Adelic Minkowski's second theorem over a division algebra

By Seiji KIMATA and Takao WATANABE

Department of Mathematics, Graduate School of Science, Osaka University,
1-16, Machikaneyama-machi, Toyonaka, Osaka 560-0043
(Communicated by Heisuke HIRONAKA, M. J. A., Dec. 12, 2000)

Abstract: We prove an analogue of Minkowski's second fundamental theorem for a vector space over a central division algebra in an adelic manner.

Key words: Minkowski's second fundamental theorem; successive minima.

0. Introduction. For a bounded o-symmetric convex body S in $\mathbf{R}^n$ with volume $V(S)$, Minkowski introduced successive minima $\lambda_1, \ldots, \lambda_n$ of S with respect to the lattice $\mathbf{Z}^n$ and proved the second fundamental theorem;

$$(1) \qquad \frac{2^n}{n!} \leq \lambda_1 \cdots \lambda_n V(S) \leq 2^n.$$

From an adelic viewpoint, this theorem was generalized first by Macfeat, and then by Bombieri and Vaaler as follows. Let k be an algebraic number field and $E = k^L$ the k-vector space. For a k-lattice M in E and a bounded o-symmetric convex body S in $E \otimes_{\mathbf{Q}} \mathbf{R}$, the successive minima $\lambda_1, \ldots, \lambda_L$ of S with respect to M is defined. Then an inequality analogous to (1) holds for $\lambda_1, \ldots, \lambda_L$ ([M, Theorem 5], [B-V, Theorems 3 and 6]).

The purpose of this paper is to generalize the Minkowski's second fundamental theorem to a vector space over a central division algebra D of an algebraic number field k. Let $E = D^L$ be a left D-vector space, Λ an order in D, M a Λ-lattice in E and S a bounded o-symmetric convex body in $E \otimes_{\mathbf{Q}} \mathbf{R}$. In Section 1, we define successive minima of S with respect to M and give an upper estimate of the product of successive minima (Theorem 1). This result is regarded as a generalization of the second fundamental theorem over the Hamilton quaternion algebra due to Weyl ([We, Theorem 1**]). As will be mentioned after Theorem 1, it is observed that this upper estimate is equivalent to the upper estimate by Macfeat and Bombieri–Vaaler. In Section 2, we will give a lower estimate of the product of successive minima (Theorem 2). This result is a strict generalization of [B-V, Theorem 6].

1991 Mathematics Subject Classification. Primary 11H06; Secondary 11R56.

1. An upper bound of successive minima. Let k be an algebraic number field, D a central division algebra of finite dimension over k and E an L-dimensional left vector space over D. A subset of D will be called an order of D if it is a subring containing 1 and a k-lattice. Let Λ be an order of D. A k-lattice of E will be called a Λ-lattice if it is a finitely generated left Λ-module.

For each place v of k, let $|\cdot|_v$ be the absolute value of the completion k_v of k at v normalized so that $|a|_v = \nu_v(aC)/\nu_v(C)$, where ν_v is a Haar measure of k_v and C is an arbitrary compact subset of k_v with nonzero measure. Let d be the degree of k over $\mathbf{Q}$, n^2 the degree of D over k. We set $D_v := D \otimes_k k_v$, $D_\infty := \prod_{v \in P_\infty} D_v$, $D_f := \prod'_{v \in P_f} D_v$ and $D_{\mathbf{A}} := D_\infty \times D_f$, where P_f (resp. P_∞) is the set of all finite (resp. infinte) places of k.

For each $v \in P_\infty$, there is an isomorphism σ_v of D_v onto $M_{m_v}(K_v)$, where if v is an unramified real (resp. a ramified real and an imaginary) place, m_v equals n (resp. $n/2$ and n) and K_v denotes $\mathbf{R}$ (resp. $\mathbf{H}$ and $\mathbf{C}$). Let $\mathbf{e}_{ij}^{(v)}$ be matrix units of $M_{m_v}(\mathbf{R})$ and $\{u_l^{(v)}\}$ the canonical basis of K_v over $\mathbf{R}$. Then $\{\mathbf{e}_{ij}^{(v)} \otimes u_l^{(v)}\}$ is a basis of $M_{m_v}(K_v)$ over $\mathbf{R}$. By this basis, $M_{m_v}(K_v)$ is identified with $\mathbf{R}^{[K_v:\mathbf{R}]n^2}$, and a Haar measure μ_v on $M_{m_v}(K_v)$ is taken as

$$\mu_v := c \prod_{i=1}^{[K_v:\mathbf{R}]n^2} dx_i,$$

where dx_i is the usual Lebesgue measure on $\mathbf{R}$ and $c = 1$ or 2^{n^2} according as v is real or imaginary. We define a Haar measure α_v on D_v as a pull-back of μ_v by σ_v and set $\alpha_\infty := \prod_{v \in P_\infty} \alpha_v$. A Haar measure α_f on D_f is taken so that the volume of $D_{\mathbf{A}}/D$ equals 1 with respect to the measure $\alpha_\infty \times \alpha_f$.

We denote by V the product measure $(\alpha_\infty \times \alpha_f)^L$ on $E_{\mathbf{A}} = (D_{\mathbf{A}})^L$.

Let Λ be an order of D and M a Λ-lattice. For $v \in P_f$, we set $M_v := \Lambda_v \otimes_\Lambda M$. For each $v \in P_\infty$, let S_v be a nonempty, open, convex, bounded and symmetric subset of E_v. Then the subset $\mathcal{S}$ of $E_{\mathbf{A}}$ is defined to be

$$\mathcal{S} := \prod_{v \in P_\infty} S_v \times \prod_{v \in P_f} M_v.$$

Definition. Let $\mathcal{S}$ be as above. For each integer l, $1 \leq l \leq L$, let

$$\lambda_l := \inf\{\lambda > 0 : (\lambda\mathcal{S}) \cap E \text{ contains } l \text{ linearly independent vectors}\},$$

where $\lambda\mathcal{S}$ denotes the set $\prod_{v\in P_\infty} \lambda S_v \times \prod_{v \in P_f} M_v$. Then $\lambda_1, \lambda_2, \ldots, \lambda_L$ will be called the successive minima for $\mathcal{S}$ with respect to the subgroup E.

Theorem 1. *Let $\mathcal{S}$ be as above. Then the successive minima $\lambda_1, \lambda_2, \ldots, \lambda_L$ satisfy the inequality*

$$(\lambda_1\lambda_2 \cdots \lambda_L)^{n^2 d} V(\mathcal{S}) \leq 2^{n^2 dL}.$$

This theorem is proved by the same way to [B-V], so we omit its proof.

Obviously, [B-V, Theorem 3] is a special case, i.e. $n = 1$, of Theorem 1. Conversely [B-V, Theorem 3] implies Theorem 1 as a consequence of the following fact;

Let $\mathcal{S}$ and $\lambda_1, \lambda_2, \ldots, \lambda_L$ be as in Theorem 1. *Regarding E as a vector space over k, one has the successive minima $\lambda'_1, \lambda'_2, \ldots, \lambda'_{n^2 L}$ for $\mathcal{S}$ in a sense of* [B-V]. *Then $\{\lambda_1, \ldots, \lambda_L\}$ is a subset of $\{\lambda'_1, \ldots, \lambda'_{n^2L}\}$ and $\lambda_i \leq \lambda'_{(i-1)n^2+1}$ holds for all i, $1 \leq i \leq L$.*

2. A lower bound of successive minima. Let v be an infinite place of k. For $x \in D_v$ we define a norm $\|x\|_v$ by

$$\|x\|_v := \mathrm{tr}({}^t\overline{\sigma_v(x)}\sigma_v(x))^{1/2}.$$

Theorem 2. *Let $\mathcal{S}$ be as in* Theorem 1. *In addition, assume that $\mathcal{S}$ satisfies the following condition*:

For each infinite place v, $xS_v \subseteq S_v$ holds for all $x \in D_v$ with $\|x\|_v = 1$.

Then the successive minima $\lambda_1, \lambda_2, \ldots, \lambda_L$ satisfy the inequality

$$\left(\frac{\{(n^2)!\sqrt{\pi}^{n^2}\}^L}{(n^2L)!\Gamma(n^2/2+1)^L}\right)^{r_1} \left(\frac{\{(2n^2)!(2\pi)^{n^2}\}^L}{(2n^2L)!\Gamma(n^2+1)^L}\right)^{r_2} \leq (\lambda_1\lambda_2\cdots\lambda_L)^{n^2d} V(\mathcal{S}) \left(\alpha_\infty(D_\infty/\Lambda)\right)^L,$$

where r_1 (resp. r_2) is the number of real (resp. imaginary) places of k.

Proof. Since M is a Λ-lattice, M contains a basis $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_L\}$ of E over D. For each λ_l, $1 \leq l \leq L$, we may associate a vector $\mathbf{u}_l$ in E such that $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_l\}$ are linearly independent over D and are contained in the set $(\lambda\mathcal{S}) \cap E$ for any $\lambda > \lambda_l$. Let $U := {}^t(\mathbf{u}_1 \ldots \mathbf{u}_L)$ be an $L \times L$ matrix. The map $\mathbf{x} \to \mathbf{x}U$ is an automorphism of $E_{\mathbf{A}}$, and by the product formula, the module of this automorphism is equal to 1, so that we have

$$V(\mathcal{S}) = V(\mathcal{S}U^{-1}).$$

The sets S_vU^{-1}, $v \in P_\infty$, and M_vU^{-1}, $v \in P_f$, have exactly the same properties as S_v and M_v. Thus the successive minima for $\mathcal{S}U^{-1}$ may be defined and are clearly equal to the successive minima $\lambda_1, \lambda_2, \ldots, \lambda_L$ for $\mathcal{S}$. Now the vectors associated with the successive minima for $\mathcal{S}U^{-1}$ may be taken as $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_L$. Thus we may assume without loss of generality that $\mathbf{u}_l = \mathbf{e}_l$ to begin with.

For each $v \in P_\infty$, we define a subset S'_v of E_v as

$$S'_v := \left\{ \mathbf{T} = \sum_{l=1}^{L} T_l\mathbf{e}_l \in E_v \,\middle|\, \sum_{l=1}^{L} \lambda_l \|T_l\|_v < 1 \right\}.$$

For $\mathbf{T} = \sum_{l=1}^L T_l\mathbf{e}_l \in S'_v - \{0\}$, there exists $c > 1$ so that $c\sum_{l=1}^L \lambda_l\|T_l\|_v = 1$. For each l whose $T_l \neq 0$, we have

$$T_l\mathbf{e}_l = c\lambda_l\|T_l\|_v \frac{T_l}{\|T_l\|_v}\left(\frac{1}{c\lambda_l}\mathbf{e}_l\right).$$

Since $(1/c\lambda_l)\mathbf{e}_l$ is contained in S_v and $T_l/\|T_l\|_v$ is an element of D_v with $\|(T_l/\|T_l\|_v)\|_v = 1$, we have

$$\frac{T_l}{\|T_l\|_v}\left(\frac{1}{c\lambda_l}\mathbf{e}_l\right) \in S_v.$$

It follows from the convexity of S_v that $\sum_{l=1}^L T_l\mathbf{e}_l$ is contained in S_v. Thus S_v contains S'_v. The volume of S'_v is given as follows: if v is real,

$$\alpha_v^L(S'_v) = \frac{1}{(\lambda_1\cdots\lambda_L)^{n^2}} \frac{((n^2)!\sqrt{\pi}^{n^2})^L}{(n^2L)!\Gamma(n^2/2+1)^L}$$

and if v is imaginary

$$\alpha_v^L(S'_v) = \frac{1}{(\lambda_1 \cdots \lambda_L)^{2n^2}} \frac{((2n^2)!(2\pi)^{n^2})^L}{(2n^2L)!\Gamma(n^2+1)^L}.$$

Let $v \in P_f$. Since Λ-lattice M contains a basis $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_L\}$ of E over D, M_v contains $(\Lambda_v)^L$, and hence

$$\alpha_f \left(\prod_{v \in P_f} \Lambda_v \right)^L \leq \alpha_f^L \left(\prod_{v \in P_f} M_v \right).$$

Since the sequence

$$0 \to \prod_{v \in P_f} \Lambda_v \to \left(D_\infty \prod_{v \in P_f} \Lambda_v \right) / \Lambda \to D_\infty / \Lambda \to 0$$

is exact and the volume of $D_{\mathbf{A}}/D = (D_\infty \prod_{v \in P_f} \Lambda_v + D)/D$ equals 1, we have

$$\alpha_\infty(D_\infty/\Lambda) = \alpha_f \left(\prod_{v \in P_f} \Lambda_v \right)^{-1}.$$

Let $\mathcal{S}' \subseteq E_{\mathbf{A}}$ be defined by

$$\mathcal{S}' := \prod_{v \in P_\infty} S'_v \times \prod_{v \in P_f} (\Lambda_v)^L.$$

Then the volume of $\mathcal{S}'$ is equal to

$$V(\mathcal{S}') = \frac{1}{(\lambda_1 \cdots \lambda_L)^{n^2 d}} \left(\frac{\{(n^2)! \sqrt{\pi}^{n^2}\}^L}{(n^2L)!\Gamma(n^2/2+1)^L} \right)^{r_1} \times \left(\frac{\{(2n^2)!(2\pi)^{n^2}\}^L}{(2n^2L)!\Gamma(n^2+1)^L} \right)^{r_2} (\alpha_\infty(D_\infty/\Lambda))^{-L}.$$

As $\mathcal{S}' \subseteq \mathcal{S}$ we have the inequality $V(\mathcal{S}') \leq V(\mathcal{S})$. □

References

[B-V] Bombieri, E., and Vaaler, J.: On Siegel's Lemma. Invent. Math., **73**, 11–32 (1983).

[M] Macfeat, R. B.: Geometry of numbers in adele spaces. Dissertations Math. (Rozprawy Mat.), vol. 138, Instytut Matematyczny Polskiej Akademii Nauk, Warszawa (1971).

[S] Siegel, C. L.: Lectures on Geometry of Numbers. Springer, Berlin-Heidelberg-New York (1989).

[W] Weil, A.: Basic Number Theory. Springer, Berlin-Heidelberg-New York (1973).

[We] Weyl, H.: Theory of reduction for arithmetical equivalence. Trans. Amer. Math. Soc., **48**, 126–164 (1940).