Canad. J. Math. 2023, pp. 1–24
http://dx.doi.org/10.4153/S0008414X2300072X

A new way to tackle a conjecture of Rémond

Arnaud Plessis

Abstract. Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a finitely generated subgroup. Denote by Γ_{div} its division group. A recent conjecture due to Rémond, related to the Zilber–Pink conjecture, predicts that the absolute logarithmic Weil height of an element of $\mathbb{Q}(\Gamma_{\mathrm{div}})^* \backslash \Gamma_{\mathrm{div}}$ is bounded from below by a positive constant depending only on Γ. In this paper, we propose a new way to tackle this problem.

1 Introduction

1.1 Rémond's conjecture

Let $\alpha \in \overline{\mathbb{Q}}$. The (absolute logarithmic) Weil height of α is the real number

$$h(\alpha) = \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \log\left(|lc(\alpha)| \prod_{\sigma} \max\{1, |\sigma\alpha|\}\right),$$

where $lc(\alpha)$ denotes the leading coefficient of the minimal polynomial of α over $\mathbb{Z}$, and where σ runs over all field embeddings $\mathbb{Q}(\alpha) \to \overline{\mathbb{Q}}$. The function $h : \overline{\mathbb{Q}} \to \mathbb{R}$ is nonnegative and vanishes precisely at μ_∞, the set of all roots of unity, and 0 by a theorem of Kronecker. It is also invariant under Galois conjugation and satisfies $h(\alpha^n) = |n| h(\alpha)$ for all $\alpha \in \overline{\mathbb{Q}}$ and all $n \in \mathbb{Z}$. For more properties on h, see [8].

Let X be a set of algebraic numbers. We say that points of small height (or short, small points) of X lie in a set $Y \subset \overline{\mathbb{Q}}$ if there exists a positive constant c such that $h(\alpha) \geq c$ for all $\alpha \in X \backslash Y$.

The case where small points of an algebraic field lie in $\mu_\infty \cup \{0\}$ has been intensively studied since the beginning of this century (see, for example, [2, 3, 5, 9, 11–14, 16, 18, 21, 22, 28]). For various technical reasons, it is difficult to adapt the ideas of these papers to locate small points of an algebraic field that are not contained in $\mu_\infty \cup \{0\}$. As far as [1] shows, the first one who managed to do this is Amoroso in 2016, see our explanation below for more details.

Consider the field $L = \mathbb{Q}(\mu_\infty, \alpha, \alpha^{1/2}, \alpha^{1/3}, \dots)$, where $\alpha \in \overline{\mathbb{Q}}^*$. It is trivial to construct small points in L^*. For instance, we have all roots of unity, but also $\alpha^{1/n}$ with n large enough since $h(\alpha^{1/n}) = h(\alpha)/n$. But does L^* also contain nonobvious

Received by the editors February 9, 2023; revised September 21, 2023; accepted October 23, 2023.
Published online on Cambridge Core October 31, 2023.
This work was funded by Morningside Center of Mathematics, CAS.
AMS subject classification: **11G50, 11R04.**
Keywords: Weil height, Rémond's conjecture, equidistribution.

small points; i.e., elements of small height not in $\{\zeta\alpha^q, \zeta \in \mu_\infty, q \in \mathbb{Q}\}$? By a result of Amoroso and Dvornicich [3], the answer is no if $\alpha \in \mu_\infty$. But this question is still open for $\alpha \notin \mu_\infty$. A very particular case of a deep and recent conjecture of Rémond, related to the Zilber–Pink conjecture, predicts a negative answer to this question (see Conjecture 1.1).

Throughout this introduction, Γ always denotes a finitely generated subgroup of $\overline{\mathbb{Q}}^*$. Define Γ_{div} as the division group of Γ, i.e., the set of $\gamma \in \overline{\mathbb{Q}}^*$ for which there exists an integer $n \in \mathbb{N} = \{1, 2, \dots\}$ satisfying $\gamma^n \in \Gamma$.

Conjecture 1.1 (Rémond [27, Conjecture 3.4]) *Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a finitely generated subgroup.*

(i) *(Strong form): There is a positive constant c such that*

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}(\Gamma_{\text{div}}, \alpha) : \mathbb{Q}(\Gamma_{\text{div}})]} \text{ for all } \alpha \in \overline{\mathbb{Q}}^* \backslash \Gamma_{\text{div}}.$$

(ii) *(Weak form): For any $\varepsilon > 0$, there exists a positive constant c_ε such that*

$$h(\alpha) \geq \frac{c_\varepsilon}{[\mathbb{Q}(\Gamma_{\text{div}}, \alpha) : \mathbb{Q}(\Gamma_{\text{div}})]^{1+\varepsilon}} \text{ for all } \alpha \in \overline{\mathbb{Q}}^* \backslash \Gamma_{\text{div}}.$$

(iii) *(Degree one form): Small points of $\mathbb{Q}(\Gamma_{\text{div}})^*$ lie in Γ_{div}.*

The reader interested on recent advances concerning Rémond's conjecture is referred to [1, 15, 23, 24, 26, 27].

Write $\langle X \rangle$ for the group generated by a set $X \subset \overline{\mathbb{Q}}^*$. We clearly have the implications $(i) \Rightarrow (ii) \Rightarrow (iii)$. The strong form generalizes the relative Lehmer's problem, which corresponds to the case $\Gamma = \{1\}$. As far as [3] and [4] show, the strong form is not yet known in any situation and both the weak form and the degree one form are only known when Γ is trivial. The first partial result going in the direction of Conjecture 1.1 for nontrivial groups was given by Amoroso. He proved that small points of $\mathbb{Q}(\zeta_3, 2^{1/3}, \zeta_{3^2}, 2^{1/3^2}, \dots)^*$, with $\zeta_n = e^{2i\pi/n}$, lie in $\langle 2 \rangle_{\text{div}}$ [1, Theorem 1.3]. The author then proved the same assertion by replacing 2 with $\alpha \in \mathbb{Q}^*$ and 3 with a rational prime $p > 2$ [23, Théorème 1.8].

The proof of these last two results relies on the "classical method," i.e., the one to treat the case where small points of an algebraic field lie in $\mu_\infty \cup \{0\}$. As already implied in [1, Remark 3.4], it seems that this method is (very) limited to handle Conjecture 1.1(iii), which explains why it is still largely open. So we need to tackle this conjecture from a totally different angle. We suggest a new one below.

1.2 Presentation of results

Let (y_n) be a sequence of $\mathbb{Q}(\Gamma_{\text{div}})^*$ such that $h(y_n) \to 0$. From Bilu's equidistribution theorem [6], it is not hard to check that

$$\frac{\#\{\sigma : \mathbb{Q}(y_n) \hookrightarrow \overline{\mathbb{Q}}, \ 1 - \varepsilon \leq |\sigma y_n| \leq 1 + \varepsilon\}}{[\mathbb{Q}(y_n) : \mathbb{Q}]} \underset{n \to +\infty}{\longrightarrow} 1$$

for all $\varepsilon > 0$ (if the sequence of terms $[\mathbb{Q}(y_n) : \mathbb{Q}]$ is bounded, then $y_n \in \mu_\infty$ for all n large enough by Northcott's theorem, and so the ratio above is 1 for all n large

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

enough). In other words, if the Weil height of y_n is small enough, then "most of" its Galois conjugates over $\mathbb{Q}$ are "close" to the unit circle. Nonetheless, as $K_\Gamma = \mathbb{Q}(\mu_\infty, \Gamma)$ is not a number field, Bilu's theorem above cannot tell anything about the location in the complex plane of Galois conjugates of y_n over K_Γ. Our results stipulate that a fairly precise knowledge of the distribution of these numbers allows us to solve a part of Conjecture 1.1(iii). In Section 3, we will prove a result reducing the study of Conjecture 1.1(iii) to the case that for all n large enough, "most of" Galois conjugates of y_n over K_Γ are "close" to the unit circle.

Let $\alpha \in \overline{\mathbb{Q}}$, and let $\varepsilon > 0$. We write $O_\Gamma(\alpha)$ for the orbit of α under $\mathrm{Gal}(\overline{\mathbb{Q}}/K_\Gamma)$ and we put

$$d_{\Gamma,\varepsilon}(\alpha) := \frac{\#\{x \in O_\Gamma(\alpha), 1-\varepsilon \le |x|^2 \le 1+\varepsilon\}}{\#O_\Gamma(\alpha)}.$$

Theorem 1.2 *Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a finitely generated subgroup. Then Conjecture 1.1(iii) is equivalent to the following assertion: Let (y_n) be a sequence of $\mathbb{Q}(\Gamma_{\mathrm{div}})^*$ such that $h(y_n) \to 0$. Assume that $d_{\Gamma,\varepsilon}(y_n) \underset{n\to+\infty}{\longrightarrow} 1$ for all $\varepsilon > 0$. Then $y_n \in \Gamma_{\mathrm{div}}$ for all n large enough.*

The length of an element $x \in \mathbb{Q}(\Gamma_{\mathrm{div}})$ is defined to be the smallest integer $l \in \mathbb{N}$ for which x can express as $x = \sum_{j=1}^{l} x_j \gamma_j$ with $x_j \in K_\Gamma$ and $\gamma_j \in \Gamma_{\mathrm{div}}$. Each element of Γ_{div} has length 1. For $N \in \mathbb{N}$, put $l_N(\Gamma)$ the set of elements of $\mathbb{Q}(\Gamma_{\mathrm{div}})$ with length $\le N$.

From Theorem 1.2, it is enough to prove the following two conjectures to deduce Conjecture 1.1(iii).

Conjecture 1.3 *Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a finitely generated subgroup, and let (y_n) be a sequence of $\mathbb{Q}(\Gamma_{\mathrm{div}})^*$ such that $h(y_n) \to 0$ and $d_{\Gamma,\varepsilon}(y_n) \underset{n\to+\infty}{\longrightarrow} 1$ for all $\varepsilon > 0$. Then there exists $N \in \mathbb{N}$ such that $y_n \in l_N(\Gamma)$ for all n large enough.*

Conjecture 1.4 *Let $N \in \mathbb{N}$, and let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a finitely generated subgroup. Let (y_n) be a sequence of $l_N(\Gamma)\backslash\{0\}$ such that $h(y_n) \to 0$ and $d_{\Gamma,\varepsilon}(y_n) \underset{n\to+\infty}{\longrightarrow} 1$ for all $\varepsilon > 0$. Then $y_n \in \Gamma_{\mathrm{div}}$ for all n large enough.*

Conjecture 1.4 with $N = 1$ was solved by Rémond, see Lemma 1.5. Conjectures 1.1(iii) and 1.3 with $N = 1$ are therefore equivalent. However, this does not remove the interest of Conjecture 1.4 because Conjecture 1.3 could be easier to show when N is large.

Both conjectures seem to be treated separately. Hence, we focus in this article on the second one only.

For a set X of algebraic numbers, write $X.\Gamma_{\mathrm{div}}$ for the set of xy with $x \in X$ and $y \in \Gamma_{\mathrm{div}}$. Note that $l_1(\Gamma) = K_\Gamma.\Gamma_{\mathrm{div}}$. The rank of an abelian group G is given by the maximal number of linearly independent elements in G. Note that Γ and Γ_{div} have the same rank.

Lemma 1.5 (Rémond) *Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a finitely generated subgroup, and let F/K_Γ be a finite extension. Then small points of $F^*.\Gamma_{\mathrm{div}}$ lie in Γ_{div}.*

Proof By Amoroso and Zannier's result [5, Theorem 1.2], small points of F^* lie in $\mu_\infty \subset \Gamma_{\mathrm{div}}$. By assumption, $\Gamma \subset \Gamma_{\mathrm{div}} \cap F^* \subset \Gamma_{\mathrm{div}}$. Thus $\Gamma, \Gamma_{\mathrm{div}} \cap F^*$ and Γ_{div} all have the same rank, which is finite since Γ is finitely generated. For $a \in F$, set

$$h_\Gamma(a) = \min\{h(a\gamma), \gamma \in \Gamma_{\text{div}}\}.$$

Thanks to a result of Rémond [26, Corollary 2.3], there is a positive constant c such that $h_\Gamma(a) \geq c$ for all $a \in F^* \backslash \Gamma_{\text{div}}$.

Let $y = a\gamma \in F^*.\Gamma_{\text{div}}$, where $a \in F^*$ and $\gamma \in \Gamma_{\text{div}}$, such that $h(y) < c$. As $c > h(y) \geq h_\Gamma(a)$, we get $a \in \Gamma_{\text{div}}$ by the foregoing. The lemma follows. ∎

Remark 1.6 This lemma can be made quantitative since [5, Theorem 1.2] and [26, Corollary 2.3] are.

Among all our theorems, the next one is the most difficult (and technical) to show. Hence, we will prove it at the end of this paper, that is in Section 8.

Theorem 1.7 *Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a finitely generated subgroup, let $N \in \mathbb{N}$, and let (y_n) be a sequence of $l_N(\Gamma)$. Assume that $d_{\Gamma,\varepsilon}(y_n) \underset{n\to+\infty}{\longrightarrow} 1$ for all $\varepsilon > 0$. Then for all $\varepsilon > 0$, we have $d_{\Gamma,\varepsilon}(y_n) = 1$ for all n large enough.*

Remark 1.8 The proof of this theorem does not hold if we study the Galois conjugates of y_n over $\mathbb{Q}$ (or $\mathbb{Q}(\Gamma)$) instead of K_Γ. The reason is that we will use Kummer theory and for this, it is primordial that our ground field contains all roots of unity.

Theorem 1.7 means that if "most of" elements in $O_\Gamma(y_n)$ are "close" to the unit circle, then they all are. Note that this theorem holds regardless of the value of $h(y_n)$, which leads to the following natural question: How are the elements of $O_\Gamma(y_n)$ scattered around the unit circle when $h(y_n)$ is small enough ? We predict they are concyclic and located on a circle centered at the origin. If it checks out, then Conjecture 1.4 would immediately fall thanks to our next theorem, a proof of which is given in Section 5.

Denote by $U(\Gamma)$ the set of algebraic numbers α such that the elements of $O_\Gamma(\alpha)$ are concyclic and located on a circle centered at the origin. Check that Γ_{div} is a subgroup of $U(\Gamma)$: Let $x \in \Gamma_{\text{div}}$, and let $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K_\Gamma)$. By definition of the division group, we have $x^n \in \Gamma$ for some $n \in \mathbb{Z}\backslash\{0\}$. Thus $\sigma(x^n) = x^n$ implying $|\sigma x| = |x|$; whence $x \in U(\Gamma)$.

Theorem 1.9 *Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a finitely generated subgroup, and let $N \in \mathbb{N}$. Then small points of $l_N(\Gamma) \cap U(\Gamma)$ lie in Γ_{div}.*

Remark 1.10 Theorem 1.9 can be made quantitative by using the arguments of this paper (see Remark 5.3 for details).

End this section by providing a collection of Γ for which small points of $l_N(\Gamma)\backslash\{0\}$ lie in $U(\Gamma)$, thus giving credit to our approach to attack Conjecture 1.1(iii).

A CM-field is a totally imaginary quadratic extension of a totally real field. The maximal totally real field extension $\mathbb{Q}^{tr}$ of $\mathbb{Q}$ having only one quadratic extension, namely $\mathbb{Q}^{tr}(i)$, the CM-fields are therefore the subfields of $\mathbb{Q}^{tr}(i)$ that are not totally real. In particular, a compositum of CM-fields is a CM-field. The classification of CM-number fields was made in [7]; these are the fields of the form $\mathbb{Q}(\alpha)$ with $\alpha \in U\backslash\{\pm 1\}$, where U denotes the set of algebraic numbers with all its conjugates over $\mathbb{Q}$ on the unit circle. Note that if $\Gamma \subset U$, then $\Gamma_{\text{div}} \subset U$. The field $\mathbb{Q}(\Gamma_{\text{div}})$ is therefore a CM-field since it is the compositum of all $\mathbb{Q}(\alpha)$ with $\alpha \in \Gamma_{\text{div}}\backslash\{\pm 1\}$.

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

Corollary 1.11 *Let $\Gamma \subset U$ be a finitely generated subgroup, and let $N \in \mathbb{N}$. Then small points of $l_N(\Gamma)\backslash\{0\}$ lie in Γ_{div}.*

Proof By a theorem of Schinzel [29, Theorem 2], see also [25], small points of $\mathbb{Q}^{tr}(i)^*$ lie in U. As $\Gamma \subset U$, the field $\mathbb{Q}(\Gamma_{\mathrm{div}})$ is a CM-field; whence $\mathbb{Q}(\Gamma_{\mathrm{div}}) \subset \mathbb{Q}^{tr}(i)$. Small points of $l_N(\Gamma)\backslash\{0\}$ therefore lie in U. The corollary now arises from Theorem 1.9 since $U \subset U(\Gamma)$ by definition. ∎

Conjectures 1.1(iii) and 1.3 are therefore equivalent for CM-fields. This corollary is the second partial result going in the direction of Conjecture 1.1(iii), and the first one of this form.

2 Kummer theory

Fix once and for all a finitely generated subgroup $\Gamma \subset \overline{\mathbb{Q}}^*$ of rank b. As Conjecture 1.1(iii), and therefore Conjecture 1.4, is true for $b = 0$ (see the introduction), we can reduce the proof of all theorems mentioned in the introduction to the case that $b > 0$. We also fix once and for all a generating set $\mathcal{F} = \{\alpha_1, \dots, \alpha_b\}$ of the torsion-free part of Γ. Finally, for $n \in \mathbb{N}$, we put $\mathcal{F}^{1/n} = \{\alpha_1^{1/n}, \dots, \alpha_b^{1/n}\}$ and we define μ_n as the set of roots of unity killed by n.

Let n be a positive integer dividing $m \in \mathbb{N} \cup \{\infty\}$ (by convention, all integers divide ∞). Galois theory claims that $\mathrm{Gal}(\mathbb{Q}(\mu_m, \mathcal{F}^{1/n})/\mathbb{Q}(\mathcal{F}))$ is isomorphic to the inner semidirect product of $\mathrm{Gal}(\mathbb{Q}(\mu_m, \mathcal{F})/\mathbb{Q}(\mathcal{F}))$ and $\mathrm{Gal}(\mathbb{Q}(\mu_m, \mathcal{F}^{1/n})/\mathbb{Q}(\mu_m, \mathcal{F}))$. Thus each element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_m, \mathcal{F}^{1/n})/\mathbb{Q}(\mathcal{F}))$ can be identified with a pair

$$(\phi_\sigma, \psi_\sigma) \in \mathrm{Gal}(\mathbb{Q}(\mu_m, \mathcal{F})/\mathbb{Q}(\mathcal{F})) \times \mathrm{Gal}(\mathbb{Q}(\mu_m, \mathcal{F}^{1/n})/\mathbb{Q}(\mu_m, \mathcal{F})).$$

Concretely, if $x = \sum_{j=1}^{l} a_j \gamma_j \in \mathbb{Q}(\mu_m, \mathcal{F}^{1/n})$ with $a_j \in \mathbb{Q}(\mu_m, \mathcal{F})$ and $\gamma_j \in \langle \mathcal{F}^{1/n} \rangle$, then $\sigma x = \sum_{j=1}^{l} \phi_\sigma(a_j)\psi_\sigma(\gamma_j)$.

The Cartesian product above can be explicitly described. The computation of the left piece can be done thanks to the class field theory and that of the right piece by using a result of Perruca and Sgobba [19, Theorem 13], see the lemma below.

Lemma 2.1 *Let $L/\mathbb{Q}(\mathcal{F})$ be a finite extension. Then there exists an integer $C \in \mathbb{N}$, depending only on Γ and L, such that for all $d_1, \dots, d_b \in \mathbb{N}$ divising m, we have*

$$G = \mathrm{Gal}(L(\mu_m, \alpha_1^{1/d_1}, \dots, \alpha_b^{1/d_b})/L(\mu_m)) \simeq \prod_{l=1}^{b} \mathbb{Z}/(d_l/c_l)\mathbb{Z}$$

for some positive integers $c_1, \dots, c_b \leq C$.

Proof Put $L_0 = L(\mu_m)$ and $L_l = L_{l-1}(\alpha_l^{1/d_l})$ for all $l \in \{1, \dots, b\}$. Let G_l denote the Galois group of the extension L_l/L_{l-1}. Galois theory tells us that G is the inner semidirect product of G_b and $\mathrm{Gal}(L_{b-1}/L_0)$. As G is abelian, this product is the Cartesian product. An easy induction shows that $G \simeq \prod_{l=1}^{b} G_l$. For all l, it is trivial that $G_l \simeq \mathbb{Z}/(d_l/c_l)\mathbb{Z}$ for some $c_l \in \mathbb{N}$. So $G \simeq \prod_{l=1}^{b} \mathbb{Z}/(d_l/c_l)\mathbb{Z}$. Write $d = \max\{d_1, \dots, d_b\}$. Theorem 13 in [19] claims that the extension $L_0(\mathcal{F}^{1/d})/L_0$ has degree at least d^b/C for some $C \in \mathbb{N}$ depending only on Γ and L. On the other hand,

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

$L_0(\mathcal{F}^{1/d})/L_0(\alpha_1^{1/d_1},\ldots,\alpha_b^{1/d_b})$ has degree at most $d^b/\prod_{l=1}^b d_l$. The multiplicativity formula for degrees proves that $\#G \geq (\prod_{l=1}^b d_l)/C$; whence $\prod_{l=1}^b c_l \leq C$. ∎

Remark 2.2 The isomorphism of Lemma 2.1 is explicit: For each $(r_1,\ldots,r_b) \in \prod_{l=1}^b \mathbb{Z}/(d_l/c_l)\mathbb{Z}$, there is an unique $\psi \in G$ such that $\psi\alpha_l^{1/d_l} = \zeta_{d_l/c_l}^{r_l}\alpha_l^{1/d_l}$ for all l. Moreover, we have $\alpha_l^{1/c_l} \in L$ since $\psi\alpha_l^{1/c_l} = (\psi\alpha_l^{1/d_l})^{d_l/c_l} = \alpha_l^{1/c_l}$ for all $\psi \in G$. By abuse of notation, this isomorphism becomes from now an equality.

Remark 2.3 The constant C of Lemma 2.1 can be explicitly determined (see [19, Remark 20] for details).

3 Proof of Theorem 1.2

It is clear that Conjecture 1.1(iii) implies the assertion stated in Theorem 1.2. Now, assume that this assertion is true and prove Conjecture 1.1(iii).

Let (x_n) be a sequence of $\mathbb{Q}(\Gamma_{\text{div}})^*$ such that $h(x_n) \to 0$. We want to show that $x_n \in \Gamma_{\text{div}}$ for all n large enough. For this, assume by contradiction that $x_n \notin \Gamma_{\text{div}}$ for infinitely many n, that is for all n by taking a suitable subsequence.

Lemma 3.1 *We have* $[\mathbb{Q}(x_n^2):\mathbb{Q}] \to +\infty$.

Proof Let l be an accumulation point of the sequence $([\mathbb{Q}(x_n^2):\mathbb{Q}])$. Passing to a subsequence, we get $[\mathbb{Q}(x_n^2):\mathbb{Q}] \to l$. If $l < +\infty$, then our sequence is bounded and Northcott's theorem implies that $x_n^2 \in \mu_\infty \subset \Gamma_{\text{div}}$ for all n large enough, which is absurd. So $l = +\infty$ and the lemma follows. ∎

Recall that $K_\Gamma = \mathbb{Q}(\mu_\infty,\Gamma) = \mathbb{Q}(\mu_\infty,\mathcal{F})$ and note that $\mathbb{Q}(\Gamma_{\text{div}}) = \bigcup_{n\in\mathbb{N}} K_\Gamma(\mathcal{F}^{1/n})$.

Lemma 3.2 *There is a sequence* (σ_n) *of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mathcal{F}))$ *such that* $d_{\Gamma,\varepsilon}(\sigma_n x_n) \underset{n\to+\infty}{\longrightarrow} 1$ *for all* $\varepsilon > 0$.

Proof Let $n \in \mathbb{N}$. There exists $m_n \in \mathbb{N}$ such that $x_n \in K_\Gamma(\mathcal{F}^{1/m_n})$. We can also find a multiple $m'_n \in \mathbb{N}$ of m_n such that:

(i) $x_n \in \mathbb{Q}(\zeta_{m'_n},\mathcal{F}^{1/m_n})$.
(ii) The restriction map $\mathrm{Gal}(K_\Gamma(\mathcal{F}^{1/m_n})/K_\Gamma) \to H_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{m'_n},\mathcal{F}^{1/m_n})/\mathbb{Q}(\zeta_{m'_n},\mathcal{F}))$ is an isomorphism.

Express x_n as $x_n = \sum_{j=1}^{l_n} a_{j,n}\gamma_{j,n}$ with $a_{j,n} \in \mathbb{Q}(\zeta_{m'_n},\mathcal{F})$ and $\gamma_{j,n} \in \langle\mathcal{F}^{1/m_n}\rangle$. Fix $\varepsilon > 0$. For any $\phi \in N_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{m'_n},\mathcal{F})/\mathbb{Q}(\mathcal{F}))$, we set

$$d_n(\phi) = \frac{\#\left\{\psi \in H_n, 1-\varepsilon \leq \left|\sum_{j=1}^{l_n}\phi(a_{j,n})\psi(\gamma_{j,n})\right|^2 \leq 1+\varepsilon\right\}}{\#H_n}$$

and we pick $\phi_n \in N_n$ such that $d_n(\phi_n) = \max_{\phi\in N_n}\{d_n(\phi)\}$.

By Galois theory, $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{m'_n},\mathcal{F}^{1/m_n})/\mathbb{Q}(\mathcal{F}))$ is isomorphic to the inner semidirect product of N_n and H_n. Denote by σ_n the element of G_n corresponding to the pair $(\phi_n,1) \in N_n \times H_n$. Section 2 tells us that $\sigma_n x_n = \sum_{j=1}^{l_n}\phi_n(a_{j,n})\gamma_{j,n}$.

From (i) and (ii), we infer that $O_\Gamma(\sigma_n x_n)$ is equal to the orbit of $\sigma_n x_n$ under H_n. Thus, it follows from the definition of $d_{\Gamma,\varepsilon}(\sigma_n x_n)$ (see Section 1.2) that

$$d_{\Gamma,\varepsilon}(\sigma_n x_n) = \frac{\#\{\psi \in H_n, 1-\varepsilon \le |\psi\sigma_n x_n|^2 \le 1+\varepsilon\}}{\# H_n} = d_n(\phi_n).$$

A small calculation gives

$$\begin{aligned} u_n &= \#\{\sigma \in G_n, 1-\varepsilon \le |\sigma x_n|^2 \le 1+\varepsilon\} \\ &= \#\left\{(\phi,\psi) \in N_n \times H_n, 1-\varepsilon \le \left|\sum_{j=1}^{l_n} \phi(a_{j,n})\psi(\gamma_{j,n})\right|^2 \le 1+\varepsilon\right\} \\ &= \sum_{\phi \in N_n} \#\left\{\psi \in H_n, 1-\varepsilon \le \left|\sum_{j=1}^{l_n} \phi(a_{j,n})\psi(\gamma_{j,n})\right|^2 \le 1+\varepsilon\right\}, \end{aligned}$$

and so

$$\frac{u_n}{\# G_n} = \frac{1}{\# N_n}\sum_{\phi \in N_n} d_n(\phi) \le d_n(\phi_n) = d_{\Gamma,\varepsilon}(\sigma_n x_n) \le 1. \tag{1}$$

Recall that $\mathcal{F}$ is a finite set. As $h(x_n^2) = 2h(x_n) \to 0$ and $[\mathbb{Q}(\mathcal{F}, x_n^2) : \mathbb{Q}(\mathcal{F})] = [\mathbb{Q}(\mathcal{F}, x_n^2) : \mathbb{Q}]/[\mathbb{Q}(\mathcal{F}) : \mathbb{Q}] \to +\infty$ by Lemma 3.1, we infer from Bilu's equidistribution theorem [30, Subsection 1.1, Theorem] applied to $K = \mathbb{Q}(\mathcal{F})$ that $u_n/\# G_n$ goes to 1 as $n \to +\infty$. Lemma follows by involving the squeeze theorem in (1). ∎

Proof of Theorem 1.4 We have $h(\sigma_n x_n) = h(x_n) \to 0$ and $d_{\Gamma,\varepsilon}(\sigma_n x_n) \underset{n\to+\infty}{\longrightarrow} 1$ for all $\varepsilon > 0$ by Lemma 3.2. Applying the assertion of Theorem 1.2 (which is assumed to be true) to $y_n = \sigma_n x_n$ shows that $\sigma_n x_n \in \Gamma_{\text{div}}$ for all n large enough.

By definition of the division group, we deduce that $\sigma_n(x_n^{j_n}) \in \langle \mathcal{F} \rangle$ for some integer $j_n \in \mathbb{N}$. As σ_n fixes the elements of $\mathcal{F}$, we conclude $x_n^{j_n} \in \langle \mathcal{F} \rangle \subset \Gamma$, which contradicts the fact that $x_n \notin \Gamma_{\text{div}}$. This finishes the proof of Theorem 1.2. ∎

4 Direct image of μ_d under a meromorphic function

Definition 4.1 Let $N \in \mathbb{N}$. Denote by $\mathcal{S}_N$ the set of integers $d \in \mathbb{N}$ for which there exists a meromorphic function $f(z) = \sum_{j=1}^N a_j z^{b_j}$ on $\mathbb{C}^*$ satisfying $|f(\zeta)| = 1$ for all $\zeta \in \mu_d$. Moreover, we impose that:

- $b_1 = 0, b_2, \ldots, b_N \in \mathbb{Z}$ are pairwise distinct integers such that $b_1, \ldots, b_N$ and d have no common positive factors other than 1;
- $a_1, \ldots, a_N \in \mathbb{C}$ satisfy $\sum_{i \in I} a_i \neq 0$ for all non-empty subsets $I \subset \{1, \ldots, N\}$.

The study of $\mathcal{S}_N$ might be of independent interest, but we only prove in this section what is needed for this article, namely the finiteness of it for all $N \in \mathbb{N}$.

Let $N \ge 2$, and let $d \in \mathcal{S}_N$ be greater than $4^N(N^2 - 1)$. The lemma below asserts that regardless of the choice of integers $b_1, \ldots, b_N$ as in Definition 4.1, at least one of them has an absolute value greater than or equal to $d/4$. We will then contradict this claim thanks to Dirichlet's theorem on simultaneous approximation.

Lemma 4.2 *Let $M \geq 2$, and let $g(z) = \sum_{j=1}^{M} u_j z^{c_j}$ be a meromorphic function on $\mathbb{C}^*$ with $u_1, \dots, u_M \in \mathbb{C}^*$ and $c_1, \dots, c_M \in \mathbb{Z}$ pairwise distinct integers. If $d \geq M^2$ is an integer such that $|g(\zeta)| = 1$ for all $\zeta \in \mu_d$, then* $\max\{|c_1|, \dots, |c_M|\} \geq d/4$.

Proof Assume by contradiction that $\max\{|c_1|, \dots, |c_M|\} < d/4$. Write

$$\{\gamma_1, \dots, \gamma_n\} = \{c_i - c_j, 1 \leq i, j \leq M\}$$

with $n \leq M^2$ and $\gamma_1, \dots, \gamma_n$ pairwise distinct. Note that $0 = c_1 - c_1 \in \{\gamma_1, \dots, \gamma_n\}$. We can thus assume that $\gamma_1 = 0$. Moreover, $\gamma_k \in [-d/2, d/2]$ for all k since $\max\{|c_1|, \dots, |c_M|\} < d/4$.

For each $k \in \{1, \dots, n\}$, define E_k as the set of pairs $(i, j) \in \{1, \dots, M\}^2$ for which $\gamma_k = c_i - c_j$. Clearly, $E_1, \dots, E_n$ is a partition of $\{1, \dots, M\}^2$. Then put $v_k = \sum_{(i,j)\in E_k} u_i \overline{u_j}$. An easy calculation gives, for all $l \in \{0, \dots, d-1\}$,

$$\begin{aligned} \sum_{k=1}^{n} \zeta_d^{l\gamma_k} v_k &= \sum_{k=1}^{n} \sum_{(i,j)\in E_k} u_i \overline{u_j} \zeta_d^{l(c_i - c_j)} \\ &= \sum_{(i,j)\in \bigsqcup_{k=1}^{n} E_k} u_i \overline{u_j} \zeta_d^{l(c_i - c_j)} = \sum_{1\leq i,j\leq M} u_i \overline{u_j} \zeta_d^{l(c_i - c_j)} \\ &= \left(\sum_{i=1}^{M} u_i \zeta_d^{lc_i} \right) \left(\sum_{j=1}^{M} \overline{u_j} \zeta_d^{-lc_j} \right) = g(\zeta_d^l)\overline{g(\zeta_d^l)} = 1, \end{aligned} \tag{2}$$

the last equality coming from the fact that $|g(\zeta)| = 1$ for all $\zeta \in \mu_d$. We recognize a linear system with n unknowns (namely, $v_1, \dots, v_n$) and d equations. By assumption, $d \geq M^2 \geq n$. The (square) matrix associated with the linear subsystem

$$\forall l \in \{0, \dots, n-1\}, \quad \sum_{k=1}^{n} \zeta_d^{l\gamma_k} v_k = 1 \tag{3}$$

is the Vandermonde matrix $\left(\zeta_d^{l\gamma_k}\right)_{\substack{0\leq l\leq n-1 \\ 1\leq k\leq n}}$. It is well-known that its determinant is $\prod_{1\leq i<j\leq n} (\zeta_d^{\gamma_j} - \zeta_d^{\gamma_i})$. As $\gamma_1, \dots, \gamma_n \in [-d/2, d/2]$ are pairwise distinct, the numbers $\zeta_d^{\gamma_1}, \dots, \zeta_d^{\gamma_n}$ are therefore pairwise distinct. Hence, the determinant above is nonzero, and so (3) has a unique solution. Thus, (2) has at most one solution. As $\gamma_1 = 0$, it follows that $(v_1, \dots, v_n) = (1, 0, \dots, 0)$ is the unique solution of (2).

Denote by i_0, resp. j_0, the element of $\{1, \dots, M\}$ such that

$$c_{i_0} = \max\{c_1, \dots, c_M\}, \text{ resp. } c_{j_0} = \min\{c_1, \dots, c_M\}. \tag{4}$$

Let $m \in \{1, \dots, n\}$ be the integer such that $\gamma_m = c_{i_0} - c_{j_0}$, and let $(i, j) \in E_m$. Then $c_i - c_j = c_{i_0} - c_{j_0}$ and (4) leads to $c_i = c_{i_0}$ and $c_j = c_{j_0}$. As $c_1, \dots, c_M$ are pairwise distinct, we get $(i, j) = (i_0, j_0)$. In conclusion, $E_m = \{(i_0, j_0)\}$.

Recall that $\gamma_1 = 0$. So the set E_1 contains at least $M \geq 2$ elements, namely, $(1, 1), \dots, (M, M)$; whence $m > 1$. But then, by the foregoing, we have

$$0 = v_m = \sum_{(i,j)\in E_m} u_i \overline{u_j} = u_{i_0} \overline{u_{j_0}},$$

i.e., either $u_{i_0} = 0$ or $u_{j_0} = 0$, which is absurd. This completes the proof. ∎

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

We can now prove the desired result.

Theorem 4.3 *For all $N \in \mathbb{N}$, the set $\mathcal{S}_N$ is finite. Moreover, $\mathcal{S}_1 = \{1\}$ and $4^N(N^2 - 1)$ is an upper bound of $\mathcal{S}_N$ for all $N \geq 2$.*

Proof Let $d \in \mathcal{S}_N$. There is a meromorphic function $f(z) = \sum_{j=1}^{N} a_j z^{b_j}$ on $\mathbb{C}^*$ such that $|f(\zeta)| = 1$ for all $\zeta \in \mu_d$, where $a_1, \dots, a_N$ and $b_1, \dots, b_N$ are as in Definition 4.1. If $N = 1$, then d has to be coprime to $b_1 = 0$, i.e., $d = 1$. As $|1| = 1$, we get $\mathcal{S}_1 = \{1\}$. Now assume that $N \geq 2$.

Dirichlet's theorem on simultaneous approximation asserts the existence of integers $p_1, \dots, p_N \in \mathbb{Z}$ and $q \in \{1, \dots, 4^N\}$ such that $|q(b_j/d) - p_j| < 1/4$ for all $j \in \{1, \dots, N\}$. Write e for the greatest common divisor of q and d, then put $q' = q/e$ and $d' = d/e$. Clearly, q' and d' are coprime, $e \in \{1, \dots, 4^N\}$ and

$$(5) \qquad \forall j \in \{1, \dots, N\}, \qquad |q' b_j - d' p_j| < d'/4.$$

Put $\{c_1, \dots, c_M\} = \{q' b_1 - d' p_1, \dots, q' b_N - d' p_N\}$, where $c_1, \dots, c_M$ are pairwise distinct. We can assume that $c_1 = q' b_1 - d' p_1$. For all $k \in \{1, \dots, M\}$, denote by E_k the set of integers $j \in \{1, \dots, N\}$ such that $c_k = q' b_j - d' p_j$. Clearly $E_1, \dots, E_M$ is a partition of $\{1, \dots, N\}$. Put $u_k = \sum_{j \in E_k} a_j$ and $g(z) = \sum_{k=1}^{M} u_k z^{c_k}$.

As $b_1 = 0$ by Definition 4.1 and $|p_1| < 1/4$ by (5), we conclude $c_1 = 0$. Let n be a common positive factor of $c_1, \dots, c_M$ and d'. From the definition of c_i, we deduce that n divides $q' b_1, \dots, q' b_N$ and $q' d'$. By Definition 4.1, $b_1, \dots, b_N$ and d' have no common positive factors other than 1 since d' divides d. Hence, n divides q'. But it divides d' too. Whence $n = 1$ since q' and d' are coprime.

We have $\sum_{k \in I} u_k \neq 0$ for all non-empty subsets $I \subset \{1, \dots, M\}$ since otherwise,

$$0 = \sum_{k \in I} u_k = \sum_{k \in I} \sum_{j \in E_k} a_j = \sum_{j \in \bigsqcup_{k \in I} E_k} a_j,$$

which disagrees with Definition 4.1. In particular, $u_1, \dots, u_M \in \mathbb{C}^*$. Finally,

$$\forall l \in \mathbb{Z}, \qquad f(\zeta_d^{ql}) = \sum_{j=1}^{N} a_j \zeta_d^{q b_j l} = \sum_{j=1}^{N} a_j \zeta_{d'}^{q' b_j l} = \sum_{j=1}^{N} a_j \zeta_{d'}^{(q' b_j - d' p_j) l}$$
$$= \sum_{k=1}^{M} \sum_{j \in E_k} a_j \zeta_{d'}^{(q' b_j - d' p_j) l} = \sum_{k=1}^{M} u_k \zeta_{d'}^{c_k l} = g(\zeta_{d'}^{l}).$$

As $|f(\zeta)| = 1$ for all $\zeta \in \mu_d$, we infer that $|g(\zeta)| = 1$ for all $\zeta \in \mu_{d'}$.

Of all this, we conclude $d' \in \mathcal{S}_M$. Recall that $d' = d/e$ with $e \in \{1, \dots, 4^N\}$, that $u_1, \dots, u_M \in \mathbb{C}^*$, that $c_1, \dots, c_M \in \mathbb{Z}$ are pairwise distinct, that $|g(\zeta)| = 1$ for all $\zeta \in \mu_{d'}$ and that $\max\{|c_1|, \dots, |c_M|\} < d'/4$ by (5). If $M \geq 2$, then Lemma 4.2 applied to $d = d'$ implies $d' = d/e < M^2$; whence $d \leq 4^N(N^2 - 1)$. If $M = 1$, then $d' = 1$ since $\mathcal{S}_1 = \{1\}$. Thus, $d \leq 4^N$ and the theorem follows. ∎

5 Proof of Theorem 1.9

Fix once and for all an integer $N \in \mathbb{N}$. Recall that the length of an element $y \in \mathbb{Q}(\Gamma_{\text{div}})$ is defined to be the smallest $l \in \mathbb{N}$ for which y can express as $y = \sum_{j=1}^{l} y_j \gamma_j$ with $y_j \in K_\Gamma =$

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

$\mathbb{Q}(\mu_\infty, \Gamma)$ and $\gamma_j \in \Gamma_{\mathrm{div}}$. The lemma below shows that the length is invariant under translation of points in Γ_{div}.

Lemma 5.1 *Let $y \in \mathbb{Q}(\Gamma_{\mathrm{div}})$, and let $z \in \Gamma_{\mathrm{div}}$. Then y and yz have the same length.*

Proof Denote by l, resp. l', the length of y, resp. yz. We can express y as $y = \sum_{j=1}^{l} y_j \gamma_j$ with $y_j \in K_\Gamma$ and $\gamma_j \in \Gamma_{\mathrm{div}}$. Hence, $yz = \sum_{j=1}^{l} y_j(\gamma_j z)$ and the definition of the length leads to $l' \le l$. The inequality $l \le l'$ is obtained by replacing y with yz and z with $z^{-1} \in \Gamma_{\mathrm{div}}$. This completes the proof. ∎

Recall that $\mathcal{F} = \{\alpha_1, \dots, \alpha_b\}$ is the torsion-free part of Γ and that $l_N(\Gamma)$ denotes the set of elements in $\mathbb{Q}(\Gamma_{\mathrm{div}})$ with length $\le N$. Concretely, each $x \in l_N(\Gamma)\backslash\{0\}$ with length l can express as $x = \sum_{j=1}^{l} x_j \prod_{t=1}^{b} \alpha_t^{k_{j,t}/d}$, where $x_j \in K_\Gamma^*$, $d \in \mathbb{N}$ and $k_{j,t} \in \mathbb{Z}$. We also recall that $U(\Gamma)$ is the set of elements in $\overline{\mathbb{Q}}^*$ for which all its conjugates over K_Γ are concyclic and located on a circle centered at the origin. Finally, recall that for any algebraic set X, we define $X.\Gamma_{\mathrm{div}}$ as the set of $x\gamma$ with $x \in X$ and $\gamma \in \Gamma$.

Proposition 5.2 *There is $m \in \mathbb{N}$ such that $l_N(\Gamma) \cap U(\Gamma) \subset K_\Gamma(\mathcal{F}^{1/m})^*.\Gamma_{\mathrm{div}}$.*

Proof Let $x \in l_N(\Gamma) \cap U(\Gamma)$ be an element of length $l \le N$ that we express as above. For each $t \in \{1, \dots, b\}$, set $j_t \in \{1, \dots, l\}$ such that $k_{j_t,t} = \min\{k_{1,t}, \dots, k_{l,t}\}$. Let D_t denote the greatest common divisor of $k_{1,t} - k_{j_t,t}, \dots, k_{l,t} - k_{j_t,t}$ and d, then $c_{j,t} = (k_{j,t} - k_{j_t,t})/D_t$ and $d_t = d/D_t$. By construction, $c_{1,t}, \dots, c_{l,t}$ and d_t have no common positive factors other than 1 for all $t \in \{1, \dots, r\}$. Finally, set

$$y = \sum_{j=1}^{l} x_j \prod_{t=1}^{b} \alpha_t^{c_{j,t}/d_t} \quad \text{and} \quad z = \prod_{t=1}^{b} \alpha_t^{k_{j_t,t}/d} \in \Gamma_{\mathrm{div}}. \tag{6}$$

We easily check that $x = yz$. As $z \in \Gamma_{\mathrm{div}}$, Lemma 5.1 tells us that y has length l too. Let $s \in \{1, \dots, b\}$ be such that $d_s = \max\{d_1, \dots, d_b\}$. If d_s is bounded from above by a constant c depending only on Γ and N, then (6) would show that $y \in K_\Gamma(\mathcal{F}^{1/c!})$. The proposition with $m = c!$ would follow since $x = yz$ with $z \in \Gamma_{\mathrm{div}}$.

Put $\{b_1, \dots, b_n\} = \{c_{1,s}, \dots, c_{l,s}\}$, where $b_1, \dots, b_n$ are pairwise distinct. We can assume that $b_1 = c_{j_s,s}$. For all $k \in \{1, \dots, n\}$, write E_k the set of $j \in \{1, \dots, l\}$ such that $b_k = c_{j,s}$. Clearly $E_1, \dots, E_n$ is a partition of $\{1, \dots, l\}$.

Lemma 2.1 applied to $L = \mathbb{Q}(\Gamma)$ and $m = \infty$ as well as the multiplicativity formula for degrees claim that the extension

$$L/M = K_\Gamma(\alpha_1^{1/d_1}, \dots, \alpha_r^{1/d_r})/K_\Gamma(\alpha_1^{1/d_1}, \dots, \alpha_{s-1}^{1/d_{s-1}}, \alpha_{s+1}^{1/d_{s+1}}, \dots, \alpha_r^{1/d_r})$$

has degree at least d_s/C for some $C > 0$ depending only on Γ. Its Galois group is therefore isomorphic to $\mathbb{Z}/(d_s/c)\mathbb{Z}$ for some $c \le C$. Put

$$y_j = x_j \prod_{t=1, t\neq s}^{b} \alpha_t^{c_{j,t}/d_t} \in M, v_k = \sum_{j \in E_k} y_j, a_k = v_k \alpha_s^{b_k/d_s} \text{ and } f(z) = \sum_{k=1}^{n} (a_k/y) z^{b_k}.$$

Note that $y = \sum_{j=1}^{l} y_j \alpha_s^{c_{j,s}/d_s}$. Establish below that $d_s/c \in \mathcal{S}_n$ (see Definition 4.1).

First, $c_{j_s,s} = 0$ by definition of $c_{j,t}$; whence $b_1 = 0$. Next, $b_1, \dots, b_n$ and d_s/c have no common positive factors other than 1 by construction of $c_{1,s}, \dots, c_{l,s}$ and d_s.

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

Assume that $\sum_{k\in I} a_k = 0$ for some subset $I \subset \{1,\dots,n\}$. Then

$$\sum_{j\in\bigsqcup_{k\in I} E_k} y_j\alpha_s^{c_{j,s}/d_s} = \sum_{k\in I}\sum_{j\in E_k} y_j\alpha_s^{c_{j,s}/d_s} = \sum_{k\in I} v_k\alpha_s^{b_k/d_s} = \sum_{k\in I} a_k = 0,$$

which allows us to deduce that

$$y = \sum_{j=1}^{l} y_j\alpha_s^{c_{j,s}/d_s} = \sum_{j\notin\bigsqcup_{k\in I} E_k} y_j\alpha_s^{c_{j,s}/d_s} = \sum_{j\notin\bigsqcup_{k\in I} E_k} x_j\prod_{t=1}^{b}\alpha_t^{c_{j,t}/d_t}.$$

The definition of the length proves that y has length at most $l - \#\bigsqcup_{k\in I} E_k$. As y has length l and $E_1,\dots,E_n$ are non-empty sets, we conclude that I is empty. The contrapositive proves that $\sum_{k\in I} a_k \neq 0$ for all non-empty subsets $I \subset \{1,\dots,n\}$.

Let $\sigma \in \mathrm{Gal}(L/M)$. As $y_j \in M$ for all j, we get $v_k \in M$ for all k. Collecting the information above, we obtain

$$(7)\qquad \begin{aligned}\sigma y &= \sigma\left(\sum_{j=1}^{l} y_j\alpha_s^{c_{j,s}/d_s}\right) = \sigma\left(\sum_{k=1}^{n}\sum_{j\in E_k} y_j\alpha_s^{c_{j,s}/d_s}\right)\\ &= \sigma\left(\sum_{k=1}^{n} v_k\alpha_s^{b_k/d_s}\right) = \sum_{k=1}^{n} v_k\alpha_s^{b_k/d_s}\zeta_{d_s/c}^{b_k l_\sigma} = yf(\zeta_{d_s/c}^{l_\sigma})\end{aligned}$$

for some $l_\sigma \in \{1,\dots,d_s/c\}$. Recall that $y = x/z$, that $x \in U(\Gamma)$ and that $z \in \Gamma_{\mathrm{div}} \subset U(\Gamma)$ (see the introduction). As $U(\Gamma)$ is a group, we deduce that $y \in U(\Gamma)$, and so $|\sigma y| = |y|$. By varying $\sigma \in \mathrm{Gal}(L/M)$, we infer thanks to (7) that $|f(\zeta)| = 1$ for all $\zeta \in \mu_{d_s/c}$. From all this, we finally conclude $d_s/c \in \mathcal{S}_n$. By Theorem 4.3, we get $d_s/c \le 4^n n^2$, i.e., $d_s \le 4^N N^2 C$, which ends the proof of the proposition. ∎

Proof of Theorem 1.9 By Proposition 5.2, small points of $l_N(\Gamma)\cap U(\Gamma)$ lie in $K_\Gamma(\mathcal{F}^{1/m})^*.\Gamma_{\mathrm{div}}$ for some $m \in \mathbb{N}$. Theorem 1.9 follows by applying Lemma 1.5 to $F = K_\Gamma(\mathcal{F}^{1/m})$. ∎

Remark 5.3 Lemma 1.5 is quantitative by Remark 1.6. Moreover, the proof of Proposition 5.2 shows that we can take $m = (4^N N^2 C)!$. Finally, C is explicit by Remark 2.3. This proves that Theorem 1.9 can be made quantitative.

6 Equidistribution

As stated in the introduction, we will use equidistribution arguments to prove Theorem 1.7, and especially Corollary 6.2. This section is therefore devoted to the proof of this corollary.

In this section, $M \in \mathbb{N}$ denotes a positive integer. The Weil height can extend to $\overline{\mathbb{Q}}^M$, see [8, Section 1.5]; call it h again. We have $h(\boldsymbol{\zeta}) = 0$ for all $\boldsymbol{\zeta} \in \mu_\infty^M$.

We say that a sequence (μ_n) of probability measures on $S = (\mathbb{C}^*)^M$ weakly converges to μ, denoted by $\mu_n \xrightarrow{w} \mu$, if $\int_S f d\mu_n \to \int_S f d\mu$ for any bounded continuous function $f : S \to \mathbb{R}$. For a finite set $F \subset S$, the discrete probability measure on S associated with it is given by

$$\mu_F = \frac{1}{\#F}\sum_{\alpha\in F}\delta_\alpha,$$

where δ_α is the Dirac measure on S supported on α.

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

Write ν_M for the uniform probability measure on S supported at the unit polycircle $|z_1| = \cdots = |z_M| = 1$, where it coincides with the normalized Haar measure.

Finally, we say that a sequence (P_n) of $(\overline{\mathbb{Q}}^*)^M$ is strict if any proper algebraic subgroup of $(\overline{\mathbb{Q}}^*)^M$ contains P_n for only finitely many n. When $M = 1$, it is equivalent to saying that $[\mathbb{Q}(P_n) : \mathbb{Q}] \to +\infty$ (see [20, Lemma 5.2.1]).

The arguments presented by Bilu in [6] are quite general and can easily be adapted to produce other equidistribution results. We see an example of this below.

Proposition 6.1 *Let $(\zeta_{m_n}^{k_{1,n}}, \dots, \zeta_{m_n}^{k_{M,n}})$ be a strict sequence with $m_n \in \mathbb{N}$ and $k_{1,n}, \dots, k_{M,n} \in \mathbb{Z}$ for all n. Then $\mu_{E_n} \xrightarrow{w} \nu_M$, where*

$$E_n = \{(\zeta_{m_n}^{sk_{1,n}}, \dots, \zeta_{m_n}^{sk_{M,n}}), s = 1, \dots, m_n\}.$$

Proof First of all, we alert the reader on the fact that the hypothesis "F_n are pairwise distinct" made in [10, Théorème 2] can be weakened in $\#F_n \to +\infty$, the former assumption being only used to get the latter one (see [10, Sous-section 5.4]).

Let $\mathbf{n} = (n_1, \dots, n_M) \in \mathbb{Z}^M \backslash \{(0, \dots, 0)\}$, and set $\chi_{\mathbf{n}} : S \to \mathbb{C}$ to be the function defined by $\chi_{\mathbf{n}}(z_1, \dots, z_M) = \prod_{i=1}^M z_i^{n_i}$. We clearly have

$$\chi_{\mathbf{n}}(E_n) = \left\{\zeta_{m_n}^{s\sum_{i=1}^M n_i k_{i,n}}, s = 1, \dots, m_n\right\}.$$

The sequence $(\zeta_{m_n}^{\sum_{i=1}^M n_i k_{i,n}})$ is strict since $((\zeta_{m_n}^{k_{1,n}}, \dots, \zeta_{m_n}^{k_{M,n}}))$ is by hypothesis. Thus

$$\#\chi_{\mathbf{n}}(E_n) \geq \left[\mathbb{Q}\left(\zeta_{m_n}^{\sum_{i=1}^M n_i k_{i,n}}\right) : \mathbb{Q}\right] \to +\infty.$$

Thanks to [10, Théorème 2], we get $\mu_{\chi_{\mathbf{n}}(E_n)} \xrightarrow{w} \nu_1$. From this observation, and following the lines of the proof of [6, Proposition 4.1], we conclude that [6, Proposition 4.1] also holds for the sequence (μ_{E_n}).

For $z = (z_1, \dots, z_M) \in S$, put $|z|_\infty = \max\{|z_1|, \dots, |z_M|\}$. Let $\varepsilon > 0$ and write

$$K_\varepsilon = \{z \in S,\ \max\{|z|_\infty, |z|_\infty^{-1}\} \leq e^{2/\varepsilon}\}.$$

Let A be the family of sets $E \subset (\overline{\mathbb{Q}}^*)^M$ that are finite, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant and such that $h(\boldsymbol{\beta}), h(\boldsymbol{\beta}^{-1}) \leq 1$ for all $\boldsymbol{\beta} \in E$. We clearly have $E_n \in A$ for all n.

Choose $E \in A$. As E is both finite and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, we can decompose it as a finite disjoint union of Galois orbits $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).\boldsymbol{\beta}_1, \dots, \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).\boldsymbol{\beta}_k$ for some $\boldsymbol{\beta}_1, \dots, \boldsymbol{\beta}_k \in E$. For each $i \in \{1, \dots, k\}$, Bilu proved in [6, Section 4] that $\sigma\boldsymbol{\beta}_i \notin K_\varepsilon$ for at most $\varepsilon[\mathbb{Q}(\boldsymbol{\beta}_i) : \mathbb{Q}]$ field embeddings $\sigma : \mathbb{Q}(\boldsymbol{\beta}_i) \to \mathbb{C}$. Thus, $E \backslash K_\varepsilon$ has at most $\varepsilon \sum_{i=1}^k [\mathbb{Q}(\boldsymbol{\beta}_i) : \mathbb{Q}] = \varepsilon \# E$ elements, i.e., $\mu_E(K_\varepsilon) \geq 1 - \varepsilon$. It remains to mimic the proof of [6, Theorem 1.1] made in [6, Section 4] to deduce the proposition. ∎

For ζ, ζ' belonging to the unit circle in $\mathbb{C}$, we denote by $[\zeta, \zeta']$ the arc of this unit circle connecting ζ and ζ' anticlockwise.

Corollary 6.2 *Let $(\zeta_{m_n}^{k_{1,n}}, \dots, \zeta_{m_n}^{k_{M,n}})$ be a strict sequence, with $m_n \in \mathbb{N}$ and $k_{1,n}, \dots, k_{M,n} \in \mathbb{Z}$ for all n. Let $\varepsilon > 0$, and let $x_1, \dots, x_M \in [0; 2\pi]$. Write $V = \prod_{j=1}^M [e^{\zeta_4(x_j - \varepsilon)}; e^{\zeta_4(x_j + \varepsilon)}]$ and denote by $\mathcal{K}_n(V)$, the set of $r \in \mathbb{Z}/m_n\mathbb{Z}$ such*

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

that $(\zeta_{m_n}^{rk_{1,n}}, \ldots, \zeta_{m_n}^{rk_{M,n}}) \in V$. *Then, for all n large enough, we have*

$$\frac{\#\mathcal{K}_n(V)}{m_n} \geq (1-\varepsilon)\left(\frac{\varepsilon}{2\pi}\right)^M.$$

Proof Let $f : \mathbb{C}^M \to [0;1]$ be any continuous function that is identically zero outside V and taking the value 1 on

$$W = \prod_{j=1}^{M}[e^{\zeta_4(x_j-\varepsilon/2)}; e^{\zeta_4(x_j+\varepsilon/2)}] \subsetneq V.$$

Let $n \in \mathbb{N}$. For $r \in \mathbb{Z}$, we set

$$P_{r,n} = \left(\zeta_{m_n}^{rk_{1,n}}, \ldots, \zeta_{m_n}^{rk_{M,n}}\right) \text{ and } E_n = \{P_{r,n}, r = 1, \ldots, m_n\}.$$

Let r_n be the smallest divisor of m_n such that $r_n k_{j,n} \equiv 0 \ (m_n)$ for all $j \in \{1, \ldots, M\}$. Thanks to the equality $P_{r+r_n,n} = P_{r,n}$, valid for all $r \in \mathbb{Z}$, we infer that $E_n = \{P_{r,n}, r = 1, \ldots, r_n\}$. Furthermore, the minimality of r_n gives $\#E_n = r_n$. Thus

$$\frac{1}{m_n}\sum_{r=1}^{m_n}\delta_{P_{r,n}} = \frac{1}{r_n}\sum_{r=1}^{r_n}\delta_{P_{r,n}} = \mu_{E_n}.$$

Combining this equality with Proposition 6.1 provides the limit

$$u_n = \frac{1}{m_n}\sum_{r=1}^{m_n} f(P_{r,n}) = \frac{1}{\#E_n}\sum_{\alpha\in E_n} f(\alpha) \to \int f d\nu_M,$$

since the sequence $(P_{1,n})$ is strict by assumption. Thus, $u_n \geq (1-\varepsilon)\int f d\nu_M$ for all n large enough. The lemma follows by noticing that the construction of f implies the inequalities $u_n \leq \frac{1}{m_n}\#\mathcal{K}_n(V)$ and $\int f d\nu_M \geq \nu_M(W) = (\varepsilon/2\pi)^M$. ■

7 A crucial subsequence

To prove our Theorem 1.7, we need to extract from (x_n) a "good" subsequence whose construction is the aim of this section.

Recall that we fixed an integer $N \in \mathbb{N}$ and a generating set $\{\alpha_1, \ldots, \alpha_b\}$ of the torsion-free part of Γ. Let (x_n) be a sequence of $l_N(\Gamma)$ (see the introduction for a definition). Each term can express as

$$x_n = \sum_{j=1}^{N} x_{j,n}\prod_{l=1}^{b}\alpha_l^{k_{j,l,n}/m_n}$$

with $x_{j,n} \in K_\Gamma = \mathbb{Q}(\mu_\infty, \Gamma)$, $m_n \in \mathbb{N}$ and $k_{j,l,n} \in \mathbb{Z}$.

By convention, a sum indexed by the empty set is always 0.

Lemma 7.1 *There exists a subsequence* $(x_{\psi(n)})$ *of* (x_n) *satisfying the following: for all* $l \in \{1, \ldots, b\}$, *there is a set* $J_l \subset \{1, \ldots, N\}$ *such that:*

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

(a) *the sequence of terms* $(\zeta_{m_{\psi(n)}}^{k_{j,l,\psi(n)}})_{j\in J_l}$ *is strict unless* J_l *is empty;*

(b) *for all* $j \in \{1,\ldots,N\}$*, there are an integer* $\lambda^{(j,l)} \in \mathbb{Z}\backslash\{0\}$ *and a tuple* $(\lambda_m^{(j,l)})_{m\in J_l} \in \mathbb{Z}^{\# J_l}$ *such that for all n,*

$$\lambda^{(j,l)} k_{j,l,\psi(n)} + \sum_{m\in J_l} \lambda_m^{(j,l)} k_{m,l,\psi(n)} \equiv 0 \ (m_{\psi(n)}).$$

Proof We compare the elements in $\mathbb{R}^2$ with the lexicographic order $\leq$.

Construct recursively sets $J_{l,t} \subset \{1,\ldots,N\}$ and functions $\psi_{l,t} : \mathbb{N} \to \mathbb{N}$, where (l,t) ranges over all elements of $I = \{1,\ldots,b\} \times \{0,\ldots,N\}$, as follows: If $t = 0$, then $J_{l,0}$ is empty and $\psi_{l,0}$ is either the identity if $l = 1$ or $\psi_{l-1,N}$ if $l > 1$. Assume that $t \geq 1$. If the sequence of terms $\left(\zeta_{m_{\psi_{l,t-1}(n)}}^{k_{j,l,\psi_{l,t-1}(n)}}\right)_{j\in J_{l,t-1}\cup\{t\}}$ is strict, then we put $J_{l,t} = J_{l,t-1} \cup \{t\}$ and $\psi_{l,t} = \psi_{l,t-1}$. If not, then put $J_{l,t} = J_{l,t-1}$. By definition of a strict sequence, there are a proper algebraic subgroup $T_{l,t}$ of $\overline{\mathbb{Q}}^*$ and a subsequence $(x_{\psi_{l,t}(n)})$ of $(x_{\psi_{l,t-1}(n)})$ such that $u_{l,t,n} = \left(\zeta_{m_{\psi_{l,t}(n)}}^{k_{j,l,\psi_{l,t}(n)}}\right)_{j\in J_{l,t}\cup\{t\}} \in T_{l,t}$ for all n.

From this construction, we easily check by induction that for all $(l,t) \in I$, either $J_{l,t}$ is empty or the sequence of terms $v_{l,t,n} = \left(\zeta_{m_{\psi_{l,t}(n)}}^{k_{j,l,\psi_{l,t}(n)}}\right)_{j\in J_{l,t}}$ is strict.

Let $(i,j) \in I$. Note that $(x_{\psi_{l,t'}(n)})$ is a subsequence of $(x_{\psi_{l,t}(n)})$ if $t' \geq t$. As $\psi_{l,0} = \psi_{l-1,N}$ if $l > 1$, an easy induction proves that $(x_{\psi_{l',t'}(n)})$ is a subsequence of $(x_{\psi_{l,t}(n)})$ for all $(l',t') \geq (l,t)$. In particular, $(x_{\psi_{b,N}(n)})$ is a subsequence of $(x_{\psi_{l,t}(n)})$.

Let $l \in \{1,\ldots,b\}$ and show that the lemma holds with $J_l = J_{l,N}$ and $\psi = \psi_{b,N}$.

(a): By the foregoing, either J_l is empty or $(v_{l,N,n})$ is strict. Item (a) follows since $(x_{\psi(n)})$ is a subsequence of $(x_{\psi_{l,N}(n)})$.

(b): If $j \in J_l$, then we get (b) by taking $\lambda^{(j,l)} = 1$, $\lambda_j^{(j,l)} = -1$ and $\lambda_m^{(j,l)} = 0$ if $m \neq j$. If $j \notin J_l$, then $j \notin J_{l,j}$ since $J_{l,j} \subset J_l$. By construction of $J_{l,j}$, it means that $u_{l,j,n} \in T_{l,j}$ for all n. Consequently, [17, Chapter 3, §3, Theorem 5] says us that there exists a tuple $\boldsymbol{\lambda} = (\lambda_m^{(j,l)})_{m\in J_{l,j}\cup\{j\}} \in \mathbb{Z}^{1+\# J_{l,j}}\backslash\{(0,\ldots,0)\}$ such that for all n,

$$\lambda_j^{(j,l)} k_{j,l,\psi_{l,j}(n)} + \sum_{m\in J_{l,j}} \lambda_m^{(j,l)} k_{m,l,\psi_{l,j}(n)} \equiv 0 \ (m_{\psi_{l,j}(n)}). \tag{8}$$

To get (b), it remains to prove that $\lambda_j^{(j,l)} \neq 0$, which is clear if $J_{l,j}$ is empty since $\boldsymbol{\lambda} \neq 0$. If not, then the sequence $(v_{l,j,n})$ is strict. In particular, $v_{l,j,n} \in T_{l,j}$ for only finitely many n. Once again, [17, Chapter 3, §3, Theorem 5] tells us that the congruence $\sum_{m\in J_{l,j}} \lambda_m^{(j,l)} k_{m,l,\psi_{l,j}(n)} \equiv 0 \ (m_{\psi_{l,j}(n)})$ holds for only finitely many n, and (8) proves that $\lambda_j^{(j,l)} \neq 0$. This completes the proof. ∎

Put $O = (0,0)$. For a point $P \in \mathbb{R}^2$ with affix z, we set $\vec{z} = \overrightarrow{OP}$. Next define $(\vec{z_1}, \vec{z_2})$ to be the angle formed by nonzero vectors $\vec{z_1}$ and $\vec{z_2}$. If $z_1 = 0$ or $z_2 = 0$, we write $(\vec{z_1}, \vec{z_2}) = 0$. We can now construct our sequence $(x_{\Phi(n)})$.

Lemma 7.2 *We keep the notation of Lemma 7.1. Put* $\theta = \prod_{j=1}^N \prod_{l=1}^b |\lambda^{(j,l)}| \in \mathbb{N}$, $\Lambda_m^{(j,l)} = -\theta\lambda_m^{(j,l)}/\lambda^{(j,l)} \in \mathbb{Z}$ *and* $K_{j,l,\psi(n)} = \sum_{m\in J_l} \Lambda_m^{(j,l)} k_{m,l,\psi(n)}$*. Then there exist a* *subsequence* $(x_{\Phi(n)})$ *of* $(x_{\psi(n)})$ *and a subset* $I \subset \{1,\ldots,N\}$ *such that:*

(a) *for all n, we have*

$$x_{\Phi(n)} = \sum_{j\in I} a_{j,\Phi(n)} \prod_{l=1}^{b} \alpha_l^{K_{j,l,\Phi(n)}/(\theta m_{\Phi(n)})} = \sum_{j\in I} z_{j,\Phi(n)},$$

where $a_{j,\Phi(n)} \in K_\Gamma(\mathcal{F}^{1/\theta})$ *and* $z_{j,\Phi(n)} = a_{j,\Phi(n)} \prod_{l=1}^{b} \alpha_l^{K_{j,l,\Phi(n)}/(\theta m_{\Phi(n)})}$*;*

(b) *the tuples* $(K_{j,1,\Phi(n)},\ldots,K_{j,b,\Phi(n)})$ *are pairwise distinct when j ranges over all elements of I;*

(c) *the sequence* $(((\overrightarrow{z_{i,\Phi(n)}},\overrightarrow{z_{j,\Phi(n)}}))_{i,j\in I})$ *converges as* $n \to +\infty$*.*

Proof Let $l \in \{1,\ldots,b\}$, and let $j \in \{1,\ldots,N\}$. A small calculation involving Lemma 7.1(b) gives $k_{j,l,\psi(n)} = (v_{j,l,\psi(n)} m_{\psi(n)} + K_{j,l,\psi(n)})/\theta$ for some $v_{j,l,\psi(n)} \in \mathbb{Z}$. Thus

$$\begin{aligned} x_{\psi(n)} &= \sum_{j=1}^{N} x_{j,\psi(n)} \prod_{l=1}^{b} \alpha_l^{k_{j,l,\psi(n)}/m_{\psi(n)}} \\ &= \sum_{j=1}^{N} \left(x_{j,\psi(n)} \prod_{l=1}^{b} \alpha_l^{v_{j,l,\psi(n)}/\theta} \right) \prod_{l=1}^{b} \alpha_l^{K_{j,l,\psi(n)}/(\theta m_{\psi(n)})}. \end{aligned}$$

Note that $x_{j,\psi(n)} \prod_{l=1}^{b} \alpha_l^{v_{j,l,\psi(n)}/\theta} \in K_\Gamma(\mathcal{F}^{1/\theta})$. If two tuples $(K_{i,1,\psi(n)},\ldots,K_{i,b,\psi(n)})$ and $(K_{j,1,\psi(n)},\ldots,K_{j,b,\psi(n)})$ are equal, we can then group the ith and the jth term in the last sum above into a single. By repeating this process as much as possible, we construct a set $I_{\psi(n)} \subset \{1,\ldots,N\}$ such that

$$x_{\psi(n)} = \sum_{j\in I_{\psi(n)}} a_{j,\psi(n)} \prod_{l=1}^{b} \alpha_l^{K_{j,l,\psi(n)}/(\theta m_{\psi(n)})},$$

where $a_{j,\psi(n)} \in K_\Gamma(\mathcal{F}^{1/\theta})$ and the tuples $(K_{j,1,\psi(n)},\ldots,K_{j,b,\psi(n)})$ are pairwise distinct when j runs over all elements of $I_{\psi(n)}$. As $I_{\psi(n)} \subset \{1,\ldots,N\}$, there is a subsequence $(x_{\phi(n)})$ of $(x_{\psi(n)})$ for which the sequence $(I_{\phi(n)})$ is constant, say to I.

By definition, $(\overrightarrow{z_{i,\phi(n)}},\overrightarrow{z_{j,\phi(n)}}) \in [0,2\pi[$ for all $i,j \in I$ and all n. Hence, Bolzano–Weierstrass theorem ensures us the existence of a subsequence $(x_{\Phi(n)})$ of $(x_{\phi(n)})$ such that the sequence $(((\overrightarrow{z_{i,\Phi(n)}},\overrightarrow{z_{j,\Phi(n)}}))_{i,j\in I})$ converges as $n \to +\infty$. This proves (c). Finally, we directly get (a) and (b) from the construction of $I_{\Phi(n)} = I$. ■

8 Proof of Theorem 1.7

Recall that $l_N(\Gamma)$ is the set of $x \in \mathbb{Q}(\Gamma_{\text{div}})$ that can express as $x = \sum_{j=1}^{N} x_j \gamma_j$ with $x_j \in K_\Gamma = \mathbb{Q}(\mu_\infty, \Gamma)$ and $\gamma_j \in \Gamma_{\text{div}}$. Clearly, $\tau x \in l_N(\Gamma)$ for all $\tau \in \text{Gal}(\overline{\mathbb{Q}}/K_\Gamma)$ since any conjugate of γ_j over K_Γ is equal to γ_j up to root of unity.

Recall that $O_\Gamma(\alpha)$ and $d_{\Gamma,\varepsilon}(\alpha)$ have been defined in Section 1.2. Note that $d_{\Gamma,\varepsilon}(\alpha) = d_{\Gamma,\varepsilon}(\beta)$ if α and β are conjugates over K_Γ, that is if $\beta \in O_\Gamma(\alpha)$.

The goal of this section is to prove the following.

Theorem 8.1 *Let* (x_n) *be a sequence of* $l_N(\Gamma)$ *such that* $d_{\Gamma,\varepsilon}(x_n) \underset{n\to+\infty}{\longrightarrow} 1$ *for all* $\varepsilon > 0$*. Let* $(x_{\Phi(n)})$ *be the sequence constructed in Lemma 7.2 from which we keep the notation. Then:*

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

(a) $\sum_{j\in I}|z_{j,\Phi(n)}|^2 \to 1$;
(b) *there exist* $\#I-1$ *elements* $j\in I$ *such that* $z_{j,\Phi(n)}\to 0$.

Proof of Theorem 1.7 by assuming Theorem 8.1 Set $v_n = \max_{x\in O_\Gamma(y_n)}\{||x|^2-1|\}$. Let $l\in\mathbb{R}\cup\{+\infty\}$ be an accumulation point of (v_n) and show that $l=0$, which will finish the proof of our theorem. Without loss of generality, assume that $v_n\to l$.

Pick $x_n\in O_\Gamma(y_n)$ such that $v_n = ||x_n|^2-1|$. By the preamble of this section, we easily infer that $x_n\in l_N(\Gamma)$ for all n and $d_{\Gamma,\varepsilon}(x_n)=d_{\Gamma,\varepsilon}(y_n)\to 1$ for all $\varepsilon>0$. Thanks to Lemma 7.2(a), we have $x_{\Phi(n)} = \sum_{j\in I} z_{j,\Phi(n)}$. As a direct consequence of Theorem 8.1, we get $|x_{\Phi(n)}|^2\to 1$. But then $v_{\Phi(n)}\to 0$; whence $l=0$. ∎

For the rest of this section, we keep (and fix) the same notation as Theorem 8.1. In order to simplify our explanation, we assume that Φ is the identity. Set $G_n = \mathrm{Gal}(K_\Gamma(\mathcal{F}^{1/(\theta m_n)})/K_\Gamma)$ and $H_n = \mathrm{Gal}(K_\Gamma(\mathcal{F}^{1/(\theta m_n)})/K_\Gamma(\mathcal{F}^{1/\theta}))$. Lemma 2.1 applied to $m=\infty, d_1=\cdots=d_b=\theta m_n$ and $L=\mathbb{Q}(\mathcal{F}^{1/\theta})$ gives

$$H_n = \prod_{l=1}^{b}\mathbb{Z}/(m_n/c_{l,n})\mathbb{Z}, \tag{9}$$

where $c_{1,n},\dots,c_{b,n}\in\mathbb{N}$ are bounded from above by a constant depending only on Γ and θ. Next, for all $m\in\mathbb{N}$, set $. : \mathbb{R}^m\times\mathbb{R}^m\to\mathbb{R}$ to be the dot product on $\mathbb{R}^m$. Finally, put $\mathbf{K}_{j,n}=(K_{j,1,n},\dots,K_{j,b,n})$ and for any $\mathbf{r}=(r_1,\dots,r_b)\in\mathbb{R}^b$, we set

$$B_{\mathbf{r},i,j,n} = (\overrightarrow{z_{i,n}},\overrightarrow{z_{j,n}}) + \frac{2\pi\,\mathbf{rc}_n.(\mathbf{K}_{j,n}-\mathbf{K}_{i,n})}{m_n},$$

where $\mathbf{rc}_n = (r_1c_{1,n},\dots,r_bc_{b,n})$.

8.1 Proof of Theorem 8.1(a)

We will deduce the limit of Theorem 8.1(a) thanks to the following equality. Recall that $x_n\in K_\Gamma(\mathcal{F}^{1/(\theta m_n)})$ by Lemma 7.2(a).

Lemma 8.2 *Let* $n\in\mathbb{N}$, *and let* $\sigma=\mathbf{r}\in H_n$. *Then*

$$|\sigma x_n|^2 = \sum_{j\in I}|z_{j,n}|^2 + \sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|\cos\left(B_{\mathbf{r},i,j,n}\right).$$

Proof As $\sigma\in H_n$, it therefore fixes the elements of $K_\Gamma(\mathcal{F}^{1/\theta})$. Let $j\in I$. By Lemma 7.2(a), we have $z_{j,n}=a_{j,n}\prod_{l=1}^{b}\alpha_l^{K_{j,l,n}/m_n}$ with $a_{j,n}\in K_\Gamma(\mathcal{F}^{1/\theta})$. A small calculation involving (9) shows that $\sigma z_{j,n} = z_{j,n}\zeta_{m_n}^{\mathbf{rc}_n.\mathbf{K}_{j,n}}$. From Lemma 7.2$(a)$ and from the cosine rule, we get

$$\begin{aligned}|\sigma x_n|^2 &= \left|\sum_{j\in I}\sigma z_{j,n}\right|^2 = \left|\sum_{j\in I} z_{j,n}\zeta_{m_n}^{\mathbf{rc_n}.\mathbf{K}_{j,n}}\right|^2\\ &= \sum_{j\in I}|z_{j,n}|^2 + \sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|\cos\left(\left(\overrightarrow{z_{i,n}\zeta_{m_n}^{\mathbf{rc}_n.\mathbf{K}_{i,n}}},\overrightarrow{z_{j,n}\zeta_{m_n}^{\mathbf{rc}_n.\mathbf{K}_{j,n}}}\right)\right).\end{aligned}$$

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

To conclude, it remains to show the equality

$$(10)\qquad |z_{i,n}||z_{j,n}|\cos\left(\left(\overrightarrow{z_{i,n}\zeta_{m_n}^{\mathbf{r}\mathbf{c}_n.\mathbf{K}_{i,n}}}, \overrightarrow{z_{j,n}\zeta_{m_n}^{\mathbf{r}\mathbf{c}_n.\mathbf{K}_{j,n}}}\right)\right) = |z_{i,n}||z_{j,n}|\cos\left(B_{\mathbf{r},i,j,n}\right),$$

which is obvious if either $z_{i,n} = 0$ or $z_{j,n} = 0$. If these complex numbers are nonzero, then (10) arises from the chain of equalities modulo 2π below

$$(\overrightarrow{\alpha\zeta_{m_n}^{\lambda}}, \overrightarrow{\beta\zeta_{m_n}^{\eta}}) \equiv (\vec{\alpha}, \overrightarrow{\beta\zeta_{m_n}^{\eta-\lambda}}) \equiv (\vec{\alpha},\vec{\beta}) + (\vec{\beta}, \overrightarrow{\beta\zeta_{m_n}^{\eta-\lambda}}) \equiv (\vec{\alpha},\vec{\beta}) + \frac{2\pi(\eta-\lambda)}{m_n}\ (2\pi),$$

which is valid for all $\alpha, \beta \in \mathbb{C}^*$ and all $\eta, \lambda \in \mathbb{R}$. ∎

Fix from now $\varepsilon > 0$. Let F_n be the set of elements $\sigma \in G_n$ satisfying $1-\varepsilon \le |\sigma x_n|^2 \le 1+\varepsilon$. It is easy to check that $d_{\Gamma,\varepsilon}(x_n) = \#F_n/\#G_n$.

Proof of Theorem 8.1 when *I* has cardinality 1 Clearly (b) arises from (a). Let j be the unique element of I. Lemma 8.2 tells us that $|\sigma x_n|^2 = |z_{j,n}|^2$ for all $\sigma \in H_n$. The fact that $d_{\Gamma,\varepsilon}(x_n) \to 1$ by assumption and that H_n has index $[K_\Gamma(\mathcal{F}^{1/\theta}) : K_\Gamma]$ in G_n provides for all n large enough an element $\sigma_n \in H_n$ belonging to F_n. In particular, $1-\varepsilon \le |\sigma_n x_n|^2 = |z_{j,n}|^2 \le 1+\varepsilon$, and so $|z_{j,n}|^2 \to 1$ proving what we desire. ∎

We now focus on the case where I has at least two elements.

Lemma 8.2 suggests us to construct for all n large enough a "good" $\sigma_n = \mathbf{r}_n \in H_n$ for which we can estimate as precisely as possible the quantities $|\sigma_n x_n|$ and $\cos(B_{\mathbf{r}_n,i,j,n})$. Its construction is the purpose of the next proposition.

Recall that J_l is defined in Lemma 7.1. Let Y be the set of pairs (l, m) such that $l \in \{1, \dots, b\}$ and $m \in J_l$. It is a non-empty set. Indeed, otherwise J_l would be empty for all l. Lemma 7.2 then implies $K_{j,l,n} = 0$ for all j, l, n. But this is possible only if I has cardinality 1 by Lemma 7.2(b), a contradiction by the foregoing.

Recall that the integer $\Lambda_m^{(i,l)}$ is defined in Lemma 7.2. Then put

$$\gamma = \max_{i,j\in I, i\neq j}\left\{\sum_{(l,m)\in Y}\left|\Lambda_m^{(j,l)} - \Lambda_m^{(i,l)}\right|\right\} + 1.$$

Let $i, j \in I$. Write $\mathbf{\Lambda}_{i,j} = (\Lambda_m^{(j,l)} - \Lambda_m^{(i,l)})_{(l,m)\in Y}$. Recall that the sequence $((\overrightarrow{z_{i,n}}, \overrightarrow{z_{j,n}}))$ converges by Lemma 7.2(c); denote by $L_{i,j}$ its limit. Finally, for $\mathbf{x} \in \mathbb{R}^{\#Y}$, we write

$$I_{i,j}(\mathbf{x}) = \left[e^{\zeta_4(L_{i,j}+\mathbf{\Lambda}_{i,j}.\mathbf{x}-\gamma\varepsilon)}; e^{\zeta_4(L_{i,j}+\mathbf{\Lambda}_{i,j}.\mathbf{x}+\gamma\varepsilon)}\right].$$

Proposition 8.3 *Let $\mathbf{x} \in \mathbb{R}^{\#Y}$. Then, for all n large enough, there exists $\sigma_{\mathbf{x},n} = \mathbf{r}_{\mathbf{x},n} \in H_n$ such that $1-\varepsilon \le |\sigma_{\mathbf{x},n}x_n|^2 \le 1+\varepsilon$. Furthermore, for each $i, j \in I$ distinct such that $\pm 1 \notin I_{i,j}(\mathbf{x})$, we have*

$$\cos(\gamma\varepsilon)\cos(L_{i,j} + \mathbf{\Lambda}_{i,j}.\mathbf{x}) + \sin(\gamma\varepsilon) \ge \cos(B_{\mathbf{r}_{\mathbf{x},n},i,j,n}) \ge \cos(\gamma\varepsilon)\cos(L_{i,j} + \mathbf{\Lambda}_{i,j}.\mathbf{x}) - \sin(\gamma\varepsilon).$$

Proof First part: As $d_{\Gamma,\varepsilon}(x_n) \to 1$, we deduce that for all n large enough,

$$(11)\qquad d_{\Gamma,\varepsilon}(x_n) = \frac{\#F_n}{\#G_n} > 1 - \frac{(1-\varepsilon)^b}{2[K_\Gamma(\mathcal{F}^{1/\theta}) : K_\Gamma]}\left(\frac{\varepsilon}{2\pi}\right)^{\sum_{l=1}^{b}\#J_l}.$$

Put $\mathbf{x} = (x_{l,m})_{(l,m)\in Y}$. For $l \in \{1,\dots,b\}$, define $\mathcal{K}_{l,n}(\mathbf{x})$ to be the set $\mathbb{Z}/(m_n/c_{l,n})\mathbb{Z}$ if J_l is empty and the set of $r \in \mathbb{Z}/(m_n/c_{l,n})\mathbb{Z}$ such that

$$(\zeta_{m_n/c_{l,n}}^{rk_{m,l,n}})_{m\in J_l} \in \prod_{m\in J_l}[e^{\zeta_4(x_{l,m}-\varepsilon)}; e^{\zeta_4(x_{l,m}+\varepsilon)}]$$

if J_l is non-empty. We have

$$\frac{\#\mathcal{K}_{l,n}(\mathbf{x})}{m_n/c_{l,n}} \geq (1-\varepsilon)\left(\frac{\varepsilon}{2\pi}\right)^{\#J_l}$$

for all n large enough. It is clear if J_l is empty. If not, then by Lemma 7.1(a), the sequence of terms $(\zeta_{m_n}^{k_{m,l,n}})_{m\in J_l}$ is strict. As $c_{l,n}$ is bounded from above by a constant depending only on Γ and θ, we deduce that the sequence of terms $(\zeta_{m_n/c_{l,n}}^{k_{m,l,n}})_{m\in J_l}$ is also strict. The desired inequality now arises from Corollary 6.2 applied to this sequence, $M = \#J_l$ and $(x_1,\dots,x_M) = (x_{l,m})_{m\in J_l}$.

Clearly, $\prod_{l=1}^{b}\mathcal{K}_{l,n}(\mathbf{x})$ is a subset of H_n by (9). Moreover, H_n has cardinality $\prod_{l=1}^{b} m_n/c_{l,n}$ and has index $[K_\Gamma(\mathcal{F}^{1/\theta}) : K_\Gamma]$ in G_n. Thus

$$\frac{\#\prod_{l=1}^{b}\mathcal{K}_{l,n}(\mathbf{x})}{\#G_n} = \frac{1}{[K_\Gamma(\mathcal{F}^{1/\theta}) : K_\Gamma]}\prod_{l=1}^{b}\frac{\#\mathcal{K}_{l,n}(\mathbf{x})}{m_n/c_{l,n}} \geq \frac{(1-\varepsilon)^b}{[K_\Gamma(\mathcal{F}^{1/\theta}) : K_\Gamma]}\left(\frac{\varepsilon}{2\pi}\right)^{\sum_{l=1}^{b}\#J_l}$$

for all n large enough. Combining this inequality and (11) provides an element $\sigma_n = \mathbf{r} = (r_1,\dots,r_b) \in F_n \cap \prod_{l=1}^{b}\mathcal{K}_{l,n}(\mathbf{x})$. This ends the first part.

Second part: Let $i, j \in I$ be as in the statement. A small calculation gives

$$\begin{aligned}\zeta_{m_n}^{\mathbf{rc}_n.(\mathbf{K}_{j,n}-\mathbf{K}_{i,n})} &= \zeta_{m_n}^{\sum_{l=1}^{b} r_l c_{l,n}(K_{j,l,n}-K_{i,l,n})} = \zeta_{m_n}^{\sum_{l=1}^{b}\sum_{m\in J_l} r_l c_{l,n}(\Lambda_m^{(j,l)}-\Lambda_m^{(i,l)})k_{m,l,n}} \\ &= \prod_{(l,m)\in Y}(\zeta_{m_n}^{r_l c_{l,n} k_{m,l,n}})^{\Delta_m^{(i,j,l)}},\end{aligned}$$

where $\Delta_m^{(i,j,l)} = \Lambda_m^{(j,l)} - \Lambda_m^{(i,l)} \in \mathbb{Z}$. Let $(l,m) \in Y$. In particular, J_l is non-empty. Recall that $r_l \in \mathcal{K}_{l,n}(\mathbf{x})$. By definition of $\mathcal{K}_{l,n}(\mathbf{x})$, we have

$$\zeta_{m_n}^{r_l c_{l,n} k_{m,l,n}} = \zeta_{m_n/c_{l,n}}^{r_l k_{m,l,n}} \in [e^{\zeta_4(x_{l,m}-\varepsilon)}; e^{\zeta_4(x_{l,m}+\varepsilon)}]$$

for all $m \in J_l$. Thus

$$\zeta_{m_n}^{\mathbf{rc}_n.(\mathbf{K}_{j,n}-\mathbf{K}_{i,n})} \in \left[\prod_{(l,m)\in Y} e^{\zeta_4\left(\Delta_m^{(i,j,l)}x_{l,m}-\varepsilon\left|\Delta_m^{(i,j,l)}\right|\right)}; \prod_{(l,m)\in Y} e^{\zeta_4\left(\Delta_m^{(i,j,l)}x_{l,m}+\varepsilon\left|\Delta_m^{(i,j,l)}\right|\right)}\right].$$

We clearly have

$$\sum_{(l,m)\in Y}\Delta_m^{(i,j,l)}x_{l,m} = \sum_{(l,m)\in Y}(\Lambda_m^{(j,l)} - \Lambda_m^{(i,l)})x_{l,m} = \mathbf{\Lambda}_{i,j}.\mathbf{x},$$

and we finally conclude from the definition of γ that

$$\zeta_{m_n}^{\mathbf{rc}_n.(\mathbf{K}_{j,n}-\mathbf{K}_{i,n})} \in [e^{\zeta_4(\mathbf{\Lambda}_{i,j}.\mathbf{x}-(\gamma-1)\varepsilon)}; e^{\zeta_4(\mathbf{\Lambda}_{i,j}.\mathbf{x}+(\gamma-1)\varepsilon)}].$$

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

On the other hand, $e^{\zeta_4(\overrightarrow{z_{i,n}},\overrightarrow{z_{j,n}})} \in [e^{\zeta_4(L_{i,j}-\varepsilon)}, e^{\zeta_4(L_{i,j}+\varepsilon)}]$ for all n large enough since $(\overrightarrow{z_{i,n}},\overrightarrow{z_{j,n}}) \to L_{i,j}$. From all this, we conclude that for all n large enough,

$$e^{\zeta_4 B_{\mathbf{r},i,j,n}} = e^{\zeta_4(\overrightarrow{z_{i,n}},\overrightarrow{z_{j,n}})} \zeta_{m_n}^{\mathbf{rc}_n.(\mathbf{K}_{j,n}-\mathbf{K}_{i,n})} \in I_{i,j}(\mathbf{x}).$$

By assumption, $\pm 1 \notin I_{i,j}(\mathbf{x})$. The real part function is therefore monotone on $I_{i,j}(\mathbf{x})$. In particular, it reaches its extrema to the two endpoints of $I_{i,j}(\mathbf{x})$. If it is decreasing, then

$$\cos(L_{i,j} + \mathbf{\Lambda}_{i,j}.\mathbf{x} - \gamma\varepsilon) \geq \cos(B_{\mathbf{r},i,j,n}) \geq \cos(L_{i,j} + \mathbf{\Lambda}_{i,j}.\mathbf{x} + \gamma\varepsilon).$$

We deduce the desired inequality thanks to the relations $\cos(x-y) = \cos(x)\cos(y) + \sin(x)\sin(y)$, $\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$, and $|\sin(x)| \leq 1$. The increasing case is similar, which proves the second part of the statement. ∎

The key to get Theorem 8.1(a) is to apply the previous proposition to a finite number of well-chosen $\mathbf{x}$. But before constructing them, we need some preliminary results.

Lemma 8.4 *Let $i, j \in I$ be distinct. Then $\mathbf{\Lambda}_{i,j}$ is nonzero.*

Proof If $\mathbf{\Lambda}_{i,j}$ is zero, then $\Lambda_m^{(j,l)} = \Lambda_m^{(i,l)}$ for all $(l,m) \in Y$, i.e., for all $l \in \{1,\dots,b\}$ and all $m \in J_l$. But then, Lemma 7.2 implies $K_{i,l,n} = K_{j,l,n}$ for all $l \in \{1,\dots,b\}$ and all n, i.e., $(K_{i,1,n},\dots,K_{i,b,n}) = (K_{j,1,n},\dots,K_{j,b,n})$ for all n. This is possible only if $i = j$ according to Lemma 7.2(b), a contradiction. The lemma follows. ∎

We can thus fix an integer $d \in \mathbb{N}$ such that for all $i, j \in I$ distinct, d does not divide at least one of the coordinates of $\mathbf{\Lambda}_{i,j}$. Put

$$Z = \{0; 2\pi/d; \dots; 2\pi(d-1)/d\}^{\#Y}.$$

Lemma 8.5 *Let $i, j \in I$ be distinct. Then $\sum_{\mathbf{z}\in Z} e^{\zeta_4 \mathbf{\Lambda}_{i,j}.\mathbf{z}} = 0$.*

Proof For brevity, write $\mathbf{\Lambda}_{i,j} = (\lambda_1,\dots,\lambda_{\#Y})$. Thus

$$\sum_{\mathbf{z}\in Z} e^{\zeta_4 \mathbf{\Lambda}_{i,j}.\mathbf{z}} = \sum_{0\leq k_1,\dots,k_{\#Y}\leq d-1} e^{\zeta_4 \sum_{t=1}^{\#Y} \lambda_t 2\pi k_t/d} = \sum_{0\leq k_1,\dots,k_{\#Y}\leq d-1} \zeta_d^{\sum_{t=1}^{\#Y}\lambda_t k_t}.$$

By definition of d, there is $u \in \{1,\dots,\#Y\}$ such that d does not divide λ_u. So

$$\sum_{\mathbf{z}\in Z} e^{\zeta_4 \mathbf{\Lambda}_{i,j}.\mathbf{z}} = \sum_{0\leq k_1,\dots,k_{u-1},k_{u+1},\dots,k_{\#Y}\leq d-1} \zeta_d^{\sum_{t=1, t\neq u}^{\#Y}\lambda_t k_t} \sum_{k_u=0}^{d-1} \zeta_d^{\lambda_u k_u}.$$

Finally, $\sum_{k=0}^{d-1} \zeta_d^{\lambda_u k} = 0$ since d does not divide λ_u. The lemma follows. ∎

We would like to apply Proposition 8.3 for all $\mathbf{x} \in Z$. However, there is no guarantee that the condition $\pm 1 \notin I_{i,j}(\mathbf{x})$ holds for all $i, j \in I$ distinct and all $\mathbf{x} \in Z$. We see below how to circumvent this difficulty.

We define $\mathcal{H}$ to be the set of $\mathbf{X} \in [0; 2\pi]^{\#Y}$ satisfying

$$\exists t \in \mathbb{Z}, \exists i \neq j \in I, \exists \mathbf{z} \in Z \text{ such that } L_{i,j} + \mathbf{\Lambda}_{i,j}.(\mathbf{X} + \mathbf{z}) - t\pi = 0.$$

As $\mathbf{\Lambda}_{i,j}$ is nonzero for all $i, j \in I$ distinct, we infer that $\mathcal{H}$ lies in a finite union of hyperplanes in $\mathbb{R}^{\#Y}$ (the equation above having no solution if $|t|$ is large enough

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

since the quantity $\mathbf{X}$ is bounded). Hence, there exists a simply-connected compact $K \subset [0; 2\pi]^{\#Y}$ such that $K \cap \mathcal{H}$ is empty. The distance δ from K to $\mathcal{H}$ is a positive real since both K and $\mathcal{H}$ are compact. For $\mathbf{x}_0 \in K$, the distance from $\mathbf{x}_0$ to $\mathcal{H}$ is

$$\min_{t\in\mathbb{Z}, i\neq j\in I, \mathbf{z}\in Z} \left\{ \frac{|L_{i,j} + \boldsymbol{\Lambda}_{i,j}.(\mathbf{x}_0 + \mathbf{z}) - t\pi|}{\sqrt{\boldsymbol{\Lambda}_{i,j}.\boldsymbol{\Lambda}_{i,j}}} \right\} \geq \delta.$$

As $\boldsymbol{\Lambda}_{i,j} \in \mathbb{Z}^{\#Y}$ is nonzero, we conclude $\sqrt{\boldsymbol{\Lambda}_{i,j}.\boldsymbol{\Lambda}_{i,j}} \geq 1$, and so

$$|L_{i,j} + \boldsymbol{\Lambda}_{i,j}.\mathbf{x} - t\pi| \geq \delta$$

for all $t \in \mathbb{Z}$, all $i, j \in I$ distinct and all $\mathbf{x} \in K + Z = \{\mathbf{X} + \mathbf{z}, \mathbf{X} \in K, \mathbf{z} \in Z\}$.

Recall that ε is as small as possible. So we can take it such that $\gamma\varepsilon < \delta$. Thus

$$t\pi \notin [L_{i,j} + \boldsymbol{\Lambda}_{i,j}.\mathbf{x} - \gamma\varepsilon; L_{i,j} + \boldsymbol{\Lambda}_{i,j}.\mathbf{x} + \gamma\varepsilon]$$

for all $t \in \mathbb{Z}$, all $i, j \in I$ distinct and all $\mathbf{x} \in K + Z$. In conclusion, $\pm 1 \notin I_{i,j}(\mathbf{x})$ for all $i, j \in I$ distinct and all $\mathbf{x} \in K + Z$.

Here is the last calculation before starting the proof of Theorem 8.1(a).

Lemma 8.6 *Let $\eta, x_j \in \mathbb{C}$ be complex numbers with $j \in I$. Then*

$$\sum_{j\in I} x_j^2 + \eta \sum_{i,j\in I, i\neq j} x_i x_j = -\frac{\eta}{2} \sum_{i,j\in I, i\neq j} (x_i - x_j)^2 + (1 + \eta(\#I - 1)) \sum_{j\in I} x_j^2.$$

Proof For brevity, put $\eta_1 = -\eta/2$ and $\eta_2 = 1 + \eta(\#I - 1)$. Then

$$\begin{aligned} \eta_1 \sum_{i,j\in I, i\neq j} (x_i - x_j)^2 + \eta_2 \sum_{j\in I} x_j^2 &= \eta_1 \sum_{i,j\in I, i\neq j} (x_i^2 + x_j^2 - 2x_i x_j) + \eta_2 \sum_{j\in I} x_j^2 \\ &= 2(\#I - 1)\eta_1 \sum_{i\in I} x_i^2 - 2\eta_1 \sum_{i,j\in I, i\neq j} x_i x_j + \eta_2 \sum_{j\in I} x_j^2 \\ &= (\eta_2 + 2(\#I - 1)\eta_1) \sum_{j\in I} x_j^2 - 2\eta_1 \sum_{i,j\in I, i\neq j} x_i x_j, \end{aligned}$$

and the lemma follows since $-2\eta_1 = \eta$ and $\eta_2 + 2(\#I - 1)\eta_1 = 1$. ■

Proof of Theorem 8.1(a) Let $\mathbf{y} \in K$. Recall that $\pm 1 \notin I_{i,j}(\mathbf{x})$ for all $i, j \in I$ distinct and all $\mathbf{x} \in \mathbf{y} + Z$. The set $\mathbf{y} + Z$ being finite, we infer that for all n large enough, Proposition 8.3 holds for all elements $\mathbf{x} \in \mathbf{y} + Z$. Choose such a n.

Lemma 8.5 easily implies $\sum_{\mathbf{x}\in\mathbf{y}+Z} \cos(L_{i,j} + \Lambda_{i.j}.\mathbf{x}) = 0$ for all $i, j \in I$ distinct. Summing over $\mathbf{y} + Z$ the chain of inequalities in Proposition 8.3 leads to

$$\sin(\gamma\varepsilon)\#Z \geq \sum_{\mathbf{x}\in\mathbf{y}+Z} \cos(B_{\mathbf{r}_{\mathbf{x},n},i,j,n}) \geq -\sin(\gamma\varepsilon)\#Z.$$

Proposition 8.3 gives $1 + \varepsilon \geq |\sigma_{\mathbf{x},n} x_n|^2 \geq 1 - \varepsilon$ for all $\mathbf{x} \in \mathbf{y} + Z$. By Lemma 8.2,

$$1 + \varepsilon \geq \sum_{j\in I} |z_{j,n}|^2 + \sum_{i,j\in I, i\neq j} |z_{i,n}||z_{j,n}| \cos(B_{\mathbf{r}_{\mathbf{x},n},i,j,n}) \geq 1 - \varepsilon.$$

By summing these inequalities over $\mathbf{y} + Z$, we conclude

$$(1 + \varepsilon)\#Z \geq \#Z \sum_{j\in I} |z_{j,n}|^2 - \sin(\gamma\varepsilon)\#Z \sum_{i,j\in I, i\neq j} |z_{i,n}||z_{j,n}|$$

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

and

$$\#Z\sum_{j\in I}|z_{j,n}|^2+\sin(\gamma\varepsilon)\#Z\sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|\geq(1-\varepsilon)\#Z.$$

Finally, Lemma 8.6 applied to $x_j=|z_{j,n}|$ and $\eta=\pm\sin(\gamma\varepsilon)$ gives us

$$\begin{aligned}1+\varepsilon &\geq \frac{\sin(\gamma\varepsilon)}{2}\sum_{i,j\in I,i\neq j}(|z_{i,n}|-|z_{j,n}|)^2+(1-(\#I-1)\sin(\gamma\varepsilon))\sum_{j\in I}|z_{j,n}|^2\\ &\geq(1-(\#I-1)\sin(\gamma\varepsilon))\sum_{j\in I}|z_{j,n}|^2\end{aligned}$$

and

$$\begin{aligned}1-\varepsilon &\leq -\frac{\sin(\gamma\varepsilon)}{2}\sum_{i,j\in I,i\neq j}(|z_{i,n}|-|z_{j,n}|)^2+(1+(\#I-1)\sin(\gamma\varepsilon))\sum_{j\in I}|z_{j,n}|^2\\ &\leq(1+(\#I-1)\sin(\gamma\varepsilon))\sum_{j\in I}|z_{j,n}|^2.\end{aligned}$$

In conclusion, for all n large enough, we have

$$\frac{1-\varepsilon}{1+(\#I-1)\sin(\gamma\varepsilon)}\leq\sum_{j\in I}|z_{j,n}|^2\leq\frac{1+\varepsilon}{1-(\#I-1)\sin(\gamma\varepsilon)},$$

i.e., $\sum_{j\in I}|z_{j,n}|^2\to 1$, which proves Theorem 8.1(a). ∎

8.2 Proof of Theorem 8.1(b)

Recall that $\pm1\notin I_{i,j}(\mathbf{x})$ for all $i,j\in I$ distinct and all $\mathbf{x}\in K\subset K+Z$. We can now show the pointwise limit below.

Lemma 8.7 *Pick $\mathbf{x}\in K$. Then $\sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|\cos\left(L_{i,j}+\boldsymbol{\Lambda}_{i,j}.\mathbf{x}\right)\to 0$.*

Proof Thanks to Theorem 8.1(a), we have $1-\varepsilon\leq\sum_{j\in I}|z_{j,n}|^2\leq 1+\varepsilon$ for all n large enough. Furthermore, for all n large enough, there is $\sigma_{\mathbf{x},n}\in H_n$ as in Proposition 8.3. Choose n large enough so that the facts above hold.

Using the triangle inequality, then Proposition 8.3, we get

$$\left|\sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|\left(\cos(B_{\mathbf{r}_{\mathbf{x},\mathbf{n}},i,j,n})-\cos(\gamma\varepsilon)\cos\left(L_{i,j}+\boldsymbol{\Lambda}_{i,j}.\mathbf{x}\right)\right)\right|\leq \sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|\sin(\gamma\varepsilon)\leq\gamma\varepsilon\sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|. \tag{12}$$

We also have $1-\varepsilon\leq|\sigma_{\mathbf{x},n}x_n|^2\leq 1+\varepsilon$ by Proposition 8.3. Recall that we have the chain of inequalities $1-\varepsilon\leq\sum_{j\in I}|z_{j,n}|^2\leq 1+\varepsilon$. Thanks to Lemma 8.2, we obtain

$$\left|\sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|\cos(B_{\mathbf{r}_{\mathbf{x},n},i,j,n})\right|\leq 2\varepsilon. \tag{13}$$

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

Applying the reverse triangle inequality to (12), it follows from (13) that

$$\cos(\gamma\varepsilon)\left|\sum_{i,j\in I, i\neq j}|z_{i,n}||z_{j,n}|\cos\left(L_{i,j}+\mathbf{\Lambda}_{i,j}.\mathbf{x}\right)\right|\leq\varepsilon\left(\gamma\sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|+2\right).$$

As $|z_{j,n}|^2\leq 1+\varepsilon$ for all $j\in I$, we finally conclude that for all n large enough,

$$\left|\sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|\cos\left(L_{i,j}+\mathbf{\Lambda}_{i,j}.\mathbf{x}\right)\right|\leq\frac{\varepsilon}{\cos(\gamma\varepsilon)}(2+\gamma(1+\varepsilon)(\#I)^2),$$

which ends the proof of the lemma. ∎

Let $\{\mathbf{c}_1,\ldots,\mathbf{c}_M\}=\{\mathbf{\Lambda}_{i,j}, i,j\in I, i\neq j\}$ be with $\mathbf{c}_1,\ldots,\mathbf{c}_M$ pairwise distinct. For $k\in\{1,\ldots,M\}$, put E_k the set of $i,j\in I$ distinct such that $\mathbf{c}_k=\mathbf{\Lambda}_{i,j}$. Clearly, $E_1,\ldots,E_k$ is a partition of $I^2\backslash\bigsqcup_{l\in I}(l,l)$.

We now state a much more precise result than Lemma 8.7.

Lemma 8.8 *We have* $\sum_{(i,j)\in E_k}|z_{i,n}||z_{j,n}|e^{\zeta_4 L_{i,j}}\to 0$ *for all* $k\in\{1,\ldots,M\}$.

Proof Write

$$C_{k,n}=\sum_{(i,j)\in E_k}|z_{i,n}||z_{j,n}|\cos(L_{i,j})\quad\text{and}\quad S_{k,n}=-\sum_{(i,j)\in E_k}|z_{i,n}||z_{j,n}|\sin(L_{i,j}).$$

The sequence of terms $(C_{k,n},S_{k,n})_{k=1}^M$ has an accumulation point in $\mathbb{R}^{2M}$ since it is bounded by Theorem 8.1(a). Let $(C_k,S_k)_{k=1}^M$ be such a point. To show our lemma, it is sufficient to get $C_k=S_k=0$ for all $k\in\{1,\ldots,M\}$. Without loss of generality, assume that $(C_{k,n},S_{k,n})_{k=1}^M\to(C_k,S_k)_{k=1}^M$.

Let $\mathbf{x}\in K$. A short calculation gives

$$\begin{aligned}\sum_{i,j\in I,i\neq j}|z_{i,n}||z_{j,n}|\cos\left(L_{i,j}+\mathbf{\Lambda}_{i,j}.\mathbf{x}\right)&=\sum_{k=1}^M\sum_{(i,j)\in E_k}|z_{i,n}||z_{j,n}|\cos\left(L_{i,j}+\mathbf{c}_k.\mathbf{x}\right)\\&=\sum_{k=1}^M C_{k,n}\cos\left(\mathbf{c}_k.\mathbf{x}\right)+S_{k,n}\sin\left(\mathbf{c}_k.\mathbf{x}\right).\end{aligned}$$

We deduce from Lemma 8.7 that $\sum_{k=1}^M C_{k,n}\cos(\mathbf{c}_k.\mathbf{x})+S_{k,n}\sin(\mathbf{c}_k.\mathbf{x})\to 0$ and the uniqueness of the limit gives

$$\sum_{k=1}^M C_k\cos\left(\mathbf{c}_k.\mathbf{x}\right)+S_k\sin\left(\mathbf{c}_k.\mathbf{x}\right)=0.$$

As K is a simply-connected compact, the Monodromy Theorem claims that this equality holds for all $\mathbf{x}\in\mathbb{C}^{\#Y}$. Thus, for such a $\mathbf{x}$, we have

$$\sum_{k=1}^M C_k\cos\left(\mathbf{c}_k.\mathbf{x}\right)=\sum_{k=1}^M S_k\sin\left(\mathbf{c}_k.\mathbf{x}\right)=0,$$

since the functions $\mathbf{x}\mapsto\sum_{k=1}^M C_k\cos(\mathbf{c}_k.\mathbf{x})$ and $\mathbf{x}\mapsto\sum_{k=1}^M S_k\sin(\mathbf{c}_k.\mathbf{x})$ are both even and odd. The tuples $\mathbf{c}_1,\ldots,\mathbf{c}_M$ being pairwise distinct by construction, we get $C_k=S_k=0$ for all $k\in\{1,\ldots,M\}$. The lemma follows. ∎

https://doi.org/10.4153/S0008414X2300072X Published online by Cambridge University Press

For all $i, j \in I$, put $\mathbf{\Lambda}_j = (\Lambda_m^{(j,l)})_{(l,m)\in Y}$ and note that $\mathbf{\Lambda}_{i,j} = \mathbf{\Lambda}_j - \mathbf{\Lambda}_i$. Thanks to Lemma 8.4, it follows that $\mathbf{\Lambda}_j$ are pairwise distinct when j runs over all elements of I. We now compare these tuples as follows: We say that $\mathbf{\Lambda}_i$ is less than $\mathbf{\Lambda}_j$ if and only if $\Lambda_m^{(i,l)} < \Lambda_m^{(j,l)}$, where (l, m) is the smallest element of Y (for the usual lexicographic order in $\mathbb{R}^2$) for which $\Lambda_m^{(i,l)}$ and $\Lambda_m^{(j,l)}$ differ.

Proof of Theorem 8.1(b) Write E for the set of elements $j \in I$ such that the sequence $(z_{j,n})$ does not go to 0. Theorem 8.1(a) claims that E is non-empty. To get (b), it suffices to prove that $\#E = 1$. Assume by contradiction that $\#E > 1$. Let $i_0, j_0 \in E$ be distinct such that $\mathbf{\Lambda}_{j_0} = \max_{h\in E} \mathbf{\Lambda}_h$ and $\mathbf{\Lambda}_{i_0} = \min_{h\in E} \mathbf{\Lambda}_h$.

Let $k \in \{1, \dots, M\}$ be the unique integer such that $(i_0, j_0) \in E_k$. Lemma 8.8 gives $\sum_{(i,j)\in E_k} |z_{i,n}||z_{j,n}|e^{\zeta_4 L_{i,j}} \to 0$. As the sequence of terms $(z_{j,n})_{j\in I}$ is bounded by Theorem 8.1(a), we get $|z_{i,n}||z_{j,n}| \to 0$ if either $i \notin E$ or $j \notin E$. From the equality

$$E_k = (E_k \cap E^2) \sqcup \{(i, j) \in E_k, i \notin E \text{ or } j \notin E\},$$

we infer that $\sum_{(i,j)\in E_k\cap E^2} |z_{i,n}||z_{j,n}|e^{\zeta_4 L_{i,j}} \to 0$.

Let $(i, j) \in E_k \cap E^2$. As $(i_0, j_0) \in E_k \cap E^2$, we have $\mathbf{\Lambda}_{i_0,j_0} = \mathbf{c}_k = \mathbf{\Lambda}_{i,j}$; whence

$$\mathbf{\Lambda}_j - \mathbf{\Lambda}_i = \mathbf{\Lambda}_{i,j} = \mathbf{\Lambda}_{i_0,j_0} = \mathbf{\Lambda}_{j_0} - \mathbf{\Lambda}_{i_0}.$$

The maximality of $\mathbf{\Lambda}_{j_0}$, together with the minimality of $\mathbf{\Lambda}_{i_0}$, shows that $\mathbf{\Lambda}_j = \mathbf{\Lambda}_{j_0}$ and $\mathbf{\Lambda}_i = \mathbf{\Lambda}_{i_0}$. Since $\mathbf{\Lambda}_j$ are pairwise distinct when j ranges over all elements of I, we deduce that $(i, j) = (i_0, j_0)$, and so $E_k \cap E^2 = \{(i_0, j_0)\}$. But then, $|z_{i_0,n}||z_{j_0,n}|e^{\zeta_4 L_{i_0,j_0}} \to 0$, i.e., either $z_{i_0,n} \to 0$ or $z_{j_0,n} \to 0$, contradicting the definition of E. Theorem 8.1(b) follows. ∎

Acknowledgment I thank Y. Bilu and M. Sombra for their helpful advice; F. Amoroso, L. Pottmeyer, G. Rémond, and the anonymous referees for their relevant suggestions; and S. Fischler for his help concerning Lemma 4.2.

References

[1] F. Amoroso, *On a conjecture of G Rémond*. Ann. Sc. Norm. Super. Pisa Cl. Sci. **15**(2016), 599–608.
[2] F. Amoroso, S. David, and U. Zannier, *On fields with the property (B)*. Proc. Amer. Math. Soc. **142**(2014), no. 6, 1893–1910.
[3] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions*. J. Number Theory **595**(2000), no. 2, 260–272.
[4] F. Amoroso and U. Zannier, *A relative Dobrowolski lower bound over abelian extensions*. Ann. Sc. Norm. Super. Pisa Cl. Sci. (4) **29**(2000), no. 3, 711–727.
[5] F. Amoroso and U. Zannier, *A uniform relative Dobrowolski's lower bound over abelian extensions*. Bull. Lond. Math. Soc., **42**(2010), no. 3, 489–498.
[6] Y. Bilu, *Limit distribution of small points on algebraic tori*. Duke Math. J. **89**(1997), no. 3, 465–476.
[7] P. Blanksby and J. Loxton, *A note on the characterization of CM-fields*. J. Aust. Math. Soc. Ser. A **26**(1978), no. 1, 26–30.
[8] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, Cambridge University Press, Cambridge, 2006.
[9] E. Bombieri and U. Zannier, *A note on heights in certain infinite extensions of* $\mathbb{Q}$. Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **12**(2001), 5–14.

[10] C. Favre and J. Rivera-Letelier, *Équidistribution quantitative des points de petite hauteur sur la droite projective*. Math. Ann. **335**(2006), 311–361.
[11] P. Fili and Z. Milner, *Equidistribution and the heights of totally real and totally p-adic numbers*. Acta Arith. **170**(2015), no. 1, 15–25.
[12] L. Frey, *Height lower bounds in some non-abelian extensions*. Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **23**(2022), no. 3, 1357–1393.
[13] A. Galateau, *Small height in fields generated by singular moduli*. Proc. Amer. Math. Soc. **144**(2016), no. 7, 2771–2786.
[14] R. Grizzard, *Relative Bogomolov extensions*. Acta Arith. **170**(2015), no. 1, 1–13.
[15] R. Grizzard, *Remarks on Rémond's generalized Lehmer problems*. Preprint, 2017. arXiv:1710.11614v2
[16] P. Habegger, *Small height and infinite nonabelian extensions*. Duke Math. J. **162**(2013), no. 11, 2027–2076.
[17] A. Onishchik and E. B. Winberg, *Lie groups and algebraic groups*, Springer, Berlin, 1990.
[18] F. Pazuki and R. Pengo, *On the Northcott property for special values of L-functions*. Preprint, 2020. arXiv:2012.00542
[19] A. Perucca and P. Sgobba, *Kummer theory for number fields and the reductions of algebraic numbers II*. Unif. Distrib. Theory **15**(2020), no. 1, 75–92.
[20] C. Petsche, *The distribution of Galois orbits of low height*. Ph.D. thesis, The University of Texas at Austin, Austin, 2003.
[21] A. Plessis, *Minoration de la hauteur de Weil dans un compositum de corps de rayon*. J. Number Theory **205**(2019), 246–276.
[22] A. Plessis, *Bogomolov Property of some infinite nonabelian extensions of a totlly v-adic field*. Preprint, 2021. arXiv:2103.07270
[23] A. Plessis, *Points de petite hauteur sur une variété semi-abélienne isotriviale de la forme* $G_m^n \times A$. Bull. Lond. Math. Soc. **54**(2022), no. 6, 2278–2296.
[24] A. Plessis, *Location of small points on an elliptic curve by an equidistribution argument*. Int. Math. Res. Not. (2023), rnad051. https://doi.org/10.1093/imrn/rnad051
[25] L. Pottmeyer, *A note on extensions of* $\mathbb{Q}^{tr}$. J. Théor. Nombres Bordeaux **28**(2016), no. 3, 735–742.
[26] L. Pottmeyer, *Fields generated by finite rank subsets of* $\overline{\mathbb{Q}}^*$. Int. J. Number Theory **17**(2021), no. 5, 1079–1089.
[27] G. Rémond, *Généralisations du problème de Lehmer et applications à la conjecture de Zilber-Pink*. Panor. Synthèses **52**(2017), 243–284.
[28] S. Sahu, *Points of small heights in certain nonabelian extensions*. Ph.D. thesis, Chennai Mathematical Institute, Chennai, 2018.
[29] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*. Acta Arith. **24**(1973), 385–399.
[30] X. Yuan, *Big line bundles over arithmetic varieties*. Invent. Math. **173**(2008), 603–649.

Morningside Center of Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China
e-mail: plessis@amss.ac.cn