# Categoricity Results for Exponential Maps of 1-Dimensional Algebraic Groups
# &
# Schanuel Conjectures for Powers and the CIT

Martin Bays

Christ Church

Oxford University

A thesis submitted for the degree of

*Doctor of Philosophy*

December 16, 2009

*To my mother and my father*

# Abstract

In the first part of this thesis, we show that the universal cover of a complex elliptic curve has a natural categorical $L_{\omega_1,\omega}$ axiomatisation, extending work of Gavrilovich and answering a question of Zilber. Following Zilber [Zil02a], we approach this via the model-theoretic criterion of *excellence*; this reduces the categoricity problem to the validity of certain versions of the Mordell-Weil theorem and of Kummer theory lifted to fields arising from certain independent configurations of algebraically closed fields, an example of such a field being $\mathbb{Q}(L_1, L_2)$ where $L_1$ and $L_2$ are algebraically closed and linearly disjoint over $\overline{\mathbb{Q}}$. We show that these lifted theorems do indeed hold, and conclude the categoricity via a direct algebraic argument.

In the second part of this thesis, we consider another locus of interaction between model theory and number theory, the Conjecture on Intersections with Tori. We show that it can be viewed as a conjecture of Schanuel type, for raising to non-standard integer powers. We then use this idea to prove a constrained version of the conjecture, via results on the truth of the Schanuel conjecture for raising to generic powers in exponential fields.

# Acknowledgements

I would like to thank

- Boris Zilber, my DPhil supervisor, for his persistent support, guidance, and subtle restraint of my capricious tendencies;
- Misha Gavrilovich, for his patience and encouragement as I followed stumbling in his footprints;
- The many other people who provided interesting and occasionally even useful mathematical conversation - allow me to name, in exact order of importance: John Baldwin, Juan-Diego Caycedo, Tom Foster, Assaf Hasson, Philipp Hieronymi, Gareth Jones, Itay Kaplan, Jonathan Kirby, Jochen Königsmann, Piotr Kowalski, Olivier Lessmann, Amador Martin-Pizarro, David Masser, Margaret Thomas, and Alex Wilkie;
- Ofer Gabber, who pointed out a fatal flaw in an earlier, drastically over-simplified version of a part of this work;
- Lyon 1, its faculty and staff, for their hospitality during my placement there, where many of the ideas of this thesis were developed; also the Marie Curie network MATHLOGAPS which put me there;
- The authors of and contributors to the Free software projects which have assisted in the authorship of this thesis, notably LaTeX, `vim`, `darcs`, `screen`, and GNU/Linux;
- Society at large, which allowed me to eat while I was doing work with no immediately obvious social benefit. I can only hope that it knows something I don't.

# Contents

## 0.1 Overview

This thesis aims to contribute to the model theoretic study of complex analytic structure. In keeping with the basic philosophy of the model theoretic approach to mathematics, this proceeds by considering certain narrowly defined parts of the wider theory and studying them in isolation. For example, we might isolate the field structure $\langle \mathbb{C}; +, \cdot \rangle$ on the complex numbers; in so doing, we forget about every other aspect of the complex numbers as we may usually think about them, in a way strongly analoguous to the passage from the complex analytic topology on $\mathbb{C}$ to the much coarser Zariski topology. The complex field is a canonical example of a model-theoretically tractable structure - its theory is uncountably categorical, and in particular stable, has quantifier elimination in the field language, and is decidable.

Now consider adding a little more complex analytic structure, for example the complex exponential map. The resulting structure $\mathbb{C}_{\exp} := \langle \mathbb{C}; +, \cdot, \exp \rangle$ encodes the interaction of complex exponentiation with algebraic geometry, and nothing more. However, it is already severely non-tractable from the point of view of traditional finitary first-order logic - it interprets arithmetic, and so its first-order theory is certainly neither decidable nor stable. Nonetheless, it is the thesis of Boris Zilber that $\mathbb{C}_{\exp}$, amongst other structures arising from complex analysis, should be treatable with the methods of stability theory - or even with categoricity theory. The existence of a countably infinite definable set, such as the kernel of exp, is a characteristic feature of (non-compact) complex analytic structure, and this already contradicts categoricity of the first-order theory. So we see that we must look beyond the confines of traditional first-order logic.

Zilber's approach is to look to infinitary logics, such as $L_{\omega_1,\omega}$, which extends usual first-order logic by allowing countably infinite conjunctions and disjunctions, or $L_{\omega_1,\omega}(Q)$ which further adds a quantifier for "there exist countably many". Analogues of first-order classification theory have been partially developed for these logics, chiefly by Shelah. In particular, Shelah isolated sufficient and (at least under certain set theoretic hypotheses) necessary conditions for categoricity in uncountable cardinalities. Chief among these is the condition of "excellence". A key idea in non-elementary classification theory is that uncountable models are built up from their countable elementary submodels, and so can be classified by looking at how these countable submodels are arranged. Excellence is a condition implying severe constraints on what configurations of countable submodels can occur; roughly, it states that any finite system of independently placed countable elementary submodels has a unique least independent amalgam.

Using these ideas, Zilber finds [Zil05a] an $L_{\omega_1,\omega}(Q)$-theory in the vocabulary of exponential fields, the theory of *pseudo-exponentiation*, which has unique models in all uncountable powers and whose unique model of cardinality continuum is not known not to be isomorphic to $\mathbb{C}_{\exp}$. In proving this categoricity, he effectively shows that it reduces to proving categoricity of a substantially weaker theory: that of the universal cover of the multiplicative group.

The complex exponential map is the universal group covering map $\exp : \mathbb{C} \to \mathbb{C}^\times$ of $\mathbb{C}^\times$, by which we mean that it satisfies the following universal property: for any group cover $\rho : G \to \mathbb{C}^\times$ with $G$ a connected topological group, where a group cover is a covering map of topological spaces which is also a group homomorphism, there exists a unique group cover $\theta : \mathbb{C} \to G$ such that $\exp = \rho \circ \theta$. In the structure $\mathbb{C}_{\exp}$, the domain and codomain of this map exp are identified. If instead we separate them out as two sorts, it is natural to consider the domain as simply a group, while the codomain should retain the full field-algebraic structure. The resulting structure $\langle (\mathbb{C}; +); (\mathbb{C}; +, \cdot); \exp \rangle$ is a weak reduct of $\mathbb{C}_{\exp}$, which in fact is quite simple from the point of view of first-order model theory - its first order theory $T_{\mathbb{G}_m}$ is superstable, and has quantifier elimination once division-by-$m$ maps are added to the covering sort. However, $\ker(\exp) \cong \mathbb{Z}$ is countably infinite, and so $T_{\mathbb{G}_m}$ is not uncountably categorical. Working in $L_{\omega_1,\omega}$ this is not a problem, as we can add an axiom ($\ker(\exp) \cong \mathbb{Z}$) fixing the isomorphism type of the kernel. Indeed, the class of models of $T_{\mathbb{G}_m} \cup \{(\ker(\exp) \cong \mathbb{Z})\}$ turns out to be uncountably categorical; the proof is in [Zil06, BZ07, Zil05b], and we will have more to say about it.

The property of uncountable categoricity in these cases splits naturally into three properties:

(A) Existence of a prime model, i.e. a countable model $C_0$ which embeds elementarily into any model.

(B) Homogeneity for countable submodels: if $C \preceq C'$ with $C$ and $C'$ countable models, then whenever $C$ embeds elementarily into an uncountable model $M$, $C'$ embeds elementarily into $M$ over $C$.

(C) Excellence.

Since a model of cardinality $\aleph_1$ is the direct limit of a chain of countable submodels and elementary embeddings, (A) and (B) suffice to prove $\aleph_1$-categoricity by a back-and-forth argument.

We have been considering complex exponentiation as the universal covering map of the multiplicative group $\mathbb{G}_m$. This is a rather special case of a universal cover of a complex variety. In his thesis [Gav06], Misha Gavrilovich considers the model theory of the universal cover of an arbitrary projective complex variety, with a structure taking into account both the algebraic structure on the variety and some homotopy theoretic information. In certain cases, in particular for abelian varieties, he finds an $L_{\omega_1,\omega}$-axiomatisation in a countable vocabulary which satisfies (B). The class of models extending a fixed countable model is therefore $\aleph_1$-categorical.

In the case of a 1-dimensional abelian variety, i.e. an elliptic curve $\mathbb{E}$, he finds that this structure reduces to a structure $\langle \mathbb{C}; \mathbb{E}(\mathbb{C}); \exp \rangle$ analogous to the two-sorted structure of complex exponentiation considered above. Here exp is now the universal group cover $\exp : \mathbb{C} \to \mathbb{E}(\mathbb{C})$, the covering sort $\mathbb{C}$ is considered in a weak linear language - namely as an $\mathrm{End}(\mathbb{E})$-module where $\mathrm{End}(\mathbb{E})$ is the ring of algebraic endomorphisms of $\mathbb{E}$ - and $\mathbb{E}(\mathbb{C})$ is considered with the full algebraic structure, i.e. with a predicate for every Zariski $k_0$-closed subset of $\mathbb{E}^n$ where

$k_0 \leq \mathbb{C}$ is the field of definition of $\mathbb{E}$. The $L_{\omega_1,\omega}$ theory in question is again just the first-order theory along with an axiom ($\ker(\exp) \cong \mathbb{Z}^2$) specifying the kernel of exp. Gavrilovich finds not only that this theory is model homogeneous, but that (perhaps after a mild extension of the theory) there is a prime model. So he proves $\aleph_1$-categoricity in this case.

We might hope that full uncountable categoricity holds, firstly because this would provide further evidence for Zilber's thesis that non-elementary stability theory is relevant to the study of natural objects of complex analysis, secondly because we would like to be able to conclude that we have found a categorical axiomatisation of $\langle \mathbb{C}; \mathbb{E}(\mathbb{C}); \exp \rangle$ without assuming the continuum hypothesis, and thirdly because it would pave the way to a study of the Weierstrass map of an elliptic curve in analogy with Zilber's study of $\mathbb{C}_{\exp}$ discussed above. What we lack for this, then, is the excellence condition. As the main result of the first Part of the present work, we prove (chapters 1-4) this excellence condition and deduce uncountable categoricity of this theory of the universal cover of an elliptic curve $\mathbb{E}$, under the assumptions that $\mathbb{E}$ is defined over a number field and has no complex multiplication.

Our methods are essentially algebraic and arithmetic in nature. In fact, we opt to give a fully self-contained proof of the categoricity result without direct appeal to the general model theoretic theory of excellence. The approach mirrors the proof referred to above for the case of the multiplicative group, and in fact we give a uniform proof which works both for the multiplicative group and for elliptic curves. The main differences between these two cases are firstly that the necessary Kummer theory is rather more subtle for elliptic curves, and secondly that the non-trivial Galois cohomology of elliptic curves adds some complications. Chapter 1 opens with a more detailed introduction to the categoricity statement and its proof.

The second Part of this thesis concerns itself with another aspect of the model theoretic study of exponentiation. We talked above about the structure $\mathbb{C}_{\exp}$ and about pseudo-exponentiation. A crucial idea behind that work is that it might be possible to regard $\mathbb{C}_{\exp}$ as being a Hrushovski-Fraissé amalgam with respect to the predimension function on finite tuples of elements:

$$\delta^{\exp}(\overline{x}) := \operatorname{trd}(\overline{x}, \exp(\overline{x})) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}).$$

This means firstly that $\delta^{\exp}$ is always non-negative on $\mathbb{C}$, and secondly that if $A$ is a subset and the relativised predimension

$$\delta^{\exp}_A(\overline{x}) := \operatorname{trd}(\overline{x}, \exp(\overline{x})/A) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}/A)$$

is always non-negative on $\mathbb{C}$, then any quantifier free formula over $A$ consistent with $\delta^{\exp}_A$ being non-negative is realised in $\mathbb{C}$ over $A$.

The first condition, that $\delta^{\exp}$ is always non-negative, is precisely Schanuel's famous conjecture on the transcendence theory of complex exponentiation.

Now let $K \leq \mathbb{C}$ be an arbitrary subfield, and consider the structure $\mathbb{C}^K := \langle(\mathbb{C}; +, (k\cdot)_{k\in K}); (\mathbb{C}; +, \cdot); \exp\rangle$, intermediate in expressive power between $\mathbb{C}_{\exp}$ and the universal cover of $\mathbb{G}_m$, which retains the $K$-vector space structure on the cover rather than just the group structure. The image under exp of the graph of multiplication by $k \in K$ is the graph of the many-valued analytic operation of raising to power $k$, so we think of $\mathbb{C}^K$ as the structure of raising to $K$-powers. In [Zil03], Zilber again considers that such structures might be Hrushovski-Fraissé amalgams with respect to embeddings respecting a predimension function; in this case, slightly simplifying his analysis, we can consider the function:

$$\delta^K(\overline{x}) := \operatorname{ld}_K(\overline{x}/\ker) + \operatorname{trd}(\exp(\overline{x})) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}/\ker),$$

defined on the cover sort, where $\ker := \ker(\exp)$.

We will refer to the condition

$$\forall\overline{x}.\delta^K(\overline{x}) \geq 0$$

as the *$K$-powers Schanuel inequality.*

In contrast to the case of $\mathbb{C}_{\exp}$, for some values of $K$ it is actually possible to prove that $\mathbb{C}^K$ satisfies the $K$-powers Schanuel inequality and is a Hrushovski-Fraissé amalgam with respect to $\delta^K$. Indeed, a consequence of the main result Theorem 1.3 of [BKW08] (which is also Theorem 7.1.3 of this thesis) is that for $\overline{\lambda} \in \mathbb{R}^n$ exponentially algebraically independent in $\mathbb{C}_{\exp}$, $\delta^{\mathbb{Q}(\overline{\lambda})}$ is non-negative on $\mathbb{C}$. Meanwhile, Zilber showed ([Zil02b, Theorem 5] and [Zil03, Fact 3]) using results of Khovanskii that the corresponding existential closedness holds for any $K \subseteq \mathbb{R}$ for which the $K$-powers Schanuel inequality holds.

Also in contrast to the case of $\mathbb{C}_{\exp}$, there is no obvious obstruction to $\mathbb{C}^K$ having a tame first-order theory. Moreover, the general theory of Hrushovski constructions indicates that if the $K$-powers Schanuel inequality and the existential closedness are first-order axiomatisable, then the theory they axiomatise will be near-model-complete and superstable. Consider the problem of axiomatising the $K$-powers Schanuel inequality. We would like to be able to say, for each $d$, "if $\operatorname{ld}_K(\overline{x}/\ker) + \operatorname{trd}(\exp(\overline{x})) \leq d$, then $\operatorname{ld}_{\mathbb{Q}}(\overline{x}/\ker) \leq d$". Now $\operatorname{ld}_{\mathbb{Q}}(\overline{x}/\ker) \leq d$ iff $\exp(\overline{x})$ is contained in an algebraic subgroup of $\mathbb{G}_m^n$ of dimension $\leq d$. For $d < n$, there are infinitely many such subgroups, and they do not form a definable family. So some sort of finiteness condition is needed so the right hand side of the implication can be written as a finite disjunction over subgroups.

Motivated by this problem, Zilber formulated the Conjecture on Intersection with Tori:

**Conjecture** (CIT)**.** *Let $W$ be a subvariety of $\mathbb{G}_m^n$ defined over $\mathbb{Q}$. There exists a finite set $\tau(W)$ of algebraic subgroups of $\mathbb{G}_m^n$ such that if $T \leq \mathbb{G}_m^n$ is an algebraic subgroup and $S$ is an irreducible component of $T \cap W$ such that*

$$\operatorname{codim}(S) < \operatorname{codim}(T) + \operatorname{codim}(W)$$

*(where $\operatorname{codim}(V) := \operatorname{codim}_{\mathbb{G}_m^n}(V) = n - \dim(V)$), then $S \subseteq T'$ for some $T' \in \tau(W)$.*

In [Zil03] he concludes the axiomatisability of the $K$-powers Schanuel inequality, leading to the result that $\mathbb{C}^{\mathbb{Q}(\overline{\lambda})}$ has superstable near-model-complete theory, under the assumption of the CIT. In fact, in a later preprint [Zil04] he performs a finer analysis which leads to an unconditional proof. Nonetheless, the CIT and related conjectures remain of great interest. Some progress towards it has been made in recent work by number theorists and arithmetic geometers - Bombieri, Masser, Zannier, Habegger and collaborators - who came independently to consider essentially the same conjecture [BMZ99, BMZ07]. Work from this direction continues; however, the full conjecture appears out of reach for now.

The CIT can itself be seen as a Schanuel conjecture for powers. We give precise statements and proofs for this in Chapter 6. Roughly, the idea is to find a structure in which the family of algebraic subgroups of $\mathbb{G}_m^n$, which correspond to kernels of integer matrices acting by raising to powers, is a definable family. The most direct and unsubtle way to do this is simply to take the ring of integers $\mathbb{Z}$ as a sort, along with its action on $\mathbb{G}_m$. Taking a (fairly) saturated model and considering linear independence with respect to the interpretation $^*\mathbb{Z}$ of this sort then takes into account varying families of subgroups, and in this way we find that the CIT corresponds to a $^*\mathbb{Z}$-powers Schanuel conjecture of roughly the same form as those above.

This suggests a model-theoretic approach to attacking the CIT. If we can find an expansion of a field in which there is a definable set $P$ containing the integers and for which raising to $P$-powers is uniformly definable, i.e. $(x, p) \mapsto x^p$ is definable, then a Schanuel inequality for $P$-powers in arbitrary models will have CIT consequences, since in elementary extensions the interpretation of $P$ will effectively contain non-standard integers. In one well-known example of this due to Zilber and Poizat, Ax's theorem can be seen to imply a Schanuel inequality for raising to constant powers in a differential field, yielding a "function-field version" of the CIT known as the *Weak CIT*.

Another version of this idea is presented in Chapter 7, this time using the real exponential field $\mathbb{R}_{\exp}$ rather than a differential field. Exponentiation allows powers to be defined uniformly, and Theorem 7.1.3 mentioned above (which in fact ultimately derives from Ax's theorem), combined with celebrated results of Wilkie on the model theory of $\mathbb{R}_{\exp}$, provides certain versions of the powers Schanuel inequality for non-standard real powers. Along with some analysis of a Diophantine type, we can deduce some limited approximations to CIT on the reals, Theorems 7.2.2 and 7.2.3 with which the thesis closes. These methods can surely be pushed further, and I hope to explore this in future work.

## 0.2 Outline of this thesis

In Chapter 1, we give a more technical and less model-theoretic introduction to the categoricity result which is the focus of Chapters 1-4, and then set up some assumptions, conventions and notations for Part I; we then discuss independent systems of algebraically closed fields, making definitions and drawing some basic results for use throughout the proof of the categoricity result. In Chapter 2, we consider the group structure of $E(k)$ for certain relevant fields $k$. In Chapter 3, we obtain some results on Kummer theory for elliptic curves over independent systems. Chapter 4 brings together these results to prove our main categoricity theorems.

The remaining chapters describe other work, related to varying extents to that of Chapters 1-4. Chapter 5 shows how results important to categoricity serve to analyse a natural topological structure on covers of semi-abelian curves. In Chapters 6 and 7, which form a Part of their own, we change tack to discuss Zilber's Conjecture on Intersections with Tori and its relation to Schanuel conjectures for non-standard integer powers. Chapter 6 gives precise statements of these connections, and Chapter 7 then uses this idea to tackle some restricted parts of the CIT.

Finally, the Appendices contain various lemmas and Facts which it seemed best to relegate to them.

# Part I

# Categoricity Results for Exponential Maps of 1-Dimensional Algebraic Groups

# Chapter 1

# Introduction and Preliminaries

## 1.1 Introduction

Let $\mathbb{E}$ be an elliptic curve over $\mathbb{C}$. Considered as a complex Lie group, $\mathbb{E}(\mathbb{C})$ is isomorphic to a complex torus $\mathbb{C}/\Lambda$, for some lattice $\Lambda \cong \mathbb{Z}^2$. If $a \in \mathbb{E}(\mathbb{C})$, for $n \in \mathbb{N}$ there are therefore $n^2$ possible choices of $n$-division point $a_n \in \mathbb{E}(\mathbb{C})$, $na_n = a$. A *division system* above $a$ is a system $(a_n)_{n\in\mathbb{N}}$ of agreeing choices $a_n$ of an $n$-division point of $a$, agreeing in the sense that $a_{mn}$ is an $m$-division point of $a_n$ ($\forall m, n \in \mathbb{N}$). A choice of a division system above $a$ corresponds to a path in a finite-branching tree of countable depth, so there are continuum many such choices.

Denote by $\hat{V} = \hat{V}(\mathbb{C})$ the group of all division systems above points of $\mathbb{E}(\mathbb{C})$, with the obvious group structure

$$(a_n)_n + (b_n)_n := (a_n + b_n)_n.$$

Equivalently, $\hat{V}$ is the inverse limit of copies of the group $\mathbb{E}(\mathbb{C})$ with respect to the multiplication-by-$m$ maps $[m]$:

$$\hat{V}(\mathbb{C}) = \varprojlim_{\mathbb{N};|} \left([m] : \mathbb{E}(\mathbb{C}) \to \mathbb{E}(\mathbb{C})\right).$$

$\hat{V}$ is a divisible abelian group. Define $\hat{\pi}$ as the map picking out the point above which a division system lies, $\hat{\pi} : \hat{V} \to \mathbb{E}; (a_n)_n \mapsto a_1$.

We denote by $T$ the kernel of $\hat{\pi}$, the group of all division systems above 0; these consist entirely of torsion elements of $\mathbb{E}$. The set of all division systems above $a \in \mathbb{E}(\mathbb{C})$ is a coset of $T$.

Now, $\mathbb{E}(\mathbb{C})$ comes equipped with the complex topology. Some division systems $(a_n)_n$ converge to $0 \in \mathbb{E}(\mathbb{C})$ in the limit $n \to \infty$, the others do not converge. Let us consider the set $V_{\mathrm{an}} \subseteq \hat{V}$ of those division systems which do converge. This set is most easily understood by considering the complex Lie exponential map. There exists a complex analytic homomorphism exp and a lattice $\Lambda \leq \mathbb{C}$ such that we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \Lambda \arrow[r] & \mathbb{C} \arrow[r, "\exp"] & \mathbb{E}(\mathbb{C}) \arrow[r] & 0 \end{tikzcd}.$$

Now any $\alpha \in \mathbb{C}$ induces the division system $(\exp(\frac{\alpha}{n}))_n$. Since exp is a local homeomorphism at the identity, the convergent division systems are precisely those of this form.

So $V_{\mathrm{an}}$ is a divisible subgroup of $\hat{V}$, and $V_{\mathrm{an}} \cap T \cong \Lambda \cong \mathbb{Z}^2$; in particular, there are only countably many convergent division systems above a given $a \in \mathbb{E}(\mathbb{C})$.

In this way, the complex topology has picked out a small class of distinguished division systems. Now forget the complex analytic structure, and consider $\mathbb{C}$ just as a field, and $\mathbb{E}(\mathbb{C})$ just as an algebraic group, leaving the choice of the distinguished set $V_{\mathrm{an}} \leq \hat{V}$ of division systems as the only trace of the analytic structure. We ask: how does this choice of $V_{\mathrm{an}} \leq \hat{V}$ interact with the algebraic structure? Can we give a description of a "purely algebraic" nature which determines the situation up to isomorphism?

To simplify some aspects of the discussion, let us assume that $\mathbb{E}$ is defined over $\mathbb{Q}$. Let us also assume that $\mathbb{E}$ has no complex multiplication. With some minor modifications which will be discussed in the body of the text, our results go through for $\mathbb{E}$ defined over an arbitrary number field; the restriction on complex multiplication, on the other hand, will remain throughout (this is a limitation of the present work, and probably is not a necessary restriction - see Section 4.5).

To formalise the question, consider the two-sorted structure $\langle \mathbb{C}; V_{\mathrm{an}}; \pi \rangle$, where the first sort is the complex field $(\mathbb{C}; +, \cdot)$, the second sort is $V_{\mathrm{an}}$ considered as a $\mathbb{Q}$-vector space $(V_{\mathrm{an}}; +, (q\cdot)_{q\in\mathbb{Q}})$, and $\pi$ is the restriction $\hat{\pi}\restriction_{V_{\mathrm{an}}}: V_{\mathrm{an}} \to \mathbb{E}(\mathbb{C})$. This choice of language means that a second structure $\langle K; V'; \pi' \rangle$ is isomorphic to $\langle \mathbb{C}; V_{\mathrm{an}}; \pi \rangle$ iff there is a field isomorphism $\sigma : \mathbb{C} \to K$ and a group isomorphism $\tau : V_{\mathrm{an}} \to V'$ such that $\pi' \circ \tau = \sigma \circ \pi$.

If $\langle K; V'; \pi' \rangle \cong \langle \mathbb{C}; V_{\mathrm{an}}; \pi \rangle$, it follows:

(I) $K$ is isomorphic as a field to $\mathbb{C}$

(II) $V'$ is a divisible torsion-free abelian group

(III) $\pi' : V' \to \mathbb{E}(K)$ is a surjective homomorphism

(IV) $\ker(\pi') \cong \mathbb{Z}^2$ as groups.

We can ask whether these necessary conditions are also sufficient, i.e. whether this description (I)-(IV) of the structure $\langle \mathbb{C}; V_{\mathrm{an}}; \pi \rangle$ suffices to determine it up to isomorphism.

Before we answer this question, let us rephrase it in a more intuitive and manageable form by noting that we can work entirely in $\hat{V}$. Let $\langle K; V'; \pi' \rangle$ satisfy (I)-(IV). By (I), we lose nothing by assuming $K = \mathbb{C}$. Let $V \leq \hat{V}$ be the group of division systems on $\mathbb{E}(\mathbb{C})$ induced by $V'$ and $\pi'$ - explicitly:

$$V := \{(\pi'({}^{v'}/_{n}))_n \mid v' \in V'\} \leq \hat{V}.$$

Then $\langle \mathbb{C}; V'; \pi' \rangle \cong \langle \mathbb{C}; V; \hat{\pi}\restriction_V \rangle$.

Let us refer to divisible subgroups $V \leq \hat{V}$ such that $\hat{\pi}(V) = \mathbb{E}(\mathbb{C})$ and $V \cap T \cong \mathbb{Z}^2$ as *standard* subgroups $V \leq \hat{V}$. So we see that any structure satisfying (I)-(IV) is isomorphic to $\langle \mathbb{C}; V; \hat{\pi}\restriction_V \rangle$ for some standard $V \leq \hat{V}$, and conversely any such satisfies (I)-(IV). Now for standard $V \leq \hat{V}$, $\langle \mathbb{C}; V_{\text{an}}; \pi \rangle \cong \langle \mathbb{C}; V; \hat{\pi}\restriction_V \rangle$ iff there exists a field automorphism $\sigma \in \text{Aut}(\mathbb{C})$ such that $\sigma(V_{\text{an}}) = V$, where we define $\sigma$ on $\hat{V}$ by $\sigma((a_n)_n) := (\sigma(a_n))_n$.

So we see that describing the isomorphism type of the structure $\langle \mathbb{C}; V_{\text{an}}; \pi \rangle$ is equivalent to describing the orbit of $V_{\text{an}}$ in $\hat{V}$ under the action of $\text{Aut}(\mathbb{C})$. In particular, (I)-(IV) describe $\langle \mathbb{C}; V_{\text{an}}; \pi \rangle$ uniquely up to isomorphism iff the set of standard $V \leq \hat{V}$ forms a single orbit under the action of $\text{Aut}(\mathbb{C})$. We will find that this is indeed the case (under our simplifying assumption that $\mathbb{E}$ is defined over $\mathbb{Q}$ - more generally, there are finitely many orbits).

This has a purely arithmetic aspect: if we replace everywhere in the above discussion $\mathbb{C}$ with $\bar{\mathbb{Q}}$, we are left with questions about the action of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $\mathbb{E}(\bar{\mathbb{Q}})$, which turn out to correspond to well-known results of Serre on Galois representations, of Bashmakov on Kummer theory for elliptic curves, and of Mordell-Weil on the structure of $\mathbb{E}(F)$ for $F$ a finitely generated extension of $\mathbb{Q}$. This part of the story was worked out by Gavrilovich in his thesis [Gav06]. To get up from $\bar{\mathbb{Q}}$ to $\mathbb{C}$, however, we require ideas of an essentially different character.

In terms of mathematical logic, to ask whether (I)-(IV) determine $\langle \mathbb{C}; V_{\text{an}}; \pi \rangle$ uniquely up to isomorphism is to ask whether they comprise a *categorical* axiomatisation. We can express (II)-(IV) as an axiom in the infinitary formal language $L_{\omega_1,\omega}$ which allows countably infinite conjunctions; if we add to this the first order condition that $K$ is an algebraically closed field of characteristic 0, we obtain an infinitary sentence $\sigma$ which, together with the condition that $K$ is of cardinality continuum, is equivalent to (I)-(IV). So in model theoretic terms, our question is that of categoricity in cardinality continuum of the $L_{\omega_1,\omega}$ sentence $\sigma$. As discussed in the introduction to the thesis, Shelah gave [She83a] [She83b] abstract conditions for such categoricity. Key to this is the condition of "excellence", which roughly states that any system of independently placed countable models has a unique least independent amalgam.

Specialising these ideas to our context, we find that we must generalise the arithmetic results to cases where the base field is a compositum of algebraically closed fields placed in a certain independent configuration ($L^-$ in Definition 1.3.1 below). In particular, we require structure theorems in the style of Mordell-Weil for the groups of $F$-rational points of $\mathbb{E}$ for $F$ a finitely generated extension of a such a field, and a version of Kummer theory which works for such bases.

The sufficiency and, in a certain sense, necessity of these conditions for categoricity was expounded by Zilber in [Zil02a]. The contribution of the present work is to show that these conditions do indeed hold. The proofs, and proper statements, are contained in Chapters 1-3. We also give, in Chapter 4, a self-contained, purely algebraic proof of categoricity from them.

## 1.2 Setup and notation

We now begin the formal presentation of the results sketched above.

We work in characteristic 0 except where otherwise stated.

$\mathcal{C}$ denotes a large algebraically closed characteristic 0 field; unless otherwise specified, all fields are assumed to be subfields of $\mathcal{C}$.

$\mathbb{G}$ is either the multiplicative group $\mathbb{G}_m$ or an elliptic curve $\mathbb{E}$ defined over a number field $k_0$. We write the group structure additively. In the case $\mathbb{G} = \mathbb{G}_m$, we let $k_0 := \mathbb{Q}$. In the case that $\mathbb{G} = \mathbb{E}$ is an elliptic curve, *we assume that the elliptic curve has no complex multiplication*, i.e. that $\operatorname{End}(\mathbb{G})$, the ring of algebraic endomorphisms (i.e. of endomorphisms with closed graph), contains only the obvious multiplication-by-$m$ endomorphisms $[m]$; i.e. $\operatorname{End}(\mathbb{G}) \cong \mathbb{Z}$.

The remainder of this section sets some notation and mentions some basic facts. This is mostly all standard or obvious, or else was already explained in the introduction. The hurried reader is advised to skim the remainder of this section, and return as necessary.

$G_m := \ker([m]) \leq \mathbb{G}(\mathcal{C})$ denotes the absolute $m$-torsion. $G_\infty := \cup_n G_n$ is the full torsion group, and for $l$ a prime, $G_{l^\infty} := \cup_n G_{l^n}$ is the $l$-power torsion.

As discussed above, for $K$ algebraically closed containing $k_0$, we define $\hat{V}(K) := \varprojlim_{\mathbb{N};|}([m] : \mathbb{G}(K) \to \mathbb{G}(K))$, the inverse limit of copies of $\mathbb{G}(K)$ with respect to the multiplication-by-$m$ maps $[m]$; we define $\hat{\pi}_n : \hat{V}(K) \to \mathbb{G}(K)$ to be the corresponding maps, so

$$[m] \circ \hat{\pi}_{nm} = \hat{\pi}_n,$$

and let $\hat{\pi} := \hat{\pi}_1$.

A field automorphism $\sigma \in \mathrm{Aut}(K/k_0)$ acts on $\mathbb{G}(K)$ and hence on $\hat{V}(K)$: $\sigma((a_m)_{m\in\mathbb{N}}) := (\sigma(a_m)_{m\in\mathbb{N}})$.

Set

$$T := \ker(\hat{\pi}) = \varprojlim_{n|m}([{}^m/_n] : G_m \to G_n);$$

we consider $T$ with the profinite topology induced by this inverse limit.

Similarly, for $l$ a prime we define the $l$-adic Tate module

$$T_l := \varprojlim_{n\leq m}([l^{m-n}] : G_{l^m} \to G_{l^n}),$$

considered as a profinite group and as a $\mathbb{Z}_l$-module.

**Fact 1.2.1.** *$G_m \cong ({}^{\mathbb{Z}}/_{m\mathbb{Z}})^d$, where $d = 1$ if $\mathbb{G} = \mathbb{G}_m$ and $d = 2$ if $\mathbb{G} = \mathbb{E}$.*

*It follows that $T \cong \hat{\mathbb{Z}}^d$ and $T_l \cong \mathbb{Z}_l^d$.*

**Definition 1.2.1.** For $k$ a field containing $k_0$ such that $G_\infty \leq \mathbb{G}(k)$, define the *$\bar{k}/k$-Kummer-Tate pairing*:

$$\begin{array}{ccccc} \langle\cdot,\cdot\rangle_\infty^{\bar{k}/k} & : & \mathrm{Gal}(\bar{k}/k) \times \mathbb{G}(k) & \to & T \\ & ; & (\sigma, a) & \mapsto & \sigma\alpha - \alpha \quad (\text{any } \alpha \in \hat{\pi}^{-1}(a)). \end{array}$$

Since $G_\infty \leq \mathbb{G}(k)$, $\langle\cdot,\cdot\rangle_\infty^{\bar{k}/k}$ is well-defined and bilinear. For any $a \in \mathbb{G}(k)$,

$\langle \cdot, a\rangle_\infty^{\bar{k}/k}$ is continuous.

For a tuple $\overline{a} \in \mathbb{G}(k)^n$, we write $\langle \cdot, \overline{a}\rangle_\infty^{\bar{k}/k}$ for the map defined co-ordinatewise,

$$\begin{array}{rcccc} \langle \cdot, \overline{a}\rangle_\infty^{\bar{k}/k} & : & \mathrm{Gal}(\bar{k}/k) & \to & T^n \\ & ; & \sigma & \mapsto & (\langle \cdot, a_i\rangle_\infty^{\bar{k}/k})_i. \end{array}$$

We set some notation and conventions for talking about places:

**Definition 1.2.2.**

- A *place* is a partial ring homomorphism of fields $\pi : K \to k$ which is maximally defined, i.e. is such that $\mathcal{O}_\pi := \mathrm{dom}(\pi) \leq K$ is a valuation ring in $K$. $\pi$ is then the residue map of the valued field $K$, and we denote by $\mathfrak{m}_\pi := \ker_\pi$, $\Gamma_\pi := {}^{K^\times}/_{\mathcal{O}_\pi{}^\times}$, and $v_\pi : K^\times \to \Gamma_\pi$ the corresponding maximal ideal, value group, and valuation.

- If $k \leq K$, we write $\pi : K \to_k k$ if $\pi\restriction k = \mathrm{id}_k$. Such a place is sometimes known as a (partial) *specialisation* of $K$ to $k$, though we will not use this terminology.

- A place $\pi : K \to k$ induces a total map on the projective spaces, $\pi : \mathbb{P}^n(K) \to \mathbb{P}^n(k)$, defined on homogeneous co-ordinates by $\pi([a_0 : \ldots : a_n]) := [\pi(a_0/a_M) : \ldots : \pi(a_n/a_M)]$, where $M$ is such that $v_\pi(a_M)$ is least among $(v_\pi(a_i))_i$.

- If $k \leq K$ and $V \leq \mathbb{P}^n$ is a projective variety defined over $k$, $\pi$ restricts to a total map $\pi : V(K) \to V(k)$.

For subfields $F, F'$ of an algebraically closed field $K$, $F \vee F'$ is the definable closure in $K$ of $F \cup F'$, i.e. the perfect closure of the compositum of $F$ and $F'$. $F \wedge F' := F \cap F'$. $F \vee \overline{a}$ is the definable closure in $K$ of $F \cup \{a_1, ..., a_n\}$.

If $A \subseteq \mathbb{G}(\mathcal{C})$ and $k_0 \leq k \leq \mathcal{C}$, by $k(A)$ we mean the field generated over $k$ by the elements of $A$, i.e. by the co-ordinates of the elements of $A$ in some $k_0$-closed affine subvariety of $\mathbb{G}$. To be concrete, we could consider $\mathbb{G}_m$ as the plane affine variety $xy = 1$, and $\mathbb{E}$ as the projective closure of a plane curve $y^2 = f(x)$ with $f \in k_0[X]$ cubic. The model-theoretic reader may like to think of $\mathbb{G}$ as an imaginary sort (once parameters are added for $k_0$), in which case (the perfect closure of) $k(A)$ is the trace on the field sort of $\mathrm{dcl}^{eq}(k \cup A)$.

Similarly, by $\mathbb{G}(k)$ we mean those points of $\mathbb{G}(\mathcal{C})$ which can be taken with co-ordinates in $k$; for perfect $k$, this is the fixed set of the action of $\mathrm{Aut}(\mathcal{C}/k)$ on $\mathbb{G}(\mathcal{C})$ (or equivalently of the action of $\mathrm{Gal}(\bar{k}/k)$ on $\mathbb{G}(\bar{k}) \subseteq \mathbb{G}(\mathcal{C})$), which is precisely the trace on the sort $\mathbb{G}$ of $\mathrm{dcl}^{eq}(k)$.

(From a model-theoretic point of view, the reason for referencing the field sort all the time is that it has elimination of imaginaries and so Galois theory works there.)

For $A$ a set, $A^{<\omega}$ is the set of all finite tuples from $A$, i.e. $A^{<\omega} = \bigcup_{n \in \mathbb{N}} A^n$. We use the same notation for $A$ a definable set.

If $G$ is an abelian group and $\Gamma \leq G$ is a subgroup, $\mathrm{pureHull}_G(\Gamma)$ is the relatively divisible subgroup $\{\gamma \in G \mid \exists m \in \mathbb{N}.\ m\gamma \in \Gamma\}$. If $G$ is torsion-free, a tuple $\overline{\gamma} \in G^n$ is *simple* iff $\overline{\gamma}$ is a $\mathbb{Z}$-basis for $\mathrm{pureHull}_G(\langle\overline{\gamma}\rangle)$. For arbitrary abelian $G$, $\overline{\gamma} \in G^n$ is *simple* iff ${}^{\overline{\gamma}}/_{\mathrm{Tor}(G)}$ is simple in the torsion-free abelian group ${}^{G}/_{\mathrm{Tor}(G)}$.

## 1.3 Independent systems of algebraically closed fields

Independent systems of algebraically closed fields will play a key rôle in our arguments. The concept of an independent system of models was first isolated by Shelah in his work on classification theory for models of an $L_{\omega_1,\omega}$ theory ([She83a], [She83b]). Here we deal with a specialisation of these ideas to the rather particular case of the theory $\mathrm{ACF}_p$ of algebraically closed fields of a fixed characteristic. The remarks in [Hru06, Section 3] are relevant here, and our presentation owes something to that work.

**Definition 1.3.1.** Write $N$ for $\{0, \ldots, N-1\}$.

A system $(L_s | s \subseteq N)$ of algebraically closed subfields of an algebraically closed field $\mathcal{C}$ is called an *independent $N$-system* iff

(i) for all $s, t$: if $s \subseteq t$ then $L_s \leq L_t$;

(ii) for all $s, t$: $L_s$ is algebraically independent from $L_t$ over $L_{s \cap t}$;

(iii) for all $s$:

$$L_s = \operatorname{acl}(\bigcup_{i \in s}(L_{\{i\}})).$$

The system is *finitary* iff each $L_s$ is of finite transcendence degree over $L_\emptyset$.

Given an independent $N$-system $(L_s)_s$, we define: $L_{(i)} := L_{N \setminus \{i\}}$, $L_{(i,j)} := L_{N \setminus \{i,j\}}$ etc, and $L^- := \operatorname{dcl}^{L_N}(\bigcup_i (L_{(i)}))$.

We further define $\overline{\lambda}_{\{i\}}$ to be an (arbitrary) transcendence basis of $L_{\{i\}}$ over $L_\emptyset$, and let $\overline{\lambda}_s := \bigcup_{i \in s}(\overline{\lambda}_{\{i\}})$.

*Remarks* 1.3.1.

- $\overline{\lambda}_s$ is a transcendence basis of $L_s$ over $L_\emptyset$.
- Since $\overline{\lambda}_{s \cap t} = \overline{\lambda}_s \cap \overline{\lambda}_t$, we can reconstruct the system from $(\overline{\lambda}_{(i)})_i$.
- It is also possible to give a definition of an independent system without assumption (iii); see [She90, XII.2.1].

### 1.3.1 Independent systems and places

In this subsection, we prove in Lemma 1.3.3 that an independent $N$-system $(L_s)_s$ can be "collapsed" by a place down to $L_{(0)}$ in a certain controlled fashion. For example, for $N = 4$, picturing the system as a tetrahedron we show that it can be collapsed to the triangle at its base in such a way that the faces of the tetrahedron map to the corresponding edges of the triangle, and moreover that the definable closure of the faces maps to the definable closure of the edges.

We make use of the Newton-Puiseux theorem and the following generalisation to arbitrary characteristic:

**Fact 1.3.1** (Raynor [Ray68], cited in [Ked01])**.** *Let $L$ be an algebraically closed field of characteristic $p$. Let $L((t^{\mathbb{Q}}))$ be the field of generalised power series in $t$ with coefficients in $L$ and rational exponents, and let $L\{\{t\}\} \leq L((t^{\mathbb{Q}}))$ be the subfield consisting of those power series with support $S$ satisfying:*

- *($p = 0$) there exists $m \in \mathbb{N}$ such that $mS \subseteq \mathbb{Z}$;*
- *($p \neq 0$) there exists $m \in \mathbb{N}$ such that $mS \subseteq \mathbb{Z}[\frac{1}{p}] := \{mp^s | m, s \in \mathbb{Z}\}$.*

*Then $L\{\{t\}\}$ is an algebraically closed field.*

**Lemma 1.3.2.** *Let $L$ be an algebraically closed subfield of an algebraically closed field $\mathcal{C}$; suppose $L$ contains algebraically closed subfields $k_i$, $i \in \{1, \ldots n\}$; let $\lambda \in \mathcal{C}$ be transcendental over $L$; let $K := \operatorname{acl}^{\mathcal{C}}(L(\lambda)) \geq L$, and let $k_i' := \operatorname{acl}^{\mathcal{C}}(k_i(\lambda))$. Further, let $k_0 \leq L$ be a perfect subfield, and let $k_0' := k_0$.*

*Then for any place $\pi : K \to_L L$ such that $\pi(\lambda) \in \bigcap_{i>0} k_i$,*

$$\pi(\bigvee_{i \geq 0} k_i') = \bigvee_{i \geq 0} k_i.$$

*Proof.* Since replacing $\lambda$ with $\lambda - \pi(\lambda)$ does not alter $K$ or $k_i'$, and $\lambda - \pi(\lambda)$ is also transcendental over $L$, we may assume that $\pi(\lambda) = 0$.

Let $L\{\{\lambda\}\}$ be the field of generalised Puiseux series, as defined in Fact 1.3.1. Let $\pi' : L\{\{\lambda\}\} \to L$ be the standard power series residue map.

$\pi'$ agrees with $\pi$ on $L(\lambda)$, so by the Conjugation Theorem [EP05, 3.2.15] we may embed $K$ into $L\{\{\lambda\}\}$ in such a way that $\pi$ agrees with $\pi'$.

Now for $i > 0$, $k_i\{\{\lambda\}\} \leq L\{\{\lambda\}\}$, the subfield of power series with coefficients from $k_i$, is algebraically closed and contains $k_i(\lambda)$, so contains $k_i'$. Similarly, $k_0' = k_0 \leq k_0\{\{\lambda\}\}$.

Now

$$\begin{aligned}\pi(\bigvee_i k_i') &\leq \pi'(\bigvee_i (k_i\{\{\lambda\}\})) \\ &\leq \pi'((\bigvee_i k_i)\{\{\lambda\}\}) \\ &= \bigvee_i k_i\end{aligned}$$

□

**Lemma 1.3.3.** *Suppose $(L_s)_{s\subseteq N}$ is a finitary independent $N$-system of algebraically closed fields. Let $C$ be a perfect subfield of $L_{(0)}$.*

*Then there exists a place $\pi : L_N \to_{L_{(0)}} L_{(0)}$ such that $\pi(C \vee \bigvee_{i>0} L_{(i)}) = C \vee \bigvee_{i>0} L_{(0,i)}$.*

*Furthermore, for any $\overline{b} \in ({L_N}^\times)^n$, $\pi$ can be chosen such that $\pi(\overline{b}) \in ({L_{(0)}}^\times)^n$.*

*Proof.* Let $\overline{\lambda}_0$ be a basis for $L_{\{0\}}$ over $L_\emptyset$.

Let $f_{i,j}(\overline{\lambda}_0) \in L_{(0)}[\overline{\lambda}_0]$ be the non-zero coefficients of a minimal polynomial in $L_{(0)}[\overline{\lambda}_0][X]$ for $b_i$ over $L_{(0)}(\overline{\lambda}_0)$. Let $\overline{a} \in L_\emptyset$ such that $f_{i,j}(\overline{a}) \neq 0$ for all $i, j$.

Inductively, we may assume that $\overline{\lambda}_0 = \overline{\lambda}_0'\lambda_0$, correspondingly $\overline{a} = \overline{a}'a$, and that we have $\pi' : L_N' \to_{L_{(0)}} L_{(0)}$ such that $\pi'(\overline{\lambda}_0') = \overline{a}'$ and $\pi'(C \vee \bigvee_{i>0} L_{(i)}') = C \vee \bigvee_{i>0} L_{(0,i)}$, where for $s \ni 0$, $L_s' := \operatorname{acl}(L_{s\setminus\{0\}}(\overline{\lambda}_0'))$.

Apply Lemma 1.3.2 to obtain $\pi'' : L_N \to_{L_N'} L_N'$ with $\pi(\lambda_0) = a$ and $\pi''(C \vee \bigvee_{i>0} L_{(i)}) = C \vee \bigvee_{i>0} L_{(i)}'$; the composition $\pi := \pi' \circ \pi''$ is then as required. □

### 1.3.2 N-uniqueness

Unassuming though it may seem, the following lemma plays a crucial rôle:

**Lemma 1.3.4.** *Let $N \geq 2$; let $(L_s)_s$, be a finitary independent $N$-system of algebraically closed fields. For $i \in N$, let $\sigma_{(i)} \in \operatorname{Aut}(L_{(i)})$ and suppose they agree on intersections, $\sigma_{(i)}\restriction_{L_{(i,j)}} = \sigma_{(j)}\restriction_{L_{(i,j)}}$.*

*Then the $\sigma_{(i)}$ are consistent, i.e. $\bigcup_i \sigma_{(i)}$ extends to $\sigma_N \in \operatorname{Aut}(L_N)$.*

*Proof.* As a consequence of 1.3.3 with $C = \emptyset$, we have that

$$L_{(0)} \cap \bigvee_{i>0} L_{(i)} = \bigvee_{i>0} L_{(0,i)} =: B.$$

That the lemma follows from this was noted in a more general context in [Hru06, Section 3]; we give a proof here. If $N = 2$, the result is clear, so suppose $N > 2$. For $s \subseteq N \setminus \{0\}$, let $L'_s := L_{s \cup 0}$. $(L'_s)_s$ is then a finitary independent $(N-1)$-system; by induction, $\bigcup_{i>0} \sigma_{(i)}$ extends to $\sigma' \in \mathrm{Aut}(\bigvee_{i>0} L_{(i)})$. Now $\sigma'$ agrees with $\sigma_{(0)}$ on the intersection $B$ of their domains, and $L_{(0)} = \mathrm{acl}(B)$. By Galois theory, specifically [Lan02, VI Thm 1.12], it follows that $\sigma'$ and $\sigma_{(0)}$ are consistent, and extend to $\sigma_N$ as required. □

*Remark* 1.3.2. In fact, Lemma 1.3.4 is known to hold in much greater generality - [dPKM06, 1.6(2)] proves that $n$-uniqueness holds over a model in arbitrary stable theories, which implies Lemma 1.3.4. The model theoretic notion of a coheir substitutes ([dPKM06, 1.5(2)]) for the specialisation argument used above.

# Chapter 2

# Local freeness

## 2.1 Statement

In this chapter, we prove:

**Theorem 2.1.1.** *In each of the following situations, $^{\mathbb{G}(k)}/_{H}$ is locally free as an abelian group:*

*(i)* $k = k'(G_\infty)$*, where* $k'$ *is a finitely generated extension of* $k_0$*, and* $H = G_\infty$*.*

*(ii)* $k \geq k'$ *is a finitely generated regular extension of a field* $k' \geq k_0$*, and* $H = \mathbb{G}(k')$*.*

*(iii)* $(L_s)_{s \subseteq N}$ *is a finitary independent* $N$*-system of algebraically closed fields,* $N \geq 1$*,* $k$ *is a finitely generated extension of* $L^-$*, and* $H := \Sigma_i \mathbb{G}(L_{(i)})$*.*

(Section B.3 contains the basic definitions and results on local freeness.)

*Remark* 2.1.1. For the case $\mathbb{G} = \mathbb{G}_m$, essentially the same statement was proved in [Zil06, BZ07]. The presentation here in this case differs substantially from that in [Zil06] for part (i), and cosmetically from that in [BZ07] for (ii) and (iii).

## 2.2 Proof of Theorem 2.1.1(i)

For $k \geq k_0$, we have the embedding

$$\restriction_{G_\infty}\colon \operatorname{Gal}(k(G_\infty)/k) \hookrightarrow \operatorname{Aut}(G_\infty)\ ,$$

where $\operatorname{Aut}(G_\infty)$ is the group of automorphisms of the abelian group $G_\infty$.

**Theorem 2.2.1.** *There exists $m$ such that every automorphism of $G_\infty$ which fixes $G_m$ is induced by some field automorphism fixing $k_0$; i.e.*

$$\restriction_{G_\infty} (\operatorname{Gal}(k_0(G_\infty)/k_0)) \geq \operatorname{Aut}(G_\infty/G_m)$$

*Proof.* For $\mathbb{G} = \mathbb{E}$, this is a theorem of Serre - see Corollary B.1.1.1.

For $\mathbb{G} = \mathbb{G}_m$, it is a standard result of the theory of cyclotomic extensions that this holds with $m = 0$ [Lan02, VI.3.1]. □

**Corollary 2.2.1.1.** *Let $k$ be a finitely generated extension of $k_0$. Then there exists $m$ such that*

$$\restriction_{G_\infty} (\operatorname{Gal}(k(G_\infty)/k)) \geq \operatorname{Aut}(G_\infty/G_m)$$

*Proof.* Let $F := k \cap k_0(G_\infty)$. $F$ is an algebraic subextension of a finitely generated extension, and so $F$ is finite over $k_0$. So $F \leq k_0(G_t)$ for some $t \in \mathbb{N}$. By Theorem 2.2.1, there exists $m_0$ such that

$$\restriction_{G_\infty} (\operatorname{Gal}(k_0(G_\infty)/k_0)) \geq \operatorname{Aut}(G_\infty/G_{m_0}).$$

Let $m := \operatorname{lcm}(m_0, t)$. Then

$$\begin{aligned}\restriction_{G_\infty} (\operatorname{Gal}(k(G_\infty)/k)) &= \restriction_{G_\infty} (\operatorname{Gal}(k_0(G_\infty)/F)) \\ &\geq \restriction_{G_\infty} (\operatorname{Gal}(k_0(G_\infty)/k_0(G_t))) \\ &\geq \operatorname{Aut}(G_\infty/G_m).\end{aligned}$$

□

**Theorem 2.2.2.** *Let $k$ be a finitely generated extension of $k_0$. Then ${}^{\mathbb{G}(k)}/_{\mathbb{G}(k)\cap G_\infty}$ is free, and is finitely generated if $\mathbb{G} = \mathbb{E}$.*

*Proof.* $\mathbb{G} = \mathbb{E}$: this is the Mordell-Weil theorem [Lan83, Theorem 6:1].

$\mathbb{G} = \mathbb{G}_m$: This is part of [Zil06, Lemma 2.1] - the following is a reproduction of the proof there.

Let $k' := k \cap \bar{\mathbb{Q}}$. $k \geq k'$ is then a regular extension, so by Proposition 2.1.1(ii) we may assume that $k = k'$.

$k$ is then a number field; let $\mathcal{O}_k$ be its ring of integers. By Dirichlet's Unit theorem, ${\mathcal{O}_k}^\times$ is finitely generated. Recall that $\mathcal{O}_k$ is a Dedekind domain and the fractional ideals, $\mathrm{Id}(\mathcal{O}_k)$, form a free abelian group with generators the prime ideals. $\theta(x) := x\mathcal{O}_k$ provides an exact sequence

$$\begin{tikzcd} {\mathcal{O}_k}^\times \arrow[r, hook] & k^\times \arrow[r, "\theta"] & \mathrm{Id}(\mathcal{O}_k) \end{tikzcd} .$$

It follows from elementary results on free abelian groups that $k^\times$ is free modulo torsion, as required. □

**Theorem 2.2.3.** *Let $k$ be a finitely generated extension of $k_0$. Then ${}^{\mathbb{G}(k(G_\infty))}/_{G_\infty}$ is free.*

*Proof.* This argument uses ideas from the argument in [Lan78, V:5].

**Claim 2.2.3.1.** *Let $n \in \mathbb{N}$. There exists $m$ such that*

$$m \cdot \mathrm{pureHull}_{\mathbb{G}(k(G_\infty))}\left(\mathbb{G}(k(G_n))\right) \leq \mathbb{G}(k(G_n)) + G_\infty. \tag{2.1}$$

*Proof.* By Corollary 2.2.1.1, let $m$ be such that

$$\restriction_{G_\infty}\left(\mathrm{Gal}(k(G_\infty)/k(G_n))\right) \geq \mathrm{Aut}(G_\infty/G_m).$$

We assume, by doubling $m$ if necessary, that $2|m$.

Let $\mu^1 := \Pi_{l|m} G_{l^\infty}$, $\mu^2 := \Pi_{l \nmid m} G_{l^\infty}$, where $l$ ranges over the primes. So $G_\infty \cong \mu^1 \times \mu^2$, and we have a corresponding isomorphism

$$\theta : \mathrm{End}(\mu^1) \times \mathrm{End}(\mu^2) \xrightarrow{\cong} \mathrm{End}(G_\infty) \; .$$

Let $\alpha_1 := m + 1 \in \mathrm{Z}(\mathrm{Aut}(\mu^1))$, let $\alpha_2 := 2 \in \mathrm{Z}(\mathrm{Aut}(\mu^2))$, and let $\alpha := \theta(\alpha_1, \alpha_2)$. Note then that $\alpha \in \mathrm{Z}(\mathrm{Aut}(G_\infty / G_m))$. So say $\tau \in \mathrm{Gal}(k(G_\infty)/k(G_n))$ induces $\alpha$. $\tau$ is central in $\mathrm{Gal}(k(G_\infty)/k(G_n))$ since $\alpha$ is central.

We will use the Kummer pairing

$$\begin{aligned} \langle \cdot, \cdot \rangle : \mathrm{Gal}(k(G_\infty)/k(G_n)) \times \mathrm{pureHull}_{\mathbb{G}(k(G_\infty))} (\mathbb{G}(k(G_n))) \to G_\infty \\ ; (\sigma, Q) \mapsto \sigma(Q) - Q \end{aligned}$$

Let $Q \in \mathrm{pureHull}_{\mathbb{G}(k(G_\infty))} (\mathbb{G}(k(G_n)))$, and let $\sigma \in \mathrm{Gal}(k(G_\infty)/k(G_n))$

$$\begin{aligned} \langle \sigma, \theta(1,m) \langle \tau, Q \rangle \rangle &= \theta(1,m)((\sigma\tau Q - \sigma Q) - (\tau Q - Q)) \\ &= \theta(1,m)(\tau - 1) \langle \sigma, Q \rangle \\ &= \theta(1,m)(\alpha - 1) \langle \sigma, Q \rangle \\ &= \theta(1,m)\theta(m,1) \langle \sigma, Q \rangle \\ &= m \langle \sigma, Q \rangle \\ &= \langle \sigma, mQ \rangle \, . \end{aligned}$$

This holds for any $\sigma$, so $mQ - \theta(1,m) \langle \tau, Q \rangle \in k(G_n)$. But $\langle \tau, Q \rangle \in G_\infty$, so $mQ \in k(G_n) + G_\infty$ as required. □

Now $\mathbb{G}(k(G_\infty)) = \bigcup_n \mathbb{G}(k(G_n))$. For each $n$, $k(G_n)$ is finitely generated over $k_0$, so by Theorem 2.2.2 ${}^{\mathbb{G}(k(G_n))}/_{G_\infty} \leq {}^{\mathbb{G}(k(G_\infty))}/_{G_\infty}$ is free. By the Claim, there exists $m$ depending on $n$ such that the pure hull of ${}^{\mathbb{G}(k(G_n))}/_{G_\infty}$ in ${}^{\mathbb{G}(k(G_\infty))}/_{G_\infty}$ is contained in ${}^1/_m \cdot {}^{\mathbb{G}(k(G_n))}/_{G_\infty}$ and so is free.

${}^{\mathbb{G}(k(G_\infty))}/_{G_\infty}$ is therefore the union of a chain of pure free subgroups, and hence is locally free.

It follows from Pontryagin's Theorem (B.3.1) that ${}^{\mathbb{G}(k(G_\infty))}/_{G_\infty}$ is free. □

## 2.3 Proof of Theorem 2.1.1(ii)

**Theorem** (2.1.1(ii))**.** *Let $k \geq k'$ be a finitely generated regular extension of a field $k' \geq k_0$. Then ${}^{\mathbb{G}(k)}/_{\mathbb{G}(k')}$ is locally free.*

*Proof.* For $\mathbb{G} = \mathbb{E}$, it follows from the function field version of the Mordell-Weil theorem, which is due to Lang-Néron [Lan83, Theorem 6:2], that ${}^{\mathbb{G}(k)}/_{\mathbb{G}(k')}$ is finitely generated, and so certainly locally free. To justify the application of this theorem, note that $\mathbb{E}$ is defined over the constant field $k'$, and any homomorphism over $k$ of elliptic curves over $k'$ is actually over $k \cap \operatorname{acl}(k') = k'$, so the $k/k'$-trace of $\mathbb{E}$ is just $\mathrm{id} : \mathbb{E} \to \mathbb{E}$.

For $\mathbb{G} = \mathbb{G}_m$, we appeal to the theory of normalisation and divisors. The proof is parallel to the proof of Theorem 2.2.2 above. First suppose that $k'$ is algebraically closed. There exists a projective normal variety $X$ such that $k$ is isomorphic over $k'$ to the function field $k'(X)$ [Mum88, III:8 Theorems 3 and 4]. The theory of Weil divisors then applies. To each prime divisor $Y \subseteq X$, we have the valuation $v_Y : k'(X)^\times \to \mathbb{Z}$. For any $f \in k'(X)$, $v_Y(f) = 0$ for all but finitely many $Y$. Let $D$ be the free abelian group generated by the prime divisors, and let $\mathrm{div} : k'(X)^\times \to D; f \mapsto \Sigma_Y v_Y(f) Y$. If $v_Y(f) = 0$ for all $Y$, $f$ is regular on the complete variety $X$ and hence is constant, i.e. $f \in k'^\times$. So we have an exact sequence:

$$\begin{tikzcd} k'^\times \arrow[r, hook] & k'(X)^\times \arrow[r, "\mathrm{div}"] & D . \end{tikzcd}$$

It follows that ${}^{k^\times}/_{k'^\times} \cong {}^{k'(X)^\times}/_{k'^\times}$ is free. This concludes in the case that $k'$ is algebraically closed. For the general case, say $k = k'(\overline{x}) \geq k'$ is a regular extension, and note that the the embedding $k' \leq k'(\overline{x})$ induces an embedding ${}^{k^\times}/_{k'^\times} \leq {}^{k'^{\mathrm{alg}}(\overline{x})^\times}/_{k'^{\mathrm{alg}\times}}$, and the latter is free by the previous argument. In particular, it is locally free as required. □

## 2.4 Proof of Theorem 2.1.1(iii)

**Lemma 2.4.1.** *Let $K \geq L$ be algebraically closed fields, and let $\pi : K \to_L L$ be a place. Let $k_0 \leq K$ be a perfect subfield such that $\pi(k_0) \leq k_0$. Let $k_1 \geq k_0$ be a finite extension.*

*Then there exists a finite extension $k' \geq k_1$, with $k' \leq L(k_1)$, such that $\pi(k') \leq k'$.*

*Proof.* We may assume that $k_1/k_0$ is Galois.

For $i \geq 1$, define $k_{i+1} := k_i \vee \pi k_i$.

Normality of a finite field extension implies [EP05, 3.2.16(2)] normality of the corresponding extension of residue fields; it follows inductively that for all $i \geq 0$, the extensions $k_{i+1}/k_i$ and $\pi k_{i+1}/\pi k_i$ are Galois.

Now $[k_{i+2} : k_{i+1}] \leq [\pi k_{i+1} : \pi k_i] \leq [k_{i+1} : k_i]$. So after some $n$, the degrees reach their minimum level, say

$$d = [\pi k_{n+2} : \pi k_{n+1}] = [k_{n+2} : k_{n+1}] = [\pi k_{n+1} : \pi k_n] = [k_{n+1} : k_n].$$

By the fundamental inequality of valuation theory [EP05, 3.3.4],

(I) any $\sigma \in \mathrm{Gal}(k_{n+1}/k_n)$ preserves $\mathcal{O}_\pi \cap k_{n+1}$;

(II) any $\sigma \in \mathrm{Gal}(k_{n+2}/k_{n+1})$ preserves $\mathcal{O}_\pi \cap k_{n+2}$.

Now $\pi k_{n+1} = (\pi k_n)(\pi\beta)$ say, some $\beta \in k_{n+1}$. Let $\beta = \beta_1, \beta_2, \ldots, \beta_s$ be the $k_n$-conjugates of $\beta$. By (I), $\beta_i \in \mathcal{O}_\pi$ for all $i$. Reducing the minimum polynomial $\Pi_i(x - \beta_i)$, we see that $s = d$ and the $(\pi k_n)$-conjugates of $\pi\beta$ are precisely $(\pi\beta_i)_i$.

Now suppose for a contradiction that $\sigma \in \mathrm{Gal}(k_{n+2}/k_{n+1}) \setminus \{\mathrm{id}\}$. $k_{n+2} = k_{n+1}(\pi\beta)$, so $\sigma(\pi\beta) = \pi\beta_i$ some $i > 1$.

Now $\beta - \pi\beta \in \mathfrak{m}_\pi \cap k_{n+1}$, but $\sigma(\beta - \pi\beta) = \beta - \sigma\pi\beta = \beta - \pi\beta_i \notin \mathfrak{m}_\pi \cap k_{n+1}$. This contradicts (II).

So $d = 1$, and so $\pi k_n \leq k_n$. □

**Lemma 2.4.2.** *Suppose $k$ is a field of characteristic $0$ such that $G_\infty \leq \mathbb{G}(k)$, $L$ is an algebraically closed subfield of $\bar{k}$, $L = \mathrm{acl}(k \cap L)$, and there exists a place $\pi : \bar{k} \to_L L$ such that $\pi(k) \subseteq (k \cap L)$.*

*Then*

*(i) For all $m \in \mathbb{N}$,*

$$m\mathbb{G}(kL) \cap \mathbb{G}(k) = m\mathbb{G}(k) + (\mathbb{G}(k) \cap \mathbb{G}(L)).$$

*(ii)*

$$\mathrm{pureHull}_{\mathbb{G}(kL)}\left(\mathbb{G}(k)\right) = \mathrm{pureHull}_{\mathbb{G}(k)+\mathbb{G}(L)}\left(\mathbb{G}(k)\right).$$

*Proof.* Let $C := k \cap L$.

(i) The $\supseteq$ direction follows from divisibility of $\mathbb{G}(L)$.

For the other direction: let $\alpha \in \mathbb{G}(kL)$ such that $x := m\alpha \in \mathbb{G}(k)$; we show that $x \in m\mathbb{G}(k) + \mathbb{G}(C)$.

Define

$$\begin{array}{rcccc} \langle \cdot, \alpha \rangle & : & \mathrm{Gal}(\bar{k}/k) & \to & G_m \\ & ; & \tau & \mapsto & \tau(\alpha) - \alpha. \end{array}$$

But $L$ is Galois over $C$ and $C = k \cap L$, so we have an exact sequence:

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}(\bar{k}/kL) \arrow[r] & \mathrm{Gal}(\bar{k}/k) \arrow[r, "\restriction_L"] & \mathrm{Gal}(L/C) \arrow[r] & 1 \end{tikzcd};$$

so $\langle \cdot, \alpha \rangle$ induces a well-defined homomorphism

$$\begin{array}{rcccc} \theta & : & \mathrm{Gal}(L/C) & \to & G_m \\ & ; & \sigma & \mapsto & \langle \tau, \alpha \rangle \end{array}$$

where $\tau\restriction_L = \sigma$.

This now becomes a question of Galois cohomology. See Section B.2 for relevant definitions.

**Claim 2.4.2.1.** *$\theta$ is a continuous $L/C$-1-cocycle.*

*Proof.* $\theta$ is a 1-cocycle since $G_\infty \leq \mathbb{G}(k \cap L)$.

Let $\Gamma := \theta^{-1}(0) = \restriction_L (\mathrm{Gal}(\bar{k}/k(\alpha))) = \mathrm{Gal}(L/L \cap k(\alpha))$.

$L \cap k(\alpha) \geq L \cap k = C$ is an algebraic subextension of a finitely generated extension, so is a finite extension. So $\Gamma$ is an open subgroup of $\mathrm{Gal}(L/C)$; it follows that $\theta$ is continuous. □

**Claim 2.4.2.2.** *There exists $\alpha_L \in \mathbb{G}(L)$ such that*

$$\forall \sigma \in \mathrm{Gal}(L/C).\ \theta(\sigma) = \langle \sigma, \alpha_L \rangle := \sigma\alpha_L - \alpha_L.$$

*Proof.*

- $\mathbb{G} = \mathbb{G}_m$: By Hilbert 90, Fact B.2.1, $\theta$ is a $L/C$-1-coboundary; in other words, there exists $\alpha_L \in \mathbb{G}(L)$ as required.
- $\mathbb{G} = \mathbb{E}$: By Fact B.2.2, there exists a $C$-torsor $\mathbb{T}$ such that for any $\beta' \in \mathbb{T}(L)$, $\langle \cdot, \beta' \rangle$ is $L/C$-cohomologous to $\theta$. So say $\alpha' \in \mathbb{E}(L)$ is such that $\langle \cdot, \beta' \rangle + \langle \cdot, \alpha' \rangle = \theta$. Let $\beta := \beta' + \alpha' \in \mathbb{T}(L)$; then $\langle \cdot, \beta \rangle = \theta$.

  Now for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$,

  $$\begin{aligned} \langle \sigma, \beta \rangle &= \langle \sigma\restriction_L, \beta \rangle \\ &= \theta(\sigma\restriction_L) \\ &= \langle \sigma, \alpha \rangle, \end{aligned}$$

  so $\beta - \alpha \in \mathbb{T}(k)$, witnessing $\bar{k}/k$-triviality of $\mathbb{T}$.

  Now $\pi(k) \subseteq k$, so $\gamma := \pi(\beta - \alpha) \in \mathbb{T}(k \cap L) = \mathbb{T}(C)$, witnessing $L/C$-triviality of $\mathbb{T}$.

So $\alpha_L := \beta - \gamma \in \mathbb{G}(L)$ is as required.

□

Now for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$,

$$\begin{aligned} \langle \sigma, \alpha_L \rangle &= \langle \sigma\restriction_L, \alpha_L \rangle \\ &= \theta(\sigma\restriction_L) \\ &= \langle \sigma, \alpha \rangle , \end{aligned}$$

so $\alpha - \alpha_L \in \mathbb{G}(k)$.

$m\alpha_L = m\alpha - m(\alpha - \alpha_L) \in \mathbb{G}(k)$, and so $x = m(\alpha - \alpha_L) + m\alpha_L \in m\mathbb{G}(k) + \mathbb{G}(k) \cap \mathbb{G}(L)$.

(ii) Let $\alpha \in \mathrm{pureHull}_{\mathbb{G}(kL)}(\mathbb{G}(k))$; say $m\alpha \in \mathbb{G}(k)$. By (i), $m\alpha \in m\mathbb{G}(k) + \mathbb{G}(k) \cap \mathbb{G}(L)$; $\mathbb{G}(L)$ is divisible and $G_m \leq \mathbb{G}(L)$, so it follows that $\alpha \in \mathbb{G}(k) + \mathbb{G}(L)$.

□

**Theorem** (2.1.1(iii))**.** *Let $(L_s)_{s\subseteq N}$ be a finitary independent $N$-system of algebraically closed fields, $N \geq 1$.*

*Let $H := \Sigma_i \mathbb{G}(L_{(i)})$.*

*Then for any finitely generated extension $L^-(\overline{\beta}) \geq L^-$,*

$$\mathbb{G}(L^-(\overline{\beta}))/_H$$

*is a locally free abelian group.*

*Proof.* A finitely generated separable field extension decomposes into a finite extension followed by a finitely generated regular extension, so by Theorem 2.1.1(ii) and Lemma B.3.2, we may suppose that $L^-(\overline{\beta}) \geq L^-$ is a finite extension.

We proceed by induction on $N$. The case $N = 1$ is immediate, since a finite extension of an algebraically closed field is trivial. So suppose $N > 1$.

Let $L := L_{(0)}$, and let $P := L_{(1)} \dots L_{(N-1)}$. Let $H' := \Sigma_{i>0}\mathbb{G}(L_{(i)})$, so $H = H' + \mathbb{G}(L)$.

We proceed to show that ${}^{\mathbb{G}(L^-(\overline{\beta}))}/_{H}$ is locally free. So let $\overline{b} \in \mathbb{G}(L^-(\overline{\beta}))^{<\omega}$; we have to show that

$$\mathrm{pureHull}_{\mathbb{G}(L^-(\overline{\beta}))/_H}\left(\left\langle {}^{\overline{b}}/_{H} \right\rangle\right)$$

is free.

Let $\overline{\lambda}$ be a transcendence basis for $L$ over $L_{\emptyset}$.

By Lemma 1.3.3, there exists a place $\pi : L_N \to_L L$ such that $\pi(P(\overline{\lambda})) \subseteq (P \cap L)(\overline{\lambda})$, and $\pi(\overline{\beta}, \overline{b}) \subseteq \mathbb{G}^n(L)$.

By Lemma 2.4.1, there exists a finite extension $k$ of $P(\overline{\lambda})(\overline{\beta}, \overline{b})$ such that $\pi(k) \subseteq k$ and $kL = L^-(\overline{\beta})$.

$k$ is a finitely generated extension of $P$, so it follows from the induction hypothesis that ${}^{\mathbb{G}(k)}/_{H'}$ is locally free.

Now

$$ {}^{\mathrm{pureHull}_{\mathbb{G}(k)+\mathbb{G}(L)}(\langle \overline{b} \rangle)}/_{H} \leq {}^{\mathrm{pureHull}_{\mathbb{G}(k)}(\langle \overline{b}, \pi(\overline{b}) \rangle)}/_{H}.$$

Indeed, suppose $\alpha \in \mathbb{G}(k) + \mathbb{G}(L)$, say $\alpha = \alpha_k + \alpha_L$, and $m\alpha \in \langle \overline{b} \rangle$. If $\mathbb{G} = E$, $\pi$ is total, and so we have immediately that $\alpha - \pi(\alpha) = \alpha_k - \pi(\alpha_k) \in \mathbb{G}(k)$. If $\mathbb{G} = \mathbb{G}_m$, we have to watch for finiteness - but indeed, $\pi(m\alpha)$ and hence $\pi(\alpha)$ are in $\mathbb{G}_m$, and so $\pi(\alpha_k) = \pi(\alpha - \alpha_L) = \pi(\alpha) - \alpha_L \in \mathbb{G}_m(k)$, and so again $\alpha - \pi(\alpha) = \alpha_k - \pi(\alpha_k) \in \mathbb{G}_m(k)$.

We use below the easy fact that for $C \leq B$ abelian groups and a divisible subgroup $A \leq B$ containing the torsion subgroup of $B$, ${}^{\mathrm{pureHull}_B(C)}/_{A} = \mathrm{pureHull}_{B/_A}\left({}^{C}/_{A}\right)$.

Now by Lemma 2.4.2(ii):

$$\begin{aligned}
\operatorname{pureHull}_{{}^{\mathbb{G}(L^{-}(\overline{\beta}))}/_{H}}\left(\left\langle {}^{\overline{b}}/_{H} \right\rangle\right) &= {}^{\operatorname{pureHull}_{\mathbb{G}(L^{-}(\overline{\beta}))}(\langle \overline{b} \rangle)}/_{H} \\
&= {}^{\operatorname{pureHull}_{\mathbb{G}(k)+\mathbb{G}(L)}(\langle \overline{b} \rangle)}/_{H} \\
&\leq {}^{\operatorname{pureHull}_{\mathbb{G}(k)}(\langle \overline{b}, \pi(\overline{b}) \rangle)}/_{H} \\
&= {}^{F}/_{\mathbb{G}(L)},
\end{aligned}$$

where

$$F := {}^{\operatorname{pureHull}_{\mathbb{G}(k)}(\langle \overline{b}, \pi(\overline{b}) \rangle)}/_{H'},$$

which is finitely generated by local freeness of ${}^{\mathbb{G}(k)}/_{H'}$.

So $\operatorname{pureHull}_{{}^{\mathbb{G}(L^{-}(\overline{\beta}))}/_{H}}\left(\left\langle {}^{\overline{b}}/_{H} \right\rangle\right)$ is a subgroup of a quotient of a finitely generated group, and so is finitely generated, and in particular is free as required.

□

*Question* 2.4.1. For $N = 1$, and $\mathbb{G} = \mathbb{E}$, ${}^{\mathbb{G}(L^{-}(\overline{\beta}))}/_{H}$ is not just locally free but actually finitely generated - this is part of the Lang-Néron theorem, as in the proof of Theorem 2.1.1(ii) above. Local freeness is all we require for the application in Chapter 4, but it is natural to ask: is ${}^{\mathbb{G}(L^{-}(\overline{\beta}))}/_{H}$ finitely generated for $N > 1$? It seems that a more subtle analysis than the one we have given would be required to answer this question.

For the multiplicative group, ${}^{\mathbb{G}(L^{-}(\overline{\beta}))}/_{H}$ certainly won't be finitely generated in general. But in the $N = 1$ case, it is free rather than merely locally free. Again, it is natural to ask whether this holds for $N > 1$.

# Chapter 3

# Kummer theory

## 3.1 Canonical bases in algebraically closed fields

All fields mentioned in this section are considered as subfields of a fixed algebraically closed field $\mathcal{C}$ of characteristic $p$, which may be 0. We need not make the common assumption that the fields be "small" relative to $\mathcal{C}$. We make occasional use of model theoretic terminology, for the sake of neatness; we are referring then to the theory of $\mathcal{C}$, i.e. $ACF_p$.

**Definition 3.1.1.** Let $F$ be a perfect field, and let $F(\overline{a})$ be a finitely generated extension.

$\mathrm{Aut}^{\overline{a}}(F)$ is the group of field automorphisms of $F$ which are consistent with fixing $\overline{a}$, i.e.

$$\mathrm{Aut}^{\overline{a}}(F) := \{\sigma \in \mathrm{Aut}(F) | \exists \tau \in \mathrm{Aut}(F(\overline{a})/\overline{a}).\ \sigma = \tau\restriction_F\}.$$

The *locus* of $\overline{a}$ over $F$ is the intersection $\mathrm{locus}(\overline{a}/F)$ of all $F$-closed subsets of $\mathbb{A}^n$ containing $\overline{a}$.

By the DCC for the $F$-Zariski topology, $\mathrm{locus}(\overline{a}/F)$ is itself $F$-closed.

Define the *canonical base* of (the type of) $\overline{a}$ over $F$, $\mathrm{Cb}(\overline{a}/F) \leq F$, to be the perfect closure of the minimal field of definition of $\mathrm{locus}(\overline{a}/F)$.

*Remark* 3.1.1. (i) $\mathrm{Cb}(\overline{a}/F)$ is therefore the perfect closure of a finitely generated extension of the prime field - see [Lan72, Theorem III.7] and the subsequent discussion, or (iii) of this remark.

(ii) The above definition makes sense in particular when $\overline{a} \in \mathrm{acl}(F)$, in which case $V$ is finite.

(iii) In model-theoretic terms, $\mathrm{tp}(\overline{a}/F)$ is not necessarily stationary. So $\mathrm{Cb}(\overline{a}/F)$ is the canonical base in the sense of [Pil96, 7.1.16] (which is denoted there by $\mathrm{Cb}_1$). It is precisely the definable closure of a canonical parameter for $\mathrm{locus}(\overline{a}/F)$.

**Lemma 3.1.1.** *Let $F \leq \mathcal{C}$ be a perfect field, let $\overline{a} \in \mathcal{C}^{<\omega}$ be a tuple. Let $V := \mathrm{locus}(\overline{a}/F)$.*

*Let $\sigma : F \to F$ be partial elementary. Then the following are equivalent:*

*(i) $\sigma$ fixes $\mathrm{Cb}(\overline{a}/F)$;*

*(ii) $V = V^\sigma$;*

*(iii) $\sigma(\mathrm{tp}(\overline{a}/F)) = \mathrm{tp}(\overline{a}/F)$ (where $\sigma$ acts formula-by-formula on the type);*

*(iv) $\sigma$ extends to a partial elementary map $\sigma : F(\overline{a}) \to F(\overline{a})$ fixing $\overline{a}$.*

*Therefore*

$$\mathrm{Aut}^{\overline{a}}(F) = \mathrm{Aut}(F/\,\mathrm{Cb}(\overline{a}/F)).$$

*Proof.* *(i)* $\iff$ *(ii)* By definitions.

*(ii)* $\implies$ *(iii)* We have $V = V^\sigma$. By quantifier elimination, it suffices to show that if $W \subseteq \mathbb{A}^{n+m}$ is a $\emptyset$-definable closed subset and $(\overline{a}, \overline{f}) \in W$, then $(\overline{a}, \sigma(\overline{f})) \in W$. But indeed, $(\overline{a}, \overline{f}) \in W$ iff $V \subseteq W(\overline{f})$ iff $V^\sigma \subseteq W(\overline{f})^\sigma$ iff $V \subseteq W(\sigma(\overline{f}))$ iff $(\overline{a}, \sigma(\overline{f})) \in W$.

*(iii)* $\implies$ *(ii)* $\overline{a} \in V^\sigma$, so $V \subseteq V^\sigma$; similarly, $V^\sigma \subseteq V$.

*(iii)* $\iff$ *(iv)* By definitions.

□

We apply these ideas to prove in the following Proposition that a tuple over $L^-$ of an independent system is essentially based in a number field; the proof is a matter of cascading finite bases down through the system to $\bar{\mathbb{Q}}$.

**Proposition 3.1.2.** *Let $N \geq 0$, and let $(L_s)_{s \subseteq N}$ be a finitary independent $N$-system of characteristic $0$ algebraically closed fields. Let $C_0 := L^-$ if $N \geq 1$; let $C_0 := k_0(G_\infty)$ if $N = 0$.*

*Let $\overline{a} \in \mathcal{C}^{<\omega}$, and define $k := C_0(\overline{a})$. Then there exists a number field $F$ such that any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/F)$ extends to some $\sigma' \in \mathrm{Aut}(\bar{k}/\overline{a})$ which restricts to an automorphism of $k$.*

*Proof.* If $N = 0$, we are done by setting $F := k_0(\mathrm{Cb}(\overline{a}/C_0))$.

Now suppose $N \geq 1$.

Let $\overline{b}_i \in L_{(i)}^{<\omega}$ be such that $\mathrm{Cb}(\overline{a}/C_0) = \mathrm{dcl}(\bigcup_i \overline{b}_i)$.

Suppose that we have defined $\overline{b}_t \in L_t^{<\omega}$ for all $t$ s.t. $|t| = n$. For each such $t$, let $S^t := \{s < t||s| = n-1\}$, and let $\overline{b}_s^t \in L_s^{<\omega}$ for $s \in S^t$ be such that $\mathrm{Cb}(\overline{b}_t / \bigvee_{s \in S^t}(L_s) = \mathrm{dcl}(\bigcup_{s \in S^t}(\overline{b}_s^t))$. Let $\overline{b}_s := \bigcup_{\{t \supset s \,:\, |t|=n\}}(\overline{b}_s^t)$.

Let $F := \mathrm{Cb}(\overline{b}_\emptyset/\bar{\mathbb{Q}})$.

Let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/F)$. Then by Lemma 3.1.1, $\sigma$ extends to $L_\emptyset$ fixing $\overline{b}_\emptyset$.

Suppose by induction that we have extended $\sigma$ to agreeing partial elementary maps $\sigma_s : L_s \to L_s$ for $|s| \leq n-1$ with $\sigma_s$ fixing $\overline{b}_s$.

Let $t \subseteq N$ such that $|t| = n$. Let $\sigma_t' := \bigcup_{s \in S^t}(\sigma_s)$, which is partial elementary by Lemma 1.3.4 applied to the independent system $(L_s|s \leq t)$. $\sigma_t'$ fixes $\overline{b}_s^t$ for all $s \in S^t$, so extends to $\sigma_t : L_t \to L_t$ fixing $\overline{b}_t$.

At stage $N-1$ we obtain partial elementary $\sigma_N' := \bigvee_i \sigma_{(i)} : C_0 \to C_0$ fixing $\bigcup_i \overline{b}_i$, which then extends to $\sigma' \in \mathrm{Aut}(C_0(\overline{a})/\overline{a})$. □

## 3.2 Bashmakov's theorem over independent systems

**Theorem 3.2.1.** *Let $N \geq 0$ and let $(L_s)_{s \subseteq N}$ be a finitary independent system of algebraically closed subfields of $\mathcal{C}$. Let $H := \Sigma_{i \in N} \mathbb{G}(L_{(i)})$ if $N > 0$; let $H := G_\infty$ if $N = 0$.*

*Let $\overline{a} \in \mathbb{G}(\mathcal{C})^n$ let $k := k_0(H, \overline{a})$, and suppose $\overline{a}$ is simple in $\mathbb{G}(k)$.*

*Then the left image of the $\bar{k}/k$-Kummer-Tate pairing,*

$$Z := \left\langle \mathrm{Gal}(\bar{k}/k), \overline{a} \right\rangle_\infty^{\bar{k}/k} \leq T^n,$$

*is of finite index in $T^n$.*

If $\mathbb{G} = \mathbb{G}_m$, Theorem 3.2.1 holds by classical Kummer theory, even without the assumptions on $k$.

So suppose $\mathbb{G} = \mathbb{E}$.

The number field case of Theorem 3.2.1, i.e. the case $N = 0$ and $\overline{a} \in \mathbb{G}(\bar{\mathbb{Q}})^n$, is a result due to Bashmakov which makes essential use of Serre's theorem B.1.1 on the image of the absolute automorphism group of a number field on the automorphism groups of the Tate modules. For the general case, we first apply Proposition 3.1.2 to show that the situation is "finitely based", providing a number field to which Serre's theorem will apply:

**Lemma 3.2.2.** *There exists a number field $k_1 \geq k_0$ such that $Z$ is $\mathrm{Aut}(\bar{\mathbb{Q}}/k_1)$-invariant.*

*Proof.* Let $F$ be as in Lemma 3.1.2, and let $k_1 := k_0(F)$. Let $\sigma \in \mathrm{Gal}(\bar{k}/k)$, and let $\tau \in \mathrm{Aut}(\bar{\mathbb{Q}}/k_1)$.

By choice of $F$, $\tau$ extends to $\tau' \in \mathrm{Aut}(\bar{k}/k_0(\overline{a}))$ such that $\tau'$ restricts to an automorphism of $k$. So $\sigma^{\tau'^{-1}} = \tau'\sigma\tau'^{-1} \in \mathrm{Gal}(\bar{k}/k)$, and

$$\begin{aligned}
\left\langle \sigma^{\tau'}, \overline{a} \right\rangle_{\infty}^{\bar{k}/k} &= \tau'\sigma\tau'^{-1}\overline{\alpha} - \overline{\alpha} && \text{(some arbitrary } \overline{\alpha} \in \hat{\pi}^{-1}(\overline{a})) \\
&= \tau'(\sigma\tau'^{-1}\overline{\alpha} - \tau'^{-1}\overline{\alpha}) \\
&= \tau' \left\langle \sigma, \overline{a} \right\rangle_{\infty}^{\bar{k}/k} && \text{(since } \tau'^{-1}\overline{\alpha} \in \hat{\pi}^{-1}(\overline{a})) \\
&= \tau \left\langle \sigma, \overline{a} \right\rangle_{\infty}^{\bar{k}/k} .
\end{aligned}$$

□

Theorem 3.2.1 follows by the arguments used in the proof of Bashmakov's theorem with Lemma 3.2.2 allowing the use of Serre's theorem. For completeness, and because the specificity of our situation simplifies some of the arguments, we give this proof below, adapting the proof presented in [Lan78] and hopefully not introducing too many errors.

For $l$ a prime and $s \in \mathbb{N}$, define $\mathrm{Aut}(T_l/E_{l^s})$ to be the kernel of the natural reduction map $\mathrm{Aut}(T_l) \to \mathrm{Aut}(E_{l^s})$.

For $s \in \mathbb{N}$ and $l$ a prime, let $Z_s$ resp. $Z_{l^\infty}$ be the projections of $Z$ to $E_s^n$ resp. $T_l^n$. Note that $Z_{l^\infty}$ is a closed subgroup and hence a $\mathbb{Z}_l$-submodule of $T_l^n$.

**Fact 3.2.3.** *1. If $s$ and $t$ are coprime, then $\mathrm{Aut}(E_{st}) = \mathrm{Aut}(E_s) \times \mathrm{Aut}(E_t)$. If further $s'|s$ and $t'|t$, then $\mathrm{Aut}(E_{st}/E_{s't'}) = \mathrm{Aut}(E_s/E_{s'}) \times \mathrm{Aut}(E_t/E_{t'})$.*

*2. For $l$ prime and $t' \geq t \geq s \in \mathbb{N}$, the restriction map $\restriction_{E_{l^t}} \colon \mathrm{Aut}(E_{l^{t'}}/E_{l^s}) \to \mathrm{Aut}(E_{l^t}/E_{l^s})$ is surjective.*

*3. So for $t, s \in \mathbb{N}$, $\restriction_{E_t} \colon \mathrm{Aut}(E_\infty/E_s) \to \mathrm{Aut}(E_t/E_t \cap E_s)$ is surjective.*

So by Lemma 3.2.2 and Fact B.1.1, for all but finitely many primes $l$, $Z_l$ is invariant under $\mathrm{Aut}(E_l) \cong \mathrm{GL}_2({}^{\mathbb{Z}}/_{l\mathbb{Z}})$, and for the remaining finitely many primes $l$ there is $s = s_l \in \mathbb{N}$ such that $Z_{l^\infty}$ is $\mathrm{Aut}(T_l/E_{l^s})$-invariant.

**Fact 3.2.4.** *Let $l$ be a prime.*

*1. The only endomorphisms of $E_l$ which are $\mathrm{Aut}(E_l)$-invariant are the scalars; i.e. $\mathrm{End}_{\mathrm{Aut}(E_l)}(E_l) \cong {}^{\mathbb{Z}}/_{l\mathbb{Z}}$*

2. *for any* $s \in \mathbb{N}$, $\mathrm{End}_{\mathrm{Aut}(T_l/E_{l^s})}(T_l) \cong \mathbb{Z}_l$.

3. *If* $N$ *is a closed subgroup of* $T_l^n$ *such that* $\pi_l(N) = E_l^n$, *then* $N = T_l^n$.

**Lemma 3.2.5.** *Let* $S$ *be a simple* $R$*-module. Then the submodules of* $S^n$ *are precisely those of the form*

$$\{\overline{x} | \bigwedge_i \Sigma_j \eta_{i,j} x_i = 0\},$$

*where* $\eta_{i,j} \in \mathrm{End}_R(S)$.

*Proof.* We show by induction that such a submodule $N \leq S^n$ is the graph of an $R$-linear map $\eta : S^d \to S^{n-d}$ from some $d$ of the co-ordinates to the rest - since such a map is easily given by a matrix with entries from $\mathrm{End}_R(S)$, the lemma follows.

This is clear for $n = 1$. Suppose it holds for $n$, let $N \leq S^{n+1}$ be a sub-$R$-module. Let $\pi : N \to S^n$ be the projection map. By induction, $\mathrm{im}(\pi)$ is the graph of an $R$-linear map $\eta$. If $\ker(\pi) = S$, $\eta$ provides the map $S^{d+1} \to S^{n-d}$. Else, by simplicity $\ker(\pi) = \{0\}$, and so $N$ is the graph of an $R$-module homomorphism $\eta' : \mathrm{im}(\pi) \to S$. So $N$ is the graph of $\theta : S^d \to S^{n-d+1}; x \mapsto (\eta x, \eta'(x, \eta x))$. □

*Proof of Theorem 3.2.1.*

Step I Let $l$ be one of the all but finitely many primes such that $Z_l$ is $\mathrm{Aut}(E_l)$-invariant. Suppose that $Z_l \neq E_l^n$.

$E_l$ is simple as a $\mathbb{Z}[\mathrm{Aut}(E_l)]$-module, so by Fact 3.2.4(i) and the Lemma 3.2.5, for some $n_i \in {}^{\mathbb{Z}}/_{l\mathbb{Z}} \cong \mathrm{End}_{\mathrm{Aut}(E_l)}(E_l)$ not all zero,

$$\forall \overline{\zeta} \in Z_l. \ \Sigma n_i \zeta_i = 0.$$

But then if $l\beta_i = a_i$, $\beta := \Sigma n_i \beta_i$ is fixed by all $\sigma \in \mathrm{Gal}(\bar{k}/k)$:

$$\sigma(\beta) - \beta = \Sigma n_i(\sigma(\beta_i) - \beta_i) = 0,$$

since $\sigma(\beta_i) - \beta_i \in Z_l$. So $\beta \in \mathbb{G}(k) \setminus \langle \overline{a} \rangle$, contradicting simplicity of $\overline{a}$.

So $Z_l = E_l^n$, so by Fact 3.2.4(iii)

$$Z_{l^\infty} = T_l^n.$$

Step II Now let $l$ be one of the finitely many remaining primes for which we only have that $Z_{l^\infty}$ is $\mathrm{Aut}(T_l/E_{l^s})$-invariant for some $s$.

Define the divisible hulls $X_l := Z_{l^\infty} \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and $V_l := T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Note that $X_l$ is an $R := \mathbb{Q}_l[\mathrm{Aut}(T_l/E_{l^s})]$-submodule of $V_l^n$.

$V_l$ is simple as an $R$-module and (by Fact 3.2.4(ii)) $End_R(V_l) = \mathbb{Q}_l$.

So again, if $X_l \neq V_l^n$ then $X_l$ is contained in a proper subgroup of form $\{\Sigma n_i x_i = 0\}$, $n_i \in \mathbb{Q}_l$ not all 0. Clearing denominators, we may suppose $n_i \in \mathbb{Z}_l$; say not all $n_i$ are 0 mod $l^t$ - then letting $n_i' := \pi_{l^t}(n_i) \in {}^{\mathbb{Z}}/_{l^t\mathbb{Z}}$ we see that

$$\forall \overline{\zeta} \in Z_{l^s}.\ \Sigma n_i' \zeta_i = 0,$$

which contradicts simplicity as above.

So $X_l = V_l^n$, and so $Z_{l^\infty}$ is of finite index in $T_l^n$.

Step III We have shown that $Z_{l^\infty}$ is equal to $T_l^n$ for all but finitely many primes, and is of finite index in $T_l^n$ for the others. Since the corresponding extensions are of coprime order and hence disjoint, we see that $Z = \Pi_l Z_{l^\infty} \leq \Pi_l T_l^n = T^n$. So $Z$ is of finite index in $T^n$, as required.

□

# Chapter 4

# Categoricity results

In this chapter, we give purely algebraic statements and proofs of the main categoricity results, as discussed in Section 1.1, and draw as corollaries the model theoretic statements outlined in Section 0.1. The proofs here are in essence stripped down versions of those in the theory of Quasi-Minimal Excellence [Zil05b].

## 4.1 Orbits of standard $V \leq \hat{V}$

Let $K$ be an algebraically closed extension of $k_0$.

**Definition 4.1.1.** A divisible subgroup $V \leq \hat{V}(K)$ is *standard* iff

- $\hat{\pi}(V) = \mathbb{G}(K)$
- $V \cap T$ is isomorphic as an abelian group to $\mathbb{Z}^d$, where $d = 1$ if $\mathbb{G} = \mathbb{G}_m$ and $d = 2$ if $\mathbb{G} = \mathbb{E}$.

The automorphism group $\mathrm{Aut}(K/k_0)$ acts on the set of standard $V \leq \hat{V}$; Theorem 4.1.1 below, which is in effect the main theorem of this Part, analyses the orbits of this action.

We say that standard $V_1, V_2 \leq \hat{V}(K)$ are $\mathrm{Aut}(K/k_0)$-*conjugate* iff there exists $\sigma \in \mathrm{Aut}(K/k_0)$ such that $V_2 = \sigma(V_1)$.

Assumptions are as in Section 1.2; in particular, note that we are assuming no complex multiplication and that $k_0$ is a number field.

We now give the full statement of our main theorem describing the orbits, although the second part of the statement uses definitions made in Section 4.3 below.

**Theorem 4.1.1.** *The action of* $\operatorname{Aut}(K/k_0)$ *on the set of standard* $V \leq \hat{V}$ *is transitive if* $\mathbb{G} = \mathbb{G}_m$*, and has finitely many orbits if* $\mathbb{G} = \mathbb{E}$*.*

*Moreover, in the latter case the orbit is determined by the algebraic type over* $k_0$ *of* ${}^{w_m(\Lambda)}/_{\pm}$*, for* $m$ *such that* $\upharpoonright_{E_\infty} \colon \operatorname{Gal}(\bar{\mathbb{Q}}/k_0) \twoheadrightarrow \operatorname{Aut}(E_\infty/E_m)$ *.*

The proof of Theorem 4.1.1 proceeds in two steps. First, in Theorem 4.2.3, we prove that standard $V \leq \hat{V}$ which coincide on $T$ are conjugate. This reduces the problem to that of analysing the orbits on $T$; Theorem 4.3.2 then characterises these orbits.

## 4.2 Categoricity over $T$

We deduce from Theorem 3.2.1 and Theorem 2.1.1 the following key lemma:

**Lemma 4.2.1.** *Let* $N \geq 0$ *and let* $(L_s)_{s \subseteq N}$ *be a finitary independent system of countable algebraically closed subfields of* $\mathcal{C}$*. Let* $H := \Sigma_{i \in N} \mathbb{G}(L_{(i)})$ *if* $N > 0$*; let* $H := G_\infty$ *if* $N = 0$*.*

*Let* $\overline{a} \in \mathbb{G}(\mathcal{C})^n$ *be linearly independent over* $H$*, let* $k$ *be a finitely generated extension of* $k_0(H, \overline{a})$*.*

*Let* $Z$ *be the left image of the* $\bar{k}/k$*-Kummer-Tate pairing,*

$$Z := \left\langle \operatorname{Gal}(\bar{k}/k), \overline{a} \right\rangle_\infty^{\bar{k}/k} \leq T^n.$$

*Then*

*(i)* $Z$ *is of finite index in* $T^n$*.*

*(ii) If $V \leq \hat{V}$ is standard, $\Lambda := V \cap T$, then*

$$Z + \Lambda^n = T^n.$$

*(iii) There exists $m \in \mathbb{N}$ such that if $\overline{a}'$ is an $m$-division point of $\overline{a}$, then for all $n \in \mathbb{N}$ all $n$-division points of $\overline{a}'$ are* $\mathrm{Gal}(\bar{k}/k(\overline{a}'))$*-conjugate.*

*Proof.* (i) $\overline{a}$ is linearly independent over $H$, and $G_\infty \leq H \leq \mathbb{G}(k)$. So the quotient map restricts to an isomorphism:

$$\mathrm{pureHull}_{\mathbb{G}(k)/_{G_\infty}}\left(\left\langle {}^{\overline{a}}/_{G_\infty}\right\rangle\right) \to \mathrm{pureHull}_{\mathbb{G}(k)/_{H}}\left(\left\langle {}^{\overline{a}}/_{H}\right\rangle\right)$$
$$ {}^{\Sigma_i q_i a_i}/_{G_\infty} \mapsto {}^{\Sigma_i q_i a_i}/_{H}$$

By Theorem 2.1.1, ${}^{\mathbb{G}(k)}/_{H}$ is locally free. So say $\overline{a}' \in \mathbb{G}(k)^n$ is such that ${}^{\overline{a}'}/_{G_\infty}$ is a basis for $\mathrm{pureHull}_{\mathbb{G}(k)/_{G_\infty}}\left(\left\langle {}^{\overline{a}}/_{G_\infty}\right\rangle\right)$. $\overline{a} = A\overline{a}' + \overline{z}$ for some integral matrix $A \in \mathrm{Mat}_{n,n}(\mathbb{Z})$ and some $\overline{z} \in G_\infty^n$, and $A$ is invertible as a rational matrix.

Now $\langle \cdot, \cdot \rangle_\infty^{\bar{k}/k}$ is linear on the right, and $G_\infty \subseteq \mathbb{G}(k)$, so

$$\left\langle \mathrm{Gal}(\bar{k}/k), \overline{a}\right\rangle_\infty^{\bar{k}/k} = A \left\langle \mathrm{Gal}(\bar{k}/k), \overline{a}'\right\rangle_\infty^{\bar{k}/k}.$$

Now $\overline{a}'$ is simple in $\mathbb{G}(k)$, so by Theorem 3.2.1, the latter is of finite index in $T^n$. $A$ has Smith normal form $PBQ$ with $P$ and $Q$ invertible integer matrices and $B$ diagonal with no entry 0, so

$$\left\langle \mathrm{Gal}(\bar{k}/k), \overline{a}\right\rangle_\infty^{\bar{k}/k} = PBQ \left\langle \mathrm{Gal}(\bar{k}/k), \overline{a}'\right\rangle_\infty^{\bar{k}/k} = B \left\langle \mathrm{Gal}(\bar{k}/k), \overline{a}'\right\rangle_\infty^{\bar{k}/k},$$

which is of finite index in $T^n$.

(ii) $Z$ is a finite index closed subgroup of $T^n$, so contains $mT^n$ for some $m \in \mathbb{N}$. Define

$$\theta : T \to G_m; \zeta \mapsto \hat{\pi}\left(\frac{\zeta}{m}\right).$$

$\ker\theta = mT$, so it suffices to show that $\theta(\Lambda) = E_m$; but indeed, this follows from surjectivity of $\hat{\pi}\restriction_V$.

(iii) Again, let $m$ be such that $mT^n \leq Z$. The result is then immediate from definitions.

□

*Remark* 4.2.1. Versions of Lemma 4.2.1(iii) have occured in the literature, sometimes under the name of "the Thumbtack Lemma" (e.g. [Bal04]). In particular, it appears in [Zil06] and [BZ07] for the case of $\mathbb{G} = \mathbb{G}_m$.

**Definition 4.2.1.** For $V \leq \hat{V}(\mathcal{C})$ standard and $D \leq \mathbb{G}(\mathcal{C})$ divisible, define $V\restriction_D := V \cap \hat{\pi}^{-1}(D)$.

**Lemma 4.2.2.** *Let $H$ be as in the statement of Lemma 4.2.1.*

*Let $D \leq \mathbb{G}(\mathcal{C})$ be a divisible extension of $H$ such that ${}^{D}/_{H}$ is of finite rank.*

*Let $V_1, V_2 \leq \hat{V}(\mathcal{C})$ be standard.*

*Suppose $\sigma \in \mathrm{Aut}(\mathcal{C}/H)$ and*

$$\sigma(V_1\restriction_D) = V_2\restriction_D .$$

*Let $D' := \mathbb{G}(\mathrm{acl}(k_0(D)))$.*

*Then there exists $\sigma' \in \mathrm{Aut}(\mathcal{C}/H)$ such that $\sigma'\restriction_D = \sigma\restriction_D$ and*

$$\sigma'(V_1\restriction_{D'}) = V_2\restriction_{D'} .$$

*Proof.* Say $D = \mathrm{pureHull}_{\mathbb{G}(\mathcal{C})}\left(\langle H\overline{d}\rangle\right)$ with $\overline{d}$ linearly independent over $H$.

${}^{D'}/_{H}$ is of countable $\mathbb{Q}$-linear dimension, so by back-and-forth it suffices to show that if $d \in D' \setminus D$ and $D_1 := \mathrm{pureHull}_{\mathbb{G}(\mathcal{C})}\left(\langle H\overline{d}d\rangle\right)$, then there exists $\sigma_1 \in \mathrm{Aut}(\mathcal{C}/H)$ such that $\sigma_1\restriction_D = \sigma\restriction_D$ and $\sigma_1(V_1\restriction_{D_1}) = V_2\restriction_{D_1})$.

Let $\overline{d}' := \overline{d}d$. Let $\overline{\alpha}'_1 = \overline{\alpha}_1\alpha_1 \in \hat{\pi}^{-1}(\overline{d}d) \cap V_1^{n+1}$, and let $\overline{\alpha}'_2 = \overline{\alpha}_2\alpha_2 \in \hat{\pi}^{-1}(\sigma(\overline{d}d)) \cap V_2^{n+1}$ where $\overline{\alpha}_2 = \sigma\overline{\alpha}_1 \in V_2^n$.

Now $\alpha_2 = \sigma\alpha_1 + \zeta$ for some $\zeta \in T$. Let $\Lambda := V_1 \cap T = V_2 \cap T$. By Lemma 4.2.1 with $k := k_0(H, \overline{d}')$,

$$\left\langle \mathrm{Gal}(\bar{k}/k), \overline{d}' \right\rangle_{\infty}^{\bar{k}/k} + \Lambda^{n+1} = T^{n+1}.$$

In particular, looking at the last variable, we have

$$\left\langle \mathrm{Gal}(\bar{k}/k), \overline{d}' \right\rangle_{\infty}^{\bar{k}/k} \cap \{\overline{0}\} \times T + \{\overline{0}\} \times \Lambda = \{\overline{0}\} \times T.$$

So say $\tau \in \mathrm{Gal}(\bar{k}/k)$ and $\lambda \in \Lambda$ are such that $\tau(\overline{\alpha}_1) = \overline{\alpha}_1$ and

$$\zeta = (\tau\alpha_1 - \alpha_1) + \lambda = \tau(\alpha_1 + \lambda) - \alpha_1.$$

So let $\sigma_1 := \sigma \circ \tau$;

$$\sigma_1(\overline{\alpha}_1(\alpha_1 + \lambda)) = \overline{\alpha}_2(\sigma\alpha_1 + \zeta) = \overline{\alpha}_2\alpha_2,$$

so $\sigma_1$ is as required. □

**Theorem 4.2.3.** *Let $K$ be an algebraically closed field extending $k_0$. Let $V_1, V_2 \leq \hat{V} := \hat{V}(K)$ be standard. Suppose $V_1 \cap T = V_2 \cap T$.*

*Then there exists $\sigma \in \mathrm{Aut}(K/k_0(G_\infty))$ such that $\sigma(V_1) = V_2$.*

*Proof.* By Lemma 4.2.2 with $D := H := G_\infty$, there exists $\sigma_{-1} \in \mathrm{Gal}(\bar{\mathbb{Q}}/k_0(G_\infty))$ such that $\sigma_{-1}(V_1\restriction_{\mathbb{G}(\bar{\mathbb{Q}})}) = V_2\restriction_{\mathbb{G}(\bar{\mathbb{Q}})}$.

So we may assume that $V_1\restriction_{\mathbb{G}(\bar{\mathbb{Q}})} = V_2\restriction_{\mathbb{G}(\bar{\mathbb{Q}})}$.

Let $(\lambda_i)_{i \in I}$ be a transcendence basis of $K$. For $s \subseteq I$, let $L_s := \mathrm{acl}^K(\{\lambda_i | i \in s\})$. We define, by structural induction on the partial order of finite subsets of $I$, an agreeing system of automorphisms $\sigma_s \in \mathrm{Aut}(L_s/\bar{\mathbb{Q}})$ for $s \subset_{\mathrm{fin}} I$.

Let $\sigma_\emptyset := \mathrm{id}_{\bar{\mathbb{Q}}}$.

Next, suppose $s$ is a singleton, $s = \{i\}$. Let $a \in \mathbb{G}(L_s) \setminus \mathbb{G}(\bar{\mathbb{Q}})$. Choose arbitrarily $\alpha_j \in V_j \cap \hat{\pi}^{-1}(a)$. $\mathbb{G}$ is an absolutely irreducible curve, so, for all $n$, $\hat{\pi}({}^{\alpha_1}/_{n}) \equiv_{\bar{\mathbb{Q}}} \hat{\pi}({}^{\alpha_2}/_{n})$; therefore $\tau(\alpha_1) = \alpha_2$ for some $\tau \in \mathrm{Aut}(L_s/\bar{\mathbb{Q}})$. By Lemma

4.2.2 with $H := \mathbb{G}(\bar{\mathbb{Q}})$ and $D := \langle Ha \rangle_{\mathbb{Q}}$, $\tau$ extends to $\sigma_s \in \mathrm{Aut}(L_s/\bar{\mathbb{Q}})$ such that $\sigma_s(V_1{\restriction}_{L_s}) = V_2{\restriction}_{L_s}$.

Now suppose $|s| \geq 2$, and suppose inductively that we have defined for each $t \subsetneq s$ an automorphism $\sigma_t \in \mathrm{Aut}(L_t/\bar{\mathbb{Q}})$, such that

$$\forall t \subsetneq s.\ \sigma_t(V_1{\restriction}_{L_t}) = V_2{\restriction}_{L_t}$$

and

$$\forall t, t' \subsetneq s.\ (t \subseteq t' \implies \sigma_t = \sigma'_t{\restriction}_{L_t}).$$

$(L_t)_{t \subsetneq s}$ is a finitary independent system of algebraically closed fields. By lemma 1.3.4, there exists $\sigma'_s \in \mathrm{Aut}(L_s/\bar{\mathbb{Q}})$ extending $\bigcup_{t \subsetneq s} \sigma_t$.

$\sigma'_s(V_1{\restriction}_H) = V_2{\restriction}_H$, so, by Lemma 4.2.2 with $D := H := L^-$, there exists $\sigma''_s \in \mathrm{Aut}(L_s/L^-)$ such that $\sigma''_s(\sigma'_s(V_1{\restriction}_{L_s})) = V_2{\restriction}_{L_s}$. Let $\sigma_s := \sigma''_s \circ \sigma'_s$; then $\sigma_s$ extends $\sigma_t$ for $t \subsetneq s$, and $\sigma_s(V_1{\restriction}_{L_s}) = V_2{\restriction}_{L_s}$.

This concludes the inductive definition of $(\sigma_s)_{s \subset_{\mathrm{fin}} I}$. Let $\sigma := \bigcup_{s \subset_{\mathrm{fin}} I} \sigma_s$ be the direct limit. Then $\sigma \in \mathrm{Aut}(K/\bar{\mathbb{Q}})$ and $\sigma(V_1) = V_2$, as required. □

## 4.3 Orbits on $T$

Suppose for the following fact and definition that we are in the case $\mathbb{G} = \mathbb{E}$.

Let $\mu_m \leq \bar{\mathbb{Q}}^\times$ denote the group of $m$th roots of unity.

**Fact 4.3.1.** *For each $m \in \mathbb{N}$, there is an $\mathrm{Aut}(\bar{\mathbb{Q}}/k_0)$-invariant non-degenerate alternating bilinear pairing $w_m : E_m^2 \to \mu_m$, called the* Weil pairing*.*

**Definition 4.3.1.** Let ${}^{\mu^*_m}/_{\pm}$ be the primitive $m$th roots of unity quotiented by the equivalence relation which identifies $\zeta$ with $\zeta^{-1}$. For $\Lambda \leq T$, $\Lambda \cong \mathbb{Z}^2$, define

$$w_m(\Lambda) := {}^{w_m(\pi_m(\overline{\lambda}))}/_{\pm},$$

where $\overline{\lambda}$ is a $\mathbb{Z}$-basis of $\Lambda$. This is well-defined by bilinearity of $w_m$ and the fact that $\overline{\lambda}$ is well-defined up to action of $GL_2(\mathbb{Z})$.

${}^{\zeta_1}/_{\pm}$ is conjugate over $k_0$ to ${}^{\zeta_2}/_{\pm}$, written ${}^{\zeta_1}/_{\pm} \equiv_{k_0} {}^{\zeta_2}/_{\pm}$, iff $\zeta_1$ is $\mathrm{Gal}(\bar{\mathbb{Q}}/k_0)$-conjugate to either $\zeta_2$ or $\zeta_2^{-1}$.

**Theorem 4.3.2.** *Let $V_1, V_2 \leq \hat{V}(K)$ be standard; let $\Lambda_i := V_i \cap T$.*

*If $\mathbb{G} = \mathbb{G}_m$, the $\Lambda_i$ are $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-conjugate.*

*If $\mathbb{G} = \mathbb{E}$, let $m$ be as in Corollary B.1.1.1, and let $\overline{\lambda}_i \in \Lambda_i^2$ be a $\mathbb{Z}$-basis for $\Lambda_i$. Then $\Lambda_1$ and $\Lambda_2$ are $\mathrm{Gal}(\bar{\mathbb{Q}}/k_0)$-conjugate iff*

$$w_m(\Lambda_1) \equiv_{k_0} w_m(\Lambda_2).$$

*Proof.* If $\mathbb{G} = \mathbb{G}_m$, this follows from the fact (see Theorem 2.2.1) that every group automorphism of $G_\infty$ is induced by an element of $\mathrm{Gal}(\mathbb{Q}(G_\infty)/\mathbb{Q})$. Indeed, say $\lambda_i$ generates $\Lambda_i$. For each $n$, $\pi_n(\lambda_i)$ generates $G_n$, so there is a unique group automorphism $\tau_n \in \mathrm{Aut}(G_n)$ such that $\tau_n(\pi_n(\lambda_1)) = \pi_n(\lambda_2)$. Then the limit $\tau := \bigcup_n \tau_n \in \mathrm{Aut}(G_\infty)$ is induced by some $\sigma \in \mathrm{Gal}(\mathbb{Q}(G_\infty)/\mathbb{Q})$; $\sigma$ then maps $\lambda_1$ to $\lambda_2$, and hence $\Lambda_1$ to $\Lambda_2$ as required.

Suppose now $\mathbb{G} = \mathbb{E}$.

If $\sigma(\Lambda_1) = \sigma(\Lambda_2)$, and $\overline{\lambda}_1$ is a $\mathbb{Z}$-basis for $\Lambda_1$, then $\overline{\lambda}_2 := \sigma(\overline{\lambda}_1)$ is a $\mathbb{Z}$-basis for $\Lambda_2$. Then by Galois-invariance of $w_m$ and definitions,

$$\begin{aligned}\sigma(w_m(\Lambda_1)) &= {}^{w_m(\sigma(\pi_m(\overline{\lambda}_1)))}/_{\pm} \\ &= {}^{w_m(\pi_m(\overline{\lambda}_2))}/_{\pm} \\ &= w_m(\Lambda_2)\end{aligned}$$

For the converse, it remains to show that if $w_m(\Lambda_1) = w_m(\Lambda_2)$, then $\Lambda_1$ and $\Lambda_2$ are conjugate. Let $\overline{\lambda}_i$ be respective bases such that $w_m(\pi_m(\overline{\lambda}_1)) = w_m(\pi_m(\overline{\lambda}_2))$. This implies that $\pi_m(\overline{\lambda}_i)$ are in the same orbit of the action of $\mathrm{SL}_2({}^{\mathbb{Z}}/_{m\mathbb{Z}})$ on $G_m$. Since the natural map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2({}^{\mathbb{Z}}/_{m\mathbb{Z}})$ is a surjection [Shi94, Lemma 1.38], there exist bases $\overline{\lambda}'_i$ such that $\pi_m(\overline{\lambda}'_1) = \pi_m(\overline{\lambda}'_2)$.

By Corollary B.1.1.1 and the argument used in the multiplicative group case above, $\overline{\lambda}'_1$ is then conjugate to $\overline{\lambda}'_2$, and hence $\Lambda_1$ is conjugate to $\Lambda_2$. □

*Proof of Theorem 4.1.1.* By Theorem 4.2.3, the orbit under $\mathrm{Aut}(K/k_0)$ of a standard $V \leq \hat{V}$ is determined by the orbit of $V \cap T$. By Theorem 4.3.2, there are only finitely many such orbits, classified as stated if $\mathbb{G} = \mathbb{E}$, and there is only one orbit if $\mathbb{G} = \mathbb{G}_m$. □

*Remark* 4.3.1. If $k_0 = \mathbb{Q}$, then all elements of $\mu_m^*$ are conjugate over $k_0$, and so there is only one orbit.

## 4.4 Categoricity

In this section we rephrase the algebraic results above in model theoretic terms, where they become statements of categoricity of certain theories in the infinitary logic $L_{\omega_1,\omega}$, as previewed in Section 0.1. We essentially follow [Zil02a].

Our language has two sorts, $\mathbb{V}$ and $\mathbb{G}$. On $\mathbb{V}$ we place the language of $\mathbb{Q}$-vector spaces, $\langle +, (q\cdot)_{q\in\mathbb{Q}}\rangle$. On $\mathbb{G}$ we place the natural language over $k_0$, which consists of a predicate for each $k_0$-closed subvariety. Finally, we have in our language a function $\exp : \mathbb{V} \to \mathbb{G}$.

We define a first-order theory $T_{\mathbb{G}}$ in this language to be the theory axiomatised by:

(I) $\mathbb{G}$ satisfies the complete first order theory of $\mathbb{G}(K)$ in the natural language, for $K$ an algebraically closed extension of $k_0$;

(II) $\mathbb{V}$ satisfies the theory of $\mathbb{Q}$-vector spaces;

(III) exp is a surjective group homomorphism.

*Remark* 4.4.1. It is proved in [Zil02a] that $T_{\mathbb{G}}$ is complete and has quantifier elimination. Note that $\left\langle \hat{V}(K); \mathbb{G}(K); \hat{\pi} \right\rangle$ is a model.

Let $d := 1$ if $\mathbb{G} = \mathbb{G}_m$ and $d := 2$ if $\mathbb{G} = \mathbb{E}$. Consider the $L_{\omega_1,\omega}$ axiom:

$$\begin{aligned}\exists\overline{\lambda} \in \ker(\exp).\ ((\neg \bigvee_{\overline{n}\in\mathbb{Z}^d} \Sigma_i n_i\lambda_i = 0) \\ \wedge \forall\zeta \in \ker(\exp).\ \bigvee_{\overline{n}\in\mathbb{Z}^d} \Sigma_i n_i\lambda_i = \zeta)\end{aligned} \qquad (\ker(\exp) \cong \mathbb{Z}^d)$$

For the multiplicative group and certain elliptic curves, in particular if $k_0 = \mathbb{Q}$, $T_{\mathbb{G}} \cup \{\ker(\exp) \cong \mathbb{Z}^d\}$ is uncountably categorical. In general, it will have finitely many models in each transcendence degree, corresponding to the finitely many orbits of Theorem 4.1.1, and we need a further axiom to ensure categoricity. Let $\exp : V \to \mathbb{G}(K)$ be a model of $T_{\mathbb{G}} \cup \{\ker(\exp) \cong \mathbb{Z}^2\}$, let $\overline{\lambda}$ be a basis of $\ker(\exp)$, let $m$ be as in Corollary B.1.1.1, and let $f$ be the minimal polynomial over $k_0$ for $w_m(\exp(\overline{\lambda}/m)) \in \mu_m^*$. Consider the $L_{\omega_1,\omega}$ axiom:

$$\exists\overline{\lambda} \in \ker(\exp)^2.\ (\ker(\exp) = \langle\overline{\lambda}\rangle \wedge f(w_m(\exp({}^{\overline{\lambda}}/_{m}))) = 0). \qquad (\mathrm{Weil}_m(f))$$

Note that this can indeed be expressed by a $L_{\omega_1,\omega}$-sentence in our language: $\ker(\exp) = \langle\overline{\lambda}\rangle$ can be expressed as in the axiom $(\ker(\exp) \cong \mathbb{Z}^d)$, and $f(w_m(\exp(\frac{\overline{\lambda}}{m}))) = 0$ can be expressed since the field $K$ is $\emptyset$-interpretable with $k_0$ as distinguished points (Fact A.2.1), and $w_m : \mathbb{G}^2 \to K$ is then an invariant map with finite domain and hence is $\emptyset$-definable.

The algebraic analysis of Theorem 4.1.1 translates straightforwardly into a categoricity result:

**Theorem 4.4.1.** $T_{\mathbb{G}} \cup \{(\ker(\exp) \cong \mathbb{Z}^d), (\mathrm{Weil}_m(f))\}$ *is uncountably categorical.*

*Proof.* Let $\langle V; G; \exp\rangle$ be an uncountable model. By Fact A.2.1, $G \cong \mathbb{G}(K)$ for some algebraically closed field $K$ of the same cardinality as $G$, so $G$ is determined up to isomorphism by the cardinality.

It remains to show that for a fixed algebraically closed $K \geq k_0$, any two models $\langle V_1; \mathbb{G}(K); \exp_1 \rangle$ and $\langle V_2; \mathbb{G}(K); \exp_2 \rangle$ are isomorphic. Let

$$V_i' := \left\{ \left( \pi' \left( \frac{v}{n} \right) \right)_n \;\middle|\; v \in V_i \right\} \leq \hat{V}(K).$$

Then $V_i' \leq \hat{V}$ is standard and $\langle V_i; \mathbb{G}(K); \exp_i \rangle$ is isomorphic to $\langle V_i'; \mathbb{G}(K); \hat{\pi}\restriction_{V_i'} \rangle$. By ($\mathrm{Weil}_m(f)$) and Theorem 4.1.1, there exists $\sigma \in \mathrm{Aut}(K/k_0)$ such that $\sigma(V_1') = V_2'$; $\sigma$ induces an isomorphism of the structures as required. □

## 4.5 Limitations and extensions

In this informal section, we briefly discuss some known, suspected, or otherwise hypothesised generalisations of these results.

We have assumed that $\mathbb{E}$ has no complex multiplication. This should not be a necessary assumption - if everywhere "abelian group" is read as "End($\mathbb{E}$)-module" and "$\mathbb{Q}$-linearly independent" as "$\mathrm{End}(\mathbb{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$-linearly independent", most parts of our treatment can be seen to go through. The Kummer theory is known to work nicely, indeed more smoothly as there is no longer the complication of needing Serre's theorem to apply. Gavrilovich has already performed the necessary analysis for the analogue of Theorem 4.3.2 in his thesis - again, there are finitely many orbits. So the generalisation to arbitrary elliptic curves over number fields should be straightforward, but remains to be done.

We have been assuming characteristic 0 throughout. In the case of the multiplicative group, the analogue of Theorem 4.2.3 holds also in characteristic $p > 0$; since in this case $\mathbb{G}$ has no $p$ torsion, "standard" kernel has to mean $\mathbb{Z}[\frac{1}{p}]$. The proof of this result is in [BZ07]; there are few departures from the proof given here in characteristic 0 for the multiplicative group. (We could easily have included this case in our presentation here, but I didn't want to have to introduce further notational intricacies.) So perhaps it would make sense to try to generalise the elliptic curve case of Theorem 4.2.3 to positive characteristic. Note that already in the multiplicative group case, the analogue of Theorem 4.3.2 fails drastically - the torsion group $G_\infty$ is precisely $\mathbb{G}({\mathbb{F}_p}^{\mathrm{alg}})$, and so it is far from true that every group automorphism of $G_\infty$ is induced by an algebraic automorphism. In this way, it is not hard to see that there are infinitely many orbits of standard $V$ on $T$. Via the Weil pairing, the same will be true of an elliptic curve over a finite field. The best we can do, then, is to obtain categoricity over the torsion in the sense of Theorem 4.2.3. As mentioned, this has been done for the multiplicative group, but remains open for elliptic curves.

Another obvious direction in which to generalise is in dimension. We have restricted ourselves to semi-abelian curves; what of semi-abelian varieties in general? Distressingly, there has been no firm substantial progress on this since Gavrilovich's thesis work, so I refer the reader to [Gav06, IV.7.4,IV.5.4.2,IV.6]. But let me also remark that I have hopes that the methods of this thesis will prove to be useful in the higher dimensional case.

# Chapter 5

# Universal covers of 1-dimensional algebraic groups as topological structures

In this isolated and rather technical chapter, we describe and elucidate the structure of a natural coarse topological structure on covers with standard kernel. Although we will not formally discuss this aspect, these structures are examples of Analytic Zariski Structures as defined by Zilber.

There is not much novelty or surprise in the results of this chapter. For the case of the multiplicative group in characteristic 0, essentially the same conclusions were drawn in the thesis [Smi07] of Lucy Smith; we generalise this here to elliptic curves in characteristic 0 and to the multiplicative group in arbitrary characteristic. Meanwhile, the thesis [Gav06] of Misha Gavrilovich contains a thorough analysis of the analytic Zariski topology on universal covers of complex abelian varieties, which turns out to be the same as the topological structure we study here. The difference between that work and the present is one of approach - Gavrilovich starts with the complex analytic picture and uses theorems of complex analysis to derive consequences of algebraic character, whereas here we start with the pure algebra. In particular, the $N = 1$ case of 4.2.1, and its corollary Lemma 5.1.1e below, is the crucial fact which allows our analysis to proceed; conversely, for abelian varieties this fact falls out ([Gav06, III.1.3.4]) of Gavrilovich's analysis.

In particular then, we define a topological structure which is the analogue in positive characteristic of a natural topological reduct of the complex analytic structure on the universal cover of $\mathbb{G}_m(\mathbb{C})$, and which is rather tractable.

## 5.1 Setup

We work in one of the following 3 contexts:

(I) $\mathbb{G} = \mathbb{G}_m$; char 0; $k_0 := \mathbb{Q}$; $R := \mathbb{Z}$; $\Gamma_{\text{ker}} := \mathbb{Z}$

(II) $\mathbb{G} = \mathbb{G}_m$; char $p > 0$; $k_0 := \mathbb{F}_p$; $R := \mathbb{Z}[1/p]$; $\Gamma_{\text{ker}} := \mathbb{Z}[1/p]$

(III) $\mathbb{G} = E$, an elliptic curve defined over a number field $k_0$; $R := \text{End}(E)$; $\Gamma_{\text{ker}} := \mathbb{Z}^2$

A *cover with standard kernel* is then a 2-sorted structure $\langle V; \mathbb{G}(K); \pi\rangle$ where $V$ has the structure of a $R$-module, $K$ is algebraically closed and $\mathbb{G}(K)$ is considered in the natural language over $k_0$, and

$$\begin{tikzcd} 0 \arrow[r] & \Gamma_{\text{ker}} \arrow[r] & V \arrow[r, "\pi"] & \mathbb{G}(K) \arrow[r] & 0 \end{tikzcd} .$$

We collect some properties which hold in these contexts:

**Lemma 5.1.1.** *(a)* $[m] : \mathbb{G}^t \to \mathbb{G}^t$ *is open and closed.*

*(b) $R$ is a Noetherian ring, and $\Lambda$ is finitely generated as a $R$ module. $k_E := \mathbb{Q} \otimes R$ is a field. If $\eta \in R$, $\ker \eta \subseteq \mathbb{G}_m := \ker[m]$ for some $m \in \mathbb{N}$.*

*(c) Let $H \leq \mathbb{G}^t$ be a proper algebraic subgroup. Then $H \leq \ker(\eta)$ for some $0 \neq \eta : \mathbb{G}^t \to \mathbb{G}^s$ represented by some $E \in \mathrm{Mat}_{s,t}(R)$.*

*(d) Let $\eta : \mathbb{G}^t \to \mathbb{G}^s$ represented by some $E \in \mathrm{Mat}_{s,t}(R)$. Let $X \subset_{\mathrm{cl}} \mathbb{G}^s$ irreducible. Let $Y$ be any irreducible component of $\eta^{-1}(X)$. Then $\eta(Y) = X$.*

*(e) Let $K \geq k_0$ be algebraically closed; let $X \subseteq \mathbb{G}^t$ be closed and irreducible in the $K$-Zariski topology, and suppose $X$ is not contained in any proper algebraic subgroup of $\mathbb{G}^t$. Then there exists $m \in \mathbb{N}$ such that any irreducible component $X'$ of $[m]^{-1}(X)$ has the property that for all $t \in \mathbb{N}$, $[t]^{-1}(X')$ is irreducible.*

*Proof.* (a) This follows from $[m]$ being finite and étale.

(b) Standard.

(c) See Lemma 6.2.1.

(d) By (a), $\eta(Y_0) = X$ for some irreducible component $Y_0$ of $\eta^{-1}(X)$. But the isomorphisms $x \mapsto x+\zeta$ for $\zeta \in \ker\eta$ act transitively on the set of irreducible components, so $\eta(Y) = \eta(Y_0) = X$ for any irreducible component $Y$.

(e) Let $\overline{a} \in X$ be generic over $K$. By (c), $\overline{a}$ is $k_E$-linearly independent over $\mathbb{G}(K)$. By (d), for any $m$ the irreducible components of $[m]^{-1}(X)$ are in bijective correspondence with the $K$-conjugacy classes of $[m]^{-1}(\overline{a})$. The result therefore follows from the $N = 1$ case of Lemma 4.2.1 when that holds.

We proved Lemma 4.2.1 only under the assumptions of characteristic 0 and no complex multiplication; however, the proof of the $N = 1$ case goes through in the current more general context. For the multiplicative group in positive characteristic, this is proved as the $n = 1$ case of [BZ07, Theorem 3], with essentially the same proof as the characteristic 0 case. For elliptic curves with complex multiplication, one can note that the complex multiplication case of Theorem 3.2.1 follows as in Chapter 3 using the complex multiplication case of Bashmakov's theorem, and conclude the $N = 1$ case of Lemma 4.2.1 from Lang-Néron as before.

□

**Definition 5.1.1.** $X \subset_{\mathrm{cl}} \mathbb{G}^n$ is *unfurled* iff $[t]^{-1}(X)$ is irreducible for all $t \in \mathbb{N}$.

**Definition 5.1.2.** For $V$ a $k_E$-vector space, perhaps with extra structure:

(i) a *definable $k_E$-linear map* is a map $\theta : V^s \to V^t$ defined by a matrix $A \in \mathrm{Mat}_{t,s}(k_E)$;

(ii) a *definable affine $k_E$-linear map* is a the composition of a definable $k_E$-linear map with a translation;

(iii) a *definable $k_E$-linear subspace* is the kernel of a definable $k_E$-linear map;

(iv) a *definable $k_E$-linear coset* is a coset of a definable $k_E$-linear subspace.

## 5.2 $T_{\mathrm{inv}}$

**Definition 5.2.1.** Given a set $S$, a *topological structure* on $S$ consists of a topology on each $S^n$ such that

(i) The co-ordinate projection maps $\mathrm{pr} : S^n \to S^m$ are continuous;

(ii) The inclusion maps

$$\iota : S^m \to S^n; (x_1, \ldots, x_m) \mapsto (x_1, \ldots, x_m, c_{m+1}, \ldots, c_n)$$

are continuous.

(iii) The diagonal $\Delta \subseteq S^2$ is closed.

A *topological structure* is a set $S$ with a topological structure on it.

*Remark* 5.2.1.

- The "co-ordinate projection maps" in (i) should be understood to include the co-ordinate permutation maps : $S^n \to S^n$.

- It follows from the axioms (i)-(iii) that fibres $C(x, c)$ of closed sets are closed, cartesian products $C_1 \times C_2$ of closed sets are closed, and that a singleton set $\{s\} \subseteq S^n$, being a fibre of $\Delta^n$, is closed.

Fix an algebraically closed field $K \geq k_0$. We consider $\mathbb{G}(K)$ as a topological structure by equipping each $\mathbb{G}^n(K)$ with the $K$-Zariski topology.

Let $\hat{\mathbb{G}}(K) := \varprojlim_{\mathbb{N};|}([m] : \mathbb{G}(K) \to \mathbb{G}(K))$ be the inverse limit of copies of $\mathbb{G}(K)$ with respect to the multiplication-by-$m$ maps $[m]$ (a "proalgebraic group"); let $\hat{\pi}_n : \hat{\mathbb{G}}(K) \to \mathbb{G}(K)$ be the corresponding maps, so

$$[m] \circ \hat{\pi}_{nm} = \hat{\pi}_n.$$

We define a topological structure on $\hat{\mathbb{G}}(K)$ by equipping $\hat{\mathbb{G}}(K)^n$ with the inverse limit topology, i.e. the coarsest topology such that all $\hat{\pi}_n : \hat{\mathbb{G}}(K)^n \to \mathbb{G}^n(K)$ are continuous. We denote this topological structure on $\hat{\mathbb{G}}(K)$ by $T_{\mathrm{inv}}$.

Since $\mathbb{G}(K)$ is an $R$-module and $[m]$ is an $R$-module homomorphism, the inverse limit $\hat{\mathbb{G}}(K)$ also acquires the structure of an $R$-module; namely, for $\eta \in R$,

$$\eta(a_i)_{i \in \mathbb{N}} := (\eta a_i)_{i \in \mathbb{N}}.$$

Note that $\eta \in R$ is continuous for the topology on $\hat{\mathbb{G}}(K)$, and the graph of $\eta$ is closed in $\hat{\mathbb{G}}(K)^2$.

*Remark* 5.2.2.
- $\hat{\pi}_n$ is open and closed.
- $k_E$-linear maps are continuous.

## 5.3 Analytic Zariski topology on covers with standard kernel

Let $\pi : V \to \mathbb{G}(K)$ be a cover with standard kernel $\Lambda := \ker(\pi) \cong \Gamma_{\mathrm{ker}}$. Let $\pi_n(x) := \pi(\frac{x}{n})$; we can define as above a topological structure $T_{\mathrm{inv}}$ on $V$ by taking as a sub-basis of closed subsets of $V^t$ all pullbacks of $K$-Zariski closed subsets of $\mathbb{G}^t(K)$ under $\pi_m$. Equivalently, $T_{\mathrm{inv}}$ is the restriction topological structure induced by the canonical embedding of $(V, \pi, \mathbb{G}(K))$ into $(\hat{V}, \hat{\pi}, \mathbb{G}(K))$.

We wish also to consider a finer topological structure on $V$:

**Definition 5.3.1.** The topological structure $T_{\mathrm{an}}$ is that which has as sub-basis of closed sets the collection $\mathcal{S}$ of sets of the form

$$(\pi_n^{-1}(X) \cap L) + A, \tag{5.1}$$

where $X \subset_{\mathrm{cl}} \mathbb{G}^t(K)$ is $K$-Zariski closed, $L$ is a definable $k_E$-linear coset in $V^t$, and $A$ is an arbitrary subset of $\Lambda^t$.

We call elements of $\mathcal{S}$ *sub-basic* closed, and finite unions of them *basic* closed.

Note that $\Lambda^t \subseteq V^t$ has the discrete topology in $T_{\mathrm{an}}$; we will see later that $T_{\mathrm{an}}$ is the coarsest topological structure which refines $T_{\mathrm{inv}}$, induces the discrete topology on $\Lambda^t$, and for which all definable $k_E$-linear maps are continuous.

Call a finite union of sets of the form 5.1 a *basic* closed set. We also define a more technically useful sub-basis:

**Definition 5.3.2.** A *fundamental* closed set is one of form

$$\theta(\pi_n^{-1}(X)),$$

where $X \subset_{\mathrm{cl}} \mathbb{G}^t(K)$ is unfurled, and $\theta : V^d \to V^t$ is a definable affine $k_E$-linear embedding.

Define $\mathcal{S}'$ to be the collection of all sets of the form

$$F + A,$$

where $A \subseteq \Lambda^t$ and $F$ is a fundamental closed set.

Call elements of $\mathcal{S}'$ *sub-basic'* closed, and finite unions of them *basic'* closed.

The following theorem reveals the structure of $T_{\mathrm{an}}$, and shows it to be really quite simple.

**Theorem 5.3.1.** *(I) Let $\theta : V^s \to V^t$ be a definable affine $k_E$-linear map. Then $\theta$ is continuous.*

*(II) The basic' closed sets are precisely the basic closed sets; in particular, $\mathcal{S}'$ forms a sub-basis of closed sets for $T_{\text{an}}$.*

*(III) $T_{\text{an}}$ is the coarsest topological structure which refines $T_{\text{inv}}$, induces the discrete topology on $\Lambda^t$, and for which all definable affine $k_E$-linear maps are continuous.*

*(IV) Fundamental closed sets are irreducible.*

*(V) There is no infinite descending chain of fundamental closed sets.*

*(VI) The fundamental closed sets are precisely the irreducible closed sets.*

*Proof.* We work in $T_{\text{an}}$ throughout.

**Lemma 5.3.2.** *Any $S \in \mathcal{S}$ is a finite union of sets of the form*

$$\pi_n^{-1}(X) \cap (L + A), \tag{5.2}$$

*where $X \subset_{\text{cl}} \mathbb{G}^t$ is closed, $A \subseteq \Lambda^t$, and $L$ is a definable $k_E$-linear coset.*

*Proof.*

$$\begin{aligned}
(\pi_n^{-1}(X) \cap L) + A &= \bigcup_{\zeta \in \mathbb{G}_n^t} ((\pi_n^{-1}(X) \cap L) + (A \cap \pi_n^{-1}(\zeta))) \\
&= \bigcup_{\zeta \in \mathbb{G}_n^t} \bigcup_{\alpha \in A \cap \pi_n^{-1}(\zeta)} ((\pi_n^{-1}(X) + \alpha) \cap (L + \alpha)) \\
&= \bigcup_{\zeta \in \mathbb{G}_n^t} \left(\pi_n^{-1}(X + \zeta) \cap (L + A \cap \pi_n^{-1}(\zeta))\right),
\end{aligned}$$

where $\mathbb{G}_n^t$ is the $n$-torsion subgroup of $\mathbb{G}^t$. □

*Proof of I.* Translations $x \mapsto x + \gamma$ are easily seen to be continuous, so we may assume that $\theta$ is a definable $k_E$-linear map.

It suffices to show that the inverse image under $\theta$ of any sub-basic closed set is closed.

By Lemma 5.3.2, it suffices to show that $\theta^{-1}(\pi_n^{-1}(X))$ and $\theta^{-1}(\bigcup_{\alpha\in A}(L+\alpha))$ are closed for any $X$, $A$, $L$.

Now $\theta$ has matrix representation $T = m^{-1}E$ for some $m \in \mathbb{N}$ and some $E \in \mathrm{Mat}_{t,s}(R)$. Write $\eta$ both for the definable linear map $V^s \to V^t$ represented by $E$ and for the definable map $\mathbb{G}^s \to \mathbb{G}^t$ represented by $E$. By definitions, $\eta\pi_n = \pi_n\eta$.

Then $\theta^{-1}(\pi_n^{-1}(X)) = [m](\pi_n^{-1}(\eta^{-1}(X))) = \pi_{nm}^{-1}(\eta^{-1}(X))$, which is closed.

Now $L = \ker(\eta') + \gamma$ say, some definable $k_E$-linear map $\eta' : V^t \to V^r$ represented by $E' \in \mathrm{Mat}_{r,t}(k_E)$. Let $A' := \eta'(A) \subseteq {}^{\Lambda^r}\!/_m$ say, and let $\gamma' := \eta'(\gamma)$. Then $\bigcup_{\alpha\in A}(L+\alpha) = \eta'^{-1}(A'+\gamma')$.

Let $\theta' := \eta' \circ \theta$; we want to show that $\theta'^{-1}(A'+\gamma')$ is closed.

Let $N := ({}^{\Lambda^r}\!/_m + \gamma') \cap \mathrm{im}(\theta')$. If $N = \emptyset$, there is nothing to prove. Else, $N$ is a coset of $M := {}^{\Lambda^r}\!/_m \cap \mathrm{im}(\theta')$, say $N = M + \nu$.

Now $M$ is a sub-$R$-module of the finitely generated $R$-module ${}^{\Lambda^r}\!/_m$, so, by Noetherianity of $R$, $M$ is finitely generated as an $R$-module; say $M = \langle\bar{\mu}\rangle_R$. Let $\bar{\mu}'$ be such that $\bar{\mu} = \theta'(\bar{\mu}')$. Since $\mathbb{Q}\otimes\Lambda^t$ is a $k_E$-subspace, we may take $\mu_i' \in \mathbb{Q}\otimes\Lambda^t$. So $M' := \langle\bar{\mu}'\rangle_R \subseteq {}^{\Lambda^t}\!/_{m'}$ for some $m'$.

Now $x \mapsto \theta'(x)+\nu; M' \to N$ is a surjection; so say $A'' \subseteq M'$, $\theta'(A'')+\nu = (A'+\gamma')\cap\mathrm{im}(\theta')$, and let $\nu' \in \theta^{-1}(\nu)$. Then

$$\begin{aligned}\theta'^{-1}(A'+\gamma') &= \ker(\theta') + A'' + \nu' \\ &= \bigcup_{\zeta\in Z_{m'}} \ker(\theta') + \nu' + \zeta + ((A''-\zeta)\cap\Lambda^t),\end{aligned}$$

where $Z_{m'}$ is a set of representatives for $\frac{{}^{\Lambda^t}/_{m'}}{\Lambda^t}$, which is finite. So $\theta'^{-1}(A'+\gamma')$ is a finite union of sub-basic, and so closed as required. □

**Lemma 5.3.3.**

*(i) Let $\theta$ be a definable $k_E$-linear embedding. Then $\theta$ is a homeomorphism.*

*(ii)* $\mathcal{S}' \subseteq \mathcal{S}$.

*Proof.* By linear algebra, there exists a definable $k_E$-linear map $\phi$ such that $\phi\restriction_{\mathrm{im}(\theta)} = \theta^{-1}$. (i) then follows from the previous lemma. For (ii): say $\phi = {}^{\eta}/_{m}$, and let $L := \mathrm{im}(\theta)$; then

$$\begin{aligned}\theta(\pi_n^{-1}(X)) &= \phi^{-1}(\pi_n^{-1}(X)) \cap L \\ &= \pi_{nm}^{-1}(\eta^{-1}(X)) \cap L\end{aligned}$$

□

**Lemma 5.3.4.** *Any set of form $C := \pi_n^{-1}(X) \cap L$, where $X$ is closed and $L$ is a $k_E$-linear coset, is a finite union of fundamental closed sets.*

*Proof.* We may assume that $X$ is irreducible, $X \subseteq \pi_n(L)$, and $L$ is a minimal definable $k_E$ coset such that $X \subseteq \pi_n(L)$.

$L = \mathrm{im}(\theta)$ for some definable affine $k_E$-linear embedding $\theta : V^s \to V^t$, say $\theta = {}^{\eta}/_{m} + \gamma$. So $C = \theta(\pi_{nm}^{-1}(\eta^{-1}(X) - \pi_{nm}(\gamma)))$.

Let $Y$ be an irreducible component of $\eta^{-1}(X)$.

**Claim 5.3.4.1.** *$Y$ is not contained in any coset of a proper algebraic subgroup of $\mathbb{G}^s$.*

*Proof.* Else, by Lemma 5.1.1c, $Y \subseteq \ker(\eta') + g$, say. Let $L' := \ker(\eta') + \gamma \subseteq V^s$, where $\pi_{nm}(\gamma) = g$. Then $Y \subseteq \pi_{nm}(L')$.

But by Lemma 5.1.1d, $X = \eta(Y) \subseteq \eta(\pi_{nm}(L')) = \pi_n(\theta(L'))$, contradicting minimality of $L$. □

So we are done by Lemma 5.1.1e. □

II is now immediate.

*Proof of III.* In light of *I* and 5.3.2, it suffices to show:

**Lemma 5.3.5.** *Let $L \subseteq V^t$ be a definable affine $k_E$-linear coset, and let $A \subseteq \Lambda^t$. Then $L + A$ is a finite union of sets of form $\theta^{-1}(A')$, with $\theta : V^t \to V^s$ definable affine $k_E$-linear and $A' \subseteq \Lambda^s$.*

*Proof.* Say $L = \ker(\phi) + \alpha$ with $\phi$ an $k_E$-linear map. Then $L + A = \phi^{-1}(\phi(A)) + \alpha$. $\phi(A) \subseteq {}^{\Lambda^s}/_m$ for some $m$; the result follows easily. □

□

**Lemma 5.3.6.** *A finite intersection of sub-basic is basic.*

*Proof.* This is straightforward from Lemma 5.3.2. □

*Proof of IV.* Let $F$ be fundamental. By 5.3.3(i), we may assume $F = \pi^{-1}(X)$ for some unfurled $X$.

By the preceding lemma, it suffices to show that $F$ is not a finite union of sub-basic proper subsets of $F$. If $S$ is sub-basic then $\pi(S)$ is closed, so it suffices to show that if $S \subseteq F$ is sub-basic and $\pi(S) = X$, then $S = F$.

Say $S = (\pi_m^{-1}(Y) \cap L) + A$ and $\pi(S) = X$.

Since $X = \pi(F)$ is unfurled,

$$\pi_m(S) = \pi_m(F).$$

Suppose $L \subsetneq V^t$. Then $X = \pi(F) = \pi(S) \subseteq \pi(L)$, so $X$ is in a proper subcoset of $\mathbb{G}^t$. But this contradicts $F$ being unfurled.

So

$$\begin{aligned} S &= \pi_m^{-1}(Y) + A \\ &= \pi_m^{-1}(\pi_m(S)) \\ &= \pi_m^{-1}(\pi_m(F)) \\ &= F. \end{aligned}$$

□

*Proof of V.* By Noetherianity of the class of definable $k_E$-linear cosets, in suffices to show that there is no infinite strictly descending chain $(F_i)$ of fundamental closed such that the $F_i$ share a common least containing definable $k_E$-linear coset $L$. But indeed, we would then have $F_i = \theta(\pi_{n_i}^{-1}(X_i))$ where $\theta$ is a definable affine $k_E$-linear embedding with $L = \mathrm{im}(\theta)$. So since $\theta$ is a homeomorphism by Lemma 5.3.3(i), we may assume $F_i = \pi_{n_i}^{-1}(X_i)$. As above, $\dim(\pi(F_{i+1})) < \dim(\pi(F_i))$, so we contradict finiteness of $\dim(\pi(F_1))$. □

*Proof of VI.* Let $C$ be irreducible closed. By II,

$$C = \bigcap_i B_i,$$

where $B_i$ is basic'.

$C$ is irreducible, so $C$ is contained in an irreducible component $F_1$ of $B_1$. By the definition of basic', $F_1$ is fundamental closed. Let $B_2' := B_2 \cap F_1$. By Lemma 5.3.6 and 5.3.3(ii), $B_2'$ is basic'.

So

$$C \subseteq F_1 \cap \bigcap_{i>1} B_i = B_2' \cap \bigcap_{i>2} B_i.$$

Let $F_2$ be the irreducible component of $B_2'$ containing $C$.

Continuing, we construct a descending chain $(F_i)_{i\in\mathbb{N}}$ of fundamental closed subsets, such that $C = \bigcap_i F_i$. By V, $C = \bigcap_i F_i = F_t$ for some $t \in \mathbb{N}$. So $C$ is fundamental, as required. □

□

*Remark* 5.3.1. Note that it is not true that any closed set is basic closed, i.e. the basic closed sets do not form a topology. Furthermore, $\pi$ is not a closed map, although the image of basic closed is closed.

# Part II

# Schanuel Conjectures for Powers and the CIT

# Chapter 6

# CIT and Nonstandard Endomorphisms

This chapter represents joint work with Boris Zilber.

The Conjecture on Intersections with Tori, as conjectured by Zilber [Zil02b, Conjecture 1], Conjecture 6.1.1 below, states that there are essentially only finitely many ways in which a fixed subvariety of $\mathbb{G}_m^n$ can have an unusually large intersection with an algebraic subgroup of $\mathbb{G}_m^n$.

In this chapter we show, Theorem 6.3.1 below, that the CIT is equivalent to a certain dimension inequality regarding non-standard integer powers. We refer to this as a "Schanuel conjecture" for non-standard integer powers, as introduced in Section 0.1. A precise statement of this Schanuel conjecture will be given in the course of this chapter, but we give a rough statement here:

Consider complex exponentiation $\exp : \mathbb{C} \to \mathbb{C}^\times$ in the language which has the field structure on $\mathbb{C}^\times$ and has a sort for $\mathbb{Z}$ acting by multiplication on the cover $\mathbb{C}$. The CIT holds iff whenever $\langle {}^*\mathbb{C}; {}^*\mathbb{Z}; {}^*\exp\rangle$ is an elementary extension, for all $\overline{x} \in {}^*\mathbb{C}^{<\omega}$

$$\mathrm{ld}_{{}^*\mathbb{Q}}(\overline{x}/\ker({}^*\exp)) + \mathrm{trd}({}^*\exp(\overline{x}/\mathbb{C})) - \mathrm{ld}_{\mathbb{Q}}(\overline{x}/\ker({}^*\exp)) \geq 0, \qquad (6.1)$$

where ${}^*\mathbb{Q}$ is the quotient field of ${}^*\mathbb{Z}$.

In fact, we will find it convenient to work in a language which doesn't explicitly mention an exponential map. Furthermore, we give statements and results in a slightly greater generality, allowing an elliptic curve and its endomorphisms to replace the rôle of the multiplicative group and integer powers.

## 6.1 The CIT for $\mathbb{G}_m$ and elliptic curves

**Definition 6.1.1.** Let $W$ and $W'$ be subvarieties of a smooth algebraic variety $V$. We say that $W$ and $W'$ *intersect atypically* iff

$$\operatorname{codim}_V(W \cap W') < \operatorname{codim}_V(W) + \operatorname{codim}_V(W'),$$

where $\operatorname{codim}_V(U) := \dim(V) - \dim(U)$; an *atypical component* of $W \cap W'$ is then an irreducible component $S$ of $W \cap W'$ witnessing atypicality of the intersection, i.e. which is such that

$$\operatorname{codim}_V(S) < \operatorname{codim}_V(W) + \operatorname{codim}_V(W').$$

*Remark* 6.1.1. By the Dimension Theorem, in the context of Definition 6.1.1, since $V$ is smooth, we have

$$\operatorname{codim}_V(W \cap W') \leq \operatorname{codim}_V(W) + \operatorname{codim}_V(W').$$

Let $\mathbb{G}$ be either the multiplicative group $\mathbb{G}_m$ or an elliptic curve $\mathbb{E}$, defined over $k_0 \geq \mathbb{Q}$.

**Conjecture 6.1.1** (CIT). *Let $W$ be a subvariety of $\mathbb{G}^n$ defined over $k_0$. There exists a finite set $\tau(W)$ of algebraic subgroups of $\mathbb{G}^n$ such that if $T \leq \mathbb{G}^n$ is an algebraic subgroup and $S$ is an atypical component of $T \cap W$, then $S \subseteq T'$ for some $T' \in \tau(W)$.*

By abuse of acronym, we refer to this conjecture as the CIT even if $\mathbb{G} \neq \mathbb{G}_m$.

Note that the algebraic subgroups in the statement of the conjecture are not assumed to be connected.

In this chapter, we show that Conjecture 6.1.1 is equivalent to a Schanuel conjecture for non-standard endomorphisms.

We also consider the following apparently stronger variant form of the conjecture, which differs only in that it allows $W$ to be defined with parameters:

**Conjecture 6.1.2** (CIT′). *Let $W$ be a subvariety of $\mathbb{G}^n$, defined over some extension $k \geq k_0$. There exists a finite set $\tau(W)$ of algebraic subgroups of $\mathbb{G}^n$ such that if $T \leq \mathbb{G}^n$ is an algebraic subgroup and $S$ is an atypical component of $T \cap W$, then $S \subseteq T'$ for some $T' \in \tau(W)$.*

This variant form appears in [BMZ07, p27]; its equivalence to Conjecture 6.1.1 will be proved in the course of the proof of Theorem 6.3.1 below.

## 6.2 Setup

Let $\mathbb{G}$ be either the multiplicative group $\mathbb{G}_m$ or an elliptic curve $\mathbb{E}$, defined over $k_0 \geq \mathbb{Q}$.

Let $R := \mathrm{End}(\mathbb{G})$ be the ring of algebraic endomorphisms of $\mathbb{G}$; let $k_E := R \otimes_{\mathbb{Z}} \mathbb{Q}$. If $\mathbb{G} = \mathbb{G}_m$, $k_E \cong \mathbb{Q}$; if $\mathbb{G} = \mathbb{E}$, $k_E$ is isomorphic either to $\mathbb{Q}$ or to a quadratic imaginary field. Assume that all the endomorphisms $r \in R$ are defined over $k_0$.

We shall consider $\mathbb{G}$ in a language which has a sort $\mathbb{R}$ for $R = \mathrm{End}(\mathbb{G})$, so elementary extensions contain “non-standard endomorphisms”.

We first fix a *standard model.* Let $F \geq k_0$ be an algebraically closed field of infinite transcendence degree (for example $F = \mathbb{C}$), and let $\langle \mathbb{G}(F); R \rangle$ be the two sorted structure where $\mathbb{G}(F)$ is taken in the natural language over $k_0$ (see Section A.2), $R$ is taken in the ring language, and the language includes a function $\cdot : R \times \mathbb{G}(F) \to \mathbb{G}(F)$ interpreted as the action of $R$ on $\mathbb{G}(F)$. We write $\mathbb{R}$ for the second sort considered as a definable set.

We will also consider elementary extensions $\langle {}^*\mathcal{G}; {}^*\mathcal{R} \rangle$ of $\langle \mathbb{G}(F); R \rangle$.

$R$ has field of fractions $k_E$, so let ${}^*k_E$ be the field of fractions of ${}^*\mathcal{R}$. Let $\mathrm{Tor}_{{}^*\mathcal{R}}$ resp. $\mathrm{Tor}_R$ be the ${}^*\mathcal{R}$- resp. $R$-torsion of ${}^*\mathcal{G}$, i.e.

$$\mathrm{Tor}_{{}^*\mathcal{R}}({}^*\mathcal{G}) := \{x \in {}^*\mathcal{G} | \exists r \in {}^*\mathcal{R}.\ rx = 0\},$$

and similarly for $\mathrm{Tor}_R({}^*\mathcal{G})$.

Then ${}^{{}^*\mathcal{G}}/_{\mathrm{Tor}_{{}^*\mathcal{R}}({}^*\mathcal{G})}$ is a ${}^*k_E$-vector space. For $\overline{x} \in {}^*\mathcal{G}^n$ and $A \subseteq {}^*\mathcal{G}$, define

$$\mathrm{ld}_{{}^*\mathcal{R}}(\overline{x}/A) := \mathrm{ld}_{{}^*k_E}(\phi(\overline{x})/\phi(A)),$$

where $\phi : {}^*\mathcal{G} \to {}^{{}^*\mathcal{G}}/_{\mathrm{Tor}_{{}^*\mathcal{R}}({}^*\mathcal{G})}$ is the quotient map and $\mathrm{ld}_{{}^*k_E}$ denotes ${}^*k_E$-linear dimension. Define $\mathrm{ld}_R$ analogously.

Equivalently, say $\overline{x} \in {}^*\mathcal{G}^n$ is *${}^*\mathcal{R}$-linearly independent* iff

$$\forall \overline{r} \in {}^*\mathcal{R}^n \setminus \{\overline{0}\}.\ \Sigma_i r_i x_i \neq 0,$$

and define $\mathrm{ld}_{{}^*\mathcal{R}}(\overline{x})$ to be the cardinality of any maximal ${}^*\mathcal{R}$-linearly independent subtuple of $\overline{x}$. Similarly for $R$.

Given a tuple $\overline{c} \in \mathbb{G}^m$, by an *algebraic coset over* $\overline{c}$ we mean a fibre $H(\overline{c}) \subseteq \mathbb{G}^m$ for some algebraic subgroup $H \leq \mathbb{G}^{n+m}$.

**Lemma 6.2.1.** *Let $H \leq \mathbb{G}^n$ be an algebraic subgroup, $d := \dim(H)$. Then there exists an algebraic homomorphism $\theta \in \mathrm{Hom}(\mathbb{G}^n, \mathbb{G}^{n-d}) \cong \mathrm{Mat}_{n-d,n}(R)$ such that $H \leq \ker\theta$ and $\dim(\ker\theta) = d$.*

*Proof.* For some co-ordinate projection $\mathrm{pr} : G \to \mathbb{G}^d$ to $d$ of the co-ordinates, $\mathrm{pr}(H) = \mathbb{G}^d$ and $\ker \mathrm{pr} \leq H$ is finite. So say $N \in \mathbb{N}$ is such that $N \ker \mathrm{pr} = \{0\}$. Then $NH$ is the graph of a homomorphism $: \mathbb{G}^d \to \mathbb{G}^{n-d}$, so $NH = \ker\theta$ for a homomorphism $\theta : \mathbb{G}^n \to \mathbb{G}^{n-d}$. □

**Lemma 6.2.2.** *Let $\overline{a} \in \mathbb{G}^n$ and $\overline{c} \in \mathbb{G}^m$. Then $\mathrm{ld}_R(\overline{a}/\overline{c})$ is the dimension of the smallest algebraic coset over $\overline{c}$ containing $\overline{a}$.*

*Proof.* We may assume that $\overline{c}$ is $R$-linearly independent. Let $H(\overline{c})$ be the smallest coset over $\overline{c}$ containing $\overline{a}$. Then $\dim(H) = \dim(H(\overline{c})) + m$ and $\mathrm{ld}_R(\overline{ac}) = \mathrm{ld}_R(\overline{a}/\overline{c}) + m$, and $H$ is the smallest subgroup containing $\overline{ac}$.

So it suffices to prove the lemma in the case that $\overline{c} = \emptyset$. So let $H$ be the smallest subgroup containing $\overline{a}$. By Lemma 6.2.1, $H \leq \ker M$ for some $M \in \mathrm{Mat}_{t,n}(R)$ with $R$-linearly independent rows, and $\dim(H) = \dim(\ker M) = n - t$. So $\dim(H) \geq \mathrm{ld}_R(\overline{a})$. The converse inequality is clear. □

## 6.3 CIT as a Schanuel conjecture for non-standard endomorphisms

**Theorem 6.3.1.** *Let $F$ be an algebraically closed field of characteristic 0 and infinite transcendence degree. Let $\mathbb{G}$ be either the multiplicative group or an elliptic curve, defined over $k_0 \leq F$, and let $R := \mathrm{End}(\mathbb{G})$.*

*Then Conjecture 6.1.1 holds for $\mathbb{G}$ iff for any elementary extension $\langle {}^*\mathcal{G}; {}^*\mathcal{R}\rangle$ of $\langle \mathbb{G}(F); R\rangle$, for any tuple $\overline{a} \in {}^*\mathcal{G}^{<\omega}$,*

$$\delta(\overline{a}) := \mathrm{ld}_{{}^*\mathcal{R}}(\overline{a}) + \mathrm{trd}(F(\overline{a})/F) - \mathrm{ld}_R(\overline{a}) \geq 0 \qquad (6.2)$$

*Proof.* We show that the following are all equivalent:

(i) $\forall \overline{a} \in {}^*\mathcal{G}^{<\omega}.\ \delta(\overline{a}) := \mathrm{ld}_{{}^*\mathcal{R}}(\overline{a}) + \mathrm{trd}(F(\overline{a})/F) - \mathrm{ld}_R(\overline{a}) \geq 0$

(ii) $\forall \overline{a} \in {}^*\mathcal{G}^{<\omega}.\ \delta(\overline{a}/\mathbb{G}(F)) := \mathrm{ld}_{{}^*\mathcal{R}}(\overline{a}/\mathbb{G}(F)) + \mathrm{trd}(F(\overline{a})/F) - \mathrm{ld}_R(\overline{a}/\mathbb{G}(F)) \geq 0$

(iii) Let $W$ be an algebraic subvariety of $\mathbb{G}^n$ defined over $F$. Then there exists a finite set $\tau_0^c(W)$ of proper algebraic subgroups such that if $C$ is an algebraic subgroup with $\dim C < \mathrm{codim}\, W$, then $C \cap W \subseteq \bigcup \tau_0^c(W)$.

(iv) CIT', Conjecture 6.1.2

(v) CIT, Conjecture 6.1.1

We prove $(ii) \Rightarrow (i) \Rightarrow (iii) \rightarrow (iv) \Rightarrow (v) \Rightarrow (ii)$:

(ii) $\Rightarrow$ (i): It suffices to show that for any $\overline{a}$,

$$\mathrm{ld}_{^*\mathcal{R}}(\overline{a}/\mathbb{G}(F)) - \mathrm{ld}_R(\overline{a}/\mathbb{G}(F)) \leq \mathrm{ld}_{^*\mathcal{R}}(\overline{a}) - \mathrm{ld}_R(\overline{a}).$$

For this, it suffices to show that if $c\overline{c} \in \mathbb{G}(F)^{1+n}$ then

$$\mathrm{ld}_{^*\mathcal{R}}(\overline{a}/c\overline{c}) - \mathrm{ld}_R(\overline{a}/c\overline{c}) \leq \mathrm{ld}_{^*\mathcal{R}}(\overline{a}/\overline{c}) - \mathrm{ld}_R(\overline{a}/\overline{c}).$$

By Steinitz exchange, this fails iff $rc \in \langle\overline{ac}\rangle_R$ for some $r \in R$ and yet for all $r' \in {}^*\mathcal{R}$, $r'c \notin \langle\overline{ac}\rangle_{^*\mathcal{R}}$. But $c \in \mathbb{G}(F)$, so this contradicts $\langle\mathbb{G}(F); R\rangle$ being elementarily embedded in $\langle{}^*\mathcal{G}; {}^*\mathcal{R}\rangle$.

(i) $\Rightarrow$ (iii): First note that for any $n$-tuple $\overline{x}$ in the sort $\mathbb{G}$ and any $t \leq n$, the condition $\mathrm{ld}_{\mathbb{R}}(\overline{x}) < n - t$ is first-order expressible in the language $\langle\mathbb{G}; \mathbb{R}\rangle$, by saying that there exists $M \in \mathrm{Mat}_{t,n}(\mathbb{R})$ with $\mathbb{R}$-linearly independent rows such that $M\overline{x} = \overline{0}$.

Suppose (iii) is false for some $W$. Then by Lemma 6.2.2, the following type over $F$ is consistent:

$$\begin{aligned}&\overline{x} \in W \wedge \mathrm{ld}_{\mathbb{R}}(\overline{x}) < \operatorname{codim} W \\ &\qquad \wedge \bigwedge_{m\in\mathbb{N}} \left( \bigwedge_{\overline{r}\in R^n} (\overline{rx} = \overline{0} \rightarrow \overline{r} = \overline{0}) \right)\end{aligned}$$

So for some elementary extension $\langle{}^*\mathcal{G}; {}^*\mathcal{R}\rangle$, the type is realised by some $\overline{a} \in {}^*\mathcal{G}^n$. But then

$$\mathrm{ld}_{^*\mathcal{R}}(\overline{a}) + \mathrm{trd}(\overline{a}/F) - \mathrm{ld}_R(\overline{a}) < \operatorname{codim} W + \dim W - n = 0.$$

(iii) $\Rightarrow$ (iv): Let $W$ be an algebraic subvariety of $\mathbb{G}^n$ defined over $k \geq k_0$. Since $F$ is of infinite transcendence degree, we may suppose $k \leq F$. We may suppose that $W$ is (absolutely) irreducible.

Now it suffices to show that for each $t \leq \dim(W)$ there exists a finite set $\tau_t(W)$ of proper subgroups of $\mathbb{G}^n$ such that if $H$ is a subgroup with $\dim(H) < \operatorname{codim}(W)+t$ then any irreducible component $S \subseteq H \cap W$ with $\dim(S) \geq t$ is contained in some $H' \in \tau_t(W)$. Indeed, we can then take $\tau(W) := \bigcup_t \tau_t(W)$. So fix $t \leq \dim(W)$.

Let Pr be the finite set of co-ordinate projection maps $\mathrm{pr} : \mathbb{G}^n \to \mathbb{G}^t$ to $t$-tuples of co-ordinates such that $\mathrm{pr}(W)$ is Zariski dense in $\mathbb{G}^t$. Since $t \leq \dim(W)$ and $\dim(\mathbb{G}) = 1$, Pr is non-empty.

Let $\overline{a} \in \mathbb{G}^t(F)$ be generic - such exists since $F$ is of infinite transcendence degree.

Note that for any $\mathrm{pr} \in \mathrm{Pr}$, we have $\overline{a} \in \mathrm{pr}(W)$ and so $W \cap \mathrm{pr}^{-1}(\overline{a}) \neq \emptyset$.

Let $\tau_t(W) := \bigcup_{\mathrm{pr}\in\mathrm{Pr}} \tau_0^c(W \cap \mathrm{pr}^{-1}(\overline{a}))$ where each $\tau_0^c(W \cap \mathrm{pr}^{-1}(\overline{a}))$ is as given by (iii). We clain that $\tau_t(W)$ is as required.

So let $H \leq \mathbb{G}^n$ be an algebraic subgroup such that $\dim(H) < \operatorname{codim}(W) + t$. Suppose $S$ is an irreducible component of $H \cap W$ with $\dim S \geq t$. Then $\mathrm{pr}(S)$ is dense for some $\mathrm{pr} \in \mathrm{Pr}$, and so $S' := S \cap \mathrm{pr}^{-1}(\overline{a}) \neq \emptyset$. Let $W' := W \cap \mathrm{pr}^{-1}(\overline{a}) \neq \emptyset$.

Since $\overline{a}$ is generic and $W$, $S$ are irreducible, we have

$$\dim W' = \dim W - t$$
$$\dim S' = \dim S - t,$$

So $\dim H < \operatorname{codim} W'$. But $S' \subseteq H \cap W'$, so $S' \subseteq\subseteq \bigcup \tau_0^c(W')$; $S$ is irreducible, so $S \subseteq H'$ for some $H' \in \tau_0^c t(W') \subseteq \tau_t(W)$.

So $\tau_t(W)$ is as required.

(iv) $\Rightarrow$ (v): Clear.

(v) $\Rightarrow$ (ii): Suppose $\overline{a} \in {}^*\mathcal{G}^n$ and $\delta(\overline{a}/\mathbb{G}(F)) < 0$. We may assume that $\overline{a}$ is $R$-linearly independent over $\mathbb{G}(F)$.

Let $W$ be the locus of $\overline{a}$ over $F$ in $\mathbb{G}^n$, i.e. the intersection of all $F$-closed subsets containing $\overline{a}$.

We may represent $W$ as $W = V(\overline{c})$ for some $k_0$-closed $V \subseteq \mathbb{G}^{n+m}$ and some $\overline{c} \in \mathbb{G}(F)^m$. We may assume that $\overline{c}$ is such that $\mathrm{ld}_{^*\mathcal{R}}(\overline{a}/\overline{c}) = \mathrm{ld}_{^*\mathcal{R}}(\overline{a}/\mathbb{G}(F))$. We may also assume that $\overline{c}$ is $R$-linearly independent (since $\overline{c} \in \langle \overline{c}' \rangle_R$ for some $R$-linearly independent $\overline{c}'$). By appropriate choice of $V$, we may also assume that $\overline{c}$ is generic in the projection $\mathrm{pr}(V)$, so $\dim(V) = \dim(W) + \dim(\overline{c})$.

Let $\tau(V)$ be as given by (v).

Suppose $H(\overline{c}) \subseteq \mathbb{G}^n$ is a proper algebraic coset over $\overline{c}$ such that $\dim(H(\overline{c})) < \mathrm{codim}_{\mathbb{G}^n}(W)$ and $H(\overline{c}) \cap W \neq \emptyset$, say $\overline{b} \in H(\overline{c}) \cap W$. Say $S$ is a component of $H \cap V$ containing $(\overline{b}, \overline{c})$. Then

$$\begin{aligned}
\mathrm{codim}_{\mathbb{G}^{n+m}}(S) &\leq (n+m) - \dim(\overline{c}) \\
&= (n+m) - (\dim(V) - \dim(W)) \\
&= \mathrm{codim}_{\mathbb{G}^{n+m}}(V) + \dim(W) \\
&< \mathrm{codim}_{\mathbb{G}^{n+m}}(V) + \mathrm{codim}_{\mathbb{G}^n}(H(\overline{c})) \\
&= \mathrm{codim}_{\mathbb{G}^{n+m}}(V) + \mathrm{codim}_{\mathbb{G}^{n+m}}(H),
\end{aligned}$$

the last equality holding since $\overline{c}$ is $R$-linearly independent. So $\overline{b} \in H'(\overline{c})$ for one of the $H' \in \tau(V)$.

So the type

$$\begin{aligned}
&\overline{x} \in W \wedge \mathrm{ld}_{\mathbb{R}}(\overline{x}/\overline{c}) < \mathrm{codim}\, W \\
&\quad \wedge \bigwedge_m \bigwedge_{(\overline{r}, \overline{r}') \in R^{n+m}} (\overline{rx} = \overline{r}'\overline{c} \to \overline{r} = \overline{0})
\end{aligned}$$

is inconsistent; but $\overline{a}$ realises it. Contradiction.

□

*Remark* 6.3.1. The inequality (6.1) corresponds precisely to the inequality (6.2) with $\mathbb{G} = \mathbb{G}_m$ and $F = \mathbb{C}$; obvious modifications to the proof of Theorem 6.3.1 therefore suffice to show the equivalence of the CIT to the statement in terms of (6.1) given in the introduction to the chapter.

# Chapter 7

# Schanuel Conjectures for Raising to Powers and the CIT

## 7.1 A Schanuel inequality for generic powers in exponential fields

The material in this section forms part of joint work with Jonathan Kirby and Alex Wilkie, [BKW08].

**Definition 7.1.1.** Field extensions $K$ and $L$ of a field $F$ are said to be *linearly disjoint* over $F$, $K \perp_F L$, iff any tuple $\overline{k}$ of elements of $K$ is linearly independent over $L$ iff it is linearly independent over $F$.

**Lemma 7.1.1.** *(i) $K \perp_F L$ iff $L \perp_F K$*

*(ii) $K \perp_F L$ iff for any tuple $k$ from $K$, $\mathrm{ld}_L(\overline{k}) = \mathrm{ld}_F(\overline{k})$*

*(iii) If $\overline{k}$ is algebraically independent over $L \geq F$, then $F(\overline{k}) \perp_F L$.*

*Proof.* (i) Standard.

(ii) $\overline{k}$ is an $L$-linear basis iff it is an $F$-linear basis.

(iii) This is [Lan02, Proposition VIII 3.3].

□

**Lemma 7.1.2.** *Suppose $K \perp_F L$. Then for any tuple $\overline{x}$ from any field extension of $KL$ and any $A \subseteq L$,*

$$\mathrm{ld}_K(\overline{x}/L) - \mathrm{ld}_F(\overline{x}/L) \leq \mathrm{ld}_K(\overline{x}/A) - \mathrm{ld}_F(\overline{x}/A)$$

*Proof.* Say $l \in L$ is a finite tuple s.t. $\mathrm{ld}_K(\overline{x}/lA) = \mathrm{ld}_K(\overline{x}/L)$ and $\mathrm{ld}_F(\overline{x}/lA) = \mathrm{ld}_F(\overline{x}/L)$.

Now:

$$\begin{aligned}
\mathrm{ld}_K(\overline{x}/A) - \mathrm{ld}_K(\overline{x}/lA) &= \mathrm{ld}_K(l/A) - \mathrm{ld}_K(l/\overline{x}A) && \text{(by addition formula)}\\
&= \mathrm{ld}_F(l/A) - \mathrm{ld}_K(l/\overline{x}A) && \text{(by Lemma 7.1.1(ii))}\\
&\geq \mathrm{ld}_F(l/A) - \mathrm{ld}_F(l/\overline{x}A)\\
&= \mathrm{ld}_F(\overline{x}/A) - \mathrm{ld}_F(\overline{x}/lA) && \text{(by addition formula)}
\end{aligned}$$

□

**Definition 7.1.1.** An *exponential field* $\langle K; +, \cdot, \exp\rangle$ is a field equipped with a homomorphism $\exp : K \to K^\times$ from the additive group to the multiplicative group.

An *exponential polynomial* $f : K^n \to K$ is a function of the form

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n, \exp(x_1), \ldots, \exp(x_n)),$$

where $g$ is a polynomial. An *exponential polynomial map* $F : K^n \to K^m$ is a map of the form $F(\overline{x}) = (f_1(\overline{x}), \ldots, f_m(\overline{x}))$ where $f_i$ are exponential polynomials. It is *defined over* $A \subseteq K$ iff the corresponding polynomials are defined over $A$. The formal derivative $\frac{\partial F}{\partial x_i} : K^n \to K^m$ of $F(x_1, \ldots, x_n)$ is defined in the obvious way by formal differentiation of polynomial maps, the rule $\frac{d\exp(x)}{dx} = \exp(x)$, and the chain rule. The Jacobian of an exponential polynomial map $F : K^n \to K^m$ at a point $\overline{a} \in K^n$ is the matrix $\mathrm{Jac}_{\overline{a}}(F) \in \mathrm{Mat}_{m,n}(K)$ with $i$th column $\frac{\partial F}{\partial x_i}(\overline{a})$. A *non-singular zero* of an exponential polynomial map $F$ is a tuple $\overline{a} \in K^n$ such that $F(\overline{a}) = \overline{0}$ and $\mathrm{Jac}_{\overline{a}}(F)$ is non-singular.

The *exponential closure* (or *étale closure*) of a subset $A \subseteq K$, $\mathrm{ecl}(A)$, is the set of all $x \in K$ such that for some tuple $\overline{y} \in K^{<\omega}$ and some exponential polynomial map $F$ defined over $A$, $x\overline{y}$ is a non-singular zero of $F$.

A tuple $\overline{p} \in K^n$ is ecl-*independent*, or *exponentially algebraically independent*, over $C \subseteq K$ iff for all $i$,

$$p_i \notin \mathrm{ecl}(C \cup \{p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_n\}).$$

The following is the main theorem of [BKW08].

**Theorem 7.1.3.** *Let $\langle K; +, \cdot, \exp\rangle$ be an exponential field, let $C \leq K$ be* ecl-*closed, and let $\overline{p} \in K^n$ be tuple* ecl-*independent over $C$. Then for any tuple $\overline{x}$ from $K$:*

$$\mathrm{ld}_{\mathbb{Q}(\overline{p})}(\overline{x}/\ker) + \mathrm{trd}(\exp(\overline{x})/C) - \mathrm{ld}_{\mathbb{Q}}(\overline{x}/\ker) \geq 0,$$

*where* ker *is the kernel of* exp.

*Proof.* Define:

$$\delta(\overline{x}) := \mathrm{trd}(\overline{x}, \exp(\overline{x})) - \mathrm{ld}_{\mathbb{Q}}(\overline{x}),$$

$$\delta_C(\overline{x}) := \delta(\overline{x}/C) = \mathrm{trd}(\overline{x}, \exp(\overline{x})/C) - \mathrm{ld}_{\mathbb{Q}}(\overline{x}/C),$$

$$d_C(\overline{x}) := \min\{\delta_C(\overline{zx}) | \overline{z} \text{ a tuple from } \mathbb{C}\},$$

$$\mathrm{ecl}_C(A) := \mathrm{ecl}(C \cup A).$$

In [Kir08], Kirby shows that $d_C$ is the dimension function of a pregeometry $\mathrm{cl}_C$ on $K$, and that $\mathrm{ecl}_C = \mathrm{cl}_C$.

So we have:

(i) $\overline{p}$ is "self-sufficient" in $\mathbb{C}_{\exp}$ with respect to $\delta_C$, i.e. for any tuple $\overline{x} \in K^{<\omega}$:

$$\delta_C(\overline{p}, \overline{x}) \geq \delta_C(\overline{p}).$$

(ii) $\overline{p}$ is algebraically independent over $C$.

(iii) $\mathbb{Q}(\overline{p})$ is linearly disjoint from $C$ over $\mathbb{Q}$ (by Lemma 7.1.1 iii).

**Lemma 7.1.4.** *For any tuples $\overline{p}, \overline{x}$:*

*(a)* $\mathrm{trd}(\exp(\overline{p})/C, \exp(\overline{x})) \leq \mathrm{ld}_{\mathbb{Q}}(\overline{p}/C, \overline{x})$

*(b)* $\mathrm{trd}(\overline{x}/C, \overline{p}) \leq \mathrm{ld}_{\mathbb{Q}(\overline{p})}(\overline{x}/C)$

*Proof.* (a) Say $p_1, \ldots, p_t$ are $\mathbb{Q}$-linearly independent over $(C, \overline{x})$, and for $i > t$, $p_i$ is in the $\mathbb{Q}$-linear span of $(C, \overline{x}, p_1, \ldots, p_t)$. Then for $i > t$, $\exp(p_i)$ is in the algebraic closure of $(C, \exp(\overline{x}), \exp(p_1), \ldots, \exp(p_t))$. So $\mathrm{trd}(\exp(\overline{p})/C, \exp(\overline{p})) \leq t = ld_Q(\overline{p}/C, \overline{x})$.

(b) Similar, since if $x_i$ is in the $\mathbb{Q}(\overline{p})$-linear span of $(x_1, \ldots, x_t, C)$ then $x_i$ is in the algebraic closure of $(C, \overline{p})$.

□

Now for any tuple $\overline{x}$ from $\mathbb{C}$ we have:

$$\begin{aligned}
n = \quad & \delta_C(\overline{p}) \\
\leq \quad & \delta_C(\overline{x}, \overline{p}) && \text{(by i)} \\
= \quad & \operatorname{trd}(\overline{x}, \exp(\overline{x}), \overline{p}, \exp(\overline{p})/C) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}, \overline{p}/C) \\
\leq \quad & \operatorname{trd}(\exp(\overline{x}), \exp(\overline{p})/C) + \operatorname{trd}(\overline{x}, \overline{p}/C) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}, \overline{p}/C) \\
= \quad & \operatorname{trd}(\exp(\overline{p})/C, \exp(\overline{x})) + \operatorname{trd}(\exp(\overline{x})/C) \\
& + \operatorname{trd}(\overline{x}/C, \overline{p}) + \operatorname{trd}(\overline{p}/C) \\
& - \operatorname{ld}_{\mathbb{Q}}(\overline{p}/C, \overline{x}) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}/C) \\
= \quad & \operatorname{trd}(\exp(\overline{p})/C, \exp(\overline{x})) - \operatorname{ld}_{\mathbb{Q}}(\overline{p}/C, \overline{x}) \\
& + \operatorname{trd}(\overline{x}/C, \overline{p}) \\
& + \operatorname{trd}(\exp(\overline{x})/C) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}/C) + \operatorname{trd}(\overline{p}/C) \\
\leq \quad & 0 \\
& + \operatorname{ld}_{\mathbb{Q}(\overline{p})}(\overline{x}/C) \\
& + \operatorname{trd}(\exp(\overline{x})/C) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}/C) + \operatorname{trd}(\overline{p}/C)
\end{aligned}$$

But by (ii), $\operatorname{trd}(\overline{p}/C) = n$, so

$$\begin{aligned}
0 &\leq \operatorname{trd}(\exp(\overline{x})/C) + \operatorname{ld}_{\mathbb{Q}(\overline{p})}(\overline{x}/C) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}/C) \\
&\leq \operatorname{trd}(\exp(\overline{x})/C) + \operatorname{ld}_{\mathbb{Q}(\overline{p})}(\overline{x}/\ker) - \operatorname{ld}_{\mathbb{Q}}(\overline{x}/\ker) \quad \text{(by (iii) and Lemma 7.1.2)}
\end{aligned}$$

As required. □

*Remark* 7.1.1. In the case that the exponential field is a model of the theory of $\mathbb{R}_{\exp}$, which is the case which will be of relevance below, the use of [Kir08] in the proof of Theorem 7.1.3 can be replaced by more specific arguments - see the proof of [BKW08, Proposition 2.1] for this.

## 7.2 Towards Real CIT

As we saw in Chapter 6, the CIT is equivalent to a Schanuel inequality for non-standard integer powers, (6.1). Theorem 7.1.3 provides such an inequality for particular rings of non-standard powers, namely those generated by exponentially algebraically independent powers. This applies in particular to models of the theory of real exponentiation. In this context, a non-standard integer is just an infinite element of an elementary extension of the real exponential field $\mathbb{R}_{\exp}$, which is easily seen to be ecl-independent over $\mathbb{R}$. This already provides a CIT-style result on the reals for families of tori parameterised by a single integer, Theorem 7.2.2 below. For arbitrarily many powers, the implication of Theorem 7.1.3 is that any failure of CIT on the reals, for a given variety $W$ over the reals, must be due to some finitely many fixed exponential-algebraic dependencies on the integer powers involved - Theorem 7.2.3 makes this precise.

**Fact 7.2.1** ([Wil96]). *Let $\mathcal{R}$ be a model of the theory of the real exponential field $\mathbb{R}_{\exp}$. Then $\mathcal{R}$ is an o-minimal structure, and the pregeometry of definable closure,* dcl*, coincides with the exponential algebraic closure operator* ecl *defined above.*

First, we give the result for a one-integer-parameter family of subtori:

**Theorem 7.2.2.** *Let $V \subseteq \mathbb{A}^n$ be an affine algebraic variety of dimension $d$ defined over $\mathbb{R}$. Let $M = M(X) = (m_{i,j}(X))_{i,j} \in \mathrm{Mat}_{d+1,n}(\mathbb{Z}[X])$.*

*Then there exists a finite set $(\overline{n}_i)_i$ of non-zero $n$-tuples of integers such that for all $N \in \mathbb{Z}$, if the rows of $M(N)$ are $\mathbb{Q}$-linearly independent then*

$$\forall \overline{y} \in (\mathbb{R}^{\times})^n.\ ((\overline{y} \in V \wedge \overline{y}^{M(N)} = \overline{1}) \rightarrow \bigvee_i \overline{y}^{\overline{n}_i} = 1),$$

*where $\overline{x}^{M(N)} = (\Pi_j x_j^{m_{i,j}(N)})_{i \in \{1,\ldots,d+1\}}$.*

*Proof.* Consider the following collection of formulae with free variables $(\overline{x}, t)$ in $\mathbb{R}_{\exp}$:

(i) $\exp(\overline{x}) \in V$

(ii) $\forall \overline{z}.\ ((\bigwedge_i \Sigma_j z_j \cdot m_{i,j}(t) = 0) \to \overline{z} = \overline{0})$

(iii) $M(t) \cdot \overline{x} := (\Sigma_j m_{i,j}(t) \cdot x_j)_i = \overline{0}$

(iv) for each $M \in \mathbb{N}$: $|t| > M$

(v) for each $\overline{m} \in (\mathbb{Z}^n \setminus \{\overline{0}\})$: $\overline{m} \cdot \overline{x} := \Sigma_j m_j \cdot x_j \neq 0$

Suppose this were a consistent type, say realised by $(\overline{a}, \tau)$ in an elementary extension ${}^*\mathcal{R} \succeq \mathbb{R}_{\exp}$. By (iv) and Archimedeanity of $\mathbb{R}$, $\tau \notin \mathbb{R}$. By (ii) and (iii), $\operatorname{ld}_{\mathbb{Q}(\tau)}(\overline{a}) < (n-d)$. By (i), $\operatorname{trd}(\overline{a}/\mathbb{R}) \leq d$. By (v), $\operatorname{ld}_{\mathbb{Q}}(\overline{a}) = n$.

So

$$\operatorname{ld}_{\mathbb{Q}(\tau)}(\overline{a}) + \operatorname{trd}(\exp(\overline{a})/\mathbb{R}) - \operatorname{ld}_{\mathbb{Q}}(\overline{a}) < 0,$$

contradicting Theorem 7.1.3 applied to ${}^*\mathcal{R}$ with $C := \mathbb{R} \leq {}^*\mathcal{R}$ (which is an ecl-closed subset by Fact 7.2.1).

So (i)-(v) are inconsistent. By the compactness theorem for first-order logic, there exists $M \in \mathbb{N}$ and a finite collection $(\overline{m}_i)_i$ of $n$-tuples of integers such that

$$\forall (\overline{x}, t) \in \mathbb{R}.\ ([\text{(i)-(iii) hold for } (\overline{x}, t)] \to (|t| \leq M \vee \bigvee_i \overline{x}^{\overline{m}_i} = 1)).$$

So let $(\overline{n}_i)_i := (\overline{m}_i)_i \cup ((m_{1,j}(t))_j)_{t \in \{-M,\ldots,M\}}$, and we are done. □

Next, we give a stronger multivariate version of Theorem 7.2.2, stating that any failure of Real CIT must be due to exponential relations between the integer powers involved.

Recall that the (o-minimal) dimension of a tuple $\overline{a}$ in an o-minimal structure $\mathcal{R}$ over a subset $C \subseteq R$, $\dim(\overline{a}/C)$, is the dimension of $\overline{a}$ over $C$ with respect to the pregeometry dcl. The dimension of a definable set $X \subseteq \mathcal{R}^n$ defined over $C \subseteq R$, $\dim(X)$, is the maximal value of $\dim(\overline{a}/C)$ for $\overline{a} \in X({}^*\mathcal{R})$ for ${}^*\mathcal{R} \succeq \mathcal{R}$ is an elementary extension.

**Theorem 7.2.3.** *Let $V \subseteq \mathbb{A}^n$ be an affine algebraic variety of dimension $d$ defined over $\mathbb{R}$. Let $s \in \mathbb{N}$. Let $M = (m_{i,j}(\overline{X}))_{i,j} \in \mathrm{Mat}_{d+1,n}(\mathbb{Z}[\overline{X}])$, $\overline{X}$ an $s$-tuple.*

*Then there exists a finite set $(\overline{n}_i)_i$ of non-zero $n$-tuples of integers, and an $\mathbb{R}_{\exp}$-definable set $X \subseteq \mathbb{R}^n$ with $\dim(X) < s$ such that for all $\overline{N} \in \mathbb{Z}^s$, if the rows of $M(\overline{N})$ are $\mathbb{Q}$-linearly independent then either $\overline{N} \in X$, or*

$$\forall \overline{x} \in (\mathbb{R}^\times)^n. \; ((\overline{x} \in V \wedge \overline{x}^{M(\overline{N})} = \overline{1}) \rightarrow \bigvee_i \overline{x}^{\overline{n}_i} = 1).$$

*Proof.* In fact, we prove the stronger statement where $\overline{N}$ ranges over $\mathbb{R}^s$.

Suppose the statement is false. Then the following type in $(\overline{z}, \overline{\nu})$ is consistent:

(i) $\exp(\overline{z}) \in V$

(ii) $M(\overline{\nu})\overline{z} = \overline{0}$

(iii) the rows of $M(\overline{\nu})$ are linearly independent over the field (this is one formula)

(iv) $\overline{\nu}$ is in no definable set over $\mathbb{R}$ of dimension less than $s$

(v) $\overline{z}$ is $\mathbb{Q}$-linearly independent

and so is realised in some elementary extension ${}^*\mathcal{R}_{\exp}$ of $\mathbb{R}_{\exp}$ by $(\overline{a}, \overline{\eta})$ say.

By (i), $\mathrm{trd}(\exp(\overline{a})/\mathbb{R}) \leq d$. By (ii) and (iii), $\mathrm{ld}_{\mathbb{Q}(\overline{\eta})}(\overline{a}) \leq n - d - 1$. By (v), $\mathrm{ld}_{\mathbb{Q}}(\overline{a}) = n$. But by (iv), $\overline{\eta}$ is ecl-independent over $\mathbb{R}$, which is ecl-closed by Lemma 7.2.1. So we have a contradiction to Theorem 7.1.3. □

# Appendix A

# Algebraic varieties as first order structures

This section aims to be a concise account of some well-known facts about the model theory of algebraic geometry, for which there appear to be no clear references.

## A.1 Interpretations

All interpretations will be $\emptyset$-interpretations. An *$A$-interpretable set* of a structure is a set of the form $D/\sim$ where $D$ is an $A$-definable set and $\sim$ is an $A$-definable equivalence relation.

**Notation A.1.1.** If $\mathcal{A}$ and $\mathcal{B}$ are first order structures, $\Gamma : \mathcal{A} \rightsquigarrow \mathcal{B}$ denotes an interpretation of $\mathcal{B}$ in $\mathcal{A}$. We denote $\bar{\Gamma} : I \to \bar{\Gamma}(I)$ the associated bijections of $\emptyset$-interpretable sets $I$ of $\mathcal{B}$ with associated $\emptyset$-interpretable sets $\bar{\Gamma}(I)$ of $\mathcal{A}$, which we may also think of as forming a map $\bar{\Gamma} : B^{eq} \to A^{eq}$. In particular we have a bijection $\bar{\Gamma} : B \to \bar{\Gamma}(B)$ of the universe of $\mathcal{B}$ with a $\emptyset$-interpretable set of $\mathcal{A}$. We also denote by $\Gamma$ the associated topological homomorphism $\Gamma : \mathrm{Aut}(\mathcal{A}) \to \mathrm{Aut}(\mathcal{B})$.

Note the contravariance: $\overline{\Gamma \circ \Delta} = \bar{\Delta} \circ \bar{\Gamma}$.

Recall

**Definition A.1.1.** A *self-interpretation* is an interpretation $\Gamma : \mathcal{A} \rightsquigarrow \mathcal{A}$ such that the associated bijection $\bar{\Gamma} : A \to \bar{\Gamma}(A)$ is $\emptyset$-definable in $\mathcal{A}$.

A *bi-interpretation* between $\mathcal{A}$ and $\mathcal{B}$ is a pair of interpretations $\Gamma : \mathcal{A} \rightsquigarrow \mathcal{B}$ and $\Delta : \mathcal{B} \rightsquigarrow \mathcal{A}$ such that $\Delta \circ \Gamma$ and $\Gamma \circ \Delta$ are self-interpretations. We denote such a bi-interpretation by

$$\Gamma : \mathcal{A} \leftrightsquigarrow \mathcal{B} : \Delta.$$

*Remark* A.1.1. Although the clearest formulation is in terms of structures as above, bi-interpretation can be seen to be a property of the corresponding pair of complete theories.

**Definition A.1.2.** In the context of a bi-interpretation $\Gamma : \mathcal{A} \leftrightsquigarrow \mathcal{B} : \Delta$, we define $\mathrm{dcl}^{\mathrm{eq}}$ on the disjoint union of $A^{eq}$ and $B^{eq}$:

$$\begin{aligned} a \in \mathrm{dcl}^{\mathrm{eq}}(\bar{a}, \bar{b}) \quad &\text{iff} \quad a \in \mathrm{dcl}^{\mathrm{eq}}_{\mathcal{A}}(\bar{a}, \bar{\Gamma}(\bar{b})) \\ b \in \mathrm{dcl}^{\mathrm{eq}}(\bar{a}, \bar{b}) \quad &\text{iff} \quad b \in \mathrm{dcl}^{\mathrm{eq}}_{\mathcal{B}}(\bar{\Delta}(\bar{a}), \bar{b}) \end{aligned}$$

We extend this to infinite sets by finite character, as usual.

**Lemma A.1.1.**

*(i)* $b \in \mathrm{dcl}^{\mathrm{eq}}_{\mathcal{B}}(\bar{b})$ *iff* $\bar{\Gamma}(b) \in \mathrm{dcl}^{\mathrm{eq}}_{\mathcal{A}}(\bar{\Gamma}(\bar{b}))$

*(ii)* $\mathrm{dcl}^{\mathrm{eq}}$ *is a closure relation on* $A^{eq} \dot{\cup} B^{eq}$.

*(iii) If* $I$ *is a* $\emptyset$*-interpretable set of* $\mathcal{B}$ *and* $C$ *is* $\mathrm{dcl}^{\mathrm{eq}}$*-closed, then* $\bar{\Gamma}(I \cap C) = \bar{\Gamma}(I) \cap C$.

*Remark* A.1.2. We could make the corresponding definitions and statements for $\mathrm{acl}^{\mathrm{eq}}$.

## A.2 Algebraic varieties in their natural language

Let $\mathbb{G}$ be an infinite abstract algebraic variety defined over a field $k$. Let $K \geq k$ be algebraically closed. We consider $\mathbb{G}(K)$ as a structure $\mathcal{G}$ in the language which has a predicate for each Zariski closed $k$-definable subset, and call this the *natural language* for the variety.

Let $\Gamma : \mathcal{K}^k \rightsquigarrow \mathcal{G}$ be an interpretation of $\mathcal{G}$ in $\mathcal{K}^k$, where $\mathcal{K}^k$ is the structure on $K$ of an algebraically closed field expanded with distinguished constants for $k$. $\Gamma$ corresponds to a choice of open cover of $\mathbb{G}$ by finitely many $k$-definable affine varieties with $k$-definable transition maps.

$\mathcal{G}$ has all the structure induced from $\mathcal{K}^k$ via $\Gamma$; i.e. for any $n$, $X \subseteq G^n$ is $\emptyset$-definable in $\mathcal{G}$ iff $\bar{\Gamma}(X) \subseteq \bar{\Gamma}(G^n)$ is $\emptyset$-interpretable in $\mathcal{K}^k$. Note that this implies that for any sort $S = {}^{G^n}/_{\sim}$ of $\mathcal{G}^{eq}$, $X \subseteq S$ is $\emptyset$-interpretable in $\mathcal{G}$ iff $\bar{\Gamma}(X) \subseteq \bar{\Gamma}(S)$ is $\emptyset$-interpretable in $\mathcal{K}^k$. It also implies that $\mathcal{G}$ has quantifier elimination.

**Fact A.2.1.** *$\mathcal{G}$ is bi-interpretable with $\mathcal{K}^k$,*

$$\Gamma : \mathcal{K}^k \leftrightsquigarrow \mathcal{G} : \Delta.$$

*Proof.* Let $f : \mathbb{G} \to K$ be a non-constant rational function defined over $k$. $K' := \operatorname{im} f \subseteq K$ is cofinite in $K$. Let $A$ be the quotient of the domain of $f$ by the equivalence relation $f(x) = f(y)$. $A$ is $\emptyset$-definable in $\mathcal{G}$, and $f$ induces a bijection $\theta : A \to K'$ which is $\emptyset$-definable in $\mathcal{K}^k$.

Now consider the equivalence relation on $A^2$,

$$(a, b) \sim (a', b') \iff \theta(a) + \theta(b) = \theta(a') + \theta(b').$$

This is $\emptyset$-definable in $\mathcal{K}^k$, and hence in $\mathcal{G}$. Let $F := {}^{A^2}/_{\sim}$, and define $\phi : F \to K$; ${}^{(a,b)}/_{\sim} \mapsto a + b$. Then $\phi$ is $\emptyset$-definable in $\mathcal{K}^k$ and is a bijection. Pulling the $\mathcal{K}^k$ structure on $K$ back to $F$ via $\phi$, $F$ becomes an isomorphic copy of $\mathcal{K}^k$ interpretable in $\mathcal{G}$.

Let $\Delta : \mathcal{G} \rightsquigarrow \mathcal{K}^k$ be the corresponding interpretation; $\bar{\Gamma} \circ \bar{\Delta} = \phi$, so $\Delta \circ \Gamma$ is a self-interpretation.

It remains to check that $\Gamma \circ \Delta$ is a self-interpretation; but indeed, the bijection $\bar{\Gamma} \circ \bar{\Delta} : \bar{\Gamma}(G) \to (\bar{\Gamma} \circ \bar{\Delta} \circ \bar{\Gamma})(G)$ is $\emptyset$-definable in $\mathcal{K}^k$ since $\phi$ is; the graph of this is precisely the image under $\bar{\Gamma}$ of the graph of $\bar{\Delta} \circ \bar{\Gamma} : G \to (\bar{\Delta} \circ \bar{\Gamma})(G)$, and so this map is part of the structure induced on $\mathcal{G}$ via $\Gamma$.

□

# Appendix B

# Miscellany

## B.1 Galois representations

We quote here some standard results which are used in a number of places in the text.

Let $\mathbb{E}$ be an elliptic curve over a number field $k_0$.

Suppose $\mathbb{E}$ has no complex multiplication, $\mathrm{End}(\mathbb{E}) \cong \mathbb{Z}$.

A Galois automorphism $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/k_0)$ induces automorphisms of each $E_n$ which commute with the maps $[m]$, and hence induces group automorphisms of $T$ and $T_l$. This gives a continuous $l$-adic representation:

$$\rho_l : \mathrm{Gal}(\bar{\mathbb{Q}}/k_0) \to \mathrm{Aut}_{\mathbb{Z}_l}(T_l).$$

The following fact, which is effectively the foundation on which our argument is built, is highly non-trivial.

**Fact B.1.1** ([Ser72]). *For each prime $l$, $\mathrm{im}(\rho_l) \leq \mathrm{Aut}_{\mathbb{Z}_l}(T_l)$ is an open subgroup. Equality holds for all but finitely many primes.*

We sometimes find it useful to use an alternative statement, concerning group automorphisms of $E_\infty$:

**Corollary B.1.1.1.** *There exists $m \in \mathbb{N}$ such that any group automorphism of $E_\infty$ fixing $E_m$ is induced by some algebraic automorphism fixing $k_0$; i.e.*

$$\upharpoonright_{E_\infty} : \mathrm{Gal}(\bar{\mathbb{Q}}/k_0) \twoheadrightarrow \mathrm{Aut}(E_\infty/E_m) \ .$$

*Proof.* Let $l_i$ be one of the finitely many primes such that $\mathrm{im}(\rho_l)$ is a proper open subgroup of $\mathrm{Aut}(T_l)$. Each $\mathrm{im}(\rho_{l_i})$, being open, contains the kernel of some reduction $\mathrm{Aut}(T_l) \to \mathrm{Aut}(E_{l_i^{n_i}})$. So

$$\upharpoonright_{E_{l_i^\infty}} : \mathrm{Gal}(\bar{\mathbb{Q}}/k_0) \twoheadrightarrow \mathrm{Aut}(E_{l_i^\infty}/E_{l_i^{n_i}}) \ ,$$

and for the other primes $l$, the image is the whole of $\mathrm{Aut}(E_{l^\infty})$. Let $m := \Pi_i l_i^{n_i}$; the desired surjection follows by composition with the isomorphism

$$\Pi_l \,\mathrm{Aut}(E_{l^\infty}) \cong \mathrm{Aut}(E_\infty).$$

□

## B.2 Galois cohomology and torsors

We include here a brief account of the material on Galois cohomology we need in the proof of Lemma 2.4.2.

**Definition B.2.1.** Let $\mathbb{G}$ be a commutative algebraic group defined over a field $k$.

- A *continuous $\bar{k}/k$-1-cocycle* is a map $\theta : \mathrm{Gal}(\bar{k}/k) \to \mathbb{G}(\bar{k})$ satisfying

  $$\forall \sigma, \tau \in \mathrm{Gal}(\bar{k}/k).\ \theta(\sigma\tau) = \theta(\sigma) + \sigma\theta(\tau)$$

  and which is continuous with respect to the Krull topology on $\mathrm{Gal}(\bar{k}/k)$ and the discrete topology on $\mathbb{G}(\bar{k})$. The continuous $\bar{k}/k$-1-cocycles form an abelian group $C^1 = C^1(\mathrm{Gal}(\bar{k}/k), \mathbb{G}(\bar{k}))$ with addition $(\theta + \theta')(\sigma) =$

$\theta(\sigma) + \theta'(\sigma)$.

- The *$\bar{k}/k$-1-coboundaries* comprise the subgroup

$$B^1 = B^1(\mathrm{Gal}(\bar{k}/k), \mathbb{G}(\bar{k})) := \{< \cdot, \alpha > | \alpha \in \mathbb{G}(\bar{k})\} \leq C^1,$$

  where $< \sigma, \alpha >:= \sigma\alpha - \alpha$.

- The *first $\bar{k}/k$ cohomology group*, $H^1 = H^1(\mathrm{Gal}(\bar{k}/k))$, is the quotient group ${}^{C^1}/_{B^1}$. Two 1-cocycles in $C^1$ with the same image in $H^1$ are said to be "cohomologous".

**Fact B.2.1** (Hilbert 90)**.** *For the multiplicative group, all continuous 1-cocycles are 1-coboundaries; i.e. for any field $k$,*

$$H^1(\mathrm{Gal}(\bar{k}/k), \mathbb{G}_m(\bar{k})) = 0.$$

For an elliptic curve, $\mathbb{G} = \mathbb{E}$, the cohomology need not be trivial. It can be studied in terms of torsors. We follow [Sil86, X.3] for this material; the reader may look there for justifications. The model-theoretic reader may also find useful the model theoretic presentation of these ideas in [Pil97].

**Definition B.2.2.**

- A *$k$-torsor* of an elliptic curve $\mathbb{E}$ over $k$ (also known as a *principal homogeneous space* for $\mathbb{E}$) is a projective curve $\mathbb{T}$ over $k$ and a simply transitive action of $\mathbb{E}$ on $\mathbb{T}$ defined over $k$,

$$\mathbb{T} \times \mathbb{E} \to \mathbb{T}$$
$$(\beta, \alpha) \mapsto \beta + \alpha.$$

- We write $\beta - \alpha$ for the unique $\gamma \in \mathbb{T}$ such that $\gamma + \alpha = \beta$.

- Two $k$-torsors $\mathbb{T}, \mathbb{T}'$ for $\mathbb{E}$ are *equivalent*, $\mathbb{T} \cong \mathbb{T}'$, iff they are $k$-definably isomorphic as torsors, i.e. iff there exists a $k$-definable bijection $\theta : \mathbb{T} \to \mathbb{T}'$

such that

$$\forall \beta \in \mathbb{T}.\ \forall \alpha \in \mathbb{E}.\ \theta(\beta+\alpha) = \theta(\beta) + \alpha.$$

$\mathbb{T}$ is said to be *trivial* iff $\mathbb{T} \cong \mathbb{E}$.

$\mathrm{WC}(\mathbb{E}/k)$ is the set of equivalence classes of $k$-torsors. It is called the *Weil-Châtelet group* - the group structure is defined via the bijection in Fact B.2.2 below.

- Given a $k$-torsor $\mathbb{T}$ and a point $\beta \in \mathbb{T}(\bar{k})$,

$$\begin{array}{rcccc} \langle \cdot, \beta \rangle & : & \mathrm{Gal}(\bar{k}/k) & \to & \mathbb{E}(\bar{k}) \\ & ; & \sigma & \mapsto & \sigma\beta - \beta \end{array}$$

is a continuous $\bar{k}/k$-1-cocycle.

**Fact B.2.2.** *The map*

$$\begin{array}{rcccccc} \theta & : & \mathrm{WC}(\mathbb{E}/k) & \to & H^1(\mathrm{Gal}(\bar{k}/k), \mathbb{E}(\bar{k})) & & \\ & ; & {}^{\mathbb{T}}/_{\cong} & \mapsto & \langle \cdot, \beta \rangle & & \textit{(any } \beta \in \mathbb{T}(\bar{k})\textit{)} \end{array}$$

*is a bijection.*

## B.3 Free and locally free abelian groups

**Definition B.3.1.** A torsion-free abelian group is *locally free* iff every finite rank subgroup is free.

**Fact B.3.1** (Pontryagin)**.** *A countable torsion-free abelian group is locally free iff it is free.*

**Lemma B.3.2.** *For torsion-free abelian groups, the properties of freeness and local freeness are preserved under taking extensions and subgroups. In other words, given an exact sequence of torsion-free abelian groups*

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & C \arrow[r] & B \arrow[r] & 0 \end{tikzcd},$$

*$C$ is (locally) free if both $A$ and $B$ are (locally) free, and $A$ is (locally) free if $C$ is (locally) free.*

*Proof.* For the case of freeness, this is standard and easily proven. The case of local freeness follows by restricting to finite rank subgroups. $\square$

# Bibliography

[Bal04] John T. Baldwin. Notes on quasiminimality and excellence. *Bull. Symbolic Logic*, 10(3):334–366, 2004.

[BKW08] Martin Bays, Jonathan Kirby, and Alex Wilkie. A schanuel property for exponentially transcendental powers. 2008. arXiv:0810.4457 [math.NT] [math.LO].

[BMZ99] E. Bombieri, D. Masser, and U. Zannier. Intersecting a curve with algebraic subgroups of multiplicative groups. *Internat. Math. Res. Notices*, (20):1119–1140, 1999.

[BMZ07] E. Bombieri, D. Masser, and U. Zannier. Anomalous subvarieties—structure theorems and applications. *Int. Math. Res. Not. IMRN*, (19):Art. ID rnm057, 33, 2007.

[BZ07] Martin Bays and Boris Zilber. Covers of multiplicative groups of algebraically closed fields in arbitrary characteristic. 2007. arXiv:0704.3561 [math.LO];.

[dPKM06] Tristram de Piro, Byunghan Kim, and Jessica Millar. Constructing the hyperdefinable group from the group configuration. *J. Math. Log.*, 6(2):121–139, 2006.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[Gav06] Misha Gavrilovich. *Model theory of the universal covering spaces of complex algebraic varieties*. PhD thesis, Oxford University, 2006.

[Hru06] Ehud Hrushovski. Groupoids, imaginaries, and internal covers. 2006. arXiv:math/0603413v1 [math.LO].

[Ked01] Kiran S. Kedlaya. The algebraic closure of the power series field in positive characteristic. *Proc. Amer. Math. Soc.*, 129(12):3461–3470 (electronic), 2001.

[Kir08] Jonathan Kirby. Exponential algebraicity in exponential fields. 2008. arXiv:0810.4285v2 [math.LO].

[Lan72] Serge Lang. *Introduction to algebraic geometry*. Addison-Wesley Publishing Co., Inc., Reading, Mass., 1972. Third printing, with corrections.

[Lan78] Serge Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1978.

[Lan83] Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Mum88] David Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1988.

[Pil96] Anand Pillay. *Geometric stability theory*, volume 32 of *Oxford Logic Guides*. The Clarendon Press Oxford University Press, New York, 1996. Oxford Science Publications.

[Pil97] Anand Pillay. Remarks on Galois cohomology and definability. *J. Symbolic Logic*, 62(2):487–492, 1997.

[Ray68] F. J. Rayner. An algebraically closed field. *Glasgow Math. J.*, 9:146–151, 1968.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[She83a] Saharon Shelah. Classification theory for nonelementary classes. I. The number of uncountable models of $\psi \in L_{\omega_1,\omega}$. Part A. *Israel J. Math.*, 46(3):212–240, 1983.

[She83b] Saharon Shelah. Classification theory for nonelementary classes. I. The number of uncountable models of $\psi \in L_{\omega_1,\omega}$. Part B. *Israel J. Math.*, 46(4):241–273, 1983.

[She90] S. Shelah. *Classification theory and the number of nonisomorphic models*, volume 92 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 1990.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Smi07] Lucy Smith. *Toric varieties as analytic Zariski structures*. PhD thesis, Oxford University, 2007.

[Wil96] A. J. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function. *J. Amer. Math. Soc.*, 9(4):1051–1094, 1996.

[Zil02a] B. Zilber. Model theory, geometry and arithmetic of the universal cover of a semi-abelian variety. In *Model theory and applications*, volume 11 of *Quad. Mat.*, pages 427–458. Aracne, Rome, 2002.

[Zil02b] Boris Zilber. Exponential sums equations and the Schanuel conjecture. *J. London Math. Soc. (2)*, 65(1):27–44, 2002.

[Zil03] B. Zilber. Raising to powers in algebraically closed fields. *J. Math. Log.*, 3(2):217–238, 2003.

[Zil04] B. Zilber. Raising to powers revisited. 2004. `http://www.maths.ox.ac.uk/~zilber/publ.html`.

[Zil05a] B. Zilber. Pseudo-exponentiation on algebraically closed fields of characteristic zero. *Ann. Pure Appl. Logic*, 132(1):67–95, 2005.

[Zil05b] Boris Zilber. A categoricity theorem for quasi-minimal excellent classes. In *Logic and its applications*, volume 380 of *Contemp. Math.*, pages 297–306. Amer. Math. Soc., Providence, RI, 2005.

[Zil06] Boris Zilber. Covers of the multiplicative group of an algebraically closed field of characteristic zero. *J. London Math. Soc. (2)*, 74(1):41–58, 2006.