Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2021) 45: 220 – 232
© TÜBİTAK
doi:10.3906/mat-2006-95

Number fields and divisible groups via model theory

Şermin ÇAM ÇELİK[1,*], **Haydar GÖRAL**[1,2]
[1]Department of Mathematics, School of Arts and Sciences, Atılım University, Ankara, Turkey
[2]Department of Mathematics, Faculty of Science, Dokuz Eylül University, İzmir, Turkey

Received: 22.06.2020 • **Accepted/Published Online:** 16.11.2020 • **Final Version:** 21.01.2021

Abstract: In this note, we first show that solutions of certain equations classify the number fields lying in imaginary quadratic number fields. Then, we study divisible groups with a predicate. We show that these structures are not simple and have the independence property under some natural assumptions.

Key words: Model theory, number fields, divisible groups

1. Introduction

Let

$$F(x_1, ..., x_k) \in \mathbb{C}\left[x_1, \frac{1}{x_1}, ..., x_k, \frac{1}{x_k}\right]$$

be a nonzero Laurent polynomial over complex numbers. Thus,

$$F(x_1, ..., x_k) = \sum_{\boldsymbol{\alpha} \in I} a_{\boldsymbol{\alpha}} x^{\boldsymbol{\alpha}}$$

for some nonempty finite subset I of $\mathbb{Z}^k$ where $a_{\boldsymbol{\alpha}} \in \mathbb{C}$ and

$$x^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_k^{\alpha_k}$$

for all $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_k) \in I$. To illustrate

$$F(x_1, x_2, x_3) = \frac{1}{x_1} + \frac{2}{x_1 x_2} + x_3$$

is a nonzero Laurent polynomial over complex numbers. A solution $\mathbf{g} = (g_1, ..., g_k) \in (\mathbb{C}^{\times})^k$ of the equation $F(x_1, ..., x_k) = 0$ is called a nondegenerate solution if for every nonempty proper subset J of I, we have

$$\sum_{\boldsymbol{\alpha} \in J} a_{\boldsymbol{\alpha}} \mathbf{g}^{\boldsymbol{\alpha}} \neq 0$$

where $\mathbf{g}^{\boldsymbol{\alpha}} = g_1^{\alpha_1} \cdots g_k^{\alpha_k}$ for all $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_k) \in J$. As $F(x_1, ..., x_k)$ is of the form

$$\frac{P(x_1, ..., x_k)}{(x_1 \cdots x_k)^m}$$

*Correspondence: sermincamcelik@gmail.com
2010 *AMS Mathematics Subject Classification:* 03C98, 03C45

for some polynomial $P(x_1, ..., x_k) \in \mathbb{C}[x_1, ..., x_k]$ and nonnegative integer m, the solutions of $F(x_1, ..., x_k) = 0$ from $(\mathbb{C}^\times)^k$ are the same as the solutions of $P(x_1, ..., x_k) = 0$ from $(\mathbb{C}^\times)^k$.

Given nonzero complex numbers $a_1, ..., a_k$, let

$$\frac{a_1}{x_1} + \cdots + \frac{a_k}{x_k} - 1 = 0 \tag{1.1}$$

be a unit equation. In 1965, Mann [13] proved that the unit equation above has only finitely many nondegenerate solutions in the group of complex roots of unity if $a_1, ..., a_k$ are all rational numbers. Then, Mann's result was generalized in [5]. For the model-theoretic approaches, the reader might consult [1, 4, 8]. In [9], Göral and Sertbaş proved that a number field K is either $\mathbb{Q}$ or an imaginary quadratic fied if and only if Equation (1.1) has only finitely many nondegenerate solutions with coordinates in $\mathcal{O}_K$ for all $a_1, ..., a_k \in \mathcal{O}_K$. Motivated by the mentioned result of [9], we state our first theorem.

Theorem 1.1 *Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. Then the following are equivalent:*

(i) K lies in an imaginary quadratic field.

(ii) For every nonzero polynomial $p(x_1, x_2, ..., x_n) \in \mathcal{O}_K[x_1, x_2, ..., x_n]$ with $n \geq 2$ and for every polynomial $q(x, y) \in \mathcal{O}_K[x, y]$ such that all variables $x_1, x_2, ..., x_n$ occur in p and for all nonzero elements $a \in \mathcal{O}_K$, the corresponding projective curve of $\mathcal{C}_{q,a} : q(x, y) + a = 0$ is smooth and of positive genus, we have that the equation

$$p\left(\frac{1}{x_1}, \frac{1}{x_2}, ..., \frac{1}{x_n}\right) + q(x, y) = 0$$

has only finitely many nondegenerate solutions $(x_1, x_2, ..., x_n, x, y)$ with coordinates in $\mathcal{O}_K$.

Now, we give an example for the previous theorem. Let $p(x_1, x_2) = x_1^2 + x_2^2$ and $q(x, y) = y^2 - x^3$. Then, Theorem 1.1 yields that the equation

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + y^2 - x^3 = 0$$

has only finitely many nondegenerate solutions in $\mathbb{Z}$. In fact, using SageMath one can obtain that all solutions are given by

$$(x_1, x_2, x, y) = (\pm 1, \pm 1, 3, \pm 5).$$

However, Theorem 1.1 is not effective as it depends on the finiteness theorem of Siegel [16].

Remark 1.2 *Note that if $\mathcal{C}$ is a smooth projective curve of degree d, then by the well-known genus-degree formula from algebraic geometry, the genus of the curve $\mathcal{C}$ is*

$$\frac{(d-1)(d-2)}{2}.$$

Therefore, if the degree of the polynomial $q(x, y)$ in Theorem 1.1 is at least 3, then the condition the corresponding projective curve of $\mathcal{C}_{q,a} : q(x, y) + a = 0$ is smooth and of positive genus for all nonzero elements $a \in \mathcal{O}_K$ can be replaced by the condition the corresponding projective curve of $\mathcal{C}_{q,a} : q(x, y) + a = 0$ is smooth for all nonzero elements $a \in \mathcal{O}_K$.

Let $f(x) = a_d(x - \alpha_1) \cdots (x - \alpha_d) \in \mathbb{C}[x]$ be a nonzero polynomial. The *Mahler measure* of f is defined by

$$m(f) = |a_d| \prod_{|\alpha_j| \geq 1} |\alpha_j|,$$

and the Mahler measure of zero is defined to be 1. In 1933, Lehmer conjectured that there exists an absolute constant $c > 1$ such that for any polynomial $f(x)$ in $\mathbb{Z}[x]$ if $m(f) > 1$, then $m(f) \geq c$. In other words, Lehmer's conjecture states that there exists an absolute constant $c > 1$ such that

$$\{m(f) : f \in \mathbb{Z}[x]\} \cap (1, c) = \emptyset.$$

This conjecture is still open. Moreover, Lehmer [12] claimed that the polynomial

$$f(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

has the smallest Mahler measure among all polynomials of Mahler measure greater than 1, and $m(f) \approx 1.17628$. This claim remains to be open as well.

Let $\overline{\mathbb{Q}}$ be the field of algebraic numbers and let α be in $\overline{\mathbb{Q}} \setminus \{0\}$ with irreducible polynomial $f(x) \in \mathbb{Z}[X]$ of degree d. The logarithmic height of α is defined as

$$h(\alpha) = \frac{\log m(f)}{d}.$$

The logarithmic height function has the following properties (see [2, Chapter 1] and [10, Part B, B.7]):

- For a nonzero rational number a/b where a and b are coprime integers,

$$h(a/b) = \max\{\log |a|, \log |b|\}.$$

- For all α in $\overline{\mathbb{Q}}$ and $n \in \mathbb{Z}$, we have $h(\alpha^n) = |n| h(\alpha)$.
- For all α and β in $\overline{\mathbb{Q}}$, we have $h(\alpha + \beta) \leq h(\alpha) + h(\beta) + \log 2$.
- For all α and β in $\overline{\mathbb{Q}}$, we have $h(\alpha\beta) \leq h(\alpha) + h(\beta)$.

For the last twenty years, the model theory of pairs has been a recurrent topic and has received continuous attention. In their paper, Casanovas and Ziegler [3] worked on stable theories with a predicate and obtained criteria for a stable structure with a predicate to be stable. In 1990, in an unpublished note, Zilber proved that the pair $(\mathbb{C}, \mu)$ is ω-stable where μ is the group of complex roots of unity. In [4], among other things, van den Dries and Günaydın generalized Zilber's work to algebraically closed fields with a multiplicative subgroup which has the Mann property.

Our setting: From now on, we fix our setting. Throughout this paper, the language L_g denotes the language of pure groups, P signifies a unary predicate, and the group G represents a divisible group which is not torsion. In particular, G is abelian and it contains a copy of $\mathbb{Q}$ as a subgroup. Throughout this note, let γ be a function from G to $\mathbb{R}$ with the following properties:

1. The function γ is not identically 0.

2. For any $g \in G$, we have $\gamma(g) \geq 0$.

3. There exists a positive real number $\ell \geq 1$ such that for any $g \in G$ and $n \in \mathbb{Z}$, we have $\gamma(g^n) = |n|^\ell \gamma(g)$.

4. For any g_1 and g_2 from G, we have $\gamma(g_1 g_2) \leq 2^{\ell-1}(\gamma(g_1) + \gamma(g_2))$.

Note that the logarithmic height function h on the multiplicative group of the field of algebraic numbers satisfies the above properties with $\ell = 1$.

Remark 1.3 *Observe that if $u \in G$ is a torsion element, then $\gamma(u) = 0$. In particular, $\gamma(1) = 0$. In fact, for any torsion element u and any element g from G, one has that $\gamma(g) = \gamma(ug)$. To see this, choose a positive integer m such that $u^m = 1$. Then $\gamma(g^m) = \gamma((ug)^m)$. Thus, we have that $m^\ell \gamma(g) = m^\ell \gamma(ug)$ and this yields that $\gamma(g) = \gamma(ug)$.*

Definition 1.4 *Let γ be a function from G to $\mathbb{R}$ with $\ell = 1$ and X be a subset of G. We say that the set X is γ-independent if for any distinct elements $g_1, ..., g_n, g_{n+1}$ from X, we have the following two properties:*

(i) $\gamma(g_1 \cdots g_n) = \gamma(g_1) + \cdots + \gamma(g_n)$,

(ii) $\gamma(g_1 \cdots g_n g_{n+1}^{-1}) = \max\{\gamma(g_1 \cdots g_n), \gamma(g_{n+1})\}$.

Let G be the multiplicative group of the field of algebraic numbers and $\gamma = h$. Let $\mathbb{P}$ denote the set of all prime numbers. Then, the set $X = \{p^r : p \in \mathbb{P}, r \in \mathbb{Q}_{>0}\}$ is γ-independent by Lemmas 2.3 and 2.4 from [7].

Our other results in this note are the following.

Theorem 1.5 *Let γ be a function from G to $\mathbb{R}$ with $\ell = 1$ and $\Gamma = \{g \in G : \gamma(g) \leq 1\}$. Suppose that there exists an infinite sequence $(\alpha_n)_n$ in G such that $\gamma(\alpha_n) > 0$ for all n and for any distinct i and j the element α_i is not in the divisible hull of α_j, and the set $X = \{\alpha_n^m : m, n \in \mathbb{N}\}$ is γ-independent. Then the pair (G, Γ) has the independence property in the language $L_g(P) = L_g \cup \{P\}$.*

Theorem 1.6 *Let $\Gamma = \{g \in G : \gamma(g) \leq 1\}$. Then the theory of (G, Γ) is not simple in the language $L_g(P) = L_g \cup \{P\}$.*

In [7], Theorem A states that the theory of $(\overline{\mathbb{Q}}, S_\varepsilon)$ is not simple and has the independence property, where $S_\varepsilon = \{a \in \overline{\mathbb{Q}} : h(a) \leq \varepsilon\}$ and $\varepsilon > 0$. Observe that applying Theorems 1.5 and 1.6, one can deduce Theorem A from [7] if we take G to be the multiplicative group $\overline{\mathbb{Q}}$, γ to be the logarithmic height function h and X to be the γ-independent set $\{p^r : p \in \mathbb{P}, r \in \mathbb{Q}_{>0}\}$.

Theorem 1.6 has another corollary that we mention now. Let $a, b \in \overline{\mathbb{Q}}$ with $4a^3 + 27b^2 \neq 0$. Recall that an elliptic curve over $\overline{\mathbb{Q}}$ is the solution set of the equation $y^2 = x^3 + ax + b$ in $\overline{\mathbb{Q}}$ with an additional point O, which is called the point at infinity. An elliptic curve $E(\overline{\mathbb{Q}})$ is an abelian group such that O is the identity element. Moreover, the group $E(\overline{\mathbb{Q}})$ is divisible. There is a canonical height function (the Néron–Tate height) on $E(\overline{\mathbb{Q}})$

which is denoted by $\hat{h}$. Besides, for any points x and y in $E(\overline{\mathbb{Q}})$, we have that $\hat{h}(x+y)+\hat{h}(x-y)=2\hat{h}(x)+2\hat{h}(y)$, and in particular $\hat{h}(x+y)\leq 2(\hat{h}(x)+\hat{h}(y))$. One can see that if we take $G=E(\overline{\mathbb{Q}})$ and $\gamma=\hat{h}$, then we have all the properties $(1)-(4)$ above with $\ell=2$ in our setting. Hence, Theorem 1.6 also yields that the pair $(E(\overline{\mathbb{Q}}),\{x\in E(\overline{\mathbb{Q}}):\hat{h}(x)\leq 1\})$ is not simple.

Next, we define nonstandard extensions since it will be helpful in Remark 2.1 and in the proof of Theorem 1.6.

Definition 1.7 *Let $\mathbb{M}$ be a nonempty structure in a countable language L. A nonstandard extension ${}^*\mathbb{M}$ of $\mathbb{M}$ is an ultrapower of $\mathbb{M}$ with respect to a nonprincipal ultrafilter on $\mathbb{N}$.*

Fix a nonstandard extension ${}^*\mathbb{M}$ of $\mathbb{M}$ with respect to a nonprincipal ultrafilter D on $\mathbb{N}$. The elements of ${}^*\mathbb{M}$ are of the form $(a_n)_n/D$ where $(a_n)_n$ is a sequence in $\mathbb{M}$. Identifying each element a of $\mathbb{M}$ with $(a)_n/D$ of ${}^*\mathbb{M}$, we regard the structure $\mathbb{M}$ as an elementary substructure of ${}^*\mathbb{M}$. If A is a subset of $\mathbb{M}$, the set ${}^*A$ is defined to be the set

$$\{(a_n)_n/D:\{n:a_n\in A\}\in D\}.$$

Observe that ${}^*A$ contains A, and any function on A extends to a well-defined function on ${}^*A$ coordinatewise. If L is the language of totally ordered rings, then ${}^*\mathbb{R}$ is an ordered field and the order on ${}^*\mathbb{R}$ is defined as $(a_n)_n/D\leq(b_n)_n/D$ if and only if $\{n:a_n\leq b_n\}\in D$. The sets ${}^*\mathbb{N}$, ${}^*\mathbb{Z}$, ${}^*\mathbb{Q}$, ${}^*\mathbb{R}$ are called hypernatural numbers, hyperintegers, hyperrational numbers and hyperreals respectively. The elements of ${}^*\mathbb{R}\setminus\mathbb{R}$ are called nonstandard real numbers. The ring of finite numbers is denoted by

$$\mathbb{R}_{\text{fin}}=\{x\in{}^*\mathbb{R}:|x|<n\text{ for some }n\in\mathbb{N}\},$$

and the elements in ${}^*\mathbb{R}\setminus\mathbb{R}_{\text{fin}}$ are called infinite. Recall that a hyperreal number ε is said to be infinitesimal if $|\varepsilon|<1/n$ for every positive integer n. It is known that for any $x\in\mathbb{R}_{\text{fin}}$ there is a unique real number $y\in\mathbb{R}$, denoted as the standard part $st(x)$ of x, such that $x-y$ is an infinitesimal. For any $x,y\in\mathbb{R}_{\text{fin}}$, we have $st(x+y)=st(x)+st(y)$ and $st(xy)=st(x)st(y)$. If I is the set of infinitesimal elements of ${}^*\mathbb{R}$, then we also have that $\mathbb{R}_{\text{fin}}/I$ is isomorphic to $\mathbb{R}$. The notion of a nonstandard extension can be extended to many-sorted structures. For more on the topic, see [6].

2. Proof of Theorem 1.1

(ii) $\Rightarrow$ (i): Assume that (i) does not hold, i.e. the number field K does not lie in an imaginary quadratic field. Then, it follows from Dirichlet's unit theorem [14, Chapter 4, Section 4] that the group $\mathcal{O}_K^\times$ of units in the ring $\mathcal{O}_K$ has rank $r=r_1+r_2-1$ at least 1, where r_1 is the number of real embeddings and r_2 is the number of pairs of complex embeddings (up to conjugation), where $[K:\mathbb{Q}]=r_1+2r_2$. As a result, the group $\mathcal{O}_K^\times$ is not finite and hence it contains a unit element u which is not a root of unity.

Let $p(x_1,x_2)=x_1+x_2\in\mathcal{O}_K[x_1,x_2]$ and $q(x,y)=y^2-x^3\in\mathcal{O}_K[x,y]$. Note that both variables x_1 and x_2 appear in the polynomial p and the curve $y^2-x^3+a=0$ is smooth of genus exactly 1 for all $a\in\mathcal{O}_K\setminus\{0\}$, and in fact it is an elliptic curve. Then, $x_1=u^m-1$, $x_2=u^{-m}-1$, $x=2$, $y=3$ yield a solution of the equation

$$\frac{1}{x_1}+\frac{1}{x_2}+y^2-x^3=0 \tag{2.1}$$

with coordinates in $\mathcal{O}_K$ for every positive integer m. Since u is not a root of unity,

$$(u^{m_1}-1, u^{-m_1}-1, 2, 3)$$

and

$$(u^{m_2}-1, u^{-m_2}-1, 2, 3)$$

give distinct solutions of Equation (2.1) for distinct positive integers m_1 and m_2. Moreover, a solution $(u^m-1, u^{-m}-1, 2, 3)$ is degenerate only if

$$\frac{1}{u^m-1}+9=0$$

or

$$\frac{1}{u^m-1}-8=0.$$

So, if there is an integer m_0 such that $u^{m_0}=8/9$, then $(u^m-1, u^{-m}-1, 2, 3)$ is a nondegenerate solution for each positive integer m except $|m_0|$. If there is no such integer m_0, then the solution $(u^m-1, u^{-m}-1, 2, 3)$ is nondegenerate for each positive integer m. In both cases, we obtain infinitely many nondegenerate solutions of Equation (2.1) with coordinates in $\mathcal{O}_K$.

(i) $\Rightarrow$ (ii): Assume that K lies in an imaginary quadratic field. So, $K=\mathbb{Q}$ or $K=\mathbb{Q}\left(\sqrt{-d}\,\right)$ for some square-free positive integer d. If $K=\mathbb{Q}$, then $\mathcal{O}_K=\mathbb{Z}$. If $K=\mathbb{Q}\left(\sqrt{-d}\,\right)$ for a square-free integer $d>0$, then $\mathcal{O}_K=\mathbb{Z}\left[\sqrt{-d}\,\right]$ when $d\not\equiv 3 \pmod 4$ and $\mathcal{O}_K=\mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ when $d\equiv 3 \pmod 4$. Since the rings $\mathbb{Z}$ and $\mathbb{Z}[\theta]$ are discrete in $\mathbb{C}$ for all $\theta\in\mathbb{C}\backslash\mathbb{R}$, in all these three cases, the ring $\mathcal{O}_K$ is discrete in $\mathbb{C}$. Equivalently, the set

$$F_b=\{\alpha\in\mathcal{O}_K : |\alpha|\leq b\}$$

is finite for all positive real numbers b.

Now, let $p(x_1,x_2,...,x_n)\in\mathcal{O}_K[x_1,x_2,...,x_n]$ be a nonzero polynomial with $n\geq 2$ and let $q(x,y)\in\mathcal{O}_K[x,y]$ be a polynomial such that all variables $x_1,x_2,...,x_n$ occur in p and for all nonzero elements $a\in\mathcal{O}_K$, the corresponding projective curve of

$$\mathcal{C}_{q,a} : q(x,y)+a=0$$

is smooth and of positive genus. Our aim is to show that the equation

$$p\left(\frac{1}{x_1},\frac{1}{x_2},...,\frac{1}{x_n}\right)+q(x,y)=0 \tag{2.2}$$

has only finitely many nondegenerate solutions $(x_1,x_2,...,x_n,x,y)$ with coordinates in $\mathcal{O}_K$.
Assume that $(a_1,a_2,...,a_n,a,b)$ is a nondegenerate solution of Equation (2.2) with coordinates in $\mathcal{O}_K$. Then,

$$p\left(\frac{1}{a_1},\frac{1}{a_2},...,\frac{1}{a_n}\right)=-q(a,b)\in\mathcal{O}_K\backslash\{0\}.$$

Since $\mathcal{O}_K$ is discrete, for all nonzero elements $x_1,x_2,...,x_n$ in $\mathcal{O}_K$,

$$\left|p\left(\frac{1}{x_1},\frac{1}{x_2},...,\frac{1}{x_n}\right)\right|<M$$

for some positive real number M. So, we get

$$p\left(\frac{1}{a_1}, \frac{1}{a_2}, ..., \frac{1}{a_n}\right) \in F_M$$

and $q(a,b) \in F_M$. Indeed, if $F_M = \{0, c_1, c_2, ..., c_m\}$, then

$$p\left(\frac{1}{a_1}, \frac{1}{a_2}, ..., \frac{1}{a_n}\right) = c_i$$

and $q(a,b) = -c_i$ for some $i = 1, 2, ..., m$. Hence, $(a_1, a_2, ..., a_n, a, b)$ is a nondegenerate solution of Equation (2.2) with coordinates in $\mathcal{O}_K$ if and only if $(a_1, a_2, ..., a_n)$ is a nondegenerate solution of the equation

$$p\left(\frac{1}{x_1}, \frac{1}{x_2}, ..., \frac{1}{x_n}\right) = c_i \tag{2.3}$$

with coordinates in $\mathcal{O}_K$ and (a,b) is a nondegenerate solution of the equation

$$q(x,y) + c_i = 0 \tag{2.4}$$

with coordinates in $\mathcal{O}_K$ for some $i = 1, 2, ..., m$. Since $c_i \in \mathcal{O}_K \backslash \{0\}$ for all $i = 1, 2, ..., m$, the curve $q(x,y) + c_i = 0$ is smooth with positive genus for all $i = 1, 2, ..., m$. Hence, Equation (2.4) has only finitely many solutions in $\mathcal{O}_K$ for all $i = 1, 2, ..., m$ by Siegel's theorem on integral points, see [11, Chapter 8] and [16]. Therefore, to show that Equation (2.2) has only finitely many nondegenerate solutions with coordinates in $\mathcal{O}_K$, it is enough to show that Equation (2.3) has only finitely many nondegenerate solutions with coordinates in $\mathcal{O}_K$ for all $i = 1, 2, ..., m$. Assume for a contradiction that there exist infinitely many nondegenerate solutions of Equation (2.3) with coordinates in $\mathcal{O}_K$ for some $i = 1, 2, ..., m$. List these nondegenerate solutions as $(s_k)_k = (a_{k1}, a_{k2}, ..., a_{kn})_k$ where $s_k \neq s_l$ for $k \neq l$. For each $j = 1, 2, ..., n$, consider the sequence $(a_{kj})_k$. If the sequence $(a_{kj})_k$ is bounded for all $j = 1, 2, ..., n$, then the set

$$\{a_{kj} : k \in \mathbb{N}, \quad j = 1, 2, ..., n\} \subseteq F_b$$

for some $b \in \mathbb{R}$, hence finite, a contradiction with $|\{s_k : k \in \mathbb{N}\}| = \infty$. Therefore, there exists $j \in \{1, 2, ..., n\}$ such that the sequence $(a_{kj})_k$ is unbounded. Without loss of generality, we may assume that $(a_{k1})_k$ is unbounded. By passing to a subsequence when necessary, we may assume that $(a_{k1})_k$ diverges to infinity and for all $j = 2, ..., n$, the sequence $(a_{kj})_k$ is either bounded or diverges to infinity. Write $p(x_1, x_2, ..., x_n)$ as a sum of its distinct, nonzero monomials as

$$p(x_1, x_2, ..., x_n) = p_1(x_1, x_2, ..., x_n) + p_2(x_1, x_2, ..., x_n) + \cdots + p_L(x_1, x_2, ..., x_n)$$

such that x_1 occurs in $p_1(x_1, x_2, ..., x_n)$. Note that for each $k \in \mathbb{N}$, we have

$$p_1\left(\frac{1}{a_{k1}}, \frac{1}{a_{k2}}, ..., \frac{1}{a_{kn}}\right) + p_2\left(\frac{1}{a_{k1}}, \frac{1}{a_{k2}}, ..., \frac{1}{a_{kn}}\right) + \cdots + p_L\left(\frac{1}{a_{k1}}, \frac{1}{a_{k2}}, ..., \frac{1}{a_{kn}}\right) = c_i. \tag{2.5}$$

For each $\ell = 1, 2, ..., L$, consider the sequence $(\delta_{\ell,k})_k$ where

$$\delta_{\ell,k} = p_\ell\left(\frac{1}{a_{k1}}, \frac{1}{a_{k2}}, ..., \frac{1}{a_{kn}}\right).$$

Then $\delta_{\ell,k} \neq 0$ for all k and $\ell = 1, 2, ..., L$ as s_k is a nondegenerate solution of Equation (2.3) for all k. Since x_1 occurs in $p_1(x_1, x_2, ..., x_n)$, we have $p_1(x_1, x_2, ..., x_n) = Ax_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}$ for some $A \in \mathcal{O}_K\backslash\{0\}$ and for some nonnegative integers $\alpha_1, \alpha_2, ..., \alpha_n$ with $\alpha_1 > 0$. Then since $((a_{k1})^{\alpha_1})_k$ diverges to infinity and $((a_{kj})^{\alpha_j})_k$ is either bounded or tends to infinity for all $j = 2, ..., n$, we have

$$\left|p_1\left(\frac{1}{a_{k1}}, \frac{1}{a_{k2}}, ..., \frac{1}{a_{kn}}\right)\right| = \left|\frac{A}{(a_{k1})^{\alpha_1}(a_{k2})^{\alpha_2}...(a_{kn})^{\alpha_n}}\right| \to 0 \text{ as } k \to \infty. \tag{2.6}$$

Hence $(\delta_{1,k})_k$ converges to 0 as $k \to \infty$. Similarly, given $\ell \in \{2, ..., L\}$, if there exists some $j \in \{1, 2, ..., n\}$ such that $(a_{kj})_k$ diverges to infinity and x_j occurs in $p_\ell(x_1, x_2, ..., x_n)$, then $(\delta_{\ell,k})_k$ converges to 0 as $k \to \infty$. Otherwise, the sequence $(\delta_{\ell,k})_k$ takes on only finitely many values. Hence, there exists a subsequence $(k_n)_n$ of positive integers such that either $\delta_{\ell,k_n} \to 0$ as $n \to \infty$ or $(\delta_{\ell,k_n})_n$ is a nonzero constant sequence for all $\ell \in \{2, ..., L\}$. Since $c_i \neq 0$, there exists at least one $\ell \in \{2, ..., L\}$ such that $(\delta_{\ell,k_n})_n$ is a nonzero constant sequence. Let $(\varepsilon_n)_n$ be the sum of all $(\delta_{\ell,k_n})_n$'s converging to 0 as $n \to \infty$ and let $(d)_n$ be the constant sequence which is the sum of all nonzero constant $(\delta_{\ell,k_n})_n$'s. Then $(\varepsilon_n)_n$ converges to 0 and since $\varepsilon_n + d = c_i$ for all n, we get $d = c_i$ and $\varepsilon_n = 0$ for all n. But this is a contradiction since $\varepsilon_n \neq 0$ for all n as each s_{k_n} is a nondegenerate solution of Equation (2.3).

Remark 2.1 *Following Equation (2.5), one may continue and end the proof of Theorem 1.1 using nonstandard analysis as follows: For each $\ell = 1, 2, ..., L$, let*

$$\delta_\ell = \left(p_\ell\left(\frac{1}{a_{k1}}, \frac{1}{a_{k2}}, ..., \frac{1}{a_{kn}}\right)\right)_k / D \in {}^*\mathbb{C}$$

where D is a nonprincipal ultrafilter on $\mathbb{N}$ and ${}^*\mathbb{C}$ is a nonstandard extension of $\mathbb{C}$ with respect to the nonprincipal ultrafilter D on $\mathbb{N}$. Just as in the the proof of Theorem 1.1 above, we have (2.6) which implies δ_1 is an infinitesimal element of ${}^*\mathbb{C}$. Given $\ell \in \{2, ..., L\}$, if δ_ℓ is not an infinitesimal element of ${}^*\mathbb{C}$, then the set

$$\left\{p_\ell\left(\frac{1}{a_{k1}}, \frac{1}{a_{k2}}, ..., \frac{1}{a_{kn}}\right) : k \in \mathbb{N}\right\}$$

is finite, hence δ_ℓ is a standard complex number. Thus, letting ε be the sum of infinitesimal δ_j's and letting s be the sum of δ_j's which are standard complex numbers, we get that ε is an infinitesimal, s is a standard complex number and $\varepsilon + s = c_i$ in ${}^*\mathbb{C}$. But this is a contradiction since $\varepsilon \neq 0$ as each s_k is a nondegenerate solution of Equation (2.3).

3. Proof of Theorem 1.5

Before proving Theorem 1.5, we need the following definition from classification theory.

Definition 3.1 *Let T be a complete L-theory where L is a language. An L-formula $\varphi(x, y)$ is said to have the independence property if in every model M of T there is a family of tuples $b_1, ..., b_n$ for each n, such that for each of the 2^n subsets I of $\{1, ..., n\}$ there is a tuple a_I in M for which*

$$M \models \varphi(a_I, b_i) \iff i \in I.$$

A theory T is said to be NIP if no formula has the independence property.

The class of stable theories is a subset of the class of NIP theories, and in fact, a theory T is stable if and only if T is simple and NIP. For the details, we refer the reader to the book [15].

Now, we start the proof of Theorem 1.5. Suppose that there exists an infinite sequence $(\alpha_n)_n$ in G such that $\gamma(\alpha_n) > 0$ for all n and for any distinct i and j the element α_i is not in the divisible hull of α_j, and the set $X = \{\alpha_n^m : m, n \in \mathbb{N}\}$ is γ-independent. Here, for an element $g \in G$ and m a positive integer, $g^{1/m}$ represents an element from the set $\{h \in G : h^m = g\}$ and we use the axiom of choice if necessary. By Remark 1.3, for any h_1, h_2 from $\{h \in G : h^m = g\}$ we know that $\gamma(h_1) = \gamma(h_2)$.

Claim: The set $Y = \{\alpha_n^m : n \in \mathbb{N}, m \in \mathbb{Q}_{\geq 0}\}$ is γ-independent.

Proof of the Claim: First, note that for any distinct i and j, the elements α_i and α_j are not in the divisible hulls of each other. In particular, we have that for any nonzero positive rational numbers q_i and q_j, the equality $\alpha_i^{q_i} = \alpha_j^{q_j}$ cannot hold. To prove the claim, take the following distinct elements

$$\alpha_1^{m_1}, ..., \alpha_n^{m_n}, \alpha_{n+1}^{m_{n+1}}$$

from Y. Write $m_i = u_i/v_i$ for $i = 1, ..., n, n+1$ where $u_i, v_i \in \mathbb{Z}$. We may suppose that the integers u_i, v_i are all positive. Then by Remark 1.3 we have:

$$\gamma(\alpha_1^{m_1} \cdots \alpha_n^{m_n}) = \gamma((\alpha_1^{t_1} \cdots \alpha_n^{t_n})^{1/v}) = \frac{1}{v}\gamma(\alpha_1^{t_1} \cdots \alpha_n^{t_n}).$$

As the set X is γ-independent, we have $\gamma(\alpha_1^{t_1} \cdots \alpha_n^{t_n}) = \gamma(\alpha_1^{t_1}) + \cdots + \gamma(\alpha_n^{t_n})$. Therefore, we have

$$\gamma(\alpha_1^{m_1} \cdots \alpha_n^{m_n}) = \frac{1}{v}\gamma(\alpha_1^{t_1}) + \cdots + \frac{1}{v}\gamma(\alpha_n^{t_n}) = \gamma(\alpha_1^{m_1}) + \cdots + \gamma(\alpha_n^{m_n}),$$

where the last equality follows from Remark 1.3. For the following several equalities, we also apply Remark 1.3 without mentioning it. Note also that $\gamma(\alpha_1^{m_1} \cdots \alpha_n^{m_n} \alpha_{n+1}^{-m_{n+1}}) = \gamma((\alpha_1^{c_1} \cdots \alpha_n^{c_n} \alpha_{n+1}^{-c_{n+1}})^{1/vv_{n+1}})$, where v is as before and $c_i = u_i v v_{n+1}/v_i$. This yields that

$$\gamma(\alpha_1^{m_1} \cdots \alpha_n^{m_n} \alpha_{n+1}^{-m_{n+1}}) = \frac{1}{vv_{n+1}}\gamma(\alpha_1^{c_1} \cdots \alpha_n^{c_n} \alpha_{n+1}^{-c_{n+1}}).$$

As X is γ-independent, we see that

$$\frac{1}{vv_{n+1}}\gamma(\alpha_1^{c_1} \cdots \alpha_n^{c_n} \alpha_{n+1}^{-c_{n+1}}) = \frac{1}{vv_{n+1}} \max\{\gamma(\alpha_1^{c_1} \cdots \alpha_n^{c_n}), \gamma(\alpha_{n+1}^{-c_{n+1}})\},$$

and this is equal to $\max\{\gamma(\alpha_1^{m_1} \cdots \alpha_n^{m_n}), \gamma(\alpha_{n+1}^{-m_{n+1}})\}$. This proves the claim.

Now let $\varphi(x, y)$ be the formula $P(xy^{-1})$. We will prove that $\varphi(x, y)$ has the independence property. Let $n \geq 1$ be given and let I be a nonempty subset of $\{1, ..., n\}$ with $|I| = r$. As the set $\{\gamma(\alpha_i^m) : m \in \mathbb{Q}_{>0}\}$ is dense in the positive real numbers for any i, we can find a positive rational number $p_i > 0$ such that

$$\frac{1}{r} < \gamma(\alpha_i^{p_i}) \leq \frac{1}{r} + \frac{1}{(n+1)^2} \tag{3.1}$$

and we define a_I to be the product $\prod_{i\in I} \alpha_i^{p_i}$. Choose also $p \in \mathbb{Q}_{>0}$ such that

$$1 < \gamma(\alpha_{n+1}^p) \leq 1 + \frac{1}{n+1}. \tag{3.2}$$

We put $a_\emptyset = \alpha_{n+1}^p$. For any subset I of $\{1,...,n\}$, combining the properties of γ and the γ-independency of our set Y with (3.1) and (3.2) above, we get that

$$1 < \gamma(a_I) \leq 1 + \frac{n}{(n+1)^2} \leq 1 + \frac{1}{n+1}. \tag{3.3}$$

Similarly, as we did before, choose a positive rational number j_m such that

$$\frac{1}{n+1} < \gamma(b_m) < \frac{1}{n}, \tag{3.4}$$

where $b_m = \alpha_m^{j_m}$. Next, we show that $\varphi(a_I, b_i)$ holds if and only if $i \in I$. If $I = \emptyset$ then as

$$\gamma(a_\emptyset b_i^{-1}) = \max\{\gamma(a_\emptyset), \gamma(b_i))\} = \gamma(a_\emptyset) > 1$$

for any i, we are done in this case. Let I be a nonempty subset of $\{1,...,n\}$. If i is not in I, then by the claim above and (3.3) we obtain that

$$\gamma(a_I b_i^{-1}) = \max\{\gamma(a_I), \gamma(b_i)\} = \gamma(a_I) > 1.$$

This contradicts the validity of $\varphi(a_I, b_i)$. Thus i must be in I. For the converse, assume that i is in $I = \{i_1, ..., i_r\}$. We may also suppose that $i = i_1$. Moreover, by (3.1) and (3.4), we see that $p_{i_1} \geq j_{i_1}$. By the properties of the function γ and the claim above, we arrive at

$$\gamma(a_I b_i^{-1}) = (p_{i_1} - j_{i_1})\gamma(\alpha_{i_1}) + p_{i_2}\gamma(\alpha_{i_2}) + \cdots + p_{i_r}\gamma(\alpha_{i_r}). \tag{3.5}$$

Combining (3.3), (3.4) and (3.5), we obtain that

$$\gamma(a_I b_i^{-1}) = (p_{i_1} - j_{i_1})\gamma(\alpha_{i_1}) + p_{i_2}\gamma(\alpha_{i_2}) + \cdots + p_{i_r}\gamma(\alpha_{i_r}) = \gamma(a_I) - \gamma(b_i) \leq 1 + \frac{1}{n+1} - \frac{1}{n+1} \leq 1.$$

Hence $\varphi(x, y)$ has the independence property and so does the pair (G, Γ).

4. Proof of Theorem 1.6

First, we give an important definition from the classification theory. Details can be found in the book [17].

Definition 4.1 *Let T be a theory and $\mathbb{M}$ be its sufficiently saturated model. A formula $\varphi(x, y)$ has the tree property if there is a tree of parameters*

$$(a_s : \emptyset \neq s \in \omega^{<\omega})$$

from $\mathbb{M}$ such that

(i) For all $s \in \omega^{<\omega}$, $(\varphi(x, a_{si}) : i < \omega)$ is 2-inconsistent.

(ii) For all $\sigma \in \omega^\omega$, $(\varphi(x, a_s) : \emptyset \neq s \subset \sigma)$ *is consistent.*

The theory T *is said to be simple if no formula has the tree property with parameters coming from a sufficiently saturated model of* T.

For instance, the theory of algebraically closed fields is simple (in fact it is ω-stable). Now, we give an example of a theory which is not simple, and we will make use of it in the proof of Theorem 1.6.

Example 4.2 *The theory of dense linear orders without end points, DLO for short, is not simple. To see this, observe that the formula* $\psi(x; y, z) : y < x < z$ *has the tree property. Let* $\mathcal{M} = \mathbb{Q} \cap (0, 1)$ *and* $\mathbb{M}$ *be a sufficiently saturated model of DLO containing* $\mathcal{M}$. *The model* $\mathbb{M}$ *is also not simple and we fix a tree of parameters* $(q_s : \emptyset \neq s \in \omega^{<\omega})$ *from the small model* $\mathcal{M}$ *of DLO for the formula* ψ *witnessing not simplicity.*

Now, we start to prove Theorem 1.6. We will prove that the pair (G, Γ) is not simple by exhibiting a formula with four free variables that has the tree property. As γ is not identically zero, let α be a torsion-free element in G with $\gamma(\alpha) > 0$. We know that for any $n \in \mathbb{Z}$, we have $\gamma(\alpha^n) = |n|^\ell \gamma(\alpha)$. Here again, for an element $g \in G$ and m a positive integer, $g^{1/m}$ represents an element from the set $\{h \in G : h^m = g\}$, and by Remark 1.3, for any h_1, h_2 from $\{h \in G : h^m = g\}$ one has $\gamma(h_1) = \gamma(h_2)$. Similarly for $r \in \mathbb{Q}$, the element α^r is just a choice. So by this choice, we have a function θ from $\mathbb{Q}$ to G sending r to α^r. Observe that the set $\{\gamma(\alpha^r) : r \in \mathbb{Q}\}$ is dense in the positive real numbers as we have $\gamma(\alpha^r) = |r|^\ell \gamma(\alpha)$ for all $r \in \mathbb{Q}$. Thus, we may suppose that $0 < \gamma(\alpha) < 1$ and in particular α belongs to Γ. Let ${}^*\mathbb{G}$ be a nonstandard extension of the many-sorted structure

$$\mathbb{G} = (G, \cdot, ^{-1}, 1, \gamma, \mathbb{R}_{\geq 0}, \theta, <, \mathbb{Q}).$$

The function γ extends to ${}^*G$ in the usual way and it takes values in nonnegative hyperreal numbers. Now the pair $({}^*G, {}^*\Gamma)$ becomes an elementary extension of (G, Γ) in the language $L_g(P)$, and ${}^*\Gamma = \{g \in {}^*G : \gamma(g) \leq 1\}$. Let $st(a)$ be the standard part of a finite hyperreal number. As $\{\gamma(\alpha^r) : r \in \mathbb{Q}\}$ is dense in the positive real numbers, we know that there is a hyperrational number $N > 1$ such that $\gamma(\alpha^N) < 1$ but the standard part of $\gamma(\alpha^N)$ is 1. We set

$$\varphi(x; y, z, t) : P\big(xz^{-1}t\big) \wedge P\big(x^{-1}yt\big).$$

We claim that this formula has the tree property. For any rational numbers $r, s \in (0, 1)$, first note that

$$\gamma\big(\alpha^N \alpha^{r-s}\big) \leq 1 \iff r \leq s. \tag{4.1}$$

Let (r_1, s_1) and (r_2, s_2) be disjoint intervals of $(0, 1)$, where $r_1 < s_1 < r_2 < s_2 \in \mathbb{Q}$. Next we show that the satisfaction

$$({}^*G, {}^*\Gamma) \models \exists x(\varphi(x, \alpha^{r_1}, \alpha^{s_1}, \alpha^N) \wedge \varphi(x, \alpha^{r_2}, \alpha^{s_2}, \alpha^N))$$

cannot be true. Assume that the above satisfaction holds. Then we have

$$\gamma\big(x\alpha^{-s_1}\alpha^N\big) \leq 1 \qquad \text{and} \qquad \gamma\big(x^{-1}\alpha^{r_2}\alpha^N\big) \leq 1.$$

So, we deduce that

$$\gamma(\alpha^{r_2 - s_1}\alpha^{2N}) = \gamma(x\alpha^{-s_1}\alpha^N x^{-1}\alpha^{r_2}\alpha^N) \leq 2^{\ell-1}(\gamma\big(x\alpha^{-s_1}\alpha^N\big) + \gamma\big(x^{-1}\alpha^{r_2}\alpha^N\big)) \leq 2^\ell.$$

This is a contradiction, as

$$\gamma(\alpha^{r_2-s_1}\alpha^{2N}) > 2^\ell$$

due to the facts that $r_2 - s_1 > 0$ and

$$st(\gamma(\alpha^{2N})) = st(2^\ell\gamma(\alpha^N)) = st(2^\ell)st(\gamma(\alpha^N)) = 2^\ell.$$

For a tuple $a = (a_1, ..., a_k) \in \mathbb{Q}^k$, we put $\alpha^a = (\alpha^{a_1}, ..., \alpha^{a_m})$. Now we choose the parameters (α^{q_s}, α^N) where the parameters $(q_s : \emptyset \neq s \in \omega^{<\omega})$ are given as in Example 4.2, and the tuple α^{q_s} is defined as above. Therefore the formula $\varphi(x; y, z, t)$ has the tree property with the above parameters since it has the item (i) from Definition 4.1 as argued above and it also has the item (ii) from Definition 4.1 by (4.1). Hence our pair is not simple.

Acknowledgements

The authors thank to the anonymous referee for the comments which immensely improved the presentation of the paper.

References

[1] Berenstein A, Vassilev E. Fields with a dense-codense linearly independent multiplicative subgroup. Archive for Mathematical Logic 2020; 59: 197-228.

[2] Bombieri E, Gubler W. Heights in Diophantine Geometry. 1st ed. Cambridge, UK: Cambridge University Press, 2007.

[3] Casanovas E, Ziegler M. Stable theories with a new predicate. The Journal of Symbolic Logic 2001; 66: 1127-1140.

[4] Van den Dries L, Günaydın A. The fields of real and complex numbers with a small multiplicative group. Proceedings of the London Mathematical Society 2006; 93 (3): 43-81.

[5] Evertse J. H, Schlickewei H. P, Schmidt W. M. Linear equations in variables which lie in a multiplicative group. Annals of Mathematics 2002; 155: 807-836.

[6] Goldblatt R. Lectures on the Hyperreals, An Introduction to Nonstandard Analysis. New York, NY, USA: Springer-Verlag, 1998.

[7] Göral H. Algebraic numbers with elements of small height. MLQ Mathematical Logic Quarterly 2019; 65 (1): 14-22.

[8] Göral H. Tame expansions of ω-stable theories and definable groups. Notre Dame Journal of Formal Logic 2019; 60 (2): 161-194.

[9] Göral H, Sertbaş D. C. Density and finiteness results on sums of fractions. Proceedings of the American Mathematical Society 2019; 147: 567-581.

[10] Hindry M, Silverman J. H. Diophantine Geometry: An Introduction. New York, NY, USA: Springer-Verlag, 2000.

[11] Lang S. Fundamentals of Diophantine Geometry. New York, NY, USA: Springer-Verlag, 1983.

[12] Lehmer D. H. Factorization of certain cyclotomic functions. Annals of Mathematics 1933; 34 (2): 461-479.

[13] Mann H. On linear relations between roots of unity. Mathematika 1965; 12: 107-117.

[14] Samuel P. Algebraic Theory of Numbers (Translated from the French by Allan J. Silberger). Boston, MA, USA: Houghton Mifflin Company, 1970.

[15] Shelah S. Classification Theory. Studies in Logic and the Foundations of Mathematics. 2nd ed. Amsterdam, Netherlands: North Holland Publishing Co., 1990.

[16] Siegel CL. Über einige Anwendungen diophantischer Approximationen. Abhandlungen der Preussischen Akademie der Wissenschaften 1929; 1 (Ges. Abh., I): 209-266.

[17] Tent K, Ziegler M. A Course in Model Theory. Lecture Notes in Logic, Series Number 40. 1st ed. Cambrdige, UK: Cambridge University Press, 2012.