JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Shabnam AKHTARI et Jeffrey D. VAALER

Lower bounds for regulators of number fieldsin terms of their discriminants

Tome 35, nº 1 (2023), p. 259-282.

https://doi.org/10.5802/jtnb.1245

© Les auteurs, 2023.

Cet article est mis à disposition selon les termes de la licence
Creative Commons attribution – pas de modification 4.0 France.
http://creativecommons.org/licenses/by-nd/4.0/fr/

CENTRE
MERSENNE

Le Journal de Théorie des Nombres de Bordeaux *est membre du*
Centre Mersenne pour l'édition scientifique ouverte
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **35** (2023), 259–282

Lower bounds for regulators of number fields in terms of their discriminants

par Shabnam AKHTARI et Jeffrey D. VAALER

Résumé. Nous prouvons une inégalité qui compare le régulateur d'un corps de nombres et la valeur absolue de son discriminant. Nous affinons les idées de Silverman [15] où de telles inégalités ont été prouvées pour la première fois. Pour démontrer nos théorèmes principaux, nous combinons ces méthodes avec les bornes pour le produit des hauteurs des unités relatives d'une extension de corps de nombres démontrées dans notre article antérieur.

Abstract. We prove inequalities that compare the regulator of a number field with the absolute value of its discriminant. We refine the ideas in Silverman's work [15] where such general inequalities are first proven. In order to prove our main theorems, we combine these refinements with the authors' previous results on bounding the product of heights of relative units in a number field extension.

1. Introduction

Let k be an algebraic number field of degree $d \geq 2$ with regulator $\operatorname{Reg}(k)$, discriminant Δ_k, and absolute discriminant $D_k = |\Delta_k|$. We denote the ring of algebraic integers in k by O_k and we write $r(k)$ for the rank of the unit group $O_k^\times$. For every number field with large enough absolute discriminant, an interesting lower bound for $\operatorname{Reg}(k)$ in terms of D_k has been established by Silverman in [15] (see also [8, 12, 13] for such lower bounds in special cases). In [10] Friedman has shown that $\operatorname{Reg}(k)$ takes its minimum value at the unique number field k_0 having degree 6 over $\mathbb{Q}$, and having discriminant equal to -10051. By Friedman's result we have

$$0.2052\cdots = \operatorname{Reg}(k_0) \leq \operatorname{Reg}(k) \tag{1.1}$$

for all algebraic number fields k. Following [15] we define

$$\rho(k) = \max\{r(k') : k' \subseteq k \text{ and } k' \neq k\}. \tag{1.2}$$

Manuscrit reçu le 31 décembre 2021, accepté le 21 mai 2022.

2020 *Mathematics Subject Classification.* 11G50, 11R04, 11R27.

Mots-clefs. Regulator and discriminant of a number field, Weil height, Arakelov height.

Shabnam Akhtari's research has been in parts supported by *the Simons Foundation Collaboration Grants*, Award Number 635880, and by *the National Science Foundation* Award DMS-2001281.

In [15] Silverman shows that

$$c_d\,(\log \gamma_d D_k)^{(r(k)-\rho(k))} < \mathrm{Reg}(k), \tag{1.3}$$

with

$$c_d = 2^{-4d^2} \quad \text{and} \quad \gamma_d = d^{-d^{\log_2 8d}}, \tag{1.4}$$

and it is understood that $1 < \gamma_d D_k$.

This lower bound is improved in [10], where Friedman shows there are computable, positive, absolute constants C_4 and C_5 such that the inequality (1.3) holds with

$$c_d = C_4 d^{-2r+\rho-\frac{1}{2}} (C_5 \log d)^{-3\rho} \quad \text{and} \quad \gamma_d = d^{-d} \tag{1.5}$$

(see the remark after the proof of Theorem C on p. 617 of [10]).

In order to sharpen the values of c_d and γ_d in the inequalities (1.3) that are given in (1.4) and (1.5), we use our results in [2, 1] that bound the regulators and relative regulators of an extension of number fields by heights of units and relative units in the number field extension. First we recall that $\rho(k) = r(k)$ if and only if k is a CM-field (see [11, Corollary 1 to Proposition 3.20]). If k is a CM-field, then the absolute discriminant of k will not appear in the lower bound in (1.3), and in this case the inequality (1.1) provides a sharp lower bound. For this reason, in our main theorems we will assume that the number field k is not a CM-field. Another simple case is when k is a totally real quadratic number field. In this case $r(k) = 1$ and $\rho(k) = 0$, and it can be easily seen that

$$\frac{1}{2} \log \frac{D_k}{4} \leq \mathrm{Reg}(k).$$

So we may assume $d \geq 3$ if need be. In Theorem 1.1 we will show that one may take $\gamma_d = d^{-d}$, and in Theorem 1.2 we will show that one may take $\gamma_d = d^{-\frac{d^{\log_2 d}}{2}}$. Both theorems provide explicit values for c_d that are larger than 2^{-4d^2}. For clarity and since different general strategies are used in the proofs, we state these two theorems separately.

Theorem 1.1. *Let k be a number field of degree $d \geq 3$ that is not a* CM*-field, with the unit rank $r = r(k)$ and absolute discriminant D_k. Let $\gamma_d = d^{-d}$ and assume that*

$$1 < \gamma_d D_k.$$

Then we have

$$\frac{(2r)!}{(r!)^3} \left(\frac{\log \log d}{2 \log d} \right)^{3\rho(k)} \left(\frac{\log (\gamma_d D_k)}{4d} \right)^{r-\rho(k)} \leq \mathrm{Reg}(k). \tag{1.6}$$

In the proof of Theorem 1.1, assuming the truth of Lehmer's conjecture, one can conclude that

$$\mathfrak{c}^{\rho(k)}\frac{(2r)!}{2^r\,(r!)^3}\left(\frac{\log(\gamma_d D_k)}{2d}\right)^{r-\rho(k)} \le \mathrm{Reg}(k),$$

where $\mathfrak{c}$ is an absolute positive constant. By appealing to a result of Amoroso and David [3], which gives a lower bound for the product of heights of algebraic numbers, we may proceed with the proof of Theorem 1.1 in Section 6 to obtain an inequality between the regulator and the absolute discriminant that is sharper than (1.6) in terms of the degree of the number field. We obtain

$$\mathfrak{c}_0\,\frac{(2r)!}{(r!)^3}\,\frac{d^{\rho(k)-1}}{(1+\log d)^{\rho(k)\kappa}}\left(\frac{\log(\gamma_d D_k)}{4d}\right)^{r-\rho(k)} \le \mathrm{Reg}(k), \tag{1.7}$$

where $\mathfrak{c}_0$ and κ depend only on $\rho(k)$ (see the remark at the end of Section 6 for an explicit version deduced from [4]).

As it is expected that the values obtained for c_d could be improved, we explore two different approaches in our proofs. Our next result is similar to Theorem 1.1, but is proven using a significantly different strategy which might be useful in some future research.

Theorem 1.2. *Let k be a number field of degree $d \ge 3$ that is not a* CM-*field, with the unit rank r and absolute discriminant D_k. Let $\gamma_d = d^{-\frac{d^{\log_2 d}}{2}}$ and assume that $1 < \gamma_d D_k$. Then we have*

$$\frac{0.2}{r!}\left(\frac{2d\log(\gamma_d D_k)}{(d-2)\,d^{\log_2 d}}\right)^{r-\rho(k)} \le \mathrm{Reg}(k). \tag{1.8}$$

We recall that $r(k)+1$ is the number of archimedean places of k, and therefore $d-2 \le 2r(k) < 2d$. Thus in Theorems 1.1 and 1.2 we may express explicit values for the constant c_d in (1.3) in terms of d only. In order to compare the values of c_d given in Theorems 1.1 and 1.2 with that in (1.5), we may use Stirling's formula

$$\sqrt{2\pi}\,n^{n+\frac{1}{2}}e^{-n} \le n! \le e\,n^{n+\frac{1}{2}}e^{-n},$$

where n is any positive integer.

For the lower bound given in (1.6) for Reg(k), we have

$$\begin{aligned}\frac{(2r)!}{(r!)^3}&\left(\frac{\log\log d}{2\log d}\right)^{3\rho(k)}\left(\frac{\log(\gamma_d D_k)}{4d}\right)^{r-\rho(k)}\\ &\geq \frac{\sqrt{2\pi}\,(2r)^{2r+\frac{1}{2}}e^{-2r}}{e^3 r^{3r+\frac{3}{2}}e^{-3r}}\left(\frac{\log\log d}{2\log d}\right)^{3\rho(k)}\left(\frac{\log(\gamma_d D_k)}{4d}\right)^{r-\rho(k)}\\ &= \frac{\sqrt{2\pi}\,2^{2r+\frac{1}{2}}e^{r}}{e^3 r^{r+1}}\left(\frac{\log\log d}{2\log d}\right)^{3\rho(k)}\left(\frac{\log(\gamma_d D_k)}{4d}\right)^{r-\rho(k)}\\ &> \frac{\sqrt{2\pi}\,2^{2\rho(k)+\frac{1}{2}}e^{r}}{e^3 d^{2r+1-\rho(k)}}\left(\frac{\log\log d}{2\log d}\right)^{3\rho(k)}\Big(\log(\gamma_d D_k)\Big)^{r-\rho(k)}.\end{aligned}$$

Therefore, Theorem 1.1 gives a lower bound that is larger than the lower bound (1.5) by at least a factor $e^{d/2}d^{-1/2}\left(\log\log d\right)^{3\rho(k)}$.

For the left-hand-side of (1.8), we have

$$\begin{aligned}\frac{0.2}{r!}&\left(\frac{2d\log(\gamma_d D_k)}{(d-2)\,d^{\log_2 d}}\right)^{r-\rho(k)}\\ &> 0.2e^{r-1}\,r^{-r-\frac{1}{2}}\,\left(d^{\log_2 d}\right)^{-r+\rho(k)}\left(2\log(\gamma_d D_k)\right)^{r-\rho(k)}\\ &> 0.2\frac{e^{r-1}}{\left(\frac{d^{\log_2 d}}{2}\right)^{r-\rho(k)}}\,d^{-r-\frac{1}{2}}\,\left(\log(\gamma_d D_k)\right)^{r-\rho(k)}.\end{aligned}$$

Therefore, the lower bound obtained in Theorem 1.2 is larger than the lower bound (1.5) by at least a factor

$$\frac{e^{d/2}\left(\log d\right)^{3\rho(k)}}{\left(\frac{d^{\log_2 d}}{2d}\right)^{r-\rho(k)}}.$$

In Theorems 1.1 and 1.2, we assume that $1 < \gamma_d D_k$. Suppose that for a number field k of degree d, we have $\gamma_d D_k \leq 1$, where γ_d is any of the values assumed in Theorems 1.1 and 1.2. Then by (1.1), we have

$$\log D_k < 5\,\log\gamma_d^{-1}\ \mathrm{Reg}(k).$$

This gives a stronger lower bound for the regulators of number fields with small absolute discriminant than those stated in our main theorems above.

This manuscript is organized as follows. Section 2 is a preliminary one and contains an overview of the Weil and Arakelov heights. In Section 3 we recall some lower bounds for the regulators and relative regulators in terms of a product of heights of ordinary and relative units. In Section 4 for an algebraic number field k of degree d, we obtain inequalities that relate Arakelov heights defined on k^d and the absolute discriminant of k. In Section 5 we prove inequalities relating the Weil and Arakelov heights.

Section 6 includes the proof of Theorem 1.1, and Section 7 includes the proof of Theorem 1.2.

2. The Weil and Arakelov heights

Let k be an algebraic number field of degree d over $\mathbb{Q}$. At each place v of k we write k_v for the completion of k at v. We work with two distinct absolute values $\| \ \|_v$ and $| \ |_v$ from each place v. These are related by

$$\| \ \|_v^{d_v/d} = | \ |_v,$$

where $d_v = [k_v : \mathbb{Q}_v]$ is the local degree at v, and $d = [k : \mathbb{Q}]$ is the global degree. If $v|\infty$ then the restriction of $\| \ \|_v$ to $\mathbb{Q}$ is the usual archimedean absolute value on $\mathbb{Q}$, and if $v|p$ then the restriction of $\| \ \|_v$ to $\mathbb{Q}$ is the usual p-adic absolute value on $\mathbb{Q}$. Then the absolute logarithmic Weil height is the map

$$h : k^{\times} \longrightarrow [0, \infty)$$

defined at each algebraic number $\alpha \neq 0$ in k by the sum

$$h(\alpha) = \sum_v \log^+ |\alpha|_v = \frac{1}{2} \sum_v |\log |\alpha|_v|. \tag{2.1}$$

In both sums there are only finitely many nonzero terms, and the equality on the right of (2.1) follows from the product formula. It can be shown that the value of $h(\alpha)$ does not depend on the field k that contains α. Hence the Weil height may be regarded as a map

$$h : \overline{\mathbb{Q}}^{\times} \longrightarrow [0, \infty).$$

Let $N \in \mathbb{N}$. At each place v of k we define a norm

$$\| \ \|_v : k_v^{N+1} \longrightarrow [0, \infty)$$

on (column) vectors $\boldsymbol{\xi} = (\xi_n)$ by

$$\|\boldsymbol{\xi}\|_v = \begin{cases} (\|\xi_0\|_v^2 + \|\xi_1\|_v^2 + \|\xi_2\|_v^2 + \cdots + \|\xi_N\|_v^2)^{\frac{1}{2}} & \text{if } v \mid \infty, \\ \max\{\|\xi_0\|_v, \|\xi_1\|_v, \|\xi_2\|_v, \ldots, \|\xi_N\|_v\} & \text{if } v \nmid \infty. \end{cases}$$

We define a second norm

$$| \ |_v : k_v^{N+1} \longrightarrow [0, \infty)$$

at each place v by setting

$$|\boldsymbol{\xi}|_v = \|\boldsymbol{\xi}\|_v^{d_v/d}.$$

A vector $\boldsymbol{\xi} \neq \mathbf{0}$ in k^{N+1} has finitely many coordinates, and it follows that

$$|\boldsymbol{\xi}|_v = 1$$

for all but finitely many places v of k. Then the Arakelov height

$$H : k^{N+1} \setminus \{\mathbf{0}\} \longrightarrow [1, \infty)$$

is defined by

$$H(\boldsymbol{\xi}) = \prod_v |\boldsymbol{\xi}|_v.$$

If $\boldsymbol{\xi} \neq \mathbf{0}$, and $\xi_m \neq 0$ is a nonzero coordinate of $\boldsymbol{\xi}$, then using the product formula we get

$$1 = \prod_v |\xi_m|_v \leq \prod_v |\boldsymbol{\xi}|_v = H(\boldsymbol{\xi}).$$

Thus H takes values in the interval $[1, \infty)$. If $\eta \neq 0$ belongs to k, and $\boldsymbol{\xi} \neq \mathbf{0}$ is a vector in k^{N+1}, then a second application of the product formula shows that

$$H(\eta\boldsymbol{\xi}) = \prod_v |\eta\boldsymbol{\xi}|_v = \prod_v |\eta|_v |\boldsymbol{\xi}|_v = \prod_v |\boldsymbol{\xi}|_v = H(\boldsymbol{\xi}).$$

More information about the Arakelov height is contained in [5].

3. Weil Heights and Regulators

Throughout this section we suppose that k and l are algebraic number fields with $k \subseteq l$. We write $r(k)$ for the rank of the unit group $O_k^\times$, and $r(l)$ for the rank of the unit group $O_l^\times$. Then k has $r(k)+1$ archimedean places, and l has $r(l)+1$ archimedean places. In general we have $r(k) \leq r(l)$, and we recall (see [11, Proposition 3.20]) that $r(k) = r(l)$ if and only if l is a CM-field, and k is the maximal totally real subfield of l.

The norm is a homomorphism of multiplicative groups

$$\mathrm{Norm}_{l/k} : l^\times \longrightarrow k^\times.$$

If v is a place of k, then each element α in $l^\times$ satisfies the identity

$$[l:k] \sum_{w|v} \log |\alpha|_w = \log |\mathrm{Norm}_{l/k}(\alpha)|_v.$$

It follows that the norm, restricted to the subgroup $O_l^\times$ of units, is a homomorphism

$$\mathrm{Norm}_{l/k} : O_l^\times \longrightarrow O_k^\times,$$

and the norm, restricted to the torsion subgroup in $O_l^\times$, is also a homomorphism

$$\mathrm{Norm}_{l/k} : \mathrm{Tor}(O_l^\times) \longrightarrow \mathrm{Tor}(O_k^\times).$$

Therefore we get a well defined homomorphism, which we write as

$$\mathrm{norm}_{l/k} : O_l^\times / \mathrm{Tor}(O_l^\times) \longrightarrow O_k^\times / \mathrm{Tor}(O_k^\times),$$

and define by

$$\mathrm{norm}_{l/k}(\alpha \, \mathrm{Tor}(O_l^\times)) = \mathrm{Norm}_{l/k}(\alpha) \, \mathrm{Tor}(O_k^\times).$$

However, to simplify notation we write

$$F_k = O_k^\times / \mathrm{Tor}(O_k^\times), \quad \text{and} \quad F_l = O_l^\times / \mathrm{Tor}(O_l^\times),$$

and we write the elements of the quotient groups F_k and F_l as coset representatives rather than cosets. Obviously F_k and F_l are free abelian groups of rank $r(k)$ and $r(l)$, respectively.

Following Costa and Friedman [6], the subgroup of relative units in $O_l^\times$ is defined by

$$\{\alpha \in O_l^\times : \mathrm{Norm}_{l/k}(\alpha) \in \mathrm{Tor}(O_k^\times)\}.$$

Alternatively, we work in the free group F_l where the image of the subgroup of relative units is the kernel of the homomorphism $\mathrm{norm}_{l/k}$. That is, we define the subgroup of *relative units* in F_l to be the subgroup

$$E_{l/k} = \{\alpha \in F_l : \mathrm{norm}_{l/k}(\alpha) = 1\}.$$

We also write

$$I_{l/k} = \{\mathrm{norm}_{l/k}(\alpha) : \alpha \in F_l\} \subseteq F_k$$

for the image of the homomorphism $\mathrm{norm}_{l/k}$. If β in F_l represents a coset in the subgroup F_k, then we have

$$\mathrm{norm}_{l/k}(\beta) = \beta^{[l:k]}.$$

Therefore the image $I_{l/k} \subseteq F_k$ is a subgroup of rank $r(k)$, and the index satisfies

$$[F_k : I_{l/k}] < \infty.$$

It follows that $E_{l/k} \subseteq F_l$ is a subgroup of rank $r(l/k) = r(l) - r(k)$, and we restrict our attention here to extensions l/k such that $r(l/k)$ is positive.

Let $\eta_1, \eta_2, \ldots, \eta_{r(l/k)}$ be a collection of multiplicatively independent relative units that form a basis for the subgroup $E_{l/k}$. At each archimedean place v of k we select a place $\widehat{w}_v$ of l such that $\widehat{w}_v | v$. Then we define an $r(l/k) \times r(l/k)$ real matrix

$$M_{l/k} = \big([l_w : \mathbb{Q}_w] \log \|\eta_j\|_w\big),$$

where w is an archimedean place of l, but $w \neq \widehat{w}_v$ for each $v|\infty$, w indexes rows, and $j = 1, 2, \ldots, r(l/k)$ indexes columns. We write l_w for the completion of l at the place w, $\mathbb{Q}_w$ for the completion of $\mathbb{Q}$ at the place w, and we write $[l_w : \mathbb{Q}_w]$ for the local degree. Of course $\mathbb{Q}_w$ is isomorphic to $\mathbb{R}$ in the situation considered here. As in [6], we define the *relative regulator* of the extension l/k to be the positive number

$$\mathrm{Reg}(E_{l/k}) = |\det M_{l/k}|. \tag{3.1}$$

It follows, as in the proof of [6, Theorem 1] (see also [7]), that the value of the determinant on the right of (3.1) does not depend on the choice of places $\widehat{w}_v$ for each archimedean place v of k.

It follows from [1, Theorem 1.2] that there exist multiplicatively independent elements $\beta_1, \beta_2, \dots, \beta_{r(k)}$ in F_k such that

$$\prod_{i=1}^{r(k)} \bigl([k:\mathbb{Q}]h(\beta_i)\bigr) \le r(k)!\,\mathrm{Reg}(k). \tag{3.2}$$

Suppose k, l are distinct algebraic number fields, that k is not $\mathbb{Q}$, k is not an imaginary quadratic extension of $\mathbb{Q}$, and $r(l) > r(k)$. In [2, Theorem 1.1] it is shown that there exist multiplicatively independent elements $\psi_1, \psi_2, \dots, \psi_{r(l/k)}$ in the group $E_{l/k}$ of relative units such that

$$\prod_{j=1}^{r(l/k)} \bigl([l:\mathbb{Q}]h(\psi_j)\bigr) \le r(l/k)!\,\mathrm{Reg}(E_{l/k}). \tag{3.3}$$

It is shown in [2] that the two sets of multiplicatively independent units in (3.2) and (3.3) can be combined. The following is Corollary 1.2 of [2].

Proposition 3.1. *Let $\beta_1, \beta_2, \dots, \beta_{r(k)}$ be multiplicatively independent units in F_k that satisfy* (3.2), *and let $\psi_1, \psi_2, \dots, \psi_{r(l/k)}$ be multiplicatively independent units in $E(l/k)$ that satisfy* (3.3). *Then the elements in the set*

$$\{\beta_1, \beta_2, \dots, \beta_{r(k)}\} \cup \{\psi_1, \psi_2, \dots, \psi_{r(l/k)}\}$$

are multiplicatively independent units in F_l, and they satisfy

$$\prod_{i=1}^{r(k)} \bigl([k:\mathbb{Q}]h(\beta_i)\bigr) \prod_{j=1}^{r(l/k)} \bigl([l:\mathbb{Q}]h(\psi_j)\bigr) \le r(l)!\,\mathrm{Reg}(l).$$

4. Arakelov heights and discriminants

In this section we suppose that $k \subseteq \overline{\mathbb{Q}}$, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$. Then we write $\sigma_1, \sigma_2, \dots, \sigma_d$, for the distinct embeddings

$$\sigma_j : k \longrightarrow \overline{\mathbb{Q}}.$$

If $\boldsymbol{\beta} = (\beta_i)$ is a (column) vector in k^d we define the $d \times d$ matrix

$$M(\boldsymbol{\beta}) = \bigl(\sigma_j(\beta_i)\bigr), \tag{4.1}$$

where $i = 1, 2, \dots, d$, indexes rows and $j = 1, 2, \dots, d$, indexes columns. We also define

$$\mathcal{B}(k) = \{\boldsymbol{\beta} = (\beta_i) \in k^d : \beta_1, \beta_2, \dots, \beta_d \text{ are } \mathbb{Q}\text{-linearly independent}\}.$$

Then the matrix $M(\boldsymbol{\beta})$ is nonsingular if and only if $\boldsymbol{\beta}$ belongs to $\mathcal{B}(k)$. Moreover, if $\alpha \ne 0$ belongs to k then

$$\det M(\alpha\boldsymbol{\beta}) = \mathrm{Norm}_{k/\mathbb{Q}}(\alpha) \det M(\boldsymbol{\beta}), \tag{4.2}$$

and if A is a $d \times d$ matrix in the general linear group $\mathrm{GL}(d, \mathbb{Q})$ we find that

$$\det M(A\boldsymbol{\beta}) = \det\bigl(AM(\boldsymbol{\beta})\bigr) = \det A \det M(\boldsymbol{\beta}). \tag{4.3}$$

These results are proved in [11, Proposition 2.9].

The product

$$M(\boldsymbol{\beta})M(\boldsymbol{\beta})^T = \big(\mathrm{Trace}_{k/\mathbb{Q}}(\beta_i\beta_j)\big)$$

is a $d \times d$ matrix with entries in $\mathbb{Q}$. Therefore, if $\boldsymbol{\beta}$ belongs to $\mathcal{B}(k)$ then

$$(\det M(\boldsymbol{\beta}))^2 = \det\big(M(\boldsymbol{\beta})M(\boldsymbol{\beta})^T\big) = \det\big(\mathrm{Trace}_{k/\mathbb{Q}}(\beta_i\beta_j)\big) \tag{4.4}$$

is a nonzero rational number, and if $\boldsymbol{\beta}$ also has entries in O_k then (4.4) is a nonzero integer. It will be convenient to define the function

$$f_k : \mathcal{B}(k) \longrightarrow [0, \infty)$$

by

$$f_k(\boldsymbol{\beta}) = \big\|\det\big(M(\boldsymbol{\beta})M(\boldsymbol{\beta})^T\big)\big\|_\infty \prod_{v\nmid\infty} \|\boldsymbol{\beta}\|_v^{2d_v}. \tag{4.5}$$

Here $\| \ \|_\infty$ is the usual archimedean absolute value on $\mathbb{Q}$, and the product on the right of (4.5) is over the set of all nonarchimedean places v of k. If $\alpha \neq 0$ belongs to k and $\boldsymbol{\beta}$ belongs to $\mathcal{B}(k)$, then it follows using (4.2) and the product formula that

$$\begin{aligned} (4.6)\quad & f_k(\alpha\boldsymbol{\beta}) \\ &= \big\|\det M(\alpha\boldsymbol{\beta})M(\alpha\boldsymbol{\beta})^T\big\|_\infty \prod_{v\nmid\infty} \|\alpha\boldsymbol{\beta}\|_v^{2d_v} \\ &= \Bigg(\|\mathrm{Norm}_{k/\mathbb{Q}}(\alpha)\|_\infty^2 \prod_{v\nmid\infty} \|\alpha\|_v^{2d_v}\Bigg)\big\|\det M(\boldsymbol{\beta})M(\boldsymbol{\beta})^T\big\|_\infty^2 \prod_{v\nmid\infty} \|\boldsymbol{\beta}\|_v^{2d_v} \\ &= \Bigg(\prod_{v\mid\infty} \|\alpha\|_v^{2d_v} \prod_{v\nmid\infty} \|\alpha\|_v^{2d_v}\Bigg) f_k(\boldsymbol{\beta}) = f_k(\boldsymbol{\beta}). \end{aligned}$$

For $\boldsymbol{\beta} = (\beta_i)$ in $\mathcal{B}(k)$, the fractional ideal generated by $\beta_1, \beta_2, \ldots, \beta_d$, is the subset

$$\mathfrak{J}(\boldsymbol{\beta}) = \{\eta \in k : \|\eta\|_v \leq \|\boldsymbol{\beta}\|_v \text{ at each } v \nmid \infty\}. \tag{4.7}$$

And the $\mathbb{Z}$-module generated by $\beta_1, \beta_2, \ldots, \beta_d$ is

$$\mathcal{M}(\boldsymbol{\beta}) = \{\boldsymbol{\xi}^T\boldsymbol{\beta} = \xi_1\beta_1 + \xi_2\beta_2 + \cdots + \xi_d\beta_d : \boldsymbol{\xi} \in \mathbb{Z}^d\}. \tag{4.8}$$

It is obvious that $\mathcal{M}(\boldsymbol{\beta})$ is a subgroup of $\mathfrak{J}(\boldsymbol{\beta})$, and both $\mathcal{M}(\boldsymbol{\beta})$ and $\mathfrak{J}(\boldsymbol{\beta})$ are free abelian groups of rank d. Hence the index $\big[\mathfrak{J}(\boldsymbol{\beta}) : \mathcal{M}(\boldsymbol{\beta})\big]$ is finite. If $\alpha \neq 0$ belongs to k and $\boldsymbol{\beta}$ is a vector in $\mathcal{B}(k)$ then using (4.7) we find that

$$\mathfrak{J}(\alpha\boldsymbol{\beta}) = \{\eta \in k : \|\eta\|_v \leq \|\alpha\|_v\|\boldsymbol{\beta}\|_v \text{ at each } v \nmid \infty\} = \alpha\mathfrak{J}(\boldsymbol{\beta}), \tag{4.9}$$

and in a similar manner we get

$$\mathcal{M}(\alpha\boldsymbol{\beta}) = \alpha\mathcal{M}(\boldsymbol{\beta}). \tag{4.10}$$

Then it follows from (4.9) and (4.10) that

$$\alpha \longmapsto \big[\mathfrak{J}(\alpha\boldsymbol{\beta}) : \mathcal{M}(\alpha\boldsymbol{\beta})\big] \tag{4.11}$$

is constant for $\alpha \neq 0$ in k.

Our next result shows that f_k takes positive integer values on $\mathcal{B}(k)$ and provides a useful upper bound for the absolute discriminant.

Proposition 4.1. *Let $\boldsymbol{\beta} = (\beta_i)$ belong to $\mathcal{B}(k)$. Let $\mathfrak{J}(\boldsymbol{\beta})$ be the fractional ideal generated by $\beta_1, \beta_2, \dots, \beta_d$ as in* (4.7)*, and let $\mathcal{M}(\boldsymbol{\beta})$ be the $\mathbb{Z}$-module generated by $\beta_1, \beta_2, \dots, \beta_d$ as in* (4.8)*. Then we have*

$$f_k(\boldsymbol{\beta}) = \big[\mathfrak{J}(\boldsymbol{\beta}) : \mathcal{M}(\boldsymbol{\beta})\big]^2 D_k \le H(\boldsymbol{\beta})^{2d}, \tag{4.12}$$

where D_k is the absolute discriminant of k, and $\big[\mathfrak{J}(\boldsymbol{\beta}) : \mathcal{M}(\boldsymbol{\beta})\big]$ is the index of $\mathcal{M}(\boldsymbol{\beta})$ in $\mathfrak{J}(\boldsymbol{\beta})$.

Proof. First we prove the equality on the left of (4.12). And we assume to begin with that $\mathfrak{J}(\boldsymbol{\beta})$ is an integral ideal, or equivalently that

$$\|\boldsymbol{\beta}\|_v \le 1 \quad \text{at each nonarchimedean place } v \text{ of } k.$$

Let $\gamma_1, \gamma_2, \dots, \gamma_d$ be a basis for $\mathfrak{J}(\boldsymbol{\beta})$ as a $\mathbb{Z}$-module, and write $\boldsymbol{\gamma} = (\gamma_j)$ for the corresponding vector in $\mathcal{B}(k)$. By a basic identity for the discriminant of an integral ideal, see [11, Proposition 2.13], we have

$$\|\det M(\boldsymbol{\gamma})M(\boldsymbol{\gamma})^T\|_\infty = \big(\mathrm{norm}_{k/\mathbb{Q}}\,\mathfrak{J}(\boldsymbol{\beta})\big)^2 D_k = \big[O_k : \mathfrak{J}(\boldsymbol{\beta})\big]^2 D_k, \tag{4.13}$$

where

$$M(\boldsymbol{\gamma}) = \big(\sigma_j(\gamma_i)\big)$$

is the $d \times d$ matrix defined as in (4.1). As $\beta_1, \beta_2, \dots, \beta_d$ belong to $\mathfrak{J}(\boldsymbol{\beta})$ there exists a unique, nonsingular, $d \times d$ matrix $A = (a_{ij})$ with entries in $\mathbb{Z}$ such that

$$\beta_i = \sum_{j=1}^{d} a_{ij}\gamma_j, \quad \text{or equivalently } \boldsymbol{\beta} = A\boldsymbol{\gamma}. \tag{4.14}$$

It follows from (4.7) that $\|\boldsymbol{\gamma}\|_v \le \|\boldsymbol{\beta}\|_v$ for each $v \nmid \infty$, and it follows from (4.14) and the strong triangle inequality that $\|\boldsymbol{\beta}\|_v \le \|\boldsymbol{\gamma}\|_v$ for each $v \nmid \infty$. Then from (4.14) we also get

$$\big[\mathfrak{J}(\boldsymbol{\beta}) : \mathcal{M}(\boldsymbol{\beta})\big] = \|\det A\|_\infty. \tag{4.15}$$

As $\mathfrak{J}(\boldsymbol{\beta})$ is an integral ideal generated (as an ideal) by $\beta_1, \beta_2, \dots, \beta_d$ and also generated (as a $\mathbb{Z}$-module) by $\gamma_1, \gamma_2, \dots, \gamma_d$, we have

$$\prod_{v \nmid \infty} \|\boldsymbol{\beta}\|_v^{-d_v} = \prod_{v \nmid \infty} \|\boldsymbol{\gamma}\|_v^{-d_v} = \mathrm{norm}_{k/\mathbb{Q}}\,\mathfrak{J}(\boldsymbol{\beta}) = \big[O_k : \mathfrak{J}(\boldsymbol{\beta})\big]. \tag{4.16}$$

We combine (4.3), (4.13), (4.15) and (4.16), and conclude that

$$\begin{aligned}\|\det M(\boldsymbol{\beta})M(\boldsymbol{\beta})^T\|_\infty \prod_{v\nmid\infty} \|\boldsymbol{\beta}\|_v^{2d_v}& \\ &= \|\det M(A\boldsymbol{\gamma})M(A\boldsymbol{\gamma})^T\|_\infty \prod_{v\nmid\infty} \|\boldsymbol{\gamma}\|_v^{2d_v} \\ &= \|\det A\|_\infty^2 \|\det M(\boldsymbol{\gamma})M(\boldsymbol{\gamma})^T\|_\infty \big[O_k : \mathfrak{J}(\boldsymbol{\beta})\big]^{-2} \\ &= \big[\mathfrak{J}(\boldsymbol{\beta}) : \mathcal{M}(\boldsymbol{\beta})\big]^2 D_k.\end{aligned}$$

This proves the equality on the left of (4.12) under the assumption that $\mathfrak{J}(\boldsymbol{\beta})$ is an integral ideal.

If $\mathfrak{J}(\boldsymbol{\beta})$ is a fractional ideal in k, but not necessarily an integral ideal, then there exists an algebraic integer $\alpha \neq 0$ in O_k such that $\alpha\mathfrak{J}(\boldsymbol{\beta}) = \mathfrak{J}(\alpha\boldsymbol{\beta})$ is an integral ideal. Therefore we get the identity

$$f_k(\alpha\boldsymbol{\beta}) = \big[\mathfrak{J}(\alpha\boldsymbol{\beta}) : \mathcal{M}(\alpha\boldsymbol{\beta})\big]^2 D_k \tag{4.17}$$

by the case already considered. We use (4.6), (4.11), and (4.17), to establish the equality on the left of (4.12) in general.

Next we prove the inequality on the right of (4.12). We assume that $\overline{\mathbb{Q}} \subseteq \mathbb{C}$, and write $|\ |$ for the usual Hermitian absolute value on $\mathbb{C}$. Each embedding

$$\sigma_j : k \longrightarrow \overline{\mathbb{Q}} \subseteq \mathbb{C}$$

determines an archimedean place v of k such that

$$\|\eta\|_v = |\sigma_j(\eta)| \quad \text{for } \eta \text{ in } k.$$

As $j = 1, 2, \ldots, d$, each real archimedean place v occurs once and each complex archimedean place v occurs twice. Then Hadamard's inequality applied to the matrix $M(\boldsymbol{\beta}) = \big(\sigma_j(\beta_i)\big)$ leads to

$$\begin{aligned}\|\det M(\boldsymbol{\beta})M(\boldsymbol{\beta})^T\|_\infty &= \big|\det\big(\sigma_j(\beta_i)\big)\big|^2 \\ &\le \prod_{j=1}^{d} \left(\sum_{i=1}^{d} |\sigma_j(\beta_i)|^2\right) \\ &= \prod_{v\mid\infty} \left(\sum_{i=1}^{d} \|\beta_i\|_v^2\right)^{d_v} \\ &= \prod_{v\mid\infty} \|\boldsymbol{\beta}\|_v^{2d_v}.\end{aligned} \tag{4.18}$$

It follows from (4.18) that

$$\begin{aligned} f_k(\boldsymbol{\beta}) &= \|\det M(\boldsymbol{\beta})M(\boldsymbol{\beta})^T\|_\infty \prod_{v\nmid\infty} \|\boldsymbol{\beta}\|_v^{2d_v} \\ &\le \prod_{v|\infty} \|\boldsymbol{\beta}\|_v^{2d_v} \prod_{v\nmid\infty} \|\boldsymbol{\beta}\|_v^{2d_v} = H(\boldsymbol{\beta})^{2d}. \end{aligned} \tag{4.19}$$

Now (4.19) verifies the inequality on the right of (4.12). □

5. Special height inequalities

In this section we present inequalities where the Arakelov height $H(\boldsymbol{\alpha})$ is bounded by the Weil height of the coordinates of $\boldsymbol{\alpha}$. Such inequalities are useful when H is applied to vectors having coordinates that satisfy simple algebraic conditions.

Lemma 5.1. *Let k be an algebraic number field and let $\alpha \neq 0$ be a point in $\overline{\mathbb{Q}}$ such that $M = [k(\alpha) : k]$. Let $\boldsymbol{a} = \big(\alpha^{m-1}\big)$ be the column vector in k^M where $m = 1, 2, \dots, M$, indexes rows. Then we have*

$$\log H(\boldsymbol{a}) \le \frac{1}{2}\log M + (M-1)h(\alpha). \tag{5.1}$$

Proof. Let l be an algebraic number field such that $k \subseteq k(\alpha) \subseteq l$ and let w be a place of l. If $w \nmid \infty$ we find that

$$|\boldsymbol{a}|_w = \max\{1, |\alpha|_w, \dots, |\alpha|_w^{M-1}\} = \max\{1, |\alpha|_w\}^{(M-1)}. \tag{5.2}$$

If $w|\infty$ we get

$$\|\boldsymbol{a}\|_w = \Big(1 + \|\alpha\|_w^2 + \|\alpha\|_w^4 + \cdots + \|\alpha\|_w^{2M-2}\Big)^{\frac{1}{2}} \le M^{\frac{1}{2}} \max\{1, \|\alpha\|_w\}^{(M-1)},$$

and then

$$\log|\boldsymbol{a}|_w \le \frac{[l_w : \mathbb{Q}] \log M}{2[l : \mathbb{Q}]} + (M-1)\log^+|\alpha|_w. \tag{5.3}$$

Combining (5.2) and (5.3), we find that

$$\begin{aligned} \log H(\boldsymbol{a}) &= \sum_w \log|\boldsymbol{a}|_w \\ &\le \sum_{w|\infty} \frac{[l_w : \mathbb{Q}_w] \log M}{2[l : \mathbb{Q}]} + (M-1)\sum_w \log^+|\alpha|_w \\ &= \frac{1}{2}\log M + (M-1)h(\alpha). \end{aligned}$$

This verifies the inequality (5.1). □

If K is a field and $K(\alpha)$ is a simple, algebraic extension of K of positive degree N, then every element η in $K(\alpha)$ has a unique representation of the form

$$\eta = \sum_{n=0}^{N-1} c(n)\alpha^n, \quad \text{where} \quad c(n) \in K.$$

This extends to fields obtained by adjoining finitely many algebraic elements using a simple inductive argument.

Lemma 5.2. *Let $K \subseteq L$ be fields, let $\alpha_1, \alpha_2, \dots, \alpha_M$, be elements of L, and assume that each α_m is algebraic over K. Define positive integers N_m by*

$$N_1 = [K(\alpha_1) : K], \tag{5.4}$$

and by

$$N_m = [K(\alpha_1, \alpha_2, \dots, \alpha_m) : K(\alpha_1, \alpha_2, \dots, \alpha_{m-1})] \tag{5.5}$$

for $m = 2, 3, \dots, M$. Then every element η in $K(\alpha_1, \alpha_2, \dots, \alpha_M)$ has a unique representation of the form

$$\eta = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \cdots \sum_{n_M=0}^{N_M-1} c(\boldsymbol{n}) \alpha_1^{n_1} \alpha_2^{n_2} \dots \alpha_M^{n_M}, \quad \textit{where} \quad c(\boldsymbol{n}) \in K. \tag{5.6}$$

Moreover, $K(\alpha_1, \alpha_2, \dots, \alpha_M)/K$ is a finite extension of degree $N_1 N_2 \dots N_M$, and the elements in the set

$$\{\alpha_1^{n_1} \alpha_2^{n_2} \dots \alpha_M^{n_M} : 0 \le n_m < N_m,\ m = 1, 2, \dots, M\} \tag{5.7}$$

form a basis for $K(\alpha_1, \alpha_2, \dots, \alpha_M)$ as a vector space over K.

Proof. We argue by induction on M. If $M = 1$ then the result is well known. Therefore we assume that $M \ge 2$. As

$$K(\alpha_1, \dots, \alpha_{M-1}, \alpha_M)/K(\alpha_1, \dots, \alpha_{M-1})$$

is a simple extension, the element η in $K(\alpha_1, \dots, \alpha_{M-1}, \alpha_M)$ has a unique representation of the form

$$\eta = \sum_{n_M=0}^{N_M-1} a(n_M) \alpha_M^{n_M}, \quad \text{where} \quad a(n_M) \in K(\alpha_1, \alpha_2, \dots, \alpha_{M-1}). \tag{5.8}$$

By the inductive hypothesis each coefficient $a(n_M)$ has a representation in the form

$$a(n_M) = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \cdots \sum_{n_{M-1}=0}^{N_{M-1}-1} b(\boldsymbol{n}', n_M) \alpha_1^{n_1} \alpha_2^{n_2} \dots \alpha_{M-1}^{n_{M-1}}, \tag{5.9}$$

where each $b(\boldsymbol{n}', n_M)$ belongs to K. When the sum on the right of (5.9) is inserted into (5.8), we obtain the representation (5.6).

We have proved that the set (5.7) spans the field $K(\alpha_1, \alpha_2, \dots, \alpha_M)$ as a vector space over K. Clearly the set (5.7) has cardinality at most $N_1 N_2 \dots N_M$. Because

$$K \subseteq K(\alpha_1) \subseteq K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \alpha_2, \dots, \alpha_M),$$

it follows from (5.4) and (5.5) that

$$[K(\alpha_1, \alpha_2, \dots, \alpha_M) : K] = N_1 N_2 \dots N_M.$$

We conclude that the set (5.7) is a basis for $K(\alpha_1, \alpha_2, \dots, \alpha_M)$ over K. Therefore the representation (5.6) is unique. □

Let k and l be distinct algebraic number fields such that $k \subseteq l$. We establish a bound for $H(\boldsymbol{\beta})$ in the special case where the coordinates of $\boldsymbol{\beta}$ generate the field extension l/k. We assume that $\alpha_1, \alpha_2, \dots, \alpha_M$, are algebraic numbers such that

$$l = k(\alpha_1, \alpha_2, \dots, \alpha_M).$$

Then it follows from Lemma 5.2 that there exist positive integers $N_1, N_2, \dots, N_M$, such that

$$N_1 N_2 \dots N_M = [l : k],$$

and the elements of the set

$$\{\alpha_1^{n_1} \alpha_2^{n_2} \dots \alpha_M^{n_M} : 0 \le n_m < N_m,\ m = 1, 2, \dots, M\} \tag{5.10}$$

form a basis for $l = k(\alpha_1, \alpha_2, \dots, \alpha_M)$ as a vector space over k. We define a tower of intermediate fields

$$k = k_0 \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_M = l, \tag{5.11}$$

by

$$k_m = k(\alpha_1, \alpha_2, \dots, \alpha_m), \quad \text{where } m = 1, 2, \dots, M.$$

Then it follows from (5.5) that

$$N_m = [k_m : k_{m-1}] = [k_{m-1}(\alpha_m) : k_{m-1}], \quad \text{for each } m = 1, 2, \dots, M,$$

and

$$N_1 N_2 \dots N_m = [k_m : k_0], \quad \text{for each } m = 1, 2, \dots, M.$$

We note that the tower of intermediate fields (5.11) depends on the ordering of the generators $\alpha_1, \alpha_2, \dots, \alpha_M$, and a permutation of these generators would (in general) change the intermediate fields in the tower.

Lemma 5.3. *Let $\boldsymbol{\beta}$ be the vector in $l^{[l:k]}$ such that the elements of the set* (5.10) *are the coordinates of $\boldsymbol{\beta}$. For each $m = 1, 2, \dots, M$, let $\boldsymbol{a}_m$ be the vector in $k_m^{N_m}$ defined by $\boldsymbol{a}_m = \left(\alpha_m^{n_m}\right)$ where $n_m = 0, 1, \dots, N_m - 1$. Then we have*

$$H(\boldsymbol{\beta}) = \prod_{m=1}^{M} H(\boldsymbol{a}_m), \tag{5.12}$$

and

$$\log H(\boldsymbol{\beta}) \le \frac{1}{2}\log[l:k] + \sum_{m=1}^{M}(N_m-1)h(\alpha_m). \tag{5.13}$$

Proof. At each archimedean place w of l we have

$$\begin{aligned}
\prod_{w|\infty}\|\boldsymbol{\beta}\|_w &= \prod_{w|\infty}\left(\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}\cdots\sum_{n_M=0}^{N_M-1}\|\alpha_1^{n_1}\|_w^2\|\alpha_2^{n_2}\|_w^2\ldots\|\alpha_M^{n_M}\|_w^2\right)^{\frac{1}{2}}\\
&= \prod_{w|\infty}\left(\prod_{m=1}^{M}\sum_{n_m=0}^{N_m-1}\|\alpha_m^{n_m}\|_w^2\right)^{\frac{1}{2}}\\
&= \prod_{m=1}^{M}\prod_{w|\infty}\left(\sum_{n_m=0}^{N_m-1}\|\alpha_m^{n_m}\|_w^2\right)^{\frac{1}{2}}\\
&= \prod_{m=1}^{M}\prod_{w|\infty}\|\boldsymbol{a}_m\|_w.
\end{aligned} \tag{5.14}$$

At each nonarchimedean place w of l we find that

$$\begin{aligned}
\prod_{w\nmid\infty}\|\boldsymbol{\beta}\|_w &= \prod_{w|\infty}\max\{\|\alpha_1^{n_1}\alpha_2^{n_2}\ldots\alpha_M^{n_M}\|_w : 0\le n_m<N_m\}\\
&= \prod_{w\nmid\infty}\prod_{m=1}^{M}\max\{\|\alpha_m^{n_m}\|_w : 0\le n_m<N_m\}\\
&= \prod_{m=1}^{M}\prod_{w\nmid\infty}\max\{\|\alpha_m^{n_m}\|_w : 0\le n_m<N_m\}\\
&= \prod_{m=1}^{M}\prod_{w\nmid\infty}\|\boldsymbol{a}_m\|_w.
\end{aligned} \tag{5.15}$$

Clearly (5.12) follows from (5.14) and (5.15). Then using (5.12) and the inequality (5.1) we get

$$\begin{aligned}
\log H(\boldsymbol{\beta}) &= \sum_{m=1}^{M}\log H(\boldsymbol{a}_m)\\
&\le \sum_{m=1}^{M}\Big(\frac{1}{2}\log N_m + (N_m-1)h(\alpha_m)\Big)\\
&= \frac{1}{2}\log[l:k] + \sum_{m=1}^{M}(N_m-1)h(\alpha_m).
\end{aligned} \tag{5.16}$$

This verifies (5.13). □

We conclude this section with an inequality that will be very useful in our proofs. Let α be an algebraic number, $m = [\mathbb{Q}(\alpha) : \mathbb{Q}]$, and $D_{\mathbb{Q}(\alpha)}$ the absolute discriminant of the number field $\mathbb{Q}(\alpha)$. From (4.12) and (5.13), we obtain

$$h(\alpha) \geq \frac{\log \frac{D_{\mathbb{Q}(\alpha)}}{m^m}}{2m(m-1)}. \tag{5.17}$$

A similar inequality has been established in [14] by a different method.

6. A special intermediate field with large rank; Proof of Theorem 1.1

Suppose k is a number field of degree d. Let r be the rank of the unit group $O_k^{\times}$ in k. By [1, Theorem 1.2] there exist multiplicatively independent elements $\alpha_1, \alpha_2, \ldots, \alpha_r$ in $O_k^{\times}$ such that

$$d^r \prod_{j=1}^{r} h(\alpha_j) \leq \frac{2^r (r!)^3}{(2r)!} \operatorname{Reg}(k), \tag{6.1}$$

where $\operatorname{Reg}(k)$ is the regulator of k. If we assume now that k is not a CM-field, then the rank of the unit group $O_k^{\times}$ is strictly larger than the rank of the unit group in each proper subfield of k. As the multiplicative group generated by $\alpha_1, \alpha_2, \ldots, \alpha_r$ has rank equal to the rank of $O_k^{\times}$, it follows that

$$k = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_r). \tag{6.2}$$

Applying Lemma 5.2 to (6.2), we conclude that there exist positive integers

$$N_1, N_2, \ldots, N_r,$$

and a corresponding tower of intermediate fields

$$k_0 = \mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq k_3 \subseteq \cdots \subseteq k_r = k,$$

such that

$$k_j = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_j), \quad \text{where } j = 1, 2, \ldots, r, \tag{6.3}$$

$$N_j = [k_j : k_{j-1}] = [k_{j-1}(\alpha_j) : k_{j-1}], \quad \text{for each } j = 1, 2, \ldots, r,$$

and

$$N_1 N_2 \ldots N_j = [k_j : \mathbb{Q}], \quad \text{for each } j = 1, 2, \ldots, r. \tag{6.4}$$

In particular, (6.4) with $j = r$ is also

$$N_1 N_2 \ldots N_r = d.$$

Moreover, from (4.12) and (5.16) we get the inequality

$$\log D_k \leq 2d \log H(\boldsymbol{\beta}) \leq d \log d + 2d \sum_{j=1}^{r} (N_j - 1) h(\alpha_j), \tag{6.5}$$

where $\boldsymbol{\beta}$ is the vector in $\mathcal{B}(k)$ such that the elements of the set

$$\{\alpha_1^{n_1}\alpha_2^{n_2}\dots\alpha_r^{n_r} : 0 \le n_j < N_j, \text{ and } j = 1, 2, \dots, r\}$$

are the coordinates of $\boldsymbol{\beta}$.

It follows from (6.3) that the unit group $O_{k_j}^{\times}$ contains the collection of j multiplicatively independent units $\alpha_1, \alpha_2, \dots, \alpha_j$. Therefore we have

$$j \le \operatorname{rank} O_{k_j}^{\times}, \quad \text{for each } j = 1, 2, \dots, r. \tag{6.6}$$

As defined in (1.2), let

$$\rho(k) = \max\{\operatorname{rank} O_{k'}^{\times} : k' \subseteq k \text{ and } k' \ne k\}.$$

Because k is not a CM-field, we have $\rho(k) < r$. It will also be convenient to define

$$q = \min\{j : 1 \le j \le r \text{ and } k_j = k\} \le \rho(k) + 1, \tag{6.7}$$

where the inequality on the right of (6.7) follows from (6.6) and the definition of $\rho(k)$. Using the positive integer q we find that

$$j \le \operatorname{rank} O_{k_j}^{\times} \le \rho(k), \quad \text{if and only if } 1 \le j \le q - 1,$$

and

$$k_j = k, \quad \text{if and only if } q \le j \le r.$$

It follows that

$$2 \le N_q = [k_q : k_{q-1}] = [k : k_{q-1}],$$

and

$$N_j = 1 \quad \text{for } q < j \le r.$$

Thus the inequality (6.5) can be written as

$$\frac{\log D_k - d\log d}{2d} \le \sum_{j=1}^{q}(N_j - 1)h(\alpha_j).$$

It is clear that an advantageous ordering of the independent units $\alpha_1, \alpha_2, \dots, \alpha_r$ would be

$$0 < h(\alpha_1) \le h(\alpha_2) \le \dots \le h(\alpha_r), \tag{6.8}$$

which we assume from now on. Finally, as $N_1, N_2, \dots, N_q$ are positive integers, the inequality

$$\sum_{j=1}^{q}(N_j - 1) \le (N_1 N_2 \dots N_q) - 1 = d - 1$$

is easy to verify by induction on q. Then from (6.8) we get

$$\begin{aligned}\frac{\log D_k - d\log d}{2d} &\le \sum_{j=1}^{q}(N_j - 1)h(\alpha_j)\\ &\le h(\alpha_q)\sum_{j=1}^{q}(N_j - 1)\\ &\le (d-1)h(\alpha_q),\end{aligned}$$

which we write as

$$\frac{\log D_k - d\log d}{2d} \le dh(\alpha_q). \tag{6.9}$$

Plainly the inequality (6.9) is of interest if and only if

$$0 < \log D_k - d\log d,$$

which is also the hypothesis of Theorem 1.1. Then it follows from (6.8) that

$$\frac{\log D_k - d\log d}{2d} \le dh(\alpha_j). \tag{6.10}$$

for each

$$j = q, q+1, q+2, \dots, r.$$

Since the value of q is unknown and depends on the ordering (6.8), we use (6.10) in the more restricted range

$$j = \rho(k)+1, \rho(k)+2, \dots, r.$$

Then (6.8) and (6.10) imply that

$$\left(\frac{\log D_k - d\log d}{2d}\right)^{r-\rho(k)} \le \prod_{j=\rho(k)+1}^{r}(dh(\alpha_j)). \tag{6.11}$$

In order to obtain the desired explicit bounds in Theorem 1.1, we apply results of Dobrowolski in [9] and Voutier in [16]. From [9] there exists a positive constant $c'(d)$, which depends only on the degree $d = [k : \mathbb{Q}]$, such that the inequality

$$c'(d) \le dh(\gamma) \tag{6.12}$$

holds for algebraic numbers γ in $k^\times$ which are not roots of unity. Then from (6.1), (6.11), and (6.12), we get

$$\begin{aligned}c'(d)^{\rho(k)}\left(\frac{\log D_k - d\log d}{2d}\right)^{r-\rho(k)} &\le \prod_{j=1}^{r}(dh(\alpha_j))\\ &\le \frac{2^r(r!)^3}{(2r)!}\,\mathrm{Reg}(k).\end{aligned} \tag{6.13}$$

From [16] we have

$$\frac{1}{4}\Big(\frac{\log\log d}{\log d}\Big)^3 \le c'(d) \tag{6.14}$$

for each number field $k \neq \mathbb{Q}$. Hence (6.13) and (6.14) lead to the explicit inequality

$$\Big(\frac{\log\log d}{2\log d}\Big)^{3\rho(k)}\Big(\frac{\log D_k - d\log d}{4d}\Big)^{r-\rho(k)} \le \frac{(r!)^3}{(2r)!}\operatorname{Reg}(k).$$

This completes the proof of Theorem 1.1.

Remark. From the work of Amoroso and David [3] (see also Theorem 4.4.7 in [5]), we get

$$c\,n^{-1}(1+\log n)^{-\rho\kappa} \le \prod_{i=1}^{\rho(k)} h(\alpha_i), \tag{6.15}$$

where

$$n = [\mathbb{Q}(\alpha_1,\ldots,\alpha_\rho):\mathbb{Q}],$$

and c and κ depend only on the number of algebraic numbers in the product on the right hand side of (6.15), which in our case is $\rho = \rho(k)$.

From (6.1), (6.11), (6.15), and since $n < d = [k:\mathbb{Q}]$, we get

$$\begin{aligned} c\,d^{\rho(k)-1}(1+\log d)^{-\rho(k)\kappa}\Big(\frac{\log D_k - d\log d}{2d}\Big)^{r-\rho(k)} &\le \prod_{j=1}^{r}(dh(\alpha_j)) \\ &\le \frac{2^r(r!)^3}{(2r)!}\operatorname{Reg}(k). \end{aligned}$$

This implies the inequality (1.7). A completely explicit version of (6.15) is given in Corollary 1.6 of [4] and implies

$$\frac{(2r)!}{(r!)^3}\,\frac{d^{\rho(k)-1}}{(1050\,\rho(k)^5\log(1.5)d)^{\rho^2(k)(\rho(k)+1)^2}}\Big(\frac{\log(d^{-d}D_k)}{4d}\Big)^{r-\rho(k)} \le \operatorname{Reg}(k),$$

where the dependence on $\rho(k)$ is unlikely to be optimal.

7. A special intermediate field with optimal discriminant; Proof of Theorem 1.2

Let k be an algebraic number field, and $\mathcal{I}(k)$ the set of intermediate number fields k' such that $\mathbb{Q} \subseteq k' \subseteq k$. We will define two maps

$$\lambda : \mathcal{I}(k) \longrightarrow \mathbb{N}\cup\{0\}$$

and

$$\aleph : \mathcal{I}(k) \longrightarrow (0,1].$$

For each number field $k' \in \mathcal{I}(k)$ we define $\lambda(k')$ to be the maximum length of a tower of subfields of k that begins at $\mathbb{Q}$ and ends at k', with $\lambda(\mathbb{Q}) = 0$. If k_1 and k_2 are distinct intermediate fields such that

$$\mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq k,$$

then it is obvious that

$$\lambda(k_1) < \lambda(k_2) \le \lambda(k) \le \log_2 d, \tag{7.1}$$

where $d = [k : \mathbb{Q}]$.

For each number field k' we write $D_{k'}$ for the absolute discriminant of k'. For $k' \subseteq k$, we have (see [11, Corollary to Proposition 4.15]) $D_{k'}^{[k:k']} \mid D_k$, and if $k' \neq k$ we have

$$D_{k'} < D_k^{[k:k']^{-1}}. \tag{7.2}$$

In order to better control the change in the absolute values of discriminants of intermediate fields, we normalize the exponent $[k : k']^{-1}$ in the above inequality. For each subfield k' of k, we define

$$\aleph(k') := \big(2[k : k']\big)^{\lambda(k') - \lambda(k)}. \tag{7.3}$$

First we prove two useful lemmas about properties of the function $\aleph$.

Lemma 7.1. *Let*

$$\mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_{N-1} \subseteq k_N = k$$

be a tower of length N, containing $N+1$ distinct number fields. We have

$$0 < \aleph(\mathbb{Q}) < \aleph(k_1) < \aleph(k_2) < \cdots < \aleph(k_{N-1}) < \aleph(k_N) = 1.$$

Proof. By the definition of the function $\aleph$ in (7.3), we have $\aleph(k) = 1$ and $\aleph(\mathbb{Q}) > 0$. Now suppose that k_1, k_2 are distinct intermediate fields, with $\mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq k$, by (7.1) we have

$$\begin{aligned}
\aleph(k_1) &= \big(2\,[k : k_1]\big)^{\lambda(k_1) - \lambda(k)} \\
&= \big(2\,[k : k_2]\big)^{\lambda(k_2) - \lambda(k)} \big(2\,[k : k_2]\big)^{\lambda(k_1) - \lambda(k_2)} \big(2\,[k_2 : k_1]\big)^{\lambda(k_1) - \lambda(k)} \\
&< \big(2\,[k : k_2]\big)^{\lambda(k_2) - \lambda(k)} \\
&= \aleph(k_2).
\end{aligned}$$

□

Lemma 7.2. *Let $\mathbb{Q} \subseteq k' \subseteq k$. Assume $\alpha \in k$ and $\alpha \notin k'$ so that $k' \subseteq k'(\alpha) \subseteq k$. We have*

$$\aleph(k'(\alpha)) - \aleph(k')[k : k'] \ge 2^{\lambda(k') - \lambda(k)} \left([k : k']\right)^{\lambda(k') - \lambda(k) + 1}. \tag{7.4}$$

Proof. Since $\lambda(k'(\alpha)) \geq \lambda(k') + 1$, using the definition of the function $\aleph$ in (7.3), we obtain

$$\begin{aligned}(7.5)\quad \aleph(k'(\alpha)) - \aleph(k')[k : k'] &\\ &= \left(2[k : k'(\alpha)]\right)^{\lambda(k'(\alpha))-\lambda(k)} - \left(2[k : k']\right)^{\lambda(k')-\lambda(k)}[k : k'] \\ &\geq 2^{\lambda(k')-\lambda(k)}\left([k : k']\right)^{\lambda(k')-\lambda(k)+1},\end{aligned}$$

where the inequality follows from our assumption that $\alpha \notin k'$ and therefore

$$2[k : k'(\alpha)] \leq [k : k']. \qquad \square$$

The proof of Lemma 7.2 explains the reason why the factor 2 in the definition of the function $\aleph$ cannot be replaced by a larger number. Unlike the inequality (7.2) which holds for every $k' \subseteq k$, we could have

$$D_{k'} < D_k^{\aleph(k')} \quad \text{or} \quad D_{k'} \geq D_k^{\aleph(k')}.$$

In fact, we have

$$1 = D_{\mathbb{Q}} < D_k^{\aleph(\mathbb{Q})} \quad \text{and} \quad D_k = D_k^{\aleph(k)}.$$

Therefore there exists a *maximal* field $k^* \in \mathcal{I}(k)$, with $k^* \neq k$ such that

$$D_{k^*} < D_k^{\aleph(k^*)},$$

where by *maximal* we mean that if $k^* \subseteq k' \subseteq k$ and $k^* \neq k'$ then

$$D_{k'} \geq D_k^{\aleph(k')}.$$

It could happen that all proper subfields of k have large enough absolute discriminant so that $k^* = \mathbb{Q}$.

Now having a maximal subfield k^* of k fixed, we will find independent units $\beta_1, \ldots, \beta_{r(k^*)}$ in k^* and independent relative units $\psi_1, \ldots, \psi_{r(k/k^*)}$ in k that satisfy Proposition 3.1. By our choice of k^*, for every $\psi \in \{\psi_1, \ldots, \psi_{r(k/k^*)}\}$, we have

$$(7.6)\qquad D_{k^*} < D_k^{\aleph(k^*)} \qquad \text{and} \qquad D_{k^*(\psi)} \geq D_k^{\aleph(k^*(\psi))}.$$

By (1.1) and (3.2), and applying [1, Theorem 1.1] to the intermediate number field k^*, we have

$$(7.7)\qquad 0.2 < \prod_{i=1}^{r(k^*)} [k^* : \mathbb{Q}]h(\beta_i).$$

Let $\psi \in \{\psi_1, \ldots, \psi_{r(k/k^*)}\}$. By [11, Proposition 4.15]),

$$(7.8)\qquad D_k^{\aleph(k^*(\psi))} \leq D_{k^*(\psi)} \leq D_{k^*}^{[k^*(\psi):k^*]} D_{\mathbb{Q}(\psi)}^{[k^*(\psi):\mathbb{Q}(\psi)]}.$$

We will consider two cases. First we assume that $k^* = \mathbb{Q}$. By definition, we have

$$\aleph(\mathbb{Q}(\psi)) = (2[k:\mathbb{Q}(\psi)])^{\lambda(\mathbb{Q}(\psi))-\lambda(k)} \geq d^{1-\log_2 d},$$

where $d = [k:\mathbb{Q}]$. Therefore, by (7.8), we have

$$D_k^{d^{1-\log_2 d}} \leq D_k^{\aleph(\mathbb{Q}(\psi))} \leq D_{\mathbb{Q}(\psi)}. \tag{7.9}$$

For the second case, assume $k^* \neq \mathbb{Q}$. By (7.6) and (7.8), and since

$$[k^*(\psi):\mathbb{Q}(\psi)] \leq \frac{d}{2},$$

we have

$$\begin{aligned} D_k^{\aleph(k^*(\psi))} &\leq D_{k^*(\psi)} \leq D_{k^*}^{[k^*(\psi):k^*]} D_{\mathbb{Q}(\psi)}^{[k^*(\psi):\mathbb{Q}(\psi)]} \\ &< D_k^{\aleph(k^*)[k^*(\psi):k^*]} D_{\mathbb{Q}(\psi)}^{d/2} \\ &\leq D_k^{\aleph(k^*)[k:k^*]} D_{\mathbb{Q}(\psi)}^{d/2}. \end{aligned} \tag{7.10}$$

Therefore,

$$\log D_{\mathbb{Q}(\psi)} > \frac{2\left(\aleph(k^*(\psi)) - \aleph(k^*)[k:k^*]\right)}{d} \log D_k \tag{7.11}$$

Taking $k' = k^*$ in (7.4), we get

$$\begin{aligned} \aleph(k^*(\psi)) - \aleph(k^*)[k:k^*] &\geq 2^{\lambda(k^*)-\lambda(k)} \left([k:k^*]\right)^{\lambda(k^*)-\lambda(k)+1} \\ &\geq d^{\lambda(k^*)-\lambda(k)} \left(\frac{d}{2}\right), \end{aligned} \tag{7.12}$$

where the last inequality is a consequence of our assumption that $k^* \neq \mathbb{Q}$, and therefore $[k:k^*] \leq \frac{d}{2}$. By (7.11) and (7.12), we have

$$D_{\mathbb{Q}(\psi)} > D_k^{d^{\lambda(k^*)-\lambda(k)}} \geq D_k^{d^{1-\log_2 d}}. \tag{7.13}$$

Let $m = [\mathbb{Q}(\psi):\mathbb{Q}]$. By (5.17), we have

$$h(\psi) \geq \frac{\log \frac{D_{\mathbb{Q}(\psi)}}{m^m}}{2m(m-1)}.$$

This, together with (7.9) and (7.13), implies that

$$h(\psi) \geq \frac{\log \frac{D_k^{d^{1-\log_2 d}}}{m^m}}{2m(m-1)}.$$

If $k^* \neq \mathbb{Q}$ or $\mathbb{Q}(\psi) \neq k$, we have $m \leq \frac{d}{2}$, and therefore,

$$h(\psi) \geq \frac{2\log D_k^{d^{1-\log_2 d}} - d\log d}{d(d-2)}. \tag{7.14}$$

In case $k^* = \mathbb{Q}$ and $\mathbb{Q}(\psi) = k$, by (5.17), we obtain

$$h(\psi) \geq \frac{\log \frac{D_k}{d^d}}{2d(d-1)} > \frac{2\, \log D_k^{d^{1-\log_2 d}} - d \log d}{d(d-2)}.$$

Now Theorem 1.2 follows from Proposition 3.1, and by (7.7), (7.14), and noticing via $r(k^*) \leq \rho(k)$ that

$$r(k/k^*) \geq r(k) - \rho(k).$$

We conclude by noting that in case k^* is $\mathbb{Q}$ or a quadratic imaginary extension of $\mathbb{Q}$, we do not need to use Proposition 3.1 on existence of multiplicatively independent relative units with small heights. Instead, we can simply apply (3.2) that guarantees the existence of multiplicatively independent (ordinary) units with small heights.

Acknowledgements. The authors are grateful to the anonymous referee for helpful comments and suggestions.

References

[1] S. Akhtari & J. D. Vaaler, “Heights, regulators and Schinzel’s determinant inequality”, *Acta Arith.* **172** (2016), no. 3, p. 285-298.

[2] ———, “Independent relative units of low height”, *Acta Arith.* **2002** (2022), no. 4, p. 389-401.

[3] F. Amoroso & S. David, “Le théorème de Dobrowolski en dimension supérieure”, *C. R. Acad. Sci. Paris* **326** (1998), no. 10, p. 1163-1166.

[4] F. Amoroso & E. Viada, “Small points on subvarieties of tori”, *Comment. Math. Helv.* **87** (2012), no. 2, p. 355-383.

[5] E. Bombieri & W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, 2006.

[6] A. Costa & E. Friedman, “Ratios of regulators in totally real extensions of number fields”, *J. Number Theory* **37** (1991), no. 3, p. 288-297.

[7] ———, “Ratios of regulators in extensions of number fields”, *Proc. Am. Math. Soc.* **119** (1993), no. 2, p. 381-390.

[8] T. W. Cusick, “Lower bounds for regulators”, in *Number theory, Noordwijkerhout 1983*, Lecture Notes in Mathematics, vol. 1068, Springer, 1984, p. 63-73.

[9] E. Dobrowolski, “On a question of Lehmer and the number of irreducible factors of a polynomial”, *Acta Arith.* **34** (1979), p. 391-401.

[10] E. Friedman, “Analytic formulas for the regulator of a number field”, *Invent. Math.* **98** (1989), no. 3, p. 599-622.

[11] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer Monographs in Mathematics, Springer, 2010.

[12] M. E. Pohst, “Regulatorabschätzungen für total reelle algebraische Zahlkörper”, *J. Number Theory* **9** (1977), p. 459-492.

[13] R. Remak, “Über Grössenbeziehungen zwischen Diskriminante und Regulator eines algebraischen Zahlkörpers”, *Compos. Math.* **10** (1952), p. 245-285.

[14] J. H. Silverman, “The Thue equation and height functions”, in *Approximations diophantiennes et nombres transcendants*, Progress in Mathematics, vol. 31, Birkhäuser, 1983, p. 259-270.

[15] ———, “An inequality relating the regulator and the discriminant of a number field”, *J. Number Theory* **19** (1984), p. 437-442.

[16] P. M. Voutier, “An effective lower bound for the height of algebraic numbers”, *Acta Arith.* **74** (1996), no. 1, p. 81-95.

Shabnam Akhtari
Department of Mathematics,
University of Oregon,
Eugene, Oregon 97403 USA
E-mail: akhtari@uoregon.edu

Jeffrey D. Vaaler
Department of Mathematics,
University of Texas,
Austin, Texas 78712 USA
E-mail: vaaler@math.utexas.edu