

Incidence systems on Cartesian powers of algebraic curves

Assaf Hasson¹ and Dmitry Sustretov²

Abstract

We show that a non locally modular reduct of the full Zariski structure of an algebraic curve interprets an infinite field.

Contents

1	Introduction	1
2	Model-theoretic background	3
3	Tangency	5
3.1	Slopes and operations on correspondences	6
3.2	Flat families and definability of tangency	13
4	Interpretation of the field	18
4.1	The group configuration	18
4.2	Some standard reductions	22
4.3	Generically unramified projections	24
4.4	Interpretation of a one-dimensional group	26
4.5	Interpretation of the field and proof of the main theorem	35

1 Introduction

In [1, §2] Artin describes the basic problem of classifying abstract plane geometries (viewed as incidence systems of points and lines) as follows “Given a plane geometry [...] assume that certain axioms of geometric nature are true [...] is it possible to find a field k such that the points of our geometry can be described by coordinates from k and lines by linear equations?”. Zilber’s trichotomy principle (to be described in more detail in the next section) can be viewed as an abstraction of the above problem, replacing the “axioms of geometric nature” with a well behaved theory of dimension (see, e.g., [33, §1]).

Conjectured in various forms by Zilber throughout the late 1970s, essentially every aspect of Zilber’s trichotomy, in its full generality, was refuted by Hrushovski [14], [13] in the late 1980s. Due to Hrushovski’s cornucopia of counterexamples the conjecture has never been reformulated. Yet, Zilber’s principle remains a central

¹was supported by ISF grants No. 181/16 and 1156/10.

²has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 843100 (NALIMDIF) and was supported by the European Research Council under the European Community’s Seventh Framework Programme (FP7/2007-2013) with ERC Grant Agreement nr. 615722 (MOTMELSUM).

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 [5, 32, 30, 6, 19]). Many of these special cases of Zilber’s trichotomy had striking applications in algebra and geometry (see [15, 16, 35]). More recently, in [40], Zilber outlines a model theoretic framework for studying far reaching extensions of the Mordell-Lang conjecture. One of the key features of Zilber’s strategy is the trichotomy theorem for Zariski Geometries [19].

The key to the classification of Desarguesian plane geometries (the fundamental theorem of projective geometry) is the reconstruction of the underlying field k as the ring of direction preserving endomorphisms of the group of translations. The reconstruction of a field out of abstract geometric data is also the essence of Zilber’s trichotomy and is the engine in many of its applications. A relatively recent application of one such result is Zilber’s model theoretic proof [39] of a significant strengthening of a theorem of Bogomolov, Korotiaev, and Tschinkel [3]. The model theoretic heart of Zilber’s proof is Rabinovich’s trichotomy theorem for *reducts* of algebraically closed fields [34]. In the concluding paragraph of the introduction to [39] Zilber writes: “It is therefore natural to aim for a new proof of Rabinovich’ theorem, or even a full proof of the Restricted Trichotomy along the lines of the classification theorem of Hrushovski and Zilber [19], 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^{3,4}:

Conjecture A. *Let \mathcal{M} be a strongly minimal reduct of the full Zariski structure on an algebraic curve M over an algebraically closed field K which is not locally modular. Then there exist \mathcal{M} -definable L, E such that $E \subseteq L \times L$ is an equivalence relation with finite classes and L/E with the \mathcal{M} -induced structure is a field K -definably isomorphic to K .*

Rabinovich [34] proved Conjecture A in the special case where $M = \mathbb{A}^1$, and her result can be extended by general principles to any rational curve. In the present paper we prove Conjecture A. Our approach to the problem follows a, by now, well known strategy introduced by Zilber and Rabinovich and owes to [24]. Using a standard model theoretic technique, Hrushovski’s field configuration (see Section 4.1 for details), the problem is reduced to showing that tangency is (up to a finite correction) reduct-definable in families.

To achieve this goal, we proceed in two steps. In the first step (carried out in Section 3) we study slopes of families of branches (at a given point) and their behaviour under composition of curves and, in case the ambient structure is an expansion of a group, under point-wise addition. This culminates in Proposition 3.15,

³The content of Conjecture A is explained for non-experts in Section 2.

⁴In the full conjecture referred to by Zilber \mathfrak{M} is the full Zariski structure on an n -dimensional constructible set (for n possibly greater than 1).

which is the key to the definability of tangency, and in Lemma 4.19, providing us with the (algebraic) group which is the template allowing us to construct the group configuration.

Section 4, where Conjecture A is proved (Theorem 4.36), is dedicated, mainly, to verifying that the assumptions of the technical result of the previous section can be met in the reduct. In Section 4.3 we show that our definition of slope is meaningful in reduct-definable families of curves (in positive characteristic). In Section 4.4, where the main step towards proving Theorem 4.36 is carried out, the key difficulty to overcome is in the application of Proposition 3.15.

As already mentioned, the general scheme of our proof seems to have much in common with Rabinovich's original work, though we were unable to understand significant parts of her argument, which are highly technical. For that reason we cannot pinpoint the reason for the present work being more general, considerably shorter, and technically simpler.

Finally, it should be mentioned that the tools developed in the present paper seem to extend naturally to various other contexts. For example, one can envisage extending the results of [21] to positive characteristic, and any algebraic group and – possibly – even a full proof of the restricted trichotomy conjecture for structures definable in ACVF (at least modulo the problem of showing that the 1-dimensional group reconstructed by our methods embeds in an algebraic group: it can probably be shown that the group will always be isomorphic to either \mathbb{G}_a or to \mathbb{G}_m).

2 Model-theoretic background

For readers unfamiliar with model theory we give a self contained exposition 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. We refer interested readers to [37, §1.1-2] for a more detailed discussion of structures and definable sets. Readers familiar with the basics of model theory are advised to skip the remainder of the present section.

Given an algebraic curve M over an algebraically closed field k (reduced, but not necessarily irreducible, smooth or projective), the *full Zariski structure on M* , denoted \mathfrak{M} , is the set of k -rational points, $M(k)$ equipped with the collection of all Boolean algebras of constructible sets on the Cartesian powers $M^n(k)$. The full Zariski structure on a curve M is an example of the model theoretic notion of a structure.

A *first-order structure* or simply a *structure* \mathcal{N} is a non-empty set N (called the universe of \mathcal{N}) equipped with a collection, $\text{Def}(\mathcal{N})$, of Boolean algebras $\text{Def}_l(\mathcal{N}) \subseteq \mathcal{P}(N^l)$ for all $l > 0$, such that $\text{Def}_l(\mathcal{N})$ contains all diagonals $\Delta_{i,j}^l := \{(x_1, \dots, x_l) : x_i = x_j\}$, and such that $\text{Def}(\mathcal{N})$ is closed under finite cartesian products and projections of the form $(x_1, \dots, x_n) \mapsto (x_1, \dots, x_{n-1})$. Somewhat analogously to geometric terminology the tuples $(x_1, \dots, x_n) \in S \subset M^l$ are called *points of the definable set S* . If $A \subseteq N$ is any set, a subset $X \subseteq N^l$ is *definable with parameters in A* (or

A-definable) if there exists a definable set $Y \subseteq N^{n+m}$ (some $m \geq 0$) such that $Y = Y_a := \{x \in N^n : (x, a) \in Y\}$ for some $a \in A$.

Note that by Chevalley's theorem (see, e.g., [23, Corollary 3.2.8]), over an algebraically closed field k , the collection of constructible sets on cartesian powers of an algebraic curve M is closed under projections, and therefore the full Zariski structure, \mathfrak{M} , on M is, indeed, a structure in the above sense. It is a well known fact (e.g., [19]) that the field k can be reconstructed from \mathfrak{M} . Let us now explain more precisely what is meant by that.

A (partial) function $f : N^n \rightarrow N$ is definable if its graph is. Thus, for example, we say that a group is definable in \mathcal{N} , if there exists a definable set $G \subseteq N^n$ and a definable function $p : G \times G \rightarrow G$ such that (G, p) is a group (note that the function $x \mapsto x^{-1}$ is automatically definable if (G, p) is a group). The definability of a field in a structure \mathcal{N} is defined analogously. It is not hard to check (and follows from the main result of [19]) that if \mathfrak{M} is the full Zariski structure on an algebraic curve M over an algebraically closed field k then a field F is definable in \mathfrak{M} (and F is isomorphic, definably in the standard field structure on k , to k).

But we need a somewhat subtler notion than definability. Consider, as a simple example, the structure \mathcal{C} with universe $\mathbb{C} \times \{0, 1\}$, and whose definable sets are all those of the form $\{(x_1, i_1), \dots, (x_n, i_n) : (x_1, \dots, x_n) \in D\}$ where D is a constructible subset of \mathbb{C}^n and $i_j \in \{0, 1\}$ for all $1 \leq j \leq n$. It is easy to verify that all functions definable in \mathcal{C} are locally constant, and therefore there is no definable field in \mathcal{C} . Consider, however, the equivalence relation $x \sim y$ (in \mathcal{C}) defined by $y \in (1, 0) \cdot x$ (recalling the interpretation of multiplication in \mathcal{C} , this is a \mathcal{C} -definable way of saying that x and y have the same first coordinate). Then \sim is a \mathcal{C} -definable equivalence relation, and \mathcal{C}/\sim is naturally isomorphic to the full Zariski structure on \mathbb{C} .

In model-theoretic terms the structure \mathcal{C} in the previous example *interprets* a field definably isomorphic to \mathbb{C} . In general, if \mathcal{N} is a structure, E a definable equivalence relation on N^n and $\pi : N^n \rightarrow N^n/E$ is the natural projection, the induced structure on N^n/E is the push-forward of the Boolean algebras on powers of N^n via π . We say that \mathcal{N} *interprets* a field if a field is definable in the structure induced on N^n/E for some n and \mathcal{N} -definable equivalence relation E on N^n .

In the above example the universe $\mathbb{C} \times \{0, 1\}$ of \mathcal{C} is definable in the full Zariski structure on \mathbb{C} , and every definable set in \mathcal{C} is definable in \mathbb{C} . But, as we have seen, \mathcal{C} is not the full Zariski structure on \mathbb{C} . The structure \mathcal{C} is an example of a *reduct* of the full Zariski structure on \mathbb{C} . Generally, if \mathcal{M} is a structure whose universe is an algebraic curve M and every \mathcal{M} -definable set is \mathfrak{M} -definable then \mathcal{M} is a *reduct* of \mathfrak{M} .

Zilber's conjecture is concerned with the question of interpreting a field in a reduct, \mathcal{M} , of the full Zariski structure, \mathfrak{M} , on an algebraic curve M . Assume that an infinite field \mathbb{F} is interpretable in \mathcal{M} . Then by [23, Theorem 3.2.20] the universe F of \mathbb{F} can be identified with a constructible subset of k^l for some l , and by [33, Theorem 4.15] k is definably isomorphic to \mathbb{F} . Thus there is a definable finite-to-finite correspondence $\Psi \subseteq F \times M$. It is easy to check that Ψ can be taken to be

\mathcal{M} -interpretable (e.g., if F is definable in \mathcal{M} then Ψ can be taken to be the graph of a projection function, the general case is slightly more delicate and we skip the details). If we push the family of affine lines in F^2 via Ψ we obtain a 1-dimensional constructible subset U of M such that for any $p, q \in U$ there is a curve $C := \Psi(L)$ – for L an affine line in F^2 – with $p, q \in C$. We have thus verified that for \mathcal{M} to interpret a field it is necessary that there exists a 2-dimensional constructible $U \subseteq M^2$ and a definable set $X \subseteq M^{2+l}$ such that $X_t := \{(x, y) : (x, y, t) \in X\}$ is 1-dimensional (or empty) for all $t \in M^l$ and such that for all $p, q \in U$ there exists $t \in M^l$ such that $p, q \in X_t$. The main result of the present work, Theorem 4.36, states that this condition is, in fact sufficient.

Definition 2.1. *Let \mathcal{M} be a reduct of the full Zariski structure \mathfrak{M} on an algebraic curve M over an algebraically closed field k . An \mathcal{M} -definable ample family of curves in M^2 is a set $X \subseteq M^{2+l}$ such that*

- $\dim(X_t) = 1$ for all $t \in M^l$ such that $X_t \neq \emptyset$ and
- there exists a 2-dimensional $U \subseteq M^2$ such that for all $p, q \in U$ there exists $t \in M^l$ with $p, q \in X_t$.

In model-theoretic terms the existence of an ample family as above is equivalent, [23, Lemma 8.1.13], to **non local modularity** of the structure \mathcal{M} .

If X is an ample family in M^2 we denote by (M, X) the smallest reduct of \mathfrak{M} containing X . We can thus formulate Conjecture A:

Conjecture B (Zilber’s restricted trichotomy in dimension 1). *Let M be an algebraic curve over an algebraically closed field k . Let $X \subseteq M^2 \times T$ be the total space of an ample family in M^2 , then a field K is interpretable in $\mathcal{M} = (M, X)$.*

In [1, §2.4] not only is the field recovered from the affine geometry, but also the geometry is recovered as the affine plane over that field. In the present setting, there are examples due to Hrushovski (see, e.g., [25]) showing that the full Zariski structure of the curve M cannot be recovered from \mathcal{M} . This can probably be achieved if X is *very ample* in the sense of [19] (namely, if the set X in Definition 2.1 separates points in M^2), but we do not study this question here.

3 Tangency

The reconstruction of the field is obtained in two steps. First, we reconstruct a 1-dimensional algebraic group, and then – using the group structure to sharpen the same arguments – we reconstruct the field. Roughly, the reconstruction of a group is obtained in three stages: first we identify a reduct definable family $X \rightarrow T$ of algebraic curves whose associated family of slopes at some point $P = (a, a) \in M^2$ is a 1-dimensional algebraic group under composition. The second, and most crucial

part of the proof is commonly dubbed *definability of tangency*. In its cleanest form this consists in showing that, given families $X \rightarrow T$ and $Y \rightarrow S$ as above, the set of all $(t, s) \in T \times S$ such that X_t is tangent (in an appropriate sense) to Y_s at P is \mathcal{M} -definable. Finally, the group is reconstructed by invoking *the group configuration theorem*, a well known model theoretic technique (to be described in more detail in the next section), using the results of the previous stages. In the next two subsections we take care of the two first stages of the this strategy.

Before starting with our set up on the technical level let us discuss some of the challenges that motivated the definitions to be shortly presented. In the implementation of the strategy outlined above two difficulties arise.

Firstly, if we consider only the first-order slopes, then due to inseparability issues in positive characteristic it becomes hard to find a 1-dimensional family of curves definable in the reduct such that its associated slopes at some point range in a 1-dimensional set — such a family is needed to construct the first group configuration (Section 4.4). The solution is to consider tangency information up to any order n and pick the order so that there are enough slopes. Interestingly — and this was apparent already in [24] — in the presence of a group structure, the problem doesn't arise, which is a good coincidence, since the second group configuration (Section 4.5) has to be built using the first-order tangency information.

Secondly, we can't work only with smooth points to define the slope, since the operations of composition and point-wise addition that are used in the construction of the group configurations do not preserve smoothness. Our approach to this is to track a particular branch of a curve at a particular point as the operations of composition and point-wise addition are applied: one can then have control over the slope of a branch, appropriately defined. Note that we use the term *branch* (Definition 3.3) in a more restrictive sense than what is usually understood by it: in a way our branches are 'always smooth' (or more precisely 'always étale over the first factor M of M^2 '), so that the notion of a slope always makes sense for them. For any curve in M^2 the projection either on the first or on the second factor M is going to be generically étale (Lemma 4.14), even in positive characteristic, and so there is going to be a unique branch at any general enough point on this curve (Lemma 3.4). This statement generalizes appropriately to families of curves too. By virtue of Propositions 3.7 and 3.9 the slopes of relevant branches can be tracked as the curves are composed and point-wise added. All curves and branches that we work with in Section 4 are obtained this way.

3.1 Slopes and operations on correspondences

First of all, our main objects of interest are definable subsets in a reduct of the full Zariski structure on a fixed curve M , we will adopt the following non-standard terminology: we will call a constructible subset $Z \subseteq M^n$ (for some n) of dimension 1 a *curve* even if it is reducible and if it has connected components of dimension 0. If a curve Z does not contain connected components of dimension 0 then we call Z a *pure-dimensional curve*. Clearly, every curve contains a maximal pure-dimensional

curve. In the few situations when we refer to abstract algebraic curves (that is, algebraic varieties of pure dimension 1 over a fixed algebraically closed field) we will use the term *algebraic curve*. We will not distinguish notationally between subsets of M^n definable in a reduct of the full Zariski structure on M and constructible subsets of the varieties (or even schemes) M^n , and in particular between definable curves and their algebro-geometric counterparts.

Recall that any algebraic variety over a perfect field admits a dense Zariski open subset that is smooth (see, e.g., Corollary to Theorem 30.5 of [27]). Let $Z \subset M^2$ be a pure-dimensional curve, and $a = (a_1, a_2) \in Z$ be a smooth point of M^2 . Since the completion of the local ring of a smooth point of a variety is a formal power series ring [27, Theorem 29.7], we can pick some isomorphisms

$$\widehat{\mathcal{O}_{M,a_1}} \cong k[[x]] \quad \widehat{\mathcal{O}_{M,a_2}} \cong k[[y]]$$

inducing an isomorphism $\widehat{\mathcal{O}_{M^2,a}} \cong k[[x, y]]$, and then $\widehat{\mathcal{O}_{Z,a}} = k[[x, y]]/(f)$ for some $f \in k[[x, y]]$. We call *branches of Z at a* the factors in the prime decomposition of f of the form $y - g_\alpha, g_\alpha \in k[[x]]$ (note that this is different from the standard use of the term, but since we will never use the term in its standard meaning in this article, no confusion will occur). In particular, if the projection of Z onto the first factor M in M^2 is étale in a neighbourhood of a , by Hensel's lemma (stated as in [28, §4, Theorem 4.2(d)]), the natural morphism $k[[x]] \rightarrow k[[x, y]]/(f)$ is an isomorphism and therefore f can be written uniquely as $u(y - g)$ where $u \in k[[x]]^\times, g \in k[[x]]$. We call the truncation to the n -th order of the series g_α the *n -th order slope of a branch α of Z* . Naturally, the slope of a branch of a pure-dimensional curve depends on the choice of the isomorphism $\widehat{\mathcal{O}_{M^2,a}} \cong k[[x, y]]$, but this choice does not affect any of the properties of slopes we will be interested in.

We view curves in M^2 as finite-to-finite correspondences between the two factors M . The purpose of the present section is to study the behaviour of slopes of branches with respect to two natural operations on correspondences: composition and “point-wise addition” (see Definition 3.8) when M has a structure of an algebraic group. We will show that if Z, W are two curves and α, β are two branches of Z, W at $a = (a_1, a_2), b = (b_1, b_2) \in M^2$ respectively, and $a_2 = b_1$ then the composition $W \circ Z$ has a branch $\beta \circ \alpha$ at (a_1, b_2) such that its slope is the composition of the n -th order slopes of α and β (as truncated polynomials) whenever the latter are defined. A similar statement can be made about the slopes of branches of curves that are ‘point-wise added’ if M has a structure of a group. Later we will construct a group configuration starting from a family of curves definable in a reduct of a full Zariski structure on M such that the set of its n -th order slopes at a given point coincides, up to a finite set, with a 1-dimensional algebraic subgroup of $\text{Aut}(k[[x]]/(x^{n+1}))$ (a truncated polynomial f corresponds naturally to the automorphism of $k[[x]]/(x^{n+1})$ sending x to f).

Since we will have to work with families of curves, we will also introduce notions of families of branches and slopes. When the characteristic of the base field is positive, we will often have to work with curves and families of curves in $M \times M^{(p^n)}$ where

$M^{(p^n)}$ is the pull-back of M by the Frobenius endomorphism on k (see Section 4.3). That is why we do not assume that factors of the ambient product variety are isomorphic in the definitions below.

Definition 3.1 (Families of curves). *If X_1, X_2 are two algebraic curves then by a family of pure-dimensional curves in $X_1 \times X_2$ we will understand a finite union Z of pure codimension 1 locally closed subsets $Z_i \subset X_1 \times X_2 \times T$, where T is a variety, such that Z_t is a pure-dimensional curve for all $t \in T$. By a family of curves we understand a constructible subset $Z \subset X_1 \times X_2 \times T$ where T is a constructible subset of a variety and such that Z_t is a curve for all $t \in T$. If $X_1 = X_2 = M$ and $T \subset M^l$ for some l and Z is definable in a reduct of the full Zariski structure on M we call it a definable family of curves.*

While families of curves arise naturally in definable context, in order to apply the machinery of slopes we need to work with families of pure-dimensional curves. As long as T is a variety, a family of curves $Z \subset X_1 \times X_2 \times T$ contains a unique maximal family of pure-dimensional curves. The total space Z of a family of pure-dimensional curves is not necessarily a variety; while this is a desirable property that will be important in Subsection 3.2, we do not include it in the definition so that it can be readily seen that the operations of composition and point-wise addition preserve the class of families of pure-dimensional curves. However, one can easily ensure that the total space is a variety at the cost of shrinking the parameter space.

Lemma 3.2. *Let T be a constructible subset of a variety, $W \subset X_1 \times X_2 \times T$ be a family of curves. Then there exists a Zariski dense subset $T' \subset T$ which is a variety and a maximal locally closed $W' \subset W \times_T T'$ which is a family of pure-dimensional curves. In particular, W' is a variety.*

Proof. It is easily checked using Noetherian induction that any constructible set contains a Zariski dense locally closed subset. In particular, there exists a dense locally closed subset $T_0 \subset T$ which is therefore a variety. Without loss of generality we may assume T_0 connected. Then $W \times_T T_0$ is a union of locally closed sets of the form $W_i \setminus Z_i, i \in I$ where W_i and $Z_i \subset W_i$ are Zariski closed and distinct, and the index set I is finite. Let $I' \subset I$ be the set of those indices i for which W_i is codimension 1 in $M^2 \times T$. Further shrinking T_0 we may assume that $\dim(W_i)_t = 1, \dim(Z_i)_t = 0$ for all $t \in T_0$ and all $i \in I'$ (in particular, $Z_i \neq \emptyset$). We put $W' = \cup_{i \in I'} W_i \setminus Z_i$. It now suffices to show that if $W_1 \setminus Z_1$ and $W_2 \setminus Z_2$ are as above then there exists a dense open $T' \subset T_0$ such that $(W_1 \setminus Z_1) \times_T T' \cup (W_2 \setminus Z_2) \times_T T'$ is locally closed, the statement of the Lemma then follows by induction on the size of I' .

We have

$$(W_1 \setminus Z_1) \cup (W_2 \setminus Z_2) = (W_1 \cup W_2) \setminus ((Z_1 \cap Z_2) \cup (Z_1 \cap (W_2 \setminus Z_2)) \cup (Z_2 \cap (W_1 \setminus Z_1)))$$

It follows from an easy dimension computation that

$$\dim(Z_1 \cap (W_2 \setminus Z_2)) < \dim Z_1 \quad \dim(Z_2 \cap (W_1 \setminus Z_1)) < \dim Z_2$$

so in particular the projections of $Z_1 \cap (W_2 \setminus Z_2)$, $Z_2 \cap (W_1 \setminus Z_1)$ to T_0 are not dense. If T' is a dense open set in the complement of the projections then

$$(W_1 \setminus Z_1) \times_T T' \cup (W_2 \setminus Z_2) \times_T T' = (W_1 \cup W_2) \times_T T' \setminus (Z_1 \cap Z_2) \times_T T'$$

which is locally closed. \square

Given a family of pure-dimensional curves Z as above, we would like to be able to pick branches of the curves Z_t depending algebraically on the parameter $t \in T$. In this case the local equation of Z in a formal neighbourhood of $\{a\} \times T$ may only exist locally on T , and in order to capture this idea we have to phrase the definition in terms of formal schemes (we refer the reader to [11, II.9] or any other standard algebraic geometry reference for the definition of formal schemes).

Definition 3.3 (Branches and families of branches). *Let $Z \subset V := X_1 \times X_2 \times T$ be a family of pure-dimensional curves, $a \in M^2$ and assume that $a \in Z_t$ for all $t \in T$. Let \hat{X}_1 be the formal completion of $X_1 \times T$ along $\{a_1\} \times T$, and let \hat{Z} be the formal completion of Z along $\{a\} \times T$. A family of branches of Z at a is a closed formal subscheme \hat{Z}_α such that the natural projection $\hat{Z}_\alpha \rightarrow \hat{X}_1$ is an isomorphism. We will call local generators of the ideal sheaf that defines \hat{Z}_α local equations of α . When $Z \subset X_1 \times X_2$ is a single curve, we regard it as a family parametrized by a single point, and we call families of branches of Z just branches. Given a family of branches α we will denote α_t the branch given by the fibres \hat{Z}_{α_t} for all $t \in T$.*

Remark. If $Z \subset X_1 \times X_2 \times T$ is a family of curves and T is a variety then in order to simplify the exposition we will refer to branches of Z meaning branches of a family of pure-dimensional curves $Z_0 \subset Z$.

Let X_i be algebraic curves, and let $a = (a_1, \dots, a_n) \in X = X_1 \times \dots \times X_n$ be a smooth point. We say that a *local coordinate system at a* is picked when an isomorphism $\widehat{\mathcal{O}_{X_i, a_i}} \cong k[[x_i]]$ is picked for each a_i ; in this case we understand that there exists an isomorphism $\mathcal{O}_{X, a} \cong k[[x_1, \dots, x_n]]$ induced by these isomorphisms. If local coordinate systems are picked at $a = (a_1, a_2) \in X_1 \times X_2$, $b = (b_1, b_2) \in X_2 \times X_3$, we understand without explicit mention that local coordinate systems are automatically picked at the points $(a_1, b_2) \in X_1 \times X_3$, $(b_2, a_1) \in X_3 \times X_1$ which will be of interest to us later on. Similarly, if X_1 has a group structure and a local coordinate system is picked at a point $a \in X_1$ then we assume it picked at any point $a' \in X_1$ via translation. The next lemma gives a sufficient condition for the existence of a family of branches at a point.

Recall that a morphism of schemes $f : X \rightarrow Y$ is called *quasi-finite* if the fibres $f^{-1}(y)$ are finite for all $y \in Y$. A quasi-finite morphism $f : X \rightarrow Y$ of locally Noetherian schemes is *unramified* if $\Omega_{X/Y} = 0$ (see [22, Ch. 6, Corollary 2.3]) where $\Omega_{X/Y}$ is the module of Kähler differentials of the morphism f . A morphism f locally of finite type is called *étale* if it is flat and unramified. Basic properties of these notions will be recalled in detail and with references in Section 3.2.

Lemma 3.4. *If $Z \subset V = X_1 \times X_2 \times T$ is a family of pure-dimensional curves and the projection $Z \rightarrow X_1$ is étale in a neighbourhood of $\{a\} \times T$ for some $a \in X_1 \times X_2$, then there exists a unique family of branches of Z at a .*

Proof. For any affine open $\text{Spec } R \subset X_1 \times T$ let $\text{Spec } R' \subset Z$ be an affine open étale over $\text{Spec } R$, let I, I' be the ideals vanishing on $\{a_1\} \times T, \{a\} \times T$ respectively, \widehat{R} and \widehat{R}' their respective completions. Then by [36, Tag 0ALJ] (\widehat{R}, I) is a Henselian pair and by [36, Tag 09XI] there exists a unique isomorphism $\widehat{R}' \rightarrow \widehat{R}$ that defines the unique family of branches. \square

Definition 3.5 (Slope). *Let X_1, X_2 be algebraic curves, $Z \subset V := X_1 \times X_2$ a pure-dimensional curve, $a \in V$ a smooth point, $a \in Z$, and $I, \mathfrak{m}_a \subset \mathcal{O}_{V,a}$ the ideals of functions that vanish on $Z, \{a\}$, respectively. Assume that a local coordinate system is chosen at a , so that $\varprojlim \mathcal{O}_{V,a}/\mathfrak{m}_a^n \cong k[[x, y]]$. A branch α of Z is therefore defined by a principal ideal J with the property that the composition $k[[x]] \rightarrow k[[x, y]] \rightarrow k[[x, y]]/J$ is an isomorphism. The inverse of this isomorphism sends y to $f \in xk[[x]]$, and $y - f \in J$. We call $f \bmod x^{n+1} \in k[x]/(x^{n+1})$ the n -th order slope of Z at α , denoted $\tau_n(Z, \alpha)$.*

Note that $\tau_n(Z, \alpha)$ depends on the choice of the local coordinate system at a , and that if an n -th order slope of Z at α is defined, then the slopes of all orders of Z at α are defined.

Remark.

- (i) Let f, g be local equations of branches α, β at a point a of pure-dimensional curves Z_1, Z_2 , respectively. If $\tau_n(Z_1, \alpha) = \tau_n(Z_2, \beta)$ but $\tau_{n+1}(Z_1, \alpha) \neq \tau_{n+1}(Z_2, \beta)$, then $f \equiv g \bmod x^{n+1}$ and therefore $f - g = x^{n+1} \cdot r$ for some unit $r \in k[[x]]$ and so

$$k[[x, y]]/(y - f, y - g) \cong k[[x]]/(x^{n+1}).$$

In particular, if Z_1, Z_2 are smooth at a and α, β are their unique respective branches at a , then the intersection multiplicity of Z_1 and Z_2 at a (as defined in, for example, [11, ex. I.5.4]) is n .

- (ii) Let $X \subset M^2 \times T, Y \subset M^2 \times S$ be families of pure-dimensional curves such that $a \in X_t \cap Y_s$ for all $t \in T, s \in S$ and $X_t \cap Y_s$ is zero-dimensional for generic t, s . Let α, β be some families of branches of X and Y at a . Then it follows from Krull's maximal ideal theorem that there exists a maximal integer n such that

$$\tau_n(X_t, \alpha_t) = \tau_n(Y_s, \beta_s)$$

for all $t \in T, s \in S$.

For the benefit of the reader we explain what data in the Definitions 3.3 and 3.5 specifies families of branches and slopes, specialising the description in the language

of formal schemes to an affine situation. Take Zariski open subsets $U \subset X_1 \times X_2$, $W \subset T$ such that $a \in U$. Let S, R be the rings of regular functions on U, W and let $J_a, J \subset R \otimes S$ be the ideals of regular functions that vanish on $\{a\} \times W, Z \cap U \times W$, respectively. We fix a local coordinate system at a which gives an isomorphism $\varprojlim (R \otimes S)/J_a^n \cong R[[x, y]]$. A choice of a family of branches α is a choice of an element $f_\alpha \in R[[x]]$ such that $y - f_\alpha \in R[[x, y]]$ generates an ideal (necessarily prime) containing $JR[[x, y]]$. The slope $\tau_n(Z_t, \alpha_t)$ is the truncated polynomial $f_\alpha \otimes k(t) \bmod x^{n+1} \in k[[x]]/(x^{n+1})$. From this description it is clear that if we regard the n -th order slope of Z at α_t as a tuple of coefficients of $f_\alpha \otimes k(t)$, then $t \mapsto \tau_n(Z_t, \alpha_t)$ is a regular function from W to \mathbb{A}^n .

Note that the notion of slope is invariant under extensions of the base field. Assume that all objects in the previous paragraph are defined over k , and let $k' \supset k$ be a field extension. Then there exists a family of branches $\alpha_{k'}$ of $Z_{k'} = Z \otimes k' \subset (X_1 \otimes k') \times (X_2 \otimes k')$ and there exists a local coordinate system at a in $(X_1 \otimes k') \times (X_2 \otimes k')$ such that the regular function

$$t \mapsto \tau_n((Z_{k'})_t, (\alpha_{k'})_t)$$

is defined by the polynomials with the same coefficients as the function

$$t \mapsto \tau_n(Z_t, \alpha_t).$$

In model-theoretic terms, this observation implies that once a point $a \in M^2$, a local coordinate system at a , and a family of branches α of Z are fixed, the slope $\tau_n(Z_t, \alpha_t)$ is definable in the language of fields over t .

Further if $X_1 \times \dots \times X_n$ is a product of k -varieties, we denote the natural projections

$$p_{i_1 \dots i_k} : X_1 \times \dots \times X_n \rightarrow X_{i_1} \times \dots \times X_{i_k}$$

denote the natural projections. Although the notion of the composition of correspondences is standard, we reintroduce it here to fix conventions.

Definition 3.6 (Composition of curves). *Let $Z \subset X_1 \times X_2 \times T$, $W \subset X_2 \times X_3 \times S$ be families of curves, and let $p_{i_1 \dots i_k}$ denote projections on products of the factors of the space $X_1 \times X_2 \times X_3 \times T \times S$. Define the family $W \circ Z$ of compositions of curves from the families W and Z to be*

$$p_{1345}(p_{124}^{-1}(Z) \cap p_{235}^{-1}(W))$$

in $X_1 \times X_3 \times T \times S$. Clearly, if Z, W are definable then so is $Z \circ W$; on the level of points:

$$W \circ Z = \{ (x, z, t, s) \in M^2 \times T \times S \mid \exists u (x, y, u, t) \in Z \text{ and } (y, z, v, s) \in W \}.$$

If for all $t \in T, s \in S$ all irreducible components of Z_t, W_s project dominantly on X_1, X_2 , respectively, then $W \circ Z$ is a family of curves parametrized by $T \times S$.

We denote by Z^{-1} the image of Z under the morphism $X_1 \times X_2 \times T \rightarrow X_2 \times X_1 \times T$ that permutes the factors X_1 and X_2 , in both geometric and definable contexts. We regard the above definitions as applicable to individual curves Z, W by putting $T = S$ to be a point.

Remark. If Z, W are families of pure-dimensional curves such that for all $t \in T, s \in S$ all irreducible components of Z_t, W_s project dominantly on X_1, X_2 , respectively, then $W \circ Z$ is a family of pure-dimensional curves.

Proposition 3.7. *Let $Z \subset X_1 \times X_2 \times T$ and $W \subset X_2 \times X_3 \times S$ be families of pure-dimensional curves, let α, β be families of branches of Z, W at $a = (a_1, a_2) \in Z, b = (b_1, b_2) \in W$, respectively, $a_2 = b_1$. Then there exists a family of branches $\beta \circ \alpha$ of $W \circ Z$ at (a_1, b_2) such that for all $t \in T, s \in S$ and for all $n > 0$*

$$\tau_n(W_s \circ Z_t, (\beta \circ \alpha)_{(t,s)}) = \tau_n(W_s, \beta_s) \circ \tau_n(Z_t, \alpha_t)$$

where the operation “ \circ ” in the right hand side expression is composition of truncated polynomials.

Proof. The proof consists essentially in unraveling the definitions. The choice of coordinate systems induces the isomorphisms

$$\widehat{\mathcal{O}_{X_1 \times X_2, a}} \cong k[[x, y]] \quad \widehat{\mathcal{O}_{X_2 \times X_3, b}} \cong k[[y, z]]$$

If the family of branches α is given Zariski locally around $t \in T$ by an equation $y - f, f \in x \mathcal{O}_{T,t}[[x]]$, and β is given by $z - g, g \in y \mathcal{O}_{S,s}[[y]]$, then let the family of branches $\beta \circ \alpha$ be given by $z - g \circ f, g \circ f \in (\mathcal{O}_{T,t} \otimes \mathcal{O}_{S,s})[[x]]$. Note that the composition $g \circ f$ of the formal power series makes sense and has a zero constant term, since both f and g have this property.

Now let h_Z, h_W be generators of the kernels of the maps $\mathcal{O}_{X_1 \times X_2 \times T, (a,t)} \rightarrow \mathcal{O}_{Z, (a,t)}, \mathcal{O}_{X_2 \times X_3, (b,s)} \rightarrow \mathcal{O}_{W, (b,s)}$, respectively, then $y - f$ divides h_X and $z - g$ divides h_Y . The germ of $W \circ Z$ around (a_1, b_2, t, s) by Definition 3.6 is cut out by the ideal $(h_X, h_Y) \cap k[[x, z]]$, and in order to show that $\beta \circ \alpha$ is a family of branches of $Y \circ X$ at this point, we need to check that $(z - g \circ f)$ contains $(h_X, h_Y) \cap (\mathcal{O}_{T,t} \otimes \mathcal{O}_{S,s})[[x, z]]$, and for that it would suffice to check that

$$(z - g \circ f) = I := (y - f, z - g) \cap (\mathcal{O}_{T,t} \otimes \mathcal{O}_{S,s})[[x, z]].$$

Indeed, it is straightforward to check that for any $n > 0$

$$(z - g \circ f) = I_n := I / (x^n, z^n)$$

and since I is the inverse limit of I_n , it follows that $(z - g \circ f) = I$. \square

Definition 3.8 (Point-wise addition of curves). *Let G be a 1-dimensional algebraic group, and let $X \subset G^2 \times T, Y \subset G^2 \times S$ be families of curves. Let $a : G \times G \rightarrow G$ be the group law, let $\Gamma_a \subset G^3$ be its graph, and denote $p_{i_1 \dots i_k}$ projections of*

$G \times G \times G \times G \times T \times S$ on the products of factors. We define the family of curves $X + Y$ of sums of elements of the families X and Y to be

$$p_{1456}(p_{234}^{-1}(\Gamma_a) \cap p_{124}^{-1}(X) \cap p_{135}^{-1}(Y))$$

in $G^2 \times T \times S$. Clearly, if X, Y are definable then so is the family $X + Y$; on the level of points:

$$X + Y := \{(a, b + c, t, s) \mid (a, b, t) \in X, (a, c, s) \in Y\}.$$

Remark. If X and Y are families of pure-dimensional curves then so is $X + Y$. It may seem from the notation above that G is supposed to be commutative, even though the definition applies even if this is not the case. In this paper we will only consider the operation “+” for curves inside groups with the commutative connected component of the identity.

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 morphism $\widehat{\mathcal{O}_{G,e}} \rightarrow \widehat{\mathcal{O}_{G,e}} \otimes \widehat{\mathcal{O}_{G,e}} \cong k[[x, y]]$ induced by the group operation morphism. The truncation to first order of a one-dimensional formal group law is $x + y$ (see, for example, [20, I.2.4]).

Proposition 3.9. *Let G be a one-dimensional algebraic group over an algebraically closed field k . Let F be the formal group law of G , and let F_n be its n -th order truncation. Let $X \subset G \times G \times T$, $Y \subset G \times G \times S$ be families of pure-dimensional curves and let α, β be families of branches at $a = (a_0, a_1), b = (b_0, b_1)$, where $b_0 = a_0$, respectively. Then there exists a family of branches $\alpha + \beta$ of $X + Y$ at $(a_0, a_1 + b_1)$ such that*

$$\tau_n(X_t + Y_s, \alpha_t + \beta_s)(x) = F_n(\tau_n(X_t, \alpha_t)(x), \tau_n(Y_s, \beta_s)(x))$$

if $\tau_n(X_t, \alpha_t)$ and $\tau_n(Y_s, \beta_s)$ are defined. In particular, if $n = 1$,

$$\tau_1(X_t + Y_s, \alpha_t + \beta_s)(x) = \tau_1(X_t, \alpha_t) + \tau_1(Y_s, \beta_s).$$

Proof. As in the proof of Proposition 3.7, this statement follows from the unfolding of the definitions. Reasoning locally, assume that α is cut out by the equation $y - f, f \in k[[x]] \otimes \mathcal{O}_{T,t}$ near t , β is cut out by $z - g, g \in k[[x]] \otimes \mathcal{O}_{S,s}$ near s . Then $\alpha + \beta$ is cut out by $y - F(f(x), g(x))$ near $(t, s) \in T \times S$. Checking that the latter power series indeed define a family of branches of $X + Y$ is straightforward and we leave it to the reader. \square

3.2 Flat families and definability of tangency

In the present section we prove the main technical result of the paper, Proposition 3.15, characterizing the tangency of two generic elements of two families of curves in terms of properties of the families definable in the reduct \mathcal{M} . While we

do not give a full definable characterization of the tangency, we prove a standard weakening of this result, which, as we will see in the concluding section of the paper, is sufficient for our needs.

The key preliminary step is the observation that if $X \subset M^2 \times T$, $Y \subset M^2 \times S$ are families of pure-dimensional curves and M, T, S are smooth, then the ‘family of intersections’ $X \times_{M^2} Y \rightarrow T \times S$ is flat if restricted to the open subset of $T \times S$ over which it has finite fibres. We refer the reader to any standard exposition of flatness, such as [28, I.§2], for details, and quickly recall some of the key facts. All schemes in this section are assumed Noetherian, and by varieties we mean schemes of finite type over an algebraically closed field k . We identify closed scheme-theoretic points of varieties with geometric points (that is, morphisms $\text{Spec } k \rightarrow X$).

First recall that a morphism $f : X \rightarrow Y$ is flat if all local rings $\mathcal{O}_{X,x}$ are flat $\mathcal{O}_{Y,f(x)}$ -modules. In particular, flatness can be checked Zariski locally on the source: if $X = \bigcup_{i=1}^n O_i$ is an open cover and O_i is flat over Y for all i then X is flat over Y [36, Tag 01U5].

Fact 3.10 (Generic Flatness, [10, IV.6.10-11]). *Let Y be an integral scheme and let $f : X \rightarrow Y$ be a dominant morphism of finite type. Then there exist open subsets $O \subset X, U \subset Y$ such that $f|_O : O \rightarrow Y, f|_{f^{-1}(U)} : f^{-1}(U) \rightarrow U$ are flat.*

Fact 3.11 ([28, Propositions I.2.4-5], [36, Tag 05BC], [36, Tag 02KB]).

- (i) *an open immersion is flat;*
- (ii) *a composition of flat morphisms is flat;*
- (iii) *let $X \rightarrow Y$ be a flat morphism and let $Z \rightarrow Y$ be a morphism. Then $X \times_Y Z \rightarrow Z$ is flat;*
- (iv) *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;*
- (v) *a finite morphism $f : X \rightarrow Y$ is flat if and only if f is a locally free morphism, that is, if $f_*\mathcal{O}_X$ is a locally free \mathcal{O}_Y -module;*
- (vi) *if A is an algebra and $I \subset A$ is an ideal, then the completion $\varprojlim A/I^n$ is flat over A .*

Lemma 3.12. *Assume that the total space X of a family of pure-dimensional curves $X \subset M^2 \times T$ is a variety. Then X flat over T .*

Proof. By definition of a family of pure-dimensional curves X is open in \bar{X} , so by Fact 3.11(i) and (ii) suffices to show flatness of \bar{X} over T . Passing to a cover of $M^2 \times T$ by affine opens $O_i = \text{Spec } B_i$ suffices to show flatness of $\bar{X} \cap O_i$ over T for all i . But this immediately follows from the definition of a family of pure-dimensional curves and Fact 3.11(iv). \square

Lemma 3.13. *Let M be a smooth algebraic curve, T, S be smooth varieties, $X \subset M^2 \times T$, $Y \subset M^2 \times S$ be families of pure-dimensional curves, and assume that X, Y are varieties. Let $U \subset T \times S$ be the set of points u such that $\dim(X \times_{M^2} Y)_u = 0$, let $Z = X \times_{M^2} Y \cap p^{-1}(U)$, where p is the projection onto $T \times S$. Then the restriction $p : Z \rightarrow U$ is flat.*

Proof. By Lemma 3.12, X is flat over T . Since M, T, S are smooth and since regular local rings are unique factorization domains, and Y is pure-dimensional, Y is cut out in $M^2 \times S$ by a principal ideal sheaf (see, for example, [26, §19, Theorems 47, 48]). Since $X \rightarrow T$ is flat, by Fact 3.11(iii) $X \times S \cong X \times_T (T \times S) \rightarrow T \times S$ is flat too. Since X is pure-dimensional, the natural closed embedding $X \times_{M^2} Y \rightarrow X \times S$ is also cut out by a principal ideal sheaf \mathcal{I} , passing by virtue of Fact 3.11(i) to a cover of $X \times S$ by affine opens $O_i = \text{Spec } B_i$ and applying Fact 3.11(iv) to the algebras B_i , this closed subscheme is flat precisely over the complement of the subvariety of $T \times S$ consisting of the points u such that the local generator of \mathcal{I} does not vanish on an irreducible component of the fibre $(X \times S)_u$. In other words, it is flat over the open subset of points $u \in T \times S$ such that $(X \times_{M^2} Y)_u$ is zero-dimensional. \square

Recall that a morphism $f : X \rightarrow Y$ is called *finite* if for any affine open $U = \text{Spec } R \subset Y$ the inverse $f^{-1}(U) = \text{Spec } S$ is affine and S is a finite R -module. A morphism is finite if and only if it is quasi-finite and proper ([9, EGA IV.18.12.4]).

Lemma 3.14. *Let $f : X \rightarrow Y$ be a quasi-finite morphism of schemes over an algebraically closed k . Consider the functions*

$$\begin{aligned} m : Y(k) &\rightarrow \mathbb{Z} & y &\mapsto \#(f^{-1}(y)), \\ w : X(k) &\rightarrow \mathbb{Z} & x &\mapsto \dim_k \mathcal{O}_{X,x} \otimes k(f(x)). \end{aligned}$$

Then

(i) $w(x) = \dim_{k(x)} \widehat{\mathcal{O}_{X,x}} \otimes k(f(x))$ where $\widehat{\mathcal{O}_{X,x}}$ is the completion $\varprojlim \mathcal{O}_{X,x}/I^n$ for any ideal $I \subset \mathcal{O}_{X,x}$;

(ii) assume that f is flat. Then m is lower semi-continuous and w is upper semi-continuous, that is, the lower level sets of m and the upper level sets of w

$$\{ y \in Y \mid m(y) \leq n \} \text{ and } \{ x \in X \mid w(x) \geq n \}$$

are closed; $y \mapsto \sum_{x \in f^{-1}(y)} w(x)$ is lower semi-continuous and is locally constant if f is finite.

Proof. Let J , resp. \hat{J} , be the ideal of $\mathcal{O}_{X,x}$, resp. $\widehat{\mathcal{O}_{X,x}}$, generated by the image of the maximal ideal of $\mathcal{O}_{Y,f(x)}$, then $\mathcal{O}_{X,x} \otimes k(f(x)) \cong \mathcal{O}_{X,x}/J$. We have a sequence of isomorphisms

$$\mathcal{O}_{X,x} \otimes k(f(x)) \cong \mathcal{O}_{X,x}/J \cong \widehat{\mathcal{O}_{X,x}}/\hat{J} \cong \widehat{\mathcal{O}_{X,x}} \otimes k(f(x))$$

where the first and the third one are tautological, and the second morphism is an isomorphism because \hat{J} is the completion of J in the I -adic topology. This proves claim (i).

That m is lower semi-continuous follows from [9, EGA IV.3.15.5.1(i)] and the fact that flat morphisms of finite type are universally open [9, EGA IV.2.4.6]. Upper semi-continuity of w follows from [36, Tag 0F3D3] and [36, Tag 0F3I] (note that the definition of w from the statement of the Lemma and one from [36] coincide on the closed scheme theoretic points of a variety over an algebraically closed field). Lower semi-continuity of $\sum_{x \in f^{-1}(u)} w(u)$ follows from [36, Tag 0F3J], that it is locally constant if f is finite follows from the definition of a weighting [36, Tag 0F3A]. \square

We can now formulate our main technical result. Roughly, it states that, in suitably chosen families of curves tangency of two curves is witnessed by a lower number of intersection points:

Proposition 3.15. *Keep notation and assumptions of Lemma 3.13 and assume further that there exists $a \in M^2$ such that X_t, Y_s pass through a for all $t \in T, s \in S$. Let α, β be families of branches at a of X, Y respectively, such that for all $t \in T, s \in S$ the slopes of α_t, β_s are defined. Define*

$$\begin{aligned} n_{\max} &= \max\{n \mid \forall (t, s) \in U(k) \tau_n(X_t, \alpha_t) = \tau_n(Y_s, \beta_s)\} \\ m_{\max} &= \max_{(t,s) \in U(k)} \#(X_t \cap Y_s) \end{aligned}$$

Then

$$\begin{aligned} \{ (t, s) \in U(k) \mid \tau_{n_{\max}+1}(X_t, \alpha_t) = \tau_{n_{\max}+1}(Y_s, \beta_s) \} &\subseteq \\ &\subseteq \{ (t, s) \in U(k) \mid \#(X_t \cap Y_s) < m_{\max} \} \end{aligned}$$

Proof. Consider $Z = X \times_{M^2} Y \cap M^2 \times U$, let $q : Z \rightarrow M^2$ be the natural projection and let $Z = \bigcup_{i=0}^n Z_i$ be the decomposition into irreducible components where $Z_0 = q^{-1}(a)$. We will first show that whenever $p^{-1}(u) \cap Z_0 \cap Z_i \neq \emptyset$ for some $i \neq 0$ we have $\#p^{-1}(u) < \max_{u \in U} \#p^{-1}(u)$. In order to do that we will show that the function $u \mapsto \#p^{-1}(u) \cap (\bigcup_{i \neq 0} Z_i)$ is lower semi-continuous.

The projection $p : Z \rightarrow U$ is flat by Lemma 3.13. By [36, Tag 04PW] the closed embedding $Z_{\text{red}} \rightarrow Z$, where Z_{red} is Z endowed with the canonical reduced structure, is flat. Since the invariant we are interested in does not depend on the scheme structure, by Fact 3.11(ii) we may assume Z reduced. Furthermore, there exists an open embedding $Z \hookrightarrow \bar{Z}$ where \bar{Z} is flat and finite over U . Indeed, let \bar{M} be a smooth proper algebraic curve that contains M as a dense subset and let \bar{X}, \bar{Y} be the closures of X, Y in $\bar{M}^2 \times T$ and $\bar{M}^2 \times S$. Let $\bar{Z} = \bar{X} \times_{\bar{M}^2} \bar{Y} \cap \bar{M}^2 \times U$, let \bar{p} be the natural projection on U and denote \hat{p} its restriction to $\hat{Z} = \bigcup_{i \neq 0} \bar{Z}_i$, where \bar{Z}_i is the irreducible component of \bar{Z} that contains Z_i for each i . By Lemma 3.13 \bar{p} is flat.

By Fact 3.11(v) the morphism \bar{p} is locally free. It is readily seen that $(\bar{p})_*\mathcal{O}_{\hat{Z}}$ is locally free of rank one less than the rank of $(\bar{p})_*\mathcal{O}_{\bar{Z}}$. Indeed, if $W = \text{Spec } A \subset U$ is an affine open such that $(\bar{p})^{-1}(W) = \text{Spec } B$ and B is a free A -module, we have that $B \cong B/\mathfrak{p} \oplus B/\mathfrak{q}$ as A -module, where $\mathfrak{p}, \mathfrak{q} \subset B$ are ideals cutting out $Z_0 \cap (\bar{p})^{-1}(W), \hat{Z} \cap (\bar{p})^{-1}(W)$, respectively. Since $Z_0 \cong U$, in particular $Z_0 \cap (\bar{p})^{-1}(W) \cong W$, and we have that $B/\mathfrak{p} \cong A$, so B/\mathfrak{q} is free. By Fact 3.11(v) again \hat{p} is flat, and by Fact 3.11(i) its restriction to $\hat{Z} \cap Z = \cup_{i \neq 0} Z_i$ is flat. We deduce by Lemma 3.14(ii) that the function $u \mapsto \#p^{-1}(u) \cap (\cup_{i \neq 0} Z_i)$ is lower semi-continuous.

Note that while Z_0 may have non-trivial scheme-theoretic structure, the restriction $p|_{Z_0} : (Z_0)_{\text{red}} \rightarrow U$ is a homeomorphism, so denote $r : U \rightarrow Z_0$ its set-theoretic inverse. Let $w : Z \rightarrow \mathbb{Z}, w(z) = \dim_k \mathcal{O}_{Z,z} \otimes k(p(z))$. We claim that w is constant on the open set $Z' = Z_0 \setminus \cup_{i \neq 0} Z_i$. By Fact 3.11(i) Z' is flat over U and by Fact 3.11(iii) it is flat over the open $p(Z') \subset U$. The restriction $p|_{Z'} : Z' \rightarrow p(Z')$ is still a homeomorphism; we will show that it is a finite morphism.

Note that since U is dense in $T \times S$ it is integral, and since Z' is dense in U , it is integral too. The scheme Z' is of finite type over a field, so clearly quasi-compact, and p is clearly separated (for example, because it is affine), so Zariski's Main Theorem (see [28, Ch. I, Theorem 1.8]) can be applied to p . Therefore, p factors into a composition of an open embedding $i : Z' \rightarrow Z''$ and a finite morphism $p' : Z'' \rightarrow p(Z')$. Since $\tilde{p} = p_{\text{red}}|_{Z'} : Z'_{\text{red}} \rightarrow p(Z')$ is an isomorphism, the morphism $p'' = i_{\text{red}} \circ \tilde{p}^{-1} \circ p'_{\text{red}} : Z'_{\text{red}} \rightarrow Z''_{\text{red}}$ restricts to the identity morphism on Z'_{red} . If $p|_{Z'} : Z' \rightarrow p(Z')$ is not finite then the open embedding i is an isomorphism and p'' is not an isomorphism. Since passing to a closed subscheme preserves finiteness, we may assume Z' to be dense in Z'' . The subset of Z''_{red} where p'' and the identity morphism coincide is closed and contains Z' , so must be the whole of Z'' , which in turn contradicts p'' not being an isomorphism.

Now by Lemma 3.14(ii) w is upper semi-continuous on $Z(k)$ and in particular on Z_0 , but since Z' is flat and finite over U , w is constant on $Z'(k)$. Therefore, w takes the value $w_{\min,0} = \min_{x \in Z_0} w(x)$ on the latter, and if $w(r(u)) > w_{\min,0}$ for some $u \in U$ then $r(u) \in Z_i \cap Z_0$ for some $i \neq 0$ and therefore $\#p^{-1}(u)$ is not maximal. It follows that

$$\{ (t, s) \in U(k) \mid w(r(u)) > w_{\min,0} \} \subseteq \{ (t, s) \in U(k) \mid \#(X_t \cap Y_s) < m_{\max} \}.$$

It is left to prove that

$$w(r(t, s)) > w_{\min,0} \text{ for all } t, s \text{ such that } \tau_{n_{\max}+1}(X_t, \alpha_t) = \tau_{n_{\max}+1}(Y_s, \beta_s).$$

To establish this, it is enough to prove the statement on an affine Zariski open subset $\text{Spec } R \subset U \times M^2$ intersecting Z_0 non-trivially. Let $f, g \in R$ be the equations of $X \times S \cap \text{Spec } R, Y \times T \cap \text{Spec } R$, respectively. Let $I \subset R$ be the ideal of functions that vanish on $q^{-1}(a)$ and let $\hat{R} = \varprojlim R/I^n$.

Let $f = f_1 \cdots f_N, g = g_1 \cdots g_K$ be decompositions into pairwise coprime factors in \hat{R} and let f_α and g_β be those factors that are local equations of α, β . Apply

the Chinese Remainder Theorem (see [2, Ch. 9, ex. 9]) twice: first, to $\widehat{R}/(f, g)$ to get the decomposition

$$\widehat{R}/(f, g) = \bigoplus_{i=1}^N \widehat{R}/(f_i, g),$$

second, to each direct summand $\widehat{R}/(f_i, g)$ to get

$$\widehat{R}/(f, g) = \bigoplus_{i=1}^N \bigoplus_{j=1}^K \widehat{R}/(f_i, g_j).$$

Both applications are justified: since f_i are pairwise coprime in \widehat{R} (that is, $(f_i) + (f_k) = \widehat{R}$ for $i \neq k$), the ideals (f_i, g) are pairwise coprime in $\widehat{R}/(g)$, similarly, for each i , the ideals (f_i, g_j) are pairwise coprime in $\widehat{R}/(f_i, g)$.

Tensoring with $k(u)$ and applying Lemma 3.14(i) we get

$$w(r(u)) = \sum_{i=1}^N \sum_{j=1}^K \dim_{k(u)} \widehat{R}/(f_i, g_j) \otimes k(u).$$

Therefore, if $u = (t, s) \in U(k)$ and $\tau_{n_{\max}+1}(X_t, \alpha_t) = \tau_{n_{\max}+1}(Y_s, \beta_s)$ then by the remark after Definition 3.5

$$\dim_k \widehat{R}/(f_\alpha, g_\beta) \otimes k(u)$$

takes a value strictly greater than the minimum it achieves on $U(k)$. By Fact 3.11(vi) \widehat{R} is a flat R -algebra, and by applying Fact 3.11(iv) twice, as in the proof of Lemma 3.13, $\text{Spec } \widehat{R}/(f_i, g_j)$ is flat over U for all i, j . Since by Lemma 3.14(ii) for each pair of prime factors f_i, g_j the value

$$\dim_k \widehat{R}/(f_i, g_j) \otimes k(u)$$

is upper semicontinuous in u , it follows that $w(r(t, s)) > w_{\min, 0}$ as soon as slopes of order $(n_{\max} + 1)$ of α_t and β_s coincide. \square

4 Interpretation of the field

In the present section we tie together the results obtained above to produce the main result of the paper. We start with some additional technicalities and reductions.

4.1 The group configuration

In stable theories – a model theoretic framework encompassing all structures considered in the present work – certain combinatorial configurations of elements are known to exist only in the presence of an interpretable group or – in a more restrictive setting – an interpretable field. It is by constructing such configurations –

using the “definable intersection theory” developed in the previous sections – that the main theorem of the present paper is proved.

Before describing these configurations in more detail we need some model theoretic preliminaries. As in Section 2, we will specialise the definitions to the setting in which they will be used. As above, we will be working in the full Zariski structure \mathfrak{M} on an algebraic curve M over an algebraically closed field k . We will be mostly concerned with a structure $\mathcal{M} := (M, X)$ where $X \subseteq M^2 \times T \subseteq M^{2+l}$ is the total space of an ample family. Throughout the text by *definable* we mean ‘definable with parameters’.

Definition 4.1. 1. If D is an \mathcal{M} -definable set we let $\dim(D) := \dim(\text{cl}(D))$ where cl denotes the Zariski closure of D .

2. If A is a set of parameters and $a \in M^l$ we denote $\dim(a/A) := \min\{\dim(D) : a \in D\}$ where D ranges over all subsets of D^l \mathcal{M} -definable over A .

3. We say that $a \in M$ is \mathcal{M} -algebraic over A if $\dim(a/A) = 0$. We denote $\text{acl}_{\mathcal{M}}(A) := \{a \in M : \dim(a/A) = 0\}$.

4. We say that a is \mathcal{M} -generic in D over A if $\dim(a/A) = \dim(D)$.

5. We say that a is \mathcal{M} -independent from B over A if $\dim(a/A) = \dim(a/AB)$.

Remark. Note that $\dim(D)$ is (by definition) the same as the algebro-geometric dimension of D . This implies that $\dim_{\mathcal{M}}(a/A) \geq \dim_{\mathfrak{M}}(a/A)$, but there is no need for equality to hold. In particular $\text{acl}_{\mathcal{M}}(A) \subseteq \text{acl}(A)$ where on the right hand side acl is the field-theoretic algebraic closure in k . It follows that \mathfrak{M} -independence (which coincides with the field-theoretic notion of algebraic independence) implies \mathcal{M} -independence, but not necessarily the other way around.

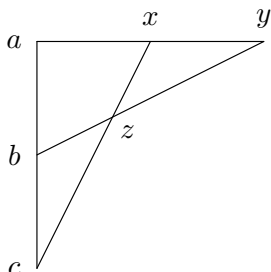
Definition 4.2. An infinite set D definable (or interpretable) in \mathcal{M} is strongly minimal if every \mathcal{M} -definable subset of D is finite or cofinite.

It is an easy exercise to verify that if D is an \mathcal{M} -definable set and $\dim(D) > 1$ then there is a projection $\pi : D \rightarrow M^{\dim(D)-1}$ and an open $U \subseteq M^{\dim(D)-1}$ such that $\pi^{-1}(u) \cap D$ is infinite for all $u \in U$. In particular, D is strongly minimal only if $\dim(D) = 1$. Thus, D is strongly minimal if and only if it is one-dimensional and cannot be written as the disjoint union of two one-dimensional \mathcal{M} -definable subsets. We say that \mathcal{M} is strongly minimal if M is (as an \mathcal{M} -definable set).

Remark. An \mathcal{M} -definable set D may be strongly minimal with respect to the structure \mathcal{M} but not with respect to the structure \mathfrak{M} .

As we will see below, we can easily reduce the proof of our main result to the case where \mathcal{M} is strongly minimal. Under this additional assumption we can finally introduce the group configuration:

Definition 4.3 (Group configuration). *Let \mathcal{M} be as above, and assume that it is strongly minimal. The set $\{ a, b, c, x, y, z \}$ of tuples*



is 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 lying on the same line are dependent, and moreover, $\dim(a, b, c) = 2n$, $\dim(a, x, y) = \dim(b, z, y) = \dim(c, x, z) = n + 1$;

Two group configurations G_1, G_2 are called inter-algebraic if for any pair of tuples $a \in G_1, a' \in G_2$ in the corresponding vertices, $\text{acl}_{\mathcal{M}}(a) = \text{acl}_{\mathcal{M}}(a')$.

Assume that G is a connected \mathcal{M} -definable group acting transitively on a strongly minimal definable set X , then one can construct a group configuration as follows: let g, h be independent generics in G and let u be a generic of X (we will justify the assumption that such generics exist later on), then $(g, h, g \cdot h, u, g \cdot u, g \cdot h \cdot u)$ is a group configuration (associated with the action of G on X). Below (Lemma 4.19) we show that, for a suitably constructed \mathcal{M} -definable family of curves passing through a fixed point, the set of n -th slopes of curves in the family coincide for some n with a one-dimensional algebraic group, H (viewed as acting on itself by multiplication). Proposition 3.15 will then allow us to ‘pull back’ a group configuration (in \mathfrak{M}) associated with this group H into a group configuration in \mathcal{M} . This will, essentially, finish the proof since:

Fact 4.4 (Hrushovski). *Let \mathcal{M} be a strongly minimal structure and let $G_1 = (a, b, c, x, y, z)$ be a group configuration. Then there exists a definable group G acting transitively on a strongly minimal set X .*

This follows from the main theorem of [4] and the fact that infinitely definable groups in stable theories are intersections of definable groups (see, for example, [33, Theorem 5.18]) and the fact that any group definable in an algebraically closed field is (definably isomorphic to) an algebraic group (see [33, Theorem 4.13]). The original proofs of these statements are contained in [12].

To construct a field we will have to work a little harder. First,

Definition 4.5. A group configuration (a_1, a_2, a_3, x, y, z) is minimal if

$$\begin{aligned} \text{acl}_{\mathcal{M}}(\text{Cb}(x, y)/a_1) &= \text{acl}_{\mathcal{M}}(a_1), \\ \text{acl}_{\mathcal{M}}(\text{Cb}(y, z)/a_2) &= \text{acl}_{\mathcal{M}}(a_2), \\ \text{acl}_{\mathcal{M}}(\text{Cb}(x, z)/a_3) &= \text{acl}_{\mathcal{M}}(a_3). \end{aligned}$$

Remark. We will not go into the definition of canonical bases (see, e.g., [31, p.19]), but for the benefit of readers unfamiliar with this model theoretic notion we mention that:

1. The minimality condition is readily checked to be equivalent to the condition that whenever there are $a'_i \in \text{acl}_{\mathcal{M}}(a_i)$ such that $(a'_1, a'_2, a'_3, x, y, z)$ is still a group configuration then $a_i \in \text{acl}_{\mathcal{M}}(a'_i)$ for all $i = 1, 2, 3$.
2. By dimension considerations it follows from the previous remark that any group configuration (a_1, a_2, a_3, x, y, z) gives rise to a minimal group configuration $(a'_1, a'_2, a'_3, x, y, z)$ with $a'_i \in \text{acl}(a_i)$ for all i . In particular, if $\dim(a_i) = 1$ for all i then (a_1, a_2, a_3, x, y, z) is a minimal configuration.
3. Roughly, $\text{Cb}((x, y)/a)$ is the model theoretic analogue of the field of definition of the locus of (x, y) over a .
4. For our purposes it will suffice to know that if $X \rightarrow T$ is a nearly faithful family of curves (see below) then t is (up to inter-algebraicity) a canonical base for x/t for any generic point of x , and if through x_1, \dots, x_k there is only one curve X_t in X then t is (up to inter-algebraicity) a canonical base of (x_1, \dots, x_k) .

For minimal group configurations we have:

Fact 4.6 ([31, Theorem V.4.5]). *If the group configuration in the statement of Fact 4.4 is, additionally, assumed to be minimal then the action of the group G on X as provided above can be taken to be faithful and this group action has an associated group configuration $G_2 = (g, h, g \cdot h, u, g \cdot u, g \cdot h \cdot u)$ inter-algebraic with G_1 . In particular, $\dim G = \dim a$.*

This, finally, allows to obtain a field as follows:

Fact 4.7 (Hrushovski, [12]). *Let G be an \mathcal{M} -definable group acting transitively and faithfully on a strongly minimal set X . Then either $\dim(G) = 1$ or there exists a definable field structure on X and either $\dim(G) = 2$ and $G \cong \mathbb{G}_a \rtimes \mathbb{G}_m$, or $\dim(G) = 3$ and $G \cong \text{PSL}_2$.*

An exposition of the above fact can be found in [33] (Theorem 3.27). Establishing that G is isomorphic to $\mathbb{G}_a \rtimes \mathbb{G}_m$ or to PSL_2 is the crucial point in the proof of Fact 4.7. In the present context, where G and X are definable in an algebraically closed field (rather, the full Zariski structure on an algebraic curve) this statement can be established using a simpler direct algebraic proof.

4.2 Some standard reductions

We make some standard simple reductions that will allow us to more easily use the results obtained in the previous sections as well as the group and field configurations described above.

Lemma 4.8. *We may assume that k is of infinite transcendence degree (over the prime field).*

Proof. Let $K \geq k$ be an algebraically closed field extension of infinite transcendence degree. We let $M' := M(K)$, and for any D \mathcal{M} -definable without parameters we let $D' := D(K)$. We obtain a structure $\mathcal{M}' := (M', X')$. By Hilbert's Nullstellensatz and Chevalley's Theorem (see, e.g., [23, Corollary 3.2.8]) X' is ample (if $U \subseteq M$ is an open set witnessing the fact that X is ample then U' witnesses that X' is). Note also that any set S \mathcal{M}' -definable without parameters is of the form D' for some \mathcal{M} -definable set, D .

Assume that a field is interpretable in \mathcal{M}' . This means that there are D, E \mathcal{M}' -definable (without parameters) and parameters $\bar{a} \in K^l$ and $\bar{b} \in K^n$ such that $E_{\bar{b}}$ is an equivalence relation (of the correct arity) and such that $D_{\bar{a}}/E_{\bar{b}}$ is an infinite field. Let $L_{\bar{c}}$ and $A_{\bar{d}}$ be the graphs of multiplication and addition respectively, for L, A \mathcal{M}' -definable without parameters.

Consider the set S of all parameters $(\bar{x}, \bar{y}, \bar{z}, \bar{w})$ such that $E_{\bar{y}}$ is an equivalence relation on $D_{\bar{x}}$ and $L_{\bar{z}}, A_{\bar{w}}$ turn $D_{\bar{x}}/E_{\bar{y}}$ into an infinite field. We claim that S is \mathcal{M}' -definable without parameters. This is easy since, if $C \subseteq M^{r+s}$ is any constructible set then the set $\{v \in M^s : |C_v| < \infty\}$ is uniformly bounded, say by N . So C_v is infinite if and only if $|C_v| > N$, which is a definable property (of v). By Hilbert's Nullstellensatz and Chevalley's Theorem again S has a point in k , meaning that an infinite field is interpretable already in k . \square

In model-theoretic terms the above lemma only means that interpretability of an (infinite) field is a first order property, and therefore preserved under the passage to elementary substructures. The most useful – for our purposes – property of fields of infinite transcendence degree is the following consequence of Chevalley's theorem and the compactness theorem of first-order logic:

Fact 4.9. *If k is of infinite transcendence degree then any \mathcal{M} -definable set D has generic points over any finite set of parameters A .*

We need the following (weak) version of [38, Theorem B.1.43]:

Fact 4.10. *If \mathcal{M} is strongly minimal and not locally modular then there exists an ample definable family of curves $X \subseteq M^2 \times M^l$ with the property that for any $t \in M^l$ the set $E_t := \{s \in M^l : |X_t \cap X_s| = \infty\}$ is finite.*

For the purposes of the present paper we call an ample definable family of curves as above a *nearly faithful family of curves*. Combined with the (easy) fact that local modularity is preserved under naming parameters ([31, Remark IV.1.8]) this gives:

Fact 4.11. *If \mathcal{M} is strongly minimal and not locally modular then there exists a nearly faithful ample family whose generic members are all strongly minimal subsets of M^2 .*

We can now show:

Lemma 4.12. *We may assume that M is a smooth curve and that \mathcal{M} is strongly minimal.*

The proof is well known (see, e.g., [31, Lemma IV.1.7] for a much more general statement). For the sake of completeness we outline a simple proof in the present context.

Proof. Clearly, if S is an \mathcal{M} -definable set, \mathcal{S} the structure with universe S and definable sets $D \cap S^l$ (as D ranges over $\text{Def}(\mathcal{M})$ and l ranges over $\mathbb{N}_{>0}$), then, if a field F is interpretable in \mathcal{S} , then F is already interpretable in \mathcal{M} . So it will suffice to show that there exists a strongly minimal set $S \subseteq \mathcal{M}$ that is not locally modular with respect to the induced structure \mathcal{S} .

Let $X \subseteq M^2 \times T$ be an ample family witnessed by an open $U \subseteq M^2$. Reducing U , if needed, we may assume that if $U_i := p_i(U)$ are the projections of U onto the two M factors, then for all $a, a' \in U_1$ the fibre $\pi_1^{-1}(a) \cap U$ is infinite and $(\pi_1^{-1}(a) \cap U) = (\pi_1^{-1}(a') \cap U)$ (up to a finite set) for all $a, a' \in U_1$. Thus, setting $Y = X \circ X^{-1}$ we immediately see that Y is ample witnessed by $U_1 \times U_1$.

Since U_1 is \mathcal{M} -definable and one-dimensional there exists some strongly minimal $M_0 \subseteq U_1$. It is clear that $Y \cap (M_0^2 \times T^2)$ is an ample family in \mathcal{M} . It would be an ample family in the induced structure on M_0 if we could replace T with some $T_0 \subseteq M_0^r$ (for some r).

Recall that an irreducible algebraic curve of degree d is uniquely determined by any $d + 1$ generic enough points on the curve. A similar argument would show that any curve in $Y \cap (M_0^2 \times T^2)$ is uniquely determined (up to a finite set) by finitely many generic enough points on the curve. More specifically, by the previous fact we may assume that X is nearly faithful. So if X_t is a curve and $p \in X_t$ is generic then $\dim(p/t) = 1$, so $\dim(p/t) < \dim(p/\emptyset)$ and by symmetry, $\dim(t/p) < \dim(t/\emptyset)$. Proceeding in a similar way, we get that $\dim(t/p_1, \dots, p_r) = 0$ for $r = \dim(T)$ and $p_1, \dots, p_r \in X_t$ generic enough. So there are only finitely many t' such that $p_1, \dots, p_r \in X_{t'}$ and by adding enough points we can assure that X_t is uniquely determined (up to a finite set) by some $p_1, \dots, p_l \in X_t$. We leave it to the reader to verify that the number l of points determining the curve can be taken to be independent of t . Since any X_t has infinitely many points in M_0^2 we get that M_0 , with the induced structure, is, indeed, strongly minimal and not locally modular. Replacing M_0 with $M_0 \cap M_{reg}$, the regular locus of M_0 , the conclusion follows. \square

To sum up:

Corollary 4.13. *To prove Conjecture A it suffice to prove: Let \mathcal{M} be a strongly minimal reduct of the full Zariski structure \mathfrak{M} on a smooth algebraic curve M over an algebraically closed field K of infinite transcendence degree. Then either \mathcal{M} is locally modular or \mathcal{M} interprets a field K -definably isomorphic to K . Moreover, we may assume that the lack of local modularity of \mathcal{M} is witnessed by a nearly faithful family of curves whose generic members are strongly minimal.*

4.3 Generically unramified projections

In order to apply the machinery of slopes and tangency discussed in Section 3.1 we need to produce, definably in \mathcal{M} , large enough families of curves where these notions are defined and carry information. Lemma 4.14 below guarantees the former requirement, namely that for any curve $X \subset M^2$ the slope is defined on a dense open subset of either X or X^{-1} (uniformly in parameters). The second requirement is more delicate, as pointed out for example in the concluding remarks of [24]. In more technical terms, the problem pointed out by Marker and Pillay is that if the projection $p_2 : Z \rightarrow M$ is everywhere ramified for a curve $Z \subset M^2$ (e.g. the curve cut out by the equation $y = x^p$ in $\mathbb{A}^1 \times \mathbb{A}^1$) then even if p_2 is dominant, $\tau_1(Z, \alpha) = 0$ for any branch α at any point of Z . In Lemma 4.16 and Lemma 4.15 we develop the tools allowing us to construct, definably in \mathcal{M} , curves in M^2 whose projections on both factors M are generically unramified.

The following lemma ensures that at least one of the projections on a factor M of a family of curves is generically étale for a general element of the family, which by Lemma 3.4 implies existence of slopes for a generic element of the family. The fact that the support of the module of Kähler differentials is closed and Fact 3.10 imply that being étale and being unramified is open on the source. In particular, in order to check whether a dominant morphism $f : X \rightarrow Y$ is étale on a dense open subset of X it suffices to check if $\Omega_{k(X)/k(Y)} = 0$, or equivalently (see [22, Exercise 6.2.9], also [22, Lemma 6.1.13]), if $k(X) \supset k(Y)$ is a separable extension. We refer the reader to any standard algebraic geometry reference (e.g. [22, Section 6], [11, Section II.8,IV.2]) for the details on Kähler differentials and ramification.

Lemma 4.14. *Let M be an irreducible algebraic curve over a field of any characteristic. Let $X \subset M^2 \times T$ be a family of pure-dimensional curves, and assume that X and T are irreducible. Then there exists a dense open subset $T' \subseteq T$ such that either $p_1 : X_t \rightarrow M$ or $p_2 : X_t \rightarrow M$ is generically étale for all $t \in T'$.*

Proof. Let ξ be the generic point of T in the scheme-theoretic sense. Denote $M_\xi = M \otimes k(\xi)$, $X_\xi = X \otimes k(\xi)$. By slightly abusing notation, denote $p_1, p_2 : X_\xi \rightarrow M_\xi$ the natural projections.

Let $\Omega_{M_\xi/k(\xi)}$, $\Omega_{X_\xi/k(\xi)}$ be the sheaves of modules of Kähler differentials on the generic fibres $M_\xi = M \otimes_k k(\xi)$ and $X_\xi = X \otimes_k k(\xi)$, respectively. Since $\iota : X_\xi \rightarrow M_\xi^2$ is a closed embedding the pull-back

$$\iota^* : p_1^* \Omega_{M_\xi/k(\xi)} \oplus p_2^* \Omega_{M_\xi/k(\xi)} \rightarrow \Omega_{X_\xi/k(\xi)}$$

is surjective. Taking stalks at the generic point χ of X_ξ we get a surjective map of vector spaces over the field $k(\chi) = k(X)$

$$\iota^* : p_1^* \Omega_{M_\xi/k(\xi)} \otimes k(\chi) \oplus p_2^* \Omega_{M_\xi/k(\xi)} \otimes k(\chi) \rightarrow \Omega_{X_\xi/k(\xi)} \otimes k(\chi).$$

Each summand on the left is either trivial or one-dimensional. Since i^* is surjective, it follows that at least one of the summands is mapped surjectively on the destination. Therefore, the stalk at $k(\chi)$ of either $\Omega_{X_\xi/k(\xi)}/p_1^* \Omega_{M_\xi/k(\xi)}$ or $\Omega_{X_\xi/k(\xi)}/p_2^* \Omega_{M_\xi/k(\xi)}$ vanishes, and we conclude. \square

Suppose we have a family of pure-dimensional curves $X \subset M^2 \times T$ such that for some $a \in X_t$ for all $t \in T$, and assume that for all t in the morphism $p_1 : X_t \rightarrow M$ is étale in some neighbourhood of a . Then by Lemma 3.4 there exists a unique branch α of X at a . It might be the case, though, that $\tau_n(X_t, \alpha)$ vanishes for all n , for all $t \in T$, if p_2 is everywhere ramified on the component of X_t that contains a . Below we show that in this case one can consider the family $X \circ X^{-1}$ which does not have this pathology, and p_1, p_2 are both generically unramified for any of its members.

Recall that if $f : X \rightarrow Y$ is a morphism of schemes over a field of characteristic p then $\text{Fr}_f : X \rightarrow X^{(p/Y)} = X \times_{f, Y, \text{Fr}_Y} Y$, the *relative Frobenius morphism*, is defined to be $\text{Fr}_X \times f$ where Fr_X, Fr_Y are the absolute Frobenius endomorphisms of X, Y , respectively. If Y is the spectrum of a field then $X^{(p/Y)}$ is denoted just $X^{(p)}$. If $X = \text{Spec } R, Y = \text{Spec } S, S = R[r_1, \dots, r_n]/I$ then $X^{(p/Y)} = R[r'_1, \dots, r'_n]/I^{(p)}$ where $I^{(p)} = \{ f^{(p)} = \sum_J a_J^p (r'_J)^J \mid f = \sum_J a_J r^J \in I \}$ (where J is a multiindex), and $\text{Fr}_{X/Y}^*(r'_i) = r_i^p$. On the level of points, if $X \hookrightarrow Y \times \mathbb{A}^n$ then

$$\text{Fr}_{X/Y}(y, x_1, \dots, x_n) = (y, x_1^p, \dots, x_n^p).$$

The natural projection $\text{Fr}_{X/Y}(X) \rightarrow Y$ is given by $(y, x_1, \dots, x_n) \mapsto y$.

Lemma 4.15. *Let $f : X \rightarrow Y$ be a finite morphism of irreducible varieties over a field of characteristic $p > 0$ and let $F = \text{Fr}_f$ be the relative Frobenius morphism. Assume that f is everywhere ramified. Then there exists an $n > 0$ such that the natural projection $F^n(X) = X \times_{f, Y, F^n} Y \rightarrow Y$ is generically unramified.*

Proof. Since f is everywhere ramified, the field extension $k(Y) \subset k(X)$ is inseparable. Let L be the separable closure of $k(Y)$ in $k(X)$, then $k(Y) \subset L$ is a separable extension and $L \subset k(X)$ is a purely inseparable extension. Since $L \subset k(X)$ is a finite extension, there exists a smallest number n such that $h^{p^n} \in L$ for any $h \in k(X)$. We claim that $k(F^n(X)) \subset L$, which will conclude the proof, as this shows that $k(F^n(X))$ is a separable extension of $k(Y)$.

To prove the above claim, let $X_0 \subset X, Y_0 \subset Y$ be dense open affine subvarieties such that X_0 is finite over Y_0 . Then $k[X_0] = k[Y_0][h_1, \dots, h_n]/I$ and $k[F^n(X_0)] = k[Y_0][g_1, \dots, g_n]/I^{(p^n)}$, and there is an embedding of rings $k[X_0] \subset k(X_0)$. It is immediate from the definition of the relative Frobenius morphism that there exists an injection $k[F^n(X_0)] \hookrightarrow L$ sending g_i to $h_i^{p^n}$, so $F^n(X_0)$ is unramified over Y_0 and we conclude. \square

Lemma 4.16. *Let $X \subset M^2 \times T$, $Y \subset M^2 \times S$ be two families of pure-dimensional curves. Let us denote projections of $M \times M \times T$, resp. $M \times M \times S$, on products of factors by q , resp. q' , with subscripts. Let $m > 1$ be an integer and let $X' = F_{q_{23}}^m(X)$, $Y' = F_{q'_{23}}^m(Y)$. Then*

$$X \circ Y^{-1} = X' \circ (Y')^{-1}.$$

Proof. Let us denote projections from $M \times M \times M \times T \times S$, $M \times M^{(p^m)} \times M \times T \times S$, onto products of factors by r , resp. r' , with subscripts. After unravelling the definitions one observes that

$$X \circ Y^{-1} = r_{1345}(Z) \quad X' \circ (Y')^{-1} = r'_{1345}(\text{Fr}_{r_{1345}}(Z))$$

for $Z = r_{1245}^{-1}(X \times S) \cap r_{2345}^{-1}(Y^{-1} \times T) \subset M^3 \times T \times S$. These projections coincide, since by the definition of the relative Frobenius morphism $r'_{1345} \circ \text{Fr}_{p_{1345}} = r_{1345}$. \square

For the benefit of the reader, let us consider the situation in Lemma 4.16 at the level of points. Denote by $F : M \rightarrow M^{(p)}$ the Frobenius morphism and assume M is affine and cut out by the equation $f(x_1, \dots, x_n)$ in \mathbb{A}^n , then $M^{(p)}$ is cut out by $f(x_1^p, \dots, x_n^p) = f^p$, and a point (x_1, \dots, x_n) is sent by F to (x_1^p, \dots, x_n^p) . The map $\text{Fr}_{q_{23}}$ in Lemma 4.16 sends a tuple $(x, y, t) \in M^2 \times T$ to $(F(x), y, t)$ and similarly for $\text{Fr}_{q'_{23}}$. By definition

$$\begin{aligned} (b, a, t) \in Y & \text{ if and only if } (F(b), a, t) \in Y', \\ (b, c, s) \in X & \text{ if and only if } (F(b), c, s) \in X'. \end{aligned}$$

Consider

$$Z = \{ (a, b, c, t, s) \mid (b, a, t) \in X, (b, c, s) \in Y \}$$

then

$$X \circ Y^{-1} = \{ (a, c, t, s) \in M^2 \times T \times S \mid \exists b (b, a, t) \in Y, (b, c, s) \in X = p_{1345}(Z) \}.$$

Also, $\text{Fr}_{r_{1345}}(a, b, c, t, s) = (a, F(b), c, t, s)$ and

$$\begin{aligned} X' \circ (Y')^{-1} &= \{ (a, c, t, s) \in M^2 \times T \times S \mid \exists b (F(b), a, t) \in Y', \\ & \quad (F(b), c, s) \in X = p_{1345}(\text{Fr}_{r_{1345}}(Z)) \}. \end{aligned}$$

4.4 Interpretation of a one-dimensional group

In the present section we construct a group interpretable in \mathcal{M} . As already explained, this will be done by constructing a group configuration in \mathcal{M} . In order to construct this group configuration a one-dimensional algebraic group (Lemma 4.19) G associated with slopes is ‘lifted’, using Proposition 3.15, to a group configuration in \mathcal{M} .

Throughout this section and until the end of this paper we fix an algebraic curve M over an algebraically closed field K of infinite transcendence degree, and a reduct \mathcal{M} of the full Zariski structure \mathfrak{M} on M . We assume that the reduct is not locally modular. By default the term *definable* will refer to definability in \mathcal{M} . Unless explicitly stated otherwise, by definable families we mean *stationary* nearly faithful ample families of curves. Where a family $X \rightarrow T$ is *stationary* if every definable open subset of T is dense.

Before we proceed, we need a couple of easy observations:

Lemma 4.17. *Let $r : \text{End}(k[\varepsilon]/(\varepsilon^{n+1})) \rightarrow \text{End}(k[\varepsilon]/(\varepsilon^2))$ be the map sending an endomorphism φ to the endomorphism $\varepsilon \mapsto \varphi(\varepsilon) \pmod{\varepsilon^2}$. Then*

$$\text{Aut}(k[\varepsilon]/(\varepsilon^{n+1})) = r^{-1}(\text{Aut}(k[\varepsilon]/(\varepsilon^2))).$$

Proof. Straightforward (see a similar statement for formal power series, for example, in [7, Corollary 7.17]). \square

Lemma 4.18. *Let $X \rightarrow T$ and $Y \rightarrow S$ be one-dimensional definable families of strongly minimal subsets of M^2 . Assume that for all $t \in T$, $s \in S$ all projections $p_i : X_t \rightarrow M$, $p_i : Y_s \rightarrow M$ are dominant. Then either for generic (t, s) the set $\{(t', s') : |X_{t'} \circ Y_{s'} \cap X_t \circ Y_s| = \infty\}$ is finite or \mathcal{M} interprets a one-dimensional group.*

Proof. Fix (t, s) generic. Since any curve in $X \circ Y$ intersecting $X_t \circ Y_s$ in an infinite set must contain (up to a finite set) a strongly minimal component of $X_t \circ Y_s$, and since only finitely many such components exist, it will suffice to show that any such component is contained in finitely many members of $X \circ Y$.

Let $E \subseteq X_t \circ Y_s$ be strongly minimal. By (the proof of) [8, Lemma 3.20] either \mathcal{M} interprets a one-dimensional group or $\dim_{\mathcal{M}}(\text{Cb}_{\mathcal{M}}(E/\emptyset)) = 2$ (the latter notation can be interpreted, equivalently, as: there exist an \mathcal{M} -definable nearly faithful family of curves defined over a two-dimensional parameter set and E is generic in that family). We may assume the latter case occurs. So, by obvious dimension considerations $s, t \in \text{acl}_{\mathcal{M}}(\text{Cb}_{\mathcal{M}}(E/\emptyset))$. So there are only finitely many (t', s') such that $E \subseteq X_{t'} \circ Y_{s'}$, which is what we had to show. \square

Remark. Recall that our aim in this section is to interpret in \mathcal{M} a strongly minimal group G . It follows from the previous lemma that one way of achieving this is to find $X \rightarrow T$ and $Y \rightarrow S$ one-dimensional definable families of strongly minimal subsets of M^2 with the property that $\{(t', s') : |X_{t'} \circ Y_{s'} \cap X_t \circ Y_s| = \infty\}$ is infinite. In order not to overload the formulation of the sequel we will tacitly assume that, whenever Lemma 4.18 is invoked, this is not the case – as otherwise we have found our group, and we can move on to the next section.

We now proceed to finding the 1-dimensional algebraic group of slopes needed for the construction of the group configuration:

Lemma 4.19. *There exists a nearly faithful definable family $Y \subset M^2 \times S$ with S strongly minimal, a locally closed irreducible set $S_0 \subset S$, a point $a = (a_1, a_2) \in M^2$, $a_1 = a_2$, such that $a \in Y_s$ for all $s \in S_0$, and a family of branches β of $Y \times_S S_0$ at a such that for some $n > 0$ the locally closed set*

$$\{ \tau_n(Y_s, \beta_s) \mid s \in S_0 \}$$

almost coincides with a one-dimensional connected subgroup $H \subset \text{Aut}(k[x]/(x^{n+1}))$.

Proof. Fix some nearly faithful definable family $X \subseteq M^2 \times T$ witnessing non local modularity of \mathcal{M} and such that X_t is strongly minimal for generic $t \in T$, as provided by Fact 4.11. We may further require that the fibres $\pi_i^{-1}(a)$ for both projections of X_t on the factors M are finite for all $a \in M$.

Pick an irreducible component X' of X dominant over an irreducible component $T_0 \subset T$ of maximal dimension, and such that X' is a family of curves. Let M_0 be the connected component of M such that $M_0^2 \times T_0$ contains X' . By Lemma 4.14 applied to the closure of X' , without loss of generality, we may assume that the restriction of p_1 to X'_t is dominant and generically étale for t in a dense subset $T_1 \subset T_0$. By Lemma 4.15 there exists a number m such that the restriction of p_{23} to $X'' = \text{Fr}_{p_{23}}^m(X') \cap M_0^2 \times T_1$ is generically unramified, and since X' is nearly faithful, the projection is also dominant. In particular for any $t \in T_1$ the projection $p_2 : X''_t \rightarrow M_0$ is generically unramified.

For each $a \in M_0^2$ consider the set $S^a \subset T_1$ of $t \in T_1$ such that $a \in X''_t$ and denote $X^a = X \cap M^2 \times S^a$. Let $U \subset X''$ be the complement of the ramification locus of the restriction of p_{23} to X'' . It follows from dimension considerations that there exists $a \in M_0^2$, and an irreducible locally closed subset $S_0 \subset S^a$ such that $\dim S_0 = 1$, $\{a\} \times S_0 \cap U$ is dense in $\{a\} \times S_0$, and $a \in X''_t$ is smooth for $t \in S_0$. Because $a \in X''_t$ is smooth for any $t \in S_0$, there exists by Lemma 3.4 a unique family of branches α of $X'' \cap M_0^2 \times S_0$ at a . Then $\tau_1(X''_t, \alpha_t) \neq 0$ for t in a dense open subset of S_0 by the choice of S_0 , and so by Lemma 4.17 $\tau_n(X''_t, \alpha_t) \in \text{Aut}(k[x]/(x^{n+1}))$ for all $n \geq 1$ for all $t \in S_0$. Pick some $t_0 \in S_0$ generic over all the data and let $Y = X^a \circ X_{t_0}^{-1}$. Then by Lemma 4.16 $X \circ X_{t_0}^{-1} \cap M_0^2 \times S_0 = X'' \circ (X''_{t_0})^{-1}$ and $\tau_1(Y_t, \alpha_t \circ \alpha_{t_0}^{-1}) = \tau_1(X''_t \circ (X''_{t_0})^{-1}, \alpha_t \circ \alpha_{t_0}^{-1}) \in \text{Aut}(k[x]/(x^{n+1}))$ for t in a dense open subset of S_0 . Clearly, $\alpha \circ \alpha_{t_0}^{-1}$ is a family of branches at a point $(a_1, a_2) \in M_0^2$ such that $a_1 = a_2$.

By Krull's Intersection theorem and since S_0 has non-zero dimension, there exists a smallest number n such that $|\{\tau_n(X_t, \alpha_t) : t \in S_0\}| > 1$. If $n = 1$ then $\{\tau_n(X_t, \alpha_t) : t \in S_0\}$ coincides with a one-dimensional subgroup of $\text{Aut}(k[x]/(x^2)) \cong k^\times$ up to a finite set. If $n > 1$ then the slope $\tau_{n-1}(X'_t, \alpha_t)$ as t ranges in S_0 is constant, and therefore $\tau_{n-1}(Y_t, \alpha_t \circ \alpha_{t_0}^{-1}) = 1$. It follows that $\tau_n(Y_t, \alpha_t \circ \alpha_{t_0}^{-1})$ almost coincides with $\text{Ker}(\text{Aut}(k[x]/(x^{n+1})) \rightarrow \text{Aut}(k[x]/(x^n)))$. In either case the family Y satisfies the main part of the lemma over the irreducible component S_0 . Near faithfulness of Y follows from Lemma 4.18 applied to X^a and $(X^a)^{-1}$, observing that Y is a subfamily of $X^a \circ (X^a)^{-1}$, and that a generic member of Y is generic (over a , not over a, t_0) in $X^a \circ (X^a)^{-1}$. \square

Before proceeding to the construction of a group in \mathcal{M} we need some more preliminary work. First, we fix some *ad hoc* terminology and notation that will simplify the discussion:

Notation Let $X \rightarrow T$ be a definable family of curves in M^2 . We denote:

1. For $a \in M^2$ let $T^a := \{X_t : a \in X_t\}$ be the definable sub-family of all curves incident to the point a .
2. $X^0 := \{X_t^0 : t \in T\}$ where X_t^0 is the set of algebro-geometric 0-dimensional components of X_t .
3. $X^1 \subseteq X \times_T T'$ is a family of pure-dimensional curves for a dense $T' \subseteq T$, as provided by Lemma 3.2.

Definition 4.20. We say that a nearly faithful \mathcal{M} -definable family of curves $X \rightarrow T$ satisfies property (a, n) for $a \in M^2$ and a positive integer n if:

1. $a \in X_t$ for all t .
2. There exists a family β of branches of X at a such that $\{\tau_n(X_t, \beta_t) : t \in T\}$ is one-dimensional and contains, up to a finite set, a one-dimensional connected algebraic group, H .
3. For all $a' \in M^2$, if $a' \neq a$ then $\dim(T^{a'}) = 0$.
4. If p belongs to a zero-dimensional component of $X_s \circ X_t$ for $s, t \in T$ \mathfrak{M} -independent generics then p is \mathfrak{M} -generic in M^2 .

The group H is the group of slopes of X at a (associated with the family of branches β).

To show the existence of families that satisfy property (a, n) for some a, n , we need to show:

Lemma 4.21. Let $X \rightarrow T, Y \rightarrow S$ be stationary families. Then there exists $X' \rightarrow T, Y' \rightarrow S$ \mathcal{M} -definable over $\text{acl}_{\mathfrak{M}}(\emptyset)$ such that

1. $X_t = X'_t, Y_s = Y'_s$ up to a finite set, for all $t \in T, s \in S$.
2. If $t \in T, s \in S$ are \mathfrak{M} -independent generics and $a \in X_t \circ Y_s$ is a zero-dimensional component then a is \mathfrak{M} -generic over \emptyset .

Proof. We may assume that for $t \in T$ generic, if a is an isolated component of X_t then $a \notin \text{acl}_{\mathfrak{M}}(\emptyset)$. Otherwise, note that by stationarity (and genericity of t) we get that $a \in X_{t'}$ for all generic $t' \in T$. So $a \in \text{acl}_{\mathfrak{M}}(\emptyset)$. Since there are at most finitely many b incident to all but finitely many $X_{t'}$, we may simply set $X' := (X \setminus \{a\}) \times T$, eliminating the problem in finitely many similar steps.

Similarly, we may assume that if $a = (a_1, a_2)$ is a zero-dimensional component of X_t then $a_1, a_2 \notin \text{acl}_{\mathfrak{M}}(\emptyset)$. Thus, we may assume that both (a_1, a_2) are \mathfrak{M} -generic over \emptyset . The same is, of course, true of Y .

Denoting X_t^0, Y_s^0 the zero-dimensional components of X_t, Y_s and noting that $(X_t \circ Y_s)^0 \subseteq X_t^0 \circ Y_s \cup X_t \circ Y_s^0$ we get that for $s, t \in T$ independent generics any isolated point of $X_t \circ Y_s$ is generic over \emptyset . \square

We have thus shown:

Corollary 4.22. *There exists $a_1 \in M$, a natural number $n > 0$ and a one-dimensional definable family of curves that satisfies property (a, n) for $a = (a_1, a_1)$.*

Proof. Clauses (1) and (2) of the definition of property (a, n) are achieved by taking a family as provided by Lemma 4.19. Condition (4) is provided by Lemma 4.18, and condition (3) is obtained by removing finitely many points common to all generic independent curves in the resulting family. \square

The same proofs give also:

Corollary 4.23. *If $X \rightarrow T$ is a family that satisfies property (a, n) , then up to – possibly – finitely many corrections, $X \circ X$ and $X \circ X^{-1}$ also satisfy property (a, n) .*

Note however that in the above corollary if X is one-dimensional then the families $X \circ X$ and $X \circ X^{-1}$ will not be one-dimensional. It follows, however, that if $t \in T$ is generic then the one-dimensional families $X \circ X_t$ and $X \circ X_t^{-1}$ will satisfy property (a, n) . The following is a strengthening of the above observation that we will need later on for technical reasons:

Lemma 4.24. *Let $X \rightarrow T$ be a family that satisfies property (a, n) . Let H be the group of slopes of X at a (associated with some family of branches). Then there exists a one-dimensional nearly faithful family of strongly minimal sets $Z \rightarrow L$ such that $a \in Z_l$ for all l , and there exists a family of branches γ at Q such that $\tau_n(Z_l, \beta_l) = 1 \in H$ for all $l \in L$.*

Proof. There exists an \mathfrak{M} -irreducible component $W \subseteq T$ such that $\tau_n(X_t, \beta_t) \in H$ for all $t \in W$ (and in particular the slope is defined). Let $t_0 \in W$ be generic. So there exists some $t_1 \in T$ such that $\tau_n(X_{t_1}, \beta_1) = \tau_n(X_{t_0}, \beta_0)^{-1}$. Let $Z_{t_0} \subseteq X_{t_1} \circ X_{t_0}$ be the \mathcal{M} -definable, strongly minimal component containing the branch $\beta_{t_1} \circ \beta_{t_0}$. Let $Z \rightarrow L$ be the \mathcal{M} -definable family whose generic member is Z_l . So there is an \mathfrak{M} -generic sub-family of $Z \rightarrow L$ with the property that $\tau_n(Z_{l'}, \gamma_{l'}) = 1$ (see Proposition 3.7) for a family γ of branches of Z at a and for all l' in that sub-family. \square

We are finally ready to prove the main result of this section:

Theorem 4.25. *Let \mathcal{M} be a non locally modular reduct of an algebraic curve M over an algebraically closed field. Then \mathcal{M} interprets a one-dimensional group.*

Proof. We prove the theorem by constructing a group configuration. By Corollary 4.13 we may assume that M is smooth and we identify M with $M(K)$ for some algebraically closed field K of infinite transcendence degree. We will freely use the remark after Definition 3.3 and Lemma 3.2, referring to branches of suitable pure-dimensional subfamilies of definable families of curves when we speak about branches of definable families of curves.

Let $X \rightarrow T$ be a one-dimensional definable family of curves that satisfies property (a, n) for some point $a = (a_1, a_1)$ as provided by Corollary 4.22, H the associated group of slopes for the family of branches β . Absorbing into the language the parameters needed to define X , we may assume that it is \emptyset -definable.

We fix a standard group configuration

$$\mathcal{H} := \{g, h, k, gh, gk, h^{-1}k\}$$

associated with the action of H on itself by multiplication.

By Lemma 4.19 there exists an irreducible component $W \subseteq T$ such that $\tau_n(X_t, \beta_t) \in H$ for all generic $t \in W$. Identifying (up to a finite set) $\{\tau_n(X_t, \beta_t) : t \in W\}$ with elements of $H \leq \text{Aut}(k[\varepsilon]/(\varepsilon^{n+1}))$ we get that $\tau_n(X_t, \beta_t)$ is \mathfrak{M} -inter-algebraic with t . At the price of replacing W with a (dense) open subset, we may assume that W is smooth.

Any \mathfrak{M} -independent points $s, t \in W$ generic over all the data are, in particular, generic and independent in the sense of the reduct \mathcal{M} . Let $u \in T$ be such that

$$\tau_n(X_u, \beta_u) = \tau_n(X_s, \beta_s)\tau_n(X_t, \beta_t) = \tau_n(X_s \circ X_t, \beta_s \circ \beta_t).$$

Such a u exists, since the relative slopes of X_t and X_s are generic in H , which is one-dimensional. Since the product of two independent generic elements of H is again generic in H , we can find such a u .

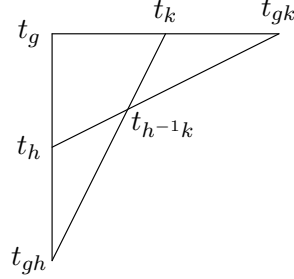
Getting back to our group configuration \mathcal{H} the above construction gives us a subset of T ,

$$\mathcal{T}_{\mathcal{H}} := \{t_g, t_h, t_k, t_{gh}, t_{gk}, t_{h^{-1}k}\}$$

such that for every $s \in \mathcal{H}$ we have $\tau_n(X_{t_s}, \beta_{t_s}) = s$. Our goal is to show that $\mathcal{T}_{\mathcal{H}}$ is a group configuration in the sense of \mathcal{M} .

We have to verify the three sets of conditions appearing in Definition 4.3. That the elements of $\mathcal{T}_{\mathcal{H}}$ are pairwise \mathcal{M} -independent follows from the fact that for all $s \in \mathcal{H}$ also $s \in \text{acl}_{\mathfrak{M}}(t_s)$ and the elements of \mathcal{H} are \mathfrak{M} -independent. That all elements in $\mathcal{T}_{\mathcal{H}}$ have dimension 1 follows from the fact that T is strongly minimal and the elements of $\mathcal{T}_{\mathcal{H}}$ are generic in T . So it remains only to verify the third set of conditions, namely, that every collinear triple of elements in the following diagram

is \mathcal{M} -dependent:



The rest of the proof will be dedicated to that end. Since the situation is symmetric, it will suffice to show that if $s, t \in W$ are generic independent $\tau(X_u, \beta_u) = \tau_n(X_s, \beta_s)\tau(X_t, \beta_t)$ then $u \in \text{acl}_{\mathcal{M}}(s, t)$. Note that since W is \mathfrak{M} -strongly minimal, $u \in \text{acl}_{\mathfrak{M}}(s, t)$.

To achieve our goal, we would like to apply Proposition 3.15 to the family $\tilde{E} \rightarrow R$ given by $X \circ X$ and the family $X \rightarrow T$, in order to show that the curve X_u intersects the curve $X_s \circ X_t$ in a smaller than generic number of points. The problem is that neither $\tilde{E} \rightarrow R$ nor $X \rightarrow T$ can be assumed to be pure-dimensional families of curves, which is a crucial assumption in the statement of the proposition. To circumvent this problem, we will show that $X_u \cap (X_s \circ X_t)$ contains no zero-dimensional components of either curve, allowing us to apply the proposition with the pure-dimensional $\tilde{E}^1 \rightarrow R$ and $X^1 \rightarrow T$ without changing the number of intersection points.

For technical reasons that will be made clear later on, we need to slightly twist the family $\tilde{E} \rightarrow R$ that we are working with. Let $Z \rightarrow L$ be a nearly faithful family of curves that satisfies property (a, m) for $m > n$, let γ be a family of branches at a , all as provided by Lemma 4.24. We let $E \rightarrow R$ be $\tilde{E} \circ Z_{l_0}$ for some $l_0 \in L$ \mathfrak{M} -generic and independent over all the data. Note that, by Proposition 3.7 and the choice of the family $Z \rightarrow L$, we have that $\tau_n(X_s \circ X_t, \beta_s \circ \beta_t) = \tau_n(X_s \circ X_t \circ Z_{l_0}, \beta_s \circ \beta_t \circ \gamma_{l_0})$ whenever both sides of the equations are defined. For the sake of clarity we let α be the family of branches of E at a . Namely, $\alpha = \beta \circ \beta \circ \gamma_{l_0}$.

It will be convenient to already note at this stage the following slight strengthening of Lemma 4.18:

Claim 1 We may assume that if $r \in R$ is generic then $|\{r' : \tilde{E}_r \cap \tilde{E}_{r'}\}| = \infty$ is finite.

Proof. The claim would follow from Lemma 4.18, if the members of X were strongly minimal. In the general case, if $r \in R$ is generic and $\tilde{E}_r = X_s \circ X_t$ then any strongly minimal $F_r \subseteq \tilde{E}_r$ is contained in $C_s \circ D_t$ for some strongly minimal $C_s \subseteq X_s$ and $D_t \subseteq X_t$. By Lemma 4.18 applied to the families $\{D_t : t \in T\}$ and $\{C_s : s \in S\}$, we get that $s, t \in \text{acl}_{\mathcal{M}}(\text{Cb}(F_r))$. Since $\text{Cb}(F_r) \in \text{acl}(\text{Cb}(E_r))$ we conclude that $s, t \in \text{acl}(\text{Cb}(E_r))$, which is what we needed. $\square_{\text{Claim 1}}$

Note that the fact that \tilde{E} is the composition of two copies of X did not play any role in the proof above, and we could invoke Lemma 4.18 with X and $(X \circ Z_{l_0})$ to

get the same conclusion for the family $E := X \circ (X \circ Z_{l_0})$.

Let us fix some additional notation. We let $R(u)$ be the set of all $r \in R$ such that E_r is tangent to X_u at a , i.e., $\tau_n(E_r, \alpha_r) = \tau_n(X_u, \beta_u)$. Let $E(u) := \{E_r : r \in R(u)\}$. In other words, $R(u)$ is the parameter set of all curves in the family $E \rightarrow R$ n -tangent to $X_s \circ X_t$ at a and $E(u)$ is the subfamily of E over the parameter set $R(u)$. So $E(u) \rightarrow R(u)$ is an \mathfrak{M} -definable subfamily of E of dimension 1. Fix, once and for all, $r = (s, t) \in R$. So $r \in R(u)$ and it is \mathfrak{M} -generic as such. Replacing, if needed, $R(u)$ with the \mathfrak{M} -definable strongly minimal component of $R(u)$ containing r we may assume that $R(u)$ is strongly minimal.

The following is the main step in the proof:

Claim 2: Assume that $u \notin \text{acl}_{\mathcal{M}}(s, t)$. Let $\{x_1, \dots, x_k\} = (X_u \cap E_r) \setminus \{a\}$. Then x_i is \mathfrak{M} -generic in X_u for all i .

Proof. First, note that $x_i \notin \text{acl}_{\mathcal{M}}(\emptyset)$, because otherwise, since $u \in T$ is generic, we would get that $\dim(T^{x_i}) = 1$, contradicting clause (3) of Definition 4.20. Note that the exact same argument shows that $x_i \notin \text{acl}_{\mathfrak{M}}(\emptyset)$. Next, as $r \in \text{acl}_{\mathcal{M}}(s, t)$ and since X is an \mathcal{M} -strongly minimal family, our negation assumption implies that u is \mathcal{M} -generic over r and by Lemma 4.18 (and the remark following it) applied to the $\text{acl}(\emptyset)$ -definable strongly minimal subsets of E_r we get that $\dim(\text{Cb}(E_r)/\emptyset) = \dim(r/\emptyset) = 2$.

Now assume that x_1 is not \mathfrak{M} -generic in X_u . Since r is \mathfrak{M} -generic in $R(u)$ (and thus also in R), it follows that $\dim(R(u)^{x_1}) = 1$. Indeed, since $\dim_{\mathcal{M}}(x_1/u) = 0$ (by assumption), it follows that $\dim_{\mathfrak{M}}(r/ux_1) = \dim_{\mathfrak{M}}(r/u)$, so r is generic in $R(u)$ over x_1 , and the strong minimality of $R(u)$ implies that $x_1 \in E_{r'}$ for all generic $r' \in R(u)$. Thus, in fact $R(u)$ is a generic subset of R^{x_1} . Recall, moreover, that there exists a family α of branches of all curves in $E(u)$ at a such that $\tau_n(E(u), \alpha_r) = \tau(X_u, \beta_u)$.

We will show that this gives the desired conclusion. We split the argument into cases according to $\dim_{\mathcal{M}}(x_1/\emptyset)$. The case $x_1 \in \text{acl}_{\mathcal{M}}(\emptyset)$ has already been discarded. If x_1 is non- \mathcal{M} -generic in M^2 then there exists a curve F , \mathcal{M} -definable over \emptyset such that x_1 is generic in F . So u is contained in the set of all u' such that $F \cap X_{u'} \cap E_r \neq \emptyset$. Because $|E_r \cap F| < \infty$ and condition (3) of Definition 4.20, there are only finitely many such u' . So u is \mathcal{M} -algebraic over r – contradicting our assumption.

Thus, we may assume that x_1 is \mathcal{M} -generic in M^2 . We will now focus on the family $E \rightarrow R$. Since x_1 is \mathcal{M} -generic in M^2 , for any $r_1, r_2 \in R^{x_1}$ independent generic, $m := |E_{r_1} \cap E_{r_2}|$ is obtained on an \mathfrak{M} -generic subset of parameters of $R \times R$. Consider the \mathfrak{M} -definable family $E^1 \rightarrow R$ of pure-dimensional curves associated with $E \rightarrow R$. Note that for \mathfrak{M} -generic independent $u, w \in R$ we have $|E_u \cap E_w| = |E_u^1 \cap E_w^1| = m$.

On the other hand, Lemma 3.13, and hence Proposition 3.15, is applicable to two copies of the family $E^1 \rightarrow R$, possibly after shrinking R so as to ensure, using Fact 3.10, that $E^1 \rightarrow R$ is flat and that R is smooth.

So, by Lemma 3.13 and Proposition 3.15 there is a dense open set $W_0 \subseteq R$ defined over \emptyset such that (keeping the above notation) for all $(v, w) \in W := W_0 \times W_0$, if $\tau_n(E_v^1, \beta_v) = \tau_n(E_w^1, \beta_w)$, then either $\dim(E_w^1 \cap E_v^1) = 1$ or $\#(E_w^1 \cap E_v^1) < m$.

For generic v the set of w such that $(v, w) \in W$ and $\dim(E_w^1 \cap E_v^1) = 1$ is finite by Claim 1. So, for generic $(v, w) \in W$ we see that $\dim(E_w^1 \cap E_v^1) = 0$ so necessarily $\#(E_w^1 \cap E_v^1) < m$. We now show that this must imply that $E_w^0 \cap E_r \neq \emptyset$ for generic w . Indeed, since W_0 is dense in R and \emptyset -definable, \mathfrak{M} -genericity of r in R implies that it is also generic in W_0 . Since $R(u)^{x_1}$ is generic in R^{x_1} (in the sense that it contains an open subset of R^{x_1}) we can find some $w \in R(u) \cap W_0$ \mathfrak{M} -generic and \mathfrak{M} -independent from r (over all the data gathered so far) so that (r, w) is \mathfrak{M} -generic in W . Moreover, by definition of $R(u)$ we know that $\tau_n(E_r^1, \beta_r) = \tau_n(E_w^1, \beta_w)$, and by what we have just said, this must imply that $\#(E_w^1 \cap E_r^1) < m$. Because x_1 is \mathcal{M} -generic in M^2 and $w, r \in R^{x_1}$ are \mathcal{M} -independent generics, they are, in fact, independent generic in R^2 over \emptyset . So $\#(E_w \cap E_r) = m$, implying that $E_w \cap E_r^0 \neq \emptyset$.

Finally, since w was \mathfrak{M} -independent from r and \mathfrak{M} -generic in $R(u)$, and since $E_r^0 \subseteq \text{acl}_{\mathfrak{M}}(r)$, we get – precisely as above – that there is some $c \in E_r^0$ such that R^c contains $R(u)$, up to a finite set. This implies that $\dim_{\mathfrak{M}}(c/u) = 0$, and therefore $\dim_{\mathfrak{M}}(c/\emptyset) \leq \dim_{\mathfrak{M}}(u/\emptyset) = 1$. This contradicts Corollary 4.23 (specifically, clause (4) of Definition 4.20). $\square_{\text{Claim 2}}$

It follows from Claim 2 that $X_u^0 \cap E_r = \emptyset$. We also need to show that X_u does not meet E_r in an isolated point of the latter. It is here that the twist of the family $\tilde{E} \rightarrow R$ by a generic curve from $Z \rightarrow L$ plays its role:

Claim 3: If $u \notin \text{acl}_{\mathcal{M}}(s, t)$ then $X_u \cap E_r^0 = \emptyset$.

Proof. Recall that $E_r = X_s \circ X_t \circ Z_{l_0}$. Assume that there exists some $x_i \in X_u \cap (X_s \circ X_t \circ Z_{l_0})^0$. By Lemma 4.21 applied to $\tilde{E}(u) \rightarrow R(u)$ and $Z \rightarrow L$, if $r' \in R(u)$ is generic and $l \in L$ is generic independent from r' , then any $x_i \in (E_{r'} \circ Z_l)^0$ is either \mathfrak{M} -generic over \emptyset or contained in one of finitely many sets of the form $\{a\} \times M$ and $M \times \{a\}$ for $a \in \text{acl}_{\mathfrak{M}}(0)$. But $X_u \cap (M \times \{a\} \cup \{a\} \times M) \subseteq \text{acl}_{\mathfrak{M}}(u)$, so $x_i \in \text{acl}_{\mathfrak{M}}(u)$, contradicting the previous claim. $\square_{\text{Claim 3}}$

The conclusion of the discussion, up to this point, is that if $u \notin \text{acl}_{\mathcal{M}}(s, t)$ then $E_r \cap X_u = E_r^1 \cap X_u^1$. This allows us to conclude that, in fact:

Claim 4: u is \mathcal{M} -algebraic over t, s .

Proof. Assume not. By Proposition 3.7 $\tau_n(X_t \circ X_s \circ Z_{l_0}, \beta_t \circ \beta_s \circ \gamma_{l_0}) = \tau_n(X_t, \beta_t) \circ \tau_n(X_s, \beta_s)$. Let $m = \max_{\bar{t}, \bar{s}, \bar{u} \in T} \#(X_{\bar{t}} \circ X_{\bar{s}} \circ Z_{l_0} \cap X_{\bar{u}})$, then by Lemma 3.14, $m = \#((X_t \circ X_s \circ Z_{l_0}) \cap X_u)$ for (t, s, u) generic in $T \times T \times T$. Let $\tilde{T} \subseteq T$ be as provided by Lemma 4.19. By Lemma 3.13 and Proposition 3.15, the set of parameters $w \in \tilde{T}$ such that $\tau_n(X_w^1, \beta_w) = \tau_n(X_t^1, \beta_t) \circ \tau_n(X_s^1, \alpha_s)$ is contained in

$$W_1 := \{ w \in T \mid \dim(X_t \circ X_s \cap X_w) = 1 \text{ or } \#((X_t \circ X_s \circ Z_{l_0})^1 \cap X_w^1) < m \}.$$

By strong minimality of T the set $\{w : \#(X_t \circ X_s \circ Z_{l_0} \cap X_w) < m\}$ is finite. Also, for \mathfrak{M} -generic w we have $(X_t \circ X_s \circ Z_{l_0})^1 \cap X_w^1 = X_t \circ X_s \circ Z_{l_0} \cap X_w$. So the set of w such that $\#((X_t \circ X_s \circ Z_{l_0})^1 \cap X_w^1) < m$ is finite. Since X satisfies property (a, n) , by Lemma 4.18 the set $\{w : \dim(X_t \circ X_s \circ Z_{l_0} \cap X_w) = 1\}$ is finite. So W_1 is finite. Similarly,

$$W := \{ w \in T \mid \dim(X_t \circ X_s \circ Z_{l_0} \cap X_w) = 1 \text{ or } \#(X_t \circ X_s \circ Z_{l_0} \cap X_w) < m \}$$

is finite, and moreover, W is \mathcal{M} -definable. Our assumption that $u \notin \text{acl}_{\mathcal{M}}(s, t)$ allows us to apply Claim 2 combined with Claim 3 to get that $X_s \circ X_t \circ Z_{l_0} \cap X_u = (X_s \circ X_t \circ Z_{l_0})^1 \cap X_u^1$. Since $u \in W_1$ it follows that $u \in W$, proving that, in fact $u \in \text{acl}(s, t)$. □_{Claim 4}

Claim 4 shows that, indeed, $\mathcal{H}_{\mathcal{T}}$ is an \mathcal{M} -group configuration, and the desired conclusion is obtained by applying Fact 4.4. □

The next proposition can be proved in greater generality (and follows, essentially, from [18, Section 3]), but we only need the following elementary result:

Proposition 4.26. *In the notation of the previous proof, assume that the group H almost coinciding with $\{\tau_n(Y_t, \alpha_t) : t \in \tilde{S}\}$ is isomorphic to \mathbb{G}_a . Then the connected component of the identity of the group from the conclusion of the theorem is not \mathfrak{M} -isomorphic to \mathbb{G}_m .*

Proof. In this proof we will be working solely in \mathfrak{M} . It suffices to show that if

$$G_1 = \{ a, b, a + b, x, x + a, x + b \} \text{ and } G_2 = \{ e, f, e \cdot f, y, e \cdot y, f \cdot y \}$$

are group configurations for the groups \mathbb{G}_a and \mathbb{G}_m , respectively, and $\text{acl}(a) = \text{acl}(e)$, $\text{acl}(b) = \text{acl}(f)$, $\text{acl}(x) = \text{acl}(y)$ then G_1 and G_2 are not inter-algebraic.

Indeed, $\dim(a, b, e + f, ef) = \dim(a, a + b, ef)$, since ef is inter-algebraic with b over a . On the other hand, $\dim(a, a + b, ef) = \dim(a + b, ef)$ since $a + b$ is inter-algebraic with a over ef . □

4.5 Interpretation of the field and proof of the main theorem

In this section we interpret the field K in the reduct \mathcal{M} , concluding the proof of the main theorem of this paper. The results of the previous subsection allow us replace \mathcal{M} with an algebraic group, G , interpretable in \mathcal{M} (we only have to verify that the induced structure is non-locally modular). As in the previous subsection, the interpretation of the field boils down to the construction of a field configuration. The construction of the field configuration will depend on whether the (connected component of the) group G is isomorphic (in K) to \mathbb{G}_a , \mathbb{G}_m or to an elliptic curve. The question to address is how to find an \mathcal{M} -definable strongly minimal $Z \subseteq G^2$ whose set of slopes $\{\tau_1(Z, z) : x \in Z\}$ (see below) is infinite. The easiest is the case of an elliptic curve:

Lemma 4.27. *Let E be an elliptic curve and Z be a closed one-dimensional irreducible subset of $G = E^2$. Identify $T_g G$ with $T_0 G$ via the isomorphism $d\lambda_g : T_0 G \rightarrow T_g G$, for $\lambda_g(x) = g \cdot x$. Suppose that for any $z \in Z$ the tangent space $T_z Z \subset T_0 G$ 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 by the Riemann-Roch formula. Since any morphism between Abelian varieties with finite fibres which preserves the identity automatically preserves the group structure by the Rigidity Lemma (see [29, p. 43]), Z is a coset of an Abelian subvariety of G . \square

To obtain the analogous results for \mathbb{G}_a we first need a couple of technical lemmas. We thank S. Pinzon for pointing out a mistake in an earlier version of the proof. The current proof builds on Pinzon's proof of an analogous statement in ACVF_p .

We start with some notation and terminology. Let M be an algebraic curve, and consider a curve $Z \subset M^2$. For every point $z \in Z$ such that p_1 is étale in a neighbourhood of z , there exists by Lemma 3.4 a unique branch at z , call it α_z . We will use the notation $\tau_n(Z, z) := \tau_n(Z, \alpha_z)$. For any group (G, \cdot) with identity $e \in G$, for any $a = (a_1, a_2) \in G^2$ define the maps $t_a : G^2 \rightarrow G^2$

$$t_a(x_1, x_2) = (a_1^{-1} \cdot x_1, a_2^{-1} \cdot x_2)$$

and for any one-dimensional locally closed subset $Z \subset G^2$ define

$$s_n(Z) = \{ \tau_n(t_z(Z), (e, e)) \mid z \in Z \} \subset k[x]/(x^{n+1}),$$

where z ranges in those points of Z for which n -th order slope is well-defined. Identifying $k[x]/(x^{n+1})$ with the affine n -space we observe that the set $s_n(Z)$ is constructible.

If $Z \subset \mathbb{G}_a^2$ is an irreducible locally closed 1-dimensional set that is not a dense subset of a coset of a subgroup then $s_1(Z)$ is clearly a 1-dimensional set when the characteristic of the ground field is 0. In positive characteristic, $s_1(Z)$ might be 0-dimensional for various reasons.

If Z is a coset of a subgroup of G then all of its translates coincide on an open dense set and therefore slopes of all orders at (e, e) are constant. In particular $\dim s_n = 0$ for all $n \geq 1$. If, however Z is not a coset, $t_z(Z)$ are distinct for different $z \in Z$ and therefore my Krull maximal ideal theorem for some n , $\tau_n(t_z(Z), (e, e))$ will vary depending on $z \in Z$. The following quantity is then well-defined:

$$N(Z) = \min\{ n \geq 1 \mid \dim s_n(Z) = 1 \}.$$

Lemma 4.28. *Let $X \subset \mathbb{G}_a^2 \times T$ be a family of curves parametrized by a curve T , and assume that $\tilde{a} = (a_1, a_2) \in X_t$ for all t in some neighbourhood of $a_3 \in T$. Let x_1, x_2, t be a choice local coordinates of $\mathbb{G}_a^2 \times T$ at $a = (a_1, a_2, a_3) \in X$ such that x_1, x_2 are local coordinates of \mathbb{G}_a^2 at \tilde{a} . Let $f \in k[[x_1, x_2, t]]$ be the local equation of X in $\mathbb{G}_a^2 \times T$ at a . Then $\tau_n(X_t, \tilde{a})$ is constant for t in a neighbourhood of a_3 if and only if $f \equiv f_0 \pmod{x_1^{n+1}}$, where $f_0 \in k[[x_1, x_2]]$.*

Proof. Let \mathcal{I} be the ideal generated by x_1, x_2 in the ring $R := [x_1, x_2] \otimes \mathcal{O}_{T, a_3}$ and let \mathcal{J} be the ideal of the same ring consisting of functions vanishing at the point a . Then $\hat{R} := \varprojlim R/\mathcal{I}^n = k[[x_1, x_2]] \otimes \mathcal{O}_{T, a_3}$ and $\varprojlim R/\mathcal{J}^n \cong k[[x_1, x_2, t]]$ for some formal parameter t and the ideal of functions vanishing on X in R generates an ideal $(\bar{f}) \subset \hat{R}$. Since R is a Noetherian local ring, the natural maps $R \rightarrow \hat{R} \rightarrow k[[x_1, x_2, t]]$ are injective. Let $f \in k[[x_1, x_2, t]]$ be the image of \bar{f} . By the definition of the slope $\tau_n(X_t, \tilde{a})$ depends only on $\bar{f}(t)$ modulo x_1^{n+1} . In particular, $\tau_n(X_t, \tilde{a})$ is constant for t in a neighbourhood of a_3 if and only if $\bar{f} \equiv \bar{f}_0 \pmod{x_1^{n+1}}$ for some $\bar{f}_0 \in k[[x_1, x_2]] \subset \hat{R}$. Let f_0 be the image of \bar{f}_0 in $k[[x_1, x_2, t]]$, then clearly, $f_0 \in k[[x_1, x_2]]$. Since $\bar{f} \equiv \bar{f}_0 \pmod{x_1^{n+1}}$ and since the map $\hat{R} \rightarrow k[[x_1, x_2, t]]$ is injective, $f \equiv f_0 \pmod{x_1^{n+1}}$ if and only if $\bar{f} \equiv \bar{f}_0 \pmod{x_1^{n+1}}$, and the statement follows. \square

Lemma 4.29. *Assume that the ground field is of positive characteristic p . Let $Z \subset \mathbb{G}_a^2$ be an irreducible pure-dimensional curve that is not contained in a coset of a subgroup of \mathbb{G}_a^2 .*

Assume that the characteristic p of the ground field is positive and assume that $(0, 0) \in Z$, and that the projection of a neighbourhood of $(0, 0) \in Z$ on the first \mathbb{G}_a is étale, so Z has a local equation $y - f$, where $f = \sum_{j>0} b_j x^j \in k[[x]]$.

Then we have:

1. $N(Z) = \min\{ p^i \mid \exists b_j \neq 0, j = m \cdot p^i, m \neq 1, p \nmid m \}$;
2. *there exists an open subset $U \subset Z$ such that*

$$\tau_{N(Z)-1}(Z - t_z(Z), (0, 0)) = 0, \quad N(Z - t_z(Z)) = N(Z)$$

for all $z \in U$ and

$$\dim\{\tau_{N(Z)}(Z - t_z(Z), (0, 0)) \mid z \in U\} = 1.$$

Proof. Let the closure of Z be cut out in \mathbb{G}_a^2 by a polynomial equation $P(x, y)$. Pick coordinates x, y, u, v on each of the factors of \mathbb{G}_a^4 . Let $Z' \subset \mathbb{G}_a^4$ be the set cut out by the equation $P(u, v)$ and let $Z'' \subset Z'$ be cut out in Z' by the equation $P(x - u, y - v)$. A fibre of Z'' over $(u_0, v_0) \in \mathbb{G}_a^2$ is thus the closure of $t_{(u_0, v_0)}Z$. We identify the completion of the local ring of Z' at $(0, 0, 0, 0)$ with $k[[x, y, u]]$ via the projection on the first three coordinates. One readily sees that the local equation of Z'' in Z' at $(0, 0, 0, 0)$ is

$$g = y - f(x - u) + f(u) \in k[[y, x, u]]$$

By Lemma 4.28, if $\dim s_n(Z) = 1$ and $\dim s_m(Z) = 0$ for all $m < n$ then a monomial of the form $u^l x^n$ for some $l > 0$ occurs with a non-zero coefficient in g . Substituting the expression for f into the above expression for g we get

$$g = y - \sum_{j>0} b_j \left(\sum_{0 < k \leq j} \binom{j}{k} (-1)^{j-k} u^{j-k} x^k \right),$$

If f contains a term ax^n then its contribution to g is the terms

$$-a \binom{n}{1} ux^{n-1}, a \binom{n}{2} u^2 x^{n-2}, \dots, a \binom{n}{n-1} (-1)^{n-1} u^{n-1} x,$$

and if $n = p^j$ then all their coefficients vanish in a characteristic p field since $\binom{p^j}{k} \equiv 0 \pmod p$ for $k < p^j$. Raising to p^j -th power is additive modulo p , so if $p \nmid m$ then $(x+u)^{mp^j} \equiv ((x+u)^m)^{p^j} \pmod p$ and since $\binom{mp^j}{lp^j}$ is the coefficient of $u^l x^{m-l}$ in $(x+u)^m$ raised to the power p^j , $\binom{mp^j}{lp^j} = \binom{m}{l}^{p^j}$.

In particular, if $n = mp^j$ and $p \nmid m$ then $\binom{mp^j}{p^j} = m^{p^j} \not\equiv 0 \pmod p$ so the term $u^{p^j} x^{(m-1)p^j}$ has a non-zero coefficient in g , which proves the first claim (and more generally $\binom{mp^j}{lp^j} \not\equiv 0 \pmod p$ if $p \nmid m, l$).

Now let W be the closed subvariety of $\mathbb{G}_a^2 \times Z \subset \mathbb{G}_a^4$ such that the fibre of W over a point $z \in Z$ is $Z - t_z(Z)$. Applying the reasoning from the proof of Proposition 3.9 we get that the local equation of W is

$$h = y - f(x-u) + f(u) + f(x),$$

Arguing as above, we see that by Lemma 4.28 to prove the second claim it suffices to show that a monomial of the form $u^j x^{N(Z)}$, $j > 0$ occurs in h with a non-zero coefficient while no monomials of the form $u^j x^n$, $j \geq 0$ occur in h with non-zero coefficients for $n < N(Z)$ (so that $h \equiv y \pmod{x^{N(Z)}}$) and for $n = mp^j$, $p \nmid m$, $p^j < N(Z)$ (so that $N(Z - t_z(Z)) = N(Z)$).

Since the term $x^{mN(Z)}$ occurs in f with a non-zero coefficient, its contribution to $f(x-u) - f(u) - f(x)$ consists of the terms $u^{lN(Z)} x^{N(Z)}$, $0 < l < m$ with non-zero coefficients. And since by definition of $N(Z)$, x^n occurs in f with non-zero coefficient if and only if $n = p^j$ or $n = mp^j$ and $p^j \geq N(Z)$, the statement from the previous paragraph is fulfilled. \square

Lemma 4.30. *Assume that the ground field is of positive characteristic p .*

Let G be an algebraic group such that the connected component of the identity G_0 is isomorphic to \mathbb{G}_a . Let $Z \subset G^2$ be a curve that is not a Boolean combination of cosets of subgroups of G^2 . Then there exists a family of pure-dimensional curves $W \subset G^2 \times Z$ definable in (G, Z) , and an irreducible component $Z_0 \subset Z \cap G_0^2$ of dimension 1, such that

$$\dim\{ \tau_1(W_z, (0,0)) \mid z \in Z_0 \} = 1.$$

Proof. Replacing Z by a shift, we may assume that there exists a pure-dimensional irreducible curve $Z_0 \subset Z$ such that $(0,0) \in Z_0$, Z_0 is not contained in a coset, and such that the projection on the first coordinate in \mathbb{G}_a^2 is étale in a neighbourhood of $(0,0) \in Z$. Consider the definable family of curves $Y \subset G^2 \times Z$ with the fibres

$$Y_z = Z - t_z(Z), z \in Z.$$

For $z \in Z_0$ the slope of Y_z at $(0, 0)$ is well-defined. By Lemma 4.29,

$$\dim\{\tau_{N(Z)}(Y_z, (0, 0)) \mid z \in Z_0\} = 1,$$

and $\tau_{N(Z)-1}(Y_z, (0, 0)) = 0$ for z in a dense subset of Z_0 . It follows that there exists $z' \in Z_0$ such that $\tau_{N(Z)}(Y_{z'}, (0, 0)) \neq 0$. It also follows from the characterization of $N(Z)$ in Lemma 4.29 that the local equation of Y_z is a $N(Z)$ -th power of a power series and therefore, $p_2 : \mathbb{G}_a^4 \rightarrow \mathbb{G}_a$ restricted to $Y' = \text{Fr}_{p_2}^m(Y)$ is generically unramified, where m is such that $p^m = N(Z)$.

In particular, for generic $z \in Z_0$, the restriction of the projection on the second coordinate of \mathbb{G}_a^2 to Y'_z is generically unramified and

$$\dim\{\tau_1(Y'_z, (0, 0)) \mid z \in Z_0\} = 1.$$

Define the family W by putting $W_z = Y_z \circ Y_{z'}^{-1}$. Then by Lemma 4.16, $W_z = Y'_z \circ (Y_{z'})^{-1}$ for z in a dense subset of Z_0 and

$$\tau_1(W_z, (a_2, b_2)) = \tau_1(Y'_z, a) \circ (\tau_1(Y_{z'}, b))^{-1}$$

for all points $a = (a_1, a_2), b = (b_1, b_2) \in Y_z$ such that $a_1 = b_1$ and such that the right-hand side makes sense. The statement of the Lemma follows. \square

Lemma 4.31. *Let G be a one-dimensional algebraic group such that the connected component of the identity G_0 is isomorphic to \mathbb{G}_m . Let $Z \subset G^2$ be a curve that is not a Boolean combination of cosets of subgroups of G^2 . Then either there exists an irreducible pure-dimensional curve $Z_0 \subset Z$ such that $\dim s_1(Z_0) = 1$, or there exists a group definable in (G, Z) such that its connected component of the identity is not isomorphic to \mathbb{G}_m .*

Proof. Pick a local coordinate systems on \mathbb{G}_m , uniformly, as in the proof of Lemma 4.30. Assume that $\dim s_1(Z) = 0$, and so $s_1(Z_i)$ is a singleton for each one-dimensional irreducible component $Z_i \subset Z$. Let Z_0 be one of the irreducible components of Z that is not contained in a coset, then there exists a smallest $n > 1$ such that $\dim s_n(Z_0) = 1$. Then, by the same reasoning as in the proof of Lemma 4.19, we may consider the family $Y \subset G^2 \times Z$ by putting $Y_z = t_z(Z) \circ (t_{z_0}(Z))^{-1}$ for some $z_0 \in Z_0$, so that $\{\tau_1(Y_z, (0, 0)) \mid z \in Z_0\}$ almost coincides with

$$\text{Ker}(\text{Aut}(k[x]/(x^{n+1})) \rightarrow \text{Aut}(k[x]/(x^n))) \cong \mathbb{G}_a.$$

The definable family Y can be used to construct a group configuration as in the proof of Theorem 4.25, and therefore a group is interpretable in (G, Z) . By Proposition 4.26, the connected component of the identity of this group is not isomorphic to \mathbb{G}_m . \square

We can finally interpret the field:

Theorem 4.32. *Let G be a one-dimensional algebraic group over an algebraically closed field, $Z \subset G^2$ a one-dimensional constructible subset that is not a Boolean combination of cosets. Then (G, \cdot, Z) interprets a field.*

Proof. Let G_0 be the connected component of the identity e of G . If $G_0 = \mathbb{G}_a$ or G_0 is an elliptic curve then, by Lemmas 4.27, 4.30, there exists a definable family $Y \subset G^2 \times S$ of curves, S strongly minimal, and an irreducible locally closed set $S_0 \subset S$ such that there is a unique family of branches α of $Y_0 = Y \cap S_0$ at $(e, e) \in G^2$, and such that $\tau_1(Y_s, \alpha_s)$ is not constant as s ranges in S_0 . By Lemma 4.31' either such a family exists, or a definable one-dimensional group G' with the connected component of the identity not isomorphic to \mathbb{G}_m (and therefore isomorphic to either \mathbb{G}_a or to an elliptic curve) is interpretable in (G, \cdot, Z) , and we may prove the theorem for the structure induced on G' . We, therefore, may continue with the assumption that such a family exists. Clearly, $Y_0 \rightarrow S_0$ and we may assume that S_0 is smooth at the price of possibly shrinking S_0 . Further shrinking S_0 we can ensure $Y_0 \rightarrow S_0$ to be flat (by Fact 3.10). Let K be a field of infinite transcendence degree over the base field k . We identify first order slopes, which are truncated polynomials in $k[\varepsilon]/(\varepsilon^2)$ divisible by ε , with K , and we will use multiplicative notation for composition. We will freely use the remark after Definition 3.3 and Lemma 3.2, referring to branches of suitable pure-dimensional subfamilies of definable families of curves when we speak about branches of definable families of curves.

Take $a_1, a_2, b_1, b_2, u \in S_0(K)$ generic and pairwise independent. Let $c_1, c_2 \in S_0(K)$ be such that

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

This is possible, since the image of the function $s \mapsto \tau_1(Y_s, \alpha_s)$ for s ranging in S_0 is of dimension 1, and the values of slopes on the right hand side of the equations above are generic in $\text{End}(k[x]/(x^2))$ for generic pairwise independent values of parameters. Therefore

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

are generic, and c_1, c_2 as required can be found in $S_0(K)$. Let z, v be such that

$$\begin{aligned}\tau_1(Y_z, \alpha_z) &= \tau_1(Y_{a_1}, \alpha_{a_1})\tau_1(Y_u, \alpha_u) + \tau_1(Y_{a_2}, \alpha_{a_2}), \\ \tau_1(Y_v, \alpha_v) &= \tau_1(Y_{b_1}, \alpha_{b_1})^{-1}\tau_1(Y_u, \alpha_u) - \tau_1(Y_{b_2}, \alpha_{b_2}).\end{aligned}$$

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

$$\tau_1(Y_z, \alpha_z) = \tau_1(Y_{c_1}, \alpha_{c_1})\tau_1(Y_v, \alpha_v) + \tau_1(Y_{c_2}, \alpha_{c_2}).$$

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 (G, \cdot, Z) . By Propositions 3.7 and 3.9,

$$\begin{aligned}\tau_1(Y_{a_1} \circ Y_{b_1}, \alpha_{a_1} \circ \alpha_{b_1}) &= \tau_1(Y_{a_1}, \alpha_{a_1})\tau_1(Y_{b_1}, \alpha_{b_1}), \\ \tau_1(Y_{a_2} \circ Y_{b_1} + Y_{b_2}, \alpha_{a_2} \circ \alpha_{b_1} + \alpha_{b_2}) &= \tau_1(Y_{a_2}, \alpha_{a_2})\tau_1(Y_{b_1}, \alpha_{b_1}) + \tau_1(Y_{b_2}, \alpha_{b_2}).\end{aligned}$$

Let $l_1 = \max_{c_1, a_1, b_1 \in S_0} \#(Y_{c_1} \cap Y_{a_1} \circ Y_{b_1})$, and let $l_2 = \#(Y_{c_2} \times_{G^2} Y_{a_2} \circ Y_{b_1} + Y_{b_2})$ for $a_1, a_2, b_1, b_2, c_1, c_2 \in S_0$ generic and independent. Since the number of intersection points is an (G, \cdot, Z) -definable 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 (G, \cdot, Z)). By Lemma 3.13 and Proposition 3.15, the (M, X) -definable set

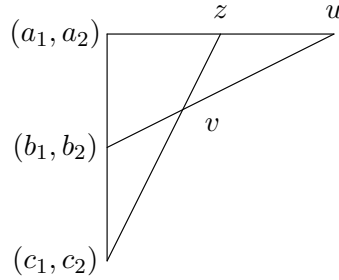
$$\{ w \in S_0 \mid \dim(Y_w \cap (Y_{a_1} \circ Y_{b_1})) = 1 \text{ or } \#(Y_w \cap (Y_{a_1} \circ Y_{b_1})) < l_1 \}$$

contains c_1 and by definition of l_1 is finite. By Lemma 3.13 and Proposition 3.15 again, the (M, X) -definable set

$$\{ w \in S_0 \mid \dim(Y_w \cap (Y_{a_2} \circ Y_{b_1} + Y_{b_2})) = 1 \text{ or } \#(Y_w \cap (Y_{a_2} \circ Y_{b_1} + Y_{b_2})) < l_2 \}$$

contains c_2 and by definition of l_2 is finite.

Arguing in a similar fashion, by application of Lemma 3.13 and Proposition 3.15, we deduce that for all lines in the diagram



each vertex is in the algebraic closure of two other collinear vertices, and so this constitutes a group configuration. Therefore, by Fact 4.4, there exists a two-dimensional group definable in (G, \cdot, Z) that acts transitively on a one-dimensional set.

The conditions of the Fact 4.6 are verified as well: for instance, for the uppermost line, $B = \{\tau_1(Y_{a_1}, \alpha_{a_1}), \tau_1(Y_{a_2}, \alpha_{a_2})\}$ is by construction a canonical base of the type $\text{tp}(\tau_1(Y_z, \alpha_z), \tau_1(Y_u, \alpha_u)/B)$ in the full Zariski structure. Since the natural morphism $S_0 \rightarrow \text{Aut}(k[\varepsilon]/(\varepsilon^2)), s \mapsto \tau_1(Y_s, \alpha_s)$ has finite fibres, a canonical base of $\text{tp}(z, u/a_1, a_2)$ is inter-algebraic with $\{a_1, a_2\}$ in the full Zariski structure. Since passing to the reduct can only enlarge a canonical base, the canonical base of $\text{tp}(z, u/a_1, a_2)$ is inter-algebraic with $\{a_1, a_2\}$. The same argument applies to $\text{tp}(u, v/b_1, b_2)$ and $\text{tp}(z, v/c_1, c_2)$.

By Fact 4.7, the group G is isomorphic to the affine group $\mathbb{G}_a(k) \rtimes \mathbb{G}_m(k)$ of an infinite definable field k . \square

In order to apply the above results we need the following, which is well known model theoretic folklore. We give a short proof specialised to the case where we need it:

Lemma 4.33. *Let G be a strongly minimal group interpretable in \mathcal{M} . Then there exists a strongly minimal $Z \subseteq G^2$ that is not a finite boolean combination of cosets of definable subgroups.*

Proof. To simplify the discussion let us call, for the purposes of this proof only, subsets of G that are finite boolean combinations of cosets of G^n (any n) G -linear. By strong minimality G is in finite-to-finite correspondence with \mathcal{M} (this follows, in general, from the fact that \mathcal{M} is unidimensional. In the present setting G can be assumed to have been obtained from Theorem 4.4 using a 1-dimensional group configuration, so the existence of a finite-to-finite correspondence follows from the statement). It follows that G is not locally modular, as the image of any ample family of 1-dimensional subsets of M^2 under this finite-to-finite correspondence is an ample family in G^2 .

Since G is not locally modular it admits, by [8, Proposition 3.21] a nearly faithful ample family of generically strongly minimal curves $X \rightarrow T \subseteq G^2 \times T$ of dimension 3 (i.e. $\dim(T) = 3$). Let G^0 denote the \mathfrak{M} -connected component of G . let $t \in T$ and $x_0 \in G^0$ be independent \mathfrak{M} -generics. Let y_0 be such that $(x_0, y_0) \in X_t$ and assume that $y_0 \in gG^0$ for some $g \in G$ (that we can choose independent from (x_0, y_0)). Then $gX_t := \{(x, y) : (x, gy) \in (G^0)^2 \cap X_t\}$ is an \mathfrak{M} -definable curve in $(G^0)^2$ and $gX := \{gX_t : t \in T\}$ is a definable family of curves in $(G^0)^2$. Since G/G^0 is finite and X is nearly faithful the correspondence $X_t \mapsto gX_t$ is finite-to-one and on a generic subset of T . Therefore gX is readily checked to be a 3-dimensional, nearly faithful ample family of curves in $(G^0)^2$. Moreover, if X_t is G -linear (for some $t \in T$) then so is gX_t . So it will suffice to show that X can be chosen so that gX_t is not G -linear for generic $t \in T$.

If G^0 is \mathfrak{M} -definably isomorphic to either \mathbb{G}_m or to an elliptic curve, \mathcal{E} , then for generic $t \in T$ gX_t is not G -linear, since there are no definable families of subgroups of \mathbb{G}_m^2 or of \mathcal{E}^2 . Let us elaborate: assume towards a contradiction that for generic $t \in T$ the curve X_t is G -linear. So gX_t is also G -linear for all such t . In this setting there are finitely many \emptyset -definable 1-dimensional subgroups H_1, \dots, H_k of $(G^0)^2$ such that gX_t coincides, up to a finite set, with a union of cosets of the H_i . Since $(G^0)^2/H_i$ is 1-dimensional for all i , near faithfulness of gX implies that gX is, at most, 1-dimensional, a contradiction.

So we are reduced to the case where G^0 is \mathfrak{M} -definably isomorphic to \mathbb{G}_a . This case is dealt with in the Lemma 4.35. \square

Lemma 4.34. *Let $X \subset \mathbb{G}_a^n$ be a hypersurface, let $a = (a_1, \dots, a_n) \in X$ be a general enough point, and let x_1, \dots, x_n be local coordinates on \mathbb{G}_a^n near a . For a value $b \in \mathbb{G}_a$ and a fixed coordinate i consider the level set*

$$X_b = \{ (y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_n) \in \mathbb{G}_a^{n-1} \mid (y_1, \dots, b, \dots, y_n) \in X \}$$

Assume that a belongs to a unique irreducible component of X_{a_i} . If X_b contains an irreducible component that is a coset of a subgroup of \mathbb{G}_a^{n-1} for all b in a neighbourhood of a_i then the local equation of X at a has the form

$$f = \sum_{j \neq i} \sum_{l > 0} \sum_{m \geq 0} c_{jlm} x_i^l x_j^m,$$

for some coefficients $c_{jlm} \in k$

Proof. Similar to proof of Lemma 4.28. Choose a curve $Z \subset X$ that contains a . Consider the following commutative diagram:

$$\begin{array}{ccc} X' := X \times_{\mathbb{G}_a} Z & \longrightarrow & X \\ \downarrow & & \downarrow \\ \mathbb{G}_a^{n-1} \times Z & \longrightarrow & \mathbb{G}_a^n \end{array}$$

where \mathbb{G}_a is the i -th factor in \mathbb{G}_a^n . Consider formal completions of the elements of the diagram along Z :

$$\begin{array}{ccc} \hat{X}' & \longrightarrow & \hat{X} \\ \downarrow & & \downarrow \\ \hat{Y}' & \longrightarrow & \hat{Y} \end{array}$$

Since a is general, $\widehat{\mathcal{O}_{Z,a}}$ is isomorphic to a power series ring, and also the image of Z under some power of a relative Frobenius is generically étale over the i -th \mathbb{G}_a . Choose local coordinates x_1, \dots, x_n on \mathbb{G}_a^n at a , and introduce local coordinates on $\mathbb{G}_a^{n-1} \times Z$ at a as follows: let $\bar{x}_1, \dots, \bar{x}_{i-1}, \bar{x}_{i+1}, \dots, \bar{x}_n$ be obtained from $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n$ by translation and let z be such that $z^{p^M} = x_i$, where M is the degree of inseparability of the field extension $k((z)) : k((x_i))$. Then

$$k[[x_1, \dots, x_n]] \subset k[[\bar{x}_1, \dots, \bar{x}_{i-1}, z, \bar{x}_{i+1}, \dots, \bar{x}_n]]$$

and we have

$$\bar{x}_j = x_j - z_j, \quad \text{for some } z_j \in k[[x_i]].$$

The formal scheme \hat{X}' is cut out in $\mathbb{G}_a^{n-1} \times Z$ by $\bar{f} \in k[[\bar{x}_1, \dots, \hat{x}_i, \dots, \bar{x}_n]] \otimes k[Z]$. If all level sets X_b for b in a neighbourhood of a_i are cosets of a subgroup of \mathbb{G}_a^{n-1} then the evaluation of \bar{f} at such points b is an additive polynomial. In particular, the image of \bar{f} in $k[[\bar{x}_1, \dots, \hat{x}_i, \dots, \bar{x}_n]] \otimes \mathcal{O}_{Z,a}$ is of the form

$$\sum_{j \neq i} \sum_{m \geq 0} \bar{c}_{jm} \bar{x}_j^{p^m}, \quad \bar{c}_{jm} \in \mathcal{O}_{Z,a}$$

Then \hat{X} is cut out in \hat{Y} by the image f of $(\bar{f})^{p^M}$ in $k[[x_1, \dots, x_n]]$. After the change of coordinates one has

$$f = \sum_{j \neq i} \sum_{m \geq 0} \bar{c}_{jm}^{p^M} (x_j - z_j)^{p^{m+M}},$$

and the statement of the lemma follows. \square

Lemma 4.35. *Let G be an algebraic group such that the connected component of the identity of G is isomorphic to \mathbb{G}_a^n . If $X \subset G^n$ is a constructible set which is not a Boolean combination of cosets of subgroups of G^n then there exists a 1-dimensional set $W \subset G^2$ definable in (G, X) that contains a locally closed irreducible subset W_0 that is not a coset of a subgroup of \mathbb{G}_a^2 .*

Proof. We proceed by downward induction on n .

If there existed $X' \subseteq X$ of maximal dimension such that its closure is a coset of subgroup there is a coset $G + a$ of a subgroup G of \mathbb{G}_a with the property that $\dim(X \cap X + g) = \dim(X)$ for all $g \in G$. By stationarity of X for all such g we have, in fact, that $X \Delta X + g$ (i.e., $\dim(X \Delta X + g) < \dim(X)$, where Δ denotes the symmetric difference). Since this is an \mathcal{M} -definable equivalence relation we get that G , and so also $G + a$ are \mathcal{M} -definable. If $X \cap G$ is a coset then $X \setminus G$ is not one, and $\dim(X \setminus G) < \dim(X)$. If $X \cap G$ is not a coset then neither is $G \setminus X$ and $\dim(G \setminus X) < \dim(X)$. Either way, if X has a top-dimensional component that is a coset then we can find a \mathcal{M} -definable subset of M^n of smaller dimension that is not. So repeating the process at most $n - 1$ times, we may assume that no such component of X exists.

Consider the $n - 1$ projections of X on various products \mathbb{G}_a^{n-1} of the factors of the direct product \mathbb{G}_a^n . If the image of any of these projections is not a coset of a subgroup, we make an induction step. Otherwise, images of X_0 under all such projections are cosets of some subgroups. Since X_0 is not a coset, the fibres of all these projections restricted to X_0 are finite, so the image is a coset of a subgroup H such that $\dim H = \dim X_0 = m$. Assume for definiteness that H is the image of the projection $\mathbb{G}_a^n \rightarrow \mathbb{G}_a^{n-1}$ that forgets the last coordinate. Consider now a projection $\pi : H \rightarrow \mathbb{G}_a^m$ with finite fibres. By quantifier elimination for algebraically closed fields, π has the form

$$\pi = (\pi_1, \dots, \pi_m) : H \rightarrow \mathbb{G}_a^m, \quad \pi_i = \text{Fr}^{-a_i} \circ \tau_i,$$

where a_i are positive integers and τ_i are morphisms of algebraic groups (for some choice of identification of H with the closed subgroup of \mathbb{G}_a^n). In particular, if $\tau = (\tau_1, \dots, \tau_m)$ then $(\tau \times \text{id})(X_0)$, where id is applied to the last coordinate, is not a coset, and all the more $(\pi \times \text{id})(X_0)$ is not one. Indeed, if $(\tau \times \text{id})X_0$ were a coset H' , then X_0 would have to be one of the irreducible components of the pre-image $(\tau \times \text{id})^{-1}H'$, which are all cosets. Since X_0 is a top-dimensional irreducible component in X , $\pi(X_0)$ is an irreducible component of the image of X under a definable projection $G^n \rightarrow G^m$. Therefore, unless $m = n - 1$, we may also make an induction step.

So we are reduced to the case where X_0 is a hypersurface in \mathbb{G}_a^n . Pick a generic point $a = (a_1, \dots, a_n) \in X_0$. Let $f \in k[[x_1, \dots, x_n]]$ be the generator of the ideal cutting out the germ of X_0 in the completed local ring $\widehat{\mathcal{O}_{\mathbb{G}_a^n, a}}$. Since X_0 is not a coset, f is not an additive series, that is, it does not consist only of monomials containing only p^j -th, $j \geq 0$, powers of variables. By Lemma 4.34 there exists a coordinate i such that level sets $(X_0)_b$ with respect to this coordinate are not cosets for b in an open neighbourhood of a_i — if it were not the case, f would be an additive series.

Clearly, the level set of X_0 is contained in the corresponding level set of X , which is a definable set contained in G^{n-1} . This finishes the induction step. \square

Remark. 1. It follows from [17, Theorem 4.1(b)] that there is some definable

$Z \subseteq G^n$ (some n) that is not affine. Reducing n to be 2 requires a little more effort.

2. In the above proof it is not hard to see that if we obtain a 2-dimensional nearly faithful family $X \rightarrow T$ such that each X_t contains (up to a finite set) a curve of the form $a_t x + b_t$ then X can be used directly to construct a field configuration.

We can now sum up everything to obtain the main result of this paper:

Theorem 4.36. *Let M be an algebraic curve and let $X \subset M^2 \times T \subset M^2 \times M^l$ be an ample family of curves. Then $\mathcal{M} = (M, X)$ interprets a field.*

Proof. By Corollary 4.13, we may assume that M is smooth, that k is of infinite transcendence degree and that X is a nearly faithful family of generically strongly minimal sets. Thus we can apply Theorem 4.25, allowing us to conclude that \mathcal{M} interprets a strongly minimal group G . By [33, Theorem 4.13], G is an algebraic group. The group G is in an \mathcal{M} -definable finite-to-finite correspondence with M , so it is a one-dimensional algebraic group. Moreover, any \mathcal{M} -definable ample family of curves in M^2 maps through this correspondence into an ample family of curves in G^2 of the same dimension. So G is not locally modular. By [17, Theorem 4.1(b)] there is some definable $Z \subseteq G$ that is not a finite boolean combination of cosets. Let us be a little more precise about this last statement: Since G is not locally modular it is not 1-based (or weakly normal, in the terminology of [17], see for example [23, Theorem 8.2.15]). So by the result of [17] just referred to one-dimensional, this implies that a generic member of a three-dimensional nearly faithful family of curves is not a Boolean combination of cosets of algebraic subgroups of G^2 (because any family of cosets of definable subgroups of G^2 can be – by dimension considerations – at most two-dimensional). Therefore, we may apply Theorem 4.32 to get the desired conclusion. \square

Remark. This field is definably isomorphic to k by [33, Theorem 4.15].

Acknowledgments. The second author thanks Boris Zilber for his remarks on an early version of the paper, and Maxim Mornev for many helpful comments. We would like to thank Moshe Kamensky for comments and suggestions, as well as Ilya Tyomkin and Martin Bays who, by reading the manuscript, helped us significantly improve it.

References

- [1] E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.
- [2] M. Atiyah and I. Mcdonald. *Commutative algebra*, addisson-wesley. *Reading Mass*, 1969.

- [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] E. Bouscaren. Group configuration (after E. Hrushovski). In A. Pillay and A. Nesin, editors, *Model theory of groups*. University of Notre Dame press, 1989.
- [5] Z. Chatzidakis and E. Hrushovski. Model theory of difference fields. *Transactions of the American Mathematical Society*, 351(8):2997–3071, 1999.
- [6] 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.
- [7] D. Eisenbud. *Commutative algebra: with a view toward algebraic geometry*. Graduate Texts in Mathematics. Springer, 1995.
- [8] P. Eleftheriou, A. Hasson, and Y. Peterzil. Strongly minimal groups in o-minimal structures. *J. Eur. Math. Soc. (JEMS)*, Oct. 2019. (to appear).
- [9] A. Grothendieck. Éléments de géométrie algébrique. *Inst. Hautes Études Sci. Publ. Math.*, 1960–1967.
- [10] A. Grothendieck. *Revêtements étales et groupe fondamental (SGA 1)*, volume 224 of *Lecture notes in mathematics*. Springer-Verlag, 1971.
- [11] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. ISBN 0-387-90244-9. Graduate Texts in Mathematics, No. 52.
- [12] E. Hrushovski. *Contributions to stable model theory*. PhD thesis, University of Berkley, 1986.
- [13] E. Hrushovski. Strongly minimal expansions of algebraically closed fields. *Israel Journal of Mathematics*, 79(2-3):129–151, 1992.
- [14] E. Hrushovski. A new strongly minimal set. *Annals of Pure and Applied Logic*, 62(2):147–166, 1993.
- [15] E. Hrushovski. The Mordell-Lang conjecture for function fields. *Journal of the American mathematical society*, 9(3):667–690, 1996.
- [16] E. Hrushovski. The Manin–Mumford conjecture and the model theory of difference fields. *Annals of Pure and Applied Logic*, 112(1):43–115, 2001.
- [17] E. Hrushovski and A. Pillay. Weakly normal groups. *Studies in Logic and the Foundations of Mathematics*, 122:233–244, 1987.
- [18] E. Hrushovski and A. Pillay. Groups definable in local fields and pseudo-finite fields. *Israel J. Math.*, 85(1-3):203–262, 1994.

- [19] E. Hrushovski and B. Zilber. Zariski geometries. *Journal of the American mathematical society*, 9(1):1–56, 1996.
- [20] J. C. Jantzen. *Representations of algebraic groups*. Number 107. American Mathematical Soc., 2007.
- [21] P. Kowalski and S. Randriambololona. Strongly minimal reducts of valued fields. *arXiv preprint*, 2014. math:1408.3298.
- [22] Q. Liu and R. Erne. *Algebraic Geometry and Arithmetic Curves*, volume 6. Oxford University Press, 2006.
- [23] D. Marker. *Model theory: an introduction*. Springer, 2002.
- [24] D. Marker and A. Pillay. Reducts of $(\mathbb{C}, +, \cdot)$ which contain $+$. *Journal of Symbolic Logic*, 55(3):1243–1251, 1990.
- [25] 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>.
- [26] H. Matsumura. *Commutative algebra*, volume 56. Addison Wesley Longman, 1970.
- [27] H. Matsumura and M. Reid. *Commutative ring theory*, volume 8. Cambridge university press, 1989.
- [28] J. Milne. *Étale cohomology*. Princeton University Press, 1980.
- [29] D. Mumford. *Abelian varieties*. Oxford University Press, 1970.
- [30] Y. Peterzil and S. Starchenko. A trichotomy theorem for o-minimal structures. *Proceedings of the London Mathematical Society*, 77(3):481–523, 1998.
- [31] A. Pillay. *Geometric stability theory*. Number 32 in Oxford logic guides. Oxford University Press, 1996.
- [32] A. Pillay and M. Ziegler. Jet spaces of varieties over differential and difference fields. *Selecta Mathematica*, 9(4):579–599, 2003.
- [33] B. Poizat. *Stable groups*, volume 87 of *Mathematical Surveys and Monographs*. AMS, 2001.
- [34] E. Rabinovich. *Definability of a field in sufficiently rich incidence systems*. QMW maths notes. University of London, Queen Mary and Westfield College, 1993.
- [35] T. Scanlon. Local André-Oort conjecture for the universal abelian variety. *Inventiones mathematicae*, 163(1):191–211, 2006.

- [36] T. Stacks Project Authors. *Stacks Project*. <https://stacks.math.columbia.edu>, 2018.
- [37] L. Van den Dries. *Tame topology and o-minimal structures*, volume 248. Cambridge university press, 1998.
- [38] B. Zilber. *Zariski Geometries: Geometry from the Logician's Point of View*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2010.
- [39] B. Zilber. A curve and its abstract Jacobian. *International Mathematics Research Notices*, 2014(5):1425–1439, 2014.
- [40] B. Zilber. Model theory of special subvarieties and Schanuel-type conjectures. *Ann. Pure Appl. Logic*, 167(10):1000–1028, 2016. ISSN 0168-0072. doi: 10.1016/j.apal.2015.02.002. URL <https://doi.org/10.1016/j.apal.2015.02.002>.

DEPARTMENT OF MATHEMATICS
BEN GURION UNIVERSITY OF THE NEGEV
P.O.B. 653
BE'ER SHEVA 84105
ISRAEL
hassonas@math.bgu.ac.il

DEPARTMENT OF MATHEMATICS
KU LEUVEN
CELESTIJNENLAAN 200B
B-3001 LEUVEN (HEVERLEE)
BELGIUM
dmitry.sustretov@kuleuven.be