

The theory of the defect and its application to the problem of local uniformization, I

Franz-Viktor Kuhlmann

Padova, February 19, 2021

Two deep open problems

Longstanding open problems in positive characteristic (their characteristic 0 counterparts were solved in the mid 1960's by Hironaka and Ax & Kochen):

- Resolution of Singularities and its local form, Local Uniformization,
- decidability of Laurent Series Fields over finite fields.

Closest approximations to the first problem to date:
Abhyankar, de Jong, Knaf & K, Temkin, Cossart & Piltant.

Closest approximations to the second problem to date: model theory of tame valued fields (K), and of separably tame valued fields (K & Pal).

Affine algebraic varieties

Algebraic geometry considers solutions of systems of polynomial equations. Take a polynomial ring $K[X_1, \dots, X_\ell]$ in several variables. Given polynomials

$$f_1, \dots, f_n \in K[X_1, \dots, X_\ell],$$

their **zero set** Z is defined to be the set of all common zeros of f_1, \dots, f_n . It is equal to the set of common zeros of all polynomials in the ideal (f_1, \dots, f_n) generated by f_1, \dots, f_n .

If this ideal is prime, then Z is called an **(affine) algebraic variety**. We will denote algebraic varieties by V . The quotient

$$K[V] := K[X_1, \dots, X_\ell] / (f_1, \dots, f_n)$$

is then an integral domain, called the **coordinate ring** of V . Its quotient field is called the **function field** of V and is denoted by $K(V)$.

Affine algebraic varieties

As a prime ideal, (f_1, \dots, f_n) is a proper ideal and consequently,

$$K \cap (f_1, \dots, f_n) = \{0\}.$$

Therefore, the canonical epimorphism

$$K[X_1, \dots, X_\ell] \rightarrow K[X_1, \dots, X_\ell] / (f_1, \dots, f_n)$$

embeds K in $K[V]$. Identifying K with its image, we can assume that K is a subfield of $K[V]$.

The function field of an affine algebraic variety

We may write

$$K[V] = K[x_1, \dots, x_\ell],$$

where x_i is the image of X_i under the canonical epimorphism. Then

$$K(V) = K(x_1, \dots, x_\ell),$$

which is finitely generated over K . Every finitely generated extension of a field K is called an **(algebraic) function field over K** . Every function field over an arbitrary field K is in fact the function field of a suitable variety defined over K .

Resolution of Singularities

Arbitrary algebraic varieties may have singularities, and for various reasons we want to avoid them. That is, we are looking for a second variety having no singularities. But this new variety cannot be arbitrary, it should be connected with the given one in a certain way. What we want is that it is obtained from the given one by a **proper birational morphism**. This implies that both varieties have the same function field.

Finding for every given variety such a second variety without singularities is the (global) solution to the problem known as **Resolution of Singularities**.

Some history of resolution

For varieties over fields of characteristic 0 it was achieved by H. Hironaka in 1964. But for varieties over fields of positive characteristic the problem remains open till the present day. Only partial results are known:

- S. Abhyankar proved resolution for surfaces, and to some extent also for dimension 3;
- A. J. de Jong proved resolution by alteration, which means that one allows a finite extension of the function field;
- V. Cossart and O. Piltant proved resolution without restrictions for dimension 3.

Local Uniformization

If we cannot solve our problems globally, we try to solve them locally. And if we are clever enough, we then may think of patching the local solutions together to obtain a global solution. **Local Uniformization** means eliminating (at least) one singularity at a time by passing to a new, birationally equivalent variety.

We are looking for a new variety where a chosen singular point becomes non-singular. But wait, this was nonsense, because what is our old, singular point on the new variety? We cannot talk of the same points of two different varieties, unless we deal with subvarieties. But passing from varieties to subvarieties or vice versa will in general not provide the solution we are looking for.

Correspondence of points

O. Zariski introduced the use of places on the function field of the variety in order to trace the point on the new variety which corresponds to the original singular point.

Let us have a closer look at our notion of “point”. As we consider just one singular point x_0 on V (and are not interested in other singular points), we can restrict our attention to an affine neighborhood of x_0 . So we may assume from the start that V is an affine variety. Assume that V is defined over K by polynomials $f_1, \dots, f_n \in K[X_1, \dots, X_\ell]$ as described above. Naively, by a point of V we then mean an ℓ -tuple (a_1, \dots, a_ℓ) of elements in an arbitrary extension field L of K such that

$$f_i(a_1, \dots, a_\ell) = 0$$

for $1 \leq i \leq n$.

Correspondence of points

This means that the kernel of the **evaluation homomorphism**

$$K[X_1, \dots, X_\ell] \rightarrow L$$

defined by

$$X_i \mapsto a_i$$

contains the ideal (f_1, \dots, f_n) . Thus it induces a homomorphism η from the coordinate ring

$$K[V] = K[X_1, \dots, X_\ell] / (f_1, \dots, f_n)$$

into L over K (“over K ” means that it leaves the elements of K fixed).

Now that we identify points with homomorphisms on the coordinate ring, why don't we try the following. We mentioned already that the new birationally equivalent variety V' must have the same function field as V , that is,

$$K(V) = K(V').$$

Why don't we just extend the homomorphism η to $K(V) = K(V')$, then restrict it to $K[V']$ and require that the point it thus designates on V' is non-singular?

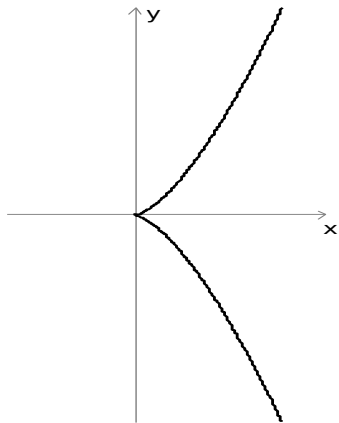
The problem is that in general there are elements in $K[V]$ that are sent to 0 by η , so where should their inverses in $K(V)$ be sent? Any extension of η to $K(V)$ will have to send them to ∞ . Hence such an extension cannot be a homomorphism, but it can be a **place** P . Then we just need to find V' such that the valuation ring \mathcal{O}_P of P contains $K[V']$ so that the restriction of P to $K[V']$ is a homomorphism and thus identifies a point of V' .

Smooth points

We can forget about the variety V and the homomorphism η and consider the function field $F = K(V)$ together with a place P instead. The task of Local Uniformization then is to find a variety V' with function field F and coordinate ring $K[V']$ on which P singles out a non-singular point. This is essentially a valuation theoretical problem, except how do we describe the property of being non-singular?

The solution is to ask for a little bit more. We want the new point to be **smooth**, meaning that the **Implicit Function Theorem** is satisfied in this point. In the following example, the point at the origin is not smooth.

Example: the Neil curve



$$y^2 = x^3$$

The topology

When most of us first learned about the Implicit Function Theorem, the topology it used was provided by the usual ordering of the real numbers. Here, however, we are dealing with valued fields, most of which do not have an ordering. But also valuations induce topologies. Note that in our (Krull) style of writing valuations, two elements a and b are close to each other if the value $v(a - b)$ is **large**.

Recall that by \mathcal{O} we denote the valuation ring of a given valued field.

The Implicit Function Theorem

Take polynomials

$$f_1, \dots, f_n \in \mathcal{O}[X_1, \dots, X_m, Y_1, \dots, Y_n] \text{ with } m > 0.$$

Set $Z = (X_1, \dots, X_m, Y_1, \dots, Y_n)$ and

$$J(Z) := \begin{pmatrix} \frac{\partial f_1}{\partial Y_1}(Z) & \dots & \frac{\partial f_1}{\partial Y_n}(Z) \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial Y_1}(Z) & \dots & \frac{\partial f_n}{\partial Y_n}(Z) \end{pmatrix}.$$

Assume that f_1, \dots, f_n admit a common zero

$$z = (x_1, \dots, x_m, y_1, \dots, y_n) \in \mathcal{O}^{m+n}$$

and that the determinant of $J(z)$ is nonzero. Then for all $(x'_1, \dots, x'_m) \in \mathcal{O}^m$ with $v(x_i - x'_i) > 2v \det J(z)$, $1 \leq i \leq m$, there exists a **unique** tuple $(y'_1, \dots, y'_n) \in \mathcal{O}^n$ such that $(x'_1, \dots, x'_m, y'_1, \dots, y'_n)$ is a common zero of f_1, \dots, f_n and

$$\min_{1 \leq i \leq n} v(y_i - y'_i) \geq \min_{1 \leq i \leq m} v(x_i - x'_i) - v \det J(z).$$

Multidimensional Hensel's Lemma

This is essentially the same as saying that the point satisfies the assumptions of the Multidimensional Hensel's Lemma:

Let $f = (f_1, \dots, f_n)$ be a system of polynomials in the variables $X = (X_1, \dots, X_n)$ and with coefficients in \mathcal{O}_v . Consider the Jacobian matrix

$$J_f(X) := \left(\frac{\partial f_i}{\partial X_j}(X) \right)_{i,j}.$$

Assume that there exists a tuple $b = (b_1, \dots, b_n) \in \mathcal{O}_v^n$ such that

$$vf_i(b) > 0 \text{ for } 1 \leq i \leq n \text{ and } v \det J_f(b) = 0.$$

Then there exists a **unique** tuple $a = (a_1, \dots, a_n) \in \mathcal{O}_v^n$ such that $f_i(a) = 0$ and that $v(a_i - b_i) > 0$ for all i .

Both presented “theorems”, like the usual Hensel’s Lemma, are rather properties of valued fields than theorems. Hence we ask: which valued fields satisfy them? In fact, every **henselian field**, i.e., valued field that satisfies Hensel’s Lemma, also satisfies the Multidimensional Hensel’s Lemma and the Implicit Function Theorem.

It is in fact the uniqueness that characterizes the property of being smooth. Every point on the Neil curve, other than the origin $(0,0)$, is smooth, even if we take it as a curve in $\mathbb{Q} \times \mathbb{Q}$ where we do not have a solution of $y^2 = x^3$ for every x .

Hence we define a point b to be **smooth** if it satisfies the assumption of the Implicit Function Theorem.

Smooth Local Uniformization

Now we can formulate the task of **Smooth Local Uniformization** as follows:

Given a function field F with a place P , does there exist a variety V' with coordinate ring $K[V']$ having quotient field F and such that P singles out a smooth point? In other words, we are looking for generators x_1, \dots, x_m of F , i.e., $F = K(x_1, \dots, x_m)$, such that $K[x_1, \dots, x_m]$ is contained in \mathcal{O}_P and (x_1P, \dots, x_mP) is a smooth point.

Among the generators we can choose a transcendence basis T . One can show that Local Uniformization for (F, P) implies that $F|K$ is separably generated, that means that T can be chosen such that the finite extension $F|K(T)$ is separable. By the Theorem of the Primitive Element, $F|K(T)$ can then be generated by a single element a .

Our problem now is to find a transcendence basis $T = \{t_1, \dots, t_n\} \subset \mathcal{O}_P$ of $F|K$ and an element $a \in \mathcal{O}_P$ algebraic over $K(T)$ such that $F = K(T, a)$ and the point (t_1P, \dots, t_nP, aP) is smooth. Performing the passage from the Implicit Function Theorem to Hensel's Lemma (see the lecture notes for the technical details), we find that this means that a satisfies the assumptions of the usual Hensel's Lemma: denote by v the valuation on F associated with P , and let f be the minimal polynomial of a over $K(T)$; then $vf(a) > 0$ (which is automatic as $f(a) = 0$) and $vf'(a) = 0$.

At this point, a word of warning is in place. Local Uniformization also requires that the new variety V' is connected with the one we started with by a proper birational morphism. This amounts to an extra condition, one may see as “Local Uniformization for $(K(T), P)$ ”, which we will ignore for now.

The extension $(K(T, a)|K(T))$

How do we know that the extension $(K(T, a)|K(T), v)$ satisfies the condition on a we have just derived?

The **henselization** of a valued field is the smallest algebraic extension that is henselian. Does our condition on a mean that a lies in the henselization of $K(T)$? The answer is NO. We will need **ramification theory** to give the correct answer.

Extensions of valuations in algebraic field extensions

Take a valued field (K, v) and set $p = \text{char } Kv$ if this is positive, and $p = 1$ otherwise. We choose an arbitrary extension \tilde{v} of v to the algebraic closure \tilde{K} of K .

Take an algebraic extension $L|K$. Then for every $\sigma \in \text{Aut}(\tilde{K}|K)$, the map

$$\tilde{v}\sigma = \tilde{v} \circ \sigma : L \ni a \mapsto \tilde{v}(\sigma a) \in \tilde{v}\tilde{K}$$

is a valuation of L which extends v .

Theorem

The set of all extensions of v from K to L is

$$\{\tilde{v}\sigma \mid \sigma \text{ an embedding of } L \text{ in } \tilde{K} \text{ over } K\}.$$

(We say that “all extensions of v from K to L are **conjugate**”.)

Ramification groups

From now on, we assume that the algebraic extension $L|K$ is normal. Hence the set of all extensions of v from K to L is given by $\{\tilde{v}\sigma \mid \sigma \in \text{Aut}(L|K)\}$. For simplicity, we denote the restriction of \tilde{v} to L again by v . The valuation ring of v on L will be denoted by \mathcal{O}_L , and its unique maximal ideal by \mathcal{M}_L . We will now define distinguished subgroups of $G := \text{Aut}(L|K)$. The subgroup

$$\begin{aligned} G^d &= G^d(L|K, v) := \{\sigma \in G \mid \forall x \in \mathcal{O}_L : v\sigma x \geq 0\} \\ &= \{\sigma \in G \mid \sigma\mathcal{O}_L \subseteq \mathcal{O}_L\} \end{aligned}$$

is called the **decomposition group of $(L|K, v)$** . It is easy to show that σ sends \mathcal{O}_L into itself if and only if the valuations v and $v\sigma$ agree on L . Thus,

$$G^d = \{\sigma \in G \mid v\sigma = v \text{ on } L\}.$$

Ramification groups

Further, the **inertia group** is defined to be

$$G^i = G^i(L|K, v) := \{\sigma \in G \mid \forall x \in \mathcal{O}_L : v(\sigma x - x) > 0\},$$

and the **ramification group** is

$$G^r = G^r(L|K, v) := \{\sigma \in G \mid \forall x \in L^\times : v(\sigma x - x) > vx\}.$$

Ramification fields

The fixed fields of G^d , G^i and G^r in the maximal separable extension field L_s of K within L are called **decomposition field**, **inertia field** and **ramification field** of $(L|K, v)$, respectively. For simplicity, let us abbreviate them by Z , T and V , respectively. (These letters refer to the German words “Zerlegungskörper”, “Trägheitskörper” and “Verzweigungskörper”.)

Remark: In contrast to the classical definition used by other authors, we take decomposition field, inertia field and ramification field to be the fixed fields of the respective groups *in the maximal separable subextension*. The reason for this will become clear later.

By our definition, V , T and Z are separable-algebraic extensions of K , and $L_s|V$, $L_s|T$, $L_s|Z$ are (not necessarily finite) Galois extensions. Further,

$$1 \subset G^r \subset G^i \subset G^d \subset G \text{ and thus, } L_s \supset V \supset T \supset Z \supset K.$$

Theorem

G^i and G^r are normal subgroups of G^d , and G^r is a normal subgroup of G^i . Therefore, $T|Z$, $V|Z$ and $V|T$ are (not necessarily finite) Galois extensions.

The decomposition field

First, we consider the decomposition field Z . In some sense, it represents all extensions of v from K to L .

Theorem

- a) $v\sigma = v\tau$ on L if and only if $\sigma\tau^{-1}$ is trivial on Z .
- b) $v\sigma = v$ on Z if and only if σ is trivial on Z .
- c) The extension of v from Z to L is unique.
- d) The extension $(Z|K, v)$ is immediate.

Assertions a) and b) are easy consequences of the definition of G^d . Assertion c) follows from assertion b) by Theorem 1. For assertion d), there is a simple proof using a trick which is mentioned in the very useful appendix of a paper by J. Ax.

The inertia field

Now we turn our attention to the inertia field T . For every $\sigma \in G^d(L|K, v)$ we have that $\sigma\mathcal{O}_L = \mathcal{O}_L$, and it follows that $\sigma\mathcal{M}_L = \mathcal{M}_L$. Hence, every such σ induces an automorphism $\bar{\sigma}$ of $\mathcal{O}_L/\mathcal{M}_L = Lv$ which satisfies $\bar{\sigma}\bar{a} = \overline{\sigma a}$. Since σ fixes K , it follows that $\bar{\sigma}$ fixes Kv .

Lemma

Since $L|K$ is normal, the same is true for $Lv|Kv$. The map

$$G^d(L|K, v) \ni \sigma \mapsto \bar{\sigma} \in \text{Aut}(Lv|Kv) \quad (1)$$

is a group homomorphism.

Theorem

a) *The homomorphism (1) is onto and induces an isomorphism*

$$\mathrm{Aut}(\mathbb{T}|\mathbb{Z}) = G^d/G^i \simeq \mathrm{Aut}(\mathbb{T}v|\mathbb{Z}v). \quad (2)$$

b) *For every finite subextension $F|\mathbb{Z}$ of $\mathbb{T}|\mathbb{Z}$,*

$$[F : \mathbb{Z}] = [Fv : \mathbb{Z}v]. \quad (3)$$

c) *We have that $v\mathbb{T} = v\mathbb{Z} = vK$. Further, $\mathbb{T}v$ is the relative separable-algebraic closure of Kv in Lv , and therefore,*

$$\mathrm{Aut}(\mathbb{T}v|\mathbb{Z}v) = \mathrm{Aut}(Lv|Kv). \quad (4)$$

We will now turn to the ramification field. We need a quick preparation.

Given any extension $\Delta \subset \Delta'$ of abelian groups, the p' -divisible closure of Δ in Δ' is defined to be the subgroup

$$\{\alpha \in \Delta' \mid \exists n \in \mathbb{N} \mid (p, n) = 1 \wedge n\alpha \in \Delta\}$$

of all elements in Δ' whose order modulo Δ is prime to p .

The ramification field

Theorem

a) *There is an isomorphism*

$$\text{Aut}(V|T) = G^i/G^r \simeq \text{Hom}(vV/vT, (Tv)^\times), \quad (5)$$

where the character group on the right hand side is the full character group of the abelian group vV/vT . Since this group is abelian, $V|T$ is an abelian Galois extension.

b) *For every finite subextension $F|T$ of $V|T$,*

$$[F : T] = (vF : vT). \quad (6)$$

c) *We have that $Vv = Tv$, and vV is the p' -divisible closure of vK in vL .*

The ramification field

Theorem

The ramification group G^r is a p -group and therefore, $L_s|V$ is a p -extension and the degree of every finite subextension of $L|V$ is a power of p .

Further, vL/vV is a p -group, and the residue field extension $Lv|Vv$ is purely inseparable.

If $\text{char } Kv = 0$, then $V = L_s = L$.

Absolute ramification theory

Absolute ramification theory is ramification theory applied to the normal extension $\tilde{K}|K$. We fix an extension of v to \tilde{K} and denote it again by v . We assume that v is non-trivial. We denote by K^{sep} the separable-algebraic closure of K . Note that

$$v\tilde{K} = vK^{\text{sep}} = \widetilde{vK},$$

where \widetilde{vK} denotes the divisible hull of vK , and

$$\tilde{K}v = K^{\text{sep}}v = \widetilde{Kv}.$$

Now we can present the basic facts of absolute ramification theory in the following picture.

Absolute ramification theory

Galois group	field		value group	residue field
	\tilde{K}		$\tilde{v}K$	$\tilde{K}v$
	purely inseparable			
1	K^{sep}	separable-algebraic closure	$\tilde{v}K$	$\tilde{K}v$
	Galois p -extension		division by p	purely inseparable
G^r	K^r	absolute ramification field	$\frac{1}{p^{r\infty}}vK$	$(Kv)^{\text{sep}}$
Char	abelian Galois p^r -extension		division prime to p	
G^i	K^i	absolute inertia field	vK	$(Kv)^{\text{sep}}$
Gal Kv	Galois			Galois
G^d	$K^d = K^h$	absolute decomposition field = henselization	vK	Kv
Gal K	K		vK	Kv





Elimination of Ramification

Ramification is the valuation theoretical expression of the failure of the Implicit Function Theorem. So we wish to **eliminate ramification** in a given valued function field $(F|K, v)$. However, ramification means more than just the change of the value groups. Already in classical algebraic number theory one calls an extension ramified also if the residue field extension is not separable. Even more general, for us ramification is everything that happens above the absolute inertia field. Then Elimination of Ramification means to find a transcendence basis T such that F lies in the **absolute inertia field** (also called **strict henselization**) of $(K(T), v)$. In other words, the element a we talked about does not have to lie in $K(T)^h$, but should lie in $K(T)^i$. We then also say that the extension $(F|K, v)$ is **inertially generated**.




Elimination of Ramification

Hence the task of Elimination of Ramification for a given valued function field $(F|K, v)$ is to show that it is inertially generated. Thus we are looking at the **structure theory of valued function fields**.





References: Valuation Theory

-  Ax, J.: A metamathematical approach to some problems in number theory. Proc. Symp. Pure Math., **20**, Amer. Math. Soc., 161–190 (1971)
-  Endler, O.: *Valuation theory*, Berlin (1972)
-  Engler, A. – Prestel, A.: *Valued fields*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.
-  Neukirch, J.: *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften **322**, Springer-Verlag, Berlin, 1999



References: Valuation Theory

-  Ribenboim, P.: *Théorie des valuations*, Les Presses de l'Université de Montréal (1964)
-  Warner, S.: *Topological fields*, Mathematics studies **157**, North Holland, Amsterdam (1989)
-  Zariski, O. – Samuel, P.: *Commutative Algebra*, Vol. II, New York–Heidelberg–Berlin (1960)

References: Resolution of Singularities

-  Abhyankar, S.: *Resolution of singularities of arithmetical surfaces*, Arithmetical Algebraic Geometry, Harper and Row, New York (1965)
-  Abhyankar, S.: *Resolution of singularities of embedded algebraic surfaces*, Academic Press, New York (1966); 2nd enlarged edition: Springer, New York (1998)
-  Cossart, V. – Piltant, O.: *Resolution of singularities of threefolds in positive characteristic. I*, Reduction to local uniformization on Artin-Schreier and purely inseparable coverings. *J. Algebra* **320** (2008), 1051–1082
-  Cossart, V. – Piltant, O.: *Resolution of singularities of threefolds in positive characteristic. II*, *J. Algebra* **321** (2009), 1836–1976

References: Resolution of Singularities

-  de Jong, A. J.: *Smoothness, semi-stability and alterations*, Publ. Math. IHES **83** (1996), 51–93
-  Hironaka, H.: *Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II*, Ann. of Math. (2) **79** (1964), 109–203; *ibid.* (2) **79** (1964), 205–326