Incidence systems on Cartesian powers of algebraic curves

Assaf Hasson and Dmitry Sustretov [1]

Abstract

We show that a reduct of the full Zariski structure of an algebraic curve, in which a pure-dimensional family of curves witnessing the lack of local modularity is definable, interprets a field.

Contents

1 Introduction **1**

2 Model theoretic background **3**
2.1 Zilber's restricted trichotomy conjecture 4
2.2 Strongly minimal sets and structures 5
2.3 Standard reductions and setup 7
2.4 The group and field configurations 8

3 Tangency **10**
3.1 Slopes and operations on correspondences 10
3.2 Flat families and definability of tangency 14

4 Interpretation of the field **17**
4.1 Generically unramified projections 17
4.2 Interpretation of a one-dimensional group 19
4.3 Interpretation of the field 22

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., [28, §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 [12], [11] in the late 1980s. Due to Hrushovski's zoo of counterexamples the conjecture has never been reformulated. Yet, Zilber's principle remains a central and powerful theme in model theory: it has been proved to hold in many natural examples such

[1] version of February 12, 2020

as differentially closed fields of characteristic 0, algebraically closed fields with a (generic) automorphism, o-minimal theories and more (see [4, 27, 25, 5, 15]). Many of these special cases of Zilber's trichotomy had striking applications in algebra and geometry ([13, 14, 30]).

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 [34] of a significant strengthening of a theorem of Bogomolov, Korotiaev, and Tschinkel ([2]). The model theoretic heart of Zilber's proof is Rabinovich' trichotomy theorem for *reducts* of algebraically closed fields [29]. In the concluding paragraph of the introduction to [34] Zilber writes: "It is therefore natural to aim for a new proof of Rabinovich' theorem, or even a full proof of the Restrited Trichotomy along the lines of the classification theorem of Hrushovski and Zilber [15], 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[2,3]:

Conjecture A. *Let $\mathcal{M}$ be a non-locally modular strongly minimal reduct of the full Zariski structure on an algebraic curve M over an algebraically closed field K. 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 [29] proved Conjecture A in the special case where $M = \mathbb{A}^1$, and her result can be extend by general principles to any rational curve. In the present paper we prove Conjecture A under a weak technical assumption. Our proof (Theorem 4.12) proceeds in four main steps:

1. Given a non locally modular reduct $\mathcal{M}$ of the full Zariski structure on an algebraic curve, fix a 2-dimensional definable family $X \subseteq M^2 \times T$ of strongly minimal sets in M^2. Throughout the text we assume that for almost all $t \in T$ the curve X_t does not have 0-dimensional irreducible components.

2. We introduce the notion of the slope of a curve $C \subseteq M^2$ at a point $P \in C$, and use it to define when two curves $X_t, X_s \in X$ incident to P are tangent at that point. We show – in what should be viewed as the technical heart of the paper – that this geometric notion is $\mathcal{M}$-definable up to an $\mathcal{M}$-definable equivalence relation with finite classes, Proposition 3.15. To do so we have to overcome two main issues. First, in positive characteristic we were unable to avoid using high order slopes. More significantly, in some instances we need to define the slope of a branch of a curve at a branch point.

[2]The content of Conjecture A is explained for the non-experts in Section 2.

[3]In 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).

3. Using our assumption of the first clause and standard model theoretic machinery we reconstruct a 1-dimensional algebraic group in $\mathcal{M}$, Subsection 4.6. To carry out this construction we have to assure the existence of enough slopes of curves from our family passing through a given point. In characteristic 0 this follows from the uniqueness of solutions of ordinary differential equations for formal power series over K. In characteristic $p > 0$ the kernel of derivation is non-trivial so extra care is needed in the choice of the family X, and we were unable to avoid having to work with high-order slopes[4].

4. This reduces us to proving Conjecture A in the context where $\mathcal{M}$ is a non-locally modular expansion of a 1-dimensional algebraic group. We apply (Subection 4.11) the tools developed in the previous sections to generalise the result of [20] (addressing the same problem for $(\mathbb{C}, +)$) to the present, fully general, context (Theorem 4.11).

The general scheme of our proof seems to have much in common with Rabinovich' original work, though we were unable to understand significant parts of her argument which are highly technical. Step (2) of the above strategy is at the conceptual and technical heart of the paper, and it relies – ultimately – on classical intersection theory. As Rabinovich's main tool for studying intersections of plane curves is the classical Bezout theorem, it stands to reason that the more advanced tools applied in Sub-section 3.2 are at the source of the greater generality of the present paper. We also believe that our more liberal application of algebro-geometric tools such as non-reduced schemes helped simplify the exposition, considerably lowering the level of combinatorial complexity.

It seems that the tools developed in the present paper can be extended to various other contexts. For example, extending the results of [17] to positive characteristic, and any algebraic group and – possibly – even a full proof of the restricted trichotomy conjecture for structures interpretable in ACVF (at least modulo the problem of showing that the 1-dimensional group reconstructed by our methods embeds in an algebraic group).

2 Model theoretic background

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

[4] In a similar situation Rabinovich, [29, Section 8, p.93] seems to claim that she can actually recover an additive subgroup of $(K^2, +)$, giving rise to a characteristic-independent argument.

2.1 Zilber's restricted trichotomy conjecture

A *first-order structure* or just *structure* $\mathcal{N}$ is a set N (called the universe of $\mathcal{N}$) equipped with a collection of boolean algebras of subsets of N^l for all strictly positive $l \in \mathbb{N}$, containing all diagonals $\Delta^l_{i,j} := \{(x_1, \dots x_l) : x_i = x_j\}$ and closed under finite Cartesian products and all projections $(x_1, \dots, x_n) \mapsto (x_1, \dots x_{n-1})$. Somewhat analogously to geometric terminology the tuples $(x_1, \dots, x_n) \in S \subset N^l$ 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 $Y \subseteq N^{l+m}$ (some $m \geq 0$) such that $Y = Y_a := \{x \in N^l : (x, a) \in Y\}$ for some $a \subseteq A$. A map $f : X \to Y, X \subset N^l, Y \subset N^m$ is called *definable* if its graph is. We refer to [32, §1.1-2] for a more detailed discussion of structures and definable sets.

Given an algebaraic curve M over an algebraically closed field k (reduced, but not necessarily irreducible, smooth or projective), the *full Zariski structure on* M is the structure with universe $M(k)$ and Boolean algebras of definable sets given by Boolean algebras of constructible sets on the Cartesian powers $M^n(k)$. This collection of sets is closed under projections by Chevalley's theorem (see, e.g., [19, Corollary 3.2.8]), and therefore $M(k)$ is a structure. Notationally, we will not distinguish between the curve M as an algebro-geometric object and its k-rational points.

Structures such as the full Zariski structure on M can be viewed as a generalisation of the notion of abstract plane geometry in the sense of [1, §2]. If $M = \mathbb{A}^1$, then the ground field k can be reconstructed – that is, interpreted in the sense of first order logic – from the incidence system of affine lines in $\mathbb{A}^2$.

Let us now explain in more detail what is meant by reconstructing the field. We say, that a field K is *interpretable in a structure* $\mathcal{N}$ if there exists a definable set $K' \subset N^m$ for some m and a definabe equivalence relation R such that K'/R is a field, the graphs of multiplication and addition operations on it are definable and such that K'/R is isomorphic to K.

Let M be a curve over an algebraically closed field k, and let $X \subset M^{2+l}$ be a constructible set and denote $X_t = \{(x_1, x_2) \in M^2 \mid (x_1, x_2, t_1, \dots, t_l) \in X\}$ for a tuple $t = (t_1, \dots, t_l) \in M^l$. Assume that $\dim X_t = 1$ for any point $t \in T = \{ (t_1, \dots, t_l) \in M^l \mid X_t \neq \emptyset \}$. We will regard such constructible sets as *families of constructible sets of dimension 1* parametrized by T. We will denote (M, X) the structure with universe M such that its collection of the Boolean algebras of definable sets is the minimal one including X. A family X of constructible sets of dimension 1 in M^2 is *ample* (terminology is borrowed from [15]) if there exists a dense open $U \subseteq M^2$ such that for any $(x, y) \in U$ there exists $t \in T$ such that $x, y \in X_t$. We are now ready to formulate Zilber's restricted trichotomy conjecture for algebraically closed fields (Conjecture A):

Conjecture B (Zilber's restricted trichotomy in dimension 1)**.** *Let M be an algebraic curve over an algebraically closed field k (not necessarily smooth, proper or irreducible). Let $X \subseteq M^2 \times T$ be the total space of an ample family of definable sets*

of dimension 1[5]*, then a field K is interpretable in $\mathcal{M} = (M, X)$.*

Note that the existence of a definable ample family of plane curves is a necessary condition for the interpretability of an infinite field in any structure interpretable in the full Zariski structure on M. For technical reasons we impose a natural restriction on X and prove (Theorem 4.12) Conjecture B under assumption that X_t is pure-dimensional for all $t \in T$ (i.e. has no components of dimension 0).

Even this weakened version of the Conjecture B is enough to prove the main theorem of [34]. In this paper Zilber considers the following problem. Let M be a smooth projective curve of genus at least 2 over an algebraically closed field k, $J(M)$ its Jacobian variety and let $\mathcal{J} := (J(M), +, M)$ be a structure generated by the graph of the group law on $J(M)$ and M as a subset in $J(M)$ under an Abel-Jacobi map. Then the question solved in Theorem 1.3 *loc.cit.* is whether the isomorphism type of the structure J determines the isomorphism type of the curve M.

The approach of Zilber is as follows: the definable set M is strongly minimal and satisfies the conditions of the Conjecture B, moreover, the family X of definable sets in M^2 from the statement of the conjecture (the witness to the lack of local modularity) consists of pure-dimensional sets. Indeed, let

$$X := \{ \ (a, b, c, d) \in M^2 \times M^2 \ \mid \ a + b = c + d \ \}$$

Then X is clearly definable in M considered as a structure and one can check that $X_{c,d} \subset M^2$ is a closed curve for all $c, d \in M^2$.

The key step of Theorem 1.3, *loc.cit.* is showing that $J(M)$ interprets the field k, and this is deduced from the fact that the structure M interprets the field k. Zilber invokes the theorem of Rabinovich [29] which he has to apply to a strongly minimal structure supported on the points of a projective line — a certain linear system on M. This circumvention is necessary as Rabinovich's theorem only solves the Conjecture B in case M is a rational curve. Our Theorem 4.12 can be used as an alternative ingredient in the proof of Theorem 1.3 of [34] that can be applied directly to M.

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., [21]) 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 [15] (namely, if X separates points in M^2), but we do not study this question here.

2.2 Strongly minimal sets and structures

We will now briefly describe the model theoretic framework suitable for discussing Zilber's restricted trichotomy conjecture. A structure $\mathcal{D}$ is *strongly minimal* if its

[5] In model theoretic jargon the existence of such a family is equivalent to non *local modularity* (of the structrue $\mathcal{M}$).

universe D is infinite and for every elementary extension D' every subset of D definable with parameters in D' is either finite or co-finite. By Chevalley's theorem mentioned above, algebraically closed fields (as well as the full Zariski structure on any irreducible curve over them) are strongly minimal. For a detailed overview of strongly minimal structures we refer the reader to [26][§2.1-2] and [19, §6.1].

Strongly minimal structures admit a natural notion of dimension: a definable set $S \subseteq D$ has dimension 1 if and only if it is infinite. $S \subseteq D^n$ has rank k if k is maximal such that there exists a projection $\pi : S \to D^k$ such that $D^k \setminus \pi(S)$ has rank smaller than k. The *degree*[6] of a definable set S is defined to be the maximal number d such that $S = \bigcup_{i=1}^{d} S_i$ where the S_i are disjoint sets definable over some parameters and satisfying $\dim S_i = \dim S$. The notion of a degree, therefore, is the model-theoretic analogue of the number of top-dimensional geometrically irreducible components of a variety. A definable set S such that $\dim S = \deg S = 1$ is also called *strongly minimal*. This terminology is justified by the fact that it can be shown that the structure with universe $S(\mathcal{D})$ and definable subsets of S^n defined to be the definable subsets of S^n in the sense of the ambient structure D, is strongly minimal.

Fact 2.1. *Let $\mathcal{D}$ be a strongly minimal structure, and $S \to T$ be a definable map. Then for any n the set*

$$\{\ t \in T\ \mid\ \dim S_t = n\ \}$$

is definable.

If p is a type then $\dim p = \min_{X \in p} \dim X$. A tuple $s \in D^n$ is *algebraic over A* if $\dim(\mathrm{tp}(s/A)) = 0$. We let $\mathrm{acl}(A)$ be the set of all elements of the universe algebraic over a set A. A type p with $S \in p$ is called *generic* in S if $\dim p = \dim S$, and its realisations are called *generic points* of S. In these terms the degree of a set S, definable over A, is the maximal number of types over B generic in S, for any parameter set $B \supseteq A$. Two tuples $x \in M^n, y \in M^l$ are called independent over a set of parameters A if $\dim \mathrm{tp}(xy/A) = \dim \mathrm{tp}(x/A) + \dim \mathrm{tp}(y/A)$. Geometrically, if x is a realization of the generic type of X and y is a realization of the generic type of Y, then x and y are independent precisely when $(x, y) \in M^{n+l}$ is a realization of the generic type of $X \times Y$.

The notion of generic points[7] plays an important role in all that follows. Recall from Subsection 2.1 that the full Zariski structure on an algebraic curve M over k extends naturally to K-point of M over any algebraically closed field $K \supset k$. Given a Zariski closed set S over k, a point $p \in S(K)$ is generic in S over k if and only if p does not belong to any Zariski closed subsets of $S(K)$ defined over k, that is, if and only if it is a generic point of S in the sense of Weil.

[6] In the model theoretic literature these notions of dimension and degree are known as Morley rank and degree (or multiplicity). The definition given here coincides with the standard definition in strongly minimal structures, [19, Theorem 6.2.19].

[7] This model theoretic terminology refers to K-rational points of a variety, and differs from the standard algebro-geometric notion of the same name.

By definition, if S_1, S_2 are strongly minimal definable subsets of D^n then $S_1 \cap S_2$ is either finite or co-finite in both S_1 and in S_2. In the latter case we write $S_1 \sim S_2$ and say that S_1 and S_2 *almost coincide*. If $X \subseteq D^2 \times T$ is definable such that X_t is strongly minimal for all $t \in T$, we call X a *definable family of strongly minimal sets in* D^2. We note that $\sim$ is definable on definable families of curves (because $|X_t \cap X_s|$ is either infinite or bounded uniformly in s, t – this is obvious for constructible families of constructible sets in algebraically closed fields, but is true for all strongly minimal structures, e.g., [26, Remark 1.5.4]). We will call a family as above *faithfully parametrized* (also called *normal family* in the literature) if the equivalence relation $\sim$ is the identity relation. We call such a family *almost faithfully parametrized* if all equivalence classes of $\sim$ are finite.

Fact 2.2 (Lascar and Pillay, [11, p. 137])**.** *Let $X \subset D^2 \times T$ be a family of curves as above. Then there exists a family of curves $X' \subset D^2 \times T'$ and a surjective map $f : T \to T'$, definable over some set of parameters, such that*

- *equivalence classes of $\sim_{X'}$ are finite,*
- *$f(s) \sim_{X'} f(t)$ if and only if $s \sim_X t$*
- *$X'_{f(t)} \sim X_t$ for any $t \in T$.*

In these terms, the strongest version of Zilber's trichotomy restricted to algebraically closed fields is:

Conjecture C. *Let k be an algebraically closed field, let $D \subset k^l$ be a constructible set and R be an equavalence relation on D. Let $\mathcal{M}$ be a strongly minimal structure with universe D/R such that any definable set in $\mathcal{M}$ is a quotient of a constructible set in D^n by R^n. Assume that there exists a definable almost faithfully parametrized family of curves $X \subset M^2 \times T$ with $\dim T = 2$. Then there exists an infinite field interpretable in $\mathcal{M}$.*

Conjecture B is a particular case of Conjecture C when the universe of $\mathcal{M}$ is an algebraic curve. In the setting of Conjecture B it follows immediately from the definitions that the model theoretic dimension coincides with the algebro-geometric dimension. More generally, if the universe M has Krull dimension n then the Krull dimension of an $\mathcal{M}$-definable set would be n times its model theoretic dimension.

2.3 Standard reductions and setup

We fix an algebraically closed field k. For the purposes of this paper by *curve* we mean a 1-dimensional algebraic variety, which we do not assume to be projective, smooth or irreducible.

In order to keep the discussion of the following reductions short we have to use some model-theoretic language that was not previously explained, but the conclusions should be clear to a reader who has followed Sections 2.1 and 2.2.

It will be convenient to use the model theoretic notion of 1-basedness ([26, Definition 2.5.6]) which, in the present context is equivalent to the non-existence of a definable ample family of plane curves[8] ([26, Proposition 5.2.8] combined with Definition 2.2.4, the comment following it and Proposition 2.6).

Note that Conjecture C immediately implies a slightly stronger statement with the degree of M not necessarily equal to 1. Indeed, suppose $M = \cup_{i=1}^{d} M_i$ where M_i are strongly minimal. By [26, Proposition 2.5.8] there is a definable strongly minimal set that is not locally modular. This can be seen as follows: X is an ample family of plane curves, so $\mathcal{M}$ is not 1-based, so some minimal type in $\mathcal{M}$-is not locally modular, and by Buechler's dichotomy ([26, Theorem 2.3.2]) it is strongly minimal.

Next, let us show that we may assume that X_t is strongly minimal for t belonging to a generic subset of T, and

Finally, if M' is the smooth locus of M, then $\mathcal{M}'$ – the set M' with the induced $\mathcal{M}$-structure is not 1-based (this follows readily from [26, Proposition 2.5.9] or simply take the restriction – in the obvious sense – of X to M'). This shows that we may assume, without loss of generality, that M is a smooth curve. Therefore to prove Conjecture B it suffices to prove it under the following assumptions:

The universe M is a smooth curve over k. The family $X \subset M^2 \times T$ is an almost faithfully parametrized family of definable curves such that $\dim T = 2, \deg T = 1$ and X_t is strongly minimal for t generic in T in the structure (M, X). Moreover, M is strongly minimal in (M, X).

When talking about curves in M^n we assume that they are Zariski closed in M^n. A *definable curve* is a definable set in M^n of dimension 1, not necessarily pure-dimensional or Zariski closed, definable in (M, X).

We conclude with a word of caution: algebraically closed fields have the definable multiplicity property ([11]), which in that context is equivalent to definability of irreducibility, that is, given a family of curves $X \subset M^2 \times T$, the set $\{t \in T : X_t \text{ is irreducible}\}$ is definable in the full Zariski structure on M. This need not be the case in (M, X), and we cannot assume that $X_t \in X$ is strongly minimal for all $t \in T$, nor it is the case for all t in some definable subset of T. This can only be achieved if t realizes the generic type of T. Note that in that case it is not automatic that the symmetric difference $X_t \triangle X_s$ is either finite or co-finite for $s, t \in T$. By compactness (of first order logic) this is true for $s, t \in T_0 \subset T$, where T_0 is definable in (M, X), $\dim T_0 = 2$. So all our discussion about passing to almost faithfully parametrized families goes through unaltered.

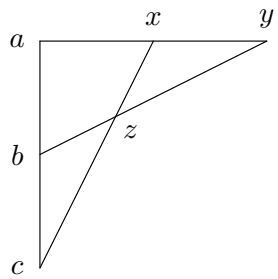
2.4 The group and field configurations

In the strongly minimal context, certain combinatorial configurations of (imaginary) elements are known to exist only in the presence of a definable group or a definable

[8] So for strongly minimal sets this notion coincides with non local modularity

field. It is by constructing such configurations that the main theorem of the present paper is proved. We will now describe these configurations in more detail:

Definition 2.3 (Group configuration)**.** *Let M be a model of a strongly minimal theory, and let* dim *the be associated dimension function on tuples.*



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

- *all elements of the diagram are pairwise independent and* $\dim(a, b, c, x, y, z) = 2n + 1$*;*
- $\dim a = \dim b = \dim c = n$*,* $\dim x = \dim y = \dim z = 1$*;*
- *all triples of tuples 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 interalgebraic *if for any pair of tuples $a \in G_1, a' \in G_2$ in the corresponding vertices,* $\mathrm{acl}(a) = \mathrm{acl}(a')$*.*

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

Fact 2.4 (Hrushovski)**.** *Let 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, independent generic elements $g, h \in G$ and $u \in X$ such that the group configuration $G_2 = (\ g, h, g \cdot h, u, g \cdot u, g \cdot h \cdot u\ )$ that is interalgeraic with G_1. In particular,* $\dim G = \dim a$*.*

This follows from the main theorem of [3] and the fact that infinitely definable groups in stable theories are intersections of definable groups (see, for example, Theorem 5.18[28]). The original proofs of these statements are contained in [10].

Recall that the canonical base of a type $p \in S_n(A)$ is a smallest set B (unique up to definable closure) such that $\dim p = \dim p|_B$.

Fact 2.5. *In the statement of Fact 2.4 assume additionally that the canonical base of* $\mathrm{tp}(x, y/a)$ *is interalgebraic with* a*, that the canonical base of* $\mathrm{tp}(z, y/b)$ *is interalgebraic with* b*, and that the canonical base of* $\mathrm{tp}(z, x/c)$ *is interalgebraic with* c*. Then the action of* G *on* X *is faithful.*

Fact 2.6 (Hrushovski, [10])**.** *Let* G *be a group of Morley rank* $n > 1$ *acting transitively and faithfully on a strongly minimal set* X*. Then there exists a definable field structure on* X *and either* $n = 2$ *and* $G \cong \mathbb{G}_a \rtimes \mathbb{G}_m$*, or* $n = 3$ *and* $G \cong \mathrm{PSL}_2$*.*

An exposition of the above fact can be found in [28] (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 2.6. 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.

3 Tangency

3.1 Slopes and operations on correspondences

In the first approximation, our strategy for building group configurations is to consider definable curves in M^2 and treat them as correspondences between the two factors M. If Z is such a correspondence, we call a *branch of* Z *at point* $a \in Z$ a prime factor of the equation of Z in the formal completion of M^2 along a and an *n-th order slope of a branch* α *of* Z *at* a a formal expansion up to n-th order of the equation of the branch α in a fixed local coordinate system. If Z, W are two curves and $a \in Z, b \in W$ are smooth points with projections on the respective factors a_1, a_2, b_1, b_2 with $a_2 = b_1$ then the composition $Z \circ W$ has a branch passing through (a_1, b_2) with the n-th order slope equal to the composition of n-th order slopes of Z and W considered as polynomials truncated at n-th order. A similar statement can be made about the slopes of branches that are "pointwise added" if M has a structure of a group, see Definition 3.6. This behaviour of the slopes is what makes the field reconstruction work later in the paper. We remark that similar approach was employed by Zilber [33, Section 3.8] using non-standard analysis techniques. Let us now proceed to the formalization of this idea.

Remark. Recall that any algebraic variety over a perefect field is generically smooth (see, e.g., Corollary to Theorem 30.5 of [22]), and that a completion of the local ring of a smooth point of a variety is a formal power series ring (Theorem 29.7, *loc.cit.*).

Definition 3.1 (Local coordinate system)**.** *Let* a *be a smooth point of a curve* X*. A* local coordinate system at P *is an isomorphism* $\widehat{\mathcal{O}_{X,a}} \xrightarrow{\sim} k[[x]]$*.*

Definition 3.2 (Branches and slope)**.** *Let* $X_1, X_2, Z \subset X_1 \times X_2$ *be curves,* $a = (a_1, a_2) \in V = X_1 \times X_2$ *be a smooth point and let* $I = \mathrm{Ker}(\mathcal{O}_{V,a} \to \mathcal{O}_{Z,a})$*. We call a generator of the principal ideal* $\hat{I} = I\widehat{\mathcal{O}_{V,a}} \subset \widehat{\mathcal{O}_{V,a}}$ *the* local equation of Z at a*. Since* Z *is reduced, the prime decomposition* $\hat{I} = I_1 \cdot \ldots \cdot I_n$ *is unique and we call*

ideals $I_1, \ldots, I_n$ branches of Z at a, *and any of their generators* local equations *of corresponding branches. Assume that local coordinate systems are chosen at* a_1, a_2, *then* $\mathcal{O}_{V,a} \cong k[[x,y]]$. *If the local equation of* α *is of the form* $y - f$ *for* $f \in k[[x]]$ *then the* n-th order slope of Z at α, *denoted* $\tau_n(Z,\alpha)$, *is the endomorphism* $\tau_n : k[x]/(x^{n+1}) \to k[x]/(x^{n+1})$ *sending* x *to* $f \mod x^{n+1}$.

Remark. It follows from standard results on étale morphisms (see, for example, [23, Section I.1.3]) that if an irreducible component Z of X is smooth at a then the slope of the branch corresponding to Z is defined at a for all orders $n \geq 1$, however, this is not necessary in general: the nodal cubic $y^2 = x^3 - x^2$ is irreducible, but has two branches at 0 with slopes defined at both of them.

By a *family of curves* we will understand a Zariski closed subset $X \subset M^2 \times T$ such that $\dim X_t = 1$ for all $t \in T$. We will understand that the definitions that we will give below for families of curves apply also to single curves regarded as families parametrized by a single point, $T = \{t\}$.

Definition 3.3 (Families of branches)**.** *Let* $X \subset M^2 \times T$ *be a family of curves and let* $a \in M^2$. *We will call elements of the primary decomposition* $\mathcal{I}_X = \mathcal{I}_1 \cdot \ldots \cdot \mathcal{I}_n$ *of the ideal sheaf* $\mathcal{I}_X$ *that cuts out* X *in the formal completion of* M^2 *along* $\{a\} \times T$ families of branches of X at a. *We will call any local generator of such ideal* $\mathcal{I}_l$ *a* local equation of the family of branches $\mathcal{I}_l$.

Clearly, for any t the ideal $\mathcal{I}_l \otimes k(t) \subset \widehat{\mathcal{O}_{M^2,a}}$ is a branch of X_t at a.

A first-order slope is a map $k[\varepsilon]/(\varepsilon^2) \to k[\varepsilon]/(\varepsilon^2)$, determined by its action on ε: $\varepsilon \mapsto c \cdot \varepsilon$. Let us remark that the scalar c is the coordinate, in a given affine chart, of the tangent space $T_a Z \in \mathbb{P}(T_a M^2)$.

From now on, if $X_1 \times \ldots \times X_n$ is a product of k-schemes, we denote $p_{i_1 \ldots i_k} : X_1 \times \ldots \times X_n \to X_{i_1} \times \ldots \times X_{i_k}$ the natural projections. Although the notion of the composition of correspondences is standard, we reintroduce it here to fix conventions.

Definition 3.4 (Composition of curves)**.**

(i) Let M *be a curve and let* T, S *be varieties, let* $X \subset M^2 \times T$, $Y \subset M^2 \times S$ *be families of curves, and let* p_i *denote projections on factors of the space* $M \times M \times M \times T \times S$. *Define the* family $Y \circ X$ of compositions of curves from X and Y *the to be support of the sheaf*

$$p_{1345*}(p_{124}^* \mathcal{O}_X \otimes p_{235}^* \mathcal{O}_Y)$$

on $M^2 \times T \times S$. *If all* X_t, Y_s *project dominantly on the first factor* M *of* M^2 *then* $Y \circ X$ *is a family of curves parametrized by* $T \times S$.

(ii) If X, Y *as above are definable, the* composition of X and Y *is the following definable set*

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

We denote by X^{-1} the image of X under the automorphism of $M^2 \times T$ that transposes the two factors M.

Remark. If $X \subset M^2$, $Y \subset M^2$ are definable sets of pure dimension 1 in a reduct of M and $\bar{X}, \bar{Y}$ are their Zariski closures then one can check that

$$\overline{X \circ Y} = \bar{X} \circ \bar{Y}$$

where the composition on the right is understood in the sense of Definition 3.4(i) and the composition on the left is understood in the sense of Definition 3.4(ii).

Proposition 3.5. *Let $X \subset M^2 \times T$ and $Y \subset M^2 \times S$ be families of curves, let α, β be families of branches of X, Y at $a = (a_1, a_2) \in X, b = (b_1, b_2) \in Y, a_2 = b_1$, respectively, and assume $\tau_n(X, \alpha_t)$ and $\tau_n(Y, \beta_s)$ are defined for all $t \in T, s \in S$. Then there exists a family of branches $\beta \circ \alpha$ of $Y \circ X$ at (a_1, b_2) such that*

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

for all $t \in T, s \in S$. The operation of composition of branches commutes with restriction to the fibre: $(\beta \circ \alpha)_{(t,s)} = \beta_s \circ \alpha_t$.

Proof. The proof consists in essentially unraveling the definitions. If the branch α is given Zariski locally around $t \in T$ by an equation $y - f$, $f \in k[[x]] \otimes \mathcal{O}_{T,t}$, and β is given by $z - g, g \in k[[y]] \otimes \mathcal{O}_{S,s}$, then let the branch $\beta \circ \alpha$ be given by $z - g \circ f$. Note that the composition $g \circ f$ makes sense, since f is a formal power series with zero constant term.

Now $y - f$ divides the generator h_X of the kernel of the morphism $\mathcal{O}_{M^2,a} \to \mathcal{O}_{X,a}$ and $z - g$ divides the generator h_Y of the kernel of the morphism $\mathcal{O}_{M^2,b} \to \mathcal{O}_{Y,b}$. The germ of $Y \circ X$ around (a_1, b_2, t, s) 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 branch of $Y \circ X$ at this point, we need to check that $(z - g \circ f)$ is a prime ideal containing $(h_X, h_Y) \cap k[[x, z]] \otimes \mathcal{O}_{T,t} \otimes \mathcal{O}_{S,s}$. This is clear from the fact that $(z - g \circ f) \subset (y - f, z - g)$. □

Definition 3.6 (Pointwise summation of curves)**.**

(i) 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 $a : G \times G \to G$ be the group law, let $\Gamma_a \subset G^3$ be its graph, and let p_i denote the projections on factors of the space $G \times G \times G \times G \times T \times S$. We define the sum $X + Y$ of X and Y *to be the support of the following module in $G^2 \times T \times S$*

$$\mathcal{O}_{X+Y} = p_{1456*}(p_{234}^* \mathcal{O}_{\Gamma_a} \otimes p_{124}^* \mathcal{O}_X \otimes p_{135}^* \mathcal{O}_Y)$$

(ii) If X and Y are definable sets, their sum is defined as follows:

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

Remark. If $X \subset M^2$, $Y \subset M^2$ are definable sets of dimension 1 in a reduct of M and $\bar{X}, \bar{Y}$ are their Zariski closures then

$$\overline{X+Y} = \bar{X} + \bar{Y}$$

where the sum in rhs is understood in the sense of Definition 3.6(i) and the sum in lhs is understood in the sense of Definition 3.6(ii).

Remark. The notation above suggests that G is commutative. The definition applies even if it is not the case, although in this paper we will only consider the operation "+" for commutative groups.

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 $\widehat{\mathcal{O}_{G,e}} \to \widehat{\mathcal{O}_{G,e} \otimes \mathcal{O}_{G,e}} \cong k[[x,y]]$ induced by the group operation morhpism. The truncation to first order of a one-dimensional formal group law is $x + y$ (see for example [16, I.2.4]).

By definition, an n-th slope is an endomorphism of $k[\varepsilon]/(\varepsilon^{n+1})$ sending ε to a truncated polynomial with zero cosntant term. While the endomorphisms of a general ring are not additive, it is a happy coincidence that $\mathrm{End}(k[\varepsilon]/\varepsilon^2)$ is a ring.

Lemma 3.7. $\mathrm{End}(k[\varepsilon]/(\varepsilon^2)) \cong k$.

Proof. Straightforward. □

Proposition 3.8. *Let G be a 1-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, viewed as a morphism from $k[\varepsilon]/(\varepsilon^{n+1})$ to $k[x,y]/(x^{n+1}, y^{n+1})$ sending ε to $F(x,y) \mod (x^{n+1}, y^{n+1})$. Let $X \subset G \times G \times T$, $Y \subset G \times G \times S$ be families of curves and assume that $\tau_n(X_t, \alpha_t), \tau_n(Y_s, \beta_s)$ are defined for all $t \in T, s \in S$ for some branches α, β at $a = (a_0, a_1), b = (b_0, b_1)$, $b_0 = a_0$. Then there exists a branch $\alpha + \beta$ of $X + Y$ at $(a_0, a_1 + b_1)$ for all $t \in T, s \in S$*

$$\tau_n(X_t + Y_s, (\alpha+\beta)_{(t,s)})(x) = F_n(\tau_n(X_t, \alpha_t)(x), \tau_n(Y_s, b_s)(x))$$

In particular, if $n = 1$,

$$\tau_1(X_t + Y_s, (\alpha+\beta)_{t,s})(x) = \tau_1(X_t, \alpha_t) + \tau_1(Y_s, \beta_s)$$

The operation $+$ on the branches commutes with restriction to the fibre: $(\alpha+\beta)_{(t,s)} = \alpha_t + \beta_s$.

Proof. As in the proof of Proposition 3.5, this statement follows from the unfolding of the definitions. Reasoning locally as in the proof of Proposition 3.5, assume that α is cut out by equation $y - f$, β is cut out by $z - g$. Then $\alpha + \beta$ is cut out by $u - F(f(x), g(x))$. Checking that this is indeed a branch of $X + Y$ is straightforward and we leave it to the reader. □

3.2 Flat families and definability of tangency

Let $X \subset M^2 \times T$, $Y \subset M^2 \times S$ be families of curves and assume that there exists $a \in M^2$ such that $a \in X_t \cap Y_s$ for all $t \in T, s \in S$. Let α, β be families of branches at a of X and Y, respectively. Assume that $X_t \cap Y_s$ is finite for (t, s) in some open dense subset of $T \times S$ and let n be maximal such that $\tau_n(X_t, \alpha_t) = \tau_n(Y_s, \beta_t)$ for all $t \in T, s \in S$ (such an n exists by Krull intersection theorem). We aim to characterize those pairs of curves which have "higher than general degree of tangency" at a, or more precisely, such that $\tau_{n+1}(X_t, \alpha_t) = \tau_{n+1}(Y_s, \beta_s)$, in terms of the number of intersection points $X_t \cap Y_s$. This will be done in Proposition 3.15, which will play the crucial role in the contsruction of group configurations in Theorems 4.6 and 4.11.

The key preliminary step is the observation that the "family of intersections" $X \times_{M^2} Y \to T \times S$ is flat if restricted to $T \times S$ minus those pairs (t, s) such that $X_t \cap Y_s$ is infinite. Since flatness of morphisms is often used in this section, we refer the reader to any standard exposition of its properties, such as [23, I.§2], for details, and quickly recall some of the key facts.

Fact 3.9 (Generic Flatness, [8, Corollaire IV.6.11])**.** *Let Y be an integral locally Noetherian scheme and let $f : X \to Y$ be a morphism of finite type. Then there exists a dense open subset $U \subset Y$ such that the restriction of f to $f^{-1}(U)$ is flat.*

Fact 3.10 ([23, Propositions I.2.4-5])**.**

(i) an open immersion is flat;

(ii) a composition of flat morphisms is flat;

(iii) let $f : X \to Y$ be flat and let $Z \to Y$ be a morphism. Then $X \times_Y Z \to Z$ 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.

Lemma 3.11. *Let M be a smooth curve, T, S be smooth varieties, $X \subset M^2 \times T$, $Y \subset M^2 \times S$ be two families of pure-dimensional curves such that all irreducible components of X, resp. Y, are dominant over T, resp. S. Let U be the set of points $u \in T \times S$ such that $\dim(X \times_{M^2} Y)_u = 0$ and let $Z = X \times_{M^2} Y \cap p^{-1}(U)$ where p is the natural projection (the fibre product here is taken in the scheme-theoretic sense). Then $p|_Z : Z \to U$ is a flat morphism of schemes.*

Proof. Since M, T, S are smooth and since regular local rings are unique factorization domains, Y is cut out in $M^2 \times S$ by a principal ideal sheaf. Then by Fact 3.10(iv) $X \to T$ is flat, and by Fact 3.10(iii) $X \times S \to T \times S$ is flat too. Since the natural closed embedding $X \times_{M^2} Y \to X \times S$ is also cut out by a principal ideal sheaf, by Fact 3.10(iv), this closed subscheme is flat precisely over the complement of the subvariety of $T \times S$ consisting of the points (t, s) such that the local generator of this ideal sheaf does not vanish on an irreducible component of the fibre $X_t \times \{s\}$. 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 finite. □

Lemma 3.12. *Let $f : X \to Y$ be a flat quasi-finite morphism. Then the function*

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

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

Proof. Follows from [7, EGA IV.3.15.5.1(i)] and the fact that flat morphisms of finite type are universally open ([7, EGA IV.2.4.6]). □

Lemma 3.13. *Let $f : X \to Y$ be a flat quasi-finite morphism of schemes. Define the multiplicity in the fibre function*

$$w : X \to \mathbb{Z} \qquad x \mapsto \dim_{k(x)} \mathcal{O}_{X,x} \otimes k(f(x))$$

and define $l : Y \to \mathbb{Z}, l(y) = \sum_{f(x)=y} w(x)$. Then w is upper semi-continuous, and if f is finite then l is locally constant.

Proof. Upper semi-continuity of w follows from [31, Tag 0F3D] and [31, Tag 0F3I].

If f is finite then by [7, EGA II.6.1.11] it is projective, and $l(y)$ is the constant term of the Hilbert polynomial, which is locally constant in a flat projective family by [7, EGA III.7.9.11]. □

Lemma 3.14. *Let Y be an irreducible variety, let $\bar{f} : \bar{X} \to Y$ be a flat finite morphism, $\iota : X \hookrightarrow \bar{X}$ be an open embedding, and let $f = \bar{f} \circ \iota$. Define the following constants*

$$l_0 = \max_{y \in Y} \sum_{f(x)=y} w(x) \qquad m_0 = \max_{y \in Y} \#f^{-1}(y)$$

Then

$$\{\ y \in Y \ \mid\ \sum_{f(x)=y} w(x) < l_0\ \} \subset \{\ y \in Y \ \mid\ \#f^{-1}(y) < m_0\ \}$$

Proof. The number $\sum_{\bar{f}(x)=y} w(x)$ is constant for all $y \in Y$ by Lemma 3.13. Suppose y is such that $\sum_{f(x)=y} w(x) < l_0$, then $f^{-1}(y) \subsetneq \bar{f}^{-1}(y)$ and hence $\#f^{-1}(y) < m_0$. □

Proposition 3.15. *Let M be a smooth curve, T, S be irreducible varieties, and let $X \subset M^2 \times T$ and $Y \subset M^2 \times S$ be families of pure-dimensional curves. Let $a = (a_1, a_2) \in M^2$ be a point such that $a \in X_t \cap Y_s$ for all $t \in T, s \in S$. Let U be the open subset of $T \times S$ such that $X_t \cap Y_s$ is finite for $(t, s) \in U$ and assume that $p : Z = X \times_{M^2} Y \to U$ is a flat morphism. Let α, β be families of branches of X,*

Y at a, respectively, such that the slopes at α_t, β_s are defined for all $t \in T, s \in S$. Define

$$\begin{aligned} n_0 &= \max\{n \mid \tau_n(X_t, \alpha_t) = \tau_n(Y_s, \beta_s) \text{ for all } t \in T, s \in S\} \\ m &= \max_{(t,s)\in U} \#(X_t \cap Y_s) \end{aligned}$$

(note that n_0 is finite by Krull intersection theorem). Then

$$\{\ (t,s) \in U\ \mid\ \tau_{n_0+1}(X_t, \alpha_t) = \tau_{n_0+1}(Y_s, \beta_s)\ \} \subseteq \{\ (t,s) \in U\ \mid\ \#(X_t \cap Y_s) < m\ \}$$

Proof. Let $q : Z \to M^2$ be the natural projection, and let $Z_0 = q^{-1}(a)$ and let W be the complement of Z_0 in Z. Let $j : U \to Z_0$ be the natural homeomorphism.

First observe that if t, s are such that $\tau_{n_0+1}(X_t, \alpha_t) = \tau_{n_0+1}(Y_s, \beta_s)$ then $w(j((t,s)))) > w_0$. Indeed, for any affine Zariski open subset $\operatorname{Spec} R \subset U \times M^2$ intersecting Z_0 non-trivially, let $I \subset R$ be the ideal of functions that vanish on $q^{-1}(a)$ and let $\hat{R} = \varprojlim R/I^n$. Let $f \in R$ be the local equation for X, and let $g \in R$ be the local equation for Y. Let $f = f_1 \cdot \ldots \cdot f_N, g = g_1 \cdot \ldots \cdot g_M$ be decompositions into factors pairwise coprime in $\hat{R}$. Then by the Chinese remainder theorem for all $u \in U$

$$w(j(u)) = \sum_{i,j} \dim_{k(j(u))} \hat{R}/(f_i, g_j) \otimes k(u)$$

Let f_α and g_β be local equations for α, β and let $w_1 = \min_{u\in U} \dim_{k(j(u))} \hat{R}/(f_\alpha, g_\beta) \otimes k(u)$. If $\tau_{n_0+1}(X_t, \alpha_t) = \tau_{n_0+1}(Y_s, \beta_s)$ then $\dim_{k(j((t,s)))} \hat{R}/(f_\alpha, g_\beta) \otimes k(t,s) > w_1$. Since by Lemma 3.13 for each pair of prime factors f_i, g_j the value

$$\dim_{k(j(u))} \operatorname{Spec} R/(f_i, g_j) \otimes k(u)$$

is upper semicontinuous in u, it follows that $w(j((t,s))) > w_0$.

We will prove the statement of the proposition assuming that the morphism $p : Z \to U$ is finite and then show how the general case can be reduced to this one. Since W is open in Z, it is flat over U by Facts 3.10(i) and (ii). By Lemma 3.13 there exists a constant l_0 such that

$$w(j(u)) + \sum_{z\in W_u} w(z) = l_0$$

for all $u \in U$. By Lemma 3.11 the morphism $W \to U$ is a composition of an open embedding and a finite flat morphism, so Lemma 3.14 can be applied to $W \to U$. We get

$$\{\ u \in U\ \mid\ \sum_{z\in W_u} w(z) < l_0 - w_0\ \} \subseteq \{\ u \in U\ \mid\ \#W_u < m - 1\ \}.$$

The latter set is the same as $\{\ u \in U\ \mid\ \#Z_u < m\ \}$ since $\#Z_u = \#W_u - 1$, and we get the desired conclusion.

If the morphism $p : Z \to U$ is not finite, it is still a composition of an open embedding and a finite flat morphism. Indeed, let $\overline{M}$ be a smooth projective curve that contains M, and let $\bar{X}, \bar{Y}$ be closures of X, Y in $\overline{M}^2 \times T, \overline{M}^2 \times S$, respectively, and let $\bar{p} : \bar{X} \times_{\overline{M}^2} \bar{Y} \to T \times S$ be the natural projection, then by Lemma 3.11 there exists an open $\bar{U} \subset T \times S, \bar{U} \supset U$ such that $\bar{X} \times_{\overline{M}^2} \bar{Y} \cap \bar{p}^{-1}(\bar{U})$ is flat over $\bar{U}$. Define $\bar{Z} = \bar{X} \times_{\overline{M}^2} \bar{Y} \cap \bar{p}^{-1}(U), \overline{W} = \bar{Z} \setminus Z_0$, note that Z_0 is a closed subscheme of $\bar{Z}$ and that since $(\bar{Z} \setminus Z_0) \cap Z = Z \setminus Z_0 = W$ it follows that $\overline{W} \setminus W = \bar{Z} \setminus Z$. Since $\bar{Z} \setminus Z$ is closed, by Lemmas 3.13 and 3.12,

$$m = \max_{u \in U} \#\bar{Z}_u \qquad \sum_{z \in \bar{Z}_u} w(z) \equiv l_0 = \max_{u \in U} \sum_{z \in Z_u} w(z)$$

We have shown before that

$$\{\ u \in U\ \mid\ \sum_{z \in \overline{W}_u} w(z) < l_0 - w_0\ \} \subseteq \{\ u \in U\ \mid\ \#\bar{Z}_u < m\ \}.$$

Observe that

$$\begin{array}{l} \{u \in U\ \mid\ \sum_{z \in W_u} w(z) < l_0 - w_0\} = \\ \{u \in U\ \mid\ \sum_{z \in \overline{W}_u} w(z) < l_0 - w_0\} \cup \bar{p}(\bar{Z} \setminus Z) \end{array}$$

and that

$$\{\ u \in U\ \mid\ \#Z_u < m\ \} = \{\ u \in U\ \mid\ \#\bar{Z}_u < m\ \} \cup p(\bar{Z} \setminus Z)$$

which implies

$$\{\ u \in U\ \mid\ \sum_{z \in W_u} w(u) < l_0 - w_0\ \} \subseteq \{\ u \in U\ \mid\ \#Z_u < m\ \}.$$

Since $w_0 + \sum_{z \in W_u} w(u) \leq w(j(u)) + \sum_{z \in W_u} w(u) \leq l_0$, the last inclusion implies the statement of the proposition. □

4 Interpretation of the field

4.1 Generically unramified projections

In positive characteristic, if the projection $p_2 : Z \to M$ 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. This situation would cause problems in the Subsections 4.2 and 4.3 when the group configurations are constructed. In this section we prove Lemmas 4.3 and 4.2 that will help us construct curves in M^2 with projections on both factors M generically unramified, and Lemma 4.1 that guarantees that for any curve $X \subset M^2$ the slope is defined on a dense open subset of either X or X^{-1}.

We recall that a quasi-finite morphism $f : X \to Y$ is unramfied in a point $x \in X$ if $k(x)/k(f(x))$ is a separable extension of fields, and $\Omega_{X/Y} \otimes k(x) = 0$. We refer the reader to any standard algebraic geometry reference (e.g. [18, Section 6.2.1], [9, Section IV.2]) for the details on Kähler differentials and ramification.

Lemma 4.1. *Let M be an irreducible curve over a field of any characteristic. Let $X \subset T \times M \times M$ be a family of closed curves parametrized by an irreducible variety T such that X is irreducible. Then there exists a dense open $U \subseteq T$ such that either $p_1 : X_t \to M$ for each $t \in U$ or $p_2 : X_t \to M$ for each $t \in U$ is étale.*

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 $p_i : X_\xi \to M_\xi$ the natural projections. The lemma is clear if either p_1 or p_2 is not dominant. So we may assume that this is not the case.

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. Consider the natural map of sheaves

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

which is surjective because X_ξ embeds into M_ξ^2. Taking stalks at the generic point χ of X_ξ we get a surjective map f of vector spaces over the field $k(\chi) = k(X)$

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

Since f is surjective and $\dim_{k(\chi)} \Omega_X \otimes k(\chi) = 1$, restiction to at least one of the summands must be an isomorphism.

Without loss of generality assume that f_1 is an isomorphism. Then the sheaf of relative differentials $\Omega_{X/M}$ (with respect to the first projection) is zero. Therefore p_1 is unramified over a dense open subset of M_ξ, and together with the Fact 3.9 , this implies, by definition, that p_1 is generically étale. □

Recall that if $f : X \to Y$ is a morphism of schemes over a field of characteristic p then $\mathrm{Fr}_f : X \to X^{(p/Y)} = X \times_{f,Y,\mathrm{Fr}_Y} Y$, the *relative Frobenius morphism*, is defined to be $\mathrm{Fr}_X \times f$ where $\mathrm{Fr}_X, \mathrm{Fr}_Y$ 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 $X = \operatorname{Spec} R, Y = \operatorname{Spec} S, S = R[r_1, \ldots, r_n]/I$ then $X^{(p/Y)} = R[r_1', \ldots, r_n']/I^{(p)}$ where $I^{(p)} = \{\ f^{(p)} = \sum_J a_J^p (r')^J \ \mid\ f = \sum_J a_J r^J \in I\ \}$ (where J is a multiindex) and $\mathrm{Fr}^*_{X/Y}(r_i') = r_i^p$. On the level of points, if $X \hookrightarrow Y \times \mathbb{A}^n$ then $\mathrm{Fr}_{X/Y}(y, x_1, \ldots, x_n) = (y, x_1^p, \ldots, x_n^p)$.

Lemma 4.2. *Let $f : X \to Y$ be a finite morphism of irreducible varieties over a field of characteristic $p > 0$ and let $F = \mathrm{Fr}_f$ be the relative Frobenius morphism. Assume that f is everywhere ramified. Then there exists $n > 0$ such that $F^n(X) \to Y$ is generically unramified.*

Proof. Since f is everywhere ramified, the field extension $k(X) \subset k(Y)$ is inseparable. Let L be the separable closure of $k(X)$ in $k(Y)$, then $k(X) \subset L$ is a separable extension and $L \subset k(Y)$ is a purely insepearable extension. Let n be the exponent of this extension, that is, the smallest natural number n such that $f^{p^n} \in k(X)$ for

any $f \in k(Y)$. We claim that $k(F^n(X)) \subset L$, and this would suffice to prove the lemma since $k(F^n(X))$ then would be separable extension of $k(Y)$.

Let $X_0 \subset X$, $Y_0 \subset Y$ be dense open affine subvarieties such that Y_0 is finite over X_0. Then $k[Y_0] = k[X_0][f_1, \ldots, f_n]/I$ and $k[F^n(Y_0)] = k[X_0][g_1, \ldots, g_n]/I^{(p^n)}$. If an embedding $k[Y_0] \subset k(Y_0)$ is chosen then it is immediate from the definition of the relative Frobenius morphism that there exists an injection $k[F^n(Y_0)] \hookrightarrow L$ sending g_i to $f_i^{p^n}$, and we conclude. □

Lemma 4.3. *Let $X \subset M^2 \times T$, $Y^2 \times S$ be two families of curves. Let $p_{23} : M^2 \times T \to M^2 \times T$, $q_{23} : M^2 \times S \to M \times S$ be projections. Let $m > 1$ be an integer and let $X' = F^m_{p_{23}}(X)$, $Y' = F^m_{q_{23}}(Y)$. Then*

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

Proof. Let $r_{1345} : M \times M \times M \times T \times S \to M \times M \times T \times S$, $r'_{1345} : M \times M^{(p)} \times M \times T \times S \to M \times M \times T \times S$ be projection morphisms. After unravelling the definitions one observes that $X \circ Y^{-1}$, resp. $X' \circ (Y')^{-1}$, is the image $r_{1345}(Z)$, resp. $r'_{1345}(Z')$, where $Z' = \mathrm{Fr}_{r_{1345}}(Z)$ and Z is a closed subscheme of $M^3 \times T \times S$. □

4.2 Interpretation of a one-dimensional group

Lemma 4.4. *Each endomorphism $\varphi \in \mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1})$ is determined by its action on ε. Denote the natural map induced by truncation $r : \mathrm{End}(k[\varepsilon]/(\varepsilon^{n+1}) \to \mathrm{End}(k[\varepsilon]/(\varepsilon^2))$. Then*

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

Proof. Straightforward (see a similar statement for formal power series, for example, in [6, Corollary 7.17]). □

Lemma 4.5. *Let M be a curve over k, and let $X \subset M^2 \times T$ be an almost faithfully parametrized family of one-dimensional constructible sets in M^2, $\dim T = 2$.*

Then there exists an almost faithfully parametrized family of definable curves $Y \subset M^2 \times S$, $\dim S = 1$, definable in (M, X), a locally closed irreducible set $S_0 \subset S$, a point $a \in M^2$, $a_1 = a_2$, such that $a \in Y_s$ for all $s \in S_0$, and a family of branches β of Y 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 $H \subset \mathrm{Aut}(k[x]/(x^{n+1}))$.

Proof. Pick an irreducible component T_0 of T of dimension 2 and an irreducible component X' of X such that X_0 dominates T_0. Let M_0 be the connected component of M such that $M_0^2 \times T_0$ contains X'. By Lemma 4.1, 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 of T_0, and by Lemma 4.2 there exists a number n such that for

t in a dense open subset of T_0 the restriction of p_2 to $X''_t = \mathrm{Fr}^n_{p_{23}}(X'_t)$ is dominant over M_0 and generically unramified.

Let U be the set of points $x \in X''$ such that the restriction of $p_2 : M_0^2 \times T \to M_0$ to X''_t, where t is such that $x \in X''_t$, is unramified at x. The set U is dense in X by construction of X'' due to Lemma 4.2. For each $a \in M_0^2$ consider the set $S^a \subset T_0$ of points t such that $a \in X''_t$. It follows from dimension considerations that there exists an $a \in M^2$ and an irreducible component $S_0 \subset S^a$ 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 $t \in S_0$.

The point $a \in X''_t$ is smooth for any $t \in S_0$, therefore, there exists a unique family of branches α of $X'' \cap M^2 \times S_0$ at a, which is also a family of branches of X'_t at a. It also follows that $\tau_1(X'_t, \alpha_t) \neq 0$ and so by Lemma 4.4 $\tau_n(X'_t, \alpha_t) \in \mathrm{Aut}(k[x]/(x^{n+1}))$ for all $n \geq 1$ for all $t \in S_0$. Pick some $t_0 in S_0$ and let $Y = X \circ X_{t_0}^{-1}$. Then by Lemma 4.3 $\tau_1(Y_t, \alpha_t \circ \alpha_{t_0}^{-1}) = \tau_1(X'_t \circ (X'_{t_0})^{-1}, \alpha_t \circ \alpha_{t_0}^{-1}) \in \mathrm{Aut}(k[x]/(x^{n+1}))$ for any $t \in S_0$. Clearly, $\alpha \circ \alpha_{t_0}^{-1}$ is a family of branches at a point $b \in M_0^2$ such that $a_1 = a_2$.

By Krull Intersection theorem, there exists the smallest number n such that the set of slopes $\tau_n(X_t, \alpha_t)$ as t ranges in S_0 is not constant, and hence one-dimensional. If $n = 1$, the family Y satisfies the statement of the Lemma over the irreducible component S_0. Otherwise, the slope $\tau_{n-1}(X'_t, \alpha_t)$ as t ranges in S_0 is constant, and therefore $\tau_{n-1}(Y_t, \alpha_t \circ \alpha_{t_0}) = 1$. It follows that $\tau_n(Y_t, \alpha_t \circ \alpha_{t_0})$ almost coincides with $\mathrm{Ker}(\mathrm{Aut}(k[x]/(x^{n+1})) \to \mathrm{Aut}(k[x]/(x^n)))$. Therefore, in this case the family Y also satisfies the statement of the Lemma over the irreducible component S_0. □

Theorem 4.6. *Let M be a smooth curve and let $X \subset M^2 \times T$ be an almost faithful family of constructible sets such that X_t is of pure dimension 1 for $t \in T_0$ where $T_0 \subset T$ is an irreducible locally closed subset,* $\dim T_0 = \dim T = 2$. *Then (M, X) interprets a one-dimensional group.*

Proof. We prove the theorem by constructing a group configuration.

Let $Y \to S$ be a definable family of curves, $\dim S = \deg S = 1$, let $S_0 \subset S$ be a locally closed irreducible set, and assume that there exists $x \in M^2$, $x_1 = x_2$ a family of branches α of Y at x such that for all $s \in S_0$ the set of slopes $\{\tau_n(Y_s, \alpha_s) \mid s \in S_0\}$ almost coincides with a connected 1-dimensional subgroup $H \subset \mathrm{Aut}(k[\varepsilon]/(\varepsilon^{n+1}))$ for some n; such a family exists by Lemma 4.5. Let $Y_0 = Y \cap M \times S_0$. We may assume that all irreducible components of $Y_0 \to S_0$ are dominant over S_0 and that S_0 is smooth at the price of possibly shrinking S_0. Let K be a field of infinite transcendence degree over the base field k. Let $s, t \in S_0(K)$ be independent generic points. Note that they are generic and independent in the sense of the reduct (M, X) too.

Pick $u \in S_0(K)$ such that

$$\tau_n(Y_u, \alpha_u) = \tau_n(Y_s, \alpha_s) \circ \tau_n(Y_t, \alpha_t).$$

Such u exists since the slopes of $\tau_n(Y_t, \alpha_t)$ and $\tau_n(Y_s, \alpha_s)$ are generic in H, and so $\tau_n(Y_s, \alpha_s) \circ \tau_n(Y_t, \alpha_t)$ is generic in H too. Since the slopes of curves parametrized by

S_0 almost coincide with H, there exists a generic parameter $u \in S_0(K)$ fitting the above equality.
Claim: u is algebraic over t, s.

Proof. By Proposition 3.5 $\tau_n(Y_t \circ Y_s, \alpha_t \circ \alpha_s) = \tau_n(Y_t, \alpha_t) \circ \tau_n(Y_s, \alpha_s)$. Let $l = \max_{\bar{t},\bar{s},\bar{u} \in S_0} \#(Y_{\bar{t}} \circ Y_{\bar{s}} \cap Y_{\bar{w}})$ then by 3.12, $l = \#((Y_t \circ Y_s) \cap Y_u)$ for (t, s, u) generic in $S_0 \times S_0 \times S_0$. By Lemma 3.11 and Proposition 3.15 the set of parameters $w \in S_0$ such that $\tau_n(Y_w, \alpha_w) = \tau_n(Y_t, \alpha_t) \circ \tau_n(Y_s, \alpha_s)$ is contained in

$$\{\ w \in S(K)\ \mid\ \dim(Y_t \circ Y_s \cap Y_w) = 1 \text{ or } \#(Y_t \circ Y_s \cap Y_w) < l\ \}$$

This set is finite, (M, X)-definable, and contains u, which is what we had to show. $\square_{\text{Claim}}$

By the same argument, t is algebraic over u, s, and s is algebraic over t, u.

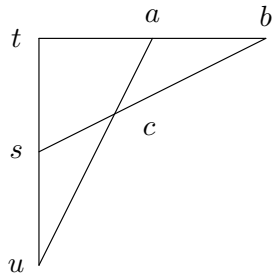
In a similar vein, let a be a point of S_0 independent from t, s, and let $b, c \in S_0$ be such that

$$\begin{aligned} \tau_n(Y_b, \alpha_b) &= \tau_n(Y_t, \alpha_t) \circ \tau_n(Y_a, \alpha_a), \text{ and} \\ \tau_n(Y_c, \alpha_c) &= \tau_n(Y_s, \alpha_s) \circ \tau_n(Y_b, \alpha_b) \end{aligned}$$

Then

$$\begin{aligned} & \tau_n(Y_c, \alpha_c) = \tau_n(Y_s, \alpha_s) \circ \tau_n(Y_b, \alpha_b) = \\ = \ & \tau_n(Y_s, \alpha_s) \circ \tau_n(Y_t, \alpha_t) \circ \tau_n(Y_a, \alpha_a) = \\ = \ & \tau_n(Y_u, \alpha_u) \circ \tau_n(Y_a, \alpha_a) \end{aligned}$$

By the same argument as above, for each line in the configuration



any vertex is algebraic over the other two, that is, this is a group configuration. By Fact 2.4 there exists a one-dimensional group interpretable in (M, X). $\square$

Proposition 4.7. *Assume that the family Y in the proof of Theorem 4.6 is such that the set of values of $\tau_n(Y_t, \alpha_t)$ almost coincides with a subgroup of $\mathrm{Aut}(k[\varepsilon]/(\varepsilon^{n+1}))$ isomorphic to $\mathbb{G}_a$. Then the connected component of the identity of the group from the conclusion of the theorem is not isomorphic to $\mathbb{G}_m$.*

Proof. 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 $\mathrm{acl}(a) = \mathrm{acl}(e), \mathrm{acl}(b) = \mathrm{acl}(f), \mathrm{acl}(x) = \mathrm{acl}(y)$ then G_1 and G_2 are not interalgebraic.

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

4.3 Interpretation of the field

Lemma 4.8. *Let E be an elliptic curve and Z be a closed one-dimensional irreducible subset of $G = E^2$. Identify T_gG with T_0G via the isomorphism $d\lambda_g : T_0G \to T_gG$, for $\lambda_g(x) = g \cdot x$. Suppose that for any $z \in Z$ the tangent space $T_zZ \subset T_0G$ is constant. Then Z is a coset of a closed subgroup of G.*

Proof. Since Z is a projective curve with a trivial tangent bundle, it is an elliptic curve itself. Since any morphism between Abelian varieties with finite fibres and preserving the identity automatically preserves the group structure by the Rigidity Theorem ([24]), Z is a coset of an Abelian subvariety of G. □

Let M be a curve, and consider a curve $Z \subset M^2$. For every point $z \in Z$ such that p_1 is étale in the neighbourhood of z, there exists a unique branch at x, call it α_z. We will use notation $\tau_n(Z, z) := \tau_n(Z, \alpha_z)$. For any group G with identity $e \in G$, for any $x = (x_1, x_2) \in G^2$ define the maps $t_x : G^2 \to G^2$ and for any one-dimensional locally closed subset $Z \subset G^2$ define the set $s_n(Z) \subset \mathrm{End}(k[x]/(x^{n+1})$:

$$t_x(y_1, \ldots, y_n) = (x_1^{-1} \cdot y_1, x_2^{-1} \cdot y_2) \quad s_n(Z) = \{\ \tau_n(t_z(Z), (e, e))\ \mid\ z \in Z\ \}$$

Also define $u_c : \mathbb{G}_a^2 \to \mathbb{G}_a^2, c \in k$

$$u_c(y_1, \ldots, y_n) = (y_1, y_2 - cy_1)$$

Lemma 4.9. *Let G be an algebraic group such that the connected component of the identity G_0 is isomorophic to $\mathbb{G}_a$. Let $Z \subset G^2$ be a one-dimensional constructible subset that is not a Boolean combination of cosets of subgroups of G^2. Then there exists a set $W \subset M^n$ definable in (G, Z), and an irreducible component $W' \subset W \cap G_0$ of pure dimension 1, such that $\dim s_1(W') = 1$. In characteristic 0, one can take $W = Z$.*

Proof. Replacing Z by a shift, we may assume that there exists an irreducible component $Z_0 \subset Z$ such that $(0, 0) \in Z_0$ that is not contained in a coset. We will construct a finite sequence of curves $W_i \subset \mathbb{G}_a^n, W_0 = Z_0$ that are irreducible components of curves definable in (G, Z), such that

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

is strictly decreasing.

We may also assume that $(0, 0) \in Z_0$. We also pick the local coordinate systems on $\mathbb{G}_a$ in a uniform way, with $\mathcal{O}_{\mathbb{A}^1,c} \cong k[[x]]$ given by sending $f - f(c)$ to x for

some fixed non-zero linear function f. Clearly, $\tau_1(u_c(Z), z) = \tau_1(Z, (0,0)) - c$ and $\tau_n(Z, y) = \tau_n(t_x(Z), t_x(y))$ for any $x \in \mathbb{G}_a^2$.

If $N(W_i) > 1$, then it follows from Proposition 3.8 that $\tau_1(W_i - t_x(W_i), (0,0)) = 0$ for all $x \in W_i$ and since W_i was not a coset, $W_i - t_x(W_i)$ also is not a coset for $x \neq 0$. Pick some such x and define $Y_i = W_i - t_x(W_i)$. If $s_1(W_i) = \{c\}$ then $s_1(Y_i) = \{0\}$ and since Y_i is not a coset, p_2 restricted to $u_c(Y_i)$ is dominant and everywhere ramified. In particular, it follows that in characteristic 0, $N(W_0) = 1$.

By Lemma 4.2 there exists a number m such that p_2 restricted to $Y_i' = \mathrm{Fr}_{p_2}^m(Y_i)_{\mathrm{red}}$ is generically unramified. Define $W_{i+1} = Y_i \circ Y_i^{-1}$, then by Lemma 4.3 $W_{i+1} = Y_i' \circ (Y_i')^{-1}$ and so p_2 restricted to W_{i+1} is generically unramified. For any point $a \in Y_i'$ such that p_1 is étale over M_0 in some neighbourhood, let $y - f$ be its local equation. Then the local equation at the point $\mathrm{Fr}_{p_2}^{-m}(a)$ is $y - f^{p^m}$. It follows that $N(W_{i+1}) < N(W_i)$. Therefore for some finite l, $N(W_l) = 1$. □

Lemma 4.10. *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 one-dimensional constructible subset that is not a Boolean combination of cosets of subgroups of G^2. Then either there exists an irreducible subset $Z_0 \subset Z$ 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 the local coordinate systems on $\mathbb{G}_m$ uniformly as in the proof of Lemma 4.9. 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 the least $n > 1$ such that $\dim s_n(Z_0) = 1$. Then by the same reasoning as in the proof of Lemma 4.5 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 $\mathrm{Ker}(\mathrm{Aut}(k[x]/(x^{n+1}) \to \mathrm{Aut}(k[x]/(x^n)) \cong \mathbb{G}_a\ \mathbb{G}_a$. The definable family Y can be used to construct a group configuration as in the proof of Theorem 4.6, and therefore a group is interpretable in (G, Z). By Proposition 4.7, the connected component of the idenity of this group is not isomorphic to $\mathbb{G}_m$. □

Theorem 4.11. *Let G be a one-dimensional algebraic group over an algebraically closed field, $Z \subset G^2$ be 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 4.8, 4.9 there exists a definable family $Y \subset G^2 \times S$ of curves, $\dim S = \deg S = 1$, and an irreducible locally closed set $S_0 \subset S$ such that there is a unique branch 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 4.10 either such family exists or a definable group G' containing $\mathbb{G}_a$ 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. We may assume that all irreducible

components of $Y_0 \to S_0$ are dominant over S_0 and that S_0 is smooth at the price of possibly shrinking S_0. Let K be a field of infinite transcendence degree over the base field k. Since $\mathrm{End}(k[x]/(x^2) \cong k$ by Proposition 3.7, we will use multiplicative notation for composiotion of slopes of first order.

Take $a_1, a_2, b_1, b_1, u \in S_0(K)$ 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, the values of slopes in the right hand side of the equations above are generic in $\mathrm{End}(k[x]/(x^2))$ for generic 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 can be picked 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 3.5 and 3.8,

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

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 intersections is a first-order property, it does not matter what particular parameters a_i, b_i, c_i we take as long as they are generic and independent (in the sense of (M, X)). By Lemma 3.11 and Proposition 3.15 the (M, X)-definable set

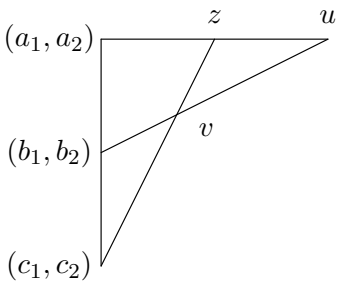
$$\{\ w \in S_0 \ \mid\ \dim(Y_w \cap (Y_{a_1} \circ Y_{b_1})) = 1 \text{ or } \#(Y_w \cap (Y_{a_1} \circ Y_{b_1})) < l_1\ \}$$

contains c_1 and by definition of l_1 is finite. By Lemma 3.11 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 3.11 and Proposition 3.15, we deduce that all 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 2.4 there exists a two-dimensional group definable in $(G, \cdot, Z)$ that acts transitively on a one-dimensional set.

The conditions of the Fact 2.5 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 $\mathrm{tp}(\tau_1(Y_z, \alpha_z), \tau_1(Y_u, \alpha_u)/B)$ in the full Zariski structure. Since the natural morphism $S_0 \to \mathrm{Aut}(k[\varepsilon]/(\varepsilon^2), s \mapsto \tau_1(Y_s, \alpha_s)$ has finite fibres, a canonical base of $\mathrm{tp}(z, u/a_1, a_2$ is interalgebraic 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 $\mathrm{tp}(z, u/a_1, a_2)$ is interalgebraic with $\{a_1, a_2\}$. The same argument applies to $\mathrm{tp}(u, v/b_1, b_2)$ and $\mathrm{tp}(z, v/c_1, c_2)$.

By Fact 2.6, the group G is isomorphic to the affine group $\mathbb{G}_a(k) \rtimes \mathbb{G}_m(k)$ of an infinite definable field k. □

Theorem 4.12. *Let M be a curve over k and let $X \subset M^2 \times T \subset M^2 \times M^l$ be a constructible set such that X_t is a pure-dimensional curve for t in a dense open subset of T. Then (M, X) interprets a field.*

Proof. Conjunction of Theorem 4.6 and Theorem 4.11. □

Remark. This field is definably isomorphic to k by [28, 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 also like to thank Moshe Kamensky for some comments and suggestions.

References

[1] E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.

[2] 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.

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

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

[5] 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.

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

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

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

[9] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. ISBN 0-387-90244-9. Graduate Texts in Mathematics, No. 52.

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

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

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

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

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

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

[16] J. C. Jantzen. *Representations of algebraic groups*. Number 107. American Mathematical Soc., 2007.

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

[18] Q. Liu and R. Erne. *Algebraic Geometry and Arithmetic Curves*, volume 6. Oxford University Press, 2006.

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

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

[21] 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`.

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

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

[24] D. Mumford. *Abelian varieties*. Oxford University Press, 1970.

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

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

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

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

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

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

[31] T. Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`, 2018.

[32] L. Van den Dries. *Tame topology and o-minimal structures*, volume 248. Cambridge university press, 1998.

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

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