

THE FIELDS OF REAL AND COMPLEX NUMBERS WITH A SMALL MULTIPLICATIVE GROUP

LOU VAN DEN DRIES AND AYHAN GÜNAYDIN

1. INTRODUCTION

Let $(\mathbb{R}, 2^{\mathbb{Z}})$ be the the *field* of real numbers with the multiplicative group of powers of 2. The elementary theory of $(\mathbb{R}, 2^{\mathbb{Z}})$ was determined in [3], with simple valuation theory as the main tool, and [3] also shows that in $(\mathbb{R}, 2^{\mathbb{Z}})$, each definable relation is a boolean combination of existentially definable relations. But multiplicative groups like $2^{\mathbb{Q}} \subseteq \mathbb{R}^{>0}$ and $2^{\mathbb{Z}}3^{\mathbb{Z}} \subseteq \mathbb{R}^{>0}$ could not be handled in this way. Using Mann [12], Zilber [21] axiomatized (\mathbb{C}, \mathbb{U}) where \mathbb{U} is the multiplicative group of roots of unity in the field \mathbb{C} of complex numbers. In [22] he showed that in (\mathbb{R}, \mathbb{U}) each definable relation is a boolean combination of existentially definable relations.

Here we extend these results to all multiplicative groups in \mathbb{C} and \mathbb{R} of *finite rank*. (The *rank* of an abelian group G is the dimension of the \mathbb{Q} -vector space $G \otimes \mathbb{Q}$, where G is viewed as \mathbb{Z} -module and the tensor product is that of \mathbb{Z} -modules. So the groups $2^{\mathbb{Z}}$, $2^{\mathbb{Q}}$, $2^{\mathbb{Z}}3^{\mathbb{Z}}$, \mathbb{U} have ranks 1, 1, 2, 0.)

A fundamental fact about these multiplicative groups of finite rank is that they have the **Mann Property**. To define this property, let K be a field and G a subgroup of its multiplicative group K^{\times} . Consider an equation

$$(*) \quad a_1x_1 + \cdots + a_nx_n = 1$$

with $n \geq 2$ and *nonzero* coefficients a_1, \dots, a_n in the *prime field* of K . A *solution* of $(*)$ in G is a tuple $(g_1, \dots, g_n) \in G^n$ such that

$$a_1g_1 + \cdots + a_ng_n = 1,$$

and a *nondegenerate* solution of $(*)$ in G is a solution (g_1, \dots, g_n) of $(*)$ in G such that $\sum_{i \in I} a_i g_i \neq 0$ for each nonempty subset I of $\{1, \dots, n\}$. We say that G has the *Mann property* (in K) if every equation $(*)$ has only finitely many nondegenerate solutions in G . We call it by this name because Mann [12] showed that \mathbb{U} has the Mann property in \mathbb{C} . Some twenty years later came the proof of the deeper theorem that any multiplicative group of finite rank in any field of characteristic 0 has the Mann property; see [17], [6], [10]. Mann's proof, however, has the virtue of being effective: for any equation $(*)$ with rational a_i it constructs all nondegenerate solutions in \mathbb{U} .

Our results concern mainly the model theory of structures (K, G) where K is algebraically closed or real closed, and where G is only assumed to have

Date: August 2005.

the Mann property, with “finite rank” as a special case. (A natural example of infinite rank is $(\mathbb{C}, \exp A)$ where $A \subseteq \mathbb{C}$ is the field of algebraic numbers.) Here are precise statements of some of these results.

Proposition 1.1. *For algebraically closed K , the following are equivalent:*

- (1) *G has the Mann Property;*
- (2) *for every algebraic set $V \subseteq K^n$ its trace $V \cap G^n$ is a finite union of cosets of subgroups of G^n ;*
- (3) *for every $X \subseteq K^n$ that is definable in (K, G) its trace $X \cap G^n$ is definable in the group G .*

Speaking informally, this result says that, for G , the Mann Property and the *Mordell-Lang property* are equivalent; in this connection, see also Pillay [15]. The subgroups of G^n in (2) come from a finite collection of subgroups of G^n that can be specified in advance in terms of n and a bound on the degree of the polynomials that define V ; see Section 5 for details.

In (3) we view (K, G) as an $\mathcal{L}(U)$ -structure where \mathcal{L} is the language of rings and U is a unary relation symbol whose interpretation in the structure (K, G) is the subset G of K .

Let Γ be a subgroup of \mathbb{C}^\times with the Mann property. In order to describe the elementary theory of (\mathbb{C}, Γ) we add a *name* for each $\gamma \in \Gamma$, and for convenience we denote this name also by γ . For each equation

$$a_1x_1 + \cdots + a_nx_n = 1 \quad (n \geq 2, a_1, \dots, a_n \in \mathbb{Q}^\times)$$

take a finite list of its nondegenerate solutions in Γ ,

$$\gamma_1 = (\gamma_{11}, \dots, \gamma_{1n}), \dots, \gamma_k = (\gamma_{k1}, \dots, \gamma_{kn}),$$

and let the corresponding *Mann axiom* of Γ be the sentence

$$\forall y \left[(U(y) \wedge \sum_{i=1}^n a_i y_i = 1 \wedge \bigwedge_I \sum_{i \in I} a_i y_i \neq 0) \longrightarrow \bigvee_{j=1}^k y = \gamma_j \right]$$

in the language $\mathcal{L}(U)$ with names for the elements of Γ , where $y = (y_1, \dots, y_n)$ is a tuple of distinct variables, $U(y)$ abbreviates $U(y_1) \wedge \cdots \wedge U(y_n)$, the conjunction \bigwedge_I is over all nonempty $I \subseteq \{1, \dots, n\}$, “ $\sum_{i=1}^n a_i y_i = 1$ ” and “ $\sum_{i \in I} a_i y_i \neq 0$ ” represent certain obvious formulas in the language of rings, and $y = \gamma_j$ abbreviates $y_1 = \gamma_{j1} \wedge \cdots \wedge y_n = \gamma_{jn}$. We view $(\mathbb{C}, \Gamma, (\gamma)_{\gamma \in \Gamma})$ as a structure for the language $\mathcal{L}(U)$ with names for the elements of Γ . The following yields a complete axiomatization of the elementary theory of $(\mathbb{C}, \Gamma, (\gamma)_{\gamma \in \Gamma})$.

Theorem 1.2. *Let K be an algebraically closed field of characteristic 0, let G be a subgroup of K^\times , and let a map $\gamma \mapsto \gamma' : \Gamma \rightarrow G$ be given. Then $(K, G, (\gamma')_{\gamma \in \Gamma}) \equiv (\mathbb{C}, \Gamma, (\gamma)_{\gamma \in \Gamma})$ if and only if*

- $(G, (\gamma')_{\gamma \in \Gamma}) \equiv (\Gamma, (\gamma)_{\gamma \in \Gamma})$ as groups with distinguished elements;
- $(K, G, (\gamma')_{\gamma \in \Gamma})$ satisfies the Mann axioms of Γ .

This theorem is proved in a stronger form in Section 6, where we also describe the definable sets of (K, G) , and show that various stability conditions on the group G are inherited by (K, G) .

To state analogous results with \mathbb{R} instead of \mathbb{C} we define for any abelian multiplicatively written group G and positive integer d ,

$$G^{[d]} := \{g^d : g \in G\} \quad (\text{its subgroup of } d^{\text{th}} \text{ powers}),$$

with the corresponding elementary invariant

$$[d]G := \begin{cases} |G/G^{[d]}| & \text{if } G/G^{[d]} \text{ is finite,} \\ \infty & \text{otherwise.} \end{cases}$$

Let Γ be a dense subgroup of the positive multiplicative group $\mathbb{R}^{>0}$ of \mathbb{R} , and suppose Γ has the Mann property. We consider (\mathbb{R}, Γ) as a structure for the language $\mathcal{L}_o(U)$ of ordered rings with a unary relation symbol U , and construe $(\mathbb{R}, \Gamma, (\gamma)_{\gamma \in \Gamma})$ as a structure for the language $\mathcal{L}_o(U)$ augmented by names for the elements of Γ . In Section 7 we prove:

Theorem 1.3. *Let K be a real closed ordered field, let G be a dense subgroup of $K^{>0}$, and let a group homomorphism $\gamma \mapsto \gamma' : \Gamma \rightarrow G$ be given. Then $(K, G, (\gamma')_{\gamma \in \Gamma}) \equiv (\mathbb{R}, \Gamma, (\gamma)_{\gamma \in \Gamma})$ if and only if*

- for each $\gamma \in \Gamma$ and each prime number p , if γ is not a p^{th} power in Γ , then γ' is not a p^{th} power in G ;
- $[p]G = [p]\Gamma$ for each prime number p ;
- for all $a_1, \dots, a_n \in \mathbb{Z}$ and $\gamma_1, \dots, \gamma_n \in \Gamma$,

$$a_1\gamma_1 + \dots + a_n\gamma_n > 0 \iff a_1\gamma'_1 + \dots + a_n\gamma'_n > 0 ;$$

- $(K, G, (\gamma')_{\gamma \in \Gamma})$ satisfies the Mann axioms of Γ .

We also include results about the definable sets in (\mathbb{R}, Γ) and the induced structure on Γ when Γ is divisible.

In Section 8 we indicate cases where the Mann property holds effectively, with decidability of some of the above theories as a consequence. One such case is $\tau(\mathbf{k}^\times)$ where $\tau : \mathbf{k} \rightarrow W[\mathbf{k}]$ is the Teichmüller character of a perfect field \mathbf{k} of characteristic $p > 0$; this relates to an issue left over from [5]. We discuss the positive characteristic case at the end of Section 8.

Originally we also planned to include results on (\mathbb{R}, Γ) where Γ is a subgroup of \mathbb{C}^\times with the Mann property. (Here \mathbb{C} is identified with \mathbb{R}^2 in the usual way so that Γ becomes a binary relation on \mathbb{R} .) But we were informed that the case of main interest, where Γ is a subgroup of the unit circle, will be treated in a paper by O. Belegradek and B. Zilber; see also [22] for $\Gamma = \mathbb{U}$. Their interest in this topic is connected with an attempt to understand quantum tori model-theoretically. To minimize overlap and because we were not aware of this connection, we decided not to execute this plan.

We thank Alex Berenstein, Clifton Ealy, David Marker, Chris Miller, Anand Pillay, and Boris Zilber for discussions related to this paper.

Conventions, Notations, and two Facts. Throughout, m and n (sometimes subscripted) range over $\mathbb{N} = \{0, 1, 2, \dots\}$. “Definable” will mean “definable with parameters” unless indicated otherwise. We let $|X|$ denote the cardinality of a set X . Given sets X and Y we write

$$f : X \xrightarrow{n} Y$$

to indicate that f is a map from X to the power set of Y such that $|f(x)| \leq n$ for all $x \in X$. For such an f its *graph* is by definition the set

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

and for $S \subseteq X$ we put $f(S) := \bigcup_{x \in S} f(x)$. If X and Y are definable in a structure \mathcal{M} , then such an f is said to be definable in \mathcal{M} if its graph is.

In Section 4 the notion of a *positive formula* becomes relevant. To define it we specify our logical symbols to be the nullary relation symbols \top and \perp (for “true” and “false”, respectively), in addition to the usual connectives \neg, \wedge, \vee , the quantifiers \exists, \forall , and the binary relation symbol $=$.

We now define *positive formulas* to be formulas that do not contain the negation symbol \neg ; they may contain \perp .

To prove that in certain theories the formulas are equivalent to formulas of a very special form we shall sometimes use the following consequence of the Stone representation theorem.

Fact 1. Let B be a boolean algebra and $S(B)$ its Stone space of ultrafilters. Let $\Psi \subseteq B$ and suppose that the map $F \mapsto F \cap \Psi : S(B) \rightarrow \mathcal{P}(\Psi)$ is injective. Then Ψ generates B as a boolean algebra.

From field theory we shall use the notions of *linear disjointness*, *freeness*, and *regular extension*, in particular the following result from [9], p. 367.

Fact 2. Let E, K, L be subfields of a field Ω such that $E \subseteq K, E \subseteq L$, and K is a regular extension of E . If K and L are free over E , then they are linearly disjoint over E .

If K is a field, then K^{ac} is its algebraic closure in the field theoretic sense. If K is an ordered field, then K^{rc} is its real closure.

Let $\mathcal{M} = (M, \dots)$ be a structure and $A \subseteq M$. Then $\text{acl}(A) \subseteq M$ is the model-theoretic algebraic closure of A in \mathcal{M} . If $\mathcal{A} = (A, \dots)$ is a substructure of \mathcal{M} , then $\text{acl}(\mathcal{A})$ is the substructure of \mathcal{M} with underlying set $\text{acl}(A)$.

2. SMALL SETS IN A STRUCTURE

This section resembles Section 1 of [4]. In the background is the fact (Lemma 6.1) that if a multiplicative group G in an algebraically closed field K has the Mann property, then G is *small* in K in a certain technical sense. Here we treat this notion of smallness in a general model-theoretic setting.

Below, \mathcal{L} is a language, $\mathcal{M} = (M, \dots)$ is an \mathcal{L} -structure, and $G \subseteq M$. If $f(G^m) = M$ for some m, n and some $f : M^m \xrightarrow{n} M$ definable in \mathcal{M} , we call

G large in \mathcal{M} , and otherwise we call G small in \mathcal{M} . In particular, if M is infinite and $|G| < |M|$, then G is small in \mathcal{M} . We also say that a set $S \subseteq M$ is G -bound (in \mathcal{M}) if $S \subseteq f(G^m)$ for some m, n and some $f : M^m \xrightarrow{n} M$ definable in \mathcal{M} . Note that the union of two G -bound sets is again G -bound, and that if $f : M^m \xrightarrow{n} M$ is definable in \mathcal{M} and $S_1, \dots, S_m \subseteq M$ are G -bound, then $f(S_1 \times \dots \times S_m)$ is G -bound. (It came to our attention that Casanovas and Ziegler [2] have another notion of *small*. It is easy to see that their notion is equivalent to ours for strongly minimal \mathcal{M} .)

We use many-valued functions in these definitions because the proof of Lemma 2.2 below would not work with single-valued functions. However, see Lemma 2.4 for the case of algebraically closed fields.

Lemma 2.1. *If G is small in \mathcal{M} and $b \in M$, then $G \cup \{b\}$ is small in \mathcal{M} .*

Proof. Let $b \in M \setminus G$ and fix some m . For $I \subseteq \{1, \dots, m\}$, put

$$G(I) := \{(a_1, \dots, a_m) \in (G \cup \{b\})^m : a_i \in G \text{ for } i \in I, a_j = b \text{ for } j \notin I\},$$

so there is a definable bijection between $G(I)$ and $G^{|I|}$, and

$$(G \cup \{b\})^m = \bigcup_{I \subseteq \{1, \dots, m\}} G(I).$$

Hence, if $f : M^m \xrightarrow{n} M$ is definable in \mathcal{M} , then

$$f((G \cup \{b\})^m) = \bigcup_I f(G(I))$$

is clearly G -bound. □

Let U be a new unary relation symbol, and consider the $\mathcal{L}(U)$ -structure (\mathcal{M}, G) . Smallness is a first-order property in the language $\mathcal{L}(U)$: there is a set of $\mathcal{L}(U)$ -sentences whose models are exactly the $\mathcal{L}(U)$ -structures (\mathcal{M}, G) such that G is small in \mathcal{M} . Thus if G is small in \mathcal{M} , and the $\mathcal{L}(U)$ -structures (\mathcal{M}, G) and (\mathcal{M}', G') are elementarily equivalent, then G' is small in \mathcal{M}' .

Lemma 2.2. *Suppose G is small in \mathcal{M} , and the $\mathcal{L}(U)$ -structure (\mathcal{M}, G) is κ -saturated where $\kappa > |\mathcal{L}|$. Then:*

- (1) *Suppose $(S_i)_{i \in I}$ is a family of G -bound subsets of M with $|I| < \kappa$. Then $\bigcup_{i \in I} S_i$ is small in \mathcal{M} .*
- (2) *Suppose $S \subseteq M$ and $|S| < \kappa$. Then $\text{acl}(G \cup S)$ is small in \mathcal{M} .*
- (3) *There is a sequence $(b_\alpha)_{\alpha < \kappa}$ in M such that no b_γ is algebraic over $G \cup \{b_\alpha : \alpha < \gamma\}$ in \mathcal{M} .*

Proof. For (1), we can assume towards a contradiction that $f : M^m \xrightarrow{n} M$ is definable in \mathcal{M} and $M = f((\bigcup_i S_i)^m)$, with each S_i of the form $g_i(G^{m_i})$ for some $g_i : M^{m_i} \xrightarrow{n_i} M$ definable in \mathcal{M} . Then $M = \bigcup f(S_{i(1)} \times \dots \times S_{i(m)})$ where the union is over all tuples $(i(1), \dots, i(m)) \in I^m$. Since each set

$f(S_{i(1)} \times \cdots \times S_{i(m)})$ is definable in (\mathcal{M}, G) , it follows by the κ -saturation of (\mathcal{M}, G) that there is a finite $J \subseteq I^m$ such that

$$M = \bigcup_{(i(1), \dots, i(m)) \in J} f(S_{i(1)} \times \cdots \times S_{i(m)}),$$

so M would be G -bound.

Now (2) follows from (1) by noting that

$$\text{acl}(G \cup S) = \bigcup_{m, n, f} f(G^m)$$

where the union is over all m, n, f with $f : M^m \xrightarrow{n} M$ definable in \mathcal{M} over S . Property (3) follows by an obvious transfinite construction using the previous lemma and (2). \square

We can now generalize a theorem of Keisler [8]:

Proposition 2.3. *Let T be an \mathcal{L} -theory with QE whose models are infinite and strongly minimal. Let \mathcal{M} and \mathcal{N} be models of T with substructures $\mathcal{G} = (G, \dots)$ and $\mathcal{H} = (H, \dots)$, such that*

- (i) G is small in \mathcal{M} and H is small in \mathcal{N} ;
- (ii) $\mathcal{G} \equiv \mathcal{H}$ and $\mathcal{M} \equiv \mathcal{N}$.

Then $(\mathcal{M}, G) \equiv (\mathcal{N}, H)$.

Proof. First some easy observations. Let $i : \mathcal{C} \cong \mathcal{D}$ be an isomorphism between substructures \mathcal{C} of \mathcal{M} and \mathcal{D} of \mathcal{N} . Then

- (a) i extends to an isomorphism $\text{acl}(\mathcal{C}) \cong \text{acl}(\mathcal{D})$;
- (b) if $x \in M \setminus \text{acl}(\mathcal{C})$ and $y \in N \setminus \text{acl}(\mathcal{D})$, then i extends to an isomorphism $\text{acl}(\mathcal{C})(x) \cong \text{acl}(\mathcal{D})(y)$ that sends x to y .

If the proposition is true for all countable \mathcal{L} , then it is clearly true for all \mathcal{L} , so we assume in the rest of the proof that \mathcal{L} is countable. With this assumption it is harmless to assume also CH, so we can reduce to the case that (\mathcal{M}, G) and (\mathcal{N}, H) are saturated and of cardinality \aleph_1 . Then \mathcal{G} and \mathcal{H} are \aleph_1 -saturated, and thus either both finite, or both of cardinality \aleph_1 . So we have an isomorphism $e : \mathcal{G} \cong \mathcal{H}$. Take a basis X of \mathcal{M} over G , and a basis Y of \mathcal{N} over H . By (3) of the previous lemma we have $|X| = |Y| = \aleph_1$. Hence by the observations at the beginning of the proof we can extend e to an isomorphism $\mathcal{G}(X) \cong \mathcal{H}(Y)$, and such an isomorphism extends to an isomorphism $\text{acl}(\mathcal{G}(X)) = \mathcal{M} \cong \text{acl}(\mathcal{H}(Y)) = \mathcal{N}$. This last isomorphism is an isomorphism $(\mathcal{M}, G) \cong (\mathcal{N}, H)$. \square

The proof yields more: Let the language \mathcal{L}^* extend \mathcal{L} by relation symbols and constant symbols. With the assumptions of the proposition, assume that \mathcal{G}^* and \mathcal{H}^* are \mathcal{L}^* -expansions of \mathcal{G} and \mathcal{H} such that $\mathcal{G}^* \equiv \mathcal{H}^*$. Then $(\mathcal{M}, \mathcal{G}^*) \equiv (\mathcal{N}, \mathcal{H}^*)$ as $\mathcal{L}^*(U)$ -structures.

If \mathcal{M} is an algebraically closed field, then the many-valued functions in the definition of “small” can be replaced by ordinary functions:

Lemma 2.4. *Let K be an algebraically closed field and suppose $G \subseteq K$ is large in K . Then there is a function $F : K^\ell \rightarrow K$, definable in K , such that $F(G^\ell) = K$.*

Proof. Take $f : K^m \xrightarrow{n} K$ definable in K such that $f(G^m) = K$. We can easily arrange that $|f(a)| = n$ for all $a \in K^m$. Let $\sigma_1, \dots, \sigma_n$ be the elementary symmetric polynomials in n indeterminates, and define $f_i : K^m \rightarrow K$ by $f_i(a) = \sigma_i(b_1, \dots, b_n)$ where $f(a) = \{b_1, \dots, b_n\}$. Then there is for each $b \in K$ an $a \in G^m$ such that $b^n + f_1(a)b^{n-1} + \dots + f_n(a) = 0$. Let E be the subfield of K generated by $f_1(G^m) \cup \dots \cup f_n(G^m)$. Then by the above, each $b \in K$ is separably algebraic of degree $\leq n$ over E , and thus $[K : E] \leq n$. By mimicking how E is generated by addition, multiplication, and division from $f_1(G^m) \cup \dots \cup f_n(G^m)$, and using a (finite) basis of K as vector space over E , we obtain functions $F_i : K^{m_i} \rightarrow K$, each definable in K , with i ranging over a countable index set I , such that

$$K = \bigcup_{i \in I} F_i(G^{m_i}).$$

We could have assumed from the outset of this proof that (K, G) is \aleph_1 -saturated, so that $K = \bigcup_{i \in I_0} F_i(G^{m_i})$ for a finite subset I_0 of I . The finitely many functions F_i with $i \in I_0$ easily yield a single function $F : K^\ell \rightarrow K$ as desired. \square

Remark. Suppose F is a subfield of the algebraically closed field K . Then F is large in K if and only if $F = K$, or F is a real closed field and $[K : F] = 2$. This follows from a theorem of E. Artin; see Lemma 3.1 in [8].

3. ALGEBRAICALLY CLOSED FIELDS WITH A MULTIPLICATIVE SET

From now on in this paper $\mathcal{L} = \{0, 1, +, -, \cdot\}$ is the language of rings. We shall also use its sublanguange $\mathcal{L}_m := \{1, \cdot\}$ of multiplicative monoids.

Throughout this section K is an algebraically closed field, with prime field \mathbb{F} , and G is a *multiplicative set in K* , that is, G is a subset of K that contains 1 and is closed under multiplication. (For example, any subring of K is a multiplicative set in K .) We consider G as an \mathcal{L}_m -structure in the obvious way. The *addition* of K also leaves a trace on G , and to deal with that we extend \mathcal{L}_m to the language

$$\mathcal{L}_m(\Sigma) := \{1, \cdot\} \cup \{\Sigma_k : k \in \mathbb{Z}^n, n = 1, 2, \dots\}$$

of *multiplicative monoids with additive relations*: here Σ_k is an n -ary relation symbol for $k = (k_1, \dots, k_n) \in \mathbb{Z}^n$. We expand the monoid G to an $\mathcal{L}_m(\Sigma)$ -structure $G(\Sigma)$ by interpreting Σ_k as the n -ary relation

$$\{(g_1, \dots, g_n) \in G^n : k_1 g_1 + \dots + k_n g_n = 0\}$$

on G . As a special case of Proposition 2.3 we have:

Corollary 3.1. *If G is small in K , then $\text{Th}(K, G)$ is completely determined by $\text{Th}(G(\Sigma))$.*

In other words, if G is small in K , and H is a small multiplicative set in an algebraically closed field L , then

$$(K, G) \equiv (L, H) \iff G(\Sigma) \equiv H(\Sigma).$$

To see how this follows from 2.3, note that algebraically closed fields can be construed as $\mathcal{L}_m(\Sigma)$ -structures, that their theory in this language admits QE, and that the substructures of an algebraically closed field L viewed as $\mathcal{L}_m(\Sigma)$ -structure are exactly the structures $H(\Sigma)$ where H is a multiplicative set in L . Also, the characteristic of an algebraically closed field is determined by the sentences $\Sigma_k(1)$ that it satisfies where $1 \leq k \in \mathbb{Z} = \mathbb{Z}^1$.

In the next result G is not assumed to be small in K .

Proposition 3.2. *Every subset of G^n definable in (K, G) is definable in the structure $G(\Sigma)$.*

Proof. Take a $|K|^+$ -saturated elementary extension (K', G') of (K, G) . Then K and $\mathbb{F}(G')$ are linearly disjoint over $\mathbb{F}(G)$. Let $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$ be in $(G')^n$ such that

$$\text{tp}_{G'(\Sigma)}(\alpha|G) = \text{tp}_{G'(\Sigma)}(\beta|G).$$

By Fact 1, it suffices to prove that then $\text{tp}_{(K', G')}(\alpha|K) = \text{tp}_{(K', G')}(\beta|K)$. The assumption on α and β gives an automorphism f of $G'(\Sigma)$ over G that takes α to β . As f preserves the Σ_k 's, it extends to a field automorphism of $\mathbb{F}(G')$ over $\mathbb{F}(G)$. By linear disjointness the latter extends to a field automorphism of $K(G')$ over K , and hence to an automorphism of K' over K . Therefore $\text{tp}_{(K', G')}(\alpha|K) = \text{tp}_{(K', G')}(\beta|K)$ as desired. \square

Remarks.

- (1) The proposition deals with a special case of the situation considered in Proposition 3.1 of [15], but is a bit stronger in that special case.
- (2) In case G is a subring of K , Proposition 3.2 says that the subsets of G^n definable in (K, G) are definable in the ring G .
- (3) The proposition fails badly when K is replaced by the field \mathbb{R} . For example, *every* subset of \mathbb{Z} is definable in (\mathbb{R}, \mathbb{Z}) . Also, $2^{\mathbb{Z}}3^{\mathbb{Z}}$ has the Mann property, but is dense in $\mathbb{R}^{>0}$, so has uncountably many subsets that are definable in $(\mathbb{R}, 2^{\mathbb{Z}}3^{\mathbb{Z}})$.

Lemma 3.3. *Let G' be a multiplicative subset of G such that $G'(\Sigma)$ is existentially closed in $G(\Sigma)$. Then $G \cap \mathbb{F}(G') = G'$ and $\mathbb{F}(G)$ is a regular extension of $\mathbb{F}(G')$.*

Proof. Let $g \in G \cap \mathbb{F}(G')$. Then

$$g = \frac{k_1 h_1 + \dots + k_n h_n}{\ell_1 h_1 + \dots + \ell_n h_n} \quad (n \geq 1)$$

where $k_1, \dots, k_n, \ell_1, \dots, \ell_n \in \mathbb{Z}$, $h_1, \dots, h_n \in G'$, $\ell_1 h_1 + \dots + \ell_n h_n \neq 0$. This expression for g yields

$$G(\Sigma) \models \Sigma_{k, -\ell}(h_1, \dots, h_n, gh_1, \dots, gh_n)$$

where $k, -\ell$ denotes the tuple $(k_1, \dots, k_n, -\ell_1, \dots, -\ell_n) \in \mathbb{Z}^{2n}$. Existential closedness gives $g' \in G'$ such that

$$G'(\Sigma) \models \Sigma_{k, -\ell}(h_1, \dots, h_n, g'h_1, \dots, g'h_n).$$

This in turn yields $g = g'$. Thus $G \cap \mathbb{F}(G') = G'$, as promised.

Next, let $a \in \mathbb{F}(G)$ be algebraic over $\mathbb{F}(G')$. We claim that then $a \in \mathbb{F}(G')$. To see this, let $X^m + c_1X^{m-1} + \dots + c_m$ with $c_1, \dots, c_m \in \mathbb{F}(G')$ be the minimum polynomial of a over $\mathbb{F}(G')$. We have

$$c_i = \frac{k_{i1}h_1 + \dots + k_{in}h_n}{k_1h_1 + \dots + k_nh_n} \quad (i = 1, \dots, m)$$

for suitable $n \geq 1$ and $k_1, \dots, k_n, k_{i1}, \dots, k_{in} \in \mathbb{Z}$ and $h_1, \dots, h_n \in G'$, with $k_1h_1 + \dots + k_nh_n \neq 0$. By taking n large enough we can also assume

$$a = \frac{\ell'_1g_1 + \dots + \ell'_ng_n}{\ell_1g_1 + \dots + \ell_ng_n}$$

where $\ell_1, \dots, \ell_n, \ell'_1, \dots, \ell'_n \in \mathbb{Z}$, $g_1, \dots, g_n \in G$, and $\ell_1g_1 + \dots + \ell_ng_n \neq 0$. Substituting these expressions in the equality $a^m + c_1a^{m-1} + \dots + c_m = 0$, clearing denominators, and multiplying out, this equality leads to

$$G(\Sigma) \models \theta(g_1, \dots, g_n, h_1, \dots, h_n)$$

where $\theta(x_1, \dots, x_n, y_1, \dots, y_n)$ is a certain atomic $\mathcal{L}_m(\Sigma)$ -formula. This gives $g'_1, \dots, g'_n \in G'$ such that, with $\ell = (\ell_1, \dots, \ell_n)$:

$$G'(\Sigma) \models \neg \Sigma_\ell(g'_1, \dots, g'_n) \wedge \theta(g'_1, \dots, g'_n, h_1, \dots, h_n),$$

which in turn yields an element

$$a' := \frac{\ell'_1g'_1 + \dots + \ell'_ng'_n}{\ell_1g'_1 + \dots + \ell_ng'_n}$$

in $\mathbb{F}(G')$ such that $a'^m + c_1a'^{m-1} + \dots + c_m = 0$, so $m = 1$ and $a = a'$.

We are done in case K has characteristic 0. Suppose K has characteristic $p > 0$, so $\mathbb{F} = \mathbb{F}_p$. It remains to show that then the subfields $\mathbb{F}(G)^p$ and $\mathbb{F}(G')$ of $\mathbb{F}(G)$ are linearly disjoint over $\mathbb{F}(G')^p$. Let $c_1, \dots, c_m \in \mathbb{F}(G')$ be linearly dependent over $\mathbb{F}(G)^p$, so $a_1^p c_1 + \dots + a_m^p c_m = 0$ where $a_1, \dots, a_m \in \mathbb{F}(G)$ are not all zero. It suffices to obtain $a'_1, \dots, a'_m \in \mathbb{F}(G')$, not all zero, such that $a_1^p c_1 + \dots + a_m^p c_m = 0$. This is done along the same lines as we proved that $\mathbb{F}(G')$ is algebraically closed in $\mathbb{F}(G)$. \square

Back-and-forth. Suppose that G is small in K and the $\mathcal{L}(U)$ -structure (K, G) is κ -saturated where κ is uncountable. Let $\text{Sub}(K, G)$ be the collection of $\mathcal{L}(U)$ -structures (K', G') where K' is an algebraically closed subfield of K of cardinality $< \kappa$, G' is a multiplicative set in K' such that $G' \subseteq G$ and $G'(\Sigma) \preceq G(\Sigma)$, and K' and $\mathbb{F}(G)$ are free over $\mathbb{F}(G')$.

Consider an element $(K', G') \in \text{Sub}(K, G)$. By Lemma 3.3 the field $\mathbb{F}(G)$ is a regular extension of $\mathbb{F}(G')$, and thus by Fact 2, K' and $\mathbb{F}(G)$ are linearly disjoint over $\mathbb{F}(G')$. Using also the other part of Lemma 3.3 we conclude that $(K', G') \subseteq (K, G)$.

Let L be a second algebraically closed field and H a small multiplicative set in L such that (L, H) is κ -saturated, and define $\text{Sub}(L, H)$ likewise. Let \mathcal{I} be the set of all isomorphisms $\iota : (K', G') \cong (L', H')$ where $(K', G') \in \text{Sub}(K, G)$ and $(L', H') \in \text{Sub}(L, H)$. (Possibly $\mathcal{I} = \emptyset$.) These definitions and the next lemma are inspired by Section 2 of [4].

Lemma 3.4. *\mathcal{I} is a back-and-forth system.*

Proof. Let $\iota : (K', G') \rightarrow (L', H')$ be in \mathcal{I} and let $\alpha \in K \setminus K'$; our task is to find an extension of ι in \mathcal{I} that contains α in its domain. We can assume K and L have the same prime field \mathbb{F} . We distinguish three cases:

(1) $\alpha \in G$: Take a multiplicative subset G'' of G of cardinality $< \kappa$ such that $G' \cup \{\alpha\} \subseteq G''$, and $G''(\Sigma) \preceq G(\Sigma)$. Then $K'(G'')$ and $\mathbb{F}(G)$ are linearly disjoint over $\mathbb{F}(G'')$. Put $K'' := K'(G'')^{\text{ac}}$, so $(K'', G'') \in \text{Sub}(K, G)$.

Since $H(\Sigma)$ is κ -saturated, we can extend $\iota|_{G'}$ to an isomorphism $G''(\Sigma) \cong H''(\Sigma)$ where H'' is a multiplicative subset of H such that $H' \subseteq H''$ and $H''(\Sigma) \preceq G(\Sigma)$. This isomorphism extends to a field isomorphism $\mathbb{F}(G'') \cong \mathbb{F}(H'')$, and by the linear disjointness of K'' and $\mathbb{F}(G)$ over $\mathbb{F}(G'')$, it extends further to a field isomorphism $K'' \cong L'' := L'(H'')^{\text{ac}}$ that belongs to \mathcal{I} .

(2) $\alpha \in K'(G)^{\text{ac}}$: Then $\alpha \in K'(g_1, \dots, g_n)^{\text{ac}}$ for suitable $g_1, \dots, g_n \in G$. Applying the previous construction n times in succession yields the desired isomorphism in \mathcal{I} .

(3) $\alpha \notin K'(G)^{\text{ac}}$: Then $(K'(\alpha)^{\text{ac}}, G') \in \text{Sub}(K, G)$. By part (2) of Lemma 2.2 we have $L'(H)^{\text{ac}} \neq L$, so we can choose $\beta \in L \setminus L'(H)^{\text{ac}}$. Then $(L'(\beta)^{\text{ac}}, H') \in \text{Sub}(L, H)$ and ι extends to a field isomorphism $K'(\alpha)^{\text{ac}} \cong L'(\beta)^{\text{ac}}$ that sends α to β and belongs to \mathcal{I} . \square

Here are some consequences of Lemma 3.4 and its proof:

Corollary 3.5. *Suppose G is small in K and the $\mathcal{L}_m(\Sigma)$ -structure $G(\Sigma)$ is ω -stable. Then the $\mathcal{L}(U)$ -structure (K, G) is ω -stable.*

Proof. We can assume that (K, G) is \aleph_1 -saturated and (K', G') is a countable elementary substructure; it remains to show that then the elements of K realize only countably many different 1-types in (K, G) over K' . By the proof of Lemma 3.4, all elements of K not in $K'(G)^{\text{ac}}$ realize the same type in (K, G) over K' . Next, let $\alpha \in K'(G)^{\text{ac}}$. Take $g_1, \dots, g_n \in G$ such that $\alpha \in K'(g_1, \dots, g_n)^{\text{ac}}$. Now that same proof shows that the type of α in (K, G) over K' is completely determined by the type of (g_1, \dots, g_n) in $G(\Sigma)$ over $G'(\Sigma)$ and the specification of a polynomial $P(X_1, \dots, X_n, Y) \in K'[X_1, \dots, X_n, Y]$ such that $P(g_1, \dots, g_n, Y) \in K'(g_1, \dots, g_n)[Y]$ is irreducible and $P(g_1, \dots, g_n, \alpha) = 0$. This leaves only countably many possibilities for the type of α in (K, G) over K' . \square

In a similar way we obtain:

Corollary 3.6. *If G is small in K and $G(\Sigma)$ is superstable (stable), then (K, G) is superstable (respectively, stable).*

Corollary 3.7. *Let G be small in K , and let K' be an algebraically closed subfield of K with a multiplicative subset G' that is small in K' . Suppose $G' \subseteq G$ with $G'(\Sigma) \preceq G(\Sigma)$, and K' and $\mathbb{F}(G)$ are free over $\mathbb{F}(G')$ in K . Then $(K', G') \preceq (K, G)$.*

Proof. Take an uncountable cardinal $\kappa > |K'|$ and a κ -saturated elementary extension (L, H) of (K', G') . Note that then $(K', G') \in \text{Sub}(L, H)$. By passing to an elementary extension of (K, G) we can also assume that (K, G) is κ -saturated, so $(K', G') \in \text{Sub}(K, G)$. The identity map on K' belongs to the back-and-forth system \mathcal{I} of Lemma 3.4. Hence (K, G) and (L, H) are elementarily equivalent over K' . Thus $(K', G') \preceq (K, G)$. \square

A relative quantifier elimination. Let $\text{ACF}(\mathfrak{m})$ be the $\mathcal{L}(U)$ -theory whose models are the structures (K, G) where K is an algebraically closed field and G a small multiplicative set in K . To eliminate quantifiers for $\text{ACF}(\mathfrak{m})$ we extend this theory by definitions to an $\mathcal{L}(U, \Sigma)$ -theory $\text{ACF}(\mathfrak{m}, \Sigma)$ by adding for each $k \in \mathbb{Z}^n$ with $n \geq 1$ the n -ary relation symbol Σ_k with its defining axiom

$$\forall y (\Sigma_k(y) \longleftrightarrow U(y) \wedge k_1 y_1 + \cdots + k_n y_n = 0)$$

where $y = (y_1, \dots, y_n)$ is a tuple of distinct variables and $U(y)$ abbreviates the formula $U(y_1) \wedge \cdots \wedge U(y_n)$. Thus each model (K, G) of $\text{ACF}(\mathfrak{m})$ expands uniquely to a model of $\text{ACF}(\mathfrak{m}, \Sigma)$, and we shall denote this expansion also by (K, G) , although $(K, G(\Sigma))$ might be more correct.

Note that $\mathcal{L}(U, \Sigma)$ contains $\mathcal{L}_m(\Sigma)$ as a sublanguage. The U -restriction of an $\mathcal{L}_m(\Sigma)$ -formula θ is the $\mathcal{L}(U, \Sigma)$ -formula θ_U defined recursively as follows:

$$\begin{aligned} \text{if } \theta \text{ is atomic, then } \theta_U &:= \theta, & \text{if } \theta = \neg\theta', \text{ then } \theta_U &:= \neg\theta'_U, \\ \text{if } \theta = \theta' \wedge \theta'', \text{ then } \theta_U &:= \theta'_U \wedge \theta''_U, & \text{if } \theta = \theta' \vee \theta'', \text{ then } \theta_U &:= \theta'_U \vee \theta''_U, \\ \text{if } \theta = \exists x\theta', \text{ then } \theta_U &:= \exists x(U(x) \wedge \theta'_U), \\ \text{if } \theta = \forall x\theta', \text{ then } \theta_U &:= \forall x(U(x) \rightarrow \theta'_U). \end{aligned}$$

Note that for an $\mathcal{L}_m(\Sigma)$ -formula $\theta(y)$ with $y = (y_1, \dots, y_n)$, a model (K, G) of $\text{ACF}(\mathfrak{m}, \Sigma)$, and $g \in G^n$ we have

$$G(\Sigma) \models \theta(g) \iff (K, G) \models \theta_U(g).$$

Let $x = (x_1, \dots, x_m)$ be a tuple of distinct variables. A *special* formula in x is by definition an $\mathcal{L}(U, \Sigma)$ -formula $\eta(x)$ of the form

$$\exists y (U(y) \wedge \theta_U(y) \wedge \phi(x, y))$$

for some $\mathcal{L}_m(\Sigma)$ -formula $\theta(y)$ and some \mathcal{L} -formula $\phi(x, y)$, $y = (y_1, \dots, y_n)$. We now have the following analogue of Theorem 1 in [4].

Theorem 3.8. *Each $\mathcal{L}(U, \Sigma)$ -formula $\psi(x)$ is equivalent in $\text{ACF}(\mathfrak{m}, \Sigma)$ to a boolean combination of special formulas in x .*

Proof. Let $(K, G) \models \text{ACF}(m, \Sigma)$ and $(L, H) \models \text{ACF}(m, \Sigma)$ be \aleph_1 -saturated, and let $\alpha = (\alpha_1, \dots, \alpha_m) \in K^m$, and $\beta = (\beta_1, \dots, \beta_m) \in L^m$ satisfy (in (K, G) and (L, H) , respectively) the same special formulas in x . So K and L have the same characteristic, and thus the same prime field \mathbb{F} (without loss). Using Fact 1, it suffices to derive from this assumption that

$$\text{tp}_{(K, G)}(\alpha) = \text{tp}_{(L, H)}(\beta).$$

Let $\mathbb{F}(G)(\alpha)$ have transcendence degree r over $\mathbb{F}(G)$; we can assume that $\alpha_1, \dots, \alpha_r$ are algebraically independent over $\mathbb{F}(G)$. We claim that then $\mathbb{F}(H)(\beta)$ has transcendence degree r over $\mathbb{F}(H)$, and that β_1, \dots, β_r are algebraically independent over $\mathbb{F}(H)$. Suppose β_1, \dots, β_r are not algebraically independent over $\mathbb{F}(H)$, say, $\beta_r \in \mathbb{F}(H)(\beta_1, \dots, \beta_{r-1})^{\text{ac}}$. Then we have an \mathcal{L} -formula $\varphi(x_1, \dots, x_r, y)$ with $y = (y_1, \dots, y_n)$, an $h \in H^n$, and an $N \in \mathbb{N}$ such that

$$L \models \varphi(\beta_1, \dots, \beta_r, h) \wedge \exists^{\leq N} x_r \varphi(\beta_1, \dots, \beta_{r-1}, x_r, h),$$

hence $(L, H) \models \exists y (U(y) \wedge \varphi(\beta_1, \dots, \beta_r, y) \wedge \exists^{\leq N} x_r \varphi(\beta_1, \dots, \beta_{r-1}, x_r, y))$, and thus $(K, G) \models \exists y (U(y) \wedge \varphi(\alpha_1, \dots, \alpha_r, y) \wedge \exists^{\leq N} x_r \varphi(\alpha_1, \dots, \alpha_{r-1}, x_r, y))$, contradicting that $\alpha_1, \dots, \alpha_r$ are algebraically independent over $\mathbb{F}(G)$. This proves our claim.

Take a countable multiplicative subset G' of G such that $G'(\Sigma) \preceq G(\Sigma)$ and $\mathbb{F}(G')(\alpha)$ has transcendence degree r over $\mathbb{F}(G')$, let $g = (g_0, g_1, g_2, \dots)$ be an enumeration of G' , and $y = (y_0, y_1, y_2, \dots)$ a list of distinct variables. Note that if $\theta_1(y), \dots, \theta_k(y)$ are $\mathcal{L}_m(\Sigma)$ -formulas and $\varphi_1(x, y), \dots, \varphi_k(x, y)$ are \mathcal{L} -formulas such that $G(\Sigma) \models \theta_j(g)$ and $K \models \varphi_j(\alpha, g)$ for $j = 1, \dots, k$, then

$$(K, G) \models \exists y (U(y) \wedge \theta_U(y) \wedge \varphi(\alpha, y)), \quad \text{where}$$

$$\theta(y) := \bigwedge_j \theta_j(y), \quad \varphi(x, y) := \bigwedge_j \varphi_j(x, y).$$

so $(L, H) \models \exists y (U(y) \wedge \theta_U(y) \wedge \varphi(\beta, y))$. Hence we have a partial y -type over β in (L, H) consisting of the formulas $U(y_i)$ for $i = 0, 1, 2, \dots$, the formulas $\theta_U(y)$ such that $G(\Sigma) \models \theta(g)$ with $\theta(y)$ an $\mathcal{L}_m(\Sigma)$ -formula, and the formulas $\varphi(\beta, y)$ such that $(K, G) \models \varphi(\alpha, g)$ with $\varphi(x, y)$ an \mathcal{L} -formula. Let $h = (h_0, h_1, h_2, \dots)$ realize this y -type in (L, H) . Note that this yields a partial elementary map between $G(\Sigma)$ and $H(\Sigma)$ given by $g_i \mapsto h_i, i = 0, 1, 2, \dots$. Put $H' := \{h_0, h_1, \dots\}$. Then H' is a multiplicative subset of H such that $H'(\Sigma) \preceq H(\Sigma)$, and we have a field isomorphism $\iota : \mathbb{F}(G')(\alpha) \cong \mathbb{F}(H')(\beta)$ sending each g_i to h_i and each α_j to β_j . Put $K' := \mathbb{F}(G')(\alpha)^{\text{ac}}$ and $L' := \mathbb{F}(H')(\beta)^{\text{ac}}$. Then $(K', G') \in \text{Sub}(K, G)$ and $(L', H') \in \text{Sub}(L, H)$ (taking $\kappa = \aleph_1$ in the subsection on back-and-forth) and we have an isomorphism $(K', G') \cong (L', H')$ that extends ι . This isomorphism carries α to β and belongs to the back-and-forth system \mathcal{I} , so we are done. \square

Multiplicative sets with extra structure. All the above in this section goes through when our multiplicative sets are equipped with extra structure. To make this precise, let \mathcal{L}_m^* be a language that extends \mathcal{L}_m only by relation symbols and constant symbols. We assume that the symbols of $\mathcal{L}_m^* \setminus \mathcal{L}_m$ are all outside $\mathcal{L}(U, \Sigma)$.

Let G^* be an \mathcal{L}_m^* -expansion of the multiplicative monoid G , and construe (K, G^*) as an $\mathcal{L}^*(U)$ -structure, where $\mathcal{L}^*(U)$ is obtained from the language $\mathcal{L}(U)$ by adding the symbols of $\mathcal{L}_m^* \setminus \mathcal{L}_m$. We also use the language

$$\mathcal{L}_m^*(\Sigma) := \mathcal{L}_m^* \cup \{\Sigma_k : k \in \mathbb{Z}^n, n = 1, 2, \dots\}.$$

Expand G^* to the $\mathcal{L}_m^*(\Sigma)$ -structure $G^*(\Sigma)$ by interpreting Σ_k as earlier in this section. The proofs of Corollary 3.1 and Proposition 3.2 go through almost without change in the present setting and yield:

Corollary 3.9. *If G is small in K , then $\text{Th}(K, G^*)$ is completely determined by $\text{Th}(G^*(\Sigma))$.*

Proposition 3.10. *Every subset of G^n definable in (K, G^*) is definable in $G^*(\Sigma)$.*

Next we consider the language

$$\mathcal{L}^*(U, \Sigma) := \mathcal{L}^*(U) \cup \{\Sigma_k : k \in \mathbb{Z}^n, n = 1, 2, \dots\},$$

and the theory $\text{ACF}^*(m, \Sigma)$ in this language, whose models are the structures $(K, G^*(\Sigma))$ where G is a small multiplicative set in an algebraically closed field K and G^* is an expansion of the multiplicative monoid G to an \mathcal{L}_m^* -structure. The U -restriction of an $\mathcal{L}_m^*(\Sigma)$ -formula θ is the formula θ_U of $\mathcal{L}^*(U, \Sigma)$ defined by the same recursive clauses as before.

Let $x = (x_1, \dots, x_m)$ be a tuple of distinct variables. A *special* formula in x is now an $\mathcal{L}^*(U, \Sigma)$ -formula $\eta(x)$ of the form

$$\exists y(U(y) \wedge \theta_U(y) \wedge \phi(x, y))$$

for some $\mathcal{L}_m^*(\Sigma)$ -formula $\theta(y)$ and some \mathcal{L} -formula $\phi(x, y)$, $y = (y_1, \dots, y_n)$. Then we have the following generalization of Theorem 3.8 :

Theorem 3.11. *Each $\mathcal{L}^*(U, \Sigma)$ -formula $\psi(x)$ is equivalent in $\text{ACF}^*(m, \Sigma)$ to a boolean combination of special formulas in x .*

4. ELIMINATION THEORY FOR GROUP ACTIONS

Here we establish some very basic facts on group actions. This will be used in the next section to derive the Mordell-Lang property from the Mann property. We do a bit more than needed for this application because it requires no more work and group actions are ubiquitous in mathematics.

Throughout this section G is a multiplicatively written group with identity 1, not necessarily commutative, and g (sometimes with a subscript or accent) ranges over elements of G . By a G -set we shall mean a nonempty set P together with an action $(g, p) \mapsto gp : G \times P \rightarrow P$. The *language* of

G -sets has for each g a unary function symbol also denoted by g ; the *theory of G -sets* in this language has as its models the G -sets P with each function symbol g interpreted as the bijection $p \mapsto gp$. The *augmented language of G -sets* has, in addition to these function symbols g , for each finitely generated subgroup F of G a nullary relation symbol s_F , and the *augmented theory of G -sets* is obtained from the theory of G -sets by adding for each F as above a defining axiom

$$s_F \longleftrightarrow \exists y(f_1y = \cdots = f_ny = y)$$

where $f_1, \dots, f_n \in G$ generate F . In the rest of this section x_1, \dots, x_m, y are distinct variables, and $x = (x_1, \dots, x_m)$.

Lemma 4.1. *Let $\phi_1(x, y), \dots, \phi_k(x, y)$ be atoms in the augmented language of G -sets. Then there are atoms $\psi_1(x), \dots, \psi_l(x)$ in this language such that the theory of augmented G -sets proves the equivalence*

$$\exists y(\phi_1(x, y) \wedge \cdots \wedge \phi_k(x, y)) \longleftrightarrow \psi_1(x) \wedge \cdots \wedge \psi_l(x).$$

Proof. First we reduce to the case that each atom $\phi_i(x, y)$ contains the variable y . Any atom $g_1u_1 = g_2u_2$ with variables u_1, u_2 , is equivalent to $u_1 = gu_2$ where $g = g_1^{-1}g_2$. Hence we can assume that each $\phi_i(x, y)$ is of the form $y = gy$, or of the form $y = gx_j$ with $j \in \{1, \dots, m\}$. If, say, $\phi_1(x, y)$ is $y = gx_j$, then the desired equivalence is

$$\exists y(\phi_1(x, y) \wedge \cdots \wedge \phi_k(x, y)) \longleftrightarrow \phi_2(x, gx_j) \wedge \cdots \wedge \phi_k(x, gx_j).$$

It remains to consider the case that $\phi_i(x, y)$ is an atom $y = g_iy$ for $i = 1, \dots, k$. Then the desired equivalence is

$$\exists y(\phi_1(x, y) \wedge \cdots \wedge \phi_k(x, y)) \longleftrightarrow s_F,$$

where F is the subgroup of G generated by g_1, \dots, g_k . □

It follows that each *positive* existential formula $\phi(x)$ in the augmented language of G -sets is equivalent in the augmented theory of G -sets to some *positive* quantifier-free formula $\phi'(x)$ of this language.

A *free G -set* is a G -set P such that $gp \neq p$ for all $g \neq 1$ and all $p \in P$. The next result is crucial in the proof of Proposition 5.6.

Corollary 4.2. *Each positive existential formula $\phi(x)$ in the language of G -sets is equivalent in the theory of free G -sets to some positive quantifier-free formula $\phi'(x)$ in this language.*

It will be useful to have a kind of normal form for conjunctions of atoms in the theory of free G -sets. Let $\phi(x)$ be a conjunction of atoms in the language of G -sets. We consider $\phi(x)$ as defining in each G -set P a certain subset of P^m . If \perp is among the atoms of $\phi(x)$, then the theory of G -sets proves $\neg\phi(x)$, and thus $\phi(x)$ defines in each G -set P the empty subset of P^m . So let us assume that \perp is not among the atoms of $\phi(x)$. Then the theory of G -sets proves $\phi(x) \longleftrightarrow \phi'(x)$ where $\phi'(x)$ is a conjunction of atoms of the form $gx_i = g'x_j$, $1 \leq i, j \leq m$. Define a graph with vertex set $\{1, \dots, m\}$

and an edge between i and j iff $\phi'(x)$ contains a conjunct $gx_i = g'x_j$. Let $I(1), \dots, I(l)$ be the distinct vertex sets of the connected components of this graph. Then $I(1), \dots, I(l)$ partition $\{1, \dots, m\}$, and the theory of free G -sets proves an equivalence

$$\phi(x) \longleftrightarrow \bigwedge_{\lambda} \left[\bigwedge_{i \in I(\lambda)} x_i = g_i x_{i(\lambda)} \right], \quad \lambda = 1, \dots, l \quad (\diamond)$$

where $i(\lambda) \in I(\lambda)$ for each λ . Thus within any block $I(\lambda)$, each variable x_i with $i \in I(\lambda)$ is equated to a fixed translate of the *distinguished* variable $x_{i(\lambda)}$ of this block.

Example. Suppose $m \geq 7$ and $\phi'(x)$ has atoms $x_1 = gx_2$, $x_2 = g'x_7$ and $x_7 = g''x_1$, and no other atoms involving x_1, x_2 or x_7 . Then $\{1, 2, 7\}$ is a block of the partition of $\{1, \dots, m\}$ figuring in the equivalence (\diamond) above. Choosing x_1 as the distinguished variable of this block, the conjunction corresponding to this block is

$$x_1 = (gg'g'')x_1 \wedge x_2 = (g'g'')x_1 \wedge x_7 = g''x_1.$$

Note that if $gg'g'' \neq 1$, then the theory of free G -sets proves $\neg\phi(x)$.

It follows from (\diamond) that $\phi(x)$ defines in each free G -set P the cartesian product $P(1) \times \dots \times P(l) \subseteq P^m$ where

$$P(\lambda) := \{(p_i) \in P^{I(\lambda)} : p_i = g_i p_{i(\lambda)} \text{ for all } i \in I(\lambda)\}$$

with the obvious identifications

$$P^m = P^{\{1, \dots, m\}} = P^{I(1)} \times \dots \times P^{I(l)}.$$

Note that if $g_{i(\lambda)} \neq 1$ for some λ , then $\phi(x)$ defines in each free G -set P the empty subset of P^m , while if $g_{i(\lambda)} = 1$ for all λ , then $\phi(x)$ defines in each free G -set P a non-empty subset of P^m .

Next we consider the case of the free G -set G , given by the (left) action $(g, h) \mapsto gh$. To discuss definability with parameters in this G -set, we consider the language of G -sets augmented by a name for the element 1 of the G -set G ; call this the *language of G -sets with 1*. This name should not be confused with the unary function symbol 1 of the language of G -sets.

Corollary 4.3. *Suppose the nonempty set $S \subseteq G^m$ is defined in G by a conjunction of atoms in the language of G -sets with 1. Then there are g_1, \dots, g_m , a set $I(0) \subseteq \{1, \dots, m\}$ (possibly empty), and a partition of $\{1, \dots, m\} \setminus I(0)$ into distinct sets $I(1), \dots, I(l)$, such that*

$$S = S(0) \times S(1) \times \dots \times S(l) \subseteq G^{I(0)} \times G^{I(1)} \times \dots \times G^{I(l)} = G^m, \text{ where}$$

$$S(0) := \{(g_i)_{i \in I(0)}\}, \quad \text{a one-element subset of } G^{I(0)}, \text{ and}$$

$$S(\lambda) := \{(g_i g)_{i \in I(\lambda)} : g \in G\}, \quad \text{a subset of } G^{I(\lambda)} \text{ for } \lambda = 1, \dots, l.$$

Note that if S has just one element we can take $I(0) = \{1, \dots, m\}$, while for $S = G^m$ we can take $I(0) = \emptyset$, $l = m$ and $I(\lambda) = \{\lambda\}$ for $\lambda = 1, \dots, m$.

This is all we need for use in the next section, but for the sake of completeness we briefly consider also the theory of *infinite* free G -sets. (If G itself is infinite, then of course all free G -sets are infinite.) One verifies easily that for any atoms $\phi_1(x, y), \dots, \phi_k(x, y)$ in the language of G -sets this theory proves an equivalence

$$\forall y(\phi_1(x, y) \vee \dots \vee \phi_k(x, y)) \longleftrightarrow \theta_1(x) \vee \dots \vee \theta_l(x)$$

for suitable atoms $\theta_1(x), \dots, \theta_l(x)$ in the language of G -sets. In combination with Corollary 4.2 this yields:

Corollary 4.4. *Every positive formula $\phi(x)$ in the language of G -sets is equivalent in the theory of infinite free G -sets to a positive quantifier-free formula $\phi'(x)$ in that language.*

Note also that the theory of infinite free G -sets is κ -categorical for infinite $\kappa > |G|$, in particular, this theory is complete. It is also easy to check that this theory has elimination of quantifiers in the language of G -sets.

5. THE MANN PROPERTY

Throughout this section, K is a field, E is a subfield of K , and G is a subgroup of the multiplicative group K^\times of K . Consider a linear equation

$$(*) \quad a_0 = a_1x_1 + \dots + a_nx_n,$$

where $a_0, a_1, \dots, a_n \in K$. A *solution* of $(*)$ in G is a tuple $(g_1, \dots, g_n) \in G^n$ such that $a_0 = a_1g_1 + \dots + a_ng_n$, and such a solution is said to be *nondegenerate* if $\sum_{i \in I} a_i g_i \neq 0$ for each non-empty proper subset I of $\{1, \dots, n\}$. In the homogeneous case $a_0 = 0$ the set of solutions in G and the set of nondegenerate solutions in G are both unions of orbits with respect to the action of G on G^n defined by $g(g_1, \dots, g_n) = (gg_1, \dots, gg_n)$. (In the introduction we only considered the *inhomogeneous* case $a_0 = 1$ with *nonzero* a_1, \dots, a_n in the *prime field* \mathbb{F} of K .)

Let us say that G has the *Mann property over E* if each equation

$$a_1x_1 + \dots + a_nx_n = 1 \quad (n \geq 2, a_1, \dots, a_n \in E^\times)$$

has only finitely many nondegenerate solutions in G . For $E = \mathbb{F}$ this is just the Mann property defined in the introduction. This terminology is temporary, since the Mann property will be shown to be equivalent to the Mann property over E . Consider a homogeneous equation

$$a_1x_1 + \dots + a_nx_n = 0, \quad (a_1, \dots, a_n \in E^\times, n \geq 1).$$

Let $S \subseteq G^n$ be its set of solutions in G and S_{nd} its subset of nondegenerate solutions in G . Then

$$S_{\text{nd}} = \bigcup_{(g_1, \dots, g_{n-1}) \in S'} (g_1, \dots, g_{n-1}, 1)G \subseteq S,$$

we have elements $g_1, \dots, g_n \in G$, a subset $I(0)$ of $\{1, \dots, n\}$, and a partition of $\{1, \dots, n\} \setminus I(0)$ into distinct sets $I(1), \dots, I(l)$, such that

$$S = S(0) \times S(1) \times \dots \times S(l) \subseteq G^{I(0)} \times G^{I(1)} \times \dots \times G^{I(l)} = G^m, \text{ where}$$

$$S(0) := \{(g_i)_{i \in I(0)}\}, \quad \text{a one-element subset of } G^{I(0)}, \text{ and}$$

$$S(\lambda) := \{(g_i g)_{i \in I(\lambda)} : g \in G\}, \quad \text{a subset of } G^{I(\lambda)} \text{ for } \lambda = 1, \dots, l.$$

Since S has more than one element, $I(0)$ is a proper subset of $\{1, \dots, n\}$, hence $l \geq 1$. Let $(s_1, \dots, s_n) \in S$. Then

$$\sum_{i=1}^n a_i s_i = \sum_{i \notin I(1)} a_i s_i + \sum_{i \in I(1)} a_i s_i g = \sum_{i \notin I(1)} a_i s_i + \left(\sum_{i \in I(1)} a_i s_i \right) g$$

for all $g \in G$, so $a = ag$ for all $g \in G$, where $a := \sum_{i \in I(1)} a_i s_i$. Hence $a = 0$, so (s_1, \dots, s_n) is a degenerate solution. \square

We can now prove:

Lemma 5.5. *Suppose that $G \subseteq E^\times$ and G has the Mann property over E . Then G has the Mann property over K .*

Proof. Let $a_1, \dots, a_n \in K^\times$, $n \geq 1$. Take a basis b_0, b_1, \dots, b_m of the E -linear subspace $E + a_1 E + \dots + a_n E$ of K with $b_0 = 1$. Write $a_j = \sum_{i=0}^m a_{ij} b_i$ with $a_{ij} \in E$. Then the solutions in G of the equation $a_1 x_1 + \dots + a_n x_n = 1$ are exactly the solutions in G of the system of equations

$$\begin{aligned} a_{01}x_1 + \dots + a_{0n}x_n &= 1 \\ a_{11}x_1 + \dots + a_{1n}x_n &= 0 \\ &\dots\dots\dots \\ &\dots\dots\dots \\ a_{m1}x_1 + \dots + a_{mn}x_n &= 0 \end{aligned}$$

Hence by Corollary 5.3 the set of solutions in G of the equation

$$a_1 x_1 + \dots + a_n x_n = 1$$

is defined in G by a positive quantifier-free formula in the language of G -sets with 1. Now apply Lemma 5.4. \square

Proposition 5.6. *Suppose that G has the Mann property. Then G has the Mann property over K .*

Proof. By the previous lemma it suffices to show that G has the Mann property over $E := \mathbb{F}(G)$. Let $a_0, a_1, \dots, a_n \in E^\times$ and consider the linear equation

$$a_0 = a_1 x_1 + \dots + a_n x_n.$$

By Lemma 5.4 it remains to show that the set S of solutions in G of this equation is defined by a positive quantifier-free formula in the language of G -sets with 1. After multiplying a_0, \dots, a_n by a suitable non-zero element

we can assume that they lie in the subring $\mathbb{F}[G]$ of E that is generated by G over \mathbb{F} . Take $g_1, \dots, g_m \in G$ such that $a_j = \sum_{i=1}^m f_{ij}g_i$, with $f_{ij} \in \mathbb{F}$ for $i = 1, \dots, m, j = 0, \dots, n$. Then we have for all $(x_1, \dots, x_n) \in G^n$:

$$\begin{aligned} (x_1, \dots, x_n) \in S &\iff \sum_i f_{i0}g_i = \sum_i f_{i1}g_ix_1 + \dots + \sum_i f_{in}g_ix_n \\ &\iff \exists y \left[\left(\bigwedge_i y_i = g_i \right) \wedge \left(\bigwedge_i y_{i1} = g_ix_1 \right) \wedge \dots \wedge \left(\bigwedge_i y_{in} = g_ix_n \right) \right. \\ &\quad \left. \wedge \sum_i f_{i0}y_i = \sum_i f_{i1}y_{i1} + \dots + \sum_i f_{in}y_{in} \right], \end{aligned}$$

where $y = (y_1, \dots, y_m, y_{11}, \dots, y_{m1}, \dots, y_{1n}, \dots, y_{mn})$ is a tuple of distinct variables, each ranging over G . By Corollary 5.1 the subset of G^{m+mn} defined by the equation

$$\sum_i f_{i0}y_i = \sum_i f_{i1}y_{i1} + \dots + \sum_i f_{in}y_{in}$$

is defined in G by a positive quantifier-free formula in the language of G -sets. Thus by Corollary 4.2 the set $S \subseteq G^n$ is defined in G by a positive quantifier-free formula in the language of G -sets with 1. \square

The next consequence may be surprising since the definition of the Mann property does not require any kind of uniform bounds.

Corollary 5.7. *Suppose G has the Mann property. Then there is for each n a natural number $A(n)$ such that for any nonzero a_1, \dots, a_n in any extension field of K the equation $a_1x_1 + \dots + a_nx_n = 1$ has at most $A(n)$ nondegenerate solutions in G .*

Proof. Consider the $\mathcal{L}(U)$ -structures (K', G') where K' is an extension field of K , G' is a subgroup of K'^\times , and (K', G') satisfies the Mann axioms for G as defined in the introduction. Then G' has the Mann property, and thus G' has the Mann property in K' . The structures $(K', G', (a)_{a \in K})$ where (K', G') is as above, are up-to-isomorphism exactly the models of a set of sentences in the language $\mathcal{L}(U)$ augmented by names for the elements of K . The uniform bound is now an easy consequence of compactness. \square

Remark. We can arrange the function $n \mapsto A(n)$ to be computable relative to the set of Mann axioms for G . It needs some care to make sense of this relative computability claim; we prefer not to elaborate here.

Mann implies Mordell-Lang. In this subsection K is algebraically closed. For any n -tuple $k = (k_1, \dots, k_n) \in \mathbb{Z}^n$, consider the *character*

$$\chi_k : (K^\times)^n \rightarrow K^\times, \quad \chi_k(x_1, \dots, x_n) := x_1^{k_1} \dots x_n^{k_n}.$$

This is a multiplicative group homomorphism. For any $d \in \mathbb{N}$, let $\mathcal{D}(n, d)$ be the finite collection of subgroups of $(K^\times)^n$ that are intersections of kernels of characters χ_k with $|k| = |k_1| + \dots + |k_n| \leq d$. The following yields (1) \Rightarrow (2) of Proposition 1.1.

Proposition 5.8. *Let $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ have degree $\leq d$, and let*

$$V = \{x \in K^n : f_1(x) = \dots = f_m(x) = 0\}.$$

Suppose G has the Mann property. Then $V \cap G^n$ is a finite union of cosets of subgroups $D \cap G^n$ of G^n with $D \in \mathcal{D}(n, d)$.

Proof. The intersection of finitely many cosets of such subgroups is either empty or again a coset of such a subgroup. Hence we may (and shall) assume that $m = 1$. Put $f := f_1$, and write $f = \sum_{i \in I} a_i X^i$ where all $a_i \in K$ and I is the set of multi-indices $i = (i_1, \dots, i_n) \in \mathbb{N}^n$ with $|i| = i_1 + \dots + i_n \leq d$. By Corollary 5.1 the set

$$\{y \in G^{|I|} : \sum_{i \in I} a_i y_i = 0\}$$

is a finite union of finite intersections of subsets of $G^{|I|}$ of the form

$$\{y \in G^{|I|} : g y_i = y_j\}$$

with $g \in G$ and $i, j \in I$. It remains to observe that for such g, i, j the set

$$\{x \in G^n : g \chi_i(x) = \chi_j(x)\}$$

is a coset of the subgroup $D \cap G^n$ of G^n where D is the kernel of χ_{i-j} . \square

Mordell-Lang implies Mann. Proposition 5.11 below says that a weak form of the Mordell-Lang property for G implies the Mann property for G . In particular, it yields (2) \Rightarrow (1) and (3) \Rightarrow (1) of Proposition 1.1.

In this subsection K is algebraically closed. We refer to [20] for the basics on algebraic groups over K , especially Chapter 3. Terminology like “open” and “closed” refers to the relevant Zariski topology. The group $(K^\times)^n$ is viewed as an algebraic torus over K in the usual way.

Lemma 5.9. *Let $a_1, \dots, a_n \in K^\times$, and let H be an infinite subgroup of $(K^\times)^n$ contained in the solution set of the equation $a_1 x_1 + \dots + a_n x_n = 1$. Then all $(h_1, \dots, h_n) \in H$ are degenerate solutions of this equation.*

Proof. Replacing H by its closure in $(K^\times)^n$ we can assume that H is a closed subgroup of $(K^\times)^n$. Let H^0 be the connected component of the identity in H , so H^0 is a closed subgroup of H and of finite index in H . Consider a coset $(b_1, \dots, b_n)H^0 \subseteq H$ of H^0 . We are going to show that this coset consists entirely of degenerate solutions of the equation above.

Let $\dim H^0 = d$. Then $d > 0$, and we have an embedding

$$\phi = (\phi_1, \dots, \phi_n) : (K^\times)^d \rightarrow (K^\times)^n$$

of algebraic groups over K with image H^0 . For $i = 1, \dots, n$ we have a tuple $e(i) = (e_{i1}, \dots, e_{id}) \in \mathbb{Z}^d$ such that $\phi_i(y) = y^{e(i)} := y_1^{e_{i1}} \dots y_d^{e_{id}}$ for all $y = (y_1, \dots, y_d) \in (K^\times)^d$. Thus

$$a_1 b_1 y^{e(1)} + \dots + a_n b_n y^{e(n)} = 1$$

for all $y \in (K^\times)^d$. Let $E := \{e(i) : i = 1, \dots, n\}$. Then this identity means that for all $y \in (K^\times)^d$ we have

$$\sum_{e \in E} c_e y^e = 1, \text{ where } c_e := \sum_{e(i)=e} a_i b_i.$$

It follows that $c_e = 0$ for all $e \neq (0, \dots, 0) \in \mathbb{Z}^d$. Note that E contains an element $e \neq (0, \dots, 0)$, since $d > 0$ and ϕ is injective. For such e we have therefore

$$\sum_{e(i)=e} a_i (b_i y^e) = y^e \cdot \sum_{e(i)=e} a_i b_i = y^e c_e = 0$$

for all $y \in (K^\times)^d$. Since the elements of $(b_1, \dots, b_n)H^0$ are exactly the $(b_1 y^{e(1)}, \dots, b_n y^{e(n)})$ with $y \in (K^\times)^d$, it follows that all these elements are degenerate solutions, as claimed. \square

Lemma 5.10. *Let H be a commutative algebraic group over K , let A be a dense subgroup of H , let B_1, \dots, B_n be subgroups of A of infinite index, and let C_i be a finite union of cosets in A of B_i , for $i = 1, \dots, n$. Then $A - (C_1 \cup \dots \cup C_n)$ is dense in H .*

Proof. Till further notice we assume that H is connected.

We first consider the special case that no B_i is dense in H . Let $U \subseteq H$ be nonempty and open. Since $\dim U = \dim H$ and the closure of each coset of each B_i in H has dimension $< \dim H$, the set $U - \text{cl}(C_1 \cup \dots \cup C_n)$ is nonempty and open in H , and thus intersects A . Hence U intersects $A - (C_1 \cup \dots \cup C_n)$.

After having settled this special case, we now proceed by induction on n . The case $n = 0$ is trivial, so let $n > 0$. We can assume that $B_i \cap B_j$ is of infinite index in B_i for all distinct i, j , since if $B_i \cap B_j$ were of finite index in B_i , $i \neq j$, then each coset of B_i is a union of finitely many cosets of $B_i \cap B_j$, so C_i is contained in a finite union of cosets of B_j , and hence we can decrease n by eliminating B_i and increasing C_j suitably.

Because of the special case treated at the beginning of the proof we can assume $\text{cl}(B_1) = H$. Take a coset aB_1 in A that is disjoint from C_1 . Then

$$\begin{aligned} aB_1 - (C_1 \cup \dots \cup C_n) &\subseteq A - (C_1 \cup \dots \cup C_n), \\ aB_1 - (C_1 \cup \dots \cup C_n) &= aB_1 - (C_2 \cup \dots \cup C_n) \\ &= a[B_1 - (C_2' \cup \dots \cup C_n')] \end{aligned}$$

where each C_j' is a finite union of cosets of $B_1 \cap B_j$ in B_1 . By the inductive assumption, $B_1 - (C_2' \cup \dots \cup C_n')$ is dense in H , hence $a[B_1 - (C_2' \cup \dots \cup C_n')]$ is dense in H , and so is $A - (C_1 \cup \dots \cup C_n)$ by the inclusions above.

We have now established the lemma under the assumption that H is connected. We now drop this assumption and consider the connected component H^0 in H of the identity of H , a closed subgroup of H of finite index. Consider a coset C of H^0 in H ; it remains to show that $C \cap [A - (C_1 \cup \dots \cup C_n)]$

is dense in C . Take a $c \in C \cap A$. Then $C \cap A = cA^0$, where $A^0 := H^0 \cap A$, hence

$$\begin{aligned} C \cap [A - (C_1 \cup \dots \cup C_n)] &= (C \cap A) - [(C \cap C_1) \cup \dots \cup (C \cap C_n)] \\ &= cA^0 - [(C \cap C_1) \cup \dots \cup (C \cap C_n)] \\ &= c[A^0 - (C_1^0 \cup \dots \cup C_n^0)] \end{aligned}$$

where $C_i^0 := c^{-1}(C \cap C_i) = H^0 \cap (c^{-1}C_i)$. Note that C_i^0 is a finite union of cosets of $B_i^0 := H^0 \cap B_i$ in H^0 , so $A^0 - (C_1^0 \cup \dots \cup C_n^0)$ is dense in H^0 (by what was proved in the connected case), so by the equalities above, $C \cap [A - (C_1 \cup \dots \cup C_n)]$ is dense in C , as desired. \square

It is an easy exercise to check that if H is a commutative group, then any boolean combination of cosets in H of subgroups of H is a finite union of sets of the form $h \cdot (A - (B_1 \cup \dots \cup B_n))$ where $h \in H$, A is a subgroup of H , and each B_i is a subgroup of A of infinite index.

Proposition 5.11. *Suppose that for all $a_1, \dots, a_n \in \mathbb{F}^\times$ the set of solutions of $a_1x_1 + \dots + a_nx_n = 1$ in G is a boolean combination of subgroups of G^n . Then G has the Mann property.*

Proof. Given a boolean combination of subgroups of G^n , represent it as a finite union of sets of the form

$$g \cdot (A - (B_1 \cup \dots \cup B_n))$$

where $g \in G^n$, A is a subgroup of G^n , and each B_i is a subgroup of A of infinite index. By Lemma 5.10 the closure of the displayed set in $(K^\times)^n$ is $g \cdot \text{cl}(A)$. Now use Lemma 5.9. \square

Lemmas for the real case. This subsection gets used in Section 7.

Lemma 5.12. *Let Γ be a subgroup of G such that for all $a_1, \dots, a_n \in E^\times$ the equation $a_1x_1 + \dots + a_nx_n = 1$ has the same nondegenerate solutions in Γ as in G . Then we have for any $g, g_1, \dots, g_n \in G$:*

- (1) *if g is algebraic over $E(\Gamma)$ of degree d , then $g^d \in \Gamma$;*
- (2) *if g_1, \dots, g_n are algebraically dependent over $E(\Gamma)$, then they are multiplicatively dependent over Γ .*

Proof. Let $g \in G$ be algebraic over $E(\Gamma)$ of degree d . Then

$$\sum_{i=0}^d \sum_{j=1}^{n_i} a_{ij} \gamma_{ij} g^i = 0$$

with all $a_{ij} \in E^\times$ and all $\gamma_{ij} \in \Gamma$, and $\sum_{j=1}^{n_d} a_{dj} \gamma_{dj} \neq 0$. Thus $n_d > 0$. Also $n_0 > 0$, since $g \neq 0$. Fix such an identity with minimal $\sum n_i$. The tuple $(\gamma_{ij} g^i)$ is a solution of the linear equation

$$\sum_{i=0}^d \sum_{j=1}^{n_i} a_{ij} x_{ij} = 0.$$

The minimality of $\sum n_i$ yields the non-degeneracy of this solution. Hence there are $h_{ij} \in \Gamma$ and $h \in G$ such that $\gamma_{ij}g^i = h_{ij}h$ for all i, j . For $i = 0$ we get $h \in \Gamma$, and then for $i = d$ this yields $g^d \in \Gamma$. This proves (1).

For (2), assume that g_1, \dots, g_{n-1} are algebraically independent over $E(\Gamma)$, but g_n is algebraic of degree d over $E(\Gamma, g_1, \dots, g_{n-1})$; it suffices to show that then $g_n^d \in \Gamma \cdot g_1^{\mathbb{Z}} \cdots g_{n-1}^{\mathbb{Z}}$. Apply (1) to $\Gamma \cdot g_1^{\mathbb{Z}} \cdots g_{n-1}^{\mathbb{Z}}$ instead of Γ . \square

Lemma 5.13. *Let Γ be as in the previous lemma, and also pure in G . Then $G \cap E(\Gamma) = \Gamma$ and $E(G)$ is a regular field extension of $E(\Gamma)$.*

Proof. The first claim does not need the purity assumption and follows from part (1) of the previous lemma. To prove the regularity, we can assume that G is finitely generated over Γ . Since G/Γ is torsion-free, it is a free as an abelian group, so there are $g_1, \dots, g_n \in G$ that generate G over Γ and are multiplicatively independent over Γ . Hence g_1, \dots, g_n are algebraically independent by (2) of the previous lemma, so $E(G)$ is a purely transcendental extension of $E(\Gamma)$. \square

The hypothesis of Lemma 5.12 can be satisfied as follows:

Lemma 5.14. *Let Γ be a subgroup of E^\times and $g \in K$ transcendental over E , and let G be the subgroup of K^\times generated by Γ and g . Then each equation $a_1x_1 + \cdots + a_nx_n = 1$ with $n \geq 1$ and all $a_i \in E^\times$ has the same nondegenerate solutions in Γ as in G .*

Proof. Write each element of G as cg^k with $c \in \Gamma, k \in \mathbb{Z}$. \square

Lemma 5.15. *Let Γ be a subgroup of E^\times , $\gamma \in \Gamma$, d a positive integer, and suppose the polynomial $X^d - \gamma \in E[X]$ is irreducible. Let $g \in K$ satisfy $g^d = \gamma$, and let G be the subgroup of K^\times generated by Γ and g . Then each equation $a_1x_1 + \cdots + a_nx_n = 1$ with $n \geq 1$ and all $a_i \in E^\times$ has the same nondegenerate solutions in Γ as in G .*

Proof. Write each element of G as cg^i with $c \in \Gamma$ and $0 \leq i < d$, and use that $1, g, \dots, g^{d-1}$ is a basis of $E(g)$ over E . \square

The last two lemmas yield a profusion of groups with the Mann property. For example, one can manufacture infinite subgroups of the multiplicative group of \mathbb{F}_p^{ac} with the Mann property; see Section 8.

Let now K be an ordered field and E an ordered subfield. It is sometimes convenient to restrict attention to pure subgroups of $E^{>0}$. For example, the subgroups $2^{\mathbb{Z}}$ and $2^{\mathbb{Z}}3^{\mathbb{Z}}$ of $\mathbb{Q}^{>0}$ are pure subgroups of $\mathbb{Q}^{>0}$, but $4^{\mathbb{Z}}$ is not.

Proposition 5.16. *Suppose Γ is a pure subgroup of $E^{>0}$ and*

$$G = \{g \in K^{>0} : g^d \in \Gamma \text{ for some positive integer } d\}.$$

Then for all $a_1, \dots, a_n \in E^\times$ the equation $a_1x_1 + \cdots + a_nx_n = 1$ has the same nondegenerate solutions in Γ as in G .

Proof. By the previous lemma and a straightforward induction it suffices to show the following:

Let p be a prime number, and let $g \in K^{>0}$ be such that $g^p = \gamma \in \Gamma$ and $g \notin \Gamma$. Then the polynomial $X^p - \gamma \in E[X]$ is irreducible, and the subgroup of $K^{>0}$ generated by g over Γ is pure in $E(g)^{>0}$.

That $X^p - \gamma$ is irreducible in $E[X]$ follows from Theorem 9.1 on page 297 of [9]. Suppose $h \in E(g)^{>0}$ is such that $h \notin \Gamma$ and $h^d \in \Gamma$ where d is an integer > 1 . We can assume that $h^m \notin \Gamma$ for $1 \leq m < d$, and it remains to show that then $h = cg^k$ for some $c \in \Gamma$ and some integer k . By the minimality property of d and Theorem 9.1 in [9] the polynomial $X^d - h$ is irreducible in $E[X]$. Because $E(h) \subseteq E(g)$ and $[E(g) : E] = p$ this yields $d = p$. Let ζ be a primitive p^{th} root of unity in the algebraic closure of K , so $E(g) \cap E(\zeta) = E$ and $E(g, \zeta)$ is a cyclic extension of degree p of $E(\zeta)$. Let $\sigma \in \text{Gal}(E(g, \zeta) | E(\zeta))$ be given by $\sigma(g) = \zeta g$. Then $\sigma(h) = \zeta^k h$ with $0 < k < p$. Writing $h = c_0 + c_1 g + \cdots + c_{p-1} g^{p-1}$ with all $c_i \in E$ this gives

$$\begin{aligned} \sigma(h) &= c_0 + \zeta c_1 g + \cdots + \zeta^{p-1} c_{p-1} g^{p-1} \\ &= \zeta^k c_0 + \zeta^k c_1 g + \cdots + \zeta^k c_{p-1} g^{p-1}. \end{aligned}$$

This forces $c_i = 0$ for all $i \neq k$, so $h = c_k g^k$, as desired. \square

In particular, this yields the Mann property for subgroups of $\mathbb{R}^{>0}$ like $2^{\mathbb{Q}}$ and $2^{\mathbb{Q}}3^{\mathbb{Q}}$ in an effective way from the Mann property for $2^{\mathbb{Z}}$ and $2^{\mathbb{Z}}3^{\mathbb{Z}}$. In the next sections we consider the groups $2^{\mathbb{Z}}$ and $2^{\mathbb{Q}}$ as members of the same family, and likewise with $2^{\mathbb{Z}}3^{\mathbb{Z}}$ and $2^{\mathbb{Q}}3^{\mathbb{Q}}$.

The last result suggests the following question: *if Γ is a pure subgroup of E^\times with the Mann property and K is algebraically closed of characteristic zero, does it follow that the divisible hull*

$$\{g \in K^\times : g^d \in \Gamma \text{ for some positive integer } d\}$$

of Γ in K^\times has the Mann property? Maybe one should assume also that all roots of unity in E belong to Γ .

6. ALGEBRAICALLY CLOSED FIELDS WITH A MULTIPLICATIVE GROUP HAVING THE MANN PROPERTY

In this section K is an algebraically closed field and G is a subgroup of K^\times with the Mann property.

Smallness. In order to use the results in Section 3 we have to show that G is small in K . We shall derive this from the fact that no infinite field is interpretable in any abelian group. (“Interpretable in a structure \mathcal{M} ” means “definable in \mathcal{M}^{eq} .”) This fact follows from three other results:

- (1) Each abelian group is one-based; see [14], pp. 157–158.
- (2) If a group is interpretable in a one-based structure, then it has an abelian subgroup of finite index; see [14], Chapter 4.

- (3) if E is an infinite field, then the group $\mathrm{SL}_2(E)$ does not have an abelian subgroup of finite index; see [9], p. 589.

Lemma 6.1. *G is small in K .*

Proof. Suppose towards a contradiction that G is large in K . Then by Lemma 2.4, we have $K = f(G^m)$ where $f : K^m \rightarrow K$ is definable in K . Consider the equivalence relation E on K^m defined by

$$aEb \iff f(a) = f(b).$$

By Proposition 3.2 the equivalence relation $E_G := E \cap G^{2m}$ on G^m is definable in the group G . The restriction $f|_{G^m} : G^m \rightarrow K$ induces a bijection $G^m/E_G \rightarrow K$. Using again Proposition 3.2, one checks easily that the addition and multiplication of K correspond under this bijection to binary operations on G^m/E_G that are definable in the many-sorted structure G^{eq} where G is considered as a group. This contradicts the fact that no infinite field is interpretable in any abelian group. \square

In combination with Lemmas 3.5, 3.6 and Corollary 5.1 this yields:

Corollary 6.2. *The $\mathcal{L}(U)$ -structure (K, G) is stable. If the group G is ω -stable (superstable), then (K, G) is ω -stable (respectively, superstable).*

Here is another consequence (not used later) of the non-interpretability of infinite fields in abelian groups. Put

$$\begin{aligned} G_0 &:= G \cup \{0\} \subseteq K, \\ G^{+n} &:= G_0 + \cdots + G_0 \subseteq K \quad (\text{with } n \text{ summands}). \end{aligned}$$

Note that $G_0 = G^{+1} \subseteq G^{+2} \subseteq G^{+3} \subseteq \dots$

Corollary 6.3. *If G is infinite, then the increasing sequence of sets (G^{+n}) is strictly increasing.*

Proof. Assume towards a contradiction that $G^{+n} = G^{+(n+1)}$, $n \geq 1$. Then $G^{+n} = G^{+m}$ for all $m \geq n$. Hence $R := G^{+n} - G^{+n}$ is the subring of K generated by G , so this ring R can be interpreted in the multiplicative-monoid-with-additive-relations $G(\Sigma)$. Since G has the Mann property, it follows that the ring R , and thus its fraction field, can be interpreted in the abelian group G ; this is impossible if R is infinite. \square

As an application, for $G = 2^{\mathbb{Z}}3^{\mathbb{Z}} \cup -2^{\mathbb{Z}}3^{\mathbb{Z}}$, there is no n such that all rational numbers are of the form a/b with $a, b \in G^{+n}$; we do not know how to prove this particular fact other than by the argument above.

More on the ω -stable case. Let H be an infinite subgroup of the multiplicative group of a field. Then H has only finitely many elements of any given finite order, so by Macintyre [11], the group H is ω -stable if and only if there is an infinite divisible subgroup D of H and a finite subgroup B of H such that $H = DB$ and $D \cap B = \{1\}$. For such D and B we have $H^{[d]} = D$ for each positive integer d that is a multiple of $|B|$, so the subgroup D does

not depend on the particular product decomposition chosen; hence D is a definable subgroup of the group H . By Szmielew's quantifier simplification for abelian groups, D has no infinite proper subgroups definable in the group H . Thus, for ω -stable H , the subgroup D is the *connected component* of the group H , and $\text{MR}(H^n) = n$ for each n , where the Morley rank is with respect to the theory of the group H . We shall use these observations for $H := G$ to prove the following:

Theorem 6.4. *Suppose G is infinite and ω -stable. Then $\text{MR}(K) = \omega$, where the Morley rank is with respect to the ω -stable theory $\text{Th}(K, G)$.*

First we show that, with the assumptions of the theorem, $\text{MR}(G^{+n}) = n$. Next we use the analysis of 1-types in the proof of Lemma 3.5 to show that these types have Morley rank $\leq \omega$. We shall need the following basic fact about Morley rank in any, not necessarily ω -stable, structure $\mathcal{M} = (M, \dots)$:

Lemma 6.5. *Suppose \mathcal{M} is ω -saturated. Let $X \subseteq M^p$, $Y \subseteq M^q$, and $f : X \rightarrow Y$ be definable in \mathcal{M} such that $|f^{-1}(y)| < \infty$ for all $y \in Y$. Then $\text{MR}(X) \leq \text{MR}(Y)$.*

Proof. By induction on $\text{MR}(Y)$. The case that $\text{MR}(Y) \in \{-\infty, 0, +\infty\}$ is obvious, so we can assume $\text{MR}(Y)$ is an ordinal ≥ 1 , and make a further reduction to $\text{MD}(Y) = 1$. Saturation gives an n such that $|f^{-1}(y)| \leq n$ for all $y \in Y$. Suppose that $\text{MR}(X) > \text{MR}(Y)$. Take disjoint definable subsets X_1, \dots, X_{n+1} of X with $\text{MR}(X_i) \geq \text{MR}(Y)$ for all i . If $\text{MR}(f(X_i)) < \text{MR}(Y)$ for some i , then by the induction hypothesis,

$$\text{MR}(X_i) \leq \text{MR}(f(X_i)) < \text{MR}(Y)$$

for such i , a contradiction. Hence $\text{MR}(f(X_i)) = \text{MR}(Y)$ for all i . As $\text{MD}(Y) = 1$, there is an element y in the intersection $f(X_1) \cap \dots \cap f(X_{n+1})$, which contradicts $|f^{-1}(y)| \leq n$. \square

If $X \subseteq G^n$ is definable in (K, G) , then by Proposition 3.2, X is definable in the group G , so the Morley rank of X with respect to the theory of (K, G) equals its Morley rank with respect to the theory of the group G .

Lemma 6.6. *Let G be infinite and ω -stable. Then $\text{MR}(G^{+n}) = n$.*

Proof. We can assume that (K, G) is ω -saturated. Consider the map

$$f : G_0^n \rightarrow G^{+n}, \quad f(g_1, \dots, g_n) = g_1 + \dots + g_n.$$

By the surjectivity of f we have $\text{MR}(G^{+n}) \leq \text{MR}(G_0^n) = \text{MR}(G^n) = n$. For the opposite inequality we argue as follows: If $I \subseteq \{1, \dots, n\}$ is nonempty, then the set

$$G_I^n := \{(g_1, \dots, g_n) \in G^n : \sum_{i \in I} g_i = 0\}$$

is contained in the image of a definable map $G^{n-1} \rightarrow K^n$, so $\text{MR}(G_I^n) < n$. Thus $\text{MR}(G_{nd}^n) = \text{MR}(G^n) = n$, where

$$G_{nd}^n := G^n \setminus \bigcup_I G_I^n \quad (I \text{ ranging over the nonempty subsets of } \{1, \dots, n\})$$

is the set of “non-degenerate” elements of G^n . By the Mann property, the restriction of the map f to G_{nd}^n satisfies the condition in Lemma 6.5, so $\text{MR}(G_{nd}^n) \leq \text{MR}(G^{+n})$, and thus $n = \text{MR}(G^n) \leq \text{MR}(G^{+n})$. \square

We can now finish the proof of Theorem 6.4:

By Lemma 6.6 we have $\text{MR}(K) \geq \omega$. For the opposite inequality we can assume that (K, G) is \aleph_1 -saturated. Let (K', G') be a countable elementary substructure of (K, G) , let $\alpha \in K$, and let \mathbf{p} be the type of α in (K, G) over K' . It suffices to show that then $\text{MR}(\mathbf{p}) \leq \omega$. First consider the case that $\alpha \in K'(G)^{\text{ac}}$, say $\alpha \in K'(g)^{\text{ac}}$ where $g \in G^n$. Take a polynomial $P(X_1, \dots, X_n, Y) \in K'[X_1, \dots, X_n, Y]$ such that $P(g, Y) \neq 0$ and $P(g, \alpha) = 0$. Let

$$X := \{(h, a) \in G^n \times K : P(h, Y) \neq 0, P(h, a) = 0\},$$

a definable subset of K^{n+1} in (K, G) over K' . The map

$$(h, a) \mapsto h : X \rightarrow G^n$$

satisfies the condition of Lemma 6.5, so $\text{MR}(X) \leq \text{MR}(G^n) = n$. The map $(h, a) \mapsto a : X \rightarrow K$ is definable over K' and contains α in its image, so $\text{MR}(\mathbf{p}) \leq \text{MR}(X) \leq n$.

By the proof of Lemma 3.5, all elements of K not in $K'(G)^{\text{ac}}$ realize the same type in (K, G) over K' . The Morley rank of this type in (K, G) must be $\leq \omega$, since the other 1-types in (K, G) over K' were just shown to have finite Morley rank.

Definable sets. With a mild assumption on G the definable relations in (K, G) are boolean combinations of existentially definable relations. To formulate this precisely, recall that $G^{[d]}$ denotes the subgroup of d^{th} powers in G . Let $\mathcal{L}(K)$ be the language of rings augmented by names for the elements of K , and let $x = (x_1, \dots, x_m)$ be a tuple of distinct variables.

Proposition 6.7. *Suppose $G/G^{[d]}$ is finite for each integer $d > 0$. Then every subset of K^m definable in (K, G) is a boolean combination of subsets of K^m defined by formulas $\exists y(U(y) \wedge \phi(x, y))$ where $\phi(x, y)$ is a quantifier-free $\mathcal{L}(K)$ -formula.*

Proof. Consider a special formula

$$\psi(x) := \exists y(U(y) \wedge \theta_U(y) \wedge \phi(x, y))$$

in x where $\phi(x, y)$ is an \mathcal{L} -formula, $y = (y_1, \dots, y_n)$, and $\theta(y)$ is an $\mathcal{L}_m(\Sigma)$ -formula. By quantifier elimination for abelian groups, the set

$$\{(g_1, \dots, g_n) \in G^n : G \models \theta(g_1, \dots, g_n)\}$$

is a boolean combination of subsets of G^n of the form

$$\{(g_1, \dots, g_n) \in G^n : \chi_k(g_1, \dots, g_n) = 1\}, \text{ and} \\ \{(g_1, \dots, g_n) \in G^n : \chi_k(g_1, \dots, g_n) \in G^{[d]}\}$$

where $k = (k_1, \dots, k_n) \in \mathbb{Z}^n$ and d is a positive integer. (One can even restrict the d to range over powers p^e of prime numbers p with exponent $e \in \mathbb{N}$.) Since $G/G^{[d]}$ is finite, the complement in G^m of a set

$$\{(g_1, \dots, g_n) \in G^m : \chi_k(g_1, \dots, g_n) \in G^{[d]}\}$$

as above is a finite union of sets of the form

$$\{(g_1, \dots, g_n) \in G^m : \chi_k(g_1, \dots, g_n) \in \gamma G^{[d]}\}$$

where $\gamma \in G$. Hence $\psi(x)$ is equivalent in (K, G) to a formula

$$\psi'(x) := \exists z (U(z) \wedge \phi'(x, z))$$

where $\phi'(x, z)$ is an $\mathcal{L}(G)$ -formula, $z = (z_1, \dots, z_N)$. (Here $\mathcal{L}(G)$ is the language \mathcal{L} augmented by names for the elements of G .) Thus the desired result follows from Theorem 3.8 and quantifier elimination for algebraically closed fields. \square

Note that the assumption on G in the proposition is satisfied when G has finite rank, and also when G is divisible.

Elementary classification within the Γ -family. Let E be a field and Γ a subgroup of E^\times with the Mann property. All multiplicative groups that contain Γ and satisfy the Mann axioms of Γ are treated below as members of the same family, the Γ -family. For example, if $\Gamma = \{1\} \subseteq \mathbb{Q}^\times$, each subgroup of \mathbb{C}^\times generated by algebraically independent elements belongs to the Γ -family. Likewise, with $E = \mathbb{Q}$ and $\Gamma = 2^\mathbb{Z}$, the subgroups $2^\mathbb{Z}$ and $2^\mathbb{Q}$ of \mathbb{C}^\times belong to the Γ -family. The formal setting is as follows.

Let $\mathcal{L}(U, \Gamma)$ be the language of rings augmented by a unary relation symbol U , and by a name (constant symbol) γ for each element $\gamma \in \Gamma$. Let $\text{ACF}(\Gamma)$ be the theory in the language $\mathcal{L}(U, \Gamma)$ whose models are the structures $(K, G, (\gamma')_{\gamma \in \Gamma})$ such that

- (1) K is an algebraically closed field of the same characteristic as E ,
- (2) G is a subgroup of K^\times ,
- (3) $\gamma \mapsto \gamma' : \Gamma \rightarrow G$ is a group homomorphism,
- (4) $(K, G, (\gamma')_{\gamma \in \Gamma})$ satisfies the Mann axioms of Γ .

Here γ' is the interpretation of (the name of) γ in $(K, G, (\gamma')_{\gamma \in \Gamma})$. If E is algebraically closed, then $(E, \Gamma, (\gamma)_{\gamma \in \Gamma})$ is clearly a model of $\text{ACF}(\Gamma)$. The theory $\text{ACF}(\Gamma)$ is never complete, but we can classify its models up to elementary equivalence. Note that for a model $(K, G, (\gamma')_{\gamma \in \Gamma})$ of $\text{ACF}(\Gamma)$ we have a unique field embedding $\mathbb{F}(\Gamma) \rightarrow K$ that sends each $\gamma \in \Gamma$ to γ' ; from now on we identify $\mathbb{F}(\Gamma)$ with a subfield of K via this embedding, and accordingly write γ instead of γ' . Theorem 1.2 from the Introduction is the special case $K = \mathbb{C}$ and $G = \Gamma$ of the next result.

Theorem 6.8. *Let $(K, G, (\gamma))$ and $(K', G', (\gamma))$ be models of $\text{ACF}(\Gamma)$. Then $(K, G, (\gamma)) \equiv (K', G', (\gamma))$ if and only if $(G, (\gamma)) \equiv (G', (\gamma))$ as groups with distinguished elements.*

Proof. We just combine earlier results. The forward direction being obvious, suppose that $(G, (\gamma)) \equiv (G', (\gamma))$ as groups with distinguished elements. In order to obtain $(K, G, (\gamma)) \equiv (K', G', (\gamma))$ it suffices by Corollary 3.9 to show that

$$(G(\Sigma), (\gamma)) \equiv (G'(\Sigma), (\gamma)) \quad (\dagger)$$

as multiplicative monoids with additive relations and distinguished elements. Construe G as a Γ -set by the action

$$(\gamma, g) \mapsto \gamma g : \Gamma \times G \rightarrow G,$$

and construe G' likewise as a Γ -set. Let any $k \in \mathbb{Z}^n$ with $n \geq 1$ be given. Applying Corollary 5.1 for $E = \mathbb{F}$, we see that the set $\Sigma_k(G) \subseteq G^n$ is defined in the Γ -set G by a positive quantifier-free formula in the language of Γ -sets. Likewise, the set $\Sigma_k(G') \subseteq G'^n$ is defined in the Γ -set G' by a positive quantifier-free formula in the language of Γ -sets. More precisely, it follows from the *proof* of Corollary 5.1 that $\Sigma_k(G)$ and $\Sigma_k(G')$ are defined in the Γ -sets G and G' by the *same* positive quantifier-free formula in the language of Γ -sets. In particular, there is a formula in the language of groups with names for the elements of Γ that defines $\Sigma_k(G)$ in $(G, (\gamma))$ and that defines $\Sigma_k(G')$ in $(G', (\gamma))$. Hence (\dagger) holds, as desired. \square

Much of this section goes through when G is equipped with extra structure, for example, one or more distinguished subgroups of G or G^2 . The interested reader can easily make this precise as needed, using the results at the end of Section 3.

7. THE REAL CASE

The modifications needed to deal with the real case are not entirely obvious. One basic fact is that a subgroup of $\mathbb{R}^{>0}$ is either cyclic and discrete (and thus taken care of in [3]), or dense, in which case a result by Robinson and Zakon [18] on regular ordered abelian groups turns out to be relevant.

Let Γ be a subgroup of $\mathbb{R}^{>0}$ with the Mann property. Examples to keep in mind are $\Gamma = \{1\}$, $\Gamma = 2^{\mathbb{Z}}$, and $\Gamma = 2^{\mathbb{Z}}3^{\mathbb{Z}}$. Let $\mathcal{L}_o(U, \Gamma)$ be the language of ordered rings augmented by a unary relation symbol U and by a name (constant symbol) γ for each element $\gamma \in \Gamma$. The *ordering axioms* of Γ are the following: given any tuple $k = (k_1, \dots, k_n)$ of integers, and any tuple $\gamma = (\gamma_1, \dots, \gamma_n)$ of elements of Γ , $n \geq 1$, the ordering axiom for k, γ is the sentence

$$k_1\gamma_1 + \dots + k_n\gamma_n > 0$$

if this sentence holds in \mathbb{R} , and otherwise it is the sentence

$$k_1\gamma_1 + \dots + k_n\gamma_n \leq 0.$$

Let $\text{RCF}(\Gamma)$ be the theory in the language $\mathcal{L}_o(U, \Gamma)$ whose models are the structures $(K, G, (\gamma')_{\gamma \in \Gamma})$ such that

- (1) K is a real closed ordered field, and G is a dense subgroup of $K^{>0}$,

- (2) $\gamma \mapsto \gamma' : \Gamma \rightarrow G$ is a group homomorphism;
- (3) $(K, (\gamma')_{\gamma \in \Gamma})$ satisfies the ordering axioms of Γ ,
- (4) $(K, G, (\gamma')_{\gamma \in \Gamma})$ satisfies the Mann axioms of Γ .

Here γ' is the interpretation of (the name of) γ in $(K, G, (\gamma')_{\gamma \in \Gamma})$. If Γ is dense in $\mathbb{R}^{>0}$, then $(\mathbb{R}, \Gamma, (\gamma)_{\gamma \in \Gamma})$ is clearly a model of $\text{RCF}(\Gamma)$. The theory $\text{RCF}(\Gamma)$ is not complete; we shall classify its models up to elementary equivalence. To do this, we introduce $\mathbb{Q}(\Gamma)$, the ordered subfield of \mathbb{R} generated by Γ . Then we have for any model $(K, G, (\gamma')_{\gamma \in \Gamma})$ of $\text{RCF}(\Gamma)$ a unique ordered field embedding $\mathbb{Q}(\Gamma) \rightarrow K$ that sends each $\gamma \in \Gamma$ to γ' , and from now on we identify $\mathbb{Q}(\Gamma)$ with an ordered subfield of K via this embedding, and accordingly write γ' instead of γ . Theorem 1.3 from the Introduction is the special case $G = \Gamma$ of the next result.

Theorem 7.1. *Let $(K, G, (\gamma))$ and $(L, H, (\gamma))$ be models of $\text{RCF}(\Gamma)$. Then $(K, G, (\gamma)) \equiv (L, H, (\gamma))$ if and only if $[p]G = [p]H$ for every prime number p , and for each $\gamma \in \Gamma$ and each $n > 0$:*

$$\gamma \text{ is an } n^{\text{th}} \text{ power in } G \iff \gamma \text{ is an } n^{\text{th}} \text{ power in } H.$$

Some remarks on regularly dense groups. We are going to use the easy but important fact that if K is a real closed field and G is a dense subgroup of $K^{>0}$, then for each $n > 0$ the group of n^{th} powers of elements of G is dense in $K^{>0}$. It follows that such G is regularly dense as an ordered group in the sense of Robinson and Zakon [18], who classified regularly dense ordered abelian groups A up to elementary equivalence by their invariants $[p]A$ as defined in the introduction. The key step in their proof is needed below, and is as follows, where for simplicity we use additive notation for the abelian groups A in question (so $[p]A = |A/pA|$ if A/pA is finite, and $[p]A = \infty$ otherwise). Recall from [18] that an ordered abelian group A is said to be *regularly dense* if A is nontrivial and for all $a, b \in A$ with $a < b$ and all $n > 0$ there is $x \in A$ with $a < nx < b$.

Let A and B be regularly dense ordered abelian groups such that $[p]A = [p]B$ for each prime number p , and let $h : A' \rightarrow B'$ be an ordered abelian group isomorphism between a pure (ordered) subgroup A' of A and a pure (ordered) subgroup B' of B . Assume B is κ -saturated, where $\kappa > |A'|$. Let $a \in A \setminus A'$. Then there exists $b \in B \setminus B'$ such that for all $a' \in A'$, $k \in \mathbb{Z}$ and $n > 0$:

- (1) $a' < na \iff h(a') < nb$;
- (2) $a' + ka \in nA \iff h(a') + kb \in nB$.

Moreover, for any such b we can extend h to an ordered group isomorphism $A'\langle a \rangle \rightarrow B'\langle b \rangle$ sending a to b , where

$$A'\langle a \rangle := \left\{ \frac{a' + ka}{n} : a' \in A', k \in \mathbb{Z}, n > 0, a' + ka \in nA \right\} \subseteq A$$

inside the divisible hull of A , and where $B'\langle b \rangle$ is defined likewise.

Proof of Theorem 7.1. The “only if” part is obvious. For the “if” part, assume that $[p]G = [p]H$ for every prime number p , and that for each $\gamma \in \Gamma$ and $n > 0$:

$$\gamma \text{ is an } n^{\text{th}} \text{ power in } G \iff \gamma \text{ is an } n^{\text{th}} \text{ power in } H.$$

We can assume also that $(K, G, (\gamma))$ and $(L, H, (\gamma))$ are κ -saturated where κ is an uncountable cardinal $> |\Gamma|$. Let $\text{Sub}(K, G)$ be the collection of $\mathcal{L}_o(U)$ -structures (K', G') where K' is a real closed ordered subfield of K of cardinality $< \kappa$, $G' \subseteq K'^{>0}$ is a pure subgroup of G containing Γ , and K' and $\mathbb{Q}(G)$ are free over $\mathbb{Q}(G')$. Note that if $(K', G') \in \text{Sub}(K, G)$, then by Lemma 5.13 we have $(K', G') \subseteq (K, G)$, the field $\mathbb{Q}(G)$ is a regular extension of $\mathbb{Q}(G')$, and thus by Fact 2, K' and $\mathbb{Q}(G)$ are linearly disjoint over $\mathbb{Q}(G')$.

We define $\text{Sub}(L, H)$ likewise. Let \mathcal{I} be the set of all isomorphisms $\iota : (K', G') \cong (L', H')$ where $(K', G') \in \text{Sub}(K, G)$, $(L', H') \in \text{Sub}(L, H)$, and $\iota\gamma = \gamma$ for all $\gamma \in \Gamma$. We first show that $\mathcal{I} \neq \emptyset$: Let

$$\begin{aligned} G' &:= \{g \in G : g^n \in \Gamma \text{ for some } n > 0\}, & K' &:= \mathbb{Q}(\Gamma)^{\text{rc}} \subseteq K \\ H' &:= \{h \in H : h^n \in \Gamma \text{ for some } n > 0\}, & L' &:= \mathbb{Q}(\Gamma)^{\text{rc}} \subseteq L. \end{aligned}$$

Then $(K', G') \in \text{Sub}(K, G)$ and $(L', H') \in \text{Sub}(L, H)$, and the ordered field isomorphism $K' \cong L'$ that is the identity on Γ belongs to \mathcal{I} .

To establish the theorem, it remains to prove:

Claim. \mathcal{I} is a back-and-forth system.

To prove the claim, let $\iota : (K', G') \rightarrow (L', H')$ be in \mathcal{I} and let $\alpha \in K \setminus K'$; our task is to find an extension of ι in \mathcal{I} that contains α in its domain. We distinguish three cases:

(1) $\alpha \in G$: By the discussion preceding this proof we can pick a $\beta \in H$ such that for all $x \in G'$, $k \in \mathbb{Z}$ and $n > 0$ we have:

$$\alpha^k x \text{ is an } n^{\text{th}} \text{ power in } G \iff \beta^k \iota(x) \text{ is an } n^{\text{th}} \text{ power in } H.$$

We shall now adjust this β to make it realize the cut in L' that corresponds under ι to the cut of α in K' . By saturation, this cut in L' is realized in L by all elements of an entire interval (p, q) where $0 < p < q$ in L . Since H is dense in $L^{>0}$ we can assume that $p, q \in H$. Also by saturation, the elements $h \in H$ that are n^{th} powers in H for each $n > 0$ lie dense in H . Hence for a suitable such h we have $p < h\beta < q$. Put

$$\begin{aligned} K'' &:= K'(\alpha)^{\text{rc}}, & G'' &= K'' \cap G, \\ L'' &:= L'(h\beta)^{\text{rc}}, & H'' &= L'' \cap H. \end{aligned}$$

By the discussion on regularly dense groups preceding this proof, and by Lemmas 5.12 and 5.13 we have $(K'', G'') \in \text{Sub}(K, G)$, $(L'', H'') \in \text{Sub}(L, H)$ and an isomorphism $(K'', G'') \rightarrow (L'', H'')$ that takes α to $h\beta$.

(2) $\alpha \in K'(G)^{\text{rc}}$: Then $\alpha \in K'(g_1, \dots, g_n)^{\text{rc}}$ for some $g_1, \dots, g_n \in G$, so we can extend ι by applying (1) n times.

(3) $\alpha \notin K'(G)^{\text{rc}}$: As in the first case, we consider the cut of α in K' . By saturation and smallness of H we have $L'(H)^{\text{rc}} \neq L$, so there is a $\beta \in L \setminus L'(H)^{\text{rc}}$ that realizes the corresponding cut in L' . By linear disjointness, we can extend ι to an isomorphism $(K'', G') \rightarrow (L'', H')$ sending α to β , where $K'' = K'(\alpha)^{\text{rc}}$ and $L'' = L'(\beta)^{\text{rc}}$. In this case the freeness of K'' and $\mathbb{Q}(G)^{\text{rc}}$ over $\mathbb{Q}(G')^{\text{rc}}$ follows from the assumption that $\alpha \notin K'(G)^{\text{rc}}$. This concludes the proof of Theorem 7.1.

The assumption that Γ is a subgroup of $\mathbb{R}^{>0}$ was made just for the sake of concreteness, and can be dropped throughout this section by replacing \mathbb{R} by any real closed field R and assuming instead that Γ is a subgroup of $R^{>0}$ with the Mann property.

Induced structure on the group. In this subsection K is a real closed field and G is a dense subgroup of $K^{>0}$ with the Mann property. For *divisible* G we can describe the structure induced on G by (K, G) as follows:

Theorem 7.2. *Suppose G is divisible and $X \subseteq G^m$. Then X is definable in (K, G) if and only if $X = Y \cap G^m$ for some $Y \subseteq K^m$ definable in K .*

Proof. The “if” direction is clear. For the converse, it suffices by Fact 1 to prove:

Claim. Let (K_1, G_1) and (K_2, G_2) be two elementary extensions of (K, G) , and let $g_1 \in G_1^m$, $g_2 \in G_2^m$ realize the same types over K in K_1 and K_2 , respectively. Then g_1 and g_2 realize the same types over K in (K_1, G_1) and (K_2, G_2) , respectively.

We may assume that (K_i, G_i) is κ -saturated for $i = 1, 2$, where $\kappa > |K|$ is an uncountable cardinal. Note that $(K_1, G_1, (g)_{g \in G})$ and $(K_2, G_2, (g)_{g \in G})$ are elementarily equivalent models of $\text{RCF}(G)$, and thus we have a back-and-forth system \mathcal{I} between (K_1, G_1) and (K_2, G_2) as defined in the proof of Theorem 7.1. Also K and $\mathbb{Q}(G_i)$ are free over $\mathbb{Q}(G)$, and G_i is divisible for $i = 1, 2$.

Put $K'_i := K(g_i)^{\text{rc}}$, $G'_i := K'_i \cap G_i$, ($i = 1, 2$). By Lemmas 5.12 and 5.13,

$$G'_i = \{(gg_i^k)^{1/n} \in K_i^{>0} : g \in G, k \in \mathbb{Z}^m, n > 0\}, \quad (i = 1, 2).$$

Since g_1 and g_2 realize the same type over K we have an ordered field isomorphism $\iota : K'_1 \rightarrow K'_2$ fixing K pointwise and taking g_1 to g_2 . Hence $\iota(G'_1) = G'_2$, so ι is an isomorphism between (K'_1, G'_1) and (K'_2, G'_2) .

It is easy to check that K'_i and $\mathbb{Q}(G_i)$ are free over $\mathbb{Q}(G'_i)$, and G'_i is a pure subgroup of G_i . Thus $(K'_i, G'_i, (g)_{g \in G}) \in \text{Sub}(K_i, G_i)$ for $i = 1, 2$ and ι is in \mathcal{I} . Therefore by the proof of Theorem 7.1, g_1 and g_2 realize the same types over K in (K_1, G_1) and (K_2, G_2) respectively. This finishes the proof of the claim and of the theorem. \square

By “ G with its induced structure” we mean the ordered group G equipped with the relations $X \subseteq G^m$ that are definable in (K, G) , ($m = 1, 2, \dots$).

Corollary 7.3. *If G is divisible, then G with its induced structure is weakly o-minimal, even in the strong sense that its theory is weakly o-minimal.*

We also note the following converse of the theorem above:

Corollary 7.4. *Suppose every set $X \subseteq G$ definable in (K, G) is of the form $Y \cap G$ with $Y \subseteq K$ definable in K . Then G is divisible.*

This is because the assumption here implies weak o-minimality of the ordered group G , which in turn implies the divisibility of G .

Definable sets. In this subsection K is a real closed field and G is a dense subgroup of $K^{>0}$ with the Mann property. With a mild assumption on G , the definable relations in (K, G) are boolean combinations of existentially definable relations. To formulate this precisely, let $\mathcal{L}_o(K)$ be the language of ordered rings augmented by names for the elements of K , and let $x = (x_1, \dots, x_m)$ be a tuple of distinct variables.

Theorem 7.5. *Suppose that $[p]G$ is finite for each prime number p . Then every subset of K^m definable in (K, G) is a boolean combination of subsets of K^m defined in (K, G) by formulas $\exists y(U(y) \wedge \phi(x, y))$ where $\phi(x, y)$ is a quantifier-free $\mathcal{L}_o(K)$ -formula.*

We shall derive this from a real analogue of the relative quantifier elimination of Section 3. The key here is the back-and-forth system constructed in the proof of Theorem 7.1.

To eliminate quantifiers for $\text{RCF}(\Gamma)$ we extend this theory by definitions to an $\mathcal{L}_o(U, \Gamma, \Sigma)$ -theory $\text{RCF}(\Gamma, \Sigma)$ by adding for each $k \in \mathbb{Z}^n$ with $n \geq 1$ the n -ary relation symbol Σ_k with the same defining axiom as in Section 3. Thus each model $(K, G, (\gamma))$ of $\text{RCF}(\Gamma)$ expands uniquely to a model of $\text{RCF}(\Gamma, \Sigma)$, and we shall denote this expansion also by $(K, G, (\gamma))$. Note that $\mathcal{L}_o(U, \Gamma, \Sigma)$ has the sublanguge $\mathcal{L}_{\text{om}}(\Gamma, \Sigma)$, the language of ordered multiplicative monoids with additive relations and a name for each element of Γ . Given a model $(K, G, (\gamma))$ of $\text{RCF}(\Gamma)$, we let $G(\Sigma)$ be the ordered multiplicative monoid G with additive relations given by the defining axioms for the Σ_k 's, and with a copy of Γ inside, construed as $\mathcal{L}_{\text{om}}(\Gamma, \Sigma)$ -structure.

The U -restriction of an $\mathcal{L}_{\text{om}}(\Gamma, \Sigma)$ -formula $\theta(y)$ is an $\mathcal{L}_o(U, \Gamma, \Sigma)$ -formula $\theta_U(y)$; it is defined by the same recursive clauses as used in Section 3 to define the U -restriction of an $\mathcal{L}_m(\Sigma)$ -formula $\theta(y)$. Note that for an $\mathcal{L}_{\text{om}}(\Gamma, \Sigma)$ -formula $\theta(y)$ with $y = (y_1, \dots, y_n)$, a model $(K, G, (\gamma))$ of $\text{RCF}(\Gamma, \Sigma)$, and $g \in G^n$ we have

$$G(\Sigma) \models \theta(g) \iff (K, G, (\gamma)) \models \theta_U(g).$$

A *special* formula in x is by definition an $\mathcal{L}_o(U, \Gamma, \Sigma)$ -formula $\eta(x)$ of the form

$$\exists y(U(y) \wedge \theta_U(y) \wedge \phi(x, y))$$

for some $\mathcal{L}_{\text{om}}(\Gamma, \Sigma)$ -formula $\theta(y)$ and some $\mathcal{L}_o(\Gamma)$ -formula $\phi(x, y)$, where $y = (y_1, \dots, y_n)$ is a tuple of variables.

Lemma 7.6. *Each $\mathcal{L}_o(U, \Gamma, \Sigma)$ -formula $\psi(x)$ is equivalent in $\text{RCF}(\Gamma, \Sigma)$ to a boolean combination of special formulas in x .*

Proof. Let κ be an uncountable cardinal $> |\Gamma|$, let $(K, G, (\gamma))$ and $(L, H, (\gamma))$ be κ -saturated models of $\text{RCF}(\Gamma, \Sigma)$ and let $\alpha = (\alpha_1, \dots, \alpha_m) \in K^m$, and $\beta = (\beta_1, \dots, \beta_m) \in L^m$ satisfy (in $(K, G, (\gamma))$ and $(L, H, (\gamma))$, respectively) the same special formulas in x . Using Fact 1, it suffices to derive from this assumption that

$$\text{tp}_{(K, G, (\gamma))}(\alpha) = \text{tp}_{(L, H, (\gamma))}(\beta).$$

The assumption on α and β easily yields that $[p]G = [p]H$ for every prime number p , and for each $\gamma \in \Gamma$ and each $n > 0$:

$$\gamma \text{ is an } n^{\text{th}} \text{ power in } G \iff \gamma \text{ is an } n^{\text{th}} \text{ power in } H.$$

Hence we have a back-and-forth system \mathcal{I} between (K, G) and (L, H) as constructed in the proof of Theorem 7.1. It remains to find an element of \mathcal{I} that has each α_j in its domain and sends α to β .

Let $\mathbb{Q}(G)(\alpha)$ have transcendence degree r over $\mathbb{Q}(G)$; we can assume that $\alpha_1, \dots, \alpha_r$ are algebraically independent over $\mathbb{Q}(G)$. As in the proof of Theorem 3.8 it follows that then $\mathbb{Q}(H)(\beta)$ has transcendence degree r over $\mathbb{Q}(H)$, and that β_1, \dots, β_r are algebraically independent over $\mathbb{Q}(H)$.

Let $\kappa_0 := \aleph_0$ if Γ is countable, including the case $\Gamma = \{1\}$, and $\kappa_0 := |\Gamma|$ otherwise; so $\kappa_0 < \kappa$. Take a subgroup G' of G containing Γ , of cardinality κ_0 , such that $G'(\Sigma) \preceq G(\Sigma)$ and α has transcendence degree r over $\mathbb{Q}(G')$. It follows that G' is a pure subgroup of G . Let $g = (g_i : i < \kappa_0)$ be an enumeration of G' , and $y = (y_i : i < \kappa_0)$ a list of distinct variables. Note that if $\theta_1(y), \dots, \theta_k(y)$ are $\mathcal{L}_{\text{om}}(\Gamma, \Sigma)$ -formulas and $\phi_1(x, y), \dots, \phi_k(x, y)$ are $\mathcal{L}_o(\Gamma)$ -formulas such that $G(\Sigma) \models \theta_j(g)$ and $K \models \phi_j(\alpha, g)$ for $j = 1, \dots, k$, then

$$(K, G, (\gamma)) \models \exists y (U(y) \wedge \theta_U(y) \wedge \phi(\alpha, y)), \quad \text{where}$$

$$\theta(y) := \bigwedge_j \theta_j(y), \quad \phi(x, y) := \bigwedge_j \phi_j(x, y).$$

So $(L, H, (\gamma)) \models \exists y (U(y) \wedge \theta_U(y) \wedge \phi(\beta, y))$. Hence we have a partial y -type over β in $(L, H, (\gamma))$ consisting of the formulas $U(y_i)$ for $i < \kappa_0$, the formulas $\theta_U(y)$ such that $G(\Sigma) \models \theta(g)$ with $\theta(y)$ an $\mathcal{L}_{\text{om}}(\Gamma, \Sigma)$ -formula, and the formulas $\phi(\beta, y)$ such that $K \models \phi(\alpha, g)$ with $\phi(x, y)$ an $\mathcal{L}_o(\Gamma)$ -formula. Let $h = (h_i : i < \kappa_0)$ realize this y -type in $(L, H, (\gamma))$. This yields a partial elementary map $g_i \mapsto h_i$, $i < \kappa_0$, between $G(\Sigma)$ and $H(\Sigma)$. Put $H' := \{h_i : i < \kappa_0\}$. Then H' is a subgroup of H such that $H'(\Sigma) \preceq H(\Sigma)$, and we have an ordered field isomorphism $\iota : \mathbb{Q}(G')(\alpha) \cong \mathbb{Q}(H')(\beta)$ sending each g_i to h_i and each α_j to β_j . Put $K' := \mathbb{Q}(G')(\alpha)^{\text{rc}}$ and $L' := \mathbb{Q}(H')(\beta)^{\text{rc}}$. Then $(K', G') \in \text{Sub}(K, G)$ and $(L', H') \in \text{Sub}(L, H)$ and we have an isomorphism $(K', G') \cong (L', H')$ that extends ι . This isomorphism carries α to β and belongs to the back-and-forth system \mathcal{I} , so we are done. \square

In order to derive Theorem 7.5 from this lemma we briefly return to the theory of regularly dense ordered abelian groups. Let for each prime number p a number $e(p) \in \mathbb{N} \cup \{\infty\}$ be given. As noted in [18], there exists an ordered additive dense subgroup A of \mathbb{R} such that $[p]A = p^{e(p)}$ for each prime number p , in particular, A is a regularly dense ordered abelian group, and thus $\exp(A)$ is a dense ordered subgroup of $\mathbb{R}^{>0}$. Here we note:

Lemma 7.7. *The (complete) theory of regularly dense ordered abelian groups A such that $[p]A = p^{e(p)}$ for all prime numbers p , admits elimination of quantifiers after extending it by definitions as follows: augment its language $\{<, 0, -, +\}$ by extra unary predicates D_n ($n > 0$), with defining axioms*

$$\forall x(D_n(x) \leftrightarrow \exists y(x = ny)).$$

This follows easily from our earlier remark on the extendability of isomorphisms between pure ordered subgroups of models of the theory in question. (Robinson and Zakon [18] state model completeness but not the stronger quantifier eliminability.)

Proof of Theorem 7.5. Consider a formula

$$\psi(x) := \exists y(U(y) \wedge \theta_U(y) \wedge \phi(x, y))$$

where $\phi(x, y)$ is an \mathcal{L}_o -formula, $y = (y_1, \dots, y_n)$, and $\theta(y)$ is an $\mathcal{L}_{\text{om}}(\Sigma)$ -formula. By the above quantifier elimination for the ordered group G , the set

$$\{(g_1, \dots, g_n) \in G^n : G \models \theta(g_1, \dots, g_n)\}$$

is a boolean combination of subsets of G^n of the form

$$\begin{aligned} &\{(g_1, \dots, g_n) \in G^n : \chi_k(g_1, \dots, g_n) = 1\}, \\ &\{(g_1, \dots, g_n) \in G^n : \chi_k(g_1, \dots, g_n) < 1\} \text{ and} \\ &\{(g_1, \dots, g_n) \in G^n : \chi_k(g_1, \dots, g_n) \in G^{[d]}\} \end{aligned}$$

where $k = (k_1, \dots, k_n) \in \mathbb{Z}^n$ and d is a positive integer. (One can even restrict the d to range over powers p^e of prime numbers p with exponent $e \in \mathbb{N}$.) Since $G/G^{[d]}$ is finite, the complement in G^n of a set

$$\{(g_1, \dots, g_n) \in G^n : \chi_k(g_1, \dots, g_n) \in G^{[d]}\}$$

as above is a finite union of sets of the form

$$\{(g_1, \dots, g_n) \in G^n : \chi_k(g_1, \dots, g_n) \in \gamma G^{[d]}\}$$

where $\gamma \in G$. Hence $\psi(x)$ is equivalent in (K, G) to a formula

$$\psi'(x) := \exists z(U(z) \wedge \phi'(x, z))$$

where $\phi'(x, z)$ is an $\mathcal{L}_o(G)$ -formula, $z = (z_1, \dots, z_N)$. (Here $\mathcal{L}_o(G)$ is the language \mathcal{L}_o augmented by names for the elements of G .) The desired result now follows from Lemma 7.6, and quantifier elimination for real closed ordered fields. This concludes the proof.

Question: do the results in this section have good analogues for structures like $(\mathbb{R}, 2^{\mathbb{Z}}, 3^{\mathbb{Z}})$ and $(\mathbb{R}, 2^{\mathbb{Q}}, 3^{\mathbb{Q}})$? This question was raised at the end of [3], but comes up in a very different way in [13]. Note that $(\mathbb{C}, 2^{\mathbb{Z}}, 3^{\mathbb{Z}})$ can be viewed as (\mathbb{C}, Γ^*) where Γ is the group $2^{\mathbb{Z}}3^{\mathbb{Z}}$ with distinguished subgroups $2^{\mathbb{Z}}$ and $3^{\mathbb{Z}}$, so the complex version of the question is under control.

8. MORE ON THE MANN PROPERTY

We present here some natural examples of groups of *infinite* rank for which the Mann property holds *effectively*. We also show that the Mann property holds effectively in the cyclic case. This yields the decidability of some of the theories discussed in the previous two sections. We conclude with a discussion of the positive characteristic case.

The group of exponentials of algebraic numbers. Let A be the field of algebraic numbers in \mathbb{C} . Then the subgroup $\exp(A)$ of \mathbb{C}^\times has the strongest possible Mann property:

Proposition 8.1. *For any $c_1, \dots, c_m \in \mathbb{Q}^\times$, the equation*

$$c_1x_1 + \dots + c_mx_m = 1$$

has the same nondegenerate solutions in $\exp(A)$ as in $\{1\}$.

To see this we use the following lemma where we assume K is a field with subfield E , and G and Γ are subgroups of K^\times with $\Gamma \subseteq G$.

Lemma 8.2. *Suppose Γ is a pure subgroup of G and each root of unity in G lies in Γ . Then the following two conditions are equivalent:*

- (1) *for any $c_1, \dots, c_m \in E^\times$ the equation $c_1x_1 + \dots + c_mx_m = 1$ has the same nondegenerate solutions in Γ as in G ;*
- (2) *whenever $g_1, \dots, g_n \in G$ are multiplicatively independent over Γ , they are algebraically independent over $E(\Gamma)$.*

Proof. The implication (1) \Rightarrow (2) is part of Lemma 5.12. Assume (2). Note that by the hypothesis on Γ the quotient G/Γ is torsion-free. To prove (1) we can further reduce to the case that this quotient group is finitely generated. Hence there are $g_1, \dots, g_n \in G$ that generate G over Γ and are multiplicatively independent over Γ . Then g_1, \dots, g_n are algebraically independent over $E(\Gamma)$. Now apply Lemma 5.14. \square

To obtain Proposition 8.1 we apply this lemma with $K = \mathbb{C}$, $E = \mathbb{Q}$, $\Gamma = \{1\}$ and $G = \exp(A)$ using Lindemann's theorem [9] that if $a_1, \dots, a_n \in A$ are linearly independent over \mathbb{Q} , then $\exp(a_1), \dots, \exp(a_n)$ are algebraically independent (which in particular yields the injectivity of $\exp|_A$).

Corollary 8.3. *The elementary theories of $(\mathbb{C}, \exp A)$ and $(\mathbb{R}, \exp(A \cap \mathbb{R}))$ are decidable.*

Algebraic independence for Teichmüller representatives. In this subsection we fix a prime number p and let $\mathbf{k} \supseteq \mathbb{F}_p$ be a perfect field of characteristic p . Let $W[\mathbf{k}]$ denote the ring of Witt vectors over \mathbf{k} , let $\tau : \mathbf{k} \rightarrow W[\mathbf{k}]$ be the Teichmüller character, and $\pi : W[\mathbf{k}] \rightarrow \mathbf{k}$ the residue map (so $\pi \circ \tau = \text{id}_{\mathbf{k}}$). We consider $W[\mathbf{k}]$ as a ring extension of $W[\mathbb{F}_p] = \mathbb{Z}_p$; thus the fraction field $W(\mathbf{k})$ of $W[\mathbf{k}]$ is a field extension of the fraction field \mathbb{Q}_p of \mathbb{Z}_p .

Theorem 8.4. *Put $T := \tau(\mathbf{k}^\times)$, a subgroup of $W(\mathbf{k})^\times$. Then*

- (1) *T has the Mann property;*
- (2) *whenever $a_1, \dots, a_n \in \mathbf{k}^\times$ are multiplicatively independent, then their images $\tau(a_1), \dots, \tau(a_n)$ are algebraically independent over \mathbb{Q}_p .*

Proof. By extending \mathbf{k} we can make \mathbf{k} algebraically closed so that \mathbb{F}_p^{ac} is an elementary substructure of \mathbf{k} . By [5] this makes the two-sorted structure $(W[\mathbb{F}_p^{\text{ac}}], \mathbb{F}_p^{\text{ac}}; \pi, \tau)$ an elementary substructure of $(W[\mathbf{k}], \mathbf{k}; \pi, \tau)$. (Here the underlying sets of the two sorts are indicated on the left of the semicolon and are equipped with their ring structure, and π and τ indicate the obvious maps between these one-sorted reducts.) The subgroup $\tau(\mathbb{F}_p^{\text{ac}\times})$ of $W(\mathbb{F}_p^{\text{ac}})^\times$ consists of roots of unity, so by [12] it has the Mann property. Now (1) and (2) follow from $(W[\mathbb{F}_p^{\text{ac}}], \mathbb{F}_p^{\text{ac}}; \pi, \tau) \preceq (W[\mathbf{k}], \mathbf{k}; \pi, \tau)$ and Lemma 5.12. \square

This ties up a loose end from [5]. At the end of that paper, the first author related a comment by Hrushovski to the effect that all \mathbb{Z} -linear relations between elements of T are generated by the \mathbb{Z} -linear relations among the roots of unity in T . The reference to [7], however, did not suffice for the first author to understand this comment. The argument above might be different from what Hrushovski had in mind.

Incidentally, the complete axiomatization in [5] of structures like $(W[\mathbf{k}], T)$ contains a red herring, namely an axiom scheme that describes the \mathbb{Z} -linear relations among the elements of T . This axiom scheme is never used in the proof of the Theorem in [5]! To set the record straight, here is what this proof gives:

Theorem 8.5. *Consider the $\mathcal{L}(U)$ -theory whose models are the structures (B, G) such that B is a henselian valuation ring with fraction field of characteristic 0, perfect residue field \mathbf{k} of characteristic $p > 0$, maximal ideal pB , and such that $G \subseteq B$ is closed under multiplication and is mapped bijectively onto \mathbf{k}^\times by the residue map $B \rightarrow \mathbf{k}$.*

Two models of this theory are elementarily equivalent if and only if their residue fields are and their value groups are.

Here the *value group* of a model (B, G) is the value group of the valuation on the fraction field of B that has B as its valuation ring, and this value group is viewed as an ordered abelian group. The notation used here is a tiny bit different from that in [5], where $(B, G \cup \{0\})$ instead of (B, G) is considered.

Theorem 8.4 now has the following variant:

Corollary 8.6. *Let (B, G) be as in Theorem 8.5, and let K be the fraction field of B . Then G is a subgroup of K^\times with the Mann property, and whenever $g_1, \dots, g_n \in G$ are multiplicatively independent, then g_1, \dots, g_n are algebraically independent (over the prime field \mathbb{Q}).*

Proof. Passing to a suitable algebraic extension field of K and replacing B by its integral closure in that extension (without changing the residue field or G) we can arrange that the value group is a \mathbb{Z} -group, so that $(B, G) \equiv (W[\mathbf{k}], T)$. Now apply Theorem 8.4. \square

Effectiveness of the Mann property in the cyclic case. The proofs in [6], [10] and [17] that finitely generated multiplicative groups in characteristic zero have the Mann property are not effective. Here we give an effective proof in the cyclic case. Let K be a field and $a \in K^\times$.

Proposition 8.7. *The group $a^\mathbb{Z}$ has the Mann property.*

Proof. This is obvious when K has characteristic $p > 0$, and also when K has characteristic 0 and a is either a root of unity or transcendental over \mathbb{Q} . Assume that K has characteristic 0 and a is algebraic over \mathbb{Q} but not a root of unity. Then we have an absolute value $|\cdot|$ on the field $\mathbb{Q}(a)$ such that $|a| > 1$. Consider a tuple $k = (k_1, \dots, k_n) \in \mathbb{Z}^n$ of nonzero integers, $n \geq 1$, and define $E(k)$ as the set of all tuples $(e_1, \dots, e_n) \in \mathbb{N}^n$ such that $0 = e_1 < \dots < e_n$, $k_1 a^{e_1} + \dots + k_n a^{e_n} = 0$ and $k_1 a^{e_1} + \dots + k_m a^{e_m} \neq 0$ for each positive $m < n$. It suffices to show that then $E(k)$ is finite. Let $(e_1, \dots, e_n) \in E(k)$. Note that $n > 1$. By descending induction on positive $m < n$ we shall obtain a bound $B(m) \in \mathbb{R}^{>0}$, depending only on k, m, n, a but not on (e_1, \dots, e_n) , such that that $e_{m+1} - e_m \leq B(m)$. From

$$k_1 + \dots + k_{n-1} a^{e_{n-1}} + k_n a^{e_n} = 0$$

we obtain $|k_n| |a|^{e_n} \leq (|k_1| + \dots + |k_{n-1}|) |a|^{e_{n-1}}$, so

$$e_n - e_{n-1} \leq \log_{|a|} \frac{|k_0| + \dots + |k_{n-1}|}{|k_n|}.$$

If the base $|a|$ logarithm on the right hand side is < 1 , then $E(k) = \emptyset$. Assume it is ≥ 1 and denote it by $B(n-1)$. Let $1 < m < n$, and suppose $B(m), B(m+1), \dots, B(n-1) \in \mathbb{R}^{>0}$ have the desired property. Let α be the least of the numbers

$$|k_m + k_{m+1} a^{i(m+1)} + \dots + k_n a^{i(n)}|$$

such that $0 < i(m+1) < \dots < i(n)$ and

$$i(m+j) \leq B(m) + \dots + B(m+j-1) \text{ for } j = 1, \dots, n-m.$$

Then $k_1 + \dots + k_{m-1} a^{e_{m-1}} + a^{e_m} (k_m + k_{m+1} a^{i(m+1)} + \dots + k_n a^{i(n)}) = 0$ with $i(m+1) := e_{m+1} - e_n, \dots, i(n) := e_n - e_m$, so

$$|a|^{e_m} \alpha \leq (|k_1| + \dots + |k_{m-1}|) |a|^{e_{m-1}}.$$

Hence

$$e_m - e_{m-1} \leq \log_{|a|} \frac{|k_1| + \cdots + |k_{m-1}|}{\alpha}.$$

If the base $|a|$ logarithm on the right hand side is < 1 , then $E(k) = \emptyset$. Assume it is ≥ 1 and denote it by $B(m-1)$. This bound has the required property. \square

This proof is effective: it leads to an algorithm that, given any irreducible polynomial $f(T) \in \mathbb{Q}[T]$, decides whether $f(\zeta) = 0$ for some root of unity $\zeta \in \mathbb{C}$, and if not, constructs for $a \in \mathbb{C}$ such that $f(a) = 0$ and any tuple $k \in \mathbb{Z}^n$ of nonzero integers, $n \geq 1$, the finite set $E(k)$ defined in the proof above.

Corollary 8.8. *Given any $a \in \mathbb{C}^\times$, the elementary theory of $(\mathbb{C}, a^{\mathbb{Z}})$ is decidable. Given any algebraic $a \in \mathbb{R}^{>0}$, the elementary theory of $(\mathbb{R}, a^{\mathbb{Z}})$ is decidable.*

The second claim depends also on a remark at the end of [3].

The positive characteristic case. Let p be a prime number. While the multiplicative group of \mathbb{F}_p^{ac} is of rank 0, it fails, of course, to have the Mann property. But we can use Lemma 5.15 to produce a natural class of infinite subgroups of this multiplicative group with the Mann property.

Recall that each nonzero $a \in \mathbb{F}_p^{\text{ac}}$ is a primitive N^{th} root of unity for a unique positive integer N , and that this N is not divisible by p . Conversely, for each positive integer N not divisible by p there is a primitive N^{th} root of unity in \mathbb{F}_p^{ac} .

Theorem 8.9. *Let P be a finite set of prime numbers $\neq p$, and let $S(P)$ be the set of positive integers all whose prime factors are in P . Then the subgroup*

$$G := \{a \in \mathbb{F}_p^{\text{ac}} : a^N = 1 \text{ for some } N \in S(P)\}$$

of the multiplicative group of \mathbb{F}_p^{ac} has the Mann property.

Proof. Take a power $q = p^e$ with $e \geq 1$ such that $l|q-1$ for all odd $l \in P$, and $4|q-1$ in case $2 \in P$. For each $l \in P$, take a primitive $(l^n)^{\text{th}}$ root of unity $\zeta(l)$ in \mathbb{F}_q where $l^n|q-1$ and $l^{n+1} \nmid q-1$, so $n = n(l) \geq 1$.

Claim. Let Γ be the subgroup of \mathbb{F}_q^\times generated by the $\zeta(l)$ with $l \in P$. Then G has the “same” Mann property over \mathbb{F}_q as its finite subgroup Γ , that is, each equation $a_1x_1 + \cdots + a_mx_m = 1$ with $m \geq 1$ and all $a_i \in \mathbb{F}_q^\times$ has the same nondegenerate solutions in Γ as in G .

To prove this claim, consider an $l \in P$, and let $n = n(l)$. Then \mathbb{F}_q does not contain a primitive $(l^{n+1})^{\text{th}}$ root of unity. But $l^{n+1}|q^l-1$, so the extension \mathbb{F}_{q^l} of \mathbb{F}_q does have a primitive $(l^{n+1})^{\text{th}}$ root of unity x with $x^l = \zeta(l)$, and has prime degree l over \mathbb{F}_q , hence the polynomial $X^l - \zeta(l) \in \mathbb{F}_q[X]$ is irreducible. Moreover, $l^{n+2} \nmid q^l-1$, and if $\lambda \in P$, $\lambda \neq l$, then $\lambda^{\nu+1} \nmid q^l-1$

with $\nu := n(\lambda)$. Let Γ' be the subgroup of $\mathbb{F}_{q^l}^\times$ generated by Γ and an x with $x^l = \zeta(l)$. Then $\Gamma' \subseteq G$ has the same Mann property over \mathbb{F}_q as Γ , by Lemma 5.15. Also, Γ' is the subgroup of $\mathbb{F}_{q^l}^\times$ generated by this x and the $\zeta(\lambda)$ with $\lambda \in P$, $\lambda \neq l$. Thus the procedure that took as input \mathbb{F}_q, Γ and produced $\mathbb{F}_{q^l}, \Gamma'$ can be repeated by taking the latter as a new input (and instead of l any element of P). In this way we produce larger and larger subgroups of G with the same Mann property as Γ over \mathbb{F}_q . Taking a suitable union we get all of G . \square

This proof is effective, so the elementary theory of $(\mathbb{F}_p^{\text{ac}}, G)$ is decidable for G as in the theorem. Note that the group G in the theorem is isomorphic to the direct product of the Prüfer groups $\mathbb{Z}(l^\infty)$ with $l \in P$; in particular, G is divisible, and thus $(\mathbb{F}_p^{\text{ac}}, G)$ is ω -stable.

Question: are there subgroups of the multiplicative group of \mathbb{F}_p^{ac} with the Mann property that are not contained in any G as in the theorem?

We finish by characterizing the multiplicative groups in extension fields of \mathbb{F}_p with the Mann property in terms of their algebraic parts:

Proposition 8.10. *Let K be any extension field of \mathbb{F}_p , and let G be a subgroup of K^\times . Then G has the Mann property if and only if the following two conditions are satisfied:*

- (1) *its subgroup $\Gamma := \{\gamma \in G : \gamma \text{ is algebraic over } \mathbb{F}_p\}$ has the Mann property;*
- (2) *whenever $g_1, \dots, g_n \in G$ are multiplicatively independent, they are algebraically independent over \mathbb{F}_p .*

Proof. Suppose G has the Mann property. Then, given any $c_1, \dots, c_m \in \mathbb{F}_p$ the equation $c_1x_1 + \dots + c_mx_m = 1$ has the same nondegenerate solutions in Γ as in G : a nondegenerate solution in G outside Γ would produce infinitely many nondegenerate solutions in G by applying powers of the Frobenius map to the solution. Thus (1) and (2) hold by Lemma 8.2.

Conversely, if (1) and (2) hold, then G has the Mann property, again by Lemma 8.2. \square

Final comments. After submitting the paper we learned of overlap with existing work: Boxall [1] and Scanlon and Voloch [19] contain Theorem 8.9 (with very different proofs from ours), and [19] also answers the question just before Proposition 8.10 affirmatively, assuming two widely believed conjectures in number theory. Poizat [16] contains special cases of Theorem 6.8.

REFERENCES

- [1] J. BOXALL *Sous-variétés algébriques de variétés semi-abéliennes sur un corps fini*, Number Theory (Paris 1992–1993), 69–80, London Math. Soc. Lecture Note Ser., 215, Cambridge Univ. Press, Cambridge, 1995.
- [2] E. CASANOVAS, M. ZIEGLER, *Stable theories with a new predicate*, Journal of Symbolic Logic **66** (2001), no.3, 1127–1140.

- [3] L. VAN DEN DRIES, The field of reals with a predicate for the powers of two, *Manuscripta Math.* **54** (1985), 187–195.
- [4] L. VAN DEN DRIES, Dense pairs of o-minimal structures, *Fund. Math.* **157** (1998), 61–78.
- [5] L. VAN DEN DRIES, On the elementary theory of rings of Witt vectors with a multiplicative set of representatives for the residue field, *Manuscripta Math.* **98** (1999), 133–137.
- [6] J.H. EVERTSE, On sums of S-units and linear recurrences, *Compositio Math.* **53** (1984), 225–244.
- [7] E. HRUSHOVSKI, The Manin-Mumford conjecture and the model theory of difference fields, *Ann. Pure Appl. Logic* **112** (2001), 43–115.
- [8] H.J. KEISLER, Complete theories of algebraically closed fields with distinguished subfields, *Michigan Math. J.* **11** (1964), 71–81.
- [9] S. LANG, *Algebra*, Addison-Wesley Publishing Co. Inc., Reading, Mass., (1997). xvi+912 pp.
- [10] M. LAURENT, Équations diophantiennes exponentielles, *Invent. Math.* **78** (1984), 299–327.
- [11] A. MACINTYRE, On ω_1 -categorical theories of abelian groups, *Fund. Math.* **70** (1971), 253–270.
- [12] H. MANN, On Linear Relations Between Roots of Unity, *Mathematika* **12** (1965), 107–117.
- [13] C. MILLER AND P. SPEISSEGER, A trichotomy for expansions of \mathbb{R}_{an} by trajectories of analytic planar vector fields, Unpublished note. Available at <http://www.math.ohio-state.edu/~miller>
- [14] A. PILLAY, *Geometric Stability Theory*, Oxford University Press, Oxford (1996).
- [15] A. PILLAY, The model-theoretic content of Lang’s conjecture, in BOUSCAREN ET AL. EDS., *Model Theory and Algebraic Geometry*, Springer Lecture Notes in Math., 1696, 101–106 (1998).
- [16] B. POIZAT, Quelques Mauvais Corps de Rang Infini, in BÉLAIR, CHATZIDAKIS ET AL. EDS., *Model Theory and Applications*, Quaderni di Matematica, 11, 349–365 (2005).
- [17] A.J. VAN DER POORTEN, H.P. SCHLICKWEI, Additive relations in fields, *J. Australian Math. Soc.* **51** (1991), 154–170.
- [18] A. ROBINSON, E. ZAKON, Elementary properties of ordered abelian groups, *Trans. AMS* **96** (1960), 222–236.
- [19] T. SCANLON, J.F. VOLOCH, Difference algebraic subgroups of commutative algebraic groups over finite fields, *Manuscripta Math.* **99** (1999), 329–339.
- [20] T.A. SPRINGER, *Linear Algebraic Groups*, second ed., Birkhäuser, Basel (1998).
- [21] B. ZILBER, A note on the model theory of the complex field with roots of unity, available at www.maths.ox.ac.uk/~zilber.
- [22] B. ZILBER, Complex roots of unity on the real plane, available at www.maths.ox.ac.uk/~zilber.

UNIVERSITY OF ILLINOIS, DEPARTMENT OF MATHEMATICS, 1409 W. GREEN STREET, URBANA, IL 61801

E-mail address: vddries@math.uiuc.edu, gunaydin@math.uiuc.edu