# A Table of Fundamental Pairs of Units in Totally Real Cubic Fields 

By T. W. Cusick and Lowell Schoenfeld

In honor of Daniel Shanks' 70 th birthday


#### Abstract

We apply a method of Cusick [5] to tabulate data on the first 250 totally real cubic fields $F$ having discriminant $D \leqslant 6,885$. Apart from $D$, we list the class number $H$ and the regulator $R$ of $F$. Also given are the integer coefficients $A, B, C$ of a defining polynomial $g(x)=x^{3}-A x^{2}+B x-C$, its index $I$, and its largest zero $R_{0}$. For $j=1,2$, we also tabulate both the integer coefficients $X_{J}, Y_{J}, Z_{J}$ for the two units $E_{J}=\left(X_{J}+R_{0} Y_{J}+R_{0}^{2} Z_{J}\right) / I$ with norm +1 , forming a fundamental pair, as well as the $E_{J}$ and the integers $F_{J}=\operatorname{trace}\left(E_{J}^{2}\right)$.


1. Introduction. The first author [4], [5] recently gave a new method for finding a fundamental pair of units in totally real cubic fields. This method is an improvement of one due to Godwin [8]. The earlier version [4] of the main theorem contained some possible exceptional cases (presumed not to exist) for which the determination of the fundamental pair was less simple. Godwin [10] gave a clever and very short argument which proved that the exceptional cases do not exist. The later paper [5] provided a much simpler proof of the main theorem in which there are no longer any exceptional cases.

The purpose of the present paper is to apply the algorithm of [5] to the actual computation of units and to tabulate the fundamental pairs of units $E_{1}$ and $E_{2}$ and other information for all the 250 totally real fields $F$ with field discriminant $D \leqslant 6,885$. The resulting table has been photographically reproduced from the computer output.

The fundamental pairs of units are standardized so as to have a norm of +1 ; in common with all integers in $F$, they have a representation

$$
\begin{equation*}
E_{J}=\left(X_{j}+R_{0} Y_{J}+R_{0}^{2} Z_{J}\right) / I \quad(j=1,2) \tag{1}
\end{equation*}
$$

Here $X_{J}, Y_{J}, Z_{J}$ are rational integers, $R_{0}$ is the largest zero of a certain irreducible, monic defining polynomial $g(x)$ with rational integer coefficients and polynomial discriminant $D_{g}$, and $I=I_{g}$, the index of $g(x)$, is the positive integer $\left(D_{g} / D\right)^{1 / 2}$.

[^0]The table lists the coefficients $A, B, C$ in

$$
\begin{align*}
g(x) & =x^{3}-A x^{2}+B x-C \\
& =\left(x-R_{0}\right)\left(x-R_{1}\right)\left(x-R_{2}\right), \quad R_{0}>R_{1}>R_{2}>0 \tag{2}
\end{align*}
$$

as well as the index $I$ of $g(x)$ and an approximation to the largest zero $R_{0}$ of $g(x)$. In addition, the coefficients $X_{J}, Y_{j}, Z_{j}$ in (1) and approximations to the units $E_{j}$ are given; also tabulated are the quantities

$$
\begin{equation*}
F_{J}=\operatorname{trace}\left(E_{J}^{2}\right) \quad(j=1,2), \tag{3}
\end{equation*}
$$

which play an important role in our determination of the $E_{ر}$. Of course, $g(x)$ is not unique but, as we explain in Section 3, we have tried to pick it so that $I$ is minimal.

The table also lists the discriminant $D$ and class number $H$ of the field $F$ as well as an approximation to its regulator $R$ defined by

$$
R=\left|\operatorname{det}\left(\begin{array}{ll}
\log \left|E_{1}\right| & \log \left|E_{1}^{\prime}\right|  \tag{4}\\
\log \left|E_{2}\right| & \log \left|E_{2}^{\prime}\right|
\end{array}\right)\right|
$$

where $E_{1}^{\prime}, E_{2}^{\prime}$ are the conjugates of $E_{1}, E_{2}$ obtained by replacing $R_{0}$ in (1) by $R_{1}$. The values for $D$ and $H$ have been copied from the table of Angell [1], as have most of the triples $A, B, C$. For $D<20,000$, a list of discriminants and class numbers has been computed independently by Godwin [9] and others.

In Section 3 we give some of the details of the computer program which determined the $X_{j}, Y_{J}, Z_{j}$ of (1). Here we give a brief outline of Cusick's algorithm on which the program is based. If $F$ is a totally real cubic field with a defining integer $r$, then any integer $\lambda$ in $F$ is of the form

$$
\begin{equation*}
\lambda=x+y r+z Q(r), \tag{5}
\end{equation*}
$$

where $Q(r)$ is a fixed quadratic in $r$ with rational coefficients and $x, y, z$ are rational integers determined by $\lambda$. For any $\alpha$ in $F$, we define

$$
\begin{equation*}
T(\alpha)=\operatorname{trace}\left(\alpha^{2}\right)=\alpha^{2}+\alpha^{\prime 2}+\alpha^{\prime \prime 2}, \quad \operatorname{norm}(\alpha)=\alpha \alpha^{\prime} \alpha^{\prime \prime} \tag{6}
\end{equation*}
$$

where $\alpha, \alpha^{\prime}, \alpha^{\prime \prime}$ denote the conjugates of $\alpha=\alpha^{(0)}$. As the function $T(\lambda)$ is a positive-definite ternary quadratic form in $x, y, z$ whose values are rational integers, we can systematically change $x, y, z$ and seek a minimal value of $T(\lambda)$ for $\lambda$ 's which are units. The minimizing unit $\lambda$ is denoted by $\varepsilon_{1}$. We then continue computing $T(\lambda)$, if necessary, until another minimizing unit $\varepsilon_{2} \neq \pm \varepsilon_{1}^{m}, m$ a rational integer, is obtained. Cusick's result [5, Theorem 1] is:

Theorem. The units $\varepsilon_{1}, \varepsilon_{2}$ are a fundamental pair of units for the totally real cubic field.

In the table, the defining integer $r$ of $F$ is called $R_{0}$ and the units $\varepsilon_{1}, \varepsilon_{2}$ are called $E_{1}, E_{2}$.
It is a consequence of (3) and $\left|E_{J} E_{J}^{\prime} E_{j}^{\prime \prime}\right|=1$ that, for example, $F_{J} \geqslant E_{J}^{\prime \prime 2}=$ $1 /\left(E_{J}^{2} E_{J}^{\prime 2}\right) \geqslant 1 /\left(F_{J} F_{j}\right)$ for $j=1,2$; more generally, for $i=0,1,2$, we have $1 / F_{J} \leqslant$ $\left|E_{J}^{(t)}\right| \leqslant F_{J}^{1 / 2}$. As $F_{J}$ is minimal, $\left|E_{J}^{(t)}\right|$ is not too small, and the relative error in computing $\left|E_{j}^{(i)}\right|$ should be good; the same is true of the absolute error in calculating $\log \left|E_{J}^{(i)}\right|$. Hence, the absolute error in finding the regulator $R$ in (4) should be satisfactory.




2. Other Tables and Methods. Most other tables of fundamental units use a method of Voronoĭ [15]. An account of this is given in the book of Delone and Faddeev [6, Chapter IV, Part A]. However, the Voronoĭ algorithm is very complicated, since it depends on a detailed consideration of sequences of points in various lattices.

We know of only two published tables of more than a few cases of fundamental pairs of units in general totally real cubic fields. The first of these, due to Billevich [2], lists the 33 fields (plus 7 duplications) with discriminant $D<1,300$. He gives the field discriminant, an integral basis, a defining polynomial for the field, and the coefficients of the fundamental pair with respect to this basis. Billevich uses his own method for the calculation of the units. With this method, computational difficulties arise for discriminants larger than the small ones considered by Billevich (see Steiner and Rudman [14]). The second table, by Williams and Zarnke [16], gives fundamental pairs for various fields determined by irreducible cubic equations; for example, they list the coefficients of a fundamental pair with respect to the natural integral basis for all the totally real cubic fields defined by $x^{3}-p x-q=0$ with $|p| \leqslant 15$, $|q| \leqslant 15$. The discriminants of the fields are not given, and no attempt is made to indicate different pairs $p, q$ that give the same field. The Voronoĭ algorithm was used to compute the units, and an account of how this algorithm was implemented is given.

Among the unpublished tables is a large one of Angell who describes it in [1]. This was obtained by using the Voronoĭ procedure on the 4,804 fields with $D<100,000$. The actual table gives the field discriminant, the class number of the field, a defining polynomial with its index, and the coefficients in a representation (1) of the fundamental units. It is known that about ten fields with $D>30,000$ are missing from this table, and that some of the fundamental units are wrong (see Ennola and Turunen [7], and Llorente and Oneto [12]). There are other errors in [1], and apparently also in [12] (see Ennola and Turunen [7]). Some of these errors presumably result from mistakes in programming the Voronoĭ algorithm for the computer, but neither [1] nor [12] gives details about how this was done.

There is a still larger unpublished table of Ennola and Turunen [7] who applied Voronor's method to the 26,440 fields with $D<500,000$. No errors are known in this table, but 300 -digit precision was used to handle the worst cases. The actual table gives the ordinal number for each field in the list, the field discriminant and class number, coefficients for an integral basis, a defining polynomial, and coefficients in a representation of two fundamental units with respect to the given integral basis.

The Voronori procedure is certainly much faster than the method of the present paper for the worst cases (essentially those in which the fundamental units have at least one large conjugate). On the other hand, the necessary programming for the Voronoir algorithm is quite intricate, as is shown by the errors in previous tables produced by that method.

One advantage of the Cusick procedure [5] is its extreme simplicity. Another advantage of the procedure used here is that it makes easier the computation of the regulator $R$ of the cubic fields. As noted in Section 1, for our units, the $\left|E_{j}^{(i)}\right|$ are not small, so that $R$ can be computed with good accuracy. However, other algorithms, including Voronor's, can perform badly in this respect. There is a good example of
this in the small table of units and regulators given by Pohst, Weiler and Zassenhaus [13, p. 301]. Even for as small a discriminant as 961, their method (which is based on the geometry of numbers, but is different from Voronor's) gives a value for the regulator which is in error by $0.16 \%$ in spite of a machine precision of 14 digits. This happened, in part, because one of the units in their fundamental pair has a small conjugate.

Regulators are not given in the first four tables mentioned. However, the units in the table of Ennola and Turunen [7] can be used for the accurate computation of regulators. This is because the unit pairs given in their table are not the pairs produced by the Voronoĭ algorithm, but rather are normalized pairs derived from the Voronoĭ units. A comparison of Ennola and Turunen's normalized pairs with our pairs shows that in each of the 250 fields, our first unit $E_{1}$ agrees with one of their units, but this is not always the case for the unit $E_{2}$.

We remark that in the special case of cyclic cubic fields, the discriminant is a square, and there always exists a fundamental pair made up of a unit and one of its conjugates. Cohn and Gorn [3] and Gras [11] use procedures simpler than Voronor's to construct tables of units in the cyclic case, although Gras does not list the units. The method of the present paper becomes much simpler in the cyclic case and always gives a fundamental pair made up of two conjugate units [4, Theorem 2], but we have chosen not to make a separate table for the cyclic case.
3. The Computer Program. This was initially written for and tested on the HP-85 microcomputer and subsequently modified and run on the CDC 6400 mainframe which produced the table above. With the exception of $R_{0}, E_{1}, E_{2}, R$ and certain bounds, all computations were done in integer arithmetic.

For each of the totally real cubic fields $F$ with discriminant $D \leqslant 6,885$, we used the table of Angell [1] to copy the value of $D, H$ and the coefficients $a, b, c$ of a polynomial

$$
h(x)=x^{3}-a x^{2}+b x-c
$$

one of whose roots, say $r$, generates $F$. Let $I_{h}$ be the index of $h(x)$ and let $D_{h}$ be its discriminant, so that $D_{h}=-4 a^{3} c+a^{2} b^{2}+18 a b c-\left(4 b^{3}+27 c^{2}\right)$.

If $D_{h}=D$, then $I_{h}=1$ and $1, r, r^{2}$ form an integral basis for $F$, called a "power basis". In this case, the program takes $g(x)$ in (2) to be $h(x)$. Then, by Angell's choice of $a, b, c$, the smallest zero $R_{2}$ of $g(x)$ is in the interval $(0,1)$ and $A, B, C>0$.

If $D_{h} \neq D$, we attempted to reduce $I_{h}$ so as to obtain a power basis. To this end, the program forms the irreducible monic polynomial $H(z)=(\gamma z+\delta)^{3} h(\zeta) / \phi$, where $\zeta=(\alpha z+\beta) /(\gamma z+\delta)$ and $\phi=\gamma^{3} h(\alpha / \gamma)$, for various rational integers $\alpha, \beta, \gamma, \delta$ in $[-10,10]$ such that $\alpha \delta \neq \beta \gamma$ and $H(z)$ has integral coefficients; of course, $H(z)$ also generates $F$. If any $H(z)$ has $I_{H}=1$, then we let $G(z)=H(z)$; otherwise, $G(z)$ was taken to be an $H(z)$ with the least index $I_{H}$ that arose from this procedure. Letting $\rho$ be the smallest zero of $G(z)$, we defined $g(x)=G(x+[\rho])$, guaranteeing that the smallest zero $R_{2}$ of $g(x)$ is in $(0,1)$ and $A, B, C>0$; also, $I_{g}=I_{G}$.

In the 250 cases we calculated, this algorithm resulted in 25 cases of index 2 compared with 45 cases in Angell's table [1] and 54 cases in the table of Ennola and Turunen [7]; we also had 2 cases of index 3, compared with 4 cases in the tables of

Angell and Ennola-Turunen. It is possible, of course, that further calculation would reduce the index in some, but not all, of these cases; e.g., in the case of $D=961$, no polynomial has index 1.

Given the polynomial $g(x)$, the program computes its zeros $R_{0}>R_{1}>R_{2}$ in (2). Next the program finds an integral basis $1, R_{0}, S$ for the field $F$. If $I_{g}=1$, the program takes $S=R_{0}^{2}=Q\left(R_{0}\right)$. Otherwise, a standard algorithm of Voronoĭ (see Delone and Faddeev [6, pp. 108-112]) was used to determine

$$
S=\left(u+v R_{0}+R_{0}^{2}\right) / I=Q\left(R_{0}\right)
$$

for suitable rational integers $u, v$, which are obtained from a solution of a simultaneous pair of congruences involving $g(x)$ and $g^{\prime}(x)$.

For any integer $\lambda$ in $F$, (6) and (5) with $r=R_{0}$ give $T(\lambda)=F(x, y, z)$, where

$$
\begin{aligned}
F(x, y, z) & =\sum_{k=0}^{2}\left\{x+y R_{k}+z Q\left(R_{k}\right)\right\}^{2} \\
& =a_{0} x^{2}+b_{0} y^{2}+c_{0} z^{2}+2\left(a_{1} y z+b_{1} x z+c_{1} x y\right)
\end{aligned}
$$

for suitable rational integers $a_{0}, b_{0}, c_{0}, a_{1}, b_{1}, c_{1}$; of course, $a_{0}=3$ and all these coefficients are expressible in terms of the power symmetric functions of the zeros $R_{k}$ of $g(x)$ or, alternatively, in terms of $A, B, C$. The program calculates these six integers and also the ten integers occurring in $N(x, y, z)=\operatorname{norm}(\lambda)$, where

$$
\begin{align*}
N(x, y, z)= & \prod_{k=0}^{2}\left\{x+y R_{k}+z Q\left(R_{k}\right)\right\} \\
= & a_{2} x^{3}+b_{2} y^{3}+c_{2} z^{3}+a_{3} x^{2} y+b_{3} x^{2} z  \tag{7}\\
& +c_{3} x y^{2}+d_{3} y^{2} z+e_{3} x z^{2}+f_{3} y z^{2}+g_{3} x y z
\end{align*}
$$

The last function is needed to test whether $N(x, y, z)= \pm 1$, i.e., whether $\lambda$ is a unit of $F$.

To facilitate the search for the minima of the positive-definite quadratic form $F(x, y, z)$, the program next determines the real coefficients $k$, appearing in the identity

$$
\begin{equation*}
F(x, y, z)=\left(k_{1} x+k_{2} y+k_{3} z\right)^{2}+\left(k_{4} y+k_{5} z\right)^{2}+\left(k_{6} z\right)^{2}, \tag{8}
\end{equation*}
$$

where

$$
\begin{gathered}
k_{1}=a_{0}^{1 / 2}, \quad k_{2}=c_{1} a_{0}^{-1 / 2}, \quad k_{3}=b_{1} a_{0}^{-1 / 2}, \quad k_{4}=\left(b_{0}-k_{2}^{2}\right)^{1 / 2} \\
k_{5}=\left(a_{1}-k_{2} k_{3}\right) / k_{4}, \quad k_{6}=\left(c_{0}-k_{3}^{2}-k_{5}^{2}\right)^{1 / 2}=\left(D / a_{0}\right)^{1 / 2} / k_{4} .
\end{gathered}
$$

The final step is to search the values of $F(x, y, z)$ until the fundamental units $\varepsilon_{1}$, $\varepsilon_{2}$ of the Theorem above are found. This is done by picking a number $L$ (say $D^{1 / 2}$ ) and only considering $x, y, z$ such that $F(x, y, z) \leqslant L$, a condition which imposes bounds on $z, y, x$, as we now explain. If the last inequality holds, then (8) shows that $|z| \leqslant L^{1 / 2} / k_{6} \equiv Z_{2}$; as $F(x, y,-z)=F(-x,-y, z)$, it suffices to consider $z \geqslant 0 \equiv Z_{1}$. Thus, $z$ must lie in the interval $\left[Z_{1}, Z_{2}\right]$. For a given $z$ of this kind, (8) also gives $\left|k_{4} y+k_{5} z\right| \leqslant\left(L-k_{6}^{2} z^{2}\right)^{1 / 2}$, so that $y$ is confined to some interval $\left[Y_{1}, Y_{2}\right]$ depending on $z$. Similarly, for given $z, y$, (8) implies that $x$ must lie in some $\left[X_{1}^{\prime}, X_{2}^{\prime}\right]$. Finally, if we let $V_{k}=y R_{k}+z Q\left(R_{k}\right)$, then (7) shows that $N(x, y, z)<-1$ if
$x<X_{1}^{\prime \prime}$, and $N(x, y, z)>1$ if $x>X_{2}^{\prime \prime}$, where

$$
X_{1}^{\prime \prime}=\min \left(-V_{0},-V_{1},-V_{2}\right)-1, \quad X_{2}^{\prime \prime}=\max \left(-V_{0},-V_{1},-V_{2}\right)+1
$$

Hence, $x$ can be restricted to $\left[X_{1}, X_{2}\right]$, where the bounds $X_{1}=\max \left(X_{1}^{\prime}, X_{1}^{\prime \prime}\right)$ and $X_{2}=\min \left(X_{2}^{\prime}, X_{2}^{\prime \prime}\right)$ depend on $z, y$. (Actually, $x$ can be confined to the union of three subintervals of $\left[X_{1}, X_{2}\right]$.)

For given $z, y, x$ in their respective ranges, the program checks the condition $N(x, y, z)= \pm 1$; if this is not satisfied, then the corresponding $\lambda$ is not a unit and the next largest $x$ is tried. Otherwise, the triple ( $x, y, z$ ) is stored in a tabie ior units after standardizing so that $N(x, y, z)=+1$. The value $F(x, y, z)$ is compured and compared with the previous minimum value for $F$, thereby keeping this minimum current. Once a unit $\lambda_{0}$ satisîying $T\left(\lambda_{0}\right) \leqslant L$ has been found, the program checks the condition $z>T\left(\lambda_{0}\right)^{1 / 2} / k_{6}$. If this hoids, then $F(x, y, z)>T\left(\lambda_{0}\right)$, so that no additional $z$ 's need be tried; i.e., the current minimum value for $F$ is $F_{1}$, and the $z, y, x$ that proáuces $F_{1}$ defines $\varepsilon_{1}=E_{1}$.

The program lets $z, y, x$ run over their respective ranges. Ïf no unit $\lambda$ with $T(\lambda) \leqslant L$ is found, then $L$ is doubled and the process is repeated.

Once $\varepsilon_{1}$ has been found, the program continues its search with the current value of $L$. Whenever it finds a unit $\lambda$, it checks that $\lambda \neq \pm \varepsilon_{1}^{m}$ for each integral $m$. If this is satisfied, then $\lambda$ becomes a candidate for $\varepsilon_{2}$; the value $T(\lambda)$ is now used to replace $L$, and appropriate bounds on $z, y, x$ are recomputed. If no independent unit $\lambda$ is found after $z, y, x$ have run through all their values, then $L$ is doubied and the computation is started from the beginning. Uitimately, a unit $\lambda \neq \pm \varepsilon_{1}^{m}$ is found, and the minimum of $T(\lambda)$ for such $\lambda$ is defined as $F_{2}$ with the associated $\lambda$ defined as $\varepsilon_{2}=E_{2}$.

In passing, we remark that our original HP-85 program reduced the positive-definite ternary form $F(x, y, z)$ to Gauss form. However, the running time for this search was no better than for the reduction in (8). We also tried changing the roies of $x, y, z$ in (8), but here, also, we achieved no improvement.
Department of Mathematics
State Unıversity of New York at Buffalo
Buffalo, New York 14214-3093

1. I. O. ANGELL, "A table of totaily real cubic fields," Math. Comp., v. 30, 1976, pp. 184-187.
2. K. K. Billevich, "On the units of algebraic fields of the third and fourth degrees" (in Russian), Mat. Sb., v. 40, 1956, pp. 123-136, and v. 48, 1959, p. 256 (some corrections).
3. H. Cohn \& S. Gorn, "A computation of cyclic cubic units," J. Res. Nat. Bur. Standards, v. 59, 1967, pp. 155-168.
4. T. W. Cusick, "Finding fundamental units in cubic fields," Math. Proc. Cambridge Philos. Soc., v. 92, 1982, pp. 385-389.
5. T. W. Cusick, "Finding fundamental units in totally real fields," Math. Proc. Cumbridge Philos. Soc., v. 96, 1984, pp. 191-194.
6. B. N. Delone \& D. K. Faddeev, The Theory of Irrationalities of the Third Degree (in Russian), Trudy Mat. Inst. Steklov., vol. 11, 1940; English transl., Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R. I., Second prunting 1978.
7. V. Ennola \& R. Turunen, "On totally real cubic fields," Math. Comp., v. 44, 1985, pp. 495-518.
8. H. J. Godwin, "The determination of units in totally real cubic fields," Proc. Cambridge Philos. Soc., v. 56, 1960, pp. 318-321.
9. H. J. Godwin, "The determination of the class-numbers of totally real cubic fields," Proc. Cambraige Phulos. Soc., v. 57, 1961, pp. 728-730.
10. H. J. Godwin, "A note on Cusick's theorem on units in totally real cubic fields," Math. Proc. Cambridge Philos. Soc., v. 95, 1984, pp. 1-2.
11. M.-N. Gras, "Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $Q$," J. Reine Angew. Math., v. 277, 1975, pp. 89-116.
12. P. Llorente \& A. V. Oneto, "On the real cubic fields," Math. Comp., v. 39, 1982, pp. 689-692.
13. M. Pohst, P. Weiler \& H. Zassenhaus, "On effective computation of fundamental units, II," Math. Comp., v. 38, 1982, pp. 293-329.
14. R. Steiner \& R. Rudman, "On an algorithm of Billevich for finding units in algebraic number fields," Math. Comp., v. 30, 1976, pp. 598-609.
15. G. F. VoronoI, On a Generalization of the Algorithm for Continued Fractions (in Russian), Doctoral thesis, Warsaw, 1896.
16. H. C. Williams \& C. R. Zarnke, Computer Calculation of Units in Cubic Fields, Proc. Second Manitoba Conf. Numer. Math., 1972, pp. 433-468.

[^0]:    Received May 12, 1986.
    1980 Mathematics Subject Classification (1985 Revision). Primary 11R27, 11R16, 11Y40; Secondary 11 Y70.

