Scuola Normale Superiore di Pisa

Classe di Scienze

Corso di Perfezionamento in Matematica

Tesi di perfezionamento

Zilber fields and complex exponentiation

Vincenzo Mantova

Relatore: Prof. Alessandro Berarducci

Referente interno: Prof. Umberto Zannier

21 Gennaio 2013

Acknowledgements

First of all, I would like to thank my supervisor Alessandro Berarducci, who followed me with great patience during these years and let me wander before settling on some definite problems. He taught me that cool and surprising things happen at every level of detail, and that connections between different parts of mathematics are always around; and that even when the technicalities abound, things can be still communicated to non-specialist, one has just to be willing (and training).

I also would like to thank Umberto Zannier, who followed me at the Scuola Normale. I had the pleasure to work with him on some side projects, and some of the things I have learned with him have made through this thesis. He taught me how to avoid being trapped by excessive formalism and language, but to go straight to the facts, focusing on what is happening rather than on the explanation.

I also have to give a special thank to Jonathan Kirby, who was very keen to update me on the whole Zilber fields situation already the first time we met, at the Geometric Model Theory conference in Oxford, 2010, and even proposed things to work on that eventually led to this thesis.

I thank Boris Zilber, who let me work in Oxford at the very end of my Ph.D., and shared many thoughts and ideas that have not had time to appear here. I thank Angus Macintyre, who insisted on the problem of involutions in at least three different public occasions where I was present, thus giving me the start, and promptly manifested interest in the results. I also thank David Masser and Jonathan Pila, for the helpful discussions on heights.

My thanks also go to my colleagues, and especially Maurizio Monge, Fabio Tonini, and Samuele Mongodi, with whom I have had several inspiring conversations on Mathematics and on some problems about this thesis as well.

I would like to thank the Scuola Normale, the University of Pisa, and the MALOA network for having provided the means to research, and to live as well; and I also thank all the institutions and people, in Italy, in Europe and in the world who care about knowledge and culture more than immediate and measurable benefits.

I would like to thank Martina, who always supported me and accepted my sudden alienation and my blabbing incomprehensible words from time to time, during the most intensive research moments.

I thank my parents, who are always at my side, and accept never to know exactly what their son is doing (but I confess that quite often I don't know either).

And last, but not least, I thank all my friends, who are now more and more scattered across Europe but never seem too far away (Internet is the coolest invention).

Contents

Introduction

It is safe to say that the study of the model theoretic properties of algebraic structures, and of fields in particular, started eighty years ago with Tarski's proof of quantifier elimination on real closed fields, and went considerably far since then: from knowing that all the definable sets in real closed and algebraically closed fields are quantifier-free definable, we are now aware of all sorts of phenomena involving definable sets, even with striking applications outside of the model theory itself.

Tools from stability theory proved to be useful to classify several tame expansions of the theory of fields, producing the so called "stability hierarchy". For example, we know that $\mathbb{R}_{\mathrm{exp}}$, $\mathbb{R}_{\mathrm{an}}$ and $\mathbb{R}_{\mathrm{an,exp}}$ are all o-minimal; that algebraically closed fields and differentially closed fields are ω-stable, and its strongly minimal sets are Zariski geometries (up to finite sets of points); that $\mathbb{C}_\mu$, where μ is a predicate for all the roots of unity, is superstable; that the algebraically closed fields with automorphisms (ACFA) are simple; the algebraically closed valued fields (ACVF) are C-minimal; and so on.

What happens, however, if we take an expansion that is necessarily not tame in the stability hierarchy? Some different sort of tameness is needed. The example we have in mind is $\mathbb{C}_{\mathrm{exp}}$, the field of complex numbers equipped with the classical exponential function. Its definable sets are certainly not tame in the first-order framework, for the following simple reason:

$$\mathbb{Z} = \{x \,:\, \forall y(\exp(y) = 1 \to \exp(xy) = 1)\}.$$

The whole Peano's Arithmetic is definable, and this is understandably 'not tame'.

Zilber's proposal was to use a form of "analytic geometry" [Zil97], obtained by generalising Zariski geometries to the non-Noetherian case, where for example infinite discrete sets, as the above $\mathbb{Z}$, are allowed. Of course, deciding whether $\mathbb{C}_{\mathrm{exp}}$ is an analytic geometry in some sense is an extremely difficult task. For example, the problem is connected to the following conjecture:

Conjecture ([Zil97])**.** *Is $\mathbb{C}_{\mathrm{exp}}$ quasi-minimal, i.e., is every definable subset of $\mathbb{C}$ either countable or co-countable?*

Note how this behaviour is analogous to the case of the pure field $\mathbb{C}$, which is strongly minimal, i.e., every definable subset of $\mathbb{C}$ is either finite or co-finite.

The behaviour of $\mathbb{C}_{\mathrm{exp}}$ is very much unknown, as we know very little of the algebraic behaviour of exp; for example, we do not know if e and π are algebraically independent. The algebra of exp plays however a crucial role also in model theory: for example, Macintyre and Wilkie proved that if a celebrated conjecture on the values of exp, Schanuel's Conjecture, holds on $\mathbb{R}$, then the first order theory of $\mathbb{R}_{\mathrm{exp}}$ is decidable.

Here the matter took a twist. Rather than studying $\mathbb{C}_{\mathrm{exp}}$ directly, Zilber showed that there is one structure similar to $\mathbb{C}_{\mathrm{exp}}$ that actually *is* quasi-minimal; and not by chance, this structure incorporates Schanuel's Conjecture. His theorem is even much stronger: there is a structure that can be axiomatised with one sentence in the infinitary language $\mathcal{L}_{\omega_1,\omega}(Q)$ which is uncountably categorical and has models of any infinite cardinality[1]. Categoricity in this language is a form of tameness, and in fact it has several model-theoretic consequences (e.g., it bounds the number of realised $\mathcal{L}_{\omega_1,\omega}$-types).

These structures were originally called pseudoexponential fields [Zil05b], but many people just call them Zilber fields. The most interesting Zilber field is the unique one of cardinality $2^{\aleph_0}$, and we will call it $\mathbb{B}_E$, where $\mathbb{B}$ is an algebraically closed field of characteristic 0 and E is a function on $\mathbb{B}$ with certain properties. Because of its uniqueness, Zilber conjectured that his $\mathbb{B}_E$ and the classical $\mathbb{C}_{\exp}$ are actually the same object, following the general idea that categorical structure should be natural ones.

However, this conjecture is a challenging one, as the very definition of $\mathbb{B}_E$ includes the rephrasing of Schanuel's Conjecture for the function E, and if we were able to prove that $\mathbb{C}_{\exp} \cong \mathbb{B}_E$, then Schanuel's Conjecture would follow as well. It is believed that the latter conjecture is at the moment out of reach, and that the solution is still quite far away. Moreover, the definition of $\mathbb{B}_E$ also requires an extra property that again is not known for $\mathbb{C}_{\exp}$.

Nevertheless, the new structure $\mathbb{B}_E$ is not an easy object, and it is quite difficult to see how it looks like. Moreover, even $\mathbb{B}_E$ is not known to be an analytic geometry. For these reasons, research is going on about finding more on $\mathbb{B}_E$, and showing similarities, and possibly differences, between $\mathbb{B}_E$ and $\mathbb{C}_{\exp}$, in the hope of catching some glimpses of the situation.

This thesis fits mostly in this line of research: what can we transfer from $\mathbb{C}_{\exp}$ to $\mathbb{B}_E$? Are we able to compare them, and either support the conjecture, or refute it?

Our main result is that one specific property of $\mathbb{C}_{\exp}$ does hold on $\mathbb{B}_E$: the existence of an involution, i.e., of an automorphism of order two, which in case of $\mathbb{C}_{\exp}$ is complex conjugation. Moreover, the involution we find on $\mathbb{B}_E$ have a fixed field that can be chosen quite arbitrarily, and it can be fixed to be exactly $\mathbb{R}$. This corrects a bit an asymmetry between $\mathbb{C}_{\exp}$ and $\mathbb{B}_E$: the only non-trivial automorphism we know on the former is complex conjugation, while the latter has plenty of automorphism; and now we know that there is also plenty of automorphism of order two. This answers a question of Zilber, Kirby, Macintyre, Onshuus and others [KMO12].

Theorem 3.36. *The Zilber field $\mathbb{B}_E$ of cardinality $2^{\aleph_0}$ has an involution whose fixed field is isomorphic to $\mathbb{R}$ with $\ker(E) = 2\pi i\mathbb{Z}$.*

Moreover, any separable real closed field of infinite transcendence degree occurs as the fixed field of a Zilber field of the same cardinality; in particular, every Zilber field of cardinality up to $2^{\aleph_0}$ has an involution.

Our starting point is a careful analysis of a general strategy for constructing exponential fields, and especially Zilber fields, already present in [Zil05b, Kir09]. Using this strategy, we construct the function E around a given field automorphism of order two, obtaining in the end a Zilber field that by construction has an involution. Moreover, we also study a few variations that yields different exponential fields with curious properties; for example, a real closed field with an order-preserving exponential function and a cosine such that certain system of equations are satisfied.

Our result would encourage the conjecture that $\mathbb{B}_E \cong \mathbb{C}_{\exp}$, and more so as the fixed field of the involution is exactly $\mathbb{R}$. Of course, we do not know if E is continuous with respect to the topology of $\mathbb{R}$, as it would essentially prove Schanuel's Conjecture. Actually, some obstructions

[1] The original proof of the theorem contained a flaw in the proof concerning the "excellence" of the sentence. A fix recently appeared in [BHH+12], where it is proved that the excellence condition is not necessary to obtain categoricity.

appear during the proof and force our involution to behave rather badly, so that the function E is not continuous with respect to the topology of $\mathbb{R}$. Hopefully, this is just an artefact of our construction.

Thesis outline

In chapter 1 we describe a framework used to study exponential fields, and give a short introduction to Zilber fields. We give their definition, together with some motivations for each of the axioms, a brief sketch of the proof of their categoricity, and some known facts that correspond to theorems of classical analysis on $\mathbb{C}_{\exp}$.

In chapter 2 we detail a general procedure to construct and extend exponential fields. We show that some properties are preserved across the extensions obtained by our procedure, and we concentrate especially on the Countable Closure Property. This results in an explicit proof that a large class of exponential fields can be embedded into Zilber fields, and that a procedure analogous to the one of [Kir09] produces Zilber fields.

In chapter 3 we adapt the general procedure to prove that on Zilber fields of cardinality up to $2^{\aleph_0}$ we can find automorphisms of order two whose fixed field, as a pure real closed field, can be fixed to be any uncountable separable real closed field of the same cardinality. The proof of the theorem requires a careful study of rotund varieties and of their Weil restriction of the scalars.

In chapter 4 we describe some other exponential fields that can be obtained using our procedure. We show that it is possible to find exponential fields with the Schanuel Property, cyclic kernel, and with automorphisms of order two where the exponential function is continuous, or where the exponential function is order-preserving on the real closed fixed field and certain system of equations are solved. The result is not in general a Zilber field, because we do not guarantee that enough systems of equations are satisfied. Moreover, with the use of some number theory, we show that there are existentially closed exponential fields with cyclic kernel whose underlying field is the field of algebraic numbers. In the latter example, the Schanuel Property does not hold, as every value of the exponential function is algebraic, and hence has transcendence degree 0.

Chapter 1

Zilber fields

As mentioned in the introduction, Zilber fields were first defined and axiomatized in [Zil05b], in a successful attempt to construct a “tame” structure out of something similar to $\mathbb{C}_{\exp}$; in particular, one that is uncountably categorical, provided that we use a powerful enough language.

In this chapter, we give a short description of a framework for exponential fields and Hrushovski amalgamation, essentially adapting from Zilber's and Kirby's works [Zil05b, Kir09], and we define Zilber fields in this framework.

1.1 Exponential fields

At a first glance, the classical notation $\mathbb{R}_{\exp}$ and $\mathbb{C}_{\exp}$ suggests to write K_E to denote the structure $(K, 0, 1, +, \cdot, E)$, where E is a unary function satisfying the following axiom.

(E) E is a homomorphism $E : (K, +) \to (K^\times, \cdot)$ (temporary definition).

However, this definition is too simple for our purposes, the main reason being that amalgamation is better done with fields where E is a partial function, but also because we want to be able to manage finitely generated structure.

Definition 1.1. A *partial exponential field*, or *partial E-field* for short, is a two-sorted structure

$$\langle \langle K; 0, 1, +, \cdot \rangle; \langle D; 0, +, (q\cdot)_{q\in\mathbb{Q}} \rangle; i : D \to K, E : D \to K \rangle$$

satisfying the axiom “(E-par)”:

$$\text{(E-par)} \quad \begin{array}{l} \langle D; 0, +, (q\cdot)_{q\in\mathbb{Q}} \rangle \text{ is a } \mathbb{Q}\text{-vector space;} \\ \langle K; 0, 1, +, \cdot \rangle \text{ is a field of characteristic } 0; \\ i : D \to K \text{ is an injective homomorphism from } \langle D, + \rangle \text{ to } \langle K, + \rangle; \\ E \text{ is a homomorphism from } \langle D, + \rangle \text{ to } \langle K^\times, \cdot \rangle. \end{array}$$

A *global E-field*, or just *E-field*, is a two sorted structure as above where the axiom (E) is satisfied:

(E) the axiom (E-par) holds, and i is surjective.

We denote (partial) E-fields with the notation K_E. Unless otherwise stated, *we identify the vector space D with its image in K*, leaving implicit the extra sort, except for the few situations where this generate ambiguities as the ones noted below.

Remark 1.2. The two-sorted definition is helpful when talking about substructures: an inclusion $K_E \subset K'_{E'}$ of structures means exactly that $K \subset K'$ is an inclusion of fields, and that $E \subset E'$ as sets, i.e., $E'_{\restriction \mathrm{dom}(E)} \equiv E$. For example, it is possible to have $K_E \subset K_{E'}$, with the function E' extending E without changing the same underlying field. (This would not apply if the partial function were obtained using a relational language.)

Definition 1.3. If X is a subset of K_E, we denote by $\langle X \rangle$ the substructure generated by X.

Remark 1.4. Please note that in general the structure generated by an $X \subset K$ would be the field $\mathbb{Q}(X)$ with a trivial exponential function whose domain is just $\{0\}$, even if $X \subset i(D)$. For this reason, we have to be careful about which sort X lives in, in order to define the correct structure. In this work, we will usually consider sets contained in D only.

Definition 1.5. If a partial E-field K_E is such that $K_E = \langle \mathrm{dom}(E) \rangle$, or in other words, if $K = \mathbb{Q}(i(\mathrm{dom}(E)), E(\mathrm{dom}(E)))$, then it is called *exponential-graph-generated* (as in [Kir09]).

We call $\mathcal{E}$ the elementary class of exponential-graph-generated partial E-fields.

We have now a minimum language to talk about exponential fields and Zilber fields. We recall that Zilber fields are meant to be a tame variant of $\mathbb{C}_{\exp}$.

In order for an E-field K_E to be a Zilber field, we want first a structure that, topological issues aside, has an exponential function describing the universal cover of the multiplicative group. Moreover, in order to obtain tameness, Zilber looked for an uncountably categorical, or at least a quasi-minimal structure, so he defined his fields as the product of a Hrushovski fusion. This turns out to be deeply related to the statement of Schanuel's Conjecture, and to a form of converse statement. As a final touch, a form of collapse is applied, and this guarantees both quasi-minimality and categoricity at once. This is detailed in the next sections.

1.2 Universal cover axioms

Since we want K_E to be similar in some way to $\mathbb{C}_{\exp}$, we want first to mimic one of the defining properties of exp: it is the universal cover of the multiplicative group of an algebraically closed field, and the covering space is identified with the additive group of the field itself. The universal cover of $\mathbb{C}^\times$ is described by the following exact sequence

$$0 \to (\mathbb{Z}, +) \to (\mathbb{C}, +) \xrightarrow{\exp} (\mathbb{C}^\times, \cdot) \to 1 \tag{1.1}$$

and we want the same to hold for K:

$$0 \to (\mathbb{Z}, +) \to (K, +) \xrightarrow{E} (K^\times, \cdot) \to 1. \tag{1.2}$$

Of course, the former sequence usually means also that exp is a continuous function, but since we have no topology on K, and the purpose of Zilber fields is to understand the algebraic behaviour independently of the topology, the latter sequence involves just pure group homomorphisms.

This is easily described by the following axioms:

(ACF_0) K is an algebraic closed field of characteristic 0;

(LOG) E is surjective (every element has a logarithm);

(STD) the kernel is a cyclic group, i.e., $\ker E = \omega\mathbb{Z}$ for some $\omega \in K^\times$.

A useful consequence of either (LOG) and of (STD) is that the image of E contains all the roots of unity. Mimicking [Zil05b], we say that an E-field with this property has "full kernel". Its role will become apparent later during amalgamation and in construction.

Definition 1.6. An E-field satisfying (ACF_0) is said to be an *EA-field.*
An E-field satisfying (LOG) is said to an *EL-field.*
An EA-field that is also an EL-field is said to be an *ELA-field.*
An E-field satisfying (STD) is said to have *standard kernel.*
An E-field containing all the roots of unity in the image of E is said to have *full kernel.*

These properties are evidently first-order axiomatizable, except for (STD); for that, we need the power of $\mathcal{L}_{\omega_1,\omega}$ in order to state that the formula that should define the integers actually defines the set $\mathbb{Z}$:

$$\forall x \left(\forall y \, (E(y) = 1 \to E(xy) = 1) \leftrightarrow \bigvee_{n \in \mathbb{Z}} x = n \right).$$

The abstract theory of the universal cover equation (1.2), where the covering space is *not* identified with the additive group, has been studied by Zilber [Zil06] in the first research stages leading to Zilber fields, and later fixed and extended to positive characteristic in [BZ11]. What was proved is that the two sorted structure (H, K), where H is a divisible, torsion-free abelian group, and K is an algebraically closed field, equipped with a function E such that

$$0 \to (\mathbb{Z}, +) \to (H, +) \xrightarrow{E} (K^\times, \cdot) \to 1, \tag{1.3}$$

has a unique isomorphism type for each uncountable K. Similarly to the case of Zilber fields, the structure is axiomatised by one sentence in $\mathcal{L}_{\omega_1,\omega}$, in order to capture the standard model of the theory of $(\mathbb{Z}, +)$, and that sentence is proven to be uncountably categorical (of course, provided we fix the characteristic of K). Further work has been done about axiomatizing the universal covers of elliptic curves and abelian varieties with analogous, but sometimes conjectural, results [Zil03, Gav12, Bay09].

1.3 Predimensions and the Schanuel Property

In order to obtain an uncountably categorical structure satisfying the above axioms, Zilber used a form of Hrushovski amalgamation with the purpose of looking at its universal models. The amalgamation is obtained using a non-negative predimension function. Let us recall what a predimension is.

Definition 1.7. Given a class $\mathcal{C}$ of finitely generated structures closed under substructure, a predimension is a function $\delta : \mathcal{C} \to \mathbb{R}_{>0} \cup \{0\}$ such that:

1. $\delta(\emptyset) = 0$;
2. for all $Z \in \mathcal{C}$, and for all X, Y substructures of Z, $\delta(\langle X \cup Y \rangle) \leq \delta(X) + \delta(Y) - \delta(X \cap Y)$ (submodularity).

When $X \subset Y$ is a subset of some structure $Y \in \mathcal{C}$, we write $\delta(X)$ to denote $\delta(\langle X \rangle)$.

In the class $\mathcal{E}$ of E-fields, the work of Zilber shows that an effective predimension is given by

$$\delta(\langle z_1, \ldots, z_n \rangle) := \mathrm{tr.deg.}(i(z_1), \ldots, i(z_n), E(z_1), \ldots, E(z_n)) - \mathrm{lin.d.}_{\mathbb{Q}}(z_1, \ldots, z_n)$$

on finitely generated structures.

It is easy to check that δ is indeed submodular. The non-negativity of this predimension function, on the other hand, holds only on a certain subclass of E-fields. Given an E-field $K_E \in \mathcal{E}$, the fact that $\delta(X) \geq 0$ holds for all its finitely generated substructures X is equivalent to the following statement.

(SP) *Schanuel Property*: for every finite tuple $\overline{z} = (z_1, \ldots, z_n) \in \mathrm{dom}(E)^n$ of $\mathbb{Q}$-linearly independent elements,

$$\mathrm{tr.deg.}_{\mathbb{Q}}(i(z_1), \ldots, i(z_n), E(z_1), \ldots, E(z_n)) \geq n.$$

We do the amalgamation on the subclass the partial E-fields where (SP) holds; therefore, our resulting K_E will have to satisfy (SP) as well. We then take this statement as one of the axioms defining K_E.

The axiom (SP) is also motivated by the following long standing conjecture, which is just the reformulation of the axiom for $\mathbb{C}_{\exp}$.

Conjecture 1.8 (Schanuel, [Lan67]). *For every finite tuple $(z_1, \ldots, z_n) \in \mathbb{C}^n$ of $\mathbb{Q}$-linearly independent elements,*

$$\mathrm{tr.deg.}(z_1, \ldots, z_n, \exp(z_1), \ldots, \exp(z_n)) \geq n.$$

This conjecture was formulated as a generalisation of some statements about the transcendence of the values of the exponential function, and it would provide an answer to essentially all the transcendence questions about numbers generated using the exponential function, the logarithm and the field operations (see [Lan67]).

This conjecture, however, is today considered out of reach for the current methods. Just to give an idea of our present knowledge, here is a partial list of the known unconditional results on the transcendence of the values of exp. All of them are implied by Schanuel's Conjecture, and as such, they also hold in any E-field satisfying (SP).

Theorem 1.9 (Hermite-Lindemann-Weierstrass, [Her73, vL82, Wei85]). *For every finite number of elements $z_1, \ldots, z_n \in \overline{\mathbb{Q}}$ that are $\mathbb{Q}$-linearly independent, the values $\exp(z_1), \ldots, \exp(z_n)$ are algebraically independent.*

Theorem 1.10 (Gelfond-Schneider, [Gel34, Sch34]). *If $\alpha, \beta \in \overline{\mathbb{Q}}$, with $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$, then any determination of α^β is transcendental.*

Theorem 1.11 (Six exponentials theorem, [Lan67, Ram67]). *If $z_1, z_2, z_3 \in \mathbb{C}$ are $\mathbb{Q}$-linearly independent, and if $y_1, y_2 \in \mathbb{C}$ are also $\mathbb{Q}$-linearly independent, then at least one of*

$$\exp(z_1 y_1), \exp(z_2 y_1), \exp(z_3 y_1), \exp(z_1 y_2), \exp(z_2 y_2), \exp(z_3 y_2)$$

is transcendental.

Theorem 1.12 (Five exponentials theorem, [Wal88]). *If $z_1, z_2 \in \mathbb{C}$ are $\mathbb{Q}$-linearly independent, $y_1, y_2 \in \mathbb{C}$ are also $\mathbb{Q}$-linearly independent, and γ is a non-zero algebraic number, then at least one of*

$$\exp(z_1 y_1), \exp(z_2 y_1), \exp(z_1 y_2), \exp(z_2 y_2), \exp\left(\gamma \frac{z_2}{z_1}\right)$$

is transcendental.

Theorem 1.13 (Nesterenko, [Nes96]). *The numbers π and $\exp(\pi)$ are algebraically independent.*

Given the function δ, and the condition $\delta(X) \geq 0$, we can start to say something about amalgamating E-fields. We therefore restrict our class $\mathcal{E}$ to the subclass all partial E-fields satisfying (SP). We call this new subclass $\mathcal{E}^0$.

We recall that any δ yields a *relative* predimension defined as

$$\delta(A/B) := \delta(A \cup B) - \delta(B).$$

In this case, it can be calculated as

$$\delta(A/B) = \text{tr.deg.}(i(A), i(B), E(A), E(B)/i(B), E(B)) - \text{lin.d.}_{\mathbb{Q}}(A/B).$$

The latter formula makes sense also when B is not finitely generated, but A is finitely generated over B; therefore, we will use it as the definition of $\delta(A/B)$.

Note that unlike the case of dimensions like the transcendence degree, the function $\delta(A/B)$ can well be negative, even if $\delta(X)$ is always non-negative. If $\delta(A/B) \geq 0$ for any finitely generated A, then we say that B is *strongly embedded* into the bigger structure. Formally:

Definition 1.14. Given two partial E-fields $K_E, K'_{E'}$ and an embedding $j : K_E \hookrightarrow K'_{E'}$ (possibly the identity), we say that K_E is *strongly embedded* in $K'_{E'}$, or $K_E \leq K'_{E'}$, if $\delta(X/j(\text{dom}(E))) \geq 0$ for all finite subset $X \subset \text{dom}(E')$.

If X, Y are two subsets of $\text{dom}(E)$ for some K_E, with $X \subset Y$, we say that $X \leq Y$ if $K_{E\restriction \text{span}_{\mathbb{Q}}(X)} \leq K_{E\restriction \text{span}_{\mathbb{Q}}(Y)}$; equivalently, if $\langle X \rangle \leq \langle Y \rangle$.

With this relation of strong embedding, we start doing an amalgamation on the category $(\mathcal{E}^0_{\text{std}}, \leq)$, where $\mathcal{E}^0_{\text{std}}$ is the subclass of $\mathcal{E}^0$ of the partial E-fields satisfying (STD).

1.4 Richness

If we consider the category $(\mathcal{E}^0_{\text{std}} \cap \mathcal{E}_{\text{fin}}, \leq)$, where $\mathcal{E}_{\text{fin}}$ is the class of finitely generated partial E-fields which are exponential-graph-generated, it turns out that the class satisfies the Joint-Embedding Property and the Amalgamation Property of Fraïssé's Limit Theorem restricted to strong embeddings, as in [Hru93]. Moreover, again thanks to [Zil06, Thm. 2], the number of isomorphism types is countable. Hence we can find a unique generic partial E-field $\mathbb{F}_E$ of cardinality $\aleph_0$, the direct limit of the above category, usually called the Hrushovski-Fraïssé limit, whose strong exponential-graph-generated and finitely generated partial E-subfields represent all the isomorphism types of $\mathcal{E}^0_{\text{std}} \cap \mathcal{E}_{\text{fin}}$, and satisfying the following "richness" property.

Definition 1.15. A partial E-field $F_E \in \mathcal{E}^0_{\text{std}}$ is *rich* if given any two $K_{E_0}, L_{E_1} \in \mathcal{E}^0_{\text{std}} \cap \mathcal{E}_{\text{fin}}$, and any two strong embeddings $j : K_{E_0} \hookrightarrow L_{E_1}$, $h : K_{E_0} \hookrightarrow F_E$, then there is a strong embedding $g : L_{E_1} \hookrightarrow F_E$ such that $g \circ h = j$.

$$\begin{tikzcd} K_{E_0} \arrow[r, "\leq", "h"'] \arrow[d, "\leq"', "j"] & F_E \\ L_{E_1} \arrow[ur, dashed, "g", "\leq"'] & \end{tikzcd}$$

To prove the existence and the uniqueness of the countable generic model, a crucial result is played by the so called "Thumbtack Lemma" [Zil06, Thm. 2]. We give the statement for a subcase which is sufficient for our purposes.

Definition 1.16. Given a number α in some algebraically closed field of characteristic zero, a *coherent system of roots*, or a *division system*, of α is a sequence $(\alpha^{1/q})_{q\in\mathbb{N}^*}$ such that $(\alpha^{1/q})^q = \alpha$ for all $q \in \mathbb{N}^*$, and $(\alpha^{1/pq})^p = \alpha^{1/q}$ for all $p, q \in \mathbb{N}^*$.

Lemma 1.17 (Thumbtack Lemma). *Let K be a finitely generated extension of $\mathbb{Q}$. Let $a_1, \dots, a_r$ be numbers in some algebraically closed field containing K, and $(a_j^{1/q})_q$ be coherent system of roots for each of them.*

Let L be the field generated by K, all the roots of unity, and all the elements $a_j^{1/q}$.

If $b_1, \dots, b_l$ are numbers in some extension of L that are multiplicatively independent modulo L, there is an $m \in \mathbb{N}^\times$ such that for any coherent systems of roots $(b_j^{1/q})_q$, the isomorphism type of the sequence $(b_1^{1/q}, \dots, b_l^{1/q})_{q\in\mathbb{N}^\times}$ over L (i.e., its quantifier-free type over L in the field language) is determined by the isomorphism type of $(b_1^{1/m}, \dots, b_l^{1/m})$ over L.

Remark 1.18. In order to show the kind of problem the Thumbtack Lemma addresses, and to explain the hypothesis of multiplicative independence, it is sufficient to look at the following example.

Let $b_1 = b_2 = t$ be some transcendental number over L. We fix an arbitrary coherent system of roots $b_1^{1/q} = t^{1/q}$ for b_1. For b_2, for any $n > 0$, we may fix $b_2^{1/q} = b_1^{1/q} = t^{1/q}$ for $q \leq n$, and for example extend it so that $b_2^{1/n^2} = \zeta_{n^2}^n t^{1/n^2} \neq b_1^{1/n^2}$. Therefore, $(b_1^{1/n}, b_1^{1/n})$ and $(b_1^{1/n}, b_2^{1/n})$ have the same isomorphism type over L, but the sequences $(b_1^{1/q}, b_1^{1/q})_{q\in\mathbb{N}^\times}$ and $(b_1^{1/q}, b_2^{1/q})_{q\in\mathbb{N}^\times}$ do not. This shows that there is no m as in lemma 1.17 if b_1, b_2 are not multiplicatively independent.

Moreover, it may be used to show that if $b_1, \dots, b_l$ are *not* multiplicatively independent, then there are $2^{\aleph_0}$ possible isomorphism types for the sequence $(b_1^{1/q}, \dots, b_l^{1/q})_{q\in\mathbb{N}^\times}$ (indeed, they correspond to points in some cartesian power of $\hat{\mathbb{Z}}$). On the other hand, lemma 1.17 implies that when $b_1, \dots, b_l$ are multiplicatively independent over L, the isomorphism types are only finitely many.

Corollary 1.19. *Let K_E be a finitely generated partial E-field with full kernel and $b_1, \dots, b_l$ be multiplicatively independent elements over K.*

Then there is an $m \in \mathbb{N}^\times$ such that the isomorphism type of any coherent $(b_1^{1/q}, \dots, b_l^{1/q})_{q\in\mathbb{N}^\times}$ over K is determined by the isomorphism type of $(b_1^{1/m}, \dots, b_l^{1/m})$.

Proof. Let $z_1, \dots, z_n$ be a $\mathbb{Q}$-linear base of $\operatorname{dom}(E)$, and let $w_1, \dots, w_s$ be some generators of K over $\mathbb{Q}(i(\operatorname{dom}(E)), E(\operatorname{dom}(E)))$. Let K_0 be the field generated by $i(z_1), \dots, i(z_n), w_1, \dots, w_s$.

Therefore, the field K is generated by K_0, by the roots of unity, and by $E(\frac{1}{q}z_1), \dots, E(\frac{1}{q}z_n)$ for $q \in \mathbb{N}^\times$. The conclusion now follows trivially from lemma 1.17. $\square$

Proposition 1.20. *There exists a unique countable rich $\mathbb{F}_E \in \mathcal{E}^0_{\text{std}}$ up to isomorphism.*

Proof. It is sufficient to show, by [Hru93], that the class $(\mathcal{E}^0_{\text{std}} \cap \mathcal{E}_{\text{fin}}, \leq)$ has the joint-embedding property, the amalgamation property, and countably many isomorphism types.

To verify amalgamation, take an amalgamation problem

$$\begin{tikzcd} & L_{E_1} \\ K_{E_0} \arrow[ur, "\leq", "h"'] \arrow[dr, "j", "\leq"'] & \\ & N_{E_2} \end{tikzcd}$$

First of all, we may assume that K_{E_0} is a maximal strong common subextension of L_{E_1} and N_{E_2}. In this case, we claim that for any $\alpha \in \mathrm{acl}(K) \cap L$, if α is in the domain or the image of E_1, then for any embedding of α into N over K, α is not in the domain, resp. the image, of E_2.

Indeed, if there is an embedding of α into N over K such that α is both in $\mathrm{dom}(E_1)$ and $\mathrm{dom}(E_2)$, then $E_1(\alpha)$ and $E_2(\alpha)$ are both transcendental over K, hence the E-subfields generated by K and α (as an element of $\mathrm{dom}(E_1)$ and $\mathrm{dom}(E_2)$) in L_{E_1} and N_{E_2} are isomorphic, and they must be both strong in L_{E_1} and N_{E_2}, against the assumption of maximality.

If instead $\alpha = E_1(\beta)$ for some $\beta \in \mathrm{dom}(E_1)$, by corollary 1.19 there is an $m \in \mathbb{N}^\times$ such that field-theoretic isomorphism type of $(E_1(\frac{1}{q}\beta))_{q\in\mathbb{N}^\times}$ over K is determined by the isomorphism type of $E_1(\frac{1}{m}\beta)$ over K. Now, if $E_1(\beta)$ is embedded into N over K, such in a way that $E_1(\beta) = E_2(\beta')$ for some $\beta' \in \mathrm{dom}(E_2)$, then $E_1(\frac{1}{m}\beta) = E_2(\frac{1}{m}\beta' + \frac{k}{m}\omega)$ for some $k \in \mathbb{N}$ and some ω such that $E(\omega) = 1$. Therefore, the E-subfields generated by K and β in L_{E_1}, and by K and $\beta' + k\omega$ in N_{E_2}, are isomorphic. As they are both strong in L_{E_1} and N_{E_2}, this contradicts again the maximality of K_{E_0}.

It is now sufficient to take an amalgam (as fields) F of L and N over K such that L and N are linearly disjoint over $\mathrm{acl}(K) \cap L \cap N$, and $F = L \cdot N$. By the above argument, the images in F of $\mathrm{dom}(E_1)$ and of $\mathrm{dom}(E_2)$ intersect only in $\mathrm{dom}(E_0)$, hence we may define (uniquely) a new exponential function E_3 on $\mathrm{dom}(E_1) + \mathrm{dom}(E_2)$ that extends both E_1 and E_2.

Moreover, since the intersection of the images is just $\mathrm{im}(E_0)$ as well, the kernel of E_3 is still $\omega\mathbb{Z}$. As F_{E_3} is clearly finitely-generated and exponential-graph-generated, it is in $\mathcal{E}^0_{\mathrm{std}} \cap \mathcal{E}_{\mathrm{fin}}$.

To verify the joint embedding property, it is sufficient to note that for any $K_E \in \mathcal{E}^0_{\mathrm{std}}$, the E-subfield generated by ω, where ω is a generator of the kernel, has a unique isomorphism type, and it is strongly embedded in K_E. Therefore, given two E-field in $\mathcal{E}^0_{\mathrm{std}} \cap \mathcal{E}_{\mathrm{fin}}$, it is sufficient to amalgamate them over $\langle\omega\rangle$.

To count the isomorphism types, consider a finitely generated partial E-field with standard kernel which is exponential-graph-generated K_E. Let $\omega, z_1, \ldots, z_n$ be a $\mathbb{Q}$-linear base of $\mathrm{dom}(E)$, with ω a generator of the kernel. Then the isomorphism type of K_E is determined by the field-theoretic isomorphism type of $K_0 := \mathbb{Q}(i(\omega), i(z_1), \ldots, i(z_n))$, that has countably many possibilities, by the isomorphism type of $K_1 := K_0(E(\frac{1}{q}\omega)_{q\in\mathbb{N}^\times})$ over K_0, which are finitely many since its Galois group permutes all the possible choices for $E(\frac{1}{dq}\omega)$, where d is the maximum (finite) integer such that $\zeta_d \in K_0$, and by the field-theoretic isomorphism type of $E(\frac{1}{q}z_1), \ldots, E(\frac{1}{q}z_n)$, for q varying in $\mathbb{N}^\times$, over K_1. But $E(z_1), \ldots, E(z_n)$ are multiplicatively independent over this field, hence their isomorphism type is determined by the isomorphism type of $E(\frac{1}{m}z_1), \ldots, E(\frac{1}{m}z_n)$ for some fixed m. Therefore there are only countably many isomorphism types.

By (AP) and (JEP), and by the fact that there are only countably many isomorphism types, there exists a unique (countable) direct limit $\mathbb{F}_E$, the Hrushovski-Fraïssé limit. □

It is not difficult to see that the richness of $\mathbb{F}_E$ implies that $\mathbb{F}$ is algebraically closed, that E is defined everywhere and that it is surjective. This provides further motivation for the axioms presented in the previous section.

Proposition 1.21. *If $F_E \in \mathcal{E}^0_{\mathrm{std}}$ is rich, then it satisfies (ACF$_0$), (E) and (LOG).*

Proof. Let K_{E_0} be a finitely generated, exponential-graph-generated subfield of F. By (SP), we can find another finitely generated, exponential-graph-generated E-subfield $K'_{E'} \subset F_E$ containing K such that $\delta(K'_{E'}) = \delta(\mathrm{dom}(E'))$ is minimal among all the possible extensions of K_E. Moreover, we may assume that $K'_{E'}$ contains $\ker(E)$. Therefore, $K'_{E'}$ is strongly embedded in F_E, because for any finite $X \subset \mathrm{dom}(E)$,

$$\delta(X/K'_{E'}) = \delta(\langle X, \mathrm{dom}(E')\rangle) - \delta(K'_{E'}) \geq 0.$$

Let α be an element of the algebraic closure of F (possibly already in F). There must be a finitely generated subfield of F such that α is algebraic on it; but since F_E is exponential-graph-generated, we may assume that there is a $K_{E_0} \subset F_E$ which is exponential-graph-generated and finitely generated such that α is algebraic on K; if $\alpha \in F$, we may assume that $\alpha \in K$ as well. By the above argument, we may assume that $K_{E_0} \leq F_E$ as well.

Let $L := \bigcup_n K(\alpha, t^{1/n})$ be the field obtained by adjoining to K the element α and a new transcendental element t (not in F) together with a coherent choice of nth roots, and let $D' := \mathrm{dom}(E_0) \oplus \langle a \rangle$ be the $\mathbb{Q}$-vector space obtained by adjoining a new $\mathbb{Q}$-linearly independent element to $\mathrm{dom}(E_0)$.

We can extend the partial E-field K_{E_0} to an E-field L_{E_1} by enlarging the domain of E_0 to D', identifying a with α, and defining $E_1 : D' \to L^\times$ as $E_1(x + \frac{p}{q}a) := E_0(x) \cdot t^{p/q}$ for $x \in \mathrm{dom}(E), p \in \mathbb{Z}, q \in \mathbb{N}^*$; note that L_{E_1} is finitely generated and exponential-graph-generated. The inclusion $K_{E_0} \hookrightarrow L_{E_1}$ is a strong embedding, and therefore there must be a strong embedding of L_{E_1} into F_E which is the identity on K_{E_0}. But this implies that $\alpha \in i(\mathrm{dom}(E))$, and in particular, $K(\alpha) \subset i(\mathrm{dom}(E))$. This implies that F is algebraically closed, and that the function i is surjective, so that (E) holds, i.e., F_E is a global E-field.

Similarly, to prove (LOG), we may define $L := \bigcup_n K(t, \alpha^{1/n})$, and L_{E_1} by identifying a with t, and defining $E_1(x + \frac{p}{q}a) := E_0(x) \cdot \alpha^{p/q}$. Again the inclusion $K_{E_0} \hookrightarrow L_{E_1}$ is a strong embedding, and implies that L_{E_1} has a strong embedding to F_E as well, whose restriction to K_{E_0} is the identity. Therefore, $\alpha \in \mathrm{im}(E)$, and in particular $F^\times \subset \mathrm{im}(E)$. The function E is then surjective over $F^\times$, so that (LOG) holds. □

The converse does not hold: (ACF_0), (E) and (LOG) do not imply that an E-field F_E rich. However, Zilber showed that it is possible to give an explicit description of richness by adding two extra conditions.

The first one is that F_E must have "infinite dimension".

Definition 1.22. A (global) *ELA*-field F_E has *infinite dimension* if

(ID) *Infinite dimension*: For all positive integers $n \in \mathbb{N}$, there is a strong $K_{E'} \leq F_E$ such that $\delta(K_{E'}) \geq n$.

The general definition of dimension will be given later in section 1.7.1.

Proposition 1.23. *If $F_E \in \mathcal{E}^0_{\mathrm{std}}$ is rich, then it satisfies (ID).*

Proof. It is sufficient to construct a partial E-field in $\mathcal{E}^0_{\mathrm{std}}$ with the desired property.

Let $K := \bigcup_{k=1}^\infty \mathbb{Q}(t_1, \ldots, t_n, s_1^{1/k}, \ldots, s_n^{1/k})$ be the field generated by $2n$ algebraically independent elements and the coherent roots of n of them (i.e., such that $(s_j^{1/km}) = s_j^{1/k}$). Let $D := \mathbb{Q}^n$ be the $\mathbb{Q}$-vector space of dimension n with base $b_1, \ldots, b_n$. We define $i(b_j) = t_j$ and $E'(\frac{p}{q}b_j) = s_j^{p/q}$, for $j = 1, \ldots, n$ and $p \in \mathbb{Z}, q \in \mathbb{N}^*$.

The exponential field $K_{E'}$ is in $\mathcal{E}^0_{\mathrm{std}}$ and satisfies $\delta(K_{E'}) = n$. However, the exponential field L_E, where L is the field generated by the roots of unity and one transcendental element t, and E_0 is the function that sends $t^{p/q}$ to ζ_q^p, with $(\zeta_q)_q$ is a coherent system of roots of 1, has a strong embedding to $K_{E'}$ and to F_E. Because of richness, there is a strong embedding of $K_{E'}$ into F_E. Since n is arbitrary, then F_E has infinite dimension, i.e., it satisfies (ID). □

The last remaining condition that yields a complete description of rich E-fields has a quite substantial technical content.

We state it now, but without explaining the meaning of the terms. We postpone all the necessary definitions until section 1.6; for now, we will just say that an "absolutely free rotund variety" is essentially a system of polynomial equations in some variables and their exponentials, with the restriction that the exponential function is iterated only once, having a solution in some strong extension of the field of definition of the system.

(SEC) *Strong Exponential-algebraic Closure*: for every absolutely free rotund variety $V \subset \mathbb{G}^n$ over K, and every finite tuple $\overline{c} \in K^{<\omega}$ such that V is E-defined over $\overline{c}$, $V(\overline{c})$ has a generic solution $\overline{z} \in K^n$.

Along with the definitions, we will also prove that (SEC) is indeed satisfied in rich E-fields, and that it is the last piece to characterise richness.

Proposition 1.24. *If $F_E \in \mathcal{E}^0_{\mathrm{std}}$ is rich, then it satisfies (SEC).*

Proposition 1.25. *If $F_E \in \mathcal{E}^0_{\mathrm{std}}$ satisfies (ACF$_0$), (E), (LOG), (STD), (ID) and (SEC), then it is rich.*

Proposition 1.26.

The proofs can be found in section 1.6.

It is interesting to note that if $\mathbb{C}_{\exp}$ were rich, then the following "converse" Schanuel's conjecture would hold, and indeed the statement of richness is similar, although a bit stronger.

Conjecture 1.27 (Converse Schanuel, [Wil02])**.** *Let F_E be a countable E-field satisfying (SP) and (STD). Then there is a field embedding $h : F \to \mathbb{C}$ such that $h(E(x)) = \exp(h(x))$ for all $x \in F$.*

Note that this conjecture partially overlaps with conjecture 1.8; for example, it would also imply that e and π are algebraically independent.

It is easy to see that a rich countable E-field with (SP) and (STD) must satisfy the statement of the Converse Schanuel's Conjecture. A full explicit proof of a stronger statement of this kind will be given in the next chapters.

The uniqueness of the above generic model $\mathbb{F}_E$ suggests to add (SEC) and (ID) to the axioms defining Zilber fields. Regarding (ID), it will turn out to be optional: the last axiom described in the next section implies (ID) in the uncountable case. The theory without (ID) is still uncountably categorical, but has several models of cardinality $\aleph_0$. In some papers, (ID) is added to the definition in order to have $\aleph_0$-categoricity, but in this work we do not assume (ID), as many of the results hold also for the countable models not satisfying (ID).

We call $\mathcal{EC}^0_{\mathrm{std}} \subset \mathcal{E}^0_{\mathrm{std}}$ the subclass satisfying (SEC).

1.5 A bound on richness

While the above axioms have only one countable model of infinite dimension, it is much more difficult to obtain something similar for larger cardinalities.

In particular, the axiom (SEC) shows that the number of solutions of a rotund variety must be at least countable, and it could happen that in some different, slightly saturated extensions, the same variety has a different number of solutions, yielding non-isomorphic models. Moreover, a model where certain kinds of variety have more than countably many solutions is not quasi-minimal.

In order to obtain a categorical sentence, a bound on the number of solutions is needed. In this case, it takes the following form.

(CCP) *Countable Closure Property*: for every absolutely free rotund variety $V \subset \mathbb{G}^n$ over K of depth 0, and every finite tuple $\overline{c} \in K^{<\omega}$ such that V is defined over $\overline{c}$, the set of the generic solutions of $V(\overline{c})$ is at most countable.

This property already appears in the original work of Shelah [She83] in a much more general context, and is reelaborated in [Zil05a] for "quasi-minimal excellent classes"; more details can be found in section 1.7.1. It is shown that this is an essential condition to obtain a categorical theory. In the case of $\mathbb{C}_{\exp}$, the generic solutions of such a variety V must lie on a discrete set, by Ax's theorem, hence (CCP) hold on $\mathbb{C}_{\exp}$ as well, giving even stronger motivation for this axiom. Informally speaking, this can be considered as a form of collapse.

Theorem 1.28 (Zilber, [Zil05b, Lemma 5.12])**.** *The exponential field $\mathbb{C}_{\exp}$ satisfies (CCP).*[1]

This axiom can be formulated using an extra quantifier Q meaning "there exist uncountably many".

The above seven axioms define what a Zilber field is, and they can be subsumed into one single formula Ψ is the infinitary language $\mathcal{L}_{\omega_1,\omega}(Q)$.

Definition 1.29. A structure K_E is a *Zilber field* if it satisfies (ACF_0), (E), (LOG), (STD), (SP), (SEC) and (CCP), or in other words, if $K_E \models \Psi$.

In contrast, we only know that $\mathbb{C}_{\exp}$ satisfies (ACF_0), (E), (LOG), (STD) and (CCP), and only some very restricted instances of (SP) and (SEC).

By Zilber's theorem [Zil05b], the sentence Ψ is uncountably categorical.

Theorem 1.30 (Zilber, [Zil05b])**.** *The sentence Ψ has models of any cardinality, and is uncountably categorical: any two models of Ψ of the same uncountable cardinality are isomorphic. Hence, there is a unique Zilber field, up to isomorphism, of any uncountable cardinality.*

The unique Zilber field of cardinality $2^{\aleph_0}$ is usually called $\mathbb{B}$, $\mathbb{B}_E$ or $\mathbb{B}_{\mathrm{ex}}$. By reason of its uniqueness, Zilber conjectured that this field is just isomorphic to $\mathbb{C}_{\exp}$. Moreover, this conjecture would also imply that $\mathbb{C}_{\exp}$ is quasi-minimal, as $\mathbb{B}_E$ is.

Theorem 1.31 (Zilber, [Zil05b])**.** *$\mathbb{B}_E$ is quasi-minimal, i.e., every definable set is either countable or co-countable.*

1.6 Absolutely free rotund varieties

When defining (SEC) and (CCP), we skipped the definition of "absolutely free rotund" variety. We explain it here, and we introduce also most of the notation that will be used in the next chapters.

Let us take some notation from Diophantine geometry: abstracting from the ground field, we denote by $\mathbb{G}_a$ the additive group, by $\mathbb{G}_m$ the multiplicative group and by $\mathbb{G}$ the product $\mathbb{G}_a \times \mathbb{G}_m$. The product operation of the last group will be denoted by $\oplus$. In more concrete words, over a given field K, $\mathbb{G}_a(K)$ is just $(K, +)$, $\mathbb{G}_m(K)$ is $(K^\times, \cdot)$, and $\mathbb{G}(K)$ is the direct product of the former ones. The group $\mathbb{G}$ is a natural environment where to look at points of the form $(z, E(z)) \in \mathbb{G}_a \times \mathbb{G}_m(K) = \mathbb{G}(K)$. Note that the group law is such that $(z, E(z)) \oplus (w, E(w))$ is just $(z + w, E(z + w))$.

[1]As mentioned in the introduction, the original proof contained a flaw that was fixed in [BHH+12].

As any abelian group, $\mathbb{G}$ has an unsurprising natural structure of $\mathbb{Z}$-module:

$$\begin{array}{rcl} (\cdot) : \mathbb{Z} \times \mathbb{G} & \to & \mathbb{G} \\ m \cdot (z, w) & \mapsto & (m \cdot z, w^m). \end{array}$$

The action can be naturally generalised to matrices with integer coefficients. Given a matrix $M \in \mathcal{M}_{k,n}(\mathbb{Z})$ of the form $M = (m_{i,j})_{1 \leq i \leq k, 1 \leq j \leq n}$, the explicit action can be written as

$$\begin{array}{rcl} (\cdot) : \mathcal{M}_{k,n}(\mathbb{Z}) \times \mathbb{G}^n & \to & \mathbb{G}^k \\ M \cdot (z_j, w_j)_{1 \leq j \leq n} & \mapsto & \left(\sum_{j=1}^n m_{i,j} z_j, \prod_{j=1}^n w_j^{m_{i,j}} \right)_{1 \leq i \leq k} . \end{array}$$

In several situations, we will abbreviate the multiplication by the scalar m, i.e., "$(m\mathrm{Id}) \cdot (z_j, w_j)$", with the expression $m \cdot (z_j, w_j)$.

For the sake of readability, we introduce a special notation for the elements of $\mathbb{G}^n$ and for the function E.

Notation 1.32. For any positive integer number n, and for any two given vectors $\overline{z} = (z_1, \ldots, z_n) \in K^n$ and $\overline{w} = (w_1, \ldots, w_n) \in (K^\times)^n$, we denote by $\langle \overline{z}; \overline{w} \rangle$ the 'interleaved' vector

$$\langle \overline{z}; \overline{w} \rangle := ((z_1, w_1), \ldots, (z_n, w_n)) \in \mathbb{G}^n(K).$$

If $\overline{z} = (z_1, \ldots, z_n) \in \mathrm{dom}(E)^n$, we write $E(\overline{z})$ to denote $(E(z_1), \ldots, E(z_n)) \in (K^\times)^n$. If $\overline{z} \in K^n$, but some components are not contained in $\mathrm{dom}(E)$, we still write $E(\overline{z})$ to denote the set of the images of the components of $\overline{z}$ in $\mathrm{dom}(E)$ (in this case, a pure set with less than n elements).

With this notation, whenever $\overline{z} \subset \mathrm{dom}(E)$, the following equation holds

$$M \cdot \langle \overline{z}; E(\overline{z}) \rangle = \langle M \cdot \overline{z}; E(M \cdot \overline{z}) \rangle,$$

where $M \cdot \overline{z}$ is now just the usual action by matrices.

The action by matrices is useful when manipulating points of the form $(z_j, E(z_j))_j \in \mathbb{G}^n(K)$. Indeed, suppose that $K_E \leq K'_{E'}$ is a strong extension with $\mathrm{dom}(E')$ finite dimensional over $\mathrm{dom}(E)$. Given a basis $\{z_j\}_{1 \leq j \leq n}$ of $\mathrm{dom}(E')$ over $\mathrm{dom}(E)$, let V be the minimum algebraic variety over $\mathbb{Q}(\mathrm{dom}(E), \mathrm{im}(E))$ containing $(z_j, E(z_j))_j \in \mathbb{G}^n(K')$. It can be verified that V must have large dimension, as the point itself must be quite transcendental because of $K_E \leq K'_{E'}$. A similar statement must hold for $M \cdot (z_j, E(z_j))_j$ for any integer matrix M. The variety itself has actually a special shape that we call "rotund".

Definition 1.33. An irreducible subvariety V of $\mathbb{G}^n$, for some positive integer n, is *rotund* if for all $M \in \mathcal{M}_{n,n}(\mathbb{Z})$ the following inequality holds:

$$\dim M \cdot V \geq \mathrm{rank} M.$$

In the original conventions of [Zil05b], a rotund variety is called "ex-normal", or just "normal", reusing a terminology common with other amalgamation constructions. However, we prefer here the convention of [Kir09] not to risk confusion with the term "normal" from algebraic geometry.

Note that in this definition we do not specify the base field over which V is irreducible; it can happen that V is irreducible, but that it splits into finitely many subvarieties when enlarging the field of definition. The absolutely irreducible components of a rotund variety, i.e., the ones irreducible over the algebraic closure, are evidently still rotund.

Proposition 1.34. *Let $K_E \subset L_{E'}$ be an extension of partial E-fields such that* $\mathrm{dom}(E') = \mathrm{dom}(E) \oplus \mathbb{Q}z_1 \oplus \cdots \oplus \mathbb{Q}z_n$.

Let $V \subset \mathbb{G}^n$ be the smallest variety defined over $\mathrm{dom}(E), \mathrm{im}(E)$ *such that*

$$\langle \overline{z}; E(\overline{z})\rangle = ((z_1, E(z_1)), \ldots, (z_n, E(z_n))) \in V.$$

Then the extension is strong if and only if V is rotund.

Proof. First of all, note that if $\overline{z} = (z_1, \ldots, z_n)$, for every matrix $M \in \mathcal{M}_{n,n}(\mathbb{Z})$,

$$\mathrm{lin.d.}_{\mathbb{Q}}(M \cdot \overline{z}/\mathrm{dom}(E)) = \mathrm{rank} M.$$

Moreover, the smallest variety defined over $\mathrm{dom}(E), \mathrm{im}(E)$ containing $\langle M \cdot \overline{z}; E(M \cdot \overline{z})\rangle$, which is just $M \cdot \langle \overline{z}; E(\overline{z})\rangle$, is exactly $M \cdot V$.

If the extension is strong, i.e., $K_E \leq L_{E'}$, we have that

$$\mathrm{tr.deg.}(M \cdot \overline{z}, E(M \cdot \overline{z})/\mathrm{dom}(E), \mathrm{im}(E)) \geq \mathrm{lin.d.}_{\mathbb{Q}}(M \cdot \overline{z}/\mathrm{dom}(E)) = \mathrm{rank} M.$$

In particular,

$$\dim M \cdot V \geq \mathrm{rank} M.$$

Conversely, if the variety is rotund, we must have that

$$\mathrm{tr.deg.}(M \cdot \overline{z}, E(M \cdot \overline{z})/\mathrm{dom}(E), \mathrm{im}(E)) \geq \mathrm{lin.d.}_{\mathbb{Q}}(M \cdot \overline{z}/\mathrm{dom}(E)) = \mathrm{rank} M.$$

This obviously holds for matrices in $\mathcal{M}_{n,n}(\mathbb{Q})$ as well (just multiply by a common denominator to get integer coefficients). This implies that for any tuple $\overline{x} \subset \mathrm{dom}(E')$, $\delta(\overline{x}/\mathrm{dom}(E)) \geq 0$, i.e., that $K_E \leq L_{E'}$. □

Moreover, the above variety V satisfies some extra properties, as it contains a point whose additive coordinates are $\mathbb{Q}$-linearly independent from $\mathrm{dom}(E)$. We name a few possible behaviours in the next definition.

Let us call π_a and π_m the projections of $\mathbb{G}$ on its two factors $\mathbb{G}_a$ and $\mathbb{G}_m$ resp.

Definition 1.35. An irreducible subvariety V of $\mathbb{G}^n$, for some integer n, is *additively free* over $\overline{c} \subset K$ if for all non-zero matrices $M \in \mathcal{M}_{n,1}(\mathbb{Z})$ the image $\pi_a(M \cdot V)$ is either infinite, or it does not contain any element of $\mathrm{span}_{\mathbb{Q}}(\overline{c})$.

Moreover, V is *multiplicatively free over $\overline{c}$* if for all non-zero matrices $M \in \mathcal{M}_{n,1}(\mathbb{Z})$ the image $\pi_m(M \cdot V)$ is either infinite, or it does not contain any element of $E(\mathrm{span}_{\mathbb{Q}}(\overline{c}))$. V is said to be *free over $\overline{c}$* if it is both additively and multiplicatively free.

V is said to be *absolutely free* when for all non-zero matrices $M \in \mathcal{M}_{1,n}(\mathbb{Z})$ both sets $\pi_a(M \cdot V)$ and $\pi_m(M \cdot V)$ are infinite.

Proposition 1.36. *Let $K_E \subset L_{E'}$ be an extension of partial E-fields such that* $\mathrm{dom}(E') = \mathrm{dom}(E) \oplus \mathbb{Q}z_1 \oplus \cdots \oplus \mathbb{Q}z_n$.

Let $V \subset \mathbb{G}^n$ be the smallest variety defined over $\mathrm{dom}(E), \mathrm{im}(E)$ *such that*

$$\langle \overline{z}; E(\overline{z})\rangle = ((z_1, E(z_1)), \ldots, (z_n, E(z_n)) \in V.$$

Then V is additively free over $\mathrm{dom}(E)$*, and* $\ker(E) = \ker(E')$ *iff it is also multiplicatively free over* $\mathrm{im}(E)$.

Moreover, $\mathrm{dom}(E') \setminus \mathrm{dom}(E)$ *and* $\mathrm{im}(E') \setminus \mathrm{im}(E)$ *do not contain algebraic elements over K iff V is absolutely free.*

As anticipated in the previous sections, richness requires that absolutely free varieties contain points of the form $\langle \overline{z}; E(\overline{z})\rangle$. Therefore, we think of these varieties as systems of polynomial-exponential equations, and of $\overline{z}$ as a solution.

Definition 1.37. If V is an absolutely free rotund variety $V \subset \mathbb{G}^n$, a vector $\overline{z} \in K^n$ is a *solution* of V if $\langle \overline{z}; E(\overline{z})\rangle \in V$.

The statement of (SEC) then requires all absolutely free rotund varieties to have solutions, but they must also be "generic". This depends on the parameters we are using to define V, hence we introduce the following notation.

Notation 1.38. We write $\overline{c}E(\overline{c})$ to denote the pure set of the elements of $\overline{c}$, together with the image of $\overline{c} \cap \mathrm{dom}(E)$ under E.

We write $V(\overline{c})$ to denote a variety V together with a finite tuple of parameters $\overline{c}$ such that V is defined over $\overline{c}E(\overline{c})$. In this case, we say that V is *E-defined over $\overline{c}$*.

Definition 1.39. A solution $\overline{z} \in K^n$ of V is a *generic solution of $V(\overline{c})$* when the corresponding point $\langle \overline{z}; E(\overline{z})\rangle \in V$ is generic over $\overline{c}E(\overline{c})$ in the algebraic sense, i.e., when

$$\mathrm{tr.deg.}_{\overline{c}E(\overline{c})}\langle \overline{z}; E(\overline{z})\rangle = \dim V.$$

A set of generic solutions $\mathcal{S}$ of $V(\overline{c})$ is *algebraically independent* (over $\overline{c}$) if for any finite subset $\{\overline{z}_1, \ldots, \overline{z}_k\} \subset \mathcal{S}$ the following holds:

$$\mathrm{tr.deg.}_{\overline{c}E(\overline{c})}(\langle \overline{z}_1; E(\overline{z}_1)\rangle, \ldots, \langle \overline{z}_k; E(\overline{z}_k)\rangle) = k \cdot \dim V.$$

The above ingredients are all that it is needed to state (SEC), so we repeat the axiom here:

(SEC) *Strong Exponential-algebraic Closure*: for every absolutely free rotund variety $V \subset \mathbb{G}^n$ over K, and every finite tuple $\overline{c} \in K^{<\omega}$ such that V is E-defined over $\overline{c}$, $V(\overline{c})$ has a generic solution $\overline{z} \in K^n$.

We can now prove that (SEC) is the last ingredient needed to get richness.

Proof of proposition 1.24. Suppose that $\mathbb{F}_E$ is rich, that $\overline{c}$ is a finite subset of $\mathbb{F}$, and that $V \subset \mathbb{G}^n$ is an absolutely free rotund variety over $\overline{c}$.

By (SP), we can extend $\overline{c}$ to a finite $\overline{c}'$ such that $\overline{c}' \leq \mathbb{F}_E$ and $\omega \in \overline{c}'$, where ω is the generator of $\ker(E)$. Let K_{E_0} be the partial E-field generated by $i^{-1}(\overline{c}')$. Note that $K_{E_0} \leq \mathbb{F}_E$.

Take a point $\langle \overline{z}; \overline{w}\rangle \in V(F)$, where F is some algebraically closed extension of K of sufficient transcendence degree, such that

$$\mathrm{tr.deg.}(\langle \overline{z}; \overline{w}\rangle / K) = \dim V.$$

Let $L := \bigcup_q K(\overline{z}, \overline{w}^{1/q})$ for some coherent choice of qth roots of the elements of $\overline{w}$. We may now define a partial exponential function E_1 on L by letting $D' := \mathrm{dom}(E_0) \oplus \langle a_1, \ldots, a_n\rangle$, where $a_1, \ldots, a_n$ are $\mathbb{Q}$-linearly independent over $\mathrm{dom}(E_0)$, identifying a_j with z_j, and extending E_0 to E_1 by putting $E_1(\frac{p}{q}a_j) := w_j^{p/q}$.

By proposition 1.34, the extension $K_{E_0} \subset L_{E_1}$ is actually strong and kernel preserving, so that L_{E_1} satisfies (STD). Therefore, L_{E_1} can be embedded strongly into $\mathbb{F}_E$. This implies that there is a $\overline{z}' \in \mathbb{F}^n$ such that $\langle \overline{z}'; E(\overline{z}')\rangle \in V$, and $\mathrm{tr.deg.}(\langle \overline{z}'; E(\overline{z}')\rangle / K) = \dim V$. In particular, $V(\overline{c})$ has a generic solution. ☐

Proof of proposition 1.25. Let $K_{E_0} \le \mathbb{F}_E$, and $K_{E_0} \le L_{E_1}$, where K_{E_0} and L_{E_1} are finitely generated partial E-fields.

We prove the statement by induction on $n = \mathrm{lin.d.}_{\mathbb{Q}}(\mathrm{dom}(E_1)/\mathrm{dom}(E_0))$, the case $n = 0$ being trivial. Let us write $\mathrm{dom}(E_1)$ as $\mathrm{dom}(E_0) \oplus \mathbb{Q}z_1 \oplus \cdots \oplus \mathbb{Q}z_n$.

First of all, suppose that there is a non-zero $\mathbb{Q}$-linear combination of $z_1, \ldots, z_n$ that falls in $\overline{K}$. After a linear base change, we may assume that in fact $z_1 \in \overline{K}$. Let us fix an embedding of $K(z_1)$ into $\mathbb{F}$ that is the identity on K.

Since $K_{E_0} \le \mathbb{F}_E$ and $K_{E_0} \le L_{E_1}$, this implies that $E(z_1)$ and $E_1(z_1)$ are both transcendental over K. We may assume that the algebraic type of any root $E_1(z_1)^{1/q}$ over K is already determined by the algebraic type of $E_1(z_1)$ over K, for all $q \in \mathbb{N} \setminus \{0\}$. In particular, the map sending $E(\frac{1}{q}z_1)$ to $E_1(\frac{1}{q}z_1)$ extend to a field isomorphism of $\bigcup_q K(z_1, E(\frac{1}{q}z_1))$ to $\bigcup_q K(z_1, E_1(\frac{1}{q}z_1))$. Therefore, we can extend the embedding $K_{E_0} \le \mathbb{F}_E$ to $\bigcup_q K(z_1, E_1(\frac{1}{q}z_1))$ identifying the images of E and E_1 on $\mathbb{Q}z_1$. This new extension has predimension 0 over K_E, hence it is still strong in $\mathbb{F}_E$; by inductive hypothesis, the embedding now extends to all L_{E_1}.

If instead some image via E_1 is in $\overline{K}$, we can again assume that $E_1(z_1) \in \overline{K}$. We may assume that the algebraic type of any coherent system of roots $(E_1(z_1)^{1/q})_q$ over K is already determined by the algebraic type of $E_1(z_1)$ over K, for all $q \in \mathbb{N} \setminus \{0\}$, up to replacing z_1 with some z_1/m. As before, we fix an embedding of $K(E_1(z_1))$ into $\mathbb{F}$ and we pick an element w such that $E(w) = E_1(z_1)$. Both w and z must be transcendental over $K(E_1(z_1))$, hence we can further extend the embedding by identifying w and z. Now, since the algebraic type of $E_1(\frac{1}{q}z_1)$ over K is determined by the type of $E_1(z_1)$, we may extend the isomorphism identifying $E_1(\frac{1}{q}z_1)$ and $E(\frac{1}{q}w)$. This extension is still strong in $\mathbb{F}_E$, and as before, by inductive hypothesis the embedding extends to L_E.

In the remaining case, the smallest variety V over K containing $\langle \overline{z}; E_1(\overline{z}) \rangle$ is absolutely free and rotund. Let us assume first that $\dim V = n$.

In this case, we may assume that the algebraic type of $E_1(\overline{z})^{1/q}$ over $K(\overline{z})$ is already determined by the algebraic type of $E_1(\overline{z})$ over K. If we now pick a solution $\overline{w}$ of V in $\mathbb{F}_E$ which is generic over some finite set of elements whose algebraic closure is $\overline{N}$, we may identify $\overline{z}$ with $\overline{w}$, and $E_1(\frac{1}{q}\overline{z})$ with $E(\frac{1}{q}\overline{w})$. This extend to an embedding, which is strong, since $\delta(\overline{w}/\mathrm{dom}(E_0)) = 0$.

If $\dim V > n$, but $\dim M \cdot V = \mathrm{rank} M$ for some non-zero matrix M of rank less than n, then the inductive hypothesis shows that the sub-E-field generated by $M \cdot \overline{z}$ can be strongly embedded in $\mathbb{F}_E$, and it is still strongly embedded in L_{E_1} since $\delta(M \cdot \overline{z}/\mathrm{dom}(E_0)) = 0$.

In the final remaining case, $\dim M \cdot V > \mathrm{rank} M$ for all non-zero matrices M. Therefore we have that z_1 and $E_1(z_1)$ are algebraically independent over K. Moreover, because of the inequality

$$\begin{pmatrix} 1 & 0 \\ 0 & M \end{pmatrix} \cdot V \ge \mathrm{rank} M + 2,$$

if we fix the first two coordinates of V to be z_1 and $E_1(z_1)$, the projection onto the other coordinates is an absolutely free rotund variety as well. This implies that the partial E-subfield generated by K_{E_0} and z_1 in L_{E_1} is still strong in L_{E_1}.

By (ID), we can find an element $w \in \mathbb{F}_E$ such that w and $E(w)$ are algebraically independent over K, and such that the partial E-field generated by $\mathrm{dom}(E_0)$ and $i^{-1}(w)$ is strong in $\mathbb{F}_E$. But then we can extend the embedding of K_{E_0} into $\mathbb{F}_E$ to z_1 as well, by identifying w with z_1 and $E(\frac{1}{q}w)$ with $E(\frac{1}{q}z_1)$. By inductive hypothesis, this now extends to L_E as well. □

As shown by the above proof, a special role is played by the varieties $V \subset \mathbb{G}^n$ such that $\dim V = n$. They are also needed to explain the axiom (CCP). For convenience, we define the following quantity.

Definition 1.40. The *depth* of a variety $V \subset \mathbb{G}^n$ is $\delta(V) := \dim V - n$.

Hence a variety with $\dim V = n$ has "depth 0". For all rotund varieties, $\delta(V) \geq 0$. The varieties of depth 0 characterise the exponential-algebraic elements, and in some sense, they represent 'finite' exponential-algebraic extensions (see [Kir09]).

Note that a generic solution of $V(\overline{c})$ has predimension over $\overline{c}$ equal to $\delta(V)$.

Now we are able to state (CCP) again.

(CCP) *Countable Closure Property*: for every absolutely free rotund variety $V \subset \mathbb{G}^n$ over K of depth 0, and every finite tuple $\overline{c} \in K^{<\omega}$ such that V is defined over $\overline{c}$, the set of the generic solutions of $V(\overline{c})$ is at most countable.

At last, we introduce another couple of definitions related to the depth of V. They will prove useful in the following constructions.

Definition 1.41. An absolutely free rotund variety $V \subset \mathbb{G}^n$ is *simple* if for all $M \in \mathcal{M}_{n,n}(\mathbb{Z})$ with $0 < \mathrm{rank} M < n$ the following strict inequality holds:

$$\dim M \cdot V > \mathrm{rank} M.$$

Simple varieties represent "simple", or "minimal" extensions, as in Hrushovski's amalgamation terminology, or in other words extensions without proper exponential-algebraic subextensions. The special case of simple algebraic extensions is then represented by the following varieties.

Definition 1.42. An absolutely free rotund variety $V \subset \mathbb{G}^n$ is *perfectly rotund* if it is simple and it has depth 0.

As it will be explained in section 1.7.1, the countable closure property actually means that the exponential-algebraic closure of a finite set is countable.

1.7 Categoricity

As mentioned in 1.30, the main theorem of [Zil05b] is that the axiomatization of Zilber fields is uncountably categorical, i.e., there is exactly one Zilber field of any given uncountable cardinality (up to isomorphism).

The theorem is quite deep, and it shows the relationship between the pregeometry induced by the above δ, certain classes of structures called "quasi-minimal excellent" and the language $\mathcal{L}_{\omega_1,\omega}(Q)$. We present a brief sketch of what happens in the paper [Zil05b].

1.7.1 Dimension

First of all, as usual, we define a dimension out of the predimension δ. We define it only for global E-fields, when $\mathrm{dom}(E)$ is the whole field.

Definition 1.43. Given a global E-field K_E satisfying (SP) and a finite subset $X \subset K$, we define

$$\partial(X) := \min_{Y \supset X} \delta(Y)$$

to be the *dimension* of X in K_E (where X and Y are seen as subsets of $\mathrm{dom}(E)$). Given two finite subsets $X, Y \subset K$, we define

$$\partial(Y/X) := \partial(XY) - \partial(X)$$

to be the *relative dimension* of Y over X in K_E. Note that by construction we have $\partial(Y/X) \geq 0$ for all X, Y.

This function is clearly well-defined, since $|Y| \geq \delta(Y) \geq 0$, and increasing. Note, however, that it depends on the whole field K_E. The dimension yields a pregeometry.

Definition 1.44. Given a global E-field K_E satisfying (SP) and a finite subset $X \subset K$, we define

$$\mathrm{cl}(X) := \{x \in K \,:\, \partial(x/X) = 0\}$$

to be the *exponential-algebraic closure* of X in K_E. When $X \subset K$ is infinite, we define

$$\mathrm{cl}(X) := \bigcup_{\substack{X' \subset X \\ X' \text{ finite}}} \mathrm{cl}(X').$$

By the definition of ∂, it is clear that cl is a monotone and idempotent operator of finite character with the exchange property, and as such it is a pregeometry on K_E. It is easy to verify that when (CCP) holds, then $\mathrm{cl}(X)$ is countable whenever X is finite, and the converse is also true. This is what gives (CCP) its name.

Remark 1.45. Given an E-field K_E in $\mathcal{EC}^0_{\mathrm{std,ccp}}$, for any subset $X \subset K$ the sub-E-field $\mathrm{cl}(X)_{E_{\restriction \mathrm{cl}(X)}}$ is again in $\mathcal{EC}^0_{\mathrm{std,ccp}}$.

1.7.2 Quasi-minimal excellent classes

Let us consider the class $(\mathcal{EC}^0_{\mathrm{std,ccp}}, \mathrm{cl})$ of the models of the above axioms, equipped with a closure operator cl for each element of the class. Zilber proved that this class is *quasi-minimal excellent.* We mention here the definition given in [Bal09], which is a simplified version of the original one that can be found in [Zil05a].

First of all, we need a few definitions.

Definition 1.46. Given two structures H, H', a *partial monomorphism* is an injective partial functions $f : H \to H'$ that preserves all the quantifier-free formulas with parameters in C.

Given a set G contained in both H, H', a partial G*-monomorphism* is a partial monomorphism in the language expanded with constants for the elements of G.

A set $C \subset H$ is *special* if there are a cl-independent subset $X \subset C$ and a finite partition $X = X_1 \cup \cdots \cup X_n$ such that $C = \mathrm{cl}(X_1) \cup \cdots \cup \mathrm{cl}(X_n)$.

Given a class of structures $\mathcal{C}$, and a pregeometry operator cl on each of its elements, we say that $(\mathcal{C}, \mathrm{cl})$ is a *quasi-minimal excellent* class if the following three properties are satisfied:

- if f is a partial monomorphism from $H \in \mathcal{C}$ to $H' \in \mathcal{C}$ taking X to X' and y to y', then $y \in \mathrm{cl}_H(X)$ if and only if $y' \in \mathrm{cl}_{H'}(X')$;
- (ω-homogeneity over submodels) given $G \subset H, H' \in \mathcal{C}$, with G empty or countable, and G closed in both H and H',
  - if f is a partial G-monomorphism with finite domain X, for all $y \in \mathrm{cl}_H(X)$ there is a $y' \in \mathrm{cl}_{H'}(f(X))$ such that $f \cup \{\langle y, y'\rangle\}$ is still a G-monomorphism;
  - any bijection between $X \subset H$ and $X' \subset H'$, with X and X' both cl-independent over G, is a partial G-monomorphism;
- (excellence) given $H \in \mathcal{C}$, and $C \subset H$ special, then for any finite $X \subset \mathrm{cl}_H(C)$ there is a finite $C_0 \subset C$ such that any C_0-monomorphism with domain X is also a C-monomorphism (i.e., the quantifier-free type of X over C is uniquely determined by its type over C_0).

In such a class, the operator cl behaves much like the algebraic closure operator.

Theorem 1.47 (Zilber, [Zil05a]). *Given two $H, H' \in \mathcal{C}$ with the countable closure property, and two* cl*-independent subsets $X \subset H$, $X' \subset H'$, then any bijection $X \to X'$ extends to an isomorphism $\mathrm{cl}_H(X) \tilde{\to} \mathrm{cl}_{H'}(X')$. In particular if H and H' are uncountable, and have the same cardinality, they are isomorphic.*

Moreover, if there is one countable model of infinite dimension, then there are models of arbitrary cardinality with the countable closure property.[2]

But then this extend to our class of exponential fields.

Theorem 1.48 (Zilber, [Zil05b]). *The class $(\mathcal{EC}^0_{\mathrm{std,ccp}}, \mathrm{cl})$ is quasi-minimal excellent*[3] *and has one countable model of infinite dimension. In particular, it has exactly one model in each uncountable cardinality up to isomorphism.*

1.8 Some known facts

We have seen that Zilber fields are unique for each uncountable cardinal. Zilber conjectured that therefore $\mathbb{C}_{\exp}$ should be exactly the unique model of cardinality $2^{\aleph_0}$, but as we have seen, this is a conjecture at least as strong as Schanuel's Conjecture, and as such, it seems quite difficult that a positive answer will appear soon.

However, we look for similarities, or possibly differences that would disprove the conjecture, between $\mathbb{B}_E$ and $\mathbb{C}_{\exp}$. Here is a short list of some theorems that have been successfully transferred between $\mathbb{B}_E$ and $\mathbb{C}_{\exp}$.

1.8.1 Strong exponential-algebraic closure

In order to prove $\mathbb{C}_{\exp} \cong \mathbb{B}_E$, one would have to prove Schanuel's Conjecture, and that $\mathbb{C}_{\exp}$ satisfies (SEC). Assuming Schanuel's Conjecture, some instances have been proved.

Theorem 1.49 (Marker [Mar06]). *Let $V \subset \mathbb{G}^1$ be an algebraic curve defined over $\mathbb{Q}$ and let $\overline{c}$ be any finite set of parameters. If Schanuel's Conjecture is true, then $V(\overline{c})$ has a generic solution.*

Some work has been done towards proving the same statement for varieties over $\mathbb{C}$, but it seems to be more difficult [Gun11].

1.8.2 Schanuel's Nullstellensatz and Picard's Little Theorem

Some difficult analytic facts appear to hold naturally on Zilber fields. In particular, it is the case for the following theorem by Henson and Rubel, sometimes called Schanuel's Nullstellensatz. In the following, an exponential polynomial is a term produced by applying the field operations and the function E to some variables.

Theorem 1.50 (Henson and Rubel [HR84]). *An exponential polynomial $F \in \mathbb{C}[x_1, \dots, x_n]^E$ has no roots in $\mathbb{C}_{\exp}$ if and only if there is another exponential polynomial $G \in \mathbb{C}[x_1, \dots, x_n]^E$ such that $F = \exp(G)$.*

[2] As mentioned in the introduction, the categoricity can be obtained also without the excellence condition, as a special form of excellence already follows from the other properties, and it is enough to prove categoricity [BHH+12].

[3] The original proof contains a mistake in the proof of excellence. By [BHH+12], categoricity follows anyway from verifying that $(\mathcal{EC}^0_{\mathrm{std,ccp}}, \mathrm{cl})$ satisfies the other properties of quasi-minimal excellence.

In turn, this is true also on Zilber fields.

Theorem 1.51 ([DMT10, Shk09]). *An exponential polynomial $F \in \mathbb{B}[x_1, \ldots, x_n]^E$ has no roots in $\mathbb{B}_E$ if and only if there is another exponential polynomial $G \in \mathbb{B}[x_1, \ldots, x_n]^E$ such that $F = E(G)$. This is true also in any E-field satisfying (SEC).*

Indeed, the proofs show that this is true in any E-field satisfying (SEC).

1.8.3 Ordered real-closed subfields

Of course, one of the characteristic aspects of $\mathbb{C}_{\exp}$ is the presence of the real line $\mathbb{R}_{\exp} \subset \mathbb{C}_{\exp}$ where $\mathbb{R}$ is real closed, hence ordered, and exp is an increasing function $\mathbb{R} \to \mathbb{R}$ surjective over the positive numbers.

It is not difficult to build abstract real closed fields equipped with increasing exponential functions; but it can be even proved that many of these fields are actually subfields of $\mathbb{B}_E$.

Theorem 1.52 ([Shk11]). *There are $2^{\aleph_0}$ pairwise non-isomorphic countable real closed fields $R \subset \mathbb{B}$ such that $E(R) = R_{>0}$, and $E_{\restriction R}$ is an increasing function. Moreover, this is true for any E-field satisfying (SP).*

1.8.4 Strong subsets

The statement of Schanuel's Conjecture can be rephrased as $\emptyset \leq \mathbb{C}_{\exp}$. Even if this is not true, we can still say that there is a *countable* strong subset, and in some sense it means that Schanuel's Conjecture is falsified only by countably many "essential" counterexamples.

Theorem 1.53 ([Kir10]). *There is a countable $C \subset \mathbb{C}$ such that $C \leq \mathbb{C}_{\exp}$.*

Furthermore, the paper [Kir10] establishes, through Ax's Theorem, a deep relationship between the predimension δ and the "exponential-algebraic closure" as defined by Macintyre [Mac96]. In particular, C is exactly $\mathrm{ecl}(\emptyset)$, the field of exponential-algebraic numbers.

1.8.5 Definable algebraic numbers

The problem of which algebraic numbers are definable in $\mathbb{C}_{\exp}$ is open, and it makes sense for exponential fields in general. All exponential fields with cyclic kernel define all the so called *real abelian numbers* $\mathbb{Q}^{\mathrm{rab}}$ (the fixed field of the unique involution of $\mathbb{Q}^{\mathrm{ab}}$, the maximal abelian extension of $\mathbb{Q}$, which is generated by the roots of unity,), but on Zilber fields these are exactly all the definable algebraic numbers.

Theorem 1.54 ([KMO12]). *Given an ELA-field with cyclic kernel, the definable algebraic numbers contains all the real abelian numbers. Moreover, inside Zilber fields no other algebraic numbers are definable.*

Chapter 2

Constructions

In this chapter, we study how to construct Zilber fields, and isolate a few facts that can be useful for understanding them. The ideas developed here will be used in the next chapter to prove that Zilber fields have involutions.

2.1 A sketch

There is a quite practical and elegant way to construct Zilber fields that dates back to the original paper [Zil05b], and has been considerably refined and formalised in [Kir09]. We sketch briefly what happens in the former paper, with some more precise statements about countability from the latter.

The first part of the construction deals with the creation of a *countable* model of the axioms. Using a countable model is indeed particularly handy, as the axiom (CCP) is verified for free. Here is how the construction works:

1. start with the partial E-field with underlying field $\overline{\mathbb{Q}}$, with E defined only on $\mathbb{Q} \cdot \omega$, for some transcendental ω, and such that $\ker(E) = \omega \cdot \mathbb{Z}$; this E-field satisfies (STD) and (SP);

2. extend the above E-field, and in general *any* countable partial E-field satisfying (SP), to a countable global ELA-field satisfying (SP) and with the same kernel; it is sufficient to add countably many algebraically independent elements to the underlying field;

3. extend the above E-field, or any countable E-field with (SP), by adding a finite number of algebraically independent elements, taking the algebraic closure, and then extending E in order to add a generic solution to an absolutely free rotund variety $V(\overline{c})$; this partial E-field has the same kernel as before and satisfies (SP), and reapplying the previous step, we can extend it to a countable global ELA-field with (SP), and the same kernel, where $V(\overline{c})$ has a generic solution;

4. enumerate all the absolutely free rotund varieties over the field just obtained, and reapply the above step until all of them have generic solutions;

5. iterate the above step ω times; the resulting ELA-field clearly satisfies (SP), (STD), but also (SEC) and has infinite dimension, plus it satisfies (CCP) since it is countable; it is therefore a Zilber field of cardinality $\aleph_0$.

This procedure is thoroughly formalised in [Kir09], where it is also proved that under suitable hypothesis the resulting ELA-fields of 2 and 3 are actually unique up to isomorphism.

We remark that in [Zil05b] the above construction is not done on countable E-fields, but on arbitrary ones, and the countable model is recovered in the end using the downward Löwenheim-Skolem theorem over a countable cl-independent set X.

Following [Zil05b], we build uncountable models starting from the countable one with a rather general trick that works on any quasi-minimal excellent class. We start with a maximal infinite cl-independent subset X of our countable model, and a proper subset $X' \subsetneq X$ of the same cardinality. While on one hand we have a proper closed embedding $\mathrm{cl}(X') \hookrightarrow \mathrm{cl}(X)$, i.e., sending closed sets to closed sets, on the other hand quasi-minimal excellence and theorem 1.47 imply that any bijection $X' \cong X$ extends to an isomorphism $\mathrm{cl}(X') \cong \mathrm{cl}(X)$. In particular, the *closed* embedding $\mathrm{cl}(X') \hookrightarrow \mathrm{cl}(X)$ can be turned "inside out", and yields another closed embedding $\mathrm{cl}(X) \hookrightarrow \mathrm{cl}(X'')$ where X'' is a cl-independent strict superset of X. Please note that in a closed embedding $H \hookrightarrow H'$, with H and H' both closed, the closure operator relative to H' coincide with the closure relative to H on the subsets of H.

This can be immediately extended to a sequence of proper closed embedding

$$\mathrm{cl}(X) \hookrightarrow \mathrm{cl}(X_1) \hookrightarrow \mathrm{cl}(X_2) \hookrightarrow \dots.$$

At limit ordinals, we take the union as usual. It is easy to see by transfinite induction that each element of the sequence has (CCP).

At each successor step, the successive element of the sequence is isomorphic to the previous one by theorem 1.47, hence (CCP) holds by inductive hypothesis. Moreover, if Y is a finite subset of the union of the sequence at a limit ordinal, then Y is contained in some $\mathrm{cl}(X_\lambda)$ for some precedent ordinal. Since the embedding are closed, then $\mathrm{cl}(Y) \subset \mathrm{cl}(X_\lambda)$, and by inductive hypothesis, it is countable, so (CCP) is verified. Going on up to an uncountable cardinal κ we obtain the Zilber field of cardinality κ.

In [Kir09], it is implicitly stated that the direct construction with countable fields can be carried on to higher cardinalities, and the resulting fields satisfy (CCP). In particular the various Zilber fields can be constructed directly without using the chain of embeddings.

The direct construction is actually more cumbersome to realise, and to check that it works, than the original Zilber's argument; however, it is needed to obtain the results of chapter 3 and chapter 4. Moreover, further complications are needed. We devote this chapter to the full description of a direct construction similar to the above one, by splitting it into its most elementary steps, and we will show how to concatenate the elementary steps to build Zilber fields. These ideas will be then adapted in the following chapters to obtain some new results on Zilber fields.

2.2 A few simplifications

In order to construct a Zilber field, we need to add solutions to rotund varieties, as in the above step 3, in order to obtain a structure with (SEC), but we need to control the number of solutions as well to have (CCP).

In order to verify the two axioms, it is useful to reduce them to two simpler statements, showing that the parameters defining the varieties are not relevant, and that is is sufficient to look only at simple varieties rather than all the rotund ones.

Fact 2.1. *Let K_E be a partial E-field. (SEC) holds on K_E if and only if the following holds:*

(SEC$_1$) *for any absolutely irreducible* simple *variety V E-defined over* some *finite $\overline{c}$, $V(\overline{c})$ has an infinite set of algebraically independent solutions.*

Fact 2.2. *Let K_E be a partial E-field. (CCP) holds on K_E if and only if the following holds:*

(CCP$_1$) *for any perfectly rotund variety V, and for any finite $\overline{c}$ such that V is E-defined over $\overline{c}$, $V(\overline{c})$ has at most countably many generic solutions.*

Hence, it is sufficient to verify (SEC$_1$) and (CCP$_1$) instead of their full versions. We use the following fact.

Proposition 2.3. *Let V be an absolutely free rotund variety. Let $\overline{c}$ and $\overline{d}$ be two finite tuples such that V is E-defined both over $\overline{c}$ and over $\overline{d}$.*

If $\mathcal{S}$ is a set of algebraically independent solutions of $V(\overline{c})$, then $\mathcal{S}$, up to removing a finite set, is an algebraically independent set of solutions of $V(\overline{d})$.

Proof. For each finite subset $\mathcal{S}' \subset \mathcal{S}$, let $\Delta(\mathcal{S})$ be the following quantity:

$$\Delta(\mathcal{S}') := \text{tr.deg.}_{\overline{c}E(\overline{c})}(\mathcal{S}') - \text{tr.deg.}_{\overline{d}E(\overline{d})}(\mathcal{S}') = \dim V \cdot |\mathcal{S}'| - \text{tr.deg.}_{\overline{d}E(\overline{d})}(\mathcal{S}').$$

Δ measures how far is $\mathcal{S}'$ from being algebraically independent over $\overline{d}$. First of all, we claim that $\Delta(\mathcal{S}')$ is bounded from above. Indeed,

$$\text{tr.deg.}_{\overline{d}E(\overline{d})}(\mathcal{S}') \geq \text{tr.deg.}_{\overline{c}E(\overline{c})\overline{d}E(\overline{d})}(\mathcal{S}') \geq \text{tr.deg.}_{\overline{c}E(\overline{c})}(\mathcal{S}') - \text{tr.deg.}_{\overline{c}E(\overline{c})}(\overline{d}E(\overline{d})),$$

and after shuffling the terms, $\Delta(\mathcal{S}') \leq \text{tr.deg.}_{\overline{c}E(\overline{c})}(\overline{d}E(\overline{d}))$. Moreover, Δ is clearly increasing.

Now let $\mathcal{S}_0$ be a finite set such that $\Delta(\mathcal{S}_0)$ is maximum. We claim that $\mathcal{S} \setminus \mathcal{S}_0$ is algebraically independent. Let us consider a finite subset $\mathcal{S}' \subset \mathcal{S} \setminus \mathcal{S}_0$; since the function Δ is increasing, we have

$$\begin{aligned}\dim V \cdot (|\mathcal{S}'| + |\mathcal{S}_0|) - \text{tr.deg.}_{\overline{d}E(\overline{d})}(\mathcal{S}' \cup \mathcal{S}_0) = \Delta(\mathcal{S}' \cup \mathcal{S}_0) = \\ = \Delta(\mathcal{S}_0) = \dim V \cdot |\mathcal{S}_0| - \text{tr.deg.}_{\overline{d}E(\overline{d})}(\mathcal{S}_0).\end{aligned}$$

This implies that

$$\dim V \cdot |\mathcal{S}'| \geq \text{tr.deg.}_{\overline{d}E(\overline{d})}(\mathcal{S}') \geq \text{tr.deg.}_{\overline{d}E(\overline{d}),\mathcal{S}_0}(\mathcal{S}') = \dim V \cdot |\mathcal{S}'|,$$

as desired. □

Proof of Facts 2.1 and 2.2. One direction is trivial for both statements, so let us see the other direction.

Let V be an absolutely free rotund variety over $\overline{c}$. By adding some elements of $\text{acl}(\overline{c}E(\overline{c}))$ to $\overline{c}$, we find that V splits into a finite union of conjugate absolutely irreducible varieties. In particular, all of them are absolutely free and rotund. If we verify that (SEC) and (CCP) hold when specialised in each of these components, then (SEC) and (CCP) are also true when specialised in V. Hence, we may assume that V is absolutely irreducible.

We proceed by induction on $n = \dim(V)$. If V is simple, and (SEC$_1$) is true, then V has infinitely many algebraically independent solutions over some set of parameters $\overline{d}$, and by proposition 2.3, up to removing a finite number of them, they are also algebraically independent over $\overline{c}$. If V is perfectly rotund, and (CCP$_1$) is true, there are at most countably many generic solutions.

Now, let us suppose that V is not simple, and that we have proved the conclusions for all the varieties of dimension smaller than V. Let $z_1, w_1, \ldots, z_n, w_n$ be the coordinate functions of V.

Let M be a matrix such that $0 < k = \mathrm{rank} M < n$ and $\dim M \cdot V = \mathrm{rank} M$. Using a suitable square invertible matrix, we may assume that M is the projection of V over the coordinates $z_1, w_1, \ldots, z_k, w_k$.

Let N be a matrix in $\mathcal{M}_{h,n-k}(\mathbb{Z})$ of maximum rank, with $h \leq n-k$. By rotundity, we have

$$\mathrm{tr.deg.}_{\overline{c}E(\overline{c})} \left(\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix} \cdot (z_1, w_1, \ldots, z_n, w_n) \right) \geq k + h.$$

But since $\dim M \cdot V = k$, this means

$$\mathrm{tr.deg.}_{\overline{c}E(\overline{c}), z_1, \ldots, z_k, w_1, \ldots, w_k} (N \cdot (z_{k+1}, w_{k+1}, \ldots, z_n, w_n)) \geq h = \mathrm{rank} N.$$

This means that whenever we specialise the first $2k$ coordinates to a generic solution of $M \cdot V$, the remaining coordinates describe a *rotund* variety of smaller dimension.

The projection $M \cdot V$ is a rotund variety of depth 0. If (SEC_1) is true, by inductive hypothesis it contains infinitely many algebraically independent solution. If (CCP_1) is true, by inductive hypothesis it contains no more than countably many generic solutions.

Now, let us suppose that $\tilde{z} = (\tilde{z}_1, \ldots, \tilde{z}_k)$ is a solution of $M \cdot V$ (if there is one). If we specialise the variables $z_1, w_1, \ldots, z_k, w_k$ to $\tilde{z}_1, E(\tilde{z}_1), \ldots, \tilde{z}_k, E(\tilde{z}_k)$, and we project onto the last $2(n-k)$ coordinates, we obtain a new variety $\tilde{V}(\overline{c}\tilde{z})$.

But $\tilde{V}$ is a *rotund* variety of dimension smaller than V. If (SEC_1) is true, by inductive hypothesis it must have infinitely many algebraically independent solutions, and combining all the generic solutions $\tilde{z}$ of $M \cdot V$ and all the solutions of the corresponding $\tilde{V}(\overline{c}\tilde{z})$, we obtain that there are infinitely many algebraically independent solutions in $V(\overline{c})$.

On the other hand, if V has depth 0, then $\tilde{V}$ has also depth 0. If (CCP_1) is true, by inductive hypothesis $M \cdot V(\overline{c})$ has at most countably many generic solutions $\overline{z}$ over $\overline{c}$, and for each of them, $\tilde{V}(\overline{c}\tilde{z})$ has at most countably many generic solutions; hence, $V(\overline{c})$ contains at most countably many generic solutions.

Hence, (SEC_1) implies (SEC) and (CCP_1) implies (CCP). □

2.3 Basic operations

In order to have a tight control of (CCP), we split the construction in its very basic operations. The reason is that by looking at the effect of each of the basic operations, we can easily bound the number of generic solutions of a perfectly rotund variety. This can be used to show an explicit proof of what is alluded to in [Kir09].

Thus, we select a few constructions that given a partial E-field K_E, and some data, yield a (strong) extension to another partial E-field $L_{E'}$.

In the most important operations, we leave the underlying field fixed, i.e., $L = K$, and we only work towards producing the function E'. We assume that K has always a transcendence degree over $\mathbb{Q}(i(\mathrm{dom}(E)), E(\mathrm{dom}(E)))$ large enough to make the constructions possible. In order to be more concise, we abbreviate the latter field as $F := \mathbb{Q}(\mathrm{dom}(E), \mathrm{im}(E))$.

DOMAIN We start with an $\alpha \in K$ given as data to the operation. If $\alpha \in \mathrm{dom}(E)$, we define $E' := E$, otherwise we do the following.

We choose an arbitrary $\beta \in K \setminus \mathrm{acl}(F \cup \{\alpha\})$, and an arbitrary coherent system of roots $\beta^{1/q}$.

We define then $E'(z + \frac{p}{q}\alpha) := E(z) \cdot \beta^{p/q}$ for all $z \in \mathrm{dom}(E)$ and $p \in \mathbb{Z}, q \in \mathbb{N}^{\times}$.

IMAGE We start with a $\beta \in K$ given as data to the operation. If $\beta \in \mathrm{im}(E)$, we define $E' := E$, otherwise we do the following.
We choose an arbitrary $\alpha \in K \setminus \mathrm{acl}(F \cup \{\beta\})$, and an arbitrary coherent system of roots $\beta^{1/q}$
We define then $E'(z + \frac{p}{q}\alpha) := E(z) \cdot \beta^{p/q}$ for all $z \in D$ and $p \in \mathbb{Z}, q \in \mathbb{N}^\times$.

SOL We start with an absolutely free rotund variety $V(\bar{c}) \subset \mathbb{G}^n$.
We choose a point $((\alpha_1, \beta_1), \dots, (\alpha_n, \beta_n)) \in V(\bar{c})$ generic over $F(\bar{c}E(\bar{c}))$.
We choose an arbitrary coherent system of roots $\beta_j^{1/q}$ of β_j, and we define

$$E'\left(z + \frac{p_1}{q_1}\alpha_1 + \dots + \frac{p_n}{q_n}\alpha_n\right) := E(z) \cdot \beta_1^{p_1/q_1} \cdot \dots \cdot \beta_n^{p_n/q_n}.$$

For completeness, we also introduce an operation whose only purpose is to extend the field K.

FIELD We start with a field extension L of K as data, and we define the new E-field as L_E.

The above operations are clearly what is used to produce all the higher level constructions that are mentioned in [Zil05b] and [Kir09]. For example, the construction of F_E^e of [Kir09], which is the free global E-field extending F_E, is done applying FIELD to add $|F|$ algebraically independent elements, then applying DOMAIN to all the original elements of F, and repeating ω times. The result is a global E-field extending F_E, and is in turn the "free global extension" of F_E.

For the applications we have in mind, it is also useful to group multiple applications of SOL to rotund varieties that are related in a certain strong way. The underlying idea is that whenever we add a generic solution $\bar{z}$ to a certain variety V, we are automatically adding new solutions to other varieties as well; in particular, $\frac{1}{n} \cdot \bar{z}$ must be a solution to some of the possibly several varieties W such that $n \cdot W = V$. Vice versa, adding a solution to W would produce a new solution to V. We group all the varieties related in this way together, so that we can add solutions to all of them at the same time.

Definition 2.4. Let V be an absolutely irreducible variety. We call the *system* $\mathcal{R}(V)$ *of the roots of* V the set of all the absolutely irreducible varieties W such that for some $p, q \in \mathbb{Z}^\times$ we have $q \cdot W = p \cdot V$.

A single application of SOL to a variety V produces new solutions to several varieties in $\mathcal{R}(V)$, but not all of them in general. However, when we want to obtain an uncountable E-field with (CCP), it helps to make sure that all the varieties in $\mathcal{R}(V)$ receives new solutions at the same time.

For this reason, in the uncountable case, rather than applying SOL to a single V, we proceed to apply apply SOL to all the varieties of $\mathcal{R}(V)$ at the same time. Again we assume that the transcendences degree of K is large enough.

ROOTS We start with an absolutely rotund variety $V(\bar{c}) \subset \mathbb{G}^n$, where $\bar{c}$ is a subset of K.
Consider an enumeration $(W_m(\bar{d}_m))_{m \in \mathbb{N}^*}$ of $\mathcal{R}(V)$, where $\bar{d}_m$ is a finite subset of $\mathrm{acl}(\bar{c}E(\bar{c}))$ containing $\bar{c}$ over which W is defined. We produce inductively a sequence of partial exponential functions E_m, starting with $E_0 := E$.
Let us suppose that E_{m-1} has been defined. If $W_m(\bar{d}_m)$ has an algebraically independent set of solutions in $K_{E_{m-1}}$, we define $E_m := E_{m-1}$; otherwise we apply SOL to $W_m(\bar{d}_m)$ over the E-field $K_{E_{m-1}}$. The resulting exponential function will be E_m.
Finally, we define $E' := \bigcup_{m \in \mathbb{N}} E_m$.

Proposition 2.5. *If K_E has $\aleph_0$, resp. $\aleph_1$, elements algebraically independent over the field $\mathbb{Q}(\mathrm{dom}(E), \mathrm{im}(E), \overline{b})$, where $\overline{b}$ includes all the parameters defining the varieties to which* SOL *is applied, and K is algebraically closed, then* DOMAIN, IMAGE *and* SOL, *resp.* ROOTS *are applicable. Moreover, the resulting $K_{E'}$ has $\aleph_0$, resp. $\aleph_1$, elements algebraically independent over $\mathbb{Q}(\mathrm{dom}(E'), \mathrm{im}(E'))$.*

Proof. It is clear that all the operations are applicable if there are sufficiently many algebraically independent elements: we need one for DOMAIN and IMAGE, $\dim(V)$ for SOL, and uncountably many for ROOTS. Since we are defining E' only on finitely many new points in the former three operations, and on countably many new points in the latter, the transcendence degree of K over $\mathbb{Q}(\mathrm{dom}(E'), \mathrm{im}(E'))$ remains countable (resp. uncountable). □

2.4 Preserved properties

It is quite straightforward to see that all the extensions produced by the above basic operations are well-defined, and are strong, kernel preserving extensions, when they are applicable.

Proposition 2.6. *If $K_E \subset L_{E'}$ is an extension produced by one of the basic operations, then $L_{E'}$ is well-defined and is a partial E-field.*

Proof. In all the operations extending E, we are defining E' on to coincide with E on $\mathrm{dom}(E)$, and extend it on $\mathbb{Q}$-linearly independent elements. In the first operation, this is guaranteed by the fact that $\alpha \notin \mathrm{dom}(E)$ and that $\mathrm{dom}(E)$ is a $\mathbb{Q}$-vector space, hence α is $\mathbb{Q}$-linearly independent from $\mathrm{dom}(E)$; for the second one, it is a consequence of α being transcendental; in the third case, it is due to the fact that V is absolutely additively free, hence the generic point $((\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n))$ is such that $\alpha_1, \ldots, \alpha_n$ is $\mathbb{Q}$-linearly independent from $\mathrm{dom}(E)$, therefore the new function is well-defined.

This automatically applies also to ROOTS, as it is a sequence of SOL operations.

The conclusion is trivial for the operation FIELD. □

Proposition 2.7. *If $K_E \subset L_{E'}$ is an extension produced by one of the basic operations, and K_E has full kernel, then the extension is kernel preserving.*

Proof. As before, the image through E' of the new $\mathbb{Q}$-linearly independent elements is multiplicatively independent from $E(\mathrm{dom}(E))$ as well. For DOMAIN, because β is transcendental over $E(\mathrm{dom}(E))$; for IMAGE, because $E(\mathrm{dom}(E))$ is divisible, and contains all the roots of unity, then $\beta \notin E(\mathrm{dom}(E))$ implies that it is multiplicatively independent from it as well; for SOL, it is because V is absolutely multiplicatively free, hence the generic point $((\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n))$ is such that $\beta_1, \ldots, \beta_n$ is multiplicatively independent from $\mathrm{dom}(E)$.

This also implies the consequence for ROOTS, as it is a sequence of SOL's, and again the consequence is trivial for FIELD. □

Proposition 2.8. *If $K_E \subset L_{E'}$ is an extension produced by one of the basic operations, then the extension is strong.*

Proof. For the first two operations, let us assume that (α, β) is one of the new points in the graph of E'. If we calculate the predimension of a tuple $\overline{z}$ in $\mathrm{dom}(E')$, we have

$$\delta(\overline{z}/\mathrm{dom}(E)) = \delta(\overline{z}', \alpha/\mathrm{dom}(E)) = \delta(\alpha/\mathrm{dom}(E)),$$

where $\overline{z}', \alpha$ is such that $\mathrm{span}_{\mathbb{Q}}(\overline{z}'\alpha) = \mathrm{span}_{\mathbb{Q}}(\overline{z})$ and $\overline{z}' \subset \mathrm{dom}(E)$. But then

$$\delta(\alpha/\mathrm{dom}(E)) = \mathrm{tr.deg.}(\alpha, \beta/\mathrm{dom}(E), E(\mathrm{dom}(E))) - \mathrm{lin.d.}_{\mathbb{Q}}(\alpha/\mathrm{dom}(E)) \geq 1 - 1 = 0.$$

This shows that the extension is strong. By proposition 1.34, the extension is strong also after the application of SOL. The conclusion is trivial for the operation FIELD. □

The above facts imply the following immediate corollary.

Corollary 2.9. *If K_E satisfies (SP), or (STD), then any extension produced by a basic operation satisfies (SP), or (STD) resp.*

2.5 Countable Closure Property

While in the previous section we have seen that it is quite immediate to verify that the properties (SP) and (STD) are preserved by the basic operations, for (CCP) some extra work is required. Here we show a further quite natural reduction: since (CCP) is about counting solutions of system of equations, the only relevant systems are the ones defined over the domain of the function E. In particular, it really depends on the function E and not on the ground field K.

Proposition 2.10. *Let K_E be a partial EA-field satisfying (SP). Then axiom (CCP) is equivalent to*

(CCP$_2$) *for any perfectly rotund variety V E-defined over* $\mathrm{dom}(E)$*, and for any finite tuple $\overline{c} \subset$* $\mathrm{dom}(E)$ *such that V is E-defined over $\overline{c}$, there are at most countably many generic solutions of $V(\overline{c})$.*

Proof. The left-to-right direction is clear. Let us prove the other direction.

Let us suppose that K_E satisfies (CCP$_2$). Let $X(\overline{c}) \subset \mathbb{G}^n$ be a perfectly rotund variety. Without loss of generality, we may assume that $\overline{c}$ is of the form $\overline{c}_0\overline{c}_1$, with $\overline{c}_0 \subset \mathrm{dom}(E)$ and $\overline{c}_1$ $\mathbb{Q}$-linearly independent from $\mathrm{dom}(E)$.

Let $\overline{d}$ be a finite subset of $\mathrm{dom}(E)$ such that

1. $\overline{c}_0\overline{d} \leq K_E$;
2. $\mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}(\overline{c}_1) = \mathrm{tr.deg.}_{\mathrm{dom}(E),\mathrm{im}(E)}(\overline{c}_1)$.

Now, let us take a generic solution $\overline{z}$ of $X(\overline{c})$. There is an invertible matrix M with coefficients in $\mathbb{Z}$ such that $M \cdot \overline{z}$ is of the form $\overline{z}_0\overline{z}_1$, with $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{c}_0\overline{d})$ and $\overline{z}_1$ $\mathbb{Q}$-linearly independent from $\mathrm{span}_{\mathbb{Q}}(\overline{c}_0\overline{d})$.

By hypothesis, $\overline{c}_0\overline{d} \leq K_E$, so for any matrix N with integer coefficients:

$$\mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}\langle N \cdot \overline{z}_1; E(N \cdot \overline{z}_1)\rangle \geq \mathrm{rank} N.$$

Moreover, since $\overline{z}_0\overline{z}_1$ is a generic point of $M \cdot X(\overline{c})$, which is a perfectly rotund variety defined over $\overline{c}$, we have

$$\mathrm{tr.deg.}_{\langle \overline{c}\overline{z}_0; E(\overline{c}\overline{z}_0)\rangle}\langle \overline{z}_1; E(\overline{z}_1)\rangle \leq |\overline{z}_1|.$$

Clearly, since $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{c}_0\overline{d})$, this implies

$$\mathrm{tr.deg.}_{\overline{c}_1\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}\langle \overline{z}_1; E(\overline{z}_1)\rangle \leq |\overline{z}_1|.$$

In particular, since $\mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}\overline{z}_1; E(\overline{c}_0\overline{d}\overline{z}_1)\rangle}(\overline{c}_1) = \mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}(\overline{c}_1)$, we have

$$|\overline{z}_1| \leq \mathrm{tr.deg.}_{\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}\langle \overline{z}_1; E(\overline{z}_1)\rangle = \mathrm{tr.deg.}_{\overline{c}_1\langle \overline{c}_0\overline{d}; E(\overline{c}_0\overline{d})\rangle}\langle \overline{z}_1; E(\overline{z}_1)\rangle \leq |\overline{z}_1|.$$

This implies that $\overline{z}_1$ is a generic solution of a perfectly rotund variety E-defined over $\overline{c}_0\overline{d}$. As there are countably many such varieties, and K_E satisfies (CCP$_2$), then there are at most countably many $\overline{z}_1$'s.

To summarise the result, we have

$$\overline{z} = M^{-1}(\overline{z}_0\overline{z}_1).$$

Since there are at most countably many matrices M, at most countably many $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{c}_0\overline{d})$ and at most countably many $\overline{z}_1$'s, then there are at most countably many $\overline{z}$. In particular, K_E satisfies (CCP). □

With a very similar argument we obtain our claimed result.

Lemma 2.11. *Let $K_E \subset K'_{E'}$ be two partial E-field satisfying (SP).*

If $\mathrm{dom}(E') = \mathrm{span}_{\mathbb{Q}}(\mathrm{dom}(E) \cup B)$ for some finite or countable $B \subset K'$, then K_E satisfies (CCP) if and only if $K'_{E'}$ does.

Proof. Clearly, if $K'_{E'}$ satisfies (CCP), then K_E does too. For the other direction, let us suppose that K_E satisfies (CCP).

By proposition 2.10, it is sufficient to prove that $K'_{E'}$ satisfies (CCP$_2$). Moreover, we may assume that $K = K'$.

Let $X(\overline{c})$ be a perfectly rotund variety, with $\overline{c} \subset \mathrm{dom}(E')$.

Let us take a generic solution of $X(\overline{c})$; by assumptions, it can be written uniquely as $\overline{z} + M \cdot \overline{b}$, with $\overline{z} \subset \mathrm{dom}(E)$, $\overline{b}$ a finite subset of B and M a matrix with coefficients in $\mathbb{Q}$. We claim that given M and $\overline{b}$, there are at most countably many $\overline{z}$'s such that $\overline{z} + M \cdot \overline{b}$ is a generic solution of $X(\overline{c})$.

Let $\overline{d}$ be a finite subset of $\mathrm{dom}(E')$ such that $\overline{b}\overline{c}\overline{d} \le K'_{E'}$.

There is an invertible matrix N with coefficients in $\mathbb{Z}$ such that $N \cdot \overline{z}$ is of the form $\overline{z}_0\overline{z}_1$, with $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{b}\overline{c}\overline{d})$ and $\overline{z}_1$ $\mathbb{Q}$-linearly independent from $\mathrm{span}_{\mathbb{Q}}(\overline{b}\overline{c}\overline{d})$. Thus $(N \cdot \overline{z} + N \cdot M \cdot \overline{b})$ is a generic solution of $N \cdot X(\overline{c})$, which is again a perfectly rotund variety defined over $\overline{c}$. For the sake of notation, let $\overline{b}_0\overline{b}_1$ be the splitting of $N \cdot M \cdot \overline{b}$ corresponding to $\overline{z}_0\overline{z}_1$.

By the hypothesis, $\overline{b}\overline{c}\overline{d} \le K'_{E'}$, so for any matrix P with integer coefficients

$$\mathrm{tr.deg.}_{\langle \overline{b}\overline{c}\overline{d}; E'(\overline{b}\overline{c}\overline{d})\rangle} \langle P \cdot \overline{z}_1; E(P \cdot \overline{z}_1)\rangle \ge \mathrm{rank} P.$$

Moreover, since $\overline{z}_0\overline{z}_1 + \overline{b}_0\overline{b}_1$ is a generic solution of $N \cdot X(\overline{c})$, we have

$$\mathrm{tr.deg.}_{\langle \overline{z}_0 + \overline{b}_0, \overline{c}; E'(\overline{z}_0 + \overline{b}_0, \overline{c})\rangle} \langle \overline{z}_1 + \overline{b}_1; E(\overline{z}_1 + \overline{b}_1)\rangle \le |\overline{z}_1|.$$

Clearly, since $\overline{z}_0 \subset \mathrm{span}_{\mathbb{Q}}(\overline{b}\overline{c}\overline{d})$, this implies

$$\mathrm{tr.deg.}_{\langle \overline{b}\overline{c}\overline{d}; E'(\overline{b}\overline{c}\overline{d})\rangle} \langle \overline{z}_1; E(\overline{z}_1)\rangle \le |\overline{z}_1|.$$

In particular, we must have

$$|\overline{z}_1| \le \mathrm{tr.deg.}_{\langle \overline{b}\overline{c}\overline{d}; E'(\overline{b}\overline{c}\overline{d})\rangle} \langle \overline{z}_1; E(\overline{z}_1)\rangle \le |\overline{z}_1|.$$

Hence $\overline{z}_1$ is a generic solution of some perfectly rotund variety E'-defined over $\overline{b}\overline{c}\overline{d}$ (i.e., defined over $\overline{b}\overline{c}\overline{d}E'(\overline{b}\overline{c}\overline{d})$); hence it is E-defined over $\overline{b}\overline{c}\overline{d}E(\overline{d})$.

To summarise the result, we have obtained that the generic solutions of $X(\overline{c})$ are of the form

$$\overline{z} = N^{-1}(\overline{z}_0\overline{z}_1) + M \cdot \overline{b},$$

where N, M are two matrices with coefficients in $\mathbb{Q}$, $\overline{b}$ is a finite subset of B, $\overline{z}_0$ is contained in $\mathrm{span}_{\mathbb{Q}}(\overline{b}\overline{c}\overline{d})$ and $\overline{z}_1$ is a generic solution of a perfectly rotund variety E-defined over $\overline{b}\overline{c}\overline{d}E'(\overline{d})$. Clearly, the possible $N, M, \overline{b}, \overline{z}_0$ and varieties over $\overline{b}\overline{c}\overline{d}E'(\overline{d})$ range in a countable set, and by (CCP) of $K'_E(= K_E)$, also $\overline{z}_1$ ranges in a countable set.

Hence, there are at most countably many generic solutions of $X(\overline{c})$ in $K'_{E'}$, i.e., (CCP) holds on $K'_{E'}$. □

Since our basic operations add at most countably many elements to the domain, the following corollary trivially follows from lemma 2.11.

Corollary 2.12. *If K_E satisfies (CCP), then any extension produced by a basic operation satisfies (CCP).*

2.6 Controlling roots

The real difficulties start when we want to iterate the basic operations over uncountable ordinals, for example if we try to produce an uncountable ELA-field, and we want to see if (CCP) is preserved after many iterations.

We can show that (CCP) is preserved if we limit ourselves to FIELD, DOMAIN and IMAGE. On the other hand, if we apply SOL to the same perfectly rotund variety $V(\overline{c})$ $\aleph_1$ times, then clearly $\mathrm{cl}(\overline{c})$ will not be countable in the resulting field. However, the operation ROOTS checks first if a variety already has enough solutions, and in that case it does not produce any changes. This is actually enough to see that ROOTS can be iterated as many times as we want while preserving (CCP).

Here we exploit heavily the system of roots. We concentrate now on how generic solutions can be transferred from one variety to another by multiplication by matrices and translations.

First of all, we wish to point out an easy but fundamental property of $\mathcal{R}(V)$.

Proposition 2.13. *If V is E-defined over $\overline{c}$, then all the varieties $W \in \mathcal{R}(V)$ are defined over* $\mathrm{acl}(\overline{c}E(\overline{c}))$. *Moreover, if $W \in \mathcal{R}(V)$, then $\mathcal{R}(W) = \mathcal{R}(V)$. In particular $\mathcal{R}(V) = \mathcal{R}(p \cdot V)$ for any $p \in \mathbb{Z}^{\times}$.*

Proof. Clearly, if $q \cdot W = p \cdot V$, then W is defined over $\mathrm{acl}(\overline{c}E(\overline{c}))$.

If $W \in \mathcal{R}(V)$, then there are $p, q \in \mathbb{Z}^{\times}$ such that $q \cdot W = p \cdot V$. If $W' \in \mathcal{R}(V)$ is another variety, there are p', q' such that $q' \cdot W' = p' \cdot V$. Multiplying both sides by p we obtain $pq' \cdot W' = p'q \cdot W$, hence $W' \in \mathcal{R}(W)$. This proves that $\mathcal{R}(V) \subset \mathcal{R}(W)$. The other inclusion follows by exchanging the roles of V and W. □

This means that the families of roots behave like equivalence classes. A similar concept explained with the language of equivalence relations is indeed present in [Kir09], where translations and Kummer-genericity are also considered when defining the equivalence.

From now on, let K_E be a fixed partial E-field.

Definition 2.14. A family $\mathcal{R}(V)$, with $\overline{c}$ E-defining V, is *completely solved* in K_E if for all $W \in \mathcal{R}(V)$ there is an infinite set of solutions of W algebraically independent over $\overline{c}$.

By proposition 2.3, this definition does not depend on the choice of $\overline{c}$.

It is easy to see that (SEC) is equivalent to saying that all the systems $\mathcal{R}(V)$ are completely solved. Indeed, the operation ROOTS applied to V makes sure that $\mathcal{R}(V)$ is completely solved.

The following facts describe the relationships that can occur between the solutions of system of roots for different varieties. First, we look at the action by matrices on $\mathbb{G}^n$.

Proposition 2.15. *Let $V \subset \mathbb{G}^n$ be an absolutely irreducible rotund variety, and let $M \in \mathcal{M}_{k,n}(\mathbb{Z})$ be an integer matrix.*

If $W \in \mathcal{R}(V)$, then $M \cdot W \in \mathcal{R}(M \cdot V)$.

Proof. If $W \in \mathcal{R}(V)$, then there are $p, q \in \mathbb{Z}^\times$ such that $q \cdot W = p \cdot V$. Multiplying by M we obtain $M \cdot q \cdot W = M \cdot p \cdot V$. However M commutes with $p \cdot \mathrm{Id}$ and $q \cdot \mathrm{Id}$, hence $q \cdot (M \cdot W) = p \cdot (M \cdot V)$, i.e., $M \cdot W \in \mathcal{R}(M \cdot V)$. □

Corollary 2.16. *Let $V \subset \mathbb{G}^n$ be an absolutely irreducible rotund variety, and let $M \in \mathcal{M}_{n,n}(\mathbb{Z})$ be a square integer matrix of maximum rank.*

If $W \in \mathcal{R}(M \cdot V)$, then there is a $W' \in \mathcal{R}(V)$ such that $M \cdot W' = W$.

Proof. Let $\tilde{M}$ be the square integer matrix such that $\tilde{M} \cdot M = |\det M| \cdot \mathrm{Id}$. Let $W'' \in \mathcal{R}(M \cdot V)$ be a variety such that $|\det M| \cdot W'' = W$. Let $W' := \tilde{M} \cdot W''$.

Clearly, $M \cdot W' = M \cdot \tilde{M} \cdot W'' = |\det M| \cdot W'' = W$, so the equality is satisfied.

Moreover, by definition of $\mathcal{R}(M \cdot V)$ there are $p, q \in \mathbb{Z}^\times$ such that $q \cdot W = p \cdot M \cdot V$. Applying $\tilde{M}$ on both sides, we obtain $q \cdot \tilde{M} \cdot W = p \cdot |\det M| \cdot V$. Replacing W with $M \cdot W'$ we obtain $q \cdot |\det M| \cdot W' = p \cdot |\det M| \cdot V$, hence $W' \in \mathcal{R}(V)$. □

Then we consider the translations by points of $\mathbb{G}^n$. We denote by $\oplus$ the group operation of $\mathbb{G}^n$.

Proposition 2.17. *Let $V \subset \mathbb{G}^n$ be an absolutely irreducible rotund variety, and let $\overline{z} \in \mathrm{dom}(E)^n$.*

If $W \in \mathcal{R}(V \oplus \langle \overline{z}; E(\overline{z})\rangle)$, then there is a rational number $\frac{p}{q} \in \mathbb{Q}^\times$ and a variety $W' \in \mathcal{R}(V)$ such that $W' \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle = W$.

Proof. By definition, there are $p, q \in \mathbb{N}^\times$ such that $q \cdot W = p \cdot (V \oplus \langle \overline{z}; E(\overline{z})\rangle)$. Let $W' := W \oplus \langle -\frac{p}{q}\overline{z}; E(-\frac{p}{q}\overline{z})\rangle$. The equality is clearly satisfied.

Moreover,

$$q \cdot W' = q \cdot \left(W \oplus \langle -\frac{p}{q}\overline{z}; E(-\frac{p}{q}\overline{z})\rangle \right) = q \cdot W \oplus \langle -p \cdot \overline{z}; E(-p \cdot \overline{z})\rangle = p \cdot V.$$

Hence, $W' \in \mathcal{R}(V)$. □

Using the above propositions we can finally say something about how generic solutions of one system of roots move to solutions of another system.

Proposition 2.18. *Let $V \subset \mathbb{G}^n$ be an absolutely irreducible rotund variety. Let $M \in \mathcal{M}_{n,n}(\mathbb{Z})$ be a square integer matrix of maximum rank and $\overline{z} \in \mathrm{dom}(E)^n$.*

The family $\mathcal{R}(V)$ is completely solved if and only if $\mathcal{R}(M \cdot V \oplus \langle \overline{z}; E(\overline{z})\rangle)$ is.

Proof. It is sufficient to verify the left-to-right direction of the implication. Indeed, if $\tilde{M}$ is the integer matrix such that $\tilde{M} \cdot M = |\det M| \cdot \mathrm{Id}$, we can also write $|\det M| \cdot V = \tilde{M} \cdot X \oplus \langle -\tilde{M} \cdot \overline{z}; E(-\tilde{M} \cdot \overline{z})\rangle$. Since $\mathcal{R}(|\det M| \cdot V) = \mathcal{R}(V)$, the roles of X and V can be exchanged to reverse the argument. Hence, from now on let us suppose that $\mathcal{R}(V)$ is completely solved.

Let $W \in \mathcal{R}(M \cdot V \oplus \langle \overline{z}; E(\overline{z})\rangle)$. By the above propositions, there is a $W' \in \mathcal{R}(V)$ and a rational number $\frac{p}{q} \in \mathbb{Q}^\times$ such that $M \cdot W' \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle = W$.

Let $\overline{c}$ be a finite set of parameters E-defining W' containing also $\overline{z}$. Clearly, W is E-defined also over $\overline{c}$, and if $\overline{x}$ is a generic solution of $W'(\overline{c})$, then $M \cdot \overline{x} + \frac{p}{q}\overline{z}$ is a generic solution of $W(\overline{c})$.

Moreover, we claim that the map $P \mapsto M \cdot P \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle$, for $P \in W'$, preserves the algebraic independence over $\overline{c}E(\overline{c})$. As the translation by $\langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle$ is an algebraic invertible map defined over $\mathrm{acl}(\overline{c}E(\overline{c}))$, it is sufficient to check this on the map $P \mapsto M \cdot P$.

However, since M is invertible, there is an integer matrix $\tilde{M}$ such that $\tilde{M} \cdot M = |\det M| \cdot \mathrm{Id}$; in particular, the composition $P \mapsto M \cdot P \mapsto \tilde{M} \cdot M \cdot P = |\det M| \cdot P$ is just the map $P \mapsto |\det M| \cdot P$. This map is algebraic and finite-to-one, hence it preserves the algebraic independence; in particular, $P \mapsto M \cdot P$ must preserve the algebraic independence.

This implies that an infinite set of algebraically independent solutions of W' is mapped to an infinite set of algebraically independent solutions of W. In particular, if $\mathcal{R}(V)$ is completely solved, then W contains an infinite set of algebraically independent solutions over $\overline{c}$. Since this holds for any W, $\mathcal{R}(M \cdot V \oplus \langle \overline{z}; E(\overline{z})\rangle)$ is completely solved. □

2.7 Preserving (CCP) after many iterations

We are ready to prove that the basic operations field, domain, image and roots can be iterated along ordinals preserving (CCP).

Let $(K^j_{E_j})_{j\leq\alpha}$ be a sequence of partial E-fields such that

- for all $j < \alpha$, $K^{j+1}_{E_{j+1}}$ is an extension of $K^j_{E_j}$ obtained by one of the basic operations DOMAIN, IMAGE, ROOTS, FIELD;
- for all $j \leq \alpha$ limit ordinals, $K^j_{E_j}$ is given by $K^j = \bigcup_{k<j} K^k$ and $E_j = \bigcup_{k<j} E_j$.

Proposition 2.19. *If $K^0_{E_0}$ satisfies (CCP), then $K^\alpha_{E_\alpha}$ satisfies (CCP).*

Proof. As already noted, by proposition 2.10 the property (CCP) is independent from the underlying field. Hence, without loss of generality, we may replace all the fields and assume that $K^j = K^\alpha = K$ for all $j < \alpha$.

Let D_j be the domain $\mathrm{dom}(E_j)$. For all $j < \alpha$ there is a finite or countable set B_j such that $D_{j+1} = \mathrm{span}_{\mathbb{Q}}(D_j \cup B_j)$. By lemma 2.11, if K_{E_j} satisfies (CCP), then $K_{E_{j+1}}$ satisfies (CCP). We claim that the induction works also at limit ordinals.

Let j be a limit ordinal such that for all $k < j$, K_{E_k} satisfies (CCP). By proposition 2.10, in order to prove (CCP) for K_{E_j} it is sufficient to verify that for any perfectly rotund variety defined over D_j, the number of generic solutions is at most countable. We may restrict to absolutely irreducible varieties by adding some parameters from $\mathrm{acl}(D_j, E(D_j))$.

Let $X(\overline{c}) \subset \mathbb{G}^n$ be a perfectly rotund variety with $\overline{c} \subset \mathrm{acl}(D_j, E(D_j))$. First of all, there must be a minimum $m < j$ such that $\overline{c} \subset \mathrm{acl}(D_m, E(D_m))$. Since K_{E_m} has (CCP) by inductive hypothesis, it is sufficient to count how many generic solutions of $X(\overline{c})$ are contained in $D^n_j \setminus D^n_m$.

If $\overline{x} \in D^n_j \setminus D^n_m$ is a generic solution of $X(\overline{c})$ in K_{E_j}, then there is a smallest $m \leq k < j$ such that $\overline{x} \in D^n_{k+1} \setminus D^n_k$. We claim that there is *at most one such k*. This implies that the the generic solutions of $X(\overline{c})$ in K_{E_α} are actually all contained in $K_{E_{k+1}}$, where (CCP) is satisfied, and therefore they are countable. Given that this holds for all varieties $X(\overline{c})$, K_{E_j} satisfies (CCP), and by induction, K_{E_α} too.

Let $\overline{x}$ be a new generic solution of $X(\overline{c})$ contained in $D^n_{k+1} \setminus D^n_k$. First of all, we claim that the solution $\overline{x}$ cannot appear as a consequence of one of the two operations DOMAIN and IMAGE.

For both operations let (α, β) the new point we are adding to the graph of E, so that $D_{k+1} = \mathrm{span}_{\mathbb{Q}}(D_k \cup \{\alpha\})$. Let F be the field generated by $D_k, E(D_k)$. By hypothesis, $\overline{c}, E(\overline{c}) \subset \mathrm{acl}(F)$.

DOMAIN, IMAGE. The vector $\overline{x}$ must be of the form $\overline{z} + \alpha \cdot \overline{m}$, where $\overline{m}$ is a vector in $\mathbb{Q}^n \setminus \{0\}$ and $\overline{z} \in D^n_k$. By using a square integer matrix M of maximum rank, we may transform the solution to one of the form

$$\langle M \cdot \overline{z} + \alpha \cdot m \cdot \overline{e}_1; E_k(M \cdot \overline{z}) \cdot \beta^{m \cdot \overline{e}_1}\rangle \in M \cdot X(\overline{c}),$$

where m is some integer and $\overline{e}_1$ is the vector $(1, 0, \dots, 0)$.

The variety $M \cdot X(\overline{c})$ is still perfectly rotund. We distinguish two cases.

If $n \geq 2$, let $\overline{e}_j$ be the vectors that are 1 on the j-th coordinate, and 0 on the rest. Let N be the matrix which is the identity on $\overline{e}_j$ for $j > 1$, and the zero map on $\overline{e}_1$. Since $M \cdot X$ is perfectly rotund, then $\dim(N \cdot M \cdot X) = n$, hence the point $\langle N \cdot M \cdot \overline{z}; E(N \cdot M \cdot \overline{z})\rangle$ has transcendence degree n over $\overline{c}E(\overline{c})$. In particular,

$$\text{tr.deg.}_{\overline{c}E(\overline{c})}\langle N \cdot M \cdot \overline{z}; E_k(N \cdot M \cdot \overline{z})\rangle = \text{tr.deg.}_{\overline{c}E(\overline{c})}\langle M \cdot \overline{z} + \alpha \cdot m \cdot \overline{e}_1; E_k(M \cdot \overline{z}) \cdot \beta^{m \cdot \overline{e}_1}\rangle.$$

This implies that α and $\beta = E(\alpha)$ are both algebraic over $\langle \overline{z}; E(\overline{z})\rangle \cup \overline{c}E(\overline{c})$, and in particular over $F(\overline{c}E(\overline{c})) \subset \text{acl}(F)$. However, we have $\text{tr.deg.}_F(\alpha, \beta) \geq 1$, a contradiction.

If $n = 1$, then $\dim X(\overline{c}) = 1$, and the new point is of the form $z + \alpha \cdot m$. Since the variety is absolutely free, we have that $z + \alpha \cdot m$ and $E_k(z) \cdot \beta^m$ are both transcendental over $\overline{c}E(\overline{c})$, but interalgebraic over $\overline{c}E(\overline{c})$; in other words, there is an irreducible polynomial over $\overline{c}E(\overline{c})$ where both of them appears. In particular, they are interalgebraic over $\text{acl}(F)$. However, by construction we either have $\text{tr.deg.}_{F(\alpha)}(\beta) = 1$ or $\text{tr.deg.}_{F(\beta)}(\alpha) = 1$, a contradiction.

The only remaining possibility is that the solution $\overline{x}$ appears during the operation ROOTS. In this case the discussion is a bit more complicated.

ROOTS. This operation is actually a sequence of multiple applications of SOL. Let us suppose that the solution $\overline{x}$ appears when we add the point $\langle \overline{\alpha}; \overline{\beta}\rangle \in V$ to the graph of the exponential function, for some simple variety $V \subset \mathbb{G}^m$ with $V \in \mathcal{R}(W)$. Let D be the domain of the exponential function before adding the point $\langle \overline{\alpha}; \overline{\beta}\rangle$, $D' := \text{span}_{\mathbb{Q}}(D \cup \overline{\alpha})$ be the domain after, and E the function E_α restricted to D'. The vector $\overline{x}$ must then be of the form $\overline{z} + M \cdot \overline{\alpha}$, for some matrix $M \in \mathcal{M}_{n,2m}(\mathbb{Q}) \setminus \{0\}$, and $\overline{z} \in D$. Let $F := \mathbb{Q}(D, E(D))$.

For now, let us assume that M is an integer matrix.

Under the above assumptions, $\text{tr.deg.}_F(\overline{\alpha}, E(\overline{\alpha})) = \dim V = m$. Moreover, for any matrix P we have $\text{tr.deg.}_F(P \cdot \overline{\alpha}, E(P \cdot \overline{\alpha})) \geq \text{rank}P$.

Now, let N be an invertible matrix with integer coefficients such that the first rows of $N \cdot M$ forms a matrix Q of maximum rank equal to $\text{rank}M$, and that the remaining rows are zero. Clearly, the point $\langle N \cdot \overline{z} + N \cdot M \cdot \overline{\alpha}; E(N \cdot \overline{z} + N \cdot M \cdot \overline{\alpha})\rangle$ is generic for $N \cdot X(\overline{c})$, which is again a simple variety.

Let $N \cdot \overline{z} = \overline{z}'\overline{z}''$, where $\overline{z}'$ is formed by the first $\text{rank}M$ coordinates and $\overline{z}''$ by the remaining $(n - \text{rank}M)$ ones. Let us suppose that $n > \text{rank}M$. By simpleness of $N \cdot X(\overline{c})$, we have $\text{tr.deg.}_{\overline{c}E(\overline{c})}(\overline{z}'', E(\overline{z}'')) > (n - \text{rank}M)$.

In particular, we also have $\text{tr.deg.}_{\overline{c}E(\overline{c}),\langle \overline{z}''; E(\overline{z}'')\rangle}(\overline{z}' + Q \cdot \overline{\alpha}, E(\overline{z}' + Q \cdot \overline{\alpha})) < \text{rank}M$. However, this contradicts the fact that $\text{tr.deg.}_F(Q \cdot \overline{\alpha}, Q \cdot E(\overline{\alpha})) \geq \text{rank}Q = \text{rank}M$. This implies that $n = \text{rank}M$.

The resulting situation is that $\langle \overline{z} + M \cdot \overline{\alpha}; E(\overline{z} + M \cdot \overline{\alpha})\rangle$ is a generic point of $X(\overline{c})$ *over* F, while it is also a generic point of $M \cdot V \oplus \langle \overline{z}; E(\overline{z})\rangle$ over F. This immediately implies the equality $M \cdot V \oplus \langle \overline{z}; E(\overline{z})\rangle = X$.

In particular, we also have

$$\dim V = \text{tr.deg.}_F(\overline{z} + M \cdot \overline{\alpha}, E(\overline{z} + M \cdot \overline{\alpha})) = \text{tr.deg.}_F(M \cdot \overline{\alpha}, E(M \cdot \overline{\alpha})) = \text{rank}M.$$

Hence M must be a square matrix of maximum rank, and now the equality $M \cdot V \oplus \langle \overline{z}; E(\overline{z})\rangle = X$ implies, by proposition 2.18, that $\mathcal{R}(V)$ is completely solved if and only if $\mathcal{R}(X)$ is. Note, moreover, that $\mathcal{R}(W) = \mathcal{R}(V)$.

If M is not an integer matrix, let l be an integer such that $l \cdot M$ is an integer matrix; the above argument applied to $l \cdot M$, $l \cdot \overline{z}$ and $l \cdot X$ implies that $\mathcal{R}(V)$ is completely solved if and only if $\mathcal{R}(l \cdot X)$ is. As $\mathcal{R}(l \cdot X) = \mathcal{R}(X)$, this is the same conclusion as before.

However, we see that after the application of ROOTS, the system $\mathcal{R}(W)$ is completely solved, hence $\mathcal{R}(X)$ is. If this happens a *second* time, for another variety W', then we find that $\mathcal{R}(W')$ is already completely solved before the start of the operation, because $\mathcal{R}(X)$ is; hence, the operation is void, a contradiction. This implies that there is at most one k.

In particular, all the generic solutions of $X(\bar{c})$ are contained in $K_{E_{k+1}}$, where (CCP) is true; hence, they are countably many K_{E_j}. By induction, (CCP) holds in K_{E_α}. □

The corollary of the above propositions is that we can construct Zilber fields quite directly with a relatively simple procedure.

Let us a saturated algebraically closed field K and let us enumerate its elements as $\{\alpha_j\}_{j<|\mathbb{F}|}$ and all the absolutely free rotund varieties as $\{V_j\}_{j<|\mathbb{F}|}$. Note that we consider each variety on itself, without referencing to a defining parameter set, as the parameters are not relevant.

We can then define a sequence of exponential functions $\{E_j\}_{j\leq|\mathbb{F}|}$ in the following way. At the base step, we define $E_0(\frac{p}{q}\omega) := \zeta_q^p$, where ω is any transcendental number, and (ζ_q) is a coherent system of roots of unity.

1. if $j = k+1$,

    (a) apply DOMAIN to α_k to obtain E' from E_k;

    (b) if $\alpha_k \neq 0$, apply IMAGE to α_k to obtain E'' from E';

    (c) if V_k is E-defined over a finite $\bar{c}$, apply DOMAIN to the elements of $\bar{c}$, then if K is uncountable, apply ROOTS to $V_k(\bar{c})$, otherwise apply SOL to $V_k(\bar{c})$, and obtain E_j from E'';

2. if j is a limit ordinal, define $E_j := \bigcup_{k<j} E_k$.

By proposition 2.5, the above operations are always possible.

Corollary 2.20. *The resulting $\mathbb{F}_{E_{|\mathbb{F}|}}$ is a Zilber field.*

Proof. The starting partial E-field $\mathbb{F}_{E_0}$ clearly satisfies (SP), (STD) and (CCP) (as the domain itself is countable).

By proposition 2.5 and corollary 2.9, all the partial E-fields $\mathbb{F}_{E_j}$ exist and satisfy (SP) and (STD) for $j \leq |\mathbb{F}|$. Moreover, the function $E_{|\mathbb{F}|}$ is clearly defined everywhere and surjective, hence $\mathbb{F}_{E_{|\mathbb{F}|}}$ is an ELA-field. Finally, since we have applied either SOL or ROOTS to each absolutely free rotund variety over $\mathbb{F}$, $\mathbb{F}_{E_{|\mathbb{F}|}}$ satisfies (SEC) as well.

If $\mathbb{F}$ is countable, then (CCP) will be verified as well. If $\mathbb{F}$ is uncountable, then by proposition 2.10 the final $\mathbb{F}_{E_{|\mathbb{F}|}}$ satisfies (CCP) too.

Therefore, $\mathbb{F}_{E_{|\mathbb{F}|}}$ is a Zilber field. □

Remark 2.21. A different procedure is detailed in [Kir09], and doesn't involve systems of roots. Start with $\mathbb{F}^0_{E_0}$ equal to the "free ELA closure of SK", where SK is the field $\mathbb{Q}^{\mathrm{ab}}(\omega)$ equipped with the function $E(\frac{p}{q}\omega) := \zeta_q^p$ for some transcendental ω, and the free ELA closure is an ELA-field containing SK which is canonical in a certain way. Enumerate all the absolutely free rotund varieties $\{V_j\}_{j<\aleph_0}$, and calculate $\mathbb{F}^1_{E_1}$ by doing the following:

1. when $j = k+1$, if V_k does not contain an infinite algebraically independent set of solutions, calculate $\mathbb{F}_E|V$ ω times, where $\mathbb{F}_E|V$ is the free ELA closure of the extension of $\mathbb{F}_E$ obtained by applying SOL applied to V, starting from $\mathbb{F}^k_{E_k}$ to obtain $\mathbb{F}^j_{E_j}$;

2. when j is a limit ordinal, define $E_j := \bigcup_{k<j} E_k$ and $\mathbb{F}^k := \bigcup_{k<j} \mathbb{F}^k$.

We then iterate repeat to calculate $\mathbb{F}^2_{E_2}$, and iterate to find $\mathbb{F}^\alpha_{E_\alpha}$ for any ordinal α. Clearly, when α is a limit ordinal, the resulting ELA-field satisfies (SEC).

It is easy to see that the above calculation can be reduced to applications of DOMAIN, IMAGE and SOL. With some adjustments to the construction, and to the proof of proposition 2.19, one can check that even in this case (CCP) is always satisfied. This implies that at limit ordinals, $\mathbb{F}^\alpha_{E_\alpha}$ is a Zilber field.

Note also that the above construction can be applied when $\mathbb{F}_{E_0}$ is *any* partial E-field satisfying (SP), (STD) and (CCP), or even with trivial kernel. Hence we also have the following.

Corollary 2.22. *Any partial E-field satisfying (SP) and (CCP), and with trivial or cyclic kernel, can be strongly embedded into a Zilber field.*

Proof. If K_E is our starting field, it is sufficient to extend K to an algebraically closed field of larger cardinality $\mathbb{F}$, and possibly extend E to E_0 so that the kernel is a cyclic group. Then the above construction continues to work, and yields a Zilber field that contains K_E strongly. □

Chapter 3

Finding involutions

The whole purpose of the previous chapter is to show one way of building Zilber field on top of a prescribed algebraically closed field of characteristic 0. After a few tweaks, we can use the same construction to give more interesting information.

Suppose that K is an algebraically closed field equipped with an automorphism $\sigma : K \to K$ such that $\sigma \neq \mathrm{Id}$, but $\sigma^2 = \mathrm{Id}$, in other words, σ is an involution. In this case, K^σ is a real closed field. Can we find a function E such that K_E is a Zilber field, and σ is also an involution of K_E, while $\sigma \circ E = E \circ \sigma$? This would be a rough analogue of $\mathbb{C}_{\exp}$ equipped with complex conjugation.

With the technique of the previous chapter, and some careful adjustments, we will prove the following:

Theorem 3.36. *The Zilber field $\mathbb{B}_E$ of cardinality $2^{\aleph_0}$ has an involution whose fixed field is isomorphic to $\mathbb{R}$ with* $\ker(E) = 2\pi i\mathbb{Z}$*.*

Moreover, any separable real closed field of infinite transcendence degree occurs as the fixed field of a Zilber field of the same cardinality; in particular, every Zilber field of cardinality up to $2^{\aleph_0}$ has an involution.

This answers the question of [KMO12], and appeared in [Man11a, Man11b]. The idea of the proof is to actually start from the real closed field, and its algebraic closure, and construct, step by step, an exponential function such that the final result commutes with the involution, and the field equipped with the function is a Zilber field.

In order to clarify the meaning of $\sigma \circ E = E \circ \sigma$, so that we can describe the construction explicitly, let us copy the usual notation for $\mathbb{C}$ and $\mathbb{R}$ to our case. We denote by R the fixed field K^σ, which is a real closed field; if i is a square root of -1, we have $K = R(i)$.

We define:

1. the *real part* of $z \in K$ as $\Re(z) := \frac{z+\sigma(z)}{2}$;
2. the *imaginary part* of $z \in K$ as $\Im(z) := \frac{z-\sigma(z)}{2i}$;
3. the *modulus* of $z \in K^\times$ as $|z| := \sqrt{z \cdot \sigma(z)}$;
4. the *phase* of $z \in K^\times$ as $\Theta(z) := \frac{z}{|z|}$ (not so usual after all).

The former two are the additive decomposition of a number of K over R, the latter are its multiplicative decomposition. The image of the function Θ is the 'unit circle', and it will be denoted by $\mathbb{S}^1(K) = \{z \in K^\times : |z| = 1\}$.

It is quite easy to see the following.

Proposition 3.1. *Let K_E be a partial E-field, and $\sigma : K \to K$ be a field automorphism of order two. Then $\sigma \circ E = E \circ \sigma$ if and only if the following three conditions are satisfied:*

1. $\mathrm{dom}(E) = (\mathrm{dom}(E) \cap R) \oplus (\mathrm{dom}(E) \cap iR)$;
2. $E(R) \subset R_{>0}$;
3. $E(iR) \subset \mathbb{S}^1(K)$.

Proof. If $\sigma \circ E = E \circ \sigma$, it is clear that $\sigma(\mathrm{dom}(E)) = \mathrm{dom}(E)$, hence for each $z \in \mathrm{dom}(E)$ we have $\Re(z), i\Im(z) \in \mathrm{dom}(E)$, therefore $\mathrm{dom}(E) = (\mathrm{dom}(E) \cap R) \oplus (\mathrm{dom}(E) \cap iR)$.

For all $x \in R$ we have $\sigma(E(x)) = E(x)$, which implies $E(x) \in R$, and since $E(x) = E\left(\frac{x}{2}\right)^2$, it is actually $E(x) \in R_{>0}$; moreover, for all $y \in R$ we have $\sigma(E(iy)) = E(-iy) = E(iy)^{-1}$, i.e., $|E(iy)| = \sqrt{\sigma(E(iy))E(iy)} = 1$.

On the other hand, suppose that the three conditions are satisfied. We have then that for all $x, y \in R$, $\sigma(E(x)) = E(x)$ and $\sigma(E(iy)) = E(iy)^{-1}$. Since any $z \in \mathrm{dom}(E)$ can be written uniquely as $x + iy$ with $x, y \in R$, and $x, iy \in \mathrm{dom}(E)$, we have

$$\sigma(E(z)) = \sigma(E(x))\sigma(E(iy)) = E(x)E(iy)^{-1} = E(x - iy) = E(\sigma(z)). \qquad \square$$

Hence, constructing a function E on a given K such that $\sigma \circ E = E \circ \sigma$ can be reduced to construct a function that satisfies the conditions of proposition 3.1. In particular, it is sufficient to construct E on R and iR independently.

It is particularly easy to see how to modify DOMAIN and IMAGE to fit with the above requirements. We assume that our starting K_E already satisfies $\sigma \circ E = E \circ \sigma$.

R-DOMAIN We start with an $\alpha \in K$. If $\alpha \in \mathrm{dom}(E)$, we define $E' := E$, otherwise we do the following.
We choose two elements $\beta \in R_{>0}, \gamma \in \mathbb{S}^1(R)$ algebraically independent over $F \cup \{\Re(\alpha), \Im(\alpha)\}$, the positive roots $\beta^{1/q}$, and an arbitrary system of roots $\gamma^{1/q}$.
We define then $E'(z + \frac{p}{q}\Re(\alpha) + i\frac{p'}{q'}\Im(\alpha)) := E(z) \cdot \beta^{p/q} \cdot \gamma^{p'/q'}$ for all $z \in \mathrm{dom}(E)$ and $p, p' \in \mathbb{Z}, q, q' \in \mathbb{N}^\times$.

R-IMAGE We start with a $\beta \in K$ given as data to the operation. If $\beta \in \mathrm{im}(E)$, we define $E' := E$, otherwise we do the following.
We choose two elements $\alpha \in R, \delta \in iR$ algebraically independent over $\alpha \in F \cup \{|\beta|, \Theta(\beta)\}$, and an arbitrary coherent system of roots $\beta^{1/q}$.
We define then $E'(z + \frac{p}{q}\alpha + \frac{p'}{q'}\delta) := E(z) \cdot |\beta^{p/q}| \cdot \Theta(\beta^{p'/q'})$ for all $z \in D$ and $p, p' \in \mathbb{Z}, q, q' \in \mathbb{N}^\times$.

Finding the right equivalent of SOL and of ROOTS is non-trivial, and is worked out in the next sections.

For SOL, the main problem is that if we define E on some vector $\overline{z}$, with image $\overline{w}$, then we are defining E on $\sigma(\overline{z})$ as well, with image $\sigma(\overline{w})$; this could produce ill-defined extensions, and even when well defined, they may not be strong. Our strategy will be to make sure that the point $\overline{z}\sigma(\overline{z})\overline{w}\sigma(\overline{w})$, or equivalently $\Re(\overline{z})\Im(\overline{z})|\overline{w}|\Theta(\overline{w})$, has the maximum possible transcendence degree. We will call such points "real generic".

The problem for ROOTS is that the new operation sol does behave differently from the original one, and (CCP) may fail after several iterations. In order to get around this problem, we make sure not only that each rotund variety has real generic solutions, but also that this solutions are dense in the order topology. When R is separable, this can be done with countable sets of solutions, and it will be enough to verify (CCP).

As a start, it is immediate to see that R-DOMAIN, and R-IMAGE similarly, is a successive application of two DOMAIN, respectively IMAGE, operations. Moreover, they clearly preserve the requirements of proposition 3.1, hence $\sigma \circ E' = E' \circ \sigma$. Hence the following.

Proposition 3.2. *Given K_E with $\sigma \circ E = E \circ \sigma$, if $K_E \subset K_{E'}$ is an extension produced by* R-DOMAIN *or* R-IMAGE*, then $\sigma \circ E' = E' \circ \sigma$, and the extension is strong and kernel preserving.*

For the other operations, much more work is needed.

3.1 $\mathbb{G}$-restriction of the scalars

In order to make K_E a Zilber field, we need to add generic solutions to absolutely free rotund varieties, but we must do this while complying with the conditions of proposition 3.1. This means that when we take a generic point $\langle \overline{z}; \overline{w} \rangle$ of some absolutely free rotund variety V, we need to define E on the imaginary and real parts of the coordinates of $\overline{z}$.

However, $\langle \Re(\overline{z})\Im(\overline{z}); |\overline{w}|\Theta(\overline{w}) \rangle$ needs not to be the generic point of an absolutely free rotund variety. In general, this could end up enlarging the kernel, or producing a non-strong extension.

We get around this problem by taking $\langle \Re(\overline{z})\Im(\overline{z}); |\overline{w}|\Theta(\overline{w}) \rangle$ as generic as possible.

Definition 3.3. If V is an absolutely free rotund variety $V(\overline{c}) \subset \mathbb{G}^n$, with $\overline{c}$ closed under σ, a generic solution $\overline{z} \in K^n$ is *real generic* if

$$\mathrm{tr.deg.}_{\overline{c}E(\overline{c})} \langle \Re(\overline{z})\Im(\overline{z}); E(\Re(\overline{z})\Im(\overline{z})) \rangle = 2 \dim V.$$

A set of real generic solutions $\mathcal{S}$ of $V(\overline{c})$ is *really algebraically independent* if for any finite subset $\{\overline{z}_1, \dots, \overline{z}_k\} \subset \mathcal{S}$ the following holds:

$$\begin{aligned}\mathrm{tr.deg.}_{\overline{c}E(\overline{c})} (\langle \Re(\overline{z}_1)\Im(\overline{z}_1); E(\Re(\overline{z}_1)\Im(\overline{z}_1)) \rangle, \dots, \langle \Re(\overline{z}_k)\Im(\overline{z}_k); E(\Re(\overline{z}_k)\Im(\overline{z}_k)) \rangle) = \\ = 2k \cdot \dim V.\end{aligned}$$

The point $\langle \Re(\overline{z})\Im(\overline{z}); |\overline{w}|\Theta(\overline{w}) \rangle$ is then a generic point of a larger variety that can be defined abstractly in terms of V. In order to do that, we add another bit of notation.

Definition 3.4. We define the group $\mathbb{G}_R := (R \times R_{>0}) \times (iR \times \mathbb{S}^1(K)) \subset \mathbb{G}^2(K)$ and the *realisation* map $r : \mathbb{G} \to \mathbb{G}_R$ as follows:

$$r \,:\, (z, w) \mapsto (\Re(z), |w|) \times (i\Im(z), \Theta(w)).$$

We extend r as a map $\mathbb{G}^n \to \mathbb{G}^{2n}$ in the following way

$$r : \langle \overline{z}; \overline{w} \rangle \mapsto \langle \Re(\overline{z}); |\overline{w}| \rangle \times \langle \Im(\overline{z}); \Theta(\overline{w}) \rangle.$$

It would have been more natural to define r as the natural coordinate-wise application $\mathbb{G}^n \to \mathbb{G}_R^n$; however, since we will need to manipulate matrices, the above extension of r to $\mathbb{G}^n$ is better suited for the task.

We apply the map r to the points of rotund varieties.

Definition 3.5. Let V be a subvariety of $\mathbb{G}^n$ for some n.

1. the *realisation* of V is the set $r(V) := \{r(\langle \overline{z}; \overline{w} \rangle) \in \mathbb{G}^{2n} \,:\, \langle \overline{z}; \overline{w} \rangle \in V\}$;

2. the $\mathbb{G}$-*restriction of the scalars* of V is the Zariski closure of $r(V)$ in $\mathbb{G}^{2n}$; it will be denoted by $\check{V}$.

Clearly, when $\langle \overline{z}; \overline{w} \rangle$ is a real generic point of V, the point $\langle \Re(\overline{z})\Im(\overline{z}); |\overline{w}|\Theta(\overline{w}) \rangle$ is a generic point of $\check{V}$, moreover contained in $r(V)$.

Remark 3.6. The group $\mathbb{G}_R$ can be thought as a semi-algebraic group over R replacing iR with R and $\mathbb{S}^1(K)$ with $\{(x, y) \in R^2 : x^2 + y^2 = 1\}$. Then $r(V)$ can be seen as a semi-algebraic subvariety of $\mathbb{G}_R^n$.

The algebraic variety $\check{V}$ is similar to the classical Weil restriction of the scalars. However, unlike the classical case, while the points of $r(V)$ are in bijection with the points of V, the set of the 'real points' of $\check{V}$ is *larger* than $r(V)$.

3.2 Density

An artefact of our proof is that the behaviour of E with respect to σ is rather bad, and essentially opposite to what happens between $\mathbb{C}_{\exp}$ and complex conjugation. In our resulting K_E, the function E must satisfy an extra 'randomness' condition with respect to the *order topology* induced by R (as with $\mathbb{C}$, we use the product topology to transfer the order topology from R to $R \oplus iR = K$). The following axiom describes what happens, and actually replaces (SEC).

(DEN) for every absolutely free rotund variety $V \subset \mathbb{G}^n$ over K, every finite tuple $\overline{c} \in K^{<\omega}$ such that V is E-defined over $\overline{c}$, and every subset $U \subset V$ open w.r.t. the order topology, there is a real generic solution $\overline{z} \in K^n$ of $V(\overline{c})$ with $\langle \overline{z}; E(\overline{z}) \rangle \in U$.

The reason for this condition will be apparent during the proof, and it is one of its current limits, as it forces E not to be continuous with respect to the order topology; hence, (DEN) is not true on $\mathbb{C}_{\exp}$ and complex conjugation (however, there could be another involution of $\mathbb{C}_{\exp}$ such that (DEN) is true with respect to its topology). We will comment later on a conjectural way of avoiding this restriction.

In order to satisfy (DEN), which is stronger then (SEC), we change our operations SOL and ROOTS.

R-SOL We start with an absolutely free rotund variety $V(\overline{c}) \subset \mathbb{G}^n$, where $\overline{c}$ is a subset of K closed under σ, and an open subset $U \subset V$ in the order topology.
We choose a point $((\alpha_1, \beta_1), \ldots, (\alpha_{2n}, \beta_{2n})) \in r(V)$ generic over $F(\overline{c}E(\overline{c}))$ for $\check{V}$.
We choose a coherent system of roots $\beta_j^{1/q}$ of β_j, positive when j is odd, and we define

$$E'\left(z + \frac{p_1}{q_1}\alpha_1 + \cdots + \frac{p_{2n}}{q_{2n}}\alpha_{2n}\right) := E(z) \cdot \beta_1^{p_1/q_1} \cdot \cdots \cdot \beta_{2n}^{p_{2n}/q_{2n}}.$$

Note that R-SOL is a special case of SOL applied to $\check{V}$ in place of V, so all of the previous results about SOL apply also to R-SOL, provided that $\check{V}$ is an absolutely free rotund variety as well. We shall see in the next section that if V is absolutely free and rotund, then $\check{V}$ is indeed always absolutely free and rotund.

R-ROOTS We start with an absolutely rotund variety $V(\overline{c}) \subset \mathbb{G}^n$, where $\overline{c}$ is a finite subset of K closed under σ.
Consider an enumeration $(W_m(\overline{d}_m), U_m)_{m<\omega}$ of all the pairs composed by a variety W_m of $\mathcal{R}(V)$ and an open subset $U_m \subset W_m$ chosen among a fixed (countable) basis of the topology on W_m, where $\overline{d}_m$ is a finite subset of $\mathrm{acl}(\overline{c}E(\overline{c}))$ over which W is defined. We

produce inductively a sequence of partial exponential functions E_m, starting with $E_0 := E$. Let us suppose that E_{m-1} has been defined. If $W_m(\overline{d}_m)$ has a dense set of really algebraically independent solutions in $K_{E_{m-1}}$, we define $E_m := E_{m-1}$; otherwise we apply R-SOL to $(W_m(\overline{d}_m), U_m)$ over the E-field $K_{E_{m-1}}$. The resulting exponential function will be E_m. Finally, we define $E' := \bigcup_{m\in\mathbb{N}} E_m$.

Again, R-ROOTS is just a sequence of SOL operations, so the previous results apply.

Proposition 3.7. *If K_E has $\aleph_0$, resp. $\aleph_1$, elements algebraically independent over the field $\mathbb{Q}(\mathrm{dom}(E), \mathrm{im}(E), \overline{c})$, where $\overline{c}$ is the possible set of parameters involved in the operations, with K algebraically closed and σ an involution of K, in the latter case such that its fixed field is separable, then* R-DOMAIN, R-IMAGE *and* R-SOL, *resp.* R-ROOTS, *are applicable. Moreover, the resulting $K_{E'}$ has $\aleph_0$, resp. $\aleph_1$, elements algebraically independent over $\mathbb{Q}(\mathrm{dom}(E'), \mathrm{im}(E'))$.*

Proof. The argument is the same as in the proof of proposition 2.5. □

3.3 Rotundity for $\mathbb{G}$-restrictions

As with SOL, the application of R-SOL produces a strong extension if and only if $\check{V}$ is absolutely free rotund. If V is absolutely free and rotund, this is the case. Similarly to the previous chapter, we will use this fact to show that we can construct E-fields where E commutes with σ, and (STD), (SP) and (SEC) are satisfied.The situation of (CCP) is quite different. In section 2.7, we managed to prove that (CCP) is preserved after uncountably many iterations of the basic operations using in an essential way the fact that we applied SOL to simple varieties only.

However, for R-SOL, even if V is simple, the corresponding $\check{V}$ is never simple, as the following trivial equation implies:

$$\dim \begin{pmatrix} \mathrm{Id} & \mathrm{Id} \end{pmatrix} \cdot \check{V} = \dim V = \mathrm{rank} \begin{pmatrix} \mathrm{Id} & \mathrm{Id} \end{pmatrix}.$$

A different argument is needed for the new operation R-SOL. The first thing we have to control is how far $\check{V}$ is from being simple. It turns out that the above example is essentially the only possible way in which $\check{V}$ is not simple.

Theorem 3.8. *Let V be an absolutely irreducible simple variety. Then $\check{V}$ is an absolutely free, absolutely irreducible rotund variety.*

Moreover, if $\dim M \cdot \check{V} = \mathrm{rank} M$ for some non-zero integer matrix of maximum rank, then V is perfectly rotund, and one of the following holds:

1. $\mathrm{rank} M = 2n$;
2. $\mathrm{rank} M = n$, *and M is of the form*
$$M = \begin{pmatrix} N & Q \end{pmatrix}$$
where N, Q are two square invertible matrices.

The proof requires several steps. From now on, let us suppose that $\check{V}$ is E-defined over some $\overline{c}$.

Proposition 3.9. *If $V \subset \mathbb{G}^n$ is absolutely irreducible, then $\check{V}$ is absolutely irreducible.*

Proof. Let V' be an absolutely irreducible variety such that $2 \cdot V' = V$.

There is a map $V' \times (V')^\sigma \mapsto \mathbb{G}^{2n}$ described by the following equation:

$$\prod_{i=1}^{n}(z_i, w_i) \times \prod_{i=1}^{n}(z'_i, w'_i) \mapsto \prod_{i=1}^{n}(z_i + z'_i, w_i w'_i) \times \prod_{i=1}^{n}\left(z_i - z'_i, \frac{w_i}{w'_i}\right).$$

It is clear that on the Zariski dense subset of $V' \times (V')^\sigma$ described by the points $P \times P^\sigma$, for $P \in V'$, the image is exactly $r(V)$; taking the Zariski closure, we obtain that this is a surjective map from $V' \times (V')^\sigma$ to $\check{V}$.

However, $V' \times (V')^\sigma$ is an absolutely irreducible variety, as it is a product of two absolutely irreducible varieties; hence $\check{V}$ is also absolutely irreducible. □

Proposition 3.10. *If $V \subset \mathbb{G}^n$ is absolutely free, then $\check{V}$ is absolutely free.*

Proof. Let $x_1, \ldots, x_n, y_1, \ldots, y_n$ be the additive coordinates of $\check{V}$; by x_i we mean the coordinates coming from the real parts of V, and by y_i the imaginary parts.

Let us suppose that for $m_1, \ldots, m_n, p_1, \ldots, p_n$ the function

$$m_1 x_1 + \cdots + m_n x_n + p_1 y_1 + \cdots + p_n y_n$$

has finite image on $\check{V}$. In particular, it is true on the points of $r(V)$; this implies that the functions

$$m_1 x_1 + \cdots + m_n x_n,\ p_1 y_1 + \cdots + p_n y_n$$

have finite image as well. However, this implies also that the image of

$$m_1 z_1 + \cdots + m_n z_n,\ p_1 z_1 + \cdots + p_n z_n$$

is not a cofinite set. By strong minimality, this implies that $m_1 z_1 + \cdots + m_n z_n$ and $p_1 z_1 + \cdots + p_n z_n$ have both finite image, but by absolute freeness of V, this implies $m_1 = \cdots = m_n = 0$ and $p_1 = \cdots = p_n = 0$.

The same argument applied to the multiplicative coordinates $\rho_1, \ldots, \rho_n, \theta_1, \ldots, \theta_n$ yields the absolute freeness of V. □

In particular, when V is an absolutely irreducible simple variety, as it is in our construction, the variety $\check{V}$ is absolutely free and absolutely irreducible. We still have to verify if it is rotund, and how far it is from being simple.

From now on, let us suppose that M is a non-zero integer matrix in $\mathcal{M}_{k,2n}(\mathbb{Z})$ of maximum rank, and that V is an absolutely irreducible simple variety. We want to determine as much as possible on $\dim M \cdot \check{V}$, in order to show that $\check{V}$ is rotund.

The main technical challenge comes from taking the functions on V as 'complex-valued', or 'two-dimensional' functions (i.e., such that their image is the complex plane minus a finite set), splitting them into components making them 'real-valued', or more precisely 'one-dimensional', and then recombining them into two-dimensional functions again. The philosophy is that unless the recombination happens in a special way, then the algebraic relations are destroyed in the process. In order to prove this, we will introduce a bit of ad-hoc notation to deal with the mixed case where some functions have been recombined into two-dimensional functions, but some still appear as one-dimensional.

The proof of the theorem then starts with finding a minimal matrix $\check{M}$ such that the coordinate functions of $M \cdot r(V)$, which can be mixed real and complex-valued, can be recovered from the coordinate functions of $r(\check{M} \cdot V)$, which are the real-valued components of the complex-valued functions of $\check{M} \cdot V$. In particular, the additive coordinates of $M \cdot r(V)$ will be recovered as $\mathbb{Q}$-linear combinations of the ones of $r(\check{M} \cdot V)$, while the multiplicative coordinates of $M \cdot r(V)$ will be multiplicatively dependent on the ones of $r(\check{M} \cdot V)$.

We then extract a special algebraically independent set of (real-valued) coordinate functions of $r(\check{M} \cdot V)$, and we will transform it to a set of (mixed) coordinate functions of $M \cdot r(V)$, such in a way that the algebraic independence is preserved. This will imply a lower bound on the dimension of $M \cdot r(V)$, and in turn of $M \cdot \check{V}$, proving that it is rotund. Moreover, when $\dim M \cdot \check{V} = \mathrm{rank} M$, we shall be able to track back the equality to $r(\check{M} \cdot V)$ and to $\check{M} \cdot V$. The simpleness of V will then imply that $\check{M}$, and in turn M, can only have a special form, proving the theorem.

3.3.1 Mixed functions

Let S be an algebraically independent subset of the coordinate functions of $M \cdot \check{V}$. Taking the restrictions to the subset $M \cdot r(V) \subset M \cdot \check{V}$, we can try to estimate the actual size of $M \cdot \check{V}$ by studying how the functions of S behave on the points of $M \cdot r(V)$, more precisely looking at how large is their image.

Note that each function in S is of the form $\overline{m} \cdot \overline{x} + \overline{q} \cdot \overline{y}$ or $\overline{\rho}^{\overline{m}} \overline{\theta}^{\overline{q}}$, where $(\overline{m}, \overline{q})$ is a row of M, and $\overline{x}, \overline{y}, \overline{\rho}, \overline{\theta}$ are the coordinate functions of $r(V)$ as a semi-algebraic variety. We introduce the following notation.

Notation 3.11. If S is a set of coordinates as above, we denote by $r(S)$ the subset of the coordinate functions of the semi-algebraic variety $r(V)$ containing $\overline{m} \cdot \overline{x}$, $\overline{q} \cdot \overline{y}$, $\overline{\rho}^{\overline{m}}$, $\overline{\theta}^{\overline{q}}$ for each $\overline{m} \cdot \overline{x} + \overline{q} \cdot \overline{y}$ or $\overline{\rho}^{\overline{m}} \overline{\theta}^{\overline{q}}$ in S.

We know that in general $\mathrm{tr.deg.}_{\overline{c}E(\overline{c})}(S) \geq \mathrm{tr.deg.}_{\overline{c}E(\overline{c})}(r(S))/2$, but this is far from being enough for our purposes. We can produce a better estimate by distinguishing, among the coordinate functions in S, the ones that vary in a one-dimensional set, and the ones that vary in a two-dimensional set, when we look at the points of $M \cdot r(V)$ only. The idea is that if one function is two-dimensional, then it contributes with transcendence degree 1 to $\mathrm{tr.deg.}_{\overline{c}E(\overline{c})} S$, but it needs two algebraically independent functions in $r(S)$ to be calculated; on the other hand, a one-dimensional function only needs one function of $r(S)$.

This is explained by the following example. Suppose that $x_1 + y_1, x_2 + y_2, x_3 + y_3$ are the coordinate functions of $\mathbb{A}^3(K)$, with x_j and y_j being their real and imaginary parts as in our current notation. Let S be $\{x_1 + y_1, x_2 + y_1, x_3 + y_1\}$. The set $r(S)$ is equal to $\{x_1, x_2, x_3, y_1\}$; hence, the rough estimate on the transcendence degree would just prove that $\mathrm{tr.deg.} S \geq 2$. However, it is clear that even if we fix the values of $x_1 + y_1$ and of $x_2 + y_1$, the remaining function $x_3 + y_1$ is still able to vary in an infinite set, so it must be $\mathrm{tr.deg.} S = 3$. This can be seen explicitly by noting that fixing $x_1 + y_1$ actually fixes the values of two functions in $r(S)$, but once that is done, fixing the value of $x_2 + y_1$ only fixes one function of $r(S)$, leaving a third one free to vary. We would like to say that $x_1 + y_1$ is 'two-dimensional', but that $x_2 + y_1$ is not.

The example shows that the definition should depend on the order of the functions: if we fix $x_2 + y_1$ first, then $x_1 + y_1$ would become 'one-dimensional'. Therefore, we define the dimensionality looking at *sequences* of functions in S.Let $(s_j)_{j<|S|}$ be a given enumeration of S.

Definition 3.12. A coordinate function $s_k \in S$ is *one-dimensional* (resp. *two-dimensional*, *zero-dimensional*) if $\mathrm{tr.deg.}_{\overline{c}E(\overline{c}), r(s_0, \ldots, s_{k-1})} r(s_k)$ is one (resp. two, zero).

Looking at the values of the functions on the points of $M \cdot r(V)$, a coordinate function is one-dimensional (resp. two-dimensional, zero-dimensional) if after fixing the values of the functions $s_0, \dots, s_{k-1}$ on $r(V)$, the image of s_k on $r(V)$ is generically a one-dimensional (resp. two-dimensional, zero-dimensional) subset of $K = R^2$. The following remark is now rather trivial, and shows the better estimate we were looking for.

Proposition 3.13. *Let S be a set of coordinate functions of $M \cdot \check{V}$ enumerated as $(s_j)_{j<|S|}$. If S contains k_1 one-dimensional functions, and k_2 two-dimensional functions, then $|S| = k_1 + k_2$ and* $\mathrm{tr.deg.}_{\overline{c}E(\overline{c})}(r(S)) = k_1 + 2k_2$.

Indeed, this is our desired correction: $\mathrm{tr.deg.}_{\overline{c}E(\overline{c})} S > \mathrm{tr.deg.}_{\overline{c}E(\overline{c})}(r(S))/2$ as soon as there are one-dimensional functions, so that we get a better bound. Moreover, number of one-dimensional functions is independent from the ordering of S.

If the dimensionality of a function does not change with the ordering, we call it pure.

Definition 3.14. A coordinate function x in S of $M \cdot \check{V}$ is *pure* if its dimension is the same in any ordering of S.

The set S is said to be *pure* if all of its functions are pure.

3.3.2 Reduction to $\check{M} \cdot V$

In order to find $\check{M}$, we first reduce M to a special form, where many linear dependences between the rows are removed.

Proposition 3.15. *There is a matrix $A \in \mathcal{M}_{k,k}(\mathbb{Z})$ of maximum rank such that $A \cdot M$ is of the following form*

$$A \cdot M = \left(\begin{array}{cc} & 0 \\ M_1 & P_1 \\ & Q_1 \\ \hline 0 & P_2 \\ 0 & Q_2 \end{array} \right)$$

with the following properties:

1. *M_1 has n columns;*
2. *the rows of M_1 are $\mathbb{Q}$-linearly independent;*
3. *the rows of M_1, P_1 and P_2 are $\mathbb{Q}$-linearly independent;*
4. *the rows of P_1, P_2, Q_1 and Q_2 are $\mathbb{Q}$-linearly independent.*

Note that with this decomposition, a suitable $\check{M}$ is the matrix

$$\begin{pmatrix} M_1 \\ P_1 \\ P_2 \end{pmatrix}.$$

Indeed, all the coordinate functions of $M \cdot r(V)$ are dependent on the ones of $r(\check{M} \cdot V)$; moreover, its rows are $\mathbb{Q}$-linearly independent, so no smaller matrix can have the same property.It amounts to using row operations in the correct order on M.

Proof. First of all, we look at the first n columns of the matrix, and we use the row operations to eliminate all the redundant vectors until we are left with some $\mathbb{Q}$-linearly independent rows, which we reorder to be in the first part of the matrix. In this way, we split the matrix into an upper half and a lower half, where the lower half has zero entries in the first n columns, and the upper half restricted to the same columns has rank equal to the number of its rows.

Now, we concentrate on the other n columns. The lower half of the matrix is made of $\mathbb{Q}$-linearly independent rows, by the original hypothesis on the rank of M. We leave them untouched, while using them in the upper half in order to eliminate the redundancies again. The row operations on the upper half cannot harm the $\mathbb{Q}$-linear independence of the first n columns. We reorder the rows so to have all the zeroes of the last n columns at the beginning, as in the figure.

At the end of these operations, we have defined M_1 as the north-west corner; we just have to look at a maximal set of rows for the last n columns which is $\mathbb{Q}$-linearly independent over the rows of M_1 in order to define who P_1, P_2, Q_1 and Q_2 are. $\square$

Since $\dim(A \cdot M \cdot \check{V}) = \dim(M \cdot \check{V})$, as A is invertible over $\mathbb{Q}$, we may assume that M is already of the above form.

Let $\check{M}$ be the matrix

$$\check{M} := \begin{pmatrix} M_1 \\ P_1 \\ P_2 \end{pmatrix}.$$

By construction, $\check{M}$ has rank equal to the number of its rows.

3.3.3 Finding many one-dimensional functions

We want now to find a set S of algebraically independent functions containing many one-dimensional functions. Clearly, for such a set S we have $\dim(M \cdot \check{V}) \geq |S|$.

In order to do that, we start from a particular set of coordinate functions of $\check{M} \cdot V$ and we transform it, using additive and multiplicative combinations, to a set of coordinate functions of $M \cdot r(V)$, while preserving algebraic independence. Choosing the right sets at the beginning, we will be able to prove that the final set is indeed large, algebraically independent and contains enough one-dimensional functions to obtain the rotundity of $\check{V}$.

First of all, we describe the set of manipulations we operate on the coordinate functions of $\check{M} \cdot V$. Let B be a set of coordinate functions on $r(\check{M} \cdot V)$.

Let q be the number of rows of Q_1. There are q rows of M_1, say $\overline{m}_1, \ldots, \overline{m}_q$, and a numbering of the rows of Q_1, say $\overline{q}_1, \ldots, \overline{q}_k$, such that for any $0 \leq j \leq q$, the $\mathbb{Q}$-linear span of $\overline{q}_1, \ldots, \overline{q}_j, \overline{m}_{j+1}, \ldots, \overline{m}_q$ together with the remaining rows of M_1, and the rows of P_1, P_2 is constant. In other words, the row $\overline{m}_1$ can be written as a $\mathbb{Q}$-linear combination of $\overline{q}_1, \overline{m}_2, \ldots, \overline{m}_k$ and of the remaining rows of $\check{M}$; then $\overline{m}_2$ can be written as a $\mathbb{Q}$-linear combination of $\overline{q}_1, \overline{q}_2, \overline{m}_3, \ldots, \overline{m}_k$ and the rest of $\check{M}$, and so on.

We call f_0 the map that sends $\overline{m}_j \cdot \overline{y} \mapsto \overline{q}_j \cdot \overline{y}$ and $\overline{\theta}^{\overline{m}_j} \mapsto \overline{\theta}^{\overline{q}_j}$, for $j = 1, \ldots, q$, and is the identity on the rest of the coordinate functions of $r(\check{M} \cdot V)$. If B is algebraically independent, then $f_0(B)$ is algebraically independent. Indeed, by the above construction of the map $\overline{m}_j \mapsto \overline{q}_j$, if we replace the functions one by one, starting with $j = 1$ and proceeding in order, the algebraic independence of B is preserved during the procedure, hence $f_0(B)$ is also algebraically independent (over $\overline{c}E(\overline{c})$). Indeed, at each replacement, the new function is either interalgebraic with the previous one, which means that all the functions needed to write $\overline{q}_j \cdot \overline{y}$ as a combination of $\overline{m} \cdot \overline{y}$'s are algebraic over B, or it is algebraically independent from B; in both cases, after the replacement the functions remain algebraically independent.

Now, call $f_1(B)$ the set $f_0(B) \cap r(C)$, where C is the set of the coordinate functions of $M \cdot r(V)$. In other words, $f_1(B)$ contains the functions of $f_0(B)$ that actually make an appearance as component of the coordinate functions of $M \cdot r(V)$. Finally, call $f_2(B)$ the set $f_1(B) \cap C$, in other words, the functions of $f_1(B)$ that correspond to the rows of M of the form $(\overline{m}, 0)$ and $(0, \overline{q})$, so that they are not summed with other functions when constructing the final coordinates of $M \cdot r(V)$. When the starting B is algebraically independent, the functions in $f_2(B)$ are purely one-dimensional as functions of $f_1(B)$, as their values are forced to vary in a one-dimensional set, while algebraic independence guarantees that they are never zero-dimensional.

In order to find our special set of coordinate functions of $\check{M} \cdot V$ to which apply the above transformations, we start from a classical combinatorial lemma [Hal35] applied to the matroid given by the algebraic closure. We just state the special instance needed for our proof.

Lemma 3.16 (Hall's Marriage Lemma)**.** *Let $X = \{x_j\}_{1\le j\le n}$ and $Y = \{y_j\}_{1\le j\le n}$ be two subsets of some field L, and $\overline{c}$ some finite subset of L.*

If $\mathrm{tr.deg.}_{\overline{c}} \bigcup_{j\in T}\{x_j, y_j\} \ge |T|$ for all $T \subset \{1, \dots, n\}$, then there is a subset $Z \subset X \cup Y$ such that

1. *$|Z \cap \{x_j, y_j\}| = 1$ for all $j \in \{1, \dots, n\}$;*
2. *$\mathrm{tr.deg.}_{\overline{c}} Z = |Z| = n$.*

If we take $L = K(W)$, where $W \subset \mathbb{G}^n$ is some rotund variety defined over some $\overline{c} \subset K$, and we take as X the additive coordinate functions of V and as Y the multiplicative coordinate functions of V, then by rotundity the hypothesis of lemma 3.16 are satisfied. Hence, we can choose an algebraically independent set of coordinate functions such that for each factor $\mathbb{G}$ of $\mathbb{G}^n$ exactly one of the two functions appear in the set.

By lemma 3.16 applied to the coordinate functions of $\check{M} \cdot V$, there is a maximal algebraically independent set H_0 of functions such that for each row $\overline{m}$ of $\check{M}$, at least one of $\overline{m} \cdot \overline{z}$ or $\overline{w}^{\overline{m}}$ is in it; let H be $r(H_0)$. This is our special set.

Let S be any maximal algebraically independent set of coordinate functions of $M \cdot r(V)$ containing $f_2(H)$. We claim that S_2 witnesses the rotundity of $\check{V}$, i.e., $|S_2| \ge \mathrm{rank}M$. Let us call m the number of rows of M of the form $(\overline{m}, \overline{q})$ with both $\overline{m}, \overline{q}$ not zero. Let k_1 the number of one-dimensional functions in S_2 , and k_2 the number of two-dimensional functions (in any ordering). Since $f_2(H)$ is pure and all its functions are one-dimensional, we know at least that $k_1 \ge |f_2(H)| \ge \mathrm{rank}M - m$.

Proposition 3.17. *The inequality $|S| \ge \mathrm{rank}M$ holds.*

In particular, $\dim M \cdot \check{V} = |S| \ge \mathrm{rank}M$, and $\check{V}$ is rotund.

Proof. By construction, $\mathrm{tr.deg.}_{\overline{c}E(\overline{c})} f_1(H) = |f_1(H)| = \mathrm{rank}M + m$.

Since S is maximal, $r(S)$ is algebraically independent and contains at least as many functions as $f_1(H)$, hence at least $\mathrm{rank}M + m$. Since $\mathrm{tr.deg.}_{\overline{c}E(\overline{c})}(r(S_0)) = k_1 + 2k_2$, this implies

$$k_1 + 2k_2 \ge \mathrm{rank}M + m.$$

Together with $k_1 \ge \mathrm{rank}M - m$ we obtain

$$2|S_0| = 2(k_1 + k_2) \ge 2\mathrm{rank}M$$

as desired. □

However, the maximality of S implies further consequences if $\dim M \cdot \check{V} = |S| = \mathrm{rank}M$.

Proposition 3.18. *If $\dim M \cdot \check{V} = \mathrm{rank}M$:*

1. *S is pure, and $k_1 = \mathrm{rank}M - m = |f_2(H)|$;*

2. V is perfectly rotund;

3. $\mathrm{rank}\check{M} = n$.

Proof. If $\dim M \cdot \check{V} = \mathrm{rank}M$, then $|S| = \mathrm{rank}M$. By $k_1 + k_2 = |S| = \mathrm{rank}M$, and $k_1 + 2k_2 = \mathrm{rank}M + k_2 \geq \mathrm{rank}M + m$, we deduce that $k_2 \geq m$; but we know also that $k_1 \geq \mathrm{rank}M - m_1$, hence we must have the two equalities $k_2 = m$, $k_1 = \mathrm{rank}M - m$.

The first equality $k_1 = \mathrm{rank}M - m$ implies that all the one-dimensional coordinates are exactly the functions in $f_2(H)$. They are pure by construction, as they correspond to the rows of M of the form $(\overline{m}, 0)$ or $(0, \overline{q})$.

Since the k_1 one-dimensional functions are all pure and one-dimensional, the remaining k_2 functions are forced to be all two-dimensional in whatever order we take them. Hence, S is pure.

Moreover, the equality implies $|f_2(H)| = \mathrm{rank}M - m$. This implies that for each row of M of the form $(\overline{m}, 0)$ or $(0, \overline{q})$, the set $f_1(H)$ contains *exactly* one of the two functions $\overline{m} \cdot \overline{x}$, $\overline{\rho}^{\overline{m}}$ or respectively $\overline{q} \cdot \overline{y}$, $\overline{\theta}^{\overline{q}}$. Since $|r(S) \setminus f_2(H)| = 2m$, we also have that for each row of M of the form $(\overline{m}, \overline{q})$ with $\overline{m}, \overline{q} \neq 0$, the set $f_1(H)$ contains *exactly* one of the two pairs $\{\overline{m} \cdot \overline{x}, \overline{q} \cdot \overline{y}\}$ and $\{\overline{\rho}^{\overline{m}}, \overline{\theta}^{\overline{q}}\}$. This can only happens if the original H_0 contains exactly one function between $\overline{m} \cdot \overline{z}$ and $\overline{w}^{\overline{m}}$ for each row $\overline{m}$ of $\check{M}$. In particular, $|H_0| = \mathrm{rank}\check{M}$, hence $\dim \check{M} \cdot V = \mathrm{rank}\check{M}$.

But since V is simple, this implies $\mathrm{rank}\check{M} = n$, and that V is perfectly rotund. □

Once we know that S is pure, however, we can actually deduce that all the functions in S have the same dimensionality, and this yields further information.

Before proving that they must have the same dimensionality, let us analyse the special subcase when S is composed only of one-dimensional functions (hence $f_2(H) = S$). In order to fully comprehend this case, we first need to establish the following two algebraic facts, which both derive from the following classical statement. Given two rational non-constant functions on a curve over $\mathbb{C}$, it is always possible to expand one function as a convergent analytic series of the other one around points where the latter function is not ramified; and when ramified, it is sufficient to extract a kth root of the second function, in which case the series is called "Puiseux series". The following version of this theorem is a reformulation for general real closed fields where we cannot have convergent series, but only finite expansions with controlled error terms.

Lemma 3.19 (Puiseux series)**.** *Let z be a non-constant regular functions on an algebraic curve $\mathcal{C}$ defined over K. Let $P \in \mathcal{C}$ be a zero of z.*

There are an open disc $D \subset K$, a definable continuous map $s : D \to \mathcal{C}$ and an integer $d > 0$ such that for all $\alpha \in D$, $z(s(\alpha)) = \alpha^d$. Moreover, for any function $w \in K(\mathcal{C}) \setminus \{0\}$ regular at P, there are an integer $k \geq 0$, an $a \in K \setminus 0$, and a number $N \in R_{>0}$ such that for all $\alpha \in D$

$$|w(s(\alpha)) - a\alpha^k| \leq N \cdot |\alpha^{k+1}|.$$

Proof. In the case $R = \mathbb{R}$, $K = \mathbb{C}$, this is a classical statement of algebraic and analytic geometry: given a desingularization $\tilde{\mathcal{C}} \xrightarrow{\pi} \mathcal{C}$, for any point $P' \in \pi^{-1}(P)$, there is a local parameter $t_{P'} \in \mathbb{C}(\mathcal{C})$, an open disc $D \subset \mathbb{C}$ centred in 0, and an analytic function $s : D \to \tilde{\mathcal{C}}(\mathbb{C})$ with $s(0) = P'$ and $t_{P'}(s(\alpha)) = \alpha$ for all $\alpha \in D$. Moreover, $z(s(\alpha))$ and $w(s(\alpha))$ can be expressed as convergent analytic power series in α. After an analytic transformation, one can find a function $s' : D \to \tilde{\mathcal{C}}(\mathbb{C})$ such that $z(s'(\alpha)) = \alpha^d$ for all $\alpha \in D$, where d in the ramification index of z at P'. We obtain our desired function taking the composition $\pi \circ s'$; since $w(s'(\alpha))$ is analytic in α as well, the inequality is satisfied.

In the general case, we still have the existence of a desingularization and of a local parameter $t_{P'} \in K(\mathcal{C})$, equipped with a continuous section $s : D \to \mathcal{C}(K)$. In order to replace the analytic argument, we observe that the following statement is true on $R = \mathbb{R}$: given w there is an open neighbourhood U of P, a positive $N \in R_{>0}$, finitely many numbers $a_j \in K \setminus \{0\}$ and integers $k_j \geq 0$, $d_j > 0$ such that for all $Q \in \mathcal{C} \cap U$ there is a j and a determination of $z^{1/d_j}(Q)$ such that

$$\left| w(Q) - a_j z^{\frac{k_j}{d_j}}(Q) \right| \leq N \cdot \left| z^{\frac{k_j+1}{d_j}}(Q) \right|.$$

It can be deduced by taking local parameters at each point P' over P in the desingularization of $\mathcal{C}$. Since the ramification indices d_j are bounded by $\deg(z)$, the exponents k_j are bounded by $\deg(w)$, and the number of local parameters is bounded by $\min\{\deg(z), \deg(w)\}$, the statement can be expressed with a first-order formula uniformly in the parameters defining $\mathcal{C}$, z and w. In particular, the statement is true on any real closed field.

Therefore, given the section $s : D \to \mathcal{C}(K)$ of a local parameter $t_{P'}$, there is an open disc $D' \subset D$ such that there exists one of the above inequalities that is satisfied for all $Q \in s(D')$. The determination of $z^{1/d_j}(Q)$ will depend on the $\alpha \in D'$ such that $s(\alpha) = Q$, and if D' is small enough, the determination of z^{1/d_j} is uniquely determined by α. Hence the inequality defines a section $s' : D' \to \mathcal{C}(K)$ such that $z(s'(\alpha)) = \alpha^d$, proving the statement. □

We use it to prove the algebraic independence of the various realisations of the coordinate functions.

Lemma 3.20. *Let V be an absolutely irreducible algebraic variety such that $\check{V}$ is defined over some $\bar{c}$. Let B be some set of algebraically independent functions on V, and let w be a function on V contained in* $\operatorname{acl}(B\bar{c})$.

If $|w| \in \operatorname{acl}(\{|z| : z \in B\} \cup \bar{c})$, or if $\Theta(w) \in \operatorname{acl}(\{\Theta(z) : z \in B\} \cup \bar{c})$, then w is multiplicatively dependent over B modulo constants.

Proof. We may assume that B is minimal, i.e., that $w \notin \operatorname{acl}(B \cup \{\bar{c}\} \setminus \{z\})$ for all $z \in B$. If $B = \emptyset$, then $w \in \operatorname{acl}(\bar{c})$, and we are done. We proceed by induction on $|B|$. Let us suppose $|B| \geq 1$.

Let us take one function $z \in B$. By minimality of B, there is a polynomial relation

$$p(z, w) = 0$$

with coefficients in $\mathbb{Q}(\bar{c}, B \setminus \{z\})$. Let us specialise all the variables in $B \setminus \{z\}$ such in a way that the above polynomial contains occurrences of both z and w. The equation defines an affine plane curve $\mathcal{C}$ with coordinate functions z and w, both non-constant. Up to replacing w with w^{-1}, we may assume that $\mathcal{C}$ contains a point P such that $z(P) = 0$.

We apply lemma 3.19 to the function z twice. First, we find a section $s : D \to \mathcal{C}(K)$ such that $z(s(\alpha)) = \alpha^d$, and moreover $a \in K^\times$, $N \in R_{>0}$ and $k \geq 0$ such that

$$|w(s(\alpha)) - a\alpha^k| \leq N \cdot |\alpha^{k+1}|.$$

Then we calculate the corresponding bounds for the function $w^d - az^k$. If it turns out to be constant, then $w^d z^{-k}$ is contained in $\operatorname{acl}(B \cup \{\bar{c}\} \setminus \{z\})$; moreover, since $|w^d z^{-k}|$ depends only on the moduli of the functions in B, but it does not depend on z, we have that $|w^d z^{-k}| \in \operatorname{acl}(\{|z'| : z' \in B \setminus \{z\}\} \cup \bar{c})$. By induction, the function $w^d z^{-k}$ is multiplicatively dependent over $B \setminus \{z\}$ modulo constants, hence w is dependent over B modulo constants, as desired. The same argument applies for $\Theta(w^d z^{-k})$, yielding the desired conclusion for $\Theta(w)$.

Otherwise, we find $b \in K^\times$, $m > 0$ and $S \in R_{>0}$ such that

$$\left| w(s(\alpha)) - a\alpha^k - b\alpha^{k+m} \right| \leq S \cdot \left| \alpha^{k+m+1} \right|.$$

Let us study the case of $|w|$. Looking at the modulus of w, we have

$$\left||w(s(\alpha))| - \left|a\alpha^k + b\alpha^{k+m}\right|\right| \leq S \cdot \left|\alpha^{k+m+1}\right|.$$

Now, let $n > 0$ be any positive integer. Let c_n be a number in $R_{>0}$ such that $c_n \in D$ and

$$c_n \leq \frac{|b|}{nS}.$$

We claim that the number of values of $|w|$ on the points $s(\alpha)$ with $|\alpha| = c_n$ is at least n. Since $|w|$ is interalgebraic with $|z|$, and $|z(s(\alpha))| = |\alpha|^d$ would be constantly c_n, the number of values of $|w|$ on the points with fixed $|z|$ should be bounded by an integer independent of c_n, a contradiction.

Indeed, if $|\alpha|$ is fixed to be c_n, the modulus of $\left|a\alpha^k + b\alpha^{k+m}\right|$ takes all the values of an interval around $|a|c_n^k$ of radius $|b|c_n^{k+m}$, while the error term in the above estimate for $|w|$ is at most $S \cdot c_n^{k+m+1}$. This implies that $|w(s(\alpha))|$ takes at least n different values.

If instead we take $\Theta(w)$, then

$$|\Theta(w(s(\alpha))) - \Theta(a\alpha^k + b\alpha^{k+m})| \leq S \cdot |\alpha^{k+m+1}| \cdot \max\left\{\frac{1}{|w(s(\alpha))|}, \frac{1}{|a\alpha^k + b\alpha^{k+m}|}\right\}.$$

We do a similar argument with different numbers. Consider the sequence

$$\alpha_n = \frac{1}{8^n} \min\left\{c_0, \frac{1}{4S} \cdot \frac{1}{\max\{|a|, |b|\}} \cdot \left|\frac{b}{a}\right|\right\} \cdot \theta,$$

where $\theta \in \mathbb{S}^1(K)$ is a fixed number such that $\Theta(\frac{b}{a}\theta^m) = i$, and c_0 is as before. In this case, we can write

$$\Theta\left(a\alpha_n^k + b\alpha_n^{k+m}\right) = \Theta\left(a\alpha_n^k\right) \cdot \Theta\left(1 + \frac{b}{a}\alpha_n^m\right) = \Theta\left(a\right) \cdot \Theta(\theta)^k \cdot \Theta\left(1 + i\left|\frac{b}{a}\alpha_n^m\right|\right)$$

so that

$$\left|\Theta(w(s(\alpha))) \cdot \Theta(a \cdot \theta^k) - \Theta\left(1 + i\left|\frac{b}{a}\alpha_n^m\right|\right)\right| \leq 4 \cdot S \cdot \max\{|a|, |b|\} \cdot |\alpha_n|^{m+1}.$$

We estimate the imaginary part of the second summand with

$$\frac{1}{2}\left|\frac{b}{a}\alpha_n^m\right| \leq \Im\left(\Theta\left(1 + i\left|\frac{b}{a}\alpha_n^m\right|\right)\right) \leq \left|\frac{b}{a}\alpha_n^m\right|.$$

However, thanks to the choice of α_n, we have that the error term is smaller

$$4 \cdot S \cdot \max\{|a|, |b|\} \cdot |\alpha_n|^{m+1} \leq \frac{1}{8^n}\left|\frac{b}{a}\alpha_n^m\right|.$$

Since $\alpha_n = \frac{1}{8}\alpha_{n-1}$, this implies that the values of $\Theta(w(s(\alpha_n)))$ are all distinct as n varies over the positive natural numbers. On the other hand, $\Theta(z(s(\alpha_n))) = \Theta(\alpha_n^d) = \theta^d$; as before, this implies that $\Theta(w)$ is algebraically independent from $\Theta(z)$, a contradiction. □

Lemma 3.21. *Let V be an absolutely irreducible algebraic variety such that V is defined over some $\bar{c}$. Let B be some set of algebraically independent functions on V, and let w be a function on V contained in* $\operatorname{acl}(B\bar{c})$.

The function $|w|$ (or $\Theta(w)$) cannot be interalgebraic with $\Re(z)$, $\Im(z)$, or $\Theta(z)$ (resp. $|z|$) over $r(B \setminus \{z\}) \cup \bar{c}$ for any $z \in B$.

Proof. Let us suppose by contradiction that the thesis is false. This implies that w is interalgebraic with z over $B \setminus \{z\} \cup \bar{c}$. As above, we find a polynomial such that

$$p(z, w) = 0$$

and a piece of Puiseux series. This time, we take just one term. Let s be the section with $\alpha^d = z(s(\alpha))$.

For $|w|$, we calculate the modulus:

$$\big||w(s(\alpha))| - |a\alpha^k|\big| \leq N \cdot |\alpha^{k+1}|.$$

For $\Theta(w)$:

$$|\Theta(w(s(\alpha))) - \Theta(a\alpha^k)| \leq N \cdot |\alpha^{k+1}| \cdot \max\left\{\frac{1}{|w(s(\alpha))|}, \frac{1}{|a\alpha^k|}\right\}.$$

If ζ_n is the non-trivial nth root of unity closest to 1, we have the estimate $|1 - \zeta_n| \geq 7/n$. If α_j is a sequence such that

- $\Theta(\alpha_j) = \zeta_n^j$,
- $|\alpha_j| < \frac{7}{4nN|a|}, c_0$,

for j that takes at least j_0 different residue classes modulo n, then $\Theta(w(\alpha_n))$ takes at least j_0 different values. Indeed, the distance between $\Theta(\zeta_n^j)$ and $\Theta(\zeta_n^{j'})$, when $j \not\equiv j' \mod n$, is at least $7/n$, while $\Theta(w(s(\alpha_j)))$ is far less than $7/2n$ from $\Theta(\alpha_j) = \zeta_n^j$.

We can either take

1. $\alpha_j := \frac{|a|}{2N} \cdot \frac{7}{2n} \cdot \zeta_n^j$, so that $|z(s(\alpha_j))|$ is constant but $\Theta(w(s(\alpha_j)))$ takes at least n different values, or
2. $\alpha_j := \frac{|a|}{2N} \cdot \frac{7}{2n} \cdot \zeta_n^j \cdot \Re(\zeta_n^{dj})^{-1/d} \cdot \Re(\zeta_n^{dm})^{1/d}$ for $n = 4dm + 1$ and $-m \leq j \leq m$, so that $\Re(z(s(\alpha_j))) = \Re(\alpha_j^d)$ is fixed, but $\Theta(w(s(\alpha_j)))$ takes at least $2m + 1$ different values, or
3. $\alpha_j := \frac{|a|}{2N} \cdot \frac{7}{2n} \cdot \zeta_n^j \cdot \Im(\zeta_n^{dj})^{-1/d} \cdot \Im(\zeta_n)^{1/d}$ for $n = 4md$ and $1 \leq j \leq 2m - 1$, so that $\Re(z(s(\alpha_j))) = \Re(\zeta_n^m)$ is fixed, but $\Theta(w(s(\alpha_j)))$ takes at least $2m - 1$ different values.

The sequence 1 show that $\Theta(w)$ and $|z|$ are algebraically independent, since $\Theta(w)$ can take arbitrarily many different values while $|z|$ is fixed. Therefore, after swapping z and w, $|w|$ and $\Theta(z)$ are algebraically independent as well.

Moreover, the sequences 2 and 3 show that $\Theta(w)$ and $\Re(z)$, resp. $\Im(z)$ are also algebraically independent.

With a similar technique, we can prove the remaining cases of $|w|$ and $\Re(z)$, $\Im(z)$. The estimate for $|w|$ is the following:

$$\big||w(s(\alpha))| - |a\alpha^k|\big| \leq N \cdot |\alpha^{k+1}|.$$

As before, we take an appropriate sequence of values

$$\alpha_j := \frac{|a|c_n}{2^{k+3}N} \cdot \left(1 + i\frac{j}{n}\right)^{1/d},$$

where j is an integer $0 \leq j < n$. The real part $\Re(\alpha_j^d)$ is constantly α_0, and for $j \neq j'$

$$||a\alpha_j^k| - |a\alpha_{j'}^k|| \geq |a| \cdot \alpha_0^k \cdot c_n,$$

where c_n is the minimum distance between two different $(1 + ij/n)^{k/d}$.

However, by construction, the error term is smaller than half the minimum distance

$$N \cdot |\alpha_j^{k+1}| \leq 2^{k+1} \cdot N \cdot \alpha_0^{k+1} \leq 2^{k+1} \cdot N \cdot \alpha_0 \cdot \alpha_0^k < \frac{1}{2} \cdot |a| \cdot c_n \cdot \alpha_0^k.$$

Therefore, $|w(s(\alpha))|$ must take at least n different values while $\Re(z(s(\alpha)))$ is constant, so it is algebraically independent from $\Re(z)$. The same argument applies taking the sequence $i\alpha_j$. □

The above lemmas are enough to prove the following.

Proposition 3.22. *If* $\dim M \cdot \check{V} = \mathrm{rank} M$*, and all the functions in* S *are one-dimensional, then* $\mathrm{rank} M = 2n$.

Proof. By proposition 3.18, we are in the case $\mathrm{rank}\check{M} = n$, $k_1 = |f_2(H)|$ and V is perfectly rotund.

In this situation we have that $k_1 = |S|$ as well, hence $S = f_2(H)$, i.e., the functions in S come only from the rows of M of the form $(\overline{m}, 0)$ or $(0, \overline{q})$; this happens exactly when $P_1 = Q_1 = 0$. We prove this by showing that $\mathrm{rank} Q_2$ must be n, as in this case we must have $\mathrm{rank} M_1 = n$ as well, and $\mathrm{rank} M = 2n$.

If $\mathrm{rank} Q_2 < n$ and $Q_2 \neq 0$, what happens is that we are able to swap one function in S with another *two* ones while preserving algebraic independence, showing that actually $\dim M \cdot \check{V} > \mathrm{rank} M$, a contradiction.

If $Q_2 = 0$, then we show that the absolute freeness of V, together with lemma 3.20 and lemma 3.21, imply that $\dim M \cdot \check{V} > n$, a contradiction.

Case $Q_2 \neq 0$**,** $\mathrm{rank} Q_2 < n$.

In this case, let $\check{M}'$ be the submatrix of $\check{M}$ of the rows $\overline{m}_1, \ldots, \overline{m}_q$ that gets substituted by the rows of Q_2. Note that $\mathrm{rank}\check{M}' = \mathrm{rank} Q_2$, by definition of Q_2, and $\mathrm{rank}\check{M}' < \mathrm{rank}\check{M} = n$.

Let us take one row $\overline{m}$ of $\check{M}$ which is not in $\check{M}'$. Then exactly one of the two pairs $\{\overline{m} \cdot \overline{x}, \overline{m} \cdot \overline{y}\}$ and $\{\overline{\rho}^{\overline{m}}, \overline{\theta}^{\overline{m}}\}$ is in H, say $\{\phi_1, \phi_2\}$. Since V is simple, then $\dim \check{M}' \cdot V > \mathrm{rank}\check{M}'$; in particular, there is a pair of functions, $\{\overline{m}' \cdot \overline{x}, \overline{m}' \cdot \overline{y}\}$ or $\{\overline{\rho}^{\overline{m}'}, \overline{\theta}^{\overline{m}'}\}$, for $\overline{m}'$ in $\check{M}'$, which is not in H and which is interalgebraic with the functions in the pair $\{\phi_1, \phi_2\}$ over $H \setminus \{\phi_1, \phi_2\}$. Let us call the new pair $\{\psi_1, \psi_2\}$. Let $\overline{q}$ be the row of Q_2 replacing the row $\overline{m}'$. This implies that the functions in $\{\phi_1, \phi_2\}$ are are interalgebraic with the $\{\psi_1, \psi_2\}$ over $H \setminus \{\phi_1, \phi_2\}$. Let H' be the set obtained from H by replacing $\{\phi_1, \phi_2\}$ with $\{\psi_1, \psi_2\}$.

By construction, $f_2(H) = f_2(H \cap H') \cup f_2(\{\phi_1, \phi_2\})$, while $f_2(H') = f_2(H \cap H') \cup f_2(\{\psi_1, \psi_2\})$. The set $f_2(\{\phi_1, \phi_2\})$ is either $\{\phi_1\}$ or $\{\phi_2\}$: if it comes from a row of the form $(\overline{m}, 0)$, since $\overline{m}$ is not replaced by a function in Q_1, then only one function in the pair is kept and the other one is discarded; if the row is $(0, \overline{p})$, then $\overline{p}$ is in P_2 and the same argument applies. On the other hand, $f(\{\psi_1, \psi_2\})$ is $\{\psi_1, \psi_2\}$, because this time both functions in the pair appears as coordinates of $M \cdot r(V)$.

This implies that $|f_2(H')| = |f_2(H)| + 1$, hence $\dim M \cdot \check{V} \geq |f_2(H')| > |f_2(H)|$, a contradiction.

Case $Q_2 = 0$**.** We claim that in this case there is a multiplicative dependency among the multiplicative coordinates of V, against the hypothesis that V is absolutely free.

Since V is absolutely free, we can choose an algebraically independent set B of coordinates of V containing at least one additive coordinate. Moreover, since V is perfectly rotund, at least one multiplicative coordinate must not be in B. Let $\overline{w}^{\overline{q}} = \overline{\rho}^{\overline{q}} \overline{\theta}^{\overline{q}}$ be this function.

By hypothesis, $\overline{w}^{\overline{q}}$ is algebraic over $B \cup \overline{c} E(\overline{c})$. Since V is absolutely free, $\overline{w}^{\overline{q}}$ is not a constant function; in particular, there must some elements $\psi \in B$ such that $\overline{w}^{\overline{q}}$ is interalgebraic with ψ over $B \setminus \{\psi\} \cup \overline{c}$.

If there is one such ψ of the form $\psi = \overline{m}\cdot\overline{z} = \overline{m}\cdot\overline{x}+\overline{m}\cdot\overline{y}$ for some $\overline{m}$, then, by lemma 3.21, each of the functions $\overline{\rho}^{\overline{q}}$ and $\overline{\theta}^{\overline{q}}$ is algebraically independent from $(r(B)\setminus\{\overline{m}\cdot\overline{y}\})\cup\overline{c}E(\overline{c})$ and also from $(r(B)\setminus\{\overline{m}\cdot\overline{x}\})\cup\overline{c}E(\overline{c})$. Since we are in the case $P_1 = Q_1 = Q_2 = 0$, either $f_2(B) \subset r(B)\setminus\{\overline{m}\cdot\overline{x}\}$ or $f_2(B) \subset r(B) \setminus \{\overline{m}\cdot\overline{y}\}$; moreover, $f_2(\{\overline{\rho}^{\overline{q}}, \overline{\theta}^{\overline{q}}\})$ contains exactly one of $\overline{\rho}^{\overline{q}}$ and $\overline{\theta}^{\overline{q}}$. But this implies that $f_2(\{\overline{\rho}^{\overline{q}}, \overline{\theta}^{\overline{q}}\})$ is algebraically independent over $f_2(B)\cup\overline{c}E(\overline{c})$, hence there is an extra coordinate function on $M\cdot r(V)$. Therefore, $\dim M\cdot\check{V} > f_2(B) = n$, a contradiction.

Let us suppose instead that all the possible ψ's are of the form $\psi = \overline{\rho}^{\overline{m}}\overline{\theta}^{\overline{m}}$. If $\overline{\rho}^{\overline{q}}$ is algebraically dependent on $(r(B) \setminus \{\overline{\theta}^{\overline{m}}\}) \cup \overline{c}E(\overline{c})$ for all the possible ψ's, then actually $\overline{\rho}^{\overline{q}} \in \operatorname{acl}(\{\overline{\rho}^{\overline{m}} : \overline{\rho}^{\overline{m}} \in r(B)\} \cup \overline{c}E(\overline{c}))$, and in particular it is contained in $\operatorname{acl}(\{|z| : z \in B\} \cup \overline{c}E(\overline{c})\}$. By lemma 3.20, there is a multiplicative relation in B over the constants, against the hypothesis of absolute freeness of V; hence, one of the possible ψ's is such that $\overline{\rho}^{\overline{q}}$ is algebraically independent from $(r(B) \setminus \{\overline{\theta}^{\overline{m}}\}) \cup \overline{c}E(\overline{c})$. With the same argument, we can verify that there is a $\psi' = \overline{\rho}^{\overline{m}'}\overline{\theta}^{\overline{m}'}$ such that the function $\overline{\theta}^{\overline{q}}$ is algebraically independent from $(r(B) \setminus \{\overline{\rho}^{\overline{m}'}\}) \cup \overline{c}E(\overline{c})$.

Moreover, again by lemma 3.21, for all the possible $\psi = \overline{\rho}^{\overline{m}}\overline{\theta}^{\overline{m}}$, $\overline{\rho}^{\overline{q}}$ is algebraically independent from $(r(B) \setminus \{\overline{\rho}^{\overline{m}}\}) \cup \overline{c}E(\overline{c})$ and $\overline{\theta}^{\overline{q}}$ is algebraically independent from $(r(B) \setminus \{\overline{\theta}^{\overline{m}}\}) \cup \overline{c}E(\overline{c})$.

Let us distinguish the two cases. If $\overline{q}$ is a row of M_1, then there is a function $\overline{\rho}^{\overline{m}}\overline{\theta}^{\overline{m}}$ such that $\overline{\rho}^{\overline{q}}$ is algebraically independent from $(r(B) \setminus \{\overline{\theta}^{\overline{m}}\}) \cup \overline{c}E(\overline{c})$; moreover, $\overline{\rho}^{\overline{q}}$ is algebraically independent from $(r(B) \setminus \{\overline{\rho}^{\overline{m}}\}) \cup \overline{c}E(\overline{c})$ as well. As before, $f_2(B) \subset r(B)$ contains exactly one function in $\{\overline{\rho}^{\overline{m}}, \overline{\theta}^{\overline{m}}\}$; therefore, $\overline{\rho}^{\overline{q}}$ is algebraically independent from $f_2(B) \cup \overline{c}E(\overline{c})$. But $f_2(\{\overline{\rho}^{\overline{q}}\}) = \{\overline{\rho}^{\overline{q}}\}$, since $\overline{q}$ is in M_1; therefore, as before, $\dim M \cdot \check{V} > f_2(B) = n$, a contradiction.

If $\overline{q}$ is a row of P_2, then as before there is a $\overline{\rho}^{\overline{m}}\overline{\theta}^{\overline{m}}$ such that $\overline{\theta}^{\overline{q}}$ is algebraically independent from $(r(B) \setminus \{\overline{\rho}^{\overline{m}}\}) \cup \overline{c}E(\overline{c})$ and from $(r(B) \setminus \{\overline{\theta}^{\overline{m}}\}) \cup \overline{c}E(\overline{c})$. This time, $f_2(\{\overline{\theta}^{\overline{q}}\}) = \{\overline{\theta}^{\overline{q}}\}$, since $\overline{q}$ is in P_1, and it is algebraically independent over $f_2(B) \cup \overline{c}E(\overline{c})$; therefore, as before, $\dim M \cdot \check{V} > f_2(B) = n$.

The only remaining case is $\operatorname{rank} Q_2 = n$. Since in this case $P_1 = 0$, each row of Q_2 is $\mathbb{Q}$-linearly dependent on the rows of M_1. Therefore, $\operatorname{rank} M_1 = n$ and $\operatorname{rank} M = 2n$, as desired. □

Proposition 3.23. *If $\dim M \cdot \check{V} = \operatorname{rank} M$, and some function in S is not one-dimensional, then all the functions in S are two-dimensional. In particular, $k_1 = 0$ and $f_2(H) = \emptyset$.*

Proof. Let us suppose that we have both kind of functions. By construction, this implies that there are some rows $(\overline{m}, \overline{q})$ in M such that one of $\overline{m}$ are $\overline{q}$ are zero, and some where both $\overline{m}$ and $\overline{q}$ are not zero. Note that S is pure.

If $(\overline{m}, 0)$ is a row of M (or $(0, \overline{p})$), then by construction exactly one of the functions $\overline{m} \cdot \overline{x}, \overline{\rho}^{\overline{m}}$ (resp. $\overline{p} \cdot \overline{y}, \overline{\theta}^{\overline{p}}$) is in S. Let ψ be the one not contained in S. We claim that ψ is contained in the algebraic closure of all the one-dimensional functions in S, in other words in $\operatorname{acl}(f_2(H) \cup \overline{c}E(\overline{c}))$.

Indeed, since $\psi \in \operatorname{acl}(S \cup \overline{c}E(\overline{c}))$, but it is not constant by absolute freeness, there must be at least one function $\chi \in S$ such that ψ is interalgebraic with χ over $(S \setminus \{\chi\}) \cup \overline{c}E(\overline{c})$. But this implies that $r(\psi)$ is interalgebraic with $r(\chi)$ over $r(S \setminus \{\chi\})$; in particular, χ is one-dimensional too. Applying this argument to all the possible χ's we obtain our claim.

However, this implies that if M' is the submatrix of M of all the rows $(\overline{m}, \overline{q})$ of M such that one of $\overline{m}$ and $\overline{q}$ is zero, we have that $\dim M' \cdot \check{V} = \operatorname{rank} M'$. But all the coordinate functions are one-dimensional on $M' \cdot \check{V}$, hence, by proposition 3.22, we have $\operatorname{rank} M' = 2n$. This implies that *all* the functions in S are one-dimensional, a contradiction.

Therefore, all the functions in S are two-dimensional. □

And then the last observation.

Proposition 3.24. *If* $\dim M \cdot \check{V} = \mathrm{rank} M$*, and all the functions in* S *are two-dimensional, then* M *is of the form*

$$M = \begin{pmatrix} N & Q \end{pmatrix}$$

where N, Q *are two matrices in* $\mathcal{M}_{n,n}(\mathbb{Z})$ *of maximum rank.*

Proof. Since the functions in S are all two-dimensional, there is no function in $f_2(H)$, hence the matrix M must be of the following form:

$$M = \begin{pmatrix} N & Q \end{pmatrix},$$

where $N = M_1$, $Q = \begin{pmatrix} P_1 \\ Q_1 \end{pmatrix}$ are some matrices in $\mathcal{M}_{k,n}(\mathbb{Z})$ of the same rank k.

Let us consider the matrix

$$M' := \begin{pmatrix} N & 0 \\ 0 & Q \end{pmatrix}.$$

Obviously, $\mathrm{rank} M' = 2k$.

Clearly, there is a surjective *algebraic* map $M' \cdot \check{V} \to M \cdot \check{V}$ which is a bijection when restricted to the realisations $M' \cdot r(V) \to M \cdot r(V)$. Since the coordinates of $M' \cdot r(V)$ are all one-dimensional, and the dimension of $M' \cdot r(V)$ as a semialgebraic variety is equal to the dimension of $M \cdot r(V)$, i.e., $2k$, then the dimension of $M' \cdot \check{V}$ is $2k$.

But this means that $\dim M' \cdot V = \mathrm{rank} M'$, and by proposition 3.22, $\mathrm{rank} M' = 2k = 2n$. Therefore, $k = n$, and we are done. □

This ends the proof of theorem 3.8.

Proof of theorem 3.8. By Propositions 3.10, 3.9 and 3.17, $\check{V}$ is absolutely free, absolutely irreducible and rotund.

Let $A \cdot M$ be the matrix obtained in proposition 3.15. By proposition 3.23, the coordinate functions of $A \cdot M \cdot r(V)$ are either one-dimensional or two dimensional. In the former case, by proposition 3.22 $A \cdot M$ is invertible, and thus M is invertible two.

In the latter case, by proposition 3.24 the matrix $A \cdot M$ has the desired form, and thus M has the desired form too. □

3.4 Solutions and roots on the $\mathbb{G}$-restrictions

We produce here an alternative version of proposition 2.18 useful to work with dense sets of real generic solutions. In order to do this, we produce a suitable generalisation taking into accounts the $\mathbb{G}$-restrictions. First of all, we introduce some other technical definitions.

Definition 3.25. An *open subsystem* of $\mathcal{R}(V)$ is a collection of subsets $\mathcal{U} := \{\mathcal{U}(W)\}_{W \in \mathcal{R}(V)}$ such that $\mathcal{U}(W) \subset W$ is open in W w.r.t. the order topology.

We extend the usual set-theoretic operations to the open subfamilies: the union of two or more open subfamilies is the subfamily of the union of the respective open sets, one subfamily $\mathcal{U}$ is contained in another $\mathcal{U}'$ if for each $W \in \mathcal{R}(V)$ we have $\mathcal{U}(W) \subset \mathcal{U}'(W)$, etc. etc.

Note that an open subsystem is essentially an open set of $\prod_{W \in \mathcal{R}(V)} W$ equipped with the product topology, with the only difference that we may have open subsystems where some $\mathcal{U}(W)$ is empty.

A trivial, but important observation is the following.

Proposition 3.26. *Suppose that the order topology on R is separable. If $\mathcal{U}$ is an open subsystem of $\mathcal{R}(V)$, and $\mathcal{U} = \bigcup_{j\in J} \mathcal{U}_j$, where each $\mathcal{U}_j$ is an open subsystem of $\mathcal{R}(V)$, then there is a countable $J_0 \subset J$ such that $\mathcal{U} = \bigcup_{j\in J_0} \mathcal{U}_j$.*

Proof. We have $\mathcal{U}(W) = \bigcup_{j\in J} \mathcal{U}_j(W)$ for each $W \in \mathcal{R}(W)$. By separability, for each W, there is a countable $J_W \subset J$ such that $\mathcal{U}(W) = \bigcup_{j\in J_W} \mathcal{U}_j(W)$. The set $J_0 = \bigcup_{W\in\mathcal{R}(V)} J_W$ is countable, and it clearly satisfies $\mathcal{U} = \bigcup_{j\in J_0} \mathcal{U}_j$. □

Definition 3.27. A family $\mathcal{R}(V)$, for $\check{V}$ E-defined over $\bar{c}$, is *densely solved* in K_E w.r.t. an open subfamily $\mathcal{U}$ if for all $W \in \mathcal{R}(V)$ there is an infinite set of solutions of W really algebraically independent over $\operatorname{acl}(\bar{c}E(\bar{c}))$ which is dense in $\mathcal{U}(W)$ w.r.t. the order topology.

We say that $\mathcal{R}(V)$ is *densely solved* in K_E if it is densely solved w.r.t. the trivial open subfamily $\mathcal{R}(V)$.

As with the definition of completely solved, this definition does not depend on $\bar{c}$. Indeed, if we use another $\bar{d}$, by proposition 2.3 a set of algebraically independent points remains algebraically independent when passing from $\bar{c}$ to $\bar{d}$, up to removing a finite set of points. As there are no isolated points in any of the varieties $W \in \mathcal{R}(V)$, thanks to the irreducibility of each W, the set of solutions remains dense after removing a finite set.

Proposition 3.28. *If $W \in \mathcal{R}(V)$, then $\check{W} \in \mathcal{R}(\check{V})$.*

Proof. There are $p, q \in \mathbb{Z}^\times$ such that $q \cdot W = p \cdot V$. Taking the realisation we obtain $q \cdot r(W) = p \cdot r(V)$; taking the Zariski closure, $q \cdot \check{W} = p \cdot \check{V}$. □

The following is the 'right' version of proposition 2.18 for densely solved families.

Proposition 3.29. *Let $V \subset \mathbb{G}^n$ be a rotund variety and K_E such that $\sigma \circ E = E \circ \sigma$. Let $N, Q \in \mathcal{M}_{n,n}(\mathbb{Z})$ be two square integer matrix of maximum rank, $\bar{z} \in \operatorname{dom}(E)^n$, and $X := \begin{pmatrix} N & Q \end{pmatrix} \cdot \check{V} \oplus \langle \bar{z}; E(\bar{z})\rangle$.*

If $\dim X = \dim V$, then there exists an open subfamily $\mathcal{U}$ of $\mathcal{R}(X)$ such that $\mathcal{R}(V)$ is densely solved if and only if $\mathcal{R}(X)$ is densely solved w.r.t. $\mathcal{U}$.

Proof. For each $W \in \mathcal{R}(V)$ we have $\check{W} \in \mathcal{R}(\check{V})$; in particular, there are $p, q \in \mathbb{Z}^\times$ such that $M \cdot \check{W} \oplus \langle \frac{p}{q}\bar{z}; E(\frac{p}{q}\bar{z})\rangle \in \mathcal{R}(X)$. Let Y be $M \cdot \check{W} \oplus \langle \frac{p}{q}\bar{z}; E(\frac{p}{q}\bar{z})\rangle$.

For brevity, let $\psi_W : W \to Y$ be the map

$$W \ni P \overset{\psi_W}{\longmapsto} \begin{pmatrix} N & Q \end{pmatrix} \cdot r(P) \oplus \langle \frac{p}{q}\bar{z}; E(\frac{p}{q}\bar{z})\rangle \in Y.$$

Let $\tilde{N}, \tilde{Q}$ be two integer matrices such that $\tilde{N} \cdot N = \tilde{Q} \cdot Q = k \cdot \mathrm{Id}$ for some $k \in \mathbb{N}^\times$. We define $\tilde{\psi}_W : \psi_W(W) \to W$ as

$$R \overset{\tilde{\psi}_W}{\longmapsto} \begin{pmatrix} \tilde{N} & 0 \\ 0 & \tilde{Q} \end{pmatrix} \cdot r\left(R \oplus \langle -\frac{p}{q}\bar{z}; E(-\frac{p}{q}\bar{z})\rangle\right).$$

Seen as maps between $r(W)$ and $r(Y)$, both are semi-algebraic map. We claim that ψ_W is finite-to-one onto its image. Indeed, if $\psi_W(P)$ is a point in the image, then

$$\tilde{\psi}_W(\psi_W(P)) = k \cdot r(P) = r(k \cdot P).$$

Since there are finitely many points P' such that $k \cdot P' = k \cdot P$, and r is injective, the map ψ_W is finite-to-one.

This implies that $o-\dim(\psi_W(W)) = o-\dim(Y)$, where by "$o-\dim$" we denote the o-minimal dimension over R. In particular, by o-minimality there is an open subset U_Y of Y such that $U_Y \subset \psi_W(W)$ and

$$o-\dim(\psi_W(W) \setminus U_Y) < o-\dim(\psi_W(W)).$$

In particular, since ψ_W is finite-to-one, $\psi_W^{-1}(U_Y)$ is an open subset of V such that

$$o-\dim(W \setminus \psi_W^{-1}(U_Y)) < o-\dim(W).$$

For each Y, we have selected an open subset U_Y, and for the remaining varieties in $\mathcal{R}(X)$, we take the empty set; this defines an open subsystem that we call $\mathcal{U}$. We claim that $\mathcal{U}$ is the desired open subsystem of $\mathcal{R}(V)$.

From now on, let $\bar{c}$ be a defining tuple for $\check{V}$ containing $r(\langle \bar{z}; E(\bar{z})\rangle)$. In particular, $\bar{c}$ also defines both V and X.

The left-to-right direction is clear: since ψ_W is continuous, algebraic, defined over $\bar{c}$, and finite-to-one, it sends really algebraically independent dense sets to really algebraically independent sets dense in the image; in particular, the image of the solutions in W through ψ_W will be a really algebraically independent set which is dense w.r.t. U_Y. As the family $\mathcal{U}$ is composed exactly by the U_Y's, the conclusion follows.

For the right-to-left we proceed as above. The map $\tilde{\psi}_W$, for $P \in U_Y$, is such that $\tilde{\psi}_W \circ \psi_W$ is exactly $k \cdot \mathrm{Id}$. Hence it is a finite-to-one algebraic continuous map, so as above it preserves really algebraically independent dense sets over $\bar{c}$.

In particular, if there is a dense set of really algebraically independent points in U_Y, then there is a corresponding dense set of really algebraically independent points in $\tilde{\psi}_W(U_Y)$. However, this set is exactly $k \cdot \psi_W^{-1}(U_Y)$. Since $\psi_W^{-1}(U_Y)$ has complement of o-minimal dimension strictly smaller than W, and locally around each point the dimension of W is always $o-\dim(W) = 2 \cdot \dim(W)$, we have that $\psi_W^{-1}(U_Y)$ is dense in W; hence, its multiple $k \cdot \psi_W^{-1}(U_Y)$ is dense in $k \cdot W$.

In particular, the image of the solutions through $\tilde{\psi}_W$ is dense in $k \cdot W$. But for all $W \in \mathcal{R}(V)$ there is a W' such that $k \cdot W' = W$; therefore, if all the open sets in the family $\mathcal{U}$ contains a dense set of really algebraically independent solutions, the same is true for all the varieties in $\mathcal{R}(V)$. □

3.5 Preserving (CCP) after many iterations II

As in proposition 2.19, we want to show that the basic operations can be iterated as many times as we want while preserving (SP), (STD) and (CCP).

Let K be a saturated algebraically closed field of characteristic 0 equipped with an involution σ such that the topology of $R = K^\sigma$ is separable.

Let $(K_{E_j})_{j \leq \alpha}$ be a sequence of partial E-fields over K, with $\sigma \circ E_0 = E_0 \circ \sigma$, such that:

- for all $j < \alpha$, $K^{j+1}_{E_{j+1}}$ is an extension of K_{E_j} obtained by one of the basic operations R-DOMAIN, R-IMAGE, R-ROOTS;
- for all $j \leq \alpha$ limit ordinal, E_j by $E_j = \bigcup_{k<j} E_j$.

Is is easy to verify that similarly to corollary 2.9, some important properties are carried from K_{E_0} to K_{E_α}.

Proposition 3.30. *If $K_E \subset K_{E'}$ is an extension produced by one of the operations* R-DOMAIN, R-IMAGE, R-SOL, R-ROOTS, *then $K_{E'}$ is well-defined, and it is a partial E-field with $\sigma \circ E' = E' \circ \sigma$.*

Proof. The property $\sigma \circ E = E \circ \sigma$ is clearly preserved, since the operation are defined such in a way that the requirements of proposition 3.1 are verified. Moreover, the operations are just compositions of special cases of the operations of the previous chapter, hence the result is a well-defined partial E-field by proposition 2.6 (we are using the fact that when V is absolutely free rotund, then $\check{V}$ is absolutely free rotund by proposition 3.10). □

Proposition 3.31. *If $K_E \subset L_{E'}$ is an extension produced by one of the operations* R-DOMAIN*,* R-IMAGE*,* R-SOL*,* R-ROOTS*, and K_E has full kernel, then the extension is kernel preserving.*

Proof. This is a corollary of proposition 2.7, again by using the fact that $\check{V}$ is absolutely free rotund. □

Proposition 3.32. *If $K_E \subset L_{E'}$ is an extension produced by one of the operations* R-DOMAIN*,* R-IMAGE*,* R-SOL*,* R-ROOTS*, then the extension is strong.*

Proof. Again, this is a corollary of proposition 2.8 by the properties of $\check{V}$. □

In particular, this is true after arbitrary many iterations.

Corollary 3.33. *If K_{E_0} satisfies (SP), or (STD), then K_{E_α} satisfies (SP), resp. (STD).*

Some substantial changes are required for (CCP), but the idea is not much different. We exploit the density of the solutions to show that the generic solutions of perfectly rotund varieties must appear on cofinal countable sets, and therefore, by induction, they are countable.

Proposition 3.34. *If K_{E_0} satisfies (CCP), then K_{E_α} satisfies (CCP).*

Proof. Let D_j be the domain $\mathrm{dom}(E_j)$. For all $j < \alpha$ there is a finite or countable set B_j such that $D_{j+1} = \mathrm{span}_{\mathbb{Q}}(D_j \cup B_j)$. By lemma 2.11, if K_{E_j} satisfies (CCP), then $K_{E_{j+1}}$ satisfies (CCP). We claim that the induction works also at limit ordinals.

Let j be a limit ordinal such that for all $k < j$, K_{E_k} satisfies (CCP). By proposition 2.10, in order to prove (CCP) for K_{E_j} it is sufficient to verify that for any perfectly rotund variety E-defined over D_j, the number of generic solutions is at most countable. We may restrict to absolutely irreducible varieties by taking them defined over $\mathrm{acl}(D_j E(D_j))$.

Let $X(\overline{c}) \subset \mathbb{G}^n$ be a perfectly rotund variety with $\overline{c}E(\overline{c}) \subset \mathrm{acl}(D_j E(D_j))$. First of all, there must be a minimum $m < j$ such that $\overline{c}E(\overline{c}) \subset \mathrm{acl}(D_m, E(D_m))$. Since K_{E_m} has (CCP) by inductive hypothesis, it is sufficient to count how many generic solutions of $X(\overline{c})$ are contained in $D_j^n \setminus D_m^n$.

If $\overline{x} \in D_j^n \setminus D_m^n$ is a generic solution of $X(\overline{c})$ in K_{E_j}, then there is a smallest $m \leq k < j$ such that $\overline{x} \in D_{k+1}^n \setminus D_k^n$. Let Λ be the set of such k's. We claim that Λ has countable cofinality. This implies that the the generic solutions of $X(\overline{c})$ in K_{E_α} are a countable union of solutions contained in $K_{E_{k+1}}$, for k running in a countable cofinal subset of Λ. Since (CCP) holds in $K_{E_{k+1}}$, the number of solutions in each $K_{E_{k+1}}$ is countable, hence their union is still countable.This shows that K_{E_j} satisfies (CCP), and by induction up to $j = \alpha$, K_{E_α} too.

Let $\overline{x}$ be a new generic solution of $X(\overline{c})$ contained in $D_{k+1} \setminus D_k$. Since the operations R-DOMAIN and R-IMAGE are just chains of DOMAIN and IMAGE operations, the same argument in the proof of proposition 2.19 applies: the extension is not produced by one of those operations.

As before, we are left with the case of the operation R-ROOTS. Let F be the field generated by $D_k, E(D_k)$. By hypothesis, $\overline{c}E(\overline{c}) \subset \mathrm{acl}(F)$.

R-ROOTS. This operation is a sequence of multiple applications of R-SOL. Let us suppose that the solution $\overline{x}$ appears when we add the point $\langle \overline{\alpha}; \overline{\beta} \rangle \in \check{V}$ to the graph of the exponential function, for some simple variety $V \subset \mathbb{G}^m$. Let D be the domain of the exponential function before adding the point $\langle \overline{\alpha}; \overline{\beta} \rangle$, and let $D' := \mathrm{span}_{\mathbb{Q}}(D \cup \overline{\alpha})$ be the domain after. The vector $\overline{x}$ must be of the form $\overline{z} + M \cdot \overline{\alpha}$, for some matrix $M \in \mathcal{M}_{n,2m}(\mathbb{Q}) \setminus \{0\}$, and $\overline{z} \in D$. Let $F := \mathbb{Q}(D, E_\alpha(D))$.

For now, let us assume that M is an integer matrix.

Under the above assumptions, $\mathrm{tr.deg.}_F(\overline{\alpha}, E_\alpha(\overline{\alpha})) = \dim \check{V} = 2m$. Moreover, for any matrix P we have $\mathrm{tr.deg.}_F(P \cdot \overline{\alpha}, E_\alpha(P \cdot \overline{\alpha})) \geq \mathrm{rank} P$.

Now, let N be an invertible matrix with integer coefficients such that the first rows of $N \cdot M$ forms a matrix Q of maximum rank equal to $\mathrm{rank} M$, and that the remaining rows are zero. Clearly, the point $\langle N \cdot \overline{z} + N \cdot M \cdot \overline{\alpha}; E_\alpha(N \cdot \overline{z} + N \cdot M \cdot \overline{\alpha}) \rangle$ is generic for $N \cdot X(\overline{c})$, which is again a simple variety.

Let $N \cdot \overline{z} = \overline{z}' \overline{z}''$, where $\overline{z}'$ is formed by the first $\mathrm{rank} M$ coordinates and $\overline{z}''$ by the remaining $(n - \mathrm{rank} M)$ ones. Let us suppose that $n > \mathrm{rank} M$. By simpleness of $N \cdot X(\overline{c})$, we have $\mathrm{tr.deg.}_{\overline{c} E_\alpha(\overline{c})}(\overline{z}'', E_\alpha(\overline{z}'')) > (n - \mathrm{rank} M)$.

In particular, we also have $\mathrm{tr.deg.}_{\overline{c} E_\alpha(\overline{c}), \langle \overline{z}''; E_\alpha(\overline{z}'') \rangle}(\overline{z}' + Q \cdot \overline{\alpha}, E_\alpha(\overline{z}' + Q \cdot \overline{\alpha})) < \mathrm{rank} M$. However, this contradicts the fact that $\mathrm{tr.deg.}_F(Q \cdot \overline{\alpha}, Q \cdot E_\alpha(\overline{\alpha})) \geq \mathrm{rank} Q = \mathrm{rank} M$. This implies that $n = \mathrm{rank} M$.

The resulting situation is that $\langle \overline{z} + M \cdot \overline{\alpha}; E_\alpha(\overline{z} + M \cdot \overline{\alpha}) \rangle$ is a generic point of $X(\overline{c})$ *over* F, while it is also a generic point of $M \cdot \check{V} \oplus \langle \overline{z}; E_\alpha(\overline{z}) \rangle$ over F. This immediately implies the equality $M \cdot \check{V} \oplus \langle \overline{z}; E_\alpha(\overline{z}) \rangle = X$.

In particular, we also have

$$\mathrm{tr.deg.}_F(\overline{z} + M \cdot \overline{\alpha}, E_\alpha(\overline{z} + M \cdot \overline{\alpha})) = \mathrm{tr.deg.}_F(M \cdot \overline{\alpha}, E_\alpha(M \cdot \overline{\alpha})) = \mathrm{rank} M.$$

By theorem 3.8, either M is invertible, or it is of the form $\begin{pmatrix} N & Q \end{pmatrix}$, with both N and Q invertible of rank $n = m$. In the former case, the above equality would imply that $\check{V}$ is simple, a contradiction. Hence, M must be of the latter form, and V must be perfectly rotund.

In particular, $\dim V = \dim X$, so by proposition 3.29 there is an open subfamily $\mathcal{U}_{V,M,\overline{z}}$ such that $\mathcal{R}(V)$ is densely solved if and only if $\mathcal{R}(X)$ is densely solved w.r.t. $\mathcal{U}_{V,M,\overline{z}}$.

If M is not an integer matrix, let l be an integer such that $l \cdot M$ is an integer matrix; the above argument applied to $l \cdot M$, $l \cdot \overline{z}$ and $l \cdot X$ implies that $\mathcal{R}(V)$ is densely solved if and only if $\mathcal{R}(l \cdot X)$ is densely solved w.r.t. $\mathcal{U}_{V,l \cdot M,l \cdot \overline{z}}$. As $\mathcal{R}(l \cdot X) = \mathcal{R}(X)$, this is just like the above conclusion.

Now, for each of the varieties such that the above situation happens, i.e., for each $\lambda \in \Lambda$, we choose, among the possibilities found above, one matrix M and one vector $\overline{z}$ such that $\mathcal{R}(V_\lambda)$ is densely solved if and only if $\mathcal{R}(X)$ is densely solved w.r.t. the family $\mathcal{U}_\lambda := \mathcal{U}_{V_\lambda,M,\overline{z}}$.

By proposition 3.26, we can extract an at most countable subset $\Lambda_0 \subset \Lambda$ such that for each $Y \in \mathcal{R}(X)$, the union $\bigcup_{\lambda \in \Lambda} \mathcal{U}_\lambda(Y)$ is equal to $\bigcup_{\lambda \in \Lambda_0} \mathcal{U}_\lambda(Y)$. We claim that Λ_0 is cofinal in Λ.

Indeed, let us take a variety V_λ with $\lambda \in \Lambda$, and let us suppose by contradiction that $\lambda > \lambda_0$ for all $\lambda_0 \in \Lambda_0$. We know that $\mathcal{R}(V_\lambda)$ is densely solved if and only if $\mathcal{R}(X)$ is densely solved w.r.t. $\mathcal{U}_\lambda$. We claim that $\mathcal{R}(X)$ is already densely solved w.r.t. $\mathcal{U}_\lambda$ *before* applying the step λ.

Indeed, fix a variety $Y \in \mathcal{R}(X)$ and consider the open subset $U := \mathcal{U}_\lambda(Y)$. By construction, $U = \bigcup_{\lambda_0 \in \Lambda_0} \mathcal{U}_{\lambda_0}(Y)$. In particular, U contains a dense set of really algebraically independent set of solutions in D^n_λ if and only if each open set $\mathcal{U}_{\lambda_0}(Y)$ does. On the other hand, each $\mathcal{U}_{\lambda_0}(Y)$ does contain such a set, since by definition of $\mathcal{U}_{\lambda_0}$, $\mathcal{R}(X)$ is densely solved w.r.t. $\mathcal{U}_{\lambda_0}$ if and only if $\mathcal{R}(V_{\lambda_0})$ is densely solved; but since we have applied R-ROOTS to V_{λ_0} at the step λ_0, this is true in $D^n_{\lambda_0+1} \subset D^n_\lambda$.

Therefore, U contains a dense set of really algebraically independent set of solutions in D^n_λ. Thus, $\mathcal{R}(V_\lambda)$ is densely solved at the step λ; this implies that the R-ROOTS operation on V_λ is actually void, so X does not get new solutions, hence $\lambda \notin \Lambda$, a contradiction.

In particular, Λ_0 is countable and cofinal in Λ. Since the set of the generic solutions of $X(\overline{c})$ contained in K_{E_j} is the union of the solutions contained in K_{E_λ} for $\lambda \in \Lambda$, by cofinality of Λ_0, this is just the union of the solutions contained in $K_{E_{\lambda_0}}$ for $\lambda_0 \in \Lambda_0$. But this is an at most countable union of countable sets, hence $X(\overline{c})$ has at most countably many generic solutions in K_{E_j}. By induction, (CCP) holds in K_{E_α}. □

As before, we can show that there is a procedure to construct Zilber fields on K such that $\sigma \circ E = E \circ \sigma$.

Let us enumerate the elements of K as $\{\alpha_j\}_{j<|\mathbb{F}|}$ and all the absolutely free rotund varieties as $\{V_j\}_{j<|K|}$. We define a sequence of exponential functions $\{E_j\}_{j\leq|\mathbb{F}|}$ in the following way. At the base step, we define $E_0(\frac{p}{q}\omega) := \zeta_q^p$, where ω is an *imaginary* transcendental number, and (ζ_q) is a coherent system of roots of unity. It is easy to see that $\sigma \circ E_0 = E_0 \circ \sigma$. We go on in the following way.

1. if $j = k + 1$,
   (a) apply R-DOMAIN to α_k to obtain E' from E_k;
   (b) if $\alpha_k \neq 0$, apply R-IMAGE to α_k to obtain E'' from E';
   (c) if V_k is E-defined over a finite $\overline{c}$, apply R-DOMAIN to the elements of $\overline{c}$, then if K is uncountable, apply R-ROOTS to V_k,$V_k(\overline{c})$, otherwise apply R-SOL to $V_k(\overline{c})$, and obtain E_j from E'';
2. if j is a limit ordinal, define $E_j := \bigcup_{k<j} E_k$.

By proposition 3.7, all the above operations are always possible.

Corollary 3.35. *The resulting $K_{E_{|K|}}$ is a Zilber field with $\sigma \circ E_{|K|} = E_{|K|} \circ \sigma$; if K is uncountable, it also satisfies (DEN).*

Proof. The starting K_{E_0} satisfies (SP), (STD) and (CCP). By corollary 3.33 and proposition 3.34, all the partial E-fields K_{E_j} satisfy (SP), (STD) and (CCP), and $\sigma \circ E_j = E_j = \sigma$. Clearly, the final $E_{|K|}$ is defined everywhere, and it is surjective, and by the application of either R-SOL or R-ROOTS on all perfectly rotund varieties, (SEC) is satisfied as well. Moreover, if K is countable, we have applied r-roots to all perfectly rotund varieties, hence (DEN) is satisfied as well.

Therefore, $K_{E_{|K|}}$ is a Zilber field, satisfying (DEN) if K is uncountable, with $\sigma \circ E_{|K|} = E_{|K|} \circ \sigma$. □

And here is the proof of our main theorem.

Theorem 3.36. *The Zilber field $\mathbb{B}_E$ of cardinality $2^{\aleph_0}$ has an involution whose fixed field is isomorphic to $\mathbb{R}$ with* $\ker(E) = 2\pi i\mathbb{Z}$.

Moreover, any separable real closed field of infinite transcendence degree occurs as the fixed field of a Zilber field of the same cardinality; in particular, every Zilber field of cardinality up to $2^{\aleph_0}$ has an involution.

Proof. Given any separable real closed field of infinite transcendence degree R, and in particular $\mathbb{R}$, it is sufficient to apply the above construction to the algebraic closure $\overline{R}$ and the unique non-trivial automorphism of $\overline{R}/R$.

In particular, in the case of $R = \mathbb{R}$, we can also fix the kernel at the starting step to be $\omega\mathbb{Z} = 2\pi i\mathbb{Z}$. □

Remark 3.37. Our construction is potentially abundant for two reasons. First, we add "real generic" solutions to rotund varieties, and it is not clear if a Zilber field with an involution is forced to satisfy this condition.

Moreover, in the operation R-ROOTS we check if the family $\mathcal{R}(V)$ is densely solved before proceeding. Actually, it would be sufficient to check if $\mathcal{R}(V)$ is completely solved, without looking at density. This would open the possibility for involutions where the sets of the solutions are not always dense, but it is unclear what could happen in this situation.

Chapter 4

Other exponential fields

With the same approach used for constructing Zilber fields, we are free to create other kind of structures with different properties. We describe here a few possibilities that may be of interest.

4.1 Continuous and order-preserving exponential functions

One of the shortcomings of our construction is that the exponential function is not continuous with respect to the order topology, neither is order-preserving on the real closed field R. This is due to some difficulties with (SEC), because systems of equations could become incompatible once one add restrictions about the ordering, and with (CCP), since it requires to use dense sets of solutions.

We can still build exponential fields where E is continuous, or order-preserving, by dropping (SEC). These examples make evident where our technique fails in producing continuous and order-preserving exponential functions.

We present first an example construction where E is increasing, at the price of dropping the axiom (SEC) from the final structure. Not everything is lost, however, as we manage to verify a partial instance of (SEC) which we call "(1-SEC)".

The following axiom is the special instance of (SEC) we manage to verify.

(1-SEC) 1-dimensional Strong Exponential-algebraic Closure: for every absolutely free rotund variety $V \subset \mathbb{G}^1$ irreducible over K, and every tuple $\overline{c} \in K^{<\omega}$ such that V is E-defined over $\overline{c}$, there is a generic solution of $V(\overline{c})$.

It is known that if Schanuel's Conjecture is true, then (1-SEC) holds on $\mathbb{C}_{\exp}$ at least for varieties over $\mathbb{Q}$ [Mar06] (see section 1.8.1). It is not known if Schanuel's Conjecture implies also (SEC) on $\mathbb{C}_{\exp}$.

The construction, with some adaptation, yields the following.

Theorem 4.1. *For all saturated algebraically closed fields K of characteristic 0 there is a function $E : K \to K^\times$ and an involution σ commuting with E such that K_E satisfies (E), (LOG), (STD), (SP), (1-SEC) and (CCP), and $E_{\restriction K^\sigma}$ is a monotone function.*

This result appears in [Man11b]. The construction is again a refinement of the original one.

O-DOMAIN We start with an $\alpha \in K$. If $\alpha \in \mathrm{dom}(E)$, we define $E' := E$, otherwise we do the following.
We choose two elements $\beta \in R_{>0}, \gamma \in \mathbb{S}^1(R)$ algebraically independent over $F \cup \{\Re(\alpha), \Im(\alpha)\}$,

with the property that for each $\varepsilon \in \mathrm{dom}(E) \cap R$, $\varepsilon < \Re(\alpha)$ if and only if $E(\varepsilon) < \beta$, the positive roots $\beta^{1/q}$, and an arbitrary system of roots $\gamma^{1/q}$.
We define then $E'(z + \frac{p}{q}\Re(\alpha) + i\frac{p'}{q'}\Im(\alpha)) := E(z) \cdot \beta^{p/q} \cdot \gamma^{p'/q'}$ for all $z \in \mathrm{dom}(E)$ and $p, p' \in \mathbb{Z}, q, q' \in \mathbb{N}^\times$.

O-IMAGE We start with a $\beta \in K$ given as data to the operation. If $\beta \in \mathrm{im}(E)$, we define $E' := E$, otherwise we do the following.
We choose two elements $\alpha \in R, \delta \in iR$ algebraically independent over $\alpha \in F \cup \{|\beta|, \Theta(\beta)\}$, with the property that for each $\varepsilon \in \mathrm{dom}(E) \cap R$, $\varepsilon < \alpha$ if and only if $E(\varepsilon) < |\beta|$, and an arbitrary coherent system of roots $\beta^{1/q}$.
We define then $E'(z+\frac{p}{q}\alpha+\frac{p'}{q'}\delta) := E(z)\cdot|\beta^{p/q}|\cdot\Theta(\beta^{p'/q'})$ for all $z \in D$ and $p, p' \in \mathbb{Z}, q, q' \in \mathbb{N}^\times$.

O-SOL We start with a perfectly rotund variety $V(\bar{c}) \subset \mathbb{G}^1$, where $\bar{c}$ is closed under σ.
We choose a point $((\alpha_1, \beta_1), (\alpha_2, \beta_2)) \in r(V)$ generic over $F(\bar{c})$ for $\check{V}$, with the property that for each $\varepsilon \in \mathrm{dom}(E) \cap R$, $\varepsilon < \alpha_1$ if and only if $E(\varepsilon) < \beta_1$.
We choose a coherent system of roots $\beta_j^{1/q}$ of β_j, positive when j is odd, and we define

$$E'\left(z + \frac{p_1}{q_1}\alpha_1 + \frac{p_2}{q_2}\alpha_2\right) := E(z) \cdot \beta_1^{p_1/q_1} \cdot \beta_2^{p_2/q_2}.$$

O-ROOTS We start with a perfectly rotund variety $V(\bar{c}) \subset \mathbb{G}^n$, where $\bar{c}$ is a subset of K closed under σ.
Consider an enumeration $(W_m(\bar{d}_m))_{m<\omega}$ of $\mathcal{R}(V)$, where $\bar{d}_m$ is a finite subset of $\mathrm{acl}(\bar{c}E(\bar{c}))$ over which W is defined.
If $W_m(\bar{d}_m)$ has infinitely many algebraically independent solutions, we proceed to the next one, otherwise we apply O-SOL to $W(\bar{d}_m)$ for $k = 0, 1, \cdots < \omega$. The final exponential function we have just obtained is our E'.

The above operations are doable when the ordered field R is sufficiently saturated.

Proposition 4.2. *If R is $|\mathrm{dom}(E)|^+$-saturated, the parameters involved have cardinality at most $|\mathrm{dom}(E)|$, and the function E restricted to R is increasing, then the operations* O-DOMAIN, O-IMAGE, O-SOL *and* O-ROOTS *are applicable. Moreover, if the resulting field is $K_{E'}$, then $|\mathrm{dom}(E)| = |\mathrm{dom}(E')|$, hence R is still $|\mathrm{dom}(E')|^+$-saturated, and E' restricted to R is increasing.*

Proof. It is clear that O-DOMAIN and O-IMAGE are doable if the ordered field is $|\mathrm{dom}(E)|^+$-saturated: provided that $E_{\restriction R}$ is increasing, the existence of α, resp. of β, is guaranteed by the fact that its desired type is defined over $|\mathrm{dom}(E)|$ and is finitely satisfiable.

For O-SOL, saturation is needed again. Let $V \subset \mathbb{G}^n$ be the absolutely free rotund variety involved. Let us fix $x_1, \ldots, x_n$ points in $\mathrm{dom}(E)$. We claim that there is a transcendental point $(z, w) \in V$ such that for some $1 \leq j < n$, $x_j < \Re(z) < x_{j+1}$ and $f(x_j) < |w| < f(x_{j+1})$.

The set $B := \bigcup_{j=0}^{n}\{(x, w) : x_j \leq x \leq x_{j+1}, f(x_j) \leq w \leq f(x_{j+1})\}$, where we assume $x_0 = -\infty$ and $x_{n+1} = +\infty$, definably disconnects the upper half plane. The image of z on V is K minus finitely many points, and the image of w is $K^\times$ minus finitely many points; hence, the image of $\Re(z)$ is the whole line R, and the image of $|w|$ is $R^\times$. Moreover, the image of $(\Re(z), |w|)$ must be definably connected, and is an open set. This implies that B disconnects the image of $(\Re(z), |w|)$.

By theorem 3.8, the o-minimal dimension of $\begin{pmatrix} 1 & 0 \end{pmatrix} \cdot r(V)$ is 2; we can verify also that the map $r(V) \to \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot r(V)$ is actually finite-to-one (see lemma 4.3). Since $r(V)$ remains connected after removing a finite set of points, the same is true for the image of $(\Re(z), |w|)$. In particular, since B disconnects the image of $(\Re(z), |w|)$, they can only intersect in the *interior* of B, but this implies that the intersection contains an open set. Therefore, there are transcendental points in the intersection.

This implies that the partial type we need to realise is finitely satisfiable; by saturation, there exists a realisation in K.

The operation O-ROOTS is then applicable by the the applicability of O-SOL.

It is clear that $|\mathrm{dom}(E)| = |\mathrm{dom}(E')|$, and that the extension remains an increasing function. □

Lemma 4.3. *Given an affine algebraic curve $\mathcal{C}$ and two non-constant algebraic functions z, w regular at all the points of $\mathcal{C}$, the map $P \mapsto (\Re(z(P)), |w(P)|)$ is finite-to-one.*

Proof. lemma 3.21 already proves that the map is generically finite-to-one, as the functions $\Re(z)$ and $|w|$ are algebraically independent.

As the above map is definable in the language of real closed fields, if it is not finite to one, there should be a semi-algebraic connected curve $\mathcal{S}$ such that for all $P \in \mathcal{S}$, $\Re(z(P)) = x$ and $|w(P)| = \rho$ for some fixed x, ρ. Let us take $P \in \mathcal{S}$ non-singular and such that z is not ramified at P; in this case, $z_P := z - z(P)$ is a local parameter at P. The expansion given of the function w in terms of z_P around any given $P \in \mathcal{S}$ is therefore of the form

$$w = a + bz_P^k + O(z_P^{k+1}),$$

with at least $b \neq 0$. This shows that if $\Im(z_P)$ varies around 0, then $|w|$ must vary; hence, it must be constant. But then z is constant on the intersection of $\mathcal{S}$ with an open neighbourhood of P, hence on an infinite set, a contradiction. □

Note that the operations are special cases of R-DOMAIN, R-IMAGE, R-SOL, and R-ROOTS, so the preservation of (SP), (STD) and (CCP) is trivial.

Proposition 4.4. *If $K_E \subset K_{E'}$ is an extension produced by one of the operations* O-DOMAIN, O-IMAGE, O-SOL, O-ROOTS, *then $K_{E'}$ is a partial E-field with $\sigma \circ E' = E' \circ \sigma$. Moreover, the extension is strong and order-preserving; if (SP), (STD) and (CCP) hold in K_E, then they hold in $K_{E'}$.*

Proof. This is a direct consequence of propositions 3.30, 3.31, 3.32. □

However, a major difference is about (CCP) after multiple iterations. Again, let $(K_{E_j})_{j\leq\alpha}$ be a sequence of partial E-fields over K, with $\sigma \circ E_0 = E_0 \circ \sigma$, whose fixed field R is α-saturated, and α is a cardinal, such that:

- for all $j < \alpha$, $K^{j+1}_{E_{j+1}}$ is an extension of K_{E_j} obtained by one of the basic operations O-DOMAIN, O-IMAGE, O-ROOTS;
- for all $j \leq \alpha$ limit ordinal, E_j by $E_j = \bigcup_{k<j} E_j$.

We can transfer easily (SP) and (STD) from K_{E_0} to K_{E_α}, and for (CCP) we need an argument similar to the one of corollary 2.12.

Let us introduce an intermediate definition between Definitions 2.14 and 3.27.

Definition 4.5. A family $\mathcal{R}(V)$, with $\bar{c}$ E-defining $\check{V}$, is *really completely solved* in K_E if for all $W \in \mathcal{R}(V)$ there is an infinite set of solutions of W really algebraically independent over $\mathrm{acl}(\bar{c}E(\bar{c}))$.

The following stronger version of theorem 3.8 holds.

Proposition 4.6. *Let $V \subset \mathbb{G}^1$ be a simple variety. If $M \in \mathcal{M}_{1,2}(\mathbb{Z})$ is such that* $\dim M \cdot \check{V} = 1$, *then M is of the form*

$$M = \begin{pmatrix} k & \pm k \end{pmatrix}$$

for some integer $k \in \mathbb{Z}$. In particular, the induced map $V \to M \cdot \check{V}$ is surjective.

Proof. It is sufficient to prove the statement on $\mathbb{R}$; since by the work of [Zil05b] the simple varieties are first-order definable, the statement is a conjunction of first-order formulas, one for each matrix $M \in \mathcal{M}_{1,2}(\mathbb{Z})$, so it transfers to all real closed fields.

By theorem 3.8, M must be of the form $M = \begin{pmatrix} a & b \end{pmatrix}$ for some non-zero integers a, b, and $\dim V = 1$.

This means that locally the functions $x + iy$ and $ax + iby$ are holomorphic functions of $\rho\theta$ and $\rho^a\theta^b$ respectively. In particular, $(x + i\frac{b}{a}y)$ is locally a holomorphic function of $\rho\theta^{b/a}$. By the Cauchy-Riemann equations in polar coordinates,

$$\frac{\partial y}{\partial \rho} = -\frac{1}{\rho} \cdot \frac{\partial x}{\partial \vartheta} \quad \text{and} \quad \frac{\frac{b}{a}\partial y}{\partial \rho} = -\frac{1}{\rho} \cdot \frac{\partial x}{\frac{b}{a}\partial \vartheta}.$$

This implies $a^2 = b^2$, i.e., $a = \pm b$.

In other words, $M \cdot \check{V}$ is either $k \cdot V$ or $\sigma(k \cdot V)$ for some integer k. This implies that the induced function $V \to M \cdot \check{V}$ is actually either $V \to k \cdot V$ or $V \to k \cdot V \to \sigma(k \cdot V)$, and both are clearly surjective. □

Using surjectivity, we can repeat the proofs of Propositions 2.18 and 3.29 to obtain the following stronger result.

Proposition 4.7. *Let $V \subset \mathbb{G}^n$ be a rotund variety and K_E a partial E-field such that $\sigma \circ E = E \circ \sigma$. Let $N, Q \in \mathcal{M}_{n,n}(\mathbb{Z})$ be two square integer matrix of maximum rank, $\overline{z} \in \mathrm{dom}(E)^n$, and $X := \begin{pmatrix} N & Q \end{pmatrix} \cdot \check{V} \oplus \langle \overline{z}; E(\overline{z})\rangle$.*

For $W \in \mathcal{R}(V)$, let $Y_W \in \mathcal{R}(X)$ be the variety $\begin{pmatrix} N & Q \end{pmatrix} \cdot \check{W} \oplus \langle \frac{p}{q}\overline{z}; E(\frac{p}{q}\overline{z})\rangle$ for some $p, q \in \mathbb{Z}^\times$. If for all W the induced map $W \to Y_W$ is surjective, then $\mathcal{R}(V)$ is really completely solved if and only if $\mathcal{R}(X)$ is.

Hence, the proof is much more similar to the one of corollary 2.12.

Proposition 4.8. *If K_{E_0} satisfies (SP), (STD) or (CCP), then K_{E_α} satisfies resp. (SP), (STD) or (CCP).*

Proof. The properties (SP) and (STD) are trivial by the above arguments. For (CCP), the proof is the same as the one of corollary 2.12, except that we replace the use of proposition 2.18 with proposition 4.7. □

Again, we can easily construct the fields of theorem 4.1 with an inductive procedure.

Let us consider a real closed field R which is $|K|$-saturated, and let L be its algebraic closure and σ the unique non-trivial automorphism of L/R.

We define a sequence of partial E-fields $\{K^{(j)}_{E_j}\}_{j \leq |K|}$ in the following way. At the base step, we define $E_0(\frac{p}{q}\omega) := \zeta_q^p$, where ω is an *imaginary* transcendental number, (ζ_q) is a coherent system of roots of unity, and $K^{(0)} = \overline{\mathbb{Q}}$. It is easy to see that $\sigma \circ E_0 = E_0 \circ \sigma$, and that the restriction to R is increasing (it is the trivial exponential function). We go on in the following way.

1. if $j = k + 1$,
   (a) temporary extend $K^{(k)}$ to L;
   (b) apply O-DOMAIN to all the elements of $K^{(k)}$ to obtain E' from E_k;
   (c) apply O-IMAGE to all the elements of $K^{(k)}(\mathrm{dom}(E'))$ to obtain E'' from E';
   (d) apply O-ROOTS to all the perfectly rotund varieties of dimension 1 defined over $K^{(k)}(\mathrm{dom}(E''), \mathrm{im}(E''))$ to obtain E_j from E'';
   (e) define $K^{(j)}$ as $K^{(k)}(\mathrm{dom}(E_j), \mathrm{im}(E_j))$;
2. if j is a limit ordinal, define $E_j := \bigcup_{k<j} E_k$ and $K^{(j)} := \bigcup_{k<j} K^{(k)}$.

Proof of theorem 4.1. Clearly, each intermediate exponential function has domain of cardinality less than $|L|$; hence, by proposition 4.2, the operations can be always applied. Note also that each intermediate field is closed under σ, hence σ restricts to an involution of the intermediate field. By proposition 4.8, the result satisfies (SP), (STD) and (CCP); moreover, by construction, it clearly satisfies (E), (LOG) and (1-SEC). Its cardinality is exactly $|K|$, hence we can identify $K^{(|K|)}$ with K. □

Note that since the resulting K_E is an E-field satisfying (STD), (SP) and (CCP), by corollary 2.22 it embeds into a Zilber field.

If we drop also (1-SEC), then it is easy to produce a *continuous* function E.

Theorem 4.9. *For all saturated algebraically closed fields K of characteristic 0 there is a function $E : K \to K^\times$ and an involution σ commuting with E such that K_E satisfies (E), (LOG), (STD), (SP), and (CCP), and E is a continuous function with respect to the topology induced by σ.*

This result is also mentioned in [Man11b].

In this case, we do not use the operations SOL and ROOTS any more. The only operations we need to define are 'C-DOMAIN' and 'C-IMAGE': we make sure at once that $E : R \to R$ is monotone and that $E : [0, \omega) \to \mathbb{S}^1(K)$ is *locally increasing*. In other words, we require that for any $i\alpha \in \mathrm{dom}(E) \cap iR$, if we consider $\mathbb{S}^1(K)$ as ordered anticlockwise starting at $E(i\alpha)$, then the map E restricted to $i \cdot [\alpha, \alpha + \omega)$ is order-preserving.

Let us suppose that K_E is a partial E-field with an involution σ, with kernel $i\omega\mathbb{Z}$, where $\omega \in R_{>0}$, and such that $E(i\frac{1}{q}\omega)$ is decreasing for $q \geq 1$ for the anticlockwise order on $\mathbb{S}^1(K)$ starting at 1.

C-DOMAIN We start with an $\alpha \in K$. If $\alpha \in \mathrm{dom}(E)$, we define $E' := E$, otherwise we do the following.
We choose two elements $\beta \in R_{>0}, \gamma \in \mathbb{S}^1(R)$ algebraically independent over $F \cup \{\Re(\alpha), \Im(\alpha)\}$, with the property that for each $\varepsilon \in \mathrm{dom}(E) \cap R$, $\varepsilon < \Re(\alpha)$ if and only if $E(\varepsilon) < \beta$, and for each $i\eta \in \mathrm{dom}(E) \cap i \cdot [\Im(\alpha) - \frac{\omega}{2}, \Im(\alpha) + \frac{\omega}{2})$, $\eta < \Im(\alpha)$ if and only if $E(\eta) < \gamma$ in the anticlockwise order on $\mathbb{S}^1(K)$ starting at $\gamma \cdot E(\frac{\omega}{2})$.
Fix the positive roots $\beta^{1/q}$, and if there exist $i\eta \in \mathrm{dom}(E) \cap i \cdot (\Im(\alpha) - \frac{\omega}{2}, \Im(\alpha))$, fix $\gamma^{1/q}$ to be the unique q-th root of γ contained in the shortest arc determined by $E(\frac{1}{q}i\eta)$ and $E(\frac{1}{q}i(\eta + \frac{\omega}{2}))$. Otherwise, fix by induction $\gamma^{1/(q+1)}$ to be the unique q-th root of γ contained in the anticlockwise arc from 1 to $\gamma^{1/q}$.
We define then $E'(z + \frac{p}{q}\Re(\alpha) + i\frac{p'}{q'}\Im(\alpha)) := E(z) \cdot \beta^{p/q} \cdot \gamma^{p'/q'}$ for all $z \in \mathrm{dom}(E)$ and $p, p' \in \mathbb{Z}, q, q' \in \mathbb{N}^\times$.

C-IMAGE We start with a $\beta \in K$ given as data to the operation. If $\beta \in \mathrm{im}(E)$, we define $E' := E$, otherwise we do the following.

We choose two elements $\alpha \in R, i\delta \in iR$ algebraically independent over $F \cup \{|\beta|, \Theta(\beta)\}$, with the property that for each $\varepsilon \in \mathrm{dom}(E) \cap R$, $\varepsilon < \alpha$ if and only if $E(\varepsilon) < |\beta|$, and for each $i\eta \in \mathrm{dom}(E) \cap i \cdot [\delta - \frac{\omega}{2}, \delta + \frac{\omega}{2})$, $\eta < \delta$ if and only if $E(\eta) < \Theta(\beta)$ in the anticlockwise order on $\mathbb{S}^1(K)$ starting at $\Theta(\beta) \cdot E(\frac{\omega}{2})$.

If there exist $i\eta \in \mathrm{dom}(E) \cap i \cdot (\delta - \frac{\omega}{2}, \delta)$, fix $\Theta(\beta)^{1/q}$ to be the unique q-th root of $\Theta(\beta)$ contained in the shortest arc determined by $E(\frac{1}{q}i\eta)$ and $E(\frac{1}{q}i(\eta + \frac{\omega}{2}))$. Otherwise, fix by induction $\Theta(\beta)^{1/(q+1)}$ to be the unique q-th root of $\Theta(\beta)$ contained in the anticlockwise arc from 1 to $\Theta(\beta)^{1/q}$.

We define then $E'(z + \frac{p}{q}\alpha + \frac{p'}{q'}\delta) := E(z) \cdot |\beta^{p/q}| \cdot \Theta(\beta)^{p'/q'}$ for all $z \in D$ and $p, p' \in \mathbb{Z}, q, q' \in \mathbb{N}^\times$.

The situation is the same as before.

Proposition 4.10. *If R is $|\mathrm{dom}(E)|^+$-saturated, the function E restricted to R is increasing, and restricted to iR is locally increasing, then the operations* C-DOMAIN *and* C-IMAGE *are applicable. Moreover, if the resulting field is $K_{E'}$, then $|\mathrm{dom}(E)| = |\mathrm{dom}(E')|$, hence R is still $|\mathrm{dom}(E')|^+$-saturated, E' restricted to R is increasing and restricted to iR is locally increasing.*

Proof. The operations can be applied for the same argument of the proof of proposition 4.2, and the function E is still increasing on R and locally increasing on iR. □

As the only operations are subcases of DOMAIN and IMAGE, we can apply directly corollary 2.9 and proposition 2.19 to know that any construction made with C-DOMAIN and C-IMAGE, starting with a partial E-field with (SP), (STD) and (CCP), produces a partial E-field with (SP), (STD) and (CCP).

As before, we construct the answer of theorem 4.9 starting with a sufficiently saturated real closed field. Let us consider again a real closed field R which is $|K|$-saturated, and let L be its algebraic closure and σ the unique non-trivial automorphism of L/R.

We define a sequence of partial E-fields $\{K_{E_j}^{(j)}\}_{j \leq |K|}$ in the following way. At the base step, we define $E_0(\frac{p}{q}\omega) := \zeta_q^p$, where ω is an *imaginary* transcendental number, and (ζ_q) is a *decreasing* coherent system of roots of unity, i.e., we take each time the qth root nearest to 1 in the upper half plane, and $K^{(0)} = \overline{\mathbb{Q}}$. It is easy to see that $\sigma \circ E_0 = E_0 \circ \sigma$, and that the restrictions to R and iR are resp. increasing and locally increasing. Then we proceed by induction.

1. if $j = k + 1$,
   (a) temporary extend $K^{(k)}$ to L;
   (b) apply C-DOMAIN to all the elements of $K^{(k)}$ to obtain E' from E_k;
   (c) apply C-IMAGE to all the elements of $K^{(k)}(\mathrm{dom}(E'))$ to obtain E_{k+1} from E';
   (d) define $K^{(k+1)}$ as $K^{(k)}(\mathrm{dom}(E_{k+1}), \mathrm{im}(E_{k+1}))$;
2. if j is a limit ordinal, define $E_j := \bigcup_{k<j} E_k$ and $K^{(j)} := \bigcup_{k<j} K^{(k)}$.

Proof of theorem 4.9. As before, each intermediate exponential function has domain of cardinality less than $|K|$; hence, by proposition 4.10, the operations can be always applied. Each intermediate field is closed under σ, hence σ restricts to an involution of the intermediate field. By the above considerations, the result satisfies (SP), (STD) and (CCP); moreover, by construction, it clearly satisfies (E) and (LOG). Since the cardinality of $K^{(|K|)}$ is exactly $|K|$, we can identify $K^{(|K|)}$ with K. It is easy to see that since E is defined on the whole K, and is increasing and locally increasing on $K \cap R$ and $K \cap iR$ resp., then it is a continuous function. □

Again, the resulting structures embed into Zilber fields.

These examples show quite well the two obstructions that our method is not able to overcome. First of all, if $V \subset \mathbb{G}^n$, it is not always true that the topological dimension of $\begin{pmatrix} \mathrm{Id} & 0 \end{pmatrix} \cdot \check{V}$ is $2n$, so the argument of proposition 4.2 does not work in the general case, and we cannot produce an order-preserving exponential function. This destroys continuity as well.

Moreover, if we want to avoid dense sets of solutions, this argument shows that if we manage to strengthen theorem 3.8 as in proposition 4.6, namely, if we discover that the map $V \to M \cdot \check{V}$ is surjective also for larger varieties other than curves, then proposition 4.7 would apply in all cases; hence, we would not need the density arguments and the second countability, as the proof of proposition 4.8 would be sufficient to get (CCP) without further complications. In particular, it would be possible to find involutions on Zilber fields of arbitrary cardinalities, using arbitrary real closed fields, and we would find models outside of the class described in section 3.2. Work is in progress about finding such a generalisation.

4.2 Algebraic exponentiation

Another curious example is built by dropping (SP) instead of (SEC). We show that it is possible to have an existentially closed *ELA*-field with standard kernel whose underlying field is the the field of algebraic numbers (for an appropriate meaning of "existentially closed"). The axiom (SEC) is also weakened a bit, as we cannot require generic solutions on algebraic numbers; we just ask that the solutions are Zariski-dense.

Theorem 4.11. *There is a function $E : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ such that $\overline{\mathbb{Q}}_E$ is an ELA-field with standard kernel and is existentially closed in the following sense:*

- *for any absolutely free variety V over $\overline{\mathbb{Q}}$ and any proper subvariety $V' \subset V$, there is an $\overline{x} \subset \overline{\mathbb{Q}}$ such that $(\overline{x}, E(\overline{x})) \in V \setminus V'$.*

This result is proved in [Man12].

If we consider the class of partial E-fields with standard kernel, then $\overline{\mathbb{Q}}_E$ is existentially closed in this class: whenever $\overline{\mathbb{Q}}_E \subset K_{E'}$, and some finite system of polynomial exponential equations and inequations with parameters in $\overline{\mathbb{Q}}$ has a solution in $K_{E'}$, then it already has a solution in $\overline{\mathbb{Q}}_E$.

The construction is easily done using the previous machinery. We define again the operations.

Q-DOMAIN We start with an $\alpha \in \overline{\mathbb{Q}}$. If $\alpha \in \mathrm{dom}(E)$, we define $E' := E$, otherwise we do the following.
We choose an element $\beta \in \overline{\mathbb{Q}}^\times$ multiplicatively independent over F, and we fix an arbitrary system of roots $\beta^{1/q}$.
We define then $E'(z + \frac{p}{q}\alpha) := E(z) \cdot \beta^{p/q}$ for all $z \in \mathrm{dom}(E)$ and $p \in \mathbb{Z}, q \in \mathbb{N}^\times$.

Q-IMAGE We start with a $\beta \in \overline{\mathbb{Q}}$. If $\beta \in \mathrm{im}(E)$, we define $E' := E$, otherwise we do the following.
We choose an element $\alpha \in \overline{\mathbb{Q}}$ $\mathbb{Q}$-linearly independent over $\mathrm{dom}(E)$ and an arbitrary coherent system of roots $\beta^{1/q}$.
We define then $E'(z + \frac{p}{q}\alpha) := E(z) \cdot \beta^{p/q}$ for all $z \in D$ and $p \in \mathbb{Z}, q \in \mathbb{N}^\times$.

Q-SOL We start with a perfectly rotund variety $V(\overline{c}) \subset \mathbb{G}^1$, and a proper Zariski-closed subset $W \subset V$.

We choose a point $\langle \overline{\alpha}; \overline{\beta} \rangle \in V \setminus W(\overline{\mathbb{Q}})$ such that $\overline{\alpha}$ is $\mathbb{Q}$-linearly independent from $\mathrm{dom}(E)$, and $\overline{\beta}$ is multiplicatively independent from $\mathrm{im}(E)$.
We choose a coherent system of roots $\beta_j^{1/q}$ of β_j, positive when j is odd, and we define

$$E'\left(z + \frac{p_1}{q_1}\alpha_1 + \cdots + \frac{p_n}{q_n}\alpha_n\right) := E(z) \cdot \beta_1^{p_1/q_1} \cdot \cdots \cdot \beta_n^{p_n/q_n}.$$

In this construction, the only difficult part is showing that the operations can be applied.

Proposition 4.12. *If* $\mathrm{dom}(E)$ *has finite* $\mathbb{Q}$*-linear dimension, then the operations* Q-DOMAIN, Q-IMAGE *and* Q-SOL *are applicable. Moreover, if the resulting field is* $\overline{\mathbb{Q}}_{E'}$*, then* $\mathrm{dom}(E')$ *has finite dimension too.*

Proof. Of course, $\overline{\mathbb{Q}}$ has infinite $\mathbb{Q}$-linear dimension, and $\overline{\mathbb{Q}}^{\times}$ has infinite multiplicative rank; hence, Q-DOMAIN and Q-IMAGE are always applicable when $\mathrm{dom}(E)$ has finite $\mathbb{Q}$-linear dimension (and therefore $\mathrm{im}(E)$ has finite multiplicative rank).

The possibility of Q-SOL is instead a consequence of proposition 4.13 that will be proved in the next section. □

Since the operations are applicable, the construction of a solution to theorem 4.11 is straightforward.

We define a sequence of partial E-fields $\{\overline{\mathbb{Q}}_{E_j}\}_{j \leq \omega}$ in the following way. At the base step, we define $E_0(\frac{p}{q}\omega) := \zeta_q^p$, where ω is any non-zero algebraic number, and (ζ_q) is a coherent system of roots of unity. Then we enumerate all the elements of $\overline{\mathbb{Q}}$ as $(\alpha_n)_{n<\omega}$ and all the pairs (V_n, W_n) where V_n is an absolutely free rotund variety over $\overline{\mathbb{Q}}$, and W_n is a proper Zariski closed subset of V_n, and proceed as follows.

1. if $j = k + 1$,
   (a) apply Q-DOMAIN to α_k to obtain E' from E_k;
   (b) apply Q-IMAGE to α_k to obtain E'' from E';
   (c) apply Q-SOL to the pair (V_n, W_n) to obtain E_{k+1} from E'';
2. if $j = \omega$, define $E_\omega = \bigcup_{j<\omega} E_j$.

It is clear that the resulting partial E-field is an ELA-field with (STD) that is existentially closed in the sense of theorem 4.11.

4.2.1 Points with independent coordinates

In order to finish the proof, we need to verify the following fact.

Proposition 4.13. *Let* $V \subset (\mathbb{G}_a \times \mathbb{G}_m)^n$ *be an irreducible absolutely free variety over* $\overline{\mathbb{Q}}$*, and let* $L < \overline{\mathbb{Q}}$*,* $M < \overline{\mathbb{Q}}^*$ *be two finite-rank subgroups. The set of points* $(\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n) \in V$ *such that* $\alpha_1, \ldots, \alpha_n$ *is* $\mathbb{Q}$*-linearly independent from* L*, and such that* $\beta_1, \ldots, \beta_n$ *are multiplicatively independent from* M*, is Zariski dense in* V*.*

It is known that if we take a variety V and some functions on it that are multiplicatively independent (the functions are allowed to be constant), then for "most" points $P \in V(\overline{\mathbb{Q}})$ the values of the functions at P are still multiplicatively independent [Mas89].

Similarly, it is also not difficult to show that at many points the specialisations of $\mathbb{Q}$-linearly independent functions are still $\mathbb{Q}$-linearly independent (again, functions are allowed to be constant). In order to put together the two statements, we first intersect our variety with hyperplanes, using Bertini's theorem, to reduce to the case when V is a curve. We first take care of the additive part.

Proposition 4.14. *Let $\mathcal{C}$ be a quasi-projective absolutely irreducible curve defined over a field K, and let $k = \overline{\mathbb{Q}} \cap K$. Let $x_1, \dots, x_n$ be some $\mathbb{Q}$-linearly independent functions in $K(\mathcal{C})$. Let $z \in K(\mathcal{C})$ be a non constant function.*

There is a number $d > 0$, not dependent on z, such that for any $\alpha \in \overline{\mathbb{Q}}$ with $[k(\alpha) : k] > d$, the specialisations of $x_1, \dots, x_n$ at any point $P \in z^{-1}(\alpha)$ are $\mathbb{Q}$-linearly independent.

Proof. Without loss of generality we may assume that $\mathcal{C}$ is smooth. We may also assume that the first functions $x_1, \dots, x_c$ are constant, while the remaining $x_{c+1}, \dots, x_n$ are not. Let e be the maximum of $[K(\mathcal{C}) : K(x_i)]$ as x_i ranges among the last $n-k$ non constant functions.

Clearly, the equation

$$m_1 x_1 + \dots + m_c x_c + m_{c+1} x_{c+1} + \dots + m_n x_n = 0,$$

with the m_i's not all zero, can be solved only in at most $(n-c)e$ points algebraic over K, since the function on the left is either constant, hence non-zero by assumption, or it has degree at most $(n-c)e$. This implies that for any $\alpha \in \overline{\mathbb{Q}}$, if $[K(\alpha) : K] = [k(\alpha) : k] > (n-c)e$, then any $P \in z^{-1}(\alpha)$ is such that $x_1(P), \dots, x_n(P)$ are $\mathbb{Q}$-linearly independent. Note that it may happen for finitely many α's that there are no points of $\mathcal{C}$ in $z^{-1}(\alpha)$, since the curve is just quasi-projective.

Indeed, let L be a normal extension of K which defines P. Clearly, $L \cap \overline{\mathbb{Q}} \supset k(\alpha)$ is a normal extension of k by the assumption $k = K \cap \overline{\mathbb{Q}}$. Since $\mathcal{C}$ is absolutely irreducible, we can extend the Galois action of $\mathrm{Gal}(L/K)$ to $\mathrm{Gal}(L(\mathcal{C})/K(\mathcal{C}))$. If there are $m_1, \dots, m_n$ such that the above equation is satisfied, then by conjugation we obtain several other $\sigma(P)$ satisfying the same equation. Since $z(\sigma(P)) = \sigma(\alpha)$, and $[k(\alpha) : k] > (n-c)e$, we find more than $(n-c)e$ distinct conjugates of P all satisfying the above equation, a contradiction. $\square$

Corollary 4.15. *Let $\mathcal{C}$ be an absolutely irreducible curve defined over k. Let $x_1, \dots, x_n$ be some $\mathbb{Q}$-linearly independent functions in $k(\mathcal{C})$.*

There is a number $d' > 0$ such that for any $P \in \mathcal{C}(\overline{k})$ with $[k(P) : k] > d'$, the specialisations of $x_1, \dots, x_n$ at P are $\mathbb{Q}$-linearly independent.

Proof. Let us take a non-constant function $z \in k(\mathcal{C})$, whose degree is at most some number e.

Let d be the number obtained by proposition 4.14, and let $d' \geq d \cdot e$. We take d' large enough such that $z(P)$ is defined for each point with $[k(P) : k] > d'$.

Now, if P is a point such that $[k(P) : k] > d' := d \cdot e$, then $z(P)$ is defined, finite and $[k(z(P)) : k] > d$. By the previous proposition, the specialisations of $x_1, \dots, x_n$ at P are $\mathbb{Q}$-linearly independent. $\square$

An analogous but different statement holds for the multiplicative case for varieties of dimension greater than 1.

Proposition 4.16. *Let V be an absolutely irreducible quasi-projective variety defined over k with $\dim(V) > 1$. Let $w_1, \dots, w_n$ be some functions in $k(V)$ that are multiplicatively independent modulo constants.*

There is a non-constant function $z \in k(V)$ such that the restrictions of $w_1, \dots, w_n$ at $V \cap \{z = \alpha\}$ are multiplicatively independent modulo constants for almost all $\alpha \in \overline{k}$.

Proof. Without loss of generality, we may assume that V is smooth and projective.

Since $w_1, \ldots, w_n$ are multiplicatively independent modulo constants, it means that the Weil divisors of $w_1, \ldots, w_n$ are $\mathbb{Q}$-linearly independent. Up to taking a multiplicative combination of the w_i's, we may assume that there are $W_1, \ldots, W_n$ distinct prime divisors such that w_i has a pole in W_i, but has no zeroes and poles among the remaining W_j's; in other words, the matrix $(o_{W_i}(w_j))_{i,j}$ is diagonal.

Up to enlarging k, we may assume that these prime divisors have degree 1 and are all defined over k. It is clear that in the space of all hyperplanes H that intersect V properly, the ones such that $H \cap W_i = H \cap W_j$, with $i \neq j$, form a proper, or even empty, Zariski closed subset. By Bertini's theorem, it is also true that the ones such that $H \cap V$ is not absolutely irreducible, and similarly the ones such that $H \cap W_i$ is not absolutely irreducible, form proper Zariski closed sets.

It is clear that we can find an hyperplane H represented by an equation $z = 0$ such that $\{z = \alpha\} \cap W_i$ and $\{z = \alpha\} \cap V$ are all smooth absolutely irreducible varieties for almost all $\alpha \in \overline{k}$. But then the restrictions of $w_1, \ldots, w_n$ to $\{z = \alpha\} \cap V$ are such that $(o_{H \cap W_i}(w_j))_{i,j}$ is still a diagonal matrix, which implies that their divisors are still $\mathbb{Q}$-linearly independent, hence the restrictions are multiplicatively independent modulo constants. □

Using the above statements, we can easily reduce to the case of curves, which we solve in the following proposition.

Proposition 4.17. *Let $\mathcal{C} \subset (\mathbb{G}_a \times \mathbb{G}_m)^n$ be an irreducible curve over $\overline{\mathbb{Q}}$ and $L < \overline{\mathbb{Q}}$, $M < \overline{\mathbb{Q}}^*$ be two finite-rank subgroups. If $\mathcal{C}$ is absolutely multiplicatively free, and additively free over L, then the set of points $(\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n) \in \mathcal{C}$ such that $\alpha_1, \ldots, \alpha_n$ is $\mathbb{Q}$-linearly independent from L, and such that $\beta_1, \ldots, \beta_n$ are multiplicatively independent from M, is Zariski dense in $\mathcal{C}$.*

Proof. Without loss of generality, we may assume that $\mathcal{C}$ is absolutely irreducible. Let $w_1, \ldots, w_n$ be the multiplicative coordinate functions of $\mathcal{C}$, and let $a_1, \ldots, a_m$ be a finite set of divisible generators of M, and let H be a hypersurface not containing $\mathcal{C}$. Let k be a number field defining $\mathcal{C}$ and H and containing $a_1, \ldots, a_m$.

Using the notation of [Mas89], we define

- $\mathcal{C}(d, h)$ the set of all points of $\mathcal{C}$ of degree at most d and height at most h;
- $\mathcal{E}(d, h)$ the set of all points of $\mathcal{C}$ of degree at most d and height at most h such that the specialisations of $w_1, \ldots, w_n$ are multiplicatively dependent on M;
- $\omega(S)$, for a finite set S, the minimum degree of an hypersurface containing all the points of S.

Applying the main result of [Mas89, §5] to $\mathbb{G}_m(k(\mathcal{C}))$ and to the group generated by $w_1, \ldots, w_n$ and $a_1, \ldots, a_n$, we find a function $c_1(d)$ and a number e such that $\omega(\mathcal{E}(d, h)) \leq c_1(d)h^e$, while we also find a c_2 such that $\omega(\mathcal{C}(d, h)) \geq \exp(c_2(d)h)$ when d is at least the degree of $\mathcal{C}$. [1]

Now using corollary 4.15 on $\mathcal{C}$ and L we obtain a number d_1 such that when $[k(P) : k] > d_1$ the additive coordinates of P are $\mathbb{Q}$-linearly independent from L. We may choose d_1 larger than the product of the degrees of $\mathcal{C}$ and H. Now let d_2, h_1, h_2 be numbers such that

$$\omega(\mathcal{C}(d_2, h_2)) \geq \exp(c_2(d_2)h_2) > \omega(\mathcal{C}(d_1, h_1)) + c_1(d_2)h_2^e \geq$$
$$\geq \omega(\mathcal{C}(d_1, h_1)) + \omega(\mathcal{E}(d_2, h_2));$$

[1] The statement of [Mas89] is actually that $\omega(\mathcal{C}(d, h)) \geq \exp(ch)$ when $d = \deg(\mathcal{C})$. However, the proof only requires that there is a dominant map $\pi : \mathcal{C} \to \mathbb{P}^m$ of degree d with $m = \dim \mathcal{C}$. Such maps exist for example for any multiple of $\deg(\mathcal{C})$, as we can compose π with dominant self maps of $\mathbb{P}^m$ which exist for any positive degree.

Then there must be a point P outside of H, of degree strictly greater than d_1, such that the specialisations of $w_1, \dots, w_n$ at P are multiplicatively independent from $a_1, \dots, a_n$, hence from M. Since its degree is greater than d_1, its additive coordinates are also $\mathbb{Q}$-linearly independent from L, as desired. □

It only remains to show that we can reduce to curves.

Proof of proposition 4.13. We prove the theorem by induction on $m = \dim(V)$. Our inductive hypothesis is that V is absolutely irreducible, absolutely multiplicatively free, and that it is additively free over L. The base case $m = 1$ is covered by proposition 4.17. Let k be a number field defining V.

Let us suppose that $m > 1$, and that we have proven the theorem for all the varieties of dimension $m-1$. Let $x_1, \dots, x_n$ be the additive coordinate functions of V, and $w_1, \dots, w_n$ be its multiplicative coordinate functions. Moreover, let $\{b_1, \dots, b_m\}$ be a $\mathbb{Q}$-basis of the vector space generated by L. By proposition 4.16, there is a non-constant function z such that for almost all $\alpha \in \overline{k}$ we have

1. $V_\alpha := V \cap \{z = \alpha\}$ is absolutely irreducible;
2. $\dim(V_\alpha) = m - 1$;
3. the functions $\{w_1, \dots, w_n\}$ restricted to V_α are multiplicatively independent modulo constants.

Now take any transcendence base of $k(V)$ of the form $X \cup \{z\}$. Then V can be seen also as a quasi-projective absolutely irreducible curve over $k(X)$, and z is a nonconstant function on it.

By applying proposition 4.14 to V seen as a curve over $K := k(X)$, as soon as $[k(\alpha) : k]$ is sufficiently large, the functions $\{x_1, \dots, x_n, b_1, \dots, b_m\}$ are $\mathbb{Q}$-linearly independent when restricted to V_α. Therefore V_α satisfies the same properties of V, and by inductive hypothesis, it contains a Zariski-dense set of points whose additive coordinates are $\mathbb{Q}$-linearly independent from L, and whose multiplicative coordinates are multiplicatively independent from M.

Now, if $W \subset V$ is a proper closed subset, then for almost all α's $W \cap V_\alpha$ is a proper closed subset of V_α. This implies that we can find such points outside of W, and in turn, they are Zariski-dense in V. □

Remark 4.18. The above proof relies on the results exposed in [Mas89]. These results depend on the Northcott Property of number fields. Using other techniques of Diophantine geometry it is possible to obtain a similar result for other finitely generated fields without the same quantitative statements, but still strong enough to obtain again proposition 4.17. This implies that this construction works also on all algebraically closed fields of characteristic 0, and in particular of any fixed transcendence degree.

Chapter 5

Conclusions

The conjecture $\mathbb{B}_E \cong \mathbb{C}_{\exp}$ is a strong one, and as we explained, it is equivalent to Schanuel's Conjecture plus that (SEC) holds on $\mathbb{C}_{\exp}$.

It is generally believed that Schanuel's Conjecture is true, even if it is considered far from being solved, as it would just settle many transcendence questions, and predicts naturally the few theorems we know; and as a nice bonus, it implies that $\mathbb{R}_{\exp}$ is decidable. If Schanuel's Conjecture is true, then at least $\mathbb{C}_{\exp}$ embeds into $\mathbb{B}_E$ (e.g., see corollary 2.22).

For (SEC), however, the conjecture is quite new, although a weaker related statement, the Converse Schanuel's Conjecture, already appeared. There doesn't seem to be a general consensus on whether it should be true or not, but it is possible that it actually follows from Schanuel's Conjecture.

We have seen that people are trying to draw analogies between $\mathbb{B}_E$ and $\mathbb{C}_{\exp}$, while we wait for new ideas to tell us more about the conjecture. An encouraging fact is that some of these analogies, as the Schanuel Nullstellensatz, follow just from (SEC).

In this work we have proved that just like $\mathbb{C}_{\exp}$ has complex conjugation, $\mathbb{B}_E$ has a 'pseudo-conjugation', an involution whose fixed field is $\mathbb{R}$ (or any separable real closed field). The proof does not follow from the axioms defining Zilber fields, but rather from the fact that it is quite easy to build exponential fields with automorphisms of order two; and with some effort, it turns out that we are able to build Zilber fields as well.

We find it interesting that (SEC), together with (CCP), is the axiom giving more difficulties. As seen in section 4.1, the issues with (CCP) requiring the use of dense sets of solutions, and separable real closed fields, would disappear if we knew that the map $V \to M \cdot \check{V}$ is surjective in the relevant cases; we feel that this statement should be true, even if we did not find a general argument for proving it, and it could be worth exploring a bit more.

Always in section 4.1 we have seen that (SEC) does not play well with order-preserving exponential functions. It is not at all clear if it is possible to repeat the same construction for higher dimensional varieties, because the projection of a rotund variety onto the real parts and moduli of its coordinate functions could be too small, and in general its shape is unknown. This is another issue worth a little more investigation.

We hope that this work can add some useful data for our understanding of $\mathbb{B}_E$, and especially on the interactions between (SEC) and other properties of exponential fields. Of course, as far as the main conjecture is concerned we are still very far away from good news; but for now, we can still add a new theorem to the list of non-refuting facts of $\mathbb{B}_E$ that give the conjecture plausibility.

Bibliography

[Bal09] John T. Baldwin. *Categoricity*. University Lecture Series. American Mathematical Society, Providence, Rhode Island, 2009. ISBN 0821848933.

[Bay09] Martin Bays. *Categoricity Results for Exponential Maps of 1-Dimensional Algebraic Groups & Schanuel Conjectures for Powers and the CIT*. Ph.d., Oxford University, 2009.

[BHH+12] Martin Bays, Bradd Hart, Tapani Hyttinen, Kesälä, and Jonathan Kirby. Quasiminimal structures and excellence, October 2012. URL `http://arxiv.org/abs/1210.2008`.

[BZ11] Martin Bays and Boris Zilber. Covers of multiplicative groups of algebraically closed fields of arbitrary characteristic. *Bulletin of the London Mathematical Society*, **43**(4):689–702, February 2011. ISSN 0024-6093. doi:10.1112/blms/bdq131.

[DMT10] Paola D'Aquino, Angus Macintyre, and Giuseppina Terzo. Schanuel Nullstellensatz for Zilber fields. *Fundamenta Mathematicae*, **207**(2):123–143, 2010. ISSN 0016-2736. doi:10.4064/fm207-2-2.

[Gav12] Misha Gavrilovich. Covers of Abelian varieties as analytic Zariski structures. *Annals of Pure and Applied Logic*, **163**(11):1524–1548, November 2012. ISSN 01680072. doi:10.1016/j.apal.2011.12.007.

[Gel34] Alexandr O. Gelfond. Sur le septième Problème de Hilbert. *Bulletin de la Académie des Sciences de l'URSS, Classe des sciences mathématiques et naturelles*, **4**:623–634, 1934.

[Gun11] Ayhan Gunaydin. Rational solutions of polynomial-exponential equations, October 2011. doi:10.1142/S1793042112500820. URL `http://arxiv.org/abs/1110.6405`.

[Hal35] Philip Hall. On Representatives of Subsets. *Journal of the London Mathematical Society*, **s1-10**(1):26–30, October 1935. ISSN 0024-6107. doi:10.1112/jlms/s1-10.37.26.

[Her73] Charles Hermite. Sur la fonctionne exponentielle. *Comptes Rendu de l'Académie des Siences*, **77**:18–24, 1873.

[HR84] C. Ward Henson and Lee A. Rubel. Some applications of Nevanlinna theory to mathematical logic: identities of exponential functions. *Transactions of the American Mathematical Society*, **282**(1):1–32, 1984.

[Hru93] Ehud Hrushovski. A new strongly minimal set. *Annals of Pure and Applied Logic*, **62**(2):147–166, 1993.

[Kir09] Jonathan Kirby. Finitely Presented Exponential Fields, December 2009. URL `http://arxiv.org/abs/0912.4019`.

[Kir10] —. Exponential algebraicity in exponential fields. *Bulletin of the London Mathematical Society*, **42**(5):879–890, June 2010. ISSN 0024-6093. doi:10.1112/blms/bdq044.

[KMO12] Jonathan Kirby, Angus Macintyre, and Alf Onshuus. The algebraic numbers definable in various exponential fields. *Journal of the Institute of Mathematics of Jussieu*, pages 1–10, April 2012. ISSN 1474-7480. doi:10.1017/S1474748012000047.

[Lan67] Serge Lang. *Introduction to transcendental numbers*. Addison-Wesley Publishing Company, Reading, Mass, 1967. ISBN 9780201041767.

[Mac96] Angus Macintyre. Exponential Algebra. In Aldo Ursini and Paolo Aglianò, editors, *Logic and Algebra*, Lecture notes in pure and applied mathematics, pages 191–210. Marcel Dekker, Inc., New York, 1996. ISBN 0-8247-9606-3.

[Man11a] Vincenzo Mantova. Involutions on Zilber fields. *Rendiconti Lincei - Matematica e Applicazioni*, **22**(2):237–244, 2011. ISSN 1120-6330. doi:10.4171/RLM/598.

[Man11b] —. Involutions on Zilber fields, September 2011. URL `http://arxiv.org/abs/1109.6155`.

[Man12] —. A pseudoexponentiation-like structure on the algebraic numbers, February 2012. URL `http://arxiv.org/abs/1202.4022`.

[Mar06] David Marker. A remark on Zilber's pseudoexponentiation. *Journal of Symbolic Logic*, **71**(3):791–798, 2006. ISSN 0022-4812. doi:10.2178/jsl/1154698577.

[Mas89] David W. Masser. Specializations of Finitely Generated Subgroups of Abelian Varieties. *Transactions of the American Mathematical Society*, **311**(1):413–424, 1989.

[Nes96] Yuri V. Nesterenko. Modular functions and transcendence questions. *Sbornik Mathematics*, **187**(9):1319–1348, 1996.

[Ram67] K Ramachandra. Contributions to the theory of transcendental numbers I, II. *Acta Arithmetica*, **14**:65–72, 73–88, 1967. ISSN 0065-1036.

[Sch34] Theodor Schneider. Transzendenzuntersuchungen periodischer Funktionen I, II. *Journal für die reine und angewandte Mathematik*, **172**:65–69, 70–74, 1934.

[She83] Saharon Shelah. Classification theory for non-elementary classes I: The number of uncountable models of $\psi \in L_{\omega_1,\omega}$. Part A. *Israel Journal of Mathematics*, **46**(3):212–240, September 1983. ISSN 0021-2172. doi:10.1007/BF02761954.

[Shk09] Ahuva C. Shkop. Henson and Rubel's Theorem for Zilber's Pseudoexponentiation, March 2009. URL `http://arxiv.org/abs/0903.1442`.

[Shk11] —. Real Closed Exponential Subfields of Pseudoexponential Fields, December 2011. URL `http://arxiv.org/abs/1112.4784`.

[vL82] Ferdinand von Lindemann. Über die Ludolph'sche Zahl. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, **2**:679–682, 1882.

[Wal88] M. Waldschmidt. On the transcendence methods of Gelfond and Scheiner in several variables. In Alan Baker, editor, *New advances in transcendence theory Proceedings of the Symposium on Transcendental Number Theory held at the University of Durham*, pages 375–398. Cambridge University Press, Cambridge, 1988.

[Wei85] Karl Weierstrass. Zu Hrn. Lindemann's Abhandlung "Über die Ludolph'sche Zahl". *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, **2**:1067–1086, 1885.

[Wil02] Scott W. Williams. Million-Buck Problems. *The Mathematical Intelligencer*, **24**(3):17–20, September 2002. ISSN 0343-6993. doi:10.1007/BF03024727.

[Zil97] Boris Zilber. Generalized analytic sets. *Algebra and Logic*, **36**(4):226–235, July 1997. ISSN 0002-5232. doi:10.1007/s10469-997-0064-5.

[Zil03] —. Model theory, geometry and arithmetic of the universal cover of a semi-abelian variety. *Model theory and applications*, **11**(C):427–458, 2003.

[Zil05a] —. A categoricity theorem for quasi-minimal excellent classes. In Andreas Blass and Yi Zhang, editors, *Logic and Its Applications*, Contemporary Mathematics, pages 297–306. American Mathematical Society, Providence, Rhode Island, 2005.

[Zil05b] —. Pseudo-exponentiation on algebraically closed fields of characteristic zero. *Annals of Pure and Applied Logic*, **132**(1):67–95, 2005. ISSN 01680072. doi:10.1016/j.apal.2004.07.001.

[Zil06] —. Covers of the Multiplicative Group of an Algebraically Closed Field of Characteristic Zero. *Journal of the London Mathematical Society*, **74**(01):41, 2006. ISSN 0024-6107. doi:10.1112/S0024610706023349.