MATHEMATICS OF COMPUTATION
VOLUME 44, NUMBER 170
APRIL 1985, PAGES 495-518

On Totally Real Cubic Fields

By Veikko Ennola and Reino Turunen

Abstract. The authors have constructed a table of the 26440 nonconjugate totally real cubic number fields of discriminant $D < 500000$ thereby extending the existing table of fields with $D < 100000$ by I. O. Angell [1]. Serious defects in Angell's table are pointed out. For each field, running number, discriminant, coefficients of a generating polynomial, integral basis, class number, and a fundamental pair of units are listed. The article contains statistics about the following subjects: distribution of class numbers; fields in which every norm-positive unit is totally positive; nonconjugate fields with the same discriminant; fields with noncyclic class group. The fields are tabulated by means of a method due to Davenport and Heilbronn [7], [8] which leads to a unique normalized generating polynomial. The given units are chosen so that the fundamental parallelogram of the unit lattice determined by the corresponding vectors in the logarithmic space is reduced.

1. Introduction. A table of totally real cubic fields of discriminant $D < 100000$ has previously been constructed by I. O. Angell [1]. In this article we shall describe the construction of an extended table for $D < 500000$. It has been deposited in the Mathematics of Computation's UMT-depository.

The motive for this work stems firstly as a by-product from the first author's wish to investigate certain parametric families of totally real cubic fields with small fundamental pairs of units and large class number, and secondly from the fact that serious defects have been discovered in Angell's table. A list of such defects which have come to our attention is as follows.

(1) There are 11 fields missing. These fields have discriminants 25717, 32404, 35996, 37108, 37133, 38905, 39992, 43165, 43173, 43176, 95484. The omission of the first field has been discovered by Franz Halter-Koch and has evidently been corrected in later versions of the table. The omission of the other ten fields has previously been independently discovered by Llorente and Oneto [15].

(2) The field with discriminant 88588 appears twice.

(3) In "Appendix of units with large coefficients" there are two errors. For $D = 81377$, the first number, and for $D = 82657$, the second one are not units: they both have norms divisible by 10.

(4) In the statistics referring to the class numbers [1, p. 186] there are several mistakes as discovered by Llorente and Oneto [15]. They give a revised version of these statistics which, however, is not fully in accordance with our results (see Section 7 below for details).

Received April 11, 1983; revised March 14, 1984.
1980 *Mathematics Subject Classification.* Primary 12A30, 12-04, 12A45, 12A50.

(5) Angell's adaptation of the Voronoi algorithm does not necessarily produce a fundamental pair of units (e.g., in the case $D = 39601 = 199^2$, the given units together with -1 generate a subgroup of index 3 in the group of units). This observation was made by M. N. Gras.

The method we have used in order to tabulate the fields is due to Davenport and Heilbronn [7], [8]. It is different from that of Angell, but a somewhat similar approach has previously been used by Llorente and Oneto [15]. As was shown by Davenport and Heilbronn, there exists a bijective discriminant-preserving map of the set of triplets of conjugate totally real cubic fields onto a subset $\mathscr{R}$ of the set of reduced integral primitive irreducible binary cubic forms. Here we have to modify slightly the classical concept of a reduced cubic form [10, Chapter XII] in order to have just a single one contained in each equivalence class. The local conditions of Davenport and Heilbronn, which are necessary and sufficient for a reduced form to belong to $\mathscr{R}$, are given below in a simplified form.

In the search for all forms in $\mathscr{R}$ with discriminants in a given range it is useful to have stringent limitations for their coefficients. We therefore present a collection of best possible inequalities satisfied by those coefficients.

From a form in $\mathscr{R}$ we construct a monic cubic polynomial with integral coefficients in an obvious manner. A polynomial obtained in that way is called a normalized cubic polynomial (NCP) and its zeros are termed normalized primitive elements (NPE). Hence, a noncyclic field is generated by a unique naturally defined NPE, while a cyclic field contains three such elements. We show that if α is an NPE of a field K, the conjugates of α have least standard deviation among all irrational algebraic integers β of K, and that this property is shared only by certain particular β's naturally related with α. If K is cyclic then, apart from sign, the NPE's are equal to the Gaussian periods for a generating cubic character of K.

Our method thus leads automatically to a complete set of different fields: in particular, no Tschirnhausen transformation or any other means are needed to test the fields for being distinct. Moreover, an integral basis of K and the value of the discriminant are readily at hand.

In order to compute the class number (class group structure) and a fundamental pair of units, we have used the classical Voronoi algorithm [9, Chapter IV]. It works very efficiently, the only drawback being the rather high degree of precision needed in a few cases due to the largeness of the units produced by the algorithm. In the unit lattice we have performed a reduction process to the effect that the final units to be listed in the table (called reduced units) are so chosen that the fundamental parallelogram of the lattice determined by the corresponding vectors in the logarithmic space is reduced. In this way we find a naturally defined fundamental pair of units, the choice of which is optimal in a certain sense.

For the extended range we give similar statistics as the one in [1] and [15] already discussed. The total number of nonconjugate fields with discriminants less than 500000 is 26440 giving the empirical density 0.05288, whereas Davenport and Heilbronn [8] proved that the asymptotic value is $(12\ \zeta(3))^{-1} = 0.06933$. So the convergence is very slow as noted in [17].

At the end of the article, there are tables of fields in which every unit is totally positive or totally negative, of nonconjugate fields with the same discriminant, and of fields with noncyclic class group. The last property is a very rare one; we have encountered only 35 such cases.

All of the computations were done on the DEC-20 computer at the University of Turku, Finland.

We would like to thank Mme. M. N. Gras, Dr. Jukka Pihko, and Professors Harvey Cohn, H. J. Godwin, Franz Halter-Koch, and Jacques Martinet for their assistance and helpful comments. We are especially indebted to the members of the staff of the Computer Centre at the University of Turku for their cooperation. The work has been supported financially by the Academy of Finland.

For any cubic field K we denote by $\mathcal{O} = \mathcal{O}_K$ the ring of integers of K. If $\beta \in K$, its conjugates are denoted either by β, β', β'' or by $\beta^{(i)}$ ($i = 0, 1, 2$; $\beta^{(0)} = \beta$). The trace and norm of β are $\operatorname{Tr}(\beta) = \beta + \beta' + \beta''$ and $N(\beta) = \beta\beta'\beta''$. We also write $N(\mathfrak{A})$ for the norm of a nonzero fractional ideal $\mathfrak{A}$ of K. The symbol □ indicates the end of a proof.

2. Reduction of Binary Cubic Forms. We shall assume in the sequel that the binary cubic forms

$$F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \tag{2.1}$$

which we are dealing with are (i) *integral*, i.e., $a, b, c, d \in \mathbf{Z}$; (ii) *primitive*, i.e., $\gcd(a, b, c, d) = 1$; (iii) *irreducible* in the ring $\mathbf{Q}[x, y]$; and (iv) have *positive discriminant*

$$D(F) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd. \tag{2.2}$$

Accordingly, when speaking simply of cubic forms we always assume that the form is binary and that these conditions are satisfied. Equivalence of forms (both cubic and quadratic) and equivalence class are understood in the wide sense, i.e., homogeneous linear substitutions with integral coefficients and determinant $= \pm 1$ are admitted. If determinant $= +1$ is required, we expressly speak of proper equivalence and proper class. The cubic form (2.1) has the quadratic covariant

$$H(x, y) = Tx^2 + Uxy + Vy^2, \tag{2.3}$$

where

$$T = b^2 - 3ac, \quad U = bc - 9ad, \quad V = c^2 - 3bd. \tag{2.4}$$

It is well-known that the quadratic form (2.3) is positive definite and its discriminant is

$$U^2 - 4TV = -3D(F) < 0. \tag{2.5}$$

According to the classical reduction theory of Arndt [2] and Hermite [13] the form (2.1) is called reduced iff (2.3) is a reduced quadratic form, i.e., either $-T < U \leqslant T < V$ or $0 \leqslant U \leqslant T = V$. In the following theorem we introduce a slightly modified concept in order to obtain a unique representative for each class.

THEOREM 1. *Every equivalence class $\mathscr{C}$ of binary cubic forms contains exactly one* REDUCED FORM $F(x, y) = F_{\mathscr{C}}(x, y)$ *satisfying one of the following conditions*:

(i) $-T < U < T < V$, $a > 0$, *and either* $b > 0$ *or* $b = 0$ *and* $d > 0$,

(ii) $0 < U = T < V$, $a > 0$, *and* $b > 3a/2$,

(iii) $0 < U < T = V$, $a > 0$, *and* $|d| > a$,

(iv) $0 = U < T = V$, $a > 0$, *and* $d < -a$,

(v) $0 < U = T = V$, $a > 0$, *and* $b > 3a/2$.

Proof. Let $\mathscr{C}$ be given. By the classical theory referred to above, we can pick a form $F(x, y) \in \mathscr{C}$ such that $-T < U \leqslant T < V$ or $0 \leqslant U \leqslant T = V$. Applying the substitution $x = -x', y = -y'$ if necessary, we may suppose that $a > 0$.

Case 1. $-T < U < T < V$. Clearly, either $F(x, y)$ or $F(x, -y)$ satisfies the conditions (i) and is thus the required $F_{\mathscr{C}}(x, y)$. Let $H_{\mathscr{C}}(x, y)$ denote the quadratic covariant of $F_{\mathscr{C}}(x, y)$. Suppose that $F_1(x, y)$ is another form in $\mathscr{C}$ satisfying (i) and let $H_1(x, y)$ denote its quadratic covariant. Since F_1 and $F_{\mathscr{C}}$ are equivalent, so are their quadratic covariants, and hence $H_1(x, y)$ is properly equivalent to $H_{\mathscr{C}}(x, y)$ or to $H_{\mathscr{C}}(x, -y)$. Since all three quadratic forms are reduced, either $H_1(x, y) = H_{\mathscr{C}}(x, y)$ or $H_1(x, y) = H_{\mathscr{C}}(x, -y)$. Let τ denote a substitution with determinant $= +1$ transforming $F_1(x, y)$ correspondingly into $F_{\mathscr{C}}(x, y)$ or $F_{\mathscr{C}}(x, -y)$ so that τ is an automorph of $H_1(x, y)$. By [11, p. 72, Theorem 57] τ is either the identity or $[x = -x', y = -y']$. The latter alternative is impossible because the leading coefficients are positive, and therefore $F_1(x, y) = F_{\mathscr{C}}(x, y)$ or $F_{\mathscr{C}}(x, -y)$. However, $F_{\mathscr{C}}(x, -y)$ does not satisfy (i). This proves the uniqueness of $F_{\mathscr{C}}$.

Case 2. $U = T < V$. The quadratic covariant of the form $F_1(x, y) = F(x, -y)$ is $H_1(x, y) = Tx^2 - Txy + Vy^2$. Then, $H_1(x + y, y) = Tx^2 + Txy + Vy^2$ is a reduced quadratic form. Consider therefore the corresponding cubic form

$$F_2(x, y) = F(x + y, -y) = ax^3 + (3a - b)x^2y$$
$$+ (3a - 2b + c)xy^2 + (a - b + c - d)y^3.$$

Suppose that $b = 3a/2$. From $U = T$, we then have $d = -a/4 + c/2$ so that $F_2(x, y) = F(x, y)$. However, it is easy to see that $F(x, y)$ would be divisible by $2x + y$ in the ring $\mathbf{Q}[x, y]$. Therefore, $b \neq 3a/2$ and either $F(x, y)$ or $F_2(x, y)$ satisfies (ii) depending upon whether $b > 3a/2$ or $b < 3a/2$.

The same argument as in the preceding case shows that any form contained in $\mathscr{C}$ and satisfying (ii) must coincide with $F_{\mathscr{C}}(x, y)$ or with $F_{\mathscr{C}}(x + y, -y)$. Since the latter form does not satisfy (ii) the uniqueness of $F_{\mathscr{C}}$ follows.

Case 3. $0 < U < T = V$. In this case $H(x, y) = Tx^2 + Uxy + Ty^2$. Consider the transformed cubic form

$$F_1(x, y) = F((\operatorname{sgn} d)y, (\operatorname{sgn} d)x)$$
$$= (\operatorname{sgn} d)\left(dx^3 + cx^2y + bxy^2 + ay^3\right)$$

the quadratic covariant of which coincides with $H(x, y)$.

Suppose first that $d = a$. From $T = V$ it then follows that $(b - c)(3a + b + c) = 0$. We cannot have $b = c$ otherwise $F(x, y)$ would be divisible by $x + y$. From $3a + b + c = 0$ we infer $U = -9a^2 - 3ab - b^2 < 0$ contrary to the assumption.

Suppose next that $d = -a$. From $T = V$ we get $(b + c)(3a - b + c) = 0$. We cannot have $b = -c$ otherwise $F(x, y)$ would be divisible by $x - y$. From $3a - b + c = 0$ it follows that $U = 9a^2 - 3ab + b^2 = T$, contradicting the assumption.

Therefore, $|d| \neq a$ and either $F(x, y)$ or $F_1(x, y)$ satisfies (iii). The uniqueness of $F_{\mathscr{C}}(x, y)$ is proved as before.

Case 4. $0 = U < T = V$. The following general identities are valid in each case

$$cT - bU + 3aV = 0, \tag{2.6}$$

$$3dT - cU + bV = 0. \tag{2.7}$$

In Case 4 we find from these identities that $c = -3a$, $b = -3d$. Therefore, $F(x, y)$ is of the form

$$F(x, y) = ax^3 - 3dx^2y - 3axy^2 + dy^3.$$

Clearly $d \neq \pm a$ because $F(x, y)$ is irreducible in $\mathbf{Q}[x, y]$. Now the cubic forms

$$\begin{aligned} &F(x, y) = ax^3 - 3dx^2y - 3axy^2 + dy^3,\\ &F(x, -y) = ax^3 + 3dx^2y - 3axy^2 - dy^3,\\ &F((\operatorname{sgn} d)y, (\operatorname{sgn} d)x) = (\operatorname{sgn} d)(dx^3 - 3ax^2y - 3dxy^2 + ay^3),\\ &F(-(\operatorname{sgn} d)y, (\operatorname{sgn} d)x) = (\operatorname{sgn} d)(dx^3 + 3ax^2y - 3dxy^2 - ay^3), \end{aligned} \tag{2.8}$$

are contained in $\mathscr{C}$ and exactly one of them satisfies (iv). By changing the notation if necessary we may assume that this form is $F(x, y)$. We have thus found $F_{\mathscr{C}}(x, y) = F(x, y)$ with quadratic covariant $H(x, y) = T(x^2 + y^2)$.

Suppose now that $F_1(x, y)$ is another form in $\mathscr{C}$ satisfying (iv) and let $H_1(x, y)$ denote its quadratic covariant. Since $H_1(x, y)$ and $H(x, y)$ are equivalent reduced quadratic forms and $H(x, y)$ is improperly equivalent to itself, we must have $H_1(x, y) = H(x, y)$. Let τ denote a substitution with determinant $= +1$ transforming $F_1(x, y)$ into $F(x, y)$ or $F(x, -y)$. Then τ is an automorph of $H(x, y)$ and by [11, loc.cit.] τ is one of the following four substitutions:

$$[x = x', y = y'], \quad [x = -x', y = -y'], \quad [x = y', y = -x'],$$
$$[x = -y', y = x'].$$

Taking into account that the leading coefficients of $F_1(x, y)$ and $F(x, y)$ are positive, it is easy to see that $F_1(x, y)$ must be one of the forms (2.8). However, only one of them satisfies (iv) and therefore $F_1(x, y) = F(x, y)$.

Case 5. $U = T = V$. From (2.6) and (2.7) we have

$$c - b + 3a = 3d - c + b = 0$$

implying $d = -a$, $c = b - 3a$. Hence, $F(x, y)$ is of the form

$$F(x, y) = ax^3 + bx^2y + (b - 3a)xy^2 - ay^3.$$

We must have $b \neq 3a/2$, otherwise $F(x, y)$ would be divisible by $x - y$. Further,

$$F(-y, -x) = ax^3 + (-b + 3a)x^2y - bxy^2 - ay^3,$$

and either $F(x, y)$ or $F(-y, -x)$ satisfies (v), i.e., is the required $F_{\mathscr{C}}(x, y)$. Choose the notation so that this form is $F(x, y)$. Its quadratic covariant is $H(x, y) = T(x^2 + xy + y^2)$. Suppose that $F_1(x, y)$ is another form in $\mathscr{C}$ satisfying (v). As in Case 4, we find that the quadratic covariant of $F_1(x, y)$ must coincide with $H(x, y)$. Again let τ denote a substitution of determinant $= +1$ transforming $F_1(x, y)$ into $F(x, y)$ or $F(-y, -x)$. By [11, loc.cit.] τ must be one of the following six substitutions:

$$[x = x', y = y'], \quad [x = -x' - y', y = x'], \quad [x = y', y = -x' - y'],$$
$$[x = -x', y = -y'], \quad [x = x' + y', y = -x'], \quad [x = -y', y = x' + y'].$$

However, simple computations show that for such τ the substitution τ^{-1} transforms $F(x, y)$ and $F(-y, -x)$ into themselves or into identically opposite forms. Since only one of these four forms satisfies (v), we have $F_1(x, y) = F(x, y)$. □

3. Inequalities Concerning Reduced Cubic Forms. A table of minimal polynomials was produced by first tabulating the relevant cubic forms. For that purpose precise estimates for the coefficients of these forms in terms of the discriminant are valuable. In the following theorem we shall present a collection of such estimates all of which are best possible. The first four are classical [3], [14], but for the convenience of the reader we give a complete proof. In a less accurate form these results are contained in [6, p. 185, Lemma 1].

THEOREM 2. *Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a reduced binary cubic form with discriminant $D = D(F)$. Then the following estimates are valid*:

$$0 < a < 2D^{1/4}/\sqrt{27}, \qquad |b| \leqslant 2D^{1/4}/\sqrt{3}, \tag{3.1}$$

$$|ad| < 4D^{1/2}/27, \qquad |bc| < D^{1/2}, \tag{3.2}$$

$$\max\{|ac^3|, |b^3d|\} < (35 + 13\sqrt{13})D/216. \tag{3.3}$$

Remark. The example $a = 1$, $b = 6$, $c = 3$, $d = -1$ shows that equality can occur in (3.1).

To show that the first inequalities in (3.1) and (3.2) are best possible take $a = 4m - 2$, $b = 6m$, $c = -6m$, $d = -4m + 1$, where m is a (large) positive integer. Then $F(x, y)$ is clearly primitive and it is irreducible in $\mathbf{Q}[x, y]$ by Eisenstein's criterion. We have

$$T = 108m^2 - 36m, \quad U = 108m^2 - 108m + 18, \quad V = 108m^2 - 18m$$

so that $0 < U < T < V$ and $F(x, y)$ is reduced. Since $D^{1/2} = 108m^2 + O(m)$ we have $aD^{-1/4} = 2/\sqrt{27} + O(m^{-1})$, $|ad|D^{-1/2} = 4/27 + O(m^{-1})$.

Next, take $a = 1$, $b = 2m + 4$, $c = 2m$, $d = -2$, where again m is a (large) positive integer. Then,

$$T = 4m^2 + 10m + 16, \quad U = 4m^2 + 8m + 18, \quad V = 4m^2 + 12m + 24,$$

whence $F(x, y)$ is reduced. We have $D^{1/2} = 4m^2 + O(m)$ and $bcD^{-1/2} = 1 + O(m^{-1})$ so that the second inequality (3.2) is best possible.

The fact that (3.3) is best possible will be obvious from the subsequent proof.

Proof of Theorem 2. The following general identities are easily seen to be true:

$$(2bT - 3aU)^2 + 27a^2D = 4T^3, \tag{3.4}$$

$$(2cT - bU)^2 + 3b^2D = 4T^2V, \tag{3.5}$$

$$(2bV - cU)^2 + 3c^2D = 4TV^2, \tag{3.6}$$

$$(2cV - 3dU)^2 + 27d^2D = 4V^3. \tag{3.7}$$

Since the form is reduced, we have

$$D = (4TV - U^2)/3 \geqslant TV \geqslant T^2. \tag{3.8}$$

From (3.4), (3.5), (3.8) we immediately obtain (3.1) with the reservation that the upper estimate of a might not be a strict inequality. However, in the case of equality we must also have equality in (3.8) and $2bT - 3aU = 0$. This would imply $T = U = V$ and $2b = 3a$ contrary to the proof of Theorem 1, Case 5.

On combining (3.4), (3.7), (3.8), we have

$$(27adD)^2 \leqslant 16(TV)^3 \leqslant 16D^3$$

implying $|ad| < 4D^{1/2}/27$ because equality cannot occur.

Using the identity

$$b^2V - bcU + c^2T = TV, \tag{3.9}$$

we find

$$2(TV)^{1/2}|bc| \leqslant b^2V + c^2T = TV + bcU \leqslant TV + |bcU|,$$

whence, by (3.8),

$$\begin{aligned}3D|bc| &= \big(2(TV)^{1/2} + |U|\big)\big(2(TV)^{1/2} - |U|\big)|bc| \\ &\leqslant \big(2(TV)^{1/2} + |U|\big)TV \leqslant 3(TV)^{3/2} \leqslant 3D^{3/2}\end{aligned}$$

so that $|bc| \leqslant D^{1/2}$. If equality occurs then $T = U = V$ and $b = c$. But in the proof of Theorem 1, Case 5 we saw that $c = b - 3a$, a contradiction. We have thus proved (3.2) and it remains to prove (3.3).

Put $\kappa = (35 + 13\sqrt{13})/216$. We shall show first that $|ac^3| < \kappa D$. From (2.4) and (3.4) we find

$$ac^3/D = (b^2 - T)^3/\big(4T^3 - (2bT - 3aU)^2\big). \tag{3.10}$$

We have the identity

$$9a^2V - 3abU + b^2T = T^2. \tag{3.11}$$

Put

$$x = 3aV^{1/2}T^{-1}, \quad y = 3aUT^{-3/2}, \quad z = 2bT^{-1/2} - 3aUT^{-3/2}.$$

From (3.11) and from the conditions of reduction we get

$$x > 0, \quad |y| \leqslant x, \quad 4x^2 - y^2 + z^2 = 4 \tag{3.12}$$

and the right-hand side of (3.10) takes the form

$$\varphi(x, y, z) = \big((y + z)^2 - 4\big)^3/\big(64(4x^2 - y^2)\big).$$

We have to study the function $\varphi(x, y, z)$ subject to the constraints (3.12). We may suppose that $z \geqslant 0$ because the change of the signs of y and z leaves φ and (3.12) unaltered. It follows, in particular, from (3.12) that $3x^2 + z^2 \leqslant 4$, and thus

$$|y| \leqslant x \leqslant 2/\sqrt{3}, \qquad 0 \leqslant z < 2. \tag{3.13}$$

If $(x, y, z) \to (0, y_0, z_0)$ subject to (3.12) and (3.13), then $y_0 = 0$, $z_0 = 2$, and it is easy to see that $\lim \varphi(x, y, z) = 0$. We may therefore assume that a point (x, y, z) satisfying (3.12) and (3.13) is so chosen that the function $|\varphi|$ subject to these constraints attains its maximum at that point.

Suppose first that $|y + z| \geqslant 2$. From (3.13) we have $y > 0$. Since

$$|\varphi(x, y, z)| = \Big(\big(y + (4 - 4x^2 + y^2)^{1/2}\big)^2 - 4\Big)^3/\big(64(4x^2 - y^2)\big)$$

is an increasing function of y we must have $y = x$ so that

$$\begin{aligned}|\varphi(x, y, z)| &= \Big(\big(x + (4 - 3x^2)^{1/2}\big)^2 - 4\Big)^3/(192x^2) \\ &= \big(x(4 - 3x^2)^{1/2} - 3x^2 + 2x^4\big)/6.\end{aligned} \tag{3.14}$$

Since $x + (4 - 3x^2)^{1/2} = y + z \geqslant 2$ implies $x \leqslant 1$, we have to compute the maximum of the function (3.14) in the interval $(0, 1]$. This is a trivial task, the maximum is $(-35 + 13\sqrt{13})/216$ attained at the point $x = ((5 - \sqrt{13})/12)^{1/2}$.

Suppose next that $|y + z| < 2$. For $z \leqslant 1$ we have

$$|\varphi(x, y, z)| = \left(4 - (y + z)^2\right)^3/(64(4 - z^2)) \\ \leqslant 1/(4 - z^2) \leqslant 1/3 < \kappa.$$

Suppose therefore that $z > 1$. Then (3.12) implies $|y| \leqslant x < 1$ so that $0 < y + z < 2$. From the choice of the point (x, y, z) it now follows that we must have $y = -x$; otherwise we could either change the sign of y or diminish y slightly and change x correspondingly in order to keep z fixed, which would give us a larger value of $|\varphi(x, y, z)|$. Therefore,

$$(3.15) \qquad |\varphi(x, y, z)| = \left(4 - \left(-x + (4 - 3x^2)^{1/2}\right)^2\right)^3/(192x^2) \\ = \left(x(4 - 3x^2)^{1/2} + 3x^2 - 2x^4\right)/6,$$

and on computing the maximum value of the function (3.15) in the interval $(0, 1)$ we obtain $|\varphi(x, y, z)| = \kappa$ for

$$(x, y, z) = \left(((5 + \sqrt{13})/12)^{1/2}, -((5 + \sqrt{13})/12)^{1/2}, ((11 - \sqrt{13})/4)^{1/2}\right).$$

Hence $|ac^3| < \kappa D$ as asserted.

The proof of $|b^3 d| < \kappa D$ is similar. We start from the expression

$$b^3 d/D = (c^2 - V)^3/\left(4V^3 - (2cV - 3dU)^2\right)$$

which is a consequence of (2.4) and (3.7), and use the identity

$$9d^2T - 3cdU + c^2V = V^2.$$

This time we write

$$x = 3|d|T^{1/2}V^{-1}, \quad y = 3dUV^{-3/2}, \quad z = 2cV^{-1/2} - 3dUV^{-3/2},$$

and the proof proceeds exactly as before. □

4. Normalized Cubic Polynomial. Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a reduced cubic form of discriminant $D = D(F)$. The *polynomial* $f(x)$ *associated with the form* $F(x, y)$ is defined as

$$(4.1) \qquad f(x) = a^{-1}F(x + (eb - s)/3, -ea),$$

where

$$(4.2) \qquad s = \begin{cases} 1 & \text{if } b \not\equiv 0 \bmod 3, \\ 0 & \text{if } b \equiv 0 \bmod 3; \end{cases} \qquad e = \begin{cases} 1 & \text{if } b \equiv 1 \bmod 3, \\ -1 & \text{if } b \not\equiv 1 \bmod 3. \end{cases}$$

Clearly $f(x)$ is a monic cubic polynomial with integral coefficients in which $-s$ is the coefficient of x^2. Writing

$$(4.3) \qquad f(x) = x^3 - sx^2 + qx - n,$$

we have

$$q = ac - (b^2 - s)/3 = (s - T)/3, \tag{4.4}$$

$$n = (2eb + s)(eb - s)^2/27 - ac(eb - s)/3 + ea^2d \tag{4.5}$$

since $s^2 = s$ and $e^2 = 1$. The discriminant of the polynomial $f(x)$ is

$$\begin{aligned} sq^2 - 4q^3 - 4sn - 27n^2 + 18sqn &= a^2D \\ &= 4T^3/27 - 3(3n - sq + 2s/9)^2. \end{aligned} \tag{4.6}$$

We note that the reduced form $F(x, y)$ is not uniquely determined by its associated polynomial. This is seen trivially by considering the forms $ax^3 + cxy^2 + dy^3$ and $x^3 + acxy^2 + a^2dy^3$ where $c < -3a \leq -3$, $0 < d < -c/(3a)$, and $\gcd(a, c, d) = 1$. (In order to ensure the required irreducibility assume, e.g., that there exists a prime p such that $p \nmid a$, $p \mid c$, $p \mid d$, $p^2 \nmid d$.) Then the forms are reduced and they both have associated polynomial $x^3 + acx + a^2d$.

It is more difficult to find examples of a pair of reduced cubic forms both having the same leading coefficient and the same associated polynomial. One such pair is

$$k^3x^3 - 3k^2(k + 1)xy^2 + (k^3 + k^2 - 3)y^3,$$

$$k^3x^3 + 3k^2(k - 1)x^2y - 3k(3k - 1)xy^2 - (k^3 + 2k^2 - 6k + 4)y^3,$$

where k is a positive integer $\equiv -1 \bmod 18$. Both forms have associated polynomial

$$x^3 - 3k^5(k + 1)x + k^8(k + 1) - 3k^6.$$

Suppose now that K is a totally real cubic field of discriminant D and let $\mathscr{B} = \{1, \alpha, \omega\}$ be an integral basis for $\mathcal{O}$ containing 1 (called *unitary* in [9, Section 15]). Following Davenport and Heilbronn [7], [8] we assign to $\mathscr{B}$ the cubic form

$$\begin{aligned} F(x, y; \mathscr{B}) = D^{-1/2}((\alpha' - \alpha'')x + (\omega' - \omega'')y)((\alpha'' - \alpha)x + (\omega'' - \omega)y) \\ \times((\alpha - \alpha')x + (\omega - \omega')y). \end{aligned}$$

It is easily seen that the equivalence class containing the form $F(x, y; \mathscr{B})$ is independent of the choice of $\mathscr{B}$ and thus depends only on K. We denote this class by $\mathscr{C}(K)$. By an abuse of notation write $F_K(x, y) = F_{\mathscr{C}(K)}(x, y)$ for the reduced form in the class $\mathscr{C}(K)$ and let $\mathscr{R}$ be the set of all forms $F_K(x, y)$, K ranging over the set of all totally real cubic fields. From [8, p. 418, Proposition 4] we have

THEOREM 3. *The assignment $K \mapsto F_K(x, y)$ induces a bijective discriminant-preserving map of the set of triplets of conjugate totally real cubic fields onto $\mathscr{R}$.*

Here, of course, the triplet is coalescent if K is cyclic. From [8] it is easy to derive the following result which is fundamental in the search of all totally real cubic fields with discriminants in a given range.

THEOREM 4. *Let $F(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ be a reduced cubic form of discriminant D. We have $F(x, y) \in \mathscr{R}$ if and only if the following Davenport-Heilbronn conditions are satisfied*:

(DH2) $D \not\equiv 0 \bmod 16$; *if* $D \equiv 4 \bmod 16$ *then* $b \equiv c \bmod 2$.

(DH3) *If* $D \equiv 0 \bmod 9$ *then* $b \equiv c \equiv 0 \bmod 3$ *and* $ad(a^2 - d^2 - ac + bd) \equiv 3$ *or* $6 \bmod 9$.

(DHp) *For every prime* $p \geqslant 5$ *such that* $D \equiv 0 \bmod p^2$ *we have* $D \not\equiv 0 \bmod p^3$, $a \not\equiv 0 \bmod p^2$, $T = b^2 - 3ac \equiv 0 \bmod p$.

Proof. Prime $p = 2$. By [8, p. 407] the local condition at the prime 2 is equivalent to the following one: If $D \equiv 0$ or $4 \bmod 16$, then $F(x, y) \equiv (ax + dy)^3 \bmod 2$, and the congruence $F(x, y) \equiv 2 \bmod 4$ has a solution.

Suppose first that this condition holds. Clearly $b \equiv c \equiv ad \bmod 2$. If ad is even we may suppose, e.g., that a is even and d is odd. The solution of $F(x, y) \equiv 2 \bmod 4$ must be $(x, y) = (1, 0)$ whence $a \equiv 2 \bmod 4$ and $D \equiv a^2d^2 \equiv 4 \bmod 16$. If ad is odd apply first the substitution $x = x' + y', y = y'$. Hence, (DH2) holds.

Suppose conversely that (DH2) is true. Let $D \equiv 4 \bmod 16$, otherwise there is nothing to prove. If $b \equiv c \equiv 0 \bmod 2$ we see from (2.2) that $D \equiv 5a^2d^2 + 2abcd \bmod 16$. Thus ad is even and $D \equiv a^2d^2 \bmod 16$ (e.g., let a be even and d odd). Since $D \not\equiv 0 \bmod 16$ we have $a \equiv 2 \bmod 4$ so that $F(x, y) \equiv y^3 \bmod 2$, $F(1, 0) \equiv 2 \bmod 4$. If $b \equiv c \equiv 1 \bmod 2$ we get from (2.2) that ad is odd. Apply the same substitution as above.

Prime $p = 3$. The local condition in [8] at the prime 3 can be written as follows: If $D \equiv 0 \bmod 9$ then $F(x, y) \equiv (ax + dy)^3 \bmod 3$, and the congruence $F(x, y) \equiv 3e \bmod 9$ has a solution for $e = 1$ or 2.

Suppose first that this condition holds and that $D \equiv 0 \bmod 9$. Clearly $b \equiv c \equiv 0 \bmod 3$. If $3 | a$ the solvability of $F(x, y) \equiv 3e \bmod 9$ plainly implies $9 \nmid a$, whence $ad(a^2 - d^2 - ac + bd) \equiv -ad^3 \equiv 3$ or $6 \bmod 9$. The same conclusion holds if $3 | d$. Therefore, let $ad \not\equiv 0 \bmod 3$. Then $a^2 - d^2 - ac + bd \equiv 0 \bmod 3$. We may assume that the solution of $F(x, y) \equiv 3e \bmod 9$ is $(x, y) = (1, 1)$ or $(1, -1)$. Accordingly either $a + b + c + d$ or $a - b + c - d$ is $\equiv 3$ or $6 \bmod 9$. In the first case, we have $a + d \equiv 0 \bmod 3$ and

$$\begin{aligned} a^2 - d^2 - ac + bd &\equiv a^2 - d^2 + (a - d)c + (a - d)b \\ &\equiv (a - d)(a + b + c + d) \equiv 3 \text{ or } 6 \bmod 9, \end{aligned}$$

and similarly, in the other case. Hence (DH3) is true.

Suppose conversely that (DH3) holds and $D \equiv 0 \bmod 9$. From $b \equiv c \equiv 0 \bmod 3$ we immediately have $F(x, y) \equiv (ax + dy)^3 \bmod 3$. If $3 | a$ then $9 \nmid a$ by (DH3), so that $F(1, 0) \equiv 3$ or $6 \bmod 9$. If $3 | d$, we similarly have $F(0, 1) \equiv 3$ or $6 \bmod 9$. Let $ad \not\equiv 0 \bmod 3$. From (DH3), $(a + d)(a - d) \equiv 0 \bmod 3$, and one may reverse the argument above.

Prime $p \geqslant 5$. The condition from [8] is the following one: If $D \equiv 0 \bmod p^2$ then $F(x, y) \equiv r(hx + ky)^3 \bmod p$ for some integers r, h, k, and the congruence $F(x, y) \equiv ep \bmod p^2$ has a solution for some $e \not\equiv 0 \bmod p$.

Suppose first that this condition is true and $D \equiv 0 \bmod p^2$. From [8, p. 410, Lemma 6] we have $D \not\equiv 0 \bmod p^3$. Further $T \equiv (3rh^2k)^2 - 3rh^3 3rhk^2 \equiv 0 \bmod p$, and similarly $U \equiv V \equiv 0 \bmod p$. If $p^2 | a$, then from $T \equiv V \equiv 0 \bmod p$ we would have $b \equiv c \equiv 0 \bmod p$ and from (2.2), $D \equiv 0 \bmod p^3$, a contradiction. Thus (DHp) holds.

Suppose conversely that (DHp) is true, and that $D \equiv 0 \bmod p^2$. If $p \nmid a$, we find from $T \equiv U \equiv 0 \bmod p$ that $c \equiv b^2/(3a) \bmod p$ and $d \equiv b^3/(27a^2) \bmod p$, and so $F(x, y) \equiv (3ax + by)^3/(27a^2) \bmod p$. If $p | a$ it follows from $T \equiv 0 \bmod p$ that $p | b$ and hence $D \equiv -4ac^3 \bmod p^2$ by (2.2). Since $p^2 \nmid a$ we get $p | c$ and thus $F(x, y) \equiv dy^3 \bmod p$. The rest now follows from [8, p. 410, Lemma 6]. □

A polynomial $f(x)$ is said to be a *normalized cubic polynomial* (abbreviated NCP) iff there is a totally real cubic field K such that $f(x)$ is the polynomial associated with the form $F_K(x, y)$. Obviously $K = \mathbf{Q}(\alpha)$, where $f(\alpha) = 0$. We shall call α a *normalized primitive element* (abbreviated NPE) of K over $\mathbf{Q}$. Thus, every noncyclic K has a unique naturally defined NPE, whereas a cyclic K contains a triplet of such elements.

5. Properties of Normalized Cubic Polynomials. In the following theorem we shall prove first that for an NPE, the conjugates have least standard deviation among all irrational algebraic integers of the cubic field in question. Later on in this section we shall see that this property almost characterizes an NPE of given trace. In the foregoing section we saw that two reduced cubic forms may have the same leading coefficient and the same associated polynomial. Here, we shall see that this is not possible if the polynomial is an NCP. We shall also construct an algorithm by means of which the corresponding form in $\mathscr{R}$ can be computed when the polynomial is given.

THEOREM 5. *Let α be an NPE of a totally real cubic field K and put* $\operatorname{Irr}(\alpha, \mathbf{Q}) = f(x) = x^3 - sx^2 + qx - n$. *For any $\xi \in K$, write*

$$R(\xi) = \tfrac{1}{2}\left((\xi - \xi')^2 + (\xi' - \xi'')^2 + (\xi'' - \xi)^2\right).$$

(i) *We have* $R(\alpha) = s - 3q = \min\{R(\xi)\}$, *the minimum being taken over all irrational algebraic integers ξ of K.*

(ii) *For any given positive integer k, there exists at most one reduced cubic form $F(x, y)$ with leading coefficient k, such that $f(x)$ is the polynomial associated with $F(x, y)$.*

(iii) *Denote $F_K(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 \in \mathscr{R}$. The form $F_K(x, y)$ can be traced back from the polynomial $f(x)$ by means of the following algorithm.*

(I) *The leading coefficient a is the largest positive integer for which an integer t can be found such that*

$$f(t) \equiv 0 \bmod a^2, \qquad f'(t) \equiv 0 \bmod a. \tag{5.1}$$

We have $b^2 - 3ac = T = s - 3q = R(\alpha)$.

(II) *If* $s = 0$, *then*

$$b = 3t + 3a\left[\tfrac{1}{2} - t/a - 9n/(2aT)\right],$$
$$c = (b^2 - T)/(3a),$$
$$d = (b^3 - 3bT - 27n)/(27a^2).$$

(III) *If* $s = 1$, *determine first*

$$g = \tfrac{1}{2} - t/a - (T - 1)/(6aT) - 9n/(2aT),$$
$$b_* = 3t - 1 + 3a[g].$$

(III.1) *If* $g \in \mathbf{Z}$, *then*

$$b = \max\{b_*, 3a - b_*\},$$
$$c = (b^2 - T)/(3a),$$
$$d = (bc - T)/(9a).$$

(III.2) *If* $g \notin \mathbf{Z}$, *then writing*

$$d_* = \left(b_*^3 + 1 - 3(b_* + 1)T - 27n\right)/(27a^2),$$

we have $c = (b_*^2 - T)/(3a)$, $(b, d) = (b_*, d_*)$ *or* $(-b_*, -d_*)$, *chosen so that the condition* (i) *or* (iii) *in Theorem* 1 *is satisfied.*

Proof. (i) By definition, $f(x)$ is the polynomial associated with the form $F_K(x, y)$. From (4.4), $T = b^2 - 3ac = s - 3q$, and on the other hand, clearly, $R(\alpha) = s^2 - 3q = s - 3q$. Let $H(x, y)$ denote the quadratic covariant of $F_K(x, y)$. Choose an irrational algebraic integer β of K so that $R(\beta)$ is least possible. By the minimality of $R(\beta)$, $(\beta - h)/k$ cannot be an algebraic integer for any pair of rational integers h, k with $k > 1$. It follows that $\mathcal{O}$ has an integral basis $\mathcal{B}$ of the form $\{1, \beta, (u + v\beta + \beta^2)/w\}$ for some integers u, v, w with $w > 0$. Since $w = [\mathcal{O}: \mathbf{Z}[\beta]]$, we find that w is equal to the leading coefficient $(\beta' - \beta'')(\beta'' - \beta)(\beta - \beta')D^{-1/2}$ of the form $F(x, y; \mathcal{B})$, provided that the order of the conjugates of β is suitably chosen. Here, $D = D(F_K)$ denotes the discriminant of K. Therefore,

$$\begin{aligned} F(x, y; \mathcal{B}) &= w(x + \gamma y)(x + \gamma' y)(x + \gamma'' y), \\ \gamma &= (v + \mathrm{Tr}(\beta) - \beta)/w. \end{aligned} \tag{5.2}$$

A simple computation now shows that the first quantity (2.4) for the form $F(x, y; \mathcal{B})$ equals $R(\beta)$. Since $F(x, y; \mathcal{B})$ and $F_K(x, y)$ are equivalent, so are their quadratic covariants, and therefore $R(\beta)$, being the leading coefficient of the former covariant, is an integer represented by the reduced quadratic form $H(x, y)$. Since T is the least nonzero integer represented by $H(x, y)$, $R(\beta) \geqslant T$, and thus necessarily $R(\beta) = T$.

(ii) Let $F(x, y)$ be a reduced cubic form with leading coefficient k such that $f(x)$ is the polynomial associated with $F(x, y)$. By (4.1), $f(x) = k^{-1}F(x - t, \pm k)$ for some integer t. Hence

$$f(t) \equiv 0 \bmod k^2, \qquad f'(t) \equiv 0 \bmod k. \tag{5.3}$$

It is easy to see that an integer t satisfying (5.3) is unique mod k. Suppose, indeed, that t' is another such integer. It follows from a theorem of Voronoi [9, p.111, Theorem I] that the numbers

$$\left(u^2 - su + q + (u - s)\alpha + \alpha^2\right)/k, \qquad u = t \text{ or } t',$$

are algebraic integers. Their difference is $(t - t')(t + t' - s + \alpha)/k$. However, as was seen above, a number of this type can be integral only for $t - t' \equiv 0 \bmod k$. The argument in the subsequent proof of (iii) now gives the uniqueness of $F(x, y)$. We observe that (ii) is true under the weaker assumption that no number of the form $(\alpha - h)/k$ with $h, k \in \mathbf{Z}$, $k > 1$ is an algebraic integer, which is equivalent to the fact that there exists an integral basis for $\mathcal{O}$ containing 1 and α.

(iii) Since the discriminant of the polynomial $f(x)$ equals a^2D, it follows immediately from the theorem of Voronoi cited above that (I) is true. From the foregoing proof of (ii) we have $t \equiv (s - eb)/3 \bmod a$.

Consider first the case $s = 0$. Then $e = -1$ and $t \equiv b/3 \bmod a$. Putting $b/3 = t + ra$, we have from (4.5)

$$aU = abc - 9a^2d = 2(t + ra)T + 9n.$$

Since $-T < U \leqslant T$, we infer

$$-aT < 2(t + ra)T + 9n \leqslant aT,$$

so that $r = [\frac{1}{2} - t/a - 9n/(2aT)]$, which gives the value of b in (II). The rest of (II) is clearly true, the expression for d being a consequence of (4.5).

Suppose now that $s = 1$. In this case the argument is slightly more complicated because we do not know beforehand whether $b \equiv 1$ or $-1 \bmod 3$. Writing $(1 - eb)/3 = t + ra$, we have this time from (4.5)

$$-eaU = 2(t + ra)T + (T - 1)/3 + 9n,$$

so that

$$r = -eU/(2T) - t/a - (T - 1)/(6aT) - 9n/(2aT).$$

It follows from the inequality $-T < U \leqslant T$ that $g - 1 \leqslant r \leqslant g$.

If $g \in \mathbf{Z}$ then $r = g$ or $g - 1$, which is possible only for $U = T$. If $b \equiv -1 \bmod 3$, then $e = -1$ and $r = g$ so that $(1 + b)/3 = t + ra$ implies $b = b_*$. If $b \equiv 1 \bmod 3$, then $e = 1$ and $r = g - 1$ so that $(1 - b)/3 = t + ra$ implies $b = 3a - b_*$. On the other hand, we have $b > 3a/2$ by Theorem 1, (ii) and (v), and therefore $b = \max\{b_*, 3a - b_*\}$ in both cases. The assertion (III.1) now follows, the value of d being obtained from the equation $U = T$.

If $g \notin \mathbf{Z}$, then $r = [g]$, $-eb = b_*$, and from (4.5), $-ed = d_*$. Clearly (III.2) is true. □

The practical implementation of the algorithm in order to compute $F_K(x, y)$ is facilitated by the fact that the computer listings contain the number a and the residue class of $t - s \bmod a$. For future reference we record here the obvious equality

$$a = [\mathcal{O}:\mathbf{Z}[\alpha]]. \tag{5.4}$$

THEOREM 6. *Let K be a given totally real cubic field. Put $F_K(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ and let $H(x, y) = Tx^2 + Uxy + Vy^2$ denote the quadratic covariant of $F_K(x, y)$. Then K is cyclic over $\mathbf{Q}$ if and only if $T = U = V$. If this is the case, then $c = b - 3a$, $d = -a$, the conductor of K is equal to T, and we have*

$$T = (u^2 + 3v^2)/4 \tag{5.5}$$

for $u = \pm(2b - 3a)$, $v = 3a$. Assuming that the sign of u is suitably chosen, u and v satisfy the conditions

$$\begin{array}{ll} u \equiv 2 \bmod 3, v \equiv 0 \bmod 3, v > 0 & \text{for } 3 \nmid T, \\ u \equiv 6 \bmod 9, v \equiv 3 \text{ or } 6 \bmod 9, v > 0 & \text{for } 3 \mid T \end{array} \tag{5.6}$$

introduced by Hasse [12, *p.* 12]. *The set $\{\alpha, \alpha', \alpha''\}$ of the NPE's of K coincides, apart from sign, with the set of the Gaussian periods for a generating cubic character of K.*

Proof. If $T = U = V$, then by (2.5) the discriminant of K equals T^2 so that K is cyclic over $\mathbf{Q}$ with conductor T. Suppose therefore, conversely for the rest of the proof, that K is cyclic over $\mathbf{Q}$. From the results of Hasse, it follows that we can write the conductor T of K in the form (5.5), where u and v satisfy (5.6). Take $a = v/3$, $b = v/2 + |u|/2$ and consider the form

$$F(x, y) = ax^3 + bx^2y + (b - 3a)xy^2 - ay^3.$$

It is well-known that either T or $T/9$ is a square-free integer. Since $T = 9a^2 - 3ab + b^2$ and $3 \nmid \gcd(a, b)$ by (5.6), it follows that $\gcd(a, b) = 1$ so that $F(x, y)$ is primitive. We have

$$a^{-1}F(3x - by, 3ay) = 27x^3 - 9Txy^2 + |u|Ty^3,$$

so that $F(x, y)$ is irreducible in the ring $\mathbf{Q}[x, y]$ by Eisenstein's criterion if $T \neq 9$. The same is clearly also true for $T = 9$. The quadratic covariant of $F(x, y)$ is $T(x^2 + xy + y^2)$, whence $F(x, y)$ is reduced. It is easy to see that the DH-conditions in Theorem 4 are satisfied so that $F(x, y) \in \mathscr{R}$. Using the notation (4.2) the polynomial associated with the form $F(x, y)$ is

$$\begin{aligned} f(x) &= x^3 - sx^2 + ((s - T)/3)x - (e(2b - 3a)T - 3sT + s)/27 \\ &= \begin{cases} x^3 - x^2 + ((1 - T)/3)x - (T(u - 3) + 1)/27 & \text{if } 3 \nmid T, \\ x^3 - (T/3)x + |u|T/27 & \text{if } 3 \mid T. \end{cases} \end{aligned}$$

Let $\theta, \theta', \theta''$ denote the Gaussian periods for a generating character of K multiplied by ± 1 as in [16, p. 7] and let $\alpha, \alpha', \alpha''$ denote the zeros of $f(x)$. Now, comparing $f(x)$ with the minimal polynomial of θ [16, pp. 8–9], we see that $\alpha = \pm\theta^{(i)}$ for some i. Therefore, $F(x, y)$ must be $F_K(x, y)$, i.e., the image of K under the bijective Davenport-Heilbronn mapping. □

THEOREM 7. *Let α be an NPE of a totally real cubic field K, $f(x) = \operatorname{Irr}(\alpha, \mathbf{Q}) = x^3 - sx^2 + qx - n$ the polynomial associated with $F_K(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, and let $H(x, y) = Tx^2 + Uxy + Vy^2$ denote the quadratic covariant of $F_K(x, y)$. For any $\beta \in \mathscr{O}$ we have $R(\beta) = R(\alpha)$ if and only if β is of the following form*:

(i) *If $T < V$, $\beta = \pm\alpha + h$, where $h \in \mathbf{Z}$.*

(ii) *If $U \neq T = V$, either $\beta = \pm\alpha + h$ or*

$$\beta = \pm(t^2 - st + q + (t - s)\alpha + \alpha^2)/a + h,$$

where $h \in \mathbf{Z}$ and $t = (s - eb)/3$, e being defined by (4.2).

(iii) *If $U = T = V$, $\beta = \pm\alpha^{(i)} + h$, where $i \in \{0, 1, 2\}$ and $h \in \mathbf{Z}$.*

Proof. It is easy to check that if β is of one of the particular types in the theorem, then $\beta \in \mathscr{O}$ and $R(\beta) = R(\alpha)$. Suppose, therefore conversely, that $\beta \in \mathscr{O}$ and $R(\beta) = R(\alpha)$. Denote $\operatorname{Irr}(\beta, \mathbf{Q}) = f_1(x) = x^3 - s_1x^2 + q_1x - n_1$. As in the proof of Theorem 5 we conclude from the minimality of $R(\beta)$, using Voronoi's theorem, that $\mathscr{O}$ has an integral basis of the form $\mathscr{B} = \{1, \beta, \rho\}$, where

$$\rho = (t_1^2 - s_1t_1 + q_1 + (t_1 - s_1)\beta + \beta^2)/a_1.$$

Here t_1 is determined mod a_1 by

$$f_1(t_1) \equiv 0 \bmod a_1^2, \qquad f_1'(t_1) \equiv 0 \bmod a_1,$$

and a_1 is the largest natural number for which these congruences have a solution. Denote $F_1(x, y) = F(x, y; \mathscr{B})$. Arranging the conjugates of β suitably, we have by (5.2),

$$\begin{aligned} F_1(x, y) = a_1(x + ((t_1 - \beta)/a_1)y)(x + ((t_1 - \beta')/a_1)y) \\ \times(x + ((t_1 - \beta'')/a_1)y). \end{aligned} \tag{5.7}$$

From (4.1) we obtain a similar factorization

$$\begin{aligned} F_K(x, y) = a(x - (e(t - \alpha)/a)y)(x - (e(t - \alpha')/a)y) \\ \times(x - (e(t - \alpha'')/a)y), \end{aligned} \tag{5.8}$$

where $t = (s - eb)/3$. Let $H_1(x, y)$ denote the quadratic covariant of $F_1(x, y)$. In the proof of Theorem 5 we saw that the leading coefficient of $H_1(x, y)$ is $R(\beta) = R(\alpha) = T$. Let (h_{ij}) denote the two-by-two matrix of a unimodular integral homogeneous linear substitution transforming $F_K(x, y)$ into $F_1(x, y)$, i.e.,

$$F_1(x, y) = F_K(h_{11}x + h_{12}y, h_{21}x + h_{22}y).$$

Then, correspondingly,

$$H_1(x, y) = H(h_{11}x + h_{12}y, h_{21}x + h_{22}y)$$

and, in particular,

$$T = Th_{11}^2 + Uh_{11}h_{21} + Vh_{21}^2. \tag{5.9}$$

Consider first the case $T < V$. It is well-known (and easy to see) that (5.9) holds only for $h_{11} = \pm 1$, $h_{21} = 0$. From the unimodularity of the substitution it follows that $h_{22} = \pm 1$. Since a and a_1 are positive, we must have $h_{11} = 1$ and $a = a_1$. From Theorem 6 we know that the conjugate fields of K are distinct and, therefore, we conclude from the factorizations (5.7) and (5.8), that

$$x + h_{12}y \pm ((t - \alpha)/a)y = x + ((t_1 - \beta)/a)y.$$

Thus (i) is true.

Consider next the case $U \neq T = V$. In this case (5.9) has the additional solution $h_{11} = 0$, $h_{21} = \pm 1$. Then $h_{12} = \pm 1$, and from (5.7) and (5.8) we obtain

$$h_{12}y - (e(t - \alpha)/a)(h_{21}x + h_{22}y) = C(x + ((t_1 - \beta)/a_1)y), \tag{5.10}$$

where C is a constant. The leading coefficient of $F_1(x, y)$ is

$$a_1 = -eh_{21}(t - \alpha)(t - \alpha')(t - \alpha'')/a^2. \tag{5.11}$$

From (5.10) and (5.11) we have by a simple computation

$$\begin{aligned}\pm\beta &= (t - \alpha')(t - \alpha'')/a + h = (t^2 - t(s - \alpha) + \alpha'\alpha'')/a + h\\ &= (t^2 - st + q + (t - s)\alpha + \alpha^2)/a + h\end{aligned}$$

for some integer h. Hence (ii) holds.

Consider finally the cyclic case $U = T = V$. In this case the number α in the previous expressions is replaceable by any of its conjugates. This gives us first of all the possibility $\beta = \pm\alpha^{(i)} + h$. In the proof of the foregoing theorem we saw that $F_K(x, y)$ is of the form $ax^3 + bx^2y + (b - 3a)xy^2 - ay^3$. We shall compute the minimal polynomial of the number

$$\beta_0 = (t^2 - st + q + (t - s)\alpha + \alpha^2)/a = (t - \alpha')(t - \alpha'')/a \tag{5.12}$$

appearing in (ii). We have $\mathrm{Irr}(\alpha, \mathbf{Q}) = a^{-1}F_K(x - t, -ea)$ so that

$$N(t - \alpha^{(i)}) = a^{-1}F_K(0, -ea) = ea^3$$

for each i and hence $N(\beta_0) = a^3$. A straightforward computation gives $\mathrm{Tr}(\beta_0) = b - 3a$. From the condition $R(\beta_0) = T = 9a^2 - 3ab + b^2$ we get the missing coefficient and the result is

$$\mathrm{Irr}(\beta_0, \mathbf{Q}) = x^3 - (b - 3a)x^2 - abx - a^3 = a^{-1}F_K(x + a, -a).$$

Comparing the two minimal polynomials, we find

$$(5.13)\qquad \beta_0 = e\alpha^{(i)} - a - et \qquad (i = 1 \text{ or } 2)$$

because it is obvious that (5.13) cannot hold for $i = 0$. Therefore, the numbers resulting from (ii) by replacing α by any of its conjugates are of the form $\pm\alpha^{(j)} + h$, where $h \in \mathbf{Z}$.

In the present case, (5.9) has the further solution $h_{11} = -1$, $h_{21} = 1$. The solution with signs reversed is not acceptable because the leading coefficient a_1 $(= a)$ of the form $F_1(x, y)$ must be positive. Since the substitution is unimodular, we have $h_{12} + h_{22} = \pm 1$. By interchanging conjugates of α if need be, we may take

$$-x + h_{12}y - (e(t-\alpha)/a)(x + h_{22}y) = C(x + ((t_1 - \beta)/a)y),$$

where C is a constant. It follows that $\beta = \pm\beta_1 + h$ where $h \in \mathbf{Z}$ and

$$\beta_1 = -a^2/(a + e(t - \alpha)).$$

We have

$$N(a + e(t-\alpha)) = eN(ea + t - \alpha) = ea^{-1}F_K(ea, -ea) = -a^3,$$

so that

$$\beta_1 = (ea + t - \alpha')(ea + t - \alpha'')/a.$$

Comparing this expression with (5.12) and using (5.13) we find

$$\beta_1 = \beta_0 + e\alpha + a + e(2t - s) = -e\alpha^{(j)} + et \qquad (j = 1 \text{ or } 2).$$

This proves (iii). □

For practical purposes it is useful to know the approximate size of the coefficients of an NCP. The following theorem contains estimates to that effect. Numerical examples show that these estimates are rather accurate.

THEOREM 8. *Let $f(x) = x^3 - sx^2 + qx - n$ be an NCP and let D denote the discriminant of the corresponding field K. Then*

$$(5.14)\qquad s = 0 \text{ or } 1,$$

$$(5.15)\qquad -D^{1/2}/3 + s/3 \leqslant q < -(D/4)^{1/3} + s/3,$$

$$(5.16)\qquad -(2/27)D^{3/4} - sD^{1/2}/9 < n < (2/27)D^{3/4}.$$

Proof. The equality (5.14) holds trivially. Write $F_K(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$. From (4.4) and (3.8) we obtain the lower estimate (5.15). From (4.6) we have $27D < 4T^3$, so that the upper estimate (5.15) also follows from (4.4). It is now easy to deduce (5.16) from (4.6) and (5.15). □

6. The Algorithm. We shall now describe our algorithm which allows one to determine a complete set of NCP's whose zeros generate all totally real cubic fields of discriminant D satisfying $X_0 < D \leqslant X$, where X_0 and X are given bounds. We start the algorithm by making a search for the relevant reduced forms. Following the classification in Theorem 1, we first determine all integral vectors (a, b, c, d) with $\gcd(a, b, c, d) = 1$ which satisfy one of the following systems of conditions (where

$\kappa = (35 + 13\sqrt{13})/216$ as in the proof of Theorem 2):

$$\text{(i.1)}\qquad 1 \leqslant a < 2X^{1/4}/\sqrt{27}, \qquad 1 \leqslant b \leqslant 2X^{1/4}/\sqrt{3},$$

$$\max\left\{-X^{1/2}/b, -(\kappa X/a)^{1/3}, (b^2 - X^{1/2})/(3a)\right\} < c$$

$$< \min\left\{X^{1/2}/b, (\kappa X/a)^{1/3}, \left(b^2 - \left(27X_0a^2/4\right)^{1/3}\right)/(3a)\right\},$$

$$\max\left\{(bc - T)/(9a), \left(c^2 - (3X + T^2)/(4T)\right)/(3b)\right\} < d$$

$$< \min\left\{(bc + T)/(9a), (c^2 - T)/(3b), \left(c^2 - 3X_0/(4T)\right)/(3b)\right\};$$

$$\text{(i.2)}\qquad 1 \leqslant a < 2X^{1/4}/\sqrt{27}, \qquad b = 0,$$

$$\max\left\{-(\kappa X/a)^{1/3}, -X^{1/2}/(3a)\right\} < c < \min\left\{-3a, -\left(X_0/(4a)\right)^{1/3}\right\},$$

$$1 \leqslant d < -c/3;$$

$$\text{(ii)}\qquad 1 \leqslant a < 2X^{1/4}/\sqrt{27}, \qquad 3a/2 < b \leqslant 2X^{1/4}/\sqrt{3},$$

$$\max\left\{-X^{1/2}/b, -(\kappa X/a)^{1/3}, (b^2 - X^{1/2})/(3a)\right\} < c$$

$$< \min\left\{b - 3a,\ X^{1/2}/b, (\kappa X/a)^{1/3}, \left(b^2 - \left(27X_0a^2/4\right)^{1/3}\right)/(3a)\right\},$$

$$d = (bc - T)/(9a);$$

$$\text{(iii.1)}\qquad 1 \leqslant a < 2X^{1/4}/\sqrt{27}, \qquad 3a/2 < b \leqslant 2X^{1/4}/\sqrt{3},$$

$$\max\{-3a, -b\} < c < b - 3a, \qquad d = (c^2 - b^2 + 3ac)/(3b);$$

$$\text{(iii.2)}\qquad 1 \leqslant a < 2X^{1/4}/\sqrt{27}, \quad -2X^{1/4}/\sqrt{3} \leqslant b < -3a, \quad b < c < -3a,$$

$$d = (c^2 - b^2 + 3ac)/(3b);$$

$$\text{(iv)}\quad 1 \leqslant a < 2X^{1/4}/\sqrt{27}, \quad 3a < b \leqslant 2X^{1/4}/\sqrt{3}, \quad c = -3a, \quad d = -b/3;$$

$$\text{(v)}\quad 1 \leqslant a < 2X^{1/4}/\sqrt{27}, \quad 3a/2 < b \leqslant 2X^{1/4}/\sqrt{3}, \quad c = b - 3a, \quad d = -a.$$

In deriving these conditions frequent use is made of (2.4), (2.5), (2.6) and (2.7). All bounds involving X or X_0 are consequences of (3.1), (3.2), (3.3), (3.4) and (3.8). All other inequalities and equalities with two exceptions are critical in the sense that their validity is necessary and sufficient for the conditions of reduction to hold in each respective case. The exceptional ones are the bounds for b in terms of a in (iii.1) and (iii.2), which are consequences of the bounds for c. If a fractional expression appears in an equality it is of course stipulated that the numerator is divisible by the denominator. An overwhelming majority of reduced forms belongs to Case (i). It is therefore of minor practical importance to include all the possible alternative bounds for the various quantities in the above estimates in other cases, and we have not always done so.

The next step is to compute the value of the discriminant D and to discard all forms which do not satisfy $X_0 < D \leqslant X$ or the conditions (DH2), (DH3), (DHp) in Theorem 4. We then determine the associated polynomial $f(x)$ from (4.1) and (4.2) and compute its zeros. If any of these zeros is a rational integer, $f(x)$ is rejected.

In this way we have found the required complete set of NCP's. Let $f(x) = x^3 - sx^2 + qx - n$ be any of these and let K be the cubic field generated by a zero α of $f(x)$. As mentioned in the Introduction, in addition to leading to a naturally defined NCP, our approach has also practical advantages compared with the usual one.

Firstly, there is no need to check whether fields of the same discriminant are the same or not. Secondly, we know that the discriminant D of the form $F_K(x, y)$ computed above is also the discriminant of the field K. Furthermore, the leading coefficient a of the form $F_K(x, y)$ satisfies (5.4) and $\mathcal{O}$ has an integral basis $\{1, \alpha, \omega\}$, where

$$\begin{aligned} &\omega = (l + m\alpha + \alpha^2)/a, \\ (6.1) \qquad &l \equiv t^2 - st + q \bmod a, \quad m \equiv t - s \bmod a, \quad t = (s - eb)/3, \\ &0 \leqslant l < a, \quad 0 \leqslant m < a, \end{aligned}$$

in the notation (4.2).

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ denote the first degree prime ideals of $\mathcal{O}$ with norm less than $D^{1/2}/9.1$. These ideals are calculated and stored in a list. It follows from a result of Davenport [5] that every ideal class of K contains a product of nonnegative powers of the ideals $\mathfrak{P}_i$. Here one has to take into account that there are only two cubic fields with discriminants $\leqslant 81$ which are exceptional and they both have class number $= 1$. By virtue of the results of H. P. F. Swinnerton–Dyer [19] one could replace the constant 9.1 by a larger one, possibly at the cost of supplementary exceptional fields.

Applying the Voronoi algorithm, we determine the class number and the structure of the class group G of the field K inductively as follows. Suppose that for some j ($1 \leqslant j \leqslant r$) we already know the subgroup H_{j-1} of G generated by the classes represented by $\mathcal{O}$ and $\mathfrak{P}_1, \ldots, \mathfrak{P}_{j-1}$. We choose a representative for each element of H_{j-1}, consider it in a natural way as a lattice $\mathfrak{A}$ in $\mathbf{R}^3$, compute a y-chain of relative minima for $\mathfrak{A}$ [9, Section 54], and calculate the lattices obtained by division of $\mathfrak{A}$ by elements of the y-chain within the bounds of one period. All these lattices are stored in a list called the comparison list. We then determine the smallest positive exponent k such that there is a lattice obtained in a similar way from an x-chain for $\mathfrak{P}_j^k$ which is already contained in the comparison list [9, p. 258, Theorem 7]. If $k = 1$, we have $H_j = H_{j-1}$. If $k > 1$, then H_j is generated by H_{j-1} and the classes containing $\mathfrak{P}_j, \ldots, \mathfrak{P}_j^{k-1}$. The enlarged comparison list is computed in an obvious way. In order to avoid lattices with large generators we replace any ideal by an equivalent one encountered in the course of the computation if the latter has smaller norm than the previous one.

Let $\mathfrak{A}$ be any nonzero integral ideal of K. Suppose that the coordinate axes in $\mathbf{R}^3$ are chosen so that the vector corresponding to any number η of K is (η, η', η''). (We shall use the same notation for such a vector and its x-coordinate). Let η_0 be a relative minimum in $\mathfrak{A}$ and let $\eta_0, \eta_1, \ldots$ be a chain of relative minima starting from η_0. For definiteness, suppose it is an x-chain. Write $|N(\eta_n)| = r_n N(\mathfrak{A})$ and take $\mathfrak{A}_n = (r_n/\eta_n)\mathfrak{A}$. Obviously, r_n is a relative minimum in the lattice $\mathfrak{A}_n$, and if ξ_{n+1} denotes the minimum point in this lattice adjacent to r_n on the x-axis [9, p. 247], then

$$\eta_{n+1} = \pm\eta_n \xi_{n+1}/r_n \qquad (n = 0, 1, \ldots).$$

This is, of course, the principle on which the application of the Voronoi algorithm is based. At each step the computation is concerned with the determination of $\mathfrak{A}_n$ and the relative minimum ξ_{n+1} adjacent to a given lattice point r_n with equal conjugates.

Let $\{1, \alpha, \omega\}$ be the integral basis satisfying (6.1). It is of substantial practical importance to know the order of magnitude of the integer coordinates of ξ_{n+1} with respect to this basis, i.e., the solution x_0, x_1, x_2 of

$$x_0 + x_1\alpha + x_2\omega = \xi_{n+1}, \quad x_0 + x_1\alpha' + x_2\omega' = \xi'_{n+1}, \quad x_0 + x_1\alpha'' + x_2\omega'' = \xi''_{n+1}. \tag{6.2}$$

It follows directly from Minkowski's theorem that $r_n \leqslant D^{1/2}$. Since ξ_{n+1} is adjacent to r_n on the x-axis, we have $|\xi'_{n+1}| < r_n$, $|\xi''_{n+1}| < r_n$, and a repeated application of Minkowski's theorem gives $|\xi_{n+1}| \leqslant D^{1/2}$ because $N(\mathfrak{A}_n) = r_n^2$. Using Schwarz's inequality we get from (6.2)

$$\begin{aligned} D^{1/2}|x_0| &= |\xi_{n+1}(\alpha'\omega'' - \alpha''\omega') + \xi'_{n+1}(\alpha''\omega - \alpha\omega'') + \xi''_{n+1}(\alpha\omega' - \alpha'\omega)| \\ &\leqslant \sqrt{3}\,D^{1/2}\big((\alpha'\omega'' - \alpha''\omega')^2 + (\alpha''\omega - \alpha\omega'')^2 + (\alpha\omega' - \alpha'\omega)^2\big)^{1/2}, \\ D^{1/2}|x_1| &= |\xi_{n+1}(\omega' - \omega'') + \xi'_{n+1}(\omega'' - \omega) + \xi''_{n+1}(\omega - \omega')| \\ &\leqslant \sqrt{3}\,D^{1/2}\big((\omega' - \omega'')^2 + (\omega'' - \omega)^2 + (\omega - \omega')^2\big)^{1/2}, \\ D^{1/2}|x_2| &= |\xi_{n+1}(\alpha'' - \alpha') + \xi'_{n+1}(\alpha - \alpha'') + \xi''_{n+1}(\alpha' - \alpha)| \\ &\leqslant \sqrt{3}\,D^{1/2}\big((\alpha'' - \alpha')^2 + (\alpha - \alpha'')^2 + (\alpha' - \alpha)^2\big)^{1/2}. \end{aligned}$$

Calculating the expressions for the symmetric functions in terms of s, q, n, a, l, m and using (5.14), (5.15), (5.16), (6.1) we obtain, after a trivial but somewhat messy computation,

$$\begin{aligned} |x_0| &\leqslant \sqrt{3}\,a^{-1}\big(l^2(2s - 6q) + 2l(-sq + 4q^2 - 3sn) \\ &\qquad + (s - 4q)(q^2 - 2sn) + 2sqn - 9n^2\big)^{1/2} \\ &< (2/3)D^{3/4}, \\ |x_1| &\leqslant \sqrt{3}\,a^{-1}\big((m + s)^2(2s - 6q) - 2(m + s)(sq - 9n) + 2q^2 - 6sn\big)^{1/2} \\ &< \sqrt{6}\,(D^{1/2}/3 + D^{1/4}), \\ |x_2| &\leqslant (6s - 18q)^{1/2} \leqslant \sqrt{6}\,D^{1/4}. \end{aligned}$$

In conclusion, we shall briefly sketch the determination of a fundamental pair of units by Voronoi's method. Take $\mathfrak{A} = \mathcal{O}$, $\eta_0 = 1$ and consider the x-chain $\eta_0, \eta_1, \ldots$ in $\mathfrak{A}$ as above. Let $\mathfrak{A}_k$ be the first repeating lattice, i.e., $\mathfrak{A}_k = \mathfrak{A}_j$ for some $0 \leqslant j < k$. Then $\varepsilon_{*1} = \eta_k/\eta_j$ is the first fundamental unit. Next let $\zeta_0, \zeta_1, \ldots$ denote the y-chain in the lattice $\mathfrak{A}_{j-1}$ starting from $\zeta_0 = \xi_j$ in the above notation. (If $j = 0$ we take $\mathfrak{A}_{-1} = \mathcal{O}$ and $\zeta_0 = 1$.) Let p be the smallest positive index for which an $h \in \{j, \ldots, k - 1\}$ can be found such that there is an equality of lattices $(1/\zeta_p)\mathfrak{A}_{j-1} = (1/\eta_h)\mathfrak{A}$. Then $\varepsilon_{*2} = (\eta_j\zeta_p)/(\eta_h\zeta_0)$ is the second fundamental unit.

The two-dimensional unit lattice in the logarithmic space is generated by the vectors $(\log|\varepsilon_{*i}|, \log|\varepsilon'_{*i}|, \log|\varepsilon''_{*i}|)$ $(i = 1, 2)$. We compute a reduced fundamental parallelogram of this lattice by the usual process, i.e., we determine a fundamental pair of units $\varepsilon_1, \varepsilon_2$, called *reduced units*, so that the form

$$\big(x\log|\varepsilon_1| + y\log|\varepsilon_2|\big)^2 + \big(x\log|\varepsilon'_1| + y\log|\varepsilon'_2|\big)^2 + \big(x\log|\varepsilon''_1| + y\log|\varepsilon''_2|\big)^2$$

is a (semi) reduced positive definite binary quadratic form. There still is a free choice between $\pm\varepsilon_i^{\pm 1}$. The choice is made so that $N(\varepsilon_i) = +1$ and two of the conjugates of

ε_i have absolute value > 1. Presumably the order of magnitude of the coordinates of the pair ε_1, ε_2 with respect to the above basis $\{1, \alpha, \omega\}$ is near the least possible.

7. Tables and Statistics. The table containing the 26440 nonconjugate totally real cubic fields with discriminants less than 500000 has been deposited in the Mathematics of Computation's UMT-depository. It consists of 10 parts, the kth part containing the fields with discriminants between $50000(k-1)$ and $50000k$. For each field $K = \mathbf{Q}(\alpha)$, where α is an NPE the following data are listed:

- running number r
- discriminant D of K
- coefficients s, q, n of the polynomial $\operatorname{Irr}(\alpha, \mathbf{Q}) = x^3 - sx^2 + qx - n$
- index a satisfying (5.4)
- numbers l, m satisfying (6.1) so that $\{1, \alpha, \omega\}$ with $\omega = (l + m\alpha + \alpha^2)/a$ is an integral basis for $\mathcal{O}$
- class number h of K
- coefficients a_{ij} ($i = 1,2$; $j = 0,1,2$) of the reduced units $\varepsilon_i = a_{i0} + a_{i1}\alpha + a_{i2}\omega$
- TP indicates that every norm-positive unit is totally positive.

The data are listed in the format

$$r \quad D \quad s \quad q \quad n \quad a \quad l \quad m \quad h \quad a_{ij} \quad (\mathrm{TP})$$

where the numbers a_{ij} are arranged in the form of one of the following three matrices depending on the space occupied by them:

$$A = (a_{10}\, a_{11}\, a_{12}\, a_{20}\, a_{21}\, a_{22}), \quad \begin{pmatrix} a_{10}\, a_{11}\, a_{12} \\ a_{20}\, a_{21}\, a_{22} \end{pmatrix}, \quad A^T \,(\text{transpose of } A).$$

The program was constructed in FORTRAN 5A for the DEC-20 system at the Computer Centre of the University of Turku. The total CPU time required was about 55 hours. Most of the calculations were performed either in integral arithmetic or double-precision arithmetic with 18 significant digits. However, when computing the units one needs a precision of much higher order of magnitude. To begin with, we used an accuracy of 120 digits. The program contained various reliability checks. The sufficiency of the space reserved for the numbers was tested, and integers being expressed as a decimal were tested to have either 00000 or 99999 as first digits after the decimal point. Finally, the norms of the reduced units were checked for actually having the value 1. If the field K under consideration failed to pass the test, a warning index in the corresponding record was given a positive value. Afterwards, we gathered together all such faulty cases and repeated the computation using 250 digits. This was found to be sufficient with the exception of three large cases requiring about 300 digits. The necessary multi-precision routines were constructed by ourselves.

The table below gives statistics referring to the class numbers. The numbers at the top of each column are the bounds on the discriminant.

As remarked in the Introduction the corresponding table in [1] is erroneous and a revised version has been given by Llorente and Oneto [15]. However, even the latter is not fully in accordance with our results. In fact there are six differences; we have found the following numbers of occurrences:

$$\text{for } 20001 \leqslant D \leqslant 30000 \text{ and class number } = \begin{cases} 1 & \text{no.} = 414 \\ 2 & \text{no.} = 27 \end{cases}$$

$$\text{for } 30001 \leqslant D \leqslant 40000 \text{ and class number } = \begin{cases} 4 & \text{no.} = 3 \\ 5 & \text{no.} = 3 \end{cases}$$

$$\text{for } 60001 \leqslant D \leqslant 70000 \text{ and class number } = \begin{cases} 2 & \text{no.} = 33 \\ 3 & \text{no.} = 32. \end{cases}$$

Class number	1 50000	50001 100000	100001 150000	150001 200000	200001 250000
1	2023	2169	2204	2204	2258
2	109	181	193	199	230
3	112	155	143	162	163
4	11	10	17	20	29
5	6	12	12	11	11
6	1	6	11	12	17
7	1	6	-	3	3
8	-	1	4	3	2
9	-	1	4	4	2
10	-	-	2	-	-
11	-	-	-	2	-
12	-	-	-	-	-
13	-	-	1	-	-
Total no of fields	2263	2541	2591	2620	2715

Class number	250001 300000	300001 350000	350001 400000	400001 450000	450001 500000
1	2261	2244	2278	2309	2270
2	216	232	238	229	232
3	156	199	155	154	193
4	26	24	26	29	32
5	12	14	14	12	21
6	10	16	9	17	11
7	5	5	1	2	6
8	1	3	2	3	2
9	3	3	5	3	2
10	-	3	1	3	1
11	-	1	-	-	-
12	1	1	-	5	3
13	-	-	1	-	1
14	-	-	1	-	1
15	-	1	-	-	-
16	-	-	-	-	1
Total no of fields	2691	2746	2731	2766	2776

The following tables contain statistics about TP-cases and about nonconjugate fields with the same discriminant. Both these phenomena are of considerable theoretical interest.

```
DISCRIMINANTS OF FIELDS IN WHICH EVERY NORM-POSITIVE UNIT IS
TOTALLY POSITIVE. IN THE CASES MARKED WITH AN ASTERISK THERE
ARE SEVERAL NONCONJUGATE FIELDS HAVING THE SAME DISCRIMINANT
ONLY ONE OF THEM POSSESSING THE TOTAL POSITIVITY PROPERTY


 15529     25717     25961     28669     29813     37229     53121     57077
 59749     66536     74708     82661     86321     88289     94441     95992*
 97997     99732    104153    109048    109621    114973    119369    124745
126857    142877    147788    148700    149189    150049    152737    154708
155917    166877    167333    171805    174829    176665    184761    189817
194549    194581    197513    206456    206764    215828    219196    225369
225653    227065    228237    230773    230825    236197    237469    241553
241556    242881    244756    249737    260117    270737    276788    277268
282593    283932    285865    289048    292088    294977    295329    297781
303156    305684    307817    313108    317620    318277    321516    324692
325153    328013    330452    333617    336517    336745    338441    341832
344065    345332    345656    348949    349693    350108    353777    353885
357656    362837    364492    375917    377780    380869    386013    387381
392881    393244    403572    404033    405528    415657    420393    420757
424505    426188    426357    428212*   429529    429569    430796    433117
437677    438344    439397    446284    448904    450353    451845    458260*
458477    464485    474952    479733    482825    485717    488201    494177
494209*   496865


DISCRIMINANTS WITH N ASSOCIATED NONCONJUGATE FIELDS FOR N > 1

                                N = 2

  3969      8281     13689     17689     29241     37300     38612     45684
 46548     47089     55700     61009     66825     67081     69012     77841
 83700     90601     92340    110889    113940    115668    138996    148372
149769    155412    157300    162324    162409    164052    168372    173556
181300    182329    182868    185652    186516    189972    191700    208980
213300    215700    215892    219961    223668    231361    235224    238140
248724    255636    257556    259700    261121    262964    263277    275700
278964    284148    296325    299700    301401    302292    305809    312481
323028    327668    331425    334260    340200    346921    348948    359700
363609    367956    370548    372276    374868    379700    391284    393012
393492    395604    399924    419796    428436    431325    431649    435348
441396    442260    452925    456948    457652    458325    460377    460404
461041    465588    470988    473300    489300    494209

                                N = 3

 22356     28212     31425     41332     47860     54324     57588     58077
 62004     62644     63028     65908     77844     82484     86485     86828
 89073     95992     97844     98132     99860    101876    105192    108729
109396    119604    122300    123860    129164    136628    138388    144212
144532    146452    150164    152212    153981    156244    161844    177741
180549    189777    198045    202932    205748    210708    214925    215796
217012    223540    223604    224084    225716    226580    235953    236277
239124    239476    240692    263196    270292    270405    275604    279284
293876    295284    302612    303220    304925    305268    313492    313620
314577    314772    317300    321364    323956    324308    325620    325809
326281    326516    327537    335732    339348    344568    344884    345716
350612    354772    358425    360948    378228    380884    383668    384404
392468    394292    397300    405965    407528    408244    410913    414708
418324    419688    424148    425493    428212    430228    438484    439124
444756    444852    448092    448929    452084    456425    456980    458260
458356    459892    462537    463988    464212    469233    469773    470569
471325    476820    477981    478521    486708    492212    492700    493925
498428

                                N = 4

 32009     42817     62501     72329     94636    103809    114889    130397
142097    151141    152949    153949    172252    173944    184137    189237
206776    209765    213913    214028    214712    219461    220217    250748
252977    255973    259653    265245    275881    282461    283673    298849
320785    321053    326945    333656    335229    341724    342664    358285
363397    371965    384369    390876    400369    412277    415432    422573
424236    431761    449797    459964    460817    468472    471057    471713
476124    476152    486221    486581    494236
```

The notable increase in local density of these $N = 3, 4$ fields as D increases, is discussed at length in [17] and is said to account for the increase in overall local density toward the theoretical limit $(12\,\zeta(3))^{-1}$ that was mentioned above.

Our final table gives a list of discriminants D and class numbers h of fields with noncyclic class group. Each of these groups is generated by two elements. For the four cases with $h = 12$ in the table there is more than one field with these D, but only one with a noncyclic group. On the other hand, both fields of $D = 431649$ have noncyclic groups so they are listed twice. The frequency of occurrence of a noncyclic class group is 35 out of 26440 so that the phenomenon is a very uncommon one indeed. This is in conformity with the comprehensive results of Buell [4] on class groups of imaginary quadratic fields.

D	h	D	h	D	h
26569	4	35537	4	76729	4
121801	4	128357	8	146853	9
151717	4	157609	4	210649	4
229577	4	240149	9	277429	4
299209	4	312709	8	314369	4
347485	4	368449	4	376712	9
394609	4	395177	4	409533	4
412277	12	424148	12	428657	8
431649	9	431649	9	442489	4
444412	8	455700	9	461041	12
468892	8	474949	4	476249	4
494209	12	496129	4		

Note added in March, 1984. After the completion of this work we have computed a supplementary table containing the values of the regulators up to $D < 200000$. A table of unit signatures is in preparation.

Department of Mathematics
University of Turku
SF-20500 Turku 50
Finland

1. I. O. Angell, "A table of totally real cubic fields," *Math. Comp.*, v. 30, 1976, pp. 184–187. MR **53** # 5528

2. F. Arndt, "Versuch einer Theorie der homogenen Funktionen des dritten Grades mit zwei Variabeln," *Arch. Math. Phys.*, v. 17, 1851, pp. 1–53.

3. F. Arndt, "Tabellarische Berechnung der reducirten binären kubischen Formen und Klassification derselben für alle successiven negativen Determinanten $(-D)$ von $D = 3$ bis $D = 2000$," *Arch. Math. Phys.*, v. 31, 1858, pp. 335–448.

4. Duncan A. Buell, "Class groups of quadratic fields," *Math. Comp.*, v. 30, 1976, pp. 610–623. MR **53** # 8008

5. H. Davenport, "On the product of three homogeneous linear forms. IV," *Proc. Cambridge Philos. Soc.*, v. 39, 1943, pp. 1–21. MR **4**, 212

6. H. Davenport, "On the class-number of binary cubic forms (I)," *J. London Math. Soc.*, v. 26, 1951, pp. 183–192; Corrigendum, v. 27, 1952, p. 512. MR **13**, 323

7. H. Davenport & H. Heilbronn, "On the density of discriminants of cubic fields," *Bull. London Math. Soc.*, v. 1, 1969, pp. 345–348. MR **40** # 7223

→ H. DAVENPORT & H. HEILBRONN, "On the density of discriminants of cubic fields. II," *Proc. Roy. Soc. London Ser. A*, v. 322, 1971, pp. 405–420. MR **58** # 10816

9. B. N. DELONE & D. K. FADDEEV, *The Theory of Irrationalities of the Third Degree*, Trudy Mat. Inst. Steklov., vol. 11, 1940; English transl., Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R. I., Second printing 1978. MR **2**, 349; **28** # 3955

10. L. E. DICKSON, *History of the Theory of Numbers*, vol. III, Carnegie Institution of Washington, Washington, 1923.

11. L. E. DICKSON, *Introduction to the Theory of Numbers*, Dover, New York, 1957.

12. 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. MR **11**, 503

13. CH. HERMITE, "Sur l'introduction des variables continues dans la théorie des nombres," *J. Reine Angew. Math.*, v. 41, 1851, pp. 191–216; Oeuvres I, Gauthier-Villars, Paris, 1905, pp. 164–192.

14. CH. HERMITE, "Sur la réduction des formes cubiques a deux indéterminées," *Comptes Rendus*, v. 48, 1859, p. 351; Oeuvres II, Gauthier-Villars, Paris, 1908, pp. 93–99.

15. P. LLORENTE & A. V. ONETO, "On the real cubic fields," *Math. Comp.*, v. 39, 1982, pp. 689–692.

16. SIRPA MÄKI, *The Determination of Units in Real Cyclic Sextic Fields*, Lecture Notes in Math., vol. 797, Springer-Verlag, Berlin and New York, 1980. MR **82a**: 12004

17. D. SHANKS, Review of I. O. Angell, "A table of totally real cubic fields," *Math. Comp.*, v. 30, 1976, pp. 670–673.

18. RENÉ SMADJA, *Calculs Effectifs sur les Ideaux des Corps de Nombres Algébriques*, Université d'Aix–Marseille, U. E. R. Scientifique de Luminy, 1976.

19. H. P. F. SWINNERTON-DYER, "On the product of three homogeneous linear forms," *Acta Arith.*, v. 18, 1971, pp. 371–385. MR **45** # 1844.