Archimedean Quadratic Modules

A Decision Problem for Real Multivariate Polynomials

Dissertation

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

Sven Wagner

Tag der mündlichen Prüfung: 05.11.2009

Referent: Prof. Dr. Alexander Prestel (Universität Konstanz)
Referent: Dr. Jochen Koenigsmann (University of Oxford)

Sven Wagner
Universität Konstanz
Fachbereich Mathematik und Statistik
78457 Konstanz, Germany
sven.wagner@uni-konstanz.de

Gewidmet Claudia und Greta

Acknowledgements

I thank my advisor Alexander Prestel. I am deeply grateful for his encouragement, his constant support and many ideas. I also thank my colleagues in Konstanz for providing a very pleasant working atmosphere. For almost three years now, I have been a member of the DFG-Graduiertenkolleg *Mathematische Logik und Anwendungen* in Freiburg, and the financial support and mathematical knowledge I have been receiving is gratefully acknowledged. Finally, I thank Claudia and Greta for their love as well as for their patience and support during the development of this work.

Konstanz, August 2009 *Sven Wagner*

Contents

Introduction

Schmüdgen proved in 1991 for all $f, h_1, \dots, h_s \in \mathbb{R}[X_1, \dots, X_n]$ that if $W_{\mathbb{R}}(h_1, \dots, h_s) := \{x \in \mathbb{R}^n \mid h_1(x) \geqslant 0, \dots, h_s(x) \geqslant 0\}$ is bounded in $\mathbb{R}^n$ and $f > 0$ on $W_{\mathbb{R}}(h_1, \dots, h_s)$, then

$$f = \sum_{\nu \in \{0,1\}^s} h_1^{\nu_1} \cdots h_s^{\nu_s} \cdot \sigma_\nu$$

where the σ_ν are sums of squares in $\mathbb{R}[X_1, \dots, X_n]$.

In 1993, Putinar asked whether there is even a simpler representiation of the form

$$f = \sigma_0 + h_1\sigma_1 + \cdots + h_s\sigma_s \quad (*)$$

where $\sigma_1, \dots, \sigma_s$ are sums of squares in $\mathbb{R}[X_1, \dots, X_n]$.

The main goal of our work is to prove that it is possible to *decide* whether given polynomials $h_1, \dots, h_s \in \mathbb{R}[X_1, \dots, X_n]$ with $W_{\mathbb{R}}(h_1, \dots, h_s)$ non-empty satisfy $W_{\mathbb{R}}(h_1, \dots, h_s)$ is bounded and allow the simpler representation for all polynomials $f \in \mathbb{R}[X_1, \dots, X_n]$ which are strictly positive on $W_{\mathbb{R}}(h_1, \dots, h_s)$.

Here, decidability means, in particular, that there exists an effective decision procedure (algorithm) that decides whether $h_1, \dots, h_s$ have this property or not, if the coefficients of $h_1, \dots, h_s$ are rational numbers. Therefore one may additionally ask for a concrete algorithm.

If $n = 1$, it can be shown that we only have to decide the boundedness of $W_{\mathbb{R}}(h_1, \dots, h_s)$ which is always possible. In her 2005 PhD-Thesis, Canto Cabral gave for the case $n = 2$ an effective decision procedure for all $h_1, \dots, h_s$ such that $W_{\mathbb{R}}(h_1, \dots, h_s)$ is non-empty and bounded. In this work, we show that decidability holds for every dimension. However, a concrete algorithm for $n > 2$ is not in sight.

Crucial for our proof are Jacobi's Representation Theorem and the Characterization Theorem of Jacobi and Prestel:

In 1999, Jacobi showed in his PhD-Thesis that, for all $h_1, \dots, h_s \in A := \mathbb{R}[X_1, \dots, X_n]$, the set $W_{\mathbb{R}}(h_1, \dots, h_s)$ is bounded and the simple representation $(*)$ holds for all polynomials f which are strictly positive on $W_{\mathbb{R}}(h_1, \dots, h_s)$ if and only if $N - \sum_{i=1}^n X_i^2$ has such an representation for some $N \in \mathbb{N}$. If the latter is true, we say that the quadratic module $M(h_1, \dots, h_s) := \sum A^2 + h_1 \sum A^2 + \cdots h_s \sum A^2$ is archimedean.

Jacobi and Prestel gave in 2001 a valuation theoretic characterization for the property of $M(h_1, \dots, h_s)$ to be archimedean. By this characterization, $M(h_1, \dots, h_s)$ is not archimedean if $W_{\mathbb{R}}(h_1, \dots, h_s)$ is not bounded or there exists a real prime ideal

$\mathfrak{p}$ of $\mathbb{R}[X_1, \ldots, X_n]$ and a real valuation v of the quotient field $F_\mathfrak{p}$ of $\mathbb{R}[X_1, \ldots, X_n]/\mathfrak{p}$ with the property $v(X_i + \mathfrak{p}) < 0$ for some $i \in \{1, \ldots, n\}$ and such that all residue forms of the regular part of the quadratic form $\langle 1 + \mathfrak{p}, h_1 + \mathfrak{p}, \ldots, h_s + \mathfrak{p} \rangle$ are not weakly isotropic over the residue field of $(F_\mathfrak{p}, v)$. To prove the decidability, we give a valuation-free statement (similar to that in our definition of archimedean above) that expresses that $M(h_1, \ldots, h_s)$ is not archimedean. The main obstacle is that the valuations that can appear above might not be suitable to work with. The value group or the residue field may not be finitely generated. So, we have to show that for any such *bad* valuation a *good* valuation with the same properties in the value group and the residue field exists.

For us, *good* valuations are the so-called Abhyankar valuations. Their value group is a finite product of copies of $\mathbb{Z}$ and their residue field is finitely generated over the ground field. We prove that in a function field F over a field K of characteristic zero, if we have given a non-trivial valuation which is trivial on K and if we also have given finitely many properties of this valuation, we can always find an Abhyankar valuation of F which is trivial on K and which satisfies the same properties. Moreover, we can choose the rank and the ordering of the value group of the Abhyankar valuation freely to a certain extent. As a consequence, the Abhyankar valuations of F which are trivial on K are dense in the Zariski space of all K-trivial valuations of F with respect to certain Hausdorff (or even compact) topologies on this space. The proof of this result uses a local uniformization theorem for such Abhyankar valuations, the Ax-Kochen-Ershov Principle from model theory and the valuation theoretic Implicit Function Theorem.

With this result, we can reprove a theorem of Schülting which is an improvement of the Bröcker-Prestel Local-Global Principle in the case of function fields over $\mathbb{R}$. Schülting showed, using deep results of Hironaka, that over these fields the weak isotropy of regular quadratic form needs only to be tested locally at all prime divisors. Prime divisors are Abhyankar valuations with value group $\mathbb{Z}$ and exactly those *good* valuations we want to consider instead of the arbitrary rank-1-valuations above. To achieve this, we modify our proof of Schülting's theorem to improve the characterization theorem of Jacobi and Prestel in such a way that only prime divisors need to be considered.

The valuation ring of a prime divisor is after a finite extension of the function field a local ring of a non-singular K-rational point of an irreducible curve defined over the residue field K of the prime divisor. We therefore have a nice description of that valuation ring with which the residue forms of a given quadratic form are easy to determine, and we use this description to give the valuation-free statement that expresses that $M(h_1, \ldots, h_s)$ is not archimedean. With this statement, we then derive the decidability.

The structure of this work is as follows:

The work is split into three chapters. In the first section of each chapter, we give an overview of the basic concepts we use in the main part of that chapter.

In Chapter 1, we give our own proof of a known result, since this is an important tool for the rest of this work. We show a local uniformization theorem for Abhyankar valuations: After a finite extension, the valuation ring of such a valuation is centered at a regular local ring. Here and below, we deal with valuations of function fields over fields of characteristic zero.

In Chapter 2, Section 2, we show that it is possible to transform an arbitrary non-trivial valuation into an Abhyankar valuation, and that in this process it is possible to preserve a finite amount of properties of the original valuation.

In Section 3 of Chapter 2, we deduce that the iterated prime divisors and the Abhyankar valuations of rank 1 lie dense in the Zariski space with respect to a refinement of the Zariski patch topology.

As an application of the result of Section 2, we give in Section 4 of Chapter 2 a new proof for Schülting's improvement of the Bröcker-Prestel Local-Glocal Principle for weak isotropy of a regular quadratic form over a function field over $\mathbb{R}$.

In Chapter 3, Section 2, we show the decidability of the weak isotropy of regular quadratic forms over a function field over $\mathbb{R}$.

In Section 3 of Chapter 3, we derive our main result: The decidability for archimedean quadratic modules if the quadratic module is finitely generated by real multivariate polynomials.

Chapter 1

Local Uniformization for Abhyankar Valuations

The goal of this chapter is to prove a local uniformization theorem for Abhyankar valuations of a function field over a field of characteristic zero: After a finite extension of F, any such valuation is centered at a regular local ring.

1.1 Preliminaries

We start with an introduction to the theory of valued fields and then take a look at some special topics: henselian valued fields, the topology induced by a valuation, Abhyankar valuations and prime divisors. If nothing else is mentioned, all definitions and unproven results can be found in [7].

1.1.1 Valued Fields

In the 1930's, Krull introduced in [12] the notion of a valuation, a generalization of absolute values. Before we give the definition, we consider a related concept also introduced by Krull: valuation rings.

1.1.1 **Definition:**

A **valuation ring** of a field K is an integral domain $\mathcal{O}$ with quotient field K such that for all $x \in K^\times$ always $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$ holds.

A valuation ring $\mathcal{O}$ of a field K is a local ring with maximal ideal $\mathfrak{m} := \{x \in K^\times \mid x^{-1} \notin \mathcal{O}\} \cup \{0\}$, and $\overline{K}^{\mathcal{O}} := \mathcal{O}/\mathfrak{m}$ is called the **residue field** of $\mathcal{O}$.

1.1.2 **Example:**

Let $\mathcal{O}$ be a local ring. Then the following statements are equivalent:

(i) $\mathcal{O}$ is a principal ideal domain but not a field.

(ii) There exists some $\pi \in \mathcal{O}$ such that π is no zero-divisor in $\mathcal{O}$, $\pi\mathcal{O}$ is the maximal ideal of $\mathcal{O}$ and $\bigcap_{i=0}^{\infty} \pi^i\mathcal{O} = \{0\}$.

If $\mathcal{O}$ satisfies these conditions, it is a valuation ring of Quot($\mathcal{O}$) and called a **discrete valuation ring**.

The following important result of Chevalley tells us that for all subrings A of field K and all prime ideals $\mathfrak{p}$ of A, there exists a valuation ring of K which is **centered at** $\mathfrak{p}$.

1.1.3 **Theorem:**

Let K be a field, let A be a subring of K and let $\mathfrak{p} \subset A$ be a prime ideal of A. Then there exists a valuation ring $\mathcal{O}$ of K such that $A \subset \mathcal{O}$ and $\mathfrak{m} \cap A = \mathfrak{p}$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$.

There are several consequences of Chevalley's Theorem.

1.1.4 **Theorem:**

Let L/K be an extension of fields. Let $\mathcal{O}$ be a valuation ring of K. Then there exists an **extension** $\mathcal{O}'$ of $\mathcal{O}$ in L, i.e., $\mathcal{O}'$ is a valuation ring of L such that $\mathcal{O}' \cap K = \mathcal{O}$.

1.1.5 **Theorem:**

a) Every valuation ring is integrally closed in its quotient field.
b) Let A be a subring of a field K, and denote by $\mathbb{V}$ the set of all valuation rings $\mathcal{O}$ of K such that $A \subset \mathcal{O}$ and $\mathfrak{m} \cap A$ is a maximal ideal of A, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$. Then the integral closure of A in K equals the intersection of all valuation rings in $\mathbb{V}$.

Another class of local rings we want to consider are the regular local rings. In some cases, regular local rings are valuation rings, but in general they are not. The following can be found in [4].

1.1.6 **Definition:**

Let K be a field, and let A be a noetherian local subring of K. A is called **regular** iff the maximal ideal $\mathfrak{m}$ of A is generated by dim A elements of A, where dim A denotes the Krull dimension of A.

1.1.7 **Theorem:**

Let A be a regular local ring. Then A is integrally closed in its quotient field.

Due to Theorem 1.1.5 we have the following relation between regular local rings and valuation rings.

1.1.8 **Corollary:**

Let A be a regular local ring with quotient field K. Then A is equal to the intersection of all valuations $\mathcal{O}$ of K that are centered at the maximal ideal of A.

1.1.9 **Theorem:** (Auslander, Buchsbaum)

Every regular local ring is a unique factorization domain.

1.1.10 **Definition:**

Let K be a field, and let $V \subset \mathbb{A}^n$ be an affine K-variety. Let P be a K-rational point of V, and let d be the dimension of V at P. Let $f_1, \dots, f_m$ be a set of generators of the corresponding ideal in $K[X_1, \dots, X_n]$. We say that V is **non-singular** at P iff the rank of the matrix

$$\left(\frac{\partial}{\partial X_j} f_i(P)\right)_{\substack{1 \leqslant i \leqslant m \\ 1 \leqslant j \leqslant n}}$$

is $n - d$.

1.1.11 **Theorem:** (Zariski, [32])

Let K be a field, and let V be an affine K-variety. Let P be a K-rational point of V. Then V is non-singular at P if and only if the local ring $\mathcal{O}_{P,V}$ of P is a regular local ring.

1.1.12 **Examples:**

1. The regular local rings of dimension 0 are exactly the fields.
2. The regular local rings of dimension 1 are exactly the discrete valuation rings.
3. Let K be a field, and let $A := K[X_1, \dots, X_n]$ be the polynomial ring in n indeterminates over K. Then, for all prime ideals $\mathfrak{p}$ of A, the localization of A at $\mathfrak{p}$ is a regular local ring.

To talk about valuations, we have to consider ordered abelian groups, and further we will distinguish between discrete and dense orders.

1.1.13 **Definition:**

Let $(G, \leqslant)$ be an **ordered abelian group**, i.e., $\leqslant$ is a linear order on G such that, for all $a, b, c \in G$, $a \leqslant b$ implies $a + c \leqslant b + c$. $(G, \leqslant)$ is said to be

(i) **discretely ordered** iff it possesses a smallest positive element and

(ii) **densely ordered** iff it has no smallest positive element.

1.1.14 **Remark:**

Let G be a finitely generated, ordered abelian group. Then G is torsion-free, and therefore, by the fundamental theorem of finitely generated abelian groups, G is isomorphic to a finite direct sum of copies of $\mathbb{Z}$.

1.1.15 **Definition:**

Let K be a field, and let $\Gamma = (\Gamma, \leqslant)$ be an ordered abelian group. A map $v \colon K \to \Gamma \cup \{\infty\}$ is called a **valuation** of K iff the following conditions hold for all $x, y \in K$:

(i) $v(x) = \infty \iff x = 0$,

(ii) $v(xy) = v(x) + v(y)$,

(iii) $v(x+y) \geqslant \min\{v(x), v(y)\}$.

Here we define $\infty + \gamma := \gamma + \infty := \infty$ for all $\gamma \in \Gamma \cup \{\infty\}$ and we let $\gamma < \infty$ for all $\gamma \in \Gamma$.
$v(K^\times)$ is a subgroup of Γ called the **value group** of v. We denote this group by Γ_v.
A pair (K, v), where K is a field and v is a valuation of K, is called a **valued field**.

1.1.16 **Proposition:**

Let (K, v) be a valued field. Then for all $x, y \in K$ the following holds:

a) $v(1) = 0$,

b) $v(x^{-1}) = -v(x)$, if $x \neq 0$,

c) $v(-x) = v(x)$ and

d) $v(x+y) = v(x)$, if $v(x) < v(y)$.

Valuation rings and valuations of a field are related in the following way.

1.1.17 **Proposition:**

Let K be a field.

a) Let v be a valuation of K. Then $\mathcal{O}_v := \{x \in K \mid v(x) \geqslant 0\}$ is a valuation ring of K with maximal ideal $\mathfrak{m}_v := \{x \in K \mid v(x) > 0\}$.

b) Let $\mathcal{O}$ be a valuation ring of K. Then
$$x\mathcal{O}^\times \leqslant y\mathcal{O}^\times :\iff yx^{-1} \in \mathcal{O}$$
defines a group order on the abelian group $\Gamma_{\mathcal{O}} := K^\times/\mathcal{O}^\times$ with respect to the additively written group operation $x\mathcal{O}^\times + y\mathcal{O}^\times := xy\mathcal{O}^\times$.
The residue map
$$\begin{array}{rcl} v_{\mathcal{O}} \colon K^\times & \twoheadrightarrow & \Gamma_{\mathcal{O}} \\ x & \mapsto & x\mathcal{O}^\times \end{array}$$
induces a valuation of K with value group $\Gamma_{\mathcal{O}}$ and valuation ring $\mathcal{O}_{v_{\mathcal{O}}} = \mathcal{O}$.

c) Let v be a valuation of K. Then
$$\begin{array}{rcl} K^\times/\mathcal{O}_v^\times & \to & \Gamma_v \\ x\mathcal{O}_v^\times & \mapsto & v(x) \end{array}$$
defines an order preserving isomorphism between the value groups of $v_{\mathcal{O}_v}$ und v.

1.1.18 **Definition:**

Let K be a field.

A valuation v of K is called **trivial** iff $\Gamma_v = v(K^\times) = \{0\}$ or, equivalently, $\mathcal{O}_v = K$.

For a valuation v of K, we denote the residue field $\overline{K}^{\mathcal{O}_v}$ also by $\overline{K}^v$.

We say that two valuations of K are **equivalent** iff they induce the same valuation ring in K, i.e., there exists an order preserving isomorphism between their value groups. This indeed defines an equivalence relation on the set of valuations of K.

Most of the time, we will identify a valuation with its equivalence class.

We now consider two important invariants of (ordered) abelian groups: rank and rational rank.

1.1.19 **Definition:**

Let G be an abelian group, so, in particular, G is a $\mathbb{Z}$-module. We call the tensor product $G_{\text{div}} := G \otimes_{\mathbb{Z}} \mathbb{Q}$ the **divisible hull** of G. The group G_{div} is a $\mathbb{Q}$-vector space, and we call $\operatorname{rr}(G) := \dim_{\mathbb{Q}}(G_{\text{div}})$ the **rational rank** of G.

1.1.20 **Remark:**

Let G be an abelian group. Then $\operatorname{rr}(G) = 0$ if and only if G is a torsion group.

1.1.21 **Proposition:**

Let G be an abelian group, and let H be a subgroup of G. Then

$$\operatorname{rr}(G) = \operatorname{rr}(H) + \operatorname{rr}(G/H).$$

1.1.22 **Proposition:**

Let $(G, \leqslant)$ be an ordered abelian group. Then there exists exactly one linear order $\leqslant_{\text{div}}$ on G_{div} such that $(G_{\text{div}}, \leqslant_{\text{div}})$ is an ordered group that extends $(G, \leqslant)$.

1.1.23 **Definition:**

Let $(G, \leqslant)$ be an ordered abelian group. A subgroup H of G is called **convex** if, for all $g \in G$ and all $h \in H$ such that $0 \leqslant g \leqslant h$, we have $g \in H$.

1.1.24 **Proposition:**

Let $(G, \leqslant)$ be an ordered abelian group. Then the following statements hold:

a) The set of convex subgroups of G is linearly ordered with respect to inclusion.

b) A subgroup H of G is convex with respect to $\leqslant$ if and only if

$$a + H \preceq b + H :\iff a \leqslant b \text{ or } a + H = b + H$$

for $a, b \in G$ defines a group order on G/H.

c) Every convex subgroup of G is pure in G.

d) If F is a subgroup of G, then $H \mapsto F \cap H$ is a surjective map from the set of all convex subgroups of $(G, \leqslant)$ to the set of all convex subgroups of $(F, \leqslant)$.

1.1.25 **Definition:**

Let $(G, \leqslant)$ be an ordered abelian group. We call the supremum of all $n \in \mathbb{N}$, for which there exists a chain $\{0\} = H_0 \subset H_1 \subset \ldots \subset H_n$ of subgroups of G which are convex with respect to $\leqslant$, the **rank** of $(G, \leqslant)$.

We say that $(G, \leqslant)$ is **archimedean** iff it has rank 1.

1.1.26 **Example:**

An ordered group is discrete and archimedean if and only if it is order-isomorphic to $\mathbb{Z}$.
The valuation rings with discrete and archimedean ordered value group are exactly the discrete valuation rings.

1.1.27 **Proposition:**

Let $(G, \leqslant)$ be an ordered abelian group, and let H be a convex subgroup of G. Consider G/H with the order induced by $\leqslant$. Then

$$\operatorname{rank}(G) = \operatorname{rank}(H) + \operatorname{rank}(G/H).$$

$(G, \leqslant)$ and $(G_{\text{div}}, \leqslant_{\text{div}})$ have the same rank.

We consider the special case of a lexicographically ordered product of two ordered groups in view of the two invariants.

1.1.28 **Corollary:**

Let $(G_1, \leqslant_1), (G_2, \leqslant_2)$ be two ordered abelian groups, and let G be the direct product of G_1 and G_2 equipped with the lexicographical ordering $\leqslant_{\text{lex}}$, i.e., $(g_1, g_2) \leqslant_{\text{lex}} (h_1, h_2)$ if and only if $g_1 <_1 h_1$ or $(g_1 = h_1$ and $g_1 \leqslant_2 g_2)$. Then $\operatorname{rr}(G) = \operatorname{rr}(G_1) + \operatorname{rr}(G_2)$ and $\operatorname{rank}(G) = \operatorname{rank}(G_1) +$ $\operatorname{rank}(G_2)$.

Proof:

First note that $G_2 \cong \{0\} \times G_2$ is a convex subgroup of G. Then the statements follow from $G_1 \cong G/(\{0\} \times G_2)$ and the propositions 1.1.21 and 1.1.27.

q.e.d.

The following relation holds between the rank and the rational rank of an ordered valued group.

1.1.29 **Proposition:**

Let G be an ordered abelian group. Then $\operatorname{rank}(G) \leqslant \operatorname{rr}(G)$.

1.1.30 **Lemma:**

Let K be a field and let $\mathcal{O}$ be a non-trivial valuation ring of K. Then there exists a 1-1 correspondence of convex subgroups of $\Gamma_{\mathcal{O}}$ and overrings of $\mathcal{O}$. If $\mathcal{O}$ has finite rank, then the rank is equal to the Krull dimension of $\mathcal{O}$.

1.1.31 **Corollary:**

Let L/K be an extension of fields, and let $\mathcal{O}$ be a valuation ring of L. Then every valuation ring $\mathcal{O}'$ of K such that $\mathcal{O}' \supset \mathcal{O} \cap K$ can be extended to a valuation ring $\mathcal{O}''$ of L such that $\mathcal{O}'' \supset \mathcal{O}$.

1.1.32 **Definition:**

Let K be a field, let v_1 be a valuation of K, and let v_2 be a valuation of the residue field $\overline{K}^{v_1}$. Let $\rho\colon \mathcal{O}_{v_1} \twoheadrightarrow \overline{K}^{v_1}$ be the residue homomorphism of v_1. Then $\mathcal{O} := \rho^{-1}(\mathcal{O}_{v_2})$ is a valuation ring of K, and the valuation $v_{\mathcal{O}}$ (or any other valuation in its equivalence class) is called the **composition of** v_1 **with** v_2 and denoted by $v_1 \circ v_2$.

1.1.33 **Proposition:**

Let K be a field, let v_1 be a valuation of K, let v_2 be a valuation of the residue field $\overline{K}^{v_1}$, and let $v = v_1 \circ v_2$ be the composition of these two valuations. Then the following holds:

a) $\mathcal{O}_v \subset \mathcal{O}_{v_1}$.

b) Γ_{v_2} is (isomorphic to) a convex subgroup of Γ_v and $\Gamma_{v_1} \cong \Gamma_v/\Gamma_{v_2}$.

c) The residue field of (K, v) is equal to the residue field of $(\overline{K}^{v_1}, v_2)$.

1.1.34 **Remark:**

Let K be a field, and let v be a valuation of K. Let $\mathcal{O} \supset \mathcal{O}_v$ be a valuation ring of K, and let v_1 be a corresponding valuation of K. The image of $\mathcal{O}_v$ under the residue homomorphism $\mathcal{O} \twoheadrightarrow \overline{K}^{v_1}$ is a valuation ring of $\overline{K}^{v_1}$. Let v_2 be a corresponding valuation of $\overline{K}^{v_1}$. Then $v = v_1 \circ v_2$.

1.1.35 **Remark:**

Let K be a field, let v_1 be a valuation of K, let v_2 be a valuation of the residue field $\overline{K}^{v_1}$, and let $v = v_1 \circ v_2$ be the composition of these two valuations. Then, by Proposition 1.1.33, we have the following exact sequence of ordered groups

$$0 \to \Gamma_{v_2} \to \Gamma_v \to \Gamma_{v_1} \to 0.$$

If Γ_{v_1} or Γ_{v_2} is a product of copies of $\mathbb{Z}$, then this exact sequence splits as an exact sequence of groups, since such a product is an injective and projective $\mathbb{Z}$-module. Hence, as a group, Γ_v is isomorphic to the group $\Gamma_{v_1} \times \Gamma_{v_2}$. Via this isomorphism, the ordering of Γ_v induces the lexicographical ordering on the product $\Gamma_{v_1} \times \Gamma_{v_2}$.

Let L/K be an extension of fields, and let v be a valuation of K. From Chevalley's Theorem, we know that there always exists an extension of v to L. Here are some important facts about extensions of valued fields.

1.1.36 **Definition:**

Let $(L, w)/(K, v)$ be an **extension of valued fields**, i.e., $\mathcal{O}_w \cap K = \mathcal{O}_v$, and we may assume that $w|_K = v$.

We have $\Gamma_v \cong K^\times/\mathcal{O}_v^\times \hookrightarrow L^\times/\mathcal{O}_w^\times \cong \Gamma_w$, so we may regard Γ_v as an ordered subgroup of Γ_w. We set $e(\mathcal{O}_w/\mathcal{O}_v) := [\Gamma_w : \Gamma_v]$ and call this the **ramification index of** $(L, w)/(K, v)$.

We also have $\overline{K}^v = \mathcal{O}_v/\mathfrak{m}_v \hookrightarrow \mathcal{O}_w/\mathfrak{m}_w = \overline{L}^w$. We set $f(\mathcal{O}_w/\mathcal{O}_v) := [\overline{L}^w : \overline{K}^v]$ and call this the **residue degree of** $(L, w)/(K, v)$.

If both, the ramification index and the residue degree of $(L, w)/(K, v)$, are equal to 1, we call this extension **immediate**.

For a finite extension of valued fields, the degree of the field extension is an upper bound for the product of the ramification index and the residue degree of this extension. This leads to the following result for arbitrary algebraic extensions.

1.1.37 **Theorem:**

Let $(L, w)/(K, v)$ be an algebraic extension of valued fields. Then:

a) Γ_w/Γ_v is a torsion group.
b) The extension $\overline{L}^w/\overline{K}^v$ is algebraic.
c) Γ_w and Γ_v have the same rank and the same rational rank.

1.1.38 **Corollary:**

Let $(L, w)/(K, v)$ be an algebraic extension of valued fields such that v is the trivial valuation of K. Then w is the trivial valuation of L.

Let L/K be a finite extension of fields, and let $\mathcal{O}$ be a valuation ring of K. It can be shown that there exist only finitely many extensions of $\mathcal{O}$ to L and then specify the inequality $ef \leqslant [L : K]$ that holds for one such extension.

1.1.39 **Theorem:** (Fundamental Inequality)

Let L/K be a finite extension of fields. Let $\mathcal{O}$ be a valuation ring of K, and let $\mathcal{O}_1, \ldots, \mathcal{O}_r$ be all extensions of $\mathcal{O}$ to L. Then

$$\sum_{i=1}^{r} e(\mathcal{O}_i/\mathcal{O}) f(\mathcal{O}_i/\mathcal{O}) \leqslant [L : K].$$

If the characteristic of the residue field (= **residue characteristic**) is equal to zero, then the fundamental inequality is actually an equality, called the **fundamental equality**.

We now take a look at two important possible extensions of a valuation to a purely transcendental extension in one variable.

1.1.40 **Proposition:**

Let (K, v) be a valued field. Then there exists exactly one extension w of v to the rational function field $K(X)$ such that $w(X) = 0$ and $\overline{X}^w$ is transcendental over $\overline{K}^v$. For this extension w, we have $\overline{K(X)}^w = \overline{K}^v(\overline{X}^w)$ and $w(K(X)^\times) = \Gamma_v$.

1.1.41 **Proposition:**

Let (K, v) be a valued field, and let Δ be an ordered abelian group that extends Γ_v. Let $\delta \in \Delta$ be such that $\delta + \Gamma_v$ is a non-torsion element of Δ/Γ_v. Then there exists exactly one extension w of v to the rational function field $K(X)$ such that $w(X) = \delta$. For this extension w, we have $\overline{K(X)}^w = \overline{K}^v$ and $w(K(X)^\times) = \Gamma_v \oplus \mathbb{Z}\delta$ with the ordering induced from Δ.

Now we consider arbitrary extensions of valued fields. Theorem 1.1.37 together with the propositions 1.1.40 and 1.1.41 provide the following.

1.1.42 **Theorem:**

Let $(L, w)/(K, v)$ be an extension of valued fields. Let $x_1, \dots, x_s \in \mathcal{O}_w$ be such that $\overline{x_1}^w, \dots, \overline{x_s}^w \in \overline{L}^w$ are algebraically independent over $\overline{K}^v$, further let $y_1, \dots, y_r \in L$ be such that $w(y_1) + \Gamma_v, \dots, w(y_r) + \Gamma_v \in \Gamma_w/\Gamma_v$ are $\mathbb{Z}$-linearly independent. Then $x_1, \dots, x_s, y_1, \dots, y_r$ are algebraically independent over K. Moreover, the restriction of w to $K(x_1, \dots, x_s, y_1, \dots, y_r)$ has residue field $\overline{K}^v(\overline{x_1}^w, \dots, \overline{x_s}^w)$ and value group $\Gamma_v \oplus \mathbb{Z}w(y_1) \oplus \cdots \oplus \mathbb{Z}w(y_r)$.

1.1.43 **Remark:**

Let $(L, w)/(K, v)$ be an extension of valued fields, and let $x_1, \dots, x_s \in \mathcal{O}_w$ be such that $\overline{x_1}^w, \dots, \overline{x_s}^w \in \overline{L}^w$ are algebraically independent over $\overline{K}^v$. If v is trivial, then the restriction of w to $K(x_1, \dots, x_s)$ is also trivial, and the restriction of the residue homomorphism $\mathcal{O}_w \twoheadrightarrow \mathcal{O}_w/\mathfrak{m}_w = \overline{L}^w$ to $K(x_1, \dots, x_s)$ is injective.

1.1.44 **Corollary:**

Let F/K be an extension of fields. Let $\mathcal{O}$ be a valuation ring of K, and let $\mathcal{O}_1 \subsetneq \cdots \subsetneq \mathcal{O}_n$ be extensions of $\mathcal{O}$ to F. Then $\operatorname{trdeg}(F/K) \geqslant n - 1$.

An important consequence of Theorem 1.1.42 is the following inequality.

1.1.45 **Theorem:** (Dimension Inequality)

Let $(L, w)/(K, v)$ be an extension of valued fields. Then

$$\operatorname{trdeg}(L/K) \geqslant \operatorname{trdeg}(\overline{L}^w/\overline{K}^v) + \operatorname{rr}(\Gamma_w/\Gamma_v).$$

Moreover, if L is finitely generated over K and the inequality above is an equality, then Γ_w/Γ_v is a finitely generated $\mathbb{Z}$-module and $\overline{L}^w$ is finitely generated over $\overline{K}^v$.

1.1.46 **Example:**

Let $F = \mathbb{R}(X_1, X_2, X_3, X_4, X_5) = \mathbb{R}(\frac{X_5}{X_4}, X_5^2 - X_4^3, X_4, X_3, X_2, X_3^3 - X_1)$. Let Δ be the ordered abelian group $\mathbb{R} \times \mathbb{R}$ with componentwise addition and the lexicographical ordering on the product. Let v be the trivial valuation of $\mathbb{R}$.

We extend v to $\mathbb{R}(\frac{X_5}{X_4})$ in such a way that the value of $\frac{X_5}{X_4}$ is $(1, 0) \in \Delta$. By Proposition 1.1.41, there is exactly one such extension, and we denote this extension again by v. The value group of this extension is $\mathbb{Z} \cdot 1 \times \{0\} \cong \mathbb{Z}$ and the residue field is $\mathbb{R}$.

We then extend v to $\mathbb{R}(\frac{X_5}{X_4}, X_5^2 - X_4^3)$ by mapping $X_5^2 - X_4^3$ to $(2\pi, 0)$. The value group of the extension is $(\mathbb{Z} \oplus \mathbb{Z}2\pi) \times \{0\}$ and the residue field is still $\mathbb{R}$.

There are two possible extensions of v to the algebraic extension $\mathbb{R}(\frac{X_5}{X_4}, X_5^2 - X_4^3, X_4)$: one of ramification index 1, where $v(X_4) = 2$ and $v(X_5) = 3$, and one of ramification index 2, where $v(X_4) = \pi - 1$ and $v(X_5) = \pi$. Note that, by the Fundamental (In-)Equality, the residue degrees of both possible extensions are 1, since the irreducible polynomial of X_4 over $\mathbb{R}(\frac{X_5}{X_4}, X_5^2 - X_4^3)$ is $T^3 - \frac{X_5}{X_4}T^2 + X_5^2 - X_4^3$. We take the extension with ramification index 1, hence the value group remains the same.

Now we extend v to $\mathbb{R}(\frac{X_5}{X_4}, X_5^2 - X_4^3, X_4, X_3)$ in such a way that the value of X_3 is zero and the residue class of X_3 is transcendental over $\mathbb{R}$. By Proposition 1.1.40, there is exactly one such extension, its value group is still $\mathbb{Z} \oplus \mathbb{Z}2\pi$ and its residue field is $\mathbb{R}(\overline{X_3}^v) \cong \mathbb{R}(X_3)$.

Applying Proposition 1.1.41 twice, we get an extension of v to $\mathbb{R}(\frac{X_5}{X_4}, X_5^2 - X_4^3, X_4, X_3, X_2, X_3^3 - X_1) = F$ where X_2 maps to $(0, 1)$ and $X_3^3 - X_1$ maps to $(0, \sqrt{2})$. Then the value group of v is $(\mathbb{Z} \oplus \mathbb{Z}2\pi) \times (\mathbb{Z} \oplus \mathbb{Z}\sqrt{2})$ and the residue field of (F, v) is $\mathbb{R}(X_3)$.

The rank of the value group is 2 and the rational rank is 4. This follows from Corollary 1.1.28.

It is possible to find a finite extension of a valued field realizing a prescribed finite extension of the value group and a prescribed finite extension of the residue field (see [6], Theorem 27.1).

1.1.47 **Theorem:**

Let (K, v) be a non-trivially valued field. For any $n \in \mathbb{N}$ such that $n \geqslant 1$, any ordered group $\Delta \supset \Gamma_v$ and any field $\mathcal{L} \supset \overline{K}^v$ such that $[\Delta : \Gamma_v] \cdot [\mathcal{L} : \overline{K}^v] = n$ there exists some extension (L, w) of (K, v) such that

- L/K is a separable extension of degree n,
- the valuation ring $\mathcal{O}_w$ of w in L is the only extension of $\mathcal{O}_v$ to L,
- the value group Γ_w of w is equal to Δ and
- the residue field $\overline{L}^w$ of w is equal to $\mathcal{L}$.

1.1.2 Henselian Valued Fields

In this section, we deal with a very nice and important class of valued fields, the henselian valued fields.

1.1.48 **Definition:**

Let (K, v) be a valued field.

(K, v) is called **henselian** iff $\mathcal{O}_v$ has a unique extension to every algebraic field extension L of K.

A valued field extension $(K^{\mathrm{h}}, v^{\mathrm{h}})$ of (K, v) is called the **henselization** of (K, v) iff $(K^{\mathrm{h}}, v^{\mathrm{h}})$ is henselian, and, for every other henselian extension (L, w) of (K, v), there exists a unique embedding of $(K^{\mathrm{h}}, v^{\mathrm{h}})$ into (L, w).

We list some of the known characterizations for the property of a valued field to be henselian. Number (ii) is also called Hensel's Lemma which is the origin of the name henselian. Hensel proved this result for the field of p-adic numbers $\mathbb{Q}_p$.
Let (K, v) be a valued field. For a polynomial $f \in \mathcal{O}_v[X]$ we denote by $\overline{f}^v$ the corresponding polynomial in $\overline{K}^v[X]$ that results by applying the residue homomorphism to the coefficients of f.

1.1.49 **Theorem:**

Let (K, v) be a valued field. The following statements are equivalent:

(i) (K, v) is henselian.

(ii) For each polynomial $f \in \mathcal{O}_v[X]$ and each element $a \in \mathcal{O}_v$ such that $v(f(a)) > 2v(\frac{\partial}{\partial X} f(a))$, there exists an element $\alpha \in \mathcal{O}_v$ with $f(\alpha) = 0$ and $v(a - \alpha) > v(\frac{\partial}{\partial X} f(a))$.

(iii) For each polynomial $f \in \mathcal{O}_v[X]$ and each element $a \in \mathcal{O}_v$ with $\overline{f}^v(\overline{a}^v) = 0$ and $\frac{\partial}{\partial X}\overline{f}^v(\overline{a}^v) \neq 0$, there exists an element $\alpha \in \mathcal{O}_v$ with $f(\alpha) = 0$ and $\overline{\alpha}^v = \overline{a}^v$.

(iv) Every polynomial $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathcal{O}_v[X]$ with $a_{n-1} \in \mathcal{O}_v^\times$ and $a_{n-2}, \ldots, a_0 \in \mathfrak{m}_v$ has a zero in K.

(v) Every polynomial $X^n + X^{n-1} + \cdots + a_0 \in \mathcal{O}_v[X]$ with $a_{n-2}, \ldots, a_0 \in \mathfrak{m}_v$ has a zero in K.

Using 1.1.49 (iii) and (iv) yields the following.

1.1.50 **Corollary:**

Let K be a field, let v_1 be a valuation of K, let v_2 be a valuation of the residue field $\overline{K}^{v_1}$, and let $v = v_1 \circ v_2$ be the composition of these two valuations. Then (K, v) is henselian if and only if (K, v_1) and $(\overline{K}^{v_1}, v_2)$ are henselian.

One can show (iv) $\Rightarrow$ (i) in Theorem 1.1.49 by using only separable polynomials.

1.1.51 **Corollary:**

Let $(L,w)/(K,v)$ be an extension of valued fields. Suppose that (L,w) is henselian and K is relatively separably closed in L. Then (K,v) is also henselian.

1.1.52 **Remarks:**

The henselization of a valued field is

1. a separable extension, since any valuation of the algebraic closure must be henselian by definition, and hence, by Corollary 1.1.51, so is every valuation of the separable closure.
2. an immediate extension.

1.1.53 **Lemma:**

Let K be a field, and let $\mathcal{O}_1$ and $\mathcal{O}_2$ be two valuation rings of K such that $\mathcal{O}_1 \subset \mathcal{O}_2$. Then the henselization of $(K,\mathcal{O}_2)$ is contained in the henselization of $(K,\mathcal{O}_1)$.

Proof:

Let $(K_1^h,\mathcal{O}_1^h)$ be the henselization of $(K,\mathcal{O}_1)$, and let $(K_2^h,\mathcal{O}_2^h)$ be the henselization of $(K,\mathcal{O}_2)$. Let $\mathcal{O}'$ be an extension of $\mathcal{O}_2$ to K_1^h such that $\mathcal{O}_1^h \subset \mathcal{O}'$ (see Corollary 1.1.31), so, by Corollary 1.1.50, $(K_1^h,\mathcal{O}')$ is also henselian. Hence $(K_2^h,\mathcal{O}_2^h)$ can be uniquely embedded into $(K_1^h,\mathcal{O}')$, and thus $K_2^h \subset K_1^h$.

q.e.d.

1.1.54 **Theorem:**

Let (K,v) be a valued field of residue characteristic 0. Then (K,v) is henselian if and only if it is **algebraically maximal**, i.e., it does not admit proper algebraic immediate extensions.

1.1.55 **Corollary:**

Let (K,v) be a valued field of residue characteristic 0. Then its henselization $(K^{\mathrm{h}},v^{\mathrm{h}})$ is algebraically maximal.

1.1.56 **Corollary:**

Let F/K be an extension of fields. Let v be a valuation of F of residue characteristic 0, and let T be a transcendence basis of F/K such that the extension (F,v) of $(K(T),v)$ is immediate. Then the henselization of $(K(T),v)$ is equal to the henselization of (F,v).

Proof:

From the definition of the henselization, it follows that $(K(T)^h, v^h) \subset (F^h, v^h)$. Since $(F, v)/(K(T), v)$ is an algebraic, immediate extension, the extension of their henselizations is also algebraic and immediate. Hence, by Corollary 1.1.55, they are equal.

q.e.d.

In a henselian valued field of residue characteristic 0, one can embed its residue field. Moreover, the following holds.

1.1.57 **Lemma:**

Let (L, v) be a henselian valued field of residue characteristic 0. Let $\rho\colon \mathcal{O}_v \longrightarrow \overline{L}^v$ be the residue homomorphism. Now, let K be a subfield of $\mathcal{O}_v$, so $\rho|_K$ is injective. Then there is an embedding $\sigma\colon \overline{L}^v \longrightarrow \mathcal{O}_v$ with $\rho \circ \sigma = \mathrm{id}_{\overline{L}^v}$ and $\sigma|_K = (\rho|_K)^{-1}$.

Proof:

Since the residue characteristic of (L, v) is zero, $\mathbb{Q}$ is a subfield of $\overline{L}^v$ which embeds canonically into L. This embedding can be extended to an embedding of $\rho(K) = \overline{K}^v$ into L by mapping $\overline{a}^v$ on a for $a \in K$. With Zorn's Lemma we find a maximal subfield M of $\overline{L}^v$ which has an embedding σ into L that extends the embedding of $\overline{K}^v$ and has the property $\rho \circ \sigma = \mathrm{id}_M$. We claim that $M = \overline{L}^v$.

Assume that there exists some $b \in \overline{L}^v \backslash M$. If b is transcendental over M, then, by Theorem 1.1.42, any representative a of b in L is transcendental over $\sigma(M)$. Therefore we could extend the embedding σ of M into L to $M(b)$ by mapping b to such a representative a, contradicting the maximality of M.
If b is algebraic over M, let $f \in \mathcal{O}_v[X]$ be the polynomial that results by applying σ on the coefficients of the irreducible polynomial g of b over M. Then $\overline{f}^v = g$. By Theorem 1.1.49 (iii), there exists some $a \in L$ such that $\overline{a}^v = b$ and $f(a) = 0$. So we could again extend σ to $M(b)$ by mapping b on a, and therefore get a contradiction.

q.e.d.

1.1.3 The Topology Induced by a Valuation

Next, we study the topology of a valued field. In the case of a henselian valued field, there exists a valuation theoretic implicit function theorem which we will quote below.

1.1.58 **Definition:**

Let K be a field, and let v be a valuation of K.
For each $\gamma \in \Gamma_v$ and each $a \in K$, we define the set

$$\mathcal{U}_\gamma(a) := \{x \in K \mid v(x - a) > \gamma\}.$$

For fixed $a \in K$, these sets form a basis of open neighbourhoods of a.
Let $\tau_v := \tau_{(K,v)} := \{U \subset K \mid \forall\ a \in U\ \exists\ \gamma \in \Gamma_v\colon \mathcal{U}_\gamma(a) \subset U\}$. Then τ_v is a topology on K, called the **topology on K induced by v**.

1.1.59 **Proposition:**

Let (K, v) be a valued field. Let τ_v be the topology on K induced by v. Then the following statements hold:

a) τ_v is Hausdorff.

b) v is trivial if and only if τ_v is discrete.

c) For all $a \in K$ and all $\gamma \in \Gamma_v$, the subsets $\{x \in K \mid v(x-a) \geqslant \gamma\}$, $\{x \in K \mid v(x-a) \leqslant \gamma\}$ and $\{x \in K \mid v(x-a) = \gamma\}$ of K are open, hence they and the sets $\mathcal{U}_\gamma(a)$ are both open and closed.
In particular, $\mathcal{O}_v$ and $\mathfrak{m}_v$ are both open and closed with respect to τ_v.

d) The field operations $+$, $\cdot$ and $^{-1}$ are continuous with respect to τ_v.

In the case of a rank-1-valuation v of a field K, one can define with respect to the topology induced by this valuation the **completion** of (K, v), which is a complete, immediate extension of (K, v) in which K lies dense. Then the following holds.

1.1.60 **Theorem:**

Let K be a field, and let v be a rank-1-valuation of K. Then the completion of K with respect to v is henselian.

1.1.61 **Lemma:**

Let (L, v) be a non-trivially valued field, and let K be a subfield of L. Then the elements of $L \backslash K$ lie dense in L with respect to the topology induced by v.

Proof:

Suppose there exist $a \in L$ and $\gamma \in \Gamma_v$ such that $\mathcal{U}_\gamma(a) \cap (L \backslash K) = \varnothing$. In particular, a lies in K. Now, let $x \in L \backslash K$. Then $x + a \in L \backslash K$, and we have that $v(x) = v((x+a) - a) \leqslant \gamma$. Hence $\mathcal{U}_\gamma(0) \cap (L \backslash K) = \varnothing$.

Let $b \in L^\times$ with $v(b) > 2\gamma$, and let $x \in L \backslash K$. Then we have $b \in K^\times$, and therefore $\frac{b}{x} \in L \backslash K$. But $v(\frac{b}{x}) > \gamma$, a contradiction.

q.e.d.

Prestel and Ziegler proved in [21] a valuation theoretic implicit function theorem by model theoretic methods.

1.1.62 **Theorem:** (Implicit Function Theorem)

Let (K, v) be a henselian valued field, and let τ_v be the topology on K induced by v. Let $f_1, \ldots, f_m \in K[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ and set

$$J := \begin{pmatrix} \frac{\partial}{\partial Y_1} f_1 & \cdots & \frac{\partial}{\partial Y_m} f_1 \\ \vdots & \ddots & \vdots \\ \frac{\partial}{\partial Y_1} f_m & \cdots & \frac{\partial}{\partial Y_m} f_m \end{pmatrix}.$$

Let $a_1, \ldots, a_n, b_1, \ldots, b_m \in K$ such that $f_1(a_1, \ldots, a_n, b_1, \ldots, b_m) = \cdots = f_m(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0$, but $\det J(a_1, \ldots, a_n, b_1, \ldots, b_m) \neq 0$. Then there are τ_v-neighbourhoods U, V of 0 such that, for all $a_1' \in a_1 + U, \ldots, a_n' \in a_n + U$, there is exactly one solution $(b_1', \ldots, b_m')$ of $f_1(a_1', \ldots, a_n', Y_1, \ldots, Y_m) = \cdots = f_m(a_1', \ldots, a_n', Y_1, \ldots, Y_m) = 0$ such that $b_1' \in b_1 + V, \ldots, b_m' \in b_n + V$.
The map $(a_1 + U) \times \cdots \times (a_n + U) \longrightarrow K^m$, $(a_1', \ldots, a_n') \mapsto (b_1', \ldots, b_m')$ is continuous.

1.1.4 Abhyankar Valuations and Prime Divisors

In the main part of this chapter, we will work with valuations of finitely generated field extensions which are trivial on the smaller field. Such valuations may have *bad* properties., e.g., the value group or residue field may not be finitely generated. For examples, see [14]. But we will consider so-called Abhyankar valuation, and we will see in this section that they do not have these *bad* properties.

1.1.63 **Definition:**

Let K be a field.

We call any finitely generated extension of K of transcendence degree $n \geqslant 1$ an **(algebraic) function field of degree n over K.**

Let F be a field extension of K. A valuation v of F which is trivial on K is called a **valuation of F/K** or a **K-trivial valuation of F.**

From the Dimension Inequality, we can immediately derive the following.

1.1.64 **Proposition:** (Abhyankar Inequality)

Let F/K be an extension of fields, and let v be a valuation of F/K. We have $K \subset \mathcal{O}_v$ and therefore $\overline{K}^v = K$. Then the following holds:

$$\operatorname{trdeg}(F/K) \geqslant \operatorname{trdeg}(\overline{F}^v/K) + \operatorname{rr}(\Gamma_v).$$

1.1.65 **Definition:**

Let us make the same assumptions as in 1.1.64. We call a valuation v of F/K satisfying the **Abhyankar Equality**

$$\operatorname{trdeg}(F/K) = \operatorname{trdeg}(\overline{F}^v/K) + \operatorname{rr}(\Gamma_v)$$

a **(K-trivial) Abhyankar valuation of** F/K.

In 1.1.46, we have given an example of an Abhyankar valuation of the rational function field $\mathbb{R}(X_1, \ldots, X_5)$ over $\mathbb{R}$.

1.1.66 **Proposition:**

Let F be a function field over a field K. Let v be an Abhyankar valuation of F/K. Then Γ_v is a finitely generated $\mathbb{Z}$-module – the product of $\operatorname{rr}(\Gamma_v)$ copies of $\mathbb{Z}$ –, and the residue field $\overline{F}^v$ is again a function field over K.

Proof:

This follows from Theorem 1.1.42 and the Fundamental Inequality 1.1.39, since an extension of finite index of an abelian group which is a finitely generated $\mathbb{Z}$-module is again a finitely generated $\mathbb{Z}$-module.

q.e.d.

1.1.67 **Lemma:**

Let F/K be an extension of fields, and let v be an Abhyankar valuation of rank $m \in \mathbb{N}$ of F/K. Then v is the composition of m Abhyankar valuations of rank 1 over K.

Proof:

Let Δ be a maximal proper convex subgroup of the value group Γ_v of v. Then $v' \colon F^\times \overset{v}{\twoheadrightarrow} \Gamma_v \twoheadrightarrow \Gamma_v/\Delta$ is a valuation of rank 1 of F/K and $\overline{v} \colon \overline{F}^{v'} \twoheadrightarrow \Delta \cup \{\infty\}$, $\overline{a}^{v'} \mapsto v(a)$, is a valuation of rank $m-1$ of $\overline{F}^{v'}/K$. Since $\overline{(\overline{F}^{v'})}^{\overline{v}} = \overline{F}^v$, we have

$$\operatorname{trdeg}(F/K) \geqslant \operatorname{trdeg}(\overline{F}^{v'}/K) + \operatorname{rr}(\Delta) \text{ and}$$

$$\operatorname{trdeg}(\overline{F}^{v'}/K) \geqslant \operatorname{trdeg}(\overline{F}^{v}/K) + \operatorname{rr}(\Gamma_v/\Delta).$$

Together with $\operatorname{rr}(\Gamma_v) = \operatorname{rr}(\Delta) + \operatorname{rr}(\Gamma_v/\Delta)$ (Proposition 1.1.21), it follows that

$$\begin{aligned} \operatorname{trdeg}(F/K) &= \operatorname{trdeg}(\overline{F}^{v}/K) + \operatorname{rr}(\Gamma_v) = \operatorname{trdeg}(\overline{F}^{v}/K) + \operatorname{rr}(\Gamma_v/\Delta) + \operatorname{rr}(\Delta) \\ &\leqslant \operatorname{trdeg}(\overline{F}^{v'}/K) + \operatorname{rr}(\Delta) \leqslant \operatorname{trdeg}(F/K), \end{aligned}$$

and hence the inequalities above have to be equalities. Thus v' and $\overline{v}$ are both Abhyankar valuations over K, and we can proceed by induction over the rank.

q.e.d.

1.1.68 **Example:**

Consider Example 1.1.46. As mentioned above, this is an Abhyankar valuation of $F = \mathbb{R}(X_1, X_2, X_3, X_4, X_5)$ over $\mathbb{R}$. It is also the composition of the following two Abhyankar valuations of rank 1:

- $v_1 \colon F^\times \twoheadrightarrow \mathbb{Z} \oplus \mathbb{Z}2\pi = \mathbb{Z}v_1(\frac{X_5}{X_4}) \oplus \mathbb{Z}v_1(X_5^2 - X_4^3)$. The residue field of (F, v_1) is $\mathbb{R}(X_1, X_2, X_3)$.
- $v_2 \colon \mathbb{R}(X_1, X_2, X_3)^\times \twoheadrightarrow \mathbb{Z} \oplus \mathbb{Z}\sqrt{2} = \mathbb{Z}v_2(X_2) \oplus \mathbb{Z}v_2(X_3^3 - X_1)$. The residue field of $(\mathbb{R}(X_1, X_2, X_3), v_2)$ is $\mathbb{R}(X_3)$.

1.1.69 **Corollary:**

Let F be a function field over a field K, and let v be an Abhyankar valuation of F/K such that $\operatorname{rr}(\Gamma_v) = r \in \mathbb{N}$. Then $\operatorname{rank}(\Gamma_v) = \operatorname{rr}(\Gamma_v) = r$ if and only if Γ_v is isomorphic to $\mathbb{Z}^r$ equipped with the lexicographical ordering.

Proof:

Obviously, $\mathbb{Z}^r$ with the lexicographical ordering has rank r. Suppose $\operatorname{rank}(\Gamma_v) = r = \operatorname{rr}(\Gamma_v)$. By Lemma 1.1.67, v is the composition of r Abhyankar valuations $v_1, \ldots, v_r$ of rank 1 over K. Remark 1.1.35 tells us that Γ_v is isomorphic to $\Gamma_{v_1} \times \cdots \times \Gamma_{v_r}$ ordered lexicographically. In particular, $r = \operatorname{rr}(\Gamma_v) = \sum_{j=1}^r \operatorname{rr}(\Gamma_{v_j})$, hence $\operatorname{rr}(\Gamma_{v_1}) = \cdots = \operatorname{rr}(\Gamma_{v_r}) = 1$, and therefore the value group of each of these r Abhyankar valuations is isomorphic to $\mathbb{Z}$.

q.e.d.

An interesting subclass of the class of all Abhyankar valuations are the divisorial valuations.

1.1.70 **Definition:**

Let F be a function field of degree n over a field K. Let v be a nontrivial valuation of F/K. If $\operatorname{trdeg}(\overline{F}^v/K) = n-1$, then the valuation v is called a **prime divisor** or a **divisorial valuation**.

1.1.71 **Proposition:**

Let F be a function field of degree n over a field K. Let v be a prime divisor of F/K. Then v is an Abhyankar valuation of F/K. Moreover, it is a discrete valuation of rank one, i.e., $\Gamma_v \cong \mathbb{Z}$.

Proof:

Since $\operatorname{rr}(\Gamma_v) \geqslant 1$, it follows from Proposition 1.1.64 that v is an Abhyankar valuation and $\operatorname{rr}(\Gamma_v) = 1$. From Proposition 1.1.66, it then follows that $\Gamma_v \cong \mathbb{Z}$.

q.e.d.

Let F be a function field over a field K. Let v be an Abhyankar valuation of F/K such that the value group Γ_v of v is $\mathbb{Z}^r$ lexicographically ordered or equivalently $\operatorname{rank}(\Gamma_v) = \operatorname{rr}(\Gamma_v) = r$ (Corollary 1.1.69). By Lemma 1.1.67, v is the composition of r Abhyankar valuations of rank 1 over K. Since the rational rank of Γ_v is r, the value group of each of these r Abhyankar valuation must have rational rank 1. Then, by the Abhyankar Equality, these valuations are prime divisors, and therefore the following definition is justified.

1.1.72 **Definition:**

Let F be a function field over a field K. We call an Abhyankar valuation of F/K with lexicographically ordered value group an **iterated prime divisor**.

1.2 Abhyankar Valuations of Rank 1

In this section, our goal is a generalization for arbitrary Abhyankar valuations of rank 1 of the second part of the following local uniformization theorem of Lang for prime divisors (see [16]).

1.2.1 **Theorem:**

Let K be a field of characteristic 0, and let F be a function field of degree 1 over K.

1. Let $F = K(x, y)$, where $f(x, y) = 0$ for some irreducible polynomial $f(X, Y) \in K[X, Y]$. Let $a, b \in K$ be such that $f(a, b) = 0$ but $\frac{\partial}{\partial Y} f(a, b) \neq 0$. Then there exists a unique discrete valuation ring $\mathcal{O}$ of F with maximal ideal $\mathfrak{m}$ such that $K \subset \mathcal{O}$ and $\overline{x} = a, \overline{y} = b \in K \subset \mathcal{O}/\mathfrak{m}$. It then follows that the element $x - a$ is a generator of the ideal $\mathfrak{m}$ and we have $K = \mathcal{O}/\mathfrak{m}$.

2. Conversely, let $\mathcal{O}$ be a discrete valuation ring of F containing K with maximal ideal $\mathfrak{m}$ such that $\mathcal{O}/\mathfrak{m} = K$. Let $x \in F$ be a generator of $\mathfrak{m}$. Then there exists some $y \in \mathcal{O}$ such that $F = K(x,y)$, and such that $f(a,b) = 0$ but $\frac{\partial}{\partial Y} f(a,b) \neq 0$ holds for an irreducible polynomial $f(X,Y) \in K[X,Y]$ of x, y over K and the residue classes $a := \overline{x} = 0, b := \overline{y} \in \mathcal{O}/\mathfrak{m} = K$.

1.2.2 **Remark:**

The first part of Theorem 1.2.1 is a special case of Theorem 1.1.11: The set $\mathcal{O}$ of all rational functions $\frac{g(x,y)}{h(x,y)} \in F$, where $g(x,y), h(x,y) \in K[x,y]$ such that $h(a,b) \neq 0$, is a discrete valuation ring with maximal ideal $\mathfrak{m} = \{\frac{g(x,y)}{h(x,y)} \in F \mid g(x,y), h(x,y) \in K[x,y],\ g(a,b) = 0,\ h(a,b) \neq 0\}$ such that $K \subset \mathcal{O}$, $\overline{x} = a, \overline{y} = b \in K \subset \mathcal{O}/\mathfrak{m}$ and $x - a$ is a generator of $\mathfrak{m}$. From this, the uniqueness of $\mathcal{O}$ follows immediately. Moreover, it follows that $K = \mathcal{O}/\mathfrak{m}$, since $K \subset \mathcal{O}$ and, for all $\frac{g(x,y)}{h(x,y)} \in \mathcal{O}$ such that $h(a,b) \neq 0$, we have $\overline{\left(\frac{g(x,y)}{h(x,y)}\right)}^{\mathcal{O}} = \frac{g(a,b)}{h(a,b)} \in K$.

Let F' be a function field over a field K' of characteristic 0, and let v be a prime divisor of F'/K'. We embed the residue field $K := \overline{F'}^v$ into the henselization (H, v) of (F', v) and consider the compositum F of F' and K in H. Then F is a function field of degree 1 over K. Lang shows in the second part of the theorem that the valuation ring of v in F is the local ring of a K-rational non-singular point of an affine irreducible curve defined over K with function field F. Moreover, in the proof of the theorem, y can be chosen in such a way that $\overline{y}^{\mathcal{O}} = 1$.

For the generalization, we will need the following result of Elliott (see [5]). Using the algorithm of Perron, Zariski proved in [31] the same result for ordered groups of rank 1. Actually, we will mostly need this result in the case of a valuation of rank 1.

1.2.3 **Lemma:**

Let G be a finitely generated ordered abelian group, i.e., $G \cong \mathbb{Z}^m$ for some $m \in \mathbb{N}$ (see Remark 1.1.14). Let $g_1, \ldots, g_n \in G$ be non-negative. Then there exist positive elements $b_1, \ldots, b_m \in G$ such that $G = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_m$ and, for all $i \in \{1, \ldots, n\}$, the element $g_i \in G$ can be written as a sum $\sum_{j=1}^m n_{ij} b_j$ with $n_{ij} \in \mathbb{N}$.

Proof:

Let $c_1, \ldots, c_m$ be a $\mathbb{Z}$-basis of G containing only positive elements. We will process the elements $g_1, \ldots, g_n$ one after the other. So we can assume without loss of generality that we have a representation $g_i = \sum_{j=1}^m n_{ij} c_j$ with $n_{ij} \in \mathbb{N}$ for all $i < n$. We write

$$g := g_n = r_1 c_1 + \cdots + r_m c_m$$

with $r_1, \ldots, r_m \in \mathbb{Z}$. Let $j_1, \ldots, j_k \in \{1, \ldots, m\}$ be all indices j with $r_j \neq 0$. We may suppose that $\{j_1, \ldots, j_k\} = \{1, \ldots, k\}$

If one of the r_j with $j \leqslant k$ is not positive, we can assume after renaming that without loss of generality $r_1 < 0$ and $r_2, \ldots, r_k > 0$: Otherwise, we can substract all but one summands $r_j c_j$ with $r_j < 0$ from g and gain an element $g' > g$. Later, we will change only the remaining basis elements (in the representation of g') to gain a representation of g' with only non-negative coefficients. Then we can re-add some $r_j c_j$ with $r_j < 0$ to g' to get an element g'' such that $g \leqslant g'' < g'$ and proceed with g'' in the same way. After finitely many steps we get a representation of g with non-negative coefficients.

We have to distinguish two cases:

First case: $c_j > c_1$ for some $1 < j \leqslant k$.
Set $c'_j := c_j - c_1$. Then $0 < c'_j < c_j$ and we have

$$g = (r_1 + r_j)c_1 + \cdots + r_j c'_j + \cdots + r_k c_k.$$

If $r_1 + r_j \geqslant 0$, we are done. Otherwise, if $r_1 + r_j < 0$, we make another case distinction, but now, since $|r_1 + r_j| = -r_1 - r_j = |r_1| - r_j < |r_1|$, we have reduced the sum of the absolute values of the coefficients.

Second case: $c_1 > c_j$ for all $1 < j \leqslant k$.
We may suppose that $c_1 > c_2 > \cdots > c_k$. Since $\sum_{j=1}^k r_j c_1 > \sum_{j=1}^k r_j c_j > 0$, we have that $\sum_{j=1}^k r_j > 0$. Denote by $e \in \{2, \ldots, k\}$ the index with $\sum_{j=1}^e r_j \geqslant 0$ and $\sum_{j=1}^{e-1} r_j < 0$, and set

$$c'_1 := c_1 - c_e, \ldots, c'_{e-1} := c_{e-1} - c_e, c'_e := c_e, \ldots, c'_k := c_k.$$

We now have

$$g = r_1 c'_1 + \cdots + r_{e-1} c'_{e-1} + \underbrace{\left(\sum_{l=1}^{e} r_l \right)}_{<r_e} c'_e + r_{e+1} c_{e+1} + \cdots + r_k c'_k.$$

Hence we have decreased the sum of the absolute values of the coefficients, and go back to the distinction of the two cases.

Note that if we change the basis of G as we do in those two cases, every element $h = \sum_{j=1}^m s_j c_j$ where $s_1, \ldots, s_m \in \mathbb{N}$ has, with respect to the new basis, again a representation with non-negative coefficients.

Since in both cases, we decrease the sum of the absolute values of the coefficients by changing the basis, we are finished after finitely many steps as described in the first case.

q.e.d.

Let F be a function field over a field K. We say that a valuation v of F/K admits **local uniformization** iff there exists an irreducible affine K-variety V with coordinate ring $K[V] \subset F$ such that F is equal to the function field $K(V)$ of V, and such that v is centered at a non-singular K-rational P point of V, i.e., $K[V] \subset \mathcal{O}_v$

and $\mathfrak{m}_v \cap K[V] = \mathfrak{m}_P$. It was proven by Zariski in [31] that, if the characteristic of K is zero, all valuations of F/K admit local uniformization. For Abhyankar valuations of F/K where the residue field is separable over K, local uniformization was shown by Knaf and Kuhlmann in [11] for all characteristics. The next lemma states that, after a finite extension, local uniformization is possible in case of an Abhyankar valuation of rank 1 with residue field K where $\mathrm{char}(K) = 0$. We include a proof of this lemma below and also a proof of a more general theorem in the next section.

1.2.4 **Lemma:**

Let K be a field of characteristic 0, and let F be a function field of degree $t \geqslant 1$ over K. Let w be an Abhyankar valuation of F/K with archimedean ordered value group $\Gamma_w \cong \mathbb{Z}^t$ having K as its residue field. Let $x'_1, \ldots, x'_t \in \mathcal{O}_w$ be such that $w(x'_1), \ldots, w(x'_t)$ generate Γ_w, and let M be a finite subset of $\mathcal{O}_w \backslash \{0\}$. Then there exist elements $x_1, \ldots, x_t \in F$, algebraically independent over K, and an element $y \in F$, algebraic over $K(x_1, \ldots, x_t)$, of degree $m \in \mathbb{N}$ such that

a) $F = K(x_1, \ldots, x_t, y)$,
b) $w(x_1), \ldots, w(x_t)$ generate Γ_w and $x_1, \ldots, x_t$ all lie in the subgroup of $F^\times$ generated by $x'_1, \ldots, x'_t$,
c) $x_1, \ldots, x_t, y - 1 \in \mathfrak{m}_w$,
d) there exists an irreducible polynomial $g(X_1, \ldots, X_t, Y) \in K[X_1, \ldots, X_t, Y]$ of Y-degree m such that $g(x_1, \ldots, x_t, y) = 0$ and $g(0, \ldots, 0, Y) = u(Y-1)Y^m$ for some $u \in K^\times$, hence, in particular, $g(\overline{x_1}^w, \ldots \overline{x_t}^w, \overline{y}^w) = 0$ but $\frac{\partial}{\partial Y} g(\overline{x_1}^w, \ldots \overline{x_t}^w, \overline{y}^w) \neq 0$, and
e) each element a of M is a product of a unit b_a and a monomial in $x_1, \ldots, x_t$, where the latter are the generators of the maximal ideal of the regular local ring $K[x_1, \ldots, x_t, y]_{(x_1, \ldots, x_t, y-1)}$ (see Theorem 1.1.11). In particular, for all valuations w' of F/K such that $(\overline{x_1}^{w'}, \ldots, \overline{x_t}^{w'}, \overline{y}^{w'}) = (0, \ldots, 0, 1)$, we have $b_a \in \mathcal{O}_{w'}^\times$ and $\overline{b_a}^{w'} = \overline{b_a}^w$ for all $a \in M$ (see Corollary 1.1.8).

After a suitable choice of y, we will encode all necessary informations as a finite subset P of the rational function field $K(x'_1, \ldots, x'_t)$. Then we will use Lemma 1.2.3 to find $x_1, \ldots, x_t$ in the subgroup of $K(\underline{x'})^\times$ generated by $x'_1, \ldots, x'_t$ in such a way that every element of P has a *nice* representation with respect to $x_1, \ldots, x_t$. This will yield the desired results.

Proof:

By Theorem 1.1.42, the elements $x'_1, \ldots, x'_t$ are algebraically independent over K, hence $F = K(x'_1, \ldots, x'_t, z)$, where z is algebraic over $K(\underline{x'})$ and (without loss of generality) lies in $\mathcal{O}_w$. The extension $(F, w)/K(\underline{x'}), w)$ is immediate, so by Corollary 1.1.56, the henselization of $(K(\underline{x'}), w)$ is equal to the henselization (H, w) of (F, w).

If $[F : K(\underline{x'})] > 1$, let $z = z_1, \ldots, z_m$ be the pairwise different conjugates of z. Since w is a valuation of rank 1, H is contained in the completion of $K(\underline{x'})$

with respect to w (see Corollary 1.1.56 and Theorem 1.1.60), thus the field $K(\underline{x}')$ lies dense in H with respect to the topology $\tau_{(H,w)}$ induced by w. We extend w to the algebraic extension $H(z_2, \ldots, z_m)$ of H. Then the restriction of the topology $\tau_{(H(\underline{z}),w)}$ on $H(\underline{z})$ induced by w to H is equal to $\tau_{(H,w)}$. Since these topologies are Hausdorff, we can find an open neighbourhood U of z which does not contain $z_2, \ldots, z_m$. Restricting U to H yields again an open neighbourhood of z, and hence, since $K(\underline{x}')$ is dense in $(H, \tau_{(H,w)})$, we can find some $d \in K(\underline{x}') \cap U$. Moreover, we can choose $d \in K(\underline{x}')$ so close to z that

$$w(z-d) > w(z_j - d) \text{ for all } j \in \{2, \ldots, m\}$$
$$\text{and } w(z-d) > 0.$$

From $z \in \mathcal{O}_w$, it follows that d lies in $\mathcal{O}_w$, too. Since (F, w) is an immediate extension of $(K(\underline{x}'), w)$, we find some $e \in K(\underline{x}')$ with $w(z-d) = w(e)$ and even $w(\frac{z-d}{e} - 1) > 0$, i.e., $w(\frac{e}{z-d}) = w(1) = 0$ and $\overline{\frac{e}{z-d}}^w = 1$. The conjugates of $y := \sigma_1(y) = \frac{e}{z-d}$ different from y are the pairwise different elements $\sigma_2(y) = \frac{e}{z_2-d}, \ldots, \sigma_m(y) := \frac{e}{z_m-d} \in \mathfrak{m}_v$, where $\mathrm{id} = \sigma_1, \ldots, \sigma_m \in \mathrm{Aut}(K(\underline{x}')^{\mathrm{alg}}/K(\underline{x}'))$. Let

$$f(Y) = \sum_{l=0}^{m} \psi_l(\underline{x}')Y^l = \prod_{j=1}^{m}(Y - \sigma_j(y))$$

be the irreducible polynomial of y over $K(\underline{x}')$. Since all conjugates of y have non-negative values, all $\psi_l(\underline{x}')$ lie in $\mathcal{O}_w$. Set $\Psi := \{\psi_0, \ldots, \psi_m\}$. We will come back to them later. If $[F : K(\underline{x}')] = 1$, we set $\Psi := \varnothing$ and $y := 1$.

We now have $F = K(\underline{x}', z) = K(\underline{x}', y)$. Since $w(x'_1), \ldots, w(x'_t)$ generate the value group of w, we can write each $a \in M$ in the following way: $a = x'^{\alpha(a)} b_a$, where $\alpha(a) \in \mathbb{Z}^t$ and $\sum_{i=1}^t \alpha(a)_i w(x'_i) = w(a) \in \mathbb{Z}^t$. Set $S_M := \{x'^{\alpha(a)} \mid a \in M\} \subset \mathcal{O}_w$. Now we fix some $a \in M$. Note that $b := b_a$ is a unit in $\mathcal{O}_w$. If $b \notin K(\underline{x}')$, we also want to consider the units $yb, \ldots, y^{m-1}b$, so set $b_j := y^j b$ for $j = 0, \ldots, m-1$. The $1 \leqslant m_j \leqslant m$ pairwise different conjugates of b_j are contained in the following set $\{b_j(\underline{x}', y) = \sigma_1(b_j(\underline{x}', y)) = \sigma_1(y)^j b(\underline{x}', \sigma_1(y)), \ldots, \sigma_m(b_j(\underline{x}', y)) = \sigma_m(y)^j b(\underline{x}', \sigma_m(y))\}$. Let $1 \in I_j \subset \{1, \ldots, m\}$ be a set of m_j indices such that $\sigma_k(b_j) \neq \sigma_l(b_j)$ for all $k \neq l \in I_j$. Using the same considerations as above, for all $j \in \{0, \ldots, m-1\}$, we find some $d_j, e_j \in K(\underline{x}') \cap \mathcal{O}_w$ such that

$$w(b_j - d_j) > w(\sigma_k(b_j) - d_j) \text{ for all } k \in I_j \backslash \{1\},$$
$$w(b_j - d_j) > 0 \text{ and}$$
$$w\left(\frac{b_j - d_j}{e_j} - 1\right) > 0.$$

Since $w(b_j) = 0$, it follows from the second condition that $w(d_j) = 0$. Moreover, b_j and d_j must have the same residue class. From the last two conditions, it follows that $w(e_j) > 0$.

Let

$$f_j(T) := \sum_{l=0}^{m_j} \psi_{jl}(\underline{x}')T^l = \prod_{k \in I_j} \left(T - \frac{e_j}{\sigma_k(b_j) - d_j} \right)$$

be the irreducible polynomial of $\frac{e_j}{b_j - d_j}$ over $K(\underline{x}')$. Set

- $D_a := \{d_j \mid j = 0, \ldots, m-1\}$,
- $E_a := \{e_j \mid j = 0, \ldots, m-1\}$ and
- $\Psi_a := \{\psi_{jl} \mid j \in \{1, \ldots, m\},\ l \in \{1, \ldots, m_j\}\}$.

Let $M_1 := \{a \in M \mid b_a \notin K(\underline{x}')\}$, $M_2 := \{a \in M \mid b_a \in K(\underline{x}')\}$ and $B := \{b_a \mid a \in M_2\}$.

Now we have collected all the data we will need. We consider the following finite set of rational functions

$$P := \left(\Psi \cup B \cup \bigcup_{a \in M_1} D_a \cup \bigcup_{a \in M_1} E_a \cup \bigcup_{a \in M_1} \Psi_a \right) \backslash \{0\} \subset K(\underline{x}')^\times \cap \mathcal{O}_w.$$

Let $\zeta \in P$ be of the form $\zeta = \frac{\zeta'(\underline{x}')}{\zeta''(\underline{x}')}$ with $\zeta', \zeta'' \in K[\underline{x}']$. Suppose $\zeta' = \sum_{\alpha \in \mathbb{N}^t} u_\alpha x'^\alpha$ and $\zeta'' = \sum_{\alpha \in \mathbb{N}^t} v_\alpha x'^\alpha$, where $u_\alpha, v_\alpha \in K$ for all $\alpha \in \mathbb{N}^t$. Since ζ lies in $\mathcal{O}_w$, we have $w(\zeta') \geqslant w(\zeta'')$. Since the values of $x'_1, \ldots, x'_t$ are $\mathbb{Z}$-linearly independent and w is trivial on K, the value of a polynomial $p \in K[\underline{x}']$ is equal to the least value of its monomials, hence $w(\zeta'') = w(x'^{\alpha''})$ for some $\alpha'' \in \mathbb{N}^t$ with $v_{\alpha''} \neq 0$. Now we can write

$$\zeta = \frac{\frac{\zeta'}{x'^{\alpha''}}}{\frac{\zeta''}{x'^{\alpha''}}} = \frac{\sum_{\alpha \in \mathbb{N}^t} u_\alpha \frac{x'^\alpha}{x'^{\alpha''}}}{\sum_{\alpha \in \mathbb{N}^t} v_\alpha \frac{x'^\alpha}{x'^{\alpha''}}} =: \frac{\eta'}{\eta''},$$

and it follows that η' lies in $\mathcal{O}_w$ and η'' lies in $\mathcal{O}_w^\times$, but in general they will not lie in $K[\underline{x}']$.

Suppose we have such a representation for all the elements in P. Then let S_P be the finite set of all products x'^α ($\alpha \in \mathbb{Z}^t$) occuring in the numerator or denominator of any such representation. Let S be the union of S_P and S_M. Now we apply Lemma 1.2.3 to the finite subset S and the subgroup G of $K(\underline{x}')^\times$ generated by $x'_1, \ldots, x'_t$ and equipped with the ordering induced by the ordering on the value group. We get positive generators $x_1, \ldots, x_t$ of G such that all elements of S are monomials in the x_i. In particular, for all elements ζ in P, we get a representation $\zeta = \frac{\xi'(\underline{x})}{\xi''(\underline{x})}$ with $\xi'(\underline{x}) \in K[\underline{x}] \cap \mathcal{O}_w$ and $\xi''(\underline{x}) \in K[\underline{x}] \cap \mathcal{O}_w^\times$.

The elements $x_1, \ldots, x_t$ are again algebraically independent over K, and we have that $F = K(\underline{x}', y) = K(\underline{x}, y)$. Now if $F = K(\underline{x}')$, there is nothing more to do: In this case, for all $a \in M$, we have $a = x'^{\alpha(a)} b_a = x^{\alpha'} b_a$, where $\alpha' \in \mathbb{N}$ and $b_a \in (K[x_1, \ldots, x_t]_{(x_1, \ldots, x_t)})^\times$, since $x'^{\alpha(a)} \in S_M \subset S$ and $b_a \in P$. Otherwise, if $[F : K(\underline{x}')] > 1$, let w' be a valuation of F/K such that $x_1, \ldots, x_t, y - 1 \in \mathfrak{m}_{w'}$. Then for any polynomial p in $K[\underline{x}]$, the residue class of p w.r.t. w' is the constant term $p(0) \in K$. Hence, we have $\overline{p(\underline{x})}^{w'} = \overline{p(\underline{x})}^{w}$ for all $p(\underline{x}) \in K[\underline{x}]$. Therefore, it follows from the last paragraph that $\overline{\zeta}^{w'} = \overline{\zeta}^{w}$ for all $\zeta \in P$.

We consider the irreducible polynomial $f(Y) = \sum_{l=0}^{m} \psi_l(\underline{x'})Y^l$ of y over $K(\underline{x}) = K(\underline{x'})$ with the representation of the non-zero coefficients we have obtained above: $\psi_l(\underline{x'}) \in K[x_1, \ldots, x_t]_{(x_1,\ldots,x_t)}$. It then follows that the residue polynomial

$$\prod_{j=1}^{m}(Y - \overline{\sigma_j(y)}^{w'}) = \overline{f(Y)}^{w'} = \overline{f(Y)}^{w} = \prod_{j=1}^{m}(Y - \overline{\sigma_j(y)}^{w}) = (Y-1)Y^{m-1}$$

is not zero and has the simple root 1. Since $\overline{\sigma_1(y)}^{w'} = \overline{y}^{w'} = 1$, every conjugate of y different from y has a positive value with respect to w'. We used that the denominators of the non-zero coefficients of the irreducible polynomial $f(Y)$ over $K(\underline{x})$ are all units in $K[x_1, \ldots, x_t]_{(x_1,\ldots,x_t)}$. If we multiply f with the least common denominator, which is hence also a unit, and replace the elements x_j by indeterminates X_j, we get an irreducible polynomial $g \in K[X_1, \ldots, X_t, Y]$ such that $g(x_1, \ldots, x_t, y) = 0$ and $g(0, \ldots, 0, Y) = u(Y-1)Y^{m-1}$ for some $u \in K^{\times}$, hence $g(\overline{x_1}^{w}, \ldots \overline{x_t}^{w}, \overline{y}^{w}) = g(0, \ldots, 0, 1) = 0$ but $\frac{\partial}{\partial Y} g(\overline{x_1}^{w}, \ldots \overline{x_t}^{w}, \overline{y}^{w}) = \frac{\partial}{\partial Y} g(0, \ldots, 0, 1) \neq 0$. In particular, $(0, \ldots, 0, 1)$ is a non-singular K-rational point of the irreducible hypersurface $g = 0$, and its local ring $K[x_1, \ldots, x_t, y]_{(x_1,\ldots,x_t,y-1)}$ is a regular local ring (see Theorem 1.1.11).

Now fix $a \in M$. Above, we had the following representation of a: $x'^{\alpha(a)} b_a$, where $w(a) = w(x'^{\alpha(a)}) \geqslant 0$ and $b := b_a \in \mathcal{O}_w^{\times}$. Rewriting this in terms of $x_1, \ldots, x_t$, we get a new representation: $x^{\alpha'} \cdot b$, where $\alpha' \in \mathbb{N}^t$, since $x'^{\alpha(a)} \in S_M \subset S$. In view of Corollary 1.1.8, we need to show that w.r.t. w' the element b is again a unit and the residue class did not change.

Again, we have to distinguish two cases. In the case $b \in K(\underline{x'})$, it follows from $b \in P$ that $\overline{b}^{w'} = \overline{b}^{w}$. In the case $b \notin K(\underline{x'})$, for each $j \in \{0, \ldots, m-1\}$, we look at the irreducible polynomial

$$f_j(T) = \sum_{l=0}^{m_j} \psi_{jl}(\underline{x'})T^l = \prod_{k \in I_j}(T - \frac{e_j}{\sigma_k(b_j) - d_j})$$

of $\frac{e_j}{b_j - d_j}$ over $K(\underline{x'}) = K(\underline{x})$.

As above, since the coefficients of $f_j(T)$ lie in P, we have $\overline{f(Y)}^{w'} = \overline{f(Y)}^{w}$, and hence the residue polynomial is not zero and it has the simple root 1 in $\overline{K(\underline{x})}^{w'} = K$. Thus, in the henselization of $(K(\underline{x}), w')$, we find a root r of $f_j(T)$ such that $\overline{r}^{w'} = 1$ is a simple root of $\overline{f(Y)}^{w'}$. But this just means that one of the conjugates of $\frac{e_j}{b_j - d_j}$ lies in the henselization of $(K(\underline{x}), w')$ and has residue class 1. Since $d_j, e_j \in P$, we have that $\overline{d_j}^{w'} = \overline{d_j}^{w} = \overline{b_j}^{w} = \overline{b}^{w}(\overline{y}^{w})^j = \overline{b}^{w} \neq 0$ and $\overline{e_j}^{w'} = \overline{e_j}^{w} = 0$. In particular, $w'(d_j) = 0$ and $w'(e_j) > 0$. Let $k(j) \in I_j$ be such that $w'(\frac{\sigma_{k(j)}(b_j) - d_j}{e_j} - 1) > 0$. Then $w'(\sigma_{k(j)}(b_j) - d_j) = w'(e_j) > 0$, and thus $w'(\sigma_{k(j)}(b_j)) = 0$ and the residue class of $\sigma_{k(j)}(b_j)$ w.r.t. w' is the same as the residue class of b w.r.t. w.

Since the w'-value of every conjugate of y different from y is positive, it follows that, for fixed $k > 1$, at most one of the elements $\sigma_k(b_j) = \sigma_k(y)^j b(\underline{x}', \sigma_k(y))$ $(0 \leqslant j \leqslant m-1)$ can be a unit in $\mathcal{O}_{w'}$, hence it follows from $k(j_1) = k(j_2)$ that $j_1 = j_2$. Therefore $\{k(0), \ldots, k(m-1)\} = \{1, \ldots, m\}$, hence there exists some $j^* \in \{0, \ldots, m-1\}$ such that $k(j^*) = 1$. Thus $y^{j^*} b = b_{j^*} = \sigma_{k(j^*)}(b_{j^*})$ is a unit in $\mathcal{O}_{w'}$ with $\overline{y^{j^*} b}^{w'} = \overline{b}^{w}$. Since y has w'-residue class 1, we have that $w'(b) = 0$ and that $\overline{b}^{w'} = \overline{b}^{w}$. Altogether, we have shown that $b = b_a$ is a unit in the regular local ring $K[x_1, \ldots, x_t, y]_{(x_1, \ldots, x_t, y-1)}$ (by Corollary 1.1.8).

q.e.d.

1.2.5 **Remark:**

Assume that F is a function field of degree 1 over a field K of characteristic 0. Let w be an Abhyankar valuation of F/K with residue field K, i.e., w is a prime divisor of F/K. In particular, it is a discrete rank-1-valuation of F. Let $x_1' \in \mathcal{O}_w$ such that $w(x_1')$ generates the value group $\mathbb{Z}$ of w, i.e., $w(x_1') = 1$. By the last Lemma, we find elements $x_1, y \in \mathcal{O}_w$ such that $F = K(x_1, y)$, and such that $g(\overline{x_1}, \overline{y}) = 0$ but $\frac{\partial}{\partial Y} g(\overline{x_1}, \overline{y}) \neq 0$ holds for an irreducible polynomial $g(X, Y) \in K[X, Y]$ of x_1, y over K, and such that $w(x_1)$ generates the value group of w and x_1 lies in the group G generated by x_1' in $F^\times$. From this it follows that $x_1 = x_1'$, and hence we have the statement of part 2 of Theorem 1.2.1.

1.3 Abhyankar Valuations of Arbitrary Rank

We will now give a generalization of Lemma 1.2.4 for Abyhankar valuations of arbitrary rank.

1.3.1 **Theorem:**

Let K be a field of characteristic 0, and let F be a function field of degree $n \geqslant 1$ over K. Let v be a non-trivial Abhankar valuation of F/K having rank m and rational rank r. Let M be a finite subset of $\mathcal{O}_v \backslash \{0\}$. Then there exist a finite extension $\tilde{F}$ of F, elements $x_1, \ldots, x_n \in F$, algebraically independent over K, elements $y_1, \ldots, y_{m+1} \in \tilde{F}$, algebraic over $K(x_1, \ldots, x_n)$, and a valuation w on $\tilde{F}$ such that

a) $\tilde{F} = K(x_1, \ldots, x_n, y_1, \ldots, y_{m+1})$,

b) w is an immediate extension of v,

c) $w(x_1), \ldots, w(x_r)$ generate the value group of w,

d) $\overline{F}^v = K(x_{r+1}, \ldots, x_n, y_{m+1}) =: \tilde{K} \subset \tilde{F}$,

e) $x_1, \ldots, x_r, y_1 - 1, \ldots, y_m - 1 \in \mathfrak{m}_w$,

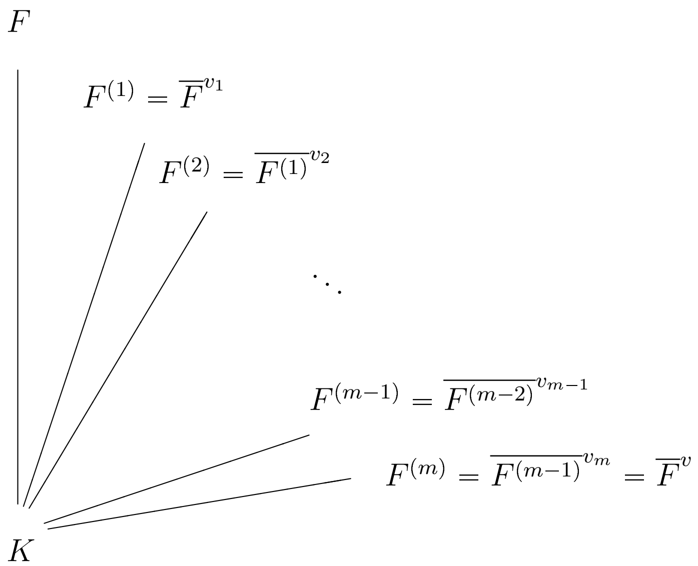
f) for all $j \in \{1, \ldots, m\}$, there exists an irreducible polynomial $g_j \in \tilde{K}[X_1, \ldots, X_r, Y_j, \ldots, Y_m]$ of Y_j-degree s_j such that $g_j(x_1, \ldots, x_r, y_j, \ldots, y_m) = 0$, $g_j(x_1, \ldots, x_r, Y_j, y_{j+1}, \ldots, y_m)$ is irreducible in $\tilde{K}(x_1, \ldots, x_r, y_{j+1}, \ldots, y_m)[Y_j]$ and $g(0, \ldots, 0, Y_j, 1, \ldots, 1) = u_j(Y_j - 1)Y_j^{s_j}$ for some $u_j \in \tilde{K}^\times$, hence $g_j(0, \ldots, 0, 1 \ldots, 1) = 0$ but $\frac{\partial}{\partial Y_j} g_j(0, \ldots, 0, 1, \ldots, 1) \neq 0$, and

g) each element a of M is a product of a unit b_a and a monomial in $x_1, \ldots, x_r$ where the latter are the generators of the maximal ideal in the regular local ring which is the localization of the ring $\tilde{K}[x_1, \ldots, x_r, y_1, \ldots, y_m]$ at the maximal ideal $(x_1, \ldots, x_r, y_1 - 1, \ldots, y_m - 1)$. In particular, for all valuations w' of $\tilde{F}/\tilde{K}$ such that $(\overline{x_1}^{w'}, \ldots, \overline{x_r}^{w'}, \overline{y_1}^{w'}, \ldots \overline{y_m}^{w'}) = (0, \ldots, 0, 1, \ldots, 1)$, we have $b_a \in \mathcal{O}_{w'}^\times$ and $\overline{b_a}^{w'} = \overline{b_a}^{w}$ for all $a \in M$.

The idea of the proof is to split the Abhyankar valuation into valuations of rank 1, embed their residue fields into a finite extension of the function field and then use a modified version of the proof of Lemma 1.2.4 for each of these valuations.

Proof:

By Lemma 1.1.67, we can write v as the composition of m valuations $v_1, \ldots, v_m$, where v_1 is an Abhyankar valuation with rank 1 of F/K, and, for all $j \in \{2, \ldots, m\}$, v_j is an Abhyankar valuation with rank 1 of the residue field of v_{j-1} over K. Let $F^{(1)}, \ldots, F^{(m)} = \overline{F}^v = \tilde{K}$ be the sequence of their residue fields.



Let

- $x'_1, \ldots, x'_{r_1} \in \mathcal{O}_{v_1}$ such that $\mathbb{Z}v_1(x'_1) \oplus \cdots \oplus \mathbb{Z}v_1(x'_{r_1}) = \Gamma_{v_1}$,
- $x'_{r_1+1}, \ldots, x'_{r_2} \in \mathcal{O}_{v_1}^\times$ such that $\mathbb{Z}v_2(\overline{x'_{r_1+1}}^{v_1}) \oplus \cdots \oplus \mathbb{Z}v_2(\overline{x'_{r_2}}^{v_1}) = \Gamma_{v_2}$,
- $x'_{r_2+1}, \ldots, x'_{r_3} \in \mathcal{O}_{v_1}^\times$ such that $\mathbb{Z}v_3(\overline{x'_{r_2+1}}^{v_1 \circ v_2}) \oplus \cdots \oplus \mathbb{Z}v_3(\overline{x'_{r_2}}^{v_1 \circ v_2}) = \Gamma_{v_3}$,
- etc.

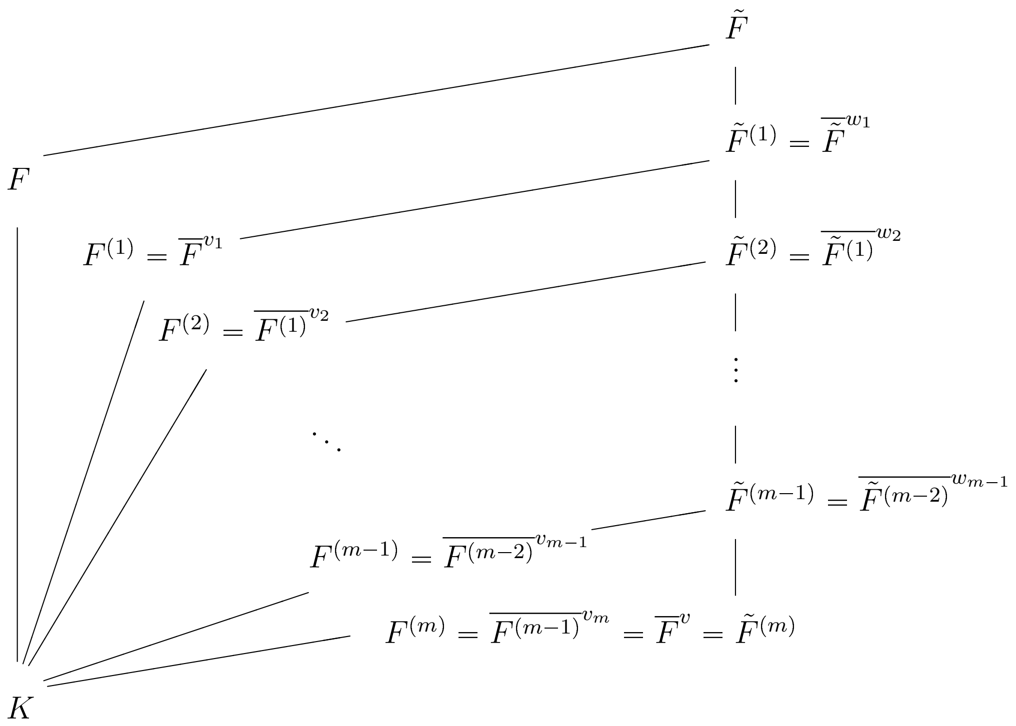
Then, by Remark 1.1.35, we have $\Gamma_v = \Gamma_{v_1} \times \cdots \times \Gamma_{v_m}$ with the lexicographical ordering of the product.

Note that $0 =: r_0 < r_1 < \cdots < r_m = r$. Further, let $x_{r+1}, \ldots, x_n \in F$ be such that $\overline{x_{r+1}}^v, \ldots, \overline{x_n}^v$ are algebraically independent over K (v is an Abhyankar valuation of F/K, hence $\operatorname{trdeg}(\overline{F}^v/K) = n - r$).

Since $F^{(m)}$ is the residue field of $F^{(m-1)}$ with respect to v_m, it can be embedded in the henselization of $(F^{(m-1)}, v_m)$ in such a way that the residue classes of $x_{r+1}, \ldots, x_n$ with respect to the composition of $v_1, \ldots, v_{m-1}$ are identified with $\overline{x_{r+1}}^v, \ldots, \overline{x_n}^v$, since these are algebraically independent over K (see Remark 1.1.43 and Lemma 1.1.57). Then we can take the compositum $\tilde{F}^{(m-1)}$ of $F^{(m-1)}$ and $F^{(m)}$ in this henselization. Set $w_m := v_m$.

Since $\tilde{F}^{(m-1)}$ is a finite extension of $F^{(m-1)}$, which in turn is the residue field of $F^{(m-2)}$ with respect to v_{m-1}, Theorem 1.1.47 tells us that there exists a finite extension $(F'^{(m-2)}, w_{m-1})$ of $(F^{(m-2)}, v_{m-1})$ such that w_{m-1} has the same value group as v_{m-1} and residue field $\tilde{F}^{(m-1)}$. In the henselization of $(F'^{(m-2)}, w_{m-1})$, we can embed $\tilde{F}^{(m-1)}$ in such a way that the residue classes of $x_{r_{m-1}+1}, \ldots, x_n$ with respect to the composition of $v_1, \ldots, v_{m-2}$ are identified with the residue classes of $x_{r_{m-1}+1}, \ldots, x_n$ with respect to the composition of $v_1, \ldots, v_{m-1}$. Let $\tilde{F}^{(m-2)}$ be the compositum of $F'^{(m-2)}$ and $\tilde{F}^{(m-1)}$ in the henselization.

If we iterate this process we get a chain $(\tilde{F} := \tilde{F}^{(0)}, w_1) \supset (\tilde{F}^{(1)}, w_2) \supset \cdots \supset (\tilde{F}^{(m-1)}, w_m)$ of valued fields



such that

(i) $\tilde{F}^{(j)}$ is a finite extension of $F^{(j)}$ for all $j < m$,

(ii) w_j is an Abhyankar valuation of rank 1 extending v_j with value group

$$\begin{aligned}\Gamma_{v_j} &= \mathbb{Z}v_j(\overline{x'_{r_{j-1}+1}}^{v_1\circ\cdots\circ v_{j-1}}) \oplus\cdots\oplus \mathbb{Z}v_j(\overline{x'_{r_j}}^{v_1\circ\cdots\circ v_{j-1}}) \\ &= \mathbb{Z}w_j(x'_{r_{j-1}+1}) \oplus\cdots\oplus \mathbb{Z}w_j(x'_{r_j})\end{aligned}$$

because of the identifications made above, and w_j has residue field $\tilde{F}^{(j)}$ if $j < m$ and $\tilde{F}^{(m)} := \overline{F}^v$ if $j = m$.

Let w be the composition of $w_1, \ldots, w_m$. By Remark 1.1.35,

$$\Gamma_w = \Gamma_{w_1} \times\cdots\times \Gamma_{w_m} = \Gamma_{v_1} \times\cdots\times \Gamma_{v_m} = \Gamma_v$$

with the lexicographical ordering on the product. Hence, the values of the elements $x'_1, \ldots, x'_r \in F$ generate the value group of w.

For all $j \in \{1, \ldots, m-1\}$, we have $\mathcal{O}_w \cap \tilde{F}^{(j)} = \mathcal{O}_{w_{j+1}}$: Let $0 \neq c \in \tilde{F}^{(j)}$. Then $w_1(c) = \cdots = w_j(c) = 0$. Since the ordering on the product of the value groups of $w_1, \ldots, w_m$ is lexicographical, it follows that $w(c)$ is non-negative if and only if $w_{j+1}(c)$ is non-negative.

Let $c \in \mathcal{O}_w$ and $j \in \{1, \ldots, m-1\}$. Then $d := \overline{c}^{w_1\circ\cdots\circ w_j} \in \mathcal{O}_{w_{j+1}}$: We have $w_1 \circ\cdots\circ w_j(c-d) > 0$, and hence $w(c-d) > 0$. Since $w(c) \geqslant 0$, we therefore have $w(d) \geqslant 0$, too. Hence $d \in \mathcal{O}_w \cap \tilde{F}^{(j)} = \mathcal{O}_{w_{j+1}}$.

For all $j \in \{1, \ldots, m\}$, the elements $x'_{r_{j-1}+1}, \ldots, x'_{r_j} \in$ are algebraically independent over $\tilde{F}^{(j)}$, and there exists some $z_j \in \tilde{F}^{(j-1)} \cap \mathcal{O}_{w_j}$, algebraic over $\tilde{F}^{(j)}(x'_{r_{j-1}+1}, \ldots, x'_{r_j})$, such that $\tilde{F}^{(j-1)} = \tilde{F}^{(j)}(x'_{r_{j-1}+1}, \ldots, x'_{r_j}, z_j)$. Let $\tilde{K} := \tilde{F}^{(m)} = \overline{F}^v$. Since v is an Abhyankar valuation of F/K, $\tilde{K}$ is finitely generated over K (see Proposition 1.1.66), and therefore there exists an element $y_{m+1} \in \tilde{K}$ such that $\tilde{K} = K(x_{r+1}, \ldots, x_n, y_{m+1})$.

Let $z_1 = \sigma_1(z_1), \sigma_2(z_1), \ldots, \sigma_{s_1}(z_1)$ be the pairwise different conjugates of z_1 over $\tilde{F}^{(1)}(x'_1, \ldots, x'_{r_1})$, where $\mathrm{id} = \sigma_1, \ldots, \sigma_{s_1} \in \mathrm{Aut}(\tilde{F}^{(1)}(\underline{x'})^{\mathrm{alg}}, \tilde{F}^{(1)}(\underline{x'}))$. Since w_1 is a valuation of rank 1, we find, as shown in the proof of Lemma 1.2.4, some $d, e \in \tilde{F}^{(1)}(\underline{x'})$ such that

$$\begin{aligned} w_1(z_1 - d) &> w_1(\sigma_k(z_1) - d) \text{ for all } k > 1, \\ w_1(z_1 - d) &> 0, \text{ and} \\ w_1(\frac{e}{z_1 - d} - 1) &> 0. \end{aligned}$$

Set $y_1 := \frac{e}{z_1 - d}$, and let

$$f_1(Y_1) = \sum_{l=0}^{s_1} \psi_l(\underline{x'}) Y_1^l = \prod_{k=1}^{s_1} (Y_1 - \sigma_k(y_1))$$

be the irreducible polynomial of y_1 over $\tilde{F}^{(1)}(x'_1, \ldots, x'_{r_1})$. Since all conjugates of y_1 lie in $\mathcal{O}_w \subset \mathcal{O}_{w_1}$, the coefficients $\psi_0, \ldots, \psi_{s_1}$ of f also lie in $\mathcal{O}_w$. For all $l \in \{0, \ldots, s_1\}$, if $\psi_l \neq 0$, we can write $\psi_l = x'^{\mu(\psi_l)} \varphi_l$ with $\mu(\psi_l) \in \mathbb{Z}^r$ and

$\varphi_l \in \mathcal{O}_w^\times$. Set $S_{f_1} := \{x'^{\mu(\psi_l)} \mid l \in \{0,\ldots,s_1\},\ \psi_l \neq 0\}$ and $\Phi_1 := \{\varphi_l \mid l \in \{0,\ldots,s_1\},\ \psi_l \neq 0\}$.
We have $\tilde{F} = \tilde{F}^{(1)}(x'_1,\ldots,x'_{r_1},z_1) = \tilde{F}^{(1)}(x'_1,\ldots,x'_{r_1},y_1)$.

Let $a \in M$. Since $\Gamma_w = \mathbb{Z}w(x'_1) \oplus \cdots \oplus \mathbb{Z}w(x'_r)$, we can write $a = x'^{\mu(a)}b_a$, where $b := b_a \in \mathcal{O}_w^\times \subset \mathcal{O}_{w_1}^\times$. Set $S_M := \{x'^{\mu(a)} \mid a \in M\}$. Suppose $b \notin \tilde{F}^{(1)}(\underline{x'})$. Set $b^{(l)} := y_1^l b$ for $l = 0,\ldots,s_1-1$. The $1 \leqslant s^{(l)} < s_1$ pairwise different conjugates of $b^{(l)}$ are contained in the set $\{\sigma_1(b^{(l)}),\ldots,\sigma_{s_1}(b^{(l)})\}$. Let $I^{(l)} \subset \{1,\ldots,s_1\}$ be a set of $s^{(l)}$ indices such that $1 \in I^{(l)}$ and $\sigma_k(b^{(l)}) \neq \sigma_{k'}(b^{(l)})$ for all $k \neq k' \in I^{(l)}$. As before, we can find for all $l \in \{0,\ldots,s_1-1\}$ some elements $d^{(l)}, e^{(l)} \in \tilde{F}^{(1)}(\underline{x'}) \cap \mathcal{O}_{w_1}$ such that

$$\begin{aligned} w_1(b^{(l)} - d^{(l)}) > w_1(\sigma_k(b^{(l)}) - d^{(l)}) \text{ for all } k \in I^{(l)}\backslash\{1\},\\ w_1(b^{(l)} - d^{(l)}) > 0, \text{ and}\\ w_1(\frac{e^{(l)}}{b^{(l)} - d^{(l)}} - 1) > 0. \end{aligned}$$

Since $b^{(l)} \in \mathcal{O}_w^\times$, it follows that $d^{(l)}$ also lies in $\mathcal{O}_w^\times$. Moreover, both elements must have the same residue class even with respect to w_1. It further follows that $w(e^{(l)}) > 0$. Let

$$f^{(l)}(T) = \sum_{t=0}^{s^{(l)}} \psi_t^{(l)} T^t = \prod_{k \in I^{(l)}} (T - \frac{e^{(l)}}{\sigma_k(b^{(l)}) - d^{(l)}})$$

be the irreducible polynomial of $\frac{e^{(l)}}{b^{(l)} - d^{(l)}}$ over $\tilde{F}^{(1)}(\underline{x'})$.
Set $\Psi^{(l)} := \{\psi_0^{(l)},\ldots,\psi_{s^{(l)}}^{(l)}\}\backslash\{0\} \subset \mathcal{O}_w \subset \mathcal{O}_{w_1}$.

Let P be a finite subset of $\tilde{F}^{(1)}(\underline{x'}) \cap \mathcal{O}_w \subset \tilde{F}^{(1)}(\underline{x'}) \cap \mathcal{O}_{w_1}$ containing Φ_1 as a subset and, for all $a \in M$, the corresponding element b if it lies in $\tilde{F}^{(1)}(\underline{x'})$, and otherwise, for all $l \in \{0,\ldots,s_1-1\}$, the set $\Psi^{(l)}$ and the elements $d^{(l)}, e^{(l)}$. Let $\zeta \in P$. As in the proof of Lemma 1.2.4, we get a representation

$$\zeta = \frac{\frac{\zeta'}{x'^{\alpha''}}}{\frac{\zeta''}{x'^{\alpha''}}} = \frac{\sum_{\alpha \in \mathbb{N}^{r_1}} u_\alpha \frac{x'^\alpha}{x'^{\alpha''}}}{\sum_{\alpha \in \mathbb{N}^{r_1}} v_\alpha \frac{x'^\alpha}{x'^{\alpha''}}} =: \frac{\eta'}{\eta''},$$

where η' lies in $\mathcal{O}_{w_1}$ and η'' lies in $\mathcal{O}_{w_1}^\times$.

Suppose we have such a representation for all the elements in P. Then let S_P be the set of all products x'^α ($\alpha \in \mathbb{Z}^{r_1}$) occuring in the numerator or denominator of any such represention. Now we apply Lemma 1.2.3 to the finite set $S := S_{f_1} \cup S_M \cup S_P$ and the subgroup $G \subset F$ of $\tilde{F}^{(1)}(x'_1,\ldots,x'_{r_1})^\times$ generated by $x'_1,\ldots,x'_{r_1}$ and equipped with the ordering induced by the ordering on the value group. We get positive generators $x_1^*,\ldots,x_{r_1}^* \in F$ of G such that all elements of S are monomials in those new generators. In particular, for all elements ζ in P, we get a representation $\zeta = \frac{\xi'(\underline{x^*})}{\xi''(\underline{x^*})}$ with $\xi'(\underline{x^*}) \in \tilde{F}^{(1)}[\underline{x^*}] \cap \mathcal{O}_{w_1}$ and $\xi''(\underline{x^*}) \in \tilde{F}^{(1)}[\underline{x^*}] \cap \mathcal{O}_{w_1}^\times$. Thus, the residue class of ζ with respect to w_1 is $\frac{\xi'(0)}{\xi''(0)}$, which lies in $\mathcal{O}_{w_2}$, since $\zeta \in \mathcal{O}_w$.

Expand the fraction $\frac{\xi'(x_1^*,\ldots,x_{r_1}^*)}{\xi''(x_1^*,\ldots,x_{r_1}^*)}$ with some product ${x'_{r_1+1}}^{\delta_{r_1+1}}\cdots {x'_r}^{\delta_r}$ with $\delta_{r_1+1},\ldots,\ \delta_r \in \mathbb{Z}$ such that $v_0^* := v_0 \cdot {x'_{r_1+1}}^{\delta_{r_1+1}}\cdots {x'_r}^{\delta_r} \in \mathcal{O}_w^\times$. Note that then $u_0^* := u_0 \cdot {x'_{r_1+1}}^{\delta_{r_1+1}}\cdots {x'_r}^{\delta_r}$ lies in $\mathcal{O}_w$. Now look at the other coefficients $u_\alpha^* := u_\alpha \cdot {x'_{r_1+1}}^{\delta_{r_1+1}}\cdots {x'_r}^{\delta_r}$ and $v_\alpha^* := v_\alpha \cdot {x'_{r_1+1}}^{\delta_{r_1+1}}\cdots {x'_r}^{\delta_r}$ $(\alpha \neq 0)$ occuring in this expanded fraction. Let $h \in \mathbb{N}$ such that $w((x'_{r_1+1})^{-h}) \leqslant \min\{w(u_\alpha^*), w(v_\alpha^*) \mid \alpha \neq 0\}$. Set $x_1 := \frac{x_1^*}{(x'_{r_1+1})^h}, \ldots, x_{r_1} := \frac{x_{r_1}^*}{(x'_{r_1+1})^h} \in \mathcal{O}_w$, and we get a new representation $\frac{\chi'(x_1,\ldots,x_{r_1})}{\chi''(x_1,\ldots,x_{r_1})}$ of ζ, where all coeffients of χ' and χ'' lie in $\mathcal{O}_w$: Let u be a coefficient corresponding to the monomial $(x^*)^\nu = (x'_{r_1+1})^{h|\nu|}x^\nu$ $(0 \neq \nu \in \mathbb{N}^{r_1})$. The new coefficient $u(x'_{r_1+1})^{h|\nu|}$ lies in $\mathcal{O}_w$.

Let M_1 be the subset of $\mathcal{O}_w \cap \tilde{F}^{(1)} \subset \mathcal{O}_{w_2}$ that consists of all coefficients occuring in the representation $\zeta = \frac{\chi'(\underline{x})}{\chi''(\underline{x})}$ of any $\zeta \in P$.

The elements $x_1, \ldots, x_{r_1}$ generate the value group of w_1. Therefore they are algebraically independent over $\tilde{F}^{(1)}$, and we further have that $\tilde{F}^{(1)}(\underline{x'}) = \tilde{F}^{(1)}(\underline{x})$. With Lemma 1.2.4, we can conclude by induction on the rank of w that we can find elements $x_{r_1+1}, \ldots, x_r \in \mathcal{O}_w \cap F$ such that

c') $w(x_{r_1+1}), \ldots, w(x_r)$ generate the value group of the restriction of w to $\tilde{F}^{(1)}$,

f') for all $j \in \{2, \ldots, m\}$, there exists an irreducible polynomial $g_j \in \tilde{K}[X_{r_{j-1}+1}, \ldots, X_r, Y_j, \ldots, Y_m]$ of Y_j-degree s_j such that $g_j(x_{r_{j-1}+1}, \ldots, x_r, y_j, \ldots, y_m) = 0$, $g_j(x_{r_{j-1}+1}, \ldots, x_r, Y_j, y_{j+1}, \ldots, y_m)$ is irreducible in $\tilde{K}(x_{r_{j-1}+1}, \ldots, x_r, y_{j+1}, \ldots, y_m)[Y_j]$ and $g(0, \ldots, 0, Y_j, 1, \ldots, 1) = u_j(Y_j - 1)Y_j^{s_j}$ for some $u_j \in \tilde{K}^\times$, hence $g_j(0, \ldots, 0, 1 \ldots, 1) = 0$ but $\frac{\partial}{\partial Y_j} g_j(0, \ldots, 0, 1, \ldots, 1) \neq 0$, and

g') for all $a_1 \in M_1$, we have that $a_1 = x_{r_1+1}^{\nu_{r_1+1}} \cdots x_r^{\nu_r} b_{a_1}$, where $\nu_{r_1+1}, \ldots, \nu_r \in \mathbb{N}$, $b_1 \in \mathcal{O}_w^\times \cap \tilde{F}^{(1)}$, and, for all valuations w' of $\tilde{F}^{(1)}/\tilde{K}$ such that $(0, \ldots, 0, 1, \ldots, 1) = (\overline{x_{r_1+1}}^{w'}, \ldots, \overline{x_r}^{w'}, \overline{y_2}^{w'}, \ldots \overline{y_m}^{w'})$, one has $b_{a_1} \in \mathcal{O}_{w'}^\times \cap \tilde{F}^{(1)}$ and $\overline{b_{a_1}}^{w'} = \overline{b_{a_1}}^{w}$, i.e., the element b_{a_1} is a unit in the localization of the ring $\tilde{K}[x_{r_1+1}, \ldots, x_r, y_2, \ldots, y_m]$ at the maximal ideal $(x_{r_1+1}, \ldots, x_r, y_2 - 1, \ldots, y_m - 1)$.

Let A be the localization of the ring $\tilde{K}[x_{r_1+1}, \ldots, x_r, y_2, \ldots, y_m]$ at the maximal ideal $(x_{r_1+1}, \ldots, x_r, y_2 - 1, \ldots, y_m - 1)$. Then A is a regular local ring.

Let w' be a valuation of $\tilde{F}/\tilde{K}$ such that $x_1, \ldots, x_r, y_1 - 1, \ldots, y_m - 1 \in \mathfrak{m}_{w'}$. Let $\zeta \in P$. We have a representation $\zeta = \frac{\chi'(x_1,\ldots,x_{r_1})}{\chi''(x_1,\ldots,x_{r_1})}$ with $\chi'(\underline{x}), \chi''(\underline{x})$ in $A[x_1, \ldots, x_{r_1}]$ and $\chi''(0) \in A^\times$. Considering w', the residue class of ζ is obviously equal to the residue class of $\frac{\chi'(0)}{\chi''(0)}$. And, since $\chi'(0), \chi''(0) \in M_1$ and $(0, \ldots, 0, 1, \ldots, 1) = (\overline{x_{r_1+1}}^{w'}, \ldots, \overline{x_r}^{w'}, \overline{y_2}^{w'}, \ldots \overline{y_m}^{w'})$, g') tells us that $\overline{\zeta}^{w'} = \overline{\zeta}^{w}$. Now we can go on as in the last part of the proof of Lemma 1.2.4 to show the remaining assertions.

The existence of g_1 as stated in f) follows from the representation of the nonzero coefficients of the irreducible polynomial f_1 of y_1 over $\tilde{F}^{(1)}(x_1, \ldots, x_{r_1})$

we gained above:

$$\psi_l = x'^{\mu(\psi_l)}\varphi_l = x^{\nu(l)}\frac{\chi_l'(x_1,\ldots,x_{r_1})}{\chi_l''(x_1,\ldots,x_{r_1})}$$

with $\nu(l) \in \mathbb{N}^{r_1}$, since $x'^{\mu(\psi_l)} \in S$, and $\chi_l', \chi_l'' \in A[x_1,\ldots,x_{r_1}]$ with $\chi_l'(0), \chi_l''(0) \in A^\times$. Therefore χ_l' and χ_l'' are units in the localization of the ring $\tilde{K}[x_1,\ldots,x_r, y_2,\ldots,y_m]$ at the maximal ideal $(x_1,\ldots,x_r,y_2-1,\ldots,y_m-1)$, hence so is φ_l. Thus, if we want to get g_1, we only have to multiply f_1 with the least common denominator of the elements φ_l in this local ring and replace x_i by X_i $(i=1,\ldots,r)$ and y_j by Y_j $(j=2,\ldots,m)$.

q.e.d.

1.3.2 **Example:**

We consider again the example from 1.1.46 and 1.1.68: v is an Abhyankar valuation of $\mathbb{R}(X_1,X_2,X_3,X_4,X_5)/\mathbb{R}$ having rank 2, value group $(\mathbb{Z}\oplus\mathbb{Z}2\pi)\times(\mathbb{Z}\oplus\mathbb{Z}\sqrt{2}) = (\mathbb{Z}v(\frac{X_5}{X_4})\oplus\mathbb{Z}v(X_5^2-X_4^3))\times(\mathbb{Z}v(X_2)\oplus\mathbb{Z}v(X_3^3-X_1))$ and residue field $\mathbb{R}(X_3)$. The valuation v is the composition of two rank-1-Abhyankar valuations v_1 and v_2 (as described in 1.1.68). Using the same notation as in Theorem 1.3.1 and its proof, we have $F=\mathbb{R}(X_1,\ldots,X_5)$, $K=\mathbb{R}$, $\overline{F}^v = \tilde{K} = \tilde{F}^{(2)} = \mathbb{R}(X_3)$, $\tilde{F}^{(1)} = \tilde{F}^{(2)}(X_2, X_3^3-X_1) = \mathbb{R}(X_1,X_2,X_3) = \overline{F}^{v_2}$, $\tilde{F} = \tilde{F}^{(1)}(\frac{X_5}{X_4}, X_5^2-X_4^3, X_4) = F$, $w_1=v_1$, $w_2=v_2$ and $w=v$.

Further, we have $x_1' = \frac{X_5}{X_4}$, $x_2' = X_5^2-X_4^3$, $x_3' = X_2$, $x_4' = X_3^3-X_1$ and $x_5 = X_3$. As y_2 and y_3, we can choose 1. As y_2, we may choose $\frac{X_4^3}{X_5^2}$, since the irreducible polynomial of this element over $\tilde{F}^1 = \mathbb{R}(X_1,\ldots,X_3)$ is $f_1(Y) = Y^3 - Y^2 + (\frac{X_5}{X_4})^6(X_5^2-X_4^3) \in \mathcal{O}_{v_1}[Y]$ which has with respect to v_1 the residue polynomial $(Y-1)Y^2$.

Let

$$\begin{aligned} g_1 &:= X_3^4X_5 + 5X_2^3X_4 - X_1X_3X_5 - 2X_1X_4,\\ g_2 &:= -X_1X_2^3 + 3X_3^2X_4 - X_2^3 + 2X_4X_5 + 7X_5,\\ g_3 &:= 3X_2X_4^5 - X_2^3X_4^3 + X_2^3X_5^2 + 7X_5^3,\\ g_4 &:= -X_3^5X_4^3 + X_3^5X_5^2 + X_1X_3^2X_4^3 - X_1X_3^2X_5^2 \text{ and}\\ g_5 &:= X_1X_2^2X_4 + X_3X_5. \end{aligned}$$

We have $v(g_1) = (2,0)$, $v(g_2) = (0,3)$, $v(g_3) = (2\pi,3)$, $v(g_4) = (2\pi,\sqrt{2})$ and $v(g_5) = (2,2)$.

Let $a_1 := \frac{g_1}{g_2}$, $a_2 = \frac{g_3}{g_4}$ and $a_3 = \frac{g_4}{g_5}$. Then $v(a_1) = (2,-3)$, $v(a_2) = (0, 3-\sqrt{2})$ and $v(a_3) = (2\pi-2, \sqrt{2}-2)$, hence $M := \{a_1,a_2,a_3\} \subset \mathcal{O}_v$.

We now write $g_1, \ldots, g_5$ in terms of $x_1', x_2', x_3', x_4', y_1$ and x_5:

$$a_1 = {x_1'}^2 {x_3'}^{-3} \frac{{x_3'}^3(x_1'x_4'x_5 + 5{x_3'}^3 + 2x_4' - 2x_5^3)y_1}{2{x_1'}^5 y_1^2 + (7{x_1'}^3 + 3{x_1'}^2 x_5^2)y_1 + (-1 + {x_4'}^3 - x_5^3){x_3'}^3},$$

$$a_2 = {x_3'}^3 {x_4'}^{-1}\Big[\frac{(3{x_1'}^{10}x_3' + 7{x_1'}^9 - 3{x_1'}^4 x_2' x_3')y_1^2 - 3{x_1'}^4 x_2' x_3' y_1}{x_2'{x_3'}^3 x_5^3} + \frac{-3{x_1'}^4 x_2' x_3' - 7{x_1'}^3 x_2' + x_2'{x_3'}^3}{x_2'{x_3'}^3 x_5^3}\Big] \text{ and}$$

$$a_3 = {x_1'}^{-2} x_2' {x_3'}^{-2} x_4' \frac{{x_3'}^2 x_5^2}{({x_3'}^2 x_5^3 - {x_3'}^2 x_4' + x_1' x_5)y_1}.$$

The fractions are units in $\mathcal{O}_v$, and we denote them by b_1, b_2 and b_3. For $i \in \{1,2,3\}$, the values of the numerator and the denominator of b_i are equal to the least value of the monomials in $x_1', \ldots, x_4'$ occuring in them. In this case, we can use Lemma 1.2.3 directly without first splitting the value group into groups of rank 1. Let G be the subgroup of $F^\times$ generated by $x_1', \ldots, x_4'$ and equipped with the ordering that is induced by the ordering of $\Gamma_v = \mathbb{Z}v(x_1') \oplus \cdots \oplus \mathbb{Z}v(x_4')$. First, for each $i \in \{1,2,3\}$, we devide the numerator and denominator of b_i with the monomial occuring in them which has the lowest value. Then we get:

$$b_1 = \frac{(x_1'x_4'x_5 + 5{x_3'}^3 + 2x_4' - 2x_5^3)y_1}{2{x_1'}^5 {x_3'}^{-3} y_1^2 + (7{x_1'}^3 {x_3'}^{-3} + 3{x_1'}^2 {x_3'}^{-3} x_5^2)y_1 + (-1 + {x_4'}^3 - x_5^3){x_3'}^3},$$

$$b_2 = \frac{(3{x_1'}^{10}{x_2'}^{-1}{x_3'}^{-2} + 7{x_1'}^9 {x_2'}^{-1}{x_3'}^{-3} - 3{x_1'}^4 {x_3'}^{-2})y_1^2 - 3{x_1'}^4 {x_3'}^{-2} y_1}{x_5^3} + \frac{-3{x_1'}^4 {x_3'}^{-2} - 7{x_1'}^3 {x_3'}^{-3} + 1}{x_5^3} \text{ and}$$

$$b_3 = \frac{x_5^2}{(x_5^3 - x_4' + x_1'{x_3'}^{-2}x_5)y_1}.$$

Then applying 1.2.3 to G and ${x_1'}^{-6}x_2', x_1'{x_3'}^{-2}, {x_1'}^7 {x_2'}^{-1}, {x_3'}^3 {x_4'}^{-1} \in \mathfrak{m}_v \cap G$ yields a new $\mathbb{Z}$-basis of G consisting of

$$x_1 = \frac{{x_1'}^7}{{x_3'}^2 x_2'}, x_2 = \frac{x_2'}{{x_1'}^6}, x_3 = \frac{x_3'}{x_4'} \text{ and } x_4 = x_4'.$$

We therefore have

$$x_1' = x_1x_2x_3^2x_4^2, x_2' = x_1^6x_2^7x_3^{12}x_4^{12}, x_3' = x_3x_4 \text{ and } x_4' = x_4.$$

Hence

$$a_1 = x_1^2x_2^2x_3x_4 \frac{(x_1x_2x_3^2x_4^3x_5 + 5x_3^3x_4^3 + 2x_4 - 2x_5)y_1}{2x_1^5x_2^5x_3^7x_4^7y_1^2 + (7x_1^3x_2^3x_3^3x_4^3 + 3x_1^2x_2^2x_3x_4x_5^2)y_1 + (-1 + x_4^3 - x_5^3)},$$

$$a_2 = x_3^3x_4^2\Big[\frac{(3x_1^4x_2^3x_3^6x_4^6 + 7x_1^3x_2^2x_3^3x_4^3 - 3x_1^4x_2^4x_3^6x_4^6)y_1^2 - 3x_1^4x_2^4x_3^6x_4^6y_1}{x_5^3} + \frac{-3x_1^4x_2^4x_3^6x_4^6 - 7x_1^3x_2^3x_3^3x_4^3 + 1}{x_5^3}\Big] \text{ and}$$

$$a_3 = x_1^4x_2^5x_3^6x_4^7 \frac{x_5^2}{(x_5^3 - x_4 + x_1x_2x_5)y_1}.$$

The irreducible polynomial f_1 of y_1 has now the form

$$f_1(Y) = Y^3 - Y^2 + x_2.$$

We have then shown for this example the statement of Theorem 1.3.1.

Chapter 2

On the Transformation of Arbitrary into Abhyankar Valuations

In this chapter, we show how to transform an arbitrary non-trivial valuation of a function field over a field of characteristic zero into an Abhyankar valuation and thereby preserve finitely many properties. From this result, we deduce the denseness of the Abhyankar valuation in a refinement of the Zariski patch topology of the Zariski space. As an application, we give a new proof of a local-global principle for weak isotropy of quadratic forms over function field over $\mathbb{R}$.

2.1 Preliminaries

In the following, we give short introductions to the theory of real fields and the theory of quadratic forms, followed by an overview of some local-global principles for quadratic forms. At the end, we take a look at the model theoretic tools that we need in the main part of this chapter, mainly the Ax-Kochen-Ershov Principle.

2.1.1 Real Fields

In the following, we will consider ordered fields, extensions of ordered fields and valuations compatible with a field ordering. All definitions and results can be found in [20].

2.1.1 **Definition:**

A linear ordering $\leqslant$ of a field K is called a **(field) ordering of** K iff, for all $a, b, c \in K$, if $a \leqslant b$ then $a + c \leqslant b + c$, and if $0 \leqslant a$ and $0 \leqslant b$ then $0 \leqslant ab$. A pair $(K, \leqslant)$, where K is a field and $\leqslant$ is an ordering of K, is called an **ordered field**.

A field K is called **real** iff there exists an ordering of K.

An ordered field $(K, \leqslant)$ is called **archimedean** iff, for all $a \in K$, there exists some $n \in \mathbb{N}$ such that $a \leqslant n$.

From the definitions, it follows immediately that every ordered field has characteristic zero, and that $\mathbb{Q}$ is dense in every archimedean ordered field. Moreover, the following can be shown.

2.1.2 **Theorem:**

Every archimedean ordered field can be order-preserving embedded into $\mathbb{R}$.

2.1.3 **Example:**

We consider the rational function field $\mathbb{R}(X)$ in one indeterminate over $\mathbb{R}$. The orderings of this field are as follows:

a) There exists exactly one ordering $\leqslant$ such that $X < \mathbb{R}$.
b) There exists exactly one ordering $\leqslant$ such that $\mathbb{R} < X$.
c) For every $a \in \mathbb{R}$, there exists exactly one ordering $\leqslant$ such that $0 < X - a < \mathbb{R}_{\geqslant 0}$.
d) For every $a \in \mathbb{R}$, there exists exactly one ordering $\leqslant$ such that $0 < a - X < \mathbb{R}_{\geqslant 0}$.

All of them are non-archimedean.

Let K be a field. We write K^2 for the set of squares in K and $\sum K^2$ for the set of finite sums of squares in K. The following important characterization of real fields was proven by Artin and Schreier.

2.1.4 **Theorem:**

Let K be a field. Then K is real if and only if $-1 \notin \sum K^2$.

As a consequence, an algebraically closed field can never be real field.

Let $(K, \leqslant)$ be an ordered field, and let $P_\leqslant$ be the set of all non-negative elements of K with respect to $\leqslant$. Then, for all $a, b \in K$, we have $a \leqslant b$ if and only if $b - a \in P_\leqslant$.

By virtue of the definition of an ordering, it follows that $P_\leqslant$ is closed under addition and multiplication. It does not contain -1, but it contains every square of K and every element of K or its additive inverse. Conversely, every subset of K with these properties defines an ordering of K.

2.1.5 **Definition:**

Let K be a field. A subset P of K such that

$$P + P \subset P, \; P \cdot P \subset P, \; -1 \notin P \text{ and } P \cup -P = K$$

is called a **positive cone of** K**.**

If P is a positive cone of K, then $K^2 \subset K$. This follows from the conditions $P \cup -P = K$ and $P \cdot P \subset P$.

2.1.6 **Lemma:**

Let K be a field.

a) For each ordering $\leqslant$ of K, the set $P_{\leqslant}$ is a positive cone of K.
b) For each positive cone of K, the relation $\leqslant_P$, defined by $a \leqslant_P b :\iff b - a \in P$ for $a, b \in K$, is an ordering of K.

From now on, we will use the notion *ordering* for both the ordering of a field and its positive cone.

2.1.7 **Definition:**

Let K be a field. We denote by $\mathrm{X}(K)$ the set of all orderings of K.
For each ordering P of K, we let $\mathrm{sign}_P\colon K^\times \to \{-1, 1\}$ be the map that is defined by $\mathrm{sign}_P(a) = 1 :\iff a \in P$ for $a \in K$.

Let L/K be an extension of fields, and let P be an ordering of L. Then $P \cap K$ is an ordering of K. As opposed to valuations, orderings are not always extendable to an arbitrary field extension. We will give some examples where extensions are possible.

2.1.8 **Theorem:**

Let K be a field, and let $L = K(\sqrt{a})$ for some $a \in K \backslash K^2$. Then an ordering P of K extends to L if and only if $a \in P$.

2.1.9 **Theorem:**

Let K be a field, and let L be a finite extension of K such that $[L : K]$ is odd. Then every ordering of K extends to L.

2.1.10 **Theorem:**

Let K be a field, and let $L = K(X)$ be the rational function field in one variable. Then every ordering of K extends to L.

2.1.11 **Definition:**

A real field is called **real closed** iff it has no proper real, algebraic extension.

The following characterization of real closed fields is due to Artin and Schreier.

2.1.12 **Theorem:**

Let K be a field. Then the following statements are equivalent:

(i) K is real closed.
(ii) K has a unique ordering $\leqslant$ and $(K, \leqslant)$ cannot be extended to any proper algebraic extension.
(iii) K^2 is an ordering of K and every polynomial $f \in K[X]$ of odd degree has a root in K.
(iv) $K \neq K(\sqrt{-1})$ and $K(\sqrt{-1})$ is algebraically closed.

2.1.13 **Definition:**

Let $(K, \leqslant)$ be an ordered field. An extension $(L, \leqslant)$ of $(K, \leqslant)$ is called a **real closure of** $(K, \leqslant)$ iff L is real closed and L/K is algebraic.

2.1.14 **Theorem:** (Artin, Schreier)

Every ordered field $(K, \leqslant)$ has (up to order-preserving K-isomorphisms) a unique real closure.

In the following, we consider valuations whose valuation ring is convex with respect to some field ordering.

2.1.15 **Definition:**

Let $(K, \leqslant)$ be an ordered field.

We call a subset M of K **convex with respect to** $\leqslant$ iff, for all $a, b \in M$ and all $c \in K$, $a \leqslant c \leqslant b$ always implies $c \in M$.

A valuation v of K is said to be **compatible with** $\leqslant$ iff its valuation ring $\mathcal{O}_v$ is convex with respect to $\leqslant$.

A valuation v of K is called **real** iff it has a real residue field.

2.1.16 **Example:**

Let $(K, \leqslant)$ be an ordered field, and let A be a subring of K. We call

$$\mathcal{O}_A(\leqslant) := \{b \in K \mid -a \leqslant b \leqslant a \text{ for some } a \in A \cap P_{\leqslant}\}$$

the **convex hull of** A **in** $(K, \leqslant)$. $\mathcal{O}_A(\leqslant)$ is a valuation ring of K that is convex with respect to $\leqslant$.

The convexity of a valuation ring can be characterized as follows.

2.1.17 **Proposition:**

Let $(K, \leqslant)$ be an ordered field, and let v be a valuation of K. Then the following statements are equivalent:

(i) v is compatible with $\leqslant$.

(ii) $\mathfrak{m}_v$ is convex with respect to $\leqslant$.

(iii) $\overline{P_{\leqslant}}^v := \{\overline{a}^v \mid a \in \mathcal{O}_v \cap P_{\leqslant}\}$ is an ordering of $\overline{K}^v$.

(iv) $1 + \mathfrak{m}_v \subset P_{\leqslant}$.

The next theorem tells us that the orderings of a valued field (K, v) with which v is compatible can be completely described by the group $\Gamma_v / 2\Gamma_v$ and the orderings of the residue field $\overline{K}^v$.

2.1.18 **Theorem:** (Baer-Krull Representation Theorem)

Let (K, v) be a valued field, and let $\{\pi_i \mid i \in I\} \subset K$ be such that $\{v(\pi_i) + 2\Gamma_v \mid i \in I\}$ is an $\mathbb{F}_2$-basis of $\Gamma_v/2\Gamma_v$ so in particular, every non-zero element of K can be written as $\prod_{i \in I} \pi^{\varepsilon_i} c^2 u$ with $\varepsilon \in \{0,1\}^I$, $c \in K$ and $u \in \mathcal{O}_v^\times$. Then the map

$$\{P \subset K \mid P \in \mathrm{X}(K),\ v \text{ is compatible with } P\} \to \{-1,1\}^I \times \mathrm{X}(\overline{K}^v)$$

defined by

$$P \mapsto \left(\eta_P, \overline{P}^v\right)$$

is bijective with inverse map

$$(\eta, Q) \mapsto P(\eta, Q),$$

where $\eta_P \colon I \to \{-1,1\}$, $i \mapsto \mathrm{sign}_P(\pi_i)$ and $P(\eta, Q) := \{a \in K^\times \mid a = \prod_{i \in I} \pi^{\varepsilon_i} c^2 u$ where $\varepsilon \in \{0,1\}^I,\ c \in K,\ u \in \mathcal{O}_v^\times$ such that $\prod_{i \in I} \eta(i)^{\varepsilon_i} \overline{u}^v \in Q\}$.

2.1.19 **Corollary:**

A field K has a non-archimedean ordering if and only if there is a non-trivial real valuation of K.

We conclude this section with a consideration of the case of a real closed field.

2.1.20 **Theorem:**

Let $(K, \leqslant)$ be an ordered field, and let v be a valuation of K which is compatible with $\leqslant$. Then K is real closed if and only if

- $\overline{K}^v$ is real closed,
- Γ_v is divisible and
- (K, v) is henselian.

2.1.2 Quadratic Forms

We will now deal with the theory of quadratic forms. Therefore, in this section, we fix a field K of characteristic unequal to 2. [20] and [7] are the sources for the definitions and results of this section.

2.1.21 **Definition:**

Let $n \in \mathbb{N}$. A **quadratic form over** K **of dimension** n is a homogeneous polynomial of degree 2 in n indeterminates.

Let $n \in \mathbb{N}$, and let f be a quadratic form of dimension n. Then

$$f(X_1, \ldots, X_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} b_{ij} X_i X_j = \sum_{i=1}^{n} \sum_{j=1}^{n} \underbrace{\frac{1}{2}(b_{ij} + b_{ji})}_{a_{ij}} X_i X_j$$

with $b_{ij} \in K$ $(i, j \in \{1, \ldots, n\})$. Set $M_f := (a_{ij})_{1 \leqslant i,j \leqslant n}$. This is a symmetric $n \times n$-matrix over K, and we have that $f(x) = x^T M_f x$ for all $x \in K^n$.

2.1.22 **Definition:**

Two quadratic forms f, g over K are called **isometric** ($f \simeq g$) iff $\dim f = \dim g$ and $M_g = P^T M_f P$ for some invertible $n \times n$-matrix P over K.

2.1.23 **Definition:**

For $a_1, \ldots, a_n \in K$, we write $\langle a_1, \ldots, a_n \rangle$ for the quadratic form $a_1 X_1^2 + \cdots + a_n X_n^2$, and call this a **diagonal form**.

2.1.24 **Proposition:**

The following holds:

a) $\langle a, -a \rangle \simeq \langle 1, -1 \rangle$ for all $a \in K^\times$.
b) $\langle a, b \rangle \simeq \langle a+b, (a+b)ab \rangle$ for all $a, b \in K$ such that $a + b \neq 0$.
c) $\langle a_1, \ldots, a_n \rangle \simeq \langle a_1 b_1^2, \ldots, a_n b_n^2 \rangle$ for all $a_1, \ldots, a_n \in K$ and all $b_1, \ldots, b_n \in K^\times$.

Every quadratic form is diagonalizable.

2.1.25 **Theorem:**

Let f be a quadratic form over K of dimension n. Then there exist $a_1, \ldots, a_n \in K$ such that $f \simeq \langle a_1, \ldots, a_n \rangle$.

2.1.26 **Definition:**

Let $f = \sum_{i=1}^n \sum_{j=1}^n a_{ij} X_i X_j$ with $a_{ij} = a_{ji} \in K$ and $g = \sum_{i=1}^m \sum_{j=1}^m b_{ij} X_i X_j$ with $b_{ij} = b_{ji} \in K$ be two quadratic forms over K. Then we define the **orthogonal sum** $f \perp g$ to be the quadratic form

$$\sum_{i=1}^n \sum_{j=1}^n a_{ij} X_i X_j + \sum_{i=n+1}^{n+m} \sum_{j=n+1}^{n+m} b_{ij} X_i X_j.$$

For $n \in \mathbb{N}$, we denote by $n \times f$ the n-fold orthogonal sum of f.

In particular, $\langle a_1, \ldots, a_n \rangle \perp \langle b_1, \ldots, b_m \rangle = \langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle$.

2.1.27 **Definition:**

Let f be a quadratic form over K of dimension n.

We say that f **represents** $a \in K$ **over** K iff there exist $b_1, \ldots, b_n \in K$ with $a = f(b_1, \ldots, b_n)$.

We call f **isotropic over** K iff it represents 0 over K non-trivially, otherwise we call f **anisotropic**.

f is said to be **weakly isotropic over** K iff $n \times f$ is isotropic over K for some $1 \leqslant n \in \mathbb{N}$, otherwise it is said to be **strongly anisotropic**.

Note that, if f and g are isometric quadratic forms over K, then f represents $a \in K$ over K if and only if g represents a over K. As a consequence, f is isotropic over K if and only if g is isotropic over K. Note also that if K is non-real, i.e., $-1 \in \sum K^2$, then every quadratic form over K is weakly isotropic.

2.1.28 **Definition:**

A quadratic form f over K is called **regular** iff $\det M_f \neq 0$.

Note that a diagonal form $\langle a_1, \ldots, a_n \rangle$ is regular if and only if none of the entries $a_1, \ldots, a_n$ equals zero.

2.1.29 **Definition:**

A regular quadratic form $\rho = \langle a_1, \ldots, a_n \rangle$ over K is said to be **indefinite with respect to an ordering** P of K iff there exist $i, j \in \{1, \ldots, n\}$ with $a_i \in P$ and $a_j \notin P$.

A regular quadratic form over K is called **totally indefinite** iff it is indefinite with respect to every ordering of K.

Note that a regular quadratic form over K is totally indefinite if and only if it is isotropic over the real closure of every ordering of K.

2.1.30 **Proposition:**

Every weakly isotropic regular quadratic form over K is totally indefinite.

2.1.31 **Definition:**

Let $\rho = \langle a_1, \ldots, a_n \rangle$ be a regular quadratic form over K, and let v be a non-trivial valuation of K of residue characteristic unequal to 2. Let $c_1, \ldots, c_s \in K$ be such that $v(c_1), \ldots, v(c_s)$ are pairwise incongruent modulo $2\Gamma_v$ and they yield a complete set of representatives of the subset $\{v(a_i) + 2\Gamma_v \mid i = 1, \ldots, n\}$ of $\Gamma_v / 2\Gamma_v$. As the element whose value is a representative of $0 + 2\Gamma_v$, we always choose 1.

For $j \in \{1, \ldots, s\}$, let $(a_{j1}, \ldots, a_{jn_j})$ be the subsequence of $(a_1, \ldots, a_n)$ containing all entries whose value is congruent to $v(c_j)$ modulo $2\Gamma_v$, and choose $b_{j1}, \ldots, b_{jn_j} \in K$ such that $u_{jk} := a_{jk} c_j^{-1} b_{jk}^2 \in \mathcal{O}_v^\times$ $(k = 1, \ldots, n_j)$. Then $\rho = \langle a_1, \ldots, a_n \rangle$ is isometric to $c_1 \rho_1 \perp \cdots \perp c_s \rho_s$, where $\rho_j = \langle u_{j1}, \ldots, u_{jn_j} \rangle$.

The regular quadratic forms $\overline{\rho_j}^v := \langle \overline{u_{j1}}^v, \ldots, \overline{u_{jn_j}}^v \rangle$ over $\overline{K}^v$ are called the **residue forms of ρ with respect to v**.

We will need the following characterization of (weak) isotropy in henselian fields with residue characteristic unequal to 2.

2.1.32 **Lemma:**

Let (H, v) be a non-trivial henselian valued field of residue characteristic unequal to 2. Then a regular quadratic form is isotropic over H if and only if at least one of its residue forms is isotropic over $\overline{H}^v$.
If $\overline{H}^v$ is real, the same holds for weak isotropy.

2.1.3 Local-Global Principles

In this section, we present some local-global principles for isotropy and weak isotropy of quadratic forms. Every result can again be found in [18], [20] or [7]. We start with Witt's Local-Global Principle for isotropy of quadratic forms over function fields of degree 1 over $\mathbb{R}$.

2.1.33 **Theorem:**

Let F be a function field of degree 1 over $\mathbb{R}$. Then every regular quadratic form over F of dimension > 2, that is isotropic over the completion of (F, v) for each valuation v of $F/\mathbb{R}$, is isotropic over F.

This theorem can be generalized as follows.

2.1.34 **Theorem:**

Let F be a function field of degree 1 over a real closed field R. Then every regular quadratic form over F of dimension > 2, that is totally indefinite over F, is isotropic over F.

In the case of an SAP-field, weak isotropy for regular quadratic forms can be characterized as follows. See [18] for the definition of an SAP-field as well as for the theorem.

2.1.35 **Theorem:**

Let K be a real field. Then K is an SAP-field if and only if the Weak Hasse Principle holds in K:
Every regular quadratic form over K that is totally indefinite is weakly isotropic over K.

Examples for SAP-fields are real fields of transcendence degree $\leqslant 1$ over a real closed field.

The following local-global principle gives a characterization for arbitrary real fields. It can be found in [18] and [7], for instance.

2.1.36 **Theorem:** (Bröcker-Prestel Local-Global Principle)

Let F be a real field. A regular quadratic form over F is weakly isotropic over F if and only if it is (weakly) isotropic over $\mathbb{R}$ for every embedding of F into $\mathbb{R}$ and if it is weakly isotropic over the henselizations with respect to all (non-trivial) real valuations on F.

There is a tightened version of this local-global principle (see [18], proof of Theorem 8.12).

2.1.37 **Theorem:**

Let F be a real field. A regular quadratic form $\rho = \langle a_1, \ldots, a_n \rangle$ over F is weakly isotropic over F if and only if it is totally indefinite over F and if it is weakly isotropic over the henselizations of (F, v) for every (non-trivial) real valuation v on F which has the property that $2 \nmid v(a_i)$ in Γ_v for some $i \in \{1, \ldots, n\}$.

2.1.4 Model Theory and the Ax-Kochen-Ershov Principle

For an introduction into model theory, we recommend [19], and recall only the most important notions and results we will use here. Concerning the Ax-Kochen-Ershov Principle, we also refer to [15].

In this section, L is always a first-order language. Let $\mathcal{A}$ be an L-structure with universe A. For a subset A' of A, we denote by $L(A')$ the extended language that results by adding to L a constant c_a for each $a \in A'$, and we denote by $(\mathcal{A}, A')$ the $L(A')$-structure that has universe A and that interpretes every symbol of L as in $\mathcal{A}$ and every constant c_a $(a \in A')$ as a. We write $\mathrm{D}(\mathcal{A})$ for the set of all atomic $L(A)$-sentences or negated atomic $L(A)$-sentences that hold in $(\mathcal{A}, A)$, and call this set the **diagram of** $\mathcal{A}$.

At first, the most important theorem of model theory.

2.1.38 **Theorem:** (Compactness Theorem)

A set Σ of L-sentences has a model if and only if every finite subset of Σ has a model.

Now, some model theoretic results which we will use later.

2.1.39 **Lemma:** (Diagram Lemma)

Let $\mathcal{A}$ be an L-structure with universe A, and let $\mathcal{B}$ be an $L(A)$-structure that is a model of $\mathrm{D}(\mathcal{A})$. Then $a \mapsto c_a^{\mathcal{B}}$ is an embedding of $\mathcal{A}$ into $\mathcal{B}$.

An important concept in model theory is the concept of saturated structures.

2.1.40 **Definition:**

Let $\mathcal{A}$ be an L-structure with universe A, and let $A' \subset A$. A set Φ of $L(A')$-formulae with one free variable is called a **type of** $(\mathcal{A}, A')$ iff there exists an elementary extension $\mathcal{B}$ of $\mathcal{A}$ and an element $b \in B := |\mathcal{B}|$ such that $(\mathcal{B}, B) \models \varphi(c_b)$ for all $\varphi \in \Phi$, and, in that case, we say that Φ is **realized (by** b**) in** $(\mathcal{B}, B)$.

The Compactness Theorem yields a test for the property of a set of $L(A)$-formulae to be a type of $(\mathcal{A}, A)$.

2.1.41 **Lemma:**

Let $\mathcal{A}$ be an L-structure with universe A. A set Φ of $L(A)$-formulae is a type of $(\mathcal{A}, A)$ if and only if every finite subset of Φ is realizable in $(\mathcal{A}, A)$.

2.1.42 **Definition:**

Let $\mathcal{A}$ be an L-structure with universe A, and let κ be an infinite cardinal number. We say that $\mathcal{A}$ is **κ-saturated** iff every type of $(\mathcal{A}, A')$ with $A' \subset A$ and $\mathrm{card}(A') < \kappa$ can be realized in $(\mathcal{A}, A)$.

2.1.43 **Remark:**

Let $\mathcal{A}$ be an L-structure. It is well known that, for every sufficiently big cardinal number κ, there exists an κ-saturated elementary extension $\mathcal{B}$ of $\mathcal{A}$.

For the rest of this section, we will consider existentially closed substructures, especially for the case of henselian valued fields.

2.1.44 **Definition:**

Let $\mathcal{A}$ be an L-structure with universe A, and let $\mathcal{B}$ be an L-extension of $\mathcal{A}$. We call $\mathcal{A}$ **existentially closed (e.c.) in** $\mathcal{B}$ if every existential $L(A)$-sentence that holds in $(\mathcal{B}, A)$ already holds in $(\mathcal{A}, A)$.

2.1.45 **Lemma:**

Let let $\mathcal{A} \subset \mathcal{B}$ be an L-extension of L-structures. Then $\mathcal{A}$ is e.c. in $\mathcal{B}$ if and only if there exists an L-extension $\mathcal{C}$ of $\mathcal{B}$ that is an elementary extension of $\mathcal{A}$.

Existential closeness in the case of a field extension can be described as follows.

2.1.46 **Proposition:**

Let K_2/K_1 be an extension of fields. Then K_1 is existentially closed in K_2 if and only if, for every finite sequence of polynomials

$$f_1, \dots, f_r \in K_1[X_1, \dots, X_m],$$

whenever there exists some $a \in K_2^m$ such that $f_1(a) = \cdots = f_r(a) = 0$, then there also exists some $b \in K_1^m$ such that $f_1(b) = \cdots = f_r(b) = 0$.

2.1.47 **Examples:**

1. With Hilbert's Nullstellensatz, it follows that, if K_1 is algebraically closed, then it is e.c. in every extension field K_2.
2. If K_1 is a real closed field and K_2 is a real extension field of K_1, then K_1 is e.c. in K_2. This follows from the existence of a real closure (Theorem 2.1.14) and the fact that the theory of real closed fields admits elimination of quantifiers (see 3.1.22).

Wheeler proved in [28] the following general characterization.

2.1.48 **Theorem:**

Let K_2/K_1 be an extension of fields. Then K_1 is e.c. in K_2 if and only if K_2/K_1 is separable, K_1 is relatively algebraically closed in K_2 and every absolutely irreducible K_1-variety, which has a K_2-rational point, has a K_1-rational point.

Now we consider ordered abelian groups.

2.1.49 **Proposition:**

Let Γ_1 be a subgroup of an ordered abelian group Γ_2. Then Γ_1 is existentially closed in Γ_2 if and only if, for all sequences of linear forms

$$l_1, \ldots, l_r, l'_1, \ldots, l'_s \in \mathbb{Z}[X_1, \ldots, X_m]$$

and for all sequences

$$\gamma_1, \ldots, \gamma_r, \gamma'_1, \ldots, \gamma'_s \in \Gamma_1,$$

whenever there exist $x_1, \ldots, x_m \in \Gamma_2$ such that

$$l_i(x_1, \ldots, x_m) = \gamma_i \text{ and } l'_j(x_1, \ldots, x_m) > \gamma'_j \ (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s),$$

then there exist $y_1, \ldots, y_m \in \Gamma_1$ having the same properties.

2.1.50 **Examples:**

Let Γ_1 be a subgroup of an ordered abelian group Γ_2

1. If Γ_1 is divisible, then Γ_1 is e.c. in Γ_2. This follows from the fact that the theory of divisible ordered abelian groups admits elimination of quantifiers.
2. If Γ_1 is regularly dense, i.e., $n\Gamma_1$ is dense in Γ_1 for all $n \in \mathbb{N}\backslash\{0\}$, and if Γ_2/Γ_1 is torsion-free, then Γ_1 is e.c. in Γ_2 (see [27], Corollary 1.5).

2.1.51 **Remark:**

An ordered abelian group Γ is regularly dense if and only if $p\Gamma$ is dense in Γ for all prime numbers p. This can be shown as follows. Let $n, m \in \mathbb{N}\backslash\{0\}$ such that $n\Gamma$ and $m\Gamma$ are dense in Γ. Let $\gamma_1, \gamma_2 \in \Gamma$ such that $\gamma_1 < \gamma_2$. Then there exist $\delta_1, \delta_2 \in \Gamma$ such that $\gamma_1 < n\delta_1 < n\delta_2 < \gamma_2$. In particular, $\delta_1 < \delta_2$, hence there exists some $\varepsilon \in \Gamma$ such that $\delta_1 < m\varepsilon < \delta_2$. Altogether, we have $\gamma_1 < n\delta_1 < nm\varepsilon < n\delta_2 < \gamma_2$, and we have shown that $nm\Gamma$ is dense in Γ.

At last, we give the reformulation of existential closeness for valued fields.

2.1.52 **Proposition:**

Let $(K_1, \mathcal{O}_1)$ be a valued field, and let $(K_2, \mathcal{O}_2)$ be an extension of $(K_1, \mathcal{O}_1)$. Then $(K_1, \mathcal{O}_1)$ is existentially closed in $(K_2, \mathcal{O}_2)$ if and only if, for all sequences of polynomials

$$f_1, \ldots, f_r, g_1, \ldots, g_s, h_1, \ldots, h_t \in K_1[X_1, \ldots, X_m],$$

whenever there exists some $a \in K_2^m$ such that

$$f_1(a) = \cdots = f_r(a) = 0,\ g_1(a), \ldots, g_s(a) \in \mathcal{O}_2 \text{ and } h_1(a), \ldots, h_t(a) \notin \mathcal{O}_2,$$

then there exists some $b \in K_1^m$ having the same properties.

The Ax-Kochen-Ershov Principle tells us that in certain cases, we can derive the existential closeness of an extension of valued fields from the existential closeness of the extension of their value groups and the extension of their residue fields.

2.1.53 **Theorem:** (Ax-Kochen-Ershov Principle)

Let $(K_1, \mathcal{O}_1)$ be a henselian valued field of residue characteristic 0, and let $(K_2, \mathcal{O}_2)$ be an extension of $(K_1, \mathcal{O}_1)$. Let $v_i\colon K_i \twoheadrightarrow \Gamma_i \cup \{\infty\}$ be corresponding valuations. If $\overline{K_1}^{v_1}$ is e.c. in $\overline{K_2}^{v_2}$ and Γ_1 is e.c. in Γ_2, then $(K_1, \mathcal{O}_1)$ is e.c. in $(K_2, \mathcal{O}_2)$.

To prove this, it has to be shown that over $(K_1, \mathcal{O}_1)$ the valued field $(K_2, \mathcal{O}_2)$ can be embedded into a $\mathrm{card}(K_1)^+$-saturated elementary extension of $(K_1, \mathcal{O}_1)$ (see Lemma 2.1.45).

2.1.54 **Remark:**

Let $(K_1, \mathcal{O}_1)$ be a henselian valued field, and let $(K_2, \mathcal{O}_2)$ be an extension of $(K_1, \mathcal{O}_1)$ such that $\overline{K_1}^{\mathcal{O}_1}$ is e.c. in $\overline{K_2}^{\mathcal{O}_2}$ and $\Gamma_{\mathcal{O}_1}$ is e.c. in $\Gamma_{\mathcal{O}_2}$. Let P be an ordering of K_2 such that $\mathcal{O}_2$ is convex with respect to P and suppose the residue field of $(K_1, \mathcal{O}_1)$ with respect to $\mathcal{O}_1$ is real closed, and therefore e.c. in the residue field of $(K_2, \mathcal{O}_2)$. Let $(L, \mathcal{O}, Q)$ be a $\mathrm{card}(K_1)^+$-saturated elementary extension of $(K_1, \mathcal{O}_1, P \cap K_1)$. In particular, $\mathcal{O}$ is convex with respect to Q and the residue field of $(L, \mathcal{O})$ is real closed. Then the residue field $\overline{K_2}^{\mathcal{O}_2}$ of $(K_2, \mathcal{O}_2)$ is order-preserving embeddable into $\overline{L}^{\mathcal{O}}$ over the real closed field $\overline{K_1}^{\mathcal{O}_1}$, and this embedding can be extended to an embedding of $(K_2, \mathcal{O}_2)$ into $(L, \mathcal{O})$ over $(K_1, \mathcal{O}_1)$.

Let $f \in K_1[X_1, \ldots, X_n]$ and $a_1, \ldots, a_n \in K_2$ such that $f(a_1, \ldots, a_n) \in \mathcal{O}_2^\times \cap P$, i.e., $\overline{f(a_1, \ldots, a_n)}^{\mathcal{O}_2} \in \overline{P}^{\mathcal{O}_2} \subset (\overline{L}^{\mathcal{O}})^2$, hence $f(a_1, \ldots, a_n) \in \mathcal{O}^\times \cap Q$. Since the extension $(L, \mathcal{O}, Q)/(K_1, \mathcal{O}_1, P \cap K_1)$ is elementary, there are $a_1', \ldots, a_n' \in K_1$ such that $f(a_1', \ldots, a_n') \in \mathcal{O}_1^\times \cap P$.

2.2 The Transformation of Arbitrary into Abhyankar Valuations

In the first chapter, we have shown a (weak) local uniformization theorem for Abhyankar valuations of function fields over fields of characteristic 0. Now we want to construct such valuations, and in this construction, we want to preserve a finite amount of properties of an arbitrary non-trivial valuation. For valuations of rank 1, this is done by an extension of the valued field in such a way that it is possible to use the Ax-Kochen-Ershov Principle to restrict the valuation to a *good* part of this valued field that contains all the relevant information. Then we built it up to an Abhyankar valuation of the function field by using the Implicit Function Theorem. For similar results, obtained with the same techniques, see [15] and [13]. We here add finitely many non-divisibilities by non-zero integers in the value group to the properties that we want to preserve. This is important for the last section of this chapter, where we (re-)prove an improvement of the Bröcker-Prestel Local-Global Principle in the case of a function field over $\mathbb{R}$.

2.2.1 **Lemma:**

Let K be a field of characteristic 0, and let F be a function field over K. Let v be a rank-1-valuation of F/K.
Let P be a subset of F such that $P = F$ or P is an ordering of F such that v is compatible with P.
Let $a_1, \ldots, a_\mu \in \mathcal{O}_v$, and let $b_1, \ldots, b_\lambda \in \mathcal{O}_v^\times \cap P$.
Let $c_1, \ldots, c_\sigma \in F^\times$ and $m_1, \ldots, m_\sigma \in \mathbb{Z}\backslash\{0\}$ such that, for all $j \in \{1, \ldots, \sigma\}$, we have that $v(c_j)$ is not divisible by m_j in Γ_v.
Let $t \in \mathbb{N}$ be the transcendence degree of F over K, let s be the maximal number of $\mathbb{Z}$-linearly independent values in $\{v(c_1), \ldots, v(c_\sigma)\}$, and let m be the maximal number of elements in $\{\overline{a_1}^v, \ldots, \overline{a_\mu}^v\}$ which are algebraically independent over K. Let $r \in \mathbb{N}$ such that $\max\{1, s\} \leqslant r \leqslant t - m$.
Then there exists some Abhyankar valuation w of F/K and some subset Q of F such that

- the value group Γ_w has rank 1 and rational rank r,
- $Q = F$ if $P = F$, otherwise Q is an ordering of F and w is compatible with Q,
- $K(\overline{a_1}^v, \ldots, \overline{a_\mu}^v) \subset \overline{F}^w$ and $\overline{Q}^w \cap K(\overline{a_1}^v, \ldots, \overline{a_\mu}^v) = \overline{P}^v \cap K(\overline{a_1}^v, \ldots, \overline{a_\mu}^v)$,
- $a_1, \ldots, a_\mu \in \mathcal{O}_w$ and $\overline{a_k}^w = \overline{a_k}^v$ $(k = 1, \ldots, \mu)$,
- $b_1, \ldots, b_\lambda \in \mathcal{O}_w^\times \cap Q$ and
- $w(c_j)$ is not divisible by m_j in Γ_w $(j = 1, \ldots, \sigma)$.

Proof:

We may assume that $c_1, \ldots, c_\sigma \in P$ and that the values $v(c_1), \ldots, v(c_s)$ are $\mathbb{Z}$-linearly independent. Then, for $s < k \leqslant \sigma$, we have $\alpha_0 v(c_k) = \sum_{1 \leqslant j \leqslant s} \alpha_j v(c_j)$ for some $(\alpha_0, \ldots, \alpha_s) \in \mathbb{Z}^{s+1}$ with $\alpha_0 \neq 0$, hence $b_{\lambda+k-s} := c_k^{\alpha_0} \prod_{1 \leqslant j \leqslant s} c_j^{-\alpha_j} \in \mathcal{O}_v^\times \cap P$. So, if $b_{\lambda+k-s} \in \mathcal{O}_w^\times$ and $\alpha_0 m_k \nmid w(\prod_{1 \leqslant j \leqslant s} c_j^{\alpha_j})$ in Γ_w for some valuation w of F, then $\alpha_0 w(c_k) = w(\prod_{1 \leqslant j \leqslant s} c_j^{\alpha_j})$, and thus $m_k \nmid w(c_k)$. We therefore may replace m_k by $\alpha_0 m_k$ and c_k by $\prod_{1 \leqslant j \leqslant s} c_j^{\alpha_j} \in K(c_1, \ldots, c_s)$. Set $\lambda' := \lambda + \sigma - s$.

We may assume that $a_1, \ldots, a_\mu \neq 0$ and that $\overline{a_1}^v, \ldots, \overline{a_m}^v \in \overline{F}^v$ are algebraically independent over K. We embed $\overline{F}^v$ into the henselization (H, v) of (F, v) in such a way that $a_1, \ldots, a_m$ are identified with their residue classes (see Remark 1.1.43 and Lemma 1.1.57). Due to the Baer-Krull Representation Theorem, P extends uniquely to H. We let $\tilde{K}$ be the algebraic closure of $K(a_1, \ldots, a_m)$ if $P = F$ and the real closure of $K(a_1, \ldots, a_m)$ with respect to P otherwise. Let $\tilde{F}$ be the compositum of F and $\tilde{K}$ in the algebraic closure of H. Note that $\tilde{F}$ is a function field of degree $\tilde{t} := t - m$ over $\tilde{K}$ and (H, v) can be extended to $\tilde{H} := H\tilde{K} \supset \tilde{F}$ in a unique way. We denote this extension by $\tilde{v}$ and note that $(\tilde{H}, \tilde{v})$ is the henselization of $(\tilde{F}, \tilde{v})$, since as an algebraic extension of the henselian valued field (H, v) it is henselian and the henselization must contain both H and $\tilde{K}$.

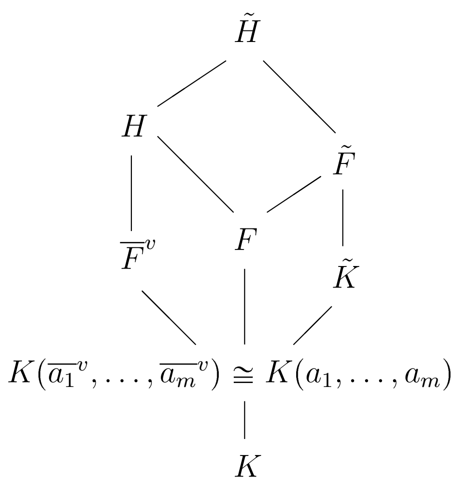
We have $\Gamma_v = v(F^\times) = \tilde{v}(\tilde{F}^\times)$: Suppose the value group $\tilde{v}(\tilde{F}^\times) = \tilde{v}(\tilde{H}^\times)$ would be strictly larger than $\Gamma_v = v(H^\times)$, hence there would exist some $d \in \tilde{K}$ such that the ramification index of $(H(d), \tilde{v})/(H, v)$ would be bigger than 1. Therefore the residue degree of this extension would have to be less than $[H(d) : H]$. Since $\overline{H(d)}^{\tilde{v}} \supset \overline{H}^v(d)$ and $\overline{H}^v \subset H$, we would have

$$[\overline{H}^v(d) : \overline{H}^v] \leqslant [\overline{H(d)}^{\tilde{v}} : \overline{H}^v] < [H(d) : H] \leqslant [\overline{H}^v(d) : \overline{H}^v],$$

a contradiction.

Since $\tilde{H}$ is contained in the real closure of (H, P), P extends to $\tilde{H}$ and $\tilde{v}$ is compatible with any such extension, since the convex hull of the valuation ring of (H, v) in $\tilde{H}$ with respect to an extension of P is a valuation ring that extends $\mathcal{O}_v$ (see Example 2.1.16), hence, as mentioned above, this must be the valuation ring of $\tilde{v}$.

The elements $x_1 := c_1, \ldots, x_s := c_s \in F \subset \tilde{F}$ are algebraically independent over $\tilde{K}$ (Theorem 1.1.42), hence they can be extended to a transcendence basis $x_1, \ldots, x_{\tilde{t}}$ of $\tilde{F}/\tilde{K}$. The extension $\tilde{F}/\tilde{K}(x_1, \ldots, x_{\tilde{t}})$ is finite, thus we have that $\tilde{F} = \tilde{K}(x_1, \ldots, x_{\tilde{t}}, y)$, where y is algebraic over $\tilde{K}(\underline{x})$. Let $f(X_1, \ldots, X_{\tilde{t}}, Y) \in \tilde{K}[X_1, \ldots, X_{\tilde{t}}, Y]$ be an irreducible polynomial with $f(\underline{x}, y) = 0$ and $\frac{\partial}{\partial Y} f(\underline{x}, y) \neq 0$.



Let $\{q_1, \ldots, q_v\}$ be the set of all prime factors of the numbers $m_1, \ldots, m_\sigma$. Let (H', v') be a henselian extension of $(\tilde{H}, \tilde{v})$ such that the value group Γ' of (H', v') is the p-divisible hull of $\Gamma_{\tilde{v}} = \tilde{v}(\tilde{F}^\times)$ for some prime number $p \notin \{2, q_1, \ldots, q_v\}$ and such that the residue field remains unchanged. This can be done by iteratively adjoining p-th roots of elements whose values are not divisible by p. For any such extension, it follows that the ramification index is p, and therefore the Fundamental (In-)Equality 1.1.39 yields that the residue degree must be 1 and the extension of the valuation is unique.
Note that $p\Gamma'$ is dense in Γ', but for all $\gamma \in \Gamma_{\tilde{v}}$, if $\pi \nmid \gamma$ in $\Gamma_{\tilde{v}}$ for some product π of prime numbers in $\{q_1, \ldots, q_v\}$, then $\pi \nmid \gamma$ in Γ', since otherwise $\pi \mid \gamma$ would happen after an extension with ramification index p, and therefore some $q \in \{q_1, \ldots, q_v\}$ would divide p, a contradiction. In particular, for all

$j \in \{1, \ldots, \sigma\}$, we have that $v'(c_j)$ is not divisible by m_j in Γ'. Note also that P extends to H', since p is odd (see Theorem 2.1.9). We denote such an extension by P'. The valuation v' is compatible with P', if P' is an ordering, since it is the unique extension of $\tilde{v}$ to H'.

Let L be the relative algebraic closure of $\tilde{K}(x_1, \ldots, x_s) = \tilde{K}(c_1, \ldots, c_s)$ in H'. If there exists some element $a \in L \cap P'$ and some prime number q such that $v'(a)$ is divisible by q in $\Gamma' = v'(H'^{\times})$ but not in $v'(L)$, then we adjoin a q-th root a' of a to H'. The unique extension v'_1 of v' to $H'(a')$ has a bigger residue field than (H', v') but the same value group: Let $b \in H'$ such that $v'_1(b) = v'_1(a')$. Then the residue class of $\frac{a'}{b}$ is not in $\overline{H'}^{v'}$, since otherwise there would be some $c \in H'^{\times}$ such that $v'_1(\frac{a'}{bc} - 1) > 0$, and, by Theorem 1.1.49 (iii), $T^q - \frac{a}{b^q c^q}$ would have a root in H', i.e., a would have a q-th root in H'. Since L is relatively algebraically closed in H', this root would also lie in L, a contradiction. Therefore the residue degree of $(H'(a'), v'_1)/(H', v')$ is equal to q, and hence the ramification index must be 1.

If P' is an ordering, it extends to an ordering on $H'(a')$ and v'_1 is compatible with this extension. Note that $L(a')$ is relatively algebraically closed in $H'(a')$. We repeat this procedure until we get an extension $(H'', v'')/(L', v'')$ where $v''(H''^{\times})/v''(L'^{\times})$ is torsion-free. Then the following statements hold:

1. (L', v'') is henselian (see Corollary 1.1.51).
2. $\overline{L'}^{v''} = \tilde{K}$, which is algebraically closed or real closed, and therefore it is existentially closed in $\overline{H''}^{v''}$ (see Example 2.1.47).
3. The value group of (L', v'') is archimedean and dense, and therefore regularly dense (see [30], Theorem 2.4). Since $v''(H''^{\times})/v''(L'^{\times})$ is torsion-free, $v'(L'^{\times})$ is existentially closed in $v''(H''^{\times})$ (see Example 2.1.50).

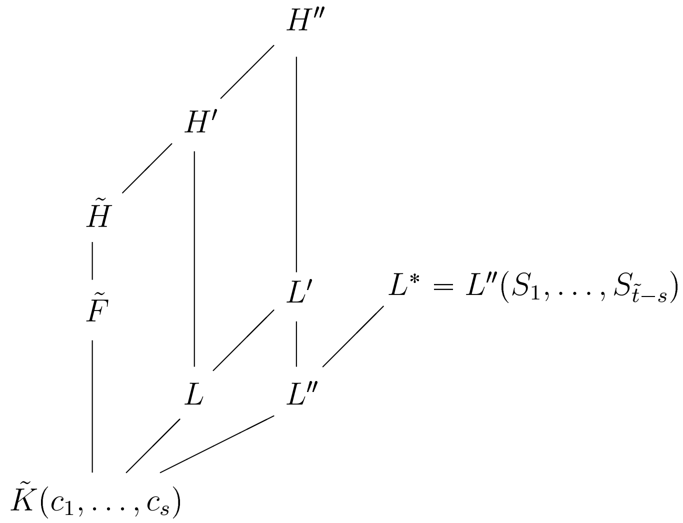
With the Ax-Kochen-Ershov Principle (2.1.53), it follows that (L', v'') is existentially closed in (H'', v''). For all $k \in \{1, \ldots, \mu\}$ and for all $l \in \{1, \ldots, \lambda'\}$, write $a_k = \frac{a'_k(\underline{x}, y)}{a''_k(\underline{x})}$ and $b_l = \frac{b'_l(\underline{x}, y)}{b''_l(\underline{x})}$ where $a'_k, b'_l \in \tilde{K}[\underline{X}, Y]$ and $a''_k, b''_l \in \tilde{K}[\underline{X}]$ with $a'_k(\underline{x}, y), a''_k(\underline{x}), b'_l(\underline{x}, y), b''_l(\underline{x}) \neq 0$. Let $\overline{a_k} := \overline{a_k}^v \in \tilde{K}$ $(k = 1, \ldots, \mu)$. The following existential sentence holds in $(H'', \mathcal{O}_{v''})$:

$$
\begin{aligned}
\exists \xi_{s+1}, \ldots, \xi_{\tilde{t}}, z, \zeta, \alpha_1, \ldots, \alpha_\mu, \beta_1, \ldots, \beta_{\lambda'}, \eta_1, \ldots, \eta_\mu, \theta_1, \ldots, \theta_{\lambda'} \\
f(x_1, \ldots, x_s, \xi_{s+1}, \ldots, \xi_{\tilde{t}}, z) = 0, \\
\frac{\partial}{\partial Y} f(\underline{x}, \underline{\xi}, z) \cdot \zeta - 1 = 0, \\
a''_1(\underline{x}, \underline{\xi}) \cdot \alpha_1 - 1 = 0, \ldots, a''_\mu(\underline{x}, \underline{\xi}) \cdot \alpha_\mu - 1 = 0, \\
b''_1(\underline{x}, \underline{\xi}) \cdot \beta_1 - 1 = 0, \ldots, b''_{\lambda'}(\underline{x}, \underline{\xi}) \cdot \beta_{\lambda'} - 1 = 0, \\
(a'_1(\underline{x}, \underline{\xi}, z) \cdot \alpha_1 - \overline{a_1}) \cdot \eta_1 - 1 = 0, \ldots, (a'_\mu(\underline{x}, \underline{\xi}, z) \cdot \alpha_\mu - \overline{a_\mu}) \cdot \eta_\mu - 1 = 0, \\
b'_1(\underline{x}, \underline{\xi}, z) \cdot \theta_1 - 1 = 0, \ldots, b'_{\lambda'}(\underline{x}, \underline{\xi}, z) \cdot \theta_{\lambda'} - 1 = 0,
\end{aligned}
$$

$$
\begin{aligned}
a_1'(\underline{x},\underline{\xi},z)\cdot\alpha_1-\overline{a_1},\dots,a_\mu'(\underline{x},\underline{\xi},z)\cdot\alpha_\mu-\overline{a_\mu}&\in\mathcal{O},\\
b_1'(\underline{x},\underline{\xi},z)\cdot\beta_1,\dots,b_{\lambda'}'(\underline{x},\underline{\xi},z)\cdot\beta_{\lambda'}&\in\mathcal{O},\\
b_1''(\underline{x},\underline{\xi})\cdot\theta_1,\dots,b_{\lambda'}''(\underline{x},\underline{\xi})\cdot\theta_{\lambda'}&\in\mathcal{O},\\
\eta_1,\dots,\eta_\mu&\notin\mathcal{O}.
\end{aligned}
$$

One solution is $(\xi_{s+1},\dots,\xi_{\tilde{t}}) = (x_{s+1},\dots,x_{\tilde{t}})$, $z = y$, $\zeta = (\frac{\partial}{\partial Y}f(\underline{x},y))^{-1}$, $(\alpha_1,\dots,\alpha_\mu) = (a_1''^{-1},\dots,a_\mu''^{-1})$, $(\beta_1,\dots,\beta_{\lambda'}) = (b_1''^{-1},\dots,b_{\lambda'}''^{-1})$, $(\eta_1,\dots,\eta_\mu) = ((a_1-\overline{a_1})^{-1},\dots,(a_\mu-\overline{a_\mu})^{-1})$ and $(\theta_1,\dots,\theta_{\lambda'}) = (b_1'^{-1},\dots,b_{\lambda'}'^{-1})$, since $a_k'a_k''^{-1}-\overline{a_k}\in\mathfrak{m}_{v''}$ $(k=1,\dots,\mu)$ and $b_l'b_l''^{-1}\in\mathcal{O}_{v''}^{\times}$ $(l=1,\dots,\lambda')$. Then there exist corresponding elements $x_{s+1}',\dots,x_{\tilde{t}}',y',\zeta',\alpha_1',\dots,\alpha_\mu'$, $\beta_1',\dots,\beta_{\lambda'}'$, $\eta_1',\dots,\eta_\mu'$, $\theta_1',\dots,\theta_{\lambda'}'\in L'$. According to Remark 2.1.54, we may assume for all $l\in\{1,\dots,\lambda'\}$ that $\frac{b_l'(\underline{x},\underline{x}',y')}{b_l''(\underline{x},\underline{x}')} = b_l'(\underline{x},\underline{x}',y')\cdot\beta_l'\in P'\cap L'$, i.e., $v''(b_l'(\underline{x},\underline{x}',y')\cdot\beta_l'-\delta_l^2)>0$ for some $\delta_l\in L'$, since the residue field $\tilde{K}$ of (L',v'') is real closed or algebraically closed.

We consider $L'' := \tilde{K}(\underline{x},\underline{x}',y',\zeta',\underline{\alpha}',\underline{\beta}',\underline{\eta}',\underline{\theta}',\underline{\delta})$ with the restriction of v'' coming from L'. Note that $v''_{|L''}$ is already an Abhyankar valuation of $L''/\tilde{K}$. Let $L^* = L''(S_1,\dots,S_{\tilde{t}-s})$ be the rational function field in $\tilde{t}-s$ indeterminates over L''. The valuation v'' can be extended uniquely to L^* in such a way that the value group is $v''(L''^{\times})\bigoplus\mathbb{Z}^{r-s}$ ordered archimedean and the residue field is $K^* := \tilde{K}(S_1,\dots,S_{\tilde{t}-r})$: This follows from the propositions 1.1.40 and 1.1.41 when we take $\Delta := \mathbb{R}$ with the usual ordering in 1.1.41 and take into account that the rational rank of $v''(L''^{\times})$ is finite.
By Theorem 2.1.10, $P'\cap L''$ can be extended to L^*. Denote the extension of the valuation v'' by v^* and the extension of $P'\cap L''$ by P^*, and note that v^* is compatible with P^*. Note also that the extension of the value group has no effect on the divisibility of the elements in $v''(L''^{\times})$. v^* is an Abhyankar valuation of $L^*/\tilde{K}$.



Let (H^*,v^*) be the henselization of (L^*,v^*). By the Implicit Function Theorem 1.1.62, there are open (w.r.t. the topology induced by v^*) subsets U,V

of H^* such that, for all $x^*_{s+1} \in x'_{s+1} + U, \dots, x^*_{\tilde{t}} \in x'_{\tilde{t}} + U$, there exists exactly one solution $(y^*, \zeta^*, \alpha^*_1, \dots, \alpha^*_\mu, \beta^*_1, \dots, \beta^*_{\lambda'}, \eta^*_1, \dots, \eta^*_\mu, \theta^*_1, \dots, \theta^*_{\lambda'})$ of

$$\begin{aligned}
f(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, Y) &= 0,\\
\frac{\partial}{\partial Y} f(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, Y) \cdot Z - 1 &= 0,\\
a''_1(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}) \cdot A_1 - 1 &= 0, \dots,\\
a''_\mu(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}) \cdot A_\mu - 1 &= 0,\\
b''_1(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}) \cdot B_1 - 1 &= 0, \dots,\\
b''_{\lambda'}(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}) \cdot B_{\lambda'} - 1 &= 0,\\
(a'_1(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, Y) \cdot A_1 - \overline{a_1}) \cdot E_1 - 1 &= 0, \dots,\\
(a'_\mu(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, Y) \cdot A_\mu - \overline{a_\mu}) \cdot E_\mu - 1 &= 0,\\
b'_1(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, Y) \cdot \Theta_1 - 1 &= 0, \dots,\\
b'_{\lambda'}(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, Y) \cdot \Theta_{\lambda'} - 1 &= 0,
\end{aligned}$$

such that $y^* \in y' + V$, $\zeta^* \in \zeta' + V$, $\alpha^*_k \in \alpha'_k + V$ $(k = 1, \dots, \mu)$, $\beta^*_l \in \beta'_l + V$ $(l = 1, \dots, \lambda')$, $\eta^*_k \in \eta'_k + V$ $(k = 1, \dots, \mu)$ and $\theta^*_l \in \theta'_l + V$ $(l = 1, \dots, \lambda')$. We can further choose U, V small enough that the following open conditions are satisfied:

$$\begin{aligned}
&a'_1(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*) \cdot \alpha^*_1 - \overline{a_1}, \dots,\\
&\quad a'_\mu(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*) \cdot \alpha^*_\mu - \overline{a_1} \in \mathcal{O}_{v^*},\\[1ex]
&b'_1(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*) \cdot \beta_1, \dots,\\
&\quad b'_{\lambda'}(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*) \cdot \beta_{\lambda'} \in \mathcal{O}_{v^*},\\[1ex]
&b''_1(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}) \cdot \theta_1, \dots,\\
&\quad b''_{\lambda'}(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}) \cdot \theta_{\lambda'} \in \mathcal{O}_{v^*},\\[1ex]
&\eta_1, \dots, \eta_\mu \notin \mathcal{O}_{v^*}
\end{aligned}$$

and $v^*(b'_1(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*) \cdot \beta_1 - \delta_l^2) > 0$ for all $l \in \{1, \dots, \lambda'\}$.

By Lemma 1.1.61, for every intermediate field $\tilde{K}(x_1, \dots, x_s) \subset N \subsetneq H^*$ which is relatively algebraically closed in H^*, the elements of $H^* \backslash N$ lie dense in H^*. Since also $\operatorname{trdeg}(H^*/\tilde{K}(x_1, \dots, x_s)) = \tilde{t} - s$, we can find (inductively) $x^*_{s+1}, \dots, x^*_{\tilde{t}} \in H^*$, algebraically independent over $\tilde{K}(x_1, \dots, x_s)$, satisfying the conditions above.

We now consider the field $F^* := \tilde{K}(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*)$ with the restrictions of v^* and P^*. Then the rational rank of the value group of (F^*, v^*) is r, since H^*/F^* is algebraic, and F^* is isomorphic to $\tilde{F}$, since

$$f(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*) = 0 = f(x_1, \dots, x_s, x_{s+1}, \dots, x_{\tilde{t}}, y).$$

Pulling back v^* from F^* to $\tilde{F}$ via this ismorphism yields an Abhyankar valuation w of $\tilde{F}/\tilde{K}$ with residue field K^* and rational rank r such that w is compatible with the pullback Q of P^*. We have $a_1, \ldots, a_\mu \subset \mathcal{O}_w$, $b_1, \ldots, b_\lambda \in \mathcal{O}_w^\times \cap Q$ and, for all $k \in \{1, \ldots, \mu\}$, $\overline{a_k}^w = \overline{a_k}^v$. For all $j \in \{1, \ldots, \sigma\}$, we have that $w(c_j)$ is not divisible by m_j in Γ_w. This follows from $c_1, \ldots, c_\sigma \in K(c_1, \ldots, c_s) \subset F^*$ and the fact that restricting the valuation to a smaller field does not effect the non-divisibility of a value by some integer. By restricting w and Q to F, we get the desired Abhyankar valuation of F/K and the desired subset of F.

q.e.d.

The following lemma will help us to use the Local Uniformization Theorem 1.3.1 to prove Lemma 2.2.1 for valuations of arbitrary rank.

2.2.2 **Lemma:**

Let K be a field of characteristic 0, and let F be a function field of degree $t \geqslant 1$ over K. Suppose there exist elements $x_1, \ldots, x_t \in F$, algebraically independent over K, and elements $y_1, \ldots, y_m \in F$, algebraic over $K(x_1, \ldots, x_t)$, such that

- $F = K(x_1, \ldots, x_t, y_1, \ldots, y_m)$ and
- for all $j \in \{1, \ldots, m\}$, there exists an irreducible polynomial $g_j \in K[X_1, \ldots, X_t, Y_j, \ldots, Y_m]$ of Y_j-degree s_j such that $g_j(x_1, \ldots, x_t, y_j, \ldots, y_m) = 0$, $g_j(x_1, \ldots, x_t, Y_j, y_{j+1}, \ldots, y_m)$ is irreducible in $K(x_1, \ldots, x_t, y_{j+1}, \ldots, y_m)[Y_j]$ and $g(0, \ldots, 0, Y_j, 1, \ldots, 1) = u_j(Y_j - 1)Y_j^{s_j}$ for some $u_j \in K^\times$, hence $g_j(0, \ldots, 0, 1 \ldots, 1) = 0$ but $\frac{\partial}{\partial Y_j} g_j(0, \ldots, 0, 1, \ldots, 1) \neq 0$.

Let w be a valuation of $K(x_1, \ldots, x_t)/K$ such that $x_1, \ldots, x_t \subset \mathfrak{m}_w$ and the value group of w is $\mathbb{Z}w(x_1) \oplus \cdots \oplus \mathbb{Z}w(x_t)$, equipped with an arbitrary ordering. Then the residue field of w is K and there exists an immediate extension of w to F (which we also denote by w) such that $y_1, \ldots, y_m \in \mathcal{O}_w^\times$ and $\overline{y_1}^w = \cdots = \overline{y_m}^w = 1$.

Proof:

By Theorem 1.1.42, the residue field of w is K. From the properties of g_m, it follows that $g_m(x_1, \ldots, x_t)$ is irreducible in $\tilde{K}(x_1, \ldots, x_t)[Y_m]$ and its leading coefficient is a unit in $\mathcal{O}_w$, hence the irreducible polynomial of y_m over $K(x_1, \ldots, x_t)$ lies in $\mathcal{O}_w[Y_m]$, and its residue polynomial has the simple root 1 in $\overline{K(x_1, \ldots, x_t)}^w = K$. Thus, by Theorem 1.1.49 (iii), in the henselization of $(K(x_1, \ldots, x_t), w)$, we find a conjugate y^* of y_m with residue class 1. Without loss of generality we can assume that $y^* = y_m$, since otherwise we could pull back the valuation through an automorphism σ of the algebraic closure of $K(x_1, \ldots, x_t)$ that maps y_m on y^*. We restrict the valuation from the henselization to $K(x_1, \ldots, x_t, y_m)$, and we will denote the restriction again by w. Note that the extension $(K(x_1, \ldots, x_t, y_m), w)/(K(x_1, \ldots, x_t), w)$ is immediate. The statement now follows by induction.

q.e.d.

We will now state the main theorem of this chapter, a generalization of Lemma 2.2.1. Here we transform a valuation of arbitrary rank to an Abhyankar valuation for which we can now also prescribe an ordering of the value group.

2.2.3 **Theorem:**

Let K be a field of characteristic 0, and let F be a function field over K. Let v be a valuation of F/K.
Let P be a subset of F such that $P = F$ or P is an ordering of F such that v is compatible with P.
Let $a_1, \ldots, a_\mu \in \mathcal{O}_v$, and let $b_1, \ldots, b_\lambda \in \mathcal{O}_v^\times \cap P$.
Let $c_1, \ldots, c_\sigma \in F^\times$ and $m_1, \ldots, m_\sigma \in \mathbb{Z}\backslash\{0\}$ such that, for all $j \in \{1, \ldots, \sigma\}$, we have that $v(c_j)$ is not divisible by m_j in Γ_v.
Let $t \in \mathbb{N}$ be the transcendence degree of F over K, let s be the maximal number of $\mathbb{Z}$-linearly independent values in $\{v(c_1), \ldots, v(c_\sigma)\}$, and let m be the maximal number of elements in $\{\overline{a_1}^v, \ldots, \overline{a_\mu}^v\}$ which are algebraically independent over K. Let $r \in \mathbb{N}$ such that $\max\{1, s\} \leqslant r \leqslant t - m$, and let $\leqslant$ be an arbitrary ordering of the group $\mathbb{Z}^r$.
Then there exists some Abhyankar valuation w of F/K and some subset Q of F such that

- the value group Γ_w is isomorphic to $(\mathbb{Z}^r, \leqslant)$,
- $Q = F$ if $P = F$, otherwise Q is an ordering of F and w is compatible with Q,
- $K(\overline{a_1}^v, \ldots, \overline{a_\mu}^v) \subset \overline{F}^w$ and $\overline{Q}^w \cap K(\overline{a_1}^v, \ldots, \overline{a_\mu}^v) = \overline{P}^v \cap K(\overline{a_1}^v, \ldots, \overline{a_\mu}^v)$,
- $a_1, \ldots, a_\mu \in \mathcal{O}_w$ and $\overline{a_k}^w = \overline{a_k}^v$ $(k = 1, \ldots, \mu)$,
- $b_1, \ldots, b_\lambda \in \mathcal{O}_w^\times \cap Q$ and
- $w(c_j)$ is not divisible by m_j in Γ_w $(j = 1, \ldots, \sigma)$.

Proof:

We first construct an Abhyankar valuation that has the last four properties and rational rank $\tilde{t} := t - \operatorname{trdeg}(\overline{F}^v/K)$. Then, using local uniformization, we switch to an Abhyankar valuation with rank 1 and rational rank $\tilde{t}$ and at last, we use Lemma 2.2.1 and again local uniformization to construct the desired Abhyankar valuation.

We may assume that $c_1, \ldots, c_\sigma \in P$ and that the values $v(c_1), \ldots, v(c_s)$ are $\mathbb{Z}$-linearly independent. Then, for $s < k \leqslant \sigma$, we have $\alpha_0 v(c_k) = \sum_{1 \leqslant j \leqslant s} \alpha_j v(c_j)$ for some $(\alpha_0, \ldots, \alpha_s) \in \mathbb{Z}^s$ with $\alpha_0 \neq 0$, hence $b_{\lambda+k-s} := c_k^{\alpha_0} \prod_{1 \leqslant j \leqslant s} c_j^{-\alpha_j} \in \mathcal{O}_v^\times \cap P$. So, if $b_{\lambda+k-s} \in \mathcal{O}_w^\times$ and $\alpha_0 m_k \nmid w(\prod_{1 \leqslant j \leqslant s} c_j^{\alpha_j})$ in Γ_w for some valuation w of F, then $\alpha_0 w(c_k) = w(\prod_{1 \leqslant j \leqslant s} c_j^{\alpha_j})$, and therefore $m_k \nmid w(c_k)$. We therefore may replace m_k by $\alpha_0 m_k$ and c_k by $\prod_{1 \leqslant j \leqslant s} c_j^{\alpha_j} \in K(c_1, \ldots, c_s)$. Set $\lambda' := \lambda + \sigma - s$.

We may also assume that $a_1, \dots, a_\mu \neq 0$. In the first part of the proof, we will not distinguish between the elements $a_1, \dots, a_\mu$ and $b_1, \dots, b_{\lambda'}$. For $l \in \{1, \dots, \lambda'\}$, let $a_{\mu+l} := b_l$. Set $\mu' := \mu + \lambda'$.

We embed $\overline{F}^v$ into the henselization (H, v) of (F, v). Set $\tilde{K} := \overline{F}^v$ and let $\tilde{F}$ be the compositum of F and $\tilde{K}$ in H. The elements $x_1 := c_1, \dots, x_s := c_s \in F \subset \tilde{F}$ are algebraically independent over $\tilde{K}$ (Theorem 1.1.42), hence they can be extended to a transcendence basis $x_1, \dots, x_{\tilde{t}}$ of $\tilde{F}/\tilde{K}$. The extension $\tilde{F}/\tilde{K}(x_1, \dots, x_{\tilde{t}})$ is finite, thus we have that $\tilde{F} = \tilde{K}(x_1, \dots, x_{\tilde{t}}, y)$, where y is algebraic over $\tilde{K}(\underline{x})$. Let $f(X_1, \dots, X_{\tilde{t}}, Y) \in \tilde{K}[X_1, \dots, X_{\tilde{t}}, Y]$ be an irreducible polynomial with $f(\underline{x}, y) = 0$ and $\frac{\partial}{\partial Y} f(\underline{x}, y) \neq 0$.

Let $\{q_1, \dots, q_v\}$ be the set of all prime factors of the numbers $m_1, \dots, m_\sigma$. Take two distinct elements $\gamma_1, \gamma_2 \in \Gamma_v$ such that $\gamma_1 < \gamma_2$ and such that there exists some prime number $q \in \{q_1, \dots, q_v\}$ with the property that no element $\eta \in \Gamma_v$ with $\gamma_1 < q \cdot \eta < \gamma_2$ exists.

Let Λ be the q-divisible hull of Γ_v, and let Δ be a $\mathrm{card}\Lambda^+$-saturated elementary extension of Λ (see Remark 2.1.43). Set

$$\Phi := \{nx \neq \gamma \mid n \in \mathbb{N},\ n \geqslant 1,\ \gamma \in \Gamma_v\} \cup \{\gamma_1 < qx < \gamma_2\},$$

where x is a variable. By Lemma 2.1.39, Φ is a type of Λ, since every finite subset of Φ is realizable in Λ. Hence, Φ is realized in Δ by some $\delta \in \Delta$, i.e., $n\delta \notin \Gamma_v$ for all $n \in \mathbb{N}$ with $n \geqslant 1$ and $\gamma_1 < q\delta < \gamma_2$. Set $\Omega := \Gamma_v \oplus \mathbb{Z}\delta$ and let $\leqslant$ be the restriction of the ordering of Δ to Ω.

Consider the field $\tilde{F}(X)$, where X is an indeterminate. By Proposition 1.1.41, there exists exactly one valuation $\tilde{v}\colon \tilde{F}(X) \to \Omega \cup \{\infty\}$ such that $\tilde{v}$ extends v and $\tilde{v}(X) = \delta$. The proposition also tells us that the value group of $\tilde{v}$ is Ω and the residue field of $(\tilde{F}(X), \tilde{v})$ remains $\tilde{K}$. Note that this extension of the value group has no effect on the divisibility of elements in Γ_v.

In the same way, we iteratively adjoin indeterminates until we get a possibly infinite purely transcendental extension (N, u) of $(\tilde{F}, v)$ having $\tilde{K}$ as its residue field, and such that $q \cdot u(N^\times)$ is dense in $u(N^\times)$ for all prime numbers $q \in \{q_1, \dots, q_v\}$. Let T be the transcendence basis of N over F consisting of all adjoined indeterminates. Let (H', u') be a henselian extension of $(H(N), u)$ such that the residue field remains $\tilde{K}$ and the value group Γ' of (H', u') is an extension of $u(N^\times)$ which is p-divisible for all prime numbers $p \notin \{q_1, \dots, q_v\}$. As described in Lemma 2.2.1, this can be done by iteratively adjoining p-th roots ($p \notin \{q_1, \dots, q_v\}$). Note that now $p\Gamma'$ is dense in Γ' for all prime numbers p, but for all $\gamma \in \Gamma_v$, if $\pi \nmid \gamma$ in Γ_v for some product π of prime numbers in $\{q_1, \dots, q_v\}$, then $\pi \nmid \gamma$ in Γ'. In particular, for all $j \in \{1, \dots, \sigma\}$, we have that $u'(c_j)$ is not divisible by m_j in Γ'. From the denseness of $p\Gamma'$ for all prime numbers p, it follows that Γ' is regularly dense (Remark 2.1.51).

Let L be the relative algebraic closure of $\tilde{K}(x_1, \dots, x_s, T)$ in H'. Then $\Gamma'/u'(L^\times)$ is torsion-free: Assume that there exist $a \in H'^\times$ and $b \in L^\times$ such that $nu'(a) = u'(b)$ for some $n \in \mathbb{N}$ such that $n > 1$. Then $u'(\frac{a^n}{b}) = 0$. Let $c \in (\overline{H'}^{u'})^\times = \tilde{K}^\times \subset L^\times$ be the residue class of $\frac{a^n}{b}$. We now consider the polynomial $h(T) = T^n - \frac{a^n}{bc}$ and use Theorem 1.1.49. Since $\overline{h(T)}^{u'} = T^n - 1$ has the simple root 1 in $\overline{H'}^{u'}$, there exists some $d \in H'$ such that $h(d) = 0$ and $u'(d) = 0$. Thus, $d^n = \frac{a^n}{bc}$, i.e., $\frac{a^n}{d^n} - bc = 0$, and hence $\frac{a}{d} \in L$, since L is relatively algebraically closed in H'. Therefore we have that $u'(a) = u'(\frac{a}{d}) \in v'(L^\times)$.

The following holds:

1. (L, u') is henselian (see Corollary 1.1.51).
2. $\overline{L}^{u'} = \tilde{K}$, and thus it is existentially closed in $\overline{H'}^{u'} = \tilde{K}$.
3. The value group $u'(L^\times)$ is regularly dense. Since $\Gamma'/u'(\tilde{L}^\times)$ is torsion-free, $u'(L^\times)$ is existentially closed in Γ' (see Example 2.1.50).

For all $k \in \{1, \dots, \mu'\}$, write $a_k = \frac{a'_k(\underline{x}, y)}{a''_k(\underline{x})}$ where $a'_k \in \tilde{K}[\underline{X}, Y]$ and $a''_k \in \tilde{K}[\underline{X}]$ with $a'(\underline{x}, y), a''_k(\underline{x}) \neq 0$. Let $\overline{a_k} := \overline{a_k}^v \in \tilde{K}$ $(k = 1, \dots, \mu')$. Again, we use the Ax-Kochen-Ershov Principle (2.1.53) to find elements $x'_{s+1}, \dots, x'_{\tilde{t}}, y', \zeta', \alpha'_1, \dots, \alpha'_{\mu'}, \eta'_1, \dots, \eta'_{\mu'} \in L$ which satisfy the following:

$$
\begin{aligned}
f(x_1, \dots, x_s, x'_{s+1}, \dots, x'_{\tilde{t}}, y') = 0,\\
\frac{\partial}{\partial Y} f(\underline{x}, \underline{x'}, y') \cdot \zeta - 1 = 0,\\
a''_1(\underline{x}, \underline{x'}) \cdot \alpha_1 - 1 = 0, \dots, a''_{\mu'}(\underline{x}, \underline{x'}) \cdot \alpha_{\mu'} - 1 = 0,\\
(a'_1(\underline{x}, \underline{x'}, y') \cdot \alpha_1 - \overline{a_1}) \cdot \eta_1 - 1 = 0, \dots, (a'_{\mu'}(\underline{x}, \underline{x'}, y') \cdot \alpha_{\mu'} - \overline{a_{\mu'}}) \cdot \eta_{\mu'} - 1 = 0,\\
a'_1(\underline{x}, \underline{x'}, y') \cdot \alpha_1 - \overline{a_1}, \dots, a'_{\mu'}(\underline{x}, \underline{x'}, y') \cdot \alpha_{\mu'} - \overline{a_{\mu'}} \in \mathcal{O}_{u'},\\
\eta_1, \dots, \eta_{\mu'} \notin \mathcal{O}_{u'}.
\end{aligned}
$$

We consider the field $L' := \tilde{K}(\underline{x}, \underline{x'}, y', \zeta', \underline{\alpha'}, \underline{\eta'})$ together with the restriction of u' coming from L, which is now an Abhyankar valuation of $L'/\tilde{K}$.

Let $L^* = L'(S_1, \dots, S_{\tilde{t}-t'})$ be the rational function field in $\tilde{t} - t'$ indeterminates over L', where t' is the transcendence degree of L' over $\tilde{K}$. By Proposition 1.1.41, the valuation u' can be uniquely extended to L^* in such a way that the value group is $u'(L'^\times) \times \mathbb{Z}^{\tilde{t}-t'}$ (with an arbitrary extension of the ordering of $u'(L'^\times)$) and the residue field is $\tilde{K}$. Denote the extension of the valuation u' by u^*. Note that the extension of the value group has no effect on the divisibility of the elements in $u'(L'^\times)$. Note also that the rational rank of $u^*(L^*)$ is $\tilde{t}$, so u^* is an Abhyankar valuation of $L^*/\tilde{K}$.

Let (H^*, u^*) be the henselization of (L^*, u^*). Using the Implicit Function Theorem, we can find $x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*, \zeta^*, \alpha^*_1, \dots, \alpha^*_{\mu'}, \eta^*_1, \dots, \eta^*_{\mu'} \in H^*$ satisfying the conditions above (with $\mathcal{O}_{u'}$ replaced by $\mathcal{O}_{u^*}$) and having the property that $x^*_{s+1}, \dots, x^*_{\tilde{t}}$ are algebraically independent over $\tilde{K}(x_1, \dots, x_s)$.

We now consider the field $F^* := \tilde{K}(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*)$ with the restriction of u^*. Then the rational rank of the value group of (F^*, u^*) is $\tilde{t}$ and F^* is isomorphic to $\tilde{F}$, since

$$f(x_1, \dots, x_s, x^*_{s+1}, \dots, x^*_{\tilde{t}}, y^*) = 0 = f(x_1, \dots, x_s, x_{s+1}, \dots, x_{\tilde{t}}, y).$$

Pulling back u^* from F^* to $\tilde{F}$ yields an Abhyankar valuation w' with residue field $\tilde{K}$ and rational rank $\tilde{t}$. We have $a_1, \ldots, a_{\mu'} \subset \mathcal{O}_{w'}$ and, for all $k \in \{1, \ldots, \mu'\}$, $\overline{a_k}^{w'} = \overline{a_k}^{v}$. For all $j \in \{1, \ldots, \sigma\}$, we have that $w'(c_j)$ is not divisible by m_j in $\Gamma_{w'}$. Restricting w' to F preserves these properties. The residue field of (F, w') is contained in $\tilde{K} = \overline{F}^{v}$.

By Theorem 1.3.1, there exist a finite extension $\hat{F}$ of F with $\hat{K} := \overline{F}^{w'} \subset \hat{F}$, elements $\hat{x}_1, \ldots, \hat{x}_{\tilde{t}} \in F$, algebraically independent over $\hat{K}$, elements $y_1, \ldots, y_{\tilde{m}} \in \hat{F}$, algebraic over $\hat{K}(\hat{x}_1, \ldots, \hat{x}_{\tilde{t}})$, and a valuation w'' on $\hat{F}$ such that

- $\hat{F} = \hat{K}(\hat{x}_1, \ldots, \hat{x}_{\tilde{t}}, y_1, \ldots, y_{\tilde{m}})$,
- w'' is an immediate extension of w',
- $w''(\hat{x}_1), \ldots, w''(\hat{x}_{\tilde{t}})$ generate the value group of w'',
- $\hat{x}_1, \ldots, \hat{x}_{\tilde{t}} \in \mathcal{O}_{w''}$ and $y_1, \ldots, y_{\tilde{m}} \in \mathcal{O}_{w''}^{\times}$ with $\overline{y_j}^{w''} = 1$ for all $j \in \{1, \ldots, \tilde{m}\}$,
- for all $j \in \{1, \ldots, \tilde{m}\}$, there exists an irreducible polynomial $g_j \in \hat{K}[X_1, \ldots, X_{\tilde{t}}, Y_j, \ldots, Y_{\tilde{m}}]$ of Y_j-degree s_j such that $g_j(\hat{x}_1, \ldots, \hat{x}_{\tilde{t}}, y_j, \ldots, y_{\tilde{m}}) = 0$, $g_j(\hat{x}_1, \ldots, \hat{x}_{\tilde{t}}, Y_j, y_{j+1}, \ldots, y_{\tilde{m}})$ is irreducible in $\hat{K}(\hat{x}_1, \ldots, \hat{x}_{\tilde{t}}, y_{j+1}, \ldots, y_{\tilde{m}})[Y_j]$ and $g(0, \ldots, 0, Y_j, 1, \ldots, 1) = u_j(Y_j - 1)Y_j^{s_j}$ for some $u_j \in \hat{K}^{\times}$, hence $g_j(0, \ldots, 0, 1 \ldots, 1) = 0$ but $\frac{\partial}{\partial Y_j} g_j(0, \ldots, 0, 1, \ldots, 1) \neq 0$, and
- each element d of $M := \{a_1, \ldots, a_{\mu'}, c_1, \ldots, c_\sigma\}$ is a product of a unit e_d and a monomial in $\hat{x}_1, \ldots, \hat{x}_{\tilde{t}}$ in the regular local ring which is the localization of the ring $\hat{K}[\hat{x}_1, \ldots, \hat{x}_{\tilde{t}}, y_1, \ldots, y_{\tilde{m}}]$ at the maximal ideal $(\hat{x}_1, \ldots, \hat{x}_{\tilde{t}}, y_1 - 1, \ldots, y_{\tilde{m}} - 1)$. In particular, for all valuations w of $\hat{F}/\hat{K}$ such that $(\overline{\hat{x}_1}^{w}, \ldots, \overline{\hat{x}_{\tilde{t}}}^{w}, \overline{y_1}^{w}, \ldots \overline{y_{\tilde{m}}}^{w}) = (0, \ldots, 0, 1, \ldots, 1)$, we have $e_d \in \mathcal{O}_w^{\times}$ and $\overline{e_d}^{w} = \overline{e_d}^{w''}$ for all $d \in M$.

Using Proposition 1.1.41, we can construct an Abhyankar valuation $\hat{v}$ of $\hat{K}(\hat{x}_1, \ldots, \hat{x}_{\tilde{t}})/\hat{K}$ that has residue field $\hat{K}$ and value group $\mathbb{Z}\hat{v}(\hat{x}_1) \oplus \cdots \oplus \mathbb{Z}\hat{v}(\hat{x}_{\tilde{t}})$, equipped with an arbitrary ordering, such that $\hat{x}_1, \ldots, \hat{x}_{\tilde{t}} \in \mathfrak{m}_{\hat{v}}$. By Lemma 2.2.2, we can find an immediate extension of $\hat{v}$ to $\hat{F}$ that has the property $y_1 - 1, \ldots, y_{\tilde{m}} - 1 \in \mathfrak{m}_{\hat{v}}$. Therefore, it follows that $a_1, \ldots, a_{\mu'} \in \mathcal{O}_{\hat{v}}$ and, for all $k \in \{1, \ldots, \mu'\}$, $\overline{a_k}^{\hat{v}} = \overline{a_k}^{w''} = \overline{a_k}^{v}$. In particular, $b_1, \ldots, b_{\lambda'} \in \mathcal{O}_{\hat{v}}^{\times}$ and $\overline{b_1}^{\hat{v}}, \ldots, \overline{b_{\lambda'}}^{\hat{v}} \in \overline{P}^{v}$. If P is an ordering, so is $\overline{P}^{v}$, since v is compatible with P. Then, by the Baer-Krull Representation Theorem 2.1.18, there exists some ordering $\hat{P}$ of $\hat{F}$ such that $\hat{v}$ is compatible with $\hat{P}$ and $b_1, \ldots, b_{\lambda'} \in \hat{P}$. It also follows that, for all $j \in \{1, \ldots, \sigma\}$, $\hat{v}(c_j)$ is not divisible by m_j in $\Gamma_{\hat{v}} = \mathbb{Z}\hat{v}(\hat{x}_1) \oplus \cdots \oplus \mathbb{Z}\hat{v}(\hat{x}_{\tilde{t}})$. Since $\hat{x}_1, \ldots, \hat{x}_{\tilde{t}} \in F$, we have $\hat{v}(F^{\times}) = \mathbb{Z}\hat{v}(\hat{x}_1) \oplus \cdots \oplus \mathbb{Z}\hat{v}(\hat{x}_{\tilde{t}})$. The properties from above are preserved if we restrict to F.

If we choose the ordering of the value group of $\hat{v}$ to be archimedean, we can use Lemma 2.2.1 to find an Abhyankar valuation with rank 1 and rational rank r with those properties, and then we can again use Theorem 1.3.1 and Lemma 2.2.2 to change the ordering of the value group.

q.e.d.

2.2.4 **Remark:**

Let us make the same assumptions as in the statement of Theorem 2.2.3. The penultimate paragraph in the proof of this theorem shows that it is also possible to find an Abhyankar valuation w of F/K that has the desired properties, but the residue field $\overline{F}^w$ is contained in $\overline{F}^v$, $\overline{Q}^w = \overline{P}^v \cap \overline{F}^w$ and the value group is isomorphic to $\mathbb{Z}^{\tilde{t}}$, equipped with an arbitrary ordering, where $\tilde{t} = t - \operatorname{trdeg}(\overline{F}^v/K)$.

2.2.5 **Remark:**

Again, we make the same assumptions as in the statement of Theorem 2.2.3. Additionally, let $d_1, \ldots, d_\tau \in P$ and we assume that P is an ordering of F. Let $\{\pi_i \mid i \in I\} \subset F \cap P$ be such that $\{v(\pi_i) + 2\Gamma_v \mid i \in I\}$ is a basis of the subspace of the $\mathbb{F}_2$-vector space $\Gamma_v/2\Gamma_v$ that is generated by $v(d_1)+2\Gamma_v, \ldots, v(d_\tau)+2\Gamma_v$. Then we have $2 \nmid v(\prod_{i\in I} \pi_i^{\nu_i})$ for all non-zero $\nu \in \{0,1\}^I$ and, for all $l \in \{1, \ldots, \tau\}$, $d_l = \prod_{i \in I} \pi_i^{\nu_i} e_l^2 u_l$ for some $\nu \in \{0,1\}^I$, some $e_l \in F$ and some $u_l \in \mathcal{O}_v^\times \cap P$.

Now we add the properties $u_1, \ldots, u_\tau \in \mathcal{O}_v^\times \cap P$ and $2 \nmid v(\prod_{i\in I} \pi_i^{\nu_i})$ for all non-zero $\nu \in \{0,1\}^I$ to the given properties that we want to preserve. Note that the the maximal number s' of $\mathbb{Z}$-linearly independent values among the values of the c_j ($j \in \{1, \ldots, \mu\}$) and the $\prod_{i\in I} \pi_i^{\nu_i}$ ($i \in I$) may be greater than the original number s. By Theorem 2.2.3, we find an ordering Q of F and an Abhyankar valuation w of F/K which is compatible with Q and which have the originally given (as listed in the theorem) and the newly added properties, where we have a certain freedom in the choice of the rational rank and the ordering of the value group of w.

In particular, the vectors $w(\pi_i) + 2\Gamma_w$ are linearly independent in $\Gamma_w/2\Gamma_w$. Therefore, we can extend them to an $\mathbb{F}_2$-basis of this vector space. Using the Baer-Krull Representation Theorem 2.1.18, we find an ordering Q' of F such that w is compatible with Q', $\overline{Q'}^w = \overline{Q}^w$ and $\pi_i \in Q'$ for all $i \in I$. Then, for all $l \in \{1, \ldots, \tau\}$, we have $d_l = \prod_{i\in I} \pi_i^{\nu_i} e_l^2 u_l \in Q'$, since $0 \neq \overline{u_l}^w \in \overline{Q}^w = \overline{Q'}^w$.

So, by giving up some of the freedom in the choice of the rational rank (and the ordering) of the value group, we can achieve $d_1, \ldots, d_\tau \in Q$ whenever $d_1, \ldots, d_\tau \in P$.

The following corollary is a generalization of the first part of Theorem 1.2.1.

2.2.6 **Corollary:**

Let K be a field of characteristic 0, and let V be an irreducible affine K-variety. Let P be a K-rational point of V. Then there exists an Abhyankar valuation w of $K(V)/K$ such that w is centered at P, i.e., $K[V] \subset \mathcal{O}_w$ and $\mathfrak{m}_w \cap K[V] = \mathfrak{m}_P$.

Proof:

By Chevalley's Theorem (1.1.3), there exists a valuation v of $K(V)$ which is centered at P, and Theorem 2.2.3 tells us that there exists some Abhyankar valuation w of $K(V)/K$ which is also centered at P.

q.e.d.

2.3 Some Denseness Properties of Abhyankar Valuations

Based on Theorem 2.2.3, we prove the denseness of iterated prime divisors and Abhyankar valuations of rank 1 in a refinement of the Zariski patch topology on the Zariski space.

2.3.1 **Definition:**

Let K be a field of characteristic 0, and let F be a field extension of K. We denote by $S(F/K)$ the set of all equivalence classes of valuations of F/K. $S(F/K)$ is called the **Zariski space** of F/K. As before, we identify a valuation v with its equivalence class. For all $a \in F$ and all natural numbers $n \geqslant 1$, let

1. $\mathcal{U}(a) := \{v \in S(F/K) \mid v(a) = 0\}$,
2. $\mathcal{V}(a) := \{v \in S(F/K) \mid v(a) > 0\}$ and
3. $\mathcal{W}(a,n) := \{v \in S(F/K) \mid n \nmid v(a)\}$.

We consider the so-called **Zariski patch topology** $\tau_{F/K}$ on $S(F/K)$ which is generated by the subbasis that consists of the sets $\mathcal{U}(a)$ and $\mathcal{V}(a)$ for all $a \in F$. We also consider the topology $\tau'_{F/K}$ that is generated by the subbasis that consists of the sets $\mathcal{U}(a)$, $\mathcal{V}(a)$ and $\mathcal{W}(a,n)$ for all $a \in F$ and all $n \in \mathbb{N}$ with $n \geqslant 1$.

2.3.2 **Proposition:**

Let K be a field of characteristic 0, and let F be a field extension of K. Then:

a) The sets $\mathcal{U}(a)$, $\mathcal{V}(a)$ and $W(a,n)$ are closed with respect to both topologies $\tau_{F/K}$ and $\tau'_{F/K}$ for all $a \in F$ and $n \in \mathbb{N}$ such that $n \geqslant 1$.

b) The set $\{v\}$ is closed with respect to both topologies $\tau_{F/K}$ and $\tau'_{F/K}$ for all $v \in S(F/K)$.

c) The topologies $\tau_{F/K}$ and $\tau'_{F/K}$ are Hausdorff.

d) $(S(F/K), \tau_{F/K})$ is compact, and $(S(F/K), \tau'_{F/K})$ is compact if and only if $\tau_{F/K} = \tau'_{F/K}$.

Proof:

a) $\mathcal{U}(0) = \varnothing$, $\mathcal{V}(0) = S(F/K)$ and $\mathcal{W}(0,n) = \varnothing$ for all $n \geqslant 1$. Let $a \in F^\times$ and $n \geqslant 1$. Then $S(F/K)\backslash\mathcal{U}(a) = \mathcal{V}(a) \cup \mathcal{V}(a^{-1})$, $S(F/K)\backslash\mathcal{V}(a) = \mathcal{U}(a) \cup \mathcal{V}(a^{-1})$ and $S(F/K)\backslash\mathcal{W}(a,n) = \bigcup\limits_{b \in F^\times} \mathcal{U}(\frac{a}{b^n})$.

b) Let $v \in S(F/K)$, and let w be in the closure of $\{v\}$. Then $\mathcal{O}_w^\times \subset \mathcal{O}_v^\times$ and $\mathfrak{m}_w \subset \mathfrak{m}_v$, and therefore $\mathcal{O}_w = \mathcal{O}_v$.

c) Let $v, w \in S(F/K)$ such that $v \neq w$, i.e., $\mathcal{O}_v \neq \mathcal{O}_w$. We may assume that there exists some $a \in \mathcal{O}_v$ such that $a \notin \mathcal{O}_w$. Then $v \in \mathcal{U}(a) \cup \mathcal{V}(a)$ and $w \in \mathcal{V}(a^{-1})$, and these two sets are open and disjoint.

d) Let $\bigcup_{i\in I}\mathcal{U}_i$ be a cover of $S(F/K)$ where, for all $i \in I$, $\mathcal{U}_i \in \tau_{F/K}$. Without loss of generality, we may assume that $\mathcal{U}_i = \mathcal{U}(a_{i1}) \cap \cdots \cap \mathcal{U}(a_{in}) \cap \mathcal{V}(b_{i1}) \cap \cdots \cap \mathcal{V}(b_{im})$ for some $a_{i1}, \ldots, a_{in}, b_{i1}, \ldots, b_{im} \in F^{\times}$. Suppose that there is no finite subcover of $S(F/K)$, i.e., for all finite $J \subset I$, there exists an valuation v_J of F/K such that $v_J \in S(F/K)\backslash \bigcup_{j\in J}\mathcal{U}_j$.

Let L be the language of valued fields. Let Σ be the union of the diagram $\mathrm{D}(F)$ of the field F, the axioms of a valued field Σ_{VF}, the set Σ_K of all $L(F)$-sentences

$$a \in \mathcal{O}$$

where $a \in K$,and the set Σ_I of all $L(F)$-sentences

$$\bigvee_{k=1}^{n}(a_{ik} \notin \mathcal{O} \vee a_{ik}^{-1} \notin \mathcal{O}) \vee \bigvee_{k=1}^{n} b_{ik}^{-1} \in \mathcal{O}$$

where $i \in I$. By the Compactness Theorem 2.1.38, Σ has a model, since every finite subset of Σ is a subset of $D(F) \cup \Sigma_{\mathrm{VF}} \cup \Sigma_K \cup \Sigma_J$ for some finite $J \subset I$, and therefore has the model $(F, \mathcal{O}_{v_J})$.

Any model of Σ is a valued field $(L, \mathcal{O}_w)$ such that L/F is a field extension (see Lemma 2.1.39), w is trivial on K and, for all $i \in I$, $w(a_{i1}), \ldots, w(a_{in}) \neq 0$ and $w(b_{i1}), \ldots, w(b_{im}) \leqslant 0$. In particular, the restriction of w to F is a valuation of F/K that lies not in $\bigcup_{i\in I}\mathcal{U}_i$, a contradiction.

Now suppose that $(S(F/K), \tau'_{F/K})$ is compact. To prove the equality of $\tau_{F/K}$ and $\tau'_{F/K}$, it is enough to show that, for all $a \in F^{\times}$ and for all $n \geqslant 1$, the set $\mathcal{W}(a, n)$ already lies in $\tau_{F/K}$. From the prove of a), we know that the with respect to $\tau'_{F/K}$ closed set $S(F/K)\backslash\mathcal{W}(a, n)$ is equal to $\bigcup_{b\in F^{\times}} \mathcal{U}(\frac{a}{b^n})$. Since the sets $\mathcal{U}(\frac{a}{b^n})$ are open with respect to $\tau'_{F/K}$ and $(S(F/K), \tau'_{F/K})$ is compact, we have that $\mathcal{W}(a, n)$ is equal to a finite intersection of complements of sets of the form $\mathcal{U}(\frac{a}{b^n})$. But these sets are open and closed with respect to both topologies (see a)). Hence, $\mathcal{W}(a, n)$ is also open with respect to $\tau_{F/K}$.

q.e.d.

Theorem 2.2.3 immediately yields the following denseness theorem.

2.3.3 **Theorem:**

Let K be a field of characteristic 0, and let F be a function field over K. Then the prime divisors of F/K are dense in $(S(F/K), \tau_{F/K})$. The iterated prime divisors of F/K and the rank-1-Abhyankar valuations of F/K are dense in $(S(F/K), \tau'_{F/K})$.

The denseness of the prime divisors in the Zariski patch topology was first proven by Kuhlmann in [13]. In his article, more denseness results for the Zariski patch topology can be found.

2.3.4 **Corollary:**

Let K be a field of characteristic 0, and let F be a function field over K of degree $t \geqslant 2$. Then $\tau_{F/K} \neq \tau'_{F/K}$. In particular, $(S(F/K), \tau'_{F/K})$ is not compact.

Proof:

Let v be a valuation of F/K with value group $\mathbb{Z} \times \mathbb{Z}$. Let $x, y \in F$ such that $v(x) = (1,0)$ and $v(y) = (0,1)$. Then $2 \nmid v(x), v(y), v(xy)$. If $\tau_{F/K}$ would be equal to $\tau'_{F/K}$, then there would be a prime divisor w of F/K for which also $2 \nmid w(x), w(y), w(xy)$. Since the value group of a prime divisor is (isomorphic to) $\mathbb{Z}$, $w(x)$, $w(y)$ and $w(xy) = w(x) + w(y)$ would all be odd integers, which is impossible.

q.e.d.

2.4 Local-Global Principles in Function Fields over $\mathbb{R}$

We will give an alternative proof of Schülting's version of the Bröcker-Prestel Local-Global Principle 2.1.36 for function fields over $\mathbb{R}$ (see [24]). In our proof Hironaka's theorem on the resolution of singularities in characteristic 0 with normal crossings on a subvariety ([8], Main Theorem II and Corollary 3) is replaced by local uniformization, the Ax-Kochen-Ershov Principle and the Implicit Function Theorem. We additionally consider function fields over archimedean real closed fields.

2.4.1 **Theorem:**

Let F be a function field over a real closed subfield R of $\mathbb{R}$. A regular quadratic form over F is weakly isotropic if and only if it is (weakly) isotropic over $\mathbb{R}$ for every embedding of F into $\mathbb{R}$ and if it is weakly isotropic over the henselizations with respect to all real prime divisors of F/R.

2.4.2 **Remark:**

If $R = \mathbb{R}$, then no embedding of F into $\mathbb{R}$ exists and we can drop this condition.

Using the tightened version of the local-global principle for weak isotropy (Theorem 2.1.37), we can prove an tightened version of Theorem 2.4.1.

2.4.3 **Theorem:**

Let F be a function field over a real closed subfield R of $\mathbb{R}$. A regular quadratic form $\langle a_1, \ldots, a_n \rangle$ over F is weakly isotropic if and only if it is indefinite with respect to every ordering of F, and if it is weakly isotropic over the henselizations with respect to all real prime divisors v of F/R having the property that $2 \nmid v(a_i)$ for some $i \in \{1, \ldots, n\}$.

For both theorems, we will essentially use the same proof with minor changes for the tightened version (indicated in parentheses).

Proof: (Theorem 2.4.1 and Theorem 2.4.3)

If F is not real, then no real valuation exists and every quadratic form is weakly isotropic over F.

If F is real, let $\rho = \langle a_1, \ldots, a_n \rangle$ be a regular quadratic form over F which is not weakly isotropic over F, but which is isotropic over $\mathbb{R}$ for every embedding of F into $\mathbb{R}$ (indefinite with respect to every ordering of F, resp.). Then, by Theorem 2.1.36 (2.1.37, resp.), ρ is not weakly isotropic over the henselization (H, v) with respect to some real valuation v of F which, by Corollary 2.1.19, must be trivial on R (and which has the property that $2 \nmid v(a_i)$ for some $i \in \{1, \ldots, n\}$). By Lemma 2.1.32, this means that every residue form of ρ is not weakly isotropic over the residue field of (H, v) which is equal to the residue field $\overline{F}^v$ of (F, v).

Choose $c_1, \ldots, c_s \in F$ such that their values in Γ_v are pairwise incongruent modulo $2\Gamma_v$ and they yield a complete set of representatives of the subset $\{v(a_i) + 2\Gamma_v \mid i = 1, \ldots, n\}$ of $\Gamma_v/2\Gamma_v$. As a representative of $0 + 2\Gamma_v$, we choose 1. Hence, we have a decomposition $\rho \simeq c_1\rho_1 \perp \cdots \perp c_s\rho_s$, where the regular quadratic forms $\overline{\rho_j}^v = \langle \overline{u_{j1}}^v, \ldots, \overline{u_{jn_j}}^v \rangle$ are the residue forms of ρ (see Definition 2.1.31), which, by assumption, are all not weakly isotropic over $\overline{F}^v$.

By Remark 2.2.4, there exists an Abhyankar valuation w of F/R with a residue field contained in $\overline{F}^v$ and a lexicographically ordered value group $\mathbb{Z}^t$, where $t = \operatorname{trdeg}(F/R) - \operatorname{trdeg}(\overline{F}^v/R)$, such that, for all $i, j \in \{1, \ldots, s\}$ with $i \neq j$, $2 \nmid w(c_i c_j)$ in Γ_w, i.e., the values of the elements $c_1, \ldots, c_s$ are pairwise incongruent modulo $2\Gamma_w$, (if $2 \nmid v(a_i)$ then $2 \nmid w(a_i)$) and $\overline{u_{jk}}^w = \overline{u_{jk}}^v$ for all $j \in \{1, \ldots, s\}$ and all $k \in \{1, \ldots, n_j\}$. Altogether, it follows that the residue forms of ρ w.r.t w are the same as the residue forms w.r.t. v, hence none of them are weakly isotropic over $\overline{F}^w \subset \overline{F}^v$. (Let $x_1, \ldots, x_t \in F$ such that $\Gamma_w = \mathbb{Z}w(x_1) \oplus \cdots \oplus \mathbb{Z}w(x_t)$ with the lexicographical ordering, and let $i \in \{1, \ldots, n\}$ such that $2 \nmid w(a_i) = \nu_1 w(x_1) + \cdots + \nu_t w(x_t)$. We may assume that $x_1, \ldots, x_t, y_1, \ldots, y_m$ satisfy the conditions listed in Theorem 1.3.1 for some $y_1, \ldots, y_m \in \tilde{F}$. Then we may assume that $2 \nmid \nu_1$, since otherwise, if $2 \mid \nu_1$ but $2 \nmid \nu_j$ for some $j > 1$, we may use Lemma 2.2.2 to change the ordering of the value group in such a way that it is again lexicographical, but now the value of x_j is bigger than the other generators.)

Now, given the real iterated prime divisor w of F/R, we can easily construct a real prime divisor of F/R with respect to which none of the residue forms of ρ are weakly isotropic over the residue field: The value group Γ_w of w is $\mathbb{Z}^t$ $(= \mathbb{Z}w(x_1) \oplus \cdots \oplus \mathbb{Z}w(x_t))$ with the lexicographical ordering, hence $\Delta := \{0\} \times \mathbb{Z}^{t-1}$ $(= \{0\} \oplus \mathbb{Z}w(x_2) \oplus \cdots \oplus \mathbb{Z}w(x_t))$ is a convex subgroup of Γ_w. We can split w into two valuations

$$w_1 \colon F \twoheadrightarrow \underbrace{\Gamma_w/\Delta}_{\mathbb{Z}} \cup \{\infty\}$$

and

$$w_2 \colon \overline{F}^{w_1} \twoheadrightarrow \Delta \cup \{\infty\},$$

where w_2 maps $\overline{x}$ to $w(x)$ for all $x \in \mathcal{O}_w^\times$. The residue field of w_2 is the real field $\overline{F}^w$, hence w_2 is real. Thus, by Corollary 2.1.19, $\overline{F}^{w_1}$ must be real, too. Altogether, it follows that w_1 is a real prime divisor of F/R.

From $\mathcal{O}_w \subset \mathcal{O}_{w_1}$, it follows that the henselization H_1 of (F, w_1) is contained in the henselization H_0 of (F, w) (Lemma 1.1.53). Thus, ρ is not weakly isotropic in H_1, since it is not weakly isotropic over H_0. (Let $i \in \{1, \dots n\}$ be the same index as above satisfying $2 \nmid w(a_i) = \nu_1 w(x_1) + \cdots + \nu_t w(x_t)$ and $2 \nmid \nu_1$. Then $2 \nmid \nu_1 w(x_1) + \Delta = \nu_1 w_1(x_1) = w_1(a_i)$.) This completes our proof.

q.e.d.

2.4.4 **Example:**

We consider the same situation as in the examples 1.1.46, 1.1.68 and 1.3.2.

Let $F = \mathbb{R}(X_1, X_2, X_3, X_4, X_5) = \mathbb{R}(x_1, x_2, x_3, x_4, x_5, y_1)$, where $x_1, \dots, x_5, y_1$ as in Example 1.3.1. Additionally to a_1, a_2 and a_3, we define

$$a_4 := X_2, \; a_5 := \frac{X_2(X_3 - 3)}{X_3^3 - X_1}, \; a_6 := \frac{(X_5^2 - X_4^3)(X_3^3 - X_1)X_4^6(1 - X_3)}{X_5^6}.$$

In terms of $x_1, \dots, x_5$ and y_1, we have

$$a_4 = x_3 x_4, \; a_5 = x_3(x_5 - 3), \; a_6 = x_2 x_4(1 - x_5).$$

Consider the regular quadratic form $\rho = \langle a_1, \dots, a_5 \rangle$ and the valuation v defined in Example 1.1.46. By Example 1.3.2 and the last paragraph, the values of the elements $c_1 := x_3 x_4$, $c_2 := x_3$ and $c_3 := x_2 x_4$ yield a complete set of representatives of the set $\{v(a_1) + 2\Gamma_v, \dots, v(a_6) + 2\Gamma_v\}$ and the residue forms over $\overline{F}^v = \mathbb{R}(x_5)$ are

$$\rho_1 = \langle \frac{-2x_5}{-1 - x_5^3}, 1 \rangle, \; \rho_2 = \langle \frac{1}{x_5}, x_5 - 3 \rangle, \; \rho_3 = \langle \frac{1}{x_5}, 1 - x_5 \rangle.$$

ρ_1 is positive definite with respect to every ordering of $\mathbb{R}(x_5)$ where $-1 < x_5 < 0$, ρ_2 is positive definite with respect to every ordering of $\mathbb{R}(x_5)$ where $3 < x_5$ and ρ_3 is positive definite with respect to every ordering of $\mathbb{R}(x_5)$ where $0 < x_5 < 1$. Hence ρ_1, ρ_2 and ρ_3 are not weakly isotropic over $\mathbb{R}(x_5) = \overline{F}^v$, and therefore ρ is not weakly isotropic over the henselization of (F, v) (Corollary 2.1.32). Thus ρ is not weakly isotropic over F. Note that $2 \nmid v(a_3) = 4v(x_1) + 5v(x_2) + 6v(x_3) + 7v(x_4)$.

Using the propositions 1.1.40 and 1.1.41, we can construct a valuation w of $\mathbb{R}(x_1, x_2, x_3, x_4, x_5)$ with lexicographically ordered value group $\mathbb{Z}w(x_2) \oplus \mathbb{Z}w(x_3) \oplus \mathbb{Z}w(x_1) \oplus \mathbb{Z}w(x_4)$ and residue field $\mathbb{R}(x_5) = \overline{F}^v$. As shown in Lemma 2.2.2, since the irreducible polynomial of y_1 over $\mathbb{R}(\underline{x})$ is $f_1(Y) = Y^3 - Y^2 + x_2$, w can be extended immediately to F in such a way that $w(y_1) = 0$ and $\overline{y_1}^w = 1$. Note that w is an iterated prime divisor $w_1 \circ \cdots \circ w_4$ of $F/\mathbb{R}$. The residue forms ρ with respect to w are obviously the same as the residue forms of ρ with respect to v, hence none of them is weakly isotropic in $\overline{F}^w = \overline{F}^v$.

The prime divisor w_1 has value group $\mathbb{Z}w(x_2)/(\{0\} \oplus \mathbb{Z}w(x_3) \oplus \mathbb{Z}w(x_1) \oplus \mathbb{Z}w(x_4))$ and residue field $\mathbb{R}(x_1, x_3, x_4, x_5)$. ρ is not weakly isotropic over the henselization of (F, w), so ρ is not weaky isotropic over the henselization of (F, w_1), and we have that $2 \nmid w_1(a_3) = 5w_1(x_2)$.

Chapter 3

Decidability for Archimedean Quadratic Modules

In this chapter, we prove our main result: the decidability of the property of a finitely generated quadratic module to be archimedean.

3.1 Preliminaries

3.1.1 Quadratic Modules

Schmüdgen proved in [23] the following representation theorem for real polynomials which are strictly positive on a basic closed semialgebraic set.

3.1.1 **Theorem:**

Let $f, h_1, \dots, h_s \in \mathbb{R}[X_1, \dots, X_n]$. If $W_{\mathbb{R}}(h_1, \dots, h_s) := \{x \in \mathbb{R}^n \mid h_1(x) \geqslant 0, \dots, h_s(x) \geqslant 0\}$ is bounded in $\mathbb{R}^n$ and $f > 0$ on $W_{\mathbb{R}}(h_1, \dots, h_s)$, then

$$f = \sum_{\nu \in \{0,1\}^s} h_1^{\nu_1} \cdots h_s^{\nu_s} \cdot \sigma_\nu$$

where σ_ν is a sum of squares in $\mathbb{R}[X_1, \dots, X_n]$.

In [22], Putinar raised the question whether in this case there is even a simpler representation of the form

$$f = \sigma_0 + h_1\sigma_1 + \cdots + h_s\sigma_s$$

where $\sigma_1, \dots, \sigma_s$ are sums of squares in $\mathbb{R}[X_1, \dots, X_n]$.
We first consider generalizations of the set

$$\{\sigma_0 + h_1\sigma_1 + \cdots + h_s\sigma_s \mid \sigma_1, \dots, \sigma_s \text{ are sums of squares in } \mathbb{R}[X_1, \dots, X_n]\}.$$

Let A be a commutative ring with 1. Let $\sum A^2$ be the subset of A containing all sums of squares in A. The following definitions and results can be found in [20] and [2].

3.1.2 **Definition:**

A subset M of A is called a **quadratic module** of A if

$$1 \in M,\ M + M \subset M,\ \left(\sum A^2\right) \cdot M \subset M \text{ and } -1 \notin M.$$

3.1.3 **Example:**

Let $a_1, \ldots, a_s \in A$. Then

$$M(a_1, \ldots, a_s) := \sum A^2 + a_1 \sum A^2 + \cdots a_s \sum A^2$$

is a quadratic module if and only if $-1 \notin M(a_1, \ldots, a_s)$.
If $\frac{1}{2} \in A$, then $-1 \in M(a_1, \ldots, a_s)$ implies that $M(a_1, \ldots, a_s) = A$.

Suppose $A = \mathbb{R}[X_1, \ldots, X_n]$, and let $h_1, \ldots, h_s \in A$. Then from $W_{\mathbb{R}}(h_1, \ldots, h_s) = \{x \in \mathbb{R}^n \mid h_1(x) \geqslant 0, \ldots, h_s(x) \geqslant 0\} \neq \varnothing$, it follows that $M(h_1, \ldots, h_s)$ is a quadratic module.

3.1.4 **Definition:**

A quadratic module M of A is called **archimedean** if, for each $a \in A$, there exists some $n \in \mathbb{N}$ such that $n - a \in M$.

3.1.5 **Lemma:**

Let $\mathbb{R}[X_1, \ldots, X_n]$ be the polynomial ring in n indeterminates over $\mathbb{R}$, and let M be a quadratic module of $\mathbb{R}[X_1, \ldots, X_n]$. Then M is archimedean if and only if there exists some $N \in \mathbb{N}$ such that $N - \sum_{i=1}^{n} X_i^2 \in M$.

In his PhD-Thesis [9], Jacobi extended Schmüdgen's representation theorem to finitely generated archimedean quadratic modules.

3.1.6 **Theorem:**

Let $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]$, and let $W_{\mathbb{R}}(h_1, \ldots, h_s) = \{x \in \mathbb{R}^n \mid h_1(x) \geqslant 0, \ldots, h_s(x) \geqslant 0\}$ be the corresponding semialgebraic set. If $M(h_1, \ldots, h_s)$ is a quadratic module, then $M(h_1, \ldots, h_s)$ is archimedean if and only if $W_{\mathbb{R}}(h_1, \ldots, h_s)$ is bounded and, for all $f \in \mathbb{R}[X_1, \ldots, X_n]$, $f > 0$ on $W_{\mathbb{R}}(h_1, \ldots, h_s)$ implies $f \in M(h_1, \ldots, h_s)$.

In [10], Jacobi and Prestel then gave a valuation theoretic characterization of archimedean quadratic modules.

3.1.7 **Theorem:**

Let $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]$ be such that $M(h_1, \ldots, h_s)$ is a quadratic module. Then $M(h_1, \ldots, h_s)$ is archimedean if and only if $W_{\mathbb{R}}(h_1, \ldots, h_s)$ is bounded and, for all real prime ideals $\mathfrak{p}$ of $\mathbb{R}[X_1, \ldots, X_n]$ and for all real rank-1-valuations v of $F_{\mathfrak{p}} := \mathrm{Quot}(\mathbb{R}[X_1, \ldots, X_n]/\mathfrak{p})$ such that $v(X_i + \mathfrak{p}) < 0$ for some $i \in \{1, \ldots, n\}$, the regular part of the quadratic form $\langle 1 + \mathfrak{p}, h_1 + \mathfrak{p}, \ldots, h_s + \mathfrak{p}\rangle$ is weakly isotropic over the completion of $(F_{\mathfrak{p}}, v)$.

3.1.8 **Remark:**

In view of Lemma 2.1.32, since the completion with respect to a rank-1-valuation is an immediate and henselian extension, we can replace the completion by the henselization in Theorem 3.1.7.

In Theorem 3.1.7, the real prime ideals $\mathfrak{p}$ where $\mathbb{R}[X_1, \ldots, X_n]/\mathfrak{p}$ has Krull dimension 0 or 1 need not to be considered:
If $\mathfrak{p}$ is a real maximal ideal of $\mathbb{R}[X_1, \ldots, X_n]$, then $\mathbb{R}[X_1, \ldots, X_n]/\mathbb{R} = \mathbb{R}$, and this field has no non-trivial real valuation (see Corollary 2.1.19).
If $\mathbb{R}[X_1, \ldots, X_n]/\mathfrak{p}$ has Krull dimension 1, then $F_\mathfrak{p}$ has transcendence degree 1 over $\mathbb{R}$, and is therefore an SAP-field. Then the henselization of $F_\mathfrak{p}$ with respect to some valuation is also an SAP-field. From the compactness of $W_\mathbb{R}(h_1, \ldots, h_s)$, it follows for all real prime ideals of $\mathbb{R}[X_1, \ldots, X_n]$ and all real rank-1-valuations v of $F_\mathfrak{p}$ with $v(X_i + \mathfrak{p}) < 0$ for some $i \in \{1, \ldots, n\}$ that in the henselization of $(F_\mathfrak{p}, v)$, the regular part of the quadratic form $\langle 1+\mathfrak{p}, h_1+\mathfrak{p}, \ldots, h_s+\mathfrak{p}\rangle$ is totally indefinite. Hence, in the case of an SAP-field, this regular quadratic form is always weakly isotropic (see Theorem 2.1.35).

So, in the case $n = 2$, the only real prime ideal that has to be considered is $\{0\}$. For more information about this case, see [2] and [3].

3.1.2 Decidability

We begin with some basic definitions and results of recursion theory, as found in [29], for instance.

3.1.9 **Definition:**

Let $n \in \mathbb{N}$ such that $n \geqslant 1$. A function $\mathbb{N}^n \to \mathbb{N}$ is called **primitive recursive** iff it can be constructed from the constant function $\mathbb{N} \to \mathbb{N}$, $x \mapsto 0$, the projections $\mathbb{N}^m \to \mathbb{N}$, $(x_1, \ldots, x_m) \mapsto x_i$ ($m \in \mathbb{N}\backslash\{0\}$, $i \leqslant m$) and the successor function $\mathbb{N} \to \mathbb{N}$, $x \mapsto x+1$ by finitely many applications of composition and primitive recursion, where the composition of $g\colon \mathbb{N}^s \to \mathbb{N}$ and $h_1, \ldots, h_s\colon \mathbb{N}^m \to \mathbb{N}$ is

$$\mathbb{N}^m \to \mathbb{N},\ (x_1, \ldots, x_m) \mapsto g(h_1(x_1, \ldots, x_m), \ldots, h_s(x_1, \ldots, x_m)),$$

and where from $g\colon \mathbb{N}^m \to \mathbb{N}$ and $h\colon \mathbb{N}^{m+2} \to \mathbb{N}$ primitive recursion yields

$$f\colon \mathbb{N}^{m+1} \to \mathbb{N}, \begin{cases} (x_1, \ldots, x_m, 0) \mapsto g(x_1, \ldots, x_m), \\ (x_1, \ldots, x_m, y+1) \mapsto h(x_1, \ldots, x_m, y, f(x_1, \ldots, x_m, y)). \end{cases}$$

A function $\mathbb{N}^n \to \mathbb{N}$ is called **recursive** iff it can be constructed from the constant function, the projections and the successor function by finitely many applications of composition, primitive recursion and the μ-operator:
Let $g\colon \mathbb{N}^{m+1} \to \mathbb{N}$ such that, for all $x_1, \ldots, x_m \in \mathbb{N}$, there exists some $y \in \mathbb{N}$ with $g(x_1, \ldots, x_m, y) = 0$, i.e. $\mu y[g(x_1, \ldots, x_m, y) = 0] := \min\{y \in \mathbb{N} \mid g(x_1, \ldots, x_m, y) = 0\}$ is always defined. Then we may apply the μ-operator to get

$$\mathbb{N}^m \to \mathbb{N},\ (x_1, \ldots, x_m) \mapsto \mu y[g(x_1, \ldots, x_m, y) = 0].$$

A partial function $\mathbb{N}^n \supset D \to \mathbb{N}$ is called **partial recursive** iff it can be constructed from the constant function, the projections and the successor function by finitely many applications of composition, primitive recursion and the μ-operator which may also be applied to (total) functions g where $\mu y[g(x_1, \ldots, x_m, y) = 0]$ is not defined (and therefore results in a partial function).

Note that total partial recursive functions are recursive.

3.1.10 **Examples:**

The following functions are primitive recursive:

- $+\colon (x, y) \mapsto x + y$, by defining $x + 0 := x$ and $x + (y + 1) := (x + y) + 1$.
- $x \mapsto x \dot{-} 1$, by defining $0 \dot{-} 1 := 0$ and $(x + 1) \dot{-} 1 := x$.
- $\dot{-}\colon (x, y) \mapsto x \dot{-} y$, by defining $x \dot{-} 0 := x$ and $x \dot{-} (y + 1) := (x \dot{-} y) \dot{-} 1$.
- $\cdot\colon (x, y) \mapsto x \cdot y$, by defining $x \cdot 0 := 0$ and $x \cdot (y + 1) := (x \cdot y) + x$.
- $(x, y) \mapsto x^y$, by defining $x^0 := 1$ and $x^{y+1} := (x^y) \cdot x$.

For every partial recursive function, there is an algorithm that describes how to compute this function. Church's Thesis states that every function which is computable via an algorithm is a partial recursive function.

3.1.11 **Definition:**

A subset A of $\mathbb{N}^n$ is called **recursive** or **decidable** iff its characteristic function is recursive. It is called **recursively enumerable** or **semidecidable** iff it is the domain of a partial recursive function.

3.1.12 **Proposition:**

A subset A of $\mathbb{N}^n$ is recursively enumerable if and only if there exists a recursive subset B of $\mathbb{N}^{n+1}$ such that $A = \{(a_1, \ldots, a_n) \mid \exists\, b \in \mathbb{N}\colon (b, a_1, \ldots, a_n) \in B\}$.

3.1.13 **Proposition:**

a) A subset of $\mathbb{N}$ is recursively enumerable if and only if it is the image of a partial recursive function $\mathbb{N} \supset D \to \mathbb{N}$.

b) A subset of $\mathbb{N}$ is recursively enumerable if and only if it is empty or the image of a primitive recursive function from $\mathbb{N}$ to $\mathbb{N}$.

c) An infinite subset of $\mathbb{N}$ is recursively enumerable if and only if it is the image of an injective recursive function from $\mathbb{N}$ to $\mathbb{N}$.

d) A subset of $\mathbb{N}$ is recursive if and only if it finite or the image of a strictly increasing recursive function from $\mathbb{N}$ to $\mathbb{N}$.

3.1.14 **Proposition:**

a) Let A, B be recursive subsets of $\mathbb{N}^n$. Then $A \cup B$, $A \cap B$ and $\mathbb{N}^n \backslash A$ are also recursive.

b) Let A be a recursive subset of $\mathbb{N}^n$, and let B be a recursive subset of $\mathbb{N}^m$. Then $A \times B$ is a recursive subset of $\mathbb{N}^{n+m}$.

c) Let A, B be recursively enumerable subsets of $\mathbb{N}^n$. Then $A \cup B$ and $A \cap B$ are also recursively enumerable.

d) Let A be a recursively enumerable subset of $\mathbb{N}^n$, and let B be a recursively enumerable subset of $\mathbb{N}^m$. Then $A \times B$ is a recursively enumerable subset of $\mathbb{N}^{n+m}$.

e) Let A be a recursively enumerable subset of $\mathbb{N}^{n+1}$. Then $\{b \in \mathbb{N}^n \mid \exists\, c \in \mathbb{N}\colon (b, c) \in A\}$ is a recursively enumerable subset of $\mathbb{N}^n$.

f) Let A be a recursively enumerable subset of $\mathbb{N}$, and let $f\colon \mathbb{N}^n \supset D \to \mathbb{N}$ be a partial recursive function. Then $f^{-1}(A)$ is a recursively enumerable subset of $\mathbb{N}^n$.

3.1.15 **Examples:**

The following sets are recursive:

- the empty set,
- the set of prime numbers,
- $\{x \in \mathbb{N} \mid x = 0\}$,
- $\{(x, y) \in \mathbb{N}^2 \mid x = y\}$,
- $\{(x, y) \in \mathbb{N}^2 \mid x < y\}$ and
- finite subsets of $\mathbb{N}^n$.

Matijasevic proved in [17] the following diophantine characterization of recursively enumerable sets.

3.1.16 **Theorem:**

A subset A of $\mathbb{N}^n$ is recursively enumerable if and only if there is a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ such that

$$A = \{(a_1, \ldots, a_n) \mid \exists\, b_1, \ldots, b_m \in \mathbb{N}\colon f(a_1, \ldots, a_n, b_1, \ldots, b_m) = 0\}.$$

3.1.17 **Proposition:**

A subset A of $\mathbb{N}^n$ is recursive if and only if A and $\mathbb{N}^n \backslash A$ are recursively enumerable.

For other countable sets, recursively enumerable and recursive subsets can be defined using Gödel numbering.

3.1.18 **Definition:**

Let S be a countable set. Then a **Gödel numbering** of S is an injective map $g\colon S \to \mathbb{N}$ such that g is computable (via an algorithm), $g(S)$ is recursive and $g^{-1}\colon g(S) \to S$ is computable.

3.1.19 **Example:**

Let $S = \mathbb{N}^2$, and let $g\colon \mathbb{N}^2 \to \mathbb{N}$, $(m, n) \mapsto 2^m \cdot 3^n$. This map is injective and computable. By the unique factorization of natural numbers into prime numbers, the set $g(S)$ is recursive and the map $g^{-1}\colon g(\mathbb{N}^2) \to \mathbb{N}^2$ is computable.

3.1.20 **Definition:**

Let S and S' be two countable sets, and let g be a Gödel numbering of S and g' be a Gödel numbering of S'.

A map from S to S' is called **recursive** iff the induced map from $g(S)$ to $g'(S')$ is the restriction of a partial recursive function.

A subset A of S is called **recursive** (**recursively enumerable**, resp.) iff the corresponding set $g(A)$ is a recursive (recursively enumerable, resp.) subset of $\mathbb{N}$.

3.1.21 **Remark:**

Using Gödel numbering, the set of rational numbers can be encoded in such a way that the field operations are recursive, and tuples of rational numbers can be encoded in such a way that all polynomials with rational coefficients are recursive.

Given a recursive language L with Gödel numbering g, the set $\Sigma := L \cup \{\wedge, \vee, \neg, \forall, \exists, (,), =, (T_i)_{i\in\mathbb{N}}, \}$ also has a Gödel numbering, say g'. The set of L-formulae is countable and can be encoded using Gödel numbering as follows: Every L-formula is a word of symbols in Σ. Map $\varphi = \sigma_1 \cdots \sigma_m$ to $2^{g'(\sigma_1)}3^{g'(\sigma_2)}5^{g'(\sigma_3)} \ldots p_m^{g'(\sigma_m)}$ where p_m is the m-th prime number. Note that the set of L-sentences is a recursive subset of the set of L-formulae.

Let $L := L_{\mathrm{OR}} := \{+, -, \cdot, 0, 1, <\}$ be the language of ordered rings, and let $L(\mathbb{Q})$ be the extended language of the L-structure $\mathbb{Q}$. Both languages are recursive. Let $(\psi_i)_{i\in\mathbb{N}}$ be a recursive enumberable sequence of $L(\mathbb{Q})$-formulae with free variables $T_1, \ldots, T_m$. Then the map $\mathbb{Q}^m \times \mathbb{N}$ into the set of $L(\mathbb{Q})$-sentences that maps (a, i) to $\psi_i(a)$ is recursive.

In [25], Tarski provided an algorithm that transforms every formula φ in the language $L_{\mathrm{OR}} = \{+, -, \cdot, 0, 1, <\}$ of ordered rings into a quantifier-free formula ψ such that ψ contains only free variables of φ and $\forall(\varphi \leftrightarrow \psi)$ holds in every real closed field. He therefore proved the following theorem.

3.1.22 **Theorem:** (Elimination of Quantifiers)

The theory of real closed fields admits elimination of quantifiers.

3.1.23 **Remark:**

A quantifier-free $L_{\mathrm{OR}}(\mathbb{Q})$-formula with free variables $T_1, \ldots, T_m$ is equivalent over every real closed field to a finite disjunction of finite conjunctions of the form

$$g = 0 \wedge f_1 > 0 \wedge \cdots \wedge f_r > 0,$$

where $g, f_1, \ldots, f_r \in \mathbb{Z}[T_1, \ldots, T_m]$.

As a consequence, we get the following (which can be found in [20]).

3.1.24 **Theorem:** (Tarski's Transfer Principle)

Let R_1 and R_2 be two real closed field, which induce the same ordering on a common subfield K. Let φ be a L_{OR}-formula with free variables $T_1, \ldots, T_m$. Then, for all $a_1, \ldots, a_m \in K$,

$$\varphi(a_1, \ldots, a_m) \text{ holds in } R_1 \iff \varphi(a_1, \ldots, a_m) \text{ holds in } R_2.$$

Altogether, Tarski developed a procedure by which one can decide whether a L_{OR}-sentence holds in a real closed field (or equivalently (by Theorem 3.1.24): in all real closed fields) or not.

3.1.25 **Theorem:**

The set of all $L_{\mathrm{OR}}(\mathbb{Q})$-sentences that hold in a real closed field (all real closed fields) is recursive.

We now extend the definition of a (semi-)decidable subset to powers of real closed fields.

3.1.26 **Definition:**

Let R be a real closed field. Let $m \in \mathbb{N}$ with $m \geqslant 1$.

A subset M of R^m is called **semidecidable** iff there exists a recursively enumerable sequence $(\psi_i)_{i \in \mathbb{N}}$ of formulae in the language of ordered rings with free variables $T_1, \ldots, T_m$ such that $M = \{a \in R^m \mid \exists\, i \in \mathbb{N}\colon \psi_i(a) \text{ holds in } R\}$.

We say that a subset M of R^m is **decidable** iff both M and $R^m \backslash M$ are semidecidable.

3.1.27 **Example:**

Let R be a real closed field. Then $\mathbb{Q}$ is a semidecidable subset of R, since $\mathbb{Q} = \{a \in R \mid \exists\, (m, n) \in \mathbb{N} \times \mathbb{N}\colon n > 0,\ na - m = 0\}$.

3.1.28 **Proposition:**

Let R be a real closed field, and let $m, m' \geqslant 1$.

a) Let M, N be semidecidable subsets of R^m. Then $M \cup N$ and $M \cap N$ are also semidecidable.

b) Let M, N be decidable subsets of R^m. Then $M \cup N$, $M \cap N$ and $R^m \backslash M$ are also decidable.

c) Let M be a semidecidable subset of R^m, and let N be a semidecidable subset of $R^{m'}$. Then $M \times N$ is a semidecidable subset of $R^{m+m'}$.

d) Let M be a decidable subset of R^m, and let N be a decidable subset of $R^{m'}$. Then $M \times N$ is a decidable subset of $R^{m+m'}$.

e) Let M be a semidecidable subset of R^{m+1}. Then $\{b \in R^m \mid \exists\, c \in R\colon (b, c) \in M\}$ is a semidecidable subset of R^m.

f) Let M be a semidecidable (decidable, resp.) subset of R^m, and let R' be a real closed subfield of R. Then $M \cap R'^m$ is a semidecidable (decidable, resp.) subset of R'^m.

g) Let M be a semidecidable (decidable, resp.) subset of R^m. Then $M \cap \mathbb{Q}^m$ is recursively enumerable (recursive, resp.).

Proof:

a) Let A be a recursively enumerable sequence of L_{OR}-formulae corresponding to M, and let B be a recursively enumerable sequence of L_{OR}-formulae corresponding to N. Then $M \cup N = \{a \in R^m \mid \exists\, \psi \in A \cup B\colon \psi(a)$ holds in $R\}$ and $M \cap N = \{a \in R^m \mid \exists\, (\psi, \varphi) \in A \times B\colon (\psi \wedge \varphi)(a)$ holds in $R\}$. Since $A \cup B$ and $A \times B$ are again recursively enumerable, $M \cup N$ and $M \cap N$ are semidecidable.

b) It suffices to show that if M and N are semidecidable, then $M \cup N$ and $M \cap N$ are again semidecidable. This is already included in the proof of a).

c) Let A be a recursively enumerable sequence of L_{OR}-formulae with free variables $T_1, \ldots, T_m$ corresponding to M, and let B be a recursively enumerable sequence of L_{OR}-formulae with free variables $T'_1, \ldots, T'_{m'}$ corresponding to N. We may assume that $\{T_1, \ldots, T_m\} \cap \{T'_1, \ldots, T'_{m'}\} = \varnothing$. Then $M \times N = \{(a, b) \in R^m \times R^{m'} \mid \exists\, (\psi, \varphi) \in A \times B\colon (\psi \wedge \varphi)(a, b)$ holds in $R\}$. Since $A \times B$ is recursively enumerable, $M \times N$ is semidecidable.

d) First we show that $R \times M$ and $M \times R$ are decidable in R^{m+1}. Using c), this follows from the fact that $R^{m+1} \backslash (R \times M) = R \times (R^m \backslash M)$ and $R^{m+1} \backslash (M \times R) = (R^m \backslash M) \times R$.
The general case now follows from c) and

$$R^{m+m'} \backslash (M \times N) = \Big(R^{m+m'} \backslash (M \times R^{m'})\Big) \cup \Big(R^{m+m'} \backslash (R^m \times N)\Big).$$

e) Let $(\psi_i)_{i \in \mathbb{N}}$ be a recursively enumerable sequence of L_{OR}-formulae corresponding to M. Then $\{b \in R^m \mid \exists\, c \in R\colon (b, c) \in M\} = \{b \in R^m \mid \exists\, i \in \mathbb{N}\colon (\exists T_{m+1} \psi_i)(b)$ holds in $R\}$.

f) We can use the same recursively enumerable sequences of L_{OR}-formulae (see Theorem 3.1.24).

g) We only have to consider a semidecidable set M. Let $(\psi_i)_{i\in\mathbb{N}}$ be a recursively enumerable sequence of L_{OR}-formulae corresponding to M. By Remark 3.1.21, the map $\mathbb{Q}^m \times \mathbb{N}$ into the set of $L_{\mathrm{OR}}(\mathbb{Q})$-sentences that maps (a, i) to $\psi_i(a)$ is recursive. Theorem 3.1.25 tells us that the set of $L_{\mathrm{OR}}(\mathbb{Q})$-sentences that hold in R is recursive. Therefore the set $M \cap \mathbb{Q}^m = \{a \in \mathbb{Q}^m \mid \exists\ i \in \mathbb{N}\colon \psi_i(a) \text{ holds in } R\}$ is recursive enumerable (see Proposition 3.1.14).

q.e.d.

3.1.3 Decidability in Polynomial Rings over Real Closed Fields

Let R be a real closed field. Consider the polynomial ring $R[X_1, \ldots, X_n]$ in n indeterminates over R. Let $d \in \mathbb{N}$, and let $R[X_1, \ldots, X_n]_d$ be the set of polynomials of degree less than or equal to d. We fix a well ordering $\preceq$ on the set of monomials in $X_1, \ldots, X_n$ that respects the multiplication (**monomial ordering**), and such that, for all $\nu, \mu \in \mathbb{N}^n$, if $\sum_{i=1}^{n} \nu_i =: |\nu| < |\mu|$ then $X^\nu \prec X^\mu$. For instance, we can use the graded lexicographical orderin. Let $f \in R[X_1, \ldots, X_n]$, and let X^δ be the greatest monomial with respect to the monomial ordering $\preceq$ that occurs in f, i.e., has a non-zero coeffient c_δ in f. Then we call $\delta(f) := \delta$ the **$\preceq$-degree**, $\mathrm{LM}(f) := X^{\delta(f)}$ the **leading monomial** and $\mathrm{LT}(f) := c_{\delta(f)}\mathrm{LM}(f)$ the **leading term** of f. Let $D := \sum_{j=0}^{d} \binom{n+j-1}{j}$ be the number of monomials of degree less than or equal to $d \in \mathbb{N}$. We identify a polynomial of degree $\leqslant d$ with the D-tuple of its coefficients which is induced by the ordering $\preceq$ of the monomials. So, we may consider $R[X_1, \ldots, X_n]_d$ as the power R^D.

3.1.29 **Definition:**

A subset M of $R[X_1, \ldots, X_n]_d^s$ is called **semidecidable** (**decidable**, resp.) iff the corresponding subset of $(R^D)^s$ is semidecidable (decidable, resp.).

3.1.30 **Examples:**

1. The set M of tuples $(h_1, \ldots, h_s) \in R[X_1, \ldots, X_n]_d^s$, such that $W_R(h_1, \ldots, h_s)$ is non-empty, is decidable, since $W_R(h_1, \ldots, h_s) \neq \varnothing$ if and only if there exists some $x \in R^n$ such that $h_1(x) \geqslant 0, \ldots, h_s(x) \geqslant 0$. Replacing the coefficients by variables yields an L_{OR}-formula ψ that defines M. Hence the negation of ψ defines the complement of M, and we have that M is decidable.
2. The set of irreducible polynomials in $R[X_1, \ldots, X_n]$ of degree $\leqslant d$ is decidable, since $f \in R[X_1, \ldots, X_n]_d$ is reducible if and only if there exist polynomials $g, h \in R[X_1, \ldots, X_n]_d \backslash R$ such that $f = gh$.
3. The set $I \cap R[X_1, \ldots, X_n]_d$ is semidecidable for each ideal $I = (f_1, \ldots, f_s)R[X_1, \ldots, X_n]$ of $R[X_1, \ldots, X_n]$.

Other examples can be derived with the help of Gröbner bases. As references for this topic, see [1] and [4].

3.1.31 **Definition:**

Let I be an ideal of $R[X_1, \ldots, X_n]$. Then a **Gröbner basis** G of I with respect to $\preceq$ is a set of generators of I such that the leading terms of the elements of G with respect to $\preceq$ generate the ideal of $R[X_1, \ldots, X_n]$ that is generated by the leading terms of all elements of I.

There exists a multivariate division with remainder dependent on $\preceq$.

3.1.32 **Theorem:**

Let $g_1, \ldots, g_s \in R[X_1, \ldots, X_n]\backslash\{0\}$. Then for every polynomial $f \in R[X_1, \ldots, X_n]$, there exist polynomials $q_1, \ldots, q_s, r \in R[X_1, \ldots, X_n]$ with

$$f = \sum_{j=1}^{s} g_j q_j + r$$

and such that $\delta(g_j q_j) \preceq \delta(f)$ $(1 \leqslant j \leqslant s)$ and no monomial occuring in r is divisible by any of the leading monomials of $g_1, \ldots, g_s$.

If we have such an expression given for f, we call r a **remainder** of f with respect to $g_1, \ldots, g_s$.

For $f, g \in R[X_1, \ldots, X_n]$, we define the polynomial $S(f, g)$ to be $\frac{\mathrm{LT}(g)f - \mathrm{LT}(f)g}{\gcd(\mathrm{LM}(f), \mathrm{LM}(g))}$.

3.1.33 **Theorem:** (Buchberger's Criterion)

Let $g_1, \ldots, g_s \in R[X_1, \ldots, X_n]\backslash\{0\}$. Then $g_1, \ldots, g_s$ are a Gröbner basis of the ideal $(g_1, \ldots, g_s)R[X_1, \ldots, X_n]$ if and only if, for all $j < k$, a remainder of $S(g_j, g_k)$ with respect to $g_1, \ldots, g_s$ is zero.

From this theorem, one can deduce that every ideal of $R[X_1, \ldots, X_n]$ has a finite Gröbner basis.

3.1.34 **Theorem:**

Let G be a Gröbner basis of an ideal of $R[X_1, \ldots, X_n]$. Then, for each polynomial f in $R[X_1, \ldots, X_n]$, there is exactly one remainder of f with respect to G.

Given a Gröbner base of an ideal, it can now be decided whether an element is a member of this ideal or not.

3.1.35 **Corollary:**

Let G be a Gröbner basis of an ideal I of $R[X_1, \ldots, X_n]$. Then, for each polynomial f in $R[X_1, \ldots, X_n]$, we have $f \in I$ if and only if the remainder of f with respect to G is zero.

From these results, the following examples of (semi-)decidable sets can be derived.

3.1.36 **Examples:**

1. Let $I = (f_1, \ldots, f_s)R[X_1, \ldots, X_n]$ be an ideal of $R[X_1, \ldots, X_n]$. By the criterion of Buchberger, the set of all tuples $(g_1, \ldots, g_r) \in R[X_1, \ldots, X_n]_d^r$ that are a Gröbner basis of I is semidecidable.
2. From Corollary 3.1.35, it follows that the set $I \cap R[X_1, \ldots, X_n]_d$ is decidable for each ideal I of $R[X_1, \ldots, X_n]$.
3. Since the membership in an ideal of $\mathbb{R}[X_1, \ldots, X_n]$ is decidable, the inclusion of one ideal in another and the equality of two ideals are also decidable.
4. Let $I = (f_1, \ldots, f_s)R[X_1, \ldots, X_n]$, $J = (h_1, \ldots, h_t)R[X_1, \ldots, X_n]$ be two ideals of $R[X_1, \ldots, X_n]$, then $(I : J) \cap R[X_1, \ldots, X_n]_d$ is decidable, since $I : J = \{f \in R[X_1, \ldots, X_n] \mid fJ \subset I\} = \{f \in R[X_1, \ldots, X_n] \mid fh_1, \ldots, fh_t \in I\}$. Furthermore, the set of all tuples $(g_1, \ldots, g_r) \in R[X_1, \ldots, X_n]_d^r$ that are a Gröbner basis of $I : J$ is semidecidable (see [1], Section 6.2).
5. For every ideal I in $R[X_1, \ldots, X_n]$, it is possible to compute the Krull dimension $\mathrm{Dim}(R[X_1, \ldots, X_n]/I)$ of $R[X_1, \ldots, X_n]/I$ (see [1], Section 6.3), hence, for all $t \leqslant n$, the set of all tuples $(f_1, \ldots, f_s) \in R[X_1, \ldots, X_n]_d^s$, such that the ideal generated by $f_1, \ldots, f_s$ has Krull dimension t, is decidable.
6. According to a lemma of Van den Dries ([26], Chapter IV, Lemma 3.1), the set $\mathrm{Prime}(R[X_1, \ldots, X_n])_d$ of tuples $(f_1, \ldots, f_s) \in R[X_1, \ldots, X_n]_d^s$, such that $I = (f_1, \ldots, f_s)R[X_1, \ldots, X_n]$ is a prime ideal of $R[X_1, \ldots, X_n]$, is semidecidable: I is a prime ideal if and only if there exist some $m \in \{0, \ldots, n\}$, an irreducible polynomial $p \in R[Y_1, \ldots, Y_m, Z]$ of positive Z-degree, polynomials $h_1, \ldots, h_n \in R[Y_1, \ldots, Y_m, Z]$, some $h \in R[Y_1, \ldots, Y_m] \backslash \{0\}$ and $g_1, \ldots, g_m, g \in R[X_1, \ldots, X_n]$ such that
   - $h^d f_j(h_1/h, \ldots, h_n/h) \in pK[Y_1, \ldots, Y_m, Z]$ $(j = 1, \ldots, s)$,
   - $p(g_1, \ldots, g_m, g) \in I$,
   - $(I : h(g_1, \ldots, g_m)R[X_1, \ldots, X_n]) = I$, $I \neq R[X_1, \ldots, X_n]$ and
   - $h(g_1, \ldots, g_m)X_i - h_j(g_1, \ldots, g_m, g) \in I$ $(i = 1, \ldots, n)$.

   The definition of a prime ideal yields the semidecidability of the set $R[X_1, \ldots, X_n]_d \backslash \mathrm{Prime}(R[X_1, \ldots, X_n])_d$, and altogether we have that $\mathrm{Prime}(R[X_1, \ldots, X_n])_d$ is decidable.

3.2 Decidability for Weakly Isotropic Quadratic Forms

We consider the real closed field $\mathbb{R}$, and let $d \in \mathbb{N}$. We fix again a monomial ordering $\preceq$ on the set of monomials in $X_1, \ldots, X_n$ such that, for all $\nu, \mu \in \mathbb{N}^n$, if $|\nu| < |\mu|$ then $X^\nu \prec X^\mu$, and consider $\mathbb{R}[X_1, \ldots, X_n]_d$ as a power of $\mathbb{R}$.

Let $\mathfrak{p}$ be a prime ideal of $\mathbb{R}[X_1,\dots,X_n]$. We want to show that the set of tuples $(f_1,\dots,f_s) \in \mathbb{R}[X_1,\dots,X_n]_d^s$, such that the regular part of the quadratic form $\langle f_1+\mathfrak{p},\dots,f_s+\mathfrak{p}\rangle$ over the function field $F_\mathfrak{p} := \mathrm{Quot}(\mathbb{R}[X_1,\dots,X_n]/\mathfrak{p})$ is non-zero and weakly isotropic, is decidable.

Let $f_1,\dots,f_s \in \mathbb{R}[X_1,\dots,X_n]_d$. Then, by definition, the regular part of $\langle f_1 + \mathfrak{p},\dots,f_s+\mathfrak{p}\rangle$ is non-zero and weakly isotropic over $F_\mathfrak{p}$ if and only if the following holds.

3.2.1 **Weak Isotropy (polynomial ring $\mathbb{R}[X_1,\dots,X_n]$, prime ideal $\mathfrak{p}$ of $\mathbb{R}[X_1,\dots,X_n]$, polynomials $f_1,\dots,f_s \in \mathbb{R}[X_1,\dots,X_n]$):**

There exist some $e \in \mathbb{N}$, some $m \in \mathbb{N}\backslash\{0\}$ and polynomials $g_1,\dots,g_{sm} \in \mathbb{R}[X_1,\dots,X_n]_e$ such that

- there exists some $i \in \{1,\dots,s\}$ with $f_i \notin \mathfrak{p}$ and at least one of the elements $g_{(i-1)m+1},\dots,g_{im}$ is not in $\mathfrak{p}$ but
- $\sum_{i=1}^{s}\sum_{j=(i-1)m+1}^{im} f_i g_j^2 \in \mathfrak{p}$.

From Theorem 2.4.1, it follows that the regular part ρ of $\langle f_1+\mathfrak{p},\dots,f_s+\mathfrak{p}\rangle$ is not weakly isotropic over $F_\mathfrak{p}$ if and only if there exists some prime divisor v of $F_\mathfrak{p}/\mathbb{R}$ such that every residue class form of ρ is not weakly isotropic over $\overline{F_\mathfrak{p}}^v$. We will now use Theorem 1.2.1 to give a valuation-free characterization of the weak isotropy of a regular quadratic form in a function field over $\mathbb{R}$.

3.2.2 **Lemma:**

Let $F = \mathbb{R}(x_1,\dots,x_n)$ be a function field of degree $t \geqslant 1$ over $\mathbb{R}$, and let $\rho = \langle a_1,\dots,a_m\rangle$ be a regular quadratic form over F. There exists a prime divisor v of $F/\mathbb{R}$ such that every residue class form of ρ is not weakly isotropic over $\overline{F}^v$ if and only if the following statement, which we denote by [PDE], holds.

There exists some element $z \in F^{\mathrm{alg}}$ such that
 z is algebraic over F and
  there exist $c_1,\dots,c_t,z',y \in F(z)$ such that
   z' is algebraic over $\mathbb{R}(c_1,\dots,c_{t-1})$ and
   there exists $p \in \mathbb{R}[c_1,\dots,c_{t-1},Z'][c_t,Y]$ such that
    $p(c_1,\dots,c_{t-1},z',c_t,y) = 0$ in $F(z)$,
    $p(c_1,\dots,c_{t-1},z',c_t,Y) \neq 0$,
    $p(c_1,\dots,c_{t-1},z',c_t,Y)$ is irreducible in $\mathbb{R}(c_1,\dots,c_{t-1},z')[c_t,Y]$,
    $p(c_1,\dots,c_{t-1},z',0,1) = 0$ in $K := \mathbb{R}(c_1,\dots,c_{t-1},z')$,
    $\frac{\partial}{\partial Y}p(c_1,\dots,c_{t-1},z',0,1) \neq 0$ in K and
   $x_1,\dots,x_n,z \in \mathbb{R}(c_1,\dots,c_t,z',y)$ and
   there exist $p_1,\dots,p_m,q_1,\dots,q_m \in \mathbb{R}[c_1,\dots,c_{t-1},z'][c_t,Y]$ and
   there exist $\alpha_1,\dots,\alpha_n \in \mathbb{Z}$ such that
    $p_i(0,1) \neq 0 \neq q_i(0,1)$,
    $a_i = c_t^{\alpha_i}\frac{p_i(c_t,y)}{q_i(c_t,y)}$ $(i = 1,\dots,m)$ and

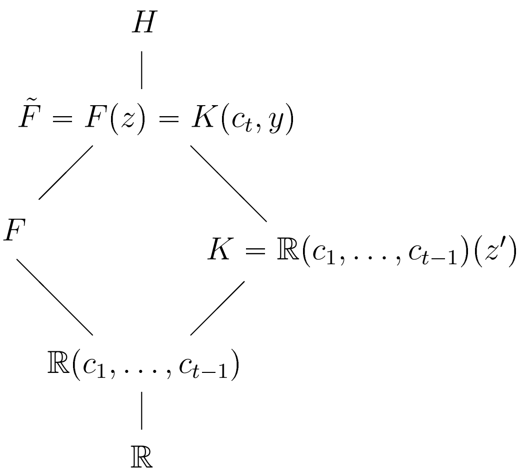
$\langle\frac{p_i(0,1)}{q_i(0,1)} \mid \alpha_i \text{ is even}\rangle$ and $\langle\frac{p_i(0,1)}{q_i(0,1)} \mid \alpha_i \text{ is odd}\rangle$ are not weakly isotropic over K.

Proof:

Suppose there exists a prime divisor v of $F/\mathbb{R}$ such that every residue class form of $\rho = \langle a_1, \ldots, a_m\rangle$ in $\overline{F}^v$ is not weakly isotropic. Let $c_1, \ldots, c_{t-1} \in F$ be such that $\overline{c_1}^v, \ldots, \overline{c_{t-1}}^v$ are algebraically independent over $\mathbb{R}$. Then $c_1, \ldots, c_{t-1}$ are also algebraically independent over $\mathbb{R}$ and we can embed $K := \overline{F}^v$ into the henselization (H, v) of (F, v) in such a way that we can identify c_i with $\overline{c_i}^v$ for all $i \in \{1, \ldots, t-1\}$. Since K is a function field of degree $t-1$ over $\mathbb{R}$, there exists some $z' \in K$ which is algebraic over $\mathbb{R}(c_1, \ldots, c_{t-1})$ such that $K = \mathbb{R}(c_1, \ldots, c_{t-1}, z')$.

We consider the compositum $\tilde{F} := F\overline{F}^v$ in H. Then $\tilde{F}$ is finite over F and a function field in one variable over K, hence there exist $z \in \tilde{F}$ such that z is algebraic over F and $\tilde{F} = F(z)$.

Let $c_t \in F$ be an uniformizing element of v. Then $c_t \in \tilde{F}$ is transcendent over K. By Theorem 1.2.1 and Remark 1.2.2 there exists some $y \in \mathcal{O}_v$ such that $\tilde{F} = K(c_t, y)$, $\overline{y}^v = 1$, and such that $q(0,1) = 0$ but $\frac{\partial}{\partial Y} q(0,1) \neq 0$ holds for an irreducible polynomial $q(X,Y) \in K[X,Y]$ of c_t, y over K.



After multiplying with the least common denominator of the coefficients of q, which lie in $K = \text{Quot}(\mathbb{R}[c_1, \ldots, c_{t-1}, z'])$, we get a polynomial $p(c_1, \ldots, c_{t-1}, z', X, Y) \in \mathbb{R}[c_1, \ldots, c_{t-1}, z'][X, Y]$ such that

$$p(c_1, \ldots, c_{t-1}, z', c_t, y) = 0 \text{ in } \tilde{F},$$

$$p(c_1, \ldots, c_{t-1}, z', c_t, Y) \neq 0,$$

$$p(c_1, \ldots, c_{t-1}, z', c_t, Y) \text{ is irreducible in } K[c_t, Y],$$

$$p(c_1, \ldots, c_{t-1}, z', 0, 1) = 0 \text{ in } K \text{ and}$$

$$\frac{\partial}{\partial Y} p(c_1, \ldots, c_{t-1}, z', 0, 1) \neq 0 \text{ in } K.$$

For $i \in \{1, \ldots, m\}$, write $a_i = c_t^{\alpha_i} b_i$ where $\alpha_i \in \mathbb{Z}$, $b_i \in \mathcal{O}_v^\times$.

By part 1 of Theorem 1.2.1, $\mathcal{O}_v$ must be the unique rank-1-valuation ring $\mathcal{O}$ of $\tilde{F}$ with maximal ideal $\mathfrak{m}$ such that $K \subset \mathcal{O}$ and $\overline{c_t} = 0, \overline{y} = 1 \in K \subset \mathcal{O}/\mathfrak{m}$. By Remark 1.2.2, $\mathcal{O}_v = \{\frac{g(c_t,y)}{h(c_t,y)} \in K(c_t, y) \mid g(c_t, y), h(c_t, y) \in K[c_t, y],\ h(0, 1) \neq 0\}$, and therefore we have $\mathcal{O}_v^\times = \{\frac{g(c_t,y)}{h(c_t,y)} \in K(c_t, y) \mid g(c_t, y), h(c_t, y) \in K[c_t, y],\ g(0, 1) \neq 0 \neq h(0, 1)\}$. Thus, for all $i \in \{1, \ldots, m\}$, $b_i = \frac{p_i}{q_i}$ for some $p_i, q_i \in K[c_t, y]$ such that $p_i(0, 1) \neq 0 \neq q_i(0, 1)$.

It now follows that $\langle \frac{p_i(0,1)}{q_i(0,1)} \mid \alpha_i \text{ is even} \rangle$ and $\langle \frac{p_i(0,1)}{q_i(0,1)} \mid \alpha_i \text{ is odd} \rangle$ are the residue forms of $\rho = \langle a_1, \ldots, a_m \rangle$ with respect to v. By assumption, they are not weakly isotropic in $\overline{\tilde{F}}^v = K = \overline{F}^v$.

Altogether, we have verified that [PDE] holds.

Now suppose [PDE] holds. In particular, we have $F(z) = K(c_t, y)$, where $K = \mathbb{R}(c_1, \ldots, c_{t-1}, z')$, for some $c_1, \ldots, c_t$, algebraically independent over $\mathbb{R}$, some z, algebraic over F, some z', algebraic over $\mathbb{R}(c_1, \ldots, c_{t-1})$, and y which is algebraic over $K(c_t)$. It also follows that $q(0, 1) = 0$ but $\frac{\partial}{\partial Y} q(0, 1) \neq 0$ where $q(X, Y) := p(c_1, \ldots, c_{t-1}, z', X, Y) \in K[X, Y]\backslash\{0\}$, which is an irreducible polynomial of c_t, y over K, since $p(c_1, \ldots, c_{t-1}, z', c_t, y) = 0$. Then, by part 1 of Theorem 1.2.1, there exists a unique discrete rank-1-valuation ring $\mathcal{O}$ of $F(z)$ with maximal ideal $\mathfrak{m}$ such that $K = \mathcal{O}/\mathfrak{m}$, $\overline{c_t}^{\mathcal{O}} = 0, \overline{y}^{\mathcal{O}} = 1 \in K = \mathcal{O}/\mathfrak{m}$, and such that c_t is a generator of $\mathfrak{m}$. Let $v \colon F(z) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ be a valuation of $F(z)$ corresponding to $\mathcal{O}$. Then v is a prime divisor of $F(z)/\mathbb{R}$. Restricting v to F yields a prime divisor of F over $\mathbb{R}$ with residue field $\overline{F}^v$ contained in K. It also follows from [PDE] that all residue forms are not weakly isotropic in K, hence they are all not weakly isotropic in $\overline{F}^v$.

q.e.d.

Let $f_1, \ldots, f_s \in \mathbb{R}[X_1, \ldots, X_n]_d$. A necessary condition for a regular quadratic form to be strongly anisotropic over a field F is that F must be real. So, if the Krull dimension of the given prime ideal $\mathfrak{p}$ is 0 and the regular part of $\langle f_1 + \mathfrak{p}, \ldots, f_s + \mathfrak{p} \rangle$ is strongly anisotropic over $F_\mathfrak{p}$, then $F_\mathfrak{p} = \mathbb{R}$, since $F_\mathfrak{p}$ is algebraic over the real closed field $\mathbb{R}$. Recall that a regular quadratic form over a real closed field is strongly anisotropic if and only if it is (positive or negative) definite. If the Krull dimension of $\mathfrak{p}$ is greater than 0 and the regular part ρ of $\langle f_1 + \mathfrak{p}, \ldots, f_s + \mathfrak{p} \rangle$ is strongly anisotropic over $F_\mathfrak{p}$, then $F_\mathfrak{p}$ is real and, by Theorem 2.4.1, there exists a real prime divisor of the function field $F_\mathfrak{p}$ over $\mathbb{R}$ such that all residue forms of ρ are strongly anisotropic over $\overline{F_\mathfrak{p}}^v$. This field is finitely generated over $\mathbb{R}$ and the transcendence degree of $\overline{F_\mathfrak{p}}^v$ over $\mathbb{R}$ is one less than the transcendence degree of $F_\mathfrak{p}$ over $\mathbb{R}$, so if it is not zero we can use Theorem 2.4.1 again for each of these residue forms. Hence after finitely many uses of Theorem 2.4.1, the transcendence degree over $\mathbb{R}$ is zero, and, as before, the residue field must be equal to $\mathbb{R}$.

Adding the last considerations to the statement of Lemma 3.2.2, we get that the regular part of $\langle f_1 + \mathfrak{p}, \ldots, f_s + \mathfrak{p} \rangle$ is strongly anisotropic over $F_\mathfrak{p}$ if and only if the following holds. (There are two versions of the following statement: *Strong Anisotropy* and *Strong Anisotropy**. Only the latter includes the part between the stars below which adds '$v(X_i + \mathfrak{p}) < 0$ for some $i \in \{1, \ldots, n\}$' to the properties of the prime divisor v of $F_\mathfrak{p}/\mathbb{R}$ whose existence we want to state.)

3.2.3 **Strong Anisotropy(*) (polynomial ring $\mathbb{R}[X_1, \ldots, X_n]$, prime ideal $\mathfrak{p}$ of $\mathbb{R}[X_1, \ldots, X_n]$, polynomials $f_1, \ldots, f_s \in \mathbb{R}[X_1, \ldots, X_n]$):**

One of the polynomials $f_1, \ldots, f_s$ is not in $\mathfrak{p}$, there exists some $t \in \mathbb{N}$ such that $\mathrm{Dim}(\mathbb{R}[X_1, \ldots, X_n], \mathfrak{p}) = t$ and:

If $t = 0$, then there exist $u_1, \ldots, u_n, r_1, \ldots, r_s \in \mathbb{R}$ such that

- $X_i - u_i \in \mathfrak{p}$ for all $i \in \{1, \ldots, n\}$ [1] and
- $f_k - r_k^2 \in \mathfrak{p}$ for all $k \in \{1, \ldots, s\}$ or
  $f_k + r_k^2 \in \mathfrak{p}$ for all $k \in \{1, \ldots, s\}$ [2]

If $t > 0$, then there exists some $e \in \mathbb{N}$ such that there exists an irreducible polynomial $g \in \mathbb{R}[X_1, \ldots, X_{n+1}]_e$ [3] such that

- $g \notin \mathfrak{p}\mathbb{R}[X_1, \ldots, X_{n+1}]$
- $\mathfrak{p}' := (\mathfrak{p}, g) \in \mathrm{Prime}(\mathbb{R}[X_1, \ldots, X_{n+1}])_e$ and:

There exist $\zeta_1, \ldots, \zeta_t, \xi_1, \ldots, \xi_t, \rho', \tau', \rho, \tau \in \mathbb{R}[X_1, \ldots, X_{n+1}]$ such that $\zeta_1, \ldots, \zeta_t, \xi_1, \ldots, \xi_t, \rho', \tau', \rho, \tau \notin \mathfrak{p}'$ and:

(Let S be the multiplicative subset of $\mathbb{R}[X_1, \ldots, X_{n+1}]$ generated by $\xi_1, \ldots, \xi_t, \tau'$ and τ. The natural homomorphism $\mathbb{R}[X_1, \ldots, X_{n+1}] \to S^{-1}\mathbb{R}[X_1, \ldots, X_{n+1}]$, $f \mapsto \frac{f}{1}$, is injective and we have that $S^{-1}\mathfrak{p}'$ is a prime ideal with the property $S^{-1}\mathfrak{p}' \cap \mathbb{R}[X_1, \ldots, X_{n+1}] = \mathfrak{p}'$, since $\xi_1, \ldots, \xi_t, \tau', \tau \notin \mathfrak{p}'$. We consider the subring $\mathbb{R}[\frac{\zeta_1}{\xi_1}, \ldots, \frac{\zeta_t}{\xi_t}, \frac{\rho'}{\tau'}, \frac{\rho}{\tau}]$. Let $\mathfrak{q}$ be the ideal $S^{-1}\mathfrak{p}' \cap \mathbb{R}[\frac{\zeta_1}{\xi_1}, \ldots, \frac{\zeta_t}{\xi_t}, \frac{\rho'}{\tau'}, \frac{\rho}{\tau}]$. [4])

There is an irreducible polynomial $g' \in \mathbb{R}[C_1, \ldots, C_{t-1}, Z']$ such that $g'(\frac{\zeta_1}{\xi_1}, \ldots, \frac{\zeta_{t-1}}{\xi_{t-1}}, \frac{\rho'}{\tau'}) \in \mathfrak{q}$ [5] and:

There exists some polynomial $h \in \mathbb{R}[C_1, \ldots, C_{t-1}, Z', C_t, Y]$ such that

- $h(\frac{\zeta_1}{\xi_1}, \ldots, \frac{\zeta_{t-1}}{\xi_{t-1}}, \frac{\rho'}{\tau'}, \frac{\zeta_t}{\xi_t}, \frac{\rho}{\tau}) \in \mathfrak{q}$,
- $h \notin g'\mathbb{R}[C_1, \ldots, C_{t-1}, Z', C_t, Y]$,
- $(g', h) \in \mathrm{Prime}(\mathbb{R}[C_1, \ldots, C_{t-1}, Z', C_t, Y])_e$ [6]
- $h(\frac{\zeta_1}{\xi_1}, \ldots, \frac{\zeta_{t-1}}{\xi_{t-1}}, \frac{\rho'}{\tau'}, 0, 1) \in \mathfrak{q}$,

[1] I.e., $\mathbb{R}[X_1, \ldots, X_n]/\mathfrak{p} \cong \mathbb{R}$

[2] I.e., the regular part of $\langle f_1 + \mathfrak{p}, \ldots, f_s + \mathfrak{p}\rangle$ is definite.

[3] For the rest of the statement, every 'there exist polynomials such that' should be read as 'there exist polynomials of degree less than or equal to e such that'.

[4] Note that if we write $c \in \mathbb{R}[\frac{\zeta_1}{\xi_1}, \ldots, \frac{\zeta_t}{\xi_t}, \frac{\rho'}{\tau'}, \frac{\rho}{\tau}]$ in the form $\frac{a}{b}$ with $a, b \in \mathbb{R}[X_1, \ldots, X_{n+1}]$ and $b \in S$, then $c \in \mathfrak{q}$ if and only if $a \in \mathfrak{p}'$. So, the membership in the ideal $\mathfrak{q}$ is decidable.

[5] Hence $(g') = \pi'^{-1}(\mathfrak{q})$ where $\pi' \colon \mathbb{R}[C_1, \ldots, C_{t-1}, Z'] \twoheadrightarrow \mathbb{R}[\frac{\zeta_1}{\xi_1}, \ldots, \frac{\zeta_{t-1}}{\xi_{t-1}}, \frac{\rho'}{\tau'}]$, $C_j \mapsto \frac{\zeta_j}{\xi_j}$ and $Z' \mapsto \frac{\rho'}{\tau'}$

[6] Hence $(g', h) = \pi''^{-1}(\mathfrak{q})$ where $\pi'' \colon \mathbb{R}[C_1, \ldots, C_{t-1}, Z', C_t, Y] \twoheadrightarrow \mathbb{R}[\frac{\zeta_1}{\xi_1}, \ldots, \frac{\zeta_{t-1}}{\xi_{t-1}}, \frac{\rho'}{\tau'}, \frac{\zeta_t}{\xi_t}, \frac{\rho}{\tau}]$, $C_j \mapsto \frac{\zeta_j}{\xi_j}$, $Z' \mapsto \frac{\rho'}{\tau'}$ and $Y \mapsto \frac{\rho}{\tau}$.

- $\frac{\partial}{\partial Y}h(\frac{\zeta_1}{\xi_1},\ldots,\frac{\zeta_{t-1}}{\xi_{t-1}},\frac{\rho'}{\tau'},0,1) \notin \mathfrak{q}$ and:

There exist $a_1,\ldots,a_{n+1},b_1,\ldots,b_{n+1} \in \mathbb{R}[C_1,\ldots,C_{t-1},Z',C_t,Y]$ such that

- $b_i(\frac{\zeta_1}{\xi_1}\ldots,\frac{\zeta_{t-1}}{\xi_{t-1}},\frac{\rho'}{\tau'},\frac{\zeta_t}{\xi_t},\frac{\rho}{\tau}) \notin \mathfrak{q}$
- $b_i(\frac{\zeta_1}{\xi_1}\ldots,\frac{\zeta_t}{\xi_{t-1}},\frac{\rho'}{\tau'},\frac{\zeta_t}{\xi_t},\frac{\rho}{\tau})\cdot X_i - a_i(\frac{\zeta_1}{\xi_1}\ldots,\frac{\zeta_{t-1}}{\xi_{t-1}},\frac{\rho'}{\tau'},\frac{\zeta_t}{\xi_t},\frac{\rho}{\tau}) \in S^{-1}\mathfrak{p}'$ [7] and:

There exist $A_1,\ldots,A_s,B_1,\ldots,B_s \in \mathbb{R}[C_1,\ldots,C_{t-1},Z',C_t,Y]$ such that

- $B_k(\frac{\zeta_1}{\xi_1}\ldots,\frac{\zeta_{t-1}}{\xi_{t-1}},\frac{\rho'}{\tau'},\frac{\zeta_t}{\xi_t},\frac{\rho}{\tau}) \notin \mathfrak{q}$
- $B_k(\frac{\zeta_1}{\xi_1}\ldots,\frac{\zeta_{t-1}}{\xi_{t-1}},\frac{\rho'}{\tau'},\frac{\zeta_t}{\xi_t},\frac{\rho}{\tau})\cdot f_k - A_k(\frac{\zeta_1}{\xi_1}\ldots,\frac{\zeta_{t-1}}{\xi_{t-1}},\frac{\rho'}{\tau'},\frac{\zeta_t}{\xi_t},\frac{\rho}{\tau}) \in S^{-1}\mathfrak{p}'$ and:

* * *

For some $i \in \{1,\ldots,n\}$, there exist $p,q \in \mathbb{R}[C_1,\ldots,C_{t-1},Z'][C_t,Y]$ and $\alpha \in \mathbb{N}$ with $\alpha \geqslant 1$ such that

- $p,q \notin (g',h)$
- $p(0,1),q(0,1) \notin g\mathbb{R}[C_1,\ldots,C_{t-1},Z']$
- $C_t^\alpha \cdot a_i \cdot q - b_i \cdot p \in (g',h)$ and:

* * *

There exist $p_1,\ldots,p_s,q_1,\ldots,q_s \in \mathbb{R}[C_1,\ldots,C_{t-1},Z'][C_t,Y]$ and $\alpha_1,\ldots,\alpha_s \in \mathbb{Z}$ such that

- $p_k,q_k \notin (g',h)$ $(k=1,\ldots,s)$
- $p_k(0,1),q_k(0,1) \notin g'\mathbb{R}[C_1,\ldots,C_{t-1},Z']$
- $A_k \in (g',h)$ or
  $\alpha_k \geqslant 0$ and $A_k\cdot q_k - C_t^{\alpha_k}\cdot B_k\cdot p_k \in (g',h)$ or
  $\alpha_k < 0$ and $C_t^{-\alpha_k}\cdot A_k\cdot q_k - B_k\cdot p_k \in (g',h)$
  $(k=1,\ldots,s)$,
- Strong Anisotropy($\mathbb{R}[C_1,\ldots,C_{t-1},Z']$, (g'),
  $\{p_k(0,1)q_k(0,1) \mid A_k \notin (g',h)$ and α_k is even$\}$) and
- Strong Anisotropy($\mathbb{R}[C_1,\ldots,C_{t-1},Z']$, (g'),
  $\{p_k(0,1)q_k(0,1) \mid A_k \notin (g',h)$ and α_k is odd$\}$).

We have shown that, before resolving the projections, the weak isotropy and the strong anisotropy of a regular quadratic form over a function field over $\mathbb{R}$ can be both expressed by a disjunction over a set of "formulae" which differ essentially by the number and degree of the polynomials involved. Applying Proposition 3.1.28 to these "formulae" (in particular, part e) to resolve the projections), we see that both properties can be expressed, respectively, by a disjunction over a recursively enumerable set of L_{OR}-formulae. Altogether, we have shown for every prime ideal $\mathfrak{p}$ of $\mathbb{R}[X_1,\ldots,X_n]$ that the set of tuples $(f_1,\ldots,f_s) \in \mathbb{R}[X_1,\ldots,X_n]_d^s$, such that the regular part of the quadratic form $\langle f_1+\mathfrak{p},\ldots,f_s+\mathfrak{p}\rangle$ over the function field $F_{\mathfrak{p}} := \mathrm{Quot}(\mathbb{R}[X_1,\ldots,X_n]/\mathfrak{p})$ is non-zero and weakly isotropic, is decidable.

[7] Hence, $\mathrm{Quot}(\mathbb{R}[X_1,\ldots,X_{n+1}]/\mathfrak{p}') = \mathrm{Quot}(S^{-1}\mathbb{R}[X_1,\ldots,X_{n+1}]/S^{-1}\mathfrak{p}') = \mathrm{Quot}(\mathbb{R}[\frac{\zeta_1}{\xi_1},\ldots,\frac{\zeta_{t-1}}{\xi_{t-1}},\frac{\rho'}{\tau'},\frac{\zeta_t}{\xi_t},\frac{\rho}{\tau}]/\mathfrak{q}) = \mathrm{Quot}(\mathbb{R}[C_1,\ldots,C_{t-1},Z',C_t,Y]/(g',h))$.

3.3 Decidability for Archimedean Quadratic Modules

We will now prove our main result: We show that it is possible to decide whether a given finitely generated quadratic module is archimedean. At first, we give a new version of the Characterization Theorem of Jacobi and Prestel (3.1.7) where the rank-1-valuations are replaced by prime divisors. Then we apply the results of the last section to conclude the proof.

Similar to our proof of the theorems 2.4.1 and 2.4.3, we apply Theorem 2.2.3 and Remark 2.2.4 on Theorem 3.1.7.

3.3.1 **Theorem:**

Let $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]$ be such that $M(h_1, \ldots, h_s)$ is a quadratic module. Then $M(h_1, \ldots, h_s)$ is archimedean if and only if $W_{\mathbb{R}}(h_1, \ldots, h_s)$ is bounded and, for all real prime ideals $\mathfrak{p}$ of $\mathbb{R}[X_1, \ldots, X_n]$ and for all real prime divisors v of $F_{\mathfrak{p}} := \mathrm{Quot}(\mathbb{R}[X_1, \ldots, X_n]/\mathfrak{p})$, such that $v(X_i + \mathfrak{p}) < 0$ for some $i \in \{1, \ldots, n\}$, the regular part of the quadratic form $\langle 1 + \mathfrak{p}, h_1 + \mathfrak{p}, \ldots, h_s + \mathfrak{p}\rangle$ is weakly isotropic over the henselization of $(F_{\mathfrak{p}}, v)$.

Proof:

Suppose $\rho := \langle 1+\mathfrak{p}, h_1+\mathfrak{p}, \ldots, h_s+\mathfrak{p}\rangle$ is not weakly isotropic in the completion with respect to some real rank-1-valuation v of $F := F_{\mathfrak{p}}/\mathbb{R}$ having the property that $v(X_i + \mathfrak{p}) < 0$ for some $i \in \{1, \ldots, n\}$). By Lemma 2.1.32, every residue form of ρ is not weakly isotropic over the residue field $\overline{F}^v$ of (F, v).

Choose $c_1, \ldots, c_s \in F$ such that their values in Γ_v are pairwise incongruent modulo $2\Gamma_v$ and they yield a complete set of representatives of the subset $\{v(a_i) + 2\Gamma_v \mid i = 1, \ldots, n\}$ of $\Gamma_v/2\Gamma_v$. As a representative of $0 + 2\Gamma_v$, we choose 1. Hence, we have a decomposition $\rho \simeq c_1\rho_1 \perp \cdots \perp c_s\rho_s$, where the regular quadratic forms $\overline{\rho_j}^v = \langle \overline{u_{j1}}^v, \ldots, \overline{u_{jn_j}}^v\rangle$ are the residue forms of ρ (see Definition 2.1.31), which are all not weakly isotropic over $\overline{F}^v$.

By Remark 2.2.4, there exists an Abhyankar valuation w of $F/\mathbb{R}$ with a residue field contained in $\overline{F}^v$ and a lexicographically ordered value group $\mathbb{Z}^t$, where $t = \mathrm{trdeg}(F/\mathbb{R}) - \mathrm{trdeg}(\overline{F}^v/\mathbb{R})$, such that, for all $i, j \in \{1, \ldots, s\}$ such that $i \neq j$, $2 \nmid w(c_ic_j)$ in Γ_w, i.e., the values of the elements $c_1, \ldots, c_s$ are pairwise incongruent modulo $2\Gamma_w$, $w(X_i + \mathfrak{p}) < 0$ and $\overline{u_{jk}}^w = \overline{u_{jk}}^v$ for all $j \in \{1, \ldots, s\}$ and all $k \in \{1, \ldots, n_j\}$. It follows that the residue forms of ρ w.r.t w are the same as the residue forms w.r.t. v, hence none of them is weakly isotropic over $\overline{F}^w \subset \overline{F}^v$.

Let $x_1, \ldots, x_t \in \mathcal{O}_w$ be such that $\Gamma_w = \mathbb{Z}w(x_1) \oplus \cdots \oplus \mathbb{Z}w(x_t)$ with the lexicographical ordering, and let $i \in \{1, \ldots, n\}$ such that $0 > w(X_i + \mathfrak{p}) = \nu_1 w(x_1) + \cdots + \nu_t w(x_t)$. We may assume that $x_1, \ldots, x_t, y_1, \ldots, y_m$ satisfy the conditions listed in Theorem 1.3.1 for some $y_1, \ldots, y_m \in \tilde{F}$. Then we may assume that $\nu_1 < 0$, since otherwise, if $\nu_1 = \cdots = \nu_{j-1} = 0$ but $\nu_j < 0$ for some $j > 1$, we may use Lemma 2.2.2 to change the ordering of the value group in such a way that it is again lexicographical, but now the value of x_j is bigger than the other generators.

Now, given the real iterated prime divisor $w = w_1 \circ \cdots \circ w_t$ of $F/\mathbb{R}$, the real prime divisor w_1 satisfies the following: $w_1(X_i + \mathfrak{p}) < 0$ and $\rho = \langle 1 + \mathfrak{p}, h_1 + \mathfrak{p}, \ldots, h_s + \mathfrak{p}\rangle$ is not weakly isotropic over the henselization of (F, w_1).

q.e.d.

Using Lemma 3.1.5, we immediately see that the set of tuples $(h_1, \ldots, h_s) \in \mathbb{R}[X_1, \ldots, X_n]_d^s$, such that $M(h_1, \ldots, h_s)$ is archimedean, is semidecidable.

3.3.2 **Archimedean (polynomials $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]$):**

There exists some $N \in \mathbb{N}$, some $m \in \mathbb{N}$ and polynomials $f_{jk} \in \mathbb{R}[X_1, \ldots, X_n]_N$ $(0 \leqslant j \leqslant s,\ 1 \leqslant k \leqslant m)$ such that

$$N - \sum_{i=1}^{n} X_i^2 = \sum_{k=1}^{m} f_{0k}^2 + h_1 \sum_{k=1}^{m} f_{1k}^2 + \cdots + h_s \sum_{k=1}^{m} f_{sk}^2.$$

Let $d \in \mathbb{N}$, and let $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]_d$. The set $W_{\mathbb{R}}(h_1, \ldots, h_s)$ is bounded if and only if there exists some $a \in \mathbb{R}$ such that, for all $x_1, \ldots, x_n \in \mathbb{R}$, if $h_1(x_1, \ldots, x_n) \geqslant 0, \ldots, h_s(x_1, \ldots, x_n) \geqslant 0$ then $x_1^2 + \cdots + x_n^2 < a^2$. Therefore, the set of all tuples $(h_1, \ldots, h_s) \in \mathbb{R}[X_1, \ldots, X_n]_d^s$, such that $W(h_1, \ldots, h_s)$ is bounded, is decidable.

From the last subsection, we can conclude that the set of all tuples $(h_1, \ldots, h_s) \in \mathbb{R}[X_1, \ldots, X_n]_d^s$, such that $W_{\mathbb{R}}(h_1, \ldots, h_s)$ is non-empty and $M(h_1, \ldots, h_s)$ is not archimedean, is semidecidable.

3.3.3 **Non-Archimedean (polynomials $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]$):**

$W_{\mathbb{R}}(h_1, \ldots, h_s)$ is non-empty and:
$W_{\mathbb{R}}(h_1, \ldots, h_s)$ is not bounded or there exist some $e \in \mathbb{N}$, some $m \in \mathbb{N}$ and polynomials $f_1, \ldots, f_m \in \mathbb{R}[X_1, \ldots, X_n]_e$ such that

- $(f_1, \ldots, f_m) \in \text{Prime}(\mathbb{R}[X_1, \ldots, X_n])_e$ and
- Strong Anisotropy*$(\mathbb{R}[X_1, \ldots, X_n], (f_1, \ldots, f_m), 1, h_1, \ldots, h_s)$.

Therefore, the set of all tuples $(h_1, \ldots, h_s) \in \mathbb{R}[X_1, \ldots, X_n]_d^s$, such that $W_{\mathbb{R}}(h_1, \ldots, h_s)$ is non-empty and $M(h_1, \ldots, h_s)$ is archimedean, is decidable.

Zusammenfassung auf Deutsch

Schmüdgen zeigte 1991, daß für alle $f, h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]$ gilt: Falls $W_{\mathbb{R}}(h_1, \ldots, h_s) := \{x \in \mathbb{R}^n \mid h_1(x) \geqslant 0, \ldots, h_s(x) \geqslant 0\}$ in $\mathbb{R}^n$ beschränkt und $f > 0$ auf $W_{\mathbb{R}}(h_1, \ldots, h_s)$ ist, so ist

$$f = \sum_{\nu \in \{0,1\}^s} h_1^{\nu_1} \cdots h_s^{\nu_s} \cdot \sigma_\nu$$

für gewisse Quadratsummen σ_ν in $\mathbb{R}[X_1, \ldots, X_n]$.

1993 stellte Putinar die Frage, ob sogar eine einfachere Darstellung der Form

$$f = \sigma_0 + h_1\sigma_1 + \cdots + h_s\sigma_s \quad (*)$$

mit $\mathbb{R}[X_1, \ldots, X_n]$–Quadratsummen $\sigma_1, \ldots, \sigma_s$ möglich ist.

Das Hauptziel unserer Arbeit ist zu zeigen, daß es möglich ist zu *entscheiden*, ob für gegebene Polynome $h_1, \ldots, h_s \in \mathbb{R}[X_1, \ldots, X_n]$ mit $W_{\mathbb{R}}(h_1, \ldots, h_s)$ nichtleer die Menge $W_{\mathbb{R}}(h_1, \ldots, h_s)$ beschränkt ist und sie die einfachere Darstellung für alle Polynome $f \in \mathbb{R}[X_1, \ldots, X_n]$, die strikt positiv auf $W_{\mathbb{R}}(h_1, \ldots, h_s)$ sind, erlauben.

Hierbei bedeutet Entscheidbarkeit insbesondere, daß ein effektives Entscheidungsverfahren (Algorithmus) existiert, das entscheidet, ob $h_1, \ldots, h_s$ diese Eigenschaft haben oder nicht, vorausgesetzt ihre Koeffizienten sind rationale Zahlen. Somit kann man zusätzlich nach einem konkretem Algorithmus fragen.

Für den Fall $n = 1$ kann gezeigt werden, daß nur die Beschränktheit von $W_{\mathbb{R}}(h_1, \ldots, h_s)$ entschieden werden muß, und das ist stets möglich. Canto Cabral gab in ihrer Dissertation 2005 für den Fall $n = 2$ ein effektives Entscheidungsverfahren für alle $h_1, \ldots, h_s$ mit nichtleerer und beschränkter Menge $W_{\mathbb{R}}(h_1, \ldots, h_s)$ an. In dieser Arbeit zeigen wir die Entscheidbarkeit für jede Dimension. Allerdings ist für $n > 2$ kein konkreter Algorithmus in Sicht.

Enorm wichtig für unseren Beweis sind der Darstellungssatz von Jacobi und der Charakterisierungssatz von Jacobi und Prestel:

1999 zeigte Jacobi in seiner Dissertation, daß für alle $h_1, \ldots, h_s \in A := \mathbb{R}[X_1, \ldots, X_n]$ genau dann die Menge $W_{\mathbb{R}}(h_1, \ldots, h_s)$ beschränkt ist und eine einfache Darstellung $(*)$ für alle Polynome f, die strikt positiv auf $W_{\mathbb{R}}(h_1, \ldots, h_s)$ sind, existiert, wenn es ein $N \in \mathbb{N}$ gibt, so daß $N - \sum_{i=1}^n X_i^2$ eine solche Darstellung besitzt. Gilt letztere Aussage, so ist der quadratische Modul $M(h_1, \ldots, h_s) := \sum A^2 + h_1 \sum A^2 + \cdots h_s \sum A^2$ archimedisch.

Jacobi und Prestel bewiesen 2001 eine bewertungstheoretische Charakterisierung der Archimedizität von $M(h_1, \ldots, h_s)$. Diese Charakterisierung besagt, daß

$M(h_1, \ldots, h_s)$ genau dann nicht archimedisch ist, wenn $W_{\mathbb{R}}(h_1, \ldots, h_s)$ nicht beschränkt ist oder es ein reelles Primideal $\mathfrak{p}$ von $\mathbb{R}[X_1, \ldots, X_n]$ und eine reelle Rang-1-Bewertung v des Quotientenkörpers $F_{\mathfrak{p}}$ von $\mathbb{R}[X_1, \ldots, X_n]/\mathfrak{p}$ mit der Eigenschaft $v(X_i + \mathfrak{p}) < 0$ für ein $i \in \{1, \ldots, n\}$ gibt, für die gilt, daß alle Restklassenformen des regulären Teils der quadratischen Form $\langle 1 + \mathfrak{p}, h_1 + \mathfrak{p}, \ldots, h_s + \mathfrak{p} \rangle$ über dem Restklassenkörper von $(F_{\mathfrak{p}}, v)$ nicht schwach isotrop sind. Um die Entscheidbarkeit zu beweisen, geben wir eine bewertungsfreie Aussage (ähnlich zu der in unserer obigen Definition der Archimedizität), die ausdrückt, daß $M(h_1, \ldots, h_s)$ nicht archimedisch ist. Das größte Hindernis dabei ist, daß man mit den oben auftauchenden Bewertungen möglicherweise nicht arbeiten kann. Die Wertegruppe oder der Restklassenkörper müssen nicht endlich erzeugt sein. Deshalb müssen wir zeigen, daß zu jeder solchen *schlechten* Bewertung, eine *gute* Bewertung mit denselben Eigenschaften in der Wertegruppe und im Restklassenkörper existiert.

Für uns sind *gute* Bewertungen die sogenannten Abhyankarbewertungen. Deren Wertegruppe ist ein endliches Produkt von Kopien von $\mathbb{Z}$ und deren Restklassenkörper ist über dem Grundkörper endlich erzeugt. Wir zeigen für Funktionenkörper F über Körpern K der Charakteristik 0, daß wenn wir eine nichttriviale Bewertung auf F gegeben haben, die trivial auf K ist, und wenn wir außerdem endlich viele Eigenschaften dieser Bewertung gegeben haben, wir stets eine Abhyankarbewertung von F finden können, die trivial auf K ist und die gleichen Eigenschaften erfüllt. Außerdem können wir dabei bis zu einem gewissen Grad den Rang und die Anordnung der Wertegruppe der Abhyankarbewertung wählen. Eine Folge davon ist, daß die Abhyankarbewertungen von F, die trivial auf K sind, im Zariskiraum aller K-trivialen Bewertungen von F bezüglich gewisser Hausdorff- (teilweise sogar kompakter) Topologien dicht liegen. Der Beweis dieses Resultats verwendet einen lokalen Uniformisierungssatz für solche Abhyankarbewertungen, nämlich das Ax-Kochen-Ershov-Prinzip aus der Modelltheorie und den bewertungstheoretischen Satz über implizite Funktionen.

Mit diesem Resultat können wir einen Satz von Schülting neu beweisen, welcher eine Verbesserung des Lokal-Global-Prinzips von Bröcker und Prestel für Funktionenkörper über $\mathbb{R}$ ist. Schülting benutzte tiefliegende Resultate von Hironaka um zu zeigen, daß über diesen Körpern die schwache Isotropie einer regulären quadratischen Form lokal nur für Primdivisoren getestet werden muß. Primdivisoren sind Abhyankarbewertungen mit Wertegruppe $\mathbb{Z}$ und genau jene *guten* Bewertungen, die wir anstatt der beliebigen Rang-1-Bewertungen, die weiter oben auftauchten, betrachten wollen. Um dies zu erreichen, modifizieren wir unseren Beweis von Schültings Satz, um den Charakterisierungssatz von Jacobi und Prestel so zu verbessern, daß nur noch Primdivisoren betrachtet werden müssen.

Der Bewertungsring eines Primdivisors ist nach einer endlichen Erweiterung des Funktionenkörpers ein lokaler Ring eines nichtsingulären K-rationalen Punktes einer irreduziblen Kurve, die über dem Restklassenkörper K des Primdivisors definiert ist. Wir haben somit eine schöne Beschreibung dieses Bewertungsringes, mit welcher die Restklassenformen einer gegebenen quadratischen Form leicht zu bestimmen sind. Wir benutzen diese Beschreibung, um die bewertungsfreie Aussage zu erhalten, die die Nichtarchimedizität von $M(h_1, \ldots, h_s)$ ausdrückt.

Mit dieser Aussage erhalten wir schließlich die Entscheidbarkeit.

Diese Arbeit ist folgendermaßen strukturiert:

Sie ist in drei Kapitel aufgeteilt. Im ersten Abschnitt jedes Kapitels geben wir eine Übersicht über die grundlegenden Begriffe, die wir im Hauptteil des Kapitels verwenden.

In Kapitel 1 geben wir einen eigenen Beweis eines bekannten Resultats an, da dieses ein wichtiges Instrument für die restliche Arbeit darstellt. Wir zeigen einen lokalen Uniformisierungssatz für Abhyankarbewertungen: Nach einer endlichen Erweiterung ist der Bewertungsring einer solchen Bewertung an einem regulären lokalen Ring zentriert. Hier und im Folgenden behandeln wir Bewertungen von Funktionenkörpern über Körpern der Charakteristik 0.

In Kapitel 2, Abschnitt 2 zeigen wir, daß es möglich ist, beliebige nichttriviale Bewertungen in Abhyankarbewertungen zu transformieren, und dabei eine endliche Anzahl von Eigenschaften der ursprünglichen Bewertung zu erhalten.

In Abschnitt 3 des Kapitels 2 folgern wir, daß die iterierten Primdivisoren und die Abhyankarbewertungen vom Rang 1 bezüglich einer Verfeinerung der konstruierbaren Topologie im Zariskiraum dicht liegen.

Als eine Anwendung des Resultats aus Abschnitt 2 geben wir in Abschnitt 4 des 2. Kapitels einen neuen Beweis für Schültings Verbesserung des Bröcker-Prestel Lokal-Global-Prinzips für schwache Isotropie regulärer quadratischer Formen über Funktionenkörpern über $\mathbb{R}$ an.

In Kapitel 3, Abschnitt 2 zeigen wir die Entscheidbarkeit der schwachen Isotropie einer regulären quadratischen Form über einem Funktionenkörper über $\mathbb{R}$.

In Abschnitt 3 des Kapitels 3 erhalten wir unser Hauptresultat: Die Entscheidbarkeit der Archimedizität quadratischer Moduln, welche von endlich vielen reellen Polynomen in mehreren Variablen erzeugt werden.

References

[1] T. Becker and V. Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra*. Number 141 in Graduate Texts in Mathematics. Springer-Verlag, 1993.

[2] M. E. Canto Cabral. *Archimedean Quadratic Modules. A Decision Procedure in Dimension Two*. PhD thesis, Universität Konstanz, 2005.

[3] M. E. Canto Cabral and A. Prestel. Quadratic modules of polynomials in two variables. *Advances in Geometry*, 8(2):189 – 204, 2008.

[4] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Number 150 in Graduate Texts in Mathematics. Springer-Verlag, 1995.

[5] G. A. Elliott. On totally ordered groups, and K_0. In D. Handelman and J. Lawrence, editors, *Ring Theory Waterloo 1978*, number 734 in Lecture Notes in Mathematics, pages 1 – 49. Springer-Verlag, 1979.

[6] O. Endler. *Valuation Theory*. Springer-Verlag, 1972.

[7] A. J. Engler and A. Prestel. *Valued Fields*. Springer-Verlag, 2005.

[8] H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. *Annals of Mathematics*, 79:109 – 326, 1964.

[9] T. Jacobi. *Über die Darstellung strikt positiver Polynome auf semialgebraischen Kompakta*. PhD thesis, Universität Konstanz, 1999.

[10] T. Jacobi and A. Prestel. Distinguished representations of strictly positive polynomials. *Journal für die reine und angewandte Mathematik*, 532:223 – 235, 2001.

[11] H. Knaf and F.-V. Kuhlmann. Abhyankar places admit local uniformization in any characteristic. *Annales Scientifiques de l'École Normale Supérieure*, 38:833 – 846, 2005.

[12] W. Krull. Allgemeine Bewertungstheorie. *Journal für die reine und angewandte Mathematik*, 167:160 – 196, 1932.

[13] F.-V. Kuhlmann. On places of algebraic function fields in arbitrary characteristic. *Advances in Mathematics*, 188:399 – 424, 2004.

[14] F.-V. Kuhlmann. Value groups, residue fields, and bad places of rational function fields. *Transactions of the American Mathematical Society*, 356:4559 – 4600, 2004.

[15] F.-V. Kuhlmann and A. Prestel. On places of algebraic function fields. *Journal für die reine und angewandte Mathematik*, 353:181 – 195, 1984.

[16] S. Lang. *Introduction to Algebraic and Abelian Functions*. Addison-Wesley, 1972.

[17] J. V. Matijasevic. Enumerable sets are diophantine. *Soviet Mathematics - Doklady*, 11:354 – 358, 1970.

[18] A. Prestel. *Lectures on Formally Real Fields*. IMPA, 1975.

[19] A. Prestel. *Einführung in die Mathematische Logik und Modelltheorie*. Vieweg, 1986.

[20] A. Prestel and C. N. Delzell. *Positive Polynomials*. Springer-Verlag, 2001.

[21] A. Prestel and M. Ziegler. Model-theoretic methods in the theory of topological fields. *Journal für die reine und angewandte Mathematik*, 299/300:318 – 341, 1978.

[22] M. Putinar. Positive polynomials on compact sets. *Indiana University Mathematics Journal*, 42(3):969 – 984, 1993.

[23] K. Schmüdgen. The K-moment problem for compact semi-algebraic sets. *Mathematische Annalen*, 289:203 – 206, 1991.

[24] H. W. Schülting. Prime divisors on real varieties and valuation theory. *Journal of Algebra*, 98:499 – 514, 1986.

[25] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. Rand Corp., 1948.

[26] L. Van den Dries. *Model Theory of Fields*. PhD thesis, Universiteit Utrecht, 1978.

[27] V. Weispfenning. Existential equivalence of ordered abelian groups with parameters. *Archive for Mathematical Logic*, 29:237 – 248, 1990.

[28] W. H. Wheeler. Model-complete theories of pseudo-algebraically closed fields. *Annals of Mathematical Logic*, 17:205 – 226, 1979.

[29] A. Yasuhara. *Recursive Function Theory and Logic*. Academic Press, 1971.

[30] E. Zakon. Generalized archimedean groups. *Transactions of the American Mathematical Society*, 99(1):21 – 40, 1961.

[31] O. Zariski. Local uniformization on algebraic varieties. *Annals of Mathematics*, 41:852 – 896, 1940.

[32] O. Zariski. The concept of a simple point on an abstract algebraic variety. *Transactions of the American Mathematical Society*, 62:1 – 52, 1947.