such that f restricts to an isomorphism on the generic fibers.*

Proof. By [**Liu06**, 8.2.39 $(a), (c)$], the effective divisor is *excellent* (cf. also [**Liu06**, 9.2.28] for this observation). Now the statement follows from [**Liu06**, 9.2.26]. □

CHAPTER 4

Cassels-Catalan Curves

In this chapter we prove that the function field of a Cassels-Catalan curve not containing $\sqrt{-1}$ can only have Pythagoras number two if its base field is hereditarily Pythagorean.
We first give a proof of geometric flavor, before we take a look at a very early version of the proof of more combinatorial flavor. In the second section of this chapter, we give a purely geometric proof for the special case of conic curves.

REMARK 4.1. A field is hereditarily Pythagorean if and only if it is real and $\sqrt{-1}$ is contained in each of its nonreal finite extensions. See [**Bec78**, III, Thm. 1].

REMARK 4.2. An ordering on a field K extends to $K(\sqrt{a})$ for $a \in K^\times$ if and only if a is positive at this ordering. See [**PD01**, 1.2.3]. In particular, $K(\sqrt{a})$ is nonreal if and only if $-a \in \sum K^{\times 2}$.

PROPOSITION 4.3. *Let C be a smooth integral curve over a non hereditarily Pythagorean field K. If $P \in C$ is a closed point with $K(P)$ nonreal and $\sqrt{-1} \notin K(P)$, then $p(K(C)) \geq 3$.*

PROOF. If $K(P)= \mathcal{O}_{C,P}/\mathfrak{m}_{C,P}$ is nonreal and $\sqrt{-1} \notin K(P)$, the assertion follows with (2.26), as $P \in C$ is a point of codimension one, whereby $\mathcal{O}_{C,P}$ is a discrete valuation ring. □

1. The general case

The proof of the following (4.4) uses a small observation on scalar restrictions obtained in the third chapter. At the end of the current section, I present my first proof for (4.4), which omits all geometry and uses only combinatorial arguments.

PROPOSITION 4.4. *Let K be an infinite field and L/K be a finite separable extension such that L is not Pythagorean. Then there exists $\xi \in L$ such that $L = K(\xi^2)$ and $\xi^2 + 1 \notin L^{\times 2}$. Moreover, there exists $\sigma \in \sum L^{\times 2} \setminus L^{\times 2}$ such that $L = K(\sigma)$ and $\sigma + 1 \notin L^{\times 2}$.*

PROOF. Fix $z \in L$ with $z^2+1 \notin L^{\times 2}$. For $\nu \in L^\times$, consider the terms $\alpha = \frac{\nu^2}{z^2}$, $\beta = \nu^2 + z^2$, $\gamma = \frac{(z^2+1)^2}{\nu^2} + z^2$, $\delta = \frac{(z^2+1)^2}{z^2\nu^2}$ and $\epsilon = \frac{z^2+1}{\nu^2}$.
In terms of elementary geometry, these are rational functions in ν over L. Let $\mathcal{G} = \{x \in L \mid K(x) = L\}$. This is a K-Zariski open subset of L, as it is the complement of the finitely many subspaces of L that correspond to the finitely many intermediate extensions of L/K. By (3.5), the preimage of $\mathcal{G}$ under any nonconstant K-rational function on L is nonempty. Moreover, it is K-open in L. As the intersection of finitely many nonempty K-open subsets of L is nonempty, there exists $\nu \in L^\times$ such that $\alpha, \beta, \gamma, \delta, \epsilon \in \mathcal{G}$.
Note that $\epsilon, \frac{1}{\epsilon} \in \sum L^{\times 2} \setminus L^{\times 2}$. If $\epsilon + 1 \notin L^{\times 2}$, we set $\sigma = \epsilon$. Otherwise we have that $\frac{1+\epsilon}{\epsilon} = \frac{1}{\epsilon} + 1 \notin L^{\times 2}$, and we set $\sigma = \frac{1}{\epsilon}$.
Note that $\alpha \in L^{\times 2}$. If $\alpha + 1 \notin L^{\times 2}$, choose $\xi = \frac{\nu}{z}$. Assume now that $\alpha + 1 \in L^{\times 2}$. Then $\beta \in L^{\times 2}$. If $\beta + 1 \notin L^{\times 2}$, choose $\xi \in L$ such that $\xi^2 = \beta$. Assume now that $\beta + 1 \in L^{\times 2}$. Then $\nu^2 + z^2 + 1 \in L^{\times 2}$ and $\nu^2 + z^2 \in L^{\times 2}$. It follows that $\frac{(z^2+1)^2}{\nu^2} + z^2 + 1 \notin L^{\times 2}$, since $z^2 + 1 \notin L^{\times 2}$. Recall that $\delta = \frac{(z^2+1)^2}{z^2\nu^2}$. If $\delta + 1 \notin L^{\times 2}$, choose $\xi = \frac{z^2+1}{z\nu}$. If $\delta + 1 \in L^{\times 2}$, then $\gamma \in L^{\times 2}$ and $\gamma + 1 \notin L^{\times 2}$, and we can choose $\xi \in L$ such that $\xi^2 = \gamma$. □

We denote by $\pm K^{\times 2}$ the set $K^{\times 2} \cup -K^{\times 2}$, for any field K.

LEMMA 4.5. *Let $u \in K^\times \setminus \pm K^{\times 2}$ and $r \geq 1$. Let $\gamma \in K_{\mathrm{alg}}$ be such that $\gamma^{2^r} = u$. Then $K^\times \cap K(\gamma)^{\times 2} = K^{\times 2} \cup uK^{\times 2}$.*

PROOF. As $-u \notin K^{\times 2}$, and thus $-u \notin 4K^{\times 4}$, the polynomial $T^{2^r} - u$ is irreducible by [**Lan02**, Chap. VI, (9.1)]. Write $d = \gamma^2$, $L = K(d)$ and $M = K(\gamma)$. Note that M/L is a quadratic extension. As $T^{2^{r-1}} - u$ is the minimal polynomial of d over K, the norm of d with respect to L/K is $\pm u$. As $u \notin \pm K^{\times 2}$, it follows that $K^\times \cap dL^{\times 2} = \emptyset$. As $L^\times \cap M^{\times 2} = L^{\times 2} \cup dL^{\times 2}$, we have that

$$K^\times \cap M^{\times 2} = K^\times \cap (L^{\times 2} \cup dL^{\times 2}) = K^\times \cap L^{\times 2}.$$

The statement thus follows by induction on r. □

COROLLARY 4.6. *Suppose $-1 \notin K^{\times 2}$. Let $u \in K^\times \setminus \pm K^{\times 2}$ and $n \in \mathbb{N}$. There exists $x \in K_{\mathrm{alg}}$ with $x^n = u$ and $K^\times \cap K(x)^{\times 2} \subseteq K^{\times 2} \cup uK^{\times 2}$.*

PROOF. If n is odd, we can choose $x \in K_{\mathrm{alg}}$ with $x^n = u$ such that $[K(x) : K]$ is odd, whereby $K^\times \cap K(x)^{\times 2} \subseteq K^{\times 2}$. Assume now that n is even. If $u \notin K^{\times 2}$, then we write $n = 2^r m$ with m odd and $r \geq 1$, and apply (4.5) together with the previous case. □

COROLLARY 4.7. *Suppose* $-1 \notin K^{\times 2}$. *Let* $v \in K^{\times} \setminus -K^{\times 2}$ *and* $m \in \mathbb{N}$. *There exists* $y \in K_{\mathrm{alg}}$ *such that* $y^m = v$ *and* $-1 \notin K(y)^{\times 2}$.

PROOF. Let $r \in \mathbb{N}$ be maximal such that $2^r|m$ and $v \in K^{\times 2^r}$. Let $u \in K$ be such that $u^{2^r} = v$. We write $m = n2^r$. If n is odd, then we can choose $y \in K_{\mathrm{alg}}$ such that $y^m = v$ and $[K(y) : K]$ is odd, and it follows trivially that $-1 \notin K(y)^{\times 2}$.
Assume that n is even. Then $u \notin K^{\times 2}$ by the maximality of r. Furthermore, we claim that $u \notin -K^{\times 2}$. If $r = 0$ we have that $u = v \notin \pm K^{\times 2}$. If $r > 0$ then $u \notin -K^{\times 2}$ by the maximality of r and the fact that $(-u)^{2^r} = v$. Using (4.6), we choose $y \in K_{\mathrm{alg}}$ such that $y^n = u$ and $K^{\times} \cap K(y)^{\times 2} \subseteq K^{\times 2} \cup uK^{\times 2}$. Then $y^m = v$ and $-1 \notin K(y)^{\times 2}$, since $u \notin -K^{\times 2}$. □

PROPOSITION 4.8. *Let* K *be a field with* $-1 \notin K^{\times 2}$. *Let* $u \in K^{\times} \setminus \pm K^{\times 2}$ *and* $v \in K^{\times} \setminus (-K^{\times 2} \cup -uK^{\times 2})$. *Let* $n, m \geq 1$. *Then there exists a finite extension* M/K *such that* $-1 \notin M^{\times 2}$, *with* $x, y \in M$ *such that* $x^n = u$ *and* $y^m = v$, *and such that* $M = K(x, y)$.

PROOF. We choose $x \in K_{\mathrm{alg}}$ such that $x^n = u$ and $K^{\times} \cap K(x)^{\times 2} \subseteq K^{\times 2} \cup uK^{\times 2}$. Then $-1, -v \notin K(x)^{\times 2}$. By (4.7) there exists $y \in K_{\mathrm{alg}}$ such that $y^m = v$ and $-1 \notin K(x, y)^{\times 2}$. Set $M = K(x, y)$. □

COROLLARY 4.9. *Let* L/K *be a finite field extension such that* L *is real and not Pythagorean. Let* $a, b \in K$ *such that* $a, b \in L^{\times 2} \cup -L^{\times 2}$. *For integers* $n, m \geq 1$, *there exists a finite extension* M/L, *such that* $-1 \notin M^{\times 2}$, *and with* $x, y \in M$ *such that* $1 = ax^n + by^m$ *and* $M = K(x, y)$. *If moreover* n *or* m *is even, then we can choose* M *to be nonreal.*

PROOF. By (4.4) there exists $\xi \in L$ with $\xi^2 + 1 \in \sum L^{\times 2} \setminus L^{\times 2}$ and $L = K(\xi^2)$, and further $\sigma \in \sum L^{\times 2} \setminus L^{\times 2}$ with $L = K(\sigma)$ and $\sigma + 1 \in \sum L^{\times 2} \setminus L^{\times 2}$.
In the case where $a, b \in L^{\times 2}$, set $u = -\frac{1}{a\sigma}$ and $v = \frac{1}{b}(1 + \frac{1}{\sigma})$. Then $u \notin \pm L^{\times 2}$ and $-v \notin L^{\times 2} \cup uL^{\times 2}$, as $-uv = \frac{1}{ab}\frac{\sigma+1}{\sigma^2}$. Moreover, $1 = au + bv$.
In the case where $-a, -b \in L^{\times 2}$, set $u = \frac{\xi^2+1}{a}$ and $v = \frac{-\xi^2}{b}$. Then $u \notin \pm L^{\times 2}$ and $-v \notin L^{\times 2} \cup uL^{\times 2}$. Moreover, $1 = au + bv$.
In the case where $-a, b \in L^{\times 2}$ set $u = \frac{\sigma+1}{a}$ and $v = \frac{-\sigma}{b}$. Then $u \notin \pm L^{\times 2}$ and $-v \notin L^{\times 2} \cup uL^{\times 2}$. Moreover, $1 = au + bv$.
In the case where $a, -b \in L^{\times 2}$ set $u = \frac{-\sigma}{a}$ and $v = \frac{\sigma+1}{b}$. Then $u \notin \pm L^{\times 2}$ and $-v \notin L^{\times 2} \cup uL^{\times 2}$. Moreover, $1 = au + bv$.
In each case, by (4.8), there exist $x, y \in L_{\mathrm{alg}}$ such that $x^n = u$, $y^m = v$ and $\sqrt{-1} \notin L(x, y)$. Moreover, since $u \in L(x, y)$ and $K(u) = L$, it

follows that $L(x,y) = K(x,y)$. Obviously $1 = ax^n + by^m$ as $1 = au + bv$. Set $M = L(x,y)$. Now suppose that n or m is even. By symmetry, we can assume that n is even. Then $x^n = u$ is both a square in M and, by the choices of u in each case, a negative sum of squares in M. Thus M is nonreal. □

THEOREM 4.10. *Let K be a field not containing $\sqrt{-1}$. Let $a, b \in K^\times$ and $n, m \in \mathbb{N}$ such that* $\mathrm{char}(K)$ *does not divide nm. Let F/K denote the function field of the plane affine curve C defined by $1 = aX^n + bY^m$. Then $p(F) = 2$ implies that K is hereditarily Pythagorean.*

PROOF. Note that the affine curve C is smooth, by (3.42). We first show that K is real. Assume that K is nonreal. Then, by (4.3), we have that $\sqrt{-1} \in K(P)$ for any point P on C. We lead this to a contradiction. If $-a \notin K^{\times 2}$, choose $x \in K_{\mathrm{alg}}$ such that $x^n = \frac{1}{a}$ and $\sqrt{-1} \notin K(x)$ as in (4.7). Then $P = (x, 0)$ is a point on C with $\sqrt{-1} \in K(P)$. If $-b \notin K^{\times 2}$ we can proceed analogous, so we consider the case where $-a, -b \in K^{\times 2}$. Choose $z \in K$ such that $z^2 + 1 \notin K^{\times 2}$. Choose again $x \in K_{\mathrm{alg}}$ such that $x^n = \frac{z^2}{-a}$ and $\sqrt{-1} \notin K(x)$. Then $\frac{1}{b} \notin K(x)^{\times 2}$ and we also find some $y \in K_{\mathrm{alg}}$ such that $y^m = \frac{-1}{b}$ and $\sqrt{-1} \notin K(x,y)$ as in (4.8). Again P is a point on C with $\sqrt{-1} \in K(P)$. Hence K is real.

Let us first consider the case where n is odd. Then F is clearly an odd degree extension of the rational function field $K(X)$. Then $p(K(X)) \leq p(F) \leq 2$ by Springer's theorem (5.1). Thus $p(K(X)) = 2$, and the claim follows from (1.5). Thus assume that n is even.

Suppose there exists a finite real extension L/K that is not Pythagorean. We can assume that $a, b \in L^{\times 2} \cup -L^{\times 2}$ since at least one of the four extensions $L(\sqrt{\pm a})(\sqrt{\pm b})$ is real, and not Pythagorean by (1.3). By (4.9) there exists a point $P \in C$ such that $-1 \notin K(P)^{\times 2}$ and $K(P)$ is nonreal. Again (4.3) yields the contradiction $p(F) \geq 3$. □

A combinatorial proof. The core of the proof of the main result (4.10) of this chapter was (4.4). The previously presented proof of (4.4) is of geometric nature. In the following, the author's firstly obtained proof for (4.4) is presented, which is of combinatorial nature. In particular, the geometric preparation on scalar restriction of the third chapter is not needed.

Let K be an infinite field and L/K a finite separable extension that is not Pythagorean. We will let $\mathcal{G}$ denote $L \setminus \bigcup \mathcal{I} = \{x \in L \mid K(x) = L\}$, the set of primitive elements for L/K.

LEMMA 4.11. *Let $c \in L^\times$, $d \in L$ and $\nu \in \mathcal{G}$. Then*
(a) we have that $c(\nu+x)^2 + d \in \mathcal{G}$ for all but finitely many $x \in K$.
(b) for each except finitely many $\alpha \in K$ there are infinitely many $x \in K$ with $\frac{c\alpha^2}{(\nu+x)^2} + d \in \mathcal{G}$.

PROOF. Let $\mathcal{I} = \{N/K \mid N \subsetneq L\}$, the finite set of intermediate fields of L/K that are different from L.
(a) For $N \in \mathcal{I}$, let $A_N = \{x \in k \mid c(\nu+x)^2 + d \in N\}$. We claim that $|A_N| \le 2$. Assume that $x_1, x_2, x_3 \in A_N$ are three distinct elements. Then

$$\begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix} \begin{pmatrix} c\nu^2 + d \\ 2c\nu \\ c \end{pmatrix} = \begin{pmatrix} c(\nu+x_1)^2 + d \\ c(\nu+x_2)^2 + d \\ c(\nu+x_3)^2 + d \end{pmatrix} \in N^3.$$

As the Vandermonde matrix on the left has nonvanishing determinant $(x_3-x_2)(x_2-x_1)(x_1-x_3)$, we can multiply across by its inverse matrix, which has coefficients in K, to obtain that $(c\nu^2+d, 2c\nu, c) \in N^3$. Thus $c \in N^\times$ and $2c\nu \in N$, whereby $\nu \in N$, contradicting the assumption that $\nu \in \mathcal{G}$. This shows that $|A_N| \le 2$ for all $N \in \mathcal{I}$. Since $\mathcal{I}$ is finite, we get that $\{x \in K \mid c(\nu+x)^2 + d \in \mathcal{G}\} = K \setminus \bigcup_{N\in\mathcal{I}} A_N$ is cofinite.
(b) Assume that there are infinitely many elements $\alpha \in K^\times$ for which the set $B_\alpha = \{x \in K \mid \frac{c\alpha^2}{(\nu+x)^2} + d \in \mathcal{G}\}$ is finite. Set $n := |\mathcal{I}|$ and choose $\alpha_0, \dots, \alpha_n \in K^\times$ such that $\alpha_0^2, \dots, \alpha_n^2$ are distinct and the sets $B_{\alpha_1}, \dots, B_{\alpha_n}$ are finite. Then $B = B_{\alpha_0} \cup \ldots \cup B_{\alpha_n}$ is finite. For every $x \in K \setminus B$ and every $0 \le i \le n$, there is a $K_{x,i} \in \mathcal{I}$ such that $\frac{c\alpha_i^2}{(\nu+x)^2} + d \in K_{x,i}$. Moreover, since $|\mathcal{I}| = n$, for each $x \in K \setminus B$ there are $0 \le i_x < j_x \le n$ such that $K_{x,i_x} = K_{x,j_x}$. As $K \setminus B$ is infinite, the pigeon-hole principle yields a pair (ℓ, m) with $0 \le \ell < m \le n$ such that $C' = \{x \in K \setminus B \mid (i_x, j_x) = (\ell, m)\}$ is infinite. For $x \in C'$ we have $K_{x,\ell} = K_{x,m}$, and we now write K_x for this field. Note that for distinct $x \in C'$, the corresponding fields K_x may not coincide. However, applying the pigeon-hole principle again, we see that there exists $N \in \mathcal{I}$ for which $C = \{x \in C' \mid K_x = N\}$ is infinite. In particular, for $x \in C$, one has that $\frac{c\alpha_\ell^2}{(\nu+x)^2} + d \in N$ and $\frac{c\alpha_m^2}{(\nu+x)^2} + d \in N$. Hence, for all $x \in C$, we have that

$$\frac{c(\alpha_\ell^2 - \alpha_m^2)}{(\nu+x)^2} = \left(\frac{c\alpha_\ell^2}{(\nu+x)^2} + d\right) - \left(\frac{c\alpha_m^2}{(\nu+x)^2} + d\right) \in N\,,$$

contradicting the result by (a), that $\frac{(\nu+x)^2}{c(\alpha_\ell^2-\alpha_m^2)} \in \mathcal{G}$ for all but finitely many $x \in K$. □

We recall (4.4) and present a geometry free proof.

PROPOSITION 4.12. *There exists* $\xi \in L$ *such that* $L = K(\xi^2)$ *and* $\xi^2 + 1 \notin L^{\times 2}$. *Moreover, there exists* $\sigma \in \sum L^{\times 2} \setminus L^{\times 2}$ *such that* $L = K(\sigma)$ *and* $\sigma + 1 \notin L^{\times 2}$.

PROOF. If $\xi \in L$ is such that $L = K(\xi^2)$ and $\eta = \xi^2 + 1 \notin L^{\times 2}$, then either $\eta + 1 \notin L^{\times 2}$ or $\frac{1}{\eta} + 1 = \frac{1}{\eta}(\eta + 1) \notin L^{\times 2}$. Hence, either $\sigma = \eta$ or $\sigma = \frac{1}{\eta}$ is such that $L = K(\sigma)$ and $\sigma + 1 \notin L^{\times 2}$. Thus, it remains to show the existence of $\xi \in L$ with $L = K(\xi^2)$ and $\xi^2 + 1 \notin L^{\times 2}$.
We may assume that $K \subsetneq L$. We fix $\nu \in \mathcal{G}$, and let $z \in L$ with $z^2 + 1 \notin L^{\times 2}$, using the fact that L is not Pythagorean.
For $\alpha \in K^\times$, let

$$\mathcal{H}_\alpha = \left\{ x \in K \;\middle|\; \frac{(\nu + x)^2}{\alpha^2} + z^2 + 1 \notin L^{\times 2} \right\}.$$

Assume firstly that $\mathcal{H}_\alpha$ is infinite for some $\alpha \in K^\times$. Consider the subset $\mathcal{H}' = \{x \in \mathcal{H}_\alpha \mid \frac{(\nu+x)^2}{\alpha^2} + z^2 \in L^{\times 2}\}$. If $\frac{(\nu+x)^2}{\alpha^2} + z^2 \in \mathcal{G}$ for some $x \in \mathcal{H}'$, then we choose $\xi \in L$ to be such that $\xi^2 = \frac{(\nu+x)^2}{\alpha^2} + z^2$, and we are done. If no such $x \in \mathcal{H}'$ exists, then $\mathcal{H}'$ is finite, by (4.11.(a))), and hence $\mathcal{H}_\alpha \setminus \mathcal{H}'$ is infinite. By (4.11)(a), we have that $\frac{(\nu+x)^2}{(z\alpha)^2} \in \mathcal{G}$ for some $x \in \mathcal{H}_\alpha \setminus \mathcal{H}'$, and as $\frac{(\nu+x)^2}{(z\alpha)^2} + 1 = \frac{1}{z^2}\left(\frac{(\nu+x)^2}{\alpha^2} + z^2\right) \notin L^{\times 2}$, we can let $\xi = \frac{(\nu+x)}{z\alpha}$.
Henceforth, suppose that $\mathcal{H}_\alpha$ is finite for all $\alpha \in K^\times$. As $z^2 + 1 \notin L^{\times 2}$, we have that

$$\frac{\alpha^2(z^2+1)^2}{(\nu+x)^2} + z^2 + 1 = (z^2+1)\frac{\alpha^2}{(\nu+x)^2}\left(\frac{(\nu+x)^2}{\alpha^2} + z^2 + 1\right) \notin L^{\times 2}$$

for every $x \in K \setminus \mathcal{H}_\alpha$. For $\alpha \in K^\times$, let

$$\mathcal{M}_\alpha = \left\{ x \in K \setminus \mathcal{H}_\alpha \;\middle|\; \frac{\alpha^2(z^2+1)^2}{(\nu+x)^2} + z^2 \in L^{\times 2} \right\}.$$

If $\mathcal{M}_\alpha$ is cofinite in K for infinitely many $\alpha \in K^\times$, then, by (4.11.(b))), there exists $\alpha \in K^\times$ and $x \in \mathcal{M}_\alpha$ such that $\frac{\alpha^2(z^2+1)^2}{(\nu+x)^2} + z^2 \in \mathcal{G}$. In this case, we can choose $\xi \in L$ to be such that $\xi^2 = \frac{\alpha^2(z^2+1)^2}{(\nu+x)^2} + z^2$, and we are done.

Assume now that $\alpha \in K^\times$ is such that $\mathcal{M}_\alpha$ is not cofinite in K. Then the set

$$K \setminus (\mathcal{H}_\alpha \cup \mathcal{M}_\alpha) = \left\{ x \in K \setminus \mathcal{H}_\alpha \;\middle|\; \frac{\alpha^2(z^2+1)^2}{z^2(\nu+x)^2} + 1 \notin L^{\times 2} \right\}$$

is infinite. It follows from (4.11.(a)) that $\frac{z^2(\nu+x)^2}{\alpha^2(z^2+1)^2} \in \mathcal{G}$ for some $x \in K \setminus (\mathcal{H}_\alpha \cup \mathcal{M}_\alpha)$, whereby we can let $\xi = \frac{\alpha(z^2+1)}{z(\nu+x)}$, completing the proof. □

2. Conics

In this section, we give a more conceptual proof for (4.10) in the special case of function fields of conics . No result of the previous section is used, instead we use a result obtained in the third chapter on generic splitting properties of quadrics and Severi-Brauer varieties.[1]

PROPOSITION 4.13. *Let C be a regular projective conic over an infinite field K, and $K(C)$ its function field. Letting L/K be a finite separable extension, we have that L is the residue field $K(P)$ of a point $P \in C$ if and only if C_L has a rational point.*

PROOF. A smooth projective conic is a one dimensional regular projective quadric. Hence (3.38) yields the result. □

REMARK 4.14. In the case where K is perfect and C/K a smooth conic, this result yields that the property *'beeing the residue field of point on C'* is a hereditary property, that is, if L is a finite field of K with $K(P) \subset L$ for some $P \in C$, then $L = K(P')$ for some $P' \in C$.
The same is not true if we replace 'smooth conic' by an arbitrary smooth projective curve over K. The Fermat curve $X^6+Y^6 = Z^6$, for example, has the 'trivial' $\mathbb{Q}$-rational points $(0:1:1)$ and $(1:0:1)$. In [**Aig57**], it was shown that $(0:1:1)$ and $(1:0:1)$ are also the only L-rational points of this curve for any quadratic field extension $L/\mathbb{Q}$, whereby $L \neq \mathbb{Q}(P)$ for any point P on $X^6+Y^6 = Z^6$.

THEOREM 4.15. *Let K be a field not containing $\sqrt{-1}$. Let F/K be the function field of a conic over K. Then $p(F) = 2$ implies that K is hereditarily Pythagorean, or even hereditarily Euclidean in the case where F is nonreal.*

PROOF. Note that $\mathrm{char}(K) \neq 2$, by the assumption that $-1 \notin K^{\times 2}$. The conic C is given by $Z^2 = aX^2 + bY^2$ where $a, b \in K^\times$. First assume that K is finite. Then every quadratic form of dimension at

[1] J. Van Geel and A. Wadsworth helped me establish this connection.

least 3 over K is isotropic, whereby the conic has a rational point and thus F/K is the rational function field $K(X)$. Hence $-1+X^2$ is a sum of 3 but not 2 squares by the second representation theorem ([**Lam05**, IX.2.1.]). Suppose that K is infinite and nonreal. Then at least one of the four biquadratic extensions $L = K(\sqrt{\pm a}, \sqrt{\pm b})$ does not contain $\sqrt{-1}$, whereby $p(L) \geq s(L) \geq 2$. Let $y \in L$ be such that $1+y^2 \in \sum L^{\times 2} \setminus L^{\times 2}$. Then $M = L(\sqrt{-(1+y^2)})$ has level 2, and M/K is a separable field extension. If $\sqrt{a} \in M$, then $(1:0:\sqrt{a}) \in C$ is an M-rational point. If $\sqrt{b} \in M$, then $(0:1:\sqrt{b}) \in C$ is an M-rational point. If $\sqrt{-a}, \sqrt{-b} \in M$, then $(\sqrt{-b} : y\sqrt{-a} : \sqrt{-(1+y^2)ab}) \in C$ is an M-rational point. In any case, C has an M-rational point, whereby (4.13) implies that C_M is rational. Thus C has a point P with $K(P) = M$ by (3.37). Since $-1 \notin M^{\times 2}$, it follows that $p(F) \geq 3$, by (4.3).

Finally, assume that K is a real field but is not hereditarily Pythagorean. Let L be a finite real extension of K that is not Pythagorean. F is the function field of a smooth projective conic C over K. The conic C is given by $Z^2 = aX^2 + bY^2$, where $a, b \in K^\times$ can be chosen such that ab is positive at a fixed ordering on L. This ordering extends either to $L(\sqrt{a}, \sqrt{b})$ or to $L(\sqrt{-a}, \sqrt{-b})$, whereby at least one of these field extensions is real. Neither of them are Pythagorean, by (1.3). We can therefore assume, without loss of generality, that either $a, b \in L^{\times 2}$ or $-a, -b \in L^{\times 2}$.

Choose $y \in L$ such that $1+y^2 \notin L^{\times 2}$ and consider $M = L(\sqrt{-(1+y^2)})$. If $a, b \in L^{\times 2}$, then $(\sqrt{a} : 0 : a)$ is an M-rational point of C. If $a, b \in -L^{\times 2}$, then $(\sqrt{-b} : y\sqrt{-a} : \sqrt{ab}\sqrt{-(1+y^2)})$ is an M-rational point, of C. In any case, C has an M-rational point, and C thus is M-rational by (4.13). By (3.37), C has a point P with $K(P) = M$. Since $\sqrt{-1} \notin M$ it follows that $p(F) \geq 3$ by (4.3).

Hence K is hereditarily Pythagorean. If F is nonreal, in addition, then $a, b \in -\sum K^{\times 2}$. Since K is Pythagorean, the corresponding conic is thus $Y^2 = -(X^2+1)$ and by $(iii) \Rightarrow (i)$ of (1.4) it follows that K is hereditarily Euclidean. □

CHAPTER 5

Local-global principles

In this chapter, we shortly introduce quadratic forms over fields and their connection to the study of sums of squares, and present Springer's Theorem for discrete valued fields. Then we present a new local-global principle that we derive from a similar on by Harbater, Harmann, and Krashen. Finally, we present a closely related local-global principle by Colliot-Thélène, Parimala, and Suresh, and include a short proof.

1. Quadratic forms

Let K be a field and $n \in \mathbb{N}$. A *quadratic form of dimension n over K* is a homogeneous quadratic polynomial in $K[x_1, \ldots, x_n]$. We call a graded K-algebra automorphism on $K[x_1, \ldots, x_n]$, where the grading is given by the total degree, a *linear change of variables.* Two quadratic forms q_1 and q_2 of dimension n over K are called *isometric*, if there exists a linear change of variables $L : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ such that $q_1 = L(q_2)$, and we then write $q_1 \cong q_2$. We call q *isotropic*, if the projective quadric $V_+(q) \subsetneq \mathbb{P}_K^{n-1}$ over K has a rational point.
Let $a_1, \ldots, a_n \in K$. we call the n-dimensional form $a_1x_1^2 + \cdots + a_nx_n^2$ a *diagonal* quadratic form, denoted $\langle a_1, \ldots, a_n\rangle$. Note that for $c_1, \ldots, c_n \in K^\times$, we have that $\langle a_1, \ldots, a_n\rangle \cong \langle c_1^2a_1, \ldots, c_n^2a_n\rangle$. If $\operatorname{char}(K) \neq 2$, then for every n-dimensional quadratic form q, there exists a linear change of variables d such that $d(q) = \langle a_1, \ldots, a_n\rangle$ and we call it a *diagonalization of q*.
For $m \leq n$, a graded K-algebra homorphisms of degree zero

$$K[x_1, \ldots, x_m] \hookrightarrow K[x_1, \ldots, x_n],$$

given by the obvious inclusion followed by a linear change of variables, is called a *dimension extension.*
We call an n-dimensional quadratic form *regular*, if it is not a dimension extension of an m-dimensional quadratic form for any $m < n$.
Conversely, for $m \leq n$, a graded K-algebra homorphisms of degree zero $K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_m]$, given by a linear change of variables

followed by the partial evaluations $x_j \mapsto 0$ for $j > m$, is called a *dimension restriction.* We call an m-dimensional quadratic form q_1 a *subform* of an n-dimensional quadratic form q_2, if $m \leq n$ and q_1 is obtained by a dimension restriction of q_2.

For an n-dimensional quadratic form q_1 and an m-dimensional quadratic form q_2, we denote by $q_1 \perp q_2$ the $n+m$-dimensional quadratic form $q_1(x_1, \dots, x_n) + q_2(x_{n+1}, \dots, x_{n+m}) \in K[x_1, \dots, x_{n+m}]$, called the *orthogonal sum of* q_1 *and* q_2. For a quadratic form q and $\ell \in \mathbb{N}$, we write $\ell \times q$ for the ℓ-fold orthogonal sum $q \perp q \perp \cdots \perp q$.
Note that, for $a \in K^\times$ and $n \in \mathbb{N}$, the fact that $a \in D_K(n)$ is equivalent to the $n+1$ dimensional form $n \times \langle 1 \rangle \perp \langle -a \rangle$ being isotropic.

Let L/K be a field extension, and q an n-dimensional quadratic form. We denote by q_L the *scalar extension of* q *to* L, considered now as a polynomial over L.

2. Isotropy over complete discrete valued fields

Let K be a field and v a nondyadic discrete valuation on K. Let $a_1, \dots, a_n \in K^\times$ and consider the regular diagonal quadratic form $\langle a_1, \dots, a_n \rangle$ over K. Fixing a uniformizer π for v, we write $a_i = b_i \pi^{v(a_i)}$ for $b_i \in K^\times$ if $v(a_i) \in 2\mathbb{Z}$, or $a_i = c_i \pi^{v(a_i)}$ for $c_i \in K^\times$ if $v(a_i) \notin 2\mathbb{Z}$, for every $i \in \{1, \dots n\}$. After renumerating the variables, we can assume that there exists $k \in \{1, \dots, n\}$ such that $v(a_i) \in 2\mathbb{Z}$ for $i \leq k$ and $v(a_i) \notin 2\mathbb{Z}$ for $i > k$.
The diagonal forms $\langle \overline{b}_1, \dots, \overline{b}_k \rangle$ and $\langle \overline{c}_{k+1}, \dots, \overline{c}_n \rangle$ over κ_v are regular, and their isometry classes are called the *first* and the *second* residue form of $\langle a_1, \dots, a_n \rangle$ *with respect to* (v, π).

Note that the first residue form does not depend on the chosen uniformizer π, while the second residue form is only independent of π up to a scalar in $\kappa_v^\times$. However, whether the second residue form is isotropic or not does not depend on the chosen uniformizer π, thus we sloppily omit to specify the uniformizer in the following (5.1).

THEOREM 5.1 (Springer). *Let* (K, v) *be a nondyadic complete discrete valued field, and* $a_1, \dots, a_n \in K^\times$*. The regular* n*-dimensional diagonal quadratic form* $\langle a_1, \dots, a_n \rangle$ *over* K *is isotropic if and only if one of its two residue forms over* κ_v *is isotropic.*

REFERENCE:. [**Lam05**, VI.1.9.] or [**Sch85**, 6.2.6].

3. Geometric local-global principle

Let T denote a complete discrete valuation ring, k its residue field, K its field of fractions, and F/K an algebraic function field. Recall that by (3.41), there exists a regular projective integral curve C over K with function field F. By (3.51), there exists a regular model $\mathcal{C}$ over T for F/K. Note that $\mathcal{C}$ is not unique. Let $X \subsetneq \mathcal{C}$ denote the special fiber of $\mathcal{C}$. For any $P \in X$, we denote by $\widehat{\mathcal{R}}_P$ the completion of the regular local domain $\mathcal{O}_{\mathcal{C},P}$ with respect to its maximal ideal $\mathfrak{m}_{\mathcal{C},P}$. Note that the natural morphism $\mathcal{O}_{\mathcal{C},P} \to \widehat{\mathcal{R}}_P$ is an embedding by (2.9), and that $\widehat{\mathcal{R}}_P$ is a regular local domain by (2.10). Its field of fractions F_P is a field extension of F. As opposed to [**HHK09**], the notation $\widehat{\mathcal{R}}_P$ and F_P in our case is not reserved for closed points $P \in X$ only. The rings and fields just defined will remain the same throughout the rest of this chapter.
The following local global principle is the main result of this section and will be deduced from [**HHK09**, 4.2]. In [**HHK11**, 9.3], the authors of [**HHK09**] also mention this consequence[1] of their previous work. The result holds more generally when T-models $\mathcal{C}$ for F/K is only considered to be normal. The proof is identical, except for a more sophisticated reasoning for why the rings $\widehat{\mathcal{R}}_P$ are domains also in the case where $\mathcal{C}$ is not regular but only normal.

THEOREM 5.2. *Let q be a regular quadratic form over F of dimension at least 3. Then q is isotropic if and only if q_{F_P} is isotropic for every $P \in X$.*

Let $U \subsetneq X$ be a nonempty open subset of the special fiber of $\mathcal{C}$. Let $\mathcal{R}_U$ denote the direct limit $\varinjlim \mathcal{O}_{\mathcal{C}}(\mathcal{W})$ of the direct system of rings $\mathcal{O}_{\mathcal{C}}(\mathcal{W})$ where $\mathcal{W} \subset \mathcal{C}$ are open neighbourhoods of U. Let $t \in T$ be a generator of the maximal ideal in T. We denote by $\widehat{\mathcal{R}}_U$ the t-adic completion $\varprojlim \mathcal{R}_U/(t^n)$.

LEMMA 5.3. *The natural map $\mathcal{R}_U \to \widehat{\mathcal{R}}_U$ is an embedding. Moreover, if U is irreducible, then $\widehat{\mathcal{R}}_U$ is a domain.*

PROOF. Let $\eta \in U$ denote the generic point of a component of X that has nonempty intersection with U. By (3.45 & 3.46), the point $\eta \in \mathcal{C}$ is regular of codimension one, whereby the ring $\mathcal{O}_{\mathcal{C},\eta}$ is a discrete valuation ring. Hence $\bigcap_{n\in\mathbb{N}} t^n \mathcal{O}_{\mathcal{C},\eta} = \{0\}$ by (2.1). As $\eta \in U$, the

[1] which they obtained independently.

obvious embedding $\mathcal{R}_U \hookrightarrow \mathcal{O}_{\mathcal{C},\eta}$ yields that $\bigcap_{n\in\mathbb{N}} t^n\mathcal{R}_U = \{0\}$, whereby the natural map $\mathcal{R}_U \to \widehat{\mathcal{R}}_U$ is an embedding by (2.9).
Now assume that U is irreducible, and let η denote the generic fiber of the irreducible component of X that contains U. The completion $\widehat{\mathcal{O}}_{\mathcal{C},\eta}$ of $\mathcal{O}_{\mathcal{C},\eta}$ with respect to $\mathfrak{m}_{\mathcal{C},\eta}$ is a discrete valuation ring and thus a domain. We are going show that $\widehat{\mathcal{R}}_U \hookrightarrow \widehat{\mathcal{O}}_{\mathcal{C},\eta}$, whereby it is a domain. First, we claim that the homomorphisms $\mathcal{R}_U/(t^n) \to \mathcal{O}_{\mathcal{C},\eta}/(t^n)$ are injective for all $n \in \mathbb{N}$, whereby it then follows that $\widehat{\mathcal{R}}_U$ embedds into $\varprojlim \mathcal{O}_{\mathcal{C},\eta}/(t^n)$. So let $f \in \mathcal{R}_U$. Suppose there exists $g \in \mathcal{O}_{\mathcal{C},\eta}$ such that $f = t^n g$. It is sufficient to show that then necessarily $g \in \mathcal{R}_U$. Let $\mathcal{W} \subset \mathcal{C}$ be an irreducible open neighbourhood of U such that $f \in \mathcal{O}_\mathcal{C}(\mathcal{W})$ and $\mathcal{W} \cap X = U$.
We claim that then $g \in \mathcal{O}_\mathcal{C}(\mathcal{W})$. Since $\mathcal{C}$ is regular and thus in particular normal, it is sufficient by [**Eis95**, 11.4] to show that $g \in \mathcal{O}_{\mathcal{C},P}$ for every codimension one point $P \in \mathcal{W}$. So let $P \in \mathcal{W}$ be of codimension one. If $P \in X$, then $P = \eta$ by the choice of $\mathcal{W}$, and thus $g \in \mathcal{O}_{\mathcal{C},P}$ by assumption. Otherwise, we have that $t \in \mathcal{O}_{\mathcal{C},P}^\times$, thus $g = \frac{1}{t^n} f \in \mathcal{O}_{\mathcal{C},P}$. Hence, $g \in \mathcal{O}_\mathcal{C}(\mathcal{W})$.
Thus $\widehat{\mathcal{R}}_U \hookrightarrow \varprojlim \mathcal{O}_{\mathcal{C},\eta}/(t^n)$ and we have that $\varprojlim \mathcal{O}_{\mathcal{C},\eta}/(t^n) \cong \widehat{\mathcal{O}}_{\mathcal{C},\eta}$ by (2.7), as $t\mathcal{O}_{\mathcal{C},\eta} = \mathfrak{m}_{\mathcal{C},\eta}^m$ for some $m \in \mathbb{N}$. □

For $U \subsetneq X$ irreducible, we denote by F_U the field of fractions of the domain $\widehat{\mathcal{R}}_U$. It is easy to see that for $\emptyset \neq U' \subseteq U$, we have $F_U \subseteq F_{U'}$. Note that if U has an open *affine* neighborhood $\mathcal{W} \subseteq \mathcal{C}$, then F is the field of fractions of $\mathcal{R}_U$, whereby F_U is a field extension of F.

We are now prepared to formulate the geometric local-global principle for quadratic forms by Harbater, Hartmann, and Krashen. Let $\mathcal{S} \subsetneq X$ denote the finite subset of points of the special fiber that lie on at least two distinct components of X. Let $f : \mathcal{C} \to \mathbb{P}^1_T$ denote a finite T-morphism as in (3.49) such that $\mathcal{S} \subset f^{-1}(\{\infty\})$, where $\infty \in \mathbb{P}^1_k = \operatorname{proj}(k[x_0, x_1])$ denotes an arbitrary rational point. Denote $\mathbb{A}^1_k = \mathbb{P}^1_k \setminus \{\infty\}$. There exists a homogeneous linear polynomial $\ell \in k[x_0, x_1]$ such that $\mathbb{A}^1_k = D_+(\ell)$. Let $L \in T[x_0, x_1]$ be a homogeneous lift of ℓ and consider the affine open neighbourhood $D_+(L)$ of $\mathbb{A}^1_k$ in $\mathbb{P}^1_T$. Since f is finite, $f^{-1}(D_+(L))$ is an affine neighbourhood of $f^{-1}(\mathbb{A}^1_k)$. In particular, the field F_U is an extension fields of F for any irreducible component U of $f^{-1}(\mathbb{A}^1_k) \subsetneq X$.

THEOREM 5.4 (Harbater, Hartmann, Krashen). *Let q be a regular quadratic form over F of dimension at least* 3. *Then q is isotropic if* *and only if for all $P \in f^{-1}(\{\infty\})$ and all irreducible components U of $f^{-1}(\mathbb{A}^1_k)$, the forms q_{F_P} and q_{F_U} are isotropic.*

REFERENCE:. [**HHK09**, 4.2].

REMARK 5.5. In [**HHK09**, 4.2], the T-curve $\mathcal{C}$ was only assumed to be normal, not necessarily regular. It is more difficult to justify the existence of F_P for a closed point $P \in X$ in this case. As we apply the theorem only in the situation where $\mathcal{C}$ is regular, we just stated it in that special case.

Note that $\widehat{\mathcal{R}}_P$ is a complete ring with respect to $\widehat{\mathfrak{m}} = \mathfrak{m}_{\mathcal{C},P}\widehat{\mathcal{R}}_P$ and $\widehat{\mathcal{R}}_P/\widehat{\mathfrak{m}} = \mathcal{O}_{\mathcal{C},P}/\mathfrak{m}_{\mathcal{C},P}$. As a first consequence of (5.4) & (2.11) we obtain the following.

COROLLARY 5.6. *Let q be a regular quadratic form over F. Let $P \in X$ be a closed point and assume there exist $a_1, \dots, a_n \in \mathcal{O}^{\times}_{\mathcal{C},P}$ such that $q \cong_F \langle a_1, \dots, a_n\rangle$. Then q_{F_P} is isotropic if $\langle \overline{a}_1, \dots, \overline{a}_n\rangle$ is isotropic as a form over $\mathcal{O}_{\mathcal{C},P}/\mathfrak{m}_{\mathcal{C},P}$.*

PROOF. Let $x_1, \dots, x_n \in \mathcal{O}_{\mathcal{C},P}$ such that $a_1x_1^2 + \dots + a_nx_n^2 \in \mathfrak{m}_{\mathcal{C},P}$ and, without loss of generality, $x_1 \in \mathcal{O}^{\times}_{\mathcal{C},P}$. The monic polynomial $f(X) = a_1X^2 + a_2x_2^2 + \dots + a_nx_n^2$ considered as a polynomial over $\widehat{\mathcal{R}}_P$ has a zero x_1 modulo $\widehat{\mathfrak{m}} = \mathfrak{m}_{\mathcal{C},P}\widehat{\mathcal{R}}_P$. Moreover $\frac{d}{dX}f(x_1) = 2a_1x_1 \in \widehat{R}^{\times}_P$. By (2.11) there exists $z \in \widehat{R}^{\times}_P$ such that $a_1z^2 + a_2x_2^2 + \dots + a_nx_n^2 = 0$. Thus $\langle a_1, \dots, a_n\rangle_{F_P}$ is isotropic. □

PROPOSITION 5.7. *Let Y be an irreducible component of X. Let η denote the generic point for Y in $\mathcal{C}$. Let q be a quadratic form over F such that q_{F_η} is isotropic. Then there exists a nonempty open subset $U \subseteq Y$ such that q_{F_U} is isotropic.*

PROOF. The point $\eta \in \mathcal{C}$ has codimension one, by (3.45 & 3.46). In particular, $\mathcal{O}_{\mathcal{C},\eta}$ is a discrete valuation ring. The completion of F with respect to the corresponding valuation is F_η. Let $s \in F$ such that $\mathfrak{m}_{\mathcal{C},\eta} = s\mathcal{O}_{\mathcal{C},\eta}$. Then there exists some $n \in \mathbb{N}$ and $u \in \mathcal{O}^{\times}_{\mathcal{C},\eta}$ such that $s^n = ut$. One can find a diagonalization $q \cong \langle a_1, \dots, a_m, sb_1, \dots, sb_\ell\rangle$, where $a_1, \dots, a_m, b_1, \dots, b_\ell \in \mathcal{O}^{\times}_{\mathcal{C},\eta}$ for some $m, \ell \in \mathbb{N}$. By (5.1), one of the two residue forms $\varphi = \langle \overline{a}_1, \dots, \overline{a}_m\rangle, \psi = \langle \overline{b}_1, \dots, \overline{b}_\ell\rangle$ over κ_v is isotropic. Let us assume, without loss of generality, that φ is isotropic. Let $x_1, \dots, x_m \in \mathcal{O}_{\mathcal{C},\eta}$, such that $a_1x_1^2 + \dots + a_mx_m^2 \in \mathfrak{m}_\eta = s\mathcal{O}_{\mathcal{C},\eta}$ and, without loss of generality, $x_1 \in \mathcal{O}^{\times}_{\mathcal{C},\eta}$. Let $w \in \mathcal{O}_{\mathcal{C},\eta}$ such that $a_1x_1^2 + \dots + a_mx_m^2 = ws$. As $\mathcal{O}_{\mathcal{C},\eta}$ is the direct limit over $\mathcal{O}_{\mathcal{C}}(\mathcal{W})$, where $\mathcal{W} \subset \mathcal{C}$ runs

over the open neighbourhoods of η in $\mathcal{C}$, we can find a neighbourhood $\mathcal{U}$ of η, such that $a_1, a_1^{-1}, \dots, a_m, a_m^{-1}, u, u^{-1}, x_1, \dots, x_m, x_1^{-1}, w, s \in \mathcal{O}_{\mathcal{C}}(\mathcal{U})$.
Set $U = Y \cap \mathcal{U}$. The polynomial $a_1T^2 + (a_2x_2^2 + \cdots + a_mx_m^2)$ has in $(\mathcal{R}_U/(s))^\times$ the simple zero $x_1 + s\mathcal{R}_U$. By (2.11) this zero lifts to a solution in $\widehat{\mathcal{R}}_U$ of $a_1T^2 + (a_2x_2^2 + \cdots + a_nx_n^2) = 0$, as $\widehat{\mathcal{R}}_U$ is complete with respect to $s\widehat{\mathcal{R}}_U$ by (2.7) and $\widehat{\mathcal{R}}_U/s\widehat{\mathcal{R}}_U \cong \mathcal{R}_U/s\mathcal{R}_U$ by (2.8). Thus $\langle a_1, \dots, a_n\rangle_{F_U}$ is isotropic and so is q_{F_U}. □

Proof of (5.2). Suppose a quadratic form q of dimension at least 3 is isotropic at F_P for every $P \in X$. By (3.45), each nonclosed point $\eta \in X$ is the generic point of an irreducible component Y_η of X. By (5.7), there exists a nonempty open $U_\eta \subseteq Y_\eta$ such that $q_{F_{U_\eta}}$ is isotropic. Set $\mathcal{S} = (X \setminus \bigcup_{\eta \in X^{(0)}} U_\eta) \cup \bigcup_{\eta \neq \rho \in X^{(0)}} (Y_\eta \cap Y_\rho)$. Then $\mathcal{S}$ is a finite set of closed points. There exists a finite T-morphism $f : \mathcal{C} \to \mathbb{P}^1_T$ such that $\mathcal{S} \subset f^{-1}(\{\infty\})$, by (3.49). Every irreducible component U of $f^{-1}(\mathbb{A}^1_k)$ is contained in U_η for some non closed point η, whereby q_{F_U} is isotropic. The assertion now follows with (5.4). □

4. Valuation theoretic local-global principle

The following local global principle will appear in [**CTPS**, 3.1]. We use our variant (5.2) of (5.4) to give a short presentation of its proof. Recall that $\Omega(F)$ denotes the set of discrete valuations on F up to equivalence.

THEOREM 5.8 (Colliot-Thélène, Parimala, Suresh). *Let q be a regular quadratic form defined over F of dimension at least 3. Then q is isotropic if and only if q_{F^v} is isotropic for every $v \in \Omega(F)$ on F.*

PROOF. Let $a_1, \dots, a_n \in F$ such that $q \cong \langle a_1, \dots, a_n\rangle$. Let $\mathcal{S} = \bigcup_{i=1}^n \operatorname{supp}(\operatorname{div}(a_i)) \subset \mathcal{C}^{(1)}$. Set

$$D = \sum_{x \in \mathcal{S}} [x],$$

i.e. the effective divisor on $\mathcal{C}$ consisting of the supports of the $\operatorname{div}(a_i)$ for each $1 \le i \le n$. There exists a birational T-morphism $g : \mathcal{C}' \to \mathcal{C}$ such that the divisor g^*D on $\mathcal{C}'$ is effective (3.27) and has normal crossings, by (3.52). This birational morphism induces a K-isomorphism $g_\eta^\# : \mathcal{O}_{\mathcal{C},\eta} \to \mathcal{O}_{\mathcal{C}',\eta'}$, where $\eta = g(\eta')$ and η' are the generic points of $\mathcal{C}$ and $\mathcal{C}'$ respectively. Since $F \cong \mathcal{O}_{\mathcal{C},\eta} \cong \mathcal{O}_{\mathcal{C}',\eta'}$, the map $g_\eta^\#$ is a K-automorphism on F. The supports of the principal divisors $\operatorname{div}(g_\eta^\#(a_i))$ on $\mathcal{C}'$ are contained in the support (3.27) of g^*D. Certainly

q is anisotropic if and only if $q' = \langle g_\eta^\#(a_1), \ldots, g_\eta^\#(a_n)\rangle$ is anisotropic. Moreover, the residue forms of q with respect to a discrete valuation v on F are anisotropic if and only if the residue forms of q' with respect to the discrete valuation $v \circ (g_\eta^\#)^{-1}$ are anisotropic. Thus q'_{F^v} is anisotropic for every $v \in \Omega(F)$ if and only if q_{F^v} is anisotropic for every $v \in \Omega(F)$.

We can thus assume that the divisor D on $\mathcal{C}$ has normal crossings to begin with. Let $X \subsetneq \mathcal{C}$ denote the special fiber. Suppose q is anisotropic over F. By (5.2) the form q_{F_P} is anisotropic for some $P \in X$. If P is a nonclosed point in $\mathcal{C}$, then $\mathcal{O}_{C,P}$ is a discrete valuation ring and F_P is the completion of the corresponding discrete valuation, by (2.18).

If P is a closed point, there exist $x, y \in \mathfrak{m}_{\mathcal{C},P}$ such that $\mathfrak{m}_{\mathcal{C},P} = (x, y)$ and $a_i = u_i x^{\ell_i} y^{s_i}$ for some $\ell_i, s_i \in \mathbb{Z}$, by (3.28). For $1 \leq i \leq 4$ there are quadratic forms $q^{(i)}$ of dimension n_i over F with $q^{(i)} = \langle u_1^{(i)}, \ldots u_{n_i}^{(i)}\rangle$ for some $u_j^{(i)} \in \mathcal{O}_{\mathcal{C},P}^\times$ for $1 \leq j \leq n_i$, such that

$$q \cong q^{(1)} \perp yq^{(2)} \perp xq^{(3)} \perp xyq^{(4)}.$$

For $1 \leq i \leq 4$ we denote the quadratic form $\langle u_1^{(i)} + \mathfrak{m}, \ldots, u_{n_i}^{(i)} + \mathfrak{m}\rangle$ over $\mathcal{O}/\mathfrak{m}$ by $\tilde{q}^{(i)}$. Note that the forms $\tilde{q}^{(i)}$ for $i = 1, \ldots, 4$ are anisotropic, as otherwise the multiple of some subform of q would become isotropic over F_P by 5.6.

The ring $\mathcal{O}_{(x)}$ is a discrete valuation ring by (2.5) with residue field isomorphic to $\mathrm{Quot}(\mathcal{O}/(x))$. The two residue forms of q with respect to its corresponding valuation and the uniformizer x are $\bar{q}^{(1)} \perp \bar{y}\bar{q}^{(2)}$ and $\bar{q}^{(3)} \perp \bar{y}\bar{q}^{(4)}$, where we write $\bar{a}$ for the residue $a + x\mathcal{O}_{(x)}$ for any $a \in F$, and we write $\bar{q}^i$ for the quadratic forms $\langle \bar{u}_1^{(i)}, \ldots, \bar{u}_{n_i}^{(i)}\rangle$ over $\mathrm{Quot}(\mathcal{O}/(x))$ for $i = 1, \ldots, 4$.

By (2.5), the ring $\mathcal{O}/(x)$ is a discrete valuation ring with uniformizer $y + (x)$ and residue field $\mathcal{O}/\mathfrak{m}$. The first and second residue form of $\bar{q}^{(1)} \perp \bar{y}\bar{q}^{(2)}$ are the anisotropic forms $\tilde{q}^{(1)}$ and $\tilde{q}^{(2)}$, whereby the first residue form $\bar{q}^{(1)} \perp \bar{y}\bar{q}^{(2)}$ of q with respect to the discrete valuation v corresponding to $\mathcal{O}_{(x)}$ is anisotropic.

Analogous, the second residue form $\bar{q}^{(3)} \perp \bar{y}\bar{q}^{(4)}$ of q with respect to v is anisotropic. This yields that q_{F^v} is anisotropic. $\square$

CHAPTER 6

Algebraic function fields over $\mathbb{R}((t))$

Other than the title of this chapter suggests, the following results all hold for function fields over a complete discrete valued field with hereditarily Euclidean residue field (which need not be real closed). [1]

Remark 6.1. Let K be a complete discrete valued field with hereditarily Pythagorean residue field. Then K is hereditarily Pythagorean itself, which follows from (2.11 & 2.22). However, $K \cong \kappa_v((t))$ is not uniquely ordered and thus not Euclidean.

1. A geometric invariant for sums of squares

Let K be a complete discrete valued field with complete discrete valuation ring T and hereditarily Euclidean residue field k. Let F/K be an algebraic function field. By (3.47 & 3.50), there exists an arithmetic surface $\mathcal{C}$ over T with function field F. Let X denote its special fiber. A generic point η_Y of an irreducible component Y of X is of codimension one in $\mathcal{C}$, by (3.46). Hence, $\mathcal{O}_{\mathcal{C},\eta_Y}$ is a discrete valuation ring, since $\mathcal{C}$ is regular. The residue field of the induced valuation $v_Y : F \to \mathbb{Z} \cup \{\infty\}$ is the function field of Y over k, i.e. an algebraic function field over k, by (3.30). Let $\mathcal{X}$ denote the set of irreducible components Y of X such that $k(Y)$ is nonreal and $\sqrt{-1} \notin k(Y)$.

Lemma 6.2. *Let $\sigma \in \sum F^{\times 2}$. Let $P \in X$ be a closed point such that $\mathcal{O}_{\mathcal{C},P}/\mathfrak{m}_{\mathcal{C},P}$ is real. Assume that $v_Y(\sigma) \in 2\mathbb{Z}$ for every $Y \in \mathcal{X}$ with $P \in Y$. Then there exists $\sigma' \in \mathcal{O}_{\mathcal{C},P}^{\times}$ such that $\sigma\sigma' \in D_F(2)$.*

Proof. The ring $\mathcal{O}_{\mathcal{C},P}$ is a regular local 2-dimensional ring, by (3.46), and so is $\mathcal{O}_{\mathcal{C},P}[\sqrt{-1}]$, by (2.6). Both rings are factorial, by (2.4). We can assume that σ factors into distinct prime elements with multiplicity one. Since $D_F(2)$ is a multiplicative group, it is sufficient to show that

[1] The idea of using the recently discovered local-global principles in [**HHK09**] and [**CTPS**] to study sums of squares in such fields are due to my advisor.

each prime factor p of σ is a unit in $\mathcal{O}_{\mathcal{C},P}$ times an element in $D_F(2)$. Note that $D_F(2)$ are exactly the norm elements of $F(\sqrt{-1})/F$. [2] Let $q \in \mathcal{O}_{\mathcal{C},P}[\sqrt{-1}]$ be a prime factor of p in $\mathcal{O}_{\mathcal{C},P}[\sqrt{-1}]$. Note that by (2.5), the localization of $\mathcal{O}_{\mathcal{C},P}$ after the height one prime (p) induces a discrete valuation v in F, and the localization of $\mathcal{O}_{\mathcal{C},P}[\sqrt{-1}]$ after (q) induces a discrete valuation w on $F(\sqrt{-1})$ extending v. By (2.21), the valuation $w \circ \iota$ is the only other valuation extension of v to $F(\sqrt{-1})$, where ι denotes the nontrivial F-automorphism on $F(\sqrt{-1})$. Since $\mathcal{O}_{\mathcal{C},P}[\sqrt{-1}]$ is invariant under ι, it is obvious that $w \circ \iota$ is induced by the localization of $\mathcal{O}_{\mathcal{C},P}[\sqrt{-1}]$ after the prime ideal (q^ι), thus q and q^ι are, up to a unit, the only prime factors of p. Moreover, κ_v is nonreal by (2.24), as $v(\sigma) \notin 2\mathbb{Z}$ although $\sigma \in \sum F^{\times 2}$. By (2.23), κ_v is either an algebraic function field over k, or an algebraic extension of k, or a finite extension of K. In the last two cases, we have $\sqrt{-1} \in \kappa_v$, by (6.1 & 4.1).
In the first case, where κ_v is an algebraic function field over k, we have that $t \in p\mathcal{O}_{\mathcal{C},P_{(p)}}$, that is, $t = p\frac{f}{g}$, where $f, g \in \mathcal{O}_{\mathcal{C},P}$ with $p \not| g$. Since $\mathcal{O}_{\mathcal{C},P}$ is factorial, it follows that $t = ph$ for some $h \in \mathcal{O}_{\mathcal{C},P}$ Let $U \subset \mathcal{C}$ be an affine neighborhood of P such that $h, p \in \mathcal{O}_{\mathcal{C}}(U) \hookrightarrow \mathcal{O}_{\mathcal{C},P}$ and such that p generates the inverse image of $p\mathcal{O}_{\mathcal{C},P}$. Hence $p\mathcal{O}_{\mathcal{C}}(U)$ is a codimension one prime ideal that corresponds to a generic point of a irreducible component Y of the special fiber X of $\mathcal{C}$ which contains P. Hence $\kappa_v = k(Y)$, by (3.23). We have that $Y \notin \mathcal{X}$, as $v(\sigma) \notin 2\mathbb{Z}$. Hence $\sqrt{-1} \in k(Y) = \kappa_v$ by definition of $\mathcal{X}$.
In any case, $\sqrt{-1} \in \kappa_v$. As $\kappa_w = \kappa_v(\sqrt{-1}) = \kappa_v$ by (2.21), it follows that $p = \gamma q^\iota q$ for some $\gamma \in F \cap \left(\mathcal{O}_{\mathcal{C},P}[\sqrt{-1}]\right)^\times = \mathcal{O}_{\mathcal{C},P}^\times$, as either $w \neq w \circ \iota$ or $[\Gamma_w : \Gamma_v] = 2$, again by (2.21). But $q^\iota q = \mathcal{N}_{F(\sqrt{-1}/F)}(q) \in D_F(2)$, showing what we wanted to show. □

Proposition 6.3. *Let $\sigma \in \sum F^{\times 2}$ and $P \in X$ a closed point. If $v_Y(\sigma) \in 2\mathbb{Z}$ for every $Y \in \mathcal{X}$ with $P \in Y$, then $\langle 1, 1, -\sigma \rangle_{F_P}$ is isotropic.*

Proof. By (3.31 & 3.23), $\mathcal{O}_{\mathcal{C},P}/\mathfrak{m}_{\mathcal{C},P}$ is the finite extension field $k(P)$ of k. If $k(P)$ is nonreal, then $\sqrt{-1} \in k(P)$, by 4.1, whereby $\langle \overline{1}, \overline{1} \rangle$ is isotropic over $k(P)$. It follows with (5.6) that $\langle 1, 1, -\sigma \rangle_{F_P}$ is isotropic, as well.
If $k(P)$ is real, then there exists $\sigma' \in \sum F^{\times 2}$ such that $\sigma' \in \mathcal{O}_{\mathcal{C},P}^\times$ and $\sigma\sigma' \in D_F(2)$ by (6.2). As $D_{F_P}(2)$ is a multiplicative subgroup of

[2]J. Van Geel suggested to me this crucial norm argument.

$\sum F_P^{\times 2}$, it is clear that $\langle 1,1,-\sigma\rangle_{F_P}$ is isotropic if and only if $\langle 1,1,-\sigma'\rangle_{F_P}$ is isotropic.
$\mathcal{O}_{\mathcal{C},P}$ is a two dimensional regular local ring with fields of fractions F. By (2.14), there exists a valuation v on F with discretely ordered value group of rank 2, such that $\mathcal{O}_{\mathcal{C},P} \subset \mathcal{O}_v$ and $\mathfrak{m}_v \cap \mathcal{O}_{\mathcal{C},P} = \mathfrak{m}_{\mathcal{C},P}$ and such that the canonical embedding $\mathcal{O}_{\mathcal{C},P}/\mathfrak{m}_{\mathcal{C},P} \hookrightarrow \mathcal{O}/\mathfrak{m}_v$ is an isomorphism. Hence, for $\sigma' \in \mathcal{O}_{\mathcal{C},P}^{\times}$, we denote by $\overline{\sigma}$ its residue in $\kappa(P) \cong \kappa_v$.
By (2.24), we get that $\overline{\sigma}' \in \sum \kappa(P)^{\times 2} = \kappa(P)^{\times 2}$ and thus the form $\langle \overline{1},\overline{1},-\overline{\sigma}'\rangle$ is isotropic over $\kappa(P)$. By (5.6), this yields that $\langle 1,1,-\sigma'\rangle_{F_P}$ is isotropic, and thus so is $\langle 1,1,-\sigma\rangle_{F_P}$. □

Each $a \in F^{\times}$ induces a map

$$\begin{aligned} \rho_a : \mathcal{X} &\to \mathbb{Z}/2\mathbb{Z} \\ Y &\mapsto v_Y(a) + 2\mathbb{Z}. \end{aligned}$$

Let $(\mathbb{Z}/2\mathbb{Z})^{\mathcal{X}}$ denote the group of mappings from $\mathcal{X}$ to $\mathbb{Z}/2\mathbb{Z}$. Recall (6.1), that K is hereditarily Pythagorean, since k is even hereditarily euclidean.

Theorem 6.4. *The group homomorphism*

$$\begin{aligned} \rho : \sum F^{\times 2} &\longrightarrow (\mathbb{Z}/2\mathbb{Z})^{\mathcal{X}} \\ \sigma &\mapsto \rho_\sigma \end{aligned}$$

is surjective with $\ker(\rho) = D_F(2)$. *In particular,* $\sum F^{\times 2}/D_F(2) \cong (\mathbb{Z}/2\mathbb{Z})^{\mathcal{X}}$.

Proof. Let $\sigma \in \sum F^{\times 2}$ such that $\rho(\sigma) = 0$. We claim that then $\langle 1,1,-\sigma\rangle$ is isotropic. By (5.2) this is the case if $\langle 1,1,-\sigma\rangle_{F_P}$ is isotropic for every $P \in X$. Let $P \in X$ be arbitrary.
In the case where $P \in X$ is a closed point $\langle 1,1,-\sigma\rangle_{F_P}$ is isotropic, by (6.3).
In the case where P is not a closed point, then $\overline{\{P\}} = Y$ is an irreducible component of X, and hence $\mathcal{O}_{\mathcal{C},P}/\mathfrak{m}_{\mathcal{C},P}$ is the algebraic function field $k(Y)$ over k, by (3.23).
If $Y \notin \mathcal{X}$, the isotropy of $\langle 1,1,-\sigma\rangle$ is easy to see. Either $k(Y)$ is nonreal and contains $\sqrt{-1}$, whereby $\langle 1,1\rangle_{F_\eta}$ is isotropic by (5.1), or $k(Y)$ is real. In this case, we can assume that $v_Y(\sigma) = 0$ and that the residue $\overline{\sigma} \in k(Y)$ is a sum of squares, by (2.24). By (1.4), the first residue form $\langle \overline{1},\overline{1},-\overline{\sigma}\rangle$ is isotropic over $k(Y)$, and hence so is $\langle 1,1,-\sigma\rangle_{F_\eta}$, by (5.1).
If $Y \in \mathcal{X}$, we use the hypothesis $\rho_\sigma = 0$, that is, $v_Y(\sigma) \in 2\mathbb{Z}$. Hence, we can assume that $v_Y(\sigma) = 0$, whereby the first residue form of $\langle 1,1,-\sigma\rangle$

is $\langle\overline{1},\overline{1},-\overline{\sigma}\rangle$ over $k(Y)$. This residue form is isotropic, by (1.4). This implies that $\langle 1,1,-\sigma\rangle_{F_\eta}$ is isotropic, by (5.1).
Thus $\ker(V)\subseteq D_F(2)$. The other inclusion $D_F(2)\subseteq\ker(V)$ is much easier to see. Suppos $\sigma\in D_F(2)\setminus\ker(V)$, then $v_i(\sigma)\notin 2\mathbb{Z}$ for one $1\le i\le n$. We can assume that $\sigma=1+a^2$ for some $a\in\mathcal{O}_{v_i}$, then in fact $v_i(a)=0$, since $v_i(\sigma)>0$. But then $-\overline{1}=\overline{a}^2\in\kappa_{v_i}$, which contradicts $\sqrt{-1}\notin\mathcal{O}_{\mathcal{C},\eta_i}/\mathfrak{m}_{\mathcal{C},\eta_i}=\kappa_{v_i}$. It follows that $\ker(V)=D_F(2)$.

Now we show that ρ is surjective. For this, it is enough to show that for every $Y\in\mathcal{X}$ there exists a $\sigma_Y\in\sum F^{\times 2}$ such that $v_Y(\sigma_Y)\notin 2\mathbb{Z}$ and $v_{Y'}(\sigma_Y)\in 2\mathbb{Z}$ for every $Y'\neq Y\in\mathcal{X}$.
Zero has a nontrivial representation as a sum of 3 squares in the algebraic function field $\kappa_{v_Y}=k(Y)$ over k, by (1.4), say $\overline{0}=1+\overline{x}^2+\overline{y}^2$. Denote $\sigma=1+x^2+y^2$ if $v_Y(1+x^2+y^2)=1$, otherwise choose a uniformizing element $s\in F$ for v_Y and note that $v_Y(\sigma)=1$ when we set $\sigma=(1+s)^2+x^2+y^2=2s+s^2+1+x^2+y^2$. In any case, there exists $\sigma\in\sum F^{\times 2}$, such that $v_Y(\sigma)=1$.
By (2.16) there exists $z\in F$ such that $2v_{Y'}(z)>v_{Y'}(\sigma)$ for every $Y'\in\mathcal{X}$ with $v_{Y'}(\sigma)\in 2\mathbb{Z}$, $2v_Y(z)>v_Y(\sigma)$, and $2v_{Y'}(z)<v_Y(\sigma)$ for every $Y'\in\mathcal{X}\setminus\{Y\}$ with $v_{Y'}(\sigma)\in\notin 2\mathbb{Z}$. Set $\sigma_Y:=\sigma+z^2$. We see then that $v_{Y'}(\sigma_Y)\in 2\mathbb{Z}$ for all $Y'\in\mathcal{X}\setminus\{Y\}$, and that $v_Y(\sigma_Y)\notin 2\mathbb{Z}$. Hence the surjectivity of ρ and hence the isomorphy $\sum F^{\times 2}/D_F(2)\cong(\mathbb{Z}/2\mathbb{Z})^{\mathcal{X}}$. □

The result (6.4) shows in particular, that $|\mathcal{X}|$ is independent of the chosen regular model over T for F/K. This fact can also be seen by a different consideration, and in more general situations.

Remark 6.5. Let T denote a discrete valuation ring with field of fractions K and hereditarily Pythagorean residue field k. Let F/K be an algebraic function field. For a regular model $\mathcal{C}$ over T of F, let again $\mathcal{X}(\mathcal{C})$ denote the set of those irreducible components of the special fiber whose function fields are nonreal and do not contain $\sqrt{-1}$. Then $|\mathcal{X}(\mathcal{C})|$ does not depend on the chosen regular model $\mathcal{C}$ of F.
Let me briefly make this plausible in the case where the genus of F is at least one. In this case, by [**Liu06**, p. 457], any regular model can be successively contracted along exceptional divisors to a particular regular model, the so-called *minimal model.* A contraction of an arithmetic surface is a morphism to another arithmetic surface that is an isomorphism everywhere except in one irreducible component of the special fiber, which is mapped to a closed point. This irreducible

component is called an *exceptional divisor*, and it follows e.g. by the so-called *Castelnuovo criterion for arithmetic surfaces* [**Liu06**, 9.3.8] that such an exceptional divisor is, as a prevariety over k, necessarily isomorphic to $\mathbb{P}^1_L$ for some finite extension L/k. The function field of this component over k is therefore isomorphic to the rational function field over L, and as such is either real or contains $\sqrt{-1}$, by (4.1). Thus the components that we are interested in, are the same as in the unique minimal model, whereby they are independent of the chosen regular model.

For an algebraic function field F over a discrete valued field (K, v) with hereditarily pythagorean residue field κ_v, we define the invariant $\chi(F) = |\mathcal{X}(\mathcal{C})|$, where $\mathcal{C}$ is an arbitrary regular model of F over the valuation ring. Under the additional assumption that κ_v is euclidean, it was shown in (6.4) that $\chi(F) = \log_2(\sum F^{\times 2}/D_F(2))$.

2. Discrete valuations and the Pythagoras number

For any field K, let

$$p'(K) = \begin{cases} p(K) & \text{if } K \text{ is real,} \\ s(K){+}1 & \text{if } K \text{ is nonreal.} \end{cases}$$

PROPOSITION 6.6. *Let K be a field that is complete with respect to a discrete nondyadic valuation and F/K an algebraic function field. Then $p(F) = \max\{p'(\kappa_v) \mid v \in \Omega(F)\}$.*

PROOF. By (2.26) & (2.25), one has that $p(F) \geq \max\{p'(\kappa_v) \mid v \in \Omega\}$. Let $n = \max\{p'(\kappa_v) \mid v \in \Omega\}$. Let $\sigma \in \sum F^{\times 2}$. We want to show that $\sigma \in D_F(n)$. Supposing otherwise, we have that $q = n \times \langle 1\rangle \perp \langle -\sigma\rangle$ is anisotropic over F. By (5.8), there exists $v \in \Omega(F)$ such that q_{F^v} is anisotropic.
Assume firstly that v is real. By (2.24) there exists $\sigma' \in \sum F^{\times 2}$ with $v(\sigma') = 0$ and $\overline{\sigma}' \in \sum \kappa_v^{\times 2}$ such that $q \cong n \times \langle 1\rangle \perp \langle -\sigma'\rangle$. The first residue form of $n \times \langle 1\rangle \perp \langle -\sigma'\rangle$ over κ_v with respect to any uniformizer π is $n \times \langle \overline{1}\rangle \perp \langle -\overline{\sigma}'\rangle$, and the second residue form is of dimension zero. By (5.1), the first residue form is anisotropic. Hence, $p(\kappa_v) > n$ gives rise to a contradiction in the case where v is real.
Assume now that v is nonreal. Then $n \times \langle \overline{1}\rangle$ is a subform of the first residue form of q with respect to an arbitrary uniformizer. Again, by (5.1), the first residue form is anisotropic. Hence, $-1 \notin D_{\kappa_v}(n)$ and thus $p'(\kappa_v) > n$, yielding the contradiction in the case where v is nonreal. □

Theorem 6.7. *Let k be a hereditarily Euclidean field and $n \in \mathbb{N}$. Let F be a algebraic function field over $k((t_1))\dots((t_n))$. Then $2 \le p(F) \le 3$.*

Proof. We show that $p(F) \le 3$ by induction over n. The claim is true for $n = 0$, since then we even have $p(F) = 2$ by (1.4).
Now, we consider the case where $n > 0$. Write $K = k((t_1))\dots((t_{n-1}))$ and consider F as an algebraic function field over $K((t_n))$.
By (6.6) we have that $p(F) = \max\{p'(\kappa_v) \mid v \in \Omega(F)\}$. If $v \in \Omega(F)$ is such that $v|_{K((t_n))}$ is trivial, then κ_v is a finite extension of the hereditarily Pythagorean field $K((t_n))$ by (2.23) and thus $p'(\kappa_v) \le 2$, by definition and 4.1.
Otherwise $v|_{K((t_n))}$ is equivalent to the discrete valuation with respect to which $K((t_n))$ is complete by (2.19). In this case (2.23) yields that κ_v is either an algebraic extension of K or an algebraic function field over K. In the first case, $p'(\kappa_v) \le 2$, by 4.1 as K is hereditarily Pythagorean. In the second case we have $p(\kappa_v) \le 3$ by the induction hypothesis, and thus $p'(\kappa_v) \le 3$, since $s(\kappa_v) \le p(\kappa_v)$ for nonreal v, and hence $s(\kappa_v) = 2$, as levels of nonreal fields are two-powers, by [**Pfi95**, 3.1.3]. □

Remark 6.8. By (2.26), $p(F) = 2$ implies that $s(\kappa_v) = 1$ for all nonreal discrete valuations v on F. Conversely, if $s(\kappa_v) = 1$ for all nonreal discrete valuations v on F, then in particular $\chi(F) = 0$, and thus $p(F) = 2$, by (6.4).

3. Examples

We apply the previous results to particular algebraic function fields $F/\mathbb{R}((t))$, in order to determine $\chi(F)$, whereby we decide in particular, whether $p(F) = 2$ or 3.
We first fix some notation. If C is a projective plane curve over a field, then it is identified (up to scalar multiples from the base field) with a homogeneous polynomial equation $f(X, Y, Z) = 0$. We write $C|_{X=1}$ for the affine chart given by the dehomogenization $f(1, Y, Z) = 0$. Similarly, we denote $C|_{Y=1}$ and $C|_{Z=1}$. We write $\frac{\partial}{\partial X}C$ for the curve given by $(\frac{\partial}{\partial X}f)(X, Y, Z) = 0$, and similarly we define $\frac{\partial}{\partial Y}C$ and $\frac{\partial}{\partial Z}C$.

The following example answers a question raised in [**BG09**, 5.15], concerning the Pythagoras number of a certain function field over $\mathbb{R}((t))$.

Example 6.9. Let $F/\mathbb{R}((t))$ be the function field of the irreducible plane curve $Y^2 = (tX - 1)(X^2 + 1)$. It was already shown by S. Tikhonov that $p(F) \ge 3$. By (6.7), it follows that $p(F) = 3$. Moreover, it was

shown in [**BG09**] that $|\sum F^{\times 2}/D_F(2)| = 2$, which is consistent with the observation that $\chi(F) = 1$, which we will show in the following.
We first claim that the model $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{R}[\![t]\!]}$ of F, given by the homogeneous equation $ZY^2 = (tX - Z)(X^2 + Z^2)$, is regular. By [**Liu06**, 4.3.36], it is sufficient for regularity that the generic fiber $\mathcal{C}_{(0)}$ and the special fiber $\mathcal{C}_{(t)}$ are smooth curves. The generic fiber is just the curve $\mathcal{C}_{(0)}$ over $\mathbb{R}((t))$ defined by $ZY^2 = (tX - Z)(X^2 + Z^2)$. The special fiber $\mathcal{C}_{(t)}$ is defined by its reduction modulo t, that is, by the equation $ZY^2 = -Z(X^2 + Z^2)$ over $\mathbb{R}$. We apply Jacobi's criterion (3.42), to show that both curves are smooth. Let us first consider the generic fiber $\mathcal{C}_{(0)}$, which is given over $\mathbb{R}((t))$ by the equation $ZY^2 = (tX - Z)(X^2 + Z^2)$. Consider the affine chart given by dehomogenizing $Z = 1$.

$$\begin{aligned} \mathcal{C}_{(0)}|_{Z=1} : &\qquad Y^2 = (tX - 1)(X^2 + 1) \\ \frac{\partial}{\partial X}\mathcal{C}_{(0)}|_{Z=1} : &\qquad 0 = 3tX^2 - 2X + t \\ \frac{\partial}{\partial Y}\mathcal{C}_{(0)}|_{Z=1} : &\qquad 0 = 2Y. \end{aligned}$$

A closed point (x, y) satisfying all three equations simultaneously, would have to satisfy $y = 0$, whereby $0 = (tx-1)(x^2+1)$ and $0 = 3tx^2-2x+t$. By $\mathcal{C}_{(0)}|_{Z=1}$, we obtain that $x = \frac{1}{t}$ or $x^2 = -1$. One checks easily that both are in contradiction to $\frac{\partial}{\partial Y}\mathcal{C}_{(0)}|_{Z=1}$.
Now, consider the dehomogenization $X = 1$.

$$\begin{aligned} \mathcal{C}_{(0)}|_{X=1} : &\qquad ZY^2 = (t - Z)(Z^2 + 1) \\ \frac{\partial}{\partial Z}\mathcal{C}_{(0)}|_{X=1} : &\qquad -Y^2 = 3Z^2 - 2tZ + 1 \\ \frac{\partial}{\partial Y}\mathcal{C}_{(0)}|_{X=1} : &\qquad 0 = 2YZ. \end{aligned}$$

A closed point (y, z) satisfying these equations, would also satisfy $y = 0$ or $z = 0$, by $\frac{\partial}{\partial Y}\mathcal{C}_{(0)}|_{X=1}$, and hence $z \neq 0$, by $\mathcal{C}_{(0)}|_{X=1}$, whereby either $z = t$ or $z^2 = -1$, which contradicts the second equation in either case. At this stage, we have verified smoothness of the generic fiber in every closed point except $(0 : 1 : 0)$. Hence, we consider this point in the affine chart given by dehomogenizing after $Y = 1$, where it corresponds to the point $(0, 0)$, which obviously does not satisfy the equations

$$\begin{aligned} \mathcal{C}_{(0)}|_{Y=1} : &\qquad Z = (tX - Z)(X^2 + Z^2) \\ \frac{\partial}{\partial Z}\mathcal{C}_{(0)}|_{Y=1} : &\qquad -1 = X^2 - 2tZX + 3Z^2. \end{aligned}$$

We have thus shown that the generic fiber is smooth. Now we consider the special fiber $\mathcal{C}_{(t)}$, firstly in the affine chart given by dehomogenizing $X = 1$.

$$\begin{aligned} \mathcal{C}_{(t)}|_{X=1} : \quad & -ZY^2 = Z(1+Z^2) \\ \frac{\partial}{\partial Y}\mathcal{C}_{(t)}|_{X=1} : \quad & 0 = 2ZY \\ \frac{\partial}{\partial Z}\mathcal{C}_{(t)}|_{X=1} : \quad & -Y^2 = 1 + 3Z^2. \end{aligned}$$

One sees easily, that a point (y, z) satisfying all three equations, also satisfies $yz = 0$ and either $y \neq 0$ or $z \neq 0$. By $\mathcal{C}_{(t)}|_{X=1}$, the fact that $z = 0$ would imply $y = 0$. Hence, $y = 0$ and $z \neq 0$. It follows the contradiction that both $z^2 = -1$ and $3z^2 = -1$. Now consider the affine chart given by dehomogizing $Z = 1$.

$$\begin{aligned} \mathcal{C}_{(t)}|_{Z=1} : \quad & -Y^2 = X^2 + 1 \\ \frac{\partial}{\partial X}\mathcal{C}_{(t)}|_{Z=1} : \quad & 0 = 2X \\ \frac{\partial}{\partial Y}\mathcal{C}_{(t)}|_{Z=1} : \quad & 0 = 2Y. \end{aligned}$$

It is obvious that no point (x, y) satisfies all three equations simultaneously. All that is left to show, is that the special fiber is also smooth in the point $(0 : 1 : 0)$. In the affine chart given by dehomogenizing $Y = 1$, this point corresponds to $(0, 0)$, which does not satisfy

$$\frac{\partial}{\partial Z}\mathcal{C}_{(t)}|_{Y=1} : \quad -1 = X^2 + 3Z^2.$$

Hence the special fiber is smooth, too, whereby $\mathcal{C}$ is a regular model for F, and therefore suitable to compute $\chi(F)$. To do so, we compute the irreducible components of $\mathcal{C}_{(t)}$, that is, the irreducible factors of the polynomial $ZY^2 + Z(X^2 + Z^2)$ over $\mathbb{R}$. These are Z and $Y^2 + X^2 + Z^2$. The first factor defines a projective line over $\mathbb{R}$, whereby its function field is real. The second factor defines a component in $\mathcal{X}$, since its function field $\mathbb{R}(X)(\sqrt{-X^2-1})$ is nonreal and does not contain $\sqrt{-1}$. Hence $\chi(F) = 1$.

Recall that, by (1.13), a function field of a conic over $\mathbb{R}((t))$ has Pythagoras number 2 if the function field is real, and Pythagoras number 3 otherwise. We conjecture that the same is true for arbitrary function fields of Fermat type over $\mathbb{R}((t))$. We will show this in some special cases, that cover in particularly the function fields of all conics over $\mathbb{R}(((t)))$.

PROPOSITION 6.10. *Let $F/\mathbb{R}(\!(t)\!)$ be the function field of the curve defined by $0 = aX^n + bY^n + cZ^n$ with $a, b \in \{\pm 1, \pm t\}$. If F is real, then $\chi(F) = 0$, whereby $p(F) = 2$. If F is nonreal, then $\chi(F) = 1$, whereby $p(F) = 3$.*

PROOF. We can assume without loss of generality that $c = 1$ and $b = \pm 1$. We first claim that the model $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{R}[\![t]\!]}$ of F, given by

$$Z^n = aX^n + bY^n,$$

is regular. By (3.43) $\mathcal{C}_{(0)} \subset \mathbb{P}^2_{\mathbb{R}(\!(t)\!)}$ is regular. Consider the special fiber $\mathcal{C}_{(t)}$, given by $Z^n = \bar{a}X^n + \bar{b}Y^n$. If $\bar{a} \neq 0$ or $n = 1$, then this curve $\mathbb{R}$ is smooth by (3.43), and hence $\mathcal{C}$ is regular, by [**Liu06**, 4.3.36]. Otherwise, if $\bar{a} = 0$ and $n > 1$, the special fiber $Z^n - \bar{b}Y^n = 0$ is smooth everywhere, except in the point $(1 : 0 : 0)$. Hence the open subscheme $\mathcal{C} \setminus \{1 : 0 : 0\}$ is regular, by [**Liu06**, 4.3.36]. We show that the closed point $P = (1 : 0 : 0) \in \mathcal{C}$ is regular, nevertheless. The point $P \in \mathbb{P}^2_{\mathbb{R}[\![t]\!]}$ corresponds to the maximal ideal $(Y, Z, t) \in \operatorname{Spec}(\mathbb{R}[\![t]\!][Y, Z]) \cong \mathbb{A}^2_{\mathbb{R}[\![t]\!]}$. The affine chart $\mathcal{C}_{X=1}$ of $\mathcal{C}$ in this affine space is given by

$$Z^n = bY^n + a.$$

By [**Liu06**, 4.2.12], we need to verify that

$$Z^n - bY^n - a \notin (Y, Z, t)^2 = (Y^2, Z^2, t^2, YZ, Yt, Zt),$$

in order to show that $\mathcal{C}$ is regular in P. This however, is obvious, since $a = \pm t \notin (X^2, Z^2, t^2, XZ, Xt, Zt)$ and $n > 1$. Hence, $\mathcal{C}$ is regular in any case.
The function field F is nonreal if and only if n is even and $a = b = -1$. In the case where F is nonreal, the special fiber

$$\bar{a}X^n + \bar{b}Y^n = Z^n$$

is geometrically irreducible, by (3.39), i.e. its function field $E/\mathbb{R}$ does not contain $\sqrt{-1}$. Moreover, E is nonreal, as $\bar{a} = \bar{b} = -1$. Thus $\chi(F) = 1$.
Now suppose F is real. In the case where $b \in \{\pm t\}$, we consider the irreducible components of the special fiber $Z^n = \bar{a}X^n$ over $\mathbb{R}$. The polynomial $Z^n - \bar{a}X^n$ decomposes into linear factors over the complex numbers $\mathbb{C}$. This means, that the irreducible factors over $\mathbb{R}$ either define projective lines over $\mathbb{R}$, or decompose into projective lines over $\mathbb{C}$ after base change. In particular, their function fields over $\mathbb{R}$ are either real, or they contain $\sqrt{-1}$. Hence, $\chi(F) = 0$ if F is real. $\square$

The problem in general is, that the fibered surface defined by

$$Z^n = aX^n + bY^n$$

over $\mathbb{R}[\![t]\!]$ needs not be regular. The process of desingularization consists of an alternating sequence of blowing up a closed point followed by a normalization of the resulting scheme. In theory, blowing ups can be computed, however normalizations - to my knowledge - cannot be computed in general.
This posed a major obstruction to my attempts to see whether $\chi(F)$ is effectively computable for a given function field $F/\mathbb{R}(\!(t)\!)$. If one already starts with a regular model for F, then the answer seems to be yes, as all the conditions on the special fiber can be formulated in a first order language over $\mathbb{R}$, which are effectively decidable by the work of Tarski [**Tar98**].

Zusammenfassung auf Deutsch

Der Hauptfokus dieser Arbeit liegt auf der Untersuchung der wechselseitigen Abhängigkeit zwischen den jeweiligen Quadratsummeneigenschaften eines angeordneten Körpers und eines endlich erzeugten Erweiterungskörpers vom Transzendenzgrad eins (im Folgenden algebraischer Funktionenkörper genannt). Dabei beschränke ich mich von Anfang an auf Situationen, in welchen der angeordnete Grundkörper relativ algebraisch abgeschlossen im Funktionenkörper ist (im Folgenden wird deshalb der Grundkörper als Konstantenkörper bezeichnet). Desweiteren beschränke ich mich auf Situationen in denen entweder die Quadratsummeneigenschaften des Konstantenkörpers oder die des Funktionenkörpers als besonders einfach vorausgesetzt sind.
Im Falle des angeordneten Konstantenkörpers ist dieses die Annahme, daß jede Quadratsumme ein Quadrat ist, und dasselbe sogar für jeden algebraischen Erweiterungskörper gilt. Wir sagen in diesem Fall, daß der Konstantenkörper *erblich pythagoräisch* ist. Im Falle des Funktionenkörpers ist es die Annahme, daß jede Quadratsumme eine Summe von zwei Quadraten ist.
Für einen gegebenen Körper nennt man (falls existent) die kleinste natürliche Zahl n mit der Eigenschaft daß jede Quadratsumme eine Summe von n Quadraten ist, die *Pythagoraszahl* des Körpers. Eine Reihe von mathematischen Resultaten, welche die vorliegende Arbeit motiviert haben, legt die Vermutung nahe, daß die Pythagoraszahl eines algebraischen Funktionenkörpers über einem erblich pythagoräischen Konstantenkörper den Wert zwei oder drei hat, und daß umgekehrt die Existenz eines algebraischen Funktionenkörpers mit Pythagoraszahl zwei die erbliche Pythagoräizität des Konstantenkörpers erzwingt.

Die vorliegende Arbeit bleibt einen allgemeinen Beweis dieser vermuteten Implikationen schuldig, jedoch vergrößert sie den Kreis der unterstützenden Beispiele erheblich. Im Folgenden geben wir einen Rückblick auf die zentralen Ergebnisse der vorliegenden Arbeit im Kontext bereits bekannter Resultate.

Es geht auf ein Resultat von Witt zurück, daß die Pythagoraszahl eines algebraischen Funktionenkörpers mit reell abgeschlossenem Konstantenkörper den Wert zwei hat. Man bemerke, daß reell abgeschlossene Körper insbesondere eindeutig angeordnet und erblich pythagoräisch sind - Körper mit letztgenannten Eigenschaften bezeichnet man auch als *erblich euklidisch*.

Aus einem Resultat [**EW87**, Theorem] von Elman und Wadsworth folgt, wie von Becher und Van Geel in [**BG09**, 4.6] gezeigt, daß sich Witts Resultat auf algebraische Funktionenkörper mit erblich euklidischen Konstantenkörpern ausdehnt - und im übrigen nur auf diese: schon über jedem erblich pythagoräischen Konstantenkörper mit mehr als einer Anordnung gibt es algebraische Funktionenkörper mit Pythagoraszahl drei, etwa der nichtangeordneten Funktionenkörper vom Geschlecht null (siehe [**BG09**, 4.7]). Desweiteren fand bereits Tikhonov (siehe Beispiel 6.9) einen angeordneten algebraischen Funktionenkörper vom Geschlecht eins über dem Körper der reellen formalen Laurantreihen, dessen Pythagoraszahl mindestens drei ist. Der Körper der reellen formalen Laurantreihen ist erblich pythagoräisch und besitzt zwei Anordnungen.

Ausgehend von diesem Beispiel geben Becher und Van Geel eine Klasse ähnlicher Beispiele [**BG09**, 5.14]. Die naheliegende Frage [**BG09**, 5.15] nach dem genauen Wert der Pythagoraszahl im Beispiel von Tikhonov wird in der vorliegenden Arbeit beantwortet: Theorem 6.7 zeigt, dass die Pythagoraszahl jedes algebraischen Funktionenkörpers über den reellen formalen Laurentreihen den Wert zwei oder drei hat.

Darüber hinaus haben bereits Becher und Van Geel für spezielle Beispiele ([**BG09**, 5.11]) untersucht, wieviele Quadratsummen in einem solchen Funktionenkörper keine Summe von zwei Quadraten sind, genauer wurde in diesen Fällen eine obere Schranke für die maximale Anzahl von Quadratsummen gegeben, die sich paarweise nicht durch Multiplikation mit Summen von zwei Quadraten ineinander überführen lassen. Die Frage nach der generellen Endlichkeit dieser oberen Schranke stellt sich von selbst.

In Theorem 6.4 bestimme ich die maximale Anzahl von Summen von drei Quadraten, welche sich auch nach Multiplikation mit einer beliebigen Summe von zwei Quadraten paarweise unterscheiden. Diese Anzahl ist endlich und in vielen Fällen effektiv berechenbar und liefert damit insbesondere eine systematische Methode, um in vielen Fällen zu entscheiden, ob ein gegebener algebraischer Funktionenkörper Pythagoraszahl zwei oder drei besitzt - dieses wird am Ende des letzten Kapitels an einigen Beispielen demonstriert.
Die Methode, die wir zum Beweis der genannten Theoreme 6.4 & 6.7 verwenden, basiert auf sogenannten Patching-Resultaten für prinzipalhomogene Räume rationaler algebraischer Gruppen über arithmetischen Kurven über vollständigen Bewertungsringen [**HHK09**], gefunden von Harbater, Hartmann und Krashen. Ich entwickele daraus eine eigene Variante eines Lokal-Global-Prinzips für quadratische Formen über algebraischen Funktionenkörpern über formalen Laurantreihenkörpern (siehe Theorem 5.2), welche dann in den Beweisen der Theoreme 6.4 & 6.7 auf die eine oder andere Art zum Einsatz kommt. Leider beschränkt sich diese Methode auf den arithmetischen Fall, das heißt es bleibt unklar, ob der Körper der reellen formalen Laurantreihen in den Aussagen der Theoreme 6.4 & 6.7 durch einen beliebigen erblich pythagoräische Konstantenkörper ersetzt werden kann. Hierzu gibt es nur vereinzelte Ergebnisse. So hat zum Beispiel Becker in [**Bec78**, Chap. III, Theorem 4] gezeigt, daß die Pythagoraszahl eines angeordneten rationalen algebraischen Funktionenkörpers genau dann den Wert zwei hat, wenn der Konstantenkörper erblich pythagoräisch ist.
Tikhonov und Yanchevskĭi [**TY05**] haben die Beweisidee von Becker auf algebraische Funktionenkörper von Geschlecht null ausgedehnt und gezeigt, daß die Pythagoraszahl eines angeordneten algebraischen Funktionenkörpers vom Geschlecht null mit erblich pythagoräischen Konstantenkörper stets den Wert zwei hat. Allerdings geht bei der Ausdehnung dieser Beweisidee der Zugang zur umgekehrte Implikation verloren, so daß die naheliegende Frage ob denn jeder algebraische Funktionenkörper vom Geschlecht null und Pythagoraszahl zwei einen erblich pythagoräischen Konstantenkörper besitzt, nicht beantwortet wurde. Die positive Antwort liefer ich mit Theorem 4.15 nach. Insbesondere weiß man nun, daß allein der Konstantenkörper (im Zusammenspiel mit der Existenz oder Nichtexistenz einer Funktionenkörperanordnung) darüber entscheidet ob die Pythagoraszahl eines beliebigen algebraischer Funktionenkörpers vom Geschlecht null den Wert zwei annimmt.

Anschließend entwickele ich das Ergebnis noch einen Schritt weiter: Ich untersuche die Klasse der Funktionenkörper von sogenannten Cassels-Catalan Kurven. Diese Klasse enthält alle Funktionenkörper vom Geschlecht null und zudem jeweils viele von beliebigem Geschlecht. Die meisten der Funktionenkörper von Cassels-Catalan Kurven höheren Geschlechts erlauben keine Stelle ungeraden Grades - genau wie fast alle algebraischen Funktionenkörper vom Geschlecht null. Ich zeige in Theorem 4.10, daß die Pythagoraszahl eines solchen Funktionenkörpers nur dann den Wert zwei haben kann, wenn der Konstantenkörper erblich pythagoräisch ist.
Zum selben Schluß, allerdings im nahezu disjunkten Fall algebraischer Funktionenkörper mit Stellen ungeraden Grades, sind bereits Becher und Van Geel in [**BG09**, 4.3] gekommen und sie haben die Frage nach dessen generellen Gültigkeit [**BG09**, 4.4] aufgeworfen: Hat jeder algebraische Funktionenkörper mit Pythagoraszahl zwei einen erblich pythagoräischen Konstantenkörper? Meine Ergebnisse liefern also neue Indizien für eine positive Antwort.
Die Methode, mit denen ich die Theoreme 4.10& 4.15 beweisen, entwickel ich im dritten Kapitel. Dort nehme ich mir die bekannte Tatsache genauer unter die Lupe, daß ein algebraischer Funktionenkörper vom Geschlecht null ein generischer Zerfällungskörper für eine Quaternionenalgebra ist. Man beobachtet, daß eine endlich separable Erweiterung des Konstantenkörpers, welcher die Quaternionenalgebra zerfällt, nicht nur das Ziel einer Stelle vom Funktionenkörper ist, sondern daß es sogar eine surjektive Stelle dieser Art gibt. Das zugehörige Theorem 3.38 bedient sich zwar einer leicht abweichenden Terminologie und ist etwas genereller, entspricht aber im eindimensionalen Spezialfall genau dem eben Beschriebenen. Es erlaubt einen knappen und konzeptuellen Beweis, von Theorem 4.15. Der Beweis von Theorem 4.10 hingegen ist technisch aufwendiger und verwendet nur ein Zwischenresultat auf dem Weg zum Zerfällungstheorem. Am Ende des ersten Abschnitts des vierten Kapitels präsentiere ich ergänzend einen Beweis der auf diesen geometrischen Zugang verzichtet und eher kombinatorisch geführt wird.

Bibliography

[Aig57] A. Aigner. Die Unmöglichkeit von $x^6 + y^6 = z^6$ und $x^9 + y^9 = z^9$ in quadratischen Körpern. *Monatshefte für Mathematik*, 62 (2):147 – 150, 1957.

[AM69] M.F. Atiyah and I.G. Macdonald. *Introduction to commutative algebra.* Reading, Mass.-Menlo Park, Calif.- London-Don Mills , Ont.: Addison-Wesley Publishing Company , 1969.

[Bec78] E. Becker. *Hereditarily-Pythagorean fields and orderings of higher level.* Monografias de Matematica, 29. Rio de Janeiro: Instituto de Matematica Pura e Aplicada, Conselho Nacional de Desenvolvimento Cientifico e Tecnologico. V, 175 p. , 1978.

[BG09] K.J. Becher and J. Van Geel. Sums of squares in function fields of hyperelliptic curves. *Mathematische Zeitschrift*, 261 (4):829 – 844, 2009.

[CTPS] J.-P. Colliot-Thélène, Parimala, and Suresh. Patching and local-global principles for homogeneous spaces over function fields of p-adic curves. `arXiv:0812.3099v3`, *to appear in Comentarii Helveticae.*

[Eis95] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Graduate Texts in Mathematics, 150. New York-Heidelberg-Berlin: Springer- Verlag. XVI, 785 p. , 1995.

[End72] O. Endler. *Valuation Theory.* Universitext. Berlin: Springer, 243 p. , 1972.

[EP05] A.J. Engler and A. Prestel. *Valued Fields.* Springer Monographs in Mathematics, 205 p., 2005.

[EW87] R. Elman and A. Wadsworth. Hereditarily quadratically closed fields. *J. Algebra*, 111:475–482, 1987.

[Har83] R. Hartshorne. *Algebraic geometry. Corr. 3rd printing.* Graduate Texts in Mathematics, 52. New York-Heidelberg-Berlin: Springer- Verlag. XVI, 496 p. , 1983.

[HH10] D. Harbater and J. Hartmann. Patching over fields. *Israel Journal of Mathematics*, 176:61–107, 2010.

[HHK09] D. Harbater, J. Hartmann, and D. Krashen. Applications of patching to quadratic forms and central simple algebras. *Inventiones mathematicae*, 178:231–263, 2009.

[HHK11] D. Harbater, J. Hartmann, and D. Krashen. Local-global principles for torsors over arithmetic curves. `arXiv:1108.3323`, *Preprint*, 2011.

[KR94] I. Kersten and U. Rehmann. Generic splitting of reductive groups. 1994.

[Lam05] T. Y. Lam. *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics 67. Providence, RI: American Mathematical Society (AMS). xxi, 550 p. $ 79.00 , 2005.

[Lan02] S. Lang. *Algebra, revised third edition.* Graduate Texts in Mathematics 211,New York, Springer Verlag, 2002.

[Liu06] Q. Liu. *Algebraic geometry and arithmetic curves. Transl. by Reinie Erné.* Oxford Graduate Texts in Mathematics 6. Oxford: Oxford University Press. xv, 577 p., 2006.

[Mat86] H. Matsumura. *Commutative ring theory.* Cambridge studies in advanced mathematics 8, Cambridge University Press, 1986.

[MPW98] A.S. Merkurjev, I.A. Panin, and A. Wadsworth. Index reduction formulas for twisted flag varieties. II. 1998.

[Mum99] D. Mumford. *The Red Book of Varieties and Schemes. Second, Expanded Edition.* Lecture Notes in Mathematics 1358, Berlin, Springer-Verlag 304 p., 1999.

[PD01] A. Prestel and C.N. Delzell. *Positive polynomials. From Hilbert's 17th problem to real algebra.* Springer Monographs in Mathematics. Berlin: Springer. viii, 268 p., 2001.

[Pfi67] A. Pfister. Zur Darstellung definiter Funktionen als Summe von Quadraten. *Invent. Math.*, 4:229–237, 1967.

[Pfi95] A. Pfister. *Quadratic Forms with Applications to Algebraic Geometry and Topology.* London Mathematical Society, Lecture Note Series 217, 1995.

[Pre78] A. Prestel. Remarks on the Pythagoras and Hasse number of real fields. *J. Reine Angew. Math.*, 303/304:284–294, 1978.

[Sch85] W. Scharlau. *Quadratic and Hermitian Forms.* Grundlehre der mathematischen Wissenschaften 270. Berlin/Heidelberg: Springer, 421 p., 1985.

[Sti09] H. Stichtenoth. *Algebraic function fields and codes. 2nd ed.* Graduate Texts in Mathematics 254. Berlin: Springer. xiii, 355 p. , 2009.

[Tar98] A. Tarski. A decision method for elementary algebra and geometry. Caviness, Bob F. (ed.) et al., Quantifier elimination and cylindrical algebraic decomposition. Proceedings of a symposium, Linz, Austria, October 6–8, 1993. Wien: Springer. Texts and Monographs in Symbolic Computation. 24-84, 1998.

[TY05] S.V. Tikhonov and V.I. Yanchevskiĭ. Pythagoras numbers of function fields of genus zero curves defined over hereditarily Pythagorean fields. Kalla, Shyam L. (ed.) et al., Proceedings of the international conference on mathematics and its applications, ICMA 2004, Kuwait, April 5–7, 2004. Kuwait: Kuwait University, Department of Mathematics and Computer Science; Kuwait: Kuwait Foundation for the Advancement of Sciences (KFAS). 438-443, 2005.