Algebraic integers of small discriminant

by

Jeffrey Lin Thunder and John Wolfskill (DeKalb, Ill.)

Introduction. For an algebraic integer α generating a number field $K = \mathbb{Q}(\alpha)$, the discriminants of α and K are related by the equation

$$(1) \qquad\qquad D(\alpha) = D(K)(I(\alpha))^2,$$

where $I(\alpha) = [\mathfrak{O}_K : \mathbb{Z}[\alpha]]$, the index of the ring generated by α in the full ring of integers $\mathfrak{O}_K$ of K. Classically, the *index* of the field K is the greatest common divisor of all indices $I(\alpha)$ for $\alpha \in \mathfrak{O}_K$ with $K = \mathbb{Q}(\alpha)$. Dedekind was the first to show that the index may not be 1 by exhibiting certain cubic and quartic fields with this property. By results of Bauer and von Żyliński early this century, it is known that a rational prime p divides the index of some field of degree d if and only if $p < d$. Later work by Engstrom [2] investigated which powers of these primes may occur as common index divisors.

In contrast to the index of the field, we focus here on the minimal index of the primitive algebraic integers of the field, which we denote by $I(K)$. In other words,

$$I(K) = \min\{I(\alpha)\},$$

where the minimum is over all $\alpha \in \mathfrak{O}_K$ with $K = \mathbb{Q}(\alpha)$. The simplest situation is of course $I(K) = 1$, in which case $\mathfrak{O}_K$ is said to have a *power basis*. This happens trivially for any quadratic field, but when the degree of K is larger than 2 one does not expect this to be the case in general. In fact, much work has been done on the problem of classifying fields of certain types which have a power basis (in some cases with complete success). We refer the reader to the papers of Gras [3 and 4] and Cougnard [1] for more on this topic.

A natural question to ask, and the one which we address here, is how large $I(K)$ can be. In view of the remarks above on the index, this is only interesting when considering fields of degree less than a given bound. Here we determine upper bounds for $I(K)$ in terms of just the degree and discriminant of K, with sharper bounds using more properties of the field. We

also construct examples which indicate that these upper bounds are sharp, at least in terms of the discriminant.

Statement of results. In the results stated below, K is a number field of degree d and discriminant $D(K)$. We write $d = r + 2s$, where r is the number of real places and s is the number of complex places of K.

THEOREM 1. *Let $d > 2$, let c denote the maximum degree of a proper subfield of K, and let t be the minimum of c and $\log_2 d$. Then*

$$I(K) < (d^2 t(2/\pi)^{s/(d-c)})^{d(d-1)/2}|D(K)|^{(d^2-3d+2c)/(4d-4c)}.$$

Note that the exponent on the discriminant in the statement of Theorem 1 is between $(d-2)/4$ and $(d-2)/2$. The upper bound for $I(K)$ in Theorem 1 is largest when c is maximal, i.e., when $c = d/2$. In this case the exponent on the discriminant is $(d-2)/2$.

COROLLARY 1. *For any number field K*

$$I(K) < (d^2 \log_2 d)^{d(d-1)/2}|D(K)|^{(d-2)/2}.$$

The upper bound for $I(K)$ in Theorem 1 is smallest when K has no non-trivial subfields. This is the case, for example, when the degree d is prime.

COROLLARY 2. *If K has no proper subfields besides $\mathbb{Q}$, then*

$$I(K) < d^{d(d-1)}|D(K)|^{(d-2)/4}.$$

The general result of Corollary 1 can be sharpened if K has a real place.

THEOREM 2. *If K has at least one real place, then*

$$I(K) \leq ((2/\pi)^s 2^{d/2})^{d-1}|D(K)|^{(d-2)/2}.$$

For an arbitrary number field K, the upper bound on $I(K)$ in Theorem 1 may be far from the truth, since of course it could happen that $I(K) = 1$. Thus, a lower bound for $I(K)$ cannot be given in general, but only for fields of some particular type. To our knowledge, the only result in this direction is that of Hall [5] who showed that $I(K)$ can be arbitrarily large for pure cubic fields. This is in marked contrast to the known result that the index of such a field is either 1 or 2. Unfortunately, it would be very difficult to deduce an explicit lower bound for $I(K)$ strictly in terms of the discriminant by Hall's argument. We will discuss this in more detail later. When the degree is even, however, we can show that the dependence on the discriminant in the upper bound of Corollary 1 cannot be improved, at least in the absence of further information about the field.

THEOREM 3. *Let $d \geq 4$ be even. Then there are infinitely many fields K of degree d such that*

$$I(K) \gg |D(K)|^{(d-2)/2},$$

where the implicit constant depends only on d.

The implicit constant in Theorem 3 is actually determined by a particular choice of a certain field of degree $d/2$. This choice can be made canonically, so that the constant depends only on d. In the case $d = 4$ the lower bound of Theorem 3 can be achieved more simply (and the implicit constant made concrete) by considering pure quartic fields.

THEOREM 4. *For an odd rational prime p, the field $K = \mathbb{Q}(\sqrt[4]{2p^2})$ satisfies $I(K) = 2^{-11}|D(K)|$.*

Proof of Theorems 1 and 2. We begin with an effective version of the primitive element theorem.

LEMMA 1. *Let α, β be algebraic over $\mathbb{Q}$ with $\alpha \notin \mathbb{Q}$ and $\beta \notin \mathbb{Q}(\alpha)$. Let $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = e$. Then $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + z\beta)$ for some $z \in \mathbb{Z}$ satisfying $|z| < e^2/2$.*

P r o o f. Let $z \in \mathbb{Z}$ and suppose that $\alpha + z\beta$ is not a primitive element of $\mathbb{Q}(\alpha, \beta)$. Then either $z = 0$ or $\alpha + z\beta = \alpha^{(i)} + z\beta^{(j)}$ for some conjugates $\alpha^{(i)}$ of α and $\beta^{(j)}$ of β distinct from α and β, respectively. Thus, the number of such integers which fail to give a primitive element is no larger than $1 + (e/2 - 1)(e - 1)$. Since $e \geq 4$, there is an integer z with $\alpha + z\beta$ a primitive element and $|z| \leq 1 + (e/2 - 1)(e - 1)/2 < e^2/2$.

Now let the notation be as in the statement of Theorem 1. Denote the embeddings of K into $\mathbb{C}$ by $a \mapsto a^{(j)}$ for $1 \leq j \leq d$, and order these so that the first r are real and $a^{(j+s)} = \overline{a^{(j)}}$ for $r < j \leq r + s$. For $\mathbf{X} \in \mathbb{R}^d$ write

$$\mathbf{X} = (\mathbf{x}_1, \ldots, \mathbf{x}_{r+s}),$$

where

$$\mathbf{x}_j \in \begin{cases} \mathbb{R} & \text{if } j \leq r, \\ \mathbb{R}^2 & \text{otherwise.} \end{cases}$$

Define $\varrho : K \to \mathbb{R}^d$ by

$$\varrho(a) = (a^{(1)}, \ldots, a^{(r)}, \Re a^{(r+1)}, \Im a^{(r+1)}, \ldots, \Re a^{(r+s)}, \Im a^{(r+s)}).$$

Let $\Lambda = \varrho(\mathfrak{O}_K)$. This is a lattice of determinant $\det(\Lambda) = 2^{-s}|D(K)|^{1/2}$ ([6, Chap. V, §2, Lemma 2]). Let $B \subset \mathbb{R}^d$ be the convex body defined by

$$B = \{\mathbf{X} \in \mathbb{R}^d : |\mathbf{x}_j| \leq 1 \text{ for all } j\}.$$

Let $\lambda_1 \leq \ldots \leq \lambda_d$ be the successive minima of Λ with respect to B. By Minkowski's second convex bodies theorem (see [7]),

$$\lambda_1 \ldots \lambda_d \leq \frac{2^d \det(\Lambda)}{\mathrm{Vol}(B)} = (2/\pi)^s |D(K)|^{1/2}.$$

Further, we have $\lambda_1 = 1$ since $\varrho(1) \in B$ and $\varrho(a) \in \lambda B$ implies that the norm $N(a)$ of a satisfies $|N(a)| \leq \lambda^d$. Hence,

$$(2) \qquad \lambda_{c+1}^{d-c} \leq \prod_{j=c+1}^{d} \lambda_j \leq (2/\pi)^s |D(K)|^{1/2}.$$

Next, we choose successive elements $\alpha_1, \ldots, \alpha_u \in \mathfrak{O}_K$ with $u \leq t$ such that $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_u)$, $\alpha_1 \notin \mathbb{Q}$, $\alpha_{j+1} \notin \mathbb{Q}(\alpha_1, \ldots, \alpha_j)$, and $\varrho(\alpha_j) \in \lambda_{c+1}B$ for each j. These may be determined as follows (the choice is not unique). Let $\alpha_1 \in \mathfrak{O}_K \setminus \mathbb{Q}$ be such that $\varrho(\alpha_1) \in \lambda_2 B$ and let $L_1 = \mathbb{Q}(\alpha_1)$. If $L_1 = K$, stop. Otherwise, let $d_1 = [L_1 : \mathbb{Q}] < d$ and let $\alpha_2 \in \mathfrak{O}_K \setminus L_1$ with $\varrho(\alpha_2) \in \lambda_{d_1+1}B$. Such an α_2 must exist since at most d_1 elements of L_1 may be linearly independent over $\mathbb{Z}$. Let $L_2 = \mathbb{Q}(\alpha_1, \alpha_2)$. If $L_2 = K$, stop. Otherwise, continue in the same fashion, eventually getting $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_u)$. Note that $u \leq \log_2 d$. Further, $u \leq c$ since $d_{u-1} \leq c$ and $1, \alpha_1, \ldots, \alpha_{u-1}$ are elements of L_{u-1} which are linearly independent over $\mathbb{Z}$.

At this point we apply Lemma 1 to obtain a primitive element $\alpha \in \mathfrak{O}_K$ of the form $\alpha = \alpha_1 + z_2 \alpha_2 + \ldots + z_u \alpha_u$, where the z_j's are rational integers with $|z_j| < d^2/2$. We have $|\alpha^{(j)}| < \lambda_{c+1} t d^2/2$ for each j, so that

$$(3) \qquad |D(\alpha)| = \prod_{i<j} |\alpha^{(i)} - \alpha^{(j)}|^2 < (d^2 t \lambda_{c+1})^{d(d-1)}.$$

Theorem 1 follows from (1)–(3).

The proof of Theorem 2 is simpler than that given for Theorem 1 above, using only Minkowski's first theorem. With Λ as above and $1 > \varepsilon > 0$ we define $C \subset \mathbb{R}^d$ by

$$C = \{\mathbf{X} \in \mathbb{R}^d : |\mathbf{x}_1| \leq (2/\pi)^s |D(K)|^{1/2}(1-\varepsilon)^{1-d}, \; |\mathbf{x}_j| \leq 1-\varepsilon \text{ for } j > 1\}.$$

Then C is a convex body with volume $\mathrm{Vol}(C) = 2^d \det(\Lambda)$. By Minkowski's first convex bodies theorem (see [7]), there is a non-zero $\alpha \in \mathfrak{O}_K$ with $\varrho(\alpha) \in C$. We claim that $K = \mathbb{Q}(\alpha)$.

To see this claim, let v be the place of K corresponding to the embedding $a \mapsto a^{(1)}$. (Note that v is real by the hypothesis of Theorem 2 and our ordering of the embeddings.) If $K \neq \mathbb{Q}(\alpha)$, then v lies above a place w of $\mathbb{Q}(\alpha)$. Since both v and w are real, we have another place v' lying above w, whence another embedding $a \mapsto a^{(l)}$ with $l \neq 1$ and $|\alpha^{(1)}| = |\alpha^{(l)}|$. But then $|\alpha^{(1)}| < 1$ by the definition of C, which implies that $|N(\alpha)| < 1$. Since α is a non-zero integral element, this is impossible and we must have $K = \mathbb{Q}(\alpha)$.

Since α is a primitive element of K its discriminant from K to $\mathbb{Q}$ is not zero. Thus,

$$
\begin{aligned}
|D(\alpha)| &= \prod_{i \neq j} |\alpha^{(i)} - \alpha^{(j)}| \\
&\leq (2(2/\pi)^s |D(K)|^{1/2} (1 - \varepsilon)^{1-d})^{2d-2} (2(1 - \varepsilon))^{(d-1)(d-2)} \\
&= (2/\pi)^{2s(d-1)} (2/(1 - \varepsilon))^{d(d-1)} |D(K)|^{d-1}.
\end{aligned}
$$

By (1) we get

$$
I(K) \leq (2/\pi)^{s(d-1)} (2/(1 - \varepsilon))^{d(d-1)/2} |D(K)|^{(d-2)/2}.
$$

Theorem 2 follows by letting $\varepsilon \to 0$.

Proof of Theorems 3 and 4. Let $d = 2n$ with $n \geq 2$. The fields K of Theorem 3 will be constructed as imaginary quadratic extensions of a fixed totally real field of degree n. A preparatory result is needed first.

LEMMA 2. *Let L be a normal totally real field of degree n. Then there exists an $\alpha \in \mathfrak{O}_L$ which is totally positive and such that $L = \mathbb{Q}(\beta^2 \alpha)$ for any non-zero $\beta \in \mathfrak{O}_L$.*

P r o o f. Each ideal class of $\mathfrak{O}_L$ contains infinitely many primes of inertial degree one (see [6], Chap. VIII, §2). Therefore, for infinitely many rational primes p there is an $\alpha_p \in \mathfrak{O}_L$ with $|N(\alpha_p)| = p$, where N denotes the norm from L to $\mathbb{Q}$. Now each α_p has some pattern of signs for its conjugates $\alpha_p^{(1)}, \ldots, \alpha_p^{(n)}$, and there are only 2^n possible such patterns. Thus, there must be distinct rational primes p_1, p_2 for which $\alpha_{p_1}^{(j)}$ and $\alpha_{p_2}^{(j)}$ have the same sign for each j. Let $\alpha = \alpha_{p_1} \alpha_{p_2}$.

We have $\alpha \in \mathfrak{O}_L$ is totally positive by construction. Let $\beta \in \mathfrak{O}_L \setminus \{0\}$. The prime ideal (p_1) splits completely in $\mathfrak{O}_L$:

$$
(p_1) = \pi_1 \ldots \pi_n,
$$

where $\pi_1 = (\alpha_{p_1})$. This implies that the order at π_1 of $\alpha\beta^2$ is odd, whereas the order at π_j is even for $j > 1$. Thus, if $F = \mathbb{Q}(\alpha\beta^2)$ and P is the prime of $\mathfrak{O}_F$ lying below π_1, then π_1 is the only prime above P. Finally, as the local degree of π_1 over p_1 is 1, we get $F = L$.

Let L and α be as in Lemma 2. In what follows, the discriminant of $\sqrt{-\alpha}$ appears. This will depend only on d if one chooses L and α in some canonical way. For example, one could choose L with minimal conductor among all nth degree totally real subfields of cyclotomic fields. Once L is fixed, choose α among those elements satisfying Lemma 2 so that $|D(\sqrt{-\alpha})|$ is minimal.

Given L and α, let p be a rational prime which is unramified in L and relatively prime to the norm of 2α. Let $K = L(\sqrt{-p\alpha})$, an imaginary quadratic

extension of L of degree $d = 2n$. Letting $\gamma = \sqrt{-p\alpha}$ we have

$$1, \gamma, \gamma^2/p, \gamma^3/p, \ldots, \gamma^{d-2}/p^{n-1}, \gamma^{d-1}/p^{n-1}$$

are elements of $\mathfrak{O}_K$ which are linearly independent over $\mathbb{Z}$. Hence

(4) $\qquad |D(K)| \leq |\text{disc}(1, \gamma, \ldots, \gamma^{d-1}/p^{n-1})| = p^n |D(\sqrt{-\alpha})| \ll p^n,$

where the implicit constant depends only on d.

Now let $\theta \in \mathfrak{O}_K$ and assume that $K = \mathbb{Q}(\theta)$. We write θ in the form

$$\theta = a + b\sqrt{-p\alpha}, \quad a, b \in L, \ b \neq 0.$$

By considering the trace and norm of θ from K to L and our hypotheses on p, we find

(5) $\qquad\qquad\qquad\qquad 4\alpha b^2 \in \mathfrak{O}_L \setminus \{0\}.$

In particular, note that $4\alpha b^2$ satisfies the statements in Lemma 2.

For $x \in L$ we denote the conjugates of x over $\mathbb{Q}$ by $x^{(1)}, \ldots, x^{(n)}$. Similarly, we let $\theta^{(j)} = a^{(j)} + b^{(j)} \sqrt{-p\alpha^{(j)}}$. Then the d conjugates of θ over $\mathbb{Q}$ are $\theta^{(1)}, \ldots, \theta^{(n)}$ and their complex conjugates. Thus,

(6) $\quad |D(\theta)|$

$$= \prod_{j=1}^{n} |\theta^{(j)} - \overline{\theta^{(j)}}|^2 \cdot \prod_{j \neq l} |\theta^{(j)} - \theta^{(l)}|^2 \cdot |\theta^{(j)} - \overline{\theta^{(l)}}|^2$$

$$= \prod_{j=1}^{n} |2b^{(j)} \sqrt{-p\alpha^{(j)}}|^2 \cdot \prod_{j \neq l} |(a^{(j)} - a^{(l)}) + i\sqrt{p}(b^{(j)} \sqrt{\alpha^{(j)}} - b^{(l)} \sqrt{\alpha^{(l)}})|^2$$

$$\times |(a^{(j)} - a^{(l)}) + i\sqrt{p}(b^{(j)} \sqrt{\alpha^{(j)}} + b^{(l)} \sqrt{\alpha^{(l)}})|^2$$

$$\geq \prod_{j=1}^{n} |2\sqrt{(p\alpha b^2)^{(j)}}|^2$$

$$\times \prod_{j \neq l} |\sqrt{(p\alpha b^2)^{(j)}} - \sqrt{(p\alpha b^2)^{(l)}}|^2 \cdot |\sqrt{(p\alpha b^2)^{(j)}} + \sqrt{(p\alpha b^2)^{(l)}}|^2$$

$$= (p/4)^{n(2n-1)} |D(\sqrt{-4\alpha b^2})|$$

$$\geq p^{n(2n-2)} 2^{-2n(2n-1)} |D(K)|$$

by (4), (5), and the choice of α. Theorem 3 follows from (1), (4) and (6).

For the proof of Theorem 4, let p be an odd prime and let $\alpha = \sqrt[4]{2p^2}$. Let $K = \mathbb{Q}(\alpha)$. Then $1, \alpha, \alpha^2/p, \alpha^3/p$ are elements of $\mathfrak{O}_K$ which are linearly independent over $\mathbb{Z}$. Further,

$$\text{disc}(1, \alpha, \alpha^2/p, \alpha^3/p) = p^{-4} D(\alpha) = 2^{11} p^2.$$

Since $\alpha^2 = p\sqrt{2}$ and p is odd, p must ramify in K; therefore p^2 divides $D(K)$. Also, α satisfies an Eisenstein polynomial for the prime 2, so the powers of α constitute a 2-local integral basis. This shows that the four elements above constitute an integral basis for K, so that

$$(7) \qquad D(K) = 2^{11}p^2 = 2^{-11}I(\alpha).$$

Now let $\theta \in \mathfrak{O}_K$ be a primitive element of K and write $\theta = a + b\alpha$, where $a, b \in \mathbb{Z}[\sqrt{2}]$ and $b \neq 0$. Denoting conjugation in $\mathbb{Q}(\sqrt{2})$ by a superscript $'$, the four conjugates of θ are $a \pm b\alpha$ and $a' \pm b'i\alpha$. Thus,

$$
\begin{aligned}
(8) \quad |D(\theta)| \\
= |2b\alpha|^2 \cdot |2b'\alpha|^2 \cdot |(a-a') + (b-ib')\alpha|^2 \cdot |(a-a') + (b+b'i)\alpha|^2 \\
\times |(a-a') - (b+b'i)\alpha|^2 \cdot |(a-a') - (b-b'i)\alpha|^2 \\
= (2\alpha)^4 |N(b)|^2 \cdot |(a-a')^2 - (b-b'i)^2\alpha^2|^2 \cdot |(a-a')^2 - (b+b'i)^2\alpha^2|^2 \\
\geq 2^8 \alpha^{12} |N(b)|^6,
\end{aligned}
$$

where $N(b)$ denotes the norm of b from $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}$. From (1), (7) and (8) we get $I(\theta) \geq p^2$, proving Theorem 4.

Finally, we remark that obtaining lower bounds for $I(K)$ appears to be far more difficult when K has odd degree. To illustrate this point, consider the simple situation $K = \mathbb{Q}(\sqrt[3]{pq^2})$, where p and q are distinct primes with $p^2 \not\equiv q^2 \pmod 9$. A typical algebraic integer in K has the form

$$\theta = w + x\sqrt[3]{pq^2} + y\sqrt[3]{p^2q}$$

with $w, x, y \in \mathbb{Z}$, and it is straightforward to compute that

$$I(\theta) = |qx^3 - py^3|.$$

Thus, $I(K)$ is determined as the smallest non-zero integer, in absolute value, represented by the binary form $F(X, Y) = qX^3 - pY^3$. Hall in [5] showed that one can make $I(K)$ arbitrarily large by imposing successive congruence conditions on p and q, so that the Thue inequality $|F(x, y)| \leq m$ has no solutions for arbitrarily large m. It would be extremely difficult to quantify m in terms of the discriminant of F, much less to obtain such a result with m a power of the discriminant in analogy with Theorems 3 and 4.

The situation is similar in any cubic field, as Hall showed. Achieving a lower bound for $I(K)$ is equivalent to showing that a certain Thue inequality has no solutions. More generally for higher degrees, achieving a lower bound for $I(K)$ is equivalent to showing that a certain norm form inequality has no solutions. Generally speaking, such results are simply out of reach at the present time.

References

[1]   J. C o u g n a r d, *Sur la monogénéité de l'anneau des entiers d'une extension diédrale imaginaire de degré* 2*p* (*p premier*), Arch. Math. (Basel) 48 (1987), 223–231.

[2]   H. T. E n g s t r o m, *On the common index divisors of an algebraic field*, Trans. Amer. Math. Soc. 32 (1930), 223–237.

[3]   M.-N. G r a s, *Non monogénéité de l'anneau des entiers des extensions cycliques de* $\mathbb{Q}$ *de degré premier* $l \geq 5$, J. Number Theory 23 (1986), 347–353.

[4]   M.-N. G r a s et F. T a n o é, *Corps biquadratiques monogènes*, Manuscripta Math. 86 (1995), 63–79.

[5]   M. H a l l, *Indices in cubic fields*, Bull. Amer. Math. Soc. 43 (1937), 104–108.

[6]   S. L a n g, *Algebraic Number Theory*, Springer, New York, 1986.

[7]   G. L e k k e r k e r k e r, *Geometry of Numbers*, Wolters-Noordhoff, Groningen, 1969.

Department of Mathematics
Northern Illinois University
DeKalb, Illinois 60115
U.S.A.
E-mail: jthunder@math.niu.edu
        wolfskil@math.niu.edu