K-Theory (2008) 38:135–152
DOI 10.1007/s10977-007-9015-0

A remark on transitivity of Galois action on the set of uniquely divisible abelian extensions in $\mathbf{Ext}^1(E(\overline{\mathbb{Q}}), \Lambda)$

Misha Gavrilovich

Received: 15 October 2005 / Accepted: 4 October 2007 / Published online: 22 December 2007

Abstract We study the double coset $Gal(\overline{\mathbb{Q}}/k)\backslash \mathrm{Ext}^1(E(\overline{\mathbb{Q}}), \Lambda)/\mathrm{Aut}(\Lambda)$, and interpret our results as partially showing that the notion of a path on a complex elliptic curve E can be characterised algebraically. The proofs show that our results are just concise reformulations of Kummer theory for E as well as the description of the image of the Galois action on the Tate module. Namely, we prove (a),(b) below by showing they are equivalent to (c) which is well-known: (a) uniquely divisible abelian $\mathrm{End}E$-module extensions of the group $E(\overline{\mathbb{Q}})$ of algebraic points of an elliptic curve, by $\Lambda \cong \mathbb{Z}^2$, lie in finitely many double cosets in $Gal(\overline{\mathbb{Q}}/k)\backslash \mathrm{Ext}^1(E(\overline{\mathbb{Q}}), \Lambda)/\mathrm{Aut}(\Lambda)$ (b) natural algebraic properties characterise the Poincaré's fundamental groupoid of a complex elliptic curve, restricted to the algebraic points, (c) up to finite index, the image of the Galois action on the sequences $(P_i)_{i>0}$, $jP_{ij} = P_i, i, j > 0$ of points $P_i \in E^k(\overline{\mathbb{Q}})$ is as large as possible with respect to linear relations between the coordinates of the points P_i's. Our original motivations come from model theory.

Keywords Fundamental groupoid · Galois group · Abelian group extensions · Categoricity · Elliptic curve · Tate module · Kummer theory · Logic

1 Introduction

In Sects. 1.1 and 1.2 we briefly state our main results and motivations; in Sects. 1.3 and 1.5 we sketch the relation to arithmetics.

1.1 Abelian group extensions

The universal covering space of an elliptic curve $A = E$ is just $\mathbb{C}$; the linear structure on $\mathbb{C}$ plays an important rôle in the theory of (complex) elliptic curves as algebraic varieties.

M. Gavrilovich (✉)
Balliol College, University of Oxford, Oxford OX1 3BJ, UK
e-mail: gavrilovich@gmail.com
URL: http://misha.uploads.net.ru

This suggests that the relevant linear structure on $\mathbb{C}$ is determined up to isomorphism by the algebraic curve itself. The linear structure is that of a uniquely divisible abelian extension of the group $E(\mathbb{C})$ by $\mathbb{Z}^2$; thus, the above considerations suggest that such an extension is unique, up to an $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$-automorphism of $E(\mathbb{C})$ and an $End\,E$-module automorphism of the kernel $\Lambda \cong \mathbb{Z}^2$.

The next proposition partially confirms these suggestions. We conjecture it holds for $\mathbb{C}$ and in general, any algebraically closed field of zero characteristic.

Note that that we consider a somewhat unusual action of $Gal(\overline{\mathbb{Q}}/k)$ on $\mathrm{Ext}^1(E(\overline{\mathbb{Q}}), \Lambda)$, namely the one induced by the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on the first argument $E(\overline{\mathbb{Q}})$ where E is defined over k.

Proposition 1 *Let E be an elliptic curve defined over a number field $k \subset \overline{\mathbb{Q}}$. Assume that all the endomorphisms of E are definable over k. Then the set of uniquely divisible* $\mathrm{End}\,E$*-module extensions in* $\mathrm{Ext}^1_{\mathrm{End}\,E\text{-}mod}(E(\overline{\mathbb{Q}}), \Lambda)$ *of* $\mathrm{End}\,E$*-modules, splits into finitely many double cosets of the set* $Gal(\overline{\mathbb{Q}}/k)\backslash \mathrm{Ext}^1(E(\overline{\mathbb{Q}}), \Lambda)/\mathrm{Aut}(\Lambda)$.

Here Λ denotes the kernel of the $\mathrm{End}\,E$-module covering map $\mathbb{C} \to E(\mathbb{C})$. We prove the proposition by an inductive argument using Kummer theory of E and the description of Galois action on the Tate module; moreover, the proof shows that Proposition 1 is equivalent to these arithmetic results.

1.2 An algebraic notion of a path up to homotopy

We ask whether *the notion of paths* (*up to fixed point homotopy*) *on an elliptic curve* $E(\mathbb{C})$ *may be described by its natural algebraic properties*. "Paths up to fixed point homotopy" are usually thought of in the context of the *Poincaré's fundamental groupoid*, which can be thought of as a 2-functor. Hence, we may reformulate the question as: *Is the fundamental groupoid functor on the complex algebraic varieties determined by its natural algebraic properties up to natural equivalence and an automorphism of the source category?*

In terms of category theory the above could be expressed as follows. Consider the composite functor $V \longrightarrow^{i} \mathfrak{Top Spaces} \longrightarrow^{h} \mathfrak{HD}$ where V is a category of algebraic varieties over a field K, $\mathfrak{Top Spaces}$ is the category of topological spaces, and $\mathfrak{HD}$ denotes a category of some kind of algebraic homotopy data associated with topological spaces, say fundamental groupoids. The composite functor $i \circ h : V \longrightarrow \mathfrak{HD}$ is a functor between two categories, both algebraically defined, and it makes sense to ask whether the composite functor $i \circ h$ can be characterised by its algebraic properties. However, there is a lot of freedom in choosing the embedding $i = i_\sigma : V \longrightarrow \mathfrak{Top Spaces}$ which depends on an embedding $\sigma : K \to \mathbb{C}$. Therefore, it may be better to ask whether the family of functors $\{i_\sigma \circ h : V \longrightarrow \mathfrak{HD} \mid \sigma : K \to \mathbb{C}\}$ admits an algebraic characterisation. In this paper we consider $V = \mathfrak{E}$ to be the full subcategory consisting of Cartesian powers of an elliptic curve, take $h = \pi_1^{\mathrm{top}}$ to be the fundamental groupoid functor (to the category of strict groupoids), and $K = \overline{\mathbb{Q}}$. Then the question becomes whether we can characterise the family of functors $\{i_\sigma \circ \pi_1 : \mathfrak{E} \longrightarrow \mathfrak{Groupoids} \mid \sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})\}$.

Proposition 2 is a partial positive answer to this question.

Proposition 2 **(**Universality of fundamental groupoid functor) *Let E and k be as in Proposition 1. Let $\mathfrak{E}$ be the full subcategory of $Var/\overline{\mathbb{Q}}$ consisting of Cartesian powers of E.*

Let $\underline{\Omega} : \mathfrak{E} \to \mathfrak{Groupoids}$ be a functor satisfying conditions (1)–(3) *of Definition 1 below* (*unique path-lifting along étale morphisms, preservation of direct product, etc*).

Assume further that

(4) $\underline{\Omega}(E)$ *is a connected groupoid*
(5) *there is an isomorphism*

$$\Omega_{0,0}(E) := \{\gamma \in \Omega(E) : s(\gamma) = t(\gamma) = 0\} \cong \mathbb{Z}^2 \text{ as } \mathrm{End}E\text{-modules}.$$

Then there exists finitely many functors $\mathbb{F}_1, \ldots, \mathbb{F}_n : \mathfrak{E} \to \mathfrak{Groupoids}$ *satisfying conditions* (1)–(5) *above such that for any functor* $\underline{\Omega}$ *satisfying* (1)–(5) *above there exists a Galois automorphism* $\sigma \in Gal(\overline{\mathbb{Q}}/k)$ *and a number* $0 < i < n + 1$ *such that* $\underline{\Omega}$ *and* $\mathbb{F}_i \circ \sigma$ *are naturally equivalent.*

Here $\mathfrak{Groupoids}$ denotes the category of strict groupoids.
We prove Proposition 2 by reducing it to Proposition 1.

1.3 Kummer theory and Galois representations

We prove Propositions 1 and 2 by a rather simple induction based on Kummer theory and the image of Galois action on the Tate module. The full proof is carried out in Sect. 4; here we just present an argument showing how these arithmetic results may be relevant. For simplicity assume $\mathrm{End}E = \mathbb{Z}$ and that E is defined over $\mathbb{Q}$. A uniquely divisible extension $H \to^{\varphi} E(\overline{\mathbb{Q}})$ induces extra structure on $E(\overline{\mathbb{Q}})$: for every point $x \in E(\overline{\mathbb{Q}})$, there is a countable family of distinguished sequences $(\varphi(v/n))_{n\in\mathbb{N}}, \varphi(v) = x$. Proposition 1 implies that for every two uniquely divisible extentsions as considered, their classes of families of distinguished sequences are conjugated by Galois action. Group automorphisms of $E(\overline{\mathbb{Q}})$ act on the set of extensions and then also on the corresponding classes of distinguished sequences; this implies that the action by Galois automorphisms and group automorphisms of $E(\overline{\mathbb{Q}})$ induce the same orbits on the set of all families of distinguished sequences associated to an extension of the required type. Therefore, if we consider action of group automorphisms on the tuples of distinguished sequences rather then on classes of families thereof, each orbit of group automorphisms action splits into at most countably many orbits of Galois action. Properties of profinite groups imply that then such an orbit splits into only finitely many orbits of Galois action. Now consider the distinguished sequences associated to $0 \in E(\overline{\mathbb{Q}})$; these form the Tate module $T(E)$; the considerations above imply that an $\mathrm{GL}_2(\hat{\mathbb{Z}})$-orbit splits into finitely many Galois orbits. This is the result of Serre on the image of Galois action on the Tate module. To see how to recover the statement of Kummer theory, consider, for example, the distinguished sequences associated to a pair of $\mathbb{Z}$-linearly independent rational points $x, y \in E(\mathbb{Q})$; similarly to above, $\hat{\mathbb{Z}}^2$ acts by shifts on the distinguished sequences associated to the points x and y, and the considerations above imply that we need that the image of Galois group action has at most finitely index in $\hat{\mathbb{Z}}$.

1.4 Model theory: motivations and generalisations

The results of this note appear naturally in a model-theoretic framework of stability theory and particularly «logically perfect structures» as developed by Zilber [23]; in this way they have been obtained in the author's DPhil thesis [6]. We believe that the context and techniques of model theory are essential to generalise our results to other varieties and fields of arbitrary cardinality including the field of complex numbers. However, in this note we do not discuss the model theoretic motivations and techniques; we refer to the the author's DPhil thesis [6] for that. The note presents only those results of the thesis which can be stated and proven in a model-theory free fashion; in particular, *the note omits the discussion of the*

Shafarevich conjecture on holomorphic convexity of universal covering spaces and the case of semi-Abelian varieties of higher dimension. The results follow a line originated by Zilber [22] treating fully the case of the multiplicative group of an algebraically closed field of characteristic 0.

1.5 Fields of arbitrary large cardinality and arithmetical questions

To prove Proposition 1 for fields of higher cardinality one needs to consider composites of linearly disjoint fields; this is a non-trivial observation due to model theory, namely the technique of *excellent classes* of Shelah [18,19]. The number theoretic questions appearing there, as shown in [22], involve linearly disjoint fields, tensor products of algebraically closed fields, and infinitely divisible points of $E(\bar{K} \otimes_{\bar{k}} \bar{K})$ over such fields. For example, a condition of the following type is useful to extend our results to fields of cardinality $\aleph_2$:

Condition of $(2, \aleph_0)$-existence. *Let $\bar{k} \subset \bar{K}$ be countable algebraically closed fields of characteristic 0. For a group H, let $\operatorname{div} H = \{h \in H : \forall N \exists n > N \exists h'\ h = nh'\}$ denote the subgroup of elements divisible by infinitely many integers. Then*

$$\operatorname{div} E(\bar{K} \otimes_{\bar{k}} \bar{K}) = E(\bar{K}) \otimes_{E(\bar{k})} E(\bar{K}) = \operatorname{div} E(\bar{K}) \otimes_{\operatorname{div} E(\bar{k})} \operatorname{div} E(\bar{K})$$

That is, a point of $E(\bar{K} \otimes_{\bar{k}} \bar{K})$ is infinitely divisible only if it so for trivial reasons, i.e. it is a product of divisible points of the copies of $E(\bar{K})$. It is conceivable that this question can be answered with techniques described in [4,10].

1.6 Structure of the paper

We state our results in detail in Sect. 2.

We prove Proposition 1 in Sect. 4. We establish the equivalence of the algebraic approach of Proposition 1 and the topological approach of Proposition 2 in Sect. 5. We state a precise conjecture about Shimura curves in Sect. 6.

We refer to [15,16] for the definitions and results on elliptic curves; see also [3–5,17,21] for later developments.

2 Results

In this section we state our results in full, and hint on a connection between the reformulations.

2.1 Uniquely divisible extensions of Abelian groups

Let E be an elliptic curve defined over a number field $k \subset \overline{\mathbb{Q}} \subset \mathbb{C}$, and let

$$0 \longrightarrow \Lambda \longrightarrow \mathbb{C} \xrightarrow{p} E(\mathbb{C}) \longrightarrow 0.$$

be the universal covering of $E(\mathbb{C})$. Let $0 \in E(k)$ denote a k-rational point which is zero of the additive group $E(\mathbb{C})$.

Proposition 1 *Let E be an elliptic curve defined over a number field $k \subset \overline{\mathbb{Q}}$. Assume that all the endomorphisms of E are definable over k. Then the set of uniquely divisible* $\operatorname{End} E$*-module extensions in* $\operatorname{Ext}^1_{\operatorname{End} E\text{-}mod}(E(\overline{\mathbb{Q}}), \Lambda)$ *of* $\operatorname{End} E$*-modules, splits into finitely many double cosets of the set* $Gal(\overline{\mathbb{Q}}/k) \backslash \operatorname{Ext}^1(E(\overline{\mathbb{Q}}), \Lambda) / \operatorname{Aut}(\Lambda)$.

We conjecture the proposition holds for any algebraically closed field of zero characteristic. Zilber [22] proves the transitivity of the $\mathrm{Aut}(\bar{K}/\mathbb{Q})$-action on $\mathrm{Ext}^1(\bar{K}^*, \mathbb{Z})$ for arbitrary algebraically closed field $K = \bar{K}$ of characteristic 0.

A way to think of the proposition is that it claims that *it is possible to describe the universal covering space of an elliptic curve in a purely algebraic way*, admittedly with respect to a rather weak, linear structure on it.

Note that the set of non-equivalent extensions $\mathrm{Ext}^1_{\mathrm{End}E\text{-mod}}(E(\overline{\mathbb{Q}}), \Lambda)$ is of cardinality $2^{\aleph_0}$. Moreover, the set of non-equivalent uniquely divisible abelian extensions is also of cardinality $2^{\aleph_0}$; indeed, any such extension can be modified by an $\mathrm{End}E$-module automorphism of $E(\overline{\mathbb{Q}})$ which generically gives rise to a different extension.

Also note that the injectivity of the profinite completion $\widehat{\Lambda}$ of the kernel Λ implies $\mathrm{Ext}^1_{\widehat{\mathrm{End}E\text{-mod}}}(E(\overline{\mathbb{Q}}), \widehat{\Lambda}) = 0$; thus if we replace Λ by $\widehat{\Lambda}$, the proposition becomes trivially true. And indeed, the theory of algebraic fundamental group can be used to define the "profinite completion" of the universal covering space of an algebraic variety in a purely algebraic way.

2.2 Relation between Propositions 1 and 2

Let us now informally indicate the relationship between Proposition 1 and Proposition 2. In Sect. 5 we use this interpretation to derive Proposition 2 from Proposition 1. Identify points in $\mathbb{C}$ and homotopy classes of paths in $E(\mathbb{C})$ starting at 1 via the period map $\gamma \longmapsto \int_\gamma dz$. Then the addition on $\mathbb{C}$ corresponds to the point-wise addition of paths, and dividing by n corresponds to the path-lifting along the étale morphism $nx : E(\mathbb{C}) \to E(\mathbb{C})$. Unique divisibility of $\mathbb{C}$ corresponds then to the unique path-lifting property along étale morphisms from $E(\mathbb{C})$ to $E(\mathbb{C})$.

These observations allow us to reformulate Proposition 1 as an algebraic characterisation of the Poincaré's fundamental groupoid of a complex elliptic curve, i.e. that *the notion of paths* (*up to fixed point homotopy*) *on a complex elliptic curve* $E(\mathbb{C})$ *may be described by its natural algebraic properties*.

The above reformulation can be naturally expressed in terms of logic by introducing a formal language to describe paths on an algebraic variety (cf. [6]). However, we can further reformulate the above in terms of category theory. Generalised slightly, the question then becomes: *Is the fundamental groupoid functor on* (*a subcategory of*) *the complex algebraic varieties determined by its natural algebraic properties up to natural equivalence and an automorphism of the source category?*

Proposition 2 provides a partial positive answer to this question; let us now introduce it in detail.

2.3 The universality property of the Poincaré's fundamental groupoid functor

In this subsection we introduce in detail the notions of category theory appropriate to state Proposition 2.

2.3.1 The example: fundamental groupoid functor $\pi_1^{\mathrm{top}}(E(\mathbb{C}))$ as a two-functor

It is convenient to consider 2-functors instead of functors to groupoids; the notions are equivalent. Before defining a 2-functor formally, we illustrate the notion by an example of Grothendieck [7].

The path 2-functor $\underline{\Omega}$ on the category $\mathfrak{Top}$ of topological spaces is a tuple $(\mathrm{Pt}, \Omega, s, t, \cdot)$ consisting of a *functor of points* $\mathrm{Pt} : \mathfrak{Top} \to \mathfrak{Sets}$ and a *paths functor* $\Omega : \mathfrak{Top} \to \mathfrak{Sets}$ together with the following data:

(1) $\mathrm{Pt}(T)$ is the set of points of topological space T and the morphism $\mathrm{Pt}(f) : \mathrm{Pt}(T_1) \to \mathrm{Pt}(T_2)$ is $f : T_1 \to T_2$ as a map of sets.
(2) $\Omega(T)$ is the set of all paths in topological space T, i.e. continuous functions $\gamma : [a, b] \to T$, $a, b \in \mathbb{R}$; similarly $\Omega(f)$, $f \in \mathrm{Hom}_{\mathfrak{Top}}(T_1, T_2)$ is the map taking a path $\gamma : [a, b] \to T_1$ into $f \circ \gamma : [a, b] \to T_2$.
(3) $s_T, t_T : \Omega(T) \to \mathrm{Pt}(T)$ are functions from the set of paths in T to their endpoints in T; the function $s(\gamma) = \gamma(a)$ (*source*) gives the beginning point of a path γ, and the function $t(\gamma) = \gamma(b)$ (*target*) gives the ending point of path γ.
(4) $\cdot_T : \Omega(T) \times \Omega(T) \to \Omega(T)$ is the partial operation of concatenation of paths, taking $\gamma_1 : [a, b] \to T$, $\gamma_2 : [b, c] \to T$ into $\gamma = \gamma_1\gamma_2$, $\gamma_{|[a,b]} = \gamma_1$, $\gamma_{|[b,c]} = \gamma_2$.

Thus, a 2-functor from $\mathfrak{Top}$ to $\mathfrak{Sets}$ consists of two functors $\mathrm{Pt}, \Omega : \mathfrak{Top} \to \mathfrak{Sets}$, and two natural transformations $s, t : \Omega \to \mathrm{Pt}$ from functor Ω to Pt; s stands for *source* and t stands for *target*. For each T, there is also a functorial associative operation $\cdot_T$ defined on $\Omega_{x,y}(T) \times \Omega_{y,z}(T) \to \Omega_{x,z}(T)$, where $\Omega_{x,y}(T) = \{\gamma \in \Omega(T) : s(\gamma) = x, t(\gamma) = y\}$, etc; the operation $\cdot$ makes $\Omega_{x,x}(T)$ into a group; in the example above, $\Omega_{x,x}(T)$ is the set of all loops in T based at $x \in T$.

In particular, for each T the set $\Omega(T)$ carries the structure of a groupoid; in fact, it is conventional to consider $\underline{\Omega}$ as a functor to the category of groupoids.

If in item (2) we define $\Omega(T)$ to be the set of all paths *up to fixed point homotopy*, then we obtain the notion of the fundamental groupoid functor. The advantage of the original definition is that one may try and define n-functors describing n-dimensional homotopies on topological space T, cf. Grothendieck [7] for motivations; Voevodsky–Kapranov [20] propose an exact definition. Grothendieck [7] explains that it is essential not to insist on strict associativity etc, but rather to consider *all the identities to hold up to a homotopy of higher dimension*. This may be useful to generalise Proposition 2.

2.3.2 Abstract fundamental groupoid functors

Here we define the path-lifting property for a 2-functor, and an abstract fundamental groupoid functor as a functor preserving direct products, possessing the path-lifting property and with a particular functor of points.

Definition 1 Let $\underline{\Omega}$ be a 2-functor from a subcategory $\mathfrak{C}$ of the category of varieties over an algebraically closed field K, into $\mathfrak{Sets}$. We say that $\underline{\Omega}$ is an *K-valued abstract fundamental groupoid functor* if $\underline{\Omega}$ satisfies the following properties:

(1) functor Pt is the functor of K-rational points:

$$\mathrm{Pt}(X) = X(K) = \mathcal{M}or_{\mathrm{Var}/K}(0, X)$$

(here 0 denotes a single point variety defined over k)
(2) functor Ω preserves direct products:

$$\Omega(X \times Y) = \Omega(X) \times \Omega(Y)$$

$$\Omega(f \times g) = \Omega(f) \times \Omega(g)$$

$$s_{X\times Y} = s_X \times s_Y, t_{X\times Y} = t_X \times t_Y$$

$$(\gamma_1 \times \gamma_2) \cdot_X (\gamma_1' \times \gamma_2') = (\gamma_1 \cdot_X \gamma_1') \times (\gamma_2 \cdot_X \gamma_2')$$

(direct product is taken in the category of $\mathfrak{S}ets$.)

(3) unique path-lifting property: if $p \in \mathrm{Hom}_{\mathfrak{E}}(X, Y)$ is an étale morphism of algebraic varieties, then for any point $x \in \mathrm{Pt}(X)$ the map

$$\Omega(p): \bigcup_{y \in \mathrm{Pt}(X)} \Omega_{x,y}(X) \to \bigcup_{z \in \mathrm{Pt}(Y)} \Omega_{p(x),z}(Y)$$

is a bijection.

2.3.3 Universality of the fundamental groupoid functor

Let

$$\mathfrak{E} \subset \mathbb{V},\ \mathcal{O}b\,\mathfrak{E} = \{E^n : n \geqslant 0\},\ \mathcal{M}or_{\mathfrak{E}}(X, Y) = \mathcal{M}or_{\mathrm{Var}/K}(X, Y)$$

be the full subcategory of the category of varieties whose objects are the Cartesian powers of E including $E^0 = 0$ a variety consisting of the single point 0. By the definition of a full subcategory, the morphisms of $\mathfrak{E}$ are morphisms of varieties between the objects of $\mathfrak{E}$.

Galois group $Gal(\overline{\mathbb{Q}}/k)$ acts on the category $\mathfrak{E}$; the action leaves the objects invariant but permutes the morphisms. Recall we assume that all endomorphisms of E preserving $0 \in E(k)$ are defined over its field k of definition.

Recall a groupoid $\Omega(E)$ is *connected* iff for every $x, y \in \mathrm{Pt}(E)$ there exists $\gamma \in \Omega(E)$ "going from point x to point y", i.e. $x = s(\gamma)$, $y = t(\gamma)$. The set of such paths satisfying $x = s(\gamma)$, $y = t(\gamma)$ is denoted by $\Omega_{x,y}(E)$.

Using the notion of an abstract fundamental groupoid functor, we restate Proposition 2; in Sect. 5 it is essentially equivalent to Proposition 1. The proof basically reconstructs the "universal covering space" V as the set of all paths $\bigcup_{*\in E(\overline{\mathbb{Q}})} \Omega_{0,*}(E)$ leaving a particular point; functoriality of $\underline{\Omega}$ allows us to define $\mathrm{End}E$-module structure on V; the unique path-lifting property of Ω ensures unique divisibility.

Proposition 2 (Universality of fundamental group functor) *Let E be an elliptic curve defined over a number field k. Let $\mathfrak{E}$ be the full subcategory of Cartesian powers of E as above.*

Let $\underline{\Omega}$ be a $\overline{\mathbb{Q}}$-valued abstract fundamental groupoid functor on category $\mathfrak{E}$. Assume

(1) *$\underline{\Omega}(E)$ is a connected groupoid*

(2) *there is an isomorphism*

$$\Omega_{0,0}(E) \cong \mathbb{Z}^2 \quad \textit{as } \mathrm{End}E\textit{-modules}.$$

Then there exists finitely many $\overline{\mathbb{Q}}$-valued abstract fundamental groupoid functors $\mathbb{F}_1, \ldots, \mathbb{F}_n : \mathfrak{E} \to \mathfrak{Groupoids}$ such that for any other abstract fundamental groupoid $\overline{\mathbb{Q}}$-valued functor $\underline{\Omega}$ there exists a Galois automorphism $\sigma \in Gal(\overline{\mathbb{Q}}/k)$ and a number $0 < i < n + 1$ such that $\underline{\Omega}$ and $\mathbb{F}_i \circ \sigma$ are naturally equivalent:

$$\underline{\Omega} \cong \mathbb{F}_i \circ \sigma$$

The conditions in the definition of an abstract fundamental groupoid functor are somewhat reminiscent of the conditions defining the scheme-theoretic algebraic fundamental group π_1^{alg} [SGA4$\frac{1}{2}$]; however, there π_1^{alg} takes values in the category of *profinite* groups, in particular $\pi_1^{\mathrm{alg}}(\mathbb{C}^*, 1) = \hat{\mathbb{Z}}$, $\pi_1^{\mathrm{alg}}(E(\mathbb{C}), 0) = \hat{\mathbb{Z}}^2$.

It is natural to consider whether a path lies in an algebraic subvariety, so if $\underline{\Omega}$ is to provide a useful notion of a path on $E(\mathbb{C})$, the 2-functor $\underline{\Omega}$ *restricted to* $\mathfrak{E}$ should be able to express when

(a representative of the homotopy class of) a path lies in an *arbitrary* algebraic subvariety of $E^n(\mathbb{C})$. This is indeed the case:

Remark 3 (Recovering $\Omega(Z)$ for arbitrary closed subvariety Z of E^n) The information contained in the functor $\pi_1^{\text{top}}|\mathfrak{E}$ restricted to the full subcategory $\mathfrak{E}$ of Cartesian powers of an elliptic curve is enough to determine whether a path lies in a closed subvariety. The key fact here is that for a normal subgroup $H \lhd \pi_1(E^n(\mathbb{C}))$, there exists an *H-Shafarevich* morphism $\text{Sh}_H : E^n \to E^m$ such that for an arbitrary irreducible $Z \subset E^n(\mathbb{C})$, it holds $Z \subset \ker f$ iff the image $Im[\pi_1(\hat{Z}, z) \to \pi_1(E^n(\mathbb{C}), z)]$ has a finite index subgroup contained in H.

3 Preliminaries

In this section we introduce the necessary preliminaries on Kummer theory of elliptic curves, in order not to interrupt the exposition later.

3.1 Kummer theory

3.1.1 The main statement of the Kummer theory for an elliptic curve

Let us state the main lemma in a form convenient to us to make an inductive process; that is a form natural from the model-theoretic point of view and corresponds to the property of *atomicity of certain formulae over the kernel*.

Lemma 4 (Kummer theory for an elliptic curve) *Let E be an elliptic curve defined over a number field k. Let $a_1, \ldots, a_n \in E(\overline{\mathbb{Q}})$ be a sequence of points linearly independent over* End$E$. *Then there exists $N \in \mathbb{Z}$ such that any two compatible sequences $(a_1^{(i)}, \ldots, a_n^{(i)})_{i\in\mathbb{N}}$, $(b_1^{(i)}, \ldots, b_n^{(i)})_{i\in\mathbb{N}}$ of division points in $E(\overline{\mathbb{Q}})$ starting at $a_1, \ldots, a_n$ and such that $a_1^{(N)} = b_1^{(N)}, \ldots, a_n^{(N)} = b_n^{(N)}$, are $Gal(\overline{\mathbb{Q}}/k)$-conjugated by $\sigma \in Gal(\overline{\mathbb{Q}}/k)$,*

$$\sigma(a_i^{(j)}) = b_i^{(j)}, \quad \textit{for all} \quad 0 \leqslant i \leqslant n,\ j \in \mathbb{N}.$$

Proof of Lemma See Bashmakov [1] for original results for elliptic curves; see [2,8,13,14] for Kummer theory of Abelian varieties, and see [3] for a summary of results of Kummer theory of Abelian varieties; we quote [3, Theorem 2] from that paper.

We now introduce the notations of Bertrand [3, Theorem 2]. Let $G = A \times L$ be a product of an Abelian variety by a torus L so that after a finite extension of k it satisfies Poincaré's complete reducibility theorem (as a variety *over* k).

Let l denote a prime. Let $G_{l^\infty} = \{x \in G(\bar{k}) : \exists n\, l^n x = 0\}$ be the l^∞-torsion of G. For a point $P \in G(\bar{k})$, let G_P be *the smallest algebraic subgroup of G containing P*, i.e. the Zariski closure of subgroup $\mathbb{Z}P$ of G, and *let G_P° be its connected component through the origin*, and finally let

$$\xi_{l^\infty}(P) : \text{Gal}(\bar{k}/k(G_{l^\infty}, P)) \longrightarrow T_{l^\infty}(A \times L)$$

$$\sigma \longmapsto \sigma(P_{l^\infty}) - P_{l^\infty}$$

for $P_{l^\infty} = \{P_{l^k}\}_{k\in\mathbb{N}}$ a compatible sequence of division points, $P_1 = P$. It can be checked by direct computation the map $\xi_{l^\infty}(P) : \text{Gal}(\bar{k}/k(G_{l^\infty}, P) \to T_{l^\infty}(A \times L)$ does not depend on the choice of P_{l^∞}.

Let $T(G_P^\circ)$ be the sequences of $T(A \times L)$ consisting of elements of G_P°; then, according to [3, Theorem 2], the image of $\xi_\infty(P) = \prod_l \xi_{l^\infty}$ has finite index in $T(G_P^\circ) \subset \prod_l T_{l^\infty}(A \times L)$, i.e. the image contains $NT(G_P^\circ)$, for some natural number $N \in \mathbb{N}$ large enough.

We claim that if we take $G = E^n$, $P = (a_1, \ldots, a_n) \in E^n(\overline{\mathbb{Q}})$, then N above is N required in Lemma. By the result cited above, it is enough to prove that if $a_1, \ldots, a_n \in E(\overline{\mathbb{Q}})$ are $\mathrm{End}E$-linearly independent, then $G_P^\circ = E^n$. Assume $G_P^\circ \neq E^n$ and consider the quotient E^n/G_P. By Poincaré's reducibility theorem, there is an isogeny $f : E^n/G_P \to E^m$, for some natural number m. Finally consider the composite morphism $g : E^n \to^\pi E^n/G_P \to^f E^m$ where $\pi : E^n \to E^n/G_P$ is the natural projection. The connected component G_P° has finite index in $\mathrm{Ker}g$ and therefore g is non-trivial and represents a non-trivial $\mathrm{End}E$-linear relation on $P \in G_P$. This is a contradiction which completes the proof. □

4 Proof of Proposition 2

In this section we state and prove Proposition 2; as was mentioned earlier, the proof is a model theoretic argument based on Kummer theory and the description of the image of Galois action on Tate module $T(E)$. However, we tried to be very explicit and have avoided any model-theoretic terminology in the exposition of the proof. The only model theory left in the proof is in the level of motivations and ideas; however, we do not attempt to explain these.

4.1 $Gal(\overline{\mathbb{Q}}/k)$-action on the uniquely divisible End E-module extensions of $E(\overline{\mathbb{Q}})$ by Λ

To fix notations for the proof, we restate Proposition 1 in an expanded form.

Proposition 1′ *Let $E(\mathbb{C})$, Λ be as above.*

(1) *There exists a uniquely divisible* $\mathrm{End}E$*-module V and a short exact sequence of* $\mathrm{End}E$*-modules*

$$0 \longrightarrow \Lambda \longrightarrow V \longrightarrow E(\overline{\mathbb{Q}}) \longrightarrow 0.$$

(2) *There exist finitely many uniquely divisible* $\mathrm{End}E$*-module extensions $W_1, \ldots, W_n$ of $E(\overline{\mathbb{Q}})$ by Λ, fitting into the short exact sequences as above, such that for any uniquely divisible* $\mathrm{End}E$*-module extension V there exist a commutative diagram*:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & V & \xrightarrow{\varphi} & E(\overline{\mathbb{Q}}) & \longrightarrow & 0 \\ & & \exists h_{|\Lambda} \downarrow & & \exists \downarrow h \in \mathrm{Hom}(V,W) & & \downarrow \exists \sigma \in Gal(\overline{\mathbb{Q}}/k) & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & W_i & \xrightarrow{\psi_i} & E(\overline{\mathbb{Q}}) & \longrightarrow & 0 \end{array}$$

Proof By assumption there is a covering

$$0 \longrightarrow \Lambda \longrightarrow \mathbb{C} \xrightarrow{p} E(\mathbb{C}) \longrightarrow 0$$

The endomorphisms act on the complex plane $\mathbb{C}$ by multiplication by complex numbers, and so in particular $\mathbb{C}$ is a uniquely divisible $\mathrm{End}E$-module. The set $E(\overline{\mathbb{Q}})$ of points of E over an algebraically closed subfield is closed under addition and $\mathrm{End}E$-multiplication i.e. is an $\mathrm{End}E$-submodule, necessarily uniquely divisible; so is then $V = p^{-1}(E(\overline{\mathbb{Q}}))$; take that to obtain a short exact sequence as above. This proves (1).

The proof of (2) occupies the rest of this section.

An $\mathrm{End}E$-linear map $h : \Lambda \to \Lambda$ induces a $\mathrm{End}E$-module automorphism $\sigma_h : E(\overline{\mathbb{Q}})_{\mathrm{tors}} \to E(\overline{\mathbb{Q}})_{\mathrm{tors}}$ of the torsion $E(\overline{\mathbb{Q}})_{\mathrm{tors}}$. To define extensions W_i's, in Sect. 4.2 we find $\mathrm{End}E$-linear automorphisms $\tau_1, \ldots, \tau_n : E(\overline{\mathbb{Q}})_{\mathrm{tors}} \to E(\overline{\mathbb{Q}})_{\mathrm{tors}}$ such that for every $\mathrm{End}E$-linear map $h : \Lambda \to \Lambda$, the induced $\mathrm{End}E$-module automorphism has form $\sigma_h = \tau_i \circ \sigma$, for some $1 \leqslant i \leqslant n$ and σ a Galois automorphism, and set $W_i = V$, $\varphi_i = \tau_i \circ p_{|V}$. The rest of proof is by induction.

Pick a maximal linearly independent set $v_0, v_1, v_2, \ldots \in V$; let $V_n = \mathrm{End}E\, v_0 + \cdots + \mathrm{End}E\, v_n$ be the submodule generated by $v_0, \ldots, v_n$, and let $\mathbb{Q}V_n = (\mathrm{End}E)^{-1}V_n = \{v : \exists N \in \mathbb{N}(Nv \in V_n)\}$ be its divisible closure. We construct by induction a partial $\mathrm{End}E$-module linear map $h_n : \mathbb{Q}V_n \to W_i$ inducing a partial Galois map $\sigma_n : \varphi(\mathbb{Q}V) \to E(\overline{\mathbb{Q}})$ so that $h = \cup h_n$ is an isomorphism of V and W_i; then the construction implies $\sigma = \cup\sigma_n$ is a total Galois map on $E(\overline{\mathbb{Q}})$ to $E(\overline{\mathbb{Q}})$, and thus there is a commutative diagram as above. At each step, we use information about arithmetics of $E(\overline{\mathbb{Q}})$ to extend $h_n : V_n \to W$.

In Sect. 4.2 the definition of W_i's allows us to start the induction and define the partial map $h_{|E_{\mathrm{tors}}}$ on the torsion of $E(\overline{\mathbb{Q}})$; in Sect. 4.2.4 we use Kummer theory to extend $h_{n-1} : V_{n-1} \to W$. The results of Kummer theory we use are given in Sect. 3.1.1.

4.2 The image of Galois representations on Tate module $T_l(E)$

4.2.1 Base of induction

In this subsection we construct a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{Q}\Lambda & \xrightarrow{\varphi} & E_{\mathrm{tors}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h_0} & & \downarrow{\scriptstyle h_0 \in \mathrm{Hom}\,(\mathbb{Q}\Lambda, W)} & & \downarrow{\scriptstyle \sigma \in Gal(\overline{\mathbb{Q}}/k)} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{Q}\Lambda & \xrightarrow{\psi\circ\tau_i} & E_{\mathrm{tors}} & \longrightarrow & 0 \end{array} \tag{1}$$

where $\tau_1, \ldots, \tau_n$ is some fixed finite collection of $\mathrm{End}E$-endomorphisms of E_{tors} independent of V, W.

In Sects. 4.2.2 and 4.2.3 we consider two cases depending on whether E has complex multiplication or not.

4.2.2 E has complex multiplication

Pick an arbitrary isomorphism $h_0 : \Lambda \to \Lambda$ and extend it uniquely to $h_0 : V_0 \to W$; we may do so by unique divisibility of V and W. Define an $\mathrm{End}E$-morphism $\tau : E_{\mathrm{tors}} \to E_{\mathrm{tors}}$ by $\tau(x) = \psi \circ h_0 \circ \varphi^{-1}(x)$. The calculation $\psi \circ h_0(y + \Lambda) = \psi \circ h_0(y)$ shows it is well-defined; linearity of τ follows from that of φ, h_0 and φ.

Ideally we would like to be able to choose $h_0 : \Lambda \to \Lambda$ so that $\tau = \tau_h : E_{\mathrm{tors}} \to E_{\mathrm{tors}}$ is induced by a Galois automorphism. Here we prove a weaker statement below.

Denote $\mathcal{O} = \mathrm{End}E$ and $E[n] = \{x \in E(\overline{\mathbb{Q}}) : nx = 0\}$ the n-torsion of E. The set $E[n]$ is a free 1-dimensional $\mathcal{O}/n\mathcal{O}$-module ([9, Chap. 8, Sect. 15, Fact 1]), and $\mathrm{Aut}_{\mathcal{O}}(E[n]) = \mathrm{Aut}_{\mathcal{O}/n\mathcal{O}-\mathrm{mod}}(E[n]) \cong (\mathcal{O}/n\mathcal{O})^*$, where $(\mathcal{O}/n\mathcal{O})^*$ denotes the group of invertible elements in $(\mathcal{O}/n\mathcal{O})^*$.

An $\mathcal{O}$-automorphism of E_{tors} is given by a compatible system of $\mathcal{O}$-automorphisms of $E[n]$, $n > 0$; thus we see that there is an action of $\hat{\mathcal{O}} = \lim_n \mathcal{O}/n\mathcal{O}$ on E_{tors} as an $\mathrm{End}E$-module; the fact that $\mathrm{Aut}_{\mathcal{O}}(E[n]) = \mathrm{Aut}_{\mathcal{O}/n\mathcal{O}-\mathrm{mod}}(E[n]) \cong (\mathcal{O}/n\mathcal{O})^*$ implies that $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \cong \hat{\mathcal{O}}$.

Now we refer to a consequence of the main theorem of complex multiplication, namely that, in notation of [9, Chap. 8, Sect. 15, Fact 2], the image of Galois group

$$G_K = Gal(K(E_{\text{tors}}) : K) \to \prod((\text{End}E)_l)^*$$

is open of finite index, i.e. ImG_K is a finite index subgroup of $\hat{\mathcal{O}}^* = \prod_l \mathcal{O}_l^*$. Choose $\tau_1, \ldots, \tau_n$ to be representatives of conjugacy classes $\mathcal{O}^*/ImG_K$; we then have that for some i $\tau_i\tau = \sigma \in ImG_K$; this choice of $h_0, \sigma = \tau_i\tau$ makes the diagram (1) commutative, as required.

4.2.3 E does not have complex multiplication

Assume that E does not have complex multiplication, i.e. End $E \cong \mathbb{Z}$; identify End$E = \mathbb{Z}$, $T(E) = \hat{\mathbb{Z}}^2$, and Aut$(T(E)) = \text{GL}_2(\hat{\mathbb{Z}})$. The maps $\varphi : V \to E(\overline{\mathbb{Q}})$, $\psi : W \to E(\overline{\mathbb{Q}})$ define embeddings $\iota_\varphi : \Lambda \to T(E)$, $\iota_\psi : \Lambda \to T(E)$ by

$$\iota_\varphi : \lambda \mapsto (\varphi(\lambda/j))_{j\in\mathbb{N}},$$
$$\iota_\psi : \lambda \mapsto (\psi(\lambda/j))_{j\in\mathbb{N}}.$$

The images $\iota_\varphi(\Lambda), \iota_\psi(\Lambda)$ of the both maps are dense in $T(E)$ due to the surjectivity of $\varphi, \psi : \mathbb{Q}\Lambda \to E_{\text{tors}}$.

Take a pair of elements $\lambda_0, \lambda_1 \in \ker\varphi \cong \Lambda$ generating Λ as an Abelian group; we want to find $\lambda_0', \lambda_1' \in \ker\psi \cong \Lambda$ and $\sigma = \sigma_0 \in Gal(\overline{\mathbb{Q}}/k)$ such that

$$\sigma\iota_\varphi(\lambda_0) = \iota_\psi(\lambda_0'),$$
$$\sigma\iota_\varphi(\lambda_1) = \iota_\psi(\lambda_1').$$

Under identification $\ker\varphi = \mathbb{Z}^2$, since vectors $\lambda_0, \lambda_1 \in \mathbb{Z}^2$ generate lattice $\mathbb{Z}^2$, it holds that $\det(\lambda_0, \lambda_1) = 1$. That implies that $\det(\iota_\varphi(\lambda_0), \iota_\varphi(\lambda_1))$ is a unit in $\hat{\mathbb{Z}} = \prod_l \mathbb{Z}_l$. Similarly $\det(\iota_\psi(\lambda_0'), \iota_\psi(\lambda_1'))$ has to be a unit in $\hat{\mathbb{Z}}$. This implies that there is an element of $\text{GL}_2(\hat{\mathbb{Z}})$ taking $(\iota_\varphi(\lambda_0), \iota_\varphi(\lambda_1)$ into $(\iota_\psi(\lambda_0'), \iota_\psi(\lambda_1'))$.

By [15] (cf. also [3, Theorem 3]), the image of the Galois group $Gal(\overline{\mathbb{Q}}/k)$ in the automorphism group Aut$(T(E)) = \text{GL}_2(\hat{\mathbb{Z}})$ contains an open subgroup $\text{GL}_2(N\hat{\mathbb{Z}}) = \ker(\text{GL}_2(\hat{\mathbb{Z}}) \to \text{GL}_2(\mathbb{Z}/N\mathbb{Z}))$, for some $N \in \mathbb{N}$ large enough. Choose $\tau_1, \ldots, \tau_n$ to be the representatives of the conjugacy classes $\text{GL}_2(\hat{\mathbb{Z}})/\text{GL}_2(N\hat{\mathbb{Z}})$; they have the required property. This finishes the proof of the base of the induction.

4.2.4 An inductive argument based on Kummer theory

Assume now that we are on inductive step $n-1$, i.e. we have defined an End$E$-linear map $h_{n-1} : \mathbb{Q}V_{n-1} \to W$ and $\sigma_{n-1} \in Gal(\overline{\mathbb{Q}}/k)$, $h_{n-1}(v_i) = w_i, 0 \leqslant i < n$ such that $\psi(h_{n-1}(v)) = \sigma_{n-1}\varphi(v)$ for every $v \in \mathbb{Q}V_{n-1}$. Consider a compatible system $(\varphi(v_0/j))_j, \ldots, (\varphi(v_n/j))_j$, $j \in \mathbb{N}$ of division points in $E(\overline{\mathbb{Q}})$, and take N as in Kummer theory Lemma 4. By the induction hypothesis we have $\sigma_{n-1}\varphi(v_0/j) = \psi(w_0/j), \ldots, \sigma_{n-1}\varphi(v_{n-1}/j) = \psi(w_{n-1}/j)$ for any j. Choose $w_n \in W$ such that $\sigma_{n-1}\varphi(v_n/N) = \psi(w_n/N)$; that is possible by surjectivity of $\psi : W \to E(\overline{\mathbb{Q}})$. By Kummer theory lemma, for N large enough, there exists $\sigma' \in Gal(\overline{\mathbb{Q}}/k)$ such that $\sigma'\sigma_{n-1}\varphi(v_0/j) = \psi(w_0/j), \ldots, \sigma'\sigma_{n-1}\varphi(v_{n-1}/j) = \psi(w_{n-1}/j)$, and $\sigma'\sigma_{n-1}\varphi(v_n/j) = \psi(w_n/j)$; let $\sigma_n = \sigma'\sigma_{n-1}$ and $h_n(v_i) = w_i, 0 \leqslant i \leqslant n$. By construction we have that $\sigma_n|_{\varphi(\mathbb{Q}V_{n-1})} = \sigma_{n-1}|_{\varphi(\mathbb{Q}V_{n-1})}$ and

$\sigma_n\varphi(v_i/j) = \psi(0_i/j), 0 \leqslant i < n+1$. This implies $\sigma_n\varphi(v) = \psi(h_n(v))$ for arbitrary $v \in \mathbb{Q}V_n$, thereby completing the induction step.

After countably many steps we construct a total $\mathrm{End}E$-linear map $h = \cup h_n : V \to W$ and $\sigma : \varphi(V) \to E(\overline{\mathbb{Q}})$. Since $\varphi(V) = E(\overline{\mathbb{Q}})$, the Galois map σ is defined on the whole of $E(\overline{\mathbb{Q}})$. Since Galois map σ is surjective, this implies $h : V \to W$ is surjective, too. This completes the proof of Proposition 1.

The last argument could in fact have been avoided by a little more careful inductive construction of h: instead of always choosing w_n to match $\varphi(v_n)$ we could have on odd steps picked an arbitrary w_n and then choosen v_n so that $\sigma_n(\varphi(v_n)) = \psi(w_n)$ while on even steps preserving the old behaviour. It is very easy to force surjectivity of the constructed map $h : V \to W$ this way; it is a very common argument in model theory called "a back-and-forth argument".

4.3 Concluding remarks

4.3.1 Freedom of choice of $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ and $h : V \to W$

Remark 5 There is some freedom in constructing $h = \cup h_n$ and $\sigma = \cup\sigma_n$: at each step we may modify the value $w_n = h_n(v_n)$ of h_n by adding any kernel element λ such that $\psi(\lambda/N) = 0$, for some $N = N_n$ large enough and depending on n. This shows there are uncountably many such σ's and h's; in fact the σ's form a conjugacy class of an uncountable subgroup H in the Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ (an an abstract group). The subgroup H is well-defined up to conjugation and can be explicitly described as the group of Galois automorphisms $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ such that the induced action $\sigma : E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}})$ (exists and) lifts up to an $\mathrm{End}E$-linear automorphism of W.

4.3.2 Image of Galois representation

Remark 6 Note that for the arguments in Sect. 4.2 it is essential that the image of the Galois action is as large as possible subject to linear dependencies. However, this is something specific to elliptic curves and false for higher dimensional Abelian varieties: one needs to take care of a symplectic form. This observation shows that the straightforward generalisation to higher dimensional Abelian varieties is false. See [6, IV Sect. 7] for a discussion of this.

4.3.3 Kummer theory

Remark 6 says that in higher dimensions, the base of the induction breaks down due to additional restrictions on the image of the Galois action. This does not happen in the the later steps of the induction process based on Kummer theory.

Remark 7 (Generalisations of Kummer theory argument) Since Kummer theory is known in much larger generality, say for a product of arbitrary Abelian varieties, complex tori $\mathbb{C}^*$ and complex lines $\mathbb{C}$ ([3]), it seems straightforward to generalise the Kummer theory argument above to such a product A. Thus, one would prove that if there exists $h_0 : \ker\varphi \to \ker\psi$ and a Galois map $\sigma_0 : E(k(T(E)) \to E(k(T(E)))$ in $\mathrm{Gal}(k(T(E))/k)$ such that $\varphi \circ \sigma_0 = h_0 \circ \psi$, then there exists $h : V \to W$ and $\sigma \in Gal(\overline{\mathbb{Q}}/k)$ making the diagram (2) commutative. That is, a morphism between kernel from $\Lambda \subset V$ to $\Lambda \subset W$ extends to a morphism on the whole of V. Model-theoretically, this means that the types of the points of universal covering space lying over algebraic points $A(\overline{\mathbb{Q}})$ is *atomic over the kernel* in the *linear* language.

Remark 8 (Failure of Kummer theory for extensions of Abelian varieties by tori) According to Ribet [8,14], Kummer theory may fail for non-trivial extensions of Abelian varieties by $(\mathbb{C}^*)^n$ due to "existence of an additional morphism"; he gives a motivic interpretation in [14]. It is natural to ask if an analogous argument could still be carried despite the failure of Kummer theory. To state a correct conjecture, we may need to use more general considerations of [6].

5 Proof of Proposition 2

In this section we derive Proposition 2 from Proposition 1 by carrying out a formal counterpart of the natural topological construction of a universal covering space. We do so by explicitly constructing an extension as in Proposition 1 from a 2-functor as in Proposition 2, and then showing that the equivalence of the constructed extensions implies the equivalence of 2-functors.

The construction is a formalisation of the geometric observation that the universal covering space with a basepoint can be canonically identified with the set of homotopy classes of paths leaving the basepoint of the base. The identification is via the unique path-lifting property of the covering map, and depends only on the choice of a basepoint in the universal covering space. In case of the universal covering space $\mathbb{C}$ of $E(\mathbb{C})$, the correspondence is given by the *period map*

$$\gamma \longmapsto \int_\gamma dz.$$

5.0.4 Recovering V as the universal covering space from the 2-functor $\underline{\Omega}$

Let $\underline{\Omega} = (\mathrm{Pt}, \Omega, s, t, \cdot)$ be a 2-functor from $\mathfrak{E}$ to $\mathfrak{S}ets$ satisfying the conditions of Definition 1. We want to construct an extension

$$0 \longrightarrow \mathbb{Z}^2 \longrightarrow V_{\underline{\Omega}} \xrightarrow{\varphi} E(\overline{\mathbb{Q}}) \longrightarrow 0$$

of $\mathrm{End}E$-modules. The topological intuition referred to above suggests that we set

$$V = V_{\underline{\Omega}} = \bigcup_{y \in \mathrm{Pt}(E)} \Omega_{0,y}(E) = \{\gamma \in \Omega(E) : s(\gamma) = 0\} \text{ (disjoint union)},$$
$$\varphi(\gamma) = t(\gamma)$$

where $0 \in E(k)$ is the zero point of the elliptic curve E.

5.0.5 Abelian group structure on $\Omega(E)$

The functoriality of $\underline{\Omega}$ transfers $\mathrm{End}E$-module structure on $E(\overline{\mathbb{Q}})$ to that on V; namely, let us check that the maps $\Omega(f)$, $f \in \mathrm{End}E$, and $\Omega(m)$, where $m : E \times E \to E$ is the morphism of addition on E, define $\mathrm{End}E$-module structure on V, or rather that their restriction to V does.

By assumption the functor $\underline{\Omega}$ preserves direct products so $\Omega(E \times E) = \Omega(E) \times \Omega(E)$, and thus there is a map

$$\Omega(m) : \Omega(E) \times \Omega(E) \to \Omega(E).$$

Maps s, t are natural transformations of Ω to Pt (as functors to $\mathcal{S}ets$) and so $s \circ \Omega(m) = \mathrm{Pt}(m) \circ s$, $t \circ \Omega(m) = \mathrm{Pt}(m) \circ t$ is the map of addition on end-points. Therefore,

$$\Omega(m)(\Omega_{x,y}(E) \times \Omega_{v,w}(E)) \subset \Omega_{x+v,y+w}(E),$$

and in particular

$$\Omega(m)(\Omega_{0,y}(E) \times \Omega_{0,z}(E)) \subset \Omega_{0,y+z}(E).$$

Thus $\Omega(m) : V \times V \to V$ gives us a binary operation. It is straightforward to show that preservation of direct products and functoriality implies that $\Omega(m)$ makes $\Omega(E)$ into an Abelian group. Let us check this.

By definition, associativity of $m : E \times E \to E$ means that $m \circ (m \times \mathrm{id}_E) = m \circ (\mathrm{id}_E \times m) : E \times E \times E \to E$; by preservation of direct products this implies $\Omega(m) \circ (\Omega(m) \times \mathrm{id}_E) = \Omega(m) \circ (\mathrm{id}_E \times \Omega(m))$ and so $\Omega(m)$ is associative. Similarly, commutativity of m means $m \circ (\mathrm{id}_1 \times \mathrm{id}_2) = m \circ (\mathrm{id}_2 \times \mathrm{id}_1) : E \times E \to E$; that similarly implies the commutativity of $\Omega(m)$. In the language of morphisms, the existence of a zero for the additive law translates to the existence of a morphism $0 : \{0\} \to E$ subject to the identifies: $m \circ (\mathrm{id} \times 0) = p_2 : \{0\} \times E \to E$ and $m \circ (0 \times \mathrm{id}) = p_1 : E \times \{0\} \to E$ corresponding to a commutative diagram:

$$\begin{array}{ccc} \{0\} \times E & \rightarrowtail & E \times E \\ & \searrow \quad \swarrow & \\ & E & \end{array}$$

Apply Ω to get $\Omega(m) \circ (\Omega(\mathrm{id}) \times \Omega(0)) = \Omega(p_2) : \Omega(\{0\}) \times \Omega(E) \to \Omega(E)$ and $\Omega(m) \circ (\Omega(0) \times \Omega(\mathrm{id})) = \Omega(p_1) : \Omega(E) \times \Omega(\{0\}) \to \Omega(E)$. Preservation of direct products implies $\Omega(m) \circ (\mathrm{id} \times \Omega(0)) = \Omega(p_2) : \Omega(\{0\}) \times \Omega(E) \to \Omega(E)$ and $\Omega(m) \circ (\Omega(0) \times \mathrm{id}) = \Omega(p_1) : \Omega(E) \times \Omega(\{0\}) \to \Omega(E)$. This implies that $\Omega(0)(\Omega(\{0\}))$ is a zero point in V.

Existence of (right) inverse corresponds to the existence of a morphism $i : E \to E$ subject to the following commutative diagram:

$$\begin{array}{ccc} E & \longrightarrow & \{0\} \\ {\scriptstyle (\mathrm{id}_E, i)}\downarrow & & \downarrow{\scriptstyle 0} \\ E \times E & \xrightarrow[m]{} & E \end{array}$$

Again functoriality ensures that $\Omega(i)$ satisfies a similar diagram, thus proving the existence of inverses.

The above checks that $\Omega(m)$ is an associative commutative partial operation on $\Omega(E)$ possessing a zero element and inverses; it is immediate to check V is closed under $\Omega(m)$ and inverse $\Omega(i)$, and so is a group.

5.0.6 Action of "fundamental group" $\Omega_{0,0}(E)$ on V via concatenation and by $\Omega(m)$-multiplication

Take a *loop* $\lambda \in \Omega_{0,0}(E)$ and $\gamma \in \Omega_{0,y}$; then both concatenation and $\Omega(m)$-product of λ and γ are well-defined; let us show that $\lambda \cdot \gamma = \Omega(m)(\lambda \times \gamma)$:

$$\Omega(m)(\lambda \times \gamma) = \Omega(m)(\lambda \cdot 0 \times 0 \cdot \gamma) = \Omega(m)(\lambda \times 0) \cdot \Omega(m)(0 \times \gamma) = \lambda \cdot \gamma.$$

The latter equality follows from the inverse element equality of morphisms $m(\mathrm{id} \times 0) = m(0 \times \mathrm{id}) = \mathrm{id}$. In the classical example, this observation corresponds to the following calculation:

$$\int\limits_{\gamma_1 \cdot \gamma_2} dz = \int\limits_{\gamma_1} dz + \int\limits_{\gamma_2} dz = \int\limits_{\gamma_1 \gamma_2} dz.$$

Here $\gamma_1 \cdot \gamma_2$ denotes the concatenation of the paths and $\gamma_1 \gamma_2$ denotes the pointwise product of the paths.

5.0.7 *Divisibility of* End$E$*-module structure and path-lifting property*

Analogously, a morphism $f \in \mathrm{End}E$, $\Omega(f) : \Omega(E) \to \Omega(E)$ defines a map $\Omega(f) : \Omega(E) \to \Omega(E)$. Arguments similar to the ones above allow us to prove that V is an End$E$-module with the operations defined above. Let us now prove that the path-lifting property implies that V is uniquely divisible. Indeed, we know that any isogeny $f \in \mathrm{End}E$ is étale [11] and we may apply the path-lifting property to get a bijection

$$\Omega(f) : \bigcup_{0 \in \mathrm{Pt}(E)} \Omega_{0,y}(E) \twoheadrightarrow \bigcup_{z \in \mathrm{Pt}(E)} \Omega_{0,z}(E).$$

That is, by definition of V, the map $\Omega(f)$ is a bijection on V, and V is uniquely divisible as required.

Finally, to get a short exact sequence as in Proposition 1, set $\varphi(w) = t(w)$. Then naturality of target map t implies $\varphi(w)$ is homomorphism of End$E$-modules; the connectivity of $\Omega(E)$ implies that φ is surjective. The kernel $\ker \varphi$ of $\varphi : V \to E(\overline{\mathbb{Q}})$ is $\Omega_{0,0}(E)$ and is isomorphic to $\mathbb{Z}^2$ by assumption.

5.0.8 *Construction of a natural transformation* $h' : \underline{\Omega} \to \pi_1^{\mathrm{top}}{}_{|\overline{\mathbb{Q}}} \circ \sigma$

For notational convenience, let $\underline{\Omega}' = (\mathrm{Pt}, \Omega', s', t', \cdot')$ denote the functor $\pi_1^{\mathrm{top}}{}_{|\overline{\mathbb{Q}}}$.

Let $W \to^{\psi} E(\overline{\mathbb{Q}})$ be the End$E$-module extension constructed from $\underline{\Omega}' = \pi_1^{\mathrm{top}}{}_{|\overline{\mathbb{Q}}}$ in the same way. Since V, W are both uniquely divisible extensions of $E(\overline{\mathbb{Q}})$ by $\mathbb{Z}^2$, we may apply Proposition 1 to get an End$E$-linear map $h : V \to W$ and $\sigma \in Gal(\overline{\mathbb{Q}}/k)$ such that $\sigma \circ \varphi = \psi \circ h$.

We want to get a natural transformation $h' : \underline{\Omega} \to \underline{\Omega}' \circ \sigma$. Recall a natural transformation $h' : \underline{\Omega} \to \underline{\Omega}' \circ \sigma$ is a family of maps (of sets with no further structure) $h'^{\Omega}_A : \Omega(A) \to \Omega' \circ \sigma(A)$ and $h'^{\mathrm{Pt}}_A : \mathrm{Pt}(A) \to \mathrm{Pt}' \circ \sigma(A)$ satisfying certain compatibly conditions expressed by commutative diagrammes (2), (3), (4).

Define $h'^{\mathrm{Pt}}_A : A(\overline{\mathbb{Q}}) \to A(\overline{\mathbb{Q}})$ by $h'^{\mathrm{Pt}}_A(x) = \sigma(x) \in \mathrm{Pt}'(A) = (\sigma A)(\overline{\mathbb{Q}}) = A(\overline{\mathbb{Q}})$ to be the map induced by Galois automorphism $\sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$.

By assumption of connectivity of $\Omega(E)$, any $\gamma \in \Omega(E)$ can be represented as product $\gamma = \gamma_1^{-1} \cdot \gamma_2$ where $\gamma_1, \gamma_2, s(\gamma_1) = s(\gamma_2) = 0$; define a map $h'_E : \Omega(E) \to \Omega'(E)$ by setting

$h'_E(\gamma) = h(\gamma_1)^{-1} \cdot h(\gamma_2)$. If ${\gamma_1}^{-1}\gamma_2 = {\gamma'_1}^{-1}\gamma'_2$ then ${\gamma_1}^{-1}\gamma'_1 = \gamma_2{\gamma'_2}^{-1} \in \Omega_{0,0}(E)$, and so

$$\begin{aligned} h(\gamma_1)^{-1} \cdot h(\gamma_2) &= h((\gamma_1{\gamma'_1}^{-1})\gamma'_1)^{-1} \cdot h((\gamma_2{\gamma'_2}^{-1})\gamma'_2) \\ &= h(({\gamma_1}^{-1}\gamma'_1) + \gamma'_1)^{-1} \cdot h((\gamma_2{\gamma'_2}^{-1}) + \gamma'_2) \\ &= (h({\gamma_1}^{-1}\gamma'_1) + h(\gamma'_1))^{-1} \cdot h(\gamma_2{\gamma'_2}^{-1}) + h(\gamma'_2) \\ &= (h(\gamma'_1))^{-1} \cdot h(\gamma'_2) = h({\gamma'_1}^{-1}) \cdot h(\gamma'_2), \end{aligned}$$

which proves that h' is well-defined. Similar calculations check that h'_E preserves concatenation $\cdot_E$: $h'(\gamma \cdot \gamma') = h'(\gamma) \cdot h'(\gamma')$ for arbitrary $\gamma, \gamma' \in \Omega(E)$.

We define $h'_{E^n} = h^{\Omega}_{E^n} : \Omega(E^n) \to \Omega'(E^n)$ from an arbitrary Cartesian power $\Omega(E^n) = \Omega(E)^n$ by $h'_{E\times E}(\gamma \times \gamma') = h'_E(\gamma) \times h'_E(\gamma')$ etc.

5.0.9 Checking that h' is a natural transformation of $\underline{\Omega}$ into $\underline{\Omega}' \circ \sigma$

To check that h' is a natural transformation of $\underline{\Omega}$ to $\underline{\Omega}' \circ \sigma$, we need to check commutativity of the following diagrams (note that σ on the *left*-hand side is *not* a morphism but a functor!):

$$\begin{array}{ccc} E^n & \xrightarrow[\mathrm{Pt}]{} & E^n(\overline{\mathbb{Q}}) \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma_{E^n}} \\ E^n & \xrightarrow{\mathrm{Pt}} & E^n(\overline{\mathbb{Q}}) \end{array} \qquad \begin{array}{ccc} A(\overline{\mathbb{Q}}) & \xrightarrow[\mathrm{Pt}(f)]{} & B(\overline{\mathbb{Q}}) \\ {\scriptstyle\sigma_A}\downarrow & & \downarrow{\scriptstyle\sigma_B} \\ A(\overline{\mathbb{Q}}) & \xrightarrow{\mathrm{Pt}(f\circ\sigma)} & B(\overline{\mathbb{Q}}) \end{array} \tag{2}$$

$$\begin{array}{ccc} E^n & \xrightarrow[\Omega]{} & \Omega(E^n) \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle h'_{E^n}} \\ E^n & \xrightarrow{\Omega'} & \Omega'(E^n) \end{array} \qquad \begin{array}{ccc} \Omega(A) & \xrightarrow[\Omega(f)]{} & \Omega(B) \\ {\scriptstyle h'_A}\downarrow & & \downarrow{\scriptstyle h'_B} \\ \Omega'(A) & \xrightarrow{\Omega'(f\circ\sigma)} & \Omega'(B) \end{array} \tag{3}$$

$$\begin{array}{ccc} \Omega(A) & \xrightarrow{s_A} & \mathrm{Pt}(A) \\ {\scriptstyle h'_A}\downarrow & & \downarrow{\scriptstyle\sigma_A} \\ \Omega'(A) & \xrightarrow{s'_A} & \mathrm{Pt}(A) \end{array} \qquad \begin{array}{ccc} \Omega(A) & \xrightarrow[t_A]{} & \mathrm{Pt}(A) \\ {\scriptstyle h'_A}\downarrow & & \downarrow{\scriptstyle\sigma_A} \\ \Omega'(A) & \xrightarrow{t'_A} & \mathrm{Pt}(A) \end{array} \tag{4}$$

$$\begin{array}{ccc} \Omega(A)\times\Omega(A) & \xrightarrow[\text{partial}]{\cdot_A} & \Omega(A) \\ {\scriptstyle h'_A\times h'_A}\downarrow & & \downarrow{\scriptstyle h'_A} \\ \Omega'(A)\times\Omega'(A) & \xrightarrow[\text{partial}]{\cdot'_A} & \Omega'(A) \end{array} \tag{5}$$

The first pair (2) expresses that $h^{\mathrm{Pt}}_A = (\sigma_A)_A$ is a natural transformation of set-valued functors from Pt to Pt $\circ\, \sigma$; the diagrams are commutative just by definition of the action of $\sigma \in Gal(\overline{\mathbb{Q}}/k)$ on category $\mathfrak{E}$. Analogously the second pair (3) expresses that h' is a natural transformation of set-valued functors Ω to $\Omega' \circ \sigma$. The first diagram in (3) says that h'_{E^n} is a map from $\Omega(E^n)$ to $\Omega'(\sigma(E^n)) = \Omega'(\sigma(E^n))$; the second one in (3) expresses the linearity of h' with respect to the morphisms of $E^n \to E^m$; that follows from End$E$-linearity of $h : V \to V$.

The third pair (4) expresses compatibility of the end-point functions and h'_A; for $A = E$, this follows from the main property $\sigma \circ s = s \circ h$ when restricted to $W^n \subset \Omega(E^n)$, and that h' preserves concatenation $\cdot_A$; preservation of direct productss allows us to extend this to arbitrary Cartesian power E^n. The diagram (5) expresses the fact that h' preserves concatenation; this is by the definition of h'.

This concludes the proof that h' is a natural transformation and that of derivation of Proposition 2 from Proposition 1.

6 Shimura curves

Arithmetics of Shimura curves is well-studied. In particular, for Shimura curves, there is a quite explicit description of Galois action analogous to the results on the Galois action on the Tate module of an elliptic curve: for curves without complex multiplication it is a result of Ohta [12]; for curves with complex multiplication this is implied by the explicit description of the Galois group provided by the theory of complex multiplication. We thank A.Yafaev for pointing and explaining us those results. These results motivate us to make the following conjecture.

Let S be a connected Shimura curve defined over a number field $k \subset \overline{\mathbb{Q}}$, and let $\mathfrak{SC}$ be full subcategory of $\mathrm{Var}/\overline{\mathbb{Q}}$ consisting of Cartesian powers of finite étale covers of S. Assume that S has a k-rational point O.

Recall we denote $\mathrm{Pt}_{\pi_1^{\mathrm{top}}|\overline{\mathbb{Q}}}(V) = V(\overline{\mathbb{Q}})$ and $\Omega_{\pi_1^{\mathrm{top}}|\overline{\mathbb{Q}}}(V) = \{\gamma \in \pi_1^{\mathrm{top}}(V(\mathbb{C})) : s(\gamma), t(\gamma) \in V(\overline{\mathbb{Q}})\}$ is the restriction of π_1^{top} to $\overline{\mathbb{Q}}$-rational points.

Conjecture 9 (Universality of fundamental groupoid functor) *Let* $\underline{\Omega} = (\mathrm{Pt}, \Omega, s_V, t_V, \cdot_V)$ *be a functor from category* $\mathfrak{E}$ *to* $\mathfrak{Groupoids}$ *such that*

(1) *the functor of points of is the functor of* $\overline{\mathbb{Q}}$*-rational points:* $\mathrm{Pt}(X) = X(\overline{\mathbb{Q}}) = \mathcal{M}or_{\mathfrak{SC}}(O, X)$, $X \in \mathfrak{SC}$.
(2) $\underline{\Omega}$ *preserves direct products:* $\underline{\Omega}(X \times Y) = \underline{\Omega}(X) \times \underline{\Omega}(Y)$.
(3) $\underline{\Omega}$ *has the unique path-lifting property along étale morphisms: for an étale morphism* $f : X \to Y$, *a path* $\gamma \in \Omega(Y)$ *and a point* $x \in \mathrm{Pt}(X)$ *such that* $\mathrm{Pt}(f)(x) = s(\gamma)$, *there exists a unique path* $\widetilde{\gamma} \in \Omega(X)$ *such that* $\Omega(f)(\widetilde{\gamma}) = \gamma$ *and* $s(\widetilde{\gamma}) = x$.

Assume further that

(4) $\underline{\Omega}(E)$ *is a connected groupoid*
(5) *there is an isomorphism*

$$\Omega_{0,0}(S) := \{\gamma \in \Omega(S) : s(\gamma) = t(\gamma) = 0\} \cong \pi_1^{\mathrm{top}}(S(\mathbb{C}), O).$$

Then there exists an automorphism $\sigma \in Gal(\overline{\mathbb{Q}}/k)$ *such that the functors* $\underline{\Omega}$ *and* $\pi_1^{\mathrm{top}}{}_{|\overline{\mathbb{Q}}} \circ \sigma : \mathfrak{E} \to \mathfrak{Groupoids}$ *are naturally equivalent:*

$$\underline{\Omega} \cong \pi_1^{\mathrm{top}}{}_{|\overline{\mathbb{Q}}} \circ \sigma$$

It is possible that only a weaker conclusion holds: there exists *finitely many* functors $\mathbb{F}_1, \ldots, \mathbb{F}_n$ satisfying (1)–(5) such that for any functor $\underline{\Omega}$ satisfying (1)–(5) there exists $\sigma \in Gal(\overline{\mathbb{Q}}/k)$ such that $\underline{\Omega} \circ \sigma$ is naturally equivalent to one of $\mathbb{F}_1, \ldots, \mathbb{F}_n$.

References

1. Bashmakov, M.: The cohomology of an abelian variety over a number field. Russ. Math. Surv. **27**, 25–70 (1972)
2. Bertrand, D.: Kummer theory of a product of an elliptic curve by the multiplicative group. Glasgow Math. J. **22**(1), 83–88 (1982)
3. Bertrand, D.: Galois representations and transcendental numbers. In: New advances in transcendence theory (Durham, 1986), pp. 37–55. Cambridge University Press, Cambridge (1988)
4. Bertrand, D.: Minimal heights and polarizations on group varieties. Duke Math. J. **80**(1), 223–250 (1995)
5. Chi, W.: l-adic and-adic representations associated to abelian varieties defined over a number field. Am. J. Math. **114**(3), 315–353 (1992)
6. Gavrilovich, M.: Model Theory of the Universal Covering Spaces of Complex Algebraic Varieties. Ph.D. thesis, Oxford University (2005), available at http://misha.uploads.net.ru/misha-thesis.pdf (submitted)
7. Grothendieck, A.: Pursuing Stacks, also known as Long Letter to Quillen, http://www.grothendieck-circe.org
8. Jacquinot, O., Ribet, K.A.: Deficient points on extensions of abelian varieties by $\mathbf{G}_m$. J. Number Theory **25**(2), 133–151 (1987)
9. Lang, S.: Elliptic curves: Diophantine analysis, vol. 231. Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Sciences). Springer, Berlin (1978)
10. Masser, D.W.: Linear relations on algebraic groups. In: New advances in transcendence theory (Durham, 1986), pp. 248–262. Cambridge University Press, Cambridge (1988)
11. Mumford, D.: Abelian varieties. Tata institute of fundamental research studies in mathematics, vol. 5. Published for the Tata Institute of Fundamental Research, Bombay (1970)
12. Ohta, M.: On l-adic representations of Galois groups obtain from certain two-dimensional abelian varieties. J. Fac. Soc. Univ. Tokyo Sect. 1A Math. **21**, 299–308 (1974)
13. Ribet, K.: Kummer theory on extensions of varieties by tori. Duke Math. J. **46**(4), 745–761 (1979)
14. Ribet, K.A.: Cohomological realization of a family of 1-motives. J. Number Theory **25**(2), 152–161 (1987)
15. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–333 (1972)
16. Serre, J.-P.: Abelian l-adic representations and elliptic curves, vol. 7, Research Notes in Mathematics. A K Peters Ltd., Wellesley, with the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original (1998)
17. Serre, J.-P.: Résumé de cours de 1986–1987. In: Œuvres. Collected papers. Springer, Berlin 1985–1998 (2000)
18. Shelah, S.: Classification theory for non-elementary classes. I. The number of uncountable models of $\psi \in L_{\omega_1,\omega}$. Part A'. Israel J. Math. **46**(3), 212–240 (1983)
19. Shelah, S.: Classification theory for non-elementary classes. I. The number of uncountable models of $\psi \in L_{\omega_1,\omega}$. Part B'. Israel J. Math. **46**(4), 241–273 (1983)
20. Voevodsky, V., Kapranov, M.: ∞-groupoids and homotopy types. Cah. Top. Géom. Diff. Cat. **32**, 29–46 (1991)
21. Zarhin, G.Y.: Torsion of Abelian varieties in finite characteristic. Math. Notes **22**, 493–498 (1978)
22. Zilber, B.: Covers of Multiplicative group of algebraically closed field, http://www.maths.ox.ac.uk/~zilber
23. Zilber, B.: Logically Perfect Structures. slides, available at http://www.maths.ox.ac.uk/~zilber