Can. J. Math., Vol. XXIX, No. 1, 1977, pp. 93–106

GAINING UNITS FROM UNITS

LEON BERNSTEIN

Dedicated to James M. Vaughn, Jr.

0. Introduction. Dirichlet was the first to give an ingenious proof of the exact (finite) number of elements in the basis of the multiplicative group of units in any algebraic number field of arbitrary degree n. These elements are called *fundamental units*. If the field is real and its generating number is a real root of a polynomial over Q of degree n, having r_1 real and r_2 pairs of conjugate complex roots, so that $r_1 + 2r_2 = n$, then Dirichlet's famous result states that the exact number of fundamental units in $Q(w)$ equals $r_1 + r_2 - 1$. This was an existence proof. Since then an eloquent choice of mathematical giants have given constructive methods to solve this intriguing problem. It suffices to single out Minkowski and Landau. But already Jacobi [**13**] had been a fore-runner by generalizing the Euclidean algorithm which was most effectively used for finding fundamental units in quadratic fields. Perron [**16**] generalized the Jacobi Algorithm for algebraic number fields of degree higher than 3 (as Jacobi had done), but he did not reveal periodic algorithms out of which units can be recovered. At the end of the last century Voronoi [**22**] gave an algorithm which solves the problem of finding fundamental units in real cubic fields. This algorithm was recently generalized by Bilevich [**11**] who extended Voronoi's algorithm for real algebraic number fields of degree four claiming that it also works for fields of higher degree (this has not been verified). In previous years substantial progress in this direction has been made by many a good mathematician, and, in order to mention only a few of them (and asking forgiveness from those who are not enumerated here, a time-saving attitude which, by no means, will diminish their historic merits), Bergmann [**1**; **2**; **3**], Hasse [**4**; **5**], Mahler [**14**; **15**], Szekeres [**21**], Zassenhaus [**25**], Halter-Koch [**12**], Stender [**18**; **19**; **20**], Yamamoto [**23**], should be singled out.

1. Explicit units in functional algebraic fields. The contribution of the mathematicians mentioned in the previous section (and of those not mentioned) to the challenging problem of inventing methods, real algorithms, to find units in algebraic number fields cannot be sufficiently admired. These results are not yet completely exhausted. They may still lead to broader achievements in the following sense: their methods are applicable to fixed numerical algebraic number fields. But the obvious and main goal of number

Received March 8, 1976.

theorists will remain—to find explicit units, or, in the ultimate case, a basis of fundamental units, for functional fields, viz. for classes of infinitely many algebraic fields generated by one or more parameters. This was first achieved by Hasse and the author [**4**; **5**] by means of the Jacobi-Perron algorithm, later by the author [**10**] by means of a generalized Jacobi-Perron algorithm, and recently by Halter-Koch [**12**] and, separately by the author without using an algorithm. All the algebraic fields in question were of degree $n \geqq 3$. Stender [**18**; **19**; **20**] and the author [**7**] proved that in the cases $n = 3, 4, 6$ the units found constitute a basis of fundamental units.

For a few infinite classes of quadratic fields a few examples had been given by Perron [**17**] and recently by some other authors. In a new paper [**8**] the author has found a few new infinite classes of real quadratic number fields and stated the fundamental unit for each of them. The author used the Euclidean algorithm for simple combined periodic fractions, and the novelty of his results is that the period can be of any length, these results being entirely different from previously known almost trivial cases given by the author [**9**] and others.

Since the main result of this paper is a method of how to find units in an extension field of any degree K relative to another algebraic field $\bar{k}$, we shall summarize the explicit units for algebraic functional fields as found by the authors mentioned in this chapter.

a) Let

$$(1.1)\qquad \begin{cases} w^n = D^n + k, & n \geqq 2; D, k \in \mathbf{Z}, \\ k|D^{n-1}, & n \text{ not a prime power} \\ k|pD^{n-1}, & n = p^v \text{ a prime power.} \end{cases}$$

Then

$$(1.2)\qquad e_s = (w - D)^{-s}(w^s - D^s), \quad 1 < s|n \quad \text{are units in } Q(w).$$

b) Let

$$(1.3)\qquad \begin{cases} P(x) = (x - D_1)(x - D_2)\cdots(x - D_n) - d; \\ D_1 > D_2 > \cdots > D_n; \quad D_1 \equiv D_i(d), \quad (i = 2, \ldots, n); \\ D_1 - D_i > nd, \quad (i = 2, \ldots, n); \quad d \in \mathbf{Z}, d \neq 0. \end{cases}$$

Then

(i) $P(x)$ has exactly n different real roots;

(ii) $P(x)$ is irreducible over Q;

(iii) If w is the largest root of $P(x)$ then

$$(1.4)\qquad e_t = d^{-1}(w - D_t)^n, \quad (t = 1, \ldots, n - 1) \text{ form a maximal independent system of units in } Q(w).$$

c) Let

$$
(1.5)\quad \begin{cases} f(x) = \Pi_{j=1}^{r_1}(x - d_j)\Pi_{j=r_1+1}^{r_1+r_2}(x - z_j)(x - \bar{z}_j) - d, \\ r_1 \geqq 0, r_2 \geqq 0, n = r_1 + 2r_2 \geqq 2; d, d_j \in \mathbf{Z}, \\ d \neq 0; d_1 > d_2 > \cdots > d_{r_i}; \\ z_j \text{ integral complex quadratic, } \bar{z}_j \text{ their conjugates;} \\ d|d_i - d_j, d|d_i - z_j, d|z_i - z_j, d|z_i - \bar{z}_j \text{ for all possible } i \text{ and } j; \\ |d_i - d_j|, |d_i - z_j|, |z_i - z_j|, |z_i - \bar{z}_j| \geqq 2; \\ \text{in both cases b) and c), for } n = 3, 4 \text{ some additional restrictions} \\ \text{are necessary.} \end{cases}
$$

Then $f(x)$ has exactly r_1 different real and exactly r_2 different pair of complex roots.

$$
(1.6)\quad e_i = \begin{cases} d^{-1}(w - d_i)^n, & i \leqq i \leqq r_1 \\ d^{-2}((w - z_j)(w - \bar{z}_j)), & r_1 + 1 \leqq j \leqq r_1 + r_2 - 1 \end{cases}
$$

form a maximal independent system of units in $Q(w), f(w) = 0$.

d) (i) Let $k = 2, 3, \ldots; x, z \in \mathbf{Z}, xz \neq 0$;

$$
(1.7)\quad \begin{cases} m = z^{k+1}\left(\sum_{i=0}^{k}\left[\binom{2k-i}{i-1} + \binom{2k+1-i}{i}\right]x^{2k+1-2i}z^{k-i}\right), \\ M = z\left(\sum_{i=0}^{k}\left[\binom{2k-i}{i-1} + \binom{2k+1-i}{i}\right]x^{2k+1-2i}z^{k-i}\right)^2; \end{cases}
$$

then

$$
(1.8)\quad e = 1 + m^{(2k+1)^{-1}}x - M^{(2k+1)^{-1}}
$$

is a unit in $Q(w)$, $w^{2k+1} = m$.

(ii) Let k, x, z be as in (i); let

$$
(1.9)\quad \begin{cases} m = \sum_{i=0}^{k} (-1)^i\left[\binom{2k-1-i}{i-1} + \binom{2k-i}{i}\right]x^{2k-2i}z^{2k-i}, \\ M = \left(\sum_{i=0}^{k} (-1)^i\left[\binom{2k-1-i}{i-1} + \binom{2k-i}{i}\right](x^2z)^{k-i}\right)^2; \end{cases}
$$

then

$$
(1.10)\quad e_1 = 1 + m^{(2k)^{-1}}x + M^{(2k)^{-1}}; e_2 = 1 - m^{(2k)^{-1}}x + M^{(2k)^{-1}}
$$

are two fundamental units (a basis) in $Q(w)$, $w^{2k} = m$, $k = 2$. For $k > 2$, e_1 and e_2 form two independent units in $Q(w)$, $w^{2k} = m$, $(k = 3, 4, \ldots)$.

e) Let

$$
(1.11)\quad m = \sum_{k=0}^{n-1} \sum_{i=k}^{n-1} \binom{i}{k} a^{in}, \quad a \in \mathbf{Z}.
$$

Then

$$
(1.12)\quad e = 1 + a^n - aw, \quad w^n = m
$$

is a unit in $Q(w)$.

f) For the quadratic case we shall enumerate only a few of the cases mentioned in this chapter.

(i) Let

$$(1.13)\quad w^2 = (A^k + a + 1)^2 - A; \quad A = 2a + 1; \quad a, k > 1$$

$$(1.14)\quad e = \left(\frac{w + A^k + (a+1)}{A}\right)^{2k} \frac{(w + A^k + a)^2}{2}, \quad N(e) = 1$$

is a fundamental unit in $Q(w)$.

(ii) Let

$$(1.15)\quad \begin{cases} w^2 = (A^k + A - 1)^2 + 4A; \quad A = 2^d b \\ b \text{ odd}; db \neq 1; k \geqq 2. \end{cases}$$

Then

$$(1.16)\quad e = \left(\frac{w + A^k + A - 1}{2A}\right)^k \frac{w + A^k + A + 1}{2}; \quad N(e) = (-1)^k;$$

is a fundamental unit in $Q(w)$.

(iii) Let

$$(1.17)\quad w^2 = [2^{(d+2)k} + (2^d - 1)]^2 + 2^{d+2}, \quad d \geqq 1.$$

Then

$$(1.18)\quad e = \left(\frac{w + 2^{(d+2)k} + 2^d - 1}{2^{d+2}}\right)^k \left(\frac{w + 2^{(d+2)k} + 2^d + 1}{2}\right); \quad N(e) = (-1)^k;$$

is a fundamental unit in $Q(w)$.

2. A lemma about units. We investigate the polynomial

$$(2.1)\quad f(x) = x^k + \alpha_1 x^{k-1} + \cdots + \alpha_{n-1} x - 1$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic integers over Q; the free element could also be $+1$. For the sake of convenience, we shall presume that all $\alpha_i (i = 1, \ldots, n - 1)$ belong to the same field, but the following lemma is correct for any algebraic integers $\alpha_i (i = 1, \cdots, n - 1)$. It can be stated as follows:

LEMMA 1. *Let*

$$(2.2)\quad \begin{cases} x^k - \beta_1 x^{k-1} - \beta_2 x^{k-1} - \cdots - \beta_{k-1} x - 1 = 0; \quad k \geqq 2 \\ \beta_i = a_{i1} + a_{i2}\rho + \cdots + a_{i,n-1}\rho^{n-1}, \\ a_{i,j} \in \mathbf{Z}, \quad (i = 1, \ldots, k-1; j = 1, \ldots, n-1) \\ \rho \text{ an algebraic integer of degree } n \geqq 2. \end{cases}$$

Then x is a unit in a field of degree $m \leqq nk$ over Q.

https://doi.org/10.4153/CJM-1977-009-5 Published online by Cambridge University Press

Proof. The proof is quite obvious. From (2.1) we see that x and x^{-1} are both algebraic integers, hence x is a unit. If $f(x)$ is irreducible over $Q(\rho)$, where ρ is as in (2.2), then x is a unit in a field of degree nk over Q; otherwise x is a unit in a field of degree nd, $d|k$ over Q. The following proof is given in order to obtain a constructive method to find x in the field $Q(x, \rho)$.

We obtain from (2.2)

$$(2.3)\quad \begin{cases} x^k - 1 = P_{1k} + P_{2k}\rho + P_{3k}\rho^2 + \cdots + P_{n,k}\rho^{n-1}; \\ P_{i,k} = b_{i1}x + b_{i2}x^2 + \cdots + b_{i,k-1}x^{k-1}; \quad b_{ij} \in \mathbf{Z}; \\ (i = 1, \ldots, n; j = 1, \ldots, k-1). \end{cases}$$

We shall now find the field equation of $x^k - 1$, and introduce the polynomials of degree $k - 1$ over $\mathbf{Z}$, viz.

$$(2.4)\quad P_{ijk} = b_{ij1}x + b_{ij2}x^2 + \cdots + b_{ij,k-1}x^{k-1}$$

where $b_{ijs} \in \mathbf{Z}$; i, j, s will become self evident. We have

$$(2.5)\quad \begin{cases} x^k - 1 = P_{11k} + P_{12k}\rho + P_{13k}\rho^2 + \cdots + P_{1nk}\rho^{n-1}, \\ \rho(x^k - 1) = P_{21k} + P_{22k}\rho + P_{23k}\rho^2 + \cdots + P_{2nk}\rho^{n-1}, \\ \rho^2(x^k - 1) = P_{31k} + P_{32k}\rho + P_{33k}\rho^2 + \cdots + P_{3nk}\rho^{n-1}, \\ \cdot \\ \cdot \\ \cdot \\ \rho^{n-1}(x^k - 1) = P_{n1k} + P_{n2k}\rho + P_{n3k}\rho^2 + \cdots + P_{nnk}\rho^{n-1}. \end{cases}$$

Carrying over in (2.5) the left sides to the right, and collecting equal powers of ρ, we obtain (since the unknowns $1, \rho, \rho^2, \ldots, \rho^{n-1}$ are linearly independent) the following determinant equation:

$$(2.6)\quad \begin{vmatrix} P_{11k} - (x^k - 1) & P_{12k} & P_{13k} & \ldots & P_{1nk} \\ P_{21k} & P_{22k} - (x^k - 1) & P_{23k} & \ldots & P_{2nk} \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ P_{n1k} & P_{n2k} & P_{n3k} & \ldots & P_{nnk} - (x^k - 1) \end{vmatrix} = 0$$

We recall that the polynomials P_{ijk} are polynomials of maximum degree $k - 1$ over the rational integers without a free element, viz. $P_{ij1} = b_{ij1}x + b_{ij2}x^2 + \cdots + b_{ij,k-1}x^{k-1}$. The determinant (2.6) has therefore the form, as the reader can easily verify,

$$(x^k - 1)^n + g_1x^{kn-1} + g_2x^{kn-2} + \cdots + g_{kn-1}x = 0$$

or

$$(2.7)\quad x^{kn} + g_1x^{kn-1} + g_2x^{kn-2} + \cdots + g_{kn-1}x + (-1)^n = 0,$$
$$g_i \in \mathbf{Z},\ (i = 1, \ldots, kn - 1).$$

From (2.7) we see that x is a unit in a field of degree kn or dn, $d > 1$, $d|k$. This completes the proof.

3. An algorithm over any algebraic field. The algorithm which is described in this chapter is a new version of the algorithm first used by Jacobi [**13**] and later generalized by Perron [**16**], my admired late teacher. Both these mathematical giants worked over the field of rationals; the author [**10**] modified the Jacobi-Perron algorithm, but also remained in Q. The algorithm, used for later purposes, is a new version of the author's modified algorithm, abandoning Q.

Definition. Let $\bar{k} = Q(\rho)$ be an algebraic number field over Q of degree n; let $K = \bar{k}(w)$ be an algebraic extension of $\bar{k}$ of degree k, $K = Q(w, \rho)$, viz.

$$(3.1)\quad \begin{cases} w^k + s_1 w^{k-1} + \cdots + s_{k-1} w + s_k = 0 \\ s_i \in k,\ (i = 1, \ldots, k),\ s_i \text{ integers.} \end{cases}$$

Let

$$(3.2)\quad \begin{cases} a^{(0)} = (a_1^{(0)}, a_2^{(0)}, \ldots, a_{k-1}^{(0)}),\ a_j^{(0)} \text{ polynomials in } w \text{ with coefficients in } \bar{k},\ (j = 1, \ldots, k-1), \\ a^{(0)} \text{ a linearly independent set of the } a_j^{(0)}, \\ a_j^{(0)} = a_j^{(0)}(\rho), \quad (j = 1, \ldots, k-1). \end{cases}$$

Then the new algorithm of $a^{(0)}$ is defined by

$$(3.3)\quad \begin{cases} a^{(v+1)} = (a_1^{(v)} - b_1^{(v)})^{-1}(a_2^{(v)} - b_2^{(v)}, \ldots, a_{k-1}^{(v)} - b_{k-1}^{(v)}, 1) \\ b_j^{(v)} = a_j^{(v)}(D), \quad D \in \bar{k}, \\ j = 1, \ldots, k-1;\ v = 0, 1, \ldots . \end{cases}$$

The sequence $\langle a^{(v)} \rangle_{v=0}$ is called the *new algorithm* of $a^{(0)}$. The new algorithm is called *periodic* if there exist rationals integer $L \geqq 0$, $m \geqq 1$ such that

$$(3.4)\quad a^{(v+m)} = a^{(v)}, \quad v = L, L+1, \ldots .$$

The sequences

$$(3.5)\quad a^{(v)}, \ldots, a^{(L-1)};\quad a^{(L)}, \ldots, a^{(L+m-1)}$$

are called respectively the *preperiod* and the *period* of the periodic new algorithm. For min L, min m they are called *primitive.* If $L = 0$, the periodic new algorithm is called *purely periodic.* L and m are called respectively the *lengths* of the preperiod and period. We need numbers $A_i^{(v)}$ defined by

$$(3.6)\quad \begin{cases} A_i^{(j)} = (\delta_{ij}), \quad \delta_i \text{ is the Kronecker delta, } i, j = 0, 1, \ldots, k-1 \\ A_i^{(v+k)} = A_i^{(v)} + \sum_{t=1}^{k-1} b_t^{(v)} A_i^{(v+t)}, \quad i = 0, \ldots, k-1. \end{cases}$$

Thus the numbers $A_i^{(j)}$ are in $\bar{k}$. They are integers, if the $b_t^{(v)}$ are integers.

https://doi.org/10.4153/CJM-1977-009-5 Published online by Cambridge University Press

The reader will have no difficulty in verifying the following formulas by induction:

$$(3.7)\qquad \begin{vmatrix} A_0^{(v)} & A_0^{(v+1)} & \cdots & A_0^{(v+k-1)} \\ A_1^{(v)} & A_1^{(v+1)} & \cdots & A_1^{(v+k-1)} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ A_{k-1}^{(v)} & A_{k-1}^{(v+1)} & \cdots & A_{k-1}^{(v+k-1)} \end{vmatrix} = (-1)^{vk}$$

$$(3.8)\qquad a_i^{(0)} = \frac{A_i^{(v)} + \sum_{t=1}^{k-1} a_t^{(v)} A_i^{(v+t)}}{A_0^{(v)} + \sum_{t=1}^{k-1} a_t^{(v)} A_0^{(v+t)}};\quad (i = 1, \ldots, k-1; v = 0, 1, \ldots)$$

$$(3.9)\qquad \prod_{t=1}^{v} a_{k-1}^{(t)} = A_0^{(v)} + \sum_{t=1}^{k-1} a_t^{(v)} A_0^{(v+t)}.$$

For further purposes we need the following

LEMMA 2. *Let the new algorithm of $a^{(0)}$ be purely periodic with length of the primitive period m. Let all $b_i^{(j)}$ $(i = 1, \ldots, k-1; j = 0, 1, \ldots)$ be integers; then*

$$(3.10)\qquad e = \prod_{t=0}^{m-1} a_{k-1}^{(t)} = A_0^{(m)} + \sum_{t=1}^{k-1} a_t^{(0)} A_0^{(m+t)}$$

is a unit in $K = Q(w, \rho)$.

Proof. The second equality in (3.10) follows from (3.9) for $v = m$, since, by hypothesis of the lemma, $a_{k-1}^{(m)} = a_{k-1}^{(0)}$ and $a_t^{(m)} = a_t^{(0)}$ $(t = 1, \ldots, k-1)$. We prove that

$$(3.11)\qquad y = A_0^{(m)} + \sum_{t=1}^{k-1} a_t^{(0)} A_0^{(m+t)}$$

is a unit in $K = Q(w, \rho)$. We obtain from (3.8), for $v = m$,

$$(3.12)\qquad \begin{cases} y = A_0^{(m)} + a_1^{(0)} A_0^{(m+1)} + a_2^{(0)} A_0^{(m+2)} + \cdots + a_{k-1}^{(0)} A_0^{(m+k-1)} \\ a_1^{(0)} y = A_1^{(m)} + a_1^{(0)} A_1^{(m+1)} + a_2^{(0)} A_1^{(m+2)} + \cdots + a_{k-1}^{(0)} A_1^{(m+k-1)} \\ a_2^{(0)} y = A_2^{(m)} + a_1^{(0)} A_2^{(m+1)} + a_2^{(0)} A_2^{(m+2)} + \cdots + a_{k-1}^{(0)} A_2^{(m+k-1)} \\ \cdot \\ \cdot \\ \cdot \\ {}_{k-1}^{(0)} y = A_{k-1}^{(m)} + a_1^{(0)} A_{k-1}^{(m+1)} \\ \qquad\qquad + a_2^{(0)} A_{k-1}^{(m+2)} + \cdots + a_{k-1}^{(0)} A_{k-1}^{(m+k-1)}. \end{cases}$$

In (3.12) we carry over the left side to the right and collect equal $a_t^{(0)}$. Since $1, a_1^{(0)}, \cdots, a_{k-1}^{(0)}$ are linearly independent and nonzero, the determinant of the new homogeneous system of equations, obtained from (3.12) must vanish.

Thus

$$(3.13)\quad \begin{vmatrix} A_0^{(m)} - y & A_0^{(m+1)} & A_0^{(m+2)} & \cdots & A_0^{(m+k-1)} \\ A_1^{(m)} & A_1^{(m+1)} - y & A_1^{(m+2)} & \cdots & A_1^{(m+k-1)} \\ \cdot \\ \cdot \\ \cdot \\ A_{k-1}^{(m)} & A_{k-1}^{(m+1)} & A_{k-1}^{(m+2)} & \cdots & A_{k-1}^{(m+k-1)} - y \end{vmatrix} = 0.$$

From (3.13) we obtain

$$(3.14)\quad y^k + c_1 y^{k-1} + c_2 y^{k-2} + \cdots + c_{k-1} y + c_k = 0$$
$$c_i \in \bar{k},\ c_i \text{ integers } (i = 1, \ldots, k).$$

Since

$$|c_k| = \left\| \begin{matrix} A_0^{(m)} & A_0^{(m+1)} & \cdots & A_0^{(m+k-1)} \\ A_1^{(m)} & A_1^{(m+1)} & \cdots & A_1^{(m+k-1)} \\ \cdot \\ \cdot \\ \cdot \\ A_{k-1}^{(m)} & A_{k-1}^{(m+1)} & \cdots & A_{k-1}^{(m+k-1)} \end{matrix} \right\| = 1$$

by (3.7), Lemma 2 follows from Lemma 1.

4. Gaining units from units. In this chapter we shall elaborate the main results of this paper, viz. the finding of units in an algebraic extension field K relative to a field k. We state

THEOREM 1. *Let* $\bar{k} = Q(\rho)$, ρ *an algebraic integer of degree. Let*

$$(4.1)\quad K = \bar{k}(w), \quad K = Q(w, \rho).$$

Moreover, let

$$(4.2)\quad \begin{cases} w^k = D^k + d; & d, D \text{ integers in } \bar{k}, \\ d|D; & k \geqq 2. \end{cases}$$

Then

$$(4.3)\quad e_s = \frac{(w - D)^s}{w^s - D^s}, \quad 1 < s|k$$

are units in the algebraic number field $Q(w, \rho)$; *the degree of* $Q(w, \rho)$ *is* kn *or* tn, $t|k$.

Proof. We carry out the new algorithm of $a^{(0)}$ over the field $\bar{k}$.

$$a^{(0)} = (f_1(w), f_2(w), \ldots, f_{k-1}(w))$$
$$(4.4)\quad b_s^{(v)} = a_s^{(v)}(D); \quad (s = 1, 2, \ldots, k-1)$$
$$(4.5)\quad a_s^{(0)} = f_s(w) = \sum_{i=0}^{s} \binom{k - s - 1 + i}{i} w^{s-i} D^i.$$

https://doi.org/10.4153/CJM-1977-009-5 Published online by Cambridge University Press

The reader will easily verify the following relations:

$$(4.6)\quad f_{k-1}(w) = \sum_{t=0}^{k-1} w^{k-1-t}D^t = \frac{d}{w-D}$$

$$(4.7)\quad b_s^{(0)} = f_s(D) = \binom{k}{s}D^s$$

$$(4.8)\quad f_1(w) - f_1(D) = w - D$$

$$(4.9)\quad f_s(w) - f_s(D) = (w - D)f_{s-1}(w).$$

It is now easily verified that, carrying out the new algorithm on $a^{(0)}$, we obtain:

$$a^{(0)} = (f_1(w), f_2(w), \ldots, f_{k-1}(w))$$

$$b^{(0)} = \left(\binom{k}{1}D, \binom{k}{2}D^2, \ldots, \binom{k}{k-1}D^{k-1}\right)$$

$$a^{(1)} = (f_1(w), f_2(w), \ldots, f_{k-2}(w), d^{-1}f_{k-1}(w))$$

$$b^{(1)} = \left(\binom{k}{1}D, \binom{k}{2}D^2, \ldots, \binom{k}{k-2}D^{k-2}\ d^{-1}\binom{k}{k-1}D^{k-1}\right)$$

$$a^{(2)} = (f_1(w), f_2(w), \ldots, d^{-1}f_{k-2}(w), d^{-1}f_{k-1}(w))$$

$$b^{(2)} = \left(\binom{k}{1}D, \binom{k}{2}D^2, \ldots, d^{-1}\binom{k}{k-2}D^{k-2}, d^{-1}\binom{k}{k-1}D^{k-1}\right)$$

.
.
.

$$a_{k-1} = (d^{-1}f_1(w), d^{-1}f_2(w), \ldots, d^{-1}f_{k-1}(w))$$

$$b_{k-1} = \left(d^{-1}\binom{k}{1}D, d^{-1}\binom{k}{2}D^2, \ldots, d^{-1}\binom{k}{k-2}D^{k-2}\ d^{-1}\binom{k}{k-1}D^{k-1}\right)$$

$$a^{(k)} = (f_1(w), f_2(w), \ldots, f_{k-1}(w)).$$

Thus we have obtained

$$(4.10)\quad a^{(k)} = a^{(0)}.$$

Thus the new algorithm is purely periodic, with length of primitive period $m = k$. By (3.10) we now obtain that a unit in $K = Q(w, \rho)$ is given by

$$(4.11)\quad \prod_{t=0}^{k-1} a_{k-1}{}^{(t)} = e_{k-1}$$

$$(4.12)\quad e_{k-1} = f_{k-1}(w)(d^{-1}f_{k-1}(w))(d^{-1}f_{k-1}(w)) \ldots (d^{-1}d_{k-1}(w))$$

and from (4.12) we obtain, in virtue of (4.6)

$$(4.13)\quad e_k = \frac{d}{(w-D)^k}\cdot$$

But, from (4.2), $d = w^k - D^k$, hence

$$(4.14)\quad e_k = \frac{w^k - D^k}{(w - D)^k}.$$

The reader should note that formula (4.11) holds only if all the $b_i^{(v)}$, appearing in the new algorithm, are algebraic integers. That this is so can be read off from $b^{(0)}, b^{(1)}, b^{(2)}, \ldots, b^{(k-1)}$, since, by the hypothesis of Lemma 3, $d|D$.

We are now ready to prove (4.3). Let $s > 1$, $s|k$. The field

$$(4.15)\quad K' = Q(w^{k/s}, \rho)$$

is a subfield of $K = Q(w, \rho)$. Now

$$(4.16)\quad w^{k/s} = ((D^{k/s})^s + d)^{1/s}, \quad d|D^{k/s}.$$

Hence, by formula (4.13)

$$(4.17)\quad e_s = \frac{d}{(w^{k/s} - D^{k/s})^s}$$

is also in unit in $Q(w^{k/s}, \rho)$ hence also in $Q(w, \rho)$. We further obtain, since $d^{-1}(w - D)^k$ is a unit, the product

$$\frac{d}{(w^{k/s} - D^{k/s})^s} \cdot \frac{(w - D)^k}{d} = \frac{((w - D)^{s/k})^s}{(w^{k/s} - D^{k/s})^s}$$

in a unit, hence also

$$(4.18)\quad e_{k/s} = \frac{(w - D)^{k/s}}{w^{k/s} - D^{k/s}}$$

is a unit. This proves Theorem 1 completely.

From Theorem 1 we obtain the interesting

COROLLARY 1. *Let $\bar{k} = Q(\rho)$ be an algebraic field, ρ an n-th degree irrational. Let K be an algebraic extension of $\bar{k}$, viz.*

$$(4.19)\quad \begin{cases} K = \bar{k}(w) = Q(\rho, w); \quad w^k = D^k + \alpha, \\ D \in \bar{k}, \alpha \text{ a unit in } \bar{k}, (k = 2, 3, \ldots). \end{cases}$$

Then

$$(4.20)\quad e_s = w^s - \alpha^s, \quad s|k$$

are units in $K = Q(\rho, w)$.

Proof. Since $\alpha|D$, we have from (4.13)

$$(4.21)\quad \frac{(w - D)^k}{\alpha}$$

is a unit in $Q(\rho, w)$. But since α is a unit, $(w - D)^k$ is a unit, so $w - D$ is a unit in $K = Q(w, \rho)$, and by (4.18)

$$(4.22) \quad e_s = w^s - D^s$$

is a unit in K. To evoke the illusion of Fermat's Last Theorem, we write α^k for α and obtain

$$(4.23) \quad w^k = D^k + \alpha^k,$$

getting the units in $Q(w, \rho)$

$$e_s = w^s - D^s, \quad s|k.$$

5. More units from units. In this chapter we state a theorem without proving it. The proof follows exactly the method used in the author's paper [**4**], mentioned previously. But while there the author operated with the Jacobi–Perron algorithm or its modification over the rationals, for the proof of the theorem stated below, the new algorithm must be used operating over any algebraic field. The proof is regretfully so long that it would take at least ten more pages to carry it out, and it is also not easy to follow because of the many complicated notations that have to be introduced.

THEOREM 2. *Let ρ be an n-th degree irrational integer and $\bar{k} = Q(\rho)$. Let*

$$(5.1) \quad \begin{cases} P(x) = (x - D_1)(x - D_2) \cdots (x - D_k) - d; \\ D_i (i = 1, \ldots, k), d \in Q(\rho) \text{ integers}, d|D_i, (i = 1, \ldots, k). \\ P(x) \text{ irreducible over } Q(\rho), P(w) = 0. \end{cases}$$

Then

$$(5.2) \quad e_i = \frac{(w - D_i)^k}{d}, \quad i = 1, \ldots, k - 1$$

form a system of independent units in $K = Q(w, \rho)$. If

$$(5.3) \quad d = \alpha, \quad \alpha \text{ a unit in } Q(\rho),$$

then

$$(5.4) \quad e_i = w - D_i, \quad (i = 1, \ldots, k - 1)$$

form a system of independent units in $Q(w, \rho)$.

From Corollary 1 we deduce a very general theorem which we shall need in the sequel.

THEOREM 3. *Let*

$$(5.5) \quad \begin{cases} \rho^n = m, & m \text{ a rational, positive integer}, \\ p^n \nmid m, & p \text{ a prime}. \end{cases}$$

Let

$$(5.6) \quad w^k = m^k + \alpha, \quad \alpha \text{ a unit in } Q(\rho).$$

Then

$$(5.7) \quad e_s = w^s - m^s, \quad s|k$$

is a unit in $Q(\rho, w)$.

Proof. The proof follows from Corollary 1, putting $D = m$.

We are now ready to state a few theorems, based on Theorem 3, and on the explicit unit as enumerated in Section one.

THEOREM 4. *Let* m *have the value from* (1.7), $\rho^{2k+1} = m$; *let* e *have the value from* (1.8); *let* $\alpha = e^t$, $(t = 1, 2, \ldots)$; *let*

$$(5.8) \quad w^a = m^a + \alpha, \quad a = 2, 3, \ldots ;$$

then

$$\beta = w^s - m^s, \quad s|a$$

is a unit in $Q(\rho, w)$.

THEOREM 5. *Let* m *have the value from* (1.9); *let* e_1, e_2 *have the values from* (1.10); *let* $\alpha = e^{t_1}e^{t_2}$, $(t_1, t_2 = 1, 2, \ldots)$; *let* $\rho^{2k} = m$ *and*

$$(5.9) \quad w^a = m^a + \alpha.$$

Then

$$\beta = w^s - m^s, \quad s|a$$

is a unit in $Q(\rho, w)$.

THEOREM 6. *Let* $m = w^2$, e *have respectively the values* (1.13), (1.14); (1.15), (1.16); (1.17), (1.18). *Let*

$$(5.10) \quad \rho^a = m^a + e^t, \quad (t = 1, 2, \ldots ; a = 2, 3, \ldots).$$

Then

$$\beta = \rho^s - m^s, \quad s|a,$$

is a unit in $Q(\rho, w)$.

Concluding, we shall demonstrate the potential of our theory by a simple example which is an illustration of Theorem 3. From this example one can learn how much more complicated the fields $K(\rho, w)$ and their units become when different structures are chosen. We choose the quadratic fields $Q(\rho)$.

$$(5.11) \quad \rho^2 = D^2 + 1, \quad D \in \mathbf{Z}, \quad |D| > 1.$$

(5.12) $\alpha = \rho - D$ is a unit in $Q(\rho)$.

Let

$$(5.13) \quad w^2 = D^2 + \alpha = D(D - 1) + \rho.$$

We construct the field $Q(\rho, w)$ and obtain from (5.13)

$$(5.14)\quad \begin{aligned} &[w^2 - D(D-1)]^2 = \rho^2 = D^2 + 1, \\ &w^4 - 2D(D-1)w^2 + D^4 - 2D^3 - 1 = 0. \end{aligned}$$

(5.13) is the field equation for w. By Theorem 3, we obtain from (5.13) that

(5.15) $\beta = w - D$ is a unit in $Q(w, \rho)$.

Here the situation is simple, since D is a rational integer. But we shall show that $w - D$ is a unit in $Q(w, \rho)$. Since β is an integer, we shall show that its field equation has the free element ± 1. We obtain from (5.14), (5.15)

$$\begin{aligned} \beta &= -D + 1\cdot w + 0\ w^2 + 0\ w^3 \\ \beta w &= 0 - D\ w + 1\cdot w^2 + 0\cdot w^3 \\ \beta w^2 &= 0 + 0\ w - D\ w^2 + 1\cdot w^3 \\ \beta w^3 &= -(D^4 - 2D^3 - 1) + 0\ w + 2D(D-1)w^2 - D\ w^3 \end{aligned}$$

and the field equation of β is

$$(5.16)\quad \begin{vmatrix} -D-\beta & 1 & 0 & 0 \\ 0 & -D-\beta & 1 & 0 \\ 0 & 0 & -D-\beta & 1 \\ -(D^4-2D^3-1) & 0 & 2D(D-1) & -D-\beta \end{vmatrix} = 0$$

from which we obtain

$$\beta^4 + 4D\beta^3 + 2D(2D+1)\beta^2 + 4D(-D^2 + D + 1)\beta - 1 = 0,$$

so that β is a unit.

References

1. G. Bergmann, *Untersuchungen zur Einheitsgruppe in den total komplexen algebraischen Zahlkoerpern sechsten Grades (Ueber P) im Rahmen der "Theorie der Netze"*, Math. Ann. *161* (1965), 349–364.

2. ——— *Zur numerischen Bestimmung einer Einheitsbasis*, Math. Ann. *166* (103–105).

3. ——— *Beispiele numerischer Einheitenbestimmung*, Math. Ann. *167* (1966), 143–168.

4. H. Hasse and L. Bernstein, *An explicit formula for the units of an algebraic number field of degree n*, Pacific J. Math. *30* (1969), 293–365.

5. ——— *Einheitenberechnung mittels des Jacobi–Perronschen Algorithmus*, J. Reine Angew. Math. *218* (1965), 51–69.

6. L. Bernstein, *The modified algorithm of Jacobi–Perron*, Mem. Amer. Math. Soc. *67* (1966).

7. ——— *On units and fundamental units*, J. Reine Angew. Math. *257* (1972), 129–145.

8. ——— *Cycles and units in the period in quadratic algebraic number fields*, Pacific J. Math., in print.

9. ——— *Periodische Kettenbrueche beliebiger Periodenlaenge*, Math. Zeit. *86* (1964), 128–135.

10. ——— *Der Hasse-Bernsteinsche Einheitensatz fuer den verallgemeinerten Jacobi–Perronschen Algorithmus*, Abh. math. Seminar *43* (1975), 192–202

11. K. K. Bilevich, *On units in algebraic fields of third and fourth degree*, (Russian) Math. Sbornik *40* (82) (1956), 123–136.

12. F. Halter-Koch, *Unanbhaengige Einheitensysteme fuer eine allgemeine Klasse algebraischer Zahlkoerper*, Abh. math. Seminar *43* (1975), 85–91.

13. C. G. J. Jacobi, *Allgemeine Theorie der kettenbruchaehnlichen Algorithmen* etc., J. Reine Angew. Math. *69* (1869), 29–64.

14. K. Mahler, *Ueber die Annaeherung akgebraischer Zahlen durch periodische Algorithman*, Acta Math. *68* (1937), 109–144.

15. ——— *Periodic algorithms for algebraic number fields*, Lectures given at the Fourth Summer Research Institute of the Australian Mathematical Soc., held at the University of Sydney, January, 1964.

16. O. Perron, *Grundlagen fuer eine Theorie des Jacobischen Kettenbruchalgorithmus*, Math. Ann. *64* (1907), 1–76.

17. ——— *Die Lehre von den Kettenbruechen* (Teubner, Stuttgart, 1954).

18. H.-J. Stender, *Eine formel fuer Grundeinheiten in reinen algebraischen Zahlkoerpern dritten, vierten und secheten Grades*, J. Number Theory, in print.

19. ——— *Ueber die Grundeinheit fuer spezielle unendliche Klassen reiner kubischer Zahlkoerper*, Abh. math. Seminar *33* (1969), 203–215.

20. ——— *Grundeinheiten fuer einige unendliche Klassen biquadratischer* etc., J. Reine Angew. Math. *264* (1973), 207–220.

21. G. Szekeres, *Multidimensional continued fractions*, Annales Univ. Sc. Budapest. de Rolando Etovos Nom., Sectio Math., Vol. XIII, (1970), 113–140.

22. G. F. Voronoi, *On a generalization of continued fractions* (Russian) Doctoral Dissertation, Warsaw (1896).

23. Y. Yamomoto, *Real quadratic number fields with large fundamental Units*, Osaka J. Math. *8* (1971), 261–271.

24. H. Yokoi, *Units and class numbers of real quadratic fields*, Nagoya Math. J. *37* (1970), 61–65.

25. H. Zassenhaus, *On the units of orders*, J. Algebra *20* (1972), 368–395.

Illinois Institute of Technology,
Chicago, Illinois