THE REAL FIELD WITH THE RATIONAL POINTS OF AN ELLIPTIC CURVE

AYHAN GÜNAYDIN AND PHILIPP HIERONYMI

Abstract. We consider the expansion of the real field by a the group of rational points of an elliptic curve over the rational numbers. We prove a completeness result, followed by a quantifier elimination result. Moreover we show that open sets definable in that structure are semi-algebraic.

1. Introduction

Here we study the expansion of the real field by the set, $\mathcal{C}$, of pairs $(x, y) \in \mathbb{Q}^2$ such that

$$y^2 = x^3 + ax + b,$$

with $a, b \in \mathbb{Q}$ such that $4a^3 + 27b^2 \neq 0$.

We consider $\big(\mathbb{R}, \mathcal{C}\big)$ as a structure in the language $\mathcal{L}_{\mathrm{o}}(P)$ extending the language $\mathcal{L}_{\mathrm{o}} = \{0, 1, +, \cdot, <\}$ of ordered rings by a binary relation symbol P. Our main result is the following.

Theorem 1.1. *Every subset of $\mathbb{R}^s$ definable in the structure $(\mathbb{R}, \mathcal{C})$ is defined by a boolean combination of formulas of the form*

$$\exists y_1 \cdots \exists y_{2n} \big[\bigwedge_{j=0}^{n-1} P(y_{2j+1}, y_{2j+2}) \wedge \phi(x, y) \big],$$

where y denotes the tuple $(y_1, \ldots, y_{2n})$, x is an s-tuple of distinct variables and $\phi(x, y)$ is a quantifier-free $\mathcal{L}_{\mathrm{o}}$-formula.

As a by-product of our techniques, we also axiomatize the first order theory of $(\mathbb{R}, \mathcal{C})$ (see Theorem 4.3).

One of our motivations for studying $(\mathbb{R}, \mathcal{C})$ is to understand the definable open sets in the sense of [3]. In the last section we prove the following.

Theorem 1.2. *Let $U \subseteq \mathbb{R}^s$ be an open set definable in $(\mathbb{R}, \mathcal{C})$. Then U is semialgebraic.*

Date: October 22, 2009.

2000 *Mathematics Subject Classification.* 03C10, 03C64, 14H52, 11U09.

The second author was funded by Deutscher Akademischer Austausch Dienst.

We prove Theorem 1.1 and Theorem 1.2 for a broader class of structures than the ones in the statements. Namely we study $(\mathbb{R}, \Gamma)$, where $\Gamma \subseteq \mathbb{R}^m$ is a dense subgroup of a group definable in $\mathbb{R}$ of dimension one, satisfying a number theoretic property. The details of the setting can be found in Section 2. In Section 3, it will be shown that the conclusion of Theorem 1.1 holds in these structures. The reader would notice that $\mathcal{C}$, considered as a subset of the projective plane $\mathbb{P}^2(\mathbb{C})$, becomes the group of rational points of an elliptic curve after adding a point at infinity. We explain this thoroughly in Section 4 and using this we illustrate how the structure $(\mathbb{R}, \mathcal{C})$ fits into the more general framework.

The current paper is not the first attempt to treat such structures. For instance, Zilber studied the real field expanded by the group of roots of unity in [13] and later Belegradek and Zilber generalized the results of that paper to the real field expanded by a subgroup of the unit circle of finite rank in [1]. The first author of the current paper studied similar structures in [6] with an approach different than the one in [1]. However neither [1] nor [6] prove anything about the structure of open definable sets. Since we prove our theorems in the generality of Section 2, we were able to get some results in that direction: Let

$$\mathbb{S} := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

be the circle group and let Γ be a finite rank subgroup of $\mathbb{S}$; that is Γ is contained in the divisible closure (in $\mathbb{S}$) of a finitely generated subgroup of $\mathbb{S}$. Now the statement analogous to Theorem 1.2 in this setting is as follows.

Theorem 1.3. *Let $U \subseteq \mathbb{R}^s$ be an open set definable in $(\mathbb{R}, \Gamma)$. Then U is semialgebraic.*

Conventions and notations. Above and in the rest of the paper m, n, s, t always denote natural numbers. Also as usual 'definable' means 'definable with parameters' and when we want to make the language and the parameters explicit we write *$\mathcal{L}$-B-definable* to mean definable in the appropriate $\mathcal{L}$-structure using parameters from the set B.

The real closure of an ordered field K is denoted by K^{rc}.

We denote the graph of a function $f : X \to Y$ by $\mathrm{gr}(f)$.

Acknowledgements. We thank L. van den Dries, C. Ealy, C. Miller, J. Ramakrishnan, S. Starchenko and B. Zilber for useful discussions on the topic. We also thank The Fields Institute for hospitality during the 'Thematic Program on O-minimal Structures and Real Analytic Geometry'; most of this paper was written during that period.

2. The Mordell-Lang property

Throughout this section K denotes a real closed field and $(\mathbb{A}, \oplus)$ is a one-dimensional group definable in K; that is $\mathbb{A} \subseteq K^m$ and $\oplus : K^m \times K^m \to K^m$

are definable in K such that $\mathbb{A}$ is of dimension one and $\oplus|(\mathbb{A}\times\mathbb{A})$ is a group operation on $\mathbb{A}$. (Here and below we do not make any distinction between an ordered field and its underlying set.)

By Proposition 2.5 of [10], we know that $\mathbb{A}$ becomes a topological group, moreover that a subset of $\mathbb{A}$ is dense in $\mathbb{A}$ in that topology if and only if it is dense in the topology induced from K^m (this last part is not necessarily correct for bigger dimensions). In [10], it is also proven that $\mathbb{A}$ must be abelian.

Let $\pi_1,\dots,\pi_m$ be the standard projections of K^m onto K. Since $\mathbb{A}$ is of dimension one, there is $i\in\{1,\dots,m\}$ such that for every $a\in\mathbb{A}$ and $j=1,\dots,m$ we have that $\pi_j(a)$ is definable over $\pi_i(a)$. For our purposes it is harmless to assume that $i=1$ and we sometimes write π instead of π_1.

For convenience we assume that $\mathbb{A}$ is definable over $\emptyset$ and for another real closed field E, we let $(\mathbb{A}(E),\oplus)$ denote the group definable in E by the formulas defining $(\mathbb{A},\oplus)$ in K.

Let $k=(k_1,\dots,k_n)$ be a tuple of integers. Consider the group character

$$\chi_k:\mathbb{A}^n\to\mathbb{A},\quad \chi_k(a_1,\dots,a_n):=k_1a_1\oplus\cdots\oplus k_na_n.$$

and let T_k denote the kernel of χ_k.

Fix $n>0$ and a tuple of distinct indeterminates $X=(X_1,\dots,X_{mn})$. In what follows we identify K^{mn} with $(K^m)^n$. In particular, for $\alpha_1,\dots,\alpha_n\in K^m$ and a polynomial $p(X)\in K[X]$, $p(\alpha_1,\dots,\alpha_n)$ means

$$p\big(\pi_1(\alpha_1),\pi_2(\alpha_1),\dots,\pi_m(\alpha_1),\dots,\pi_1(\alpha_n),\dots,\pi_m(\alpha_n)\big).$$

In a similar fashion, for a subfield L of K and a subset S of $\mathbb{A}$, $L(S)$ denotes the subfield $L\big(\pi_1(S)\cup\cdots\cup\pi_m(S)\big)$ of K and $L[S]:=L\big[\pi_1(S)\cup\cdots\cup\pi_m(S)\big]$.

Finally for a polynomial $p(X)$ as above we put

$$V(p):=\{\alpha\in K^{mn}:p(\alpha)=0\},$$

the *zero set of* $p(X)$ (in K).

In the rest of this section let L be a subfield of K and G a subgroup of $\mathbb{A}$.

Definition 2.1. We say that G has the *Mordell-Lang property over L* if for every polynomial $p(X)\in L[X]$, there are $g_1,\dots,g_t\in G^n$ and $k_1,\dots,k_t\in\mathbb{Z}^n$ such that

$$V(p)\cap G^n=\bigcup_{i=1}^{t}g_i\oplus(T_{k_i}\cap G^n).$$

The reason for calling this property with this name is that it is the conclusion of a conjecture of Lang generalizing a conjecture of Mordell for abelian varieties. We refer the reader to [9] for the precise statement of the conjecture and its history.

We proceed to show that if G has the Mordell-Lang property over $\mathbb{Q}$, then it has the Mordell-Lang property over K.

Lemma 2.2. *Let L contain $\mathbb{Q}(G)$ and suppose that G has the Mordell-Lang property over L. Then G has the Mordell-Lang property over L^{rc}.*

Proof. Let $\alpha \in K$ be algebraic over L of degree $d > 1$. It suffices to show that G has the Mordell-Lang property over $L(\alpha)$. Take a polynomial $p(X) \in L[\alpha][X]$. Write

$$p(X) = p_0(X) + p_1(X)\alpha + \cdots + p_{d-1}(X)\alpha^{d-1},$$

where $p_i(X) \in L[X]$ for $i = 0, 1, \ldots, d-1$. Then for $g = (g_1, \ldots, g_n) \in G^n$

$$p(g) = 0 \iff p_i(g) = 0 \text{ for each } i \in \{0, 1, \ldots, d-1\}.$$

Therefore

$$V(p) \cap G^n = \bigcap_{i=0}^{d-1} V(p_i) \cap G^n = V(p_1^2 + \cdots + p_{d-1}^2) \cap G^n.$$

By the Mordell-Lang property over L, we know that $V(p_1^2 + \cdots + p_{d-1}^2) \cap G^n$ is a finite union of cosets of kernels of χ_k in G^n, thus so is $V(p) \cap G^n$. □

We need the following notation in the next step: For $s \in \mathbb{N}$ and a tuple $i = \big(i(1), \ldots, i(s)\big) \in \mathbb{N}^s$, $|i|$ denotes $i(1) + \cdots + i(s)$, and for a tuple $Y = (Y_1, \ldots, Y_s)$ of distinct indeterminates, Y^i is the monomial

$$Y_1^{i(1)} Y_2^{i(2)} \cdots Y_s^{i(s)}.$$

Likewise for $\alpha = (\alpha_1, \ldots, \alpha_s) \in K^s$, α^i means $\alpha_1^{i(1)} \alpha_2^{i(2)} \cdots \alpha_s^{i(s)}$.

Lemma 2.3. *Let G have the Mordell-Lang property over $\mathbb{Q}$. Then G has the Mordell-Lang property over $\mathbb{Q}(G)$.*

Proof. Take a polynomial $p(X) \in \mathbb{Q}[G][X]$ of degree d. Write

$$p(X) = \sum_{|i| \leq d} \sum_{j} a_{i,j}\, g^j X^i,$$

where i and j run through elements of $\mathbb{N}^{mn}$ and $\mathbb{N}^{mt}$ respectively, $a_{i,j} \in \mathbb{Q}$, and $g = (g_1, \ldots, g_t) \in G^t$.

Let $Y = (Y_1, \ldots, Y_{mt})$ be a tuple of indeterminates different than X and put $q(X, Y) = \sum_{|i| \leq d} \sum_j a_{i,j}\, X^i Y^j \in \mathbb{Q}[X, Y]$. For $g^* \in G^n$ we have

$$p(g^*) = 0 \iff q(g^*, g) = 0.$$

Now the result follows since G has the Mordell-Lang property over $\mathbb{Q}$. □

Proposition 2.4. *Let G have the Mordell-Lang property over $\mathbb{Q}$. Then G has the Mordell-Lang property over K.*

Proof. Let $E \subseteq K$ be a finitely generated extension of $\mathbb{Q}(G)^{\mathrm{rc}}$, and take a transcendence basis $\alpha = (\alpha_1, \ldots, \alpha_t)$ of E over $\mathbb{Q}(G)^{\mathrm{rc}}$.

Take a polynomial $p(X) \in E[X]$, and write

$$p(X) = \sum_i p_i(X) \alpha^i,$$

where $i = \big(i(1), \ldots, i(t)\big)$ runs through elements of $\mathbb{N}^t$ such that $|i| \leq s$ for some $s \in \mathbb{N}$ and $p_i(X) \in \mathbb{Q}(G)^{\mathrm{rc}}[X]$.

Now it is easy to see that for $g \in G^n$

$$p(g) = 0 \Longleftrightarrow p_i(g) = 0 \text{ for each } i.$$

Hence $V(p) \cap G^n$ is of the desired form since G has the Mordell-Lang property over $\mathbb{Q}(G)^{\mathrm{rc}}$ by the previous two lemmas. □

From now on we assume that G has the Mordell-Lang property over $\mathbb{Q}$. As a consequence of the proposition above it is harmless to simply say that G has the Mordell-Lang property.

2.1. **The main lemma.** We prove an analog of Lemma 5.12 in [4], which is the most useful consequence of the Mordell-Lang property. We take this opportunity to introduce some more algebraic notations and conventions.

Let G' be a subgroup of $\mathbb{A}$ containing G and $g^*, g_1^*, \ldots, g_n^*$ elements of G'. We say that g^* is *algebraic over L* if $\pi(g^*)$ is algebraic over L, and similarly $g_1^*, \ldots, g_n^*$ are *algebraically dependent over L* if $\pi(g_1^*), \ldots, \pi(g_n^*)$ are algebraically dependent over L. Also we say that $g_1^*, \ldots, g_n^*$ are *linearly dependent over G* if there is $k \in \mathbb{Z}^n \setminus \{(0, \ldots, 0)\}$ such that $\chi_k(g_1^*, \ldots, g_n^*) \in G$.

We say that G' *satisfies the same Mordell-Lang conditions as G* if for every polynomial $p \in \mathbb{Q}[X]$

$$V(p) \cap (G')^n = g_1 \oplus (T_{k_1} \cap (G')^n) \cup \cdots \cup g_t \oplus (T_{k_t} \cap (G')^n),$$

with $g_1, \ldots, g_t \in G^n$ and $k_1, \ldots, k_t \in \mathbb{Z}^n$.

Note that if G' satisfies the same Mordell-Lang conditions as G, then G' has the Mordell-Lang property as well.

Lemma 2.5. *Let G' be a subgroup of $\mathbb{A}$ containing G and $g^*, g_1^*, \ldots, g_n^* \in G'$. Suppose that G' satisfies the same Mordell-Lang conditions as G. Then we have:*
(1) *If g^* is algebraic over $\mathbb{Q}(G)$, then $dg^* \in G$ for some $d \geq 1$.*
(2) *If $g_1^*, \ldots g_n^*$ are algebraically dependent over $\mathbb{Q}(G)$, then they are linearly dependent over G.*

Proof. We just prove (1), and (2) can be proven using similar arguments. Let $X = (X_1, \ldots, X_m)$ and $Y = (Y_1, \ldots, Y_{mt})$ be tuples of distinct indeterminates, and take a polynomial $P(X, Y) \in \mathbb{Q}[X, Y]$ and $h \in G^t$ such that $p(g^*, h) = 0$ and $p(X, h)$ is not the zero polynomial. Then by the assumption there exist $k \in \mathbb{Z}^{t+1}$ and $h' \in G^{t+1}$ such that $(g, h) \in h' \oplus (T_k \cap (G')^{t+1})$. Note that $k_1 \neq 0$, because otherwise $p(g', h) = 0$ for every $g' \in G'$ and hence $p(X, h)$ is the zero polynomial. Now it is easy to see that $dg^* \in G$ with $d := |k_1|$. □

2.2. **Smallness revisited.** The aim of this subsection is to prove Corollary 2.10 below, which is used in Section 3 in a very essential way. That result is a consequence of an abstract condition called *smallness*, which in turn is satisfied by the groups with the Mordell-Lang property (see Lemma 2.9 below).

Here we define smallness only in the setting of fields, in contrary to [4] where it is defined in a more general model theoretic setting. First we recall some notations: For a positive integer l, an *l-valued map*, denoted as $f : X \xrightarrow{l} Y$, is a map from X to $\mathcal{P}(Y)$ such that $|f(x)| \leq l$ for every $x \in X$; and such a map is *definable* in a given structure $\mathcal{M}$ if its *graph*

$$\{(x, y) \in X \times Y : y \in f(x)\}$$

is definable in $\mathcal{M}$. For $A \subseteq X$, we let $f(A) := \bigcup_{a\in A} f(a)$.

Definition 2.6. Let E be a field. A subset X of E^s is called *large* if there is an l-valued map $f : E^{sn} \xrightarrow{l} E$ definable in the field E such that $f(X^n) = E$; otherwise we say that X is *small*.

Note that smallness is an elementary property of the pair (E, X) construed as a structure in the language of ordered rings expanded by an s-ary relation symbol. It is also easy to see that if E is an ordered field, then a set $X \subseteq E^s$ is large if and only if there is a usual function $g : E^{sn'} \to E$ definable in E such that $g(X^{n'}) = E$ (This is still true if E is an algebraically closed field, but requires more work).

Remark. Let E be an algebraically closed field and F a subfield. By using results from [8] we get that F is large in E if and only if either $F = E$ or F is a real closed field such that $F(\sqrt{-1}) = E$.

We first mention a result that has been neglected in [2]. It must be known by many people, but we could not find a reference for it anywhere. So we include a proof as well.

Lemma 2.7. *Suppose that E is a real closed field. Let $f : E^s \to E$ be definable in the field E, and let C be the algebraic closure, $E(\sqrt{-1})$, of E. Then there is an l-valued function $\tilde{f} : C^s \xrightarrow{l} C$ definable in the field C such that $f(\alpha) \in \tilde{f}(\alpha)$ for each $\alpha \in E^s$.*

Proof. [1] Let $X \subseteq E^{s+1}$ be the graph of f . Write X as $\bigcup_{i=1}^{t} U_i \cap Z_i$ where each U_i is a nonempty open subset of E^{s+1} defined by polynomial inequalities and each Z_i is an intersection of zero sets in E^{s+1} of polynomials. Being the graph of a function, X contains no open set. This means that none of the Z_i's is all of E^{s+1}.

Let $\tilde{Z}_i \subseteq C^{s+1}$ be the zero set (in C^{s+1}) of the polynomials defining Z_i. Note that $\tilde{Z}_i \cap E^{s+1} = Z_i$.

[1] We thank C. Ealy for helping with this proof

There is a definable subset V_i of C^s of dimension less than s such that for every $\alpha \in C^s \setminus V_i$, the fiber $\tilde{Z_i}(\alpha)$ is a finite set. Indeed if there were a definable subset of C^s of dimension s with 1-dimensional fibers of Z_i above it, then $\tilde{Z_i}$ would be of dimension $s+1$, and this could only happen if $\tilde{Z_i}$ were all of C^{s+1}. Moreover for $i = 1, \ldots, t$ there is $N_i \in \mathbb{N}$ such that $|\tilde{Z_i}(\alpha)| \leq N_i$ for every $\alpha \in C^s \setminus V_i$. Let $D_i \subseteq E$ be the projection of $U_i \cap Z_i$ to the first s coordinates. We claim that D_i is contained in $C^s \setminus V_i$. Suppose not and take $\alpha \in V_i \cap D_i$. As $\alpha \in D_i$, we have $(U_i \cap Z_i)(\alpha)$ is a singleton, namely $\{f(\alpha)\}$. On the other hand, since $\alpha \in V_i$, $\tilde{Z_i}(\alpha)$ is an infinite subset, and in particular, an infinite subset of $\{\alpha\} \times C \subseteq C^{s+1}$ that is definable in the field C. Since C is an algebraically closed field, $\tilde{Z_i}(\alpha)$ is a cofinite subset of $\{\alpha\} \times C$. But that would mean that $(U_i \cap \tilde{Z_i})(\alpha) = (U_i \cap Z_i)(\alpha)$ would be an infinite set, providing the contradiction that proves the claim.

Now define $\tilde{f}$ as follows: For $\alpha \in C^s \setminus V_i$, let $\tilde{f_i}(\alpha) = Z_i(\alpha)$. Then put $\tilde{f} := \bigcup_{i=1}^{t} \tilde{f_i}$. Note that on D_i , $\tilde{f_i}(x)$ contains $f(x)$. The union of the D_i's is C^s, so the lemma follows. □

We immediately get the following consequence.

Corollary 2.8. *Let E be a real closed field and let $X \subseteq E^s$ be small in the algebraically closed field $E(\sqrt{-1})$. Then X is small in E.*

Remember that in the beginning of this section we fixed K to be a real closed field and G a subgroup of a one dimensional group definable in K with the Mordell-Lang property. In that setting we get the following.

Lemma 2.9. *The group G is small in K.*

Proof. Take a proper elementary extension (K^*, G^*) of (K, G). It suffices to show that G^* is small in K^*. By the previous corollary and the remark preceding Lemma 2.9, it is enough to prove that $\mathbb{Q}(G^*, \sqrt{-1}) \neq K^*(\sqrt{-1})$. Hence we need to show that $\mathbb{Q}(G^*) \neq K^*$.

Take a subset B of G^* that is linearly independent over G and is maximal with respect to this property. Clearly $B \neq \emptyset$. By Lemma 2.5 we have that B is algebraically independent over $\mathbb{Q}(G)$, and hence $\mathbb{Q}(G, B)$ is a purely transcendental extension of $\mathbb{Q}(G)$. Then $\mathbb{Q}(G^*)$ cannot be real closed, as for every $g^* \in G^*$, there is a positive integer d such that $dg^* \in \mathbb{Q}(G, B)$. Hence $\mathbb{Q}(G^*) \neq K^*$. □

A consequence of smallness is the following.

Corollary 2.10. *Let $f : K^{mn} \to K$ be definable in the field K. Then $K \setminus f(G^n)$ is dense in K.*

Proof. Assume that a nonempty interval I of K is contained in $f(G^n)$. Take a function $g : K \to K$ definable in the ordered field K that maps I onto K. Now $(g \circ f)(G^n) = K$ contradicting the smallness of G. □

3. Model theory

Let $\mathbb{A}(\mathbb{R}) \subseteq \mathbb{R}^m$ be a one dimensional group definable in the real field $\mathbb{R}$ over $\emptyset$, and fix a subgroup Γ of $\mathbb{A}(\mathbb{R})$ with the Mordell-Lang property such that $|\Gamma/n\Gamma|$ is finite for every $n > 0$. Also $\mathbb{A}(\mathbb{R})$ becomes a real Lie group of dimension one. Hence it has finitely many n-torsion elements for each $n > 0$.

Let $\mathcal{L}_{\mathrm{o}}(P)$ be the language $\mathcal{L}_{\mathrm{o}}$ of ordered rings expanded by an m-ary relation symbol P (note that $m = 2$ in the introduction). Also let $\mathcal{L}_{\mathrm{o}}(\Gamma)$ be the language $\mathcal{L}_{\mathrm{o}}$ augmented by constant symbols $\pi(\gamma)$ for each $\gamma \in \Gamma$ and let $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$ the language $\mathcal{L}_{\mathrm{o}}(\Gamma)$ extended by P. For simplicity of notation we denote $\mathcal{L}_{\mathrm{o}}(\Gamma)$-structures by $\big(K,(\gamma)_{\gamma\in\Gamma}\big)$, rather than $\big(K,(\pi(\gamma))_{\gamma\in\Gamma}\big)$; similarly $\big(K,G,(\gamma)_{\gamma\in\Gamma}\big)$ are $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-structures.

3.1. **The theory.** Let T be $\mathcal{L}_{\mathrm{o}}(\Gamma)$-theory of $\big(\mathbb{R},(\gamma)_{\gamma\in\Gamma}\big)$ and let $T(\Gamma)$ be the $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-theory extending T whose models are of the form $\big(K,G,(\gamma)_{\gamma\in\Gamma}\big)$ satisfying the following:

(1) G is a dense subgroup of $\mathbb{A}(K)$,
(2) for every $n > 0$ and $g \in G$, if $ng \in \Gamma$, then $g \in \Gamma$,
(3) for every $n > 0$, $|G/nG| = |\Gamma/n\Gamma|$,
(4) G satisfies the same Mordell-Lang conditions as Γ (see page 5).

It is easy to see that the first three conditions are first order in the language $\mathcal{L}(P;\Gamma)$; for the last one we fix $\gamma_1,\dots,\gamma_t \in \Gamma^n$ and $k_1,\dots,k_t \in \mathbb{Z}^n$ for a given polynomial $p(X) \in \mathbb{Q}[X]$ such that that

$$V(p)\cap\Gamma^n = \bigcup_{i=1}^{t} \gamma_i \oplus (T_{k_i}\cap\Gamma^n),$$

and consider the formula

$$\forall x_1\cdots\forall x_{mn} \bigwedge_{j=0}^{n-1} P(x_{jm+1},\dots,x_{jm+m}) \to \big[p(x_1,\dots,x_{mn})=0$$
$$\leftrightarrow \bigvee_{i=1}^{t} \chi_{k_i}\big((x_1,\dots,x_m),\dots,(x_{mn-m+1},\dots,x_{mn})\big) = \chi_{k_i}(\gamma_i)\big].$$

Note that if Γ is dense in $\mathbb{A}(\mathbb{R})$, then $(\mathbb{R},\Gamma)$ is a model of $T(\Gamma)$. We are proceeding to show that $T(\Gamma)$ is complete in that case. We achieve that by constructing a back-and-forth system between models of $T(\Gamma)$. The same back-and-forth system gives that $T(\Gamma)$ has quantifier elimination up to formulas of the form

$$\exists y_1\cdots\exists y_{mn}\big(\bigwedge_{j=0}^{n-1} P(y_{mj+1},\dots,y_{mj+m}) \wedge \phi(x,y_1,\dots,y_{mn})\big)$$

where x is a tuple of distinct variables and ϕ is a formula in the language $\mathcal{L}_{\mathrm{o}}(\Gamma)$.

In the rest of this section $\big(K, G, (\gamma)_{\gamma\in\Gamma}\big)$ ranges over models of $T(\Gamma)$, and we denote them simply by (K, G).

For $k = (k_1, \ldots, k_n) \in \mathbb{Z}^n$ and $e \in \mathbb{N}$, define

$$D_{k,e} := \chi_k^{-1}\big(eG\big) \cap G^n.$$

Note that $D_{k,e}$ is a subset of G^n definable in $\mathcal{L}_{\mathrm{o}}(P)$ and that $(eG)^n \subseteq D_{k,e}$. Hence we have that $D_{k,e}$ is of finite index in G^n as eG is of finite index in G. Thus both $D_{k,e}$ and $G^n \setminus D_{k,e}$ are finite unions of cosets (in G^n) of $(eG)^n$. Using the fact that $eG \cap e'G = \mathrm{lcm}(e, e')G$ for $e, e' \in \mathbb{N}$, we get the following consequence.

Lemma 3.1. *Let $n > 0$, $k_1, \ldots, k_s \in \mathbb{Z}^n$ and $e_1, \ldots, e_t \in \mathbb{N}$. Then every boolean combination (in G^n) of cosets of D_{k_i,e_j} in G^n with $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, t\}$ is a finite union of cosets of $(lG)^n$, where l is the lowest common multiple of $e_1, \ldots, e_t$.*

Remark. Note that l in the lemma depends only on $e_1, \ldots, e_t$ and not on G or $k_1, \ldots, k_s$.

Note that since G is dense in $\mathbb{A}(K)$ and multiplication by n is a continuous bijection on $A(K)$, we have that nG is dense in G and also that $D_{k,e}$ is dense in G^n for every $k \in \mathbb{Z}^n$ and $e \in \mathbb{N}$.

Recall that a subgroup H of G is called *pure* if $h \in nG$ implies $h \in nH$ for every $h \in H$ and $n > 0$. For a pure subgroup H of G and a subset A of G, let $H_G\langle A\rangle$ be the set of $g \in G$ such that ng is in the subgroup of G generated by H and A for some $n > 0$; that is there are $h \in H$, $a_1, \ldots, a_t \in A$, and $k_1, \ldots, k_t \in \mathbb{Z}$, such that $ng = h \oplus k_1a_1 \oplus \cdots \oplus k_ta_t$. When the ambient group G is clear from the context, we omit G from the notation. Note that $H_G\langle A\rangle$ is the smallest pure subgroup of G containing both H and A.

We mention some lemmas that will be useful in the rest of the section.

Lemma 3.2. *Let H be a pure subgroup of G containing Γ and let $g \in G$. Then*

$$\big(\mathbb{Q}(H, g)^{\mathrm{rc}}\big)^m \cap G = H_G\langle g\rangle.$$

Proof. It is easy to see that $H_G\langle g\rangle \subseteq \big(\mathbb{Q}(H, g)^{\mathrm{rc}}\big)^m \cap G$ since all the torsion elements of G are algebraic over $\mathbb{Q}$. Now take $g' \in (\mathbb{Q}(H, g)^{\mathrm{rc}})^m \cap G$. Since G satisfies the same Mordell-Lang conditions as H, we can apply Lemma 2.5 to get that g and g' are linearly dependent over H. Thus $g' \in H_G\langle g\rangle$. □

We can strengthen this lemma as follows.

Lemma 3.3. *Let H, g be as in the previous lemma and let A be a subset of K algebraically independent over $\pi(G)$. Then*

$$\big(\mathbb{Q}(A,H,g)^{\mathrm{rc}}\big)^m \cap G = H_G\langle g\rangle.$$

Proof. By the previous lemma, all we need to show is

$$\big(\mathbb{Q}(A,H,g)^{\mathrm{rc}}\big)^m \cap G \subseteq \big(\mathbb{Q}(H,g)^{\mathrm{rc}}\big)^m \cap G. \tag{3.1}$$

Let $g' \in \big(\mathbb{Q}(A,H,g)^{\mathrm{rc}}\big)^m \cap G$. So $\pi(g') \in \mathbb{Q}(A,g,H)^{\mathrm{rc}}$. Let A' be a minimal subset of A such that $\pi(g') \in \mathbb{Q}(A',g,H)^{\mathrm{rc}}$. For a contradiction, suppose that A' is nonempty and let $a \in A'$. By minimality of A', we have that $g' \notin (\mathbb{Q}(A'\setminus\{a\},H,g)^{\mathrm{rc}})^m$. But then the Steinitz Exchange Principle implies that $a \in \mathbb{Q}(A' \setminus \{a\}, H, g, g')^{\mathrm{rc}}$. Since $g, g' \in G$, we get that

$$a \in \mathbb{Q}(A' \setminus \{a\}, G)^{\mathrm{rc}}.$$

This contradicts with the assumption that A is algebraically independent over $\pi(G)$. Hence A' is empty and $g' \in \big(\mathbb{Q}(H,g)^{\mathrm{rc}}\big)^m \cap G$. □

Corollary 3.4. *Let $g \in G$. If g is $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$\emptyset$-definable, then $g \in \Gamma$.*

Proof. Using Lemma 3.2, we have $\langle\Gamma\rangle := \Gamma_G\langle 0\rangle = \big(\mathbb{Q}(\Gamma)^{\mathrm{rc}}\big)^m \cap G$. But $\langle\Gamma\rangle = \Gamma$ by axiom (2). □

Lemma 3.5. *Suppose that (K,G) is $|\Gamma|^+$-saturated. Let $S \subseteq K^m$ be an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$\emptyset$-definable set and D a dense subset of G. Then $\pi\big((D \setminus \Gamma) \cap S\big)$ is dense in the interior of $\pi(\mathbb{A}(K) \cap S)$.*

Proof. By cell decomposition for o-minimal structures, $\mathbb{A}(K) \cap S$ is a union of 1-dimensional cells $C_1, \ldots, C_n$ and finitely many points. We can reduce to the case that every cell C_i is open in $\mathbb{A}(K)$. We now show that if any of these finitely many points is in D, then it is in Γ. So suppose $g \in D$ is one of these points. This implies that g is $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$\emptyset$-definable, since $\mathbb{A}(K) \cap S$ is. Then $g \in \Gamma$ by Corollary 3.4. Since (K,G) is $|\Gamma|^+$-saturated and D is dense in G, we have that $D \setminus \Gamma$ is dense in $\bigcup_{i=1}^n C_i$. Hence $\pi((D \setminus \Gamma) \cap S)$ is dense in the interior of $\pi(\mathbb{A}(K) \cap S)$. □

3.2. **Back-and-forth and completeness.** Fix two $|\Gamma|^+$-saturated models (K,G) and (K',G') of $T(\Gamma)$, and let $\mathcal{S}$ be the collection of $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-isomorphisms

$$\beta : \big(\mathbb{Q}(A,H)^{\mathrm{rc}}, H\big) \to \big(\mathbb{Q}(A',H')^{\mathrm{rc}}, H'\big)$$

where H and H' are pure subgroups of cardinality at most $|\Gamma|$ of G and G' containing Γ and A and A' are finite subsets of K and K' that are algebraically independent over $\mathbb{Q}(G)$ and $\mathbb{Q}(G')$ respectively and $\beta(A) = A'$.

Note that by Lemma 3.3, $(\mathbb{Q}(A,H)^{\mathrm{rc}}, H)$ and $(\mathbb{Q}(A',H')^{\mathrm{rc}}, H')$ as above become $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-substructures of (K,G) and (K',G') respectively. Moreover the map β is a partial elementary map between the ordered fields K and K' (in the language $\mathcal{L}_{\mathrm{o}}$).

Lemma 3.6. *The collection $\mathcal{S}$ is a back-and-forth-system.*

Proof. Let $\beta : (\mathbb{Q}(A,H)^{\mathrm{rc}}, H) \to (\mathbb{Q}(A',H')^{\mathrm{rc}}, H')$ be in $\mathcal{S}$ and take $a \in K \setminus \mathbb{Q}(A,H)^{\mathrm{rc}}$. By symmetry it is enough to prove that there is $\tilde{\beta} \in \mathcal{S}$ such that $\tilde{\beta}$ extends β and $a \in \mathrm{dom}(\tilde{\beta})$.

Case 1: $a \in \pi(G)$.
Take $b \in K^{m-1}$ such that $(a,b) \in G$. Since $G \subseteq \mathbb{A}(K)$ and $\mathbb{A}(K)$ is $\mathcal{L}_{\mathrm{o}}$-$\emptyset$-definable of dimension 1, there is $\mathcal{L}_{\mathrm{o}}$-$\emptyset$-definable function $f : K \to K^{m-1}$ such that $b = f(a)$. Let $q(x,y)$ be the $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-type consisting of the $\mathcal{L}_{\mathrm{o}}$-type of (a,b) over $\mathbb{Q}(A,H)^{\mathrm{rc}}$ and for every $l \in \mathbb{Z}$, $h \in H$ and $s > 0$ one of the formulas

$$l(x,y) \oplus h \in sG, \tag{3.2}$$

$$l(x,y) \oplus h \notin sG, \tag{3.3}$$

depending on whether it holds true in K that $l(a,b) \oplus h \in sG$ or not. Further let $q'(x,y)$ be the type over $\mathbb{Q}(A',H')^{\mathrm{rc}}$ corresponding to $q(x,y)$ via β. We want to find an $a' \in K'$ such that $(a', f(a'))$ realizes $q'(x,y)$. By compactness and saturation of (K',G'), it is enough to show that every finite subset of $q'(x,y)$ can be realized in (K',G'). By o-minimality of T, this reduces to find $a' \in K'$ for every $c,d \in \mathbb{Q}(A,H)^{\mathrm{rc}}$ with $c < a < d$ and finite collection of formulas $\phi_1, \ldots, \phi_n$ of the form (3.2) or (3.3) with $(K,G) \models \bigwedge_{i=1}^{n} \phi_i(a,b)$ such that

$$(K',G') \models \beta(c) < a' < \beta(d) \wedge \bigwedge_{i=1}^{n} \phi_i(a', f(a')). \tag{3.4}$$

By Lemma 3.1, the set

$$Y := \{g \in G' \ : \ (K',G') \models \bigwedge_{i=1}^{n} \phi_i(g)\}$$

is a finite union of cosets of tG' in G' for some $t \in \mathbb{N}$. Since tG' is dense in G', we have that Y is dense in G' as well. By Lemma 3.5, the set $\pi\big((Y \setminus \Gamma) \cap \mathrm{gr}(f)\big)$ is dense in the interior of $\pi(\mathbb{A}(K') \cap \mathrm{gr}(f))$. As β is a partial $\mathcal{L}_{\mathrm{o}}$-elementary map, $\pi(\mathbb{A}(K) \cap \mathrm{gr}(f))$ is $\mathcal{L}_{\mathrm{o}}(\Gamma)$-definable and a is in it, we can assume that the interval (c,d) is a subset of $\pi(\mathbb{A}(K) \cap \mathrm{gr}(f))$. Hence it follows that the interval $\big(\beta(c), \beta(d)\big)$ is a subset of $\pi(\mathbb{A}(K') \cap \mathrm{gr}(f))$ and that $\pi((Y \setminus \Gamma) \cap \mathrm{gr}(f)) \cap \big(\beta(c), \beta(d)\big)$ is a dense subset of $\big(\beta(c), \beta(d)\big)$. Now take any $a' \in \pi\big((Y \setminus \Gamma) \cap \mathrm{gr}(f)\big) \cap \big(\beta(c), \beta(d)\big)$. This a' satisfies (3.4). It is clear that $H_G\langle (a,b) \rangle$ and $H'_{G'}\langle (a', f(a')) \rangle$ are pure subgroups of G and G' respectively. Let $\tilde{\beta}$ be the $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-isomorphism that extends β to $\mathbb{Q}(A,H,a)^{\mathrm{rc}}$ and maps a to a'. By conditions (3.2) and (3.3), we get for every $h \in G$ that $h \in H_G\langle (a,b) \rangle$ if and only if $\tilde{\beta}(h) \in H'_{G'}\langle (a', f(a')) \rangle$. Hence $\tilde{\beta}$ is an $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-isomorphism between $\big(\mathbb{Q}(A,H,a)^{\mathrm{rc}}, H_G\langle (a,b) \rangle\big)$ and $\big(\mathbb{Q}(A',H',a')^{\mathrm{rc}}, H'_{G'}\langle (a', f(a')) \rangle\big)$ and $\tilde{\beta} \in \mathcal{S}$.

Case 2: $a \in \mathbb{Q}(A,G)^{\mathrm{rc}}$.
Let $g_1, \ldots, g_n \in G$ such that $a \in \mathbb{Q}\big(A, \{g_1, \ldots, g_n\}\big)^{\mathrm{rc}}$. By applying the

previous case n times, we get a $\tilde{\beta} \in \mathcal{S}$ such that $g_1, \ldots, g_n \in \operatorname{dom}(\tilde{\beta})$. Since $\operatorname{dom}(\tilde{\beta})$ is a model of T, we have $a \in \operatorname{dom}(\tilde{\beta})$.

Case 3: $a \notin \mathbb{Q}(A, G)^{\mathrm{rc}}$.
Let C be the cut of a in $\mathbb{Q}(A, H)^{\mathrm{rc}}$ and let C' be the corresponding cut of C under β in $\mathbb{Q}(A', H')^{\mathrm{rc}}$. By saturation, we can assume that there are $c', d' \in K'$ such that every element in the interval (c', d') realizes the cut C'. Let $d \in K^{|A|}$ be the set A written as a tuple. Let $f_1, \ldots, f_n$ be $\emptyset$-definable functions in the language $\mathcal{L}_{\mathrm{o}}(\Gamma)$. By Corollary 2.10, we know that there exists $b' \in (c', d')$ such that for $i = 1, \ldots, n$ and every tuple $g_1', \ldots, g_t'$ of elements of G'

$$f_i(g_1', \ldots, g_t', \beta(d)) \neq b'.$$

Thus by saturation, there is an $a' \in (c', d')$ such that $a' \notin \mathbb{Q}(A', G')^{\mathrm{rc}}$. Since a' realizes the cut C', there is an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-isomorphism $\tilde{\beta}$ from $\mathbb{Q}(A, a, H)^{\mathrm{rc}}$ to $\mathbb{Q}(A', a', H')^{\mathrm{rc}}$ extending β and sending a to a'. Since $a \notin \mathbb{Q}(A, G)^{\mathrm{rc}}$ and $a' \notin \mathbb{Q}(A', G')^{\mathrm{rc}}$, we get that

$$\mathbb{Q}(A, a, H)^{\mathrm{rc}} \cap G = H \text{ and } \mathbb{Q}(A', a', H')^{\mathrm{rc}} \cap G' = H'.$$

Since $\beta(H) = H'$ and $\tilde{\beta}$ extends β, we get that $\tilde{\beta}$ is an $\mathcal{L}_{\mathrm{o}}(P; \Gamma)$-isomorphism from $(\mathbb{Q}(A, a, H)^{\mathrm{rc}}, H)$ to $(\mathbb{Q}(A', a', H')^{\mathrm{rc}}, H')$ with $\tilde{\beta}(A \cup \{a\}) = A' \cup \{a'\}$. Thus we have that $\tilde{\beta} \in \mathcal{S}$. □

Now the proof of completeness becomes an easy consequence of this lemma.

Theorem 3.7. *Let Γ be dense in $\mathbb{A}(\mathbb{R})$. Then the theory $T(\Gamma)$ is complete.*

Proof. Take $|\Gamma|^+$-saturated models (K, G) and (K', G') of $T(\Gamma)$, and let $\mathcal{S}$ be as above. It only remains to show that $\mathcal{S}$ is non-empty. But it is easy to see that the identity map on $\mathbb{Q}(\Gamma)^{\mathrm{rc}}$ belongs to $\mathcal{S}$. □

3.3. **Quantifier elimination.** Let $x = (x_1, \ldots, x_t)$ be a tuple of distinct variables. For every $\mathcal{L}_{\mathrm{o}}(P; \Gamma)$-formula $\phi(x)$ of the form

$$\exists y_1 \cdots \exists y_{mn} \bigwedge_{j=0}^{n-1} P(y_{mj+1}, \ldots, y_{mj+m}) \wedge \psi(x, y_1, \ldots, y_{mn}), \tag{3.5}$$

where $\psi(x, y)$ is an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-formula, let P_ϕ be a new relation symbol of arity t, and let $\mathcal{L}_{\mathrm{o}}(P; \Gamma)^+$ be the language $\mathcal{L}_{\mathrm{o}}(P; \Gamma)$ together with relation symbols P_ϕ (for various x).

Let $T(\Gamma)^+$ is the $\mathcal{L}_{\mathrm{o}}(P; \Gamma)^+$-theory extending the theory $T(\Gamma)$ by an axiom:

$$\forall x \big(P_\phi(x) \leftrightarrow \phi(x) \big),$$

for each ϕ of the form (3.5).

With this notation in hand we are ready to prove the promised quantifier elimination result.

Theorem 3.8. *The theory $T(\Gamma)^+$ has quantifier elimination.*

Proof. Let (K, G) and (K', G') be two $|\Gamma|^+$-saturated models of $T(\Gamma)^+$ and let $\mathcal{S}$ be the back-and-forth system between (K, G) and (K', G') constructed above. Also take $a = (a_1, \ldots, a_n) \in K^n$ and $b = (b_1, \ldots, b_n) \in (K')^n$ have the same quantifier-free $\mathcal{L}_{\mathrm{o}}(P;\Gamma)^+$-type. In order to prove quantifier elimination, we just need to find $\tilde{\beta} \in \mathcal{S}$ sending a to b. Without loss of generality, we can assume that $a_1, \ldots, a_r$ are maximally algebraically independent over $\mathbb{Q}(G)$. Since a and b have the same quantifier-free $\mathcal{L}_{\mathrm{o}}(P;\Gamma)^+$-type, we get that $b_1, \ldots, b_r$ are algebraically independent over $\mathbb{Q}(G')$. Let β be the $\mathcal{L}_{\mathrm{o}}(\Gamma)$-isomorphism between $\mathbb{Q}(a_1, \ldots, a_r)^{\mathrm{rc}}$ and $\mathbb{Q}(b_1, \ldots, b_r)^{\mathrm{rc}}$. We will now show that β extends to an isomorphism $\tilde{\beta}$ in the back-and-forth-system $\mathcal{S}$ sending a to b. Let $g_1, \ldots, g_t \in G$ be such that $a_{r+1}, \ldots, a_n$ are in $\mathbb{Q}(a_1, \ldots, a_r, g_1, \ldots, g_t)^{\mathrm{rc}}$. Let $q(x_1, \ldots, x_t)$ be the $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-type consisting of the $\mathcal{L}_{\mathrm{o}}(\Gamma)$-type of $(g_1, \ldots, g_t)$ over $\mathbb{Q}(a_1, \ldots, a_r)^{\mathrm{rc}}$ and for every $k_1, \ldots, k_t \in \mathbb{Z}$, $s \in \mathbb{N}$ and $\gamma \in \Gamma$ one of the formulas

$$\bigoplus_{i=1}^{t} k_i x_i \oplus \gamma \in sG, \text{ or} \tag{3.6}$$

$$\bigoplus_{i=1}^{t} k_i x_i \oplus \gamma \notin sG, \tag{3.7}$$

depending on whether $\bigoplus_{i=1}^{t} k_i g_i \oplus \gamma \in sG$. Let q' be type corresponding to q under β. We want to find $h_1, \ldots, h_t \in G'$ realizing q'. By compactness and saturation of (K', G'), it is enough to show that every finite subset of q' can be realized. So let $\psi(x, b_1, \ldots, b_r)$ be an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-formula in q' and $\chi_1(x, b_1, \ldots, b_r), \ldots, \chi_e(x, b_1, \ldots, b_r)$ be finitely many formulas in q' of the (3.6) and (3.7). Put $\chi = \bigwedge_{i=1}^{e} \chi_i$. By Lemma 3.1, the set

$$Y := \big\{(h_1, \ldots, h_t) \in G'^t \ : \ (K', G') \models \chi(h_1, \ldots, h_t, b_1, \ldots, b_r))\big\}$$

is a finite union of cosets of lG' in G' for some $l \in \mathbb{N}$. So the formula $\chi_i(x, b_1, \ldots, b_r)$ is equivalent to an $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-formula of the form (3.5). Hence the disjunction $\psi \wedge \chi$ is also of this form. Hence

$$\exists y_1 \cdots \exists y_t \bigwedge_{i=1}^{t} P(y_i) \wedge \psi(y_1, \ldots, y_t, b_1, \ldots, b_r) \wedge \chi(y_1, \ldots, y_t, b_1, \ldots, b_r)$$

is a quantifier-free $\mathcal{L}_{\mathrm{o}}(P;\Gamma)^+$-formula. Since $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_r)$ have the same quantifier-free $\mathcal{L}_{\mathrm{o}}(P;\Gamma)^+$-type, the formula

$$\exists y_1 \cdots \exists y_t \bigwedge_{i=1}^{t} P(y_i) \wedge \psi(y_1, \ldots, y_t, b_1, \ldots, b_r) \wedge \chi(y_1, \ldots, y_l, b_1, \ldots, b_r)$$

holds in (K', G'). So p' is finitely satisfiable. Now let $h_1, \ldots, h_t \in G'$ realize p'. Then β extends to a field isomorphism

$$\tilde{\beta} : \mathbb{Q}\big(a_1, \ldots, a_r, g_1, \ldots, g_t\big)^{\mathrm{rc}} \to \mathbb{Q}\big(b_1, \ldots, b_r, h_1, \ldots, h_t\big)^{\mathrm{rc}}.$$

By the construction of $g_1, \dots, g_t$ and $h_1, \dots, h_t$, we have that

$$\bigoplus_{i=1}^{t} k_i g_i \oplus \gamma \in sG \text{ if and only if } \bigoplus_{i=1}^{t} k_i h_i \oplus \beta(\gamma) \in sG'$$

for all $k_1, \dots, k_t \in \mathbb{Z}$, $s \in \mathbb{N}$ and $\gamma \in \Gamma$. Hence $\tilde{\beta}$ is an $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-isomorphism of

$$\big(\mathbb{Q}(a_1, \dots, a_r, g_1, \dots, g_t)^{\mathrm{rc}}, \Gamma_G\langle g_1, \dots, g_t\rangle\big) \text{ and}$$
$$\big(\mathbb{Q}(b_1, \dots, b_r, h_1, \dots, h_t)^{\mathrm{rc}}, \Gamma_{G'}\langle h_1, \dots, h_t\rangle\big).$$

It is also easy to see that $\tilde{\beta} \in \mathcal{S}$.

□

3.4. **Induced structure.** Let (K, G) be a model of $T(\Gamma)$. Here we study the subsets of G^n definable in (K, G).

Let B be a set of parameters such that $B \setminus \pi(G)$ is algebraically independent over $\mathbb{Q}(G)$.

Proposition 3.9. *Let $X \subseteq G^n$ be definable in $\big(K, G, (\gamma)_{\gamma\in\Gamma}\big)$ with parameters from B. Then X is a finite union of sets of the form*

$$E \cap \bigcup_{i=1}^{t} \gamma_i \oplus (sG)^n, \tag{3.8}$$

where E is $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$B$-definable, $\gamma_1, \dots, \gamma_t \in \Gamma^n$, and $s \in \mathbb{N}$.

Proof. We may assume that (K, G) is a $|\Gamma|^+$-saturated model of $T(\Gamma)$. Let $\mathcal{S}$ be the back and forth system of $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-isomorphisms between (K, G) and itself constructed above. Take $g, h \in G^n$ such that for every $E \subseteq K^{mn}$ definable in $\big(K, (\gamma)_{\gamma\in\Gamma}\big)$ over B, $\gamma_1, \dots, \gamma_t \in \Gamma^n$, and $s \in \mathbb{N}$ we have that

$$g \in E \cap \bigcup_{i=1}^{t} \gamma_i \oplus (sG)^n \Leftrightarrow h \in E \cap \bigcup_{i=1}^{t} \gamma_i \oplus (sG)^n. \tag{3.9}$$

Note that by Lemma 3.1, the collection of finite unions of sets of the form (3.8) is closed under boolean operations. Hence it suffices to show that there is $\beta \in \mathcal{S}$ fixing B such that β maps g to h. Since h satisfies all $\mathcal{L}_{\mathrm{o}}(\Gamma)$-formulas over B which are satisfied by g, there is an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-isomorphism from $\mathbb{Q}(g, B)^{\mathrm{rc}}$ to $\mathbb{Q}(h, B)^{\mathrm{rc}}$ fixing B and mapping g to h. To show that $\beta \in \mathcal{S}$, it is only left to prove that β takes $G \cap (\mathbb{Q}(B, g)^{\mathrm{rc}})^m$ to $G \cap (\mathbb{Q}(B, h)^{\mathrm{rc}})^m$. Using Lemma 3.3 it suffices to show $\beta(\Gamma\langle(\mathbb{Q}(B)^{\mathrm{rc}})^m \cap G, g\rangle) = \Gamma\langle(\mathbb{Q}(B)^{\mathrm{rc}})^m \cap G, h\rangle$. It is enough to show for all $\gamma \in \Gamma^n$, $k \in \mathbb{Z}^n$ and $s \in \mathbb{N}$ that

$$g \in \gamma \oplus D_{k,s} \text{ if and only if } h \in \gamma \oplus D_{k,s},$$

since we can choose representatives for cosets of $D_{k,s}$ in G^n from Γ^n. By Lemma 3.1, there are $\gamma_1, \dots, \gamma_{t_1}, \delta_1, \dots, \delta_{t_2} \in \Gamma^n$ such that $\gamma \oplus D_{k,s} = \bigcup_{i=1}^{t_1} \gamma_i \oplus (sG)^n$ and $G^n \setminus (\gamma \oplus D_{k,s}) = \bigcup_{i=1}^{t_2} \delta_i \oplus (sG)^n$. We are done since by assumption $g \in \gamma \oplus D_{k,s}$ if and only if $h \in \gamma \oplus D_{k,s}$. □

Corollary 3.10. *Let $X \subseteq G^n$ be definable in $\big(K, G, (\gamma)_{\gamma\in\Gamma}\big)$ with parameters from B. Then the topological closure $\overline{X}$ of X is definable in $\big(K, (\gamma)_{\gamma\in\Gamma}\big)$ over B.*

Proof. We prove that there is an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$B$-definable set $E \subseteq K^{mn}$ such that X is a dense subset of E. We do this by induction on n. For $n = 0$, the case is trivial. So let $n > 0$. By Proposition 3.9 we may assume that there exist an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$B$-definable set E_0 and an $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-$\emptyset$-definable set D_0 which is dense in G^n such that $X = E_0 \cap D_0$. Without loss of generality, we can assume that $E_0 \subseteq \mathbb{A}(K)^n$ and that E_0 is a cell. First consider the case that E_0 is open. Then X is dense in E_0. Now consider the case that $\dim E_0 = s$ for $s < nm$. We can assume that there are an open cell $C \subset K^s$, a projection $\pi : K^{mn} \to K^s$ and an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$B$-definable continuous function f such that $\pi(E_0) = C$ and $f(C) = E_0$. Consider the set

$$V' := \{(g_1, \ldots, g_s) \in \pi(G^n) \cap C \ : \ f(g_1, \ldots, g_s) \in D_0\}.$$

By the induction hypothesis, there is an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$B$-definable subset E_1 of C such that V' is dense in E_1. By continuity of the f, the image of V' under f is dense in the image of E_1 under f. Set $E := f(E_1)$. Since $X = f(V')$, we have that X is dense E.

□

4. Elliptic curves

Fix $a, b \in \mathbb{Q}$ such that $4a^3 + 27b^2 \neq 0$ and let Δ be the subset of $\mathbb{R}^2$ defined by

$$\{(x, y) \in \mathbb{R}^2 \ : \ y^2 = x^3 + ax + b\}.$$

Further let $(c, d) \in \mathbb{Q}^2 \setminus \Delta$ and define

$$\Delta^* := \Delta \cup \{(c, d)\} \text{ and } \Delta^*(\mathbb{Q}) := \Delta \cap \mathbb{Q}^2.$$

In this section, we show that Δ^* can be given the structure of a definable group in $\mathbb{R}$ such that $\Delta^*(\mathbb{Q})$ becomes a subgroup with the Mordell-Lang property. Further we establish that $\Delta^*(\mathbb{Q})$ is dense in Δ^* whenever it is infinite.

Let $\mathbb{P}^2(\mathbb{C})$ denote the complex projective plane and we write its elements as $(\alpha : \beta : \gamma)$. Let $\mathcal{E}$ consist of $(\alpha : \beta : \gamma) \in \mathbb{P}^2(\mathbb{C})$ such that

$$\beta^2\gamma = \alpha^3 + a\alpha\gamma^2 + b\gamma^3.$$

Then $\mathcal{E}$ is an *elliptic curve* and it is well-known that it becomes a group with a group operation $\oplus$ given by rational functions and identity element $\mathcal{O} := (0 : 1 : 0)$ (see for instance III.2.3 in [11]). Now Δ^* can be mapped injectively into $\mathcal{E}$ by

$$\iota : \Delta^* \to \mathcal{E}$$
$$(x, y) \mapsto \begin{cases} \mathcal{O}, & \text{if } (x, y) = (c, d); \\ (x : y : 1), & \text{otherwise.} \end{cases}$$

We write $\mathcal{E}(\mathbb{R})$ for the image of Δ^* under the map ι and $\mathcal{E}(\mathbb{Q})$ for image of $\Delta^*(\mathbb{Q})$.

It is easy to see that both $\mathcal{E}(\mathbb{R})$ and $\mathcal{E}(\mathbb{Q})$ are subgroups of $\mathcal{E}$. Thus the map ι induces a group structure on Δ^* and $\Delta^*(\mathbb{Q})$ becomes a subgroup of Δ^*. Since the group structure on $\mathcal{E}$ is given by rational functions, the group structure on Δ^* is semialgebraic. Further since $\mathcal{E}$ is compact, $\mathcal{E}(\mathbb{Q})$ is dense in $\mathcal{E}(\mathbb{R})$ whenever $\Delta^*(\mathbb{Q})$ is infinite. Hence $\Delta^*(\mathbb{Q})$ is dense in Δ^* if it is infinite.

It is just left to show that $\Delta^*(\mathbb{Q})$ has the Mordell-Lang property. Note that for this it is enough to show that for every algebraic subset V of $\mathcal{E}^n$ the set $V \cap \mathcal{E}(\mathbb{Q})^n$ is a finite union of cosets in $\mathcal{E}(\mathbb{Q})^n$ of subgroups of $\mathcal{E}(\mathbb{Q})^n$ given as the kernel of maps of the form

$$(x_1, \dots, x_n) \mapsto k_1 x_1 \oplus \cdots \oplus k_n x_n : \mathcal{E}(\mathbb{Q})^n \to \mathcal{E}(\mathbb{Q}),$$

with $k_1, \dots, k_n \in \mathbb{Z}$.

The elliptic curve $\mathcal{E}$ is a complex Lie group and it is analytically isomorphic to a complex torus $\mathbb{C}/\Lambda$ where $\Lambda \subseteq \mathbb{C}$ is a lattice; which can be taken to be $\mathbb{Z} + \mathbb{Z}\theta\sqrt{-1}$ for some $\theta \in \mathbb{R}$ since $\mathcal{E}$ is defined over $\mathbb{Q}$ (see VI.5.5 and VI.6.7(d) in [11]). This isomorphism uses the Weierstrass elliptic function $\wp$ attached to Λ, namely

$$z + \Lambda \mapsto \begin{cases} (\wp(z) : \wp'(z) : 1) & \text{if } z \notin \Lambda, \\ \mathcal{O} & \text{otherwise.} \end{cases}$$

The endomorphism ring of $\mathcal{E}$ is either $\mathbb{Z}$ or $\mathbb{Z}[\tau]$ for some $\tau \in \mathbb{C}$ with τ^2 is a negative integer. In the second case, we say $\mathcal{E}$ has *complex multiplication by* τ.

The key fact we use is the following special case of Faltings' Theorem (see [5]).

Theorem 4.1. *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}$ and Γ a finitely generated subgroup of $\mathcal{E}$. Then for every algebraic subset V of $\mathcal{E}^n$, the set $V \cap \Gamma^n$ is a finite union of cosets of subgroups $A \cap \Gamma^n$ of Γ^n, where A is an algebraic subgroup of $\mathcal{E}^n$.*

By the Mordell-Weil Theorem, $\mathcal{E}(\mathbb{Q})$ is indeed a finitely generated subgroup of the elliptic curve $\mathcal{E}$. In the case that $\mathcal{E}$ does not have complex multiplication, all algebraic subgroups of $\mathcal{E}^n$ are given as the kernels of maps of the form

$$(x_1, \dots, x_n) \mapsto k_1 x_1 \oplus \cdots \oplus k_n x_n : \mathcal{E}^n \to \mathcal{E}, \tag{4.1}$$

where $k_i \in \mathbb{Z}$ for $i = 1, \dots, n$. So in this situation we get the desired result by Theorem 4.1.

Now consider an elliptic curve $\mathcal{E}$ with complex multiplication by τ. This case is a bit more complicated, because an algebraic subgroup of $\mathcal{E}^n$ is of the kernel of a map of the form

$$(x_1, \ldots, x_n) \mapsto \bigoplus_{i=1}^{n} (k_i + l_i\tau)x_i : \mathcal{E}^n \to \mathcal{E}, \tag{4.2}$$

with $k_i, l_i \in \mathbb{Z}$. However, the next lemma implies that the cosets of the intersection of such an algebraic subgroup and $\mathcal{E}(\mathbb{Q})^n$ is a finite union of cosets of the intersection of $\mathcal{E}(\mathbb{Q})^n$ with subgroups given as kernels of maps of the form (4.1) with $k_i \in \mathbb{Z}$. Hence the result follows again from Theorem 4.1.

Lemma 4.2. *The intersection of $\mathcal{E}(\mathbb{R})$ with its image under τ is finite.*

Proof. In this case $\mathcal{E}$ is isomorphic to $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$. Since $\mathcal{E}$ is defined over $\mathbb{Q}$, the series expansions of $\wp$ and $\wp'$ have only real coefficients. Hence $\wp$ and $\wp'$ map equivalence classes of elements of the real axis to elements of the real axis. In particular, $(\wp : \wp' : 1)$ maps the set $\{t + \Lambda : t \in \mathbb{R} \cap [0, 1)\}$ into $\mathcal{E}(\mathbb{R})$. Let S be the inverse image of $\mathcal{E}(\mathbb{R})$ under $(\wp : \wp' : 1)$. Because $\mathcal{E}(\mathbb{R})$ is a one dimensional subgroup of $\mathcal{E}$ which has at most two connect components, S is either

$$\{t + \Lambda : t \in \mathbb{R} \cap [0, 1)\} \text{ or } \{t + \frac{s}{2} \cdot \tau + \Lambda : t \in \mathbb{R} \cap [0, 1), s \in \{0, 1\}\}.$$

In other words, S is a finite union of lines parallel to the real axis. Since on $\mathbb{C}/\Lambda$ the endomorphism of $\mathcal{E}$ corresponding to τ is just multiplication by the complex number τ, the set τS is a finite union of lines parallel to the imaginary axis. Hence the intersection of S and τS is finite and so is the intersection of $\mathcal{E}(\mathbb{R})$ and its image under τ. □

Hence Δ^* can be taken as $\mathbb{A}(\mathbb{R})$ of the previous section and $\Delta^*(\mathbb{Q})$ as Γ (It is clear from the finite generatedness of $\Delta^*(\mathbb{Q})$ that $\Delta^*(\mathbb{Q})/n\Delta^*(\mathbb{Q})$ is finite for every $n > 0$). Also $\mathcal{C}$ from the introduction is just $\Delta^*(\mathbb{Q}) \setminus \{(c, d)\}$ and thus $(\mathbb{R}, \mathcal{C})$ and $(\mathbb{R}, \Delta^*(\mathbb{Q}))$ are quantifier-free interdefinable over $\emptyset$. Therefore Theorem 1.1 follows immediately from Theorem 3.8 when $\Delta^*(\mathbb{Q})$ is infinite (If $\Delta^*(\mathbb{Q})$ is finite, then Theorem 1.1 is trivial). Also Theorem 3.7 takes the following form in this setting.

Theorem 4.3. *Suppose that $\Delta^*(\mathbb{Q})$ is infinite. Let K be a real closed field and G a dense subgroup of $\mathcal{E}(K)$ with a group morphism $\delta \mapsto \delta' : \Delta^*(\mathbb{Q}) \to G$. and let Δ' be the image of $\Delta^*(\mathbb{Q})$ under this map. Then*

$$\big(K, G, (\pi(\delta'))_{\delta \in \Delta^*(\mathbb{Q})}\big) \equiv \big(\mathbb{R}, \Delta^*(\mathbb{Q}), (\pi(\delta))_{\delta \in \Delta^*(\mathbb{Q})}\big)$$

if and only if

- $\big(K, (\pi(\delta'))_{\delta \in \Delta^*(\mathbb{Q})}\big) \equiv \big(\mathbb{R}, (\pi(\delta))_{\delta \in \Delta^*(\mathbb{Q})}\big)$,
- *for every $n > 0$ and $g \in G$ we have that $g \in \Delta'$ whenever $ng \in \Delta'$,*
- *for every $n > 0$, $|G/nG| = |\Delta'/n\Delta'|$,*
- *G satisfies the same Mordell-Lang conditions as Δ'.*

5. Open core

Here we work in a more general setting than the previous sections: Let $\mathcal{R} = (R, <, +, \dots)$ be an o-minimal expansion of a densely ordered abelian group in a language $\mathcal{L} = \{<, +, \dots\}$ and let $T_{\mathcal{R}}$ be its theory. Take a small subset G of R^m, and let $T_{\mathcal{R}}(G)$ be the theory of $(\mathcal{R}, G)$ in the language $\mathcal{L}(P) = \mathcal{L} \cup \{P\}$, where P is a new m-ary relation symbol. We denote models of $T_{\mathcal{R}}(G)$ by $(\mathcal{M}, P)$, where $\mathcal{M}$ is an $\mathcal{L}$-structure. In what follows, we say that a set $B \setminus P$ is dcl-*independent over* P if for every $b \in B$, the singleton $\{b\}$ is not definable in $\mathcal{M}$ over $\pi_1(P) \cup \dots \cup \pi_m(P) \cup B \setminus \{b\}$. (Here and in the rest of the section for a subset A of M, $A \setminus P$ means $A \setminus (\pi_1(P) \cup \dots \cup \pi_m(P))$, and we do not make a distinction between the relation symbol P and its interpretation.) For convenience in some of the proofs we also assume that $\mathcal{L}$ has two constant symbols c, d. This way we can combine two $\mathcal{L}$-definable functions by preserving the parameter set as follows: Let $f_1 : X_1 \to M$ and $f_2 : X_2 \to M$ be two functions definable in $\mathcal{M}$ over B, then the function

$$f : (X_1 \times \{(c, d)\}) \cup (X_2 \times \{(d, c)\}) \to M$$

given by $f(x_1, c, d) = f_1(x_1)$ and $f(x_2, d, c) = f_2(x_2)$, is definable in $\mathcal{M}$ over the same parameter set B.

Definition 5.1. Let $\mathcal{A} = (A, <, \dots)$ be an ordered structure and let T' be its theory.
(i) The *open core*, denoted by $\mathcal{A}^\circ$, of $\mathcal{A}$ is the the structure $\big(A, (U)\big)$, where U ranges over definable open subsets of A^n for various $n > 0$.

(ii) We say that a theory T is an *open core* of T' if for every $\mathcal{B}' \models T'$, there is $\mathcal{B} \models T$ such that $(\mathcal{B}')^\circ$ is interdefinable with $\mathcal{B}$.

Our main result is the following.

Theorem 5.2. *Suppose that for every $(\mathcal{M}, P) \models T_{\mathcal{R}}(G)$ we have that*

(i) *every subset of M^s definable in $(\mathcal{M}, P)$ is a boolean combination of subsets of M^s defined by*

$$\exists y_1 \cdots \exists y_{mn} \bigwedge_{j=0}^{n-1} P(y_{mj+1}, \dots, y_{mj+m}) \wedge \phi(x, y_1, \dots, y_{mn}),$$

where x is an s-tuple of distinct variables and ϕ is an $\mathcal{L}$-formula,

(ii) *for every parameter set B such that $B \setminus P$ is* dcl*-independent over P, and for every set $V \subset P^s$ definable in $(\mathcal{M}, P)$ over B, its topological closure $\overline{V} \subseteq M^{ms}$ is definable in $\mathcal{M}$ over B.*

Then $T_{\mathcal{R}}$ is an open core of $T_{\mathcal{R}}(G)$.

On the basis of Theorem 3.8 and Corollary 3.10, this result has the following consequence.

Corollary 5.3. *Let Γ be as in Section 3. If Γ is also dense, then* RCF *is an open core of $T(\Gamma)$.*

Combining this with the work of the previous section we get Theorem 1.2 in the following form.

Corollary 5.4. *The theory of real closed fields is an open core of the theory of $(\mathbb{R}, \mathcal{C})$. In particular every open subset of $\mathbb{R}^s$ definable in $(\mathbb{R}, \mathcal{C})$ is definable in the real field.*

We prove Theorem 5.2 using the following special case (precisely when T is o-minimal) of Theorem 4.14 from [3].

Theorem 5.5. *Let T be an o-minimal theory extending the theory of densely ordered abelian groups and let $T' \supseteq T$. Then the following are equivalent:*

- *T is an open core of T'.*
- *For every $\mathcal{A} \models T'$, every unary open set definable in $\mathcal{A}$ is a finite union of intervals and every cofinitely continuous unary function definable in $\mathcal{A}$ is given piecewise by function definable in the reduct of $\mathcal{A}$ to the language of T.*

We begin with some technical results. In what follows we assume that every model $(\mathcal{M}, P)$ of $T_{\mathcal{R}}(G)$ satisfies the conditions (i) and (ii) of Theorem 5.2. Also B always refers to a parameter set such that $B \setminus P$ is dcl-independent over P. Note that condition (ii) is equivalent to the following condition:

(ii′) for every $V \subseteq P^s$ definable in $(\mathcal{M}, P)$ over B, there is $E \subseteq M^{ms}$ definable in $\mathcal{M}$ over B such that V is a dense subset of E.

Lemma 5.6. *Let $X \subseteq M^{mn}$ and $f : X \to M^k$ be definable in $\mathcal{M}$ over B and let $V \subset P^n$ be definable in $(\mathcal{M}, P)$ over B. Then there is $E \subseteq M^{mn}$ definable in $\mathcal{M}$ over B such that $X \cap V$ is a dense subset of E and $f(X \cap V)$ is dense in $f(E)$.*

Proof. By cell decomposition in $\mathcal{M}$, we can assume that X is a cell and f is continuous on X. By (ii′), there is an $\mathcal{L}$-definable set E such that $X \cap V$ is dense in E. Since f is continuous on X, the image of $X \cap V$ is dense in the image of E. □

Lemma 5.7. *Let $X \subseteq M^{mn}$ and $f_1, f_2 : X \to M$ be definable in $\mathcal{M}$ over B and let $D \subset X \cap P^n$ be definable in $(\mathcal{M}, P)$ over B. Then the set*

$$\bigcup_{d \in D} \{a \in M : f_1(d) < a < f_2(d)\}$$

is definable in $\mathcal{M}$ over B.

Proof. Let $f : X \to M^2$ be the function given by $x \mapsto (f_1(x), f_2(x))$ for $x \in X$. By Lemma 5.6, there is an $\mathcal{L}$-B-definable set E such that D is dense in E and $f(D)$ is dense in $f(E)$. Hence

$$\bigcup_{d \in D} \{a : f_1(d) < a < f_2(d)\} = \bigcup_{e \in E} \{a : f_1(e) < a < f_2(e)\}.$$

Now note that the right hand side of the equation is $\mathcal{L}$-B-definable. □

Proposition 5.8. *Every unary open set definable set in $(\mathcal{M}, P)$ is definable in $\mathcal{M}$.*

Proof. Let X be an open subset of M definable in $(\mathcal{M}, P)$. By condition (i) of Theorem 5.2, X is a boolean combination of sets of the form

$$\bigcup_{u \in P^n} \{a \in M \ : \ \mathcal{M} \models \phi(a, u)\}, \tag{5.1}$$

where ϕ is an $\mathcal{L}$-formula. By cell decomposition, we may assume that X is a boolean combination of sets of the form

$$\{a \in M : f(u) = a \text{ for some } u \in D\} \tag{5.2}$$

$$\{a \in M : f_1(u) < a < f_2(u) \text{ for some } u \in E\} \tag{5.3}$$

where f, f_1, f_2 are $\mathcal{L}$-definable functions and D, E are $\mathcal{L}(P)$-definable subset of P^n. By writing X in conjunctive normal form, $X = \bigcap X_i$, where either X_i or $M \setminus X_i$ is a finite union of sets of the form (5.2) and (5.3). Using the observation at the end of the first paragraph of this section, we may even assume that X_i is of the form

$$f_1(D_1) \cup (M \setminus f_2(D_2)) \cup \bigcup_j Y_j \cup (M \setminus Z_j), \tag{5.4}$$

where Y_j, Z_j are of the form (5.3), f_1, f_2 are $\mathcal{L}$-definable functions and D, E are $\mathcal{L}(P)$-definable subsets of P^n. Since X is open, we have that X is the intersection of the interiors of the X_i's. Hence it is only left to show that for every i the interior of X_i is $\mathcal{L}$-definable. So consider now the set X_i of the form (5.4). First note that by Lemma 5.7, the set $\bigcup_j Y_j \cup (M \setminus Z_j)$ is $\mathcal{L}$-definable. Thus X_i is of the form

$$f_1(D_1) \cup (M \setminus f_2(D_2)) \cup Y, \tag{5.5}$$

where Y is an $\mathcal{L}$-definable set. Consider the set

$$D := \{u \in D_2 \ : \ (\mathcal{M}, P) \models \forall v \in D_1 \ f_1(v) \neq f_2(u)\}$$

By Lemma 5.6, there is an $\mathcal{L}$-definable set E such that D is dense in E and $f_2(D)$ is dense in $f_2(E)$. Hence we get by equation (5.5) that

$$\begin{aligned} X_i &= f_1(D_1) \cup (M \setminus f_2(D_2)) \cup Y \\ &= f_1(D_1) \cup (f_2(E) \setminus f_2(D)) \cup (M \setminus f_2(E)) \cup Y. \end{aligned}$$

Note that D is defined in a way to guarantee that $f_1(D_1) \cup (f_2(E) \setminus f_2(D))$ is codense in the interior of its topological closure. Set $Y' := (M \setminus f_2(E)) \cup Y$. We are going to show that the interior of X_i is a subset of the topological closure $\overline{Y'}$ of Y' . For a contradiction, suppose x is in the interior of X_i and not in $\overline{Y'}$. Hence there is an open interval $I \subset X_i \setminus \overline{Y'}$ containing x. But $X_i \setminus \overline{Y'}$ is codense in in the interior of its topological closure. This is a contradiction to $I \subset X_i \setminus \overline{Y'}$. Hence the interior of X_i is in the interior of $\overline{Y'}$. But for every set definable in an o-minimal structure, the interior of

the topological closure of a definable set is just the interior of the set itself. Hence the interior of X_i is in the interior of Y'. Since $Y' \subseteq X_i$, we have that X_i is the interior of Y' and so is $\mathcal{L}$-definable. □

Proposition 5.9. *Every cofinitely continuous $\mathcal{L}(P)$-definable function is piecewise $\mathcal{L}$-definable.*

Proof. We may assume that $(\mathcal{M}, P)$ is $|\mathcal{L}|^+$-saturated. Let $f : M \to M$ be a cofinitely continuous function which is defined by an $\mathcal{L}(P)$-B-formula $\phi(x, y)$. Take $a \in M$ such that $(\{a\} \cup B) \setminus P$ is dcl-independent over P. Note that by saturation and smallness of P, such elements form a dense subset W of M.

By Lemma 5.7 and condition (i), we can assume that $\phi(a, y)$ is a conjunction of disjunction of formulas of the form

(1) $\forall u \in D_1 \; y \neq f_1(a, u)$,
(2) $\exists v \in D_2 \; y = f_2(a, v)$,
(3) an $\mathcal{L}$-B-formula $\psi(a, y)$,

where f_1, f_2 are $\mathcal{L}$-B-definable functions and D_1, D_2 are $\mathcal{L}(P)$-$(B \cup \{a\})$-definable subsets of P^n. Set $X_a := \{y : \mathcal{M} \models \psi(a, y)\}$ and define D_a to be the set

$$\{u \in D_2 \; : \; (\mathcal{M}, P) \models \forall v \in D_1 \; f_1(a, v) \neq f_2(a, v)\}.$$

By Lemma 5.6 there is an $\mathcal{L}$-$(B \cup \{a\})$-definable set E_a such that D_a is dense in E_a and $f_2(D_a)$ is dense in $f_2(E_a)$. First note that $f(a)$ must be in the $\mathcal{L}$-$(B \cup \{a\})$-definable set $Y_a := f_2(E_a) \cap X_a$. If there is no open interval around $f(a)$ in Y_a, then $f(a)$ is $\mathcal{L}$-B-definable over a. So assume for a contradiction, that there is an open interval I around $f(a)$ in Y_a. Then $f_2(D_a) \cap I$ is dense in I. Hence there are infinitely many $b \in I$ such that $\phi(a, b)$ holds. This is a contradiction to f being a function. Hence $f(a)$ is $\mathcal{L}$-B-definable over a.

By the compactness theorem, we get finitely many $\mathcal{L}$-B-definable functions $h_1, \ldots, h_s$ such that for every $a \in W$, there is $i \in \{1, \ldots, s\}$ with $f(a) = h_i(a)$. Let Z_0 be the finite set of points of discontinuity of f. By monotonicity theorem of o-minimal structures, there is a finite set Z_1 such that for every $c, d \in Z_1$ with $(c, d) \cap Z_1 = \emptyset$ and for $i, j \in \{1, \ldots, s\}$, h_i, h_j are monotone on (c, d), and either h_i and h_j are equal on (c, d) or

- $h_i(x) < h_j(x)$ for every $x \in (c, d)$ or
- $h_i(x) > h_j(x)$ for every $x \in (c, d)$.

Hence for $c, d \in Z_0 \cup Z_1$ with $(c, d) \cap (Z_0 \cup Z_1) = \emptyset$, f is continuous on (c, d). Further $W \cap (c, d)$ is dense in (c, d) and for every $w \in W \cap (c, d)$ we have $f(w) = h_i(w)$ for some $i \in \{1, \ldots, s\}$. Since f is continuous on (c, d) and all the h_i's are a positive distant apart, it follows from o-minimality that there is $i \in \{1, \ldots, s\}$ such that f and h_i are equal on a dense subset of (c, d) and hence equal on (c, d). So f is given piecewise by $\mathcal{L}$-B-definable functions.

□

Now Theorem 5.2 follows directly from Theorem 5.5 in combination with Propositions 5.8, 5.9.

Remark. As a consequence of Theorem 5.2, we take care of an unfinished business from [7]. Namely we can simplify Theorem 1.3 of that paper by removing the assumption (iii), since it follows from the first two assumptions using Theorem 5.2.

5.1. **Subgroups of the unit circle.** Let Γ be a subgroup of the unit circle $\mathbb{S}$ of finite rank. Here we illustrate how Theorem 1.3 follows from Corollary 5.3. Note that if Γ is finite, then Theorem 1.3 is trivial, so we assume that it is infinite. Now all we need to show is that Γ has the Mordell-Lang property.

Note that Γ is a subgroup of $\mathbb{C}^\times$. Then according to [12] it has the property that for every $a_1, \dots, a_n \in \mathbb{Q}$, there are only finitely many $(\gamma_1, \dots, \gamma_n) \in \Gamma^n$ such that $a_1\gamma_1 + \cdots + a_n\gamma_n = 1$ and $\sum_{i\in I} a_i\gamma_i \neq 0$ for every nonempty subset I of $\{1, \dots, n\}$. Then using Proposition 5.8 of [4] we get that for every algebraic set $V \subseteq \mathbb{C}^n$ the set $V \cap \Gamma^n$ is a finite union of cosets in Γ^n of subgroups $T_k \cap \Gamma^n$ for various $k \in \mathbb{Z}^n$. Thus it follows that Γ has the Mordell-Lang property.

References

[1] Oleg Belegradek and Boris Zilber. The model theory of the field of reals with a subgroup of the unit circle. *J. Lond. Math. Soc. (2)*, 78(3):563–579, 2008.

[2] Alexander Berenstein, Clifton Ealy, and Ayhan Günaydın. Thorn independence in the field of real numbers with a small multiplicative group. *Ann. Pure Appl. Logic*, 150(1-3):1–18, 2007.

[3] Alfred Dolich, Chris Miller, and Charles Steinhorn. Structures having o-minimal open core. To appear in Trans. Amer. Math. Soc.

[4] Lou van den Dries and Ayhan Günaydın. The fields of real and complex numbers with a small multiplicative group. *Proc. London Math. Soc. (3)*, 93(1):43–81, 2006.

[5] Gerd Faltings. The general case of S. Lang's conjecture. In *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*, volume 15 of *Perspect. Math.*, pages 175–182. Academic Press, San Diego, CA, 1994.

[6] Ayhan Günaydın. *Model Theory of Fields with Multiplicative Groups*. PhD thesis, University of Illinois at Urbana-Champaign, 2008.

[7] Ayhan Günaydın and Philipp Hieronymi. Dependent pairs. Submitted.

[8] H. Jerome Keisler. Complete theories of algebraically closed fields with distinguished subfields. *Michigan Math. J.*, 11:71–81, 1964.

[9] Serge Lang. *Number theory. III*, volume 60 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1991. Diophantine geometry.

[10] Anand Pillay. On groups and fields definable in o-minimal structures. *J. Pure Appl. Algebra*, 53(3):239–255, 1988.

[11] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[12] A.J. van der Poorten and H.P. Schlickewei. Additive relations in fields. *J. Australian Math. Soc.*, 51:154–170, 1991.

[13] Boris Zilber. Complex roots of unity on the real plane. Available at the webpage `www.maths.ox.ac.uk/∼zilber`, 2003.

Centro de Matemática e Aplicações Fundamentais, Av. Prof. Gama Pinto, 2, 1649-003 Lisboa, Portugal

Department of Mathematics & Statistics, McMaster University, 1280 Main Street West Hamilton, ON, L8S 4K1, Canada
E-mail address: ayhan@ptmat.fc.ul.pt
E-mail address: P@hieronymi.de