Publ. Math. Debrecen
89/4 (2016), 513–523
DOI: 10.5486/PMD.2016.7801

On some norm inequalities and discriminant inequalities in CM-fields

By KÁLMÁN GYŐRY (Debrecen)

To the memory of Professor A. Kertész

Abstract. This is a shortened and slightly modified English version of our paper "Sur une classe des corps de nombres algébriques et ses applications", published in this journal in 1975; see Győry [10]. In that paper we studied an important class of number fields, namely the totally imaginary quadratic extensions of totally real number fields. We obtained among others some new norm inequalities and discriminant inequalities in such number fields. That time several different names were used in the literature for these number fields. This is the reason that the title of Győry [10] is not informative enough. Probably it is partly due to this fact that the results of [10] are less known. Nowadays, the name CM-field is generally accepted for the number fields under consideration. The purpose of this paper is to better call the attention to our norm inequalities and discriminant inequalities in CM-fields and to their applications.

1. Introduction

In 1975, we investigated in [10] some arithmetical properties of totally imaginary quadratic extensions of totally real number fields. We collected some known and proved some new characterizations of these fields, established some new norm inequalities and discriminant inequalities in such fields, and presented some applications. At that time there was not yet a generally accepted name for this class of

Mathematics Subject Classification: 11R06,11R21,11R99.
Key words and phrases: CM-field, characterization, norm, discriminant of algebraic number, inequalities.
The author is supported by the OTKA grants 104208 and 115479.

number fields. For example, they were called in [23] fields with "Einheitsdefekt", cf. also [22], [4], in [7] "allowed" fields, in [8], [9] and later in [24] "kroneckerien" (in English "Kroneckerian") or "K-corps", in [6], [3] and later in [5], [16] J-fields*, and in many works CM-fields, see, e.g., Shimura and Taniyama [26], Shimura [25], Washington [27], Narkiewicz [19]. By now, the name CM-field has become accepted.

With this shortened, English version of [10], we should like to make more known the results of [10], especially the norm inequalities and discriminant inequalities. In Section 2, the characterizations of CM-fields from [10] are presented without proof, in Sections 3, 4 and 5, the norm and discriminant inequalities are restated with proofs. Some earlier and recent applications are also mentioned.

For other properties of CM-fields, we refer to Shimura and Taniyama [26], Shimura [25], Győry [10], Washington [27], Narkiewicz [19], Okazaki [20], and the references given there.

2. Characterizations of CM-fields

In this section we present those characterizations of CM-fields which were published in Győry [10]. Some of them were already well-known, the others were published in [10] for the first time.

For an algebraic number field K, denote by K_0 its maximal real subfield, and by $K\psi$ or $\overline{K}$ its complex conjugate in $\mathbb{C}$. Similarly, the complex conjugate of $\alpha \in K$ will be denoted by $\alpha\psi$ or $\overline{\alpha}$. If K is non-real and $\overline{K} = K$, K is a quadratic extension of K_0.

We shall use the following notation. Let $E^{(r)}_{K/\mathbb{Q}}(\alpha)$ be the elementary symmetric function of degree r of the conjugates of $\alpha \in K$ relative to $K/\mathbb{Q}$. In particular, $E^{(1)}_{K/\mathbb{Q}}(\alpha) = Tr_{K/\mathbb{Q}}(\alpha)$ and $E^{(n)}_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\alpha)$, where n denotes the degree of K over $\mathbb{Q}$. We note that $E^{(r)}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$ for each r with $1 \le r \le n$, and if α is integer in K, then $E^{(r)}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Theorem 1. *For a non-real algebraic number field K of degree n, the following assertions are equivalent:*

(a) K is a totally imaginary quadratic extension of a totally real number field;

(b) $K\psi = K$ and $\sigma\psi = \psi\sigma$ for each $\mathbb{Q}$-isomorphism σ of K in $\mathbb{C}$;

*In some papers totally real number fields are also included in the definitions.

(c) there exists an algebraic number field $F \supseteq K$ such that the extensions ${}^{F}/_{\mathbb{Q}}$ and ${}^{F_0}/_{\mathbb{Q}}$ are normal;

(d) $\overline{K} = K$ and there exists a constant $0 < c \leq 1$ such that

$$|N_{K/\mathbb{Q}}(\alpha)| \geq c \min\{|N_{K/\mathbb{Q}}(\operatorname{Re}\alpha)|, |N_{K/\mathbb{Q}}(i \operatorname{Im}\alpha)|\}$$

for all $\alpha \in K$;

(e) $\overline{K} = K$, and for an r with $1 \leq r < n$ and for all non-zero $\alpha \in K$

$$E^{(r)}_{K/\mathbb{Q}}(\alpha\overline{\alpha}) > 0;$$

(f) $\overline{K} = K$, and for every unit ε in K, $\overline{\varepsilon} = \zeta\varepsilon$ with a root of unity $\zeta \in K$;

(g) $\overline{K} = K$ and $[U : \{V, U_0\}] \leq 2$, where U, U_0 denote the unit groups of K and K_0 respectively, and V is the group of roots of unity in K.

We note that among the assertions (a),…,(g) several implications were already known before Győry [10]. Namely, the implication (a)⇒(e) is trivial, (a)⇔(b) was well-known. For (a)⇔(g), see [15], [23], [22], for (g)⇒(f) [23] and [4], for (e)⇒(a) (with $r = 1$) [25], and for (c)⇒(d), see [7]. The implications (e)⇒(b)⇒(c)⇒(a) and (d)⇒(f)⇒(g)⇒(a) were proved in Győry [10], which completed the proof of equivalence of (a),…,(g).

For a latter characterization, see [2]. See also [18] and [21].

In Győry [10], (f) and (g) are considered in a more general case, for S-units, where S is a finite set of places of K containing all infinite places, and each finite place in S is "real" in the sense defined in [10].

The following consequence of Theorem 1 is frequently needed in applications. For a proof, see Győry [10].

Corollary 1.1. *Let K_i be a totally real number field or a totally imaginary quadratic extension of a totally real number field for $i = 1, \ldots, m$. The subfields, intersections and composits of these fields are also of this type.*

3. Norm inequalities

Let K be a number field of degree n. As above, for $\alpha \in K$ we denote by $E^{(r)}_{K/\mathbb{Q}}(\alpha)$ the elementary symmetric function of degree r of the conjugates of α relative to ${}^{K}/_{\mathbb{Q}}$. We recall that if K is a CM-field, then $E^{(r)}_{K/\mathbb{Q}}(\alpha\overline{\alpha}) > 0$ for all $1 \leq r \leq n$ and for all non-zero $\alpha \in K$.

Theorem 2. *Let K be a CM-field of degree n, and let $\alpha_1, \dots, \alpha_k$ be non-zero elements of K with $k \geq 2$. Then*

$$\left\{E^{(r)}_{K/\mathbb{Q}}(\alpha_1\overline{\alpha_1} + \cdots + \alpha_k\overline{\alpha_k})\right\}^{1/r} \geq \sum_{i=1}^{k} \left\{E^{(r)}_{K/\mathbb{Q}}(\alpha_i\overline{\alpha_i})\right\}^{1/r} \quad \text{for } r = 1, \dots, n. \tag{1}$$

Further, equality holds if and only if $r = 1$ or $\alpha_i\overline{\alpha_i} = \lambda_i\alpha_1\overline{\alpha_1}$ with some $\lambda_i \in \mathbb{Q}$, $i = 1, \dots, k$.

Since $E^{(n)}_{K/\mathbb{Q}} = N_{K/\mathbb{Q}}$ and $N_{K/\mathbb{Q}}(\alpha_i\overline{\alpha_i}) = N^2_{K/\mathbb{Q}}(\alpha_i)$ for $i = 1, \dots, k$, Theorem 2 gives immediately the following.

Corollary 2.1. *Under the assumptions of Theorem 2, we have*

$$\left\{N_{K/\mathbb{Q}}(\alpha_1\overline{\alpha_1} + \cdots + \alpha_k\overline{\alpha_k})\right\}^{1/n} \geq \sum_{i=1}^{k} \left\{N^{2}_{K/\mathbb{Q}}(\alpha_i)\right\}^{1/n}.$$

Further, equality holds if and only if $\alpha_i\overline{\alpha_i} = \lambda_i\alpha_1\overline{\alpha_1}$ with some positive $\lambda_i \in \mathbb{Q}$, $i = 1, \dots, k$.

From this Corollary one can deduce the next theorem.

Theorem 3. *Let K be a CM-field of degree n. Then, for all non-zero $\alpha \in K$,*

$$\left\{N^{2}_{K/\mathbb{Q}}(\alpha)\right\}^{1/n} \geq \left\{N^{2}_{K/\mathbb{Q}}(\operatorname{Re}\alpha)\right\}^{1/n} + \left\{N^{2}_{K/\mathbb{Q}}(i\operatorname{Im}\alpha)\right\}^{1/n}. \tag{2}$$

The equality holds only if at least one of $\operatorname{Re}\alpha = 0$, $i\operatorname{Im}\alpha = 0$, or $\left(\frac{\operatorname{Re}\alpha}{i\operatorname{Im}\alpha}\right)^2 \in \mathbb{Q}$ hold.

We present a consequence of Theorem 3.

Corollary 3.1. *Let K be a CM-field, and let α, β be non-zero integers in K such that α/β is not real and $\alpha + \beta$ is real or purely imaginary. Then*

$$N_{K/\mathbb{Q}}\left(\frac{\alpha + \beta}{2}\right) \leq N_{K/\mathbb{Q}}(\alpha\beta). \tag{3}$$

The equality holds if and only if α/β is purely imaginary, and (i) $\alpha - \overline{\alpha}$ and $\beta - \overline{\beta}$ are units when $\alpha + \beta$ is real, or (ii) $\alpha + \overline{\alpha}$ and $\beta + \overline{\beta}$ are units when $\alpha + \beta$ is purely imaginary.

For the above α, β, (3) implies the inequality

$$N_{K/\mathbb{Q}}\left(\frac{\alpha + \beta}{2}\right) \leq \frac{N^{2}_{K/\mathbb{Q}}(\alpha) + N^{2}_{K/\mathbb{Q}}(\beta)}{2}.$$

The above norm inequalities were applied in Győry and Lovász [7], Győry [11], and Aubry and Poulakis [1] to diophantine equations, and in Győry [8], [9], [10], [12], [13], Schinzel [24], and Győry, Hajdu and Tijdeman [14] to irreducible polynomials.

4. Discriminant inequalities

For a non-rational algebraic number α, we denote by $D(\alpha)$ the discriminant of α relative to the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. Further, for number fields K, K' with $K \supset K'$ and $K = K'(\alpha)$, $D_{K/K'}(\alpha)$ will denote the discriminant of α relative to the extension K/K'. For $K' = K$, we put $D_{K/K} = 1$.

Theorem 4. *Let α be an algebraic number of degree $n \geq 2$. Suppose that $K = \mathbb{Q}(\alpha)$ is a CM-field, and that the degrees $k = [K' : \mathbb{Q}]$ and $\ell = [K'' : \mathbb{Q}]$ of $K' = \mathbb{Q}(\operatorname{Re}\alpha)$ and $K'' = \mathbb{Q}(i \operatorname{Im}\alpha)$ are greater than 1. Then*

$$|D(\alpha)|^{2/n} \geq |D(\operatorname{Re}\alpha)^{(n/k)^2} N_{K'/\mathbb{Q}}(D_{K/K'}(\alpha))|^{2/n} + |D(i \operatorname{Im}\alpha)^{(n/\ell)^2} N_{K''/\mathbb{Q}}(D_{K/K''}(\alpha))|^{2/n}, \tag{4}$$

and equality holds if and only if $k = \ell = 2$.

The trivial cases $k = 1$ and $\ell = 1$ are excluded. Then, for $k = 1$, we have $\operatorname{Re}\alpha \in \mathbb{Q}$ and $D(i \operatorname{Im}\alpha) = D(\alpha)$, and, for $\ell = 1$, $i \operatorname{Im}\alpha = 0$ and $D(\operatorname{Re}\alpha) = D(\alpha)$.

The next Corollary is an immediate consequence of Theorem 4.

Corollary 4.1. *Under the assumptions of Theorem 4, we have*

$$|D(\alpha)|^{2/n} \geq |D(\operatorname{Re}\alpha)|^{2n/k^2} + |D(i \operatorname{Im}\alpha)|^{2n/\ell^2},$$

subject to the condition that α is an algebraic integer.

For an algebraic integer α satisfying the assumptions of Theorem 4, denote by D_K, $D_{K'}$ and $D_{K''}$ the discriminant of K, K' and K'', respectively. Let $I(\alpha)$ denote the index of α in the ring of integers O_K of K, that is $I(\alpha) = [O_K : \mathbb{Z}[\alpha]]$. As is known, $D(\alpha) = I^2(\alpha) D_K$.

Corollary 4.2. *Under the notation and assumptions of Theorem 4, suppose that α, $\operatorname{Re}\alpha$ and $i \operatorname{Im}\alpha$ are algebraic integers. Then we have*

$$|D(\alpha)|^{2/n} \geq |D_K|^{2/n} \left\{ |D_{K'}|^{\frac{2(n-k)}{k^2}} + |D_{K''}|^{\frac{2(n-\ell)}{\ell^2}} \right\} \tag{5}$$

and

$$I(\alpha)^{4/n} \geq |D_{K'}|^{\frac{2(n-k)}{k^2}} + |D_{K''}|^{\frac{2(n-\ell)}{\ell^2}}. \tag{6}$$

The inequality (6) gives a lower bound for $I(\alpha)$. In particular, it follows that $I(\alpha) \geq |D_{K'}|$ if $n \geq 2k$, and $I(\alpha) \geq |D_{K''}|$ if $n \geq 2\ell$. But under the assumptions of Corollary 4.2, we have $|D_{K'}| \geq 5$ and $|D_{K''}| \geq 3$. This implies that in these cases α cannot be a ring generator of O_K over $\mathbb{Z}$, i.e. $\{1, \alpha, \ldots, \alpha^{n-1}\}$ cannot be a power integral basis in O_K.

Further consequences of Theorem 4 can be found in Győry [10].

5. Proofs

To prove Theorem 2, we shall need the following lemma, due to Marcus and Lopez [17]. For $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{R}^n$, we denote by $E_r(\mathbf{a})$ the elementary symmetric function of degree r of the coordinates of $\mathbf{a}$.

Lemma. *Let $\mathbf{a_1} = (a_{11}, \dots, a_{1n})$, $\mathbf{a_2} = (a_{21}, \dots, a_{2n}) \in \mathbb{R}^n$ with positive coordinates. Then*

$$\Big\{E_r(\mathbf{a_1} + \mathbf{a_2})\Big\}^{1/r} \geq \Big\{E_r(\mathbf{a_1})\Big\}^{1/r} + \Big\{E_r(\mathbf{a_2})\Big\}^{1/r}, \quad r = 1, \dots, n.$$

The equality holds only if $r = 1$ or $\mathbf{a_2} = \lambda \mathbf{a_1}$ with some positive real λ.

Proof. See Marcus and Lopez [17]. □

Proof of Theorem 2. If $\mathbf{a_1}, \dots, \mathbf{a_k} \in \mathbb{R}^n$ with positive coordinates, the Lemma implies

$$\Big\{E_r(\mathbf{a_1} + \dots + \mathbf{a_k})\Big\}^{1/r} \geq \sum_{i=1}^{k} \Big\{E_r(\mathbf{a_i})\Big\}^{1/r} \tag{7}$$

for $r = 1, \dots, n$. Further, in (7) equality holds if and only if $r = 1$ or $\mathbf{a_i} = \lambda_i \mathbf{a_1}$ with some positive reals λ_i, $i = 1, \dots, k$.

Let K_0 be the maximal real subfield of K. By Theorem 1, K_0 is totally real. Further, if $\alpha_i \in K$, it follows that $\alpha_i \overline{\alpha_i} \in K_0$ for $i = 1, \dots, k$. We infer that

$$(\alpha_i \overline{\alpha_i})\sigma = \left(\frac{\alpha_i + \overline{\alpha_i}}{2}\right)^2 \sigma - \left(\frac{\alpha_i - \overline{\alpha_i}}{2}\right)^2 \sigma, \quad i = 1, \dots, k, \tag{8}$$

for each $\mathbb{Q}$-isomorphism σ of K in $\mathbb{C}$. The $\frac{\alpha_i + \overline{\alpha_i}}{2}$ is totally real, hence we have

$$\left(\frac{\alpha_i + \overline{\alpha_i}}{2}\right)^2 \sigma = \left[\left(\frac{\alpha_i + \overline{\alpha_i}}{2}\right)\sigma\right]^2 \geq 0, \quad i = 1, \dots, k. \tag{9}$$

Further, $\frac{\alpha_i - \overline{\alpha_i}}{2}$ and its conjugates are purely imaginary, whence

$$-\left(\frac{\alpha_i - \overline{\alpha_i}}{2}\right)^2 \sigma = -\left[\left(\frac{\alpha_i - \overline{\alpha_i}}{2}\right)\sigma\right]^2 \geq 0, \quad i = 1, \dots, k. \tag{10}$$

Consequently, (8), (9) and (10) imply that $\alpha_i \overline{\alpha_i}$ is totally positive for $i = 1, \dots, k$. Denoting by $\mathbf{a_i}$ the vector whose coordinates are the conjugates of $\alpha_i \overline{\alpha_i}$, we obtain $E^{(r)}_{K/\mathbb{Q}}(\alpha_i \overline{\alpha_i}) > 0$ for $1 \leq r \leq n$ and $1 \leq i \leq k$. Further, (7) gives (1), where equality holds if and only if $r = 1$ or

$$\left(\frac{\alpha_i \overline{\alpha_i}}{\alpha_1 \overline{\alpha_1}}\right)\sigma = \frac{(\alpha_i \overline{\alpha_i})\sigma}{(\alpha_1 \overline{\alpha_1})\sigma} = \lambda_i, \quad i = 1, \dots k,$$

for all σ, whence $\alpha_i \overline{\alpha_i} = \lambda_i \alpha_1 \overline{\alpha_1}$ with $\lambda_i \in \mathbb{Q}$, $i = 1, \dots, k$. □

Proof of Theorem 3. By assumption, K is a CM-field. Hence, if α is a non-zero element of K, $\operatorname{Re}\alpha$ is totally real, $i\operatorname{Im}\alpha \in K$, and, if $i\operatorname{Im}\alpha \neq 0$, then its conjugates are all purely imaginary. We apply Corollary 2.1 with the choice $k = 2$, $\alpha_1 = \operatorname{Re}\alpha$, and $\alpha_2 = i\operatorname{Im}\alpha$. Then $\alpha_1\overline{\alpha_1} + \alpha_2\overline{\alpha_2} = \alpha\overline{\alpha}$, and in view of $N_{K/\mathbb{Q}}(\alpha\overline{\alpha}) = N^2_{K/\mathbb{Q}}(\alpha)$, we deduce (2). If $\operatorname{Re}\alpha = 0$ of $i\operatorname{Im}\alpha = 0$, then clearly equality holds in (2). If $\operatorname{Re}\alpha$ and $i\operatorname{Im}\alpha$ are different from zero, then by Corollary 2.1 equality holds if and only if $\alpha_2\overline{\alpha_2} = \lambda\alpha_1\overline{\alpha_1}$, that is if $\left(\frac{\operatorname{Re}\alpha}{i\operatorname{Im}\alpha}\right)^2 = -\lambda^{-1} \in \mathbb{Q}$. □

Proof of Corollary 3.1. Put $\gamma := \alpha + \beta$. First suppose that γ is real. Since, by assumption, α/β is not real, we have $\gamma \neq 0$ and neither α nor β is real. Further, it follows that $\gamma = \overline{\alpha} + \overline{\beta}$ and

$$\begin{aligned} 2i\operatorname{Im}\alpha\overline{\beta} &= \alpha\overline{\beta} - \overline{\alpha}\beta = (\alpha+\beta)\overline{\beta} - (\overline{\alpha}+\overline{\beta})\beta \\ &= \gamma\overline{\beta} - \gamma\beta = \gamma(\overline{\beta} - \beta) = -2\gamma i\operatorname{Im}\beta \in K. \end{aligned}$$

Since α and β are non-zero integers in K, we infer that $\beta - \overline{\beta} = 2i\operatorname{Im}\beta$ is a non-zero integer in K. Using Theorem 3, we deduce that

$$\begin{aligned} \mathrm{N}_{K/\mathbb{Q}}(\alpha+\beta) = N_{K/\mathbb{Q}}(\gamma) &\leq N_{K/\mathbb{Q}}(\gamma\cdot 2i\operatorname{Im}\beta) = N_{K/\mathbb{Q}}(2i\operatorname{Im}\alpha\overline{\beta}) \\ &\leq N_{K/\mathbb{Q}}(2\alpha\overline{\beta}) = N_{K/\mathbb{Q}}(2)N_{K/\mathbb{Q}}(\alpha\beta), \end{aligned}$$

whence we get (3). Further, in this case equality holds if and only if $\operatorname{Re}\alpha\overline{\beta} = 0$ and $2i\operatorname{Im}\beta = \beta - \overline{\beta}$, as well as, by symmetry, $\alpha - \overline{\alpha}$ are units in K. But it is easy to see that $\operatorname{Re}\alpha\overline{\beta} = 0$ if and only if α/β is purely imaginary, which proves our assertion when γ is real.

Consider now the case when $\gamma = \alpha+\beta$ is purely imaginary. Then $\overline{\alpha}+\overline{\beta} = -\gamma$, and α/β being not real, we deduce that $\operatorname{Re}\alpha \neq 0$, $\operatorname{Re}\beta \neq 0$. Further, we have

$$\begin{aligned} 2i\operatorname{Im}\alpha\overline{\beta} &= \alpha\overline{\beta} - \overline{\alpha}\beta = (\alpha+\beta)\overline{\beta} - (\overline{\alpha}+\overline{\beta})\beta \\ &= \gamma\overline{\beta} + \gamma\beta = \gamma(\beta + \overline{\beta}) = \gamma\cdot 2\operatorname{Re}\beta, \end{aligned}$$

where $2\operatorname{Re}\beta = \beta + \overline{\beta}$ is integer in K. Using again Theorem 3, it follows that

$$\begin{aligned} N_{K/\mathbb{Q}}(\alpha+\beta) = N_{K/\mathbb{Q}}(\gamma) &\leq N_{K/\mathbb{Q}}(\gamma\cdot 2\operatorname{Re}\beta) = N_{K/\mathbb{Q}}(2i\operatorname{Im}\alpha\overline{\beta}) \\ &\leq N_{K/\mathbb{Q}}(2\alpha\overline{\beta}) = N_{K/\mathbb{Q}}(2)N_{K/\mathbb{Q}}(\alpha\beta), \end{aligned}$$

which implies (3). Further, equality holds if and only if $\operatorname{Re}\alpha\overline{\beta} = 0$ and $2\operatorname{Re}\beta = \beta + \overline{\beta}$, as well as, similarly, $\alpha + \overline{\alpha}$ are units in K. But, as above, $\operatorname{Re}\alpha\overline{\beta} = 0$ if and only if α/β is purely imaginary. This completes the proof. □

For a non-rational algebraic number α, we denote by $\delta(\alpha)$ the different of α relative to the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. If K, K' are number fields with $K \supset K'$ and $K = K'(\alpha)$, $\delta_{K/K'}(\alpha)$ will denote the different of α relative to K/K'.

Proof of Theorem 4. Let $\varphi_1, \dots, \varphi_n$ be the distinct $\mathbb{Q}$-isomorphisms of $K = \mathbb{Q}(\alpha)$ in $\mathbb{C}$ with $\alpha\varphi_1 = \alpha$. Then the different of α is

$$\delta(\alpha) = (\alpha - \alpha\varphi_2) \cdots (\alpha - \alpha\varphi_n),$$

and its discriminant

$$D(\alpha) = D_{K/\mathbb{Q}}(\alpha) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(\delta(\alpha)). \tag{11}$$

By Theorem 1, we have

$$2\,\mathrm{Re}(\alpha\varphi_j) = \alpha\varphi_j + \overline{\alpha\varphi_j} = (\alpha + \overline{\alpha})\varphi_j = 2(\mathrm{Re}\,\alpha)\varphi_j \text{ for } j = 1, \dots, n,$$

and similarly for $i\,\mathrm{Im}\,\alpha$. Let L be the normal closure of K over $\mathbb{Q}$, and let $[L : \mathbb{Q}] = N$. By Theorem 1 and Corollary 1.1, L is also a CM-field, and it follows from (11) and Theorem 3 that

$$\begin{aligned} |D(\alpha)|^{2/n} &= |D(\alpha)|^{\frac{2[L:K]}{N}} = |N_{L/\mathbb{Q}}((\alpha - \alpha\varphi_2) \cdots (\alpha - \alpha\varphi_n))|^{2/N} \\ &= \prod_{j=2}^{n} |N_{L/\mathbb{Q}}(\alpha - \alpha\varphi_j)|^{2/N} \geq \prod_{j=2}^{n} \Big\{ |N_{L/\mathbb{Q}}(\mathrm{Re}\,\alpha - (\mathrm{Re}\,\alpha)\varphi_j)|^{2/N} \\ &\quad + |N_{L/\mathbb{Q}}(i\,\mathrm{Im}\,\alpha - (i\,\mathrm{Im}\,\alpha)\varphi_j)|^{2/N} \Big\}. \end{aligned} \tag{12}$$

Since $\mathrm{Re}\,\alpha$ is real in K, its degree k over $\mathbb{Q}$ is less than n. Among the numbers $\mathrm{Re}\,\alpha$, $(\mathrm{Re}\,\alpha)\varphi_2, \dots, (\mathrm{Re}\,\alpha)\varphi_n$, k is distinct, and each of them occurs n/k times (and similarly for $i\,\mathrm{Im}\,\alpha, \dots, (i\,\mathrm{Im}\,\alpha)\varphi_n$, with multiplicity n/ℓ). Denote by $\delta(\mathrm{Re}\,\alpha)$ the different of $\mathrm{Re}\,\alpha$, and consider the product of those terms $N_{L/\mathbb{Q}}(\mathrm{Re}\,\alpha - (\mathrm{Re}\,\alpha)\varphi_j)$, $j = 2, \dots, n$, which are different from zero in (12). Then we have

$$\begin{aligned} \prod_{\varphi_j;\mathrm{Re}\,\alpha \neq (\mathrm{Re}\,\alpha)\varphi_j} |N_{L/\mathbb{Q}}(\mathrm{Re}\,\alpha - (\mathrm{Re}\,\alpha)\varphi_j)| &= |N_{L/\mathbb{Q}}(\delta(\mathrm{Re}\,\alpha))^{n/k}| \\ &= |N_{K'/\mathbb{Q}}(\delta(\mathrm{Re}\,\alpha))|^{[L:K']\frac{n}{k}} = |D(\mathrm{Re}\,\alpha)|^{nN/k^2}. \end{aligned} \tag{13}$$

Consider now in (12) the product of those terms $N_{L/\mathbb{Q}}(i\,\mathrm{Im}\,\alpha - (i\,\mathrm{Im}\,\alpha)\varphi_j)$ for which $\mathrm{Re}\,\alpha = (\mathrm{Re}\,\alpha)\varphi_j$, $2 \leq j \leq n$. The number of these φ is $n/k - 1$; suppose that $\varphi_2, \dots, \varphi_{n/k}$ are these $\mathbb{Q}$-isomorphisms. Since $i\,\mathrm{Im}\,\alpha \in K$ and $\mathbb{Q}(i\,\mathrm{Im}\,\alpha, \mathrm{Re}\,\alpha) =$

K, we infer that $i\,\mathrm{Im}\,\alpha$ is of degree n/k over K'. But $\varphi_1,\dots,\varphi_{n/k}$ leave the elements of K' fixed, and $(i\,\mathrm{Im}\,\alpha)\varphi_1 = i\,\mathrm{Im}\,\alpha,\dots,(i\,\mathrm{Im}\,\alpha)\varphi_{n/k}$ are pairwise distinct. Hence these numbers are the conjugates of $i\,\mathrm{Im}\,\alpha$ over K'. Therefore, we obtain that

$$\begin{aligned}\prod_{\varphi;\mathrm{Re}\,\alpha=(\mathrm{Re}\,\alpha)\varphi} |N_{L/\mathbb{Q}}(i\,\mathrm{Im}\,\alpha-(i\,\mathrm{Im}\,\alpha)\varphi)| &= \prod_{j=2}^{n/k} |N_{L/\mathbb{Q}}(i\,\mathrm{Im}\,\alpha-(i\,\mathrm{Im}\,\alpha)\varphi_j)|\\ &= |N_{L/\mathbb{Q}}(\delta_{K/K'}(i\,\mathrm{Im}\,\alpha))| = |N_{K'/\mathbb{Q}}(N_{L/K'}(\delta_{K/K'}(i\,\mathrm{Im}\,\alpha)))|\\ &= |N_{K'/\mathbb{Q}}(N_{K/K'}(\delta_{K/K'}(i\,\mathrm{Im}\,\alpha))^{[L:K]})|\\ &= |N_{K'/\mathbb{Q}}(D_{K/K'}(i\,\mathrm{Im}\,\alpha))|^{N/n}. \qquad (14)\end{aligned}$$

We repeat this procedure for $i\,\mathrm{Im}\,\alpha$ and $\mathrm{Re}\,\alpha$ as well. If there exists a φ_j such that $(\mathrm{Re}\,\alpha)\varphi_j \neq \mathrm{Re}\,\alpha$ and $(i\,\mathrm{Im}\,\alpha)\varphi_j \neq i\,\mathrm{Im}\,\alpha$, then it follows from (12), (13) and (14) that

$$\begin{aligned}|D(\alpha)|^{2/n} \geq{}& |D(\mathrm{Re}\,\alpha)|^{\frac{2n}{k^2}}|N_{K'/\mathbb{Q}}(D_{K/K'}(i\,\mathrm{Im}\,\alpha))|^{2/n}\\ &+ |D(i\,\mathrm{Im}\,\alpha)|^{\frac{2n}{\ell^2}}\cdot|N_{K''/\mathbb{Q}}(D_{K/K''}(\mathrm{Re}\,\alpha))|^{2/n}.\end{aligned}$$

Because $D_{K/K'}(i\,\mathrm{Im}\,\alpha) = D_{K/K'}(\alpha)$ and $D_{K/K''}(\mathrm{Re}\,\alpha) = D_{K/K''}(\alpha)$, in this case (4) is proved.

It remains the case when, for each j, $(\mathrm{Re}\,\alpha)\varphi_j = \mathrm{Re}\,\alpha$ or $(i\,\mathrm{Im}\,\alpha)\varphi_j = i\,\mathrm{Im}\,\alpha$. But the number of $\mathbb{Q}$-isomorphisms which leave $\mathrm{Re}\,\alpha$ resp. $i\,\mathrm{Im}\,\alpha$ fixed is n/k resp. n/ℓ. Consequently, the number of $\mathbb{Q}$-ismorphisms leaving at least one of $\mathrm{Re}\,\alpha$ and $i\,\mathrm{Im}\,\alpha$ fixed is at most $\frac{n}{k}+\frac{n}{\ell}-1$, hence $n \leq \frac{n}{k}+\frac{n}{\ell}-1$, and so $1+\frac{1}{n} \leq \frac{1}{k}+\frac{1}{\ell}$. Since, by assumption, $k,\ell > 1$, we arrived at a contradiction.

The above argument and Theorem 3 imply that in (4) equality occurs if and only if $(\mathrm{Re}\,\alpha)\varphi_j \neq \mathrm{Re}\,\alpha$ and $(i\,\mathrm{Im}\,\alpha)\varphi_j \neq i\,\mathrm{Im}\,\alpha$ do not hold at the same time only for one j, and if, for this j, $\left(\frac{\mathrm{Re}(\alpha-\alpha\varphi_j)}{i\,\mathrm{Im}(\alpha-\alpha\varphi_j)}\right)^2 \in \mathbb{Q}$. In this case, the number of isomorphisms φ_j which leave at least one of $\mathrm{Re}\,\alpha$ and $i\,\mathrm{Im}\,\alpha$ fixed is $n-1 \leq \frac{n}{k}+\frac{n}{\ell}-1$, whence $1 \leq \frac{1}{k}+\frac{1}{\ell}$, and finally $k=\ell=2$, $n=4$. Conversely, suppose that $\alpha = \mathrm{Re}\,\alpha + i\,\mathrm{Im}\,\alpha$, where $\mathrm{Re}\,\alpha$ and $i\,\mathrm{Im}\,\alpha$ are quadratic algebraic numbers. Then $K = \mathbb{Q}(\alpha)$ is a CM-field which satisfies the conditions of the theorem with $n=4$ and $k=\ell=2$. Further, it is easy to see that in (4) equality holds. □

Proof of Corollary 4.2. Let $D_{K/K'}$ and $D_{K/K''}$ denote the relative discriminant of K over K' and K'', respectively (with the convention that $D_{K/K}=1$).

Then $D_{K/K'}$ divides $D_{K/K'}(\alpha)$, and $D_{K/K''}$ divides $D_{K/K''}(\alpha)$ in the ring of integers of K' resp. of K'', and $D_{K'} \mid D(\mathrm{Re}\,\alpha)$, $D_{K''} \mid D(i\,\mathrm{Im}\,\alpha)$ in $\mathbb{Z}$. In view of the transitivity formula

$$D_K = N_{K'/\mathbb{Q}}(D_{K/K'})D_{K'}^{[K:K']} = N_{K''/\mathbb{Q}}(D_{K/K''})D_{K''}^{[K:K'']},$$

hence (4) implies (5), whence (6) immediately follows. □

References

[1] Y. Aubry and D. Poulakis, Thue equations and CM-fields, *Ramanujan J.* (2016), DOI: 10.1007/s11139-015-9749-x.

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

[3] A. Candiotti, Computations of Iwasawa invariants and K_2, *Compositio Math.* **29** (1974), 89–111.

[4] P. Dénes, Über Einheiten von algebraischen Zahlkörpern, *Monatsh. Math.* **55** (1951), 161–163.

[5] V. Ennola, J-fields generated by roots of cyclotomic integers, *Mathematika* **25** (1978), 242–250.

[6] R. Gold, The nontriviality of certain $\mathbb{Z}_\ell$-extensions, *J. Number Theory* **6** (1974), 369–373.

[7] K. Győry and L. Lovász, Representation of integers by norm forms II., *Publ. Math. Debrecen* **17** (1970), 173–181.

[8] K. Győry, Sur l'irréductibilité d'une classe des polynômes I., *Publ. Math. Debrecen* **18** (1971), 289–307.

[9] K. Győry, Sur l'irréductibilité d'une classe des polynômes II., *Publ. Math. Debrecen* **19** (1972), 293–326.

[10] K. Győry, Sur une classe des corps de nombres algébriques et ses applications, *Publ. Math. Debrecen* **22** (1975), 151–175.

[11] K. Győry, Représentation des nombres entiers par des formes binaires, *Publ. Math. Debrecen* **24** (1977), 363–375.

[12] K. Győry, On the irreducibility of a class of polynomials III., *J. Number Theory* **15** (1982), 164–181.

[13] K. Győry, On the irreducibility of a class of polynomials IV., *Acta Arith.* **62** (1992), 399–405.

[14] K. Győry, L. Hajdu and R. Tijdeman, Irreducibility criteria of Schur-type and Pólya-type, *Monatsh. Math.* **163** (2011), 415–443.

[15] E. Hecke, Bestimmung der Klassenzahl einer neuen Reihe von algebraischen Zahlkörpern, *Nachr. Akad. Wiss. Göttingen, Math.-Phys. Klasse* **1921** (1921), 1–23.

[16] C. W. Lloyd-Smith, On minimal diameters of algebraic integers in J-fields, *J. Number Theory* **21** (1985), 299–318.

[17] M. Marcus and L. Lopez, Inequalities for symmetric functions and Hermitian matrices, *Canad. J. Math.* **9** (1957), 305–312.

[18] C. R. MacCluer and C. J. Parry, Units of modulus 1, *J. Number Theory* **7** (1975), 317–375.

[19] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Second edition, *Springer-Verlag*, *Berlin*, 1990.

[20] R. Okazaki, Inclusion of CM-fields and divisibility of relative class numbers, *Acta Arith.* **92** (2000), 319–338.

[21] C. J. Parry, Units of algebraic number fields *J. Number Theory* **7** (1975), 385–388; Corrigendum, *ibid.* **9** (1977), 278.

[22] R. Remak, Über Größenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers, *Compositio Math.* **10** (1952), 245–285.

[23] R. Remak, Über algebraische Zahlkörper mit schwachem Einheitsdefekt, *Compositio Math.* **12** (1954), 35–80.

[24] A. Schinzel, Polynomials With Special Regard to Reducibility, With an appendix by Umberto Zannier, Encyclopedia of Mathematics and its Applications, Vol. **77**, *Cambridge University Press*, *Cambridge*, 2000.

[25] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, *Iwanami Shoten, Publishers*, *Tokyo*, 1971.

[26] G. Shimura and Y. Taniyama, Complex Multiplication of Abelian Varieties and Its Applications to Number Theory, *Math. Soc. Japan*, *Tokyo*, 1961.

[27] L. C. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Mathematics, Vol. **83**, *Springer-Verlag*, *New York*, 1982.

KÁLMÁN GYŐRY
INSTITUTE OF MATHEMATICS
UNIVERSITY OF DEBRECEN
H-4002 DEBRECEN
P. O. BOX 400
HUNGARY

E-mail: gyory@science.unideb.hu

(Received August 6, 2016)