10. *On Siegel Eigenforms*

By Nobushige KUROKAWA
Department of Mathematics, Tokyo Institute of Technology

(Communicated by Kunihiko KODAIRA, M. J. A., Jan. 12, 1981)

Introduction. We note some properties of Siegel eigenforms of general degree relating to the algebra of Hecke operators. We refer to [5]–[7] for motivations and examples. (These examples satisfy the "multiplicity one conjecture".)

§ 1. Eigencharacters. For integers $n \geqq 1$ and $k \geqq 0$, we denote by $M_k(\Gamma_n)$ the vector space over the complex number field $\boldsymbol{C}$ consisting of all Siegel modular forms of degree n and weight k. The space of cusp forms is $S_k(\Gamma_n) = \mathrm{Ker}\,(\Phi : M_k(\Gamma_n) \to M_k(\Gamma_{n-1}))$, where Φ is the Siegel operator. As usual we understand that $M_k(\Gamma_0) = S_k(\Gamma_0) = \boldsymbol{C}$ for $k \geqq 0$; see § 3 for Siegel modular forms of degree zero. For each integer $n \geqq 1$, we denote by $L = L^{(n)}$ the abstract Hecke algebra of degree n over $\boldsymbol{C}$ as in Andrianov [1, § 1.3]. For each integer $k \geqq 0$, we denote by $\tau = \tau_k^{(n)} : L \to \mathrm{End}_{\boldsymbol{C}}(M_k(\Gamma_n))$ the representation of L on $M_k(\Gamma_n)$ defined in Andrianov [1, (1.3.3)]. We denote by $\boldsymbol{T} = \boldsymbol{T}(M_k(\Gamma_n)) = \tau(L)$ the $\boldsymbol{C}$-algebra of all Hecke operators on $M_k(\Gamma_n)$. We put $\hat{\boldsymbol{T}} = \mathrm{Hom}_{\boldsymbol{C}}(\boldsymbol{T}, \boldsymbol{C})$ ($\boldsymbol{C}$-algebra homomorphisms), and for each $\lambda \in \hat{\boldsymbol{T}}$ we put $M_k(\Gamma_n; \lambda) = \{f \in M_k(\Gamma_n) \mid Tf = \lambda(T)f \text{ for all } T \in \boldsymbol{T}\}$ and $m(\lambda) = \dim_{\boldsymbol{C}} M_k(\Gamma_n; \lambda)$ the "multiplicity" of λ. We denote by $\Lambda(\boldsymbol{T}) = \{\lambda \in \hat{\boldsymbol{T}} \mid m(\lambda) \geqq 1\}$ the set of all "eigencharacters" of $\boldsymbol{T}$. Then ${}^{\#}\Lambda(\boldsymbol{T}) \leqq \dim_{\boldsymbol{C}} M_k(\Gamma_n)$, where ${}^{\#}\Lambda(\boldsymbol{T})$ denotes the cardinality of $\Lambda(\boldsymbol{T})$. A formulation of the "multiplicity one conjecture" is that $m(\lambda) = 1$ for all $\lambda \in \Lambda(\boldsymbol{T})$. This is equivalent to the following equality ${}^{\#}\Lambda(\boldsymbol{T}) = \dim_{\boldsymbol{C}} M_k(\Gamma_n)$, since we have $M_k(\Gamma_n) = \oplus_\lambda M_k(\Gamma_n; \lambda)$ and $\dim_{\boldsymbol{C}} M_k(\Gamma_n) = \sum_\lambda m(\lambda)$ where λ runs over $\Lambda(\boldsymbol{T})$. We say that a modular form f in $M_k(\Gamma_n)$ is an eigen modular form (or "eigenform") if f is a non-zero modular form belonging to $M_k(\Gamma_n; \lambda)$ for a $\lambda \in \Lambda(\boldsymbol{T})$. Such a λ is uniquely determined by f, and we denote it by $\lambda(f)$. In this case we denote by $\lambda(T, f)$ the value of $\lambda(f)$ at $T \in \boldsymbol{T}$: $Tf = \lambda(T, f)f$. We write $\lambda(m, f) = \lambda(T(m), f)$ for each integer $m \geqq 1$, where $T(m) \in \boldsymbol{T}$ is the Hecke operator studied by Maass [8] normalized as in Andrianov [1, (1.3.15)].

The Fourier expansion of a modular form f in $M_k(\Gamma_n)$ is denoted by $f = \sum_{T \geqq 0} a(T, f) q^T$ with $q^T = \exp(2\pi\sqrt{-1} \cdot \mathrm{trace}\,(TZ))$ where Z is a variable on the Siegel upper half space of degree n and T runs over all $n \times n$ symmetric semi-integral positive semi-definite matrices. Let R be a subring of $\boldsymbol{C}$. We put $M_k(\Gamma_n)_R = \{f \in M_k(\Gamma_n) \mid a(T, f) \in R \text{ for all } T \geqq 0\}$ (an R-module) and $M_k(\Gamma_n; \lambda)_R = M_k(\Gamma_n; \lambda) \cap M_k(\Gamma_n)_R$ (an R-

module) for each $\lambda \in \hat{\boldsymbol{T}}$ ($\boldsymbol{T}=\boldsymbol{T}(M_k(\Gamma_n))$). We denote by $L_R=L_R^{(n)}$ the abstract Hecke algebra of degree n over R, and we put $\boldsymbol{T}_R=\boldsymbol{T}_R(M_k(\Gamma_n))=\tau(L_R)$ (an R-algebra). For each $\lambda \in \hat{\boldsymbol{T}}$ we denote by λ_R the restriction of λ on $\boldsymbol{T}_R$, and we put $\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(\mathrm{Image}\,(\lambda_{\boldsymbol{Q}}))=\boldsymbol{Q}(\lambda(\boldsymbol{T}_{\boldsymbol{Q}}))$ (an extension field of $\boldsymbol{Q}$) and $\boldsymbol{Z}(\lambda)=\boldsymbol{Q}(\lambda)\cap\bar{\boldsymbol{Z}}$ (=the integral closure of $\boldsymbol{Z}$ in $\boldsymbol{Q}(\lambda)$), where $\boldsymbol{Q}$ is the rational number field, $\boldsymbol{Z}$ is the rational integer ring, and $\bar{\boldsymbol{Z}}$ is the ring of all algebraic integers in $\boldsymbol{C}$.

Theorem 1. *Let* $\lambda \in \Lambda(\boldsymbol{T}(M_k(\Gamma_n)))$ *for* $n\geqq 1$ *and even* $k\geqq 0$. *Then*:

(1) $\boldsymbol{Q}(\lambda)$ *is a totally real finite extension of* $\boldsymbol{Q}$.

(2) $\mathrm{Image}\,(\lambda_{\boldsymbol{Z}})\subset \boldsymbol{Z}(\lambda)$ *for* $n\leqq 2$.

Before the proof of Theorem 1, we note the following facts.

(A) $M_k(\Gamma_n)_{\boldsymbol{Z}}\otimes_{\boldsymbol{Z}}\boldsymbol{C}=M_k(\Gamma_n)$ for $n\geqq 1$ and even $k\geqq 0$.

(B) $M_k(\Gamma_n)_{\boldsymbol{Q}}$ is stable under $\boldsymbol{T}_{\boldsymbol{Q}}$ for $n\geqq 1$ and $k\geqq 0$.

(B*) $M_k(\Gamma_n)_{\boldsymbol{Z}}$ is stable under $\boldsymbol{T}_{\boldsymbol{Z}}$ for $n\leqq 2$ and $k\geqq 0$.

The fact (A) is proved in Eichler [3] and Baily [2]; see Igusa [4, Introduction]. Here we note the following easily proved fact: let R be a subring of $\boldsymbol{C}$, K the quotient field of R, and $\boldsymbol{f}=\{f_1,\cdots,f_r\}$ a finite subset of $M_k(\Gamma_n)_R$ for $n\geqq 1$ and $k\geqq 0$, then the following are equivalent: (1) $\boldsymbol{f}$ is linearly independent over R, (2) $\boldsymbol{f}$ is linearly independent over K, (3) $\boldsymbol{f}$ is linearly independent over $\boldsymbol{C}$. The fact (B) follows from Maass [8, (62) (63)] and Žarkovskaja [9, (2.4)]. For $n=1$, (B*) is well-known, and for n=2, (B*) follows from Andrianov [1, (2.1.11)]. We note that (B*) seems to hold for $n\geqq 3$ also if $k\geqq n$. (Since $M_k(\Gamma_n)=0$ for $n\leqq 2$ and $k<n$, we do not need the condition $k\geqq n$ in the above (B*) for $n\leqq 2$, but we would need this condition in the general case containing the case of level$>$1.)

Proof of Theorem 1. We denote by Aut $(\boldsymbol{C})$ the group of all field-automorphisms of $\boldsymbol{C}$. Take a $\sigma\in\mathrm{Aut}\,(\boldsymbol{C})$. For each $f=\sum_{T\geqq 0}a(T,f)q^T \in M_k(\Gamma_n)$ we put $\sigma(f)=\sum_{T\geqq 0}\sigma(a(T,f))q^T$. By (A), $\sigma(f)$ belongs to $M_k(\Gamma_n)$. For each $\lambda\in\hat{\boldsymbol{T}}$ we define $\sigma(\lambda)\in\hat{\boldsymbol{T}}$ by $\sigma(\lambda)(T)=\sigma(\lambda(T))$ for each $T\in\boldsymbol{T}_{\boldsymbol{Q}}$ and using $\boldsymbol{T}=\boldsymbol{T}_{\boldsymbol{Q}}\otimes_{\boldsymbol{Q}}\boldsymbol{C}$. For $f\in M_k(\Gamma_n)$ and $T\in\boldsymbol{T}_{\boldsymbol{Q}}$, we have $\sigma(Tf)=T(\sigma(f))$ by (B). In particular, for each $f\in M_k(\Gamma_n;\lambda)$ with $\lambda\in\hat{\boldsymbol{T}}$, we have $\sigma(f)\in M_k(\Gamma_n;\sigma(\lambda))$. Hence, if $\lambda\in\Lambda(\boldsymbol{T})$, then $\sigma(\lambda)\in\Lambda(\boldsymbol{T})$ and $\sigma(\boldsymbol{Q}(\lambda))=\boldsymbol{Q}(\sigma(\lambda))$. Since $\Lambda(\boldsymbol{T})$ is a finite set, $\boldsymbol{Q}(\lambda)$ is a finite extension of $\boldsymbol{Q}$ for each $\lambda\in\Lambda(\boldsymbol{T})$. Since $\mathrm{Image}\,(\lambda_{\boldsymbol{Q}})\subset\boldsymbol{R}$ for all $\lambda\in\Lambda(\boldsymbol{T})$ where $\boldsymbol{R}$ is the real number field (this fact follows from the hermiteness of Hecke operators in $\boldsymbol{T}_{\boldsymbol{Q}}$ (or $\boldsymbol{T}_{\boldsymbol{R}}$), see Andrianov [1, Theorem 1.3.4]), $\boldsymbol{Q}(\lambda)$ is a totally real extension of $\boldsymbol{Q}$ for each $\lambda\in\Lambda(\boldsymbol{T})$. This proves (1). To prove (2) we take a $\boldsymbol{Z}$-basis $\{h_1,\cdots,h_r\}$ of $M_k(\Gamma_n)_{\boldsymbol{Z}}$. By (A), this is a $\boldsymbol{C}$-basis of $M_k(\Gamma_n)$. Put $\boldsymbol{h}={}^t(h_1,\cdots,h_r)$, and take a $T\in\boldsymbol{T}_{\boldsymbol{Z}}$. Since $\boldsymbol{T}_{\boldsymbol{Z}}\subsetneq\mathrm{End}_{\boldsymbol{Z}}\,(M_k(\Gamma_n)_{\boldsymbol{Z}})$ for $n\leqq 2$ by (B*), we have $T\boldsymbol{h}=M\boldsymbol{h}$ with a matrix $M\in M(r,\boldsymbol{Z})$. Hence $\det\,(X-M)=\prod_\lambda(X-\lambda(T))^{m(\lambda)}$ is a monic polynomial in $Z[X]$, where X is an indeterminate and λ runs over $\Lambda(T)$. Hence $\lambda(T) \in \bar{Z}$. So we have (2). Q.E.D.

Theorem 2. *Let $\lambda \in \Lambda(T(M_k(\Gamma_n)))$ for $n \geqq 1$ and even $k \geqq 0$. Then:* $M_k(\Gamma_n;\lambda)_{Z(\lambda)} \otimes_{Z(\lambda)} C = M_k(\Gamma_n;\lambda)$.

Proof. We take a Z-basis $\{h_1, \cdots, h_r\}$ of $M_k(\Gamma_n)_Z$, which is a C-basis of $M_k(\Gamma_n)$ by (A). For each $T \in T_Q$, $Th_i = \sum_{j=1}^r \beta_{ij}(T) h_j$ with $\beta_{ij}(T) \in Q$ by (B). For each vector $x = (x_1, \cdots, x_r) \in C^r$ we put $f(x) = \sum_{i=1}^r x_i h_i$. For each $\lambda \in \Lambda(T)$ we put $V(\lambda) = \{x \in C^r \mid f(x) \in M_k(\Gamma_n;\lambda)\}$ (a C-vector space), then $f: V(\lambda) \to M_k(\Gamma_n;\lambda)$ is a C-linear isomorphism and $\dim_C V(\lambda) = m(\lambda)$. By (B) we have $T_Q \subsetneq \mathrm{End}_Q(M_k(\Gamma_n)_Q)$, hence T_Q is a finite dimensional Q-algebra. We take a Q-basis S of T_Q, which is a finite set. We have: $x \in V(\lambda) \Leftrightarrow f(x) \in M_k(\Gamma_n;\lambda) \Leftrightarrow Tf(x) = \lambda(T)f(x)$ for all $T \in S$ $\Leftrightarrow \sum_{i=1}^r \beta_{ij}(T) x_i = \lambda(T) x_j$ for $j = 1, \cdots, r$ and $T \in S$. Since the coefficients $\lambda(T)$ and $\beta_{ij}(T)$ belong to $Q(\lambda)$, there exists a basis $\{a_1, \cdots, a_{m(\lambda)}\}$ of $V(\lambda)$ such that $a_j \in Q(\lambda)^r$. We take non-zero $\gamma_j \in Z(\lambda)$ such that $a_j^* = \gamma_j a_j \in Z(\lambda)^r$. Then $f(a_j^*) \in M_k(\Gamma_n;\lambda)_{Z(\lambda)}$ and $V(\lambda) = Ca_1^* \oplus \cdots \oplus Ca_{m(\lambda)}^*$. Hence we have Theorem 2. Q.E.D.

§ 2. Fourier coefficients of eigenforms. For each eigen modular form f in $M_k(\Gamma_n)$ for $n \geqq 1$ and $k \geqq 0$, we put $Q(f) = Q(\lambda(f))$ and $Z(f) = Z(\lambda(f))$. As a particular case of Theorem 2 we have the following

Theorem 3. *Let f be an eigen modular form in $M_k(\Gamma_n)$ for $n \geqq 1$ and even $k \geqq 0$. Assume that $m(\lambda(f)) = 1$. Then there exists a non-zero constant $\gamma \in C$ such that γf belongs to $M_k(\Gamma_n)_{Z(f)}$.*

We refer to [5]–[7] for examples satisfying the assumption in Theorem 3. Here we pose a problem. Let $k \geqq 0$ be an integer, and let $\boldsymbol{f} = (f_n \mid n(1) \leqq n < n(2))$ be a system of eigen modular forms $f_n \in M_k(\Gamma_n)$ satisfying $\Phi f_n = f_{n-1}$ for $n(1) < n < n(2)$, where $0 \leqq n(1) < n(2) \leqq \infty$ including$n(2) = \infty$. We call such a system $\boldsymbol{f}$ as an "eigensystem" of "length" $\ell(\boldsymbol{f}) = n(2) - n(1) - 1$. We denote by $Q(\boldsymbol{f})$ the composite field of $Q(f_n)$ for all n, and put $Z(\boldsymbol{f}) = Q(\boldsymbol{f}) \cap \bar{Z}$. (Possibly, $Q(\boldsymbol{f}) = Q(f_n)$ and $Z(\boldsymbol{f}) = Z(f_n)$ for each n.) Assume that $\ell(\boldsymbol{f}) < \infty$, $m(\lambda(f_n)) = 1$ for all n, and k is even. Then, by Theorem 3, there exists a non-zero constant $\gamma \in C$ such that $\gamma f_n \in M_k(\Gamma_n)_{Z(\boldsymbol{f})}$ for all n. Does this hold without the above assumptions (in particular, for the case $\ell(\boldsymbol{f}) = \infty$)? We may assume that $\boldsymbol{f}$ is "maximal" in the following sense: $\Phi(f_{n(1)}) = 0$ and when $n(2) < \infty$ there exists no eigen modular form $g \in M_k(\Gamma_{n(2)})$ satisfying $\Phi(g) = f_{n(2)-1}$.

§ 3. Siegel modular forms of degree zero. For our purpose, it is convenient to include Siegel modular forms of degree zero. The following may be considered as definitions. For each integer $k \geqq 0$, $M_k(\Gamma_0) = S_k(\Gamma_0) = C$. The Hecke algebra $L^{(0)} = C$ acts on $M_k(\Gamma_0) = C$ by multiplication, $T = T(M_k(\Gamma_0)) \cong C$, $\Lambda(T) = \{I\}$, $Q(I) = Q$, and $Z(I) = Z$, where $I: \boldsymbol{T} \to \boldsymbol{C}$ is the natural isomorphism (the identity map). For each subring R of $\boldsymbol{C}$, $M_k(\Gamma_0)_R = S_k(\Gamma_0)_R = R$, $L_R^{(0)} = R$, and $\boldsymbol{T}_R = \boldsymbol{T}_R(M_k(\Gamma_0)) \cong R$. A modular form $f \in M_k(\Gamma_0)$ is eigen if and only if $f \neq 0$. If f is eigen, then $\lambda(f) = I$, $\boldsymbol{Q}(f) = \boldsymbol{Q}$, $\boldsymbol{Z}(f) = \boldsymbol{Z}$, and the L-function is $L(s, f) = \sum_{m \geq 1} \lambda(T(m), f) m^{-s} = \prod_p (1 - \lambda(T(p), f) p^{-s})^{-1} = \zeta(s)$ where $T(m) = 1$ and $\lambda(T(m), f) = 1$ for each integer $m \geq 1$ and p runs over all prime numbers. Then, Theorems 1–3 hold trivially for the case of degree zero.

§ 4. **Congruences.** Let $\lambda^{(1)}$ and $\lambda^{(2)}$ be eigencharacters of $\boldsymbol{T}(M_k(\Gamma_n))$ for integers $n \geq 0$ and $k \geq 0$. Let $K = \boldsymbol{Q}(\lambda^{(1)})\boldsymbol{Q}(\lambda^{(2)})$ be the composite field, and $\mathcal{O}$ the integer ring of K. For an ideal $\mathfrak{c}$ of $\mathcal{O}$, we write $\lambda^{(1)} \equiv \lambda^{(2)}$ mod $\mathfrak{c}$ if Image $(\lambda_{\boldsymbol{Z}}^{(1)} - \lambda_{\boldsymbol{Z}}^{(2)}) \subset \tilde{\mathfrak{c}}$, where $\tilde{\mathfrak{c}} = \{\alpha/\beta \mid \alpha \in \mathfrak{c}, \beta \in \mathcal{O}, ((\beta), \mathfrak{c}) = \mathcal{O}\} \subset K$ is an $\mathcal{O}$-module. For $n \leq 2$, this is equivalent to Image $(\lambda_{\boldsymbol{Z}}^{(1)} - \lambda_{\boldsymbol{Z}}^{(2)}) \subset \mathfrak{c}$ by Theorem 1(2).

In the following table, we note two examples of congruences; one is Ramanujan's congruence, and the other is Theorem 1 of [6].

	degree 0	degree 1	degree 2
L-functions	$691 \mid \zeta^*(12)$	$71^2 \mid L_2^*(38, \Delta_{20})$	
congruences		$\lambda(\Delta_{12}) \equiv \lambda(E_{12})$ mod 691	$\lambda(\chi_{20}^{(3)}) \equiv \lambda([\Delta_{20}])$ mod 71^2

Here we used the notations of [5] and [6], and we put $\zeta^*(s) = \zeta(s)(2\pi)^{-s}\Gamma(s)$; for each even integer $k \geq 2$, we have $\zeta^*(k) = (-1)^{1+k/2} \cdot B_k/2k$, where B_k is the k-th Bernoulli number. These congruences may suggest the higher degree cases.

References

[1] A. N. Andrianov: Euler products corresponding to Siegel modular forms of genus 2. Russian Math. Surveys, **29**, 45–116 (1974) (English translation).
[2] W. L. Baily: Automorphic forms with integral Fourier coefficients. Lect. Notes in Math., vol. 155, Springer-Verlag, pp. 1–8 (1970).
[3] M. Eichler: Zur Begründung der Theorie der automorphen Funktionen in mehreren Variablen. Aequationes Math., **3**, 93–111 (1969).
[4] J. Igusa: On the ring of modular forms of degree two over $\boldsymbol{Z}$. Amer. J. Math., **101**, 149–183 (1979).
[5] N. Kurokawa: Examples of eigenvalues of Hecke operators on Siegel cusp forms of degree two. Invent. Math., **49**, 149–165 (1978).
[6] ——: Congruences between Siegel modular forms of degree two. Proc. Japan Acad., **55**A, 417–422 (1979).
[7] ——: On Eisenstein series for Siegel modular groups. ibid., **57**A, 51–55 (1981).
[8] H. Maass: Die Primzahlen in der Theorie der Siegelschen Modulfunktionen. Math. Ann., **124**, 87–122 (1951).
[9] N. A. Žarkovskaja: On the connection of the eigenvalues of Hecke operators and the Fourier coefficients of eigenfunctions for Siegel's modular forms of genus n. Math. USSR Sbornik, **25**, 549–557 (1975) (English translation).