Incidence systems on Cartesian powers of curves

VERSION OF JANUARY 18, 2017

Assaf Hasson and Dmitry Sustretov [1]

Abstract

We show that a non-locally modular reduct of the Zariski structure of an algebraic curve interprets a field. This answers a question of Zilber's.

Contents

[1]Has been supported by a fellowship of the Center for Advanced Studies in Mathematics at Ben-Gurion University of the Negev during the work on the article. The research leading to these results has received funding from the European Research Council under the European Unions Seventh Framework Programme (FP7/2007- 2013)/ERC Grant Agreement No. 291111.

1 Introduction

Zilber's trichotomy principle (to be described in more detail below) has an unsual status in mathematics. Conjectured in various forms by Zilber throughout the late 1970s, essentially every aspect of the conjecture was refuted by Hrushovski [20], [19] in the late 1980s. Due to Hrushovski's zoo of counterexamples the conjecture has never been reformulated. Yet, Zilber's principle remains a central and powerful theme in model theory: it has been proved to hold in many natural examples such as differentially closed fields of characteristic 0, algebraically closed fields with a (generic) automorphism, o-minimal theories and more (see [7, 34, 31, 8, 24]). Many of these special cases of Zilber's trichotomy had striking applications in algebra and geometry ([21, 22, 37]).

A relatively recent application of one such result is Zilber's model theoretic proof [42] of a significant strengthening of a theorem of Bogomolov, Korotiaev, and Tschinkel ([3]). The model theoretic heart of Zilber's proof is Rabinovich' trichotomy theorem for *reducts* of algebraically closed fields [36]. In the concluding paragraph of the introduction to [42] Zilber writes: "It is therefore natural to aim for a new proof of Rabinovich' theorem, or even a full proof of the Restrited Trichotomy along the lines of the classification theorem of Hrushovski and Zilber [24], or by other modern methods [...]. This is a challenge for the model-theoretic community."

The conjecture referred to in Zilber's text above can be formulated as follows:

Conjecture A. *Let (M, Ω_0) be a non-locally modular strongly minimal reduct of an algebraic curve M over an algebraically closed field K. Then, there exist definable $L, E \in \Omega_0$ such that $E \subseteq L \times L$ is an equivalence realtion with finite equivalence classes and L/E with the induced structure from (M, Ω_0) is a field K-definably isomorphic to K.*

Rabinovich [36] proved Conjecture A in the special case where $M = \mathbb{A}^1$, and her result can be extend by general principles to any rational curve. In the present paper we prove Conjecture A. Our proof (Theorem 6.15), despite Zilber's expectations as quoted above, is geometric in nature and does not use any advanced model theoretic machinery. Roughly, it proceeds in four main steps:

1. Given a reduct (M, Ω_0) of the full Zariski structure on an algebraic curve M, the non-modularity assumption provides a definable 2-dimensional (almost) faithful family $X \subseteq M^2 \times T$ of curves in M^2. Throughout the text we make the assumption that for almost all $t \in T$ the curve X_t is pure-dimensional (i.e., it does not have 0-dimensional irreducible components). This assuption considerably simplifies the discussion, and is justified in Section 6.

2. We introduce the notion of the slope of a curve $C \subseteq M^2$ at a point $P \in C$, and use it to define when two curves $X_t, X_s \in X$ incident to P are tangent at that point. The main technical observation is that this geometric notion of tangency can be detected (up to an equivalence relation with finite classes)

definably in the reduct. That is, that there exists a definable set $T_0 \subseteq T \times T$ and an equivalence relation E with finite classes, such that for any $(t,s) \in T_0$ there are $t'Et$ and $s'Es$ such that $X_{t'}$ is tangent to $X_{s'}$ at P, Proposition 5.18.

3. This allows us, using our assumption of the first clause and – by now – standard model theoretic machinery, to reconstruct a 1-dimensional algebraic group in the reduct, Subsection 5.6.

4. The above reduces us to proving Conjecture A in the context where (M,Ω_0) is a non-locally modular expansion of a 1-dimensional algebraic group. This problem was studied by Marker and Pillay in the context of the additive group in characteristic 0, [27]. In Subection 5.8 we show how to apply the tools developed in the previous sections to generalise the result of [27] to the present, fully general, context (Theorem 5.24).

The general scheme of our proof seem to have much in common with Rabinovich' original work, though we were unable to understand significant parts of her argument which are highly technical. Step (2) of the above strategy is at the conceptual and technical heart of the paper, and it relies – ultimately – on classical, but non-trivial intersection theory. As Rabinovich' main tool for studying intersections of plane curves is the classical Bezout theorem, it stands to reason that the more advanced tools applied in Sub-section 5.5 are at the source of the greater generality of the present paper. We also believe that our more liberal application of algebro-geometric tools such as non-reduced schemes helped simplify the exposition, considerably lowering the level of combinatorial complexity.

As in Rabinovich' work — and in most of the works which followed it — step (3) of the above strategy, the reconstruction of a group from a 1-dimensional family $S \subseteq M^2 \times T$ of curves incident to a point $(Q,Q) \in M^2$ is obtained as follows: pick $s,t \in T$ independent generics, find $r \in T$ such that the curve S_r is tangent to (in our termonology: "has the same slope as") the curve $S_s \circ S_r$ at (Q,Q), and prove that the mapping $(s,t) \mapsto r$ is (almost) definable and is (roughly) a group operation on T. This strategy can only work if the set of slopes of the family S at the point (Q,Q) is infinite. For a field K in characteristic 0 this is fairly easy, and follows from the uniqueness of solutions of ordinary differential equations for formal power series over K. This is, of course, not the case in characteristic $p > 0$ where the kernel of derivation is non-trivial. This calls for extra care in the choice of the family S, and we were unable to avoid having to work with high-order slopes, which is the source of some additional technicalities. This allows us to reconstruct a 1-dimensional algebraic group[2], which we then – using a case by case analysis – apply to construct a 2-dimensional family of plane curves with an infinite set of 1-slopes at every generic point of the diagonal.

It seems that the tools developed in the present paper can be extended to various other contexts our the tools developed in the present paper can be adapted to other

[2]In a similar situation Rabinovich, [36, Section 8, p.93] seems to claim that she can actually recover an additive subgroup of $(K^2,+)$, given rise to a characteristic-independent argument.

contexts as well. E.g., extending the results of [25] to positive characteristic, and any algebraic group and – possibly – even a full proof of the restricted trichotomy conjecture for structures interpretable in ACVF[3].

Section 6 seems to have no obvious counterpart in existing model theoretic literature. It seems that the results of that section could be applied in any topological context where definable nowhere locally constant unary functions are open with finite fibres (see, e.g., [40, Theorem 5.5]). It seems that coupled with analogous results (yet to be proved) for the uniform definability of the frontier of plane curves a version of Theorem 6.2 could be proved for all dimensions. Namely, that reduct-definable reduct-irreducible are pure-dimensional. This could be a key for a shorter proof of the restricted trichotomy conjecture, using the machinery of Zariski Geometries, possibly in all dimensions.

Acknowledgements. The second author thanks Boris Zilber for his remarks on an early version of the paper, Maxim Mornev for many helpful comments, and Qiaochu Yuan for suggesting the elegant proof of Lemma 4.1. We would also like to thank Moshe Kamensky for some comments and suggestions.

2 Model theoretic background

For readers unfamiliar with the model theoretic jargon we give a self contained explanation of Conjecture A. In order to keep this introduction as short as possible, we specialise our definitions to the setting in which they will be applied. Readers familiar with the basics of model theory are advised to skip to Subsection 2.3.

2.1 Interpretations, Zilber trichotomy

A structure $\mathcal{M}$ is a set M, called the universe of the structure, together with a collection of Boolean algebras $\mathrm{Def}(\mathcal{M})$ of subsets of M^n (for all $n \in \mathbb{N}$), called definable sets, and satisfying the following requirements:

1. $\mathrm{Def}(\mathcal{M})$ is closed under all projections and permutations of coordinates;
2. All diagonals, i.e. sets of the form $\{\ (x_1, \dots, x_n) \in M^n \ \mid\ x_i = x_j\ \}$, are in $\mathrm{Def}(\mathcal{M})$;
3. If $D \in M^{n+m}$ is definable and $a \in M^n$ then $\{x \in M^m : (a, x) \in D\}$ is definable.

Usually a structure $\mathcal{M}$ is given by specifying the universe M and a collection of distinguished subsets of powers of M, called *atomic* definable sets. The class $\mathrm{Def}(\mathcal{M})$ is then the class of sets generated by the atomic definable sets. A function $f : M^n \to M$ is definable if its graph is a definable set. For example, given a field F with the graphs of addition and multiplication as atomic sets, the additive and multiplicative

[3] At least modulo the conjecture that any 1-dimensional group interpretable in ACVF is Zariski dense in an algebraic group.

inverses are definable and so is every constructible set. If F is algebraically closed then, by a theorem of Chevalley, these are the only definable sets.

An algebraic curve $\mathcal{C}$ defined over a field k can be made into a structure as follows: fix some field $k \leq K$ and let M be the set of K-rational points of $\mathcal{C}$. Set $\text{Def}(\mathcal{C})$ to be the collection of all Zariski closed subsets of M^n defined over k. This is the *full Zariski structure on* M. Throughout this paper we will be working inside a the full Zariski structure of one fixed curve over a fixed algebraically closed field of infinite transcendence degree. In general, our structure will not consist of the full Zariski structure, as explained below.

A structure $\mathcal{N}$ is a *reduct* of a structure $\mathcal{M}$ if $N = M$ and $\text{Def}(\mathcal{N}) \subseteq \text{Def}(\mathcal{M})$, that is, if the two structures share the same universe and any set definable in $\mathcal{N}$ is already definable in $\mathcal{M}$. Given a structure $\mathcal{M}$ and a (definable) $D \subseteq M^n$ the *induced structure* on D is the structure $\mathcal{D}$, with universe D and whose atomic[4] definable sets are all sets of the form $D^k \cap S$ where $S \subseteq M^{nk}$ is definable in $\mathcal{M}$. The structure $\mathcal{M}$ is *interpretable* in an algebraically closed field K if it is the reduct of the structure induced from K on some constructible subset of K^n (some $n \in \mathbb{N}$).

Basic examples of reducts of an algebraically closed field K, are the trivial reduct, whose only atomic sets are the diagonals, and the reducts generated by the additive or multiplicative groups. More complicated examples consist of those structures generated, say, by the additive group and one non-linear polynomial. It is not too hard to show that in the first two of these examples the field K cannot be definably reconstructed. It is somewhat harder to show ([27]) that in the latter example, the field can be definably reconstructed. The problem of classifying those reducts – and, more generally, structures interpretable in algebraically closed fields – allowing a reconstruction of the field is the subject of Zilber's restricted Trichotomy conjecture.

To give a precise formulation of Zilber's trichotomy conjecture we need some more definitions. A saturated (see below) structure $\mathcal{M}$ is *strongly minimal* if all definable subsets of M are finite or co-finite. For example, it follows immediately from Chevalley's theorem that algebraically closed fields (of infinite transcendence degree) are strongly minimal. Clearly, if $\mathcal{M}$ is strongly minimal then so is every reduct of $\mathcal{M}$. However, given a reducible algebraic curve C and $\mathcal{D}$, a reduct of the induced structure on C, the resulting structure need not be strongly minimal.

From now $\mathcal{M}$ will denote a strongly minimal reduct of the full Zariski structure of an algebraic curve, M, over an algebraically closed field K. We will not assume that M is an irreducible curve.

In the present context, the *Morley rank* of a set $S \subseteq M^n$ definable in $\mathcal{M}$ can be identified with the dimension of its Zariski closure (as an affine variety) – see also Lemma 2.1 below. A definable set $S \subseteq M^n$ of Morely rank 1 is called a *curve*, and if $n = 2$ it is a *plane curve*. A *definable family of $\mathcal{M}$-definable subsets of M^n* is a collection $\{D_a : a \in S\}$ where $D \subseteq M^{m+n}$, $S \subseteq M^m$ are definable and for $a \in S$ we denote $D_a := \{x \in M^n : (a, x) \in D\}$. In the present text we will denote

[4]In the context of the present paper, in fact, any definable set in the induced structure is of that form.

such a family as a function $f : D \to S$ with f onto S. It is well known (see, for example, Lemma 6.2.20 in [26]) that if $\mathcal{M}$ is strongly minimal and $f : D \to S$ is a definable family of plane curves, then the equivalence relation on S given by $s \sim t \iff \#(D_s \triangle D_t) < \infty$ is definable. We say that the family $f : D \to S$ is *(almost) faithful* if $\sim$ is trivial on S (has only finite classes). If $f : D \to S$ is an almost faithful definable family of plane curves the dimension of the family is the dimension of S.

As a consequence of weak elimination of imaginaries in $\mathcal{M}$ (see, for example, Lemma 1.6 in [33]) for any $\mathcal{M}$-definable family $f : D \to S$ of plane curves there exists an almost faithful definable family $f' : D \to S'$ such that for every $s \in S$ there exists $s' \in S'$ such that $\#(D_s \triangle D'_{s'}) < \infty$. We say that $\mathcal{M}$ is locally modular if every almost faithful family of plane curves is at most 1-dimensional.

Clearly, algebraically closed fields are not locally modular as is witnessed by the definable family of affine lines $f : D \to K^2$ given by $f(x, y, a, b) = (a, b)$ where $D(x, y, a, b) := \{(x, y, a, b) : ax + b = y\}$. It follows that if K can be reconstructed in $\mathcal{M}$ then $\mathcal{M}$ is not locally modular. Thus, Zilber's conjecture, asserts that a field (necessarily isomorphic to K) can be reconstructed in the structure $\mathcal{M}$ if and only if $\mathcal{M}$ is not locally modular.

We remark that the model theoretic notion of a family of curves is looser than standard notions studied in algebraic geometry, e.g., no flatness conditions are imposed.

2.2 Generic parameters, imaginaries, canonical bases

We will now introduce more subtle model theoretic notions used in the text, referring to [26, 9, 6, 32] for a more thorough exposition.

The *language* (or *signature*) of a structure $\mathcal{M}$ specified by its atomic definable sets is a set of symbols (with prescribed arities), $\mathcal{L}$, and a function τ (the interpretation of $\mathcal{L}$ in M) from $\mathcal{L}$ onto the class of atomic definable sets. We say that $\mathcal{M}$ is an $\mathcal{L}$-structure.

Given an $\mathcal{L}$-structure $\mathcal{M}$, a key notion in model theory is that of a set being definable over a set of parameters $A \subseteq M$. The class of $\emptyset$-definable sets is the minimal subclass of $Def(M)$ that is closed under (fintite) boolean operations, projections and containing all diagonals. A set definable set $D \subseteq M^n$ is A-definable if there is a $\emptyset$-definable set $D' \subseteq M^{n+m}$ (some m) such that $D = \{x \in M : (x, \bar{a}) \in D'\}$ where $\bar{a}$ is a tuple from A (of length m).

An algebraically closed field K is *saturated* if it is of infinite transcendence degree over its prime field. Any structure interpretable in a saturated algebraically closed field is itself saturated. For saturated structures the notion of a definable set D being A-definable is equivalent to D being invariant (set-wise) under all automorphisms of $\mathcal{M}$ fixing A point-wise (where an automorphism of $\mathcal{M}$ is any bijection respecting all atomic sets).

A *(complete) type* over a set A is an (ultra)-filter of A-definable sets (i.e., a (maximal) collection of A-definable sets with the finite intersection property). Unless specifically stated otherwise, all types in the present paper will be complete. If $\mathcal{M}$ is saturated and $|A| < |M|$ and p is a type over A then, in fact, the intersection of all definable sets in p is non-empty. Throughout this paper all sets of parameters will be small, i.e., of cardinality smaller than that of M. An element $b \in \bigcap_{D \in p} D$ is *a realisation* of p. The *rank of a type* p is the minimum rank of a formula in p. If p is a type over A and q is a type over B we say that q extends p if $p \subseteq q$. We say that q is a non-forking extension over p if p and q have the same rank.

Given an element $b \in M$ and a set of parameters A *the type of* b *over* A is the collection of all A-definable sets D such that $b \in D$. This is denoted $\text{tp}(b/A)$. In a saturated structure $\mathcal{M}$, for any set of parameters A any type p over A is the type of some element. Given an element b and parameters sets $A \subseteq B$ we say that b does not fork with B over A (or that b is independent from B over A) if the $\text{tp}(b/B)$ is a non-forking extension of $\text{tp}(b/A)$. In the context of algebraically closed fields this amounts to the locus of b over B being equal to the locus of b over A.

If $\mathcal{M}$ is saturated any type over A can be identified with the an orbit of the automorphism group of $\mathcal{M}$ fixing A point-wise. In this language the rank of a type is the Krull dimension of the closure (in K) of the orbit associated with that type.

Given an A-definable set D a type in D is any type p (over a parameter set $B \supseteq A$) such that $D \in p$. Since algebraic varieties have only finitely many irreducible components of maximal rank, and since $\mathcal{M}$ is a reduct of the full Zariski structure on M, it follows that for any definable set D there are finitely many types in D of maximal rank. Those are the *generic types in* D. A set D is stationary if it has a unique generic type (over any set of parameters B. E.g., if the closure of D is an absolutely irreducible variety). This implies that at the price of extending the set of parameters any definable set D can be definably split into finitely many (disjoint) stationary sets. We observe that for a stationary set D the generic type of D can be conveniently described as the type given by D and the negation of all A-definable subsets of D of rank smaller than the rank of D. We say that a type p over A is stationary if there is a definable set $D \in p$ of minimal rank which is stationary.

We will say that an $\mathcal{M}$-definable property holds for *almost all elements of* D if every generic element of D satisfies that property.

An element $b \in D$ is *generic in* D *(over* A*)* if it is a realisation of a generic type in D (equivalently, if its type over A is generic in D). Manipulations of realisations of generic types is a common technique in model theory (used non-trivially throughout Section 6, for example). This may seem unclear to non-specialists due to the fact that the term "generic point" does not refer to exactly the same notion as in the theory of schemes. For example, a generic point of an irreducible variety in the sense of scheme theory is unique, whereas two realisations x, y of the unique generic type of $\mathbb{A}^1$ may be independent so that the type of the tuple $(x, y) \in \mathbb{A}^2$ is the generic type of $\mathbb{A}^2$, but if they are dependent (x, y) will be a generic point of a subvariety of $\mathbb{A}^2$ projecting dominantly on both coordinates of the affine plane.

Further, a fibre X_a of a definable set $X \subset M^{m+n}$, where a is a realisation of the generic type of a variety $Y \subset M^m$, corresponds to the base change of X to the generic point of Y in the scheme-theoretic sense. The points of X_a in a saturated model are then generic points of subvarieties of X that project dominantly on Y.

Note that if D is $\mathcal{M}$-definable it is certainly K-definable, so it makes sense to talk about a K-generic element of D. Such an element is also generic in the sense of $\mathcal{M}$. Throughout this text, unless specifically stated otherwise, all generics will be taken with respect to the full Zariski structure.

A type p over a parameter set A is algebraic if it has rank 0. In the context of saturated structures this is equivalent to the orbit associated with p being finite (which is the same as the type having only finitely many realisations in $\mathcal{M}$). An element b is algebraic over A if $\mathrm{tp}(b/A)$ is algebraic. In the context of algebraically closed fields an element is algebraic over A in the model theoretic sense precisely if it is algebraic over the field generated by A in the usual algebraic sense. However, if $\mathcal{M}$ is a reduct of the full Zariski structure on M the algebraic closure in the sense of $\mathcal{M}$ will, in general, be smaller than in the algebraic sense. A set A is *algebraically closed* if any element algebraic over A is in A. In the context of algebraically closed fields a set A is algebraically closed precisely if it is an algebraically closed subfield.

The above description of the algebraic closure in a structure $\mathcal{M}$ is adequate in the context of algebraically closed fields, but is not quite strong enough for our purposes. This can be better explained by considering the action of the automorphism group of $\mathcal{M}$ fixing a parameter set A not only on elements of the universe, but also as definable sets. In the context of algebraically closed fields, if V is an affine variety (or, more generally, a constructible set) and A is an algebraically closed field containing the field of definition of V then either $\mathrm{Aut}(K/A)$ fixes V set-wise or it has an infinite orbit. If $\mathcal{M}$ is a reduct of the full Zariski structure on M this need not be the case.

To addres this problem recall that if D is an A-definable set then $D = D'(\bar{a})$ for some $\emptyset$-definable set D' and $\mathrm{dom}(\bar{a}) \subseteq A$. Let T be the projection of D' onto the coordinates corresponding to $\bar{a}$. Consider the (definable) equivalence relation on T given by $t \sim s$ if $D(s) = D(t)$ (as sets). It is clear that the orbit of D under $\mathrm{aut}(M/A)$ is in bijection with the quotient space $T/\sim$. In the context of algebraically closed fields $T/\sim$ can be naturally identified with a constructible set, and it follows that if $T/\sim$ is finite then the elements of this algebraic set are algebraic over A. We say that a structure has *elimination of imaginaries* if for any $\emptyset$-definable set T and any $\emptyset$-definable equivalence relation E on T there is a $\emptyset$-definable set S and a $\emptyset$-definable function $f : T \to S$ such that $f(x) = f(y)$ if and only if $E(x, y)$. The above discussion can be readily adapted to show that algebraically closed fields admit elimination of imaginaries.

In the more general context we are working in there is no reason to assume that $\mathcal{M}$ has elimination of imaginaries. There is a standard model theoretic technique for adding, to any structure $\mathcal{M}$, any $\emptyset$-definable set T and any $\emptyset$-definable equivalence relation E on T a new *sort* (which we identify with T/E) and a new function symbol $\pi_E : T \to T/E$ (which we identify with the natural projection map). The resulting structure is denoted $\mathcal{M}^{eq}$ and it is an easy exercise to verify that $\mathcal{M}^{eq}$ admits elimination of imaginaries. The elements of the new sorts are called *imaginary elements.*

The new elements we added to $\mathcal{M}$ are referred to as *imaginary elements* and they should be thought of as canonical names for equivalence classes of $\emptyset$-definable equivalence relations. Throughout this text, when referring to the algebraic closure of a parameter set A we will be implicitly referring to the algebraic closure including imaginary elements (i.e., including names for definable equivalence relations with a finite number of classes). In the next subsection we will give a more concrete description of the treatment of imaginaries in the present paper.

One of the most striking and powerful applications of imaginary elements is that they allow us to treat definable sets as elements of our structure. That is, if $D = D'(\bar{a})$ is definable (with D' $\emptyset$-definable), T and $\sim$ are as in the previous paragraph, then D is identified with $[\bar{a}]/\sim$, and the latter is called *a code for D*, or *a canonical parameter for D*. Note that the canonical parameter of a definable set is not uniquely determined, but the rank of its type is, which will suffice for all our applications.

2.3 Remarks on the model-theoretic setup

Throughout the paper K is an algebraically closed field of infinite transcendence degree. We fix M, an algebraic curve over K and $\mathcal{M}$ a non-locally modular reduct of the full Zariski structure on M.

The following lemma justifies the correspondence between Morley rank and Krull dimension introduced above:

Lemma 2.1. *For any $\mathcal{M}$-definable set $Z \subset M^n$ the Morley rank of Z in $\mathcal{M}$ coincides with the Krull dimension of the Zariski closure of Z.*

Proof. The claim is clear if $Z = M^k$. In general Z has Morley rank k if and only if k is maximal such that some projection $\pi : Z \to M^k$ contains an $\mathcal{M}$-generic point of M^k. So such a projection of Z contains a K-generic point, so the Morley rank is bounded from above by the Krull dimension of K. As the other inequality is obvious (K-generic points being obviously $\mathcal{M}$-generic), the lemma is proved. □

We proceed with a few basic reductions and conventions that will simplify the exposition and the notation. First, there is no harm assuming that $\mathcal{M} = (M, X)$, where X is a predicate naming the total space of a 2-dimensional (almost) faithful family $X \to T$ of plane curves (in the sense of the structure $\mathcal{M}$). Indeed, since $\mathcal{M}$ is non-locally modular, there exists a 2-dimensional family of plane curves, X, and (M, X) is a reduct of $\mathcal{M}$. If a field is interpretable in (M, X) it is necessarily interpretable already in $\mathcal{M}$. Next we need the following easy observation:

Remark. Let D be a strongly minimal set definable in $\mathcal{M}$. Then D with the full induced structure is non-locally modular.

It is an easy exercise to verify that the notion of interpretablity is transitive, namely, that if a structure $\mathcal{N}$ is interpretable in $\mathcal{M}$ and $\mathcal{D}$ is interpretable in $\mathcal{N}$

then $\mathcal{D}$ is interpretable in $\mathcal{M}$. Thus, if D is a strongly minimal set definable in $\mathcal{M}$ and $\mathcal{D}$ is the $\mathcal{M}$-induced structure on D, in order to show that $\mathcal{M}$ interprets a field it will suffice to show that $\mathcal{D}$ interprets a field. Therefore, we may assume, e.g., that the curve M is regular (by removing its non-regular locus, which is finite, and in particular definable in any structure on M). Similarly, after showing that a 1-dimensonal group is interpretable in $\mathcal{M}$ we may assume – by replacing $\mathcal{M}$ with the universe of the group with its full induced structure – that $\mathcal{M}$ itself expands an algebraic group.

While algebraically closed fields have elimination of imaginaries there is no reason for the same to be true in $\mathcal{M}$. However, by the previous paragraph, any strongly minimal structure $\mathcal{D}$ interpretable (allowing imaginary elements) in $\mathcal{M}$ is already interpretable in K. Since K does have elimination of imaginaries, the structure $\mathcal{D}$ can be identified with the reduct of the full Zariski structure on some algebraic curve D over K. In particular, if $\mathcal{D}$ is non-locally modular then it falls in the scope of Conjecture A, justifying the reduction of the previous paragraph.

The above allows us to tacitly assume that the structure $\mathcal{M}$ has elimination of imaginaries. This is merely a matter of convenience. As explained in the previous paragraphs, using elimination of imaginaries for algebraically closed fields, and changing the ground structure as we go, we can avoid almost any usage of imaginaries. There is, however, one exception. We cannot assure the existence of a faithful 2-dimensional family of plane curves in $\mathcal{M}$ without allowing the parameter space T of the family to range over imaginary sorts. Though all proofs in the present work could go through essentially unaltered if X were an almost faithful family of plane curves, this could somewhat hamper the clarity of the exposition by adding simple, unnecessary, technicalities which we prefer to avoid.

3 Slopes

The main object of study in the present section is slopes (of various orders) of a curve at a regular point. While the notions we are interested in make sense in a wider context, we only study them in the context of curves in Cartesian powers M^n of an algebraic curve over an algebraically closed field. We introduce the operation of composition (Subsection 3.1) and taking sum of curves in the presence of an underlying group structure (Subsection 3.2).

First, we adopt the convention to call *curve* a variety of dimension 1, not necessarily regular or irreducible; when we talk about curves in M^n, we assume that they are Zariski closed in M^n. A *definable curve* is a definable set in M^n, of dimension 1, not necessarily pure-dimensional or Zariski closed where $(M, \dots)$ is a reduct of the full Zariski structure on an algebraic curve M.

Definition 3.1 (Local coordinate system). *Let P be a regular point of a variety X of dimension n. A* local coordinate system *at P is an isomorphism $\widehat{\mathcal{O}_{X,P}} \xrightarrow{\sim} k[[x_1, \dots, x_n]]$.*

By Corollary to Theorem 30.5 [29] any variety over a field is generically regular, and by Theorem 29.7 *loc.cit.* a completion of a regular local ring over a field is a formal power series ring.

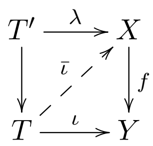
If X is one-dimensional and a local coordinate system is chosen at P then for all $n > 0$ the inclusion $\mathcal{O}_{X,x} \to \widehat{\mathcal{O}_{X,x}}$ followed by the reduction maps $k[[x]] \to k[[x]]/(x^{n+1}) \cong k[x]/(x^{n+1})$ gives rise to closed embeddings $\operatorname{Spec} k[x]/(x^{n+1}) \hookrightarrow M$ with the closed point of $\operatorname{Spec} k[x]/(x^{n+1})$ mapped to P.

If $i_1 : \widehat{\mathcal{O}_{X,P_1}} \xrightarrow{\sim} k[[x]], i_2 : \widehat{\mathcal{O}_{Y,P_2}} \xrightarrow{\sim} k[[y]]$ are local coordinate systems at regular points $P_1 \in X, P_2 \in Y$ then there is a natural local coordinate system at the point $(P_1, P_2) \in X \times Y$,

$$i_1 \otimes i_2 : \mathcal{O}_{X,\widehat{P_1 \otimes \mathcal{O}}_{Y,P_2}} \to \varprojlim (k[x]/(x^n) \otimes k[y]/(y^n)) \cong k[[x, y]].$$

Remark. From now on, whenever we mention that we choose a local coordinate system at $(P_1, P_2) \in M^2$ for M a curve, we do so by choosing local coordinate systems i_1, i_2 at $P_1, P_2 \in M^2$ and then passing to $i_1 \otimes i_2$.

Finally, let $f : X \to Y$ be a morphism of schemes. Recall ([13] EGA IV.17.1) that a morphism f is *formally étale* if for any scheme T, closed subscheme T' defined by a nilpotent ideal and any two compatible morphisms $\lambda : T' \to X$ and $\iota : T \to Y$ there is a unique morphism $\bar{\iota} : T \to X$ such that the following diagram commutes



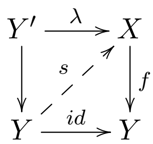
Observe that a closed embedding ι lifts to a closed embedding $\bar{\iota}$ and it follows automatically that f induces an isomorphism between two copies of T embedded into X and Y.

A morphism $f : X \to Y$ is *étale* if it is flat and unramified.

An étale morphism of schemes $f : X \to Y$ is formally étale (SGA1 [15], Corollaire I.5.6), and a formally étale morphism which is locally of finite presentation is étale ([13] EGA IV, Corollaire 17.6.2). Since in what follows we deal mainly with schemes of finite type over fields, we will not distinguish between these two notions.

Lemma 3.2. *Let $f : X \to Y$ be an étale morphism. Assume Y is the spectrum of a local Artinian algebra over a field. Then sections of f are in one-to-one correspondence with closed points in the fibre over the closed point of Y. For any such section s the composition $f \circ s$ is an isomorphism.*

Proof. By definition of formally étale morphism, given any morphism $\lambda : Y' \to X$ where Y' is a reduced subscheme supported at a closed point of X yields a unique section s that makes the following diagram commute:



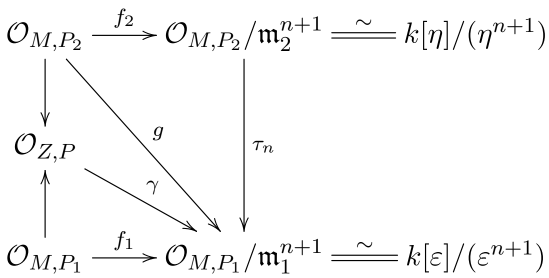
That $s \circ f$ is an isomorphism follows from Corollary I.5.3, SGA1 [15]. $\square$

Definition 3.3 (Scheme-theoretic image). *Let $f : X \to Y$ be a morphism of schemes. The* scheme theoretic image of X in Y *is the smallest closed subscheme of Y through which f factors.*

Lemma 3.4. *Let $\mathcal{O}_X$ be a local ring with residue field k and let $f : \mathcal{O}_{X,x} \to k[\varepsilon]/(\varepsilon^{n+1})$ be a morphism. Then f factors through $\mathcal{O}_{X,x}/\mathfrak{m}^{n+1}$ where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}_{X,x}$.*

Proof. One observes easily that $f^{-1}(\mathfrak{p}) \subset \mathfrak{m}^{n+1}$ where $\mathfrak{p}$ is the radical ideal of $k[\varepsilon]/(\varepsilon^{n+1})$, since $\mathfrak{p}^{n+1} = 0$. This implies the statement of the lemma. $\square$

Let M be a curve, and assume a local coordinate system is chosen at a regular point $P = (P_1, P_2) \in M^2$. Let $Z \subseteq M \times M$ be a curve such that the projection of Z on the first factor M is étale in an open neighbourhood of P. Consider the diagram



where $\mathfrak{m}_1, \mathfrak{m}_2$ are maxmial ideals of $\mathcal{O}_{M,P_1}, \mathcal{O}_{M,P_2}$, respectively. The isomorphisms on the right are provided by the local coordinate systems at P_1 and P_2. The morphism γ is a lifting of f_1 that follows from etaleness of $\mathcal{O}_{Z,P}$ over $\mathcal{O}_{M,P_1}$. The morphism g is the composition of the structure morphism of the $\mathcal{O}_{M,P_2}$-algebra $\mathcal{O}_{Z,(P_1,P_2)}$ and γ. By Lemma 3.4, g factors through $\mathcal{O}_{M,P_2}/\mathfrak{m}^{n+1}$. The morphism τ_n that comes out of this factorization, can be regarded as an endomorphism of $k[\varepsilon]/(\varepsilon^{n+1})$ after one identifies $k[\eta]/(\eta^{n+1})$ with $k[\varepsilon]/(\varepsilon^{n+1})$.

Definition 3.5 (Slope). *Let M be a curve, and let $Z \subset M \times M$ be a curve as above. The* n-th order slope of Z at (P_1, P_2) *is the endomorphism $\tau_n : k[\varepsilon]/(\varepsilon^{n+1}) \to k[\varepsilon]/(\varepsilon^{n+1})$ arising from the construction above. In general, we will denote the slope of Z at P, which is an element of* $\mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1}))$, *as $\tau_n(Z, P)$.*

Similarly, in the above setting if N is an algebraic variety over k and $Z \subset M^2 \times N$ a curve, $P = (P_1, P_2, P_3) \in Z$ a regular point and such that the projection p_1 on the first factor M is étale in an open neighbourhood of (P_1, P_2, P_3), one can consider the diagram as above, and consider the lifting γ of the morphism f_1 that exists by etaleness of $\mathcal{O}_{Z,P}$ over $\mathcal{O}_{M,P_1}$. By Lemma 3.4, g factors through $\mathcal{O}_{M,P_2}/\mathfrak{m}^{n+1}$. The morphism τ_n that comes out of this factorization, can be regarded as an endomorphism of $k[\varepsilon]/(\varepsilon^{n+1})$ after one identifies $k[\eta]/(\eta^{n+1})$ with $k[\varepsilon]/(\varepsilon^{n+1})$.

Definition 3.6 (Relative slope)**.** *The n-th order slope of Z at (P_1, P_2, P_3) relative to N is the endomorphism $\tau_n : k[\varepsilon]/(\varepsilon^{n+1}) \to k[\varepsilon]/(\varepsilon^{n+1})$ arising from the construction above. We will denote the relative slope by $\tau_n(Z/N, P) \in \mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1})$.*

The need for this seemingly artificial definition will become apparent in the next section; it serves the same purpose as the notion of "branches of curves" in [41, Section 3.8].

In the above definition, and later in this article, we assume that a choice of local coordinate systems for M at the relevant points has been made.

A first-order slope is a map $k[\varepsilon]/(\varepsilon^2) \to k[\varepsilon]/(\varepsilon^2)$, which is determined by its action on ϵ, $\epsilon \mapsto a \cdot \epsilon$. We observe that the scalar a is just a component of the normalised Plücker coordinates of the tangent subspace in the given local coordinate system. Clearly, two curves having the same first order slope at a point are tangent at this point.

Definition 3.7 (Formal power series expansion)**.** *In the setting of Definition 3.5 consider the endomorphism*

$$A = \varprojlim_n \tau_n(Z, (P_1, P_2)) \in \varprojlim(\mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1}) \cong \mathrm{End}(k[[x]])$$

We call $A(x)$ the formal power series expansion *of Z at (P_1, P_2).*

Similarly, if $Z \subset M^2 \times N$, we call teh relative formal power series expansion of Z at $Q \in Z$ the result of ethe application of the endomorphism

$$\varprojlim \tau_n(Z/N, Q)$$

to $x \in k[[x]]$.

Proposition 3.8. *Assume local coordinate systems are chosen at (P_1, P_2), then there is a canonical isomorphism $\widehat{\mathcal{O}_{(P_1,P_2),M^2}} \to k[[x, y]]$. The formal power series expansion of X at (P_1, P_2) is $f \in k[[\varepsilon]]$ if and only if the morphism $\mathcal{O}_{(P_1,P_2),M} \to k[[\varepsilon]]$ given by $x \mapsto \varepsilon, y \mapsto f$ factors through $\mathcal{O}_{(P_1,P_2),X}$.*

Proof. Straightforward from the definitions. □

Later on we will needing the following charactersiation of invertible endomorphisms from $\mathrm{End}(k[\varepsilon]/(\varepsilon\,/n + 1)$:

Proposition 3.9. *Let $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^{n+1}))$ denote the set of automorphisms of $k[\varepsilon]/(\varepsilon^{n+1})$. Consider the restriction map $\mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1})) \to \mathrm{End}(k[\varepsilon]/(\varepsilon^2))$ defined by $\varphi \mapsto (f \mapsto \varphi(f)/(x^2))$. Then $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^{n+1}))$ is the pre-image of $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^2))$.*

Proof. An endomorphism $\varphi \in \mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1}))$ is invertible if and only if there exists f such that $\varphi(f) = x$. By Corollary 7.17, [10], an endomorphism of $k[[x]]$ defined by sending x to f is an automorphism if and only if $f \in (x)$ but not $f \in (x^2)$. As any $\varphi \in \mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1}))$ extends uniquely to $\mathrm{End}(k[[x]])$, the conclusion follows. □

Definition 3.10 (Graph of a morphism)**.** *Let $f : X \to Y$ be a morphism of schemes over some base scheme S. The* graph *of the morphism f is the unique closed subscheme $Z \subset X \times_S Y$ such that the projection on X restricted to Z is an isomorphism and $f = p_Y \circ p_X^{-1}$.*

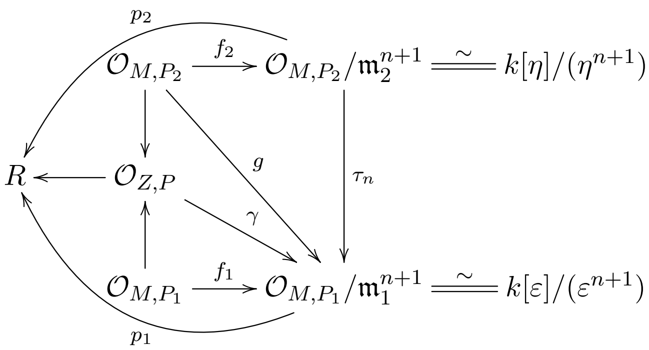
Lemma 3.11. *Let $Z \subset M \times M$ be a locally closed set of dimension 1 such that the slope is well-defined at $P \in Z$. Let $\mathcal{O}_{M^2,P} \to k[\varepsilon,\eta]/(\varepsilon^{n+1},\eta^{n+1})$ be the natural morphism induced by the local coordinate system.*

Define

$$R := \mathcal{O}_{Z,P} \otimes_{\mathcal{O}_{M^2,P}} k[\varepsilon,\eta]/(\varepsilon^{n+1},\eta^{n+1}) \text{ and } \bar{Z} := \operatorname{Spec} R$$

Then $\bar{Z}$, identified with a closed subscheme of $\operatorname{Spec} k[\varepsilon,\eta]/(\varepsilon^{n+1},\eta^{n+1})$*, is the graph of $\tau_n(Z,P)$. If $p_2 : Z \to M$ is étale in an open neighbourhood of P then it is is an automorphism of $k[\varepsilon]/(\varepsilon^{n+1})$.*

Proof. Consider R in relation to the objects in the diagram used in the definition of slope. The ring R has a natural $\mathcal{O}_{M^2,P}/\mathfrak{m}^{n+1}$-algebra structure, and hence a natural $\mathcal{O}_{M,P_1}/\mathfrak{m}_1^{n+1}$-algebra and $\mathcal{O}_{M,P_2}/\mathfrak{m}_2^{n+1}$-algebra structure:



The map $p_1 \otimes p_2$ is factors through quotient of $k[\varepsilon,\eta]/(\varepsilon^{n+1},\eta^{n+1})$. It follows from the fact that $\mathcal{O}_{Z,P}$ is étale over $\mathcal{O}_{M,P_1}$ that the morphism p_1 is an isomorphism, and if $\mathcal{O}_{Z,P}$ is supposed étale over $\mathcal{O}_{M,P_2}$, p_2 is an isomorphism too. The statement of the lemma follows from the commutativity of the diagram. □

Lemma 3.12. *Let $Z \subset M^2 \times N$ be a locally closed set of dimension 1 such that relative slope is well-defined at $P \in Z$, and let $p : Z \to M^2$ be the projection on the factor M^2, with p_1, p_2 projections on the first and second copies of M. Let $\mathcal{O}_{M^2,P} \to k[\varepsilon,\eta]/(\varepsilon^{n+1},\eta^{n+1})$ be the natural morphism induced by the local coordinate system.*

Define

$$R := \mathcal{O}_{Z,P} \otimes_{\mathcal{O}_{M^2,P}} k[\varepsilon,\eta]/(\varepsilon^{n+1},\eta^{n+1}) \text{ and } \bar{Z} := \operatorname{Spec} R$$

Then the scheme-theoretic image of $\bar{Z}$ under π is the graph of $\tau_n(Z/N,P)$. If $p_2 : Z \to M$ is étale in an open neighbourhood of P then it is an automorphism of $k[\varepsilon]/(\varepsilon^{n+1})$.

Proof. Similar to the proof of the previous lemma. In the situation of the present lemma, as R is isomorphic a quotient $k[\varepsilon,\eta]/(\varepsilon^{n+1},\eta^{n+1})$ of, $\operatorname{Spec} R$ is by definition the scheme-theoretic image of $\bar{Z}$ under p. □

3.1 Composition of curves

We have identified the slope of a curve at a regular point with an automorphism of $\operatorname{Spec} k[\varepsilon]/(\varepsilon^{n+1})$. We note that the group of automorphisms of $\operatorname{Spec} k[\varepsilon]/(\varepsilon^2)$ is $\mathbb{G}_m(k)$, and that in general an automorphism group of a fat point $\operatorname{Spec} k[\varepsilon]/(\varepsilon^{n+1})$ is unipotent of rank n. Our goal in Section 5 will be to recover $\mathbb{G}_m(k)$ by identifying its points with the (first order) slopes of a family of curves in M^2. In positive characteristic we will have to resort to higher order slopes and we will not be able assure that the group recovered will indeed be $\mathbb{G}_m(k)$, but the general outline of the construction remains the same. The group operation on slopes arises from the operation of composition of curves. In this subsection we develop the necessary machinery.

We adopt the notational convention to denote by p with subscripts the projections from a product of several schemes or varieties on the product of factors of the product, with the numbers of these fuctors mentioned in the subscript. For example, p_{124} on $M \times M \times M \times N \times N'$ is the projection on the product $M \times M \times N$ where the two M's are the first and the second factors M.

First, by way of motivation, let us consider the following operation on pairs of curves in M^2, regarded as correspondences.

Definition 3.13 (Composition). *Let X, Y be two curves in M^2, cut out by ideal sheaves I_X, I_Y respectively. Then call their* composition*, and denote $Y \circ X$, the scheme cut out by the ideal sheaf*

$$(p_{13})_*(p_{12}^* I_X \otimes p_{23}^* I_Y)$$

where p_{ij} is the projection from M^3 onto the product of i-th and j-th factor. This is by definition the scheme-theoretic image under p_{13} of the scheme $X \times_{p_2,p_1} Y$, naturally embedded into M^3. One can show that the if X and Y are graphs of functions $f, g : M \to M$, then their composition is the graph of the function $f \circ g : M \to M$. If X and Y are one-dimensional definable subsets of M^2 then define their composition $Y \circ X$ to be the definable set

$$Y \circ X := \{\ (x,z) \in M^2 \ \mid\ \exists y \ \ (x,y) \in X \text{ and } (y,z) \in X\ \}$$

In case X and Y are closed, this definition coincides with the scheme-theoretic one on points.

One can show that

$$\tau_n(Y \circ X, (P_1, P_3)) = \tau_n(X, (P_1, P_2))\tau_n(Y, (P_2, P_3)) \tag{1}$$

if all the slopes that occur in the equation are well-defined. Unfortunately, even if the slope is defined for X at (P_1, P_2) and for Y at (P_2, P_3), the composition $Y \circ X$ may be not regular at (P_1, P_3).

Moreover, it will become apparent later — when we reconstruct groups and fields from a reduct of a curve M defined over a field of positive characteristic — that it is necessary to work with curves that are embedded into M^n for $n > 2$.

We generalise, therefore, the Definition 3.13 in two directions: firstly, to apply to curves embedded into M^n, $n > 2$, secondly, to produce curves that are known to have a well-defined relative slope at a certain point so as to make an analogue of equation (1) well-defined.

Definition 3.14 (Relative composition). *Let M be a curve over an algebraically closed field, N, N' some varieties, and let $X \subset M^2 \times N, Y \subset M^2 \times N'$ be curves. Then we call the* relative composition $Y \circ X$ of X and Y *the subscheme of dimension 1 cut out in $M^3 \times N \times N'$ by the ideal sheaf*

$$p_{124}^* I_X \otimes p_{235}^* I_Y$$

where p with subscripts are projections from $M^3 \times N \times N'$ on the products of factors with corresponding numbers.

If X, Y as above are definable sets then we call the relative composition of X and Y the definable set

$$\{\ (x, y, z, u, v) \in M^3 \times N \times N' \ \mid\ (x, y, u) \in X \text{ and } (y, z, v) \in Y\ \}3$$

In order to prove the Proposition that relates the relative compostion and composition of slopes, we need recall the following version of the projection formula:

Lemma 3.15. *Let $p : X \to Y$ be an affine morphism of schemes, and let $\mathcal{E}, \mathcal{F}$ be coherent sheaves on X, Y respectively. Then the natural morphism*

$$p_*\mathcal{E} \otimes \mathcal{F} \to p_*(\mathcal{E} \otimes p^*\mathcal{F})$$

is an isomorphism.

Proof. Follows from Corollaire I.9.3.9, [14]. □

Proposition 3.16. *Let X and Y be as in the Definition 3.14, and let $P_1, P_2, P_3, P_4 \in M$ be such that the slope of X is well-defined at (P_1, P_2, P_3), and the slope of Y is well-defined at $(P_1, P_2, P_4) \in Y$ in some chosen local coordinate systems. Then for any $n > 0$*

$$\begin{aligned} \tau_n(Y \circ X/M \times N \times N',\quad & (P_1, P_2, P_3, P_4, P_5)) = \\ & = \tau_n(X/N, (P_1, P_2, P_4)) \cdot \tau_n(Y/N', (P_2, P_3, P_5)) \end{aligned}$$

where the relative slope in the left hand side is relative to the product of the second factor M in M^3 and $N \times N'$.

Proof. Denote $T = \operatorname{Spec} k[\varepsilon]/(\varepsilon^{n+1})$, the Cartesian powers of T embed according to chosen local coordinate systems into the Cartesian powers of M.

By Lemma 3.12, for all $n > 0$,

$$\Gamma(\tau_n(X/N, (P_1, P_2, P_4))) \cong p_{12}(X \times_{M^2} T^2)$$

and

$$\Gamma(\tau_n(Y/N', (P_2, P_3, P_5))) \cong p_{23}(Y \times_{M^2} T^2)$$

Denote I_X, I_Y the ideal sheaves that cut out $X \times_{M^2} T^2$, respectively $Y \times_{M^2} T^2$, in $M^2 \times N$, respectively $M^2 \times N'$.

Let f and g be the endomorphisms of T associated to $\tau_n(X/N, (P_1, P_2, P_4))$ and $\tau_n(Y/N', (P_2, P_3, P_5))$. Let $\gamma_X : T \to T \times T \times N, \gamma_Y : T \to T \times T \times N'$ be the sections of the projection $X \times_{M^2} T^2 \subset T \times T \times N$, respectively $Y \times_{M^2} T^2 \subset T \times T \times N'$, on the first factor T. Let $\eta_Y : T \times T \times N \to T \times T \times T \times N \times N'$ be the map that acts as identity on the first T and on N and as γ_Y on the second T but sends the result to the product of second, third and fifth factors of the destinantion.

One gets immediately from these definitions that

$$p_1 \circ \gamma_X = f \qquad p_{124} \circ \eta_Y = \mathrm{id}$$

and that $p_{235}^* I_Y \cong \eta_{Y*} \mathcal{O}_{T \times T \times N}$, and that $I_X \cong \gamma_{X*} \mathcal{O}_T$.

It follows from the definition of relative composition and Lemma 3.12 that

$$p_{13*}(p_{124}^* I_X \otimes p_{235}^* I_Y)$$

is the ideal that cuts out the graph of $\tau_n(Y \circ X/M \times N \times N', (P_1, P_2, P_3, P_4, P_5))$ in $T \times T$.

Then by Lemma 3.15 (which we can apply because the map η_Y is affine and all the sheaves involved are coherent),

$$\begin{array}{rl} & p_{13*}(p_{124}^* I_X \otimes p_{235}^* I_Y) = \\ = & p_{13*}(p_{124}^* I_X \otimes \eta_{Y*} \mathcal{O}_{T \times T \times N}) = \\ = & p_{13*} \eta_{Y*} \eta_Y^* p_{124}^* \gamma_{X*} \mathcal{O}_T = \\ = & (p_{13} \circ \eta_Y)^* (p_{124} \circ \eta_Y)^* \gamma_{X*} \mathcal{O}_T = \\ = & (p_{13} \circ \eta_Y \circ \gamma_{X*}) \mathcal{O}_T \end{array}$$

The composition $p_3 \circ \eta_Y \circ \gamma_{X*} : T \to T$ is the morpmism $g \circ f$,: indeed, in the diagram

$$\begin{array}{ccccc} T & \xrightarrow{\gamma_X} & T \times T \times N & \xrightarrow{\eta_Y} & T \times T \times T \times N \times N' \\ & \searrow^{f} & \downarrow p_2 & \searrow^{g \circ p_2} & \downarrow p_3 \\ & & T & \xrightarrow{g} & T \end{array}$$

the commutativity of the upper left triangle follows from the definition of γ_X, and commutativity of the upper right triangle follows from the definiton of η_Y.

We have shown, therefore, that $p_{13*}(p_{124}^* I_X \otimes p_{235}^* I_Y)$ is the ideal $(\mathrm{id} \times (g \circ f))_* \mathcal{O}_T$ which is, by definition,the ideal that cuts out the graph of $g \circ f$ in $T \times T$. $\square$

This proposition can be applied to curves in M^2 by taking N, N' to be points.

Recall that formal power series can be composed in the following sense: given an element $y \in k[[x]]$ from the maximal ideal, there exists a unique homomorphism of topological rings $f_y : k[[x]] \to k[[x]]$ mapping x to y (see [4], IV,§3 for example). The image of a power series $z \in k[[x]]$ under f_y is the composition of the power series y with the power series z. Since the expansion of a curve Z at a regular point is defined through the inverse system of n-slopes, it is then easy to verify that, by of Proposition 3.16, the power series expansion or $W \circ V$ is the composition of the power series expansion of V with the power series expansion of W, expansions taken at appropriate points.

Lemma 3.17. *Fix local coordinate systems at $P_1, P_2, P_3 \in M$. Let $Z_1, Z_2 \subseteq M^2$ be curves with $(P_1, P_2) \in Z_1$ and $(P_2, P_3) \in Z_2$ both regular points on the respective curves. Let $f_1, f_2 \in k[[x]]$ be the associated power series expansions of Z_1, Z_2 at (P_1, P_2) and at (P_2, P_3) respectively. Assume that $f_1 = g_1^{p^n}, f_2 = g_2^{p^m}$ with $g_1, g_2 \in k[[x]]$. Then the power series expansion of $Z_1 \circ Z_2^{-1}$ at (P_3, P_1) is given by $h := (g_1 \circ g_2)^{p^{n-m}}$.*

Proof. First let us prove the statement for $M = \mathbb{A}^1$ and $P_1 = P_2 = P_3 = 0$. Since Z_1, Z_2 are regular at $(0, 0)$ only one irreducible component of each of Z_1, Z_2 passes through $(0, 0)$, so we may assume that Z_1 and Z_2 are irreducible. In that case it is enough to notice that if a formal power series expansion of a curve at $(0, 0)$ is of the form f^{p^n} then this curve is a composition (in the sense of Section 3.1) of some curve with formal power series expansion f and the graph of the n-th power of the Frobenius morphism $\mathbb{A}^1 \to \mathbb{A}^1$, and the necessary statement follows.

For the general case, find projections $p_i : M \to \mathbb{A}^1$ that map P_i to 0 and such that p_i is étale in a neighbourhood of P_i. Since étale morphisms induce isomorphisms of completed local coordinate rings, local coordinate systems at P_1, P_2, P_3 are induced by precomposing with p_1, p_2, p_3 respectively. Observe that the slope of Z_1 at (P_1, P_2) coincides with the slope of $(p_1 \times p_2)(Z_1)$ and similarly for Z_2 and $(p_2 \times p_3)(Z_2)$. Then the statement follows from the statement for $\mathbb{A}^1$ which we have already proved. □

3.2 Sum of curves

We are now going to define another binary operation on curves in M^2 and more generally in M^n, $n > 2$, making use of an algebraic group structure on M. This operation amounts to the application of the group law to the second coordinate of points in M^2 and we call it, abusing terminology and notation, "the sum of curves". As the operation of composition, it can be defined in a compatible way scheme theoretically. When applied to graphs of maps from the double point to an algebraic group, the operation amounts to addition of tangent vectors which can be taken as a justification for the terminology. Ultimately, this operation will allow us to recover,in Section 5.8, the additive group of the field and the action of multiplicative group on it.

Definition 3.18 (Sum of definable curves in M^2)**.** *Let $(G,+)$ be a definable group and let $X, Y \subset G \times G$ be definable curves. Define:*

$$X + Y := \{(x,u) \in G \times G \mid \exists y, z \in G \;\; (x,y) \in X \quad \textit{and } (x,z) \in Y, \\ \textit{and } u = y + z)\}$$

Remark. The notation above suggests that G is commutative. The definition applies even if it is not the case, although in this paper we will only deal with G which are Abelian or Abelian-by-finite.

Note that the sum of curves does not in general define a group law on the class of all definable curves in G^2: in fact, the obvious candidate for a curve "opposite" to a curve X,

$$-X := \{\ (x,-y) \ \mid \ (x,y) \in X \ \}$$

is an opposite with respect to "+" only if X is a graph of a function.

The compatible scheme-theoretic operation is defined as follows:

Definition 3.19 (Scheme-theoretic sum of curves)**.** *Let G be an algebraic group, $X, Y \subset G \times G$ curves. Define $X+Y$ to be the curve cut out in $G \times G$ by the ideal*

$$I_{X+Y} = (p_1 \times a \circ p_{23})_*(p_{12}^* I_X \otimes p_{13}^* I_Y)$$

where $a : G \times G \to G$ is the group law morphism.

Guided by the same considerations that motivated the intruduction of the relative composition (Definition 3.14), we define an operation on curves in G^n that generalizes that of Definition 3.19 and 3.18, with the aim of expressing the relative slope of the result of this operation as a sum of relative slopes of its arguments.

Definition 3.20 (Relative sum)**.** *Let G be an algebraic group, N, N' algebraic varieties, and $X \subset G^2 \times N$, $Y \subset G^2 \times N'$ be curves. We define the* relative sum $X+Y$ of X and Y *to be the curve cut out by the ideal*

$$I_{X+Y} = (\mathrm{id} \times a \circ p_{24})_*(p_{123}^* I_X \otimes p_{145}^* I_Y)$$

where $a : G \times G \to G$ is the group law morphism and p_{ij}, p_{ijk} are projections on products of factors of $G^3 \times N \times N'$.

If X and Y are definable sets, their relative sum is defined on as follows:

$$X + Y := \{(a,b,c,d,e,b+d) \mid (a,b,c) \in X, (a,d,e) \in Y\}$$

Let G be a one-dimensional algebraic group, then the *formal group law of G* is defined as the image of the topological generator of $k[[x]] \cong \widehat{\mathcal{O}_{G,e}}$ under the morhpism $\widehat{\mathcal{O}_{G,e}} \to \widehat{\mathcal{O}_{G,e}} \hat{\otimes} \widehat{\mathcal{O}_{G,e}} \cong k[[x,y]]$ induced by the group operation morhpism. It is a well-known fact lower order terms of a one-dimensional formal group law are $x+y$.

If $F \in k[[x,y]]$ is a one-dimensional formal group law, we denote F_n its n-th order truncation in $k[x,y]/(x^{n+1}, y^{n+1})$.

Proposition 3.21. *Let G be an algebraic group over an algebraically closed field k with the group law morphism $a : G \times G \to G$.*

Let $X \subset G \times G \times N$, $Y \subset G \times G \times N'$ be curves and assume slopes are well-defined at points $(P_1, P_2, P_3) \in X, (P_1, P_4, P_5) \in Y$. Then for all $n \geq 1$

$$\begin{aligned}\tau_n(X + Y/G^2 \times N \times N', \quad & (P_1, P_2, P_3, P_4, P_5, P_2 + P_4) = \\ & = F_n(\tau_n(X/N, (P_1, P_2, P_3)), \tau_n(Y/N', (P_1, P_4, P_5)))\end{aligned}$$

where F is the formal group law of G, and F_n is regarded as a morphism from $k[\varepsilon]/(\varepsilon^{n+1})$ to $k[x, y]/(x^{n+1}, y^{n+1})$ which sends ε to $F_n(x, y)$. In particular, for $n = 1$,

$$\begin{aligned}\tau_n(X + Y/G^2 \times N \times N', \quad & (P_1, P_2, P_3, P_4, P_5, P_2 + P_4) = \\ & = \tau_n(X/N, (P_1, P_2, P_3)) + \tau_n(Y/N', (P_1, P_4, P_5))\end{aligned}$$

Proof. Denote $T = \operatorname{Spec} k[\varepsilon]/(\varepsilon^{n+1})$. As in Proposition 3.16, Cartesian powers of T embed into Cartesian powers of G according to the local coordinate systems chosen.

By Lemma 3.12, for all $n \geq 0$,

$$\Gamma(\tau_n(X/N, (P_1, P_2, P_3))) \cong p_{12}(X \times_{G^2} T^2)$$

and

$$\Gamma(\tau_n(Y/N', (P_1, P_4, P_5))) \cong p_{12}(Y \times_{G^2} T^2)$$

Denote I_X, I_Y the ideal sheaves that cut out $X \times_{G^2} T^2$, respectively $Y \times_{G^2} T^2$, in $G^2 \times N$, respectively $G^2 \times N'$.

Let f, g be the endomorphisms of T associated to $\tau_n(X/N, (P_1, P_2, P_3))$ and $\tau_n(Y/N', (P_1, P_4, P_5))$. Let $\gamma_X : T \to T \times T \times N, \gamma_Y : T \to T \times T \times N'$ be the sections of the projection $X \times_{M^2} T^2 \subset T \times T \times N$, respectively $Y \times_{M^2} T^2 \subset T \times T \times N'$, on the first factor T. Let $\eta_Y : T \times T \times N \to T \times T \times N \times T \times N'$ be the map that acts as identity on the first T and on N and as γ_Y on the second T but sends the result to the product of second, third and fifth factors of the destinantion.

The following identities follow immediately from these definitions:

$$p_2 \gamma_X = f \qquad p_{123} \circ \eta_Y = \mathrm{id}$$

and that $p_{145}^* I_Y \cong \eta_{Y*} \mathcal{O}_{T \times T \times N}$,and that $I_X \cong \gamma_{X*} \mathcal{O}_T$.

It follows from the definition of relative sum and Lemma 3.12 that

$$p_{16*}(\mathrm{id} \times F_n \circ p_{24})(p_{123}^* I_X \otimes p_{145}^* I_Y)$$

is the ideal that cuts out the graph of

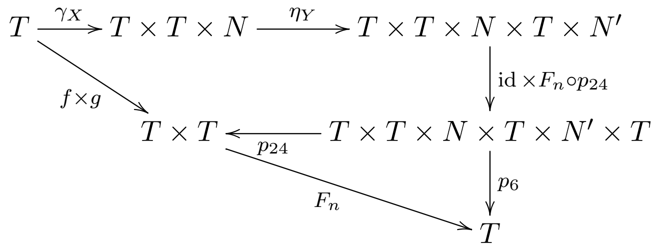
$$\tau_n(X + Y/G^2 \times N \times N', (P_1, P_2, P_3, P_4, P_5, P_2 + P_4)$$

in $T \times T$.

Then applying Lemma 3.15 and simplifying, we obtain

$$\begin{aligned}
& p_{16*}(\mathrm{id} \times F_n \circ p_{24})_*(p_{123}^* I_X \otimes p_{145}^* I_Y) = \\
= \ & p_{16*}(\mathrm{id} \times F_n \circ p_{24})_*(p_{123}^* I_X \otimes \eta_{Y*}\mathcal{O}_{T\times T\times N}) = \\
= \ & p_{16*}(\mathrm{id} \times F_n \circ p_{24})_*\eta_{Y*}(\eta_Y^* p_{123}^* I_X \otimes \mathcal{O}_{T\times T\times N}) = \\
= \ & p_{16*}(\mathrm{id} \times F_n \circ p_{24})_*\eta_{Y*}\eta_Y^* p_{123}^* \gamma_{X*}\mathcal{O}_T = \\
= \ & (p_{16} \circ (\mathrm{id} \times F_n \circ p_{24}) \circ \eta_Y \circ \gamma_X)\mathcal{O}_T.
\end{aligned}$$

The composition $p_{16} \circ (\mathrm{id} \times F_n \circ p_{24}) \circ \eta_Y \circ \gamma_X : T \to T$ is the morpmism $\mathrm{id} \times F_n \circ f \times g$: indeed, the diagram



commutes, the commutation of the upper cycle follows from the definitions of γ_X and η_Y, and commutation of the lower cycle is immediate.

The conclusion of the proposition follows. □

An element of $\mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1}))$ is completely determined by the truncated polynomial with zero constant term which is the value of the endomorphism on the generator ε; addition of such truncated polynomials defines addition on $\mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1}))$ such that composition of endomorphisms is distributive over it, and makes $\mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1}))$ into a ring.

Corollary 3.22. *With the ring structure described above,* $\mathrm{End}(k[\varepsilon]/(\varepsilon^2))$ *is isomorphic to* k*.*

Proof. This is a consequence of Propositions 3.16 and 3.21. □

4 Differential equations in formal power series

4.1 Uniqueness of solutions

We will be using the uniqueness of solutions of differential equations in formal power series over a field of characteristic 0 on several occasions. Though it is well-known we include the short proof for the sake of completeness. It is stated precisely in the form needed for us.

Lemma 4.1 (Picard-Lindelöf for formal power series)**.** *Let* k *be a field of characteristic 0. Let* $f(x, y) \in k[[x, y]]$ *be a formal series. Then there exists a unique* $y \in xk[[x]]$ *such that*

$$y' = f(x, y)$$

where y' *is a formal derivative.*

Proof. Denote $f(x,y) := \sum\limits_{i,j=0}^{\infty} f_{i,j}x^iy^j$ and define a map $\varphi : xk[[x]] \to xk[[x]]$ by setting

$$y \mapsto \int_0^x f(\alpha,y)d\alpha := \sum_{i,j=0}^{\infty} f_{i,j}\int_0^x \alpha^i y^j d\alpha$$

where $\int_0^x$ denotes formal antiderivative with zero constant term. Then φ is well defined, and we claim that it is a contracting map. Indeed, let $v : k[[x]] \to \mathbb{Z}$ be the valuation on the ring of formal series, $\|\cdot\|_v$ the associated norm $\|x\|_v = e^{-v(x)}$ (which is trivially 1 on constants).

$$\|\varphi(y_1) - \varphi(y_0)\|_v = \|\sum_{i,j=0}^{\infty} f_{i,j}\int_0^x \alpha^i(y_1^j - y_0^j)\|_v d\alpha \leq \frac{1}{e}\|y_1 - y_0\|_v$$

As $(k[[x]], ||\cdot||_v)$ is a complete metric space, the Banach fixed point theorem asserts that φ has a unique fixed point. By definition of ϕ this fixed point is a solution of the given differential equation. □

4.2 Differential equations for slopes

On $\mathbb{A}^1$ there are natural local coordinate systems at any point x_0 given by the projective system of morphisms $k[x] \to k[\varepsilon]/(\varepsilon^n)$, $x \mapsto \varepsilon + x_0$. We would like to have in a similar vein a coherent choice of local coordinate systems at every point of a dense open subset of an arbitrary curve. Let U is a curve and suppose an étale morphism $u : U \to \mathbb{A}^1$ is chosen, then for any closed point $y \in U$ the pullback of $x - u(y) \in k[x]$ gives canonical choice of uniformizer in $\mathcal{O}_{U,y}$, and hence local coordinate systems are chosen at each such y; these are the local coordinate systems that come from isomorphisms $\widehat{\mathcal{O}_{U,y}} \cong \widehat{\mathcal{O}_{\mathbb{A}^1,u(y)}}$. We will refer to such local coordinate systems as *liftings* of local coordinate systems on $\mathbb{A}^1$.

Lemma 4.2. *Let u, v be two étale maps from U, V to $\mathbb{A}^1$, and let p be the product map $p := u \times v : U \times V \to \mathbb{A}^2$. Then for any $n > 0$, for any closed subscheme Z of $U \times V$ and any point $Q \in Z$*

$$\tau_n(Z,Q) = \tau_n(p(Z), p(Q))$$

where the local coordinate systems on $U \times V$ and on $\mathbb{A}^2$ are chosen as above.

Proof. By Lemma 3.11, $S := \operatorname{Spec} \mathcal{O}_{Z,Q} \otimes_{\mathcal{O}_{U\times V,Q}} k[\varepsilon,\eta]/(\varepsilon^n,\eta^n)$ is the graph $\tau_n(Z,Q)$, and $\operatorname{Spec} \mathcal{O}_{p(Z),p(Q)} \otimes_{\mathcal{O}_{\mathbb{A}^2,p(Q)}} k[\varepsilon,\eta]/(\varepsilon^n,\eta^n) = p(S)$ is the graph of $\tau_n(p(Z),p(Q))$. It is left to notice that the map $u \times v$ induces an isomorphism between $\operatorname{Spec} \mathcal{O}_{U\times V,Q} \otimes k[\varepsilon,\eta]/(\varepsilon^n,\eta^n)$ and $\operatorname{Spec} \mathcal{O}_{\mathbb{A}^2,p(Q)} \otimes k[\varepsilon,\eta]/(\varepsilon^n,\eta^n)$, by étaleness and the choice of local coordinate systems, and furchermore, S and $p(S)$ are isomorphic. □

Lemma 4.3. *Let $Z \subset \mathbb{A}^2$ be a curve defined by an equation $h(x,y) = 0$, $Q \in Z$ a regular point such that the projection of Z on the first factor is étale. Let $f \in k[[x]]$ be the formal power series expansion of Z in the natural local coordinate system on $\mathbb{A}^2$ at Q. Then $h(x, f) = 0$.*

Proof. Without loss of generality one may assume $Q = (0,0)$. Then the fact that n-th order slope of Z is the endomorphism f_n of $k[\varepsilon]/(\varepsilon^n)$ means that the morphism of algebras

$$k[x,y] \to k[\varepsilon]/(\varepsilon^n) \qquad x \mapsto \varepsilon,\ y \mapsto f_n(\varepsilon)$$

factors through $k[x,y]/h$, i.e. $h(x, f_n) = 0 \mod x^n$ [It may be worth giving slightly more detail why this is true. Maybe as an example following the definition of slope. This is also used below, so would be good to have explicitly, and will also clarify the definition of slope]. The conclusion of the lemma follows by passing to the limit. □

Let U, V be open subsets of M, and let $u : U \to \mathbb{A}^1, v : V \to \mathbb{A}^1$ be étale maps. Let $Z \subset U \times V$ be a regular curve such that the projection of Z on U is étale, and for any point $Q = (Q_1, Q_2) \in U \times V$ the first order slope of Z at Q is well-defined (with respect to the liftings of the natural local coordinate systems at $u(Q_1), v(Q_2)$ to Q_1, Q_2) provided by the Lemma 4.2). Let $Z' \subset U \times V \times \mathbb{A}^1$ be the closed curve such that $(x, y, s) \in Z'$ if s is the first order slope of Z at (x, y).

Proposition 4.4. *In the above setting, Let $k[[u,v]] \cong \widehat{\mathcal{O}_{M^2,Q}}$ be the isomorphism given by the chosen local coordinate system at Q, and $\eta : \operatorname{Spec} k[[x]] \to Z$ the morphism given by the morphism of rings*

$$\eta^* : \mathcal{O}_{Z,Q} \to k[[x]], u \mapsto x, v \mapsto f$$

where $f \in xk[[x]]$. Consider the morphism $\eta' : \operatorname{Spec} k[[x]] \to U \times V \times \mathbb{A}^1$ defined by the morphism of rings

$$\eta'^* : \mathcal{O}_{U \times V \times \mathbb{A}^1, Q_1 \times \{0\}} \to k[[x]], u \mapsto x, v \mapsto f, w \mapsto f'$$

where and f' is the formal derivative of f'. Then η' factors through Z'.

Proof. By Lemma 4.2 the slope of Z at Q is the same as the slope of $(u \times v)(Z)$ at $(u(Q_1), v(Q_2))$, in their respective local coordinate systems. So it suffices to prove the statement assuming that Z is a locally closed subset of $\mathbb{A}^2$. Without loss of generality we may assume $Q = (0,0)$.

Let Z be defined by a polynomial $h(u,v)$. The slope of Z at a point $(x,y) \in \mathbb{A}^2$ is given by the expression

$$\frac{\dfrac{\partial h}{\partial u}(x,y)}{\dfrac{\partial h}{\partial v}(x,y)}$$

where the derivatives are formal. Let $f \in k[[x]]$ be a formal power series such that $h(x, f) = 0$ as provided by Lemma 4.3. Then

$$\frac{d}{dx}h(x,f) = \frac{\partial h}{\partial u}(x,f) + \frac{\partial h}{\partial v}(x,f)f'$$

by the chain rule (Corollaire 1, [4], IV.§6), and $\frac{d}{dx}h(x,f) = 0$ by our choice of f. Therefore

$$\frac{\frac{\partial h}{\partial u}(x,f)}{\frac{\partial h}{\partial v}(x,f)} = f'$$

and $(x, f, f') \in Z'$. $\square$

Corollary 4.5. *Let $u : U \to \mathbb{A}^1, v : V \to \mathbb{A}^1$ be étale. Let $Q \in U \times V$ and let X be a curve incident to Q such that its projection to U is étale. Let $Z \subset U \times V \times \mathbb{A}^1$ be a closed subset that is étale over $U \times V$. Assume $X' \subset X \times \mathbb{A}^1$ is a closed subset such that $(x, y, s) \in X'$ if the first order slope of X at the point (x, y) is s, in the local coordinate system which is a lifting of the natural local coordinate system at $(u(x), v(x))$.*

Then there exist formal power series $h \in k[[x, y]]$ such that for any X as above, with a fixed slope at Q, and such that $X' \subset Z$, and $f = \varprojlim_n \tau_n(X, Q)(x) \in k[[x]]$, the formal power series expansion of X at Q,

$$f' = h(x, f)$$

where f' is the formal derivative of f.

In the statement of this corollary Z should be regarded a "multi-valued distribution", a variety that specified what slopes X is allowed to have at a particular point.

Proof. By the same reasoning as in the proof of Lemma 4.4 we can reduce the situation to U, V open subsets of $\mathbb{A}^1$ and X a locally closed subset of $\mathbb{A}^2$.

Let $s_0 = \tau_1(X, 0)$, we have the following commutative diagram

$$\begin{array}{ccccc}
\widehat{\mathcal{O}_{\mathbb{A}^3,(0,0,s_0)}} \cong k[[x,y,z]] & \xrightarrow{f_1} & \widehat{\mathcal{O}_{Z,0}} & \xrightarrow{f_2} & \widehat{\mathcal{O}_{X',(0,0,s_0)}} \\
\uparrow & \swarrow_{g}^{\sim} & & & \uparrow \\
\widehat{\mathcal{O}_{\mathbb{A}^2,(0,0)}} \cong k[[x,y]] & & \longrightarrow & & \widehat{\mathcal{O}_{X,(0,0)}}
\end{array}$$

where g is an isomorphism by étaleness of the projection of Z on $\mathbb{A}^2$ and the map f_1 is given on generators as follows (identifying $\widehat{\mathcal{O}}$ via the g): $x \mapsto x, y \mapsto y, z \mapsto h$ for some $h \in k[[x, y]]$. On the other hand, by Proposition 4.4, the compostion of maps f_1 and f_2 is given on generators as follows $x \mapsto x, y \mapsto f, z \mapsto f'$. The conclusion of the Corollary follows. $\square$

4.3 Divided power structures and an ODE for $\mathbb{G}_m$

Later in Section 5 we will be looking at curves is the product of two copies of the multiplicative group $\mathbb{G}_m \times \mathbb{G}_m$, and in connection with this we will need to consider formal power series solutions to the differential equation

$$y' = a \cdot \frac{1+y}{1+x} \tag{2}$$

Below we collect some facts about solutions to this equation, especially that the situation in positive characteristic requires a somewhat subtle treatment.

Let k be a field of characteristic 0. Consider *binomial power series* for $a \in k$, defined as

$$(1+x)^a = \sum_{k=0}^{\infty} \frac{a \cdot (a-1) \dots (a-k)}{k!} x^k$$

If a is integer then this is a polynomial, but the formal power series are well-defined for any $a \in k$.

Proposition 4.6. *Let k be a field of characteristic 0. The unique solution of the differential equation (2) is the binomial power series $(1+x)^a - 1$. These formal power series are algebraic over $k[x]$ only if a is rational.*

Proof. Observe that $\frac{d}{dx}(1+x)^a = a(1+x)^{a-1}$, then it's easy to check that $(1+x)^a$ is a solution by direct substitution.

For the second point observe that if a is not rational, then powers of $(1+x)^a$ generate a module of infinite rank over $k[x]$, and so $(1+x)^a$ is not algebraic. One uses the property

$$(1+x)^a(1+x)^b = (1+x)^{a+b}$$

which can be easily derived oven for a not rational (see Section 2 of [12] and references therein). ☐

Even though uniqueness of solutions of ODEs fails in positive characteristic in general, we can say something about solutions to the equation (2). Unfortunately, the binomial power series are not even well-defined in positive characteristic, because integers dividing the characteristic appear in denominators of the coefficients.

In order to remedy that, we consider solutions of differential equation (2) in a bigger ring that $k[[x]]$ maps to. This ring is the completion of the divided power polynomials ring $k\langle x\rangle$ of $k[x]$ with respect to a certain filtration. For definition and properties of divided power structures we refer to [2], see also [1].

The facts about $k\langle x\rangle$ that we will need are few. The ring $k\langle x\rangle$ is generated over k by variables $x^{[n]}, n \in \mathbb{N}$, subject to relations

$$x^{[n]}x^{[m]} = \frac{(n+m)!}{n!m!} x^{[n+m]}$$

($x^{[0]}$ customarily means 1).

Consider the homomorphism $\varphi : k[x] \to k\langle x\rangle$ that sends x to $x^{[1]}$. The kernel of this morphism is the ideal generated by x^p. Define the derivation D_x on the generators by $D_x x^{[n]} = x^{[n-1]}$. The homomorphism φ has the following property:

$$\varphi(p'(x)) = D_x\varphi(p(x))$$

Consider the completion $\widehat{k\langle x\rangle}$ of $k\langle x\rangle$ with respect to the filtration by the ideals generated by sequences of elements of the form $x, x^{[2]}, x^{[3]}, \ldots, x^{[i]}$. The homomorphism φ above extends to a morphism $\bar{\varphi} : k[[x]] \to \widehat{k\langle x\rangle}$, and the derivation D_x is extended in a unique way to $\widehat{k\langle x\rangle}$. The compatibility of derivations is preserved: $\bar{\varphi}(p'(x)) = D_x\bar{\varphi}(p(x))$.

Define *divided power binomial series*

$$(1+x)^a = \sum_{n=0}^{\infty} a\cdot(a-1)\cdot\ldots\cdot(a-n+1)x^{[n]}$$

in $\widehat{k\langle x\rangle}$.

Lemma 4.7. *Let k be a field of positive characteristic $p > 0$. The differential equation* (2) *has a solution*

$$(1+x)^a - 1$$

in $\overline{k\langle x\rangle}$ if and only if $a \in \mathbb{F}_p$. Let $y_1, y_2 \in k[[x]]$ be two distinct solutions, then $\dfrac{y_1+1}{y_2+1}$ belongs to $k((x^p))$ and is non-constant.

Proof. Observe that if $f \in k[[x]]$ is a solution to (2), then $\bar{\varphi}(f)$ is a solution to (2) (with derivation interpreted as D_x).

If $a \in \mathbb{F}_p$, the binomial formal power series is a polynomial which is a solution to equation 2 by direct verification. If $a \notin \mathbb{F}_p$ then the divided powers binomial power series is a solution to (2) by direct verification.

Let y_1, y_2 be distinct solutions in $\widehat{k\langle x\rangle}$ of the equation (2). Then

$$D_x\left(\frac{y_1+1}{y_2+1}\right) = \frac{y_1'(y_2+1) - y_2'(y+1)}{(y_2+1)^2} = \frac{a(y_1+1)(y_2+1) - a(y_2+1)(y_1+1)}{(1+x)(y_2+1)^2} = 0$$

and therefore $\dfrac{y_1+1}{y_2+1}$ is a constant. One checks that if $\dfrac{y_1+1}{y_2+1}$ is a constant then it must be 1. The same argument in $k[[x]]$ yields that formal power series solutions y_1, y_2 have the property that $\dfrac{y_1+1}{y_2+1} \in k((x^p))$.

If $a \in \mathbb{F}_p$ then an algebraic solution y_1 must have the property that $\dfrac{y_1+1}{(1+x)^a}$ is algebraic.

If $a \notin \mathbb{F}_p$, one checks that $(1+x)^a \in \widehat{k\langle x\rangle}$ is not in the image of φ (since it has $x^{[n]}$ terms for $n \geq p$) and so there are no solutions in $k[[x]]$. $\square$

5 Interpretation of a field from a pure-dimensional witness family

Restricting to the regular locus of M we may assume that M is regular, which will be the standing assumption in the present section.

A reduct of M is non-locally modular if and only if there exists a *faithful* (in the terminology of [41]; the term *normal* is commonly used in the literature) definable family of strongly minimal sets $X \subset M^2 \times T$, i.e. a family such that $\dim T = 2$, $\dim X_t = 1$ for $t \in U$, $\dim T \setminus U \leq 1$ and such that $\dim(X_t \setminus X_s) \cup (X_s \setminus X_t) = 0$ for $t \neq s$. Let M be a one-dimensional algebraic curve. Throughout this section the family of curves that witness of lack of local modularity of $\mathcal{M}$ will be denoted X with parameter space T, unless this notation is explicitly claimed to be used for something else.

For the purposes of the present paper we fix the following set the following set of conventions:

Definition 5.1. *Let M be a curve over an algebraically closed field.*

1. *by a* family of curves *in M^2 we understand a locally closed subset $X \subseteq M^2 \times T$ for some T such that the fibres (which are not assumed irreducible) X_t are of dimension 1 for all $t \in T$;*
2. *by a* family of curves *in $M^2 \times N$ for some variety N we understand a locally closed subset $X \subseteq M^2 \times N \times T$ for some T such that the fibres (which are not assumed irreducible) X_t are of dimension 1 for all $t \in T$ and such that projection on M^2 has finite fibres;*
3. *we call a family of curves* pure-dimensional *if all irreducible components of fibres X_t are of the same dimension for all $t \in T$;*
4. *the family of* (scheme-theoretic) intersections *of two families of curves $X \subseteq M^2 \times T$ and $Y \subseteq M^2 \times S$ is the surjective morphism $(X \times S) \times_{M^2 \times T \times S} (Y \times T) \to T \times S$ (that is, the family of closed subschemes of M^2 whose fibre over (t, s) is $X_t \times_{M^2} Y_s$);*
5. *we call the family of* (scheme-theoretic) relative intersections *of two families of curves $X \subseteq M^2 \times N \times T$ and $Y \subseteq M^2 \times N' \times S$ the surjective morphism $(X \times S) \times_{M^2 \times T \times S} (Y \times T) \to T \times S$ (that is, the family of closed subschemes of $M^2 \times N \times N'$ whose fibre over (t, s) is $X_t \times_{M^2} Y_s$). This coincides with the notion for families of curves in M^2 defined above if one takes N and N' to be points.*

In this section we assume that X is a family of pure dimensional curves, namely, that X_t has only components of dimension 1 for t generic. We first prove that then $\mathcal{M}$ interprets a one-dimensional group. Then, assuming that there is a group structure on M, we prove that $\mathcal{M}$ interprets a field.

Here is some notation that we will systematically use.

For any point $Q \in M^2$, any family $Y \subset M^2 \times S$ of curves we denote $Y^Q \to S^Q$ the subfamily of curves containing the point Q. For any family of curves $Y \subset M^2 \times N \times S$ we denote $Y^Q \to S^Q$ the subfamily of curves such that their projection on M^2 contains Q. We will call such curves *relatively incident to Q*.

For any family of curves X, for any curve $Z \subset M^2 \times N$ denote $Z \circ X \to T$ the family such that $(Z \circ X)_t = Z \circ X_t$; similarly, $X \circ Z$ denotes the family $(X \circ Z)_t = X_t \circ Z$.

For two (definable) families $Y_1 \subset S_1 \times M^2, Y_2 \subset S_2 \times M^2$ of curves in M^2 we will denote $Y_1 \circ Y_2$ the (definable) family parametrized by $S_1 \times S_2$ with the curve $(Y_1)_{s_1} \circ (Y_2)_{s_2}$ corresponding to parameters s_1, s_2; similarly, the notation $Y_1 + Y_2$ will be used for families of curves in G^2 where G has a structure of a group.

We will say that two sets Y and Z of the same dimension *almost coincide* if $\dim(Y \setminus Z) \cup (Z \setminus Y) < \dim Y (= \dim Z)$. We will say that a property holds for *almost all points* of a definable set Y if it holds for a set of points Y' that almost coincides with Y.

5.1 Generically étale projections

In order for slopes (defined in Section 3) to be well-defined we need projections of curves in $M \times M$ on the first factor M to be étale in a Zariski open neighbourhood of the point. The following lemma asserts that at least one of the "coordinate" projections of a curve $X \subset M \times M$ does satisfy this requirement generically. The statement of the lemma is obvious in characteristic 0, but the existence of everywhere ramified morphisms in positive characteristic makes it non-trivial in this case.

Lemma 5.2. *Let M be a one-dimensional closed irreducible curve over a field of positive characteristic. Let $X \subset M \times M$ be an irreducible closed curve, and $p_1, p_2 : X \to M$ be the projections on the respective factors M. Then there exists a dense open $O \subset M$ such that either p_1 restricted to $X \cap O \times M$ or p_2 restricted to $X \cap M \times O$ is étale.*

Proof. The lemma is clear if one of the projections p_i is not dominant. So we may assume that this is not the case.

Let $\Omega_{M/k}$, $\Omega_{X/k}$ be the sheaves of modules of Kähler differentials over k of M and of X respectively. Consider the natural map of sheaves

$$p_1^*\Omega_{M/k} \oplus p_2^*\Omega_{M/k} \to \Omega_{X/k}$$

which is surjective because X is embedded into M^2. Localising at the generic point χ of X we get a surjective map, f, of vector spaces over the field $k(\chi) = k(X)$

$$f : p_1^*\Omega_{M/k} \otimes k(\chi) \oplus p_2^*\Omega_{M/k} \otimes k(\chi) \to \Omega_{X/k} \otimes k(\chi).$$

Then $f = f_1 \oplus f_2$ where $f_i : p_i^*\Omega_{M/k} \otimes k(\chi) \to \Omega_X \otimes k(\chi)$ is a $k(X)$-linear map. As f is surjective and $\dim_{k(X)} \Omega_X \otimes k(\chi) = 1$, at least one function out of f_1 and f_2 must be an isomorphism.

Assume that for example f_1 is an isomorphism. Then the sheaf $\Omega_{X/M}$ of relative differentials on X over M with respect to the first projection, is isomorphic over a dense open set to the structure sheaf. So p_1 is generically unramified. The statement of the lemma then follows from generic flatness (Fact 5.11). $\square$

Lemma 5.3. *If the field of definition of M is of positive charactrestic p, and assume that the projection of X on the first M is étale. Then there exists a number n such that the second projection of the preimage X' of curve X under the maps $\mathrm{Fr}^n_{M^2/M} : M \times M^{1/p^n} \to M \times M$, where $\mathrm{Fr}_{M^2/M}$ is the relative Frobenius morphism that respects p_2, are both generically étale.*

Proof. Without loss of generality assume that f_1 is an isomorphism. Therefore $f_2 = 0$ which implies that p_2 induces an extension of function fields $k(M) \subset k(X)$ that factors into a sequence of a separable extension an a purely inseparable one: $k(M) \subset k(X') \subset k(X)$. By definition of the relative Frobenius, it raises the elements of $k(X)$ that do not belong to $k(M)$ to the p-th power, so $k(\mathrm{Fr}^n_{M^2/M}(X)) \subseteq k(X')$ for n equal to the degree of inseparability of the extension $[k(X') : k(X)]$. $\square$

Lemma 5.4. *Let M be a one-dimensional closed irreducible curve over a field of any characteristic. Let $X \subset T \times M \times M$ be a family of closed curves. Then for any irreducible component $T_0 \subset T$, $M_0 \subset M$ there exists a dense open $U \subseteq T_0$ and a dense open $O \subseteq M$ such that either p_1 restricted to $X_t \cap O \times M$ or p_2 restricted to $X_t \cap M \times O$ is étale for all $t \in U$.*

Proof. Follows from the previous lemma applied to the generic fibre of the family $X \to T$. $\square$

5.2 Finding enough slopes in characteristic 0

In order to obtain a one-dimensional group configuration in the reduct $\mathcal{M}$ we need to produce families of curves, incident or relatively incident to a point $Q \in M^2$, such that for some n the (relative) n-slopes, as s runs in a nirreducible component of teh prarameter set, containts a one-dimensional set that almost coincides with a one-dimensional subgroup of $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^{n+1})$ for some n. We will present two approaches, the first uses Lemma 4.1 in a significant way, and works only in characteristic zero. It gives a set $O \subset M^2$, dense in an irreducible component of M^2, such that $X^Q \to T^Q$ has the required propriety for any $Q \in O$. The second approach, presented in next subsection, works in any characteristic but gives a single family that satisfies the property for a number n that generally speaking may be strictly greater than 1.

Lemma 5.5. *Let M be an algebraic curve (not necessarily irreducible) over an algebraically closed field of characteristic 0, and let $X \subset S \times M^2$ be a 2-dimensional faithful family of closed irreducible one-dimensional subsets of M^2. Then there exists an open subset $O \subset M^2$ such that for any point $Q \in O$ the set $\tau_1(X_s, Q)$, as s runs in a T^Q, is one-dimensional.*

Proof. Assume not. Then one can pick an Zariski open set $O \subset M^2$, dense in an irreducible component of M^2, such that $\tau_1(X_s, Q)$ is finite for all $Q \in O$.

Pick some étale projections $u : U \to \mathbb{A}^1, v : V \to \mathbb{A}^1$. By Lemma 4.2 the projections $(u \times v)(X_s)$ will have finitely many slopes at points of some dense open subset of $\mathbb{A}^2$, call it O'.

Let Z be the locally closed subset of $U \times V \times \mathbb{A}^1$ such that a point (x, y, s) belongs to Z if a curve from the family X incident to (x, y) has the slope s at (x, y) in the natural local coordinate system. Shrinking O' if necessary we may assume that Z is étale over O'. Pick a point $Q \in O'$ and pick one of the finitely many first-order slopes the curves from the family X has at Q, call it a. Then by Corollary 4.5 for any curve $X_t \subset U \times V$ with $\tau_1(X_t, Q) = a$, the formal power series expansion f at a point $Q \in O'$ must satisfy a differential equation

$$f' = h(x, f)$$

for some $h \in k[[x, y]]$. By Lemma 4.1 there is only one solution $f \in xk[[x]]$ per slope value at Q. But according to our assumption about X there are infinitely many curves incident to Q, which is a contradiction. $\square$

5.3 Finding enough slopes in positive characteristic

The simplest example that illustrates how the approach of the previous section breaks down in the positive characteristic is the family of curves on $\mathbb{A}^2$ defined in the standard coordinates (x, y) by the equations $y = x + ax^p + b$, which all have the same slope 1 in the standard coordinates. As turns out, the fact that the formal power series expansions of curves differ by formal power series that lie in $x^p k[[x^p]]$, is the only obstacle to finding families with "enough slopes".

Lemma 5.6. *Let M be a curve over an algebraically closed field of positive characteristic, and let $X \subset M^2 \times T$ be a family of curves.*

Then there exists a point $Q \in M^2$ and a one-dimensional definable family of curves $Y \to S$ relatively incident to Q such that for some n, the set of slopes $\tau_n(Y/N, Q')$ contains a one-dimensional set that almost coincides with a subgroup of $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^{n+1}))$.

Proof. By Lemma 5.3 for every irreducible component of M_0 of M, for every irreducible component of T_0 there exists a number n such that for any $t \in T_0$ generic the projections of $\mathrm{Fr}_{M^2/M} \times \mathrm{id}_T(X_t) \cap M_0 \times M_0^{(p)}$ on M_0 and $M_0^{(p)}$ are generically étale.

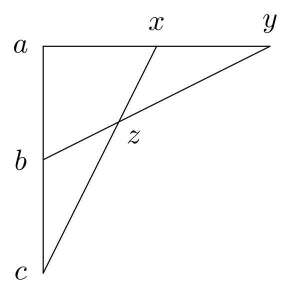
It follows that for a generic point Q in one of irreducible components M_0, the formal power series expansions of curves X_t with t generic in T^Q are of the form f^{p^n} for some $f \in \mathrm{Aut}(k[[x]])$.

Then by Lemma 3.17 the curves $X'_t = X_t \circ X_{t_0}^{-1}$ for some $t_0 \in T$ have relative power series expansion at a point Q' that lies in $xk[[x]]$. Let n be smallest number such that the set of relative slopes $\tau_n(X'_t/M, Q')$ is one-dimensional. If $n = 1$, we are done. Otherwise, $\tau_{n-1}(X'_t/M, Q')$ is finite. Then for some $t_1 \in T$, the set of relative slopes $\tau_{n-1}(X'_t \circ X_{t_1}^{-1}/M^2, Q'')$ for some Q'' contains the identity, and therefore $\tau_n(X'_t \circ X_{t_1}^{-1}/M^2, Q'')$ contains a set that almost coincides with a subgroup of $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^{n+1}))$. □

5.4 The group and field configurations

In the strongly minimal context, certain configuration of (imaginary) elements are known to exist only in the presence of a definable group or a definable field. We will now describe this in more detail:

Definition 5.7 (Group configuration)**.** *Let M be a model of a strongly minimal theory, and let* dim *the be associated dimension function on tuples.*



The set $\{\ a, b, c, x, y, z\ \}$ of tuples is called a group configuration *if there exists an integer n such that*

- *all elements of the diagram are pairwise independent and* $\dim(a, b, c, x, y, z) = 2n + 1$*;*
- $\dim a = \dim b = \dim c = n$*,* $\dim x = \dim y = \dim z = 1$*;*
- *all triples of tuples that lie on the same line are dependent, and moreover,* $\dim(a, b, c) = 2n$*,* $\dim(a, x, y) = \dim(b, z, y) = \dim(c, x, z) = n + 1$*;*

If G is a connected group definable in a strongly minimal theory, acting transitively on a strongly minimal definable set X, then one can construct a group configuration as follows: let g, h be independent realisations of the generic type of G and let x be a realisation of a generic type of X, then $(\ g, h, g \cdot h, u, g \cdot u, g \cdot h \cdot u\ )$ is a group configuration.

Fact 5.8 (Hrushovski)**.** *Let M be a strongly minimal structure and let $(\ a, b, c, x, y, z\ )$ be a group configuration. Then there exists a definable group G acting transitively on a strongly minimal set X with the associated group configuration $(\ g, h, g \cdot h, u, g \cdot u, g \cdot h \cdot u\ )$ such that* $\mathrm{acl}(a) = \mathrm{acl}(g), \mathrm{acl}(b) = \mathrm{acl}(h), \mathrm{acl}(g \cdot h) = \mathrm{acl}(c), \mathrm{acl}(x) = \mathrm{acl}(u), \mathrm{acl}(y) = \mathrm{acl}(g \cdot u), \mathrm{acl}(z) = \mathrm{acl}(g \cdot h \cdot u)$*. In particular,* $\dim G = \dim a$*.*

This follows from Main Theorem of [5] and the fact that infinitely definable groups in stable theories are intersections of definable groups (see, for example, Theorem 5.18[35]). The original proofs of these statements are contained in [17].

Fact 5.9. *If in the statement of Fact 5.8 one requires that the canonical base of* $\mathrm{tp}(x, y/a)$ *is interalgebraic with* a *and similarly for* $\mathrm{tp}(z, y/b)$ *and* $\mathrm{tp}(z, x/c)$ *then the action of* G *on* X *is faithful.*

Fact 5.10 (Hrushovski)**.** *Let* G *be a group of Morley rank* $n > 1$ *acting transitively and faithfully on a strongly minimal set* X*. Then there exists a definable field structure on* X *and either* $n = 2$ *and* $G \cong \mathbb{G}_a \rtimes \mathbb{G}_m$*, or* $n = 3$ *and* $G = \mathrm{PSL}_2$*.*

The original reference is [17], an exposition can also be found in [35] (Theorem 3.27).

Note that the crucial point in the proof of Fact 5.10 is establishing that G isomorphic to $\mathbb{G}_a \rtimes \mathbb{G}_m$ or PSL_2, and in case G and X are definable in an algebraically closed field (the context in which this theorem will be applied in this article) or a Zariski structure of an algebraic curve, this statement can be proved directly and much more easily.

5.5 Flat families and intersections

As already explained, identifying $\mathcal{M}$-definably when two curves (coming from two distinct but fixed definable families) are tangent at a point $Q \in M^2$ is the key to reconstructing the multiplictative and additive groups of the field. As we will see, this approach can only work if we can show that tangency of two definable curves incident to Q is a non-generic phenomenon. In the present subsection we develop the tools allowing us to show that this can, indeed, be achieved.

Given a strongly minimal family $X \to T$ of $\mathcal{M}$-definable plane curves incident to a point $(Q, Q) \in M^2$ we form the composition family $X \circ X$ and normalise it to obtain a family $Y \to S$. Our aim is to construct an $\mathcal{M}$-definable function from S to T taking s to t if X_t has the same slope at (Q, Q) as Y_s. This will allow us to construct a group configuration based on an $\mathcal{M}$-definable function $T \times T \to T$, which by the results of Subsection 3.1 corresponds to multiplication in K. The main goal of this Subsection is, therefore, given two definable families of curves (incident to a fixed point (Q, Q)), X and Y, to detect $\mathcal{M}$-definably and uniformly when a curve X_t and a curve Y_s have the same slope at (Q, Q). We obtain a good approximation of this goal in Proposition 5.18 under suitable flatness assumptions. This is one of the main technical results of the paper.

This strategy is implemented in the present subsection in a slightly greater generality, for families of curves in a Cartesian product of M^2 and a variety, and relative intersections, which is necessary for technical reasons.

We start with recalling a few well-known geometric facts.

Fact 5.11 (Generic Flatness, Corollaire IV.6.11 in [15])**.** *Let* Y *be an integral locally Noetherian scheme and let* $f : X \to Y$ *be a morphism of finite type. Then there exists a dense open subset* $U \subset Y$ *such that the restriction of* f *to* $f^{-1}(U)$ *is flat.*

Fact 5.12 (Local flatness criterion, Proposition I.2.5 in [30])**.** *Let B be a flat A-algebra and consider $b \in B$. If the image of b in $B/\mathfrak{m}B$ is not a zero divisor for any maximal ideal $\mathfrak{m}$ of A then $B/(b)$ is a flat A-algebra.*

Fact 5.13 (Zariski's Main Theorem, Theorem 1.8 in [30])**.** *If Y is a quasi-compact scheme and $f : X \to Y$ is a separated quasi-finite morphism, then f factors as a composition $\bar{f} \circ \iota$ where $\bar{f}$ is finite and ι is an open immersion.*

Lemma 5.14. *Suppose that M is a regular curve, and N, N' are regular varieties. Let $X \subset M^2 \times N \times T$, $Y \subset M^2 \times N' \times S$ be two families of pure-dimensional curves, and suppose that X is flat over T. Then the family of scheme-theoretic relative intersections of X and Y is flat over $T \times S \setminus D$ where D is the set of pairs (t, s) such that the relative intersection $X_t \cap Y_s$ infinite.*

Proof. Since flatness is local on the source we may assume that all varieties involved are affine.

Suppose first that X and Y are Zariski closed. Since regular local rings are unique factorization domains, X and Y are locally cut out by a single equation, and the relative scheme-theoretic intersection of X and Y is a closed subscheme of $X \times N' \times S$ that is locally the zero locus of a regular function f on $M^2 \times N \times N' \times T \times S$ restricted to $X \times N' \times S$. By Fact 5.12, this closed subset is flat precisely over the complement of the subvariety of $T \times S$ consisting of those points (t, s) where f does not vanish on an irreducible component of $X_t \times \{s\}$. In other words, it is flat over the subvariety of points (s, t) where the relative intersection $X_t \times_{M^2} Y_s$ is finite.

In general, since X and Y are families of pure-dimensional curves, their relative intersection is dense in the relative intersection of their Zariski closures. The statement of the lemma follows, since flatness is local on the source. ☐

Lemma 5.15. *Let $f : X \to Y$ be a flat quasi-finite morphism. Then the function*

$$n : Y \to \mathbb{Z} \qquad y \mapsto \#(f^{-1}(y))$$

is lower semi-continuous, i.e. the lower level sets $\{ \ y \ | \ \#(f^{-1}(y)) \leq n \ \}$ are closed.

Proof. Follows from (i) of Proposition 15.5.1 of EGA IV.3 [13] and the fact that flat morphisms of finite type are universally open (see EGA IV [13], 2.4.6). ☐

Lemma 5.16. *Let $f : X \to Y$ be a flat quasi-finite morphism. Then, denoting the fibre over a point $y \in Y$ as X_y, the function*

$$l : Y \to \mathbb{Z} \qquad y \mapsto \dim_{k(y)} H^0(X_y, \mathcal{O}_{X_y})$$

is lower semi-continuous. If f is finite, then l is locally constant.

Proof. Recall that a finite morphism is projective (EGA II 6.1.11 [13]). Thus, if f is finite the lemma follows from the fact that $\dim_{k(y)} H^0(X_y, \mathcal{O}_{X_y})$ is the constant term of the Hilbert polynomial, and the Hilbert polynomial of a flat projective family is locally constant (cf. EGA III 7.9.11).

In the general case, by Zariski's Main theorem f factors as a compostion $\bar{f} \circ \iota$ where $\bar{f} : \bar{X} \to Y$ is finite (and hence projective) and $\iota : X \hookrightarrow \bar{X}$ is an open immersion. Let Z_i be connected components of $\bar{X} \setminus X$. By the previous paragraph the function $y \mapsto H^0((Z_i)_y, \mathcal{O}_{(Z_i)_y})$ is constant on $f(Z_i)$. Therefore those lower level sets $\{ y \in Y \mid l(y) \leq n \}$ that are properly contained in Y consist of unions of Z_i. □

Lemma 5.17. *Let Y be an irreducible variety and let $f : X \to Y$ be a flat quasi-finite morphism. Let N_1, N_2 be the values of the semi-continuous functions l, n of Lemmas 5.15,5.16 on some dense open subset of Y. Then*

$$\{ y \in Y \mid \dim_{k(y)} H^0(X_y, \mathcal{O}_{X_y}) < N_1 \} \subset \{ y \in Y \mid \#f^{-1}(y) < N_2 \}$$

Proof. Factor f according to Zariski's Main Theorem as the composition of a finite $\bar{f} : \bar{X} \to Y$ and an open immersion $\iota : X \hookrightarrow \bar{X}$. The number $\dim_{k(y)} H^0(X_y, \mathcal{O}_{X_y})$ is constant on $\bar{X}$ by Lemma 5.16. Suppose y is such that $\dim_{k(y)} H^0(X_y, \mathcal{O}_{X_y}) < N_1$, then $f^{-1}(y) \subsetneq \bar{f}^{-1}(y)$ and hence $\#f^{-1}(y) < N_2$. □

Now we can prove the main result of the present subsection describing the behaviour of intersection multiplicities in families of curves. The setting is as follows. We are given a regular curve M, and a point $P = (P_1, P_2) \in M^2$, with a fixed local coordinate system associated to it, two families of curves $X \subset M^2 \times N \times T$ and $Y \subset M^2 \times N' \times S$. In the applications X and Y will be $\mathcal{M}$-definable and $\mathcal{M}$-irreducible, and the first family will be a obtained as a result of composition of two families of curves (as in Proposition 3.16), or by forming an affine combination of three families of curves (see Section 3.2). We assume, moreover, that all curves X_t are incident to a fixed point $Q \in M^2 \times N$, and that all curves Y_s are incident to Q', so that projections of Q and Q' to M^2 are both P; in the applications this will be achieved by fixing higher dimensional families and working with subfamilies passing through the point Q. We want to identify those parameters t, s such that $\tau_n(X_t/N, Q) = \tau_n(Y_s/N', Q)$. The reason to consider the relative slope and families of curves in $M^2 \times N, M^2 \times N'$ is discussed in Section 3.1 after the Definition 3.14.

In this context there is a natural number a, such that $|X_t \cap Y_s \times N| = a$ for all t, s in a dense open subset of $T \times S$. We will also assume that there exists a natural number n, smallest such that $\tau_n(X_t/M, P) \neq \tau_n(Y_s, P)$ on a dense open subset of $S \times T$. We point out that in the applications, at this stage, we cannot assure that this can be done $\mathcal{M}$-definably. We will circumvent this problem by applying the analysis to each open irreducible component of $S \times T$ separately. We will, therefore, assume that S and T are irreducible.

In the next proposition we show that, in the setting described above, for each pair (t, s) assumed generic in the parameter variety $T \times S$, if a curve from X is "tangent" to a curve from Y at P in the sense that $\tau_n(X_t/M, Q) = \tau_n(Y_s, p(Q))$

then, $|X_t \cap Y_s \times N| < l$. This will allow us to approximate tangency $\mathcal{M}$-definably, up to finitely many false positives, which will be enough for our purposes.

Proposition 5.18. *In the setting described above, let n be the minimal number such that for generic $(t, s) \in T \times S$*

$$\tau_n(X_t/N, Q) \neq \tau_n(Y_s/N', Q')$$

Consider the family of relative intersections $(X \times S) \times_{M^2} (Y \times T) \subset M^2 \times N \times N' \times T \times S$, and assume that it is proper over $T \times S$. Then there exist dense open $T' \subset T$ and $S' \subset S$ such that

$$\{(t, s) \in T' \times S' : \tau_n(X_t/M, Q) = \tau_n(Y_s, p(Q))\} \subseteq \{(t, s) : \#(X_t \times_{M^2} Y_s) < a\}.$$

Proof. By Fact 5.11 there exist $T' \subset T$, $S' \subseteq S$ dense open such that X is flat over T' and Y is flat over S'. Let $(X \times S) \times_{M^2} (Y \times T)$ be the family, parametrized by $T' \times S'$ of scheme-theoretic relative intersections of X_t and Y_s (with possibly non-reduced structure), and let $U \subset T' \times S'$ be the set of (t, s) such that $X_t \times_{M^2} Y_s$ is finite. Let Z denote the preimage of U in $(X \times S) \times_{M^2} (Y \times T)$.

The variety Z is flat over U by Lemma 5.14 and the definition of U. Let Q_0 be the image of $Q \times Q'$ in $M^2 \times N \times N'$. Let Z_0 be the irreducible component of Z supported at $\{Q_0\} \times U$, and let W be the complement of Z_0 in Z.

Below we will use subscripts to denote *scheme-theoretic* fibres: $Z_{t,s} = Z \otimes k(t, s)$ where $k(t, s)$ is the residue field of $(t, s) \in U$.

In this notation, we have to show that

$$\{\ (t, s) \in U \ \mid\ \tau_n(X_t/N, Q) = \tau_n(Y_s/N', Q')\ \} \subseteq \{\ (t, s) \in U \ \mid\ \#Z_{t,s} < a\ \}$$

where $a = \#Z_{t,s}$ for $(t, s) \in U$ generic.

Let us first prove this statement when the morphism $Z \to U$ is finite. Then the number $\dim H^0(Z_{t,s}, \mathcal{O}_{Z_{t,s}})$ is constant for all $(t, s) \in U$ by Lemma 5.16. Note that

$$\dim H^0((Z_0)_{(t,s)}, \mathcal{O}_{Z_{t,s}}) + \dim H^0(W_{t,s}, \mathcal{O}_{Z_{t,s}}) = \dim H^0(Z_{t,s}, \mathcal{O}_{Z_{t,s}}) = b$$
and
$$\#Z_{t,s} = \#W_{t,s} - 1$$

For generic t, s, $\dim H^0(\{Q\}, \mathcal{O}_{Z_{t,s}}) = n$ and therefore $\dim H^0(W_{t,s}, \mathcal{O}_{W_{t,s}}) = b - n$. If the pair t, s is such that $\tau_n(X_t/N, Q) = \tau_n(Y_s, Q')$ then

$$\dim H^0((Z_0)_{t,s}, \mathcal{O}_{Z_{t,s}}) > n$$

and therefore $\dim H^0(W_{t,s}, \mathcal{O}_{W_{t,s}}) < b - n$.

Applying Lemma 5.17 to W we get

$$\{\ (t, s) \in U \ \mid\ \dim H^0(W_{t,s}, \mathcal{O}_{W_{t,s}}) < b - n\ \} \subseteq \{\ (t, s) \in U \ \mid\ \#W_{t,s} < a - 1\ \}.$$

The latter set is the same as $\{\ (t, s) \in U \ \mid\ \#Z_{t,s} < a\ \}$ which yields the statement of the Proposition.

If $Z \to U$ is not finite then compactify it using Zariski's Main Theorem: find a finite morphism $\bar{Z} \to U$ such that Z is an open subscheme of Z, let $\overline{W}$ be the complement of Z_0 in $\bar{Z}$; note that $\overline{W} \setminus W = \bar{Z} \setminus Z$. Assume that $a = \#\bar{Z}_{t,s}, b = \dim H^0(\overline{W}_{t,s}, \mathcal{O}_{\overline{W}_{t,s}})$ for t, s generic, then we have just shown that

$$\{ (t,s) \in U \mid \dim H^0(\overline{W}_{t,s}, \mathcal{O}_{\overline{W}_{t,s}} < b - n \} \subseteq \{ (t,s) \in U \mid \#\bar{Z}_{t,s} < a \}.$$

Observe that

$$\begin{aligned}\{(t,s) \in U \mid \dim \quad & H^0(W_{t,s}, \mathcal{O}_{W_{t,s}}) < b - n\} = \\ & = \{ (t,s) \in U \mid \dim H^0(\overline{W}_{t,s}, \mathcal{O}_{\overline{W}_{t,s}} < b - n \} \cup p(\bar{Z} \setminus Z)\end{aligned}$$

and that

$$\{ (t,s) \in U \mid \#\bar{Z}_{t,s} < a \} = \{ (t,s) \in U \mid \#Z_{t,s} < a \} \cup p(\bar{Z} \setminus Z)$$

where p is the the projection of Z onto U, which implies

$$\{ (t,s) \in U \mid \dim H^0(W_{t,s}, \mathcal{O}_{W_{t,s}} < n - b \} \subseteq \{ (t,s) \in U \mid \#Z_{t,s} < a \}.$$

The last inclusion implies the statement of the Proposition. □

5.6 Interpretation of a one-dimensional group

Theorem 5.19. *Let $\mathcal{M}$ be a non-locally modular reduct of an algebraic curve M over an algebraically closed field, with $X \to T$ a 2-dimensional definable faithful family of pure-dimensional curves. Then $\mathcal{M}$ interprets a one-dimensional group.*

Proof. The theorem will follow after construction of a group configuration. We work with almost faithful families of curves $Y \to S$ in $M^2 \times N$, where N is some definable set (curves in M^2 is a particular case, when N is a point), where S is strongly minimal (as a set definable in $\mathcal{M}$), subject to requirements:

- all curves Y_s are incident to a point P
- there exists an irreducible component $S' \subset S$ of dimension 1 such that for all $s \in S'$ the relative slope $\tau_n(Y_s/N, P)$ is well-defined at P for some n;
- the set of relative slopes $\tau_n(Y_s/N, P)$ of all curves with parameter s in S', which is a constructible subset in $\mathrm{Aut}(k[\varepsilon\,/(\varepsilon^{n+1})]$, containts a one-dimensional set that almost coincides with a closed one-dimensional subgroup H of $\mathrm{Aut}(k[\varepsilon\,/(\varepsilon^{n+1})]$.

We require three such families, incident to points Q_{12}, Q_{21}, Q_{11}, and relatively incident to (P_1, P_2), (P_2, P_1) and (P_1, P_1), respectively, for some $P_1, P_2 \in M$, and such that the group H defined above is the same for all three families. In this case the relative slope of a composition of curves in first two families can be compared to the relative slope of a curve in the third family using the results of the previous section.

So let M be a curve and let $\mathcal{M}$ be its non-locally modular reduct with a definable family $X \subset M^2 \times T$ of curves that witnesses the lack of local modularity. If the characteristic of the base field is 0, then by Lemma 5.5 there exists a dense open subset $U \subset M^2$ such that for any point $Q \in U$, the first-order slopes of curves in the family $X^Q \to T^Q$ almost coincide with $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^2))$, for parameter t ranging in some irreducible component of T^Q. Pick three points $P_1, P_2 \in M$ such that $(P_1, P_2), (P_2, P_1), (P_1, P_1) \in U$, and consider families of curves $X^{(P_1,P_2)}, X^{(P_2,P_1)}, X^{(P_1,P_1)}$.

For any characteristic of the field of definition of M, by Lemma 5.6 there exists a family of curves $X \subset M^2 \times N \times T$ (with N possibly a point), relatively incident to $P_{12} = (P_1, P_2) \in M$, an irreducible component T' of T^P such that the set of slopes $\tau_n(X_t/N, P_{12})$ for all $t \in T'$ containts a one-dimensional set that almost coincides with a one-dimensional subgroup H of $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^{n+1})$. By Proposition 3.16, the set slopes of the compositions $X_t \circ X_s^{-1}$ almost coincides with H. Therefore for the purposes of the group configuration construction one can take families X, X^{-1} and $X \circ X_t^{-1}$ for some $t \in T'$ generic enough.

Let $X \subset M^2 \times N_{12} \times T_{12}, Y \subset M^2 \times N_{21} \times T_{21}, Z \subset M^2 \times N_{21} \times T_{21}$ be the three families that satisfy the requirements that are stated in the beginning of the proof, and let W_{12}, W_{21}, W_{11} be the irreducible components of T_{12}, T_{21}, T_{11}, respectively, that make the assumptions in the beginning of the proof true.

Let s, t be independent generic points of W_{12}, W_{21}. Note that they are generic and independent in the sense of the reduct $\mathcal{M}$ too.

Let u be a point of W_{11} such that

$$\tau_n(Z_u/N_{11}, Q_{11}) = \tau_n(Y_s/N_{12}, Q_{12})\tau_n(X_t/N_{21}, Q_{21}).$$

Such u exists since relative slopes of X_t and Y_s are generic in a one-dimensional subgroup $H \subset \mathrm{Aut}(k[\varepsilon]/(\varepsilon^{n+1})$, so the right-hand side value is generic in the same subgroup. Since slopes of curves parametrized by parameters in W_{11} almost coincide with H, there exists a generic parameter $u \in W_{11}$ that fits the above equality.

Let us show that u is algebraic over t, s. Let P' be the the image of $Q_{12} \times Q_{21}$ under the composition of maps

$$M^2 \times N \times M^2 \times N' \to M^2 \times N \times_{p_2, M^2, p_1} M^2 \times N' \hookrightarrow M^1 \times N \times N'$$

By Proposition 3.16

$$\tau_n(X_t \circ Y_s/M \times N_{12} \times N_{21}, P') = \tau_n(X_t/N_{12}, Q_{12})\tau_n(Y_s/N, Q_{21})$$

(the relative slope is with respect to the second factor M in M^3). By Proposition 5.18 the definable set

$$\{\ w \in W \ \mid\ \#(X_t \circ Y_s \times_{M^2} Z_w) < l\ \}$$

where $l = \#((X_t \circ Y_s) \times_{M^2} Z_w)$ for w generic independent from t, s, contains the set of parameters $w \in W$ such that $\tau_n(Z_w, P) = \tau_n(X_t, P)\tau_n(Y_s, P)$. By the very definition this set, definable in $\mathcal{M}$, contains finitely many points, and algebraicity of u over s, t follows.

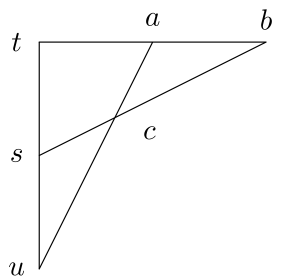
In a similar vein, let a be a point of W_{23} independent from t, s, and let $b \in W_{11}, c \in W_{12}$ be points of W such that

$$\begin{aligned} \tau_n(Z_b/N_{11}, Q_{11}) &= \tau_n(X_t/N_{12}, Q_{12})\tau_n(Y_a/N_{21}, Q_{21}), \text{ and} \\ \tau_n(X_c/N_{12}, Q_{12}) &= \tau_n(Y_s/N_{21}, Q_{21})\tau_n(Z_b/N_{11}, Q_{11}) \end{aligned}$$

Then

$$\begin{aligned} & \tau_n(X_c/N_{12}, Q_{12}) = \tau_n(Y_s/N_{21}, Q_{21})\tau_n(Z_b/N_{11}, Q_{11}) = \\ = \ & \tau(Y_s/N_{21}, Q_{21})\tau_n(X_t/N_{12}, Q_{12})\tau_n(Y_a/N_{21}, Q_{21}) = \\ = \ & \tau_n(Z_u/N_{11}, Q_{11})\tau_n(Y_a/N_{21}, Q_{21}) \end{aligned}$$

By the same argument as above, b is algebraic over a and t, c is algebraic over s and b, and c is also algebraic over a and u, all in the sense of $\mathcal{M}$. This implies that



is a group configuration.

Applying Fact 5.8 we obtain a one-dimensional group interpreted in $\mathcal{M}$. □

5.7 Families of curves in reducts of one-dimensional groups

In the previous subsection we showed that a non-locally modular reduct of the full Zariski structure on an algebraic curve M over an algebraically closed field interprets a strongly minimal group, call it H. The group H is interpretable in an algebraically closed field and therefore is definably isomorphic to a 1-dimensional algebraic group by a model-theoretic version of a theorem of Weil on birational group laws (see [33], [39], [38]). Since $\mathcal{M}$ is non-locally modular, so is H (with the full structure induced from $\mathcal{M}$). Thus, by replacing M with H, we may assume that $\mathcal{M}$ expands a group. In this setting our goal is to construct a second group configuration, which will allow us to reconstruct the field in $\mathcal{M}$.

Let H be a connected one-dimensional algerbaic group, and let $Z \subset H^2$ be an irreducible one-dimensional subset that is not a coset (such sets are components of definable sets that witness non-local modularity in reducts of groups by a theorem of Hrushovski and Pillay [23]). We prove that shifts of Z incident to the identity of H^2 have infinitely many distinct first order slopes at the identity. This will be necessary to construct a two-dimensional group configuration. In characteristic 0, an alternative way to obtain a family of curves with enough distinct first-order slopes is to consider a two-dimensional family of curves in H^2 and apply Lemma 5.5, then shift the family obtained to the identity. Note that the proof of following lemma is characteristic-free.

Lemma 5.20. *Let A be an elliptic curve and let Z be a closed one-dimensional irreducible subset of $G = A^2$. The tangent spaces to G at any point g can be identified with T_0H via the isomorphism $d\lambda_g : T_0G \to T_gG$, where $\lambda_g(x) = g \cdot x$. Suppose that for any $z \in Z$ the tangent space $T_zZ \subset T_0G$ is constant. Then Z is a coset of a closed subgroup of G.*

Proof. Since Z is a projective curve with a trivial tangent bundle, it is an elliptic curve itself. Since any algebraic variety morphism between Abelian varieties with finite fibres and preserving the identity automatically preserves the group structure by Rigidity Theorem, Z is a coset of an Abelian subvariety of G. □

Let $H = \mathbb{G}_a$ or $H = \mathbb{G}_m$. Let Z be a locally closed one-dimensional irreducible subset of $G = H^2$ such that the restriction to Z of the projection on the first factor H is étale (possibly, after removing finitely many points). For any $x \in Z$ denote the translate

$$Y_x := Z \cdot x^{-1} = \{ \; u \cdot x^{-1} \in G \;\mid\; u \in Z \; \}$$

This defines a family $Y \to Z$ of curves incident to (e, e), parametrized by Z.

Lemma 5.21. *In the setting as above, assume H is defined over a field of characteristic 0. Fix a local coordinate system at the identity point $e \in H$ so that the slope of any curve incident to (e, e) is well-defined. Suppose that the slope $\tau_1(Y_x, (e, e))$ is constant for x in an open neighbourhood of (e, e). Then Z coincides with an open subset of a closed subgroup of G.*

Proof. Without loss of generality we may assume that $(e, e) \in Z$.

Let $H = \mathbb{G}_m$, and let Z be cut out by an equation $h(x, y) = 0$. Then $Y_{(x_0,y_0)}$ is cut out by the equation $h(x \cdot x_0, y \cdot y_0)$, and

$$\tau_1(Y_{(x_0,y_0)}, (e, e)) = \left.\frac{\partial_x h(x \cdot x_0, y \cdot y_0)}{\partial_y (x \cdot x_0, y \cdot y_0)}\right|_{x=1,y=1} = \frac{\partial_x h(x_0, y_0) \cdot x_0}{\partial_y h(x_0, y_0) \cdot y_0}$$

Therefore, if f is the expansion of Z into formal power series at the identity then by Proposition 4.4 $\dfrac{\partial_x h(x, f)}{\partial_y h(x, f)}$ is f', the formal derivative of f. If $\tau_1(Y_x, (e, e))$ is constant for x is the neighbourhood of (e, e), then for some $a \in k$ the formal power series f satisfies the differential equation

$$f' \cdot \frac{x + 1}{f + 1} = a$$

Similarly, for the additive group ($H = \mathbb{G}_a$)

$$\tau_1(Y_{(x_0,y_0)}, (e, e)) = \left.\frac{\partial_x h(x + x_0, y + y_0)}{\partial_y h(x + x_0, y + y_0)}\right|_{x=0,y=0} = \frac{\partial h_x(x_0, y_0)}{\partial_y h(x_0, y_0)}$$

and the corresponding differential equation is

$$f' = a$$

The series $f = ax$ satisfies the second equation, and by Lemma 4.1 this is the only solution with zero constant term. It follows that Z is defined by the equation $y = ax$, and so is a subgroup of $\mathbb{G}_a \times \mathbb{G}_a$.

In case $H = \mathbb{G}_m$ it follows from Lemma 4.6 that $f = (x+1)^a - 1$ is the unique formal power series solution of the differential equation

$$y' = a\frac{f+1}{x+1}$$

and is only integral over $k[x]$ if a is rational, in which case f is a formal power series expansion at $(1,1)$ of an irreducible component of a curve defined by an equation $y^n = x^m$. But all such curves are subgroups of $\mathbb{G}_m \times \mathbb{G}_m$. □

Lemma 5.22. *In the same setting, suppose that* $H = \mathbb{G}_a$ *is defined over a field of positive characteristic. Suppose that* Z *is not a coset of a subgroup of* G *and that the projection of* Z *on the first factor* H *is étale on some dense open set. Then there exists a family of curves relatively incident to* $(0,0) \in \mathbb{G}_a \times \mathbb{G}_a$ *such that the set of first order slopes at* $(0,0)$ *almost coincides with* $\mathrm{Aut}(\mathrm{Spec}\, k[\varepsilon]/(\varepsilon^2))$.

Proof. The proof is based on the iterated application of the following observation.

Claim. Let $W \subset \mathbb{G}_a \times \mathbb{G}_a \times N$ be a curve, where N is a Cartesian product of finitely many $\mathbb{G}_a$-s, and assume that $(0,0,\ldots,0) \in W$. For any $t \in p(W)$, where p is the projection on M^2, let W_t denote the shift by t:

$$W_t := \{\ (x-t, y-t, z)\ \mid\ (x,y,z) \in W\ \}$$

Let f_t be the relative formal power series expansion of W_t at $(0,0,\ldots,0)$. Let W_0 be the irreducible component of W that contains 0. Then there are two mutually exclusive possibilities:

- $f_{(0,0)} = ax + g^{p^n}$ for some $g \in xk[[x]]$ and $\tau_1(W_t/N, (0,0,\ldots,0)$ is constant for t generic in W_0 finite.
- the set of $\tau_1(W_t/N, (0,0,\ldots,0)$ as t varies in W_0 (and hence in W) almost coincides with $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^2))$.

Proof of claim. Suppose the second possibility of the Claim is not the case. Since W_0 is irreducible, $\tau_1(W_t/N, (0,0,\ldots,0)$ takes a single value, say, a. By the same argument as in the proof of Lemma 5.21 f satisfies the differential equation

$$f' = a$$

The solutions of the differential equation are of the form $ax + g^{p^n}$, where $g \in (x) \subset k[[x]]$, by direct observation. If $f = ax$ then $p(Z)$ is a coset, contradicting our assumption. ♢

Now let $W \subset M^2 \times N$ be a curve such that $p(W)$ is not a coset in $\mathbb{G}_a \times G_a$, $(0,0) \in p(W)$ and relative slope is well-defined at $(0,0)$. Initially, we take W to be a shift of Z. Let W_0 be the irreducible component of W that contains $(0,0)$.

Let f_t be the formal power series expansion of W_t at $(0,0)$, let l be the largest integer such that $\tau_l(W/N,(0,0))$ depends non-trivially on t.

If $l = 1$, we are done.

If $l > 1$, since W is not a coset, by Claim above, $f_t = ax + (g_t)^{p^n}$, where $g_t \in (x) \subset k[[x]]$. Consider $W'_t := W - W_{t_0}$. By Proposition 3.21 the relative formal power series expansion of W' at $(0,0,\ldots,0)$ is h^{p^n}, where $h_t = g_t - g_{t_0}$.

Then h_t is a relative formal power series expansion of $W''_t = \mathrm{Fr}^n_{M^2\times N/M\times N}(W'_t)$ at $(0,0,\ldots,0)$. Pick some t_1 such that $h_{t_1} \neq 0$. Then by Claim either $h_{t_1} = bx + (h'_{t_1})^{p^n}$, $b \neq 0$, or shifts of W''_{t_1} have infinitely many relative first order slopes at $(0,0,\ldots,0)$.

In the latter case note that by Lemma 3.17, $\tau_1(W''_{t_1} - t \circ (W''_{t_0})^{-1}/N, (0,0,\ldots,0)) = \tau_1(W'_{t_1} - t \circ W'^{-1}_{t_0})$, and so shifts of $W'_{t_1} - t \circ (W'_{t_0})^{-1}$ is the family that satisfies the requirements of the Lemma statement.

In the former case, the relative formal power series expansion relative slope of $W''_t \circ W''^{-1}_{t_1}$ is well-defined, and is of the form $x + (h''_t)^{p_n}$ by Lemma 3.17. Clearly, the smallest number l' such that $\tau_{l'}(W'_t \circ (W'_{t_1})^{-1}/N, (0,0,\ldots,0))$ is non-constant for generict t in W_0, is strictly less than l, so we may run the proof again on the definable curve $W'_t \circ (W'_{t_1})^{-1}$. After finitely many iterations, l must be 1. ☐

Lemma 5.23. *In the same setting, suppose that $H = \mathbb{G}_m$ is defined over a field of positive characteristic. Suppose that Z is not a coset of a subgroup of G and that the projection of Z on the first factor H is étale on some dense open set. Then there exists a family of curves incident to a point $Q \in \Delta_M$ such that the set of first order slopes at Q almost coincides with* $\mathrm{Aut}(\mathrm{Spec}\, k[\varepsilon]/(\varepsilon^2))$.

Proof. The proof follows exactly the same strategy as Lemma 5.22, with the following changes.

The formal power series expansion of a curve Z in $\mathbb{G}_m \times \mathbb{G}_m$ such that its shifts have the same first order slopes satisfies the equation

$$f' = a \cdot \frac{1+f}{1+x}$$

for some element $a \in k$.

By Lemma 4.7 the solutions of the differential equation are of the form $g(1+x)^a - 1$ where $g \in 1 + (x^{p^n}) \subset k[[x]]$. If $f = (1+x)^a$ for a rational then Z is the curve defined by $y^m = x^n$ where $a = \dfrac{m}{n}$.

If Z_1 and Z_2 are two curves with formal power series expansions, $g_1(1+x)^a - 1$ and $g_2(1+x)^a - 1$, with $g_1, g_2 \in 1 + (x^{p^n}$ then by Proposition 3.21, $Z_1 - Z_2$ has power series expansion

$$(g_1(1+x)^a - 1) - (g_1(1+x)^a - 1) - \frac{g_1(1+x)^a - 1}{g_2(1+x)^a - 1} = \frac{g_1}{g_2} - 1$$

which clearly belongs to $(x^{p^n}) \subset k[[x^{p^n}]]$. ☐

5.8 Interpretation of the field

With the preparations made in the previous section we can now show that a non-locally modular reduct of one-dimensional algebraic group interprets a field. This strengthens the main result of [27].

Theorem 5.24. *Let $\mathcal{M} = (G, \cdot, \dots)$ be a reduct of one-dimensional algebraic group $(G, \cdot)$ over an algebraically closed field of any characteristic, which is not locally modular. Then $\mathcal{M}$ interprets a field.*

Proof. By Lemma 5.20, Lemma 5.21, Lemma 5.22 or Lemma 5.23 there exists a definable family $Y \subset G \times G \times N \times S$, where N is a Cartisian product of several copies of G, of curves incident to $P = (e, e, \dots, e)$ and an irreducible set $S_0 \subset S$ such that for s generic in S_0, the relative slope $\tau_1(Y_s/N, (e, e, \dots, e)$ is not constant.

Take $a_1, a_2, b_1, b_1, u \in S_0$ generic and pairwise independent (in the sense of the reduct structure $\mathcal{M}$). Let c_1, c_2 be such that (all slopes are taken at P)

$$\begin{aligned}\tau_1(Y_{c_1}/N, P) &= \tau_1(Y_{a_1}/N, P)\tau_1(Y_{b_1}/N, P)\\ \tau_1(Y_{c_2}/N, P) &= \tau_1(Y_{a_2}/N, P)\tau_1(Y_{b_1}) + \tau(Y_{b_2}/N, P)\end{aligned}$$

Since the image of the function $x \mapsto \tau_1(Y_x, P)$ for x ranging in S_0 is one-dimensional the values of expressions in the right-hand-side are generic in $\mathrm{End}(\mathrm{Spec}\, k[\varepsilon]/(\varepsilon^2))$ for generic values of parameters. Therefore

$$\tau_1(Y_{a_1}/N, P)\tau_1(Y_{b_1}/N, P) \text{ and } \tau_1(Y_{a_2}/N, P)\tau_1(Y_{b_1}/N, P) + \tau_1(Y_{b_2}/N, P)$$

are generic, and c_1, c_2 with such slopes can be picked in S_0.

Let z, v be such that

$$\begin{aligned}\tau_1(Y_z/N, P) &= \tau_1(Y_{a_1}/N, P)\tau_1(Y_u/N, P) + \tau_1(Y_{a_2}/N, P)\\ \tau_1(Y_v/N, P) &= \tau_1(Y_{b_1}/N, P)^{-1}\tau_1(Y_u/N, P) - \tau_1(Y_{b_2}, P)\end{aligned}$$

By a similar reasoning, z, v are generic. It also follows form the way c_1, c_2, z, v were defined that

$$\tau_1(Y_z/N, P) = \tau_1(Y_{c_1}/N, P)\tau_1(Y_v/N, P) + \tau_1(Y_{c_2}/N, P)$$

We will now show that (c_1, c_2) is algebraic over (a_1, a_2) and (b_1, b_2) in the sense of $\mathcal{M}$. Denote P' and P'' points in $G^3 \times N \times N$, repectively in $G^4 \times N \times N \times N$, that project to identity on every factor. By Proposition 3.16, the remark before Proposition 3.21, and Lemma 3.12

$$\begin{aligned}\tau_1(Y_{a_1} \circ Y_{b_1}/G \times N \times N, P') &= \tau_1(Y_{a_1}/N, P)\tau_1(Y_{b_1}/N, P),\\ \tau_1(Y_{a_2} \circ Y_{b_1} + Y_{b_2})/G^2 \times N \times N \times N, P'') &= \tau_1(Y_{a_2}/N, P)\tau_1(Y_{b_1}/N, P) + \tau_1(Y_{b_2}/N, P)\end{aligned}$$

Let $l_1 = \#(Y_{c_1} \times_{G^2} Y_{a_1} \circ Y_{b_1}), l_2 = \#(Y_{c_2} \times_{G^2} Y_{a_2} \circ Y_{b_1} + Y_{b_2})$ for $a_1, a_2,\ b_1, b_2,$ $c_1, c_2 \in S_0$ generic and independent. Since the number of intersections is a first-order property, it does not matter what particular parameters a_i, b_i, c_i we take as long as they are generic and independent (in the sense of the reduct structure $\mathcal{M}$). By Proposition 5.18 the $\mathcal{M}$-definable set

$$\{\ w \in S_0 \ \mid\ \#(Y_w \times_{G^2} (Y_{a_1} \circ Y_{b_1})) < l_1\ \}$$

contains c_1 and by definition of l_1 is finite. By Proposition 5.18 again the $\mathcal{M}$-definable set

$$\{\ w_2 \in S_0 \ \mid\ \#(Y_w \times_{G^2} (Y_{a_2} \circ Y_{b_1} + Y_{b_2})) < l_2\ \}$$

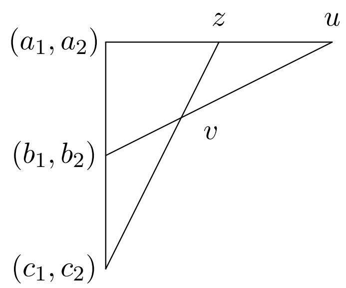
contains c_2 and by definition of l_2 is finite.

Arguing in a similar fashion, by application of Proposition 5.18, we deduce that

- c_1 and c_2 are algebraic over z, v,
- a_1 and a_2 are algebraic over z, u,
- b_1 and b_2 are algebraic over v, u

in the reduct $\mathcal{M}$.

It follows from the discussion above that



constitutes a group configuration. Therefore, by Fact 5.8 there exists a two-dimensional group definable in $(G, \cdot, Z)$ that acts transitively on a one-dimensional set. One checks that the conditions of the Fact 5.9 are verified as well. By Fact 5.10, the group G is isomorphic to the affine group $\mathbb{G}_a(k) \rtimes \mathbb{G}_m(k)$ of an infinite definable field k. □

Theorem 5.25. *Let $\mathcal{M}$ be a non-locally modular reduct of an algebraic curve M over an algebraically closed field M, that has a definable faithful two-dimensional family $X \to T$ of pure-dimensional curves. Then M interprets a field.*

Proof. Conjunction of Theorem 5.19 and Theorem 5.24. □

6 Getting rid of zero-dimensional components

In the previous section we defined a group and then a field in $\mathcal{M}$ given a sufficiently large definable family of plane curves, X, whose generic fibres have no 0-dimensional connected components. The aim of this section is to construct such a family in $\mathcal{M}$.

The distinction between genericity in the sense of the reduct, $\mathcal{M}$, and in the sense of the full Zariski structure on M will be of importance in the some of the subtler arguments of the present section. To distinguish between the two we use *reduct generic* for the former, and *generic* or *field generic* for the latter. Note that field genericity implies reduct genericity but not, a priori, vice versa. Similarly, $\mathrm{acl}_{\mathcal{M}}(\cdot)$ denotes the (model theoretic) algebraic-closure operator in the sense of $\mathcal{M}$ while $\mathrm{acl}(\cdot)$ will denote the (finer) field theoretic algebraic closure.

Drawing upon a tradition in the model-theoretic literature, one-dimensional definable sets in M^2 will be refereed to as "plane curves".

6.1 Preliminaries

For a 1-dimensional definable set, Z , denote Z^1 the union of its 1-dimensional connected components, Z^0 the union of its 0-dimensional components, $\overline{Z^1}$ the closure of Z^1 and $\mathrm{Fr}(Z) = \overline{Z^1} \setminus Z^1$. The same notation will apply for families: if $Y \to S$ is a family of one-dimensional sets, then e.g. $\mathrm{Fr}(Y) \to S$ is the family consisting of frontiers of elements of the family Y.

The results of this section use only basic intersection theory and are, to a large extent, independent from previous sections. Our main results (stated in somewhat greater generality than we actually need) is:

Theorem 6.1. *Let M be an algebraic curve over an algebraically closed field k. Let $\mathcal{M}$ be a strongly minimal non-locally modular reduct of the k-induced structure on M. Let $S \subseteq M^2$ be an $\mathcal{M}$-definable strongly minimal set. Then $\mathrm{Fr}(S) \subseteq \mathrm{acl}_{\mathcal{M}}([S])$, where* Fr *is taken with respect to the Zariski topology and $[S]$ is a canonical parameter for S.*

This theorem follows from the following, somewhat more technical result:

Proposition 6.2. *Let $\mathcal{M}$ be as above. Let $X \to T$ be a faithful $\mathcal{M}$-definable family of curves with $\dim(T) \geq 3$. Assume, moreover, that if $t \in T$ is generic and P is a $\emptyset$-dimensional component of X_t then P is generic over $\emptyset$ and $S \notin \mathrm{acl}(t)$. Then there exists an $\mathcal{M}$-definable family of plane curves $\widetilde{X} \to T$ such that for all $t \in T$:*

1. $X_t \sim \widetilde{X}_t$.
2. $\widetilde{X}_t$ *is pure-dimensional.*

Our strategy is as follows. First, we show the existence of an $\mathcal{M}$-definable family of plane curves $X \to T$ satisfying all the technical assumptions of the previous proposition. Fixing $s \in T$ field generic and $P \in X_s^0$ our assumptions assure that any generic independent $t, u \in T^P$ are, in fact, generic independent over $\emptyset$. Assuming, as we may, that T is $\mathcal{M}$-irreducible it follows that $\#(X_t \cap X_u)$ is independent of the choice of t, u. Moreover, we show that $\#(X_t \cap X_u) = \#(\overline{X_t^1} \cap \overline{X_u^1})$. Assuming towards a contradiction that $P \notin \mathrm{acl}_{\mathcal{M}}(s)$ we get immediately that $\#(X_t \cap X_u) = \#(X_t \cap X_s)$, implying – as P is isolated in X_s – that $\#(\overline{X_t^1} \cap \overline{X_u^1}) > \#(\overline{X_t^1} \cap \overline{X_s^1})$. We then apply basic intersection theory to show that, as t was arbitrary, this leads to a contradiction.

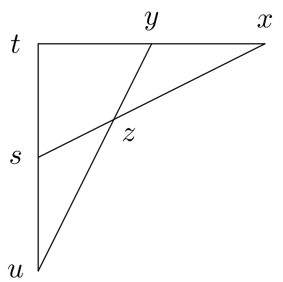
We start by addressing the technical requirements Proposition 6.2. This will require a few steps. The first result we need is well known to the experts, and goes back to Hrushovski's PhD thesis and Buechler's works from the early 1980s (see e.g., [18, p.88]). As we were unable to find an explicit reference, we give a brief overview of the proof:

Lemma 6.3. *If $\mathcal{M}$ is a non-locally modular strongly minimal set there is no bound on the dimension of definable families of plane curves.*

Proof. Clearly, if a field is interpretable in $\mathcal{M}$ then the lemma is true. It will suffice, therefore, to prove that if Z is an n-dimensional ($n \geq 2$) faithful family then either $\dim(Z \circ Z) > n$ or a field is interpretable in $\mathcal{M}$.

Let S' be a parameter set for the normalisation of $Z \circ Z$. We prove that if $\dim S' = n$ then $\mathcal{M}$ interprets an infinite field. Our assumption implies that there exists an $\mathcal{M}$-definable finite-to-finite correspondence $\mu : S' \vdash S$. By definition, there is also an $\mathcal{M}$-definable function $p : S \times S \to S'$ (defined by the requirement that $Z_t \circ Z_s$ is – up to a finite set – the curve defined by $p(t, s)$).

Let t, s be reduct generic independent elements of S and $u \in \mu(p(t, s))$. Let x be a reduct generic point of M, and $y \in Z_t(x)$, $z \in Z_s^{-1}(x)$. Construct the following configuration:



As $y \in Z_t \circ Z_s(z)$ it follows that y is inter-$\mathcal{M}$-algebraic with x over u, implying that the above is, in fact, a group configuration. By Fact 5.8 there exists an $\mathcal{M}$-definable group G of dimension n acting definably on a definable set X of dimension 1. The canonical base of $\mathrm{tp}(y, x/t)$ is inter-algebraic with t by faithfulness of the family Z, and similarly for the canonical bases of $\mathrm{tp}(z, x/s)$ and $\mathrm{tp}(z, x, /u)$. Therefore by Fact 5.9 the action of G on X is faithful. By Fact 5.10 there exists a field definable in $\mathcal{M}$. ☐

In the discussion that follows canonical parameters (see Sub-section 2.2) will play an important role. To simplify the discussion, we will denote, given a definable set

S, its canonical parameter $[S]$. As explained in the introduction $[S]$ is not uniquely determined, but $\mathrm{acl}([S])$ is, which will suffice for our purposes. Formally, we have to distinguish between $\mathcal{M}$-canonical parameters and field-canonical parameters. In practice, and in order to overload the notation, we will always use $\mathcal{M}$-canonical parameters (as long as the definable sets in questions are $\mathcal{M}$-definable, of course). Note, and this will be used implicitly throughout, that if $X \to T$ is a faithful $\emptyset$-definable family (of plane curves) then t is a canonical parameter for X_t.

Now we turn to the genericity of isolated points (in the sense of the assumptions of Proposition 6.2):

Lemma 6.4. *Let $S \subseteq M^2$ be an $\mathcal{M}$-definable curve with $[S] \notin \mathrm{acl}(\emptyset)$. Let $Z \to T$ be an $\mathcal{M}$-irreducible n-dimensional $\mathcal{M}$-definable faithful family of plane curves for some $n \geq 2$. Then there exists an $\mathcal{M}$-definable family of plane curves $Z' \to T$ with $Z'_t \sim Z_t$ for all $t \in T$ and such that for any $t \in T$ generic over $[S]$ any point in $(S \circ Z'_t)^0$ is field generic.*

Proof. We may assume that S is $\mathcal{M}$-irreducible (otherwise, repeat the argument for each $\mathcal{M}$-component of S separately) and projecting dominantly on both coordinates. We may also assume that there is no point $P \in M^2$ incident to Z_t for all generic t. We may assume that if $(p, q) \in S^0$ then $p, q \notin \mathrm{acl}(\emptyset)$, as if that is not the case we can replace Z with $Z \setminus (\{p\} \times M \times T \cup M \times \{q\} \times T)$.

Now note that if $(p, q) \in S^0$ then $p, q \in \mathrm{acl}([S])$. Thus, if $t \in T$ is generic over $[S]$ then any point of the form (p, r), where $(q, r) \in Z_t$, is generic over $\emptyset$. Indeed, since q is generic over $\emptyset$ and t is generic over q any point $(q, r) \in Z_t$ is generic in Z_t, therefore generic over $\emptyset$.

If for some $(p, q) \in Z_t^0$, say, $p \in \mathrm{acl}(\emptyset)$ then, by genericity of t and the $\mathcal{M}$-irreducibility of $Z \to T$, for all $t' \in T$ generic we have that $(p, q') \in Z_{t'}^0$ for some q'. Similarly if $q \in \mathrm{acl}(0)$. Let $\{p_1, \ldots, p_k\} \subseteq \mathrm{acl}(\emptyset)$ such that $(p_i, q) \in Z_t^0$ for some $q \in M$. Similarly, define $\{q_1, \ldots, q_r\}$. Setting $Z' \to T$ by defining

$$Z' = Z_t \setminus \bigcup_{i=1}^{k} \{p_i\} \times M \times T \cup \bigcup_{i=1}^{r} M \times \{q_i\} \times T$$

we may assume that for generic $t \in T$ and any $(p, q) \in Z_t^0$ both p and q are generic (not necessarily independent) over $\emptyset$.

Under these assumptions, if $(p, q) \in Z_t^0$ for $t \in T$ generic over $[S]$ then any point (r, q) for $r \in M$ such that $(r, p) \in S$ is generic over $\emptyset$. Indeed, as $[S] \notin \mathrm{acl}(\emptyset)$ and $[S]$ is independent from t over $\emptyset$ (by symmetry) we get that $r \notin \mathrm{acl}(p, q)$ and by exchange $q \notin \mathrm{acl}(r, p)$. So $\dim(p, q, r) = 3$.

As $(S \circ Z_t)^0 \subseteq S^0 \circ Z_t \cup S \circ Z_t^0$, the conclusion of the lemma follows. $\square$

We may now conclude:

Corollary 6.5. *There exists an $\mathcal{M}$-definable family of plane curves $X \to T$ satisfying the assumptions of Proposition 6.2.*

Proof. Fix $Z \to T$ a faithful $\mathcal{M}$-definable family of plane curves of dimension at least 3, as provided by non local modularity. Fix a generic Z_{t_0} in that family. By the previous lemma, we can find $Z' \to T$ of the same dimension such that $X := Z_{t_0} \circ Z'$ has the desired properties. $\square$

Notation We fix a family $X \to T$ satisfying the assumptions of Proposition 6.2. As the proof proceeds we may replace X with other families (such as $X \circ X^{-1}$) satisfying stronger assumptions. In order not to overload the notation, we will be explicit about any such replacement, and will still denote the resulting family $X \to T$.

6.2 Indistinguishable points

Our aim is to use intersection theory in order to identify the isolated components of X_t for $t \in T$ generic. Our setting, however, only allows us direct access to global intersection properties (such as the number of geometric intersection points of two curves), and for such global phenomena the existence of isolated points, frontier points and other local obstructions of similar flavour, may interfere with the geometric argument. We now turn to studying the nature of these possible obstructions.

Definition 6.6. *Let $X \to T$ be a definable family of plane curves, $P \in M^2$ any point. A point $Q \neq P$ is* X-indistinguishable *from P if $T^P \sim T^Q$. The point Q is* frontier-P-indistinguishable *(with respect to a field generic type p extending X) if $Q \in \mathrm{Fr}(X_t)$ for all (field) generic $t \in T^P$ such that $t \models p$.*

Note that for an $\mathcal{M}$-definable family Y of plane curves the property of being Y-indistinguishable is $\mathcal{M}$-definable, while the property of being frontier indistinguishable is, a priori, only definable in the full Zariski structure on M.

Remark. In the definition of frontier indistinguishable points (and in all further references to frontier point in the present section) we have intentionally omitted any clear reference to the topological space where this frontier is computed. In the algebro-geometric context of the present text this has no importance (in the proof of Proposition 6.2 we will consider an open embedding of M into a regular proper curve, M_2, and frontier will always refer to the ambient Zariski topology). In other contexts where one may consider generalising the results of this section the main requirement to keep in mind is that the frontier of a plane curve be finite.

There are known examples, due to Hrushovski (see, e.g., [28]) of strongly minimal reducts of algebraically closed fields where to any generic point, P, there exists $Q \neq P$ interalgebraic with P over $\emptyset$ and indistinguishable (with respect to any $\emptyset$-definable family of plane curves) from P. In the present sub-section we show how indistinguishable points can be avoided:

Proposition 6.7. *Let $X \to T$ be an $\mathcal{M}$-definable faithful $\mathcal{M}$-stationary family of plane curves. Then, after possibly removing finitely many points from M:*

1. *If there are no generic X-indistinguishable points, then there are no generic $X \circ X^{-1}$-indistinguishable points.*
2. *There exists an $\mathcal{M}$-definable equivalence relation $\sim$ on M such that there are no $(X/\sim) \circ (X/\sim)^{-1}$-indistinguishable points in $M/\sim \times M/\sim$, where*

$$X/\sim \to T := \{([x],[y],t) : t \in T, (x,y) \in X_t\}.$$

Proof. Let us denote $XX := X \circ X^{-1}$. The proof proceeds by a series of claims. The key observation is:

Claim I: Suppose that any generic $P \in M^2$ has some $Q \in M^2$ that is XX-ind. from it. Then for all generic r there is s such that (p_1, r) is X-indistinguishable from (q_1, s) and (p_2, r) is X-indistinguishable from (q_2, r). In particular $q_1 \in \mathrm{acl}_{\mathcal{M}}(p_1)$.

Proof. Let $P = (p_1, p_2)$ and $Q = (q_1, q_2)$ be generic and XX-indistinguishable. Fix any $r \in M$, and any generic (over all the data) $t \in T^{(p_1,r)}$. Let $S := X_t(q_1)$. Then S is finite. The assumption that P is XX-indistinguishable from Q implies that any generic curve through (p_2, r) also passes through (q_2, s) for some $s \in S$. Since S is finite and $T^{(p_2,r)}$ is stationary there is $s \in S$ such that any generic curve through (p_2, r) passes through (q_2, s). I.e. (p_2, r) is X-indistinguishable from (q_2, s). Since r was generic, this implies that for all generic r there exists s such that (p_2, r) is X-indistinguishable from (q_2, s).

So fix a generic u such that $(p_2, r) \in X_u$. Then $(q_2, s) \in X_u$. By the exact same argument as above, we get that for any generic enough $w \in T^(p_1, r)$ we get $(q_1, s) \in X_w$. I.e., (p_1, r) is X-indistinguishable from (q_1, s). This implies that q_1 is algebraic over p_1. For otherwise, any generic point (p_1, r) would have infinitely many points X-indistinguishable from it, contradicting the faithfulness of the family. $\square_{\text{Claim I}}$

From this we can immediately conclude the first part of the proposition:

Claim II: If $X \to T$ has no generic indistinguishable points then neither does XX.

Proof. Suppose that P, Q are generic XX-indistinguishable points. Then for all generic $r \in M$ there is some s such that (p_1, r) is X-indistinguishable from (p_1, s). Since there are no generic X-indistinguishable points, we get that – fixing a generic r – $(p_1, r) = (q_1, s)$. In particular $p_1 = q_1$. So we are reduced to showing that there are no XX-indistinguishable points of the form (p, q) (p, r). For fix t generic over all the data and let $\{p_1, \ldots, p_k\} := X_t(p)$. If $(p.q)$ and (p, r) are XX-indistinguishable then for generic $s \in T^{(q,p_1)}$ there is some p_i such that $s \in T^{(r,p_i)}$. Since T^Q is irreducible for generic Q this i cannot depend on s. So (q, p_1) is X-indistinguishable from (r, p_i). So $q = r$. This shows that there are no generic XX-indistinguishable points. $\square_{\text{Claim II}}$

Now we can construct the desired equivalence relation:

Claim III: Define $q \sim p$ if for every generic r there exists s such that (p, r) is X-indistinguishable from (q, s). Then $\sim$ is an equivalence relation once we remove finitely many points.

Proof. There are finitely many points $P \in M^2$ such that T^P is generic in T. Removing their coordinates, we may assume those do not exist. So $\sim$ is generically symmetric, and therefore symmetric on co-finitely many points. So we only have to check transitivity. Assume that $p \sim q \sim r$. Then for every generic r there exists s as in the claim. Our assumptions imply that r is generic over q, so there is u such that $(q, s) \sim (r, u)$ and since $(p, r) \sim (q, s)$ and by genericity $T^{(p,r)}$, $T^{(q,s)}$ and $T^{(r,u)}$ are irreducible, the claim follows. $\square_{\text{Claim III}}$

By construction of $\sim$ and by Claim I, if $([p], [q])$ and $([r], [s])$ are $(X/{\sim})(X/{\sim})$-indistinguishable (in $M^2/{\sim}$) then $[p] = [r]$ and $[q] = [s]$. This finishes the proof of the proposition. $\square$

The last proposition show that, at the cost of passing, to $M/{\sim}$ (and replacing $X/{\sim}$ with $(X/{\sim}) \circ (X/{\sim})^{-1}$) we may assume that there are no X-indistinguishable points. Indeed, by (the proof of) Lemma 6.3 there are $\mathcal{M}$-definable families of plane curves of arbitrary dimension, satisfying the conclusion of Theorem 6.2, and admitting no indistinguishable points.

Remark. The structure $(\mathcal{M}/{\sim}, X/{\sim})$ is interpretable in $\mathcal{M}$, and therefore already in our original algebraically closed field. There is, therefore, no harm assuming that $(\mathcal{M}/{\sim}, X/{\sim})$ is, in fact, $\mathcal{M}$.

6.3 Counting geometric intersection points

Intuitively, if $s \in T$ is generic, $P \in X_s^0$ and $t \in T^P$ then we expect $\#(X_t^1 \cap X_s^1)$ non-generic – because P is a superfluous intersection point. If that were the case P would be member of the $\mathcal{M}$-s-definable algebraic set of all those points on X_s such that $\#(X_t^1 \cap X_s^1)$ is non-generic for all generic t passing through them. In the present sub-section we show that this intuition is as true as one could expect in the present setting. Namely, that the above intuition holds on the level of $\bar{X}^1$, namely on the level of closures of the 1-dimensional components of members of X.

First we study the intersection of any two field generic curves. Our first observation is obvious, but we isolate it for future reference:

Lemma 6.8. *Let $A \subseteq M$ be small and P any point, generic enough over $\emptyset$. Then for any $t \in T^P$ field generic over A and any curve, C, field-definable over A we have that* $\operatorname{acl}(A) \cap C \cap X_t \subseteq \{P\}$.

Proof. The assumption that P is generic enough in M^2 assures that T^P is $\mathcal{M}$-irreducible, and since $\dim(T) \geq 2$ it is also infinite. Thus, if some field generic $t \in T$ satisfies $Q \in X_t \cap C \cap \mathrm{acl}(A)$ then the set $\{t' \in T^P : Q \in X_{t'}\}$ is $\mathcal{M}$-definable of maximal rank, implying that Q is X-indistinguishable from P. So $Q = P$. $\square$

Lemma 6.9. *Let $X \to T$ be as above. Let $t, u \in T$ be field generic independent over $\emptyset$ (satisfying the same field-type over $\emptyset$). Then*

$$X_t \cap X_u = \overline{X_t^1} \cap \overline{X_u^1} \setminus C$$

Where C is the set of frontier P-indistinguishable points for some (equivalently, any) $P \in X_t \cap X_u$.

Proof. Let $P \in X_t \cap X_u$ be any point. By the previous lemma P is field generic in X_t and by symmetry P is also generic in X_u. Since P was arbitrary $X_t \cap X_s \subseteq \overline{X_t^1} \cap \overline{X_u^1}$, with the desired conclusion. More precisely,

$$2\dim(T) = \dim(P, t, u) = \dim(u) + \dim(P/u) + \dim(t/P, u) = \dim(T) + 1 + \dim(t/P, u)$$

implying that u, t are independent generics in T^P, so that – by definition of frontier indistinguishable points – $C \cap X_t \cap X_s = \emptyset$. $\square$

In the application our main concern will be in the situation where $s \in T$ is generic but $X_u \in T^P$ for some $P \in X_s^0$. We prove:

Lemma 6.10. *Let $s \in T$ be generic, $P \in X_s^0$ and $(t, u) \in T^P \times T^P$ generic independent from s over P. Then either $P \in \mathrm{acl}_{\mathcal{M}}(s)$ or $\#(\overline{X_t^1} \cap \overline{X_s^1}) < \#(\overline{X_t^1} \cap \overline{X_u^1})$.*

Proof. We assume that $P \notin \mathrm{acl}_{\mathcal{M}}(s)$ (as we will see later on, this assumption will ultimately lead to a contradiction). So $P \in X_s$ is $\mathcal{M}$-generic.

Claim I: $\mathrm{tp}_{\mathcal{M}}(s, t) = \mathrm{tp}_{\mathcal{M}}(t, u)$.

Proof. To see this, note that, by assumption T is $\mathcal{M}$-irreducible (i.e., has a unique generic type). By the choice of X the point P is (field) generic (over $\emptyset$) and therefore T^P has a unique $\mathcal{M}$-generic type p. Thus $T^P \times T^P$ has a unique $\mathcal{M}$-generic type, denoted $p \otimes p$ and by construction $(t, u) \models p \otimes p$. It will now suffice to show that $(s, t) \models p \otimes p$. Indeed, as t is generic in T^P over s this reduces to proving that $s \models p$. Our assumption that $P \notin \mathrm{acl}_{\mathcal{M}}(s)$ implies that $\dim_{\mathcal{M}}(P, s) = \dim_{\mathcal{M}}(s) + 1$. So $\dim_{\mathcal{M}}(s/P) = \dim_{\mathcal{M}}(T) - 1 = \dim_{\mathcal{M}}(T^P)$. As p is the unique type in T^P of maximal dimension, the claim is proved.

$\square_{\text{Claim I}}$

It follows that $\#(X_t \cap X_s) = \#(X_t \cap X_u)$. By Lemma 6.8 $X_s^0 \cap X_t = \{P\}$. For exactly the same reason $\mathrm{Fr}(X_s) \cap X_t = \emptyset$.

Claim II: Let $Q \in X_s \cap \mathrm{acl}(t)$ then $Q \in \mathrm{acl}(s)$.

Proof. First, observe that as $\dim(T) > 2$ and P is field generic over $\emptyset$ we get

$$\dim\{s' \in S : P \in X^0_{s'}\} > 0,$$

i.e., $s \notin \operatorname{acl}(P)$. Let $\phi(x,t)$ isolate $\operatorname{tp}(Q/t)$. By compactness we may assume that for any $t' \equiv_P t$ (in the full structure) the formula $\phi(x,t')$ is algebraic. Consider

$$F := \{Q' : \dim\{t \in T^P : Q' \models \phi(x,t)\} \geq \dim(T) - 2\}.$$

Then $\dim(F) \leq 1$ and $Q \in F$. Therefore, as F is definable over P, we get that $F \cap X_s$ is finite, so $Q \in \operatorname{acl}(s)$. $\square_{\text{Claim II}}$

It follows from the above claim that $X_s \cap X^0_t = \emptyset$. Indeed, the claim implies that any $Q \in X_s \cap X^0_t$ is algebraic over s, now apply Lemma 6.8.

Using the same claim again we see that if $Q \in X_s \cap \operatorname{Fr}(X_t)$ then Q is frontier P-indistinguishable. So we get that $B := X_s \cap \operatorname{Fr}(X_t) \subseteq C$, where C is the set of all frontier P-indistinguishable points (in the notation of the previous lemma).

Summing up all of the above, together with the previous lemma, we get:

$$\#(X_t \cap X_s) = \#(X_t \cap X_u).$$

But

$$\#(X_t \cap X_s) = \#(\overline{X^1_t} \cap \overline{X^1_s}) - |B| + 1$$

where P accounts for the extra point on the left hand side. On the other hand

$$\#(X_t \cap X_u) = \#(\overline{X^1_t} \cap \overline{X^1_u}) - |C|$$

and as $B \subseteq C$ the desired conclusion follows. $\square$

The previous lemma gives us the advantage of working with families of closed curves, allowing us to use intersection theory. The fact that the family we will be working with is (a priori) only definable in the full structure, and not necessarily in $\mathcal{M}$ will not be of importance, as we will show that the conclusion of the previous lemma leads to a contradiction, unless for generic $s \in T$ and $P \in X^0_s$ we have that $P \in \operatorname{acl}_{\mathcal{M}}(s)$.

6.4 Multiplicities

We remind that if $X, Y \subset M^2$ are curves and $Q \in X \cap Y$ is a point on both, then the intersection multiplicity of X and Y at Q is defined as

$$\operatorname{mult}(X, Y; Q) = \dim_k \mathcal{O}_{M^2,Q}/I_X I_Y$$

where I_X and I_Y are the ideals cutting out the germs of X and Y around Q. In the application the curves X and Y will be generic members of definable families of curves, say $X = X_a$ and $Y = Y_b$. Viewing them as curves over fields the fields

$k(a)$ and $k(b)$ (the respective function fields of locus(a) and locus(b)) the intersection multiplicity of X_a, Y_b at a point $Q \in \mathrm{acl}(a,b)$ can be computed by

$$\mathrm{mult}(X_a, Y_b; P) = \dim_{k(a,b)^{alg}} \mathcal{O}_{M^2,P}/I_{X_a} I_{Y_b}$$

where I_{X_a}, I_{Y_b} are the ideals cutting out the germs at Q of $X_a \otimes k(a,b)^{alg}$ and of $Y_b \otimes k(a,b)^{alg}$ respectively, and $k(a,b)$ is the function field of locus(a,b).

The key local property of the intersection multiplicity used below is given by the following lemma:

Lemma 6.11. *Let R be a regular local ring over a field k, and I_1, I_2, I_3 ideals such that R/I_1, R/I_2, R/I_3 are regular. Assume that $R/(I_1I_2)$,$R/(I_2I_3)$ and $R/(I_1I_3)$ are finite-dimensional k-vector spaces. Then*

$$\dim_k R/(I_1I_2) \geq \min\{\dim_k R/(I_1I_3), \dim_k R/(I_2I_3)\}$$

Proof. By symmetry of the statement it suffices to show that if

$$\begin{aligned} \dim_k R/(I_1I_2) &\geq \dim_k R/(I_1I_3), \\ \dim_k R/(I_1I_2) &\geq \dim_k R/(I_2I_3), \end{aligned}$$

then $\dim_k R/(I_1I_3) = \dim_k R/(I_2I_3)$.

By regularity of R/I_2, all 0-dimensional quotient algebras are of the form $k[a]/(a^n)$ for some generator; for two such algebras $k[a]/(a^n), k[a]/(a^m), n > m$ there exists a natural reduction morphism $k[a]/(a^n) \to k[a]/(a^m)$. It follows from the first inequality above that there exists a morphism of this form

$$f : R/(I_1I_2) \to R/(I_3I_2) \cong R/I_3 \otimes R/I_2.$$

We get the following diagram:

$$\begin{array}{ccc} R/I_2 & \longrightarrow & R/I_3 \otimes R/I_2 \\ \Big\downarrow p & \overset{f}{\nearrow} & h \Big\uparrow \Big\downarrow \mathrm{id} \otimes p \\ R/(I_1I_2) & \xrightarrow[i_{12}]{} & R/I_3 \otimes R/(I_1I_2) \end{array}$$

where h is defined by $a \otimes b \mapsto a \cdot f(b)$.

One observes that both morphisms h and $\mathrm{id} \otimes p$ are surjective, and since $R/I_3 \otimes R/I_2$ and $R/I_3 \otimes R/(I_1I_2)$ are finite-dimensional vector spaces, they are bijective and so isomorphisms. By a similar argument, $R/I_3 \otimes R/(I_1I_2)$ is isomorphic to $R/I_3 \otimes R/I_1$, and therefore $R/I_3 \otimes R/I_1$ is isomorphic to $R/I_3 \otimes R/I_2$. □

Geometrically, the above lemma expresses the fact that if X, Y and Z are curves in M^2 all meeting at a common point, Q, regular on all three, and if $\mathrm{mult}(X, Y; Q) = \mathrm{mult}(X, Z; Q)$ then $\mathrm{mult}(Y, Z; Q) \geq \mathrm{mult}(X, Y; Q)$. We point out that this lemma is not true if regularity of all curves in question at Q is assumed (e.g., if Q is a branch point of X, but is regular on Y and Z).

Lemma 6.12. *Let $s \in T$ be generic, $P \in X_s^0$ and $t \in T^P$ generic over s. Let $Q \in X_t \cap X_s$. Assume that all geometric intersection points (that is, defined over* $\mathrm{acl}(t,s)$*) are regular. Then there exists a number m such that* $\mathrm{mult}(X_{t'}, X_s, Q') = m$ *whenever t', Q' are such that* $\mathrm{tp}(t', s, Q) = \mathrm{tp}(t, s, Q')$.

Proof. In algebro-geometric terms we are looking at a point $W \in X_t \otimes k(t,s) \cap X_s \otimes k(t,s)$ which is regular on both X_t and X_s, with a residue field which is an algebraic extension of $k(t,s)$. The fiber product $Z = X_t \times_{M^2} X_s = \operatorname{Spec} \mathcal{O}_{M^2,W}/I_{X_t}I_{X_s}$ is then a spectrum of an algebra of the form $k(t,s)[\epsilon]/(\epsilon^{m+1})$.

For any geometric point $\eta : \operatorname{Spec} k(t,s)^{alg} \to Z$, since localization commutes with base change, $\mathcal{O}_{M^2,\eta}/I_{X_t}I_{X_s} \cong \mathcal{O}_{M^2,W}/I_{X_t}I_{X_s} \otimes k(t,s)^{alg}$. Therefore, the multiplicity at η is $\dim_{k(t,s)^{alg}} \mathcal{O}_{M^2,W}/I_{X_t}I_{X_s} \otimes k(t,s)^{alg} = \dim \operatorname{Spec} k(t,s)^{alg}[\epsilon]/(\epsilon^{m+1}) = m$. □

We can now show:

Lemma 6.13. *Let $s \in T$ be generic, $P \in X_s^0$. Let $Q \in X_s$ be generic over P and $t, u \in T^P \cap T^Q$ independent generics. Assume that* $\mathrm{tp}(t/P,Q) = \mathrm{tp}(u/P,Q)$ *and* $\mathrm{tp}(s) = \mathrm{tp}(t)$ *where all types are taken with respect to the full structure. Then* $\mathrm{mult}(X_t, X_s, Q) \le \mathrm{mult}(X_u, X_t, Q)$.

Proof. By our choice of $X \to T$ we know that $\dim(P) = 2$ and as $\dim(T) > 2$ we get $\dim(T^P) \ge 2$. Moreover, as in the proof of Claim II of Lemma 6.10, $s \notin \mathrm{acl}(P)$. This implies that $Q \mathop{\smile\!\!\!\!\!\mid}_{\emptyset} P$, whence $\dim(T^P \cap T^Q) = \dim(T) - 2 \ge 1$. Thus, if $t \in T^P \cap T^Q$ is generic we have

$$\dim(T) + 2 = \dim(t, P, Q) = \dim(Q/t, P) + \dim(t/P) + \dim(P).$$

Since $\dim(Q/t, P) = 1$ this implies that $\dim(t/P) = \dim(T) - 1$, so t is generic in T^P. Similarly, if $t, u \in T^P \cap T^Q$ we have:

$$2\dim(T) = \dim(P) + \dim(t, u/P) + \dim(Q/t, u, P)$$

and as $Q \in \mathrm{acl}(t, u, P)$ this implies that $\dim(t, u/P) = 2\dim(T) - 2$, i.e., (t, u) are independent generics in T^P. Since P is generic over $\emptyset$ this implies that t, u are independent generic over $\emptyset$ as well.

Thus Q is regular on both X_u and X_t. Assume towards a contradiction that $\mathrm{mult}(X_s, X_t, Q) > \mathrm{mult}(X_t, X_u, Q)$. By Lemma 6.12, since $\mathrm{tp}(t/P,Q) = \mathrm{tp}(u/P,Q)$, also $\mathrm{mult}(X_s, X_u, Q) = \mathrm{mult}(X_s, X_t, Q)$, and so $\mathrm{mult}(X_u, X_s, Q) > \mathrm{mult}(X_t, X_u, Q)$. But by Lemma 6.11, $\mathrm{mult}(X_t, X_u, Q) \ge \mathrm{mult}(X_u, X_s, Q)$, a contradiction. □

The global implication of the previous (local) lemma is:

Lemma 6.14. *Let $s \in T$ be generic $P \in X_s^0$. Let $t, u \in T^P$ be independent generic over all the data (satisfying the same type in the full structure). Then*

$$\sum_{Q \in \overline{X_s^1} \cap \overline{X_t^1}} \mathrm{mult}(\overline{X_s^1}, \overline{X_t^1}, Q) < \sum_{Q \in \overline{X_u^1} \cap \overline{X_t^1}} \mathrm{mult}(\overline{X_u^1}, \overline{X_t^1}, Q)$$

Proof. For simplicity we will assume that all curves in question have a unique 1-dimensional component (with respect to the full structure). Otherwise we repeat the argument component by component.

Denote $\mathcal{Q} := \overline{X_s^1} \cap \overline{X_t^1}$. By Lemma 6.8 all points in $\mathcal{Q}$ are field generic in both X_s and X_t. As we assumed that X_s and X_t are irreducible, and – restricting to an irreducible component of T^P – we get by Lemma 6.12 that there exists a number m such that whenever $t \in T^P$ is field generic (of a fixed type) $\operatorname{mult}(\overline{X_s^1}, \overline{X_t^1}, Q) = m$ for any $Q \in \overline{X_s^1} \cap \overline{X_t^1}$. Similarly, there exists n such that whenever $t, u \in T^P$ are independent generics, satisfying the same field theoretic type $\operatorname{mult}(\overline{X_u^1}, \overline{X_t^1}, Q) = n$ for any $Q \in \overline{X_s^1} \cap \overline{X_t^1}$.

By Lemma 6.13 we get $m \leq n$. By Lemma 6.10 we have that $\#\mathcal{Q} < \#(\overline{X_u^1} \cap \overline{X_t^1})$, with the desired conclusion.

□

We point out that the last lemma is not true if our family has indistinguishable points: If, in the notation of the previous lemma, P is X-indistinguishable from a point Q which is a branch point of X_s. This is the only place where assuring that X has no indistinguishable generic points was crucial for the proof.

Proof of Proposition 6.2. Fix a family $X \to T$ as provided by Corollary 6.5. Quotienting by an equivalence relation with finite classes, we may assume, by Proposition 6.7, that there are no X-indistinguishable generic points. If for $s \in T$ generic $X_s^0 \subseteq \operatorname{acl}_{\mathcal{M}}(s)$ then, by compactness (and induction on $\dim(T)$) we have nothing to prove. So assume that this is not the case. We will derive a contradiction.

We have already identified M with its regular locus (by simply removing all singularities). So we may assume M is regular. Now choose a proper curve M_1 containing M as an open subset. Consider the normalization M_2 of M_1. Note that M_1 projects onto M_1 and is regular since normal varieties have singularities in codimension 2. The projection is an isomorphism after restriction to the regular locus of M_1: local rings of regular points of M_2 are integral closures of local rings of regular points of M_1, and regular local rings of dimension 1 are integrally closed. It follows that there exists an open embedding of M_1 into M_2, and hence of M into M_2.

Let $s \in T$ be field generic and $P \in X_s^0$ such that $P \notin \operatorname{acl}_{\mathcal{M}}(s)$, $Q \in S$ a field generic point. Let $t, u \in T^P \cap T^Q$ be field independent generic over all the data. By our assumption it follows from Lemma 6.10 that $\#(\overline{X_s^1} \cap \overline{X_t^1}) < \#(\overline{X_u^1} \cap \overline{X_t^1})$, where the closure is taken in (some Cartesian power of) M_2.

As follows from intersection theory on proper regular varieties, the intersection number is stable in algebraic families ([11], Corollary 10.2.2). Therefore the sum of local intersection multiplicities over all intersection points should be the same for pairs X_t, X_s and X_t, X_u. This is in direct contradiction with the previous lemma. □

Though Proposition 6.2 suffices for our needs in the current paper, we give the proof of Theorem 6.1, whose statement is cleaner, and may be of interest on its own right.

Proof of Theorem 6.1. Let S be any $\mathcal{M}$-definable curve. Absorbing the parameters required to define S, we may assume that S is $\emptyset$-definable. Let $X \to T$ be any $\mathcal{M}$-definable family of plane curves satisfying the assumptions of Proposition 6.2. For simplicity, we may also assume that X satisfies the conclusion of the proposition. Consider the family $S \circ X \to T$. Our assumption implies that for a generic $t \in T$ the only isolated points of $S \circ X_t$ are of the form $S^0 \circ \overline{X_t^1}$ (as $\overline{X_t^1} = \overline{X_t}$). Applying Proposition 6.2 to $S \circ X_t$ (for some generic $t \in T$) we get a curve $Z_t \sim S \circ X_t$ such that $Z_t^0 = \emptyset$ (and Z_t is definable over t). So $S^0 \subseteq \{P \in S : P \circ X_t \setminus Z_t \neq \emptyset\}$. Note that the right hand side is t-definable (and finite). So

$$S_0 := \bigcap_{t \in T \text{ generic}} \{P \circ X_t \setminus Z_t \neq \emptyset\}$$

and by definabilty of Morley rank the right hand side is $\emptyset$-$\mathcal{M}$-definable. $\square$

Note that the proof of Theorem 6.1 follows almost formally from Proposition 6.2, and has little to do with the topological definition of the set of 0-dimensional components. The only property of 0-dimensional components used in the proof is that if D has no 0-dimensional components then $(S \circ D)^0 \subseteq S^0 \circ D$.

Also the proof of Proposition 6.2 does not seem endemic to algebraic geometry. The only algebro-geometric ingredients used in the proof are

1. Finiteness of the frontier of (plane) curves.
2. Lower semi-continuity of the intersection number in flat families.
3. The multiplicity inequality of Lemma 6.11

The last two of these three properties seem to have satisfactory analogues in a variety of analytic and topological settings. E.g., the lower semi-continuity of the intersection number in flat families may be replaced in certain contexts with the invariance of the topological degree under homotopy (and see, e.g., [16, Lemma 4.19, Lemma 4.20]). The multiplicity inequality is a refinement of ideology that tangency should be an equivalence relation. In many respect this is the cornerstone upon which Zilber's Trichotomy – suggesting the construction of a field from purely geometric, even combinatorial, data – relies. It is therefore reasonable to expect to have natural analogues in any context in which one can reasonably hope to prove this trichotomy.

Theorem 6.15 (Main theorem)**.** *Let M be an algebraic variety of dimension 1 defined over an algebraically closed field k. Let $X \subset T \times M^2$ be a family of constructible subsets of M^2 generically of dimension and Morley degree 1. Then the structure $\mathcal{M} = (M, X)$ interprets an infinite field.*

Proof. By Lemma 6.10 and Proposition 6.2 there exists a two-dimensional family of curves definable in (M, X) with generic fibre of pure dimension 1. By Theorem 5.19 a one-dimensional group G is definable in $\mathcal{M}$. The structure induced on G by $\mathcal{M}$ is non-locally modular, so the theorem is reduced to the case when there is a group structure on M.

A non-locally modular strongly minimal group G has a definable set $Z \subset G^2$ which is not a coset. Use it to produce the definition of a field by Theorem 5.25. □

References

[1] A. Baker. Differential equations in divided power algebras, recurrence relations and formal groups. *Preprint*, 1995.

[2] P. Berthelot. *Cohomologie cristalline des schémas de characteristique $p > 0$.* Springer-Verlag, 1974.

[3] F. Bogomolov, M. Korotiaev, and Y. Tschinkel. A Torelli theorem for curves over finite fields. *Pure and Applied Mathematics Quarterly*, 6(1):245–294, 2010.

[4] N. Bourbaki. *Algèbre.* Number pts. 4-5 in Actualités scientifiques et industrielles. Hermann, 1959.

[5] E. Bouscaren. Group configuration (after E. Hrushovski). In A. Pillay and A. Nesin, editors, *Model theory of groups.* University of Notre Dame press, 1989.

[6] E. Bouscaren. *Model theory and algebraic geometry: an introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture.* Springer, 2009.

[7] Z. Chatzidakis and E. Hrushovski. Model theory of difference fields. *Transactions of the American Mathematical Society*, 351(8):2997–3071, 1999.

[8] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil. Model theory of difference fields, II: Periodic ideals and the trichotomy in all characteristics. *Proceedings of the London Mathematical Society*, 85(02):257–311, 2002.

[9] R. Cori and D. Lascar. *Mathematical Logic: Part II.* Oxford University Press, 2001.

[10] D. Eisenbud. *Commutative algebra: with a view toward algebraic geometry.* Graduate Texts in Mathematics. Springer, 1995.

[11] W. Fulton. *Intersection Theory.* Ergebnisse Der Mathematik Und Ihrer Grenzgebiete, 3. Folge, Bd. 2. Springer-Verlag GmbH, 1998.

[12] D. Goss. Polynomials of binomial type and lucas theorem. *Proceedings of the American Mathematical Society*, 2015.

[13] A. Grothendieck. Éléments de géométrie algébrique. *Inst. Hautes Études Sci. Publ. Math.*, 1960–1967.

[14] A. Grothendieck. *Éléments de géométrie algébrique.* Springer, 1971.

[15] A. Grothendieck. *Revêtements étales et groupe fondamental (SGA 1)*, volume 224 of *Lecture notes in mathematics.* Springer-Verlag, 1971.

[16] A. Hasson and P. Kowalski. Strongly minimal expansions of $(\mathbb{C}, +)$ definable in o-minimal fields. *Proc. Lond. Math. Soc. (3)*, 97(1):117–154, 2008. ISSN 0024-6115. doi: 10.1112/plms/pdm052.

[17] E. Hrushovski. *Contributions to stable model theory.* PhD thesis, University of Berkley, 1986.

[18] E. Hrushovski. Unidimensional theories: an introduction to geometric stability theory. *Studies in Logic and the Foundations of Mathematics*, 129:73–103, 1989.

[19] E. Hrushovski. Strongly minimal expansions of algebraically closed fields. *Israel Journal of Mathematics*, 79(2-3):129–151, 1992.

[20] E. Hrushovski. A new strongly minimal set. *Annals of Pure and Applied Logic*, 62(2):147–166, 1993.

[21] E. Hrushovski. The Mordell-Lang conjecture for function fields. *Journal of the American mathematical society*, 9(3):667–690, 1996.

[22] E. Hrushovski. The Manin–Mumford conjecture and the model theory of difference fields. *Annals of Pure and Applied Logic*, 112(1):43–115, 2001.

[23] E. Hrushovski and A. Pillay. Weakly normal groups. *Studies in Logic and the Foundations of Mathematics*, 122:233–244, 1987.

[24] E. Hrushovski and B. Zilber. Zariski geometries. *Journal of the American mathematical society*, 9(1):1–56, 1996.

[25] P. Kowalski and S. Randriambololona. Strongly minimal reducts of valued fields. *arXiv preprint*, 2014. math:1408.3298.

[26] D. Marker. *Model theory: an introduction.* Springer, 2002.

[27] D. Marker and A. Pillay. Reducts of $(\mathbb{C}, +, \cdot)$ which contain $+$. *Journal of Symbolic Logic*, 55(3):1243–1251, 1990.

[28] G. A. Martin. Definability in reducts of algebraically closed fields. *J. Symbolic Logic*, 53(1):188–199, 1988. ISSN 0022-4812. doi: 10.2307/2274437. URL `http://dx.doi.org/10.2307/2274437`.

[29] H. Matsumura and M. Reid. *Commutative ring theory*, volume 8. Cambridge university press, 1989.

[30] J. Milne. *Étale cohomology*. Princeton University Press, 1980.

[31] Y. Peterzil and S. Starchenko. A trichotomy theorem for o-minimal structures. *Proceedings of the London Mathematical Society*, 77(3):481–523, 1998.

[32] A. Pillay. *Geometric stability theory*. Number 32 in Oxford logc guides. Oxford University Press, 1996.

[33] A. Pillay. Model theory of algebarically closed fields. In E. Bouscaren, editor, *Model theory and algebraic geometry: an introduction to E. Hrushovski's proof of the geometric Mordell-Lang conjecture*. Springer, 2009.

[34] A. Pillay and M. Ziegler. Jet spaces of varieties over differential and difference fields. *Selecta Mathematica*, 9(4):579–599, 2003.

[35] B. Poizat. *Stable groups*, volume 87 of *Mathematical Surveys and Monographs*. AMS, 2001.

[36] E. Rabinovich. *Definability of a field in sufficiently rich incidence systems*. QMW maths notes. University of London, Queen Mary and Westfield College, 1993.

[37] T. Scanlon. Local André-Oort conjecture for the universal abelian variety. *Inventiones mathematicae*, 163(1):191–211, 2006.

[38] L. Van den Dries. Weil's group chunk theorem: A topological setting. *Illinois Journal of Mathematics*, 34(1):127–139, 1990.

[39] A. Weil. On algebraic groups of transformations. *American Journal of Mathematics*, 77(2):355–391, 1955.

[40] G. T. Whyburn. *Topological analysis*. Princeton Mathematical Series. No. 23. Princeton University Press, Princeton, N. J., 1958.

[41] B. Zilber. *Zariski Geometries: Geometry from the Logician's Point of View*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2010.

[42] B. Zilber. A curve and its abstract Jacobian. *International Mathematics Research Notices*, 2014(5):1425–1439, 2014.

Department of Mathematics
Ben Gurion University of the Negev
P.O.B. 653
Be'er Sheva 84105
Israel
hassonas@math.bgu.ac.il

Laboratoire Paul Painlevé
CNRS U.M.R. 8524
59 655 Villeneuve d'Ascq Cedex
France
Dmitry.Sustretov@math.univ-lille1.fr