BULL. AUSTRAL. MATH. SOC. 11S70
VOL. 43 (1991) [325–329]

ON THE GENERATORS OF S-UNIT GROUPS IN ALGEBRAIC NUMBER FIELDS

B. BRINDZA

Given a finitely generated multiplicative subgroup U_S in a number field, we employ a simple argument from the geometry of numbers and an inequality on multiplicative dependence in number fields to obtain a minimal set of generators consisting of elements of relatively small height.

1. INTRODUCTION

Let K be an algebraic number of degree n over $\mathbb{Q}$, with discriminant D, regulator R and class number h. Let r denote the rank of its group of units.

Denote by S a finite set of absolute values of K including all its archimedean (infinite) values; let s be its cardinality. An element α of K is called an S-unit if $|\alpha|_v = 1$ for every absolute value not in S. It is a well known generalisation of Dirichlet's unit theorem that the S-units of K form a finitely generated subgroup U_S of rank $s-1$ in $\mathsf{K}^{\times}$.

It turns out that wide classes of diophantine problems can be reduced to additive relations on S-units. It is therefore of interest to find effective bounds for the generators of groups U_S. Of course, it is a simple matter to construct $s-1$ multiplicatively independent elements by using the prime ideals corresponding to the nonarchimedean values in S. That yields a subgroup of finite index in U_S (see, for example [3], Lemma 4). However, the best known bounds for the "size" of the representatives of the quotient group is exponential in n and R.

In this note we construct a set of generators $\pi_1, \ldots, \pi_{s-1}$ for the non-torsion subgroup of U_S (so that its quotient with U_S is just the cyclic group of roots of unity in K).

Received 16 May 1990
Work supported by an Australian Research Council National Research Fellowship held at Macquarie University

2. The main result

As usual we denote by $h(\ )$ the absolute logarithmic height

$$h(\gamma) = \frac{1}{[\mathsf{K}:\mathsf{Q}]}\log\left(\prod_v \max(1, |\gamma|_v)\right)$$

of elements of K (with the product running over the values v of K, so normalised that one has the product formula and that rational integers h have $\mathrm{h}(h) = \log h$). Furthermore, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the prime ideals of K corresponding to the nonarchimedean (finite) values of S and set $P = \max_j(2, \operatorname{Norm}\mathfrak{p}_j)$.

Theorem. *There are S-units $\pi_1, \ldots, \pi_{s-1}$ satisfying*

$$h(\pi_1)\cdots h(\pi_{s-1}) < s!(c\,|D|\log P)^s,$$

where c is a field constant

$$c = \left(6n^3/\log n\right)^n,$$

so that each $\alpha \in U_S$ can be written as a product

$$\alpha = \rho\pi_1^{k_1}\cdots\pi_{s-1}^{k_{s-1}},$$

with ρ a root of unity and the rational integers k_i satisfying

$$\max_{1\leqslant i\leqslant s-1}|k_i| \leqslant (s!)^2c^{2s}(|D|\log P)^s h(\alpha).$$

The proof relies on a simple argument from the geometry of numbers and a result of Loxton and van der Poorten [5] on multiplicative relations in number fields.

3. Preliminary results

A real-valued function f on R^m is said to be a convex distance function if it satisfies

$$f(\mathbf{x}) \geqslant 0 \text{ for all } \mathbf{x} \in \mathsf{R}^m,$$
$$f(\lambda\mathbf{x}) = |\lambda|\,f(\mathbf{x}) \text{ for all } \lambda \in \mathsf{R} \text{ and } \mathbf{x} \in \mathsf{R}^m,$$
$$f(\mathbf{x}+\mathbf{y}) \leqslant f(\mathbf{x}) + f(\mathbf{y}) \text{ for all } \mathbf{x}, \mathbf{y} \in \mathsf{R}^m.$$

Lemma 1. *Let L be a full lattice in R^m and let f be a convex distance function on R^m. Suppose $\mathbf{x}_1, \ldots, \mathbf{x}_m$ are linearly independent elements of L. Then there is a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ for L so that for $i = 1, \ldots, m$*

$$f(\mathbf{b}_i) \leqslant \max\left(f(\mathbf{x}_i), \frac{1}{2}(f(\mathbf{x}_1) + \cdots + f(\mathbf{x}_i))\right).$$

Proof: See, for example, Lemma 8, p.235 of Cassels [1]. ∎

https://doi.org/10.1017/S0004972700029129 Published online by Cambridge University Press

REMARK. Since we may assume, without loss of generality, that $f(\mathbf{x}_1) \leqslant \cdots \leqslant f(\mathbf{x}_m)$, we obtain for $i = 1, \ldots, m$ that

$$f(\mathbf{b}_i) \leqslant \max\left(1, \frac{1}{2}i\right) f(\mathbf{x}_i).$$

Denote by ω the number of roots of unity in K. If ϕ is Euler's totient function then $\phi(\omega) \mid [\mathsf{K} : \mathsf{Q}]$ and it follows that $\omega(\mathsf{K}) < 4n \log\log 6n$. Further let $\lambda(n)$ be a positive number with the property that $h(\alpha) < \lambda(n)/n$ and α have degree at most n; then α is zero or a root of unity. Then, from a result of Dobrowolski [2], it follows readily that we may choose $\lambda(n)$ as $\log n / 6n^3$.

LEMMA 2. *Let $\alpha_1, \ldots, \alpha_k$ be nonzero elements of K with the property that there are rational integers $m_1, \ldots, m_k$ not all zero, so that*

$$\alpha_1^{m_1} \cdots \alpha_k^{m_k} = 1.$$

Then there are rational integers $q_1, \ldots, q_k$, not all zero such that

$$\alpha_1^{q_1} \cdots \alpha_k^{q_k} = 1$$

and
$$|q_l| \leqslant (k-1)!\omega \prod_{j \neq l} (n\, h(\alpha_j)/\lambda(n)) \text{ for } l = 1, \ldots, k.$$

PROOF: See Loxton and van der Poorten [5]. $\square$

4. PROOF OF THE THEOREM

Given $\alpha \in U_S$, denote by $\mathsf{v}(\alpha)$ the s-tuple $(\log|\alpha|_v)_{v \in S}$. This yields a correspondence between U_S and a full lattice in R^{s-1}, with just the roots of unity in K corresponding to the zero vector.

Now, for each $i = 1, \ldots, i = t$ let ϑ_i be the generator of the principal ideal $\mathfrak{p}_i^h$ satisfying

$$\left|\log|\text{Norm}\,\vartheta_i|^{-1/n} |\vartheta_i^{(j)}|\right| \leq \frac{1}{2} cr\, R \text{ for } j = 1, \ldots, j = n,$$

where the $\vartheta_i^{(j)}$ denote the field conjugates over Q of ϑ_i. Further, let $\{\varepsilon_1, \ldots, \varepsilon_r\}$ denote a multiplicatively independent set of (ordinary) units of K satisfying

$$h(\varepsilon_1) \cdots h(\varepsilon_r) \leqslant n^n R.$$

For the propriety of the claims inherent in these definitions, see [4].

Given an s-tuple $\mathbf{x} = (x_1, \ldots, x_s)$ we set $f(\mathbf{x}) = (1/2n)(|x_1| + \cdots + |x_s|)$. Then f is a convex distance function and, for $\alpha \in S$, the product formula in K yields

$$f(\mathbf{v}(\alpha)) = \frac{1}{2n} \sum_{v \in S} |\log |\alpha|_v| = \frac{1}{n} \sum_{v \in S} \max(0, \log |\alpha|_v)$$
$$= \frac{1}{2n} \sum_{v} \max(0, \log |\alpha|_v) = h(\alpha).$$

The elements $\varepsilon_1, \ldots, \varepsilon_r, \vartheta_1, \ldots, \vartheta_t$ are multiplicatively independent, and $s - 1 = r + t$, so their corresponding vectors are linearly independent. Then, by Lemma 1, we see that there is a set $\{\pi_1, \ldots, \pi_{s-1}\}$ of generators of U_S with

$$\begin{aligned} h(\pi_1) \cdots h(\pi_{s-1}) &= f(\mathbf{v}(\pi_1)) \cdots f(\mathbf{v}(\pi_{s-1})) \\ &\leqslant 2^{-(s-1)}(s-1)! f(\mathbf{v}(\varepsilon_1)) \cdots f(\mathbf{v}(\varepsilon_r)) f(\mathbf{v}(\vartheta_1)) \cdots f(\mathbf{v}(\vartheta_t)) \\ &= 2^{-(s-1)}(s-1)! \left(\prod_{i=1}^{r} h(\varepsilon_i) \right) \left(\prod_{j=1}^{t} h(\vartheta_j) \right), \end{aligned}$$

which establishes the first part of the theorem.

But the relation

$$\alpha = \rho \pi_1^{k_1} \cdots \pi_{s-1}^{k_{s-1}}$$

asserts that

$$1 = \alpha^{-\omega} \pi_1^{\omega k_1} \cdots \pi_{s-1}^{\omega k_{s-1}},$$

so by Lemma 2 we have rational integers $q_0, q_1, \ldots, q_{s-1}$ not all zero, such that

$$1 = \alpha^{q_0} \pi_1^{q_1} \cdots \pi_{s-1}^{q_{s-1}}$$

and

$$|q_i| \leqslant (s-1)! \omega \, \mathrm{h}(\alpha) \prod_{j \neq i} (n \, \mathrm{h}(\pi_j)/\lambda(n)).$$

Of course $q_0 \neq 0$ since the π_j are multiplicatively independent.

Moreover, the equation

$$1 = \alpha^{-\omega q_0} \pi_1^{\omega k_1 q_0} \cdots \pi_{s-1}^{\omega k_{s-1} q_0} = \alpha^{-\omega q_0} \pi_1^{-\omega q_1} \cdots \pi_{s-1}^{-\omega q_{s-1}}$$

yields

$$1 = \pi_1^{\omega k_1 q_0 + \omega q_1} \cdots \pi_{s-1}^{\omega k_{s-1} q_0 + \omega q_{s-1}},$$

whence

$$k_1 q_0 + q_1 = \cdots = k_{s-1} q_0 + q_{s-1} = 0.$$

Hence $|k_i| \leq q_i$ for $i = 1, \ldots, s-1$ which completes the proof. $\square$

5. Concluding remarks

The usual regulator argument (for example [6], p.103), already alluded to, does not yield an upper bound for the k_j because the elements $\pi_1, \ldots, \pi_{s-1}$ do not necessarily generate relatively prime ideals. Thus there does not seem to be an obvious way to use such $\mathfrak{p}$-adic relations as

$$\operatorname{ord}_{\mathfrak{p}} \alpha = \sum_{i=1}^{s-1} \operatorname{ord}_{\mathfrak{p}} \pi_i.$$

References

[1] J.W.S. Cassels, *An introduction to diophantine approximation: Cambridge Tracts in Mathematics and Mathematical Physics* 45 (Cambridge University Press, Cambridge, 1965).

[2] E. Dobrowolski, 'On a question of Lehmer and the number of irreducible factors of a polynomial', *Acta Arith.* **34**, 391–401.

[3] J.-H. Evertse and Győry, 'Thue-Mahler equations with a small number of solutions', *J. für Math.* **392** (1989), 1–21.

[4] K. Győry, 'On the solutions of linear diophantine equations in algebraic integers of bounded norm', *Ann. Univ. Sci. Budapest, Eötvös Sect. Math.* **22/23**, 225–233.

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

[6] T.N. Shorey and R. Tijdeman, *Exponential diophantine equations: Cambridge Tracts in Mathematics* 87 (Cambridge University Press, Cambridge, 1986).

Mathematics Institute
Kossuth Lájos University
H – 4010 Debrecen Pf. 12
Hungary

https://doi.org/10.1017/S0004972700029129 Published online by Cambridge University Press