SIMULTANEOUS RATIONAL APPROXIMATIONS TO ALGEBRAIC NUMBERS

BY L. G. PECK

Communicated by N. C. Ankeny, December 17, 1960

Let K be an algebraic number field of degree $n+1$ over the rationals. The conjugates $K^{(0)}, K^{(1)}, \cdots, K^{(n)}$ are arranged so that $K^{(0)}, K^{(1)}, \cdots, K^{(r)}$ are real and

$$K^{(r+s+k)} = \overline{K^{(r+k)}}, \qquad (k = 1, 2, \cdots, s).$$

Here $r+2s=n$. It will be assumed throughout that $r \geqq 0$, so that $K^{(0)}$ is real. Numbers in K are denoted by Greek letters, superscripts being used for the corresponding conjugates. We shall frequently omit the superscript $^{(0)}$; this identification of K with $K^{(0)}$ will cause no confusion. Trace and norm of elements of K are denoted by S and N, respectively.

Let $\beta_0, \cdots, \beta_n$ be elements of K which are linearly independent over the rationals. It is well known that infinitely many sets of rational integers $(q_0, q_1, \cdots, q_n)$ can be found satisfying,

$$(1) \qquad q_0 > 0, \qquad \text{g.c.d.}(q_0, q_1, \cdots, q_n) = 1,$$

and (omitting the superscript $^{(0)}$)

$$(2) \qquad \left| \frac{\beta_j}{\beta_0} - \frac{q_j}{q_0} \right| < C q_0^{-1-1/n}, \qquad (j = 1, \cdots, n),$$

with the constant $C=1$. It will be shown here how to determine all solutions of (1), (2). From this will be deduced not only the known fact that if C is too small (2) has no solutions, but also the hitherto unknown result that the sharper inequalities

$$(3) \qquad \begin{aligned} |q_0\beta_j - q_j\beta_0| &< C q_0^{-1/n}(\log q_0)^{-1/(n-1)}, \\ |q_0\beta_n - q_n\beta_0| &< C q_0^{-1/n}, \end{aligned} \qquad (j = 1, \cdots, n-1),$$

have infinitely many solutions.

This result sharpens some of the conclusions of Cassels and Swinnerton-Dyer (I), but does not furnish any further evidence for or against the conjecture of Littlewood which is considered in their paper.

A number of interesting problems can be raised in connection with (3). In one direction it can be asked whether $n-1$ of the inequalities (2) can be improved with factors which are not all the same; e.g., one might conjecture that we can find infinitely many solutions of the inequalities

$$\begin{aligned} |q_0\beta_j - q_j\beta_0| &< Cq_0^{-1/n}/f_j(q_0), \\ |q_0\beta_n - q_n\beta_0| &< Cq_0^{-1/n}, \end{aligned} \qquad (j = 1, \cdots, n-1),$$

with $f_1(q_0) \cdots f_{n-1}(q_0) = \log q_0$ and $f_j(q_0) \geqq 1$ $(j=1, \cdots, n-1)$.

A much more difficult set of problems is in the direction of the Thue-Siegel-Roth theorem, in which one tries to specify the functions f_j in such a way that the corresponding inequalities have at most a finite number of solutions. In view of Roth's theorem one might conjecture that $f_j = q_0^{-\epsilon}$ would have the indicated effect, but this is by no means obvious.

The numbers $\beta_0, \cdots, \beta_n$ form the basis of a module M. Denote by R the set of all integers ρ in K such that $\rho\beta$ is in M whenever β is in M. Clearly R is a ring. By the Dirichlet theory of units, we may find a basis $\epsilon_1, \cdots, \epsilon_{r+s}$ of the units in R. Since the only roots of unity in K are ± 1 (because $K^{(0)}$ is real) every unit ϵ in R is uniquely expressible in the form

$$\epsilon = \pm \epsilon_1^{g_1} \epsilon_2^{g_2} \cdots \epsilon_{r+s}^{g_{r+s}}. \tag{4}$$

Let $C_1 = \max_{i,j=1,\cdots,r+s} |\log|\epsilon_j^{(i)}||$. Then, for any real number T we can find integers $g_1, \cdots, g_{r+s}$ such that

$$-n^{-1}T - \frac{1}{2}C_1 \leqq \sum_{j=1}^{r+s} g_j |\log \epsilon_j^{(i)}| < -n^{-1}T + \frac{1}{2}C_1, \qquad (i = 1, \cdots, r+s),$$

and, since $N(\epsilon_j) = 1$,

$$T - \frac{n}{2}C_1 < \sum_{j=1}^{r+s} g_j |\log \epsilon_j| \leqq T + \frac{n}{2}C_1.$$

Using (4) with the sign chosen so that $\epsilon > 0$, we obtain

$$|\epsilon^{(i)}| < C_2\epsilon^{-1/n} \tag{5}$$

with a constant $C_2 = e^{C_1}$ which depends only on the ring R. A unit $\epsilon > 1$ which satisfies (5) will be called *dominant*. We have proved that for every real $T > 1$ there is a dominant unit ϵ satisfying $T \leqq \epsilon < C_2^n T$.

The elements δ of K, such that $S(\delta\beta) =$ a rational integer for every β in M, form another module D. A basis $\delta_0, \delta_1, \cdots, \delta_n$ of D is obtained by solving the equations

$$S(\beta_i\delta_j) = \begin{cases} 1, & (i = j) \\ 0, & (i \neq j) \end{cases} \qquad (i, j = 0, \cdots, n). \tag{6}$$

Because of the discreteness of D, there is, among the nonzero elements of D, one whose norm has minimal absolute value; this minimal norm will be denoted by v. Note also that if ρ is in R and δ in D then $\rho\delta$ is in D.

Choose $\delta = a_0\delta_0 + a_i\delta_i + \cdots + a_n\delta_n$ in D so that $\delta\beta_0 > 0$ and g.c.d.$(a_0, a_i, \cdots, a_n) = 1$. If ϵ is a unit in R and $\epsilon\delta = q_0\delta_0 + q_1\delta_1 + \cdots + q_n\delta_n$ we must have g.c.d.$(q_0, \cdots, q_n) = 1$. For if g.c.d.$(q_0, \cdots, q_n) = q$, it is clear that $q^{-1}\epsilon\delta$ is in D, whence $\epsilon^{-1}q^{-1}\epsilon\delta = q^{-1}\delta$ is in D and q divides g.c.d.$(a_0, \cdots, a_n) = 1$.

As defined above, we have

$$q_k = S(\epsilon\delta\beta_k), \qquad (k = 0, \cdots, n). \tag{7}$$

Thus, if we assume that ϵ is dominant, we have

$$\begin{aligned} \left| q_k\beta_0 - q_0\beta_k \right| &= \left| \sum_{j=1}^{n} (\beta_k^{(j)}\beta_0 - \beta_k\beta_0^{(j)})\delta^{(j)}\epsilon^{(j)} \right| \\ &< C_3\epsilon^{-1/n}, \qquad (k = 1, \cdots, n), \end{aligned} \tag{8}$$

while

$$\left| q_0 - \epsilon\delta\beta_0 \right| = \left| \sum_{j=1}^{n} \epsilon^{(j)}\delta^{(j)}\beta_0^{(j)} \right| < C_4\epsilon^{-1/n}.$$

The last two inequalities imply (2). The constants C_3, C_4, C depend on $a_0, \cdots, a_n$, but we may remove this dependence if the choice of δ is made from a fixed bounded region.

Suppose conversely that (1) and (2) hold (with some $C > 0$). Define $\zeta = q_0\delta_0 + \cdots + q_n\delta_n$, so that ζ is in D. We have

$$\zeta^{(i)} = \frac{1}{\beta_0}\sum_{j=1}^{n} (q_j\beta_0 - q_0\beta_j)\delta_j^{(i)} + \frac{q_0}{\beta_0}\sum_{j=0}^{n} \beta_j\delta_j^{(i)}, \qquad (i = 0, \cdots, n).$$

It follows easily from (6) that the last sum is 1 or 0 according as $i = 0$ or $i \neq 0$. Thus

$$\left| \zeta - \frac{q_0}{\beta_0} \right| - Cq_0^{-1/n} \sum_{j=1}^{n} \left| \delta_j \right|,$$

while

$$\left| \zeta^{(i)} \right| < Cq_0^{-1/n} \sum_{j=1}^{n} \left| \delta_j^{(i)} \right|, \qquad (i = 1, \cdots, n).$$

Choose a dominant unit ϵ such that $|q_0/\beta_0| \leqq \epsilon < C_2^n |q_0/\beta_0|$ and set $\delta = \pm\epsilon^{-1}\zeta$ with the sign chosen so that $\delta > 0$. Then

$$0 < \delta < 1 + C |\beta_0|^{-1} q_0^{-1-1/n} \sum_{j=1}^{n} |\delta_j|,$$

while

$$0 < |\delta^{(i)}| < C |\epsilon^{(i)}|^{-1} q_0^{-1/n} \sum_{j=1}^{n} |\delta_j^{(i)}|.$$

Thus

$$\begin{aligned} 0 < |N(\delta)| &< C^n \epsilon q_0^{-1} \prod_{i=1}^{n} \sum_{j=1}^{n} |\delta_j^{(i)}| (1 + O(q_0^{-1-1/n})) \\ &< (C\,C_2)^n C_4, \end{aligned}$$

where C_4 depends only on $\beta_0, \cdots, \beta_n$. It follows that δ is an element of D which lies in a bounded region (which will be vacuous if $C \leqq v^{1/n}/C_2 C_4^{1/n}$) and that the q_k are given by (7).

The proof of (3) is based on a special choice of δ in (7) together with a sharper form of (5) for a certain infinite set of dominant units.

To obtain the latter, let

$$\epsilon_k^{(j)} = \begin{cases} \epsilon_k^{-1/n} e^{\phi_{jk}} e_{jk}, & (j = 1, \cdots, r), \\ \epsilon_k^{-1/n} e^{\phi_{jk} + 2i\pi\psi_{jk}}, & (j = r+1, \cdots, r+s), \end{cases}$$

where ϕ_{jk} and ψ_{jk} are real and $e_{jk} = \pm 1$.

If the dominant unit ϵ is given by (4) we have

$$\left| \sum_{k=1}^{r+s} \phi_{jk} g_k \right| = \left| \log |\epsilon^{1/n} \epsilon^{(j)}| \right| < C_1, \qquad (j = 1, \cdots, r+s).$$

Also, we can find rational integers h_j such that

$$|(2\pi)^{-1} \arg \epsilon^{(j)}| = \left| \sum_{k=r+1}^{r+s} \psi_{jk} g_k + h_j \right| \leqq 1/2.$$

Now there are at least $M+1$ distinct dominant units ϵ in the interval $1 \leqq \epsilon < e^{(M+1)nC_1}$. By the well known schubfachprinzip of Dirichlet we may therefore find two—call them η and θ—such that $1 \leqq \theta < \eta < e^{(M+1)nC_1}$,

$$\left| \log |\eta^{1/n} \eta^{(j)}| - \log |\theta^{1/n} \theta^{(j)}| \right| < 2C_1/M^{1/(n-1)}, \ (j = 2, \cdots, r+s)$$

and

$$\pi^{-1} |\arg \eta^{(j)} - \arg \theta^{(j)}| \leqq M^{-1/(n-1)}, \qquad (j = r+1, \cdots, r+s).$$

Thus the unit $\epsilon=\eta/\theta$ satisfies $1<\epsilon<C_2^nT$ (where $T=e^{MnC_1}$) and

$$\begin{aligned} \left|\log\left|\epsilon^{1/n}\epsilon^{(j)}\right|\right| &< 2(C_1^n n/\log T)^{1/(n-1)}, \qquad (j=2,\cdots,r+s),\\ \left|\arg\epsilon^{(j)}\right| &\leqq 2\pi(C_1 n/\log T)^{1/(n-1)}, \qquad (j=r+1,\cdots,r+s). \end{aligned}$$

Moreover, since

$$\sum_{j=1}^{r}\log\left|\epsilon^{1/n}\epsilon^{(j)}\right| + 2\sum_{j=r+1}^{r+s}\log\left|\epsilon^{1/n}\epsilon^{(j)}\right| = 0,$$

we have also

$$\left|\log\left|\epsilon^{1/n}\epsilon^{(1)}\right|\right| < 2(n-1)(C_1^n n/\log T)^{1/(n-1)}.$$

It follows that

$$\epsilon^{(j)} = \left|\epsilon^{(j)}\right| \exp(i\arg\epsilon^{(j)}) = \epsilon^{-1/n}(1+O(\log T)^{-1/(n-1)}), \qquad (j=1,\cdots,r+s), \tag{9}$$

which is the required refinement of (5).

If we choose $\delta=\delta_n$ in (7) and make use of (6) and (9) we can improve (8) as follows:

$$\begin{aligned} \left|q_k\beta_0-q_0\beta_k\right| &= \epsilon^{-1/n}\left(\left|\sum_{j=1}^{n}(\beta_k^{(j)}\beta_0-\beta_k\beta_0^{(j)})\delta_n^{(j)}\right| + O(\log T)^{-1/(n-1)}\right)\\ &= \begin{cases} O(\epsilon^{-1/n}(\log T)^{-1(n-1)}) & (k=1,\cdots,n-1)\\ O(\epsilon^{-1/n}) & (k=n). \end{cases} \end{aligned}$$

This, together with $1<\epsilon<C_2^nT$, implies (3).

Reference

(I) J. W. S. Cassels and H. P. F. Swinnerton-Dyer, *On the product of three homogeneous linear forms and indefinite ternary quadratic forms*, Philos. Trans. Roy. Soc. London. Ser. A, vol. 248 (1955) pp. 73–96.

Boston, Massachusetts