A QUANTITATIVE VERSION OF DIRICHLET'S S-UNIT THEOREM IN ALGEBRAIC NUMBER FIELDS

L. Hajdu

To Professor L. Tamássy on his 70th birthday

1. Introduction

By Dirichlet's unit theorem the unit group of an algebraic number field is finitely generated. This theorem was later generalized for S-units (see e.g. [9]). A maximal system of multiplicatively independent units or S-units with bounded heights is often needed in the applications of Baker's theory to diophantine equations. Several results can be found in the literature (see e.g. [13] and [12] and the references given there) which provide effective upper bounds for the heights of such units. It is, however, more convenient to use systems of fundamental units with bounded heights. For ordinary units Siegel [14], and for S-units Brindza [2] derived explicit upper bounds for the heights of fundamental units. The purpose of this paper is to give another, extended version of Brindza's theorem. Thanks to its supplements (included in our Theorem), this new version seems to be even more applicable to effective investigation of diophantine problems. In the proof we combine some arguments of the papers [14], [15], [7] and [2].

2. Notation and results

Let K be an algebraic number field of degree $n \geq 2$ with discriminant D and class number h. Let M_K be the set of places on K (i.e. equivalence classes of multiplicative valuations on K). The rational number field $\mathbb{Q}$ has only one infinite place ∞, containing the ordinary absolute value, and a finite place for each prime number p. In ∞ we choose a representative $|\ .\ |_\infty$ which is equal to the ordinary absolute value. In the place corresponding to p (which is also denoted by p) we choose the valuation $|\ .\ |_p$ such that $|\ p\ |_p = p^{-1}$ as representative. In each place v of M_K we choose a valuation as follows. Let $p \in M_\mathbb{Q}$ be such that $v \mid p$ (i.e. the restrictions to $\mathbb{Q}$ of the valuations in v belong to p; in particular v is infinite if and only if $v \mid \infty$). We put $n_v = [K_v : \mathbb{Q}_p]$, where K_v and $\mathbb{Q}_p$ denote the completions of K at v and $\mathbb{Q}$ at p, respectively. In v choose the valuation $|\ .\ |_v$ satisfying

$$|\ \alpha\ |_v = |\ \alpha\ |_p^{n_v/n} \qquad \text{for each } \alpha \text{ in } \mathbb{Q}.$$

By these choices for the valuations we have the product formula

$$\prod_{v \in M_K} |\ \alpha\ |_v = 1 \quad \text{for } \alpha \in K \setminus \{0\}\ .$$

Let S_∞ be the set of all infinite places on K, and let S be a finite subset of M_K containing S_∞. Let s denote the cardinality of S, and let $v_1, \ldots, v_s$ be the elements of S. Denote by O_S and U_S the set of S-integers and S-units of K, respectively. If $\alpha \in U_S$ then we have

$$\prod_{v \in S} |\ \alpha\ |_v = 1\ .$$

Suppose that $s \geq 2$. (That is, only the case of $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, $S = S_\infty$ is excluded. In this case the unit group U_S contains roots of unity only.) For an element η of K let $\mathrm{h}(\eta)$ denote the absolute logarithmic height and $N_S(\eta)$ the S-norm of η, that is

$$h(\eta) = \log \left(\prod_{v \in M_K} \max(1, |\eta|_v) \right) ,$$

$$N_S(\eta) = \left(\prod_{v \in S} |\eta|_v \right)^n .$$

If $S = S_\infty$ then we clearly have $N_S(\eta) = |N_{K/\mathbb{Q}}(\eta)|$. (For the above definitions and notation we refer to [7] and [8].) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the prime ideals of K corresponding to the finite valuations of S. By the above-mentioned generalization of Dirichlet's unit theorem, U_S is of rank $s-1$. Let $\{\pi_1, ..., \pi_{s-1}\}$ be an arbitrary system of fundamental S-units for K. Denote by R_S the absolute value of the determinant of the matrix $(\log |\pi_i|_{v_j})_{i,j=1,\ldots,s-1}$. It is easy to verify that R_S does not depend on the choice of the system of fundamental S-units $\pi_1, ..., \pi_{s-1}$. Then with the above notation we have

Theorem. *There exists a system $\{\eta_1, \ldots, \eta_{s-1}\}$ of fundamental S-units for K such that*

$$h(\eta_1) \ldots h(\eta_{s-1}) \leq c_1 , \tag{1}$$

where

$$c_1 = 2\,(s-1)!\,(s-1)^{s-1}\,R_S ,$$

and

$$h(\eta_i) \leq c_1 \left(\frac{6n^3}{\log n} \right)^{s-2} , \quad 1 \leq i \leq s-1.$$

Further, the elements e_{ij} of the inverse of the matrix $(\log |\eta_i|_{v_j})_{i,j=1,\ldots,s-1}$ satisfy

$$|e_{ij}| \leq c_2 , \qquad i,j = 1, \ldots, s-1 \tag{2}$$

with

$$c_2 = 2^{2-s}\,(s-1)!\,(s-2)!\,\frac{6n^4}{\log n} .$$

Moreover, every S-integer α of K can be written in the form

$$\alpha = \beta\,\eta_1^{k_1} \ldots \eta_{s-1}^{k_{s-1}} , \tag{3}$$

where

$$h(\beta) < \frac{s^{\frac{5}{2}}}{2}\,c_3 + \frac{1}{n}\log N_S(\alpha) .$$

Here $k_1, \ldots, k_{s-1}$ are rational integers satisfying

$$\max_{1 \leq i \leq s-1} |k_i| < c_1\,(s-1)!\,\left(\frac{s^{\frac{5}{2}}}{2}\,c_3 + \frac{1}{n}\log N_S(\alpha) \right) (6n^4/\log n)^{s+2}\,h(\alpha) ,$$

with

$$c_3 = \frac{(s-1)\,c_1}{(\log n/6n^3)^{s-2}} .$$

Remark. Put $P = \max_{1\le j\le t}(e, \text{Norm } \mathfrak{p}_j)$. It should be observed that our estimates are independent of P.

Brindza [2] proved the estimate

$$h(\pi_1)\ldots h(\pi_{s-1}) \ < \ s!((6n^3/\log n)^n \mid D \mid \log P)^s$$

for a system of fundamental S-units $\pi_1, \ldots, \pi_{s-1}$, where the upper bound depends on D and P instead of R_S. A similar estimate can be deduced from (1) by estimating R_S from above in terms of D and P. Indeed, denote by ω the number of roots of unity in K and by r_1 and $2r_2$, respectively, the number of real and non-real embeddings of K into the field of complex numbers. Following an argument of Pethő [12] one can estimate the S-regulator R_S in the following way:

$$R_S \ \le \ \frac{4\omega}{2^{r_1+r_2}\pi^{r_2}h}\left(\frac{e}{n-1}\right)^{n-1}(h\ \log P)^{s-r_1-r_2} \mid D \mid^{\frac{1}{2}} (\log \mid D \mid)^{n-1} \ .$$

By the inequality $\omega \le 4n\log\log\,(n+7)$ (see [11]) and by an upper bound for hR_{S_∞} obtained by Siegel [14] and a lower bound for R_{S_∞} due to Zimmert [16] we get

$$R_S \ \le \ \left(300\log P \mid D \mid^{\frac{1}{2}} \left(\frac{e}{2}\ \log \mid D \mid\right)^{n-1}\right)^{s-\frac{n}{2}} \ .$$

A variant of (1) and (2) was obtained by Stark [15], but only for ordinary, multiplicatively independent units. For multiplicatively independent S-units, analogues of (3) were given by Coates [5], Evertse and Győry [7] and Pethő [12].

3. Proof

We keep the notation of Section 2. For $\eta \in K$ put

$$\overline{\mid \eta \mid}_S \ = \ \max_{1\le i\le s} \mid \eta \mid_{v_i} \ .$$

Further, for $\eta \in U_S$ write

$$L(\eta) = \max_{1\le i\le s-1} \mid \log \mid \eta \mid_{v_i} \mid \ .$$

To the proof of the Theorem we need two lemmas.

Lemma 1. *There exists a system $\{\xi_1, \ldots, \xi_{s-1}\}$ of multiplicatively independent S-units in K for which*

$$L(\xi_1)\ldots L(\xi_{s-1}) \le \ R_S \ .$$

Proof. In the special case $S = S_\infty$, Lemma 1 is proved in [13] (cf. Lemma A.13, p.22). The whole argument can trivially be adapted to the general case, and Lemma 1 follows.

Lemma 2. *Let η be an S-unit, which is not a root of unity. Then we have*

$$\frac{6n^4}{\log n}\ L(\eta) \ge \ 1 \ . \tag{4}$$

Proof. If η is an ordinary unit, then $\mid \eta \mid_{v_j} \ = \ 1$ for all finite valuations $v_j \in S$. Then

$$\log \overline{\mid \eta \mid}_S \le n\ L(\eta)$$

(see [13] p. 22), and by a result of Dobrowolski [6] we have

$$L(\eta) \geq \frac{\log n}{6n^4} \ ,$$

which implies (4). Next suppose that $|\ \eta\ |_{v_j} \neq 1$ for some finite valuation $v_j \in S$. If $|\ \eta\ |_{v_j} \leq 1$, then $|\ \eta\ |_{v_j} \leq \frac{1}{2^{1/n}}$, whence

$$-\log |\ \eta\ |_{v_j} \geq \frac{1}{n} \log 2 \ .$$

While if $|\ \eta\ |_{v_j} > 1$, then $|\ (\eta^{-1})\ |_{v_j} < 1$ and so

$$\log |\ \eta\ |_{v_j} \geq \frac{1}{n} \log 2 \ .$$

Thus we get $L(\eta) \geq \frac{1}{n} \log 2$, whence (4) follows.

Proof of the Theorem. By Lemma 1 there are multiplicatively independent S-units $\xi_1, \ \ldots, \xi_{s-1}$ for which

$$L(\xi_1) \ \ldots \ L(\xi_{s-1}) \leq \ R_S \ . \tag{5}$$

We can suppose that

$$L(\xi_1) \leq \ \ldots \ \leq L(\xi_{s-1}) \ .$$

Denote by $\mathbb{R}$ the set of real numbers. The function $L(\mathbf{x}) = \max\limits_{1 \leq i \leq s-1} |\ x_i\ |$, $\mathbf{x} \in \mathbb{R}^{s-1}$, $\mathbf{x} = (x_1, \ \ldots, x_{s-1})$, is a convex distance function on $\mathbb{R}^{s-1}$ (see the proof of Lemma 3 in [3]), hence there are $\eta_1, \ \ldots, \eta_{s-1}$ fundamental S-units with

$$L(\eta_i) \leq \ \max\ (1, \frac{i}{2})\ L(\xi_i) \ , \qquad\qquad i = 1, \ \ldots, s-1 \tag{6}$$

(cf. [4], Lemma 8, p.135 and [2]). By $h(\eta_i) \leq 2(s-1)L(\eta_i), \ i = 1, ..., s-1$, (5) and (6), we have

$$h(\eta_1) \ \ldots \ h(\eta_{s-1}) \ \leq \ 2\ (s-1)!\ (s-1)^{s-1}\ R_S \ . \tag{7}$$

For any nonzero $\eta \in O_S$ which is not a root of unity the inequality

$$h(\eta) \geq \log \overline{|\ \eta\ |}_S \geq \min\ (\frac{\log n}{6n^3}, \frac{1}{n} \log 2) \ = \ \frac{\log n}{6n^3} \tag{8}$$

holds. Together with (7) this implies

$$h(\eta_i) \leq 2\ (s-1)!\ (s-1)^{s-1}\ \left(\frac{6n^3}{\log n}\right)^{s-2}\ R_S \ , \ \ 1 \ \leq \ i \ \leq \ s-1, \tag{9}$$

and the first part of the Theorem is proved.

To the proof of (2) denote by E the matrix $(\log |\ \eta_i\ |_{v_j})_{i,j=1,\ldots,s-1}$, and by e_{ij} the elements of the inverse of E , i, j=1, . . . , s−1 . By Lemma 2 and (5), (6) we obtain

$$\prod_{\substack{i=1 \\ i \neq k}}^{s-1} L(\eta_i) \ \leq \ \frac{6n^4}{\log n}\ \frac{(s-1)!}{2^{s-2}}\ R_S \ .$$

Hence we get by Cramer's rule

$$| e_{ij} | \leq \frac{6n^4}{\log n} \, 2^{2-s} \, (s-1)! \, (s-2)! \; = \; c_2 \quad ,$$

and (2) is proved.

Now we turn to the proof of the third part of the Theorem. For a given S-integer α of K we denote by $\mathrm{V}(\alpha)$ the vector $(\log | \alpha |_v - \frac{1}{sn} \log N_S(\alpha))_{v \in S}$ (see [7]). The image of the S-units of K under this map is a lattice in the logarithmic space (see [1], Chapter 2 and [2]). The diameter of the fundamental domain of this lattice spanned by the basis $(\log | \eta_1 |_v)_{v \in S}, \ldots, (\log | \eta_{s-1} |_v)_{v \in S}$ is clearly less than

$$\sum_{j=1}^{s-1} \sqrt{\sum_{i=1}^{s} \log^2 | \eta_j |_{v_i}} \quad .$$

Then, by (8) and (9), we have

$$| \log | \eta_i |_v | \leq \; (s-1) \; \log \overline{| \eta_i |}_S \leq (s-1) \; h(\eta_i) \leq c_3$$

for $v \in S$ and $i = 1, \ldots, s-1$. Thus we have

$$\frac{1}{2} \sum_{j=1}^{s-1} \sqrt{\sum_{i=1}^{s} \log^2 | \eta_j |_{v_i}} \; \leq \; \frac{1}{2} \, c_3 \, (s-1) \, \sqrt{s} \quad .$$

Hence there are rational integers $k_1, \ldots, k_{s-1}$ with

$$| V(\alpha) - V({\eta_1}^{k_1} \ldots {\eta_{s-1}}^{k_{s-1}}) | \leq \; \frac{1}{2} \, c_3 \, (s-1) \, \sqrt{s} \quad .$$

It yields

$$h(\alpha \, {\eta_1}^{-k_1} \ldots {\eta_{s-1}}^{-k_{s-1}}) \; < \; \frac{s^{\frac{5}{2}}}{2} \, c_3 \; + \; \frac{1}{n} \log N_S(\alpha) \; .$$

To obtain a bound for $| k_i |$, i=1, . . . , s−1, put $\beta = \; \alpha \, \eta_1^{-k_1} \ldots \eta_{s-1}^{-k_{s-1}}$ and consider the following equation:

$$1 \; = \; \frac{\alpha}{\beta} \, \eta_1^{-k_1} \ldots \eta_{s-1}^{-k_{s-1}} \quad .$$

Now using a theorem of [10] and following an argument of [2], we get

$$\max_{1 \leq i \leq s-1} | k_i | \leq \; c_1 \; (s-1)! \; \omega \; (6n^4 / \log n)^{s+1} \; h(\alpha) \; h(\beta) \; .$$

Since $\omega \leq 4n \log\log \, (n+7)$, the Theorem is proved.

I would like to thank B. Brindza, K. Győry, A. Pethő and Á. Pintér for their valuable remarks.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York and London, 1966.

[2] B. Brindza, *On the generators of S-unit groups in algebraic number fields*, Bull. Austral Math. Soc. **43** (1991), 325-329.

[3] B. Brindza, *Cryptography and Number Theory*, Cambridge Univ. Press, 1990, pp. 213-220.

[4] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer-Verlag, 1959.

[5] J. Coates, *An effective p-adic analogue of a theorem of Thue II*, Acta Arith. **16** (1970), 399-412.

[6] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391-401.

[7] J. H. Evertse and K. Győry, *Thue-Mahler equations with a small number of solutions*, J. Reine Angew. Math. **399** (1989), 60-80.

[8] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *New Advances in Transcendence Theory (A. Baker ed.)*, Cambridge Univ. Press, 1988, pp. 110-174.

[9] H. Hasse, *Number Theory*, Springer-Verlag, 1980.

[10] J. H. Loxton and A. J. van der Poorten, *Multiplicative dependence in number fields*, Acta Arith. **42** (1983), 291-302.

[11] M. Mignotte and M. Waldschmidt, *Linear forms in two logarithms and Schneider's method (III)*, Ann. Fac. Sci. Toulouse **97** (1989), 43-75.

[12] A. Pethő, *Beiträge zur Theorie der S-Ordnungen*, Acta Math. Acad. Sci. Hung. **37** (1981), 51-57.

[13] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge Univ. Press, 1986.

[14] C. L. Siegel, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen **2** (1969), 71-86.

[15] H. M. Stark, *Effective estimates of solutions of some diophantine equations*, Acta Arith. **24** (1973), 250-259.

[16] H. Zimmert, *Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung*, Invent. Math. **62** (1981), 367-380.

Lajos Hajdu
Institute of Mathematics
Kossuth Lajos University
H - 4010 Debrecen
Hungary