MATHEMATICS OF COMPUTATION
VOLUME 38, NUMBER 158
APRIL 1982, PAGES 627-632

The Computation of a Certain Metric Invariant of an Algebraic Number Field

By Horst Brunotte

Abstract. Let F be an algebraic number field and denote by $N(a)$ the absolute norm and by $\overline{a}$ the maximum of the absolute values of the conjugates of the element a of F. Define c_F to be the best possible constant with the property: For every $a \in F$ there exists a unit u of F such that $\overline{ua} \leqslant c_F N(a)^{1/[F:\mathbf{Q}]}$. An algorithm for the computation of c_F is described and some examples are given.

1. Introduction. Let F be an algebraic number field of degree d over the field of rational numbers $\mathbf{Q}$, U the group of units of F, and $\sigma_1,\ldots,\sigma_r$ a full set of representatives of nonconjugate embeddings of F into the field of complex numbers $\mathbf{C}$. We denote by c_F the best possible constant with the property: For every $a \in F$ there exists a unit $u \in U$ such that

$$\max\{|\sigma_1(ua)|,\ldots,|\sigma_r(ua)|\} \leqslant c_F N(a)^{1/d};$$

here $N(b)$ is the absolute value of the usual norm of the element b of F.

The existence of and upper bounds for c_F are well known (e.g., [6, p. 526]; [7, p. 351]; [9, p. 22]; [10, p. 271]; [13, p. 260]), and it was shown in [3] that the constant c_F can be computed effectively. Further some properties and an application of c_F were investigated, and the value of c_F was given for the case $r \leqslant 2$.

In the present note an algorithm for the computation of c_F for the case $r > 2$ is described. However, this algorithm works well only if the degree and the absolute value of the discriminant D of F are small; this is mainly due to the fact (see the first step of the algorithm in Section 3) that the computation of a full system of nonequivalent integers of F of absolute norm $\leqslant (2/\pi)^t\sqrt{|D|}$ (t = number of complex primes of F) may require much computation time. Therefore the algorithm is used here to find the constant c_F for some cyclotomic fields of small degree (see Table 2).

As a by-product of these computations, it is shown that the algorithm proposed by W. E. H. Berwick [1] for the computation of fundamental units of F for the case $r = 3$ cannot be generalized for $r > 3$ (see Section 5 for details).

It should be noted that one can define a similar constant $c_F(U_0)$ for any subgroup U_0 of finite index in U. It can be derived easily from [3] that the analogue of Algorithm C below will also give the constant $c_F(U_0)$.

Received October 15, 1980; revised June 10, 1981.
1980 *Mathematics Subject Classification.* Primary 12A45.

2. Auxiliary Results and an Upper Bound for c_F. Let $e_i = 1$ if σ_i is real, $e_i = 2$ if σ_i is complex, $a^{(i)} = \sigma_i(a)$ $(i = 1,\ldots,r)$ and $\overline{a} = \max\{|a^{(1)}|,\ldots,|a^{(r)}|\}$ $(a \in F)$. For $(b_1,\ldots,b_r) \in \mathbf{R}^r$ we denote by $U(b_1,\ldots,b_r)$ the set of units u of F such that $|u^{(i)}| \leqslant b_i$ $(i = 1,\ldots,r)$. We shall assume throughout that $u_1,\ldots,u_{r-1}$ is a fundamental system of units of F, and for $u \in U$ we denote by $\nu_1(u),\ldots,\nu_{r-1}(u) \in \mathbf{Z}$ the exponents in the representation $u = wu_1^{\nu_1(u)} \cdot \cdots \cdot u_{r-1}^{\nu_{r-1}(u)}$ with w a root of unity in F.

The results of the following lemmas are used for the computation of c_F; their proofs are left to the reader.

LEMMA 1. *Let $b_1,\ldots,b_r \in \mathbf{R}_+$, $u \in U(b_1,\ldots,b_r)$, and let $(a_{\rho i})_{\rho,i=1,\ldots,r-1}$, be the inverse of the (regular) $(r-1) \times (r-1)$-matrix*

$$\begin{pmatrix} e_1 \log\left|u_1^{(1)}\right| & \cdots & e_1 \log\left|u_{r-1}^{(1)}\right| \\ \vdots & & \vdots \\ e_{r-1} \log\left|u_1^{(r-1)}\right| & \cdots & e_{r-1} \log\left|u_{r-1}^{(r-1)}\right| \end{pmatrix}.$$

Then the following inequalities hold:

$$\left|\nu_\rho(u)\right| \leqslant \sum_{i=1}^{r-1} |a_{\rho i}| \max\left\{e_i \log b_i,\ \sum_{\substack{j=1\\ j\neq i}}^{r} e_j \log b_j\right\} \qquad (\rho = 1,\ldots,r-1),$$

$$\sum_{\rho=1}^{r-1} \nu_\rho(u) \log\left|u_\rho^{(r)}\right| \leqslant \log b_r.$$

COROLLARY. *Let $F/\mathbf{Q}$ be Galois, $u \in U$, and assume that for every $\rho, \tau \in \{1,\ldots, r-1\}$ there exists an automorphism σ of F such that $|\nu_\tau(\sigma u)| = |\nu_\rho(u)|$. Then for $\rho = 1,\ldots,r-1$,*

$$\left|\nu_\rho(u)\right| \leqslant e_1(r-1)(\log\overline{u})\min\left\{\sum_{i=1}^{r-1} |a_{ki}| \;\middle|\; k = 1,\ldots,r-1\right\},$$

where $(a_{ki})_{k,i=1,\ldots,r-1}$ is the matrix defined in Lemma 1.

Remark. In special cases the bounds for the ν_ρ's may be sharpened as the following example shows. Let $\mathbf{Q}^{(n)}$ be the nth cyclotomic field, U_n the units and W_n the roots of unity of $\mathbf{Q}^{(n)}$, $m = \varphi(n)/2$ (Euler's φ-function) and $b \in \mathbf{R}$, $b > 1$. For $n = 7, 11, 13$ using the fundamental system of units of $\mathbf{Q}^{(n)}$ as described in Table 2 (see Section 4) and the Galois module structure of U_n, one can find a full system of representatives of nonconjugate $u \in U_n$ modulo W_n with $1 < \overline{u} \leqslant b$ by checking all integral $\nu_1,\ldots,\nu_{m-1}$ which satisfy conditions (i), (ii), (iii):

(i) $|\nu_\rho| \leqslant 2(m-1)(\log b)\min\{\sum_{i=1}^{m-1} |a_{ki}| \mid k = 1,\ldots,m-1\}$ $(\rho = 1,\ldots,m-1)$,

(ii) $\sum_{\rho=1}^{m-1} \nu_\rho \log|u_\rho^{(m)}| \leqslant \log b$,

(iii) $\nu_1 \geqslant 1$.

For let $n = 7$ (the other cases are dealt with similarly) and let $u \in U_7$ such that $1 < \overline{u} \leqslant b$. Using the fundamental system of units of $\mathbf{Q}^{(7)}$, as given in Table 2, the conjugates of $u = u_1^{\nu_1}u_2^{\nu_2}$ are $u' = u_1^{\nu_2}u_2^{-\nu_1-\nu_2}$ and $u'' = u_1^{-\nu_1-\nu_2}u_2^{\nu_1}$. It suffices to show that one of the pairs $(\nu_1(u), \nu_2(u))$, $(\nu_1(u'), \nu_2(u'))$, $(\nu_1(u''), \nu_2(u''))$ satisfies condition (iii) above, because by Lemma 1 and its corollary each of these three pairs satisfies (i) and (ii). If $\nu_1 \geqslant 1$, the first pair will do. If $\nu_1 = 0$, choose either the second or the third pair according as $\nu_2 > 0$ or $\nu_2 < 0$. In case $\nu_1 < 0$, take the second pair if $\nu_2 > 0$ and the third pair otherwise.

LEMMA 2. *Let $u \in U$, $\rho \in \{1,\dots,r-1\}$, $v_k = u_\rho^k u$ for $k \in \mathbf{Z}$, and suppose $\overline{v_1} \geqslant \overline{v_0}$. Then $\overline{v_k} \geqslant \overline{v_0}$ for all $k \in \mathbf{N}$.*

LEMMA 3 (B. L. VAN DER WAERDEN [13]). *Let D be the discriminant of F, t the number of complex primes of F, $g_F = (2/\pi)^t\sqrt{|D|}$, R the ring of integers of F, and $a_1,\dots,a_s \in R$ a full set of representatives of nonassociate $a \in R \setminus \{0\}$ such that $N(a) \leqslant g_F$. For each $j \in \{1,\dots,r\}$ there exists a unit $u \in U$ such that $|u^{(i)}| < 1$ for $i \neq j$ and*

$$|u^{(j)}| \leqslant \left(g_F \max\left\{\left|a_l^{(k)}\right|^{-d} \middle| l = 1,\dots,s;\ k = 1,\dots,r\right\}\right)^{1/e_j}.$$

The proof of the following proposition, which gives an upper bound for c_F, is analogous to that of the first part of [10, Satz 8] and will be omitted.

PROPOSITION 1.

$$c_F \leqslant \max_{i=1,\dots,r}\left\{\prod_{\rho=1}^{r-1}\max\left\{1, \left|u_\rho^{(i)}\right|\right\}\right\}.$$

Examples. Using the units (or their inverses) of $\mathbf{Q}^{(p)}$, as given in Table 2 below, the following upper bounds for $c_{\mathbf{Q}^{(p)}}$ for primes p with $7 \leqslant p \leqslant 19$ can be obtained (see Table 1).

TABLE 1

p	upper bound for $c_{\mathbf{Q}^{(p)}}$
7	2.246 980
11	5.432 324
13	7.345 947
17	18.048 74
19	30.037 10

3. Outline of the Algorithm. The algorithm for the computation of c_F will be given in the style of Knuth [8]. It was shown in [3] that this algorithm does in fact yield the constant c_F.

ALGORITHM C (*Computation of* c_F).

C 1. (Computation of units $v_1,\dots,v_r \in U$ with the property $|v_\rho^{(j)}| < 1$ for $\rho, j = 1,\dots,r$; $\rho \neq j$.) Compute a full system of representatives $a_1,\dots,a_s \in R$ of the nonassociate $a \in R \setminus \{0\}$ such that $N(a) \leqslant g_F$ (see Lemma 3). Put

$$b_j = \left(g_F \max\left\{|a_l^{(k)}|^{-d} \middle| l = 1,\dots,s;\ k = 1,\dots,r\right\}\right)^{1/e_j} \qquad (j = 1,\dots,r).$$

Apply Lemmas 1 and 2 to find $v_1,\dots,v_r$ in the set $U(b_1,\dots,b_r)$. (Remark. As the bounds $b_1,\dots,b_r$ given in C 1 may be much too large, one should first compute the units $u \in U(b_1,\dots,b_r)$ with small $\nu_1(u),\dots,\nu_{r-1}(u)$.)

TABLE 2

n	$u_1,\dots,u_{m-1}$	$u_{11},\dots,u_{1,m-1}$	$c_{\mathbf{Q}^{(n)}}$
7	$u_1 = \dfrac{\sin(2\pi/7)}{\sin(\pi/7)}$	$0.445\dots$	$(u_{13}u_{23})^{1/3} = 1.593\,845\dots$
	$u_2 = \dfrac{\sin(3\pi/7)}{\sin(\pi/7)}$	$1.24\dots$	
		$1.80\dots$	
9	$u_1 = -\omega_9^{(2)}$	$1.87\dots$	$(u_{11}u_{13}^{-1})^{1/3} = 1.755\,652\dots$
	$u_2 = \omega_9^{(1)} + \omega_9^{(2)}$	$1.53\dots$	
		$0.347\dots$	
11	$u_\rho = \dfrac{\sin((\rho+1)\pi/11)}{\sin(\pi/11)}$	$1.68\dots$	$(u_{12}u_{13}u_{15}^{2}u_{22}^{-1}u_{25}^{-1}u_{33}^{-1}u_{35}u_{42})^{1/5}$
	$(\rho = 1,\dots,4)$	$0.830\dots$	$= 1.901\,021\dots$
		$1.30\dots$	
		$0.284\dots$	
		$1.91\dots$	
13	$u_\rho = \dfrac{\sin((\rho+1)\pi/13)}{\sin(\pi/13)}$	$1.77\dots$	$(u_{11}^{2}u_{13}u_{14}u_{16}^{2}u_{34}^{-1}u_{41}^{-1}u_{43}^{-1})^{1/6}$
	$(\rho = 1,\dots,5)$	$1.13\dots$	$= 2.137\,071\dots$
		$0.709\dots$	
		$1.49\dots$	
		$0.241\dots$	
		$1.94\dots$	
15	$u_1 = 1 - \zeta_{15}$	$0.415\dots$	$(u_{11}^{-2}u_{14}^{-1})^{1/4} = 1.632\,900\dots$
	$u_2 = \dfrac{3+\sqrt{5}}{4} + \dfrac{1}{2}(\omega_{15}^{(2)} - \omega_{15}^{(7)})$	$1.98\dots$	
	$u_3 = \dfrac{3-\sqrt{5}}{4} + \dfrac{1}{2}(\omega_{15}^{(1)} - \omega_{15}^{(4)})$	$1.48\dots$	
		$0.813\dots$	
16	$u_1 = 1 + \sqrt{2} + \omega_{16}^{(1)}$	$4.26\dots$	$(u_{11}u_{12}^{-2}u_{14}^{-2})^{1/4} = 2.232\,495\dots$
	$u_2 = 1 - \sqrt{2} + \omega_{16}^{(5)}$	$1.17\dots$	
	$u_3 = 1 + \sqrt{2} + \omega_{16}^{(7)}$	$0.566\dots$	
		$0.351\dots$	
17	$u_\rho = \dfrac{\sin((\rho+1)\pi/17)}{\sin(\pi/17)}$		
	$(\rho = 1,\dots,7)$		
19	$u_\rho = \dfrac{\sin((\rho+1)\pi/19)}{\sin(\pi/19)}$		
	$(\rho = 1,\dots,8)$		
20	$u_1 = 1 - \zeta_{20}$	$0.312\dots$	$(u_{11}^{-1}u_{12}u_{21}^{-1}u_{23}^{-2})^{1/4} = 1.787\,799\dots$
	$u_2 = \dfrac{1+\sqrt{5}}{2} + \dfrac{1}{2}(\omega_{20}^{(1)} - \omega_{20}^{(9)})$	$0.907\dots$	
	$u_3 = \dfrac{1-\sqrt{5}}{2} + \dfrac{1}{2}(\omega_{20}^{(3)} - \omega_{20}^{(7)})$	$1.97\dots$	
		$1.78\dots$	

C 2. (Computation of the set $U' = U(\overline{v}_1,\dots,\overline{v}_r)$.) The set U' is computed by applying Lemmas 1 and 2.

C 3. (Computation of the sequence of successive minima of the absolute values of the conjugates of u^{-1}, $u \in U'$.) Do steps C 3.1, C 3.2, C 3.3 for $i = 1,\dots,r$, and then go to step C 4.

C 3.1 (Initialize). Put $k = 1$ and $a_{i,1} = \min\{|u^{(i)}|^{-1} \mid u \in U'\}$.

C 3.2 (Finding candidates for the next successive minimum). Define $A_{i,k} = \{|u^{(i)}|^{-1} \mid u \in U' \text{ and } 1 \leqslant |u^{(i)}| < a_{i,k}^{-1}\}$.

C 3.3 (Recurrence step). If $A_{i,k} = \varnothing$, put $q_i = k + 1$, $a_{i,k+1} = 1$, and take the next i. If $A_{i,k} \neq \varnothing$, put $a_{i,k+1} = \min A_{i,k}$, set $k \leftarrow k + 1$, and go to C 3.2.

C 4. (Definition of the set A.) Define

$$A = \left\{(a_1,\ldots,a_r) \in \prod_{i=1}^{r} \{a_{i,1},\ldots,a_{i,q_i}\} \mid \max\{a_1,\ldots,a_r\} = 1, \right.$$
$$\left. \max\left\{|u^{(1)}|a_1,\ldots,|u^{(r)}|a_r\right\} \geqslant 1 \text{ for all } u \in U'\right\}.$$

C 5. (Final step.) Put $c_F = (\min\{\prod_{i=1}^{r} a_i^{e_i} \mid (a_1,\ldots,a_r) \in A\})^{-1/d}$. (Remark. In some special cases one need not test every $(a_1,\ldots,a_r) \in A$ in order to find c_F; e.g., using the Galois group of $\mathbf{Q}^{(n)}$ in the examples mentioned below, one may restrict oneself to the case $a_1 = 1$.)

4. Examples. In this section we give the results of the computation of the constant $c_{\mathbf{Q}^{(n)}}$ of some cyclotomic fields $\mathbf{Q}^{(n)}$. For brevity we write $u_{\rho j} = |u_\rho^{(j)}|$, where $u_1,\ldots,u_{m-1}$ $(m = \varphi(n)/2)$ is the fundamental system of units of $\mathbf{Q}^{(n)}$ which is described in the second column of Table 2 (here we write $\omega_n^{(k)} = \zeta_n^k + \zeta_n^{-k}$, and ζ_n denotes a primitive nth root of unity); for these systems of fundamental units the reader is referred to [2, Kap. V], [4, pp. 91, 94], and [5, Kap. III, Satz 27], respectively. In order to fix the different embeddings of $\mathbf{Q}^{(n)}$ into $\mathbf{C}$, the first three digits of the absolute values of the conjugates of u_1 are listed in the third column of Table 2. Finally the first seven digits of $c_{\mathbf{Q}^{(n)}}$ for $6 \leqslant \varphi(n) \leqslant 12$ are given in the fourth column of Table 2.

Remarks. (i) In computing $c_{\mathbf{Q}^{(n)}}$, real numbers a and b with $|a - b| < m \cdot 10^{-15}$ were regarded as being equal.

(ii) The computations were carried out partly on the TR 445 of the Universität Düsseldorf and partly on the CYBER 76 of the Universität Köln.

5. Remark on an Algorithm of W. E. H. Berwick. Let F be an algebraic number field, and let $\sigma_1,\ldots,\sigma_r$ be a full set of representatives of nonconjugate embeddings of F into $\mathbf{C}$. For $\rho = 1,\ldots,r$, let

$$U_\rho = \left\{u \in U \,\middle|\, |\sigma_i(u)| < 1 \text{ for all } i \neq \rho\right\},$$

and choose $u_\rho \in U_\rho$ such that

$$|\sigma_\rho(u_\rho)| = \min\left\{|\sigma_\rho(u)| \,\middle|\, u \in U_\rho\right\}.$$

One may ask whether or not the set $\{u_1,\ldots,u_r\}$ contains a fundamental system of units of F.

This question was answered in the affirmative by W. E. H. Berwick [1] for the case $r = 3$; in fact he proved that any two elements of the set $\{u_1, u_2, u_3\}$ form a fundamental system of units of F (for an application of Berwick's algorithm see,e.g., [12]). However, it was conjectured (e.g., [11, p. 6.09]) that the answer to the above question should be no if $r > 3$. The following examples show the truth of this conjecture: Let V_n be the subgroup of U_n (see the remark following Lemma 1) generated by W_n and the conjugates of a unit $u \in U_n$ with the properties

(i) $|u^{(j)}| < 1$ for all $j > 1$,

(ii) $|u^{(1)}|$ minimal among all units in U_n which satisfy (i).

In the examples mentioned below u is unique up to roots of unity, and it is plain that Algorithm C also gives the unit u. The index $(U_n : V_n)$ for some n is listed in Table 3.

TABLE 3

n	11	13	15	16	20
$(U_n : V_n)$	11	14	4	4	3

6. Acknowledgement. I would like to express my thanks to Professor F. Halter-Koch for his constant interest in the computations described above and to Mr. Dirk Paggel for his help in implementing the programs on the computer. I thank the referee for valuable comments on the first draft of this note. Finally I am indebted to the Universität Essen—Gesamthochschule for the provision of computer time.

Haüs-Endt-Str. 88
D-4000 Düsseldorf 13
West Germany

1. W. E. H. BERWICK, "Algebraic number fields with two independent units," *Proc. London Math. Soc.*, v. 34, 1932, pp. 360–378.

2. S. I. BOREWICZ & I. R. ŠAFAREVIČ, *Zahlentheorie*, Birkhäuser, Basel-Stuttgart, 1966.

3. H. BRUNOTTE, "Bemerkungen zu einer metrischen Invarianten algebraischer Zahlkörper," *Monatsh. Math.*, v. 90, 1980, pp. 171–184.

4. H. HASSE, "Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern," *Abh. Deutsch. Akad. Wiss. Berlin Math.-Nat. Kl.* 1948, No. 2, 1950.

5. H. HASSE, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.

6. H. HASSE, *Zahlentheorie*, Akademie-Verlag, Berlin, 1969.

7. O. KÖRNER, "Erweiterter Goldbach-Vinogradovscher Satz in beliebigen algebraischen Zahlkörpern," *Math. Ann.*, v. 143, 1961, pp. 344–378.

8. D. E. KNUTH, *The Art of Computer Programming*, Vol. 2: *Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969.

9. G. J. RIEGER, "Über die Darstellung ganzer algebraischer Zahlen durch Quadrate," *Arch. Math.*, v. 14, 1963, pp. 22–28.

10. C. L. SIEGEL, "Darstellung totalpositiver Zahlen durch Quadrate," *Math. Z.*, v. 11, 1921, pp. 246–275.

11. R. SMADJA, *Calculs Effectifs sur les Idéaux des Corps de Nombres Algébriques*, Univ. D'Aix-Marseille, U.E.R. Sci. de Luminy, 1976.

12. E. THOMAS, "Fundamental units for orders in certain cubic number fields," *J. Reine Angew. Math.*, v. 310, 1979, pp. 33–35.

13. B. L. VAN DER WAERDEN, "Ein logarithmenfreier Beweis des Dirichletschen Einheitensatzes," *Abh. Math. Sem. Univ. Hamburg*, v. 6, 1928, pp. 259–262.