Trends in Mathematics - New Series
Information Center for Mathematical Sciences
Volume 11, Number 2, 2009, pages 95–108

ASARC Workshop
Daecheon & Muju 2009

NORMAL BASES OF RAY CLASS FIELDS OVER IMAGINARY QUADRATIC FIELDS

HO YUN JUNG, JA KYUNG KOO, AND DONG HWA SHIN

Abstract. We first develop a criterion to determine normal bases (Theorem 2.4), and by making use of necessary lemmas which were refined from [3] we further prove that singular values of certain Siegel functions form normal bases of ray class fields over all imaginary quadratic fields other than $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ (Theorem 4.5 and Remark 4.6). This result would be an answer for the Lang-Schertz conjecture ([7] p. 292 or [13] p. 386) on a ray class field with any modulus generated by an integer ≥ 2 (Remark 4.7).

1. Introduction

Let L be a finite Galois extension of a field K. Then from the normal basis theorem ([17]) we know that there exists a normal basis of L over K, namely a basis of the form $\{x^\gamma : \gamma \in \mathrm{Gal}(L/K)\}$ for a single element $x \in L$.

Okada ([9]) showed that if $k \geq 1$ and $q > 2$ are integers with k odd and T is a set of representatives for which $(\mathbb{Z}/q\mathbb{Z})^\times = T \cup (-T)$, then the real numbers $\left(\frac{1}{\pi}\frac{d}{dz}\right)^k(\cot \pi z)|_{z=a/q}$ for $a \in T$ form a normal basis of the maximal real subfield of $\mathbb{Q}(e^{2\pi i/q})$ over $\mathbb{Q}$. Replacing the cotangent function by the Weierstrass $\wp$-function with fundamental period i and 1, he further obtained in [10] normal bases of class fields over the Gauss' number field $\mathbb{Q}(\sqrt{-1})$. This result was due to the fact that the Gauss' number field has class number 1, which can be naturally extended to any imaginary quadratic field with class number 1.

After Okada, Taylor ([16]) and Schertz ([12]) established Galois module structures of rings of integers of certain abelian extensions over an imaginary quadratic

2000 *Mathematics Subject Classification.* 11F11, 11F20, 11R37, 11Y40.
Key words and phrases. class fields, modular forms and functions, normal bases.
This research was supported by Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (2009-0063182).

field, which are analogues to the cyclotomic case ([8]). They also found normal bases by special values of modular functions. And, Komatsu ([4]) considered certain abelian extensions L and K of $\mathbb{Q}(e^{2\pi i/5})$ and constructed a normal basis of L over K by special values of Siegel modular functions.

In this paper we shall present normal bases of ray class fields over all imaginary quadratic fields ($\neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$) in terms of singular values of certain Siegel functions (Theorem 4.5 and Remark 4.6) by applying a criterion for determining normal bases which will be developed in Section 2.

More precisely, for any pair $(r_1,\ r_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ we define a *Siegel function* $g_{(r_1,\ r_2)}(\tau)$ on $\mathfrak{H}$ (the complex upper half-plane) by the following infinite product expansion

$$g_{(r_1,\ r_2)}(\tau) = -q_\tau^{\frac{1}{2}\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)}(1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}) \tag{1.1}$$

where $\mathbf{B}_2(X) = X^2 - X + \frac{1}{6}$ is the second Bernoulli polynomial, $q_\tau = e^{2\pi i\tau}$ and $q_z = e^{2\pi i z}$ with $z = r_1\tau + r_2$. Then it is a modular unit in the sense of [6].

Let $K \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field of discriminant d_K and $\mathcal{O}_K = \mathbb{Z}[\theta]$ be its ring of integers with

$$\theta = \begin{cases} \frac{\sqrt{d_K}}{2} & \text{for } d_K \equiv 0 \pmod 4 \\ \frac{-1+\sqrt{d_K}}{2} & \text{for } d_K \equiv 1 \pmod 4). \end{cases}$$

In what follows we denote the Hilbert class field and the ray class field modulo N of K for a positive integer N by H and $K_{(N)}$, respectively. We showed in [3] that for $N \geq 2$ the singular value $x = g_{(0,\ \frac{1}{N})}^{\frac{-12N}{\gcd(6,\ N)}}(\theta)$ is a primitive generator of $K_{(N)}$ over K except possibly finitely many cases. We achieved this result by showing that the absolute value of x is the smallest one among all its conjugates.

In this article, however, we will prove that if $N \geq 2$, then the conjugates of a high power of x form a normal basis of $K_{(N)}$ over K by applying Theorem 2.4 and Lemmas 4.2 $\sim$ 4.4. And, as for the action of $\mathrm{Gal}(K_{(N)}/K)$ on x in the process we adopt the idea of Stevenhagen-Gee ([15], [2]) which will be summarized in Section 3. This fact is also related to the Lang-Schertz conjecture on the Siegel-Ramachandra invariant to construct ray class fields $K_{(N)}$.

2. A criterion to determine normal bases

In this section let L be a finite abelian extension of a number field K with $G = \mathrm{Gal}(L/K) = \{\gamma_1 = \mathrm{id}, \cdots, \gamma_n\}$. Further we let $|\cdot|$ be the usual absolute value defined on $\mathbb{C}$.

Lemma 2.1. *A set of elements* $\{x_1, \cdots, x_n\}$ *in* L *is a* K*-basis of* L *if and only if*

$$\det\left(x_i^{\gamma_j^{-1}}\right)_{1\le i,\ j\le n} \neq 0.$$

Proof. Straightforward. □

By $\widehat{G}$ we mean the character group of G. Then we have the *Frobenius determinant relation*:

Lemma 2.2. *If* f *is any* $\mathbb{C}$*-valued function on* G*, then*

$$\prod_{\chi\in\widehat{G}} \sum_{1\le i\le n} \chi(\gamma_i^{-1}) f(\gamma_i) = \det\left(f(\gamma_i\gamma_j^{-1})\right)_{1\le i,\ j\le n}.$$

Proof. See [7] Chapter 21 Theorem 5. □

Combining Lemmas 2.1 and 2.2 we derive the following proposition:

Proposition 2.3. *The conjugates of an element* $x \in L$ *form a normal basis of* L *over* K *if and only if*

$$\sum_{1\le i\le n} \chi(\gamma_i^{-1}) x^{\gamma_i} \neq 0 \quad \textit{for all } \chi \in \widehat{G}.$$

Proof. For an element $x \in L$, set $x_i = x^{\gamma_i}$ for $1 \le i \le n$. Then we get that

the conjugates of x form a normal basis of L over K

$\iff$ $\{x_1, \cdots, x_n\}$ is a K-basis of L by definition of a normal basis

$\iff$ $\det\left(x_i^{\gamma_j^{-1}}\right)_{1\le i,\ j\le n} \neq 0$ by Lemma 2.1

$\iff$ $\sum_{1\le i\le n} \chi(\gamma_i^{-1}) x_i \neq 0$ for all $\chi \in \widehat{G}$ by Lemma 2.2 with $f(\gamma_i) = x_i$.

□

Now we present a useful criterion which enables us to determine whether the conjugates of an element $x \in L$ form a normal basis of L over K.

Theorem 2.4. *Assume that there exists an element* $x \in L$ *such that*

$$\left|\frac{x^{\gamma_i}}{x}\right| < 1 \quad \textit{for } 1 < i \le n. \tag{2.1}$$

Then the conjugates of a high power of x *form a normal basis of* L *over* K*.*

Proof. By the hypothesis (2.1) we can take a suitably large integer m such that

$$\left|\frac{x^{\gamma_i}}{x}\right|^m \le \frac{1}{\#G} \quad \text{for } 1 < i \le n \tag{2.2}$$

where $\#G$ is the cardinality of G. Then for $\chi \in \widehat{G}$ we have

$$\begin{aligned} \left|\sum_{1\le i\le n}\chi(\gamma_i^{-1})(x^m)^{\gamma_i}\right| &\ge |x^m|\left(1-\sum_{1<i\le n}\left|\frac{(x^m)^{\gamma_i}}{x^m}\right|\right) \quad \text{by the triangle inequality} \\ &\ge |x^m|\left(1-\frac{1}{\#G}(\#G-1)\right)=\frac{|x^m|}{\#G}>0 \quad \text{by (2.2).} \end{aligned}$$

Therefore the conjugates of x^m form a normal basis of L over K by Proposition 2.3. □

3. Action of Galois groups

We shall investigate an algorithm to find all conjugates of the singular value of a modular function, from which we can determine the conjugates of singular values of certain Siegel functions due to [2], [15] or [3].

For a positive integer N let $\mathcal{F}_N$ be the field of modular functions of level N defined over $\mathbb{Q}(\zeta_N)$ with $\zeta_N = e^{2\pi i/N}$. Then $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1 = \mathbb{Q}(j)$ (j =the elliptic modular function) and its Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ ([7] or [14]).

Throughout this section we let K be an imaginary quadratic field with discriminant d_K and set

$$\theta = \begin{cases} \frac{\sqrt{d_K}}{2} & \text{for } d_K \equiv 0 \pmod 4 \\ \frac{-1+\sqrt{d_K}}{2} & \text{for } d_K \equiv 1 \pmod 4. \end{cases} \tag{3.1}$$

Under the properly equivalent relation, primitive positive definite binary quadratic forms $aX^2+bXY+cY^2$ of discriminant d_K determine a group $\mathrm{C}(d_K)$, called the *form class group of discriminant* d_K. We identify $\mathrm{C}(d_K)$ with the set of all *reduced quadratic forms*, which are characterized by the conditions

$$-a < b \le a < c \quad \text{or} \quad 0 \le b \le a = c \tag{3.2}$$

together with the discriminant relation

$$b^2 - 4ac = d_K. \tag{3.3}$$

From the above two conditions for reduced quadratic forms we have

$$1 \le a \le \sqrt{\tfrac{-d_K}{3}}. \tag{3.4}$$

Then it is well-known that $\mathrm{C}(d_K)$ is isomorphic to $\mathrm{Gal}(H/K)$ ([1]). For a reduced quadratic form $Q = aX^2+bXY+cY^2$ of discriminant d_K we define a CM-point

$$\theta_Q = \frac{-b+\sqrt{d_K}}{2a}. \tag{3.5}$$

Furthermore, we define $\beta_Q = (\beta_p)_p \in \prod_{p\,:\,\text{primes}} \mathrm{GL}_2(\mathbb{Z}_p)$ as

$$\beta_p = \begin{cases} \begin{pmatrix} a & \frac{b}{2} \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} -\frac{b}{2} & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c \\ \begin{pmatrix} -\frac{b}{2} - a & -\frac{b}{2} - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c \end{cases} \quad \text{for } d_K \equiv 0 \pmod 4 \tag{3.6}$$

and

$$\beta_p = \begin{cases} \begin{pmatrix} a & \frac{b-1}{2} \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} \frac{-b-1}{2} & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c \\ \begin{pmatrix} \frac{-b-1}{2} - a & \frac{1-b}{2} - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c \end{cases} \quad \text{for } d_K \equiv 1 \pmod 4. \tag{3.7}$$

Proposition 3.1. *Let N be a positive integer. If $h \in \mathcal{F}_N$ is defined and finite at θ and Q is a reduced quadratic form of discriminant d_K, then the value $h^{\beta_Q}(\theta_Q)$ belongs to $K_{(N)}$. Here, we note that there exists $\beta \in \mathrm{GL}_2^+(\mathbb{Q}) \cap \mathrm{M}_2(\mathbb{Z})$ such that $\beta \equiv \beta_p \pmod{N\mathbb{Z}_p}$ for all primes p dividing N by the Chinese remainder theorem. Then the action of β_Q on $\mathcal{F}_N$ is understood as that of β which is an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \cong \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$. Furthermore, we have an isomorphism*

$$\begin{array}{ccc} \mathrm{C}(d_K) & \longrightarrow & \mathrm{Gal}(H/K) \\ Q & \mapsto & \left(h(\theta) \mapsto h^{\beta_Q}(\theta_Q) \right)\Big|_H \end{array}$$

where $h \in \mathcal{F}_N$ is defined and finite at θ.

Proof. See [15] or [2]. □

The next proposition explicitly describes the Shimura's reciprocity law ([7] or [14]).

Proposition 3.2. *Let $\min(\theta,\ \mathbb{Q}) = X^2 + BX + C \in \mathbb{Z}[X]$. For a positive integer N the matrix group*

$$W_{N,\,\theta} = \left\{ \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \ :\ t,\ s \in \mathbb{Z}/N\mathbb{Z} \right\}$$

gives rise to a surjection

$$\begin{array}{ccc} W_{N,\ \theta} & \longrightarrow & \mathrm{Gal}(K_{(N)}/H) \\ \alpha & \mapsto & \Big(h(\theta)\mapsto h^{\alpha}(\theta)\Big) \end{array}$$

where $h\in\mathcal{F}_N$ *is defined and finite at* θ. *The action of* α *on* $\mathcal{F}_N$ *is the action as an element of* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}\cong\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$. *If* $K\neq\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$, *then the kernel is* $\{\pm 1_2\}$.

Proof. See [15] or [2]. □

Combining the above two propositions we achieve the following result.

Proposition 3.3. *Let* $K\neq\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ *be an imaginary quadratic field and* N *be a positive integer. Then we have a bijective map*

$$\begin{array}{ccc} W_{N,\ \theta}/\{\pm 1_2\}\times\mathrm{C}(d_K) & \longrightarrow & \mathrm{Gal}(K_{(N)}/K) \\ \alpha\times Q & \longmapsto & \Big(h(\theta)\mapsto h^{\alpha\cdot\beta_Q}(\theta_Q)\Big) \end{array}$$

where $h\in\mathcal{F}_N$ *is defined and finite at* θ.

Proof. One can justify the assertion by observing the following diagram:

$$\begin{array}{lll} \underline{\text{Fields}} & \underline{\text{Galois groups}} & \\ K_{(N)} & & \\ \Big| & \Big\{\Big(h(\theta)\mapsto h^{\alpha}(\theta)\Big)\ :\ \alpha\in W_{N,\ \theta}/\{\pm 1_2\}\Big\} & \text{by Proposition 3.2} \\ H & & \\ \Big| & \Big\{\Big(h(\theta)\mapsto h^{\beta_Q}(\theta_Q)\Big)\Big|_H\ :\ Q\in\mathrm{C}(d_K)\Big\} & \text{by Proposition 3.1} \\ K & & \end{array}$$

where $h\in\mathcal{F}_N$ is defined and finite at θ. □

Proposition 3.3 and the transformation formulas of Siegel functions in the next proposition enable us to find all conjugates of the singular value $g_{(0,\ \frac{1}{N})}^{\frac{-12N}{\gcd(6,\ N)}}(\theta)$, which will be used to prove our main theorem.

Proposition 3.4. *Let* $N\geq 2$. *For* $(v,\ w)\in\mathbb{Z}^2\setminus N\mathbb{Z}^2$ *the function* $g_{(\frac{v}{N},\ \frac{w}{N})}^{\frac{-12N}{\gcd(6,\ N)}}(\tau)$ *satisfies*

$$g_{(\frac{v}{N},\ \frac{w}{N})}^{\frac{-12N}{\gcd(6,\ N)}}(\tau)=g_{(\frac{-v}{N},\ \frac{-w}{N})}^{\frac{-12N}{\gcd(6,\ N)}}(\tau)=g_{(\langle\frac{v}{N}\rangle,\ \langle\frac{w}{N}\rangle)}^{\frac{-12N}{\gcd(6,\ N)}}(\tau)$$

where $\langle X \rangle$ is the fractional part of $X \in \mathbb{R}$ with $0 \le \langle X \rangle < 1$. It belongs to $\mathcal{F}_N$ and α in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \cong \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$ acts on the function by

$$\left(g_{(\frac{v}{N},\ \frac{w}{N})}^{\frac{-12N}{\gcd(6,\ N)}}(\tau) \right)^{\alpha} = g_{(\frac{v}{N},\ \frac{w}{N})\alpha}^{\frac{-12N}{\gcd(6,\ N)}}(\tau).$$

Proof. See [5] Proposition 2.4 and Theorem 2.5. □

4. Normal bases of $K_{(N)}$ over K

Let $K \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field so that $d_K \le -7$, and let θ be defined as in (3.1) and $N \ge 2$ be an integer. If we put

$$D = \sqrt{\frac{-d_K}{3}} \quad \text{and} \quad A = |e^{2\pi i \theta}| = e^{-\pi\sqrt{-d_K}},$$

then $A^{\frac{1}{D}} = e^{-\pi\sqrt{3}}$, which is independent of K.

Although the following lemmas were studied in [3], we present the proofs for the sake of completeness.

Lemma 4.1. *We have the following inequalities:*

(i) $1 < \left| \frac{1-\zeta_N}{1-A^{\frac{1}{DN}}} \right| < A'(N)$ *where* $A'(N) = \begin{cases} 2.141 & \text{if } N = 2,\ 3 \\ 1.903 & \text{if } N = 4 \\ 1.773 & \text{if } N = 5 \\ 1.678 & \text{if } N = 6 \\ 1.606 & \text{if } N = 7,\ 8 \\ 1.508 & \text{if } N = 9,\ 10,\ 11 \\ 1.42 & \text{if } N = 12, \cdots, 17 \\ 1.332 & \text{if } N = 18,\ 19,\ 20 \\ 1.306 & \text{if } N \ge 21. \end{cases}$

(ii) *If $N \ge 2$, then $\left| \frac{1-\zeta_N}{1-\zeta_N^t} \right| \le 1$ for all $t \in \mathbb{Z} \setminus N\mathbb{Z}$.*

(iii) *If $N \ge 4$, then $\left| \frac{1-\zeta_N}{1-\zeta_N^t} \right| \le \frac{1}{\sqrt{2}}$ for $2 \le t \le \frac{N}{2}$.*

(iv) *If $N \ge 2$, then $A^{\frac{1}{2}\left(\mathbf{B}_2(0)-\mathbf{B}_2(\frac{1}{N})\right)} \left| \frac{1-\zeta_N}{1-A^{\frac{1}{N}}} \right| < 0.76$.*

(v) *$\frac{1}{1-A^{\frac{X}{a}}} < 1 + A^{\frac{X}{1.03a}}$ for $1 \le a \le D$ and all $X \ge \frac{1}{2}$.*

(vi) *$1 + X < e^X$ for all $X > 0$.*

Proof. (i) Since $\left| \frac{1-\zeta_N}{1-A^{\frac{1}{DN}}} \right| = \frac{2\sin\frac{\pi}{N}}{1-e^{-\frac{\pi\sqrt{3}}{N}}}$, it is numerically routine to check the inequality (i).

(ii) $\left| \frac{1-\zeta_N}{1-\zeta_N^t} \right| = \left| \frac{\sin\frac{\pi}{N}}{\sin\frac{\pi t}{N}} \right| \le 1$ for all $t \in \mathbb{Z} \setminus N\mathbb{Z}$.

(iii) If $N \ge 4$ and $2 \le t \le \frac{N}{2}$, then $\left|\sin\frac{\pi t}{N}\right| \ge \sin\frac{2\pi}{N}$. Thus

$$\left| \frac{1-\zeta_N}{1-\zeta_N^t} \right| = \left| \frac{\sin\frac{\pi}{N}}{\sin\frac{\pi t}{N}} \right| \le \frac{\sin\frac{\pi}{N}}{\sin\frac{2\pi}{N}} = \frac{1}{2\cos\frac{\pi}{N}} \le \frac{1}{2\cos\frac{\pi}{4}} = \frac{1}{\sqrt{2}}.$$

(iv) Since $d_K \leq -7$, we get $A = e^{-\pi\sqrt{-d_K}} \leq e^{-\pi\sqrt{7}}$. It then follows that

$$A^{\frac{1}{2}\left(\mathbf{B}_2(0)-\mathbf{B}_2(\frac{1}{N})\right)}\left|\frac{1-\zeta_N}{1-A^{\frac{1}{N}}}\right| \leq e^{-\frac{\pi\sqrt{7}}{2}(\frac{1}{N}-\frac{1}{N^2})}\frac{2\sin\frac{\pi}{N}}{1-e^{-\frac{\pi\sqrt{7}}{N}}}.$$

And, one can readily show that the last term on $N \geq 2$ is less than 0.76.

(v) The given inequality is equivalent to

$$A^{\frac{X}{a}\frac{3}{103}} + A^{\frac{X}{a}} < 1.$$

Since $A \leq e^{-\pi\sqrt{7}} < 1$, $1 \leq a \leq D$ and $X \geq \frac{1}{2}$, we obtain

$$A^{\frac{X}{a}\frac{3}{103}} + A^{\frac{X}{a}} \leq A^{\frac{1}{2D}\frac{3}{103}} + A^{\frac{1}{2D}} = e^{-\frac{\pi\sqrt{3}}{2}\frac{3}{103}} + e^{-\frac{\pi\sqrt{3}}{2}} < 1$$

by the fact $A^{\frac{1}{D}} = e^{-\pi\sqrt{3}}$.

(vi) It is immediate from the shape of the graph of the equation $Y = 1+X-e^X$ for $X > 0$.

□

Lemma 4.2. *Assume the condition*

$$\begin{cases} d_K \leq -11, & N = 2,\ 3 \\ d_K \leq -8, & N = 4 \\ d_K \leq -31, & N = 5 \\ d_K \leq -23, & N = 6 \\ d_K \leq -19, & N = 7,\ 8 \\ d_K \leq -15, & N = 9,\ 10,\ 11 \\ d_K \leq -11, & N = 12, \cdots, 17 \\ d_K \leq -8, & N = 18,\ 19,\ 20 \\ d_K \leq -7, & N \geq 21. \end{cases} \tag{4.1}$$

Let $Q = aX^2 + bXY + cY^2$ be a reduced quadratic form of discriminant d_K and θ_Q as in (3.5). If $a \geq 2$, then the inequality

$$\left|\frac{g^{-1}_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0,\ \frac{1}{N})}(\theta)}\right| < 1$$

holds for $(s,\ t) \in \mathbb{Z}^2 \setminus N\mathbb{Z}^2$.

Proof. We may assume $0 \leq s \leq \frac{N}{2}$ by Proposition 3.4. And, note that $2 \leq a \leq D$ by (3.4). By definition (1.1) we have

$$\left|\frac{g^{-1}_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0,\ \frac{1}{N})}(\theta)}\right|$$

$$\leq A^{\frac{1}{2}\left(\mathbf{B}_2(0)-\frac{1}{a}\mathbf{B}_2(\frac{s}{N})\right)}\left|\frac{1-\zeta_N}{1-e^{2\pi i(\frac{s}{N}\theta_Q+\frac{t}{N})}}\right|\prod_{n=1}^{\infty}\frac{(1+A^n)^2}{(1-A^{\frac{1}{a}(n+\frac{s}{N})})(1-A^{\frac{1}{a}(n-\frac{s}{N})})}.$$

If $s=0$, then we get by Lemma 4.1(ii)

$$\left|\frac{1-\zeta_N}{1-e^{2\pi i(\frac{s}{N}\theta_Q+\frac{t}{N})}}\right| = \left|\frac{1-\zeta_N}{1-\zeta_N^t}\right| \le 1.$$

If $s \neq 0$, then by the fact $2 \le a \le D$ and Lemma 4.1(i) we derive

$$\left|\frac{1-\zeta_N}{1-e^{2\pi i(\frac{s}{N}\theta_Q+\frac{t}{N})}}\right| \le \left|\frac{1-\zeta_N}{1-A^{\frac{s}{Na}}}\right| \le \left|\frac{1-\zeta_N}{1-A^{\frac{1}{ND}}}\right| < A'(N).$$

Let

$$A'(s,\ N) = \begin{cases} 1 & \text{if } s=0 \\ A'(N) & \text{if } s \neq 0. \end{cases}$$

On the other hand, it follows from the facts $\mathbf{B}_2(\frac{1}{2}),\ \mathbf{B}_2(\frac{1}{3}),\ \mathbf{B}_2(\frac{1}{4}) < 0$ and $A<1$ together with the assumption $a \ge 2$ that

$$A^{\frac{1}{2}\left(\mathbf{B}_2(0)-\frac{1}{a}\mathbf{B}_2(\frac{s}{N})\right)} \le A^{\varepsilon(s,\ N)}$$

where

$$\varepsilon(s,\ N) = \begin{cases} \frac{1}{2}\big(\mathbf{B}_2(0)-\frac{1}{2}\mathbf{B}_2(0)\big) = \frac{1}{24} & \text{if } s=0 \text{ or } N \ge 5 \\ \frac{1}{2}\mathbf{B}_2(0) = \frac{1}{12} & \text{otherwise.} \end{cases}$$

Therefore, we achieve that

$$\begin{aligned}
\left|\frac{g^{-1}_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0,\ \frac{1}{N})}(\theta)}\right| &\le A^{\varepsilon(s,\ N)}A'(s,\ N)\prod_{n=1}^{\infty}\frac{(1+A^n)^2}{(1-A^{\frac{n}{D}})(1-A^{\frac{1}{D}(n-\frac{1}{2})})} \\
&\qquad \text{by the facts } 2 \le a \le D,\ 0 \le s \le \tfrac{N}{2} \\
&< A^{\varepsilon(s,\ N)}A'(s,\ N)\prod_{n=1}^{\infty}(1+A^n)^2(1+A^{\frac{n}{1.03D}})(1+A^{\frac{1}{1.03D}(n-\frac{1}{2})}) \\
&\qquad \text{by Lemma 4.1(v)} \\
&< A^{\varepsilon(s,\ N)}A'(s,\ N)\prod_{n=1}^{\infty}e^{2A^n+A^{\frac{n}{1.03D}}+A^{\frac{1}{1.03D}(n-\frac{1}{2})}} \quad \text{by Lemma 4.1(vi)} \\
&= A^{\varepsilon(s,\ N)}A'(s,\ N)e^{\frac{2A}{1-A}+\frac{A^{\frac{1}{1.03D}}+A^{\frac{1}{2.06D}}}{1-A^{\frac{1}{1.03D}}}} \\
&= \begin{cases} e^{-\frac{\pi\sqrt{-d_K}}{24}}\ e^{\frac{2e^{-\pi\sqrt{-d_K}}}{1-e^{-\pi\sqrt{-d_K}}}+\frac{e^{-\frac{\pi\sqrt{3}}{1.03}}+e^{-\frac{\pi\sqrt{3}}{2.06}}}{1-e^{-\frac{\pi\sqrt{3}}{1.03}}}} & \text{if } s=0 \\ e^{-\frac{\pi\sqrt{-d_K}}{24}}A'(N)\ e^{\frac{2e^{-\pi\sqrt{-d_K}}}{1-e^{-\pi\sqrt{-d_K}}}+\frac{e^{-\frac{\pi\sqrt{3}}{1.03}}+e^{-\frac{\pi\sqrt{3}}{2.06}}}{1-e^{-\frac{\pi\sqrt{3}}{1.03}}}} & \text{if } s\neq 0 \text{ and } N \ge 5 \\ e^{-\frac{\pi\sqrt{-d_K}}{12}}A'(N)\ e^{\frac{2e^{-\pi\sqrt{-d_K}}}{1-e^{-\pi\sqrt{-d_K}}}+\frac{e^{-\frac{\pi\sqrt{3}}{1.03}}+e^{-\frac{\pi\sqrt{3}}{2.06}}}{1-e^{-\frac{\pi\sqrt{3}}{1.03}}}} & \text{if } s\neq 0 \text{ and } N \le 4 \end{cases} \\
&< 1 \quad \text{under the condition (4.1).}
\end{aligned}$$

This proves the lemma. □

Lemma 4.3. *Assume that* $d_K \leq -7$ *and* $N \geq 2$. *Let* $Q = X^2 + bXY + cY^2$ *be a reduced quadratic form of discriminant* d_K *and* θ_Q *as in (3.5). Then we have the inequality*

$$\left| \frac{g^{-1}_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0,\ \frac{1}{N})}(\theta)} \right| < 1$$

for $s,\ t \in \mathbb{Z}$ *with* $s \not\equiv 0 \pmod{N}$.

Proof. We may assume $1 \leq s \leq \frac{N}{2}$ by Proposition 3.4. Then we derive from (1.1) that

$$\begin{aligned}
\left| \frac{g^{-1}_{(\frac{s}{N},\ \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0,\ \frac{1}{N})}(\theta)} \right| &\leq A^{\frac{1}{2}\left(\mathbf{B}_2(0)-\mathbf{B}_2(\frac{s}{N})\right)} \left| \frac{1-\zeta_N}{1-A^{\frac{s}{N}}} \right| \prod_{n=1}^{\infty} \frac{(1+A^n)^2}{(1-A^{n+\frac{s}{N}})(1-A^{n-\frac{s}{N}})} \\
&< A^{\frac{1}{2}\left(\mathbf{B}_2(0)-\mathbf{B}_2(\frac{1}{N})\right)} \left| \frac{1-\zeta_N}{1-A^{\frac{1}{N}}} \right| \prod_{n=1}^{\infty} \frac{(1+A^n)^2}{(1-A^n)(1-A^{n-\frac{1}{2}})} \quad \text{by the fact } 1 \leq s \leq \tfrac{N}{2} \\
&< 0.76 \prod_{n=1}^{\infty} (1+A^n)^2 (1+A^{\frac{n}{1.03}})(1+A^{\frac{1}{1.03}(n-\frac{1}{2})}) \quad \text{by Lemma 4.1(iv) and (v)} \\
&< 0.76 \prod_{n=1}^{\infty} e^{2A^n + A^{\frac{n}{1.03}} + A^{\frac{1}{1.03}(n-\frac{1}{2})}} = 0.76 e^{\frac{2A}{1-A} + \frac{A^{\frac{1}{1.03}} + A^{\frac{1}{2.06}}}{1-A^{\frac{1}{1.03}}}} \quad \text{by Lemma 4.1(vi)} \\
&\leq 0.76 e^{\frac{2e^{-\pi\sqrt{7}}}{1-e^{-\pi\sqrt{7}}} + \frac{e^{-\frac{\pi\sqrt{7}}{1.03}} + e^{-\frac{\pi\sqrt{7}}{2.06}}}{1-e^{-\frac{\pi\sqrt{7}}{1.03}}}} < 1 \quad \text{by the fact } d_K \leq -7.
\end{aligned}$$

□

Lemma 4.4. *Assume the same condition as in Lemma 4.3. Let* $Q = X^2 + bXY + cY^2$ *be a reduced quadratic form of discriminant* d_K *and* θ_Q *as in (3.5). Then we deduce*

$$\left| \frac{g^{-1}_{(0,\ \frac{t}{N})}(\theta_Q)}{g^{-1}_{(0,\ \frac{1}{N})}(\theta)} \right| < 1$$

for $t \in \mathbb{Z}$ *with* $t \not\equiv 0,\ \pm 1 \pmod{N}$.

Proof. If $N = 2$ or 3, there is nothing to prove. Thus, let $N \geq 4$. Here we may assume $2 \leq t \leq \frac{N}{2}$ by Proposition 3.4. Then we get that

$$\begin{aligned}\left|\frac{g_{(0,\ \frac{t}{N})}^{-1}(\theta_Q)}{g_{(0,\ \frac{1}{N})}^{-1}(\theta)}\right| &\leq \left|\frac{1-\zeta_N}{1-\zeta_N^t}\right| \prod_{n=1}^{\infty} \frac{(1+A^n)^2}{(1-A^n)^2} \\ &< \tfrac{1}{\sqrt{2}} \prod_{n=1}^{\infty} (1+A^n)^2(1+A^{\frac{n}{1.03}})^2 \quad \text{by Lemma 4.1(iii) and (v)} \\ &< \tfrac{1}{\sqrt{2}} \prod_{n=1}^{\infty} e^{2A^n+2A^{\frac{n}{1.03}}} \quad \text{by Lemma 4.1(vi)} \\ &= \tfrac{1}{\sqrt{2}} e^{\frac{2A}{1-A}+\frac{2A^{\frac{1}{1.03}}}{1-A^{\frac{1}{1.03}}}} \leq \tfrac{1}{\sqrt{2}} e^{\frac{2e^{-\pi\sqrt{7}}}{1-e^{-\pi\sqrt{7}}}+\frac{2e^{-\frac{\pi\sqrt{7}}{1.03}}}{1-e^{-\frac{\pi\sqrt{7}}{1.03}}}} < 1 \quad \text{by the fact } d_K \leq -7,\end{aligned}$$

which proves the lemma. □

Now we are ready to prove our main theorem concerning normal bases of $K_{(N)}$ over almost all K.

Theorem 4.5. *Assume the condition (4.1). Then for a suitably large integer m the conjugates of the value*

$$g_{(0,\ \frac{1}{N})}^{\frac{-12Nm}{\gcd(6,\ N)}}(\theta)$$

form a normal basis of $K_{(N)}$ over K.

Proof. For simplicity we put $x = g_{(0,\ \frac{1}{N})}^{\frac{-12N}{\gcd(6,\ N)}}(\theta)$, which belongs to $K_{(N)}$ by Proposition 3.4 and the main theorem of complex multiplication ([7] or [14]). Then it suffices to show by Theorem 2.4 that

$$\left|\frac{x^\gamma}{x}\right| < 1 \text{ for all } \gamma \in \mathrm{Gal}(K_{(N)}/K) \setminus \{\mathrm{id}\}. \tag{4.2}$$

To this end we consider by Propositions 3.3 and 3.4 a conjugate x^γ of x which is of the form

$$x^\gamma = \left(g_{(0,\ \frac{1}{N})}^{\frac{-12N}{\gcd(6,\ N)}}\right)^{\alpha\cdot\beta_Q}(\theta_Q) = g_{(\frac{s}{N},\ \frac{t}{N})\beta_Q}^{\frac{-12N}{\gcd(6,\ N)}}(\theta_Q)$$

for some $\alpha = \pm\left(\begin{smallmatrix} t-Bs & -Cs \\ s & t\end{smallmatrix}\right) \in W_{N,\ \theta}/\{\pm 1_2\}$, where $\min(\theta,\ \mathbb{Q}) = X^2+BX+C$, and $Q = aX^2+bXY+cY^2$ is a reduced quadratic form of discriminant d_K. If $a \geq 2$, the inequality (4.2) holds by Lemma 4.2. If $a = 1$, we derive from the conditions (3.2) and (3.3) that

$$Q = \begin{cases} X^2 - \frac{d_K}{4}Y^2 & \text{for } d_K \equiv 0 \pmod 4 \\ X^2+XY+\frac{1-d_K}{4}Y^2 & \text{for } d_K \equiv 1 \pmod 4), \end{cases} \tag{4.3}$$

which yields $\beta_Q \equiv 1_2 \pmod N$ by the relations (3.6) and (3.7). Thus $x^\gamma = g_{(\frac{s}{N},\ \frac{t}{N})}^{\frac{-12N}{\gcd(6,\ N)}}(\theta_Q)$. Moreover, if $(s,\ t) \not\equiv (0,\ \pm 1) \pmod N$, then the inequality (4.2) is also true by Lemmas 4.3 and 4.4. Here it is not necessary to consider the remaining case where $a = 1$ and $(s,\ t) \equiv (0,\ \pm 1) \pmod N$, because $\gamma = \mathrm{id} \in \mathrm{Gal}(K_{(N)}/K)$ in this case. Therefore (4.2) holds for all $\gamma \in \mathrm{Gal}(K_{(N)}/K) \setminus \{\mathrm{id}\}$ as desired. $\square$

Remark 4.6. Observe that the fields $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$ and $\mathbb{Q}(\sqrt{-19})$ have class number 1 ([1]). For such a field K there is only one reduced quadratic form of discriminant d_K as in (4.3). Hence Theorem 4.5 is true for this K and all $N \geq 2$, because we don't need to apply Lemma 4.2 in the proof. Lastly, we list the other fields K and integers N which cannot be covered by our argument as follows:

TABLE 1. Exceptions of Theorem 4.5

K	d_K	(N, a singular value whose conjugates form a normal basis of $K_{(N)}$ over K)
$\mathbb{Q}(\sqrt{-15})$	-15	$\big(5,\ g_{(0,\ \frac{1}{5})}^{-60}(\frac{-1+\sqrt{-15}}{2})\big)$, $\big(6,\ g_{(0,\ \frac{1}{6})}^{-12}(\frac{-1+\sqrt{-15}}{2})\big)$ $\big(7,\ g_{(0,\ \frac{1}{7})}^{-84}(\frac{-1+\sqrt{-15}}{2})\big)$, $\big(8,\ g_{(0,\ \frac{1}{8})}^{-48}(\frac{-1+\sqrt{-15}}{2})\big)$
$\mathbb{Q}(\sqrt{-5})$	-20	$\big(5,\ g_{(0,\ \frac{1}{5})}^{-60}(\sqrt{-5})\big)$, $\big(6,\ g_{(0,\ \frac{1}{6})}^{-12}(\sqrt{-5})\big)$
$\mathbb{Q}(\sqrt{-23})$	-23	$\big(5,\ g_{(0,\ \frac{1}{5})}^{-60}(\frac{-1+\sqrt{-23}}{2})\big)$
$\mathbb{Q}(\sqrt{-6})$	-24	$\big(5,\ g_{(0,\ \frac{1}{5})}^{-60}(\sqrt{-6})\big)$

Even in these remaining 8 cases, however, one can verify Theorem 4.5 by numerical computation. For example, let $K = \mathbb{Q}(\sqrt{-5})$ and $N = 6$. Then $d_K = -20$, $\theta = \sqrt{-5}$ and

$$\begin{aligned}
&\mathrm{C}(d_K) = \big\{Q_1 = X^2 + 5Y^2,\quad Q_2 = 2X^2 + 2XY + 3Y^2\big\}\\
&\theta_{Q_1} = \sqrt{-5},\quad \theta_{Q_2} = \tfrac{-1+\sqrt{-5}}{2}\\
&\beta_{Q_1} = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\quad \beta_{Q_2} = \left(\begin{smallmatrix}1&5\\3&2\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}\\
&W_{N,\ \theta}/\{\pm 1_2\} = \big\{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}2&3\\3&2\end{smallmatrix}\right),\ \left(\begin{smallmatrix}3&2\\2&3\end{smallmatrix}\right)\big\} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}.
\end{aligned}$$

If $x = g_{(0,\ \frac{1}{N})}^{\frac{-12N}{\gcd(6,\ N)}}(\theta) = g_{(0,\ \frac{1}{6})}^{-12}(\sqrt{-5})$, then by Propositions 3.3 and 3.4 its conjugates are

$$\begin{aligned}
&x_1 = x, && x_2 = g_{(\frac{1}{6},\ 0)}^{-12}(\sqrt{-5}), && x_3 = g_{(\frac{3}{6},\ \frac{2}{6})}^{-12}(\sqrt{-5})\\
&x_4 = g_{(\frac{2}{6},\ \frac{3}{6})}^{-12}(\sqrt{-5}), && x_5 = g_{(\frac{3}{6},\ \frac{2}{6})}^{-12}(\tfrac{-1+\sqrt{-5}}{2}), && x_6 = g_{(\frac{1}{6},\ \frac{5}{6})}^{-12}(\tfrac{-1+\sqrt{-5}}{2})\\
&x_7 = g_{(\frac{3}{6},\ \frac{1}{6})}^{-12}(\tfrac{-1+\sqrt{-5}}{2}), && x_8 = g_{(\frac{5}{6},\ \frac{4}{6})}^{-12}(\tfrac{-1+\sqrt{-5}}{2})
\end{aligned}$$

possibly with certain multiplicity. Hence by using MAPLE one can check that

$$\left|\frac{x_i}{x_1}\right| < 10^{-4} < \frac{1}{\#\mathrm{Gal}(K_{(6)}/K)} = \frac{1}{8} \quad \text{for } i = 2, \cdots, 8.$$

Therefore $\{x_1, \cdots, x_8\}$ becomes a normal basis of $K_{(6)}$ over K by Theorem 2.4. Moreover, one can also show that the minimal polynomial of x would be

$$\begin{aligned}(X - x_1) \cdots (X - x_8) \quad = \quad & X^8 - 1263840X^7 + 42016796X^6 + 72894400X^5 \\ & +15056640X^4 - 4525280X^3 + 167196X^2 - 1280X + 1\end{aligned}$$

with integer coefficients ([5]).

Remark 4.7. Let K be an imaginary quadratic field and $\mathfrak{f}$ ($\neq \mathcal{O}_K$) be a nonzero integral ideal of K. We denote by $\mathrm{Cl}(\mathfrak{f})$ the ray class group and write C_0 for its unit class. By definition the ray class field $K_\mathfrak{f}$ modulo $\mathfrak{f}$ is a finite abelian extension of K whose Galois group is isomorphic to $\mathrm{Cl}(\mathfrak{f})$ via the Artin map. If $C \in \mathrm{Cl}(\mathfrak{f})$, then we take an integral ideal $\mathfrak{c}$ in C so that $\mathfrak{f}\mathfrak{c}^{-1} = [z_1,\ z_2]$ with $z = \frac{z_1}{z_2} \in \mathfrak{H}$. Now we define the *Siegel-Ramachandra invariant* by

$$g_\mathfrak{f}(C) = g^{12N(\mathfrak{f})}_{(\frac{a}{N(\mathfrak{f})},\ \frac{b}{N(\mathfrak{f})})}(z) \tag{4.4}$$

where $N(\mathfrak{f})$ is the smallest positive integer in $\mathfrak{f}$ and $a,\ b \in \mathbb{Z}$ such that $1 = \frac{a}{N(\mathfrak{f})} z_1 + \frac{b}{N(\mathfrak{f})} z_2$. This value depends only on the class C and belongs to $K_\mathfrak{f}$ ([6]).

Ramachandra showed in [11] that for arbitrary modulus $\mathfrak{f}$ the ray class field $K_\mathfrak{f}$ can be generated over K by certain elliptic unit, but his invariant involves too complicated product of high powers of singular values of the Klein forms and singular values of the Δ-function to use in practice. Thus, Lang proposed in his book ([7] p. 292) to find a simpler one by utilizing the Siegel-Ramachandra invariant, and Schertz found it in [13], namely $g_\mathfrak{f}(C_0)$ (so any $g_\mathfrak{f}(C)$) as a primitive generator of $K_\mathfrak{f}$ over K under some conditions on $\mathfrak{f}$. And he further conjectured ([13] p. 386) that $g_\mathfrak{f}(C_0)$ becomes a ray class invariant without any assumption on $\mathfrak{f}$.

On the other hand, the modulus $\mathfrak{f}$ can be enlarged by class field theory so that we may assume $\mathfrak{f} = N\mathcal{O}_K$. If $K \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$ and $\mathfrak{f} = N\mathcal{O}_K$ for an integer $N (\geq 2)$, then $N(\mathfrak{f}) = N$ and we may choose $\mathcal{O}_K \in C_0$ so that $\mathfrak{f}\mathcal{O}_K^{-1} = [N\theta,\ N]$ where θ is defined as in (3.1). Hence we know by definition (4.4)

$$g_\mathfrak{f}(C_0) = g^{12N}_{(0,\ \frac{1}{N})}(\theta).$$

Therefore, Theorem 4.5 and Remark 4.6 indicate that $g_\mathfrak{f}(C_0)$ is indeed a primitive generator of $K_\mathfrak{f}$ over K, which would be an answer for the Lang-Schertz conjecture on the Siegel-Ramachandra invariant to construct $K_\mathfrak{f}$ when the modulus $\mathfrak{f}$ is $N\mathcal{O}_K$.

References

1. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., 1989.

2. A. Gee, *Class invariants by Shimura's reciprocity law*, J. Theor. Nombres Bordeaux 11 (1999), no. 1, 45-72.
3. H. Y. Jung, J. K. Koo and D. H. Shin, *Ray class invariants over imaginary quadratic fields*, submitted.
4. K. Komatsu, *Construction of a normal basis by special values of Siegel modular functions*, Proc. Amer. Math. Soc. 128 (2000), no. 2, 315-323.
5. J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit., 264 (2010) 137-177.
6. D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, 1981.
7. S. Lang, *Elliptic Functions, 2nd edition*, Spinger-Verlag, 1987.
8. H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. 201 (1959) 119-149.
9. T. Okada, *On an extension of a theorem of S. Chowla*, Acta Arith. 38 (1980/81), no. 4, 341-345.
10. T. Okada, *Normal bases of class field over Gauss' number field*, J. London Math. Soc. (2) 22 (1980), no. 2, 221-225.
11. K. Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math. (2) 80(1964), 104-148.
12. R. Schertz, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory 39 (1991), no. 3, 285-326.
13. R. Schertz, *Construction of ray class fields by elliptic units*, J. Theor. Nombres Bordeaux 9 (1997), no. 2, 383-394.
14. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.
15. P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class Field Theory-Its Centenary and Prospect (Tokyo, 1998), 161-176, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.
16. M. J. Talyor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math. (2) 121 (1985), no. 3, 519-535.
17. B. L. van der Waerden, *Algebra, Vol I*, Springer-Verlag, 2003.

Department of Mathematical Sciences, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: DOSAL@math.kaist.ac.kr

Department of Mathematical Sciences, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: jkkoo@math.kaist.ac.kr

Department of Mathematical Sciences, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: shakur01@kaist.ac.kr