A METHOD FOR FINDING UNITS IN CUBIC ORDERS OF A NEGATIVE DISCRIMINANT*

BY I. V. USPENSKY

Among other extremely remarkable things in Hermite's famous letters to Jacobi† we find a very brief outline of a method which can be used for the actual discovery of units in cubic orders. Much, however, remained to be done in order that Hermite's ideas could be embodied in a really practical method easily applicable to numerical examples. Zolotareff was the first to develop Hermite's suggestion in the case of a negative discriminant. In his little known but remarkable thesis On an indeterminate equation of the third degree published in Russian in 1869, Zolotareff developed a method for finding units in the order $x+y\theta+z\theta^2$ where θ is a root of the irreducible equation $\theta^3=A$, based on Hermite's principle of continuous variables; that is, on the study of successive minima of a certain positive ternary form containing a continuous parameter.

Zolotareff's most important contribution consisted in the peculiar manner of reducing the study of successive minima of a ternary quadratic form to a similar problem concerning binary forms. In itself Zolotareff's method is remarkable, but it requires further complements in order to give all the successive minima, as is strictly required by Hermite's principle, and these complements unfortunately detract much from its practical value. When studying Zolotareff's paper I noticed, however, that, by retaining his basic idea, but departing from Hermite's requirement to consider minima of a variable ternary form, one can build up a new method for finding units in cubic orders of a negative discriminant which can be applied to numerical examples with comparative ease. The best method hitherto known for that purpose is one given by Voronoi in 1896‡.

I do not venture to say that the new method explained in this paper is more expedient. That may be decided only by application of both to numerous examples.

1. An order (or ring) in an algebraic field is a system of integers of that

^{*} Presented to the Society, August 29, 1929; received by the editors in August, 1930.

[†] See Hermite's Collected Works, vol. 1, pp. 131-135.

[‡] G. Voronoi, On a Generalization of the Algorithm of Continued Fractions, Warsaw, 1896 (in Russian).

This remarkable thesis contains also a method of finding two fundamental units in the case of a positive discriminant.

field containing the rational unit and reproducing itself by addition, subtraction, and multiplication of its numbers. An order in a cubic field can be built up by repeated addition and subtraction of three fundamental numbers, $1, \alpha, \beta$, forming its basis. Hence the numbers of an order are obtained from its basic form

$$\phi = x + \alpha y + \beta z$$

by giving to x, y, z all rational integral values. As the numbers α^2 , $\alpha\beta$, β^2 by definition belong to the order they must be contained in the preceding linear form for suitable integral values of the variables. Together with 1, α , β , the numbers 1, $\alpha+c$, $\beta+d$, where c and d are arbitrary integers, form a basis of the same order. By selecting c and d in a proper way the product

$$(\alpha + c)(\beta + d)$$

will be a rational integer. Hence we can always select a basis 1, α , β in such a way that the product $\alpha\beta$ is a rational integer. We shall call a basis of this kind a normal basis. Supposing that the basis is normal we must have the equations

$$\alpha\alpha = e + f\alpha + g\beta,$$

$$\alpha\beta = c,$$

where e, f, g and c are integers. By elimination of β we find the equation which α satisfies,

$$\alpha^3 - f\alpha^2 - e\alpha - cg = 0.$$

Similarly β is a root of the equation

$$\beta^3 + (e/g)\beta^2 + (cf/g)\beta - c^2/g = 0$$

and

$$\beta^2 = -cf/g + (c/g)\alpha - (e/g)\beta.$$

But as β^2 belongs to the order, k = c/g and l = e/g are integers. Thus every order has a basis 1, α , β , where α and β are roots of the respective equations

$$\alpha^3 - f\alpha^2 - gl\alpha - kg^2 = 0,$$

$$\beta^3 + l\beta^2 + kf\beta - k^2g = 0,$$

f, g, k, l being certain integers. Moreover

(1)
$$\alpha \alpha = lg + f\alpha + g\beta,$$
$$\alpha \beta = kg,$$
$$\beta \beta = -kf + k\alpha - l\beta.$$

2. Denoting by α' , α'' conjugate numbers to α and using similar notation for β , the discriminant of the order is given by

$$\begin{vmatrix} 1 & \alpha & \beta \\ 1 & \alpha' & \beta' \\ 1 & \alpha'' & \beta'' \end{vmatrix}^2 = -D,$$

and from now on we shall suppose it to be negative so that D > 0.

By α we denote a number of the real cubic field; then its conjugates α' , α'' are conjugate imaginary numbers. It is easy to see that the discriminant of α is

$$\mathcal{D}(\alpha) = -Dg^2$$

and likewise

By taking

$$\mathcal{D}(\beta) = -Dk^2.$$

3. For practical purposes it is advisable to select numbers α , β of a normal basis in a special way. Namely, we shall take for α a number of the order for which the expression

$$-(\alpha'-\alpha'')^2+2(\alpha-\alpha')(\alpha-\alpha'')$$

is minimum; that is, can only increase if we substitute for α any other number of the order. Let 1, A, B be any normal basis of the order, so that we have

$$AA = LG + FA + GB,$$

AB = KG.

$$\alpha = P + AX + BY,$$

the preceding expression becomes

$$\psi = -(A' - A'')^2 (X - (A/G)Y)^2 + (A - A')(A - A'')(X - (A'/G)Y)(X - (A''/G)Y),$$

which is a positive quadratic form with the determinant -3D. Let the minimum of this form be attained for $X = \lambda$, $Y = \mu$, these being relatively prime numbers. Then we can take for α the number

$$\alpha = P + \lambda A + \mu B$$

where the integer P remains arbitrary. Denoting by λ' , μ' two integers satisfying the equation

$$\lambda \mu' - \lambda' \mu = 1,$$

we can take for the second number of the basis

$$\beta = Q + \lambda' A + \mu' B,$$

and finally dispose of P and Q so as to make the basis 1, α , β normal.

Thus we finally reach the following conclusion: for any given cubic order a normal basis 1, α , β can be found such that

$$-(\alpha'-\alpha'')^2+2(\alpha-\alpha')(\alpha-\alpha'')$$

is minimum; the value of this minimum never exceeds $2D^{1/2}$. On the other hand, as

$$-(\alpha'-\alpha'')^2(\alpha-\alpha')^2(\alpha-\alpha'')^2=Dg^2,$$

it is easy to see that

$$- (\alpha' - \alpha'')^2 + 2(\alpha - \alpha')(\alpha - \alpha'') \ge 3(Dg^2)^{1/3}.$$

In the following we shall suppose that the normal basis of the order has been chosen as explained in this paragraph.

4. Again let ϕ represent the basic form of the order

$$\phi = x + \alpha y + \beta z$$

and ϕ', ϕ'' its conjugates. For the sake of simplicity introducing the notation

$$\Phi = \phi' \phi''$$

we shall consider a positive ternary quadratic form

$$f = 2\Phi + \phi^2/\Delta$$

containing a continuously varying positive parameter Δ . The discriminant of this form is D/Δ . Besides the form f we shall consider its adjoint form F whose expression is

$$F = -(\alpha'' - \alpha')^2 \omega^2 + 2(\alpha - \alpha')(\alpha - \alpha'')\Omega/\Delta,$$

where ω is a linear form of the contragredient variables X, Y, Z defined by

$$(\alpha'' - \alpha')\omega = Z(\alpha'' - \alpha') + Y(\beta' - \beta'') + X(\alpha'\beta'' - \alpha''\beta'),$$

while

$$\Omega = \omega' \omega''$$

Referring to the equations (1) we easily find

$$\omega = Z + (\alpha/g)Y + (\beta + l)X.$$

Numbers ω for integral values of X, Y, Z constitute a modulus with the basis 1, α/g , β . It can be readily verified that the product of any number of this modulus by any number of the order again belongs to the same modulus. According to Dedekind's terminology the cubic order $[1, \alpha, \beta]$ is the order of the modulus $[1, \alpha/g, \beta]$. They coincide if and only if g = 1. Needless to say that the discriminant of F is D^2/Δ^2 .

We can express x, y, z linearly in ϕ , ϕ' , ϕ'' and similarly X, Y, Z are expressible linearly in ω , ω' , ω'' . By substituting these expressions in the bilinear form

$$Xx + Yy + Zz$$
,

we can find a remarkable expression of the latter. But such a straightforward way would lead to complicated calculations. The best and most elegant way is to proceed as follows.

Let i, i_1 , i_2 be three mutually perpendicular unit vectors, so that performing the scalar multiplication we have

$$ii = 1$$
, $ii_1 = i_1i = 0$,
 $i_1i_1 = 1$, $ii_2 = i_2i = 0$,
 $i_2i_2 = 1$, $i_1i_2 = i_2i_1 = 0$.

Now take the scalar product of the vector

$$A = i(\alpha'' - \alpha')\omega + i_1(\alpha - \alpha'')\omega' + i_2(\alpha' - \alpha)\omega''$$

by the vector

$$B = i\phi + i_1\phi' + i_2\phi''.$$

We have first

$$A \cdot B = (\alpha'' - \alpha')\phi\omega + (\alpha - \alpha'')\phi'\omega' + (\alpha' - \alpha)\phi''\omega''.$$

On the other hand, if we express A, B as linear functions of x, y, z and X, Y, Z with vectorial coefficients, we easily find

$$A \cdot B = \begin{vmatrix} 1 & \alpha & \beta \\ 1 & \alpha' & \beta' \\ 1 & \alpha'' & \beta'' \end{vmatrix} (Xx + Yy + Zz) = (-D)^{1/2}(Xx + Yy + Zz)$$

and thus

(2)
$$(-D)^{1/2}(Xx + Yy + Zz) = (\alpha'' - \alpha')\phi\omega + (\alpha - \alpha'')\phi'\omega' + (\alpha' - \alpha)\phi''\omega''$$

This is the required expression.

5. The following simple proposition is of fundamental importance for what follows.

Let f(x, y, z) be a positive ternary quadratic form with the discriminant D, and F(x, y, z) its adjoint form with discriminant D^2 . There exist two triads of integers x, y, z; X, Y, Z without common factor connected by the bilinear relation

$$Xx + Yy + Zz = 0$$

and satisfying the inequalities

$$f(x, y, z) < \frac{4}{3} D^{1/3}, \ F(X, Y, Z) < \frac{4}{3} D^{2/3}.$$

For we can first find a triad x, y, z without common factor, so as to make

$$f(x, y, z) < \frac{4}{3}D^{1/3}$$
.

On the other hand, the bilinear relation

$$Xx + Yy + Zz = 0$$

is satisfied in the most general manner by

$$X = \lambda \alpha + \mu \alpha',$$

$$Y = \lambda \beta + \mu \beta',$$

$$Z = \lambda \gamma + \mu \gamma'.$$

where λ , μ are arbitrary integers and α , β , γ ; α' , β' , γ' are two independent and fundamental solutions of the indeterminate equation

$$\xi x + \eta y + \zeta z = 0.$$

Introducing these expressions for X, Y, Z into F we obtain a binary form in λ , μ whose determinant is -Df(x, y, z). Hence, it is possible to take for λ , μ relative prime numbers so as to have

$$F(X, Y, Z) \leq \left[\frac{4}{3}Df(x, y, z)\right]^{1/2},$$

whence

$$F(X, Y, Z) < \frac{4}{3}D^{2/3}.$$

The numbers X, Y, Z have no common divisor if λ and μ are relatively prime.

6. Whatever positive value we attribute to Δ it is possible therefore to find two triads x, y, z; X, Y, Z consisting of numbers without common divisor and satisfying the inequalities

$$\begin{split} f &= 2\Phi + \frac{\phi^2}{\Delta} < \frac{4}{3} \left(\frac{D}{\Delta}\right)^{1/3}, \\ F &= - (\alpha'' - \alpha')^2 \omega^2 + 2(\alpha - \alpha')(\alpha - \alpha'') \frac{\Omega}{\Lambda} < \frac{4}{3} \left(\frac{D}{\Lambda}\right)^{2/3}, \end{split}$$

together with the bilinear relation

$$Xx + Yy + Zz = 0.$$

Let us seek further information concerning these triads when $\Delta = 1$. When $\Delta = 1$ it is easy to present f and F in the form

$$f = 3(x + ly + mz)^{2} + \frac{1}{3}\psi(y, z),$$

$$F = \psi(Y', Z') + (D/3)X^{2},$$

where $\psi(y, z)$ is the form

$$\psi(y, z) = -(\alpha'' - \alpha')^{2}(y - (\alpha/g)z)^{2} + 2(\alpha - \alpha')(\alpha - \alpha'')(y - (\alpha'/g)z)(y - (\alpha''/g)z),$$

and

$$Y' = -Z + mX,$$
 $Z' = Y - lX,$ $l = \frac{1}{3}f, \ m = -\frac{1}{3}l, \ n = \frac{-\frac{2}{3}lf + l\alpha - f\beta}{gl + f\alpha + 3g\beta - \frac{1}{2}f^2}.$

If we want to make

$$F < (4/3)D^{2/3}$$

we have necessarily

$$X^2 < 4D^{-1/3}$$

and hence X=0 if only $D \ge 64$. On the other hand, the minimum of $\frac{1}{3}\psi(y,z)$ is attained for y=1, z=0, if the basis was selected according to the explanations in §3. Now, if this minimum is $\ge (4/3)D^{1/3}$, which is certainly the case if g>1, it is obvious that the inequality

$$f < (4/3)D^{1/3}$$

cannot be satisfied except by taking $x = \pm 1$, y = 0, z = 0. But it may happen that this minimum is $<(4/3)D^{1/3}$. The smallest value of $\frac{1}{3}\psi(y,z)$ corresponding to $z\neq 0$ is then $>\frac{1}{4}D^{2/3}$ and this is surely $>(4/3)D^{1/3}$ if D>151. Hence, if D>151 we have necessarily z=0.

The excluded cases deserve special attention. There are only a finite number of cubic orders with $D \le 151$. They are*

^{*} See B. Delaunay's beautiful paper in Mathematische Zeitschrift, vol. 30 (1930).

$$D = 140; [1, \theta, \theta^{2}]; \theta^{3} + 2\theta - 2 = 0;$$

$$D = 139; [1, \theta, \theta^{2}]; \theta^{3} - 8\theta - 9 = 0;$$

$$D = 135; [1, \theta, \theta^{2}]; \theta^{3} - 3\theta - 3 = 0;$$

$$D = 116; [1, \theta, \theta^{2}]; \theta^{3} - \theta^{2} - 2 = 0;$$

$$D = 108; [1, \theta, \theta^{2}]; \theta^{3} - 2 = 0;$$

$$D = 107; [1, \theta, \theta^{2}]; \theta^{3} - 2\theta^{2} + 4\theta - 1 = 0;$$

$$D = 104; [1, \theta, \theta^{2}]; \theta^{3} - \theta - 2 = 0;$$

$$D = 87; [1, \theta, \theta^{2}]; \theta^{3} + \theta^{2} + 2\theta - 1 = 0;$$

$$D = 83; [1, \theta, \theta^{2}]; \theta^{3} + 2\theta^{2} + 2\theta - 1 = 0;$$

$$D = 76; [1, \theta, \theta^{2}]; \theta^{3} - \theta^{2} + 3\theta - 1 = 0;$$

$$D = 59; [1, \theta, \theta^{2}]; \theta^{3} + 2\theta - 1 = 0;$$

$$D = 44; [1, \theta, \theta^{2}]; \theta^{3} + \theta^{2} + \theta - 1 = 0;$$

$$D = 31; [1, \theta, \theta^{2}]; \theta^{3} + \theta - 1 = 0;$$

$$D = 23; [1, \theta, \theta^{2}]; \theta^{3} - \theta - 1 = 0.$$

It can be verified directly that for $D \ge 76$ it always turns out that z=0 while in the remaining cases the fundamental unit is obvious. Thus if $D \ge 76$ we have X=0 and z=0 and the bilinear relation reduces to

$$Yy = 0$$
.

Hence, if $y \neq 0$ we have Y = 0, X = 0, $Z = \pm 1$ and if $Y \neq 0$ we have $x = \pm 1$, y = 0, z = 0. If, therefore, for $\Delta = 1$ we try to satisfy the inequalities

$$f < (4/3)D^{1/3},$$

 $F < (4/3)D^{2/3},$

together with the relation

$$Xx + Yy + Zz = 0,$$

it turns out that necessarily either $\phi = \pm 1$ or $\omega = \pm 1$ provided $D \ge 76$. As

$$-(\alpha' - \alpha'')^2 + 2(\alpha - \alpha')(\alpha - \alpha'') \le 2D^{1/2}$$

it is obvious that for $\Delta = 1$ the triads 1, 0, 0 and 0, 0, 1 satisfy all the requirements.

7. As we have seen, for any particular value of Δ there exist two triads x_0 , y_0 , z_0 ; X_0 , Y_0 , Z_0 consisting of numbers without common divisor, connected by the bilinear relation

$$X_0x_0 + Y_0y_0 + Z_0z_0 = 0$$

and satisfying the inequalities

$$f<\frac{4}{3}\left(\frac{D}{\Delta}\right)^{1/3},$$

$$F<\frac{4}{3}\left(\frac{D}{\Delta}\right)^{2/3}.$$

When Δ starts to increase these inequalities continue to hold, but that cannot go on indefinitely. The triad x_0 , y_0 , z_0 has to be replaced by another triad when the following equality is reached:

$$f = \frac{4}{3} \left(\frac{D}{\Delta}\right)^{1/3}.$$

Likewise, the triad X_0 , Y_0 , Z_0 has to be replaced when Δ attains such a value that

(b)
$$F = \frac{4}{3} \left(\frac{D}{\Delta}\right)^{2/3}.$$

Equations (a) and (b) have each two positive roots and their greatest roots which interest us can be found as follows.

Let

$$\Gamma = \frac{8}{27}D\left(\frac{k}{\tau_1}\right)^3,$$

where

$$k = \frac{1}{4}N(\phi_0)\left(\frac{D}{27}\right)^{-1/2}; \ \phi_0 = x_0 + \alpha y_0 + \beta z_0,$$

and τ_1 is the smallest positive root of the equation

$$\tau^3 - \tau + k = 0.$$

Then the value of Δ beyond which the triad x_0 , y_0 , z_0 cannot be retained is given by

$$\Delta_0 = \Gamma \Phi_0^{-3} = \Gamma (\phi_0 / N(\phi_0))^3$$
.

Similarly, putting

$$\Gamma' = \frac{8}{27^{1/2}} D | \alpha'' - \alpha' |^{-3} \tau_2^3,$$

where τ_2 is the greatest root of the equation

$$\tau^3 - \tau + k = 0.$$

and

$$k = \frac{g}{4}N(\omega_0)\left(\frac{D}{27}\right)^{-1/2},$$

we have for the greatest root of the equation (b) the following expression:

$$\Delta_1 = \Gamma' \omega_0^{-3} = \Gamma' (\Omega_0 / N(\omega_0))^3$$
.

Suppose now that $\Delta_0 < \Delta_1$. Then we have to change the triad x_0 , y_0 , z_0 when the variable parameter Δ reaches the value Δ_0 , the second triad remaining the same in a certain interval beyond Δ_0 . The new triad following x_0 , y_0 , z_0 can be determined by the process described in §5. For practical purposes it is advantageous to proceed in the following manner.

Determine three integers l, m, n from the equations

$$ny_0 - mz_0 = X_0,$$

 $lz_0 - nx_0 = Y_0,$
 $mx_0 - ly_0 = Z_0,$
 $x = \lambda x_0 + \mu l,$

and set

(A)
$$y = \lambda y_0 + \mu n,$$
$$z = \lambda z_0 + \mu n.$$

By substituting these expressions into the form ϕ it becomes

$$\phi = \phi_0 \lambda + (l + m\alpha + n\beta)\mu.$$

Multiplying it by Φ_0 we obtain another linear form,

$$g = N(\phi_0)\lambda + A\mu,$$

where A is a determined number of the order. Now the binary quadratic form

$$T = 2G + N(\phi_0)g^2/\Gamma,$$

where

$$G = g'g''N(\phi_0)^{-1}$$

differs but by a constant factor from f. By reduction of the form T we obtain integers λ , μ making f minimum. Substituting the values of λ , μ thus found, into (A), we obtain a triad x_1 , y_1 , z_1 taking the place of x_0 , y_0 , z_0 .

The advantage of considering the form T instead of f resides in the fact that coefficients of g and G are moderate numbers limited by D.

If $\Delta_1 < \Delta_0$ we have to change the triad X_0 , Y_0 , Z_0 and this can be done as follows.

Determine three integers L, M, N from the equations

$$NY_0 - MZ_0 = x_0,$$

 $LZ_0 - NX_0 = y_0,$
 $MX_0 - LY_0 = z_0,$

and set

(B)
$$X = \lambda X_0 + \mu L,$$
$$Y = \lambda Y_0 + \mu M,$$
$$Z = \lambda Z_0 + \mu N.$$

By this substitution the form ω becomes

$$\omega = \omega_0 \lambda + (N + M\alpha/g + L(\beta + l))\mu$$

and, multiplying it by Ω_0 , we obtain another linear form in λ , μ ,

$$N(\omega_0)\lambda + B\mu = N(\omega_0)h.$$

The binary quadratic form

 $V = h^2 + 2H/\Gamma_1,$ $H = N(\omega_0)h'h''$

where

and

differs but by a constant factor from F. By the process of reduction we find integers λ , μ giving a minimum of V or F and substituting them into (B) we have a triad X_1 , Y_1 , Z_1 following X_0 , Y_0 , Z_0 .

 $\Gamma_1 = 8(D/27)^{1/2} \tau_2^3 g^{-1}$

8. The process described in the preceding paragraph is simple and the only objection that could be raised is that Γ and Γ' are determined by the solution of the cubic equation

$$\tau^3 - \tau + k = 0$$

which may appear burdensome. However, this equation having three real roots can easily be solved by known and handy formulas. On the other hand, because of the existence of three real roots we have necessarily

$$k<\frac{2\cdot 3^{1/2}}{9}<0.385,$$

and it is easy to form a small table giving $\log \tau_2$ and $\log (k/\tau_1)$ to three decimal places, which is amply sufficient in most cases. If such a table cannot be used, which can happen only under extremely exceptional circumstances, then direct solution becomes necessary. However, the labor involved in this

solution is quite insignificant compared with that required by numerous other operations. From the fact that

$$k<\frac{2\cdot 3^{1/2}}{9},$$

it follows readily that numbers ϕ and ω obtained in the described manner have their norms limited by D; we have in fact

$$N(\phi) < (8/27)D^{1/2}, \ N(\omega) < (8/27)D^{1/2}g^{-1}.$$

To facilitate the application of our method to numerical examples, we give here a small table mentioned above.

TABLE I

k	$\log au_2$	k	$\log au_2$	k	$\log au_2$	k	$\log au_{2}$	k	$\log au_2$
0.01 0.02 0.03 0.04 0.05 0.06 0.07	9.998-10 9.996 9.993 9.991 9.989 9.986 9.984	0.10 0.11 0.12 0.13 0.14 0.15 0.16	9.976 9.973 9.970 9.967 9.964 9.961 9.958	0.19 0.20 0.21 0.22 0.23 0.24 0.25	9.948 9.944 9.940 9.936 9.932 9.928 9.923	0.28 0.29 0.30 0.31 0.32 0.33 0.34	9.908 9.902 9.896 9.889 9.882 9.874 9.864	0.360 0.362 0.364 0.366 0.368 0.370 0.372	9.8410 9.8382 9.8350 9.8318 9.8283 9.8247 9.8206
0.08	9.981 9.979	0.17	9.955 9.951	0.26 0.27	9.918 9.913	0.35 0.36	9.854 9.841	0.374 0.376	9.8162 9.8113

TABLE II

k	$\log{(k/ au_1)}$	k	$\log \over (k/ au_1)$	k	$\log \over (k/ au_1)$	k	$\log \over (k/ au_1)$	k	$\log \atop (k/\tau_1)$
0.01	0.000	0.10	9.996	0.19	9.983	0.28	9.956	0.360	9.9004
0.02	0.000	0.11	9.994	0.20	9.981	0.29	9.952	0.362	9.8977
0.03	0.000	0.12	9.994	0.21	9.978	0.30	9.947	0.364	9.8949
0.04	9.999-10	0.13	9.992	0.22	9.976	0.31	9.942	0.366	9.8919
0.05	9.999	0.14	9.991	0.23	9.973	0.32	9.936	0.368	9.8887
0.06	9.998	0.15	9.990	0.24	9.970	0.33	9.929	0.370	9.8883
0.07	9.998	0.16	9.988	0.25	9.967	0.34	9.921	0.372	9.8815
0.08	9.997	0.17	9.986	0.26	9.964	0.35	9.912	0.374	9.8773
0.09	9.996	0.18	9.985	0.27	9.960	0.36	9.900	0.376	9.8727

9. Starting with the triads $x_0=1$, $y_0=0$, $z_0=0$; $X_0=0$, $Y_0=0$, $Z_0=1$ corresponding to $\Delta=1$ and letting Δ increase, we come to $\Delta=\Delta_0$ determined according to the explanation in (7) where new triads x_1 , y_1 , z_1 ; X_1 , Y_1 , Z_1 replace the old ones and these triads hold until Δ reaches the value $\Delta_1>\Delta_0$ where new triads x_2 , y_2 , z_2 ; X_2 , Y_2 , Z_2 appear in place of x_1 , y_1 , z_1 ; X_1 , Y_1 , Z_1 and so on. Thus we can form an infinite chain of triads

$$\left\{\begin{array}{c} x_0, y_0, z_0 \\ X_0, Y_0, Z_0 \end{array}\right\}; \left\{\begin{array}{c} x_1, y_1, z_1 \\ X_1, Y_1, Z_1 \end{array}\right\}; \left\{\begin{array}{c} x_2, y_2, z_2 \\ X_2, Y_2, Z_2 \end{array}\right\}; \cdots,$$

and two series of corresponding values of Φ and ω ,

(A)
$$\Phi_0 = 1, \Phi_1, \Phi_2, \Phi_3, \cdots,$$

(B)
$$\omega_0 = 1, \, \omega_1, \, \omega_2, \, \omega_3, \, \cdots$$

Let E>1 be the direct fundamental unit of the order and $\epsilon=E^{-1}$ the inverse unit. If series (A) and (B) are extended sufficiently we necessarily find ϵ either in (A) or in (B). To prove this statement we observe first that numbers in the sequence

$$\Delta_0 < \Delta_1 < \Delta_2 < \Delta_3 < \cdots$$

finally surpass any given limit so that the unit E falls into the interval between two consecutive numbers of this sequence. Let x, y, z; X, Y, Z be two triads corresponding to $\Delta = E^3$. We have

$$2\Phi + \phi^{2}/E^{3} < \frac{4}{3} \left(\frac{D}{E^{3}}\right)^{1/3},$$

$$- (\alpha'' - \alpha')^{2}\omega^{2} + 2(\alpha - \alpha')(\alpha - \alpha'')\frac{\Omega}{E^{3}} < \frac{4}{3} \left(\frac{D}{E^{3}}\right)^{2/3},$$

Xx + Yy + Zz = 0,

and

or, by formula (2),

$$(3) \qquad (\alpha'' - \alpha')\phi\omega + (\alpha - \alpha'')\phi'\omega' + (\alpha' - \alpha)\phi''\omega'' = 0.$$

Setting

$$E^{-1}\phi = \overline{\phi} = \overline{x} + \alpha \overline{y} + \beta \overline{z},$$

$$E\omega = \overline{\omega} = \overline{Z} + (\alpha/\varrho)\overline{Y} + (\beta + l)\overline{X}.$$

where \bar{x} , \bar{y} , \bar{z} ; \bar{X} , \bar{Y} , \bar{Z} are integers, the preceding inequalities may also be written as follows:

(4)
$$2\bar{\Phi} + \bar{\phi}^2/1 < (4/3)D^{1/3}, \\ - (\alpha'' - \alpha')^2\bar{\omega}^2 + 2(\alpha - \alpha')(\alpha - \alpha'')\bar{\Omega}/1 < (4/3)D^{2/3}.$$

Now

$$\bar{\phi}\bar{\omega} = \phi\omega$$

and by virtue of (3) and (2)

$$\overline{X}\bar{x} + \overline{Y}\bar{v} + \overline{Z}\bar{z} = 0.$$

It follows from the inequalities (4) that either $\overline{\Phi} = 1$ or $\overline{\omega} = 1$ provided $D \ge 76$. In the former case we have $\Phi = \epsilon$ and in the latter case $\omega = \epsilon$.

10. We are sure, therefore, to find the unit ϵ in (A) or in (B) as soon as the variable parameter Δ reaches the value $\Delta = E^3$. But it may happen that a unit appears in (A) or in (B) before that, and then the question arises whether this is a fundamental unit or not. To settle this question we observe that any unit which may appear in (A) or (B) is <1. Let it be, for example, Φ_k . If $\overline{\Delta}$ is the parameter value for which the equality

$$2\Phi_0 + \frac{\phi_0^2}{\Delta} = \frac{4}{3} \left(\frac{D}{\Delta}\right)^{1/3}$$

is reached, the parameter value corresponding to the equality

$$2\Phi_k + \frac{{\phi_k}^2}{\Delta} = \frac{4}{3} \left(\frac{D}{\Delta}\right)^{1/3}$$

is $\overline{\Delta}\Phi_k^{-3}$, and evidently this must be $>\overline{\Delta}$; that is, $\Phi_k<1$.

In a similar manner it can be proved that any unit ω_k in (B) must be <1. Suppose now that Φ_k is the first unit we meet in the series (A) and (B). It must be a positive power of ϵ , say ϵ^n . Accepting $\overline{\Delta}$ in the same meaning as before, we see that the inequality

(C)
$$2\epsilon^n + \frac{E^{2n}}{\Delta} < \frac{4}{3} \left(\frac{D}{\Delta}\right)^{1/3}$$

holds up to

$$\Delta = \bar{\Delta}E^{3n} > E^{3n}.$$

On the other hand, if n>1 the first parameter value where Φ_k appears must be $\langle E^3 \rangle$, so that (C) holds good for

$$\Delta = E^3, E^6, \cdots, E^{3n}.$$

If $n \ge 3$ we take in (C) $\Delta = E^{3n-3}$ and $\Delta = E^{3n-6}$, and the resulting inequalities are equivalent to

$$2\epsilon + E^2 < (4/3)D^{1/3}; \ 2\epsilon^2 + E^4 < (4/3)D^{1/3},$$

and, supposing $D \ge 76$, we have, by §6.

$$E = a + b\alpha$$
, $E^2 = a' + b'\alpha$,

which is impossible. Hence $n \le 2$. If n = 2, in a similar manner we see that the fundamental unit must be binary,

$$E = a + b\alpha$$

and it is very easy to discover whether the unit ϕ_k , given by our process, can be a square of the binary unit.

If ω_k is the first unit we meet in (A) or (B), in exactly the same manner it may be shown that it is the fundamental unit ϵ unless it is a square of the binary (fundamental) unit, provided again $D \ge 76$. Thus our operations may be stopped as soon as we find in (A) or (B) a unit, and if this is not a fundamental unit, the latter can easily be found. For the remaining discriminants ≤ 59 the method undergoes slight modifications and easily leads to fundamental units.

Note. Although the discovery of the fundamental unit presents no difficulty, it can be shown in certain cases that the first unit found in (A) or (B) is necessarily a fundamental unit. For instance, that is true in the case of the order with basic form

$$\phi = x + y\theta + z\theta^2,$$

where θ is a root of the irreducible equation

$$\theta^3 = A$$
.

11. Before passing to numerical examples designed to illustrate the foregoing method, it is well to collect certain formulas which greatly simplify the march of operations. The first necessary step is to find an appropriate basis of the order as explained in §2. For that purpose one may have a ready expression of the form denoted there by ψ . Written in the usual manner this form is

$$(5) \psi = 3(gl - f^2/3 + f\alpha + 3g\beta, -(2/3)lf + l\alpha - f\beta, -kf - l^2/3 + 3k\alpha - l\beta).$$

When an appropriate basis has been found, we know the corresponding coefficients f, g, k, l and have the following equations which are constantly used:

(6)
$$\alpha \alpha = gl + f\alpha + g\beta,$$
$$\alpha \beta = kg,$$
$$\beta \beta = -kf + k\alpha - l\beta;$$

(7)
$$\alpha' + \alpha'' = f - \alpha, \quad \beta' + \beta'' = -l - \beta,$$
$$\alpha'\alpha'' = g\beta, \qquad \beta'\beta'' = k\alpha,$$
$$\alpha'\beta'' + \alpha''\beta' = -kg - lf + l\alpha - f\beta.$$

Also, it is useful to have before one's eyes the expressions of forms T and V. We have

$$T = 2G + N(\phi_0)g^2/\Gamma,$$

$$g = \Phi_0(\lambda\phi_0 + \mu(l + m\alpha + n\beta)) = N(\phi_0)\lambda + A\mu,$$

$$G = g'g''N(\phi_0)^{-1},$$

$$\Gamma = (8/27)D(k/\tau_1)^3, \quad k = \frac{1}{4}N(\phi_0)(D/27)^{-1/2}.$$

Similarly

$$V = h^2 + 2H/\Gamma_1,$$

$$\Omega_0[\lambda\omega_0 + \{N + M(\alpha/g) + L(\beta + l)\}\mu] = N(\omega_0)h,$$

$$H = N(\omega_0)h'h'',$$

$$\Gamma_1 = 8(D/27)^{1/2}\tau_2^3g^{-1}.$$

As to parameter values where either the triad x_0 , y_0 , z_0 or X_0 , Y_0 , Z_0 has to be changed, they are given by

$$\Delta = \Gamma \Phi_0^{-3}, \ \Delta_1 = \Gamma_1 D^{1/2} g \omega_0^{-3} \ | \ \alpha'' - \alpha' \ |^{-3}.$$

Finally, to obtain $|\alpha'' - \alpha'|$ we have the equation

$$|\alpha'' - \alpha'|^2 = -gl - f^2 + f\alpha + 3g\beta.$$

In finding approximate values of different numbers, it is hardly ever necessary to retain more than three or even two decimals. It is advisable once and for all to have logarithms of

$$8D/27$$
, $8(D/27)^{1/2}g^{-1}$, $gD^{1/2} | \alpha'' - \alpha' |^{-3}$

and also the value of

$$4(D/27)^{1/2}$$
.

As to τ_2 and k/τ_1 , their logarithms are supplied by the auxiliary tables in §8. The different numerical operations required by the method are uniform and go quickly and smoothly after a certain amount of practice.

12. For the first example, let us consider the order $[1, \theta, \theta^2]$ where θ is a root of the equation

$$\theta^3 - \theta^2 + 3\theta - 5 = 0$$

The discriminant of this order is -524, so that D=524. The basis 1, θ , θ^2 is not normal, but the equivalent normal basis is easily found to be

$$1, A = -1 + \theta, B = 3 + \theta^2.$$

Corresponding to this basis we have

$$f = -2$$
, $g = 1$, $k = 2$, $l = -4$.

From (5) we find

$$\psi = 3(-16/3 - 2A + 2B, -16/3 - 4A + 2B, -4/3 + 6A + 4B).$$

On the other hand

$$A = 0.403; B = 4.968,$$

approximately, and

$$\frac{1}{3}\psi = (8.77; 2.99; 20.96).$$

This is a reduced form and therefore the basis 1, A, B satisfies all the requirements. Denoting by α , β the last two numbers of this basis, we have

$$\alpha = 0.403; \ \beta = 4.968,$$

and by (6) and (7)

$$\alpha\alpha = -4 - 2\alpha + \beta, \quad \beta\beta = 4 + 2\alpha + 4\beta, \quad \alpha\beta = 2,$$

$$\alpha' + \alpha'' = -2 - \alpha, \quad \beta' - \beta'' = 4 - \beta,$$

$$\alpha'\alpha'' = \beta, \quad \beta'\beta'' = 2\alpha,$$

$$\alpha'\beta'' + \alpha''\beta' = -10 - 4\alpha + 2\beta.$$

Next we find

$$\begin{array}{l} \log \ (8D/27) \ = \ 2.191; \ \log \ \big[8(D/27)^{1/2} \big] \ = \ 1.547; \ 4(D/27)^{1/2} \ = \ 17.62; \\ \left| \ \alpha^{\prime\prime} \ - \ \alpha^{\prime} \ \right| \ ^2 \ = \ 14.10; \ \log \ \big[D^{1/2} \ \right| \ \alpha^{\prime\prime} \ - \ \alpha^{\prime} \ \big|^{-3} \big] \ = \ \overline{1}.636. \end{array}$$

Having found these numbers we can proceed to our operations. We start with triads

$$x_0 = 1$$
, $y_0 = 0$, $z_0 = 0$, $X_0 = 0$, $Y_0 = 0$, $Z_0 = 1$,

corresponding to $\Delta = 1$, and seek the next following triad.

First operation. As $\phi_0 = 1$, $\Phi_0 = 1$, $N(\phi_0) = 1$, we have

$$k = 0.057$$

and from the tables on p. 12,

$$\log \tau_{2} = \overline{1}.987; \log (k/\tau_{1}) = \overline{1}.998;$$

$$\frac{2.191}{3 \log (k/\tau_{1}) = \overline{1}.994} \frac{3 \log \tau_{2} = \overline{1}.547}{\log \Gamma = 2.185;} \frac{3 \log \tau_{2} = \overline{1}.961}{\log \Gamma_{1} = 1.508}; \Gamma = 153.1; \Gamma_{1} = 32.21;$$

$$\frac{1.508}{1.636}$$

$$\log \Delta = 2.185; \overline{1.144} = \log \Delta_{1}.$$

As $\Delta > \Delta_1$ the second triad has to be changed first. Following the indications in §7 we must find integers L, M, N satisfying the system of equations

$$N \cdot 0 - M \cdot 1 = 1;$$
 $M = -1;$
 $L \cdot 1 - N \cdot 0 = 0;$ $L = 0;$
 $M \cdot 0 - L \cdot 0 = 0;$ $N \text{ arbitrary}.$

Next we find the binary form in λ , μ

$$\omega = \lambda + \mu(N - \alpha),$$

and choose N so as to make $N-\alpha$ as small as possible. We must take N=0 and then

$$h = \omega = \lambda - \mu\alpha,$$

$$h^2 = (1, -\alpha, -4 - 2\alpha + \beta) = (1; -0.403; 0.162),$$

$$2H = 2h'h'' = (2, 2 + \alpha, 2\beta) = (2; 2.403; 9.936),$$

$$2H/\Gamma_1 = (0.062; 0.075; 0.308),$$

$$1000V = (1062, -328, 470).$$

Hence, the minimum of V is attained for $\lambda = 0$, $\mu = \pm 1$. We take $\lambda = 0$, $\mu = -1$ to make ω positive. Thus

 $\omega_1 = \alpha$

and
$$\Omega_{1} = \alpha'\alpha'' = \beta, \ N(\omega_{1}) = 2,$$

$$k = 0.114; \qquad \log \tau_{2} = \overline{1}.972;$$

$$\frac{1}{1}.636$$

$$\overline{1}.636$$

$$\overline{1}.099$$

 $\frac{\overline{1.916}}{\log \Gamma_1 = \overline{1.463}}; \ \Gamma_1 = 29.04; \ \overline{2.283} = \log \Delta_1.$

Second operation. As the new value for Δ_1 is greater than the previously found Δ , now we have to change the first triad. From the equations

$$n \cdot 0 - m \cdot 0 = 0$$
, $l \cdot 0 - n \cdot 1 = 1$, $m \cdot 1 - l \cdot 0 = 0$,

we find m = 0, n = -1, l arbitrary, and consequently

$$\phi = \lambda + (l - \beta)\mu.$$

For the sake of simplicity we shall take l=0 and then

$$\phi = g = \lambda - \beta \mu,$$

$$g^2 = (1, -\beta, 4 + 2\alpha + 4\beta) = (1; -4.968; 24.678),$$

$$N(\phi_0)g^2/\Gamma = (0.006; -0.032; 0.161),$$

$$2G = (2, -4 + \beta, 4\alpha) = (2; 0.968; 1.612),$$

$$1000T = (2006, 936, 1773).$$

Hence $\lambda = 0$, $\mu = -1$, and

$$\phi_1 = \beta; \ \Phi_1 = 2\alpha; \ N(\phi_1) = 4;$$

$$k = 0.227; \ \log(k/\tau_1) = \overline{1}.974;$$

$$\frac{2.191}{\overline{1}.922} \qquad \qquad \overline{1.719}$$

$$\log \Gamma = \overline{2.113}; \ \Gamma = 129.7; \ \overline{2.394} = \log \Delta.$$

Third operation. Now we have to change the second triad. Solving the equations

$$N \cdot 1 - M \cdot 0 = 0$$
; $L \cdot 0 - N \cdot 0 = 0$; $M \cdot 0 - L \cdot 1 = 1$,

we find L = -1, N = 0 and take M = 2. Then

$$\omega = \lambda \alpha + (4 + 2\alpha - \beta)\mu, \quad h = \lambda - \alpha \mu,$$

$$h^2 = (1; -0.403; 0.162),$$

$$2H = (4; 4.806; 19.872),$$

$$2H/\Gamma_1 = (0.138; 0.165; 0.684),$$

$$1000V = (1138, -238, 846),$$

whence $\lambda = 0$, $\mu = 1$ and

$$\omega_2 = -4 - 2\alpha + \beta$$
, $\Omega_2 = 4 + 2\alpha + 4\beta$; $N(\omega_2) = 4$; $k = 0.227$; $\log \tau_2 = \overline{1}.933$; $\frac{1}{1}.346$

$$\begin{array}{c}
\frac{1.340}{1.636} \\
\frac{1.547}{1.799} \\
\frac{1}{3.629} \\
\log \Gamma_1 = 1.346; \ \Gamma_1 = 22.18; \ 3.343 = \log \Delta_1.
\end{array}$$

Fourth operation. Now we have to change the first triad and accordingly find l, m, n from the equations

$$n \cdot 0 - m \cdot 1 = 1$$
; $l \cdot 1 - n \cdot 0 = -2$; $m \cdot 0 - l \cdot 0 = 0$.

We find l = -2, m = -1, while n remains arbitrary. Taking n = 0 we have

$$\phi = \lambda \beta - (2 + \alpha)\mu; \ g = 4\lambda + (8 - 2\beta)\mu;$$

$$G = 4(2, 2 + \beta/2, \alpha + 2\beta) = 4(2; 4.484; 10.339);$$

$$N(\phi_1)g^2 = 4(16, 32 - 8\beta, 80 + 8\alpha - 16\beta) = 4(16; -7.744; 3.736);$$

$$N(\phi_1)g^2/\Gamma = 4(0.124; -0.060; 0.029);$$

 $250T = (2124, 4424, 10368) \begin{pmatrix} 1-2\\0&1 \end{pmatrix} (2124, 176, 1168).$

Hence $\lambda = 2$, $\mu = -1$ and

$$\phi_2 = 2 + \alpha + 2\beta, \quad \Phi_2 = -4 - 2\alpha + \beta; \quad N(\phi_2) = 2;$$
 $k = 0.114; \quad \log(k/\tau_1) = \overline{1}.994;$

$$\frac{2.191}{\overline{1}.982} \qquad \qquad \frac{2.173}{\overline{3}.629}$$

$$\log \Gamma = 2.173; \quad \Gamma = 149.0; \quad 4.544 = \log \Delta.$$

Fifth operation. Again the second triad has to be changed. From

$$-2N = 2$$
, $-N = 1$, $M + 2L = 2$,

we find N = -1, M = 2 - 2L and take L = 1. Thus

$$\omega = (-4 - 2\alpha + \beta)\lambda + (-5 + \beta)\mu;$$

$$h = \lambda - \frac{1}{2}\alpha\mu;$$

$$H = (4, 4 + 2\alpha, 2\beta);$$

$$2H/\Gamma_1 = (0.181; 0.217; 0.448);$$

$$h^2 = (1; -0.202; 0.040);$$

$$1000V = (1181, 15, 448),$$

whence $\lambda = 0$, $\mu = -1$,

$$\omega_3 = 5 - \beta$$
, $\Omega_3 = 5 + 2\alpha + 5\beta$, $N(\omega_3) = 1$.

Thus ω_3 is an algebraic unit and as it is not a square of the binary unit of the form $a+b\alpha$ it must be the required fundamental unit ϵ :

$$\epsilon = 5 - \beta$$

or

$$\epsilon = 2 - \theta^2$$
, $E = 18 + 2\theta + 5\theta^2$.

13. For the last application of the method we shall find the fundamental unit in the field determined by the root of the equation

$$\theta^3 = 19$$
.

A basis of integers of this field is

$$1, \theta, \frac{1+\theta+\theta^2}{3},$$

and we obtain a suitable normal basis by taking

$$\alpha = \theta - 1, \ \beta = \frac{1 + \theta + \theta^2}{3}.$$

For this basis we have

$$f = -3$$
, $g = 3$, $k = 2$, $l = -1$,

and

$$\alpha\alpha = -3 - 3\alpha + 3\beta, \ \beta\beta = 6 + 2\alpha + \beta,$$

$$\alpha\beta = 6, \ \alpha'\alpha'' = 3\beta, \ \beta'\beta'' = 2\alpha,$$

$$\alpha' + \alpha'' = -3 - \alpha, \ \beta' + \beta'' = 1 - \beta,$$

$$\alpha'\beta'' + \alpha''\beta' = -9 - \alpha + 3\beta.$$

Moreover,

$$\alpha = 1.668; \ \beta = 3.596; \ D = 3.19^2;$$

$$4(D/27)^{1/2} = 25.33; \ \log (8D/27) = 2.506; \ \log \left[8(D/27)^{1/2} g^{-1} \right] = 1.228;$$

$$\log \left[D^{1/2} g \mid \alpha'' - \alpha' \mid ^{-3} \right] = 0.$$

Starting with $\phi_0 = 1$, $\omega_0 = 1$, we have respectively

$$k = 0.04; \ 3 \log (k/\tau_1) = \overline{1.997}$$

$$\frac{2.506}{2.503}; \ \Gamma = \Delta = 318.4;$$
 $k = 0.12; \ 3 \log \tau_2 = \overline{1.910}$

$$\frac{1.228}{1.138}; \ \Gamma_1 = \Delta_1 = 13.74.$$

First operation. We take M = -1, L = 0, N = 1, so that

$$h = \omega = \lambda + \mu(1 - \alpha/3),$$

$$2H = (2, 3 + \alpha/3, 4 + \frac{2}{3}\alpha + \frac{2}{3}\beta),$$

$$100V = (115, 70, 75) \binom{1-1}{0} (115, -45, 50).$$

Hence

$$\lambda = 1, \mu = -1; \omega_1 = \alpha/3, \Omega_1 = \beta/3, N(\omega_1) = \frac{2}{3};$$

$$k = 0.08; 3 \log \tau_2 = \overline{1.943}$$

$$\log \Gamma_1 = \frac{1.228}{\overline{1.171}}; \Gamma_1 = 14.83;$$

$$\overline{1.245}$$

$$\overline{1.926} = \log \Delta_1.$$

Second operation. Here we have N=1, L=0, M=0, and

$$\omega = \frac{1}{3}\lambda\alpha + \mu;$$

$$h = \lambda + (\beta/2)\mu; 2H = (4/3, (1-\beta)/3, 2\alpha/3);$$

$$100V = (109, 174, 331) \binom{1-2}{0} (109, -44, 71).$$

Hence $\lambda = 2$, $\mu = -1$ and

$$\omega_2 = -1 + 2\alpha/3, \ \Omega_2 = 3 + 2\alpha/3 + 4\beta/3, \ N(\omega_2) = 1;$$
 $k = 0.12; \ 3 \log \tau_2 = \overline{1.910}$
 $\frac{1.228}{1.138}; \ \Gamma_1 = 13.74;$
 $\frac{2.849}{3.987} = \log \Delta_1.$

Third operation. Now the first triad is to be changed. Here we find

l = 0, m = -1, n = -2,

$$\phi = \lambda - (\alpha + 2\beta)\mu = g;$$

$$G = (1, \frac{1}{2} + \frac{1}{2}\alpha + \beta, -18 + 6\alpha + 9\beta);$$

$$100T = (200, 983, 4899) {1 - 5 \choose 0 - 1} (200, -17, 69),$$

whence $\lambda = 5$, $\mu = -1$ and

and

$$\phi_1 = 5 + \alpha + 2\beta$$
, $\Phi_1 = 2 + \alpha - \beta$, $N(\phi_1) = 1$.

Here, for the first time, we find an algebraic unit. As ϕ_1 is not a square of a binary unit it must be the direct fundamental unit of the field. Thus

$$E = 5 + \alpha + 2\beta = \frac{1}{3}(14 + 5\theta + \theta^2),$$

$$\epsilon = 2 + \alpha - \beta = \frac{1}{3}(2 + 2\theta - \theta^2).$$

STANFORD UNIVERSITY,
STANFORD UNIVERSITY, CALIF.