IAS SUMMER 2024 COLLABORATION REPORT : PROBLEMS ON HEIGHTS AND CM-FIELDS

SHABNAM AKHTARI, JEFFREY D. VAALER AND MARTIN WIDMER

1. Introduction and Background

Let K be an algebraic number field of degree d over $\mathbb{Q}$, v a place of K, and K_v the completion of K at v. We select two absolute values from the place v. The first is denoted by $\| \ \|_v$ and defined by:

(i) if $v|\infty$ then $\| \ \|_v$ is the unique absolute value on K_v that extends the usual absolute value on $\mathbb{Q}_\infty = \mathbb{R}$,

(ii) if $v|p$ then $\| \ \|_v$ is the unique absolute value on K_v that extends the usual p-adic absolute value on $\mathbb{Q}_p$.

The second absolute value is denoted by $| \ |_v$ and defined by $|x|_v = \|x\|_v^{d_v/d}$ for all x in K_v, where $d_v = [K_v : \mathbb{Q}_v]$ is the local degree. If α is in the multiplicative group $K^\times$ then the product formula asserts that

$$\prod_v |\alpha|_v = 1. \tag{1.1}$$

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and $\overline{\mathbb{Q}}^\times$ the multiplicative group of nonzero elements in $\overline{\mathbb{Q}}$. The *absolute, Weil height* (or simply the *height*)

$$H : \overline{\mathbb{Q}}^\times \to [0, \infty)$$

is defined as follows. Let α be a nonzero algebraic number, select an algebraic number field K containing α and write $\mathcal{M}_K$ for the collection of all places of K. Then define

$$H(\alpha) = \prod_{v \in \mathcal{M}_K} \max\{1, |\alpha|_v\}, \tag{1.2}$$

where the formally infinite product on the right of (1.2) has at most finitely many terms distinct from 1. Then $H(\alpha)$ is well defined because the product on the right of (1.2) does not depend on the choice of K. Sometimes we use the *absolute, logarithmic Weil height* which is

$$h(\alpha) = \log H(\alpha) = \sum_{v \in \mathcal{M}_K} \log^+ |\alpha|_v. \tag{1.3}$$

Combining (1.1) and (1.3) we get the useful identity

$$2h(\alpha) = \sum_v \big|\log |\alpha|_v\big|, \tag{1.4}$$

where $| \ |$ (an absolute value without a subscript) is the usual archimedean absolute value on $\mathbb{R}$ or $\mathbb{C}$.

For each number field K we define two multiplicative subgroups

$$\mathcal{S}_K = \bigl\{\alpha \in K^{\times} : \|\alpha\|_w = 1 \text{ at each archimedean place } w \text{ of } K\bigr\}, \tag{1.5}$$

and

$$\mathcal{U}_K = \bigl\{\alpha \in K^{\times} : \|\alpha\|_w = 1 \text{ at each nonarchimedean place } w \text{ of } K\bigr\}. \tag{1.6}$$

It follows easily that

$$\mathcal{S}_K \cap \mathcal{U}_K = \operatorname{Tor}\bigl(K^{\times}\bigr).$$

Then $\mathcal{U}_K$ is the group of *units* in O_K and

$$\mathcal{U}_K / \operatorname{Tor}\bigl(\mathcal{U}_K\bigr)$$

is a free abelian group of finite rank. The group $\mathcal{S}_K$ is less well known. However, it can be shown either $\mathcal{S}_K = \{\pm 1\}$, or

$$\mathcal{S}_K / \operatorname{Tor}\bigl(\mathcal{S}_K\bigr)$$

is a free abelian group with countably infinite rank.

Next we recall that a number field K is a CM-field if K is totally complex, and there exists a totally real subfield $k \subseteq K$ such that K/k is a quadratic extension. The term CM-*field* originates in the work [8] of Shimura and Taniyama on abelian varieties. It is known that the composite of each finite collection of CM-fields is a CM-field. And if K is a CM-field then each conjugate of K over $\mathbb{Q}$ is a CM-field, and also the Galois closure of K is a CM-field.

It follows from a result of Blanksby and Loxton [2] that if L is an algebraic number field and $\alpha \neq \pm 1$ is an element of the group $\mathcal{S}_L$, then the subfield

$$K = \mathbb{Q}(\alpha) \subseteq L$$

is a CM-field. Moreover, if L is itself a CM-field then there exists an element $\beta \neq \pm 1$ in the group $\mathcal{S}_L$ such that $L = \mathbb{Q}(\beta)$. It is clear from these remarks that $\mathcal{S}_L = \{\pm 1\}$ if and only if no subfield of L is a CM-field.

Let K be a CM-field and $k \subseteq K$ the totally real subfield such that K/k is a quadratic extension. Then K/k is a Galois extension and we write $\tau : K \to K$ for the unique automorphism that generates the Galois group $\operatorname{Aut}(K/k)$. It follows that

$$\operatorname{Norm}_{K/k}(\alpha) = \alpha\tau(\alpha).$$

And if K is a CM-field it can be shown that the group $\mathcal{S}_K$ is the kernel

$$\mathcal{S}_K = \{\alpha \in K^{\times} : \operatorname{Norm}_{K/k}(\alpha) = 1\}.$$

When K is a CM-field it is useful to define the homomorphism

$$\psi : K^{\times} \to K^{\times}$$

at α in $K^{\times}$ by

$$\psi(\alpha) = \frac{\alpha}{\tau(\alpha)}.$$

Applying Hilbert's Theorem 90 we find that

$$\{\alpha \in K^{\times} : \psi(\alpha) = 1\} = k^{\times}, \quad \text{and} \quad \{\psi(\alpha) : \alpha \in K^{\times}\} = \mathcal{S}_K.$$

It follows that ψ induces an isomorphism

$$\widetilde{\psi} : K^{\times}/k^{\times} \to \mathcal{S}_K. \tag{1.7}$$

Combining (1.7), a result of Brandis [3], and a result of Lawrence [5], we find that the multiplicative group $\mathcal{S}_K$ is a free abelian group of countably infinite rank.

2. Generators of number fields with small height

Let K be an algebraic number field, Δ_K the discriminant of K, and $d = [K : \mathbb{Q}]$ its degree. We also define the positive constant

$$c_K = \left(\frac{2}{\pi}\right)^{s/d} \bigl|\Delta_K\bigr|^{1/2d},$$

where s is the number of complex places of K. In [7] W. Ruppert asked the following question:

Question 2.1. [Ruppert, 1998] *Does there exist a positive constant $A = A(d)$ such that if K is an algebraic number field of degree d over $\mathbb{Q}$, then there exists an element α in K such that*

$$K = \mathbb{Q}(\alpha), \quad \textit{and} \quad H(\alpha) \le A\bigl|\Delta_K\bigr|^{1/2d}\,?$$

In [7, Proposition 2] Ruppert obtained a positive answer to his question when $[K : \mathbb{Q}] = 2$. He also proved that if K is a real quadratic extension of $\mathbb{Q}$, then the generator α can be selected from the ring O_K of algebraic integers in K. In [9] the second and third named collaborators provided the following partial answer to Ruppert's question.

Theorem 2.1. *Assume that K has an embedding into $\mathbb{R}$. Then there exists an algebraic integer α in O_K such that*

$$K = \mathbb{Q}(\alpha), \quad \textit{and} \quad H(\alpha) \le c_K.$$

In Theorem 2.1 the generator α is an algebraic integer, a requirement that was *not* stated in Ruppert's question, while the height of α is bounded in a manner that was anticipated in Ruppert's question. Hence Theorem 2.1 generalizes Ruppert's earlier result to number fields K that have at least one real embedding.

In a recent work [1] we proved the following new result.

Theorem 2.2. *Assume that K is a number field such that*

$$c_K < \min\bigl\{H(\alpha) : \alpha \in O_K \ \textit{and}\ K = \mathbb{Q}(\alpha)\bigr\}, \tag{2.1}$$

and let F denote the maximal totally real subfield of K. Then K/F is a Galois extension, K is totally complex, and $\operatorname{Tor}\bigl(K^{\times}\bigr) = \{\pm 1\}$.

During our stay at IAS, we generalized the above theorem further. We proved the following.

Theorem 2.3. *Let $\mathcal{H} \ge 1$. Assume that K is a number field such that*

$$c_K\mathcal{H} < \min\bigl\{H(\alpha) : \alpha \in O_K \ \textit{and}\ K = \mathbb{Q}(\alpha)\bigr\}.$$

Then K is totally complex, K is Galois over its maximal totally real subfield F, and every $\alpha \in O_K$ with $\overline{|\alpha|} \le \mathcal{H}$ lies in F.

In the above theorem, $\overline{|\alpha|}$ denotes the house of α, that is the maximal modulus of the algebraic conjugates of α.

In addition, for every integer $N \geq 2$ we constructed a family of examples of CM-fields of degree $d = 2N$ that satisfy (2.1). These new findings will be added to our previously submitted manuscript [1].

While at IAS, we met and discussed this ongoing project with Michael Mossinghoff, an expert in computational number theory who works at Center for Communications Research, Princeton. By incorporating some experimental approaches, we hope to have a more precise classification of number fields without small integral generators in the near future.

3. Equidistribution of points in $\mathcal{S}_K$

Let K be a CM-field. We assume that K is embedded in $\mathbb{C}$ and write $|\ | : \mathbb{C} \to [0, \infty)$ for the ordinary archimedean absolute value on $\mathbb{C}$. Then

$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$$

is a compact, abelian group and the dual of $(\mathbb{T}, \cdot)$ is the discrete group $(\mathbb{Z}, +)$. Each continuous character on $\mathbb{T}$ is given by a map

$$z \mapsto z^n, \quad \text{for a unique } n \text{ in } \mathbb{Z}. \tag{3.1}$$

Obviously $n = 0$ determines the principal character.

As K is embedded in $\mathbb{C}$ it follows from (1.5) that each element α in $\mathcal{S}_K$ is contained in $\mathbb{T}$. If $F : \mathbb{T} \to \mathbb{C}$ is continuous, or if F has bounded variation, we write

$$\mathcal{S}_K(F, \mathcal{H}) = \sum_{\substack{\alpha \in \mathcal{S}_K \\ H(\alpha) \leq \mathcal{H}}} F(\alpha)$$

where $1 \leq \mathcal{H}$. We have been working on showing that the points of $\mathcal{S}_K$ are equidistributed in $\mathbb{T}$ when ordered by increasing height. For $n \neq 0$ the maps (3.1) are the nonprincipal characters on $\mathbb{T}$. Therefore it follows from Weyl's criterion (see [4, Chapter 1, Section 2]) that the points of $\mathcal{S}_K$ are equidistributed in $\mathbb{T}$ when ordered by increasing height if and only if

$$\lim_{\mathcal{H} \to \infty} \frac{\mathcal{S}_K(z^n, \mathcal{H})}{\mathcal{S}_K(1, \mathcal{H})} = 0 \tag{3.2}$$

for each nonzero integer n. For imaginary quadratic fields K such a result has been established by Petersen and Sinclair [6].

We have improved our earlier work on this topic during our visit to IAS and have established an explicit estimate for the sums $\mathcal{S}_K(F, \mathcal{H})$ for an arbitrary CM-field K. Such a bound leads to a corresponding estimate for the discrepancy of the finite subset

$$\big\{\alpha \in \mathcal{S}_K : H(\alpha) \leq \mathcal{H}\big\} \subseteq \mathbb{T}.$$

Our immediate future plan is to prepare and submit an article containing these new results on equidistribution in CM-fields.

References

[1] S. Akhtari, J. D. Vaaler, and M. Widmer. A note on small generators of number fields, II. *Submitted.*, 2023.

[2] P. E. Blanksby and J. H. Loxton. A note on the characterization of CM-fields. *J. Austral. Math. Soc. (Series A)*, 26:26–30, 1978.

[3] A. Brandis. Über die multiplicative Struktur von Körpererweiterungen. *Math. Zeit.*, pages 71–73, 1965.

[4] L. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences.* Dover Publications, Mineola, New York, 2006.

[5] J. Lawrence. Countable abelian groups with a discrete norm are free. *Proc. Amer. Math. Soc.*, 297:352–354, 1984.

[6] K. L. Petersen and C. D. Sinclair. Equidistribution of algebraic numbers of norm one in quadratic number fields. *Inter. Jour. Num. Th.*, 7(7):1841–1861, 2011.

[7] W. Ruppert. Small generators of number fields. *Manuscripta Math.*, 96(1):17–22, 1998.

[8] G. Shimura and Y. Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6. Math. Soc. Japan, Tokyo, 1961.

[9] J. D. Vaaler and M. Widmer. A note on generators of number fields. In *Diophantine methods, lattices and the arithmetic theory of quadratic forms*, volume 587 of *Contemp. Math.*, pages 201–211. Amer. Math. Soc., Providence, RI, 2013.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802 USA

Email address: `akhtari@psu.edu`

Department of Mathematics, University of Texas, Austin, TX 78712 USA

Email address: `vaaler@math.utexas.edu`

Department of Mathematics, Royal Holloway, University of London, Egham, TW20 0EX UK

Email address: `martin.widmer@rhul.ac.uk`