IRIS AperTO

UNIVERSITÀ DEGLI STUDI DI TORINO

AperTO - Archivio Istituzionale Open Access dell'Università di Torino

Algebraic numbers of small Weil's height in CM-fields: on a theorem of Schinzel

This is the author's manuscript

Original Citation:

Availability:

This version is available http://hdl.handle.net/2318/1944872 since 2023-11-28T14:48:16Z

Published version:

DOI:10.1016/j.jnt.2006.04.005

Terms of use:

Open Access

Anyone can freely access the full text of works made available as "Open Access". Works made available under a Creative Commons license can be used according to the terms and conditions of said license. Use of all other works requires consent of the right holder (author or publisher) if not exempted from copyright protection by the applicable law.

(Article begins on next page)

18 September 2024

Algebraic Numbers of Small Weil's height in CM-fields: on a Theorem of Schinzel

Francesco Amoroso* & Filippo A. E. Nuccio†

1 Introduction

Let $\mathbb{K}$ be a CM-field. A. Schinzel proved ([Sch 1973]) that the Weil height of non-zero algebraic numbers in $\mathbb{K}$ is bounded from below by an absolute constant C outside the set of algebraic numbers such that $|\alpha| = 1$ (since $\mathbb{K}$ is CM, $|\alpha| = 1$ for some archimedean place guarantees $|\alpha| = 1$ for all archimedean places). More precisely, his result reads as follows: for any $\alpha \in \mathbb{K}^\times$, $|\alpha| \neq 1$, we have

$$h(\alpha) \geq C := \frac{1}{2} \log \left(\frac{1+\sqrt{5}}{2} \right) .$$

E. Bombieri and U. Zannier, motivated also by the above result, asked (private communication to the first author) for an absolute lower bound for the height of non-zero algebraic numbers lying in a complex abelian extension outside the set of roots of unity. This question was solved by R. Dvornicich and the first author (see [AmoDvo 2000]), who proved that for any α in a complex abelian extension, $\alpha \neq 0$ and α not a root of unity, we have

$$h(\alpha) \geq C_{\mathrm{ab}} := \frac{\log 5}{12} .$$

In the same paper it was shown that C_{ab} cannot be replaced by any constant $> (\log 7)/12$, since there exists an element α in a cyclotomic field such that $h(\alpha) = (\log 7)/12$; we note that $(\log 7)/12 < C$.

One may now ask whether the abelianity condition is necessary for this latter lower bound or if this bound holds in general for CM fields. As a first step towards an answer, in his Master Thesis ([Nuc 2004]) the second author uses the classification of all dihedral principal CM fields given by S. Louboutin and R. Okazaky (see [LouOka 1994]) to prove the following:

*Laboratoire de Mathématiques "N. Oresme", U.M.R. 6139 (C.N.R.S.), Université de Caen, Campus II, BP 5186, F–14032 Caen Cedex. e-mail: amoroso@math.unicaen.fr

†Dipartimento di Matematica "G. Castelnuovo", Università "La Sapienza", Piazzale Aldo Moro, 2 I–00185 Roma. e-mail: nuccio@mat.uniroma1.it

Theorem 1.1 *There exists a normal CM-field* $\mathbb{L}$ *(of degree 8 and such that* $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \cong D_4$*, the dihedral group of order 8) whose ring of integers* $\mathcal{O}_{\mathbb{L}}$ *contains an element* γ *of height*

$$h(\gamma/\bar{\gamma}) = \frac{\log |N_{\mathbb{Q}}^{\mathbb{L}}(\gamma)|}{[\mathbb{L} : \mathbb{Q}]} = \frac{\log 2}{8} < C_{\mathrm{ab}} \ .$$

Motivated by this example, we formulate the following natural question in this context:

Question 1.2 *Does there exist an absolute constant* $C_{\mathrm{CM}} \in (0, C_{\mathrm{ab}})$ *such that for every CM field* $\mathbb{K}$ *and for every* $\alpha \in \mathbb{K}^{\times} \setminus \mathbb{K}_{\mathrm{tors}}$*,* $h(\alpha) > C_{\mathrm{CM}}$ *holds?*

We prove the following theorem, which gives a negative answer to the previous question:

Theorem 1.3 *There exists an infinite sequence* (α_k) *of algebraic numbers such that the fields* $\mathbb{Q}(\alpha_k)$ *are CM-fields,* α_k *is not a root of unity,* $d_k = [\mathbb{Q}(\alpha_k) : \mathbb{Q}] \to +\infty$ *and*

$$h(\alpha_k) \sim \frac{\log(d_k)}{d_k} = o(1)$$

as $k \to +\infty$*.*

As an application of the main theorem in [AmoDvo 2000], a lower bound for the norm of algebraic integers γ such that $\gamma/\bar{\gamma}$ is not a root of unity was given (see [AmoDvo 2000], Corollary 1):

Theorem (Amoroso-Dvornicich) Let γ be an integer lying in an abelian extension $\mathbb{L}$ of $\mathbb{Q}$. Then, if $\gamma/\bar{\gamma}$ is not a root of unity,

$$\frac{\log |N_{\mathbb{Q}}^{\mathbb{L}}(\gamma)|}{[\mathbb{L} : \mathbb{Q}]} \geq \frac{\log 5}{12} \ .$$

Our result allows us to show that also this bound is not anymore true if the abelianity condition is dropped (see Theorem 5.1).

Our proof relies on elementary facts about reciprocal polynomials and on an operator δ introduced by the first author (see [Amo 1995]). We will construct two families of polynomials having all their roots on the unit circle and with "small" leading coefficient. We will eventually show that these polynomials are either irreducible or have a (non monic) irreducible factor of high degree: this will ensure their roots have small height. Moreover, having all their roots on the unit circle, the fields defined by those polynomials are CM-fields.

The paper is organized as follows: in section 2 we recall some basic facts on Weil's height and on CM-fields and we introduce δ. The third section is devoted to the dihedral example. In the two following sections, we produce the two families mentioned above. Finally, in the last section, we propose a conjecture about polynomials defining CM-fields.

Acknowledgement. *We are indebted to D. Simon for a useful discussion about Theorem 5.1. The second author is also grateful to J. Cougnard for enlightening comments on Section 3. We are finally indebted to the Referee for several useful suggestions, specially for the remark following conjecture 6.1.*

2 Auxiliary results

2.1 Weil's height

Let $\alpha \in \overline{\mathbb{Q}}$ and let $\mathbb{K}$ be a number field containing α. We denote by $\mathcal{M}_{\mathbb{K}}$ the set of places of $\mathbb{K}$. For $v \in \mathbb{K}$, let $\mathbb{K}_v$ be the completion of $\mathbb{K}$ at v and let $|\cdot|_v$ be the (normalized) absolute value of the place v. Hence, if v is an archimedean place associated with the embedding $\sigma\colon \mathbb{K} \hookrightarrow \overline{\mathbb{Q}}$

$$|\alpha|_v = |\sigma\alpha|,$$

and, if v is a non archimedean place associated to the prime ideal $\mathfrak{p}$ over the rational prime p,

$$|\alpha|_v = p^{-\lambda/e},$$

where e is the ramification index of $\mathfrak{p}$ over p and λ is the exponent of $\mathfrak{p}$ in the factorization of the ideal (α) in the ring of integers of $\mathbb{K}$. This standard normalization agrees with the product formula

$$\prod_{v\in\mathcal{M}_{\mathbb{K}}} |\alpha|_v^{[\mathbb{K}_v:\mathbb{Q}_v]} = 1$$

which holds for $\alpha \in \mathbb{K}^\times$. We define the (Weil) height of α by

$$h(\alpha) = \frac{1}{[\mathbb{K}:\mathbb{Q}]} \sum_{v\in\mathcal{M}_{\mathbb{K}}} [\mathbb{K}_v:\mathbb{Q}_v] \log\max\{|\alpha|_v, 1\}.$$

It is easy to check that $h(\zeta) = 0$ for every root of unity $\zeta \in \bar{\mathbb{Q}}$: it is in fact equivalent to Kronecker's Theorem.

For later use, we also need (see for instance [Wal 2000], chapitre 3):

Remark 2.1 *Let α be a non-zero algebraic numbers and let $P(X) \in \mathbb{Z}[X]$ be its minimal polynomial over the integers, i.e. $P(\alpha) = 0$ and P is irreducible of leading leading coefficient $\ell > 0$. Let $K = \mathbb{Q}(\alpha)$; then*

$$\log \ell = \sum_{v\in\mathcal{M}_{\mathbb{K}},\, v\nmid\infty} [\mathbb{K}_v:\mathbb{Q}_v] \log\max\{|\alpha|_v, 1\}.$$

2.2 Reciprocal polynomials and CM fields

We now recall some basic facts about reciprocal and antireciprocal polynomials.

Definition 2.2 *Let $P(X) \in \mathbb{C}[X]$ be a polynomial of degree d. If $P(X) = X^d\overline{P}(X^{-1})$, then P is said to be reciprocal. If $P(X) = -X^d\overline{P}(X^{-1})$, it is said to be antireciprocal.*

Let us emphasise that the factors of a reciprocal or antireciprocal polynomial with real coefficients should have specific form. Firstly, if $P(X) \in \mathbb{R}[X]$ is a reciprocal (or antireciprocal) polynomial of degree d and α is a root of P, then $\alpha \neq 0$ and α^{-1} is still a root of P. If now $P(\pm 1) \neq 0$, the distinct values $\{\alpha, \alpha^{-1}\}$ are two roots of the polynomial having the same multiplicity and the polynomial is reciprocal of even degree, all of its roots being "coupled". We can then factorise a general reciprocal (or antireciprocal) polynomial P as

$$P(X) = (X-1)^a(X+1)^bQ(X)$$

where $Q(X)$ is reciprocal not vanishing at ± 1 of degree $2k$ and $d = a+b+2k$. Moreover, $a \equiv 1 \bmod 2$ if P is antireciprocal and $b \equiv 1 \bmod 2$ if P is reciprocal of odd degree or if it is antireciprocal of even degree.

A totally imaginary quadratic extension $\mathbb{K}$ of a totally real number field $\mathbb{K}^+$ is said to be a CM-field. As mentioned in the introduction, one of the main properties of CM-fields is the following: let $\alpha \in \mathbb{K}$ and assume that $|\tau\alpha| = 1$ for some embedding τ; then for any embedding σ we have $|\sigma\alpha| = 1$. Indeed, the complex conjugation induces an automorphism on $\mathbb{K}$ which is independent of the embedding into $\mathbb{C}$ (see [Was 1982], p.38). The following characterizes CM-fields and will be useful in our main construction:

Proposition 2.3 *A number field $\mathbb{K} \neq \mathbb{Q}$ is CM if and only if there exists a monogenic*[1] *element $\alpha \in \mathbb{K}$ such that $|\sigma\alpha| = 1$ for all embedding σ.*

Proof : Let $\mathbb{K}$ be a CM-field and let $\gamma \in \mathbb{K}$ be a monogenic element. For $n \in \mathbb{Z}$ we put

$$\alpha_n = \frac{\gamma + n}{\bar{\gamma} + n}\ .$$

Clearly, $|\sigma\alpha_n| = 1$ for every σ. In order to show that some α_n is monogenic, let us point out that there are two different integers n, $m \in \mathbb{Z}$ such that $\alpha_n \neq \alpha_m$ and $\mathbb{Q}(\alpha_n) = \mathbb{Q}(\alpha_m)$, since the number of subfields of $\mathbb{K}$ is finite. Therefore,

$$\gamma = \frac{m\alpha_n(1-\alpha_m) - n\alpha_m(1-\alpha_n)}{\alpha_m - \alpha_n} \in \mathbb{Q}(\alpha_n)$$

and $\mathbb{K} = \mathbb{Q}(\alpha_n)$.

[1] We say that α in a number field $\mathbb{K}$ is *monogenic* with respect to $\mathbb{K}$ when $\mathbb{K} = \mathbb{Q}(\alpha)$.

Conversely, let us assume that $\mathbb{K} = \mathbb{Q}(\alpha)$ where $|\sigma\alpha| = 1$ for all embedding σ. Put

$$\mathbb{K}^+ = \mathbb{Q}(\alpha + \alpha^{-1}) \ ;$$

then $\mathbb{K}^+$ is a totally real field and $[\mathbb{K} : \mathbb{K}^+] = 2$, because $\alpha \notin \mathbb{R}$ and $\mathbb{K} \neq \mathbb{Q}$.

Q.E.D.

Thus, a CM field can be defined by an irreducible polynomial $P \in \mathbb{Q}[X]$ vanishing only on the unit circle. We also remark that such a polynomial must be reciprocal, since $|\alpha| = 1 \Rightarrow \bar{\alpha} = \alpha^{-1}$.

2.3 A Differential Operator

We now introduce an operator δ (see [Amo 1995]) over $\mathbb{C}[X]$ which has all the properties of a derivation but linearity: if $P(X) \in \mathbb{C}[X]$ is a polynomial with complex coefficients of degree d (we set $\deg(0) = 0$), we define

$$\delta(P)(X) = X\frac{\mathrm{d}P}{\mathrm{d}X}(X) - \frac{d}{2}P(X) \ .$$

It is obvious that, if we denote by p_d the leading coefficient of P, the leading coefficient of $\delta(P)$ is $dp_d/2$, and that $\delta(P)$ and P have the same degree. Moreover, a classical property of a derivation is satisfied:

$$\delta(PQ) = \delta(P)Q + \delta(Q)P \ ;$$

therefore, for $n \in \mathbb{N}$,

$$\delta(P^n) = nP^{n-1}\delta(P) \ .$$

The following remark (due to D. Simon) can also be useful. Let D the derivation

$$D(F) = \frac{1}{2}\left(X\frac{\partial F}{\partial X} - Y\frac{\partial F}{\partial Y}\right)$$

on $\mathbb{C}[X, Y]$. Then for any $P \in \mathbb{C}[X]$ we have $\delta(P)(X) = D({}^hP)(X, 1)$, where ${}^hP(X, Y) = Y^{\deg(P)}P(X/Y)$ is the homogenization of P.

Having recalled all these basic facts, we can prove the main property of the operator δ (see also [Amo 1995], Prop. 1):

Lemma 2.4 *Let $P(X) \in \mathbb{C}[X]$ be a reciprocal polynomial (resp. antireciprocal) having all its roots on the unit circle. Then $\delta(P)(X)$ is an antireciprocal (resp. reciprocal) polynomial whose roots still lie on the unit circle. Moreover, if $\alpha_1, \ldots, \alpha_k$ are the distinct roots of $P(X)$ of multiplicity $m_1, \ldots, m_k$, then $\delta(P)(X)$ vanishes at α_j with multiplicity $m_j - 1$ for $j = 1, \ldots, k$, and at certain $\beta_1, \ldots, \beta_k$ with multiplicity equal to 1. Finally, the set $\{\alpha_1, \ldots, \alpha_k\}$ and $\{\beta_1, \ldots, \beta_k\}$ are intercalated.*[2]

[2]Two finite sets $S, T \subset \{z \in \mathbb{C}, |z| = 1\}$ are *intercalated* if they have the same cardinality and if there is one, and only one, $\alpha \in S$ between each pair of consecutive β, $\beta' \in T$ along the unit circle.

Proof : We begin by showing that δ transforms reciprocal polynomials into antireciprocal ones, and vice versa: directly from the definition, it is clear that the condition of being reciprocal (resp. antireciprocal) for a polynomial

$$P(X) = \sum_{j=0}^{d} a_j X^j$$

turns out to be $a_j = \overline{a_{d-j}}$ (resp. $a_j = -\overline{a_{d-j}}$). Looking closely at the definition of δ and setting

$$\delta(P)(X) = \sum_{j=0}^{d} b_j X^j,$$

it is clear that for $j = 1, \dots, d$ we have $b_j = (j - d/2)a_j$ and therefore

$$b_{d-j} = (d - j - d/2)a_{d-j} = (d/2 - j)a_{d-j} \ .$$

Thus, when P is reciprocal, $a_j = \overline{a_{d-j}}$ implies $b_j = -\overline{b_{d-j}}$ and so $\delta(P)$ is antireciprocal; and when P is antireciprocal, $a_j = -\overline{a_{d-j}}$ implies $b_j = \overline{b_{d-j}}$ and so $\delta(P)$ is reciprocal.

Let us now suppose P to be a reciprocal polynomial of degree d and let $\alpha_j = e^{i\vartheta_j}$: then

$$f(t) = e^{-i\frac{d}{2}t} P(e^{it})$$

is a periodic real function (in fact $\overline{f(t)} = e^{i\frac{d}{2}t}\overline{P}(e^{-it}) = f(t)$) of period equal to 2π which vanishes at $\{\vartheta_1, \dots, \vartheta_k\} \subset [0, 2\pi)$. Thanks to Rolle's Theorem, $f'(t)$ vanishes at certain $\{\phi_1, \dots, \phi_k\}$ and the sets

$$\{e^{i\vartheta_1}, \dots, e^{i\vartheta_k}\} \qquad \text{and} \qquad \{e^{i\phi_1}, \dots, e^{i\phi_k}\}$$

are intercalated. But

$$\begin{aligned} f'(t) &= \frac{\mathrm{d}}{\mathrm{d}t}\big(e^{-i\frac{d}{2}t}P(e^{it})\big) = e^{-i\frac{d}{2}t}\frac{\mathrm{d}P(e^{it})}{\mathrm{d}t} - i\frac{d}{2}e^{-i\frac{d}{2}t}P(e^{it}) \\ &= ie^{it-i\frac{d}{2}t}P'(e^{it}) - i\frac{d}{2}e^{-i\frac{d}{2}t}P(e^{it}) = ie^{-i\frac{d}{2}t}\Big(e^{it}P'(e^{it}) - \frac{d}{2}P(e^{it})\Big) \\ &= ie^{-i\frac{d}{2}t}\delta(P)(e^{it}), \end{aligned} \tag{2.1}$$

and so $\{e^{i\phi_1}, \dots, e^{i\phi_k}\}$ are roots of $\delta(P)$. But, if $e^{i\vartheta_j}$ is a root of $P(X)$ having multiplicity m_j, then $e^{i\vartheta_j}$ is a root of $P'(X)$ having exact multiplicity equal to $m_j - 1$; hence we see, from (2.1), that $e^{i\vartheta_j}$ is a root of $\delta(P)(X)$ having multiplicity $m_j - 1$. Finally $\deg\big(\delta(P)\big) = \deg(P) = d$, and so the relation

$$d = k + (m_1 - 1) + \cdots + (m_k - 1)$$

shows that $\delta(P)(X)$ can have no other roots, and that $\{e^{i\phi_1}, \ldots, e^{i\phi_k}\}$ are simple roots.

If P were antireciprocal the same argument would lead to our conclusion, using the function $g(t) = if(t)$.

Q.E.D.

3 A Dihedral Example

The main idea for this construction is the relation between the norm and the height of certain algebraic numbers pointed out in [AmoDvo 2000], Corollary 1: if γ is an algebraic integer of a CM-field $\mathbb{K}$ such that the ideals (γ) and $(\bar{\gamma})$ are coprime (and then $\gamma/\bar{\gamma}$ is not a root of unity), thus

$$h(\gamma/\bar{\gamma}) = \frac{\log |N_{\mathbb{Q}}^{\mathbb{K}}(\gamma)|}{[\mathbb{K} : \mathbb{Q}]} \ . \tag{3.1}$$

Working in principal fields one has elements of norm p for each prime $\mathfrak{p}|p$, provided its inertial degree equals 1, and relation (3.1) may therefore be easily employed. We shall then consider (letting notations be as in [LouOka 1994]), the fields $\mathbb{L}_{p,q}$, which are the unique cyclic quartic extensions of $\mathbb{Q}(\sqrt{pq})$ unramified at the finite places and are dihedral octic CM-fields. In the sequel $e_{\mathbb{F}}^{\mathbb{K}}(\mathfrak{f})$, $f_{\mathbb{F}}^{\mathbb{K}}(\mathfrak{f})$ (or simply $e(\mathfrak{f}), f(\mathfrak{f})$ when there is no ambiguity) will denote ramification index and inertial degree, respectively, of a prime ideal $\mathfrak{f} \subseteq \mathcal{O}_{\mathbb{K}}$ in an extension $\mathbb{K}/\mathbb{F}$: moreover, we will feel free to write $e(\ell), f(\ell)$ for some rational prime ℓ when considering normal extensions $\mathbb{K}/\mathbb{Q}$.

Looking for elements whose height is smaller than the constant C_{ab} quoted in the introduction, we want

$$\frac{\log \ell}{8} < \frac{\log 5}{12} \ ,$$

that forces $\ell = 2$; since we should require $f(2) = 1$ in order to use (3.1), we need $f_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{pq})} = 1$, i.e. either $p, q \equiv 1 \bmod 2$ or $p = 2$ and $q \equiv 1 \bmod 2$. Comparing these conditions with the list of all dihedral octic principal CM-fields given in the paper [LouOka 1994], the only fields we can consider are the $\mathbb{L}_{p,q}$ with $p < q$ and

$$(p, q) \in \big\{(2, 17), (2, 73), (2, 89), (2, 233), (2, 281), (17, 137), (73, 97)\big\} \ .$$

Claim 3.1 $f_{\mathbb{Q}}^{\mathbb{L}_{2,17}}(2) = 1$.

We shall prove Claim 3.1 later on, and use it now to prove Theorem 1.1: from now on, we set $\mathbb{L} := \mathbb{L}_{2,17}$.

Proof of Theorem 1.1: First of all, $e_{\mathbb{Q}}^{\mathbb{L}}(2) = 2$, because $\mathbb{L}/\mathbb{Q}(\sqrt{34})$ is unramified at the finite places; indeed, Claim 3.1 implies that the prime 2 is factorised in $\mathcal{O}_{\mathbb{L}}$ as

$$2\mathcal{O}_{\mathbb{L}} = (\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4)^2 \ .$$

and we will fix the four primes $\{\mathfrak{p}_i\}_{i=1}^4$ from now on. Let us emphasize that having $\mathrm{Gal}(\mathbb{L}/\mathbb{Q}) \cong D_4$, the Galois structure of the extension is as follows:

$$\begin{tikzcd}
 & & \mathbb{L} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash, "2"] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{K}_1 \arrow[dr, dash] & \mathbb{K}_2 \arrow[d, dash] & \mathbb{Q}(\sqrt{2}, \sqrt{17}) := \mathbb{L}^+ \arrow[dl, dash] \arrow[d, dash, "2"] \arrow[dr, dash] & \mathbb{F}_1 \arrow[d, dash] & \mathbb{F}_2 \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{34}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{17}) \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

where $\mathbb{K}_1 \cong \mathbb{K}_2 \ncong \mathbb{F}_1 \cong \mathbb{F}_2$ are non-normal quartic CM-fields. If $\mathcal{D}_i$ denotes the decomposition subgroup at $\mathfrak{p}_i$ for $i = 1, \ldots, 4$, the conditions $f(2) = 1$ and $e(2) = 2$ imply that $|\mathcal{D}_i| = 2$ for $i = 1, \ldots, 4$. We need only to show that for at least one (and then for all) index i, the complex conjugation χ does not belong to $\mathcal{D}_i$, because then the ideals $\mathfrak{p}_i$ and $\chi(\mathfrak{p}_i) = \overline{\mathfrak{p}_i}$ will be coprime. If $\mathbb{L}^i := \mathbb{L}^{D_i}$ are the decomposition subfields and we fix an index i, it is well known that $\mathfrak{p}_i \cap \mathcal{O}_{\mathbb{L}^i}$ is unramified in $\mathbb{L}^i/\mathbb{Q}$ and that $e(\mathfrak{p}_i \cap \mathcal{O}_{\mathbb{L}^i}) = e(\mathfrak{p}_i) = 2$ in $\mathbb{L}/\mathbb{L}^i$: since $\mathbb{L}/\mathbb{Q}(\sqrt{34})$ is unramified at the finite places, we cannot have

$$\mathbb{L} \supset \mathbb{L}^i \supset \mathbb{Q}(\sqrt{34})$$

and therefore $\mathbb{L}^i \neq \mathbb{L}^+ = \mathbb{L}^{\{e,\chi\}}$, showing that $\chi \notin \mathcal{D}_i$ for all i. Therefore, if $(\gamma) = \mathfrak{p}_1$, the ideals (γ) and $(\overline{\gamma})$ are coprime, and (3.1) gives

$$h(\gamma/\bar{\gamma}) = \frac{\log |N_{\mathbb{Q}}^{\mathbb{L}}(\gamma)|}{[\mathbb{L} : \mathbb{Q}]} = \frac{\log 2}{8} < C_{\mathrm{ab}} \ .$$

Q.E.D.

Concerning Claim 3.1, an easy computation made with Pari-GP allows one to obtain much more: $(2, 17)$ is the only pair of primes such that $f_{\mathbb{Q}}^{\mathbb{L}_{p,q}}(2) = 1$. But within the scope of our construction, it is enough to show that the inertial degree of (2) in $\mathbb{L}_{2,17}$ equals 1 $\big($since examples in other fields would not have smaller height, because $[\mathbb{L}_{p,q} : \mathbb{Q}] = 8$ for all $(p, q)\big)$ and this can be shown in a much more theoretical way, as follows.

Theorem (7) of [LouOka 1994] explicitly gives the construction of $\mathbb{L}_{p,q}$, defining them as the unique cyclic quartic extension of $\mathbb{Q}(\sqrt{qp})$ unramified at finite places. In particular, they are precisely the ray class fields for the modulus $\mathfrak{m} = \infty$ of $\mathbb{Q}(\sqrt{qp})$: therefore, Class Field Theory gives an isomorphism between their Galois groups over $\mathbb{Q}(\sqrt{qp})$ and the narrow class group $\mathcal{C}_+$ of $\mathbb{Q}(\sqrt{qp})$ via Artin recpirocity map:

$$\begin{aligned} \varphi : \mathcal{C}_+ &\xrightarrow{\cong} \mathrm{Gal}(\mathbb{L}_{p,q}/\mathbb{Q}(\sqrt{qp})) \\ \bar{\mathfrak{p}} &\longmapsto (\mathfrak{p}, \mathrm{Gal}(\mathbb{L}_{p,q}/\mathbb{Q}(\sqrt{qp}))) \end{aligned}$$

where $(\mathfrak{p}, \mathrm{Gal}(\mathbb{L}_{p,q}/\mathbb{Q}(\sqrt{qp})))$ is the Frobenius of the prime $\mathfrak{p}$ in the abelian extension $\mathbb{L}_{p,q}/\mathbb{Q}(\sqrt{qp})$. Since inertial degree of a prime coincides with the order of its Frobenius, it suffices to verify that the primes over (2) in $\mathbb{Q}(\sqrt{pq})$ become trivial in the narrow class group – i.e. they have a totally positive generator – to establish Claim 3.1. Throughout we fix $(p, q) = (2, 17)$ and we set $\mathbb{L} := \mathbb{L}_{2,17}$. It is well known (see, for instance, [Coh 1980]) that $(2)\mathcal{O}_{\mathbb{Q}(\sqrt{34})} = (2, \sqrt{34})^2$: but $(2, \sqrt{34}) = (6 + \sqrt{34})$, because $2 = (6 + \sqrt{34})$ $(6 - \sqrt{34})$ while $\sqrt{34} = (6 + \sqrt{34})(-17 + 3\sqrt{34})$, and $(6 + \sqrt{34})$ is totally positive, so that $\varphi(6 + \sqrt{34}) = 1$ and Claim 3.1 is established. Actually, the same computation may be performed to show that $\mathbb{L}$ is the only field satisfying our condition, but it becomes much longer: the key point is that 34 is the only product pq of primes in our list being $\equiv -2$ modulo a perfect square.

4 A First Family

We are now ready to produce the first family of polynomials that we have mentioned in the introduction.

Proof of Theorem 1.3: For $n \in \mathbb{N}$, $n \geq 2$ we put

$$\Phi_n(X) = \prod_{m \leq n} \phi_m(X),$$

(where $\phi_m(X)$ is the *m-th* cyclotomic polynomial) and let $2s(n) = 2s$ denote its degree. An elementary estimate (see for instance [HarWri 1938], Theorem 330) gives

$$2s = \frac{3n^2}{\pi^2} + O\big(n \log n\big) \ . \tag{4.1}$$

According to Bertrand's Postulate (*op. cit.*, Theorem 418), for all n there exists a natural integer $r < s$ such that $r + s := \ell$ is a prime number: we define

$$R_n(X) = (X-1)^{2r}\Phi_n(X) \in \mathbb{Z}[X] \ .$$

Claim 4.1 *At most one cyclotomic polynomial $\phi_\nu(X) \neq X - 1$ may divide $\delta(R_n)$, in which case $n \leq \nu \leq c_1 n \log n$, where c_1 is some positive absolute constant.*

Lemma 2.4 gives $\phi_\nu \nmid R_n$ for $\nu = 2, \dots n$. On the other hand, assume $\nu > c_1 n \log n$ and let p be the smallest prime not dividing ν. Then, by elementary number theory, $p \leq c_2 \log n$ for some absolute constant $c_2 > 0$. Therefore, if c_1 is sufficiently large, $\nu/p > n$. If we had $\phi_\nu \mid \delta(R_n)$, then the polynomial $\delta(R_n)$ would have two roots $e^{2\pi i/\nu}$ and $e^{2p\pi i/\nu}$ lying on the unit circle and such that no root of R_n would lie between them all along the unit circle (since $0 < 1/\nu < p/\nu < 1/n$) , thus contradicting Lemma 2.4. By the same argument, if we had $\phi_l \phi_\nu \mid \delta(R_n)$, with $l > \nu$, we would find two roots $\{e^{2\pi i/\nu}, e^{2\pi i/l}\}$ having no root of R_n between them, which is also absurd by Lemma 2.4. Finally, again by the same Lemma, $\phi_\nu^2 \nmid \delta(R_n)$ for $\nu > n$, because of the bound for roots multiplicity of $\delta(R_n)$. Claim 4.1 is then established.

We may therefore factorise $\delta(R_n)$ as

$$\delta(R_n)(X) = (X-1)^{2r}\phi_\nu(X)^\epsilon P_n(X),$$

where $n < \nu < c_1 n \log n$ and $\epsilon \in \{0, 1\}$. Moreover, the leading coefficient $\delta(R_n)$ is equal to the prime $\ell = r + s$, and so $P_n(X)$ is an irreducible polynomial of degree d, where

$$d = 2s - \epsilon\varphi(\nu) \in \big(2s - c_1 n \log n, 2s\big] \ .$$

But $s \leq \ell < 2s$ and thus, thanks to (4.1), $\ell = d + O(\sqrt{d})$: then we have

$$\log \ell \sim \log d$$

for $n \to +\infty$. Let α_n be a root of P_n; the field

$$\mathbb{K}_n = \mathbb{Q}(\alpha_n),$$

is a CM-field (by Proposition 2.3). Moreover, since the only contribution to Weil's height of α_n (of absolute value 1) comes from the non-archimedean places and since P_n has leading coefficient ℓ,

$$h(\alpha_n) = \frac{\log \ell}{d} \sim \frac{\log d}{d}$$

(see remark 2.1).

Q.E.D.

5 A Second Family

Although the preceding construction already shows the impossibility of finding an absolute lower bound for Weil's height in non necessarily normal CM-fields (the case of a normal non-abelian CM-field being still open), we shall present a second family of polynomials which shows that also the bound given by the theorem of Dvornicich and the first author quoted in the introduction is not anymore true if the abelianity condition is dropped.

Theorem 5.1 *There exists a sequence (α_p) (p prime ≥ 5) of algebraic numbers such that:*

- *the fields $\mathbb{E}_p = \mathbb{Q}(\alpha_p)$ are CM-fields of degree $p-1$;*
- *we have $h(\alpha_p) = (\log p)/(p-1)$;*
- *$\gamma_p = 1/(\alpha_p - 1)$ is an algebraic integer, $\bar{\gamma}_p/\gamma_p = -\alpha_p$ and*

$$N_{\mathbb{Q}}^{\mathbb{E}_p}(\gamma_p) = p\ .$$

Proof : Let $p \geq 5$ be a prime number. Since $(X-1)\phi_{2p}(X)$ is antireciprocal of odd degree, Lemma 2.4 and the remarks following Definition 2.2 ensure that

$$R_p(X) := \frac{2\delta\big((X-1)\phi_{2p}(X)\big)}{X+1}\ .$$

is a polynomial with integer coefficients, not vanishing at ± 1.

Claim 5.2 *The polynomials R_p are irreducible.*

Reducing $R_p \bmod p$ is an easy task, which we can fulfill by simply pointing out that

$$\phi_{2p}(X) \equiv (X+1)^{p-1} \bmod p$$

and so

$$(p-1)(X+1)^{p-2}2\delta(X+1) \equiv 2\delta\big(\phi_{2p}(X)\big) \equiv -(X+1)^{p-2}(X-1) \bmod p\ ,$$

which finally gives

$$\begin{aligned}(X+1)R_p(X) &= 2\delta(X-1)\phi_{2p}(X) + 2(X-1)\delta\big(\phi_{2p}(X)\big)\\ &\equiv (X+1)^p - (X+1)^{p-2}(X-1)^2 \bmod p\\ &\equiv 4X(X+1)^{p-2} \bmod p\end{aligned}$$

and the factorization of $\overline{R_p[X]} \in \mathbb{F}_p[X]$ is

$$R_p(X) \equiv 4X(X+1)^{p-3} \bmod p\ . \tag{5.1}$$

Since the leading coefficient of R_p is precisely p, the irreducibility of R_p will follow as soon as we show that it has no cyclotomic factors. Indeed, let us suppose that $\phi_n(X) \mid R_p(X)$. Since $R_p(\pm 1) \neq 0$, we have $n \geq 3$; but then equation (5.1) forces the condition $\phi_n(-1) \equiv 0 \bmod p$. It is well known (see [Apo 1970]) that this condition is verified if and only if $n = 2p^m$, while $\varphi(n) = \deg(\phi_n) \leq \deg(R_p) = p-1$ implies $n = 2p$, which is absurd by Lemma 2.4. Claim 5.2 follows.

The arguments of Section 4 now imply that the polynomials R_p define CM-fields $\mathbb{E}_p$ of degree $p-1$ which contain elements α_p (the roots of $R_p(X)$) whose heights are

$$h(\alpha_p) = \frac{\log(p)}{p-1}\ .$$

We now prove that $\gamma_p = 1/(\alpha_p - 1)$ is an algebraic integer of norm p. Indeed, γ_p is a root of

$$F_p(X) = X^{p-1} R_p\Big(1 + \frac{1}{X}\Big)\ .$$

The leading coefficient of F_p is

$$\lim_{X\to+\infty} \frac{F_p(X)}{X^{p-1}} = \lim_{X\to+\infty} R_p\Big(1+\frac{1}{X}\Big) = R_p(1)\ ;$$

but we have

$$R_p(X) = \phi_{2p}(X) + 2\frac{X-1}{X+1}\delta\big(\phi_{2p}(X)\big) \Rightarrow R_p(1) = \phi_{2p}(1) = 1\ ,$$

and so $\gamma_p \in \mathcal{O}_{\mathbb{E}_p}$. Concerning its norm, we begin writing

$$R_p(X) = p\prod_{i=1}^{p-1}(X-\alpha_i)\ ;$$

then

$$N_{\mathbb{Q}}^{\mathbb{E}_p}(\gamma_p) = \prod_{i=1}^{p-1}(\alpha_i - 1)^{-1} = pR_p(1)^{-1} = p\ .$$

We finally remark that $\bar{\gamma}_p/\gamma_p = (\alpha_p - 1)/(\bar{\alpha}_p - 1) = -\alpha_p$, since $|\alpha_p| = 1$.

Q.E.D.

Remark 5.3 *The existence of the element γ_p shows that in the trivial class of the ideals class group of $\mathbb{E}_p$ there are always two primes over p. More precisely, it could be proved (using for instance the results of [DelDvoSim 2004]) that the prime p splits in the ring of integers of $\mathbb{E}_p$ as*

$$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^{p-3}$$

where $\mathfrak{p}_1 = (1/(\alpha_p - 1))$ and $\mathfrak{p}_2 = \overline{\mathfrak{p}_1} = (\alpha_p/(\alpha_p - 1))$: the fields $\mathbb{E}_p$ are therefore far from being normal over $\mathbb{Q}$.

6 A Conjecture on polynomials defining CM-fields

Let

$$\mathbf{Cycl} = \left\{\phi_1^{e_1} \cdots \phi_k^{e_k}, \text{ such that } k \in \mathbb{N} \text{ and } e_1, \ldots, e_k \in \mathbb{N}\right\}.$$

be the set of products of cyclotomic polynomials. The possibility of finding these families of CM-fields defined by polynomials in the image

$$\delta\big(\mathbf{Cycl}\big)$$

leads us to suppose that every CM-field may be otained in such a fashion. Some computations lead us to propose the following conjecture:

Conjecture 6.1 *Let $\mathbb{K}$ be a CM-field defined by a root of an irreducible polynomial $P \in \mathbb{Z}[X]$. Then there exist Φ, $\tilde{\Phi} \in$ **Cycl** and a rational r such that*

$$\delta(\Phi) = r\,\tilde{\Phi}P\ .$$

Moreover, we can perhaps choose $r = \pm 1$.

Let P as in conjecture 6.1 and assume that there exist Φ, $\tilde{\Phi} \in$ **Cycl** and a rational r such that

$$\delta(\Phi) = r\,\tilde{\Phi}P\ .$$

Let $m \in \mathbb{N}$ and put $P_m(X) = P(X^m)$, $\Phi_m(X) = \Phi(X^m)$ and $\tilde{\Phi}_m(X) = \tilde{\Phi}(X^m)$. Then the polynomial P_m defines again a CM field and

$$\delta(\Phi_m) = rm\,\tilde{\Phi}_m P_m\ ,$$

which gives some evidence to conjecture 6.1.

References

[Amo 1995] F. Amoroso, *Sur des polynômes de petites mesures de Mahler.* Comptes rendus de l'Académie des Sciences de Paris, Série I-Mathématiques **CCCXXI**, 11-14 (1995).

[AmoDvo 2000] F. Amoroso and R. Dvornicich, *A Lower Bound for the Height in Abelian Extensions.* Journal of Number Theory **LXXX**, 260-272 (2000).

[Apo 1970] T. M. Apostol, *Resultants of Cyclotomic Polynomials.* Proceedings of the American Mathematical Society **XXIV**, 457-562 (1970).

[Coh 1980] H. Cohn, *Advanced Number Theory.* Dover Publications, New York, 1980.

[DelDvoSim 2004] I. Del Corso, R. Dvornicich and D. Simon, *Decomposition of Primes in Nonmaximal Orders.* Rapport de recherche 2004-14. Laboratoire LMNO, CNRS, UMR 6139, Université de Caen.

[HarWri 1938] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers.* Oxford Science Publications - Oxford University Press, Oxford, 1938.

[LouOka 1994] S. Louboutin and R. Okazaki, *Determination of All Non-Normal Quartic CM-fields and of All Non-Abelian Normal Octic CM-fields with Class Number One.* Acta Arithmetica **LXVII**, 47-62 (1994).

[Nuc 2004] F. A. E. Nuccio, *Minorazione dell'altezza di Weil in campi di numeri abeliani e CM.* Master Thesis, Università di Torino, 2004.

[Sch 1973] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number.* Acta Arithmetica **XXIV**, 385-399 (1973).

[Wal 2000] M. Waldschimdt, *Diophantine Approximation on Linear Algebraic Groups.* Springer-Verlag, New York, 2000.

[Was 1982] L. C. Washington, *Introduction to Cyclotomic Fields.* Springer-Verlag, New York, 1982.