FUNDAMENTA
MATHEMATICAE
211 (2011)

The real field with the rational points of an elliptic curve

by

Ayhan Günaydın (Lisboa) and
Philipp Hieronymi (Hamilton, ON, and Urbana, IL)

Abstract. We consider the expansion of the real field by 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 semialgebraic.

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*

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

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 4.4).

One of our motivations for studying $(\mathbb{R}, \mathcal{C})$ is to understand open definable 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.*

2010 *Mathematics Subject Classification*: 03C10, 03C64, 14H52, 11U09.
Key words and phrases: real field, definable set, elliptic curve, open core.

DOI: 10.4064/fm211-1-2

We prove Theorems 1.1 and 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 one-dimensional connected group definable in $\mathbb{R}$, satisfying a number-theoretic property. The details of the setting can be found in Section 2. In Section 3, we show that the conclusion of Theorem 1.1 holds for 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 [15] 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 [8] with an approach different than the one in [1]. However neither [1] nor [8] 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 unit circle and let Γ be a finite rank subgroup of $\mathbb{S}$; that is, Γ is contained in the divisible closure 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 $\mathrm{gr}(f)$.

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 [12], there is a topology on $\mathbb{A}$ definable in K such that $\mathbb{A}$ becomes a topological group. We will refer to this topology as the *t-topology*. Further, a subset of $\mathbb{A}$ is called *t-dense* (respectively *t-connected, t-compact*) if it is dense (respectively connected, compact) in the t-topology. A function $f : \mathbb{A}^n \to \mathbb{A}$ is said to be *t-continuous* if it is continuous with respect to the t-topology.

By Claim I in the proof of Proposition 2.5 in [12], the t-topology agrees with the topology induced from K^m except for finitely many points; that is, there is a finite subset X of $\mathbb{A}$ such that the topologies on $\mathbb{A} \setminus X$ induced from $\mathbb{A}$ and K^m are equivalent.

In [12], it is proven that $\mathbb{A}$ must be abelian-by-finite. By Theorem 1.1 of [6] we also know that $\mathbb{A}$ has finitely many n-torsion elements for each $n > 0$.

Throughout the rest of the paper, we assume that $(\mathbb{A}, \oplus)$ *is t-connected.*

By Proposition 2.12 of [12] it follows that $\mathbb{A}$ does not have any proper infinite definable subgroup. Combining this with the previous paragraph we see that $\mathbb{A}$ is abelian and divisible.

Note that the t-connectedness assumption is not very restrictive, because every group definable in K is a finite union of cosets of its t-connected component.

Let $\pi_1, \ldots, \pi_m$ be the standard projections of K^m onto K. For our purposes it is harmless to assume that there is $i \in \{1, \ldots, m\}$ such that for every $a \in \mathbb{A}$ and $j = 1, \ldots, m$ the image $\pi_j(a)$ is $\mathcal{L}_{\mathrm{o}}$-definable over $\pi_i(a)$. Moreover we take i to be 1 and we sometimes write π instead of π_1.

For convenience we also 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 $k = (k_1, \ldots, k_n)$ be a tuple of integers. Consider the group character

$$\chi_k : \mathbb{A}^n \to \mathbb{A}, \qquad \chi_k(a_1, \ldots, a_n) := k_1 a_1 \oplus \cdots \oplus k_n a_n,$$

and let T_k denote the kernel of χ_k.

Fix $n > 0$ and a tuple of distinct indeterminates $X = (X_1, \ldots, X_{mn})$. We usually denote an element of the polynomial ring $K[X]$ by p (possibly with subscripts) and if we want to make the variables precise, we write $p(X)$. In what follows we identify K^{mn} with $(K^m)^n$. In particular, for $\alpha_1, \ldots, \alpha_n \in K^m$ and a polynomial $p \in K[X]$, $p(\alpha_1, \ldots, \alpha_n)$ means

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

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

Finally for a polynomial p as above we put

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

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

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

Definition 2.1. We say that G has the *Mordell–Lang property over L* if for every $n > 0$ and for every polynomial $p \in L[X]$, there are $g_1, \ldots, g_t \in G^n$ and $k_1, \ldots, k_t \in \mathbb{Z}^n$ such that

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

The reason for this name is that this property is the conclusion of a conjecture of Lang generalizing a conjecture of Mordell for abelian varieties. We refer the reader to [10] 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 $p \in L[\alpha][X]$. Write

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

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

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

Therefore

$$V(p) \cap G^n = \bigcap_{i=0}^{d-1} V(p_i) \cap G^n = V(p_0^2 + \cdots + p_{d-1}^2) \cap G^n.$$

By the Mordell–Lang property over L, we know that $V(p_0^2 + \cdots + p_{d-1}^2) \cap G^n$ is a finite union of cosets of the 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 $i = (i(1), \ldots, i(s)) \in \mathbb{N}^s$, $|i|$ denotes $i(1) + \cdots + i(s)$, and for a tuple $Y = (Y_1, \ldots, Y_s)$ of distinct indeterminates, Y^i is the monomial

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

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

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 $p \in \mathbb{Q}[G][X]$ of degree d. Write

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

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

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

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 $p \in E[X]$, and write

$$p = \sum_i p_i \alpha^i,$$

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

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

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

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.

For a subset S of $K[X]$, let

$$V(S) := \bigcap_{p \in S} V(p).$$

Let $C = K(\sqrt{-1})$ be the algebraic closure of K and identify C with K^2 in the usual way. We get the following consequence of the Mordell–Lang property.

Corollary 2.5. *Let $X \subset C^{mn}$ be definable in the field C. Then $X \cap G^n$ is definable in the group $(G, \oplus)$.*

Proof. By quantifier elimination for algebraically closed fields, it suffices to show that for every $S \subseteq K[X]$, there are $s, t \in \mathbb{N}$ and $g_{i,j} \in G^n$ and

$k_{i,j} \in \mathbb{Z}^n$ for $i = 1, \dots, s$ and $j = 1, \dots, t$ such that

$$V(S) \cap G^n = \bigcap_{i=1}^{s} \bigcup_{j=1}^{t} g_{i,j} \oplus (T_{k_{i,j}} \cap G^n).$$

This easily follows from the Mordell–Lang property combined with Hilbert's Basis Theorem. ∎

Remark. Note that we cannot get this result with K in place of C. Vaguely speaking, it is not possible to define the trace of ordering on the group G.

2.1. The main lemma. We prove an analog of Lemma 5.12 in [5], 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 $g', g'_1, \dots, g'_n$ elements of G'. We say that g' is *algebraic over* L if $\pi(g')$ is algebraic over L, and similarly $g'_1, \dots, g'_n$ are *algebraically dependent over* L if $\pi(g'_1), \dots, \pi(g'_n)$ are algebraically dependent over L. Also we say that $g'_1, \dots, g'_n$ are *linearly dependent modulo* G if there is $k \in \mathbb{Z}^n \setminus \{(0, \dots, 0)\}$ such that $\chi_k(g'_1, \dots, g'_n) \in G$.

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

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

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

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

Lemma 2.6. *Let G' be a subgroup of $\mathbb{A}$ containing G and suppose that G' satisfies the same Mordell–Lang conditions as G. Then $g'_1, \dots, g'_n \in G'$ are linearly dependent modulo G whenever they are algebraically dependent over $\mathbb{Q}(G)$.*

Proof. We just prove the case $n = 1$ and the general case can be proven using similar arguments. So let $g' \in G'$ be algebraically dependent over $\mathbb{Q}(G)$. Let $X = (X_1, \dots, X_m)$ and $Y = (Y_1, \dots, Y_{mt})$ be tuples of distinct indeterminates, and take a polynomial $p(X_1, Y) \in \mathbb{Q}[X_1, Y]$ and $h \in G^t$ such that $p(\pi(g'), h) = 0$ and $p(X_1, h)$ is not the zero polynomial. Then considering $p(X_1, Y)$ as an element of $K[X, Y]$ and using the Mordell–Lang condition for $n = t + 1$ we get $k \in \mathbb{Z}^{t+1}$ 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 $p(\pi(g''), h) = 0$ for every $g'' \in G'$ and hence $p(X_1, h)$ is the zero polynomial. Now it is easy to see that $k_1 g' \in G$. ∎

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 Proposition 2.9 below).

Here we define smallness only in the setting of fields; in Section 5, we define it in a more general 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 2.7. Let E be a field. A subset X of E^s is called *large* if there is a map $f : E^{sn} \to E$ definable in the field E such that $f(X^n) = E$; otherwise we say that X is *small*.

Remarks. (1) Smallness is an elementary property of the pair (E, X) construed as a structure in the language of rings expanded by an s-ary relation symbol.

(2) If E is an ordered field or is an algebraically closed field, then X is large if and only if there is a multi-valued map $f : E^{sn} \xrightarrow{l} E$ definable in the field E such that $f(X) = E$. It is easy to see this when E is an ordered field, and for algebraically closed fields see Lemma 2.4 in [5] (note that the definition of large is different in that paper).

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

Remember that at the beginning of this section we fixed K to be a real closed field and G a subgroup of a t-connected one-dimensional group definable in K with the Mordell–Lang property. Let $C = K(\sqrt{-1})$.

Lemma 2.8. *If $X \subseteq K^s$ is small in C, then X is small in K.*

Proof. By the first of the remarks above we may assume that K is $\aleph_0$-saturated. Also by the second remark, it is enough to prove the following:

Claim. *Let $f : K^s \to K$ be definable in the field K. Then there is a multi-valued function $\tilde{f} : C^s \xrightarrow{l} C$ definable in the field C such that $f(\alpha) \in \tilde{f}(\alpha)$ for each $\alpha \in K^s$.*

Proof of the claim. Suppose that f is definable over $B \subseteq K$ and let $\alpha \in K^s$. Then $f(\alpha)$ is in the definable closure in K of $B \cup \{\alpha\}$. Hence $f(\alpha)$

is in the algebraic closure in C of $B \cup \{\alpha\}$. Let this be witnessed by a formula $\phi(x, y)$ in the language of rings; that is,

$$C \models \phi(\alpha, f(\alpha)) \text{ and } |\{y \in C : C \models \phi(\alpha, y)\}| < \infty. \tag{2.1}$$

By quantifier elimination for algebraically closed fields, the second part of (2.1) is expressible by a formula in the language of rings. By saturation of K, there are formulas $\phi_1, \ldots, \phi_t$ in the language of rings such that for all $\alpha \in K^s$ there is $i \in \{1, \ldots, t\}$ such that (2.1) holds with ϕ in place of ϕ_i.

For $\alpha \in C$, let I_α be the set

$$\{i \in \{1, \ldots, t\} : |\{y \in C : C \models \phi_i(\alpha, y)\}| < \infty\}.$$

Now define a multi-valued function $\tilde{f} : C^s \to C$ by

$$\tilde{f}(x) := \begin{cases} \bigcup_{i \in I_x} \{y \in C : C \models \phi_i(x, y)\} & \text{if } I_x \neq \emptyset, \\ \{0\} & \text{otherwise.} \end{cases} \blacksquare$$

We need the following general model-theoretic fact in the next proposition.

Fact. *A field is interpretable in an abelian group only if it is finite.*

Proof. For this, recall the well-known model-theoretic results that every abelian group is one-based and that a group interpretable in a one-based structure has an abelian subgroup of finite index (see [13]). Now the fact follows since $\mathrm{SL}_2(E)$ does not have an abelian subgroup of finite index for an infinite field E. ∎

Now we are ready to prove the following.

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

Proof. By Lemma 2.8, it is enough to show that G is small in the algebraically closed field C. For a contradiction let $f : C^{mn} \to C$ be definable in the field C such that $f(G^n) = C$. Let $R \subseteq C^{2mn}$ be the equivalence relation on C^{mn} defined as follows:

$$R(x, y) \;\Leftrightarrow\; f(x) = f(y),$$

and put $R_G := R \cap G^{2n}$, which is definable in the group $(G, \oplus)$ by Corollary 2.5. Then f gives a bijection between G^n/R_G and C, and we carry over the addition and multiplication on C to G^n/R_G using this bijection, which are interpretable in $(G, \oplus)$. This gives an infinite field interpretable in an abelian group, contradicting the fact above. ∎

A consequence of smallness is the following.

Corollary 2.10. *Let $f_1, \ldots, f_l : K^{mn} \to K$ be definable in the ordered field K. Then $K \setminus \bigcup_{i=1}^{l} f_i(G^n)$ is dense in K.*

Proof. Let $f : K^{mn} \to K$ be the l-valued map taking $\alpha \in K^{mn}$ to the set $\{f_1(\alpha), \dots, f_l(\alpha)\}$. 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. Remember that $(\mathbb{A}, \oplus)$ is a one-dimensional t-connected group definable in a real closed field K over $\emptyset$. As before for another real closed field E, we let $\mathbb{A}(E)$ denote the group definable in E by the formulas defining $\mathbb{A}$ in K. As mentioned above, such a group is abelian, divisible and has finitely many n-torsion points for every $n > 0$.

Fix a subgroup Γ of $\mathbb{A}(\mathbb{R})$ with the Mordell–Lang property such that $|\Gamma/n\Gamma|$ is finite for every $n > 0$.

3.1. The theory. 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 $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$ be the language $\mathcal{L}_{\mathrm{o}}(\Gamma)$ extended by P. For simplicity of notation we denote $\mathcal{L}_{\mathrm{o}}(\Gamma)$-structures by $(K, (\gamma)_{\gamma\in\Gamma})$, rather than $(K, (\pi(\gamma))_{\gamma\in\Gamma})$; similarly $(K, G, (\gamma)_{\gamma\in\Gamma})$ are $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-structures.

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

(1) G is a t-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 20).

Using Proposition 2.5 of [12] once again, we get a finite subset S of $\mathbb{A}(K)$ such that a subset X of $\mathbb{A}(K)$ is t-dense if and only if $X \setminus S$ is dense in $\mathbb{A}(K) \setminus S$. Hence condition (1) is first order in the language $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$. It is easy to see that conditions (2) and (3) are also first order in the language $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$; 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 $p \in \mathbb{Q}[X]$ such that

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

and consider the formula

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

Note that if Γ is t-dense in $\mathbb{A}(\mathbb{R})$, then $(\mathbb{R}, \Gamma)$ is a model of $T(\Gamma)$. We proceed 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

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

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 $(K, G, (\gamma)_{\gamma \in \Gamma})$ 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

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

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 $D_{k,e}$ 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 the coset representatives can be chosen from Γ^n by axiom (3). Moreover, l in the lemma depends only on $e_1, \ldots, e_t$ and not on G or $k_1, \ldots, k_s$.

Lemma 3.2. *Let $\gamma \in \mathbb{A}(K)^n$, $k \in \mathbb{Z}^n$ and $e \in \mathbb{N}$. Then $\gamma \oplus D_{k,e}$ is t-dense in $\mathbb{A}(K)^n$.*

Proof. Since G is t-dense in $\mathbb{A}(K)$ and multiplication by e is a t-continuous map on $\mathbb{A}(K)$, it follows that $(eG)^n$ is t-dense in $(e\mathbb{A}(K))^n$. Since $\mathbb{A}(K)^n$ is divisible, $(eG)^n$ is t-dense in $\mathbb{A}(K)^n$. Since $(eG)^n \subseteq D_{k,e}$, we see that $D_{k,e}$ is t-dense in $\mathbb{A}(K)^n$. Since addition is t-continuous, $\gamma \oplus D_{k,e}$ is t-dense $\mathbb{A}(K)^n$. ∎

Recall that a subgroup H of G is called *pure* if $nG \cap H = nH$ for every $n > 0$. For a subset X of G we let $\langle X \rangle_G$ be the subgroup of G generated by X and we let $[X]_G$ be the subgroup of G consisting of g such that $ng \in \langle X \rangle_G$ for some $n > 0$. When the ambient group G is clear from the context, we omit G from both of these notations.

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

LEMMA 3.3. *Let H be a pure subgroup of G containing Γ and let $g \in G$. Then*

$$(\mathbb{Q}(H,g)^{\mathrm{rc}})^m \cap G = [H \cup \{g\}].$$

Proof. It is easy to see that $[H \cup \{g\}] \subseteq (\mathbb{Q}(H,g)^{\mathrm{rc}})^m \cap G$. 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 2.6 to deduce that g and g' are linearly dependent modulo H. Thus $g' \in [H \cup \{g\}]$. ∎

We can strengthen this lemma as follows.

LEMMA 3.4. *Let H, g be as in the previous lemma and let X be a subset of K algebraically independent over $\pi(G)$. Then*

$$(\mathbb{Q}(X,H,g)^{\mathrm{rc}})^m \cap G = [H \cup \{g\}].$$

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

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

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

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

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

COROLLARY 3.5. *Let $g \in G$. If g is $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$\emptyset$-definable, then $g \in \Gamma$.*

Proof. Using Lemma 3.3, we have $[\Gamma] = (\mathbb{Q}(\Gamma)^{\mathrm{rc}})^m \cap G$. But $[\Gamma] = \Gamma$ by axiom (2). ∎

LEMMA 3.6. *Suppose that (K,G) is $|\Gamma|^+$-saturated. Let S be an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$\emptyset$-definable subset of $\mathbb{A}(K)$ and let D be a t-dense subset of G. Then the projection $\pi((D \setminus \Gamma) \cap S)$ is dense in the interior of $\pi(S)$.*

Proof. Let $Y \subseteq \mathbb{A}(K)$ be the finite set of points where the t-topology does not agree with the induced topology from K^m. Hence $D \setminus Y$ is dense in $\mathbb{A}(K) \setminus Y$. By the construction of the t-topology in [12], every point of Y is $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$\emptyset$-definable. Hence $G \cap Y \subseteq \Gamma$ by Corollary 3.5.

By o-minimality, $\pi(S)$ is a finite union of open intervals and points. So suppose there is $g \in D$ such that $\pi(g)$ is one of these points. This implies that $\pi(g)$ is $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$\emptyset$-definable, since S is. Then $g \in \Gamma$ by Corollary 3.5. Hence $\pi((D \setminus \Gamma) \cap S)$ is in the interior of $\pi(S)$.

Since (K,G) is $|\Gamma|^+$-saturated, $\pi(\Gamma)$ is discrete in K. Because $D \setminus Y$ is dense in $\mathbb{A}(K) \setminus Y$ and $Y \cap D \subseteq \Gamma$, we conclude that $\pi((D \setminus \Gamma) \cap S)$ is dense in the interior of $\pi(S)$. ∎

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

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

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

Note that by Lemma 3.4, $(\mathbb{Q}(X, H)^{\mathrm{rc}}, H)$ and $(\mathbb{Q}(X', H')^{\mathrm{rc}}, H')$ 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 3.7. *The collection $\mathcal{S}$ is a back-and-forth system.*

Proof. Let $\beta : (\mathbb{Q}(X, H)^{\mathrm{rc}}, H) \to (\mathbb{Q}(X', H')^{\mathrm{rc}}, H')$ be in $\mathcal{S}$ and take $a \in K \setminus \mathbb{Q}(X, H)^{\mathrm{rc}}$. 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 an $\mathcal{L}_{\mathrm{o}}$-$\emptyset$-definable function $f : K \to K^{m-1}$ such that $b = f(a)$. Let $q(x)$ be the $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-type consisting of the $\mathcal{L}_{\mathrm{o}}$-type of a over $\mathbb{Q}(X, H)^{\mathrm{rc}}$ and for every $l \in \mathbb{Z}$, $h \in H$ and $s > 0$ one of the formulas

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

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

depending on whether $l(a, b) \oplus h \in sG$ or not. Further let $q'(x)$ be the type over $\mathbb{Q}(X', H')^{\mathrm{rc}}$ corresponding to $q(x)$ via β. We want to find an $a' \in K'$ such that a' realizes $q'(x)$. By saturation of (K', G'), it is enough to show that every finite subset of $q'(x)$ can be realized in (K', G'). By o-minimality of T, this reduces to finding $a' \in K'$ for every $c, d \in \mathbb{Q}(X, H)^{\mathrm{rc}}$ 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 and the remark succeeding it,

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

is a finite union of cosets of tG' in G' for some $t \in \mathbb{N}$, and the representatives of these cosets can be chosen to be in Γ. Then by Lemmas 3.2 and 3.6, the set $\pi((D \setminus \Gamma) \cap \mathrm{gr}(f))$ is dense in the interior of $\pi(\mathbb{A}(K') \cap \mathrm{gr}(f))$.

Since $\pi(\mathbb{A}(K) \cap \mathrm{gr}(f))$ is $\mathcal{L}_{\mathrm{o}}(\Gamma)$-definable and a is in it, we can assume that the interval (c, d) is a subset of $\pi(\mathbb{A}(K) \cap \mathrm{gr}(f))$. As β is a partial $\mathcal{L}_{\mathrm{o}}$-elementary map, it follows that the interval $(\beta(c), \beta(d))$ is a subset of $\pi(\mathbb{A}(K') \cap \mathrm{gr}(f))$ and that $\pi((D \setminus \Gamma) \cap \mathrm{gr}(f)) \cap (\beta(c), \beta(d))$ is a dense subset of $(\beta(c), \beta(d))$. Now take any $a' \in \pi((D \setminus \Gamma) \cap \mathrm{gr}(f)) \cap (\beta(c), \beta(d))$. This a' satisfies (3.4). It is clear that $[H \cup \{(a, b)\}]_G$ and $[H' \cup \{(a', f(a'))\}]_{G'}$ are pure subgroups of G and G' respectively. Let $\tilde{\beta}$ be the $\mathcal{L}_{\mathrm{o}}(P; \Gamma)$-isomorphism that extends β to $\mathbb{Q}(X, H, a)^{\mathrm{rc}}$ and maps a to a'. By conditions (3.2) and (3.3), we deduce that $\tilde{\beta}$ maps $[H \cup \{(a, b)\}]_G$ onto $[H' \cup \{(a', f(a'))\}]_{G'}$. Hence $\tilde{\beta}$ is an $\mathcal{L}_{\mathrm{o}}(P; \Gamma)$-isomorphism between $(\mathbb{Q}(X, H, a)^{\mathrm{rc}}, [H \cup \{(a, b)\}]_G)$ and $(\mathbb{Q}(X', H', a')^{\mathrm{rc}}, [H' \cup \{(a', f(a'))\}]_{G'})$ and $\tilde{\beta} \in \mathcal{S}$.

Case 2: $a \in \mathbb{Q}(X, G)^{\mathrm{rc}}$. Let $g_1, \ldots, g_n \in G$ be such that $a \in \mathbb{Q}(X, \{g_1, \ldots, g_n\})^{\mathrm{rc}}$. By applying the previous case n times, we get a $\tilde{\beta} \in \mathcal{S}$ such that $g_1, \ldots, g_n \in \mathrm{dom}(\tilde{\beta})$. Since $\mathrm{dom}(\tilde{\beta})$ is a real closed field, we have $a \in \mathrm{dom}(\tilde{\beta})$.

Case 3: $a \notin \mathbb{Q}(X, G)^{\mathrm{rc}}$. Let C be the cut of a in $\mathbb{Q}(X, H)^{\mathrm{rc}}$ and let C' be the cut in $\mathbb{Q}(X', H')^{\mathrm{rc}}$ corresponding to C via β. 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 $u \in K^{|X|}$ be the set X written as a tuple. Let $f_1, \ldots, f_n : K^{mt+|X|} \to K$ be $\emptyset$-definable functions in the language $\mathcal{L}_{\mathrm{o}}(\Gamma)$. By Corollary 2.10, 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',

$$f_i(g'_1, \ldots, g'_t, \beta(u)) \neq b'.$$

Thus by saturation, there is an $a' \in (c', d')$ such that $a' \notin \mathbb{Q}(X', G')^{\mathrm{rc}}$. Since a' realizes the cut C', there is an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-isomorphism $\tilde{\beta}$ from $\mathbb{Q}(X, a, H)^{\mathrm{rc}}$ to $\mathbb{Q}(X', a', H')^{\mathrm{rc}}$ extending β and sending a to a'. Since $a \notin \mathbb{Q}(X, G)^{\mathrm{rc}}$ and $a' \notin \mathbb{Q}(X', G')^{\mathrm{rc}}$, using Lemma 3.4 we get

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

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

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

Theorem 3.8. *Let Γ be t-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 nonempty. But it is easy to see that the identity map on $(\mathbb{Q}(\Gamma)^{\mathrm{rc}}, \Gamma)$ belongs to $\mathcal{S}$. ∎

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

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

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 the relation symbols P_ϕ (for various x).

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

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

for each ϕ of the form (3.5).

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

THEOREM 3.9. *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 $a = (a_1, \dots, a_n) \in K^n$ and $b = (b_1, \dots, b_n) \in (K')^n$ with 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 may assume that $\{a_1, \dots, a_r\}$ is a transcendence basis of $\mathbb{Q}(G,a)$ over $\mathbb{Q}(G)$. Since a and b have the same quantifier-free $\mathcal{L}_{\mathrm{o}}(P;\Gamma)^+$-type, we see that $\{b_1, \dots, b_r\}$ is a transcendence basis of $\mathbb{Q}(G',b)$ over $\mathbb{Q}(G')$. Let β be the $\mathcal{L}_{\mathrm{o}}(\Gamma)$-isomorphism between $\mathbb{Q}(a_1, \dots, a_r, \Gamma)^{\mathrm{rc}}$ and $\mathbb{Q}(b_1, \dots, b_r, \Gamma)^{\mathrm{rc}}$ sending a to b. We will now show that β extends to an isomorphism $\tilde{\beta}$ in the back-and-forth system $\mathcal{S}$. Let $g_1, \dots, g_t \in G$ be such that $a_{r+1}, \dots, a_n$ are in $\mathbb{Q}(a_1, \dots, a_r, g_1, \dots, g_t, \Gamma)^{\mathrm{rc}}$. Let $q(x_1, \dots, x_t)$ be the $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-type consisting of the $\mathcal{L}_{\mathrm{o}}(\Gamma)$-type of $(g_1, \dots, g_t)$ over $\mathbb{Q}(a_1, \dots, a_r)^{\mathrm{rc}}$ and for every $k_1, \dots, k_t \in \mathbb{Z}$, $s \in \mathbb{N}$ and $\gamma \in \Gamma$ one of the formulas

$$\bigwedge_{i=1}^{t} P(x_i) \wedge \bigoplus_{i=1}^{t} k_i x_i \oplus \gamma \in sG, \quad \text{or} \tag{3.6}$$

$$\bigwedge_{i=1}^{t} P(x_i) \wedge \bigoplus_{i=1}^{t} k_i x_i \oplus \gamma \notin sG, \tag{3.7}$$

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

By Lemma 3.1, the set

$$\{(h_1,\dots,h_t)\in G'^t : (K',G')\models \chi(h_1,\dots,h_t)\}$$

is a finite union of cosets of $(lG')^t$ in $(G')^t$ for some $l\in\mathbb{N}$. So the formula $\chi(x)$ is equivalent to an $\mathcal{L}_{\mathrm{o}}(P;\Gamma)$-formula of the form (3.5). Hence the disjunction $\psi\wedge\chi$ is a quantifier-free $\mathcal{L}_{\mathrm{o}}(P;\Gamma)^+$-formula. Since $(a_1,\dots,a_r)$ and $(b_1,\dots,b_r)$ have the same quantifier-free $\mathcal{L}_{\mathrm{o}}(P;\Gamma)^+$-type, and

$$\exists x(\psi\wedge\chi)(x,a_1,\dots,a_r)$$

holds in (K,G), the corresponding formula $\exists x(\psi\wedge\chi)(x,b_1,\dots,b_r)$ holds in (K',G'). So q' is finitely satisfiable. Now let $h_1,\dots,h_t\in G'$ realize q'. Then β extends to a field isomorphism

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

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

$$\bigoplus_{i=1}^{t}k_ig_i\oplus\gamma\in sG \quad\text{if and only if}\quad \bigoplus_{i=1}^{t}k_ih_i\oplus\beta(\gamma)\in sG'$$

for all $k_1,\dots,k_t\in\mathbb{Z}$, $s\in\mathbb{N}$ and $\gamma\in\Gamma$. Hence $\tilde{\beta}$ is 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 3.10. *Let $X\subseteq G^n$ be definable in $(K,G,(\gamma)_{\gamma\in\Gamma})$ with parameters from B. Then X is a finite union of sets of the form*

$$E\cap(\gamma\oplus(sG)^n), \tag{3.8}$$

where E is $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$B$-definable, $\gamma\in\Gamma^n$, 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. Let $g,h\in G^n$ be such that for every $E\subseteq K^{mn}$ definable in $(K,(\gamma)_{\gamma\in\Gamma})$ over B, $\gamma_1,\dots,\gamma_t\in\Gamma^n$, and $s\in\mathbb{N}$ we have that

$$g\in E\cap(\gamma\oplus(sG)^n)\Leftrightarrow h\in E\cap(\gamma\oplus(sG)^n). \tag{3.9}$$

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 and mapping 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 3.4 it suffices to show

$$\beta([\Gamma\cup((\mathbb{Q}(B)^{\mathrm{rc}})^m\cap G)\cup\{g\}])=[\Gamma\cup((\mathbb{Q}(B)^{\mathrm{rc}})^m\cap G)\cup\{h\}].$$

It is enough to show for all $\gamma \in \Gamma^n$, $k \in \mathbb{Z}^n$ and $s \in \mathbb{N}$ that

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

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

Proof. By Lemma 1.3.4 of [4] the topological closure of a set definable in the ordered field K is again definable in the ordered field K. So it suffices to 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. The case $n = 0$ is trivial. So let $n > 0$. By Proposition 3.10 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 $D_0 \subseteq G^n$ such that $X = E_0 \cap D_0$. By Lemma 3.2, we can assume that D_0 is t-dense in $\mathbb{A}(K)^n$. Since the t-topology and the induced topology from K^m coincide apart from finitely many points, we can even assume that D_0 is dense in a $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$\emptyset$-definable S_0. By cell decomposition, we can assume that E_0 is a cell and that $E_0 \subseteq S_0 \cap \mathbb{A}(K)^n$. Hence $\dim E_0 \leq n$. First consider the case that $\dim E_0 = n$. By Lemma 4.1.15 of [4], we can assume that E_0 is open in S_0. Since D_0 is dense in S_0, X is dense in E_0. Now consider the case that $\dim E_0 = s$ for $s < n$. We can assume that there is an $\mathcal{L}_{\mathrm{o}}(\Gamma)$-$B$-definable set $C \subseteq \mathbb{A}(K)^s$, a projection $\pi : K^{mn} \to K^{ms}$ 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

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

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 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 conclude 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

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

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.

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 over $\mathbb{Q}$ and identity element $\mathcal{O} := (0 : 1 : 0)$ (see for instance III.2.3 in [14]). Now Δ^* can be mapped injectively into $\mathcal{E}$ by

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

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

The elliptic curve $\mathcal{E}$ is a complex Lie group and as such it is isomorphic to a complex torus $\mathbb{C}/\Lambda$ where $\Lambda \subseteq \mathbb{C}$ is a lattice. This isomorphism uses the Weierstrass elliptic function $\wp$ attached to Λ, namely

$$f : \mathbb{C}/\Gamma \to \mathcal{E}, \quad z + \Lambda \mapsto \begin{cases} (\wp(z) : \wp'(z) : 1) & \text{if } z \notin \Lambda, \\ \mathcal{O} & \text{otherwise.} \end{cases}$$

We also have the quotient map $q : \mathbb{C} \to \mathbb{C}/\Gamma$.

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

In the case that $\mathcal{E}$ does not have complex multiplication, all algebraic subgroups of $\mathcal{E}^n$ are the kernels of maps of the form

$$(x_1, \dots, x_n) \mapsto k_1x_1 \oplus \cdots \oplus k_nx_n : \mathcal{E}^n \to \mathcal{E}, \tag{4.1}$$

where $k_i \in \mathbb{Z}$ for $i = 1, \dots, n$.

If the elliptic curve $\mathcal{E}$ has complex multiplication by τ, then the situation is a bit more complicated, because an algebraic subgroup of $\mathcal{E}^n$ is the kernel of a map of the form

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

with $k_i, l_i \in \mathbb{Z}$. However, using the following lemma we still have control over the intersection of these subgroups with $\mathcal{E}(\mathbb{Q})^n$.

LEMMA 4.1. *Let $\mathcal{E}$ be an elliptic curve with complex multiplication by τ. Then 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 $\Lambda = \mathbb{Z}+\mathbb{Z}\tau$ (see C.11.6 in [14]). Since τ is purely imaginary, the series expansions of $\wp$ and $\wp'$ have

only real coefficients (see Theorem VI.3.5 in [14]). Then f maps the set $[0,1)+\Lambda$ into $\mathcal{E}(\mathbb{R})$. Let S be the inverse image of $\mathcal{E}(\mathbb{R})$ under f. Being a one-dimensional group definable in the ordered field $\mathbb{R}$, Δ^* has finitely many connected components and so does $\mathcal{E}(\mathbb{R})$. Thus S is the image under q of a finite union of lines in $\mathbb{C}$ parallel to the real axis. On $\mathbb{C}/\Lambda$ the endomorphism of $\mathcal{E}$ corresponding to τ is just multiplication by the complex number τ (this means the map taking $x+\Lambda$ to $\tau x+\Lambda$; see Theorem VI.4.1 in [14]). Hence τS is the image under q of a finite union of lines parallel to the imaginary axis. Therefore the intersection of S and τS is finite and so is the intersection of $\mathcal{E}(\mathbb{R})$ and its image under τ. ∎

The key fact we use is the following special case of Faltings' Theorem (see [7]).

THEOREM 4.2. *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 $\mathcal{E}^n$.*

Now we are ready to prove that $\Delta^*(\mathbb{Q})$ has the Mordell–Lang property.

PROPOSITION 4.3. *The group $\Delta^*(\mathbb{Q})$ has the Mordell–Lang property.*

Proof. 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 kernels of maps of the form

$$(x_1,\dots,x_n)\mapsto k_1x_1\oplus\cdots\oplus k_nx_n : \mathcal{E}(\mathbb{Q})^n\to\mathcal{E}(\mathbb{Q}),$$

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

By the Mordell–Weil Theorem, $\mathcal{E}(\mathbb{Q})$ is indeed a finitely generated subgroup of the elliptic curve $\mathcal{E}$. So in the case that $\mathcal{E}$ does not have complex multiplication, Theorem 4.2 gives the desired result directly.

If $\mathcal{E}$ has complex multiplication, say by τ, then Lemma 4.1 implies that the cosets of the intersection of $\mathcal{E}(\mathbb{Q})^n$ an algebraic subgroup of $\mathcal{E}^n$ given as the kernel of a map of the form (4.2) 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). Hence the result follows again from Theorem 4.2. ∎

Proof of Theorem 1.1. Note that $\mathcal{C}$ from the introduction is just $\Delta^*(\mathbb{Q})$ without (c,d) and thus $(\mathbb{R},\mathcal{C})$ and $(\mathbb{R},\Delta^*(\mathbb{Q}))$ are quantifier-free interdefinable over $\emptyset$. Hence it suffices to prove Theorem 1.1 with $\Delta^*(\mathbb{Q})$ in place of $\mathcal{C}$.

If $\Delta^*(\mathbb{Q})$ is finite, then Theorem 1.1 is trivial. Hence we may assume that $\Delta^*(\mathbb{Q})$ is infinite. First note that Δ has either one or two connected components depending on whether the polynomial $p(X)=X^3+aX+b$ has one or three real roots. By the construction in [12, p. 247], the t-topology

on Δ^* is given by

$$\{Z \subseteq \Delta^* : g \oplus Z \cap \Delta \text{ is open for every } g \in \Delta^*\}.$$

One can easily check that the number of t-connected components of Δ^* coincides with the number of connected components of Δ. Since Δ^* can be embedded into $\mathbb{P}^2(\mathbb{C})$, Δ^* is t-compact. Let H be the t-connected component of Δ^* containing the identity of the group Δ^*. By [12, Corollary 2.10], H is definable. Since Δ^* has at most two t-connected components, the index of H in Δ^* is at most 2. Hence $H \cap \Delta^*(\mathbb{Q})$ is infinite since $\Delta^*(\mathbb{Q})$ is infinite. Since H is t-compact, t-connected and 1-dimensional, $H \cap \Delta^*(\mathbb{Q})$ is t-dense in H. Moreover, since H is a subgroup of Δ^* of finite index, the structures $(\mathbb{R}, H \cap \Delta^*(\mathbb{Q}))$ and $(\mathbb{R}, \Delta^*(\mathbb{Q}))$ are existentially interdefinable over $\emptyset$. Now H can be taken as $\mathbb{A}(\mathbb{R})$ of the previous section and $\Delta^*(\mathbb{Q}) \cap H$ as Γ (it is clear that $(\Delta^*(\mathbb{Q}) \cap H)/n(\Delta^*(\mathbb{Q}) \cap H)$ is finite for every $n > 0$). Therefore Theorem 1.1 follows immediately from Theorem 3.9. ∎

Also Theorem 3.8 takes the following form in this setting.

THEOREM 4.4. *Suppose that $\Delta^*(\mathbb{Q})$ is infinite. Let K be a real closed field and G be a subgroup of $\Delta^*(K)$ 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

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

if and only if

- $(K, (\pi(\delta'))_{\delta \in \Delta^*(\mathbb{Q})}) \equiv (\mathbb{R}, (\pi(\delta))_{\delta \in \Delta^*(\mathbb{Q})})$,
- *for every $n > 0$ and $g \in G$ we have $g \in \Delta'$ whenever $ng \in \Delta'$,*
- *for every $n > 0$, $|G/nG| = |\Delta'/n\Delta'|$,*
- *for every t-connected component Y of $\Delta(\mathbb{R})$,*

$$\Delta^*(\mathbb{Q}) \cap Y \text{ is dense in } Y \;\Leftrightarrow\; G \cap Y(K) \text{ is dense in } Y(K).$$

- *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 $\mathcal{R} = (R, <, +, \ldots)$ be an o-minimal expansion of a densely ordered abelian group in a language $\mathcal{L} = \{<, +, \ldots\}$ and let $T_{\mathcal{R}}$ be its theory. We say that a subset D of R^m is *small* if for every function $f : R^{mn} \to R$ definable in $\mathcal{R}$ and every interval $I \subseteq R$ we have $I \nsubseteq f(D^n)$. Note that for real closed fields this notion of smallness is equivalent to the notion defined in Section 2. Now take a small subset G of R^m. 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 is dcl-*independent*

over P if for every $b \in B$, the singleton $\{b\}$ is not definable in $\mathcal{M}$ over $\pi_1(P) \cup \cdots \cup \pi_m(P) \cup B \setminus \{b\}$. (Here and in the rest of the section we do not make a distinction between the relation symbol P and its interpretation; also for a subset A of M, we write $A \setminus P$ rather than $A \setminus (\pi_1(P) \cup \cdots \cup \pi_m(P))$.) 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

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

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

Definition 5.1. Let $\mathcal{A} = (A, <, \ldots)$ 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 $(A, (U))$, 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 $\mathcal{B}$.

The main result of this section is the following.

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

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

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

where x *is an* s*-tuple of distinct variables and* ϕ *is an* $\mathcal{L}$*-*M*-formula,*
(ii) *for every parameter set* B *such that* $B \setminus P$ *is* dcl*-independent over* P*, and for every set* $V \subseteq P^s$ *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 3.9 and Corollary 3.11, this result has the following consequence.

Corollary 5.3. *Let* $\mathbb{A}$ *and* Γ *be as in Section* 3*. If* Γ *is t-dense in* $\mathbb{A}(\mathbb{R})$*, 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 definable in the reduct of $\mathcal{A}$ to the language of T.*

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. We show that such a model $(\mathcal{M}, P)$ satisfies the second condition of Theorem 5.5.

After extending $\mathcal{L}$ by constants, we can assume that

(i′) every $\mathcal{L}$-$\emptyset$-definable set in M^s is a boolean combination of subsets of M^s defined by

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

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

In the following, B always refers to a finite parameter set such that $B \setminus P$ is dcl-independent over P. Indeed any definable set can be defined over such a B: say X is defined over a finite set A, then choose $A_0 \subseteq A \setminus P$ which is dcl-independent over P. Then X is definable over a finite subset B of $A_0 \cup P$ and it is clear that $B \setminus P$ is dcl-independent over P.

Clearly condition (ii) is equivalent to the following:

(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.

We begin with some technical results.

LEMMA 5.6. *Let $X \subseteq M^{mn}$ and $f : X \to M^k$ be definable in $\mathcal{M}$ over B and let $V \subseteq P^n$ 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 o-minimality of $\mathcal{M}$, there are definable subsets $X_1, \ldots, X_l$ of X such that $X = \bigcup_{i=1}^{l} X_i$ and f is continuous on X_i for $i = 1, \ldots, l$. Hence we can assume that 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. ∎

LEMMA 5.8. *Let $X \subseteq M$ be $\mathcal{L}(P)$-B-definable. Then X is a finite intersection of sets of the form*

$$f_1(D_1) \cup (M \setminus f_2(D_2)) \cup Y,$$

where for $i = 1, 2$, $f_i : M^{mn_i} \to M$ are $\mathcal{L}$-B-definable functions, $D_i \subseteq P^{n_i}$ are $\mathcal{L}(P)$-B-definable and $Y \subseteq M$ is $\mathcal{L}$-B-definable.

Proof. By condition (i′) of Theorem 5.2, X is a boolean combination of sets of the form

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

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

$$\{a \in M : h_1(u) < a < h_2(u) \text{ for some } u \in C\}, \tag{5.1}$$

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

where $f, h_1, h_2 : M^{mn} \to M$ are $\mathcal{L}$-B-definable functions and C, D are $\mathcal{L}(P)$-B-definable subset of P^n. After writing X in conjunctive normal form we get $X = \bigcap X_i$, where X_i is a finite union of sets of the form (5.1) or (5.2) and of sets whose complements are of of the form (5.1) or (5.2). Using the observation at the end of the first paragraph of this section, we may even assume that X_i is of the form

$$f_1(D_1) \cup (M \setminus f_2(D_2)) \cup \bigcup_j Y_j \cup (M \setminus Z_j),$$

where Y_j, Z_j are of the form (5.1), f_1, f_2 are $\mathcal{L}$-B-definable functions and D_1, D_2 are $\mathcal{L}(P)$-B-definable subsets of P^n. By Lemma 5.7, the set $\bigcup_j Y_j \cup (M \setminus Z_j)$ is $\mathcal{L}$-B-definable. Thus each X_i is of the form

$$f_1(D_1) \cup (M \setminus f_2(D_2)) \cup Y,$$

where Y is an $\mathcal{L}$-B-definable set. ∎

REMARK. By applying this lemma to the complement of X we deduce that X is a finite union of sets of the form

$$g_1(E_1) \cap (M \setminus g_2(E_2)) \cap Z,$$

where for $i = 1, 2$, $g_i : M^{mn_i} \to M$ are $\mathcal{L}$-B-definable functions, $E_i \subseteq P^{n_i}$ are $\mathcal{L}(P)$-B-definable and $Z \subseteq M$ is $\mathcal{L}$-B-definable.

PROPOSITION 5.9. *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 $(\mathcal{M}, P)$, say over B with $B \setminus P$ dcl-independent over P. By Lemma 5.8, there are sets $X_1, \ldots, X_l \subseteq M$ such that $X = \bigcap_{i=1}^{l} X_i$ and every X_i is of the form

$$f_1(D_1) \cup (M \setminus f_2(D_2)) \cup Y, \tag{5.3}$$

where f_1, f_2 are $\mathcal{L}$-B-definable functions, D_1, D_2 are $\mathcal{L}(P)$-B-definable subsets of P^n and Y is an $\mathcal{L}$-B-definable subset of M. Since X is open,

$$X = \bigcap_{i=1}^{l} \mathring{X}_i,$$

where $\mathring{X}_i$ is the interior of X_i. Hence it is only left to show that $\mathring{X}_i$ is definable in $\mathcal{M}$. It suffices to show that X_i is the union of a set S with empty interior and a set V definable in $\mathcal{M}$, because such a V is a finite union of intervals and points and S contributes only to the frontier of X_i. Hence the interior of X_i is the interior V.

Therefore, let X_i be of the form (5.3). Consider the set

$$D := \{u \in D_2 : f_2(u) \notin Y \cup f_1(D_1)\}.$$

By Lemma 5.6, there is an $\mathcal{L}$-B-definable set E such that D is dense in E and $f_2(D)$ is dense in $f_2(E)$. Hence by (5.3) we get

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

By smallness of P, $f_1(D_1)$ has empty interior. Since $f_2(D)$ is dense in $f_2(E)$, the set $f_2(E) \setminus f_2(D)$ has empty interior as well. Since $f_1(D_1) \cap f_2(D)$ is empty, the intersection $f_2(E) \cap f_1(D_1)$ is a subset of $f_2(E) \setminus f_2(D)$. Hence $f_1(D_1) \cup (f_2(E) \setminus f_2(D))$ has empty interior, since $f_2(E)$ is a finite union of intervals and points. Thus X_i is a union of a set with empty interior and a set definable in $\mathcal{M}$. ∎

PROPOSITION 5.10. *Every cofinitely continuous $\mathcal{L}(P)$-definable unary function is $\mathcal{L}$-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 $\mathcal{L}(P)$-B-definable, where $B \setminus P$

is dcl-independent over P. Take $a \in M$ such that $(\{a\} \cup B) \setminus P$ is dcl-independent over P. Denote the set of such elements by W. Note that W is $\mathcal{L}(P)$-type-definable, since it is the intersection of all sets of the form

$$M \setminus \{f(d_1, \ldots, d_n) : d_1, \ldots, d_n \in P\}$$

where $n \in \mathbb{N}$ and $f : M^{mn} \to M$ is an $\mathcal{L}$-$\emptyset$-definable function. By saturation and smallness of P, W is dense in M.

First, we will show that $f(a)$ is $\mathcal{L}$-B-definable over a. By the remark after Lemma 5.8, the singleton set $\{f(a)\}$ is of the form

$$f_1(D_1) \cap (M \setminus f_2(D_2)) \cap Y,$$

where f_1, f_2 are $\mathcal{L}$-$(B \cup \{a\})$-definable functions, D_1, D_2 are $\mathcal{L}(P)$-$(B \cup \{a\})$-definable subsets of P^n, and Y is an $\mathcal{L}$-$(B \cup \{a\})$-definable subset of M. Define D to be the set

$$\{u \in D_1 : f_1(u) \in Y \setminus f_2(D_2)\}.$$

Note that $f_1(D) = f_1(D_1) \cap (M \setminus f_2(D_2)) \cap Y$ and hence $f_1(D) = \{f(a)\}$. By Lemma 5.6, there is an $\mathcal{L}$-$(B \cup \{a\})$-definable set E such that D is dense in E and $f_1(D)$ is dense in $f_1(E)$. Since $f_1(D)$ is a singleton, it equals $f_1(E)$ and hence $f(a)$ is $\mathcal{L}$-$(B \cup \{a\})$-definable.

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 the monotonicity theorem for 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 distance 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 an $\mathcal{L}$-B-definable function. ∎

Now Theorem 5.2 follows directly from Theorem 5.5 in combination with Propositions 5.9, 5.10.

Remark. As a consequence of Theorem 5.2, we take care of an unfinished business from [9]. Namely we can simplify Theorem 1.3 of that paper in the case when the predicate is dense by removing the assumption (iii), since it follows from the first two assumptions using Theorem 5.2.

Subgroups of the unit circle. Let Γ be a subgroup of the unit circle $\mathbb{S}$ of finite rank. Note that if Γ is finite, then Theorem 1.3 is trivial, so we assume that it is infinite. Then Γ is t-dense in $\mathbb{S}$ and Γ has the Mordell–Lang property by [11, Theorem 2]. It is also clear that $|\Gamma/\Gamma^{[n]}|$ is finite for every $n > 0$. Therefore Theorem 1.3 follows from Corollary 5.3.

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 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. We also thank the referee for many very detailed comments, as they helped us a lot to improve the paper.

The second author was supported by Deutscher Akademischer Austausch Dienst.

References

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

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

[3] A. Dolich, C. Miller, and C. Steinhorn, *Structures having o-minimal open core*, Trans. Amer. Math. Soc. 362 (2010), 1371–1411.

[4] L. van den Dries, *Tame Topology and o-Minimal Structures*, London Math. Soc. Lecture Note Ser. 248, Cambridge Univ. Press, Cambridge, 1998.

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

[6] M. J. Edmundo and M. Otero, *Definably compact abelian groups*, J. Math. Logic 4 (2004), 163–180.

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

[8] A. Günaydın, *Model theory of fields with multiplicative groups*, PhD thesis, Univ. of Illinois at Urbana-Champaign, 2008.

[9] A. Günaydın and P. Hieronymi, *Dependent pairs*, J. Symbolic Logic, to appear.

[10] S. Lang, *Number Theory. III*, Encyclopaedia Math. Sci. 60, Springer, Berlin, 1991.

[11] M. Laurent, *Équations exponentielles-polynômes et suites récurrentes linéaires. II*, J. Number Theory 31 (1989), 24–53.

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

[13] —, *Geometric Stability Theory*, Oxford Logic Guides 32, Oxford Univ. Press, New York, 1996.

[14] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1992.

[15] B. Zilber, *Complex roots of unity on the real plane*, www.maths.ox.ac.uk/˜zilber, 2003.

Ayhan Günaydın
Centro de Matemática
e Aplicações Fundamentais
Av. Prof. Gama Pinto, 2
1649-003 Lisboa, Portugal
E-mail: ayhan@ptmat.fc.ul.pt

Philipp Hieronymi
Department of Mathematics & Statistics
McMaster University
1280 Main Street West
Hamilton, ON, L8S 4K1, Canada
Current address:
Department of Mathematics
University of Illinois
1409 W. Green Street
Urbana, IL 61801, U.S.A.
E-mail: P@hieronymi.de

Received 3 June 2009;
in revised form 13 August 2010