2015

Lifting Problems and Their Independence of the Coefficient Field

Matti Perttu Åstrand
University of Pennsylvania, mattiastr@gmail.com

Lifting Problems and Their Independence of the Coefficient Field

Abstract

Our aim is to find out new things about lifting problems in general and Oort groups in particular. We would like to know more about what kind of rings are needed to find liftings to characteristic 0 of covers of curves in characteristic p. For this, we use explicit parametrization of curves and model theory of algebraically closed fields and valued fields. The geometric machinery we need includes local-global principle of lifting problems and HKG-covers of ring extensions. We won't use formal or rigid geometry directly, although it is used to prove some of that machinery. Also we need some model theoretical results such as AKE-principles and Keisler-Shelah ultrapower theorem. To be able to use model theoretical tools we need to assume some bounds on the complexity of our curves. The standard way to do this is to bound the genus. What we want is that for the finite group G, the curves of a fixed genus can be lifted over a fixed ring extension. This kind of question — where both the curve and the ring are bounded — is well suited for model theoretical tools. For a fixed finite group G, we will show that for genus g and an algebraic integer π, the statement "every G-cover Y → P 1 with genus g has a lifting over W (k)[π]" does not depend on k. In other words, it is either true for all algebraically closed fields k or none of them. This gives some reason to believe that being an Oort group does not depend on the field k. Also it might help in finding explicit bounds on the ring extension needed.

Degree Type

Dissertation

Degree Name

Doctor of Philosophy (PhD)

Graduate Group

Mathematics

First Advisor

Florian Pop

Keywords

branched cover, lifting, ultraproduct

LIFTING PROBLEMS AND THEIR INDEPENDENCE OF THE COEFFICIENT FIELD

Matti Perttu Åstrand

A DISSERTATION

in

Mathematics

Presented to the Faculties of the University of Pennsylvania

in

Partial Fulfillment of the Requirements for the
Degree of Doctor of Philosophy

2015

Supervisor of Dissertation

_____

Florian Pop
Samuel D. Schack Professor of Algebra

Graduate Group Chairperson

_____

David Harbater
Christopher H. Browne Distinguished Professor in the School of Arts and Sciences

Dissertation Committee:
Florian Pop, Samuel D. Schack Professor of Algebra
David Harbater, Christopher H. Browne Distinguished Professor
Henry Towsner, Assistant Professor of Mathematics

Acknowledgments

First I want to thank whoever was in the admission committee five years ago and decided to give me the chance to live the life of a graduate student at Penn. When I got here, it wasn't the thought of graduating some day that was driving me, but I just wanted to experience graduate school, and (mostly) it has been what I hoped it would. I have been able to do the work I enjoy in a great environment: I have College green as my backyard, Houston hall as my living room, and the library as my study room.

My advisor Florian Pop deserves my thanks for sharing his mathematical insights, having patience with my extended periods of low productivity, and having trust that I will eventually get some work done after I run out of things to procrastinate with. Other professors I should thank for mathematical help include David Harbater, Ted Chinburg, Henry Towsner and Franz-Viktor Kuhlmann.

Penn Math department is a great place for research thanks to all graduate students and faculty: people there are passionate about mathematical research and have fun doing it. This positive atmosphere passes on from person to person and everyone who joins the department will be infected by it. All the people in our department should be thanked for this.

Thank you Xinyu for teaching me the value of hard work.

ABSTRACT

LIFTING PROBLEMS AND THEIR INDEPENDENCE OF THE COEFFICIENT FIELD

Matti Perttu Åstrand

Florian Pop

Our aim is to find out new things about lifting problems in general and Oort groups in particular. We would like to know more about what kind of rings are needed to find liftings to characteristic 0 of covers of curves in characteristic p. For this, we use explicit parametrization of curves and model theory of algebraically closed fields and valued fields. The geometric machinery we need includes local-global principle of lifting problems and HKG-covers of ring extensions. We won't use formal or rigid geometry directly, although it is used to prove some of that machinery. Also we need some model theoretical results such as AKE-principles and Keisler-Shelah ultrapower theorem. To be able to use model theoretical tools we need to assume some bounds on the complexity of our curves. The standard way to do this is to bound the genus. What we want is that for the finite group G, the curves of a fixed genus can be lifted over a fixed ring extension. This kind of question — where both the curve and the ring are bounded — is well suited for model theoretical tools. For a fixed finite group G, we will show that for genus g and an algebraic integer π, the statement "every G-cover $Y \to \mathbb{P}^1$ with genus g has a lifting over $W(k)[\pi]$" does not depend on k. In other words, it is either true for all algebraically closed fields k or none of them. This gives some reason to believe that being an Oort group does not depend on the field k. Also it might help in finding explicit bounds on the ring extension needed.

Contents

1 Introduction **1**

1.1 Bird's eye view of lifting problems 1

1.2 Oort groups 3

1.3 Outline of the thesis 5

2 Curves over valuation rings **7**

2.1 Valuation rings 7

2.2 Curves over fields 8

2.3 Curves over rings 11

3 Lifting problems **14**

3.1 Lifting problem of curves 14

3.2 Local lifting problem 15

4 Reductions of lifting problems **17**

4.1 Local-global principle 17

4.2 HKG-covers of the projective line 18

5 Model theory generalities **20**

5.1 First order languages 20

5.2 Algebraically closed fields 24

5.3 Diagram and elementary diagram 25

5.4 Ultraproducts 27

6 Model theory of valued fields **30**

6.1 Ax-Kochen-Ershov principles 30

6.2 Ultraproducts and Witt vectors 31

7 Model theory of curves and their covers **33**

7.1 Interpretations 33

7.2 Varieties in the projective space 35

7.3 Maps between projective varieties 37

7.4 Group action on a curve 39

7.5 G-covers of curves 40

8 Ultraproducts of curves **43**

8.1 Projective lines 43

8.2 Birational approach: valuations on function fields 44

8.3 Embedding to projective space 47

9 Reduction with a fixed ring extension **49**

9.1 Statement 49

9.2 Proof of Step 1 51

9.3 Proof of Step 2 53

1 Introduction

1.1 Bird's eye view of lifting problems

Lifting problems can be seen as trying to find an inverse to reduction modulo a prime. Simplest example of a reduction is the map $\mathbb{Z} \to \mathbb{Z}/p$: for an integer, the map gives its residue class mod p. A lifting problem is roughly speaking starting from something in terms of $\mathbb{Z}/p$ and trying to find a similar looking "thing" in terms of $\mathbb{Z}$.

A silly example is just lifting elements of the ring: since the reduction map $\mathbb{Z} \to \mathbb{Z}/p$ is surjective, every element in $\mathbb{Z}/p$ has a preimage in $\mathbb{Z}$. A more interesting question is about finding solutions to polynomial equations: the polynomial $x^2 + 1$ has a root $2 \in \mathbb{Z}/5$ but it clearly does not have a root in $\mathbb{Z}$. Thus the "lifting problem" of finding roots of arbitrary polynomials with integer coefficients fails for that reduction map.

However, there is a class of rings where these polynomial lifting problems can be solved, namely henselian rings. A local ring R is *henselian* if it satisfies the Hensel's lemma: if $f(t) \in R[t]$ is a polynomial such that its reduction over $k = R/m$ has a simple root, then there is a preimage of that root in the map $R \to R/m$ which itself is a root of $f(t)$.

In other words, a ring is henselian if simple roots of polynomials can be lifted against the reduction map. This is equivalent to a more general formulation for systems of equations:

Lemma (Hensel, multivariate version)**.** *Let R be a henselian local ring with maximal ideal m. Suppose $f_1, \ldots, f_n \in R[x_1, \ldots, x_n]$ are polynomials in n variables and $\alpha_1, \ldots, \alpha_n \in k = R/m$ are values in the residue field satisfying the following conditions:*

- *$f_i(\alpha) = 0$ in k for all $i = 1, \ldots, n$, where $\alpha = (\alpha_1, \ldots, \alpha_n)$*

- *The Jacobian matrix* $(\partial f_i/\partial x_j)$ *evaluated at* α *gives an invertible matrix in* $k^{n\times n}$.

Then there exists a point $\beta \in R^n$ *which maps to* α *in the reduction* $R \to R/m$ *and satisfies* $f_i(\beta) = 0$ *in* R *for all* $i = 1, \ldots, n$.

One way to think about this formulation is that if the polynomials $f_1, \ldots, f_n$ considered over the residue field k define a 0-dimensional affine variety X over k, then any smooth rational point in $X(k)$ is a reduction of some smooth point in $\mathcal{X}(R)$, where $\mathcal{X} \subseteq R^n$ is the affine R-scheme defined by the same polynomials $f_1, \ldots, f_n$ when considered over the ring R.

Yet another way is to look at rational points as morphisms of varieties: a smooth point of $X(k)$ is a smooth morphism

$$\operatorname{Spec} k \to X = \operatorname{Spec} k[x_1, \ldots, x_n]/(f_1, \ldots, f_n).$$

Note that $\operatorname{Spec} k$ is the terminal object in the category of k-schemes. Hensel's lemma says that any such morphism comes from a smooth morphism

$$\operatorname{Spec} R \to \mathcal{X} = \operatorname{Spec} R[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$$

as a base change under the map $\operatorname{Spec} R \to \operatorname{Spec} k$. That is, the base change functor

$$(-) \times_R \operatorname{Spec} k \colon R\text{-}Schemes \to k\text{-}Schemes$$

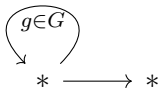
has the given morphism $\operatorname{Spec} k \to X$ in its image. This particular base change functor is also called the *special fiber*.

$$\begin{array}{ccc} \operatorname{Spec} k & \longrightarrow & X \\ \downarrow & & \downarrow \\ \operatorname{Spec} R & \overset{\exists}{\dashrightarrow} & \mathcal{X} \end{array}$$

Thus the Hensel's lemma can be considered a result about 0-dimensional lifting problems. If we want to increase the dimension, the next step would be 1-dimensional varieties, i.e. curves. Here we formulate the lifting problem in a slightly different way.

We still assume a local ring R and consider the residue field $R \to k$. We will think of geometric objects as "diagrams" in the category of k-schemes or R-schemes. A diagram means a collection of schemes and morphisms between them. It can be represented as a functor from a category J to the category of k-schemes (e.g. J could be a finite category).

The lifting problem then is: given such a diagram of k-schemes, does there exist a diagram in R-schemes that maps to it under the special fiber functor from R-schemes to k-schemes? Often we restrict ourselves to a smaller class of schemes instead of considering the category of all schemes: e.g. we require them to be of finite type, smooth, flat and projective.



The particular problem we will study in this thesis has to do with a diagram that is a finite group G acting on a curve. We also include the quotient object of this action by having the G-cover $Y \to X$ in the diagram. This is in fact a diagram in the category having two objects, an arrow from Y to itself for every group element, one arrow $Y \to X$ for the covering map, and only the identity arrow from X to itself.

1.2 Oort groups

The exact formulation of lifting problem will be given in a later section, after we have talked about Witt vectors and curves over valuation rings. We are particularly interested in the

groups G for which all of such lifting problems have a solution over some ring R. We call such groups *Oort groups*. Let's now review what is known about Oort groups.

First, Grothendieck proved as part of his study of the tame fundamental group that every group G whose order is prime to p is an Oort group (although he didn't use the term). This is because every tamely ramified G-cover lifts to characteristic 0 (see SGA I [Gro71]), and if $|G|$ is prime to p, then every G-cover is tamely ramified.

Let p be a prime, and let G be a group of the form $Z/m \ltimes P$, where P is a p-group and m not divisible by p. This kind of groups are called *cyclic by p*, and they are important because they are the kind of groups that can be inertia groups, as we will see later in Section 3. We know that all the Oort groups that are cyclic by p for fields k of characteristic p are contained in the following list:

1. Cyclic groups
2. Dihedral groups D_{2p^n} of order $2p^n$ for some $n \geq 1$
3. If $p = 2$, also include the alternating group A_4

This was proven by Chinburg, Guralnick and Harbater (see [CGH08] and [CGH11]). We also know a partial converse to this: suppose G is cyclic by p. Then we know the following:

1. If G is cyclic, then G is an Oort group. This is the *Oort conjecture* stated by Frans Oort [Oor87] (see also [Oor95]). It was proven in the case $|G| = pm$ with m prime to p by Oort, Sekiguchi and Suwa [SOS89] and in the case $|G| = p^2m$ by Green and Matignon [GM98]. The general case was proven in 2012 by Obus, Wewers [OW14] and Pop [Pop14].

2. If $G = D_{2p}$, then G is an Oort group. This is due to Pagot [Pag02] in case $p = 2$ and Bouw and Wewers [BW06] for odd p.

3. The group A_4 is announced to be an Oort group for $p = 2$ by Bouw (unpublished, see [BW06, §1.3]).

4. If G is an arbitrary finite group, then it is an Oort group if and only if all of its subgroups that are cyclic by p are Oort groups.

It is still unknown whether D_{2p^n} is an Oort group for arbitrary n.

If we can prove that among cyclic by p-groups, the Oort groups are exactly the ones given in the list above, then this will imply that being an Oort group doesn't depend on the field k: if a group G is Oort group for one algebraically closed field of characteristic p, then it is an Oort group for all such fields. This is not known, and this question will not be answered in this thesis. However, we have reasons to believe that it is true, and we prove a related result: we will prove that if the ring R can be chosen to be large enough to allow liftings over R for all covers of curves with a given genus, then the same is true for all algebraically closed fields of characteristic p.

1.3 Outline of the thesis

In Section 2 we introduce and define carefully what we mean by curves over valuation rings, and we will also prove important result on representing curves of a given genus with finitely many parameters. This lets us define what exactly we mean by lifting problems in Section 3, and we state some reformulations of lifting problems in Section 4.

In Section 5 we recall the basics of first order model theory that are necessary to us,

including diagram and elementary diagram theory of a structure, the theory of algebraically closed fields and ultraproducts of structures. Some facts on the model theory specific to valued fields and rings are given in Section 6. This includes a version of Ax-Kochen-Ershov principle for finitely ramified fields and how the ring of Witt vectors behaves under ultraproducts.

We will build some explicit formulas for expressing statements about curves and their covers in Section 7, starting from varieties in general and parametrizing smooth curves, covers of curves and expressing statements e.g. about a group acting on a curve and ramification of a cover. Next in Section 8 we will talk about ultraproducts of curves: how they are constructed, what the function field looks like and what its rational points are. Finally in Section 9 we show a proof of the main result on a certain statement about existence of liftings over a given ring being independent of the field of coefficients.

2 Curves over valuation rings

2.1 Valuation rings

We will not work with arbitrary commutative rings: the rings we are concerned with are called valuation rings. Examples of valuation rings are among others:

- localization of a Dedekind ring at a prime ideal
- ring of holomorphic functions defined in some neighborhood of a given point on a Riemann surface

Let R be an integral domain and K its field of fractions. We say that R is a *valuation ring* if for every element $x \in K^\times$ we have either $x \in R$ or $x^{-1} \in R$. In that case, the *value group* is the quotient group $\Gamma = K^\times/R^\times$, and we will consider it as an additive group. Denote the projection map $K^\times \to \Gamma$ by v. The group Γ is an ordered abelian group, with ordering defined as

$$v(x) \geq 0 \iff x \in R.$$

This defines a total ordering or Γ as long as R is a valuation ring.

Note that the map $v\colon K^\times \to \Gamma$ is a surjective group homomorphism, and satisfies the property

$$\forall x, y \in K^\times\, v(x) \geq 0, v(y) \geq 0 \implies v(x+y) \geq 0.$$

For any field K, such a homomorphism from $K^\times$ to any ordered abelian group is called a *valuation*. The set of valuations of a field is in bijection with the valuation subrings of K with fraction field K.

We call R a *discrete valuation ring* if its value group Γ is isomorphic to $\mathbb{Z}$. Most of the rings we will consider later are discrete valuation rings.

Perhaps the most important discrete valuation ring for us is the ring of Witt vectors $W(k)$. Suppose first that k is a field of characteristic p which is perfect, i.e. $k^p = k$. The Witt ring $W(k)$ can be defined as the unique ring A satisfying the following properties:

1. The ideal pA is maximal, and
2. the residue field is $A/pA = k$
3. A is complete and Hausdorff with respect to the p-adic topology, i.e. the map $A \to \lim A/p^n A$ is an isomorphism.

Any ring satisfying 1. and 3. is called a *strict p-ring*. Thus the Witt ring $W(k)$ can be defined as the unique strict p-ring with residue field k. The fact that there is a unique such ring is due to Serre [Ser79, II.5], as is the fact that $W(k)$ is functorial in k.

2.2 Curves over fields

Before we talk about curves over valuation rings, let's recall basics of projective curves over fields. They are well behaved enough to be easier to understand, and provide a stepping stone towards the more general and slightly more complicated description of curves over rings. For introduction to algebraic curves, see e.g. [Mir95].

For simplicity, we assume that k is an algebraically closed field. By "curve over k" we will always mean a complete normal curve. In the case where k is perfect (e.g. algebraically closed) this will mean that the curve is in fact smooth and projective. These curves can be

described in different ways, and we will use two different descriptions depending on context. The set of points of a curve over k can be described as

1. the set of valuations of a function field K of one variable over k, or

2. an algebraic set inside the projective space $\mathbb{P}^n$.

Since we have already talked about valuations above, let's start from the "birational" approach, thinking of points as valuations of the function field.

Suppose K is a finite separable extension of the rational function field $k(t)$. In particular this implies that K has transcendence degree 1 over k. The curve with function field K is given by the set of valuations of K that are trivial on the subfield k. All of them are discrete valuations. In particular, for every function field in one variable over k, there is a unique curve with function field K, up to a unique isomorphism. This fact is not true for higher dimensional varieties, for example surfaces.

Let C be the curve with function field K. A divisor of the curve is a $\mathbb{Z}$-linear combination $\sum_P n_P P$ of points of C. In other words, the set of divisors is the free abelian group generated by the set of points of C:

$$\mathrm{Div}(C) = \bigoplus_P \mathbb{Z}P$$

If $f \in K^\times$ is an element in the function field, then it gives a divisor by

$$\mathrm{div}(f) = \sum_P v_P(f)P.$$

Since we think of points as valuations, the divisor is very simple to define. We can also define the linear system of a divisor $D = \sum_P n_P P$ as

$$L(D) = \{f \in K^\times \mid v_P(f) + n_P \geq 0\} = \{f \in K^\times \mid \mathrm{div}(f) + D \geq 0\}.$$

This is clearly a vector space over k.

There is a distinguished divisor W on the curve C, called *canonical divisor*. We don't need to go into details of how it is defined: it comes from any rational differential on C. But for us it is important because of Riemann-Roch theorem: for any divisor $D \in \mathrm{Div}(C)$, we have

$$\dim L(D) - \dim L(W - D) = \deg(D) + 1 - g,$$

where the dimensions are over the ground field k, and $g = \dim L(W)$ is the *genus* of the curve.

Embedding to projective space One feature of curves that will be important for us is that they can be embedded in projective space and described with finitely many parameters from the field k. The number of parameters is not bounded, so there is no universal parametrization of all curves. However, if we first fix the genus g of our curves, then there is a uniform bound on the number of parameters, so we can talk about the "space" of curves of genus g.

Let's see how this is done. We start with a curve C over the field k, and we pick an arbitrary divisor D with degree $2g + 1$. Then we can see from Riemann-Roch that $\dim L(D) = g + 2$ and for any two points P, Q of the curve C we have

$$\dim L(D - P - Q) = g = \dim L(D) - 2,$$

which means that the divisor D "separates points and tangents". If $f \in L(D)$, then it defines a rational map from C to $\mathbb{A}^1$: at every point P on C such that neither D nor $\mathrm{div}(f)$ contain P, we have $f \in \mathcal{O}_P$ and it maps to $\mathcal{O}_P/m_P \cong k$. This gives a value $f(P) \in k$.

Let $f_0, \ldots, f_{g+1}$ be a basis of $L(D)$. They all define rational maps to $\mathbb{A}^1$, so we can combine those to get a rational map to $\mathbb{P}^{g+1}$. This rational map can be extended to a regular map from $C \to \mathbb{P}^{g+1}$, since C is a complete curve. By the choice of D we know that it separates points and tangents, so the map will be an embedding onto a smooth curve in the projective space $\mathbb{P}^{g+1}$.

Also the degree of the curve in $\mathbb{P}^{g+1}$ is known: it is equal to $\deg(D)$, which is $2g+1$. Thus the curve is isomorphic to some curve in $\mathbb{P}^{g+1}$ of degree $2g+1$. To have these explicit numbers will be useful to us later when we want to parametrize the curves of genus g.

2.3 Curves over rings

When we consider curves over rings, things don't go so easily. First of all, the schemes that we call curves are technically of dimension 2. If $\mathcal{O}_K$ is a valued ring with a rank 1 valuation, then $\operatorname{Spec} \mathcal{O}_K$ has dimension 1, and a scheme of relative dimension 1 over $\operatorname{Spec} \mathcal{O}_K$ is then itself dimension 2. However, we call them curves because they are "relative curves" over $\mathcal{O}_K$. In particular, the fibers of the map $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_K$ at any point $s \in \operatorname{Spec} \mathcal{O}_K$ are curves over $k(s)$.

Let's fix some assumptions: when we talk about "curves over $\mathcal{O}_K$", we mean a proper integral normal flat $\mathcal{O}_K$-scheme $\mathcal{X}$, whose every irreducible component has relative dimension 1 over $\operatorname{Spec} \mathcal{O}_K$. This in fact implies that $\mathcal{X}$ is projective.

Birational description Let K be a valued field and $\mathcal{O}_K$ its valuation ring. While the projective curves over $\mathcal{O}_K$ are not quite uniquely characterized by their function fields, we can still say some things about how they are related to valuations of the function fields.

These results are mostly due to Green, Matignon and Pop [GMP92].

First, let F be a function field in one variable over the field K. This means that F is a finitely generated extension of K of transcendence degree 1 over K. We are going to consider valuations on F which prolong the valuation v_K of K. In particular we are interested in *constant reductions* of F/K: they are the prolongations v of v_K to F for which the residue field extension Fv over $Kv = k$ is a function field in one variable. In other words, they are valuations for which we can reduce the function field and the field of constants and get another function field in one variable over the residue field k. Note that this corresponds to a unique (smooth projective) curve over k.

Now, let V be a finite set of constant reductions on F. If there exists a *V-regular* function $f \in F$, then we can construct an $\mathcal{O}_K$-curve $\mathcal{C}_V$. The element f being V-regular means that it satisfies the following:

- for all valuations $v \in V$, the restriction to $K(f)$ is equal to the Gauss valuation on $K(f)$ extending v_K
- the degrees satisfy $\deg(f) = \sum_{v \in V} \deg(fv)$, where fv is the reduction of f in the residue field Fv.

Note that not every set V of constant reductions has a V-regular function. For instance, V must contain all prolongations of the Gauss valuation $v_{K,f}$ on $K(f)$ to F.

The construction of $\mathcal{C}_V$ is not too complicated: it is the normalization of $\mathbb{P}^1_{\mathcal{O}_K}$ in the field extension $K(f) \hookrightarrow F$. Here we identify the field $K(f)$ with the function field of $\mathbb{P}^1_{\mathcal{O}_K}$. More precisely we define $\mathcal{C}_V$ as $\operatorname{Spec} R_1 \cup \operatorname{Spec} R_2$, where R_1 and R_2 are the integral closures of $\mathcal{O}_K[f]$ and $\mathcal{O}_K[f^{-1}]$ inside the field F respectively. As their intersection $R_1 \cap R_2$ is exactly

the integral closure of $\mathcal{O}_K[f, f^{-1}]$, this is precisely the normalization of $\mathbb{P}^1_{\mathcal{O}_K}$.

Now we can state the result by Green, Matignon, Pop [GMP92]:

Theorem. *Let K be a valued field, F a function field in one variable over K and V a finite set of constant reductions of F. Then the $\mathcal{O}_K$-curve $\mathcal{C}_V$ defined as above is independent of the choice of the V-regular function f, it is locally of finite presentation over $\mathcal{O}_K$ and the morphism $\mathcal{C}_V \to \mathbb{P}^1_{\mathcal{O}_K}$ is finite.*

In case that K is algebraically closed valued field, we get furthermore that every $\mathcal{O}_K$-curve $\mathcal{X}$ is isomorphic to $\mathcal{C}_V$ for a unique set V. In fact, the set V is the set of valuations corresponding to generic points of the irreducible components of the closed fiber of $\mathcal{X}$.

Note that the second part of the theorem won't apply to most of this thesis, since we don't deal with algebraically closed valued fields. But by another result of the same authors [GMP90, Theorem 3.1], if K is henselian valued field then every finite set V of constant reductions has a function $f \in F$ such that V is exactly the set of prolongations of the Gauss valuation on $K(f)$. Also, the curves we will consider are proper normal curves over complete discrete valuation rings and they have good reduction, and all such curves are isomorphic to some $\mathcal{C}_V$ where in fact V will consist of the good reduction v of F.

3 Lifting problems

3.1 Lifting problem of curves

We are now ready to state precisely the kind of lifting problem studied in this thesis. We assume that k is an algebraically closed field of characteristic p, and G is a finite group. Let Y be a smooth projective curve over k together with an action of G on Y by k-morphisms. Let X be the quotient object $X = Y/G$ so we have a (possibly branched) G-cover $Y \to X$.

Definition. *Let R be a finite extension of the ring $W(k)$ of Witt vectors. We say that a G-cover of k-curves $Y \to X$* lifts over *R if there exists a G-cover of smooth flat projective R-curves $\mathcal{Y} \to \mathcal{X}$ whose special fiber is isomorphic to the given cover $Y \to X$.*

So this particular lifting problem asks for

- existence of the curves $\mathcal{Y}$ and $\mathcal{X}$ whose special fibers are the given curves Y and X
- an R-morphism $\mathcal{Y} \to \mathcal{X}$
- an action of the same group G on $\mathcal{Y}$ such that the morphism is a G-cover

It turns out that the first requirement can always be satisfied. It is a classical result that every smooth projective k-curve can be realized as the special fiber of an R-curve, due to Deuring, Grothendieck, Deligne-Mumford, Popp and others. However, having the compatible group action is harder to satisfy.

If G is a finite group for which all G-covers of k-curves lift over some R finite over $W(k)$, then G is called an *Oort group* for k. In the introduction we discussed what is known about Oort groups.

3.2 Local lifting problem

There is a different kind of lifting problem which seemingly doesn't talk about curves at all. This is called *local lifting problem*, and it concerns just extensions of complete discrete valuation rings.

Again, k is an algebraically closed field of characteristic p. We are concerned with complete discrete valuation rings of equal characteristic with residue field k. We know from Cohen structure theorem that such rings are always isomorphic to the ring of power series $k[[t]]$.

Suppose that A is a finite Galois extension of the valued ring $k[[t]]$, having a finite group G as a Galois group. Note that this implies that A itself is also a complete DVR with equal characteristic p, and thus it also has the same structure $A \cong k[[z]]$ for a uniformizer $z \in A$. Also since the power series ring $k[[t]]$ is henselian we know that there is only one extension of the valuation to A, so the action of G must preserve the valuation of A.

Let us recall some things from decomposition theory. First, the decomposition group of the extension is G itself as we just noticed that its action preserves the valuation. Second, there is an exact sequence of groups

$$1 \to I \to G \to Gal(k'|k) \to 1,$$

where I is the inertia group of the extension $A/k[[t]]$ and $Gal(k'|k)$ is the absolute Galois group of the residue extension. But we assumed k to be algebraically closed, so the residue extension must be trivial! Thus $Gal(k'|k) = 1$, so in fact the inertia group I must also be equal to G itself.

Next, we know various things about the structure of the inertia group, which in our case

is G. It has a filtration to subgroups called *ramification groups*, which we denote

$$G = G_0 \supseteq G_1 \supseteq \dots$$

The structure of the successive quotients G_i/G_{i+1} is known quite precisely:

- The first quotient G_0/G_1 is isomorphic to a (finite) subgroup of the multiplicative group $k^\times$, which means that it is cyclic and prime to p
- All higher quotients G_i/G_{i+1} for $i \geq 1$ are isomorphic to a subgroup of the additive group of k, so in particular they are direct products of copies of the cyclic group $\mathbb{Z}/p$.

For details of the derivations of these facts, see [Ser79, Ch IV]. We conclude that G_1 is a p-group, and G/G_1 is cyclic of order m prime to p. In fact G is a semidirect product $\mathbb{Z}/m \ltimes G_1$ of cyclic group $\mathbb{Z}/m$ prime to p, and a p-group G_1.

Now we can state the *local lifting problem*: again, let R be a finite extension of the Witt ring $W(k)$. We say that a G-extension $A/k[[t]]$ is *locally liftable over* R if there exists a G-extension $A_R/R[[T]]$ of rings such that the tensor product with k gives the original extension $A/k[[t]]$. By the derivation above, such extensions can only exist for groups that have the form $G = \mathbb{Z}/m \ltimes P$, where P is a p-group and m is prime to p. The relationship of this problem to the lifting problem of curves will become obvious shortly.

4 Reductions of lifting problems

4.1 Local-global principle

We are going to use two principles to reduce the lifting problem to a specific case of covering the projective line $\mathbb{P}^1$. Both principles allow us to transform the lifting problem to different formulations, and both of them have the important property that they preserve ramification groups of the covers or extensions.

The first of these principles is one kind of *local-global principle*. It transforms the lifting problem of a general branched cover to finitely many local lifting problems.

Consider the following situation:

- Let $Y \to X$ be a Galois-cover of smooth, projective, connected k-curves.
- Let $y_1, \ldots, y_s$ be the points of Y where the cover has nontrivial inertia group: denote the inertia group at y_j by I_j for $j = 1, \ldots, s$.
- Then each I_j acts on the complete local ring $\widehat{\mathcal{O}}_{y_j} \cong k[[z]]$, fixing the subring $\widehat{\mathcal{O}}_{x_j} \cong k[[t]]$ where $y_j \mapsto x_j \in X$ in the covering map.

Then we have the following theorem:

Theorem. *Let R be a finite ring extension of $W(k)$. In the situation above, the cover $Y \to X$ lifts over R iff each complete local extension $\widehat{\mathcal{O}}_y \hookleftarrow \widehat{\mathcal{O}}_x$ lifts over R.*

Saïdi [Sai12] has proven this using formal patching theory, as have Chinburg, Guralnick and Harbater [CGH08]. For this particular formulation see [Obu12, Theorem 3.1].

This result allows us to make a connection between Oort groups and *local Oort groups*. A group G is called a local Oort group, if every G-extension $k[[z]] \hookleftarrow k[[t]]$ of complete discrete

valuation rings lifts to characteristic zero, i.e. every local lifting problem with group G has a solution. It is true that G is an Oort group if and only if it is a local Oort group, although it doesn't quite trivially follow from the local-global principle.

Note: In this reduction, the ramification groups are automatically preserved: extension of complete local rings comes directly from the cover of curves.

4.2 HKG-covers of the projective line

The second reduction we will perform is transforming the local lifting problem back into geometric form, but a very specific case of the problem.

Let's first define a subclass of G-covers of curves.

Definition. *Let $Y \to \mathbb{P}^1_k$ be a G-cover of $\mathbb{P}^1$ over k. We say that it is a* Harbater-Katz-Gabber-cover *(or HKG-cover), if it satisfies the following requirements:*

- *The cover is étale outside $\{0, \infty\} \subseteq \mathbb{P}^1_k(k)$*
- *The cover is tamely ramified over ∞*
- *The cover is totally ramified over* 0

If we want to specify the group acting on Y, we may call $Y \to \mathbb{P}^1_k$ (somewhat clumsily) a "G-HKG-cover".

Suppose we are given such cover $Y \to \mathbb{P}^1_k$. Since it is totally ramified over 0, there is only one preimage of 0 in $Y(k)$, call it y. If we look at the cover locally at y, we can consider the extension of complete local rings $\widehat{\mathcal{O}}_y \hookleftarrow \widehat{\mathcal{O}}_{(t=0)} = k[[t]]$. Again, because the inertia group is all of G, this is a G-extension of complete local rings.

Thus we have a mapping from HKG-covers to G-extensions of $k[[t]]$. In fact this mapping has an inverse: as proven by Harbater [Har80] in the case $m = 1$ and Katz and Gabber in general [Kat86], this actually gives an equivalence of categories between the G-HKG-covers and G-extensions of $k[[t]]$: for every G-extension of $k[[t]]$ there is (essentially) a unique G-HKG-cover of $\mathbb{P}^1$ whose complete local ring extension at $t = 0$ is the given extension.

This also means that a G-extension of $k[[t]]$ lifts over a ring $R \hookleftarrow W(k)$ if and only if the corresponding G-HKG-cover lifts over R. We will use this and reduce the local lifting problem to a global lifting problem for HKG-covers. Thus we have gone from the global problem to local lifting problem, and then back to a specific case of the global problem.

5 Model theory generalities

5.1 First order languages

Let us recall the basics of first order logic. We will introduce the concepts that are most important for us, using the language of rings as an example. Rings are the structures we are mostly concerned with, so it is useful to see what the general model theoretical concepts look like in the case of rings.

We have to start with a *language*: a first order language may contain three kinds of symbols: relations, functions and constants. Both the relation and function symbols have specified their arity $n \geq 0$. Constants can be seen as functions with arity 0. Every language has equality symbol "=" built in automatically: it is a binary relation which is always interpreted as the equality of elements of the structure.

In the case of rings, the language $\mathcal{L}_{rings}$ contains two binary functions $+$ and $\cdot$, constants 0 and 1, and no relations other than equality.

A *structure* in a given language is a set of elements, together with interpretations of the symbols of the language with appropriate types. For instance, a structure in the language $\mathcal{L}_{rings}$ is a set R together with two functions $R^2 \to R$ (for addition and multiplication) and two distinguished elements $0, 1 \in R$. Note that the language itself only specifies the signature of the structure, it says nothing about what properties the structure must satisfy (such as an operation being commutative, associative etc.) For that we need formulas.

A *formula* in a language can be one of the following:

- an atomic formula, i.e. either equality of two terms, such as $1 + 0 = 1$ or $x + y = z$, or it can be a relation between some number of terms, such as $x \geq 0$ (assuming the

relation symbol $\geq$ is included in the language)

- any boolean combination of formulas is itself a formula, e.g.

$$\neg(x < 0) \vee (x \cdot x \geq 0).$$

- any formula under a quantifier is a formula, e.g.

$$\exists y(x = y \cdot y)$$

Note that the quantifier is always over the set of elements: $\exists y$ always means $\exists y \in R$ if R is the set of elements of the structure. We cannot quantify for instance over the functions from R to R, so for example we cannot say the following:

$$\exists f \colon R \to R \; (\forall x \in R \, \exists y \in R \, (f(y) = x) \wedge \exists x, y \in R \, (x \neq y \wedge f(x) = f(y)))$$

which would be equivalent to the set R being infinite. This is only possible in second-order logic, which we don't use in this thesis. In fact, finiteness of a structure cannot be expressed in first order.

For a structure of $\mathcal{L}_{rings}$ to be an actual ring, it has to satisfy some properties. The theory of commutative rings is axiomatized by the following formulas:

$$\begin{aligned}
&\{\forall x, y, z \, (x + (y + z) = (x + y) + z \wedge x(yz) = (xy)z), \\
&\forall x \, (x + 0 = x \wedge 1x = x1 = x), \\
&\forall x, y \, (x + y = y + x \wedge xy = yx), \\
&\forall x, y, z \; (x(y + z) = xy + xz) \, , \\
&0 \neq 1\}
\end{aligned}$$

With appropriate first order formulas, we can express all axioms of integral domains, fields, algebraically closed fields etc. For instance, the formula $\forall x \exists y (x = 0 \vee xy = 1)$ expresses that every nonzero element has an inverse.

We say that a theory is *complete* if it determines the truth of every sentence in the language. So if T is a complete theory, then for every sentence φ, the theory T must imply either φ or $\neg\varphi$. Note that every structure M has a complete theory: the complete theory satisfied by M is

$$Th(M) = \{\varphi \mid M \models \varphi\}.$$

We say that two structures M and N of the same language are *elementarily equivalent*, if they have the same complete theory: $Th(M) = Th(N)$. In other words they must satisfy exactly the same sentences in their language. In that case we will write $M \equiv N$.

Types One of the most useful concepts in model theory is types. (For introduction, see [Mar02, § 4.1]) If $\mathcal{L}$ is a language and T is a theory in the language $\mathcal{L}$, then the set $S_n(T)$ is defined to be the set of all complete consistent theories in a new language $\mathcal{L}(\bar{x})$ containing T, where we add a tuple $\bar{x} = (x_1, \ldots, x_n)$ of new variable symbols. The elements of $S_n(T)$ are called *types*. In other words an element $p \in S_n(T)$ is a set of formulas $\varphi(\bar{x})$ with free variables $\bar{x}$, such that for every such formula, p contains either $\varphi(\bar{x})$ or $\neg\varphi(\bar{x})$.

We say that an n-tuple $\bar{a}$ in a structure M of a theory T *satisfies* a type $p \in S_n(T)$ if it satisfies all the formulas in p. In other words, p is the type of $\bar{a}$, or

$$p = tp(\bar{a}) = \{\varphi(\bar{x}) \mid M \models \varphi(\bar{a})\}.$$

The type of $\bar{a}$ tells everything about the tuple $\bar{a}$ that can be expressed in first order. For instance, in the theory of rings the type of a tuple $\bar{a} \in R^n$ tells (among other things) which

polynomials in $R[x_1, \ldots, x_n]$ vanish at $\bar{a}$. It might tell other things as well, depending what kind of ring R is. Later we will see what the types look like in the case of algebraically closed fields.

The set of types $S_n(T)$ also has a topology, the so called *Stone topology*. The open subsets of $S_n(T)$ are generated by the sets

$$D(\varphi(\bar{x})) = \{p \in S_n(T) \mid p \ni \varphi(\bar{x})\}.$$

Note that these generating open sets satisfy $D(\neg\varphi(\bar{x})) = S_n(T) \setminus D(\varphi(\bar{x}))$, so they are in fact clopen. This means that the space $S_n(T)$ is 0-dimensional. It is also compact and Hausdorff, which makes it a lot easier to work with that the Zariski topology of schemes.

For a proper introduction to first order model theory, see e.g. [Mar02] or [Poi00].

Definable sets If M is a structure in some language, satisfying a complete theory T, then a *definable set* is $D \subseteq M^n$ for some n, such that there exists a formula $\varphi(\bar{x})$ with free variables $\bar{x} = (x_1, \ldots, x_n)$ such that

$$D = \{\bar{a} \in M^n \mid M \models \varphi(\bar{a})\}.$$

Note that two formulas $\varphi(\bar{x})$ and $\psi(\bar{x})$ define the same set if and only if

$$T \models \forall\bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})).$$

This means that we could as well take the equivalence classes of formulas under this equivalence relation to be definable sets. That way, it wouldn't depend on a particular model of the theory T.

Since a type in $S_n(T)$ is determined by the formulas it satisfies, we can also think of types

as determining exactly the definable sets it belongs to. In some sense types and definable sets are in dual position.

5.2 Algebraically closed fields

To us the most important first order theory we will use is the theory of algebraically closed fields. It is a quite well behaved theory: all formulas can be reduced to polynomial equations in a sense we will see shortly.

The language of fields is $\mathcal{L}_{rings}$, the same as the language of rings. The theory of algebraically closed fields include the axioms of commutative rings, the statement that every nonzero element has an inverse, and a statement that every monic polynomial of degree at least 1 has a root:

$$\forall a_1, a_2, \ldots, a_n \exists x \, (x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0).$$

We need one of these axioms for every $n \geq 1$.

These axioms together define the class of algebraically closed fields. The set of these is denoted by ACF. It is not a complete theory however: we didn't specify the characteristic. Once we specify the characteristic, it becomes complete: the theory ACF_p is the same as ACF together with the formula $1 + \cdots + 1 = 0$, where 1 is added p times. The theory ACF_0 is also ACF together with countably many formulas $1 + \cdots + 1 \neq 0$ for any number $n \geq 1$ of 1's added together. Both ACF_0 and ACF_p for p prime turn out to be complete theories.

The theory ACF has the property called *quantifier elimination*: for any formula $\varphi(\bar{x})$ in the language of fields with free variables $\bar{x}$, there exists a formula $\psi(\bar{x})$ with no quantifiers

that is equivalent to $\varphi(\bar{x})$, meaning

$$ACF \models \forall \bar{x}\,(\varphi(\bar{x}) \iff \psi(\bar{x})).$$

Note that even though the theory ACF is not complete, it still has quantifier elimination: the equivalent formula $\psi(\bar{x})$ can be chosen independently of the characteristic.

An important consequence of quantifier elimination is another property called *model completeness*. This means that any extension $k \hookrightarrow l$ of algebraically closed fields is an elementary extension, meaning that any tuple $\bar{x}$ in k has the same type in k and in l. In other words it satisfies the same formulas in k and l. If a formula $\varphi(\bar{x})$ is quantifier-free, then for any tuple $\bar{a} \in k$ satisfies it in k if and only it satisfies $\varphi(\bar{a})$ in l. Since every formula is equivalent to a quantifier-free one, we see that the same is true for every formula, so any tuple in k has the same type in k and l.

Because of quantifier elimination, any type $p \in S_n(k)$ (where $k \models ACF_p$) is determined by the polynomials in $k[x_1, \ldots, x_n]$ satisfied by any tuple of type p. Clearly the set of such polynomials has to be a prime ideal, so the types in $S_n(k)$ are in bijection with the points of $\mathbb{A}^n_k$, including both closed points and generic points of all closed subsets of $\mathbb{A}^n_k$.

5.3 Diagram and elementary diagram

Let's fix a first order language L and a structure M in that language. We want to define a new language and a theory which characterizes the *extensions* of the structure M. Define the language L_M to be L combined with constant symbols for every element $a \in M$. That is, it has the same function and relation symbols as L but we add a lot of new constant symbols.

We can now define a theory $\mathrm{diag}(M)$ to be the set of all quantifier-free formulas that are true in M, with elements taken from M:

$$\mathrm{diag}(M) = \{\varphi(\bar{a}) \mid \varphi(\bar{x}) \text{ q.f. formula}, \ \bar{a} \in M, M \models \varphi(\bar{a})\}$$

Note that this can be written as a sentence without free variables precisely because we have added constant symbols for every element of M.

Thus $\mathrm{diag}(M)$ contains formulas $a \neq b$ for any two different elements in M. Let N be any model of $\mathrm{diag}(M)$. Then N must have interpretations for every element of M, and they are all different elements. Thus we get an injective map $f\colon M \to N$.

This map is also a homomorphism: for instance if M has an operation $*$, then whenever elements of M satisfy $a * b = c$, then the corresponding elements of N must satisfy the same, because it was expressed by a quantifier-free formula:

$$f(a) * f(b) = f(c).$$

What this means is that we can identify M as a *submodel* of N, and in fact the models of $\mathrm{diag}(M)$ are exactly the extensions of the structure M.

Another construction is the *elementary diagram* of a structure M. The language is the same L_M as above, but the new theory $\mathrm{eldiag}(M)$ is different. Instead of just the quantifier-free formulas in M, we include all first order formulas:

$$\mathrm{eldiag}(M) = \{\varphi(\bar{a}) \mid \varphi(\bar{x}) \text{ first order formula}, \ \bar{a} \in M, M \models \varphi(\bar{a})\}$$

The elementary diagram is a strong theory: in fact it contains the complete first order theory of M (in the original language L). Again, any model N of $\mathrm{eldiag}(M)$ has a copy of the structure M inside it. But now, the embedding $f\colon M \to N$ is actually an *elementary*

embedding: for any tuple $\bar{a} \in M$, the image $f(\bar{a})$ satisfies exactly the same formulas as $\bar{a}$ does. In other words, the function f preserves the *types* of all elements (and tuples).

This kind of extension of M is called an *elementary extension*. We conclude that the models of eldiag(M) are exactly the elementary extensions of M.

5.4 Ultraproducts

We will now introduce the notations and some facts about ultraproducts that will be used later. Ultraproduct is a way of combining a set of structures into a new structure that will preserve many properties of the original structures. This is different for instance from the direct product: the direct product of fields is not itself a field.

Definition. *Suppose I is a nonempty set. An* ultrafilter *on I is a collection $\mathcal{U} \subseteq \mathcal{P}(I)$ of subsets of I satisfying the following conditions:*

- $\emptyset \notin \mathcal{U}$
- *if $A \subseteq B \subseteq I$ and $A \in \mathcal{U}$, then also $B \in \mathcal{U}$*
- *if $A, B \in \mathcal{U}$, then $A \cap B \in \mathcal{U}$*
- $I \in \mathcal{U}$
- *for all $A \subseteq I$ we have either $A \in \mathcal{U}$ or $I \setminus A \in \mathcal{U}$*

If we have a set I together with an ultrafilter $\mathcal{U}$, then the subsets A with $A \in \mathcal{U}$ are called "large" subsets of I. With this intuition, the axioms for ultrafilters make sense.

If some statement $\phi(i)$ is true for a large subset of the $i \in I$, we say that the statement

holds "for almost all $i \in I$". We will write

$$\forall_{\mathcal{U}} i \in I \colon \phi(i),$$

as a shorthand for

$$\exists A \in \mathcal{U} \colon (\forall i \in A \colon \phi(i)).$$

Suppose I is a set with an ultrafilter $\mathcal{U}$, and for all $i \in I$ we have a model M_i in the same first order language (e.g. fields, rings, ordered sets). Now we can define the ultraproduct of M_i as the set ${}^*M = \prod_{\mathcal{U}} M_i$ of equivalence classes of the cartesian product $\prod_{i \in I} M_i$ under the equivalence relation

$$(a_i) \sim (b_i) \iff \forall_{\mathcal{U}} i \in I \colon (a_i = b_i).$$

That is, we identify two tuples (a_i) and (b_i) if they agree for most $i \in I$.

The structure of ${}^*M$ is defined using the structures of the M_i: say they are ordered fields. Then the operations of ${}^*M$ is defined coordinatewise, e.g. for addition:

$$(a_i) + (b_i) = (a_i + b_i).$$

The ordering relation is defined as

$$(a_i) < (b_i) \iff \forall_{\mathcal{U}} i \in I (a_i < b_i).$$

The axioms of ultrafilters imply that these are well-defined.

An important property for ultraproducts is that they preserve all first order formulas:

Theorem (Łos)**.** *Let I be a set with an ultrafilter $\mathcal{U}$, and for each $i \in I$, let M_i be a structure in the same language. If $\varphi(\bar{x})$ is a formula in that language and $\bar{a}_i \in M_i$ is a tuple for each $i \in I$, then ${}^*M \models \varphi((\bar{a}_i))$ if and only if*

$$\forall_{\mathcal{U}} (M_i \models \varphi(\bar{a}_i)).$$

This is called Łos's theorem. This fact ensures that an ultraproduct of fields is a field and so on. The ultraproduct satisfies all first order properties that are satisfied by almost all of the M_i.

One special case of ultraproduct is the case where all the M_i are equal: in that case ${}^*M$ is called the *ultrapower* of M with the ultrafilter $\mathcal{U}$. The first order theory of ${}^*M$ will be the same as that of M.

Keisler-Shelah A crucial theorem we will need later is the Keisler-Shelah ultrapower theorem: two structures are elementarily equivalent if and only if they have isomorphic ultrapowers.

Theorem. *Let M and N be two structures of the same first order language, and assume they have the same complete first order theory. Then there exists a set I and an ultrafilter $\mathcal{U}$ on I so that*

$$\prod_{\mathcal{U}} M \cong \prod_{\mathcal{U}} N.$$

This was first formulated and proven by Keisler [Kei61] to follow from continuum hypothesis, and later by Shelah [She71] without set theoretic assumptions.

6 Model theory of valued fields

6.1 Ax-Kochen-Ershov principles

We are going to use some facts about model theory of the Witt ring $W(k)$. The ring $W(k)$ is a definable subset of its fraction field K, which is a complete discretely valued field, and has p as a uniformizer. This field falls under the class of finitely ramified fields.

Definition. *Let K be a valued field in mixed characteristic $(0, p)$, with valuation $v\colon K^\times \to \Gamma$. We say that K is* finitely ramified*, if there are only finitely many elements $\gamma \in \Gamma$ with $0 < \gamma < v(p)$.*

In many cases we know that the elementary theory of a valued field is determined by the elementary theory of its residue field and value group, by the so called *Ax-Kochen-Ershov principle*. In the case of finitely ramified fields the AKE-principle is true: If K and L are finitely ramified valued fields, whose value groups satisfy $vK \equiv vL$ and residue fields $Kv \equiv Lv$, then $K \equiv L$.

We are going to need a relative version of the AKE-principle:

Theorem. *Let $K \leq L$ be an extension of finitely ramified valued fields. If the extensions of value groups and residue fields are both elementary, then the extension of the valued fields itself is also elementary. That is, if $vK \preccurlyeq vL$ and $Kv \preccurlyeq Lv$, then $K \preccurlyeq L$.*

This result was proven by Ershov [Ers67] and independently by Ziegler [Zie72, Satz V.5.I.3]. See also [Kuh12]. Thus we know that if $k_1 \preccurlyeq k_2$ is an elementary extension of fields, it induces an elementary extension of valued rings $W(k_1) \preccurlyeq W(k_2)$. Recently Rideau has given another proof of this in terms of difference fields [Rid14, Cor 6.30].

6.2 Ultraproducts and Witt vectors

Let's study how the ring of Witt vectors over fields behaves in ultraproducts. As a set, we will consider $W(k)$ to be simply the set of functions $\mathbb{N} \to k$.

Suppose we have an indexed collection of fields k_i, where $i \in I$. We can make two kinds of ultraproduct constructions on Witt vectors:

- First construct the ultraproduct of k_i, say ${}^*k = (\prod_i k_i)/\mathcal{U}$. Then simply form the Witt ring of ${}^*k$, which is $W({}^*k)$. Set theoretically, this is the set of functions $\mathbb{N} \to {}^*k$.

- Alternatively, we can form the Witt rings $W(k_i)$ of each k_i, and form the ultraproduct of those. This we denote by ${}^*W(k)$, and as a set it is the ultraproduct of the function sets

$$ {}^*(\mathbb{N} \to k_i). $$

These two constructions are not the same: suppose $a \in W({}^*k)$. Then a is determined by $a_n \in {}^*k$ for all $n \in \mathbb{N}$, and a_n is determined by $a_{ni} \in k_i$ for $i \in I$.

What is the condition for two elements in $W({}^*k)$ to be equal? Say $a, b \in W({}^*k)$. Then we have an equivalence:

$$
\begin{aligned}
& a = b \\
\iff & \forall n \in \mathbb{N} : a_n = b_n \\
\iff & \forall n \in \mathbb{N} \, \forall_{\mathcal{U}} i \in I : a_{ni} = b_{ni}
\end{aligned}
$$

On the other hand, if $a \in {}^*W(k)$, then a is determined by $a_i \in W(k_i)$ for $i \in I$, so again

a consists of $a_{ni} \in k_i$. But now the condition for equality is:

$$\begin{aligned} & a = b \\ \iff & \forall_{\mathcal{U}} i \in I : a_i = b_i \\ \iff & \forall_{\mathcal{U}} i \in I \, \forall n \in \mathbb{N} : a_{ni} = b_{ni} \end{aligned}$$

These conditions for equality in ${}^*W(k)$ and $W({}^*k)$ are not the same. Namely, the equality in ${}^*W(k)$ is stronger, and we have a well-defined map ${}^*W(k) \to W({}^*k)$. But in the other direction we don't have a well defined map.

The only case where the sets would be the same is when the ultrafilter $\mathcal{U}$ satisfies *countable intersection property*, meaning that intersection of any countable collection of large sets is large. These ultrafilters are rare: the existence of such ultrafilter on an infinite set would imply the existence of a measurable cardinal. It is hence consistent with the axioms of set theory that there does not exist any ultrafilter with countable intersection property.

7 Model theory of curves and their covers

Projective varieties are subsets of $\mathbb{P}^n_k$ defined by a finite number of polynomials. As polynomials themselves have finitely many coefficients, every projective variety is defined by a finite amount of data in the field k. This allows us to use model theory of fields to talk about varieties.

What does it mean to "talk about varieties" in the language of fields? For this purpose, we will first introduce the concept of *interpretation*, and then show how sets of varieties and maps between them can be interpreted from the coefficient field.

7.1 Interpretations

We will use the concept of interpretation of some structure in the language of another structure.

Definition. *Let M be a structure in a language $\mathcal{L}$. We say that a structure N in another language $\mathcal{L}'$ is* interpreted from *M if it is defined in the following way:*

- *The set of elements of N is given by D/E, where $D \subseteq M^n$ is a definable set and $E \subseteq D \times D$ is a definable equivalence relation.*
- *For every relation symbol in $\mathcal{L}'$ of arity k, the relation in D^k is given by a definable set and it must be compatible with the equivalence relation E.*
- *Function symbols in $\mathcal{L}'$ are treated as relations, with the additional requirement that the interpretation must actually be a graph of a function.*

Often we say that some set A (possibly with some structure) is interpreted from a structure M if there is an obvious bijection between A and a set interpreted from M.

Example: fraction field A simple example of interpretation is the fraction field of an integral domain. Let A is an integral domain, considered a structure in the language of rings. We will define $K = \operatorname{Frac} A$ as an interpretation from A: first, the set of elements is

$$D = \{(x, y) \in A^2 \mid y \neq 0\}.$$

Clearly D is a definable set. We define an equivalence relation E on D by

$$(x_1, y_1)\, E\, (x_2, y_2) \iff x_1 y_2 = x_2 y_1.$$

Now D/E is the set of elements in $\operatorname{Frac} A$.

Also the field operations in $\operatorname{Frac} A$ can be defined with first order formulas: for instance, addition is defined by

$$\begin{aligned} &(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \\ \iff &(x_1 y_2 + x_2 y_1, y_1 y_2) = (x_3, y_3) \\ \iff &(x_1 y_2 + x_2 y_1) y_3 = y_1 y_2 x_3, \end{aligned}$$

which is a first order formula in A. It is straightforward to define multiplication and rest of the field structure.

If a structure N is interpreted from a structure M, then every sentence in N can be translated into a sentence in M by replacing all symbols of N with the corresponding formulas in M that define them. In other words, everything that can be expressed about N in its language, can be already expressed in the language of M.

For instance, any sentence about the field $\operatorname{Frac} A$ can be translated into a sentence in A. To say that every nonzero element in $\operatorname{Frac} A$ has an inverse, we translate the sentence

$\forall a \exists b(a = 0 \vee ab = 1)$ into a formula

$$\forall x_1, y_1(y_1 \neq 0 \to \exists x_2, y_2(y_2 \neq 0 \wedge (x_1 = 0 \vee x_1 x_2 = y_1 y_2))),$$

which is true in all integral domains, as it should be since the sentence $\forall a \exists b(a = 0 \vee ab = 1)$ is true in all fields.

We will use this fact about interpretation to translate statements about curves and covers to statements in the language of fields.

7.2 Varieties in the projective space

We want to give interpretations of various geometric objects in terms of the base field k. As always, we assume k to be algebraically closed field of characteristic p. We'll start from the sets $\mathbb{P}^n_k(k)$, that is, points of the projective space.

Points in the projective space As we know from geometry, the points in $\mathbb{P}^n(k)$ are in bijection with one-dimensional subspaces of k^{n+1}. They can be represented by nonzero tuples in k^{n+1}, identifying the ones that are scalar multiplies of each other. This gives an interpretation of $\mathbb{P}^n(k)$, as D/E, by defining $D = k^{n+1} \setminus \{0\}$, and the equivalence relation E as

$$(x_0, \ldots, x_n)E(y_0, \ldots, y_n) \iff \exists \lambda(y_0 = \lambda x_0 \wedge \cdots \wedge y_n = \lambda x_n).$$

Polynomials and varieties Projective varieties are subsets of $\mathbb{P}^n_k = \operatorname{Proj} k[T_0, \ldots, T_n]$ defined by a finite number of homogeneous polynomials. First, interpreting homogeneous polynomials of degree d is simple: they are linear combinations of monomials of degree d. Since there are $\binom{d+n}{n}$ monomials of degree d in the variables $T_0, \ldots, T_n$, such a polynomial

is determined by $\binom{d+n}{n}$ parameters from k. This means that we can define the set of homogeneous polynomials of degree d as

$$Poly_{d,n} = k^{\binom{d+n}{n}}.$$

Now, a variety inside $\mathbb{P}^n$ is defined by some number of polynomials of finite degree. Clearly we can't interpret all of them at once: that would be infinite dimensional collection of them. But if we bound the complexity, we can interpret the varieties defined by l polynomials of degree at most d:

$$Var_{d,l,n} = (\bigcup_{i \leq d} Poly_{i,n})^l.$$

If we have a variety $X \in Var_{d,l,n}$ and $p \in \mathbb{P}^n(k)$, the relation "$p \in X(k)$" is definable: it is true if and only if p satisfies all the polynomials in the definition of X. This gives a definable relation between points and varieties.

Jacobian matrix First, the set of matrices of size $m \times n$ is definable by simply listing the entries: $Matrix_{m,n} = k^{mn}$.

The map taking a variety $X \in Var_{d,l,n}$ and a point $p \in X(k)$ to the Jacobian matrix in $Matrix_{l,n+1}$ is also definable: its entries are the partial derivatives of the polynomials defining X evaluated at p. That is, if $X \subseteq \mathbb{P}^n_k$ is defined by polynomials $f_1, \ldots, f_l \in k[T_0, \ldots, T_n]$, then the Jacobian matrix is (a_{ij}) with

$$a_{ij} = \frac{\partial f_i}{\partial T_j}(p).$$

Note that this is not quite a well defined map $X(k) \to Matrix_{l,n+1}$: it depends on the particular homogeneous coordinates of the point. But taking a different coordinates for the

same point gives matrices that are scalar multiples of each other, and the only thing we will care about the matrix is its rank, so this is good enough for us.

If we have $A \in Matrix_{m,n}$ and an integer r, then the predicate "rank $A < r$" is equivalent to saying that all $r \times r$ minor determinants of A are zero. Clearly this is definable. With this we can also express "rank $A = r$" by

$$(\text{rank } A < r + 1) \wedge \neg(\text{rank } A < r).$$

Dimension and smoothness Let $X \in Var_{d,l,n}$ be a variety inside $\mathbb{P}^n$ and $p \in X(k)$ a point in it. One can see that the tangent space of X at p has dimension m if and only if the rank of the Jacobian matrix is equal to $n - m$. As we saw above, both the Jacobian matrix and its rank are definable, so this predicate is also definable. Denote this predicate by $TDim_m(X, p)$

If $X \in Var_{d,l,n}$ is a variety, we can express that X is smooth of (pure) dimension m by saying that the tangent space at every point in $X(k)$ has dimension m:

$$Smooth_m(X) \iff \forall p \in X(k)(TDim_m(X, p)).$$

Smooth curves From above we see in particular that the set of smooth varieties of pure dimension 1 (i.e. curves) inside $\mathbb{P}^n$ (with the fixed bounds d and l) is interpretable from k. Denote the set of smooth curves inside $Var_{d,l,n}$ by $SC_{d,l,n}$.

7.3 Maps between projective varieties

Rational maps Now let's move on to interpreting maps between varieties. Recall that a rational map between two projective spaces $\mathbb{P}^n$ and $\mathbb{P}^{n'}$ can be given by $n' + 1$ polynomials

in $k[T_0, \ldots, T_n]$ of the same degree d. The polynomials give a well-defined rational map as long as they are not all identically zero: this is a definable set

$$RatMap_d(\mathbb{P}^n, \mathbb{P}^{n'}) \subseteq (Poly_{d,n})^{n'+1}.$$

We can define which points $p \in \mathbb{P}^n(k)$ are in the domain of (the definition of) a rational map $f\colon \mathbb{P}^n \to \mathbb{P}^{n'}$ simply by checking whether some of the polynomials have nonzero value at the point p. Thus the relation "$p \in \mathrm{dom}(f)$" is a definable subset of $\mathbb{P}^n(k) \times RatMap_d(\mathbb{P}^n, \mathbb{P}^{n'})$.

Note that this only gives the points where the particular definition of the rational map is defined, so in fact the definable set $\mathrm{dom}(f)$ only gives an open subset of the domain of the actual rational map f. This will be enough for us.

Evaluating and comparing maps Consider the evaluation function

$$RatMap_d(\mathbb{P}^n, \mathbb{P}^{n'}) \times \mathbb{P}^n(k) \to \mathbb{P}^{n'}(k),$$

which takes $f\colon \mathbb{P}^n \to \mathbb{P}^{n'}$ and a point $p \in \mathbb{P}^n(k)$, and sends it to $f(p)$. It is a partial function: the value $f(p) \in \mathbb{P}^{n'}$ is defined when $p \in \mathrm{dom}(f)$. This function is definable, since it simply evaluates the polynomials at the point p.

Now, suppose we have two subvarieties $X \in Var_{m,l,n}$ and $Y \in Var_{m,l,n'}$. The set $RatMap_d(X, Y)$ of rational maps $X \to Y$ is the subset of $RatMap_d(\mathbb{P}^n, \mathbb{P}^{n'})$ of those maps f with

$$\mathrm{dom}(f) \cap X(k) \neq \emptyset \quad \text{and } \forall p \in \mathrm{dom}(f) \cap X(k)\colon (f(p) \in Y(k))$$

Both of these conditions are definable. We can also express that a rational map is not

constant:

$$NonConst(f) \iff \exists p, q \in \mathbb{P}^n(k) \colon (p, q \in \mathrm{dom}(f) \wedge f(p) \neq f(q))$$

Two rational functions are equal if they agree in the intersection of their domains

$$f = g \iff \forall p \in \mathrm{dom}(f) \cap \mathrm{dom}(g) \colon (f(p) = g(p)).$$

Note that it is enough for the functions to agree in some open subset of the variety where they are defined. If the functions were not the same, they would only agree in some closed subvariety of X.

Rational maps between smooth curves In the case that Y and X are smooth curves, every rational map is regular, and every nonconstant map is surjective. In that case we can define the set of morphisms from X to Y as the set rational maps, and they will automatically be regular.

Remark: Note that even between smooth curves, the way we defined rational maps doesn't let us have a definable total function from $X(k)$ to $Y(k)$. This is because even if the map itself is regular, the definition with specific polynomials might not work at every point. We could salvage this by defining a rational map by patching finitely many definitions, and requiring that they agree in the intersection of their domains and the union of their domains covers all of $X(k)$. That would add more complexity to the parametrization and for simplicity, we will deal with only one polynomial definition of the maps.

7.4 Group action on a curve

Now that we have language to talk about curves and maps between them, we can start talking about group actions and covers of curves, again in the first order language.

Fix a finite group G, and a bound d on degree. An action of G on a smooth curve $Y \in SC_{m,l,n}$ is defined by rational maps $h_g \in RatMap_d(Y, Y)$ for each $g \in G$ (we talk about rational maps because we have parametrization for them, but as we saw above they will in fact be regular). We require these maps to satisfy $h_1 = \mathrm{id}$ and $h_g \circ h_{g'} = h_{gg'}$ for all $g, g' \in G$. These are definable statements, so we conclude that the set of G-actions on Y (with bound d on the degrees) is a definable subset of $(RatMap_d(Y, Y))^{|G|}$.

Also saying that the G-action is faithful can be expressed with a first order formula: it means that $h_g \neq \mathrm{id}$ for all $g \neq 1$.

From now on, write gp instead of $h_g(p)$. If H is any subgroup of G, the set of points in $Y(k)$ whose stabilizer G_p is exactly H can be defined: for $g \in G$, we have

$$g \in G_p \iff gp = p.$$

For instance, the set of "unramified" points is the set of points p with $G_p = 1$, and it is a definable set.

7.5 G-covers of curves

Suppose we have a finite group G and two smooth curves $X \in SC_{m,l,n}$ and $Y \in SC_{m,l,n'}$. Then a G-cover from Y to X consists of the following data:

- A rational (nonconstant) map $f\colon Y \to X$
- A faithful action of G on the curve Y

We have seen that these can be interpreted over the field k, given a bound on the degree of f and the group action. In addition we require them to satisfy the following law:

$$\forall p, q \in Y(k)\,(f(p) = f(q) \iff \exists g \in G\colon (gp = q))\,.$$

In other words, the group action maps each fiber to itself and acts transitively on the fibers. Note that since G is a fixed finite group, the quantifier "$\exists g \in G$" can be expressed with a finite conjunction which is allowed in first order logic.

Thus the set $GCover_{G,d}(X, Y)$ of G-covers where degree of both f and maps of the G-action is bounded by d can be interpreted over the field k.

HKG-covers Next, we want to interpret the G-HKG-covers $f\colon X \to \mathbb{P}^1_k$, because later we want to make some statements quantifying over all of them. At this point, we should suppose the group G has the structure $G = \mathbb{Z}/m \ltimes P$, where m is prime to p and P is a p-group, because all inertia groups have this form. Recall that the conditions for being an HKG-cover is that f is unramified outside $\{0, \infty\}$, totally ramified over 0 and tamely ramified with index m over ∞.

These things can be expressed with formulas: for being totally ramified over 0 we can use formula such as

$$\exists! q \in X(k)(f(q) = 0),$$

namely being totally ramified means that the point 0 has only one preimage. Saying that f is unramified outside $\{0, \infty\}$ can be expressed by

$$\forall p \in \mathbb{P}^1(k) \setminus \{0, \infty\}\ \exists^{=|G|} q \in X(k)(f(q) = p),$$

in other words that the point $p \neq 0, \infty$ has exactly $|G|$ preimages in $X(k)$. Here we use the quantifier "$\exists^{=n}$" to specify the number of elements satisfying a predicate. This is easy to do in first order logic.

Finally, the condition at ∞ can be expressed by saying that the point ∞ has $|P|$ preimages

and each of those has stabilizer with order m:

$$\exists^{=|P|} q \in X(k)(f(q) = \infty) \bigwedge \forall q \in f^{-1}(\infty)(|G_q| = m).$$

Thus we can conclude that the HKG-covers with the fixed curve X (with fixed bound on degrees) can be parametrized. Remembering that smooth curves (again, with fixed bounds) can be parametrized over k, we can actually parametrize all HKG-covers with the fixed group G.

8 Ultraproducts of curves

8.1 Projective lines

We would like to combine the model theory of curves we did earlier with ultraproducts of fields. That is, if we have a collection of fields and curves defined over those fields, can we define ultraproduct of those curves, which would be a curve over the ultraproduct of the given fields?

Let's start with a simple situation: we have a collection of algebraically closed fields k_i of the same characteristic p indexed by $i \in I$. We want to look at the projective lines $\mathbb{P}^1_{k_i}$ over each field k_i, and find/define the ultraproduct of those curves, given an ultrafilter $\mathcal{U}$ of I. This would presumably be a curve over the field ${}^*k = \prod_{\mathcal{U}} k_i$.

The function field of $\mathbb{P}^1_{k_i}$ is the rational function field $K_i = k_i(t)$. The closed points of the curve correspond to discrete valuations of K_i, so if we have valuations $v_i \colon K_i^\times \to \mathbb{Z}$, it gives a closed point of $\mathbb{P}^1_{k_i}$.

Define ${}^*K$ to be the ultraproduct of all K_i:

$$ {}^*K = \prod_{\mathcal{U}} K_i. $$

Now if we are given any discrete valuations v_i on K_i, we can combine them to a valuation

$$ {}^*v \colon {}^*K \to {}^*\mathbb{Z}, $$

but this is not a discrete valuation: its image is in the bigger ordered abelian group ${}^*\mathbb{Z}$. In fact ${}^*K$ is not the function field we are looking for.

Note that the field ${}^*K$ is not the same as ${}^*k(t)$: any element of the latter has finite degree.

Consider the degree maps $\deg\colon K_i \to \mathbb{N}$. We can combine them to a map

$$^*\deg\colon {}^*K \to {}^*\mathbb{N}.$$

Again, this map goes to a bigger set than $\mathbb{N}$. Note however that the preimage of $\mathbb{N} \subseteq {}^*\mathbb{N}$ is a subfield of ${}^*K$: we can easily see that it is closed under the field operations.

In fact, the preimage happens to be exactly ${}^*k(t)$. To see this, suppose $f \in {}^*K$ has degree $n \in \mathbb{N}$. Then there is a large subset of $i \in I$ with $\deg(f_i) = n$, and this means that for those i,

$$f_i = \frac{p_i}{q_i} \quad \text{with } p_i, q_i \in k_i[t],\ \deg(p_i) + \deg(q_i) = n.$$

Because there are finitely many choices for the numbers $\deg(p_i), \deg(q_i)$, they have the same degree for a large subset of I. Thus we find polynomials $p(t), q(t) \in {}^*k[t]$ that define an element of ${}^*k(t)$, and $f = p(t)/q(t) \in {}^*k(t)$ is that element.

The field ${}^*k$ is also the function field of the curve $\mathbb{P}^1_{{}^*k}$, which turns out to be the ultraproduct of the curves $\mathbb{P}^1_{k_i}$ in some sense. For instance, the set of ${}^*k$-points of this curve is exactly the ultraproduct of the sets of k_i-points in the curves $\mathbb{P}^1_{k_i}$:

$$\mathbb{P}^1_{{}^*k}({}^*k) = \prod_{\mathcal{U}} (\mathbb{P}^1_{k_i}(k_i)).$$

This happens more generally, as we will see next.

8.2 Birational approach: valuations on function fields

Now, consider a more general situation: we have again a collection of algebraically closed fields k_i of characteristic p. Suppose for each i, we have a function field K_i represented as a finite separable extension of the rational function field $k_i(t)$.

We do need to make one crucial assumption: we assume that the genus of K_i as a function field over k_i is bounded. The genus here means the genus of the (unique) smooth projective curve over k_i with function field K_i. We will prove the following result:

Proposition. *Suppose $k_i \models ACF_p$ for all $i \in I$, and K_i is a function field in one variable over k_i. Assume that the genus of K_i is bounded. If we then define a field K as*

$$K = \{(f_i) \in \prod_{\mathcal{U}} K_i \mid \exists n \in \mathbb{N} \forall_{\mathcal{U}} i \in I(\deg(f_i) \leq n)\},$$

then the set of valuations on K is in bijection with the ultraproduct of the sets of valuations of each K_i.

Once we fix the genus, the degree of K_i over $k_i(t)$ is also bounded. Also, if $f \in K_i$ generates the field over $k_i(t)$, the minimal polynomial of f over $k_i(t)$ is bounded in the sense that it has bounded degree and all the coefficients have a bounded degree as elements of $k_i(t)$, the bound depending only on the genus.

This means that the field K_i is described by finite amount of data over k_i: the coefficients of the minimal polynomial of f over $k_i(t)$, which themselves have bounded degree. This means we can move over to ultraproducts: let ${}^*k$ be an ultraproduct of the fields k_i.

Construct a polynomial over ${}^*k(t)$ by choosing a generator f_i of each K_i over $k_i(t)$ and consider its minimal polynomial. We can map the minimal polynomials to a polynomial over ${}^*k(t)$ as we saw above that they are bounded. This new polynomial will be irreducible because all the minimal polynomials of f_i are irreducible. Denote by K the field extension of ${}^*k(t)$ by adjoining a root of this polynomial.

What is the relationship between K and the ultraproduct of the K_i? As we did above for projective lines, consider the degree function from each $K_i^\times$ to $\mathbb{N}$, defined to be the sum

of absolute values of the valuations:

$$\deg\colon K_i^\times \to \mathbb{N}$$

$$\deg(g) = \sum_v |v(g)|$$

Again, these degree functions can be combined to get a function

$${}^*\deg\colon \prod_{\mathcal{U}} K_i \to {}^*\mathbb{N}.$$

We will see shortly that K is exactly the subset of elements in $\prod_{\mathcal{U}} K_i$ whose degree is actually in $\mathbb{N} \subseteq {}^*\mathbb{N}$.

Suppose an element $\alpha \in K_i$ has degree bounded by some $n \in \mathbb{N}$. We can see that α can be written as a $k_i(t)$-linear combination of powers of the generator f_i, and in fact the degrees of the coefficients in $k_i(t)$ have a bound that only depends on n.

If we have an element $(\alpha_i) \in \prod_{\mathcal{U}} K_i$ whose degree is finite, then there is some $n \in \mathbb{N}$ such that $\deg(\alpha_i) = n$ for most i. This means that every such α_i can be written as a linear combination of the powers of f_i with the same bound on the coefficients, so those coefficients depend on finite amount of data from the fields k_i. Now we can again combine that data together to the ultraproduct, so we get a ${}^*k(t)$-linear combination of the generator of K, i.e. we get an element of K.

Conversely, we clearly have a map from K to the ultraproduct of K_i which preserves the degree. We conclude that again, we can identify K with the subfield of $\prod_{\mathcal{U}} K_i$ with bounded degree:

$$K \cong \{\alpha \in \prod_{\mathcal{U}} K_i \mid {}^*\deg(\alpha) \in \mathbb{N}\}.$$

What are the valuations of K? We are interested in the points of the smooth projective curve with function field K, which correspond to valuations of K. Suppose we have a

valuation v_i on each K_i, so we have a map $v_i \colon K_i^\times \to \mathbb{Z}$. These can be combined into a valuation

$$^*v \colon \prod_{\mathcal{U}} K_i \to {}^*\mathbb{Z},$$

so we have (possibly non-discrete) valuation of the ultraproduct. However, if we restrict it to the subfield K, we actually get a map $K^\times \to \mathbb{Z}$: if $\alpha \in K$, then it comes from some (α_i) and we have for most i

$$|v_i(\alpha_i)| \leq \deg(\alpha_i) = {}^*\deg(\alpha) \in \mathbb{N},$$

since we chose the element α from the subfield K. Thus the valuations of α_i are actually bounded by the degree, so we get a map $v \colon K^\times \to \mathbb{Z}$.

Recall that the ${}^*k$-points of the smooth projective curve with function field K is in bijection with the discrete valuations of the field K. We have now constructed a map from the ultraproduct of k_i-points of the curve X_i with function field K_i to the ${}^*k$-points of the curve X with function field K. In other words, we have a map

$$\prod_{\mathcal{U}} X_i(k_i) \to X({}^*k).$$

To see that this map is actually a bijection, we will consider these curves in terms of how they are embedded to projective spaces.

8.3 Embedding to projective space

Another way to approach ultraproduct of curves is to consider curves as subvarieties of $\mathbb{P}^n$. This way we will be able to prove that the set of points of the ultraproduct is given by the ultraproduct of points on the individual curves. In other words, that the map we defined above is bijective.

Again, suppose X_i is a curve over the field k_i with bounded genus. This means we may as well assume that they all have genus g. Then, as we have seen earlier, we have a bound on n, d, m such that all of the curves can be embedded in the projective space $\mathbb{P}^n$ onto a smooth curve defined by at most m polynomials of degree at most d.

Suppose the curve X_i is defined as a subset of $\mathbb{P}^n_{k_i}$ by polynomials $f^i_1, \ldots, f^i_m$ of degree d. Then we can combine these to get polynomials ${}^*f_1, \ldots, {}^*f_m$ over the field ${}^*k$ that define a curve in $\mathbb{P}^n_{{}^*k}$. These are still well defined polynomials since we have the bounds on the degrees. Let ${}^*X$ be the curve defined by ${}^*f_1, \ldots, {}^*f_m$.

What are the ${}^*k$-points of ${}^*X$? They are points in $\mathbb{P}^n({}^*k)$ which satisfy all the polynomials ${}^*f_1, \ldots, {}^*f_m$. Since this is a definable set over ${}^*k$, it is preserved in ultraproduct: if $\bar{a} = (a_0, \ldots, a_n)$ are the homogeneous coordinates of a point in $\mathbb{P}^n({}^*k)$, then we have equivalence

$$\begin{aligned}
&\bar{a} \in {}^*X({}^*k) \\
\iff &{}^*f_j(\bar{a}) = 0 \quad \text{for } j = 1, \ldots, m \\
\iff &\forall_{\mathcal{U}} i \in I \, \forall j = 1, \ldots, m \colon (f^i_j(\bar{a}^i) = 0) \\
\iff &\forall j = 1, \ldots, m \, \forall_{\mathcal{U}} i \in I \colon (f^i_j(\bar{a}^i) = 0) \\
\iff &\forall j = 1, \ldots, m \colon (\bar{a}^i \in X_i(k_i)).
\end{aligned}$$

In other words, the point set of the curve ${}^*X$ is the ultraproduct of the point sets of the individual curves X_i.

9 Reduction with a fixed ring extension

9.1 Statement

We want to make a reduction of the lifting problem of G-covers of curves. Specifically, we want to show that the liftability of certain kinds of covers doesn't depend on the field it is defined over. Instead of working with the general formulation of the lifting problem, we use the reductions described earlier and only consider the case of HKG-covers $Y \to \mathbb{P}^1$. Note that the local-global principle and HKG-covers imply that G being an Oort group is equivalent to every G-HKG-cover having a lifting.

First, we fix some parameters of the lifting problem:

- Fix the finite group $G = \mathbb{Z}/m \ltimes P$ acting on the curve Y, where P is a p-group and m is prime to p. We may assume the group has this form because it is going to be the inertia group of a cover at a point, and (as we saw in Section 3) the inertia group will always have this form.

- Fix a bound g on the genus of Y: we consider the curves Y with genus at most g. (Alternatively we could assume a bound on the ramification groups over $0 \in \mathbb{P}^1(k)$)

- We fix π which is an algebraic integer over $\mathbb{Z}_p$, and we will always consider the ring extension $W(k)[\pi]$ of $W(k)$. Denote this ring by $R(k) = W(k)[\pi]$.

Note that we *do not* fix the field k: the purpose of this section is to show that the lifting problem is independent of k in a certain sense.

Remark: The fact that we only consider rings of the form $W(k)[\pi]$ is not a serious restriction. It is proven by Pop [Pop14] that if a cover lifts over some finite extension of $W(k)$, then

there exists a lifting over a ring of the form $W(k)[\pi]$ as above.

Define a class $C_{G,g,\pi}$ of fields as follows:

Definition. *Field $k \models ACF_p$ is in class $C_{G,g,\pi}$ if every G-HKG-cover $Y_k \to \mathbb{P}^1_k$ over k with genus of Y at most g has a lifting over the ring $R(k) = W(k)[\pi]$.*

Recall that by G-HKG-cover we mean a G-cover that is a HKG-cover.

The aim of this section is to prove the following result:

Theorem. *The class $C_{G,g,\pi}$ is an elementary class within ACF_p, which means that it contains either all the fields in ACF_p or none of them.*

Consequences What does this theorem mean for Oort groups? This result does not answer the question on whether being an Oort group depends on the field k. If G is an Oort group, it means that for every G-cover there exists a ring R and a lifting of the cover over R. What this result talks about is the statement: for every genus g there exists a ring $R_g \hookleftarrow W(k)$ of the form $R_g = W(k)[\pi_g]$ such that every G-cover over k with genus g has a lifting over R_g. The theorem above says that this stronger statement does not depend on k.

It could be possible that there is an Oort group which does not allow a fixed π that gives a ring extension of $W(k)$, even for a fixed genus. That kind of group would be an Oort group but would not satisfy the stronger statement. If we can prove that being an Oort group implies that the ring extension is bounded for a bounded genus, then this would also imply that being Oort is independent of k.

Strategy of proof For brevity, write C for the class $C_{G,g,\pi}$. Our strategy for proving this statement is to use ultraproducts:

1. Prove that C is closed under ultraproducts

2. Prove that if an ultrapower ${}^*k$ of a field k is in C, then k itself is in C

Now, by the fact that any two elementarily equivalent models have isomorphic ultrapowers, these two facts will imply our proposition. Namely, if k and l are both algebraically closed fields of characteristic p, then they satisfy the same complete first order theory. Thus, by Keisler-Shelah theorem, there is an ultrafilter $\mathcal{U}$ on some set such that the ultrapowers are isomorphic: $k^{\mathcal{U}} \cong l^{\mathcal{U}}$. If we have proven the two steps above, we have equivalence

$$k \in C \iff k^{\mathcal{U}} \in C \iff l^{\mathcal{U}} \in C \iff l \in C,$$

so k is in the class C exactly when l is.

9.2 Proof of Step 1

First we want to prove that the class C is closed under ultraproducts: that is, let k_i be a field in the class C for all i in some set I, and let ${}^*k$ be an ultraproduct of the fields k_i. We want to prove that ${}^*k$ is also in C.

Suppose that $Y_{{}^*k} \to \mathbb{P}^1_{{}^*k}$ is a G-HKG-cover of curves. What we want to show is that there is a lifting of this cover over $R({}^*k) = W({}^*k)[\pi]$.

The curve $Y_{{}^*k}$ and the cover $Y_{{}^*k} \to \mathbb{P}^1_{{}^*k}$ are defined by a finite number of polynomials equations: the curve is embedded in some projective space and the cover is a regular map to $\mathbb{P}^1$. We can take the coefficients of these polynomials and map them to almost all k_i, which gives us covers $Y_{k_i} \to \mathbb{P}^1_{k_i}$ for all i.

The following things are true for each curve Y_{k_i}:

- The G-action on Y_{*k} is also defined by some polynomials, and those polynomials give rise to a G-action on Y_{k_i}. It is a faithful G-action, so we get a smooth G-cover $Y_{k_i} \to \mathbb{P}^1_{k_i}$.

- The ramification of the cover $Y_{k_i} \to \mathbb{P}^1_{k_i}$ is the same as the ramification of the original cover for almost all i. This is because the ramification filtration depends on the polynomials defining the G-action. In particular, they have the same ramification filtration at $t = 0$, they are tamely ramified at $t = \infty$ and unramified elsewhere.

- This means that almost all of the covers $Y_{k_i} \to \mathbb{P}^1_{k_i}$ are HKG-covers with the same ramification at $t = 0$ as the original cover.

As we assume that the fields k_i are in the class $C_{G,g,\pi}$, we know that each of these covers has a lifting over the ring $R_i = R(k_i)$. Denote the lifting by $\mathcal{Y}_{R_i} \to \mathbb{P}^1_{R_i}$.

Now, to prove part 1 we have to come up with a smooth G-cover of curves over $R({}^*k)$ whose special fiber is $Y_{*k} \to \mathbb{P}^1_{*k}$.

We can take the ultraproduct of the curves $\mathcal{Y}_{R_i}$ to get a curve $\mathcal{Y}_{*R}$. This requires that all of the liftings $\mathcal{Y}_{R_i}$ are embedded into $\mathbb{P}^N$ for a bounded N, and the polynomials defining the curve have bounded degrees, and also that the polynomials defining the group action by G have bounded degree. We know that this is true because each curve $\mathcal{Y}_{R_i}$ have the same genus as its special fiber Y_{k_i}. As these curves Y_{k_i} all come from the original curve Y_{*k}, they all have the same genus. This implies that all $\mathcal{Y}_{R_i}$ embed into the same projective space and that their degrees are bounded.

As $\mathcal{Y}_{R_i}$ is a curve over R_i, their ultraproduct is a curve over the ring

$$ {}^*R = \prod_{\mathcal{U}} R_i = (\prod_{\mathcal{U}} W(k_i))[\pi] = {}^*W(k)[\pi], $$

which is not what we wanted: our goal is to find a lifting over the ring $R({}^*k)$. Luckily, there is a canonical map ${}^*W(k) \to W({}^*k)$: the elements of $W(k_i)$ are sequences $(a_{i0}, a_{i1}, \dots)$ of elements of k_i. An element of ${}^*W(k)$ is then a $\mathcal{U}$-tuple of such sequences. If two such tuples are equal, they must be equal at every component, so we can send a tuple of sequences to a sequence of tuples. This is precisely the map we defined in Section 6.

This map ${}^*W(k) \to W({}^*k)$ can clearly be extended to a map ${}^*R(k) \to R({}^*k)$. Now we can use this map to form the base change of $\mathcal{Y}_{{}^*R(k)} \to \mathbb{P}^1_{{}^*R(k)}$ to get a cover of curves

$$\mathcal{Y}_{R({}^*k)} \to \mathbb{P}^1_{R({}^*k)}.$$

Is this a lifting of the original $Y_{{}^*k} \to \mathbb{P}^1_{{}^*k}$? Consider the map ${}^*R(k) \to {}^*k$: it is equal to the composition

$${}^*R(k) \to R({}^*k) \to {}^*k.$$

The base change of each cover $\mathcal{Y}_{R_i} \to \mathbb{P}^1_{R_i}$ is the cover $Y_i \to \mathbb{P}^1_{k_i}$, and thus the base change of the ultraproduct

$$\mathcal{Y}_{{}^*R(k)} \to \mathbb{P}^1_{{}^*R(k)}$$

is equal to the ultraproduct of the base changes $Y_{{}^*k} \to \mathbb{P}^1_{{}^*k}$. This means that also the special fiber (i.e. base change under $R({}^*k) \to {}^*k$) of $\mathcal{Y}_{R({}^*k)} \to \mathbb{P}^1_{R({}^*k)}$ is equal to the cover $Y_{{}^*k} \to \mathbb{P}^1_{{}^*k}$, so it has a smooth lifting like we wanted.

9.3 Proof of Step 2

Next we want to prove the other direction: if k is a field whose ultrapower ${}^*k$ is in the class $C_{G,g,\pi}$, then k itself is in $C_{G,g,\pi}$. Suppose that ${}^*k \in C_{G,g,\pi}$.

Let $Y_k \to \mathbb{P}^1_k$ be a G-HKG-cover of curves. We want to construct a lifting of this cover over the ring $R(k)$. First, form the base change of this cover under the diagonal embedding $k \hookrightarrow {}^*k$ to get a G-cover $Y_{{}^*k} \to \mathbb{P}^1_{{}^*k}$. This is also a HKG-cover, as the base change preserves the ramification behaviour of the cover. (We also see this because the base change is really the ultrapower of copies of our original cover.)

Now, by the assumption that ${}^*k \in C_{G,g,\pi}$, we know that the cover $Y_{{}^*k} \to \mathbb{P}^1_{{}^*k}$ has a lifting over $R({}^*k)$, denote it by

$$\mathcal{Y}_{R({}^*k)} \to \mathbb{P}^1_{R({}^*k)}.$$

Recall that the diagonal map $k \hookrightarrow {}^*k$ is an elementary embedding. We know by AKE-principle that $W(k)$ and $W({}^*k)$ are elementarily equivalent, which implies that also the rings $R(k)$ and $R({}^*k)$ are elementarily equivalent. This means that $R({}^*k)$ can be elementarily embedded into an ultrapower of $R(k)$, denote this by $R({}^*k) \hookrightarrow *R(k)$. Note that the two "stars" might be different: we don't necessanily have a map $R({}^*k) \hookrightarrow {}^*R(k)$.

We can also do the same with the elementary diagram of $R(k)$. The models of this theory are elementary extensions of $R(k)$, and again by the AKE-principle the ring $R({}^*k)$ is such an extension. This way we can make sure that the embedding $R({}^*k) \hookrightarrow *R(k)$ is an $R(k)$-homomorphism.

Now we can form the base change of the cover $\mathcal{Y}_{R({}^*k)} \to \mathbb{P}^1_{R({}^*k)}$ to get a new cover

$$\mathcal{Y}_{*R(k)} \to \mathbb{P}^1_{*R(k)}.$$

What does the curve $\mathcal{Y}_{*R(k)}$ look like? Since the cover is defined over the ring $*R(k)$, we can consider it as an ultraproduct of covers over $R(k)$.

Taking the special fiber of $\mathcal{Y}_{*R(k)} \to \mathbb{P}^1_{*R(k)}$ then gives a cover $Y_{*k} \to \mathbb{P}^1_{*k}$ over the

"big" ultrapower of k. Because we constructed the embedding $R(^*k) \to {}^*R(k)$ to be an $R(k)$-homomorphism, the residue extension ${}^*k \to {}^*k$ is also a k-embedding. The functoriality of base change (and special fiber) then implies that this special fiber

$$Y_{^*k} \to \mathbb{P}^1_{^*k}$$

is the base change of our original cover $Y_k \to \mathbb{P}^1_k$ in the diagonal embedding $k \hookrightarrow {}^*k$.

Since the base change is liftable over ${}^*R(k)$, the lifting gives a lifting over $R(k)$ in almost all coordinates of the ultrapower. In particular, this means the set of liftings must be nonempty.

References

[BW06] Irene I Bouw and Stefan Wewers. The local lifting problem for dihedral groups. *Duke Mathematical Journal*, 134(3):421–452, 2006.

[CGH08] Ted Chinburg, Robert Guralnick, and David Harbater. Oort groups and lifting problems. *Compositio Mathematica*, 144(04):849–866, 2008.

[CGH11] Ted Chinburg, Robert Guralnick, and David Harbater. The local lifting problem for actions of finite groups on curves. In *Annales scientifiques de l'Ecole normale supérieure*, volume 44, pages 537–605. Elsevier, 2011.

[Ers67] Yuri Ershov. On the elementary theory of maximal valued fields III. *Algebra i Logika Sem.*, 6(3):31–38, 1967.

[GM98] Barry Green and Michel Matignon. Liftings of Galois covers of smooth curves. *Compositio Mathematica*, 113(3):237–272, 1998.

[GMP90] Barry Green, Michel Matignon, and Florian Pop. On valued function fields II regular functions and elements with the uniqueness property. *J. reine angew. Math*, 412:128–149, 1990.

[GMP92] Barry Green, Michel Matignon, and Florian Pop. On valued function fields III, reductions of algebraic curves. *J. reine angew. Math*, 432:117–133, 1992.

[Gro71] Alexandre Grothendieck. Séminaire de géométrie algébrique du Bois Marie-1960-61 - Revêtements étales et groupe fondamental-(SGA 1). *Lecture notes in mathematics*, 224, 1971.

[Har80] David Harbater. Moduli of p-covers of curves. *Communications in Algebra*, 8(12):1095–1122, 1980.

[Kat86] Nicholas M Katz. Local-to-global extensions of representations of fundamental groups. In *Annales de l'institut Fourier*, volume 36, pages 69–106, 1986.

[Kei61] H Jerome Keisler. Ultraproducts and elementary classes. In *Indagationes Mathematicae (Proceedings)*, volume 64, pages 477–495. Elsevier, 1961.

[Kuh12] Franz-Viktor Kuhlmann. The algebra and model theory of tame valued fields. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2012.

[Mar02] David Marker. *Model theory: an introduction*. Springer, 2002.

[Mir95] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5. American Mathematical Soc., 1995.

[Obu12] Andrew Obus. The (local) lifting problem for curves. In *Galois-Teichmüller Theory and Arithmetic Geometry*, volume 63 of *Advanced studies in pure mathematics*, pages 359–412. Mathematical Society of Japan, 2012.

[Oor87] Frans Oort. Lifting algebraic curves, abelian varieties, and their endomorphisms to characteristic zero. *Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985)*, 46:165–195, 1987.

[Oor95] Frans Oort. Some questions in algebraic geometry. *Utrecht University*, 1995.

[OW14] Andrew Obus and Stefan Wewers. Cyclic extensions and the local lifting problem. *Annals of Mathematics*, 180(1):233–284, 2014.

[Pag02] Guillaume Pagot. *Relèvement en caractéristique zéro d'actions de groupes abéliens de type (p,..., p)*. PhD thesis, Bordeaux 1, 2002.

[Poi00] Bruno Poizat. *A course in model theory: an introduction to contemporary mathematical logic*. Springer Science & Business Media, 2000.

[Pop14] Florian Pop. The Oort conjecture on lifting covers of curves. *Annals of Mathematics*, 180(1):285–322, 2014.

[Rid14] Silvain Rideau. Some properties of analytic difference fields. *arXiv preprint arXiv:1401.1765*, 2014.

[Sai12] Mohamed Saidi. Fake liftings of Galois covers between smooth curves. In *Galois-Teichmüller Theory and Arithmetic Geometry*, volume 63 of *Advanced studies in pure mathematics*, pages 457–501. Mathematical Society of Japan, 2012.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67. Springer New York, 1979.

[She71] Saharon Shelah. Every two elementarily equivalent models have isomorphic ultrapowers. *Israel Journal of Mathematics*, 10(2):224–233, 1971.

[SOS89] Tsutomi Sekiguchi, Frans Oort, and Noriyuki Suwa. On the deformation of Artin-Schreier to Kummer. In *Annales scientifiques de l'École Normale Supérieure*, volume 22, pages 345–375. Société mathématique de France, 1989.

[Zie72] Martin Ziegler. *Die elementare Theorie der henselschen Körper: Diss.* Universität Köln, 1972.