A SURVEY AND A COMPLEMENT OF FUNDAMENTAL HERMITE CONSTANTS

Takao Watanabe

In this note, we give an account of further development of generalized Hermite constants after [W1]. In [W5], we introduced the fundamental Hermite constant $\gamma(G, Q, k)$ of a pair (G, Q) of a connected reductive group G and a maximal parabolic subgroup Q of G both defined over a global field k. Though we use adelic language, the definition of $\gamma(G, Q, k)$ is given as a natural generalization of the definition of the original Hermite constant γ_n. It was proved in [W5], among other things, that some properties of Hermite–Rankin's constant, e.g., Rankin's inequality, can be generalized to fundamental Hermite constants. We will give a survey of these results in the first two sectons of this note. In Section 1, we recall Hermite–Rankin's constant and its generalization due to Thunder [T2]. Section 2 is a summary of our papers [W5] and [W6], in which we define the fundamental Hermite constant $\gamma(G, Q, k)$ and state properties of $\gamma(G, Q, k)$. In Example 1, we show that Thunder's generalization is none other than the fundamental Hermite constant of GL_n defined over an algebraic number field. Section 3 is a complement of properties of fundamental Hermite constants, in which we will study a behavior of fundamental Hermite constants under central k-isogenies.

1. Hermite's constant and some generalizations. Let $\mathcal{L}^n$ be the set of all lattices of rank n in the Euclidean space $\mathbb{R}^n$. For $L \in \mathcal{L}^n$, we denote by $d(L)$ the volume of the fundamental parallelepiped of L and by $m_1(L)$ the square of the length of minimal vectors in L, i.e., $m_1(L) = \min_{0 \neq x \in L} ||x||^2$. Hermite proved that the inequality

$$m_1(L) \leq \left(\frac{2}{\sqrt{3}}\right)^{n-1} d(L)^{2/n}$$

holds for all $L \in \mathcal{L}^n$. This implies $m_1(L)/d(L)^{2/n}$ is bounded on $\mathcal{L}^n$. As a consequence of the reduction theory, it is known that the function $L \mapsto m_1(L)/d(L)^{2/n}$ defined on $\mathcal{L}^n$ has the maximum:

$$\gamma_n = \max_{L \in \mathcal{L}^n} \frac{m_1(L)}{d(L)^{2/n}},$$

which is called Hermite's constant. Hermite's constant is connected with the density δ_n of the densest lattice packing of spheres in $\mathbb{R}^n$ as follows:

$$\delta_n = \gamma_n^{n/2} \frac{V(n)}{2^n},$$

where $V(n)$ denotes the volume of the unit ball in $\mathbb{R}^n$, i.e., $V(n) = \pi^{n/2}/\Gamma(1+n/2)$. By $\delta_n \leq 1$ and the mean value argument of geometry of numbers, one has an estimate of the form

$$\left(\frac{2\zeta(n)}{V(n)}\right)^{2/n} \leq \gamma_n \leq 4\left(\frac{1}{V(n)}\right)^{2/n} .$$

This upper bound was given by Minkowski. The lower bound was first stated by Minkowski and was proved by Hlawka. Korkine and Zolotareff [K-Z, §5, 5°] proved that γ_n^n is a rational number for each n.

The next step of Hermite's constant is the following extension due to Rankin. For $1 \leq d \leq n-1$, define the lattice invariant $m_d(L)$ by

$$m_d(L) = \min_{\substack{x_1,\cdots,x_d \in L \\ x_1\wedge\cdots\wedge x_d \neq 0}} \det({}^t x_i x_j)_{1\leq i,j\leq d} .$$

Then Rankin [R] defined the constant:

$$\gamma_{n,d} = \max_{L\in\mathcal{L}^n} \frac{m_d(L)}{d(L)^{2d/n}} ,$$

where the maximum of the right-hand side is attained. Obviously, $\gamma_{n,1}$ equals γ_n. Rankin proved that $\gamma_{n,d}$ satisfies the inequality

$$\gamma_{n,d} \leq \gamma_{m,d}(\gamma_{n,m})^{d/m}$$

for $1 \leq d < m \leq n-1$, and obtained $\gamma_{4,2} = 3/2$. Rankin's inequality and the duality relation $\gamma_{n,d} = \gamma_{n,n-d}$ yield Mordell's inequality $\gamma_n^{n-2} \leq \gamma_{n-1}^{n-1}$ ([Mo]).

As a generalization of Hermite–Rankin's constant, Thunder [T2] defined the constant $\gamma_{n,d}(k)$ for any algebraic number field k. We will recall Thunder's definition of $\gamma_{n,d}(k)$ in the next section (see Example 1) and express $\gamma_{n,d}(k)$ in terms of fundamental Hermite constants of GL_n defined over k. Thunder proved the following results:

(1) $\gamma_{n,d}(\mathbb{Q})$ is equal to Rankin's constant $\gamma_{n,d}$.
(2) $\gamma_{n,d}(k) = \gamma_{n,n-d}(k)$ for $1 \leq d \leq n-1$.
(3) $\gamma_{n,d}(k) \leq \gamma_{m,d}(k)(\gamma_{n,m}(k))^{d/m}$ for $1 \leq d < m \leq n-1$.
(4) $$\left(\frac{n|D_k|^{d(n-d)/2}}{\mathrm{Res}_{s=1}\zeta_k(s)} \frac{\prod_{j=n-d+1}^{n} Z_k(j)}{\prod_{j=2}^{d} Z_k(j)}\right)^{2/(n[k:\mathbb{Q}])} \leq \gamma_{n,d}(k) \leq \left(\frac{2^{r_1+r_2}|D_k|^{1/2}}{V(n)^{r_1/n}V(2n)^{r_2/n}}\right)^{2d/[k:\mathbb{Q}]} .$$

Here $Z_k(s) = (\pi^{-s/2}\Gamma(s/2))^{r_1}((2\pi)^{1-s}\Gamma(s))^{r_2}\zeta_k(s)$ denotes the zeta function of k, D_k the discriminant of k and r_1 (resp. r_2) the number of real (resp. imaginary) places of k.

We particularly write $\gamma_n(k)$ for $\gamma_{n,1}(k)$. Newman ([N, XI]) and Icaza ([I]) also considered $\gamma_n(k)$ based on Humbert's reduction theory. Tables below show the known explicit values of $\gamma_n(k)$ (cf. [BCIO], [G-L], [N]).

n	2	3	4	5	6	7	8
γ_n	$2/\sqrt{3}$	$\sqrt[3]{2}$	$\sqrt{2}$	$\sqrt[5]{8}$	$\sqrt[6]{64/3}$	$\sqrt[7]{64}$	2

d	-1	-2	-3	-7	-11	2	3	5
$\gamma_2(\mathbb{Q}(\sqrt{d}))$	$\sqrt{2}$	2	$\sqrt{6}/2$	$\sqrt{21}/3$	$\sqrt{22}/2$	$2/\sqrt{2\sqrt{6}-3}$	2	$2/\sqrt[4]{5}$

By using the Voronoi theory, Coulangeon [Co] proved that $\gamma_n(k)$ is an algebraic number for all n if the class number of k is equal to one.

2. Fundamental Hermite constants. Thunder's definition shows that $\gamma_{n,d}(k)$ is a quantity attached to the Grassmann variety of d-dimensional subspaces in k^n. This suggests that there exists an analogue of Hermite's constant for any generalized flag variety $Q\backslash G$, where G denotes a connected reductive algebraic group defined over k and Q a k-parabolic subgroup of G. We introduced such a constant in terms of a strongly k-rational representation π of G in [W1]. This constant, say γ_π^G, was named a generalized Hermite constant attached to π, because $\gamma_{n,d}(k)$ is equal to $\gamma_{\pi_d}^{GL_n}$ of the d-th exterior representation π_d of GL_n. A strongly k-rational representation is used for embedding k-rationally $Q\backslash G$ into a projective space. We note that there are infinitely many strongly k-rational representations of G if G is isotropic. In a subsequent paper [W5], we gave a more natural definition of the generalized Hermite constant of $Q\backslash G$ provided that Q is maxmal. This new definition depends only on G, Q and does not need a strongly k-rational representaton π. We write $\gamma(G, Q, k)$, or simply γ_Q, for this new constant. Two constants γ_π^G and γ_Q have a relation of the form $\gamma_\pi^G = (\gamma_Q)^{c_\pi}$, where c_π is a positive rational number depending on π. In other words, γ_Q is considered as an essential part of γ_π^G in the sense that it is independent of any embedding of $Q\backslash G$ into a projective space. In this section, we first recall the definition of γ_Q, and then we state some properties of γ_Q.

In the following, k denotes a global field, i.e., an algebraic number field or a function field of one variable over a finite field. We fix a connected reductive algebraic group G defined over k, a minimal k-parabolic subgroup P of G and a maximal standard k-parabolic subgroup Q of G. By "standard", we means Q contains P. To define notations, we take a connected k-subgroup R of G. Let $R(k)$ denote the group of k-rational points of R, $R(\mathbb{A})$ the adele group of R and $\mathbf{X}_k^*(R)$ the module of k-rational characters of R. For $a \in R(\mathbb{A})$, define the homomorphism $\vartheta_R(a)$ from $\mathbf{X}_k^*(R)$ into the group $\mathbb{R}_+$ of positive real numbers by $\vartheta_R(a)(\chi) = |\chi(a)|_{\mathbb{A}}$ for $\chi \in \mathbf{X}_k^*(R)$, where $|\cdot|_{\mathbb{A}}$ stands for the idele norm of the idele group of k. Then ϑ_R gives rise to a homomorphism from $R(\mathbb{A})$ into $\mathrm{Hom}(\mathbf{X}_k^*(R), \mathbb{R}_+)$. The kernel of ϑ_R is denoted by $R(\mathbb{A})^1$. If R is a standard k-parabolic subgroup, U_R and M_R stand for the unipotent radical and a Levi subgroup of R, respectively. If R is a minimal

k-parabolic subgroup P, we can take M_P as the centralizer of a maximal k-split torus S of G. In general, we take M_R such that $M_P \subset M_R$. The maximal central k-split torus of M_R is denoted by Z_R. We fix a good maximal compact subgroup K of $G(\mathbb{A})$.

We define the height function H_Q on $G(\mathbb{A})$. Since Q is maximal, $\mathbf{X}_k^*(M_Q/Z_G)$ is of rank one and has a generator $\widehat{\alpha}_Q$ such that $\widehat{\alpha}_Q|_S$ is contained in the closed cone generated by the simple roots with respect to (P, S) over $\mathbb{R}$. Define the map $z_Q\colon G(\mathbb{A}) \longrightarrow Z_G(\mathbb{A})M_Q(\mathbb{A})^1\backslash M_Q(\mathbb{A})$ by $z_Q(g) = Z_G(\mathbb{A})M_Q(\mathbb{A})^1 m$ if $g = umh$, $u \in U_Q(\mathbb{A}), m \in M_Q(\mathbb{A})$ and $h \in K$. This is well defined and a left $Z_G(\mathbb{A})Q(\mathbb{A})^1$-invariant. Then the function $H_Q\colon G(\mathbb{A}) \longrightarrow \mathbb{R}_+$ is defined by $H_Q(g) = |\widehat{\alpha}_Q(z_Q(g))|_{\mathbb{A}}^{-1}$ for $g \in G(\mathbb{A})$.

We set $Y_Q = Q(\mathbb{A})^1\backslash G(\mathbb{A})^1$ and $X_Q = Q(k)\backslash G(k)$. Then X_Q is regarded as a subset of Y_Q. Since $Z_G(\mathbb{A})^1 = Z_G(\mathbb{A}) \cap G(\mathbb{A})^1 \subset M_Q(\mathbb{A})^1$, z_Q maps $Y_Q = Q(\mathbb{A})^1\backslash G(\mathbb{A})^1$ to $M_Q(\mathbb{A})^1\backslash(M_Q(\mathbb{A}) \cap G(\mathbb{A})^1)$. Namely, we have the following commutative diagram:

$$\begin{array}{ccc} Y_Q & \xrightarrow{z_Q} & M_Q(\mathbb{A})^1\backslash(M_Q(\mathbb{A}) \cap G(\mathbb{A})^1) \\ \downarrow & & \downarrow \\ Z_G(\mathbb{A})Q(\mathbb{A})^1\backslash G(\mathbb{A}) & \xrightarrow{z_Q} & Z_G(\mathbb{A})M_Q(\mathbb{A})^1\backslash M_Q(\mathbb{A}) \end{array}$$

Since both vertical arrows are injective, H_Q is restricted to Y_Q. Let $B_T = \{y \in Y_Q\colon H_Q(y) \leq T\}$ for $T > 0$. We can prove the following.

Proposition. *For $T > 0$ and any $g \in G(\mathbb{A})^1$, $B_T \cap X_Q g$ is a finite subset of Y_Q. Hence, one can define the function*

$$\Gamma_Q(g) = \min\{T > 0\colon B_T \cap X_Q g \neq \emptyset\} = \min_{y \in X_Q g} H_Q(y)$$

on $G(\mathbb{A})^1$. Then the maximum

$$\gamma(G, Q, k) = \max_{g \in G(\mathbb{A})^1} \Gamma_Q(g)$$

exists.

The existence of the maximum is a result of the reduction theory due to Borel–Harich-Chandra and Harder. The constant $\gamma_Q = \gamma(G, Q, k)$ is called the fundamental Hermite constant of (G, Q) over k. An interesting thing is a similarity between the definitions of γ_n and γ_Q. Namely, γ_n is represented as

$$\gamma_n = \max_{\substack{g \in GL_n(\mathbb{R}) \\ |\det g| = 1}} \min\{T > 0\colon B_T^n \cap g\mathbb{Z}^n \neq \{0\}\},$$

where B_T^n denotes the ball of radius T with center 0 in $\mathbb{R}^n$. On the other hand, by definition,

$$\gamma_Q = \max_{g \in G(\mathbb{A})^1} \min\{T > 0\colon B_T \cap X_Q g \neq \emptyset\}.$$

Thus X_Q plays a role of the lattice $\mathbb{Z}^n$ and B_T is an analogue of the ball B_T^n. In some cases, it is more convenient to consider the constant

$$\widetilde{\gamma}(G,Q,k)=\max_{g\in G(\mathbb{A})}\min_{y\in X_Q g} H_Q(g)\,.$$

If k is an algebraic number field, then $\widetilde{\gamma}(G,Q,k)$ is always equal to $\gamma(G,Q,k)$ as the natural map $Y_Q \longrightarrow Z_G(\mathbb{A})Q(\mathbb{A})^1\backslash G(\mathbb{A})$ is bijective. The next example shows a relation between $\gamma(GL_n,Q,k)$ and $\gamma_{n,d}(k)$.

Example 1. Let $V_{n,d}(k)=\bigwedge^d k^n$ be the d-th exerior product of k^n and $V_{n,d}(\mathbb{A})=V_{n,d}(k)\otimes_k\mathbb{A}$ the adele space of $V_{n,d}(k)$. We fix a k-basis $\mathbf{e}_1,\cdots,\mathbf{e}_n$ of k^n, and identify the group of linear automorphisms of k^n with $GL_n(k)$. For $1\le d\le n-1$, $Q_d(k)$ denotes the stabilizer of the subspace spanned by $\mathbf{e}_1,\cdots,\mathbf{e}_d$ in $GL_n(k)$. A k-basis of $V_{n,d}(k)$ is formed by the elements $\mathbf{e}_I=\mathbf{e}_{i_1}\wedge\cdots\wedge\mathbf{e}_{i_d}$ with $I=\{1\le i_1<i_2<\cdots<i_d\le n\}$. Let k_v be the completion field of k at a place v and $|\cdot|_v$ the usual normalized absolute value of k_v. The local height $H_v\colon V_{n,d}(k)\otimes_k k_v\longrightarrow\mathbb{R}_+$ is defined by

$$H_v\Big(\sum_I a_I\mathbf{e}_I\Big)=\begin{cases}\left(\sum_I |a_I|_v^{2/[k_v:\mathbb{R}]}\right)^{[k_v:\mathbb{R}]/2} & (v\text{ is infinite})\\ \sup_I(|a_I|_v) & (v\text{ is finite})\end{cases}$$

Note that $|a|_v=a\overline{a}$ if $k_v=\mathbb{C}$. Then the global height $H_{n,d}\colon V_{n,d}(k)\longrightarrow\mathbb{R}_+$ is defined to be the product of all H_v, i.e.,

$$H_{n,d}(x)=\prod_v H_v(x)$$

for $x\in V_{n,d}(k)$. This is immediately extended to the subset $GL(V_{n,d}(\mathbb{A}))V_{n,d}(k)$ of the adele space $V_{n,d}(\mathbb{A})$ by

$$H_{n,d}(Ax)=\prod_v H_v(A_v x)$$

for $A=(A_v)_v\in GL(V_{n,d}(\mathbb{A}))$ and $x\in V_{n,d}(k)$. Especially, for $g\in GL_n(\mathbb{A})$ and $x_1,\cdots,x_d\in k^n$, the height $H_{n,d}(gx_1\wedge\cdots\wedge gx_d)$ of $gx_1\wedge\cdots\wedge gx_d$ is defined. Then there exists the following maximum:

$$\widehat{\gamma}_{n,d}(k)=\max_{g\in GL_n(\mathbb{A})}\min_{\substack{x_1,\cdots,x_d\in k^n\\ x_1\wedge\cdots\wedge x_d\neq 0}}\frac{H_{n,d}(gx_1\wedge\cdots\wedge gx_d)}{|\det g|_{\mathbb{A}}^{d/n}}.$$

In the case that k is an algebraic number field, Thunder's $\gamma_{n,d}(k)$ is defined by

$$\gamma_{n,d}(k)=\widehat{\gamma}_{n,d}(k)^{2/[k:\mathbb{Q}]}$$

It is immediate to see that

$$\frac{H_{n,d}(g^{-1}\mathbf{e}_1 \wedge \cdots \wedge g^{-1}\mathbf{e}_d)}{|\det g^{-1}|_{\mathbb{A}}^{d/n}} = H_{Q_d}(g)^{\gcd(d,n-d)/n}$$

for $g \in GL_n(\mathbb{A})$, and hence

$$\widehat{\gamma}_{n,d}(k) = \widetilde{\gamma}(GL_n, Q_d, k)^{\gcd(d,n-d)/n}.$$

In general, $Z_{GL_n}(\mathbb{A})GL_n(\mathbb{A})^1$ is an index finite normal subgroup of $GL_n(\mathbb{A})$, but it is not necessarily equal to $GL_n(\mathbb{A})$ if k is a function field. Let Ξ be a complete set of representatives for the cosets of $Z_{GL_n}(\mathbb{A})GL_n(\mathbb{A})^1\backslash GL_n(\mathbb{A})$. If we put

$$\begin{aligned}\widehat{\gamma}_{n,j}(k)_\xi &= \max_{g \in Z_{GL_n}(\mathbb{A})GL_n(\mathbb{A})^1\xi} \min_{\substack{x_1,\cdots,x_d \in k^n \\ x_1\wedge\cdots\wedge x_d \neq 0}} \frac{H_{n,d}(gx_1 \wedge \cdots \wedge gx_d)}{|\det g|_{\mathbb{A}}^{d/n}} \\ &= \frac{1}{|\det \xi|_{\mathbb{A}}^{d/n}} \max_{g \in GL_n(\mathbb{A})^1\xi} \min_{\substack{x_1,\cdots,x_d \in k^n \\ x_1\wedge\cdots\wedge x_d \neq 0}} H_{n,d}(gx_1 \wedge \cdots \wedge gx_d)\end{aligned}$$

for $\xi \in \Xi$, then

$$\widehat{\gamma}_{n,d}(k) = \max_{\xi \in \Xi} \gamma_{n,d}(k)_\xi,$$

and in particular, for the unit element $\xi = 1$,

$$\widehat{\gamma}_{n,d}(k)_1 = \gamma(GL_n, Q_d, k)^{\gcd(d,n-d)/n}.$$

If k is a number field, $Z_{GL_n}(\mathbb{A})GL_n(\mathbb{A})^1 = GL_n(\mathbb{A})$ holds, and hence one has

$$\widetilde{\gamma}(GL_n, Q_d, k) = \gamma(GL_n, Q_d, k) = \gamma_{n,d}(k)^{n[k:\mathbb{Q}]/(2\gcd(d,n-d))}.$$

We summarize the properties of $\gamma(G, Q, k)$.

Theorem 1. *Assume the exact sequence*

$$1 \longrightarrow Z \longrightarrow G \overset{\beta}{\longrightarrow} G' \longrightarrow 1$$

of connected reductive groups defined over k satisfies the following two conditions:

- *Z is central in G.*
- *Z is isomorphic to a product of tori of the form $R_{k'/k}(GL_1)$, where each k'/k is a finite separable extension and $R_{k'/k}$ denotes the functor of restriction of scalars from k' to k.*

Then $\gamma(G, Q, k)$ is equal to $\gamma(G', \beta(Q), k)$.

Theorem 2. *If k/ℓ is a finite separable extension, then $\gamma(R_{k/\ell}(G), R_{k/\ell}(Q), \ell)$ is equal to $\gamma(G, Q, k)$.*

Theorem 3. *Let R and Q be two different maximal standard k-parabolic subgroups of G, $Q^R = M_R \cap Q$ a maximal standard parabolic subgroup of M_R and $M_Q^R = M_R \cap M_Q$ a Levi subgroup of Q^R. We write $\widehat{\alpha}_Q^R$ for the $\mathbb{Z}$-basis $\widehat{\alpha}_{Q^R}$ of $\mathbf{X}_k^*(M_Q^R/Z_R)$. Then $\mathbb{Q}$-vector space $\mathbf{X}_k^*(M_Q^R/Z_G) \otimes_{\mathbb{Z}} \mathbb{Q}$ is spanned by $\widehat{\alpha}_Q^R$ and $\widehat{\alpha}_R|_{M_Q^R}$. If we take $\omega_1, \omega_2 \in \mathbb{Q}$ such that*

$$\widehat{\alpha}_Q|_{M_Q^R} = \omega_1 \widehat{\alpha}_Q^R + \omega_2 \widehat{\alpha}_R|_{M_Q^R} ,$$

then one has an inequality of the form

$$\gamma(G, Q, k) \leq \widetilde{\gamma}(M_R, Q^R, k)^{\omega_1} \gamma(G, R, k)^{\omega_2} .$$

Example 2. We illustrate that Theorem 1 and Theorem 3 are generalizations of the duality relation (2) and Rankin's inequality (3) in §1, respectively. We use the same notations as in Example 1. First, we consider the automorphism $\beta\colon GL_n \longrightarrow GL_n$ defined by $\beta(g) = w_0({}^t g^{-1})w_0^{-1}$, where

$$w_0 = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix} \in GL_n(k).$$

Since $\beta(Q_d) = Q_{n-d}$, Theorem 1 deduces

$$\gamma(GL_n, Q_d, k) = \gamma(GL_n, Q_{n-d}, k).$$

If k is a number field, this implies the duality relation (2). Next, for $i, j \in \mathbb{Z}$ with $1 \leq i < j \leq n-1$, we take two maximal standard k-parabolic subgroups $R = Q_j$ and $Q = Q_i$ of GL_n. Then, $M_R = GL_j \times GL_{n-j}$, $M_Q = GL_i \times GL_{n-i}$ and $M_Q^R = GL_i \times GL_{j-i} \times GL_{n-j}$. It is easy to see

$$\omega_1 = \frac{n}{j} \frac{\gcd(i, j-i)}{\gcd(i, n-i)} , \qquad \omega_2 = \frac{i}{j} \frac{\gcd(j, n-j)}{\gcd(i, n-i)} .$$

Theorem 3 deduces

$$\gamma(GL_n, Q_i, k) \leq \widetilde{\gamma}(M_{Q_j}, Q_i^{Q_j}, k)^{\frac{n}{j} \frac{\gcd(i,j-i)}{\gcd(i,n-i)}} \gamma(GL_n, Q_j, k)^{\frac{i}{j} \frac{\gcd(j,n-j)}{\gcd(i,n-i)}} .$$

If k is a number field, this and Example 1 imply Rankin's inequality (3).

Let $\tau(G)$ (resp. $\tau(Q)$) be the Tamagawa number of G (resp. Q) and $\omega_{\mathbb{A}}^G$ (resp. $\omega_{\mathbb{A}}^{U_Q}$ and $\omega_{\mathbb{A}}^{M_Q}$) the Tamagawa measure of $G(\mathbb{A})$ (resp. $U_Q(\mathbb{A})$ and $M_Q(\mathbb{A})$). The modular character

δ_Q^{-1} of $Q(\mathbb{A})$ is defined by the relation $d\omega_{\mathbb{A}}^{U_Q}(m^{-1}um) = \delta_Q(m)^{-1} d\omega_{\mathbb{A}}^{U_Q}(u)$ for $u \in U_Q(\mathbb{A})$ and $m \in M_Q(\mathbb{A})$. We define constants $\widehat{e}_Q$ and $C_{G,Q}$ as follows:

- $\delta_Q(m) = |\widehat{\alpha}_Q(m)|_{\mathbb{A}}^{\widehat{e}_Q}$ for all $m \in M(\mathbb{A})$.
- $d\omega_{\mathbb{A}}^G(g) = C_{G,Q}^{-1}\delta_Q(m)^{-1} d\omega_{\mathbb{A}}^{U_Q}(u) d\omega_{\mathbb{A}}^{M_Q}(m) d\nu_K(h)$ for all $g = umh$, $u \in U_Q(\mathbb{A})$, $m \in M_Q(\mathbb{A})$ and $h \in K$.

Here ν_K denotes the Haar measure of K normalized so that $\nu_K(K) = 1$. By an argument of the mean value theorem, we can show the following theorem.

Theorem 4. *One has an estimate of the form*

$$\left(C_{G,Q} \cdot D_{G,Q} \cdot E_Q \cdot \frac{\tau(G)}{\tau(Q)} \right)^{1/\widehat{e}_Q} \leq \gamma(G, Q, k)\,,$$

where $D_{G,Q}$ and E_Q are given as follows:

$$D_{G,Q} = \begin{cases} \dfrac{[\mathbf{X}_k^*(Z_G) : \mathbf{X}_k^*(G)]}{[\mathbf{X}_k^*(Z_Q) : \mathbf{X}_k^*(M_Q)]} & (\mathrm{ch}(k) = 0), \\ \dfrac{(\log q)^{\mathrm{rank}\,\mathbf{X}_k^*(G)}[\mathrm{Hom}(\mathbf{X}_k^*(G), q^{\mathbb{Z}}) : \mathrm{Im}\,\vartheta_G]}{(\log q)^{\mathrm{rank}\,\mathbf{X}_k^*(M_Q)}[\mathrm{Hom}(\mathbf{X}_k^*(M_Q), q^{\mathbb{Z}}) : \mathrm{Im}\,\vartheta_{M_Q}]} & (\mathrm{ch}(k) > 0), \end{cases}$$

$$E_Q = \begin{cases} \widehat{e}_Q[\mathbf{X}_k^*(Z_Q/Z_G) : \mathbf{X}_k^*(M_Q/Z_G)] & (\mathrm{ch}(k) = 0), \\ (1 - q_0^{-\widehat{e}_Q}) & (\mathrm{ch}(k) > 0). \end{cases}$$

Here, if $\mathrm{ch}(k) > 0$, then q denotes the cardinality of the constant field of k and $q_0 > 1$ the generator of the subgroup $|\widehat{\alpha}_Q(M_Q(\mathbb{A}) \cap G(\mathbb{A})^1)|_{\mathbb{A}}$ of the cyclic group $q^{\mathbb{Z}}$ generated by q. Moreover, this inequality is strict if $\mathrm{ch}(k) > 0$.

We note that $\gamma(G, Q, k) \in q_0^{\mathbb{Z}}$ if $\mathrm{ch}(k) > 0$.

Example 3. Let $G = GL_n$ and $Q = Q_d$. If $\mathrm{ch}(k) = 0$, Theorem 4 is essentially the same as the lower bound of (4) in §1. If $\mathrm{ch}(k) > 0$, we obtain $q_0 = q^{n/\gcd(d,n-d)}$ and

$$\left(\frac{q^{(g(k)-1)(d(n-d)+1)}(q-1)(1-q^{-n})}{h_k} \frac{\prod_{i=n-d+1}^{n} \zeta_k(i)}{\prod_{i=2}^{d} \zeta_k(i)} \right)^{1/\gcd(d,n-d)} < \gamma(GL_n, Q_d, k)\,,$$

where $g(k)$ denotes the genus of k, h_k the divisor class number of k and $\zeta_k(s)$ the congruence zeta function of k. On the other hand, from the definition of $\widehat{\gamma}_{n,d}(k)$ and Thunder's theorem on an analogue of Minkowski's second convex bodies theorem ([T1]), it follows that

$$1 \leq \gamma(GL_n, Q_d, k) \leq \widetilde{\gamma}(GL_n, Q_d, k) \leq q^{ndg(k)/\gcd(d,n-d)} = q_0^{dg(k)}\,.$$

If $g(k) = 0$, i.e., k is a rational function field over $\mathbb{F}_q$, this implies $\gamma(GL_n, Q_d, k) = \widetilde{\gamma}(GL_n, Q_d, k) = 1$. If $g(k) = 1$ and $d = 1$, the first inequality and the upper bound of the second inequality give

$$q^{n-1} \cdot \frac{(q-1)(q^{2n} + a_1 q^n + q)}{(q + a_1 + 1)(q^{2n} - q^{n+1})} < \gamma(GL_n, Q_1, k) \le \widetilde{\gamma}(GL_n, Q_1, k) \le q^n \,,$$

where $h_k = a_1 + q + 1$. Combining this with the Hasse–Weil bound $|a_1| \le 2\sqrt{q}$, we have $\gamma(GL_n, Q_1, k) = \widetilde{\gamma}(GL_n, Q_1, k) = q^n$ provided that $h_k \le q - 1$.

Except for the case where G is either an inner form of a general linear group or an orthogonal group defined over an algebraic number field ([W2], [W3]), we have no any result on an upper bound of $\gamma(G, Q, k)$.

Theorems 1 – 4 and Example 3 were proved in [W5]. Furthermore, we can add a small result on $\widetilde{\gamma}(GL_n, Q_1, k)$.

Theorem 5. *We define the constant Δ_k as follows:*

$$\Delta_k = \begin{cases} |D_k| & (k \text{ is an algebraic number field of absolute discriminant } D_k). \\ q^{2g(k)-2} & (k \text{ is a function field of genus } g(k) \text{ and constant field } \mathbb{F}_q). \end{cases}$$

If ℓ is a separable extension of k with degree r, then

$$\frac{\widetilde{\gamma}(GL_n, Q_1, \ell)}{\Delta_\ell^{n/2}} \le r^{-nrs_k/2} \cdot \frac{\widetilde{\gamma}(GL_{nr}, Q_1, k)}{\Delta_k^{nr/2}} \,,$$

where s_k denotes the number of infinite places of k.

This theorem was first proved in [O-W] in the case of $k = \mathbb{Q}$. See [W6] for a genral case.

Remark. By definition, $\gamma(G, Q, k)$ measures the existence of rational points in B_T. Namely, if $T \ge \gamma(G, Q, k)$, then $B_T \cap X_Q g \ne \emptyset$ for any $g \in G(\mathbb{A})^1$, especially $g = e$. If k is an algebraic number field, the cardinality of $B_T \cap X_Q g$ is increasing in proportion to the volume of B_T as $T \to \infty$. More precisely, one has

$$\lim_{T \to \infty} \frac{\sharp(B_T \cap X_Q g)}{\omega_Y(B_T)} = \frac{\tau(Q)}{\tau(G)}$$

for all $g \in G(\mathbb{A})^1$, where $\omega_Y = \omega_{\mathbb{A}}^Q \backslash \omega_{\mathbb{A}}^G$ is the Tamagawa measure on Y. The volume $\omega_Y(B_T)$ is equal to $(C_{G,Q} D_{G,Q} E_Q)^{-1} T^{\widehat{e}_Q}$. See [W4] for details.

3. Behavior of fundamental Hermite constants under isogenies. Theorem 1 asserts that the fundamental Hermite constants is invariant under some kind of central extensions. It is natural to ask how the fundamental Hermite constatns behaves under central isogenies. We show the following.

Theorem 6. *Let*

$$1 \longrightarrow F \longrightarrow \widehat{G} \xrightarrow{\ \beta\ } G \longrightarrow 1$$

be a separable central k-isogeny of a connected reductive k-group G and Q a maximal k-parabolic subgroup of G. Then

$$\gamma(\widehat{G}, \widehat{Q}, k)^{d_\beta} \leq \gamma(G, Q, k)\,,$$

where $\widehat{Q} = \beta^{-1}(Q)$ and $d_\beta = [\mathbf{X}_k^*(M_{\widehat{Q}}/Z_{\widehat{G}}) : \mathbf{X}_k^*(M_Q/Z_G)]$.

Proof. We note that $X_{\widehat{Q}} = \widehat{Q}(k)\backslash\widehat{G}(k)$ is isomorphic with $X_Q = Q(k)\backslash G(k)$ as F is central in G. Since $\mathbf{X}_k^*(F)$ is a torsion group, β gives rise to an isomorphism between $\mathrm{Hom}(\mathbf{X}_k^*(\widehat{G}), \mathbb{R}_+)$ and $\mathrm{Hom}(\mathbf{X}_k^*(G), \mathbb{R}_+)$. This implies that $\beta(\widehat{G}(\mathbb{A})^1)$ is contained in $G(\mathbb{A})^1$. By the similar reason, $\beta(\widehat{Q}(\mathbb{A})^1)$ is contained in $Q(\mathbb{A})^1$. Therefore, one has the following commutative diagram:

$$\begin{array}{ccc} X_{\widehat{Q}} & \xrightarrow[\cong]{\ \beta\ } & X_Q \\ \big\downarrow & & \big\downarrow \\ Y_{\widehat{Q}} & \xrightarrow{\ \beta\ } & Y_Q \end{array}$$

The central isogeny

$$1 \longrightarrow F/F \cap Z_{\widehat{G}} \longrightarrow M_{\widehat{Q}}/Z_{\widehat{G}} \xrightarrow{\ \beta\ } M_Q/Z_G \longrightarrow 1$$

yields the exact sequence

$$1 \longrightarrow \mathbf{X}_k^*(M_Q/Z_G) \xrightarrow{\ \beta^*\ } \mathbf{X}_k^*(M_{\widehat{Q}}/Z_{\widehat{G}}) \longrightarrow \mathbf{X}_k^*(F/F \cap Z_{\widehat{G}}).$$

Since $\mathbf{X}_k^*(M_Q/Z_G) = \mathbb{Z}\widehat{\alpha}_Q$ and $\mathbf{X}_k^*(M_{\widehat{Q}}/Z_{\widehat{G}}) = \mathbb{Z}\widehat{\alpha}_{\widehat{Q}}$ by definition, $\beta^*(\widehat{\alpha}_Q)$ is equal to $d_\beta\widehat{\alpha}_{\widehat{Q}}$. Moreover, by definition of the map z_Q, it is easy to see that the following diagram is commutative:

$$\begin{array}{ccc} \widehat{G}(\mathbb{A}) & \xrightarrow{\ z_{\widehat{Q}}\ } & Z_{\widehat{G}}(\mathbb{A})M_{\widehat{Q}}(\mathbb{A})^1\backslash M_{\widehat{Q}}(\mathbb{A}) \\ {\scriptstyle\beta}\big\downarrow & & \big\downarrow{\scriptstyle\beta} \\ G(\mathbb{A}) & \xrightarrow{\ z_Q\ } & Z_G(\mathbb{A})M_Q(\mathbb{A})^1\backslash M_Q(\mathbb{A}) \end{array}$$

Then, for any $g \in \widehat{G}(\mathbb{A})$, one has

$$H_Q(\beta(g)) = |\widehat{\alpha}_Q(z_Q(\beta(g)))|_{\mathbb{A}}^{-1} = |\widehat{\alpha}_Q(\beta(z_{\widehat{Q}}(g)))|_{\mathbb{A}}^{-1} = |\widehat{\alpha}_{\widehat{Q}}(z_{\widehat{Q}}(g))|_{\mathbb{A}}^{-d_\beta} = H_{\widehat{Q}}(g)^{d_\beta}.$$

From $\beta(\widehat{G}(\mathbb{A})^1) \subset G(\mathbb{A})^1$ and $X_{\widehat{Q}} \cong X_Q$, it follows that

$$\max_{g \in G(\mathbb{A})^1} \min_{x \in X_Q} H_Q(xg) \geq \max_{g \in \widehat{G}(\mathbb{A})^1} \min_{x \in X_{\widehat{Q}}} H_Q(\beta(xg)) = \max_{g \in \widehat{G}(\mathbb{A})^1} \min_{x \in X_{\widehat{Q}}} H_{\widehat{Q}}(xg)^{d_\beta}.$$

This leads us to $\gamma(G, Q, k) \geq \gamma(\widehat{G}, \widehat{Q}, k)^{d_\beta}$. □

If k is an algebraic number field, we have a more precise result. In the following, we assume G is an almost simple isotropic group and

$$1 \longrightarrow F \longrightarrow \widetilde{G} \xrightarrow{\ \beta\ } G \longrightarrow 1$$

is the simply connected covering of G defined over an algebraic number field k. We put

$$G(\mathbb{A}_\infty) = \prod_{\substack{w \\ \text{infinite}}} G(k_v) \times \prod_{\substack{v \\ \text{finite}}} K_v\,,$$

where K_v denotes the v-component of the fixed good maximal compact subgroup K of $G(\mathbb{A})$. It is known that $G(k)G(\mathbb{A}_\infty)$ is a normal subgroup of $G(\mathbb{A})$ and $G(k)G(\mathbb{A}_\infty)\backslash G(\mathbb{A}) = G(k)\backslash G(\mathbb{A})/G(\mathbb{A}_\infty)$ is a finite set ([P-R, Proposition 8.8]). Let Ξ_G be a complete set of representatives of $G(k)G(\mathbb{A}_\infty)\backslash G(\mathbb{A})$. For each $\xi \in \Xi_G$, we set

$$\gamma(G, Q, k)_\xi = \max_{g \in G(k)G(\mathbb{A}_\infty)\xi} \min_{x \in X_Q g} H_Q(x)\,,$$

and especially

$$\gamma(G, Q, k)_{\mathrm{pr}} = \max_{g \in G(k)G(\mathbb{A}_\infty)} \min_{x \in X_Q g} H_Q(x)\,.$$

From $G(\mathbb{A}) = G(\mathbb{A})^1$, it follows that

$$\gamma(G, Q, k) = \max_{\xi \in \Xi_G} \gamma(G, Q, k)_\xi\,.$$

Theorem 7. *Being the notations and assumptions as above, we have*

$$\gamma(\widetilde{G}, \widetilde{Q}, k)^{d_\beta} = \gamma(G, Q, k)_{\mathrm{pr}}\,,$$

where $\widetilde{Q} = \beta^{-1}(Q)$ *and* $d_\beta = [\mathbf{X}_k^*(M_{\widetilde{Q}}) : \mathbf{X}_k^*(M_Q)]$.

Proof. Since $\Gamma_Q(g) = \min_{x \in X_Q} H_Q(xg)$ is left $G(k)$-invariant and right K-invariant, it is sufficient to prove that $G(k)\beta(\widetilde{G}(\mathbb{A}))K = G(k)G(\mathbb{A}_\infty)$. By the proof of [P-R, Proposition 8.8], one has $[G(\mathbb{A}) : G(\mathbb{A})] \subset \beta(\widetilde{G}(\mathbb{A})) \subset G(k)G(\mathbb{A}_\infty)$. This implies $G(k)\beta(\widetilde{G}(\mathbb{A}))K \subset G(k)G(\mathbb{A}_\infty)$. To prove the converse, we must show $G(k_w) \subset \beta(\widetilde{G}(k_w))K_w$ for any infinite place w. This is obvious if $k_w = \mathbb{C}$. Thus we assume $K_w = \mathbb{R}$. Since $\widetilde{G}(\mathbb{R})$ is connected as a real Lie group ([B-T, (4.7)]), $\beta(\widetilde{G}(\mathbb{R}))$ coincides with the topologically connected component $G(\mathbb{R})^0$ of $G(\mathbb{R})$. Then $G(\mathbb{R}) = G(\mathbb{R})^0 K_w$ follows from the maximality of K_w (cf. [P-R, Proposition 3.10]). □

In general, if $\beta_1 \colon G_1 \longrightarrow G$ is a central finite covering of G, we have $G(k)G(\mathbb{A}_\infty) \subset G(k)\beta(G_1(\mathbb{A}))K \subset G(\mathbb{A})$. Therefore, there exists a subset Ξ_{G,G_1} of Ξ_G such that

$$\gamma(G_1, Q_1, k)^{d_{\beta_1}} = \max_{\xi \in \Xi_{G,G_1}} \gamma(G, Q, k)_\xi \,,$$

where $Q_1 = \beta_1^{-1}(Q)$ and $d_{\beta_1} = [\mathbf{X}_k^*(M_{Q_1}) : \mathbf{X}_k^*(M_Q)]$.

As a corollary of Theorems 1 and 7, we obtain the following.

Corollary. *If k is an algebraic number field and Q_d the maximal parabolic subgroup of GL_n given as in Example 1, then*

$$\gamma(SL_n, Q_d \cap SL_n, k)^{n/\gcd(d,n-d)} = \gamma(PGL_n, Z_{GL_n}\backslash Q_d, k)_{\mathrm{pr}}$$

In particular, if the ideal class group $I_k = k^\times \mathbb{A}_\infty^\times \backslash \mathbb{A}^\times$ of k satisfies $I_k = I_k^n$, then

$$\gamma(SL_n, Q_d \cap SL_n, k)^{n/\gcd(d,n-d)} = \gamma(PGL_n, Z_{GL_n}\backslash Q_d, k) = \gamma(GL_n, Q_d, k).$$

References

[BCIO] R. Baeza, R. Coulangeon, M. I. Icaza and M. O'Ryan, *Hermite's constant for quadratic number fields*, Experimental Math. **10** (2001), 543 - 551.

[B-I] R. Baeza and M. I. Icaza, *On Humbert–Minkowski's constant for a number field*, Proc. Amer. Math. Soc. **125** (1997), 3195 - 3202.

[B-T] A. Borel and J. Tits, *Compléments à l'article: Groupes réductifs*, Publ. Math. Inst. Hautes Etud. Sci. **41** (1972), 253 - 276.

[C] H. Cohn, *A numerical survey of the floors of various Hilbert fundamental domains*, Math. Comp. **21** (1965), 594 - 605.

[Co] R. Coulangeon, *Voronoï theory over algebraic number fields*, Réseaux Euclidiens, Designs Sphériques et Formes Modulaires (J. Martinet, ed.), L'Enseignement Math., 2001, pp. 147 - 162.

[G-L] P. M. Gruber and C. G. Lekkerkerker, *Geometry of Numbers, 2nd ed.*, North-Holland, 1987.

[I] M. I. Icaza, *Hermite constant and extreme forms for algebraic number fields*, J. London Math. Soc. **55** (1997), 11 - 22.

[K-Z] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. **6** (1873), 366 - 389.

[Mo] L. J. Mordell, *Observation on the minimum of a positive quadratic form in eight variables*, London Math. Soc. **19** (1944), 1 - 6.

[N] M. Newman, *Integral Matrices*, Academic Press, 1972.

[P-R] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, 1994.

[R] R. A. Rankin, *On positive definite quadratic forms*, J. London Math. Soc. **28** (1953), 309 - 319.

[O-W] S. Ohno and T. Watanabe, *Estimates of Hermite constants for algebraic number fields*, Comm. Math. Uni. Sancti Pauli **50** (2001), 53 - 63.

[T1] J. L. Thunder, *An adelic Minkowski-Hlawka theorem and an application to Siegel's lemma*, J. reine angew. Math. **475** (1996), 167 - 185.

[T2] ———, *Higher dimensional analogues of Hermite's constant*, Michigan Math. J. **45** (1998), 301 - 314.

[W1] T. Watanabe, *On an analog of Hermite's constant*, J. Lie Theory **10** (2000), 33 - 52.

[W2] ———, *Upper bounds of Hermite constants for orthogonal groups*, Comm. Math. Uni. Sancti Pauli **48** (1999), 25 - 33.

[W3] ———, *Hermite constants of division algebras*, Monatshefte für Math. **135** (2002), 157 - 166.

[W4] ———, *The Hardy–Littlewood property of flag varieties* (to appear in Nagoya Math. J.).

[W5] ———, *Fundamental Hermite constants of linear algebraic groups* (to appear in J. Japan Math. Soc.).

[W6] ———, *Estimates of Hermite constants for algebraic number fields II*, preprint.

Department of Mathematics, Graduate School of Science, Osaka University, Toyonaka, Osaka, 560-0043 Japan

E-mail address: `watanabe@math.wani.osaka-u.ac.jp`