Rev. Mat. Iberoamericana **22** (2006), no. 1, 357–368

On Hilbert modular forms modulo p: explicit ring structure

Shoyu Nagaoka

Abstract

H. P. F. Swinnerton-Dyer determined the structure of the ring of modular forms modulo p in the elliptic modular case. In this paper, the structure of the ring of Hilbert modular forms modulo p is studied. In the case where the discriminant of corresponding quadratic field is 8 (or 5), the explicit structure is determined.

1. Introduction

In [9] Swinnerton-Dyer determined the structure of the ring of modular forms modulo p in the elliptic modular case. The result has been applied in several fields in the theory of modular forms, for example, the $p-$adic theory of modular forms (e.g. cf. Serre [8]). In this note, we try to generalize the result to the case of symmetric Hilbert modular forms for real quadratic fields of small discriminant. We have already developed a generalization in the Siegel modular case of degree 2, which is important in our proof (cf. Theorem 4.1). A geometric approach has been developed in recent studies by E. Goren (for example, [3] and [4]).

2. Hilbert modular forms for a real quadratic field

Let $\mathbb{K}$ be a real quadratic field with the discriminant $d_{\mathbb{K}}$ and the ring of integers $\mathcal{O}_{\mathbb{K}}$. We denote by $\mathbb{H}$ the upper-half plane in $\mathbb{C}$. The Hilbert modular group $\Gamma_{\mathbb{K}} := SL(2, \mathcal{O}_{\mathbb{K}})$ acts on $\mathbb{H}^2 = \mathbb{H} \times \mathbb{H}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ (z_1,\, z_2) := \left(\frac{az_1 + b}{cz_1 + d},\, \frac{\bar{a}z_2 + \bar{b}}{\bar{c}z_2 + \bar{d}} \right),$$

where $\bar{x}$ denotes the conjugation of $x \in \mathbb{K}$ over $\mathbb{Q}$.

2000 Mathematics Subject Classification: 11F41.
Keywords: Hilbert modular forms, modular forms mod p.

Let $A_{\mathbb{C}}(\Gamma_{\mathbb{K}})_k$ be the complex vector space of symmetric Hilbert modular forms of parallel weight k for $\Gamma_{\mathbb{K}}$. Each element $f(\tau)$ of $A_{\mathbb{C}}(\Gamma_{\mathbb{K}})_k$ admits a Fourier expansion of the form

$$f(\tau) = \sum_{0 \ll \nu \in \mathfrak{d}_{\mathbb{K}}^{-1}} a_f(\tau) \exp\left[2\pi\sqrt{-1}\mathrm{tr}(\nu\tau)\right],$$

where $\tau = (z_1,\ z_2) \in \mathbb{H}^2$, $\mathrm{tr}(\nu\tau) = \nu z_1 + \bar{\nu} z_2$ and the summation is extended over the elements ν in the inverse different $\mathfrak{d}_{\mathbb{K}}^{-1}$ which are semi-totally positive.

From now on, we restrict ourselves to the case

$$\mathbb{K} = \mathbb{Q}(\sqrt{2}).$$

(There is another case $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ where our discussion leads to similar results: cf. section 5, Remark (2)).

In this case, we have $d_{\mathbb{K}} = 8$ and $\mathfrak{d}_{\mathbb{K}} = 2\sqrt{2}\mathcal{O}_{\mathbb{K}}$. We fix an integral basis $\{1,\ \sqrt{2}\}$ and introduce new variables:

$$x =: \exp\left[\pi\sqrt{-1}(z_1 - z_2)/\sqrt{2}\right],\ q = \exp\left[\pi\sqrt{-1}(z_1 + z_2)\right].$$

Then, the above Fourier expansion is rewritten as

$$\begin{aligned} f(\tau) &= \sum_{\nu = (\alpha + \beta\sqrt{2})/2\sqrt{2} \gg 0} a_f(\nu) x^\alpha q^\beta \\ &= a_f(0) + a_f((-1+\sqrt{2})/2\sqrt{2})x^{-1}q + a_f(1/2)q + a_f((1+\sqrt{2})/2\sqrt{2})xq \\ &\quad + a_f((-2+2\sqrt{2})/2\sqrt{2})x^{-2}q^2 + a_f((-1+2\sqrt{2})/2\sqrt{2})x^{-1}q^2 + a_f(1)q^2 \\ &\quad + a_f((1+2\sqrt{2})/2\sqrt{2})xq^2 + a_f((2+2\sqrt{2})/2\sqrt{2})x^2q^2 + \cdots. \end{aligned}$$

By semi-positivity of ν, we may regard f as an element of formal power series ring $\mathbb{C}\left[x^{-1}, x\right] [\![q]\!]$. For a subring R in $\mathbb{C}$,

$$A_R(\Gamma_{\mathbb{K}})_k := \{f \in A_{\mathbb{C}}(\Gamma_{\mathbb{K}})_k \mid a_f(\nu) \in R \text{ for all } \nu\} \subset R\left[x^{-1}, x\right] [\![q]\!]$$

and

$$A_R^{(m)}(\Gamma_{\mathbb{K}}) := \bigoplus_{k \geq 0} A_R(\Gamma_{\mathbb{K}})_{km}.$$

For an even positive integer k, we can define the normalized Eisenstein series of weight k for $\Gamma_{\mathbb{K}}$ whose Fourier expansion is

$$G_k(\tau) = 1 + \kappa_k \sum_{\substack{\nu \in \mathfrak{d}_{\mathbb{K}}^{-1} \\ 0 \neq \nu \gg 0}} \sigma_{k-1}(\nu) \exp\left[2\pi\sqrt{-1}\mathrm{tr}(\nu\tau)\right] \tag{2.1}$$

where

$$\kappa_k := \zeta_{\mathbb{K}}(k)^{-1} \cdot (2\pi)^{2k} \cdot [(k-1)!]^{-2} \cdot d_{\mathbb{K}}^{1/2-k},$$
$$\sigma_{k-1}(\nu) := \sum_{(\nu)\mathfrak{d}_{\mathbb{K}} \subset \mathfrak{b}} |N(\mathfrak{b})|^{k-1}.$$

Since $\kappa_k \in \mathbb{Q}$, we have $G_k \in A_{\mathbb{Q}}(\Gamma_{\mathbb{K}})_k$.

Let $E_k(z)$ be the normalized Eisenstein series of weight k for $SL(2,\mathbb{Z})$, and let $\Delta(z)$ be a cusp form defined by

$$\Delta(z) = 2^{-6} \cdot 3^{-3} \, (E_4^3(z) - E_6^2(z)).$$

It is well-known that

$$E_k \in A_{\mathbb{Q}}(SL(2,\mathbb{Z}))_k \quad \text{and} \quad \Delta \in A_{\mathbb{Z}}(SL(2,\mathbb{Z}))_{12}.$$

For a function $f((z_1,z_2))$ on $\mathbb{H}^2$, we define a function on $\mathbb{H}$ by

$$\mathbb{D}(f)(z) := f((z,z)).$$

By the definiton of Hilbert modular form, we see that the map $\mathbb{D}$ induces an $R-$linear map

$$\mathbb{D} \, : \, A_R(\Gamma_{\mathbb{K}})_k \longrightarrow A_R(SL(2,\mathbb{Z}))_{2k}.$$

In fact, if

$$f(\tau) = \sum a_f(\nu) \exp\left[2\pi\sqrt{-1}\mathrm{tr}(\nu\tau)\right]$$

in $A_R(\Gamma_{\mathbb{K}})_k$, then the Fourier expansion of $\mathbb{D}(f)$ is

$$\mathbb{D}(f)(z) = \sum_{n=0}^{\infty} c_f(n) \exp\left[2\pi\sqrt{-1}nz\right], \; c_f(n) = \sum_{\mathrm{tr}(\nu)=n} a_f(\nu).$$

Put

$$\begin{aligned} H_2 :=& \quad G_2 \\ =& \quad 1 + 2^4 \cdot 3\{(x^{-1}+3+x)q+ \\ & \qquad +(7x^{-2}+8x^{-1}+15+8x+7x^2)q^2+\cdots\}, \end{aligned}$$

(2.2)
$$\begin{aligned} H_4 :=& \quad 2^{-6} \cdot 3^{-2} \cdot 11(G_2^2 - G_4) \\ =& \quad (x^{-1}-2+x)q + (-4x^{-2}-8x^{-1}+24-8x-4x^2)q^2 \cdots, \end{aligned}$$

$$\begin{aligned} H_6 :=& \quad -2^{-8} \cdot 3^{-3} \cdot 13^{-1} \cdot 5 \cdot 7^2 G_2^3 - 2^{-7} \cdot 3^{-3} \cdot 5^{-1} \cdot 13^{-1} 19^2 G_6 \\ & \quad +2^{-8} \cdot 3^{-2} \cdot 5^{-1} \cdot 13^{-1} \cdot 11 \cdot 59 G_2 G_4 \\ =& \quad q + (-2x^{-2}-16x^{-1}+12-16x-2x^2)q^2+\cdots . \end{aligned}$$

Proposition 2.1 *Let $\mathbb{Z}_{(p)}$ be the local ring at p (p : prime).*

(1) $H_k \in A_{\mathbb{Z}}(\Gamma_{\mathbb{K}})_k \subset A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_k$ *(k=2, 4, 6) and*

$$\mathbb{D}(H_2) = E_4,\ \mathbb{D}(H_4) = 0,\ \mathbb{D}(H_6) = \Delta.$$

(2) If $f \in A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_k$, *($k$: even), then there exists a polynomial* $P(X_1, X_2, X_3) \in \mathbb{Z}_{(p)}[X_1, X_2, X_3]$ *satisfying*

$$f = P(H_2, H_4, H_6).$$

Namely,

$$A^{(2)}_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}}) = \mathbb{Z}_{(p)}[H_2, H_4, H_6].$$

Proposition 2.2 *([6, Propositions 3.1, 3.2])*

(1) There exists an odd weight form H_9 with integral Fourier coefficients:

$$H_9 = q - (96^{-1}x + 336 + 96x)q^2 + \cdots \in A_{\mathbb{Z}}(\Gamma_{\mathbb{K}})_9 \subset A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_9.$$

(2) If k is odd, then $A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_k = H_9 \cdot A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_{k-9}$.

(3) H_9^2 has a polynomial expression in H_2,H_4, and H_6:

$$H_9^2 = H_2^3 H_6^2 + 2^2 H_2^2 H_4^2 H_6 - 2^5 \cdot 3^2 H_2 H_4 H_6^2 - 2^{10} H_4^3 H_6 - 2^6 \cdot 3^3 H_6^3. \tag{2.3}$$

3. Siegel modular form and modular embedding

Let $A_{\mathbb{C}}(\Gamma_{\mathbb{K}})_k$ be the complex vector space of Siegel modular forms of weight k for $\Gamma_n := Sp(n, \mathbb{Z})$. As is well known, each element $F(Z)$ in $A_{\mathbb{C}}(\Gamma_n)_k$ admits a Fourier expansion of the form

$$F(Z) = \sum_{T \geq 0} a_F(T) \exp\left[2\pi\sqrt{-1}\mathrm{tr}(TZ)\right],\ Z \in \mathbb{H}_n,$$

where $\mathbb{H}_n$ is the Siegel upper-half space of degree n and the summation is extended over all half-integral, positive semi-definite, symmetric matrices of degree n. As in the previous case, we can define an $R-$module $A_R(\Gamma_n)_k$.

We now introduce a modular embedding from $A_{\mathbb{C}}(\Gamma_{\mathbb{K}})_k$ ($\mathbb{K} = \mathbb{Q}(\sqrt{2})$) to $A_{\mathbb{C}}(\Gamma_2)_k$.

We fix a fundamental unit $\varepsilon = 1 + \sqrt{2}$ in $\mathcal{O}_{\mathbb{K}}$ and define a matrix A by

$$A = \begin{pmatrix} \alpha & \bar{\alpha} \\ \bar{\alpha} & -\alpha \end{pmatrix},\ \alpha = \sqrt{\varepsilon/2\sqrt{2}},\ \bar{\alpha} = \sqrt{-\bar{\varepsilon}/2\sqrt{2}}.$$

First, we define a mapping $\Phi : \mathbb{H}^2 = \mathbb{H} \times \mathbb{H} \longrightarrow \mathbb{H}_2$ by

$$\begin{aligned} \Phi(\tau) = \Phi((z_1, z_2)) &:= A \begin{pmatrix} z_1 & 0 \\ 0 & z_2 \end{pmatrix} A \\ &= \begin{pmatrix} \mathrm{tr}((\varepsilon/2\sqrt{2})\tau) & \mathrm{tr}((1/2\sqrt{2})\tau) \\ \mathrm{tr}((1/2\sqrt{2})\tau) & \mathrm{tr}((-\bar{\varepsilon}/2\sqrt{2})\tau) \end{pmatrix}. \end{aligned} \tag{3.1}$$

Secondly, we define a mapping $\Psi : \Gamma_{\mathbb{K}} = SL(2, \mathcal{O}_{\mathbb{K}}) \longrightarrow \Gamma_2 = Sp(2, \mathbb{Z})$ by

$$\begin{aligned} \Psi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) &= \Psi\left(\begin{pmatrix} a_1 + a_2\sqrt{2} & b_1 + b_2\sqrt{2} \\ c_1 + c_2\sqrt{2} & d_1 + d_2\sqrt{2} \end{pmatrix}\right) \\ &= \begin{pmatrix} a_1 + a_2 & a_2 & b_1 + b_2 & b_2 \\ a_2 & a_1 - a_2 & b_2 & b_1 - b_2 \\ c_1 + c_2 & c_2 & d_1 + d_2 & d_2 \\ c_2 & c_1 - c_2 & d_2 & d_1 - d_2 \end{pmatrix}. \end{aligned} \tag{3.2}$$

Proposition 3.1 *([6, Proposition 2.1]) If F is a Siegel modular form in $A_{\mathbb{C}}(\Gamma_2)_k$, then $\Phi(F) = F \circ \Phi$ is a symmetric Hilbert modular form in $A_{\mathbb{C}}(\Gamma_{\mathbb{K}})_k$.*

We calculate the Fourier coefficient of $\Phi(F)$. Set

$$F(Z) = \sum_{T \geq 0} a_F(T) \exp\left[2\pi\sqrt{-1}\mathrm{tr}(TZ)\right].$$

We take a half-integral, positive semi-definite matrix

$$T = \begin{pmatrix} m & l/2 \\ l/2 & n \end{pmatrix}, \quad (m,\, n,\, l \in \mathbb{Z}).$$

Since

$$\exp\left[2\pi\sqrt{-1}\mathrm{tr}(T\Phi(\tau))\right] = x^{m-n+l} q^{m+n},$$

we have

$$\Phi(F)(\tau) = \sum_{(\alpha+\beta\sqrt{2})/2\sqrt{2} \gg 0} \left(\sum_{\substack{m-n+l=\alpha \\ m+n=\beta}} a_F\left(\begin{pmatrix} m & l/2 \\ l/2 & n \end{pmatrix}\right) \right) x^\alpha q^\beta. \tag{3.3}$$

Corollary 3.1 *Let R be a subring of $\mathbb{C}$. If $F \in A_R(\Gamma_2)_k$, then*

$$\Phi(F) \in A_R(\Gamma_{\mathbb{K}})_k.$$

4. Hilbert modular form modulo p

As before, p be a prime number, and let $\mathbb{Z}_{(p)}$ be the local ring at p. We set

$$\begin{aligned} A_{\mathbb{F}_p}(\Gamma_{\mathbb{K}})_k &:= \{\tilde{f} = \sum \widetilde{a_f(\nu)} x^\alpha q^\beta | f \in A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_k\} \\ &\subset \mathbb{F}_p\left[x^{-1}, x\right] [\![q]\!], \end{aligned}$$

where the tilde denotes the reduction modulo p. Let $A^{(m)}_{\mathbb{F}_p}(\Gamma_{\mathbb{K}})$ denote the subring of $\mathbb{F}_p\left[x^{-1}, x\right] [\![q]\!]$ generated by $A_{\mathbb{F}_p}(\Gamma_{\mathbb{K}})_k$ for $k = 0,\, m,\, 2m,\, 3m, \cdots$. The first theorem is as follows.

Theorem 4.1 (Existence Theorem) *Assume that* $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ *and* $p \geq 3$. *Then, there exists a Hilbert modular form* $f_{p-1} \in A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_{p-1}$ *satisfying*

$$f_{p-1} \equiv 1 \pmod{p},$$

where the congruence is the Fourier coefficientwise congruence.

Proof. First assume that $p \geq 5$. By [7, Theorem A] there exists a Siegel modular form $F_{p-1} \in A_{\mathbb{Z}_{(p)}}(\Gamma_2)_{p-1}$ satisfying

$$F_{p-1} \equiv 1 \pmod{p}.$$

If we set

$$f_{p-1} := \Phi(F_{p-1}),$$

then, by (3.3), we see that

$$f_{p-1} \in A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_{p-1}$$

has the desired property. When $p = 3$, we can take $f_{p-1} = f_2 = G_2$. ■

Remark. In the original (elliptic modular) case, it is easy to find such modular form: the weight $p-1$ Eisenstein series E_{p-1} satisfies $E_{p-1} \equiv 1 \pmod{p}$. However, the Hilbert-Eisenstein series G_{p-1} does not satisfy the congruence $G_{p-1} \equiv 1 \pmod{p}$ in general. In fact, $G_{12} \not\equiv 1 \pmod{13}$ (for example, [3, p. 373]).

In the following we shall determine the structure of $A^{(2)}_{\mathbb{F}_p}(\Gamma_{\mathbb{K}})$ under the condition

$$p \equiv 3 \pmod{4}.$$

Theorem 4.2 *Assume that* $\mathbb{K} = \mathbb{Q}(\sqrt{2})$.
(1) If $p \geq 5$ *is a prime number such that* $p \equiv 3 \pmod 4$, *then*

$$A^{(2)}_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_p\big[\tilde{H}_2, \tilde{H}_4, \tilde{H}_6\big]/(\tilde{A}_p(\tilde{H}_2, \tilde{H}_4, \tilde{H}_6) - 1)$$

where H_2, H_4, *and* H_6 *are generators of* $A^{(2)}_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})$ *(cf. Proposition 2.1) and* $A_p(X_1, X_2, X_3) \in \mathbb{Z}_{(p)}[X_1, X_2, X_3]$ *is a polynomial defined by*

$$f_{p-1} = A_p(H_2, H_4, H_6).$$

(2) If $p = 2$ *or* 3, *then*

$$A^{(2)}_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_p\big[\tilde{H}_4, \tilde{H}_6\big].$$

Proof. (1) We recall the identities

$$\mathbb{D}(H_2) = E_4, \quad \mathbb{D}(H_4) = 0, \quad \mathbb{D}(H_6) = \Delta$$

and consider the following diagram:

$$\begin{array}{ccccc}
\mathbb{Z}_{(p)}[X_1, X_2, X_3] & \longrightarrow & \mathbb{F}_p[X_1, X_2, X_3] & \xrightarrow{\varphi} & A^{(2)}_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) \\
{\scriptstyle \mathbb{D}'}\big\downarrow & & {\scriptstyle \tilde{\mathbb{D}}'}\big\downarrow & & {\scriptstyle \tilde{\mathbb{D}}}\big\downarrow \\
\mathbb{Z}_{(p)}[Y_1, Y_2] & \longrightarrow & \mathbb{F}_p[Y_1, Y_2] & \xrightarrow{\varphi'} & A^{(2)}_{\mathbb{F}_p}(SL(2,\mathbb{Z}))
\end{array}$$

where

$\varphi :$ $\quad \varphi(\tilde{P}(X_1, X_2, X_3)) := \tilde{P}(\tilde{H}_2, \tilde{H}_4, \tilde{H}_6)$.

$\varphi' :$ $\quad \varphi'(\tilde{Q}(Y_1, Y_2)) := \tilde{Q}(\tilde{E}_4, \tilde{E}_6)$.

$\mathbb{D}' :$ $\quad \mathbb{D}'(P(X_1, X_2, X_3)) := P(Y_1,\, 0,\, 2^{-6} \cdot 3^{-3}(Y_1^3 - Y_2^2))$.

$\tilde{\mathbb{D}}' :$ $\quad \tilde{\mathbb{D}}'(\tilde{P}(X_1, X_2, X_3)) := \tilde{P}(Y_1,\, 0,\, \tilde{a}(Y_1^3 - Y_2^2)), \quad \tilde{a} = 2^{-6} \cdot 3^{-3} \bmod p$.

$\tilde{\mathbb{D}} :$ $\quad \tilde{\mathbb{D}}(\tilde{f}) = \widetilde{\mathbb{D}(f)}, \quad \tilde{f} = \sum \widetilde{a_f(\nu)} x^\alpha q^\beta \in A_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) \subset \mathbb{F}_p[x^{-1}, x][\![q]\!]$.

By Proposition 2.1,(2), the map φ is surjective. For the Hilbert modular form f_{p-1}, we represent it as a polynomial in H_2, H_4, and H_6

$$f_{p-1} = A_p(H_2, H_4, H_6),\ A_p(X_1, X_2, X_3) \in \mathbb{Z}_{(p)}[X_1, X_2, X_3].$$

The congruence $f_{p-1} \equiv 1 \pmod p$ implies $\tilde{A}_p - 1 \in \mathrm{Ker}\varphi$. Therefore it suffices to show that

$$\mathrm{Ker}\varphi = (\tilde{A}_p - 1) \quad \text{(principal ideal)}.$$

To prove this, we first note that

$$\mathrm{Im}\tilde{\mathbb{D}} = A^{(4)}_{\mathbb{F}_p}(SL(2,\mathbb{Z})) \subset A^{(2)}_{\mathbb{F}_p}(SL(2,\mathbb{Z}))$$

and

$$\text{Krull } \dim A^{(4)}_{\mathbb{F}_p}(SL(2,\mathbb{Z})) = \text{Krull } \dim A^{(2)}_{\mathbb{F}_p}(SL(2,\mathbb{Z})) = 1.$$

The first identity in the second formula comes from the fact that $\tilde{E}_6$ is integral over $A^{(4)}_{\mathbb{F}_p}(SL(2,\mathbb{Z}))$. Since $\mathrm{Ker}\tilde{\mathbb{D}} \neq 0$ (for example, $0 \neq \tilde{H}_4 \in \mathrm{Ker}\tilde{\mathbb{D}}$), we have

$$\text{Krull } \dim A^{(2)}_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) = 2$$

Hence, the irreducibility of $\tilde{A}_p - 1$ implies our statement:

$$A^{(2)}_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_p\big[\tilde{H}_2, \tilde{H}_4, \tilde{H}_6\big]/(\tilde{A}_p(\tilde{H}_2, \tilde{H}_4, \tilde{H}_6) - 1)$$

We shall show *the irreducibility* under the condition $p \equiv 3 \pmod 4$. For this purpose, we recall the corresponding fact in the elliptic modular case. The normalized Eisenstein series E_{p-1} satisfies $E_{p-1} \equiv 1 \pmod p$. Moreover, if we represent E_{p-1} as

$$E_{p-1} = B_p(E_4, E_6) \qquad \text{with } B_p(Y_1, Y_2) \in \mathbb{Z}_{(p)}[Y_1, Y_2],$$

then $B_p(Y_1, Y_2) - 1$ is irreducible in $\mathbb{F}_p[Y_1, Y_2]$ (cf. [9]). From this fact, we get the decomposition

$$(4.1) \qquad \tilde{\mathbb{D}}'(\tilde{A}_p(X_1, X_2, X_3) - 1) = (\tilde{B}_p(Y_1, Y_2) + 1)(\tilde{B}_p(Y_1, Y_2) - 1).$$

Here, we note that both factors $\tilde{B}_p + 1$ and $\tilde{B}_p - 1$ are irreducible. Now we assume that $\tilde{A}_p - 1$ is reducible. Then, the shape of the decomposition must be

$$(4.2) \quad \tilde{A}_p - 1 = (\tilde{G}^{(a)} + \tilde{G}^{(a-1)} + \cdots + \tilde{G}^{(0)})(\tilde{H}^{(a)} + \tilde{H}^{(a-1)} + \cdots + \tilde{H}^{(0)}),$$

where $G^{(j)}$ (also $H^{(j)}$) is a polynomial consisting of terms such as

$$a_{\alpha\beta\gamma} X_1^{\alpha} X_2^{\beta} X_3^{\gamma}$$

with $2\alpha + 4\beta + 6\gamma = j$, namely, terms of isobaric degree j. Combining (4.1) and (4.2), we have $2a = p-1$. Since a is even, the prime p must be congruent to one modulo 4. This contradicts our assumption. (2) If $p = 2$ or 3, then $\tilde{H}_2 = 1$. Moreover, $\tilde{H}_4$ and $\tilde{H}_6$ are algebraically independent because the Fourier expansion of H_4 (resp. H_6) starts at the term $(x^{-1} - 2 + x)q$ (resp. q). ■

From the above result and Proposition 2.2, we can easily determine the structure of the whole ring $A_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) = A^{(1)}_{\mathbb{F}_p}(\Gamma_{\mathbb{K}})$.

Set

$$\begin{aligned} C(X_1, X_2, X_3, X_4) := {} & X_1^3 X_3^2 + 2^2 X_1^2 X_2^2 X_3 - 2^5 \cdot 3^2 X_1 X_2 X_3^2 - 2^{10} X_2^3 X_3 \\ & - 2^6 \cdot 3^3 X_3^3 - X_4^2 \in \mathbb{Z}[X_1, X_2, X_3, X_4] \end{aligned}$$

It should be noted that the polynomial is chosen as

$$C(H_2, H_4, H_6, H_9) = 0, \quad \text{(cf. (2.3))}.$$

Let $\tilde{C}_p(X_1, X_2, X_3, X_4) \in \mathbb{F}_p[X_1, X_2, X_3, X_4]$ be the reduction modulo p. Combining this and Theorem 4.2, we obtain the following:

Theorem 4.3 *Assume that* $\mathbb{K} = \mathbb{Q}(\sqrt{2})$.

(1) If $p \geq 5$ *and* $p \equiv 3 \pmod 4$, *then*

$$A_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_p\big[\tilde{H}_2, \tilde{H}_4, \tilde{H}_6, \tilde{H}_9\big]/(\tilde{A}_p(\tilde{H}_2, \tilde{H}_4, \tilde{H}_6) - 1, \tilde{C}_p(\tilde{H}_2, \tilde{H}_4, \tilde{H}_6, \tilde{H}_9)).$$

(2) If $p = 2$ *or* 3,

$$A_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_p\big[\tilde{H}_4, \tilde{H}_6, \tilde{H}_9\big]/(\tilde{C}_p),$$

that is

$$\begin{aligned} A_{\mathbb{F}_3}(\Gamma_{\mathbb{K}}) &\cong \mathbb{F}_3\big[\tilde{H}_4, \tilde{H}_6, \tilde{H}_9\big]/(\tilde{H}_6^2 + \tilde{H}_4^2 \tilde{H}_6 + 2\tilde{H}_6 + 2\tilde{H}_9^2), \\ A_{\mathbb{F}_2}(\Gamma_{\mathbb{K}}) &= \mathbb{F}_2\big[\tilde{H}_4, \tilde{H}_6\big] = \mathbb{F}_2\big[\tilde{H}_4, \tilde{H}_9\big]. \end{aligned}$$

5. Remark

(1) Case $p \equiv 1 \pmod 4$:

In the above discussion, the result was restricted to the case $p \equiv 3 \pmod 4$. What about the case $p \equiv 1 \pmod 4$? In this case also, the irreducibility of $\tilde{A}_p - 1$ produces similar results. The first few examples show the irreducibility.

$\boxed{p = 5:}$ $\tilde{A}_5 - 1 = X_1^2 + 4X_2 - 1$, $\mathbb{D}'(\tilde{A}_5 - 1) = Y_1^2 - 1$, $\tilde{B}_5 - 1 = Y_1 - 1$.

$p = 7$: $\tilde{A}_7 - 1 = X_1^3 + 3X_1X_2 + X_3 - 1$, $\mathbb{D}'(\tilde{A}_7 - 1) = Y_2^2 - 1$, $\tilde{B}_7 - 1 = Y_2 - 1$.

$p = 11$: $\tilde{A}_{11} - 1 = X_1^5 + 2X_1^3X_2 + 10X_1^2X_3 + X_1X_2^2 + X_2X_3 - 1$, $\mathbb{D}'(\tilde{A}_{11} - 1) = Y_1^2Y_2^2 - 1$, $\tilde{B}_{11} - 1 = Y_1Y_2 - 1$.

$\boxed{p = 13:}$ $\tilde{A}_{13} - 1 = X_1^6 + 11X_1^4X_2 + 3X_1^3X_3 + 11X_1^2X_2^2 + 2X_1X_2X_3 + 10X_2^3 + 12X_3^2 - 1$,

$\mathbb{D}'(\tilde{A}_{13} - 1) = 10Y_1^6 + 5Y_1^3Y_2^2 + 12Y_2^4 - 1$, $\tilde{B}_{13} - 1 = 6Y_1^3 + 8Y_2^2 - 1$.

(2) Case for $\mathbb{K} = \mathbb{Q}(\sqrt{5})$:

The proposed method is applicable for the case $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. In this paper, we present the statement without proof.

Let G_k be the normalized Eisenstein series of weight k for $\Gamma_{\mathbb{Q}(\sqrt{5})}$. We define four modular forms $J_k (k = 2,\, 6,\, 10\, 12)$ as follows:

$$\begin{aligned}
J_2 :=& G_2 \\
=& 1 + 2^3 \cdot 3 \cdot 5\{(x^{-1}+x)q + (x^{-4}+5x^{-2}+6+5x^2+x^4)q^2 + \cdots\}, \\
J_6 :=& 2^{-5}\cdot 3^{-3}\cdot 5^{-2}\cdot 67(G_2^3 - G_6) \\
=& (x^{-1}+x)q + (x^{-4}+20x^{-2}-90+20x^2+x^4)q^2 \cdots , \\
J_{10} :=& 2^{-10}\cdot 3^{-5}\cdot 5^{-5}\cdot 7^{-1}(412751G_{10} - 5\cdot 67\cdot 2293G_2^2G_6 + 2^2\cdot 3\cdot 7\cdot 4231G_2^5) \\
=& (x^{-1}-x)^2q^2 - 2(x^{-1}-x)(x^{-4}+10x^{-2}-10x^2-x^4)q^3 + \cdots , \\
J_{12} :=& 2^{-2}(J_6^2 - J_2J_{10}) \\
=& q^2 + (x^{-5}-15x^{-3}-10x^{-1}-10x-15x^3+x^5)q^3 + \cdots ,
\end{aligned}$$

where $x = \exp\left[\pi\sqrt{-1}(z_1 - z_2)/\sqrt{5}\right]$, $q = \exp\left[\pi\sqrt{-1}(z_1 + z_2)\right]$.

Theorem 5.1 (Existence Theorem) *Assume that* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ *and* $p \geq 3$. *Then, there exists a Hilbert modular form* $f_{p-1} \in A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_{p-1}$ *satisfying*

$$f_{p-1} \equiv 1 \pmod{p}.$$

Theorem 5.2 *Assume that* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$.
(1) If $p \geq 5$ *is a prime number such that* $p \equiv 3 \pmod 4$, *then*

$$A^{(2)}_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_p\left[\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}\right]/(\tilde{A}_p(\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}) - 1)$$

where $J_2,\ J_6,\ J_{10}$ *are generators of* $A^{(2)}_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})$ *and*

$$A_p(X_1, X_2, X_3) \in \mathbb{Z}_{(p)}\left[X_1, X_2, X_3\right]$$

is a polynomial defined by

$$f_{p-1} = A_p(J_2, J_6, J_{10}).$$

(2)

$$\begin{aligned}
&A^{(2)}_{\mathbb{F}_3}(\Gamma_{\mathbb{K}}) = \mathbb{F}_3\left[\tilde{J}_6, \tilde{J}_{10}\right]. \\
&A^{(2)}_{\mathbb{F}_2}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_2\left[\tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{12}\right]/(\tilde{J}_6^2 + \tilde{J}_{10}^2).
\end{aligned}$$

Proposition 5.1 *([6, Theorem 3.1 and Proposition 3.3])*
(1) There exists an odd weight form J_{15} *with integral Fourier coefficients:*

$$J_{15} = q^2 - (x^{-5} + 275x^{-1} + 275x + x^5)q^3 + \cdots \in A_{\mathbb{Z}}(\Gamma_{\mathbb{K}})_{15} \subset A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_{15}.$$

(2) If k is odd, then $A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_k = J_{15} \cdot A_{\mathbb{Z}_{(p)}}(\Gamma_{\mathbb{K}})_{k-15}$.
(3) J_{15}^2 *has the following polynomial expressions:*

$$\begin{aligned} J_{15}^2 &= 5^5 J_{10}^3 - 2\cdot 3^3 J_6^5 + 2\cdot 5^2 J_2 J_6^3 J_{10} + 2\cdot 5^3 J_2 J_6 J_{10} J_{12} + J_2^3 J_{12}^2 \\ &= 5^5 J_{10}^3 - 2\cdot 3^3 J_6^5 + 2^{-1}\cdot 3^2\cdot 5^2 J_2 J_6^3 J_{10} - 2^{-1}\cdot 5^3 J_2^2 J_6 J_{10}^2 \\ &\quad + 2^{-4} J_2^3 J_6^4 - 2^{-3} J_2^4 J_6^2 J_{10} + 2^{-4} J_2^5 J_{10}^2. \end{aligned}$$

Set

$$\begin{aligned} C(X_1, X_2, X_3, X_4) :&= X_4^2 - 5^5 X_3^3 + 2\cdot 3^3 X_2^5 - 2^{-1}\cdot 3^2\cdot 5^2 X_1 X_2^3 X_3 \\ &\quad + 2^{-1}\cdot 5^3 X_1^2 X_2 X_3^2 - 2^{-4} X_1^3 X_2^4 + 2^{-3} X_1^4 X_2^2 X_3 \\ &\quad - 2^{-4} X_1^5 X_3^2 \in \mathbb{Q}\,[X_1, X_2, X_3, X_4] \end{aligned}$$

If $p \neq 2$, then $C(X_1, X_2, X_3, X_4) \in \mathbb{Z}_{(p)}\,[X_1, X_2, X_3, X_4]$. Denote by $\tilde{C}_p(X_1, X_2, X_3, X_4) \in \mathbb{F}_p\,[X_1, X_2, X_3, X_4]$ the reduction modulo $p\,(p \neq 2)$.

Theorem 5.3 *Assume that* $\mathbb{K} = \mathbb{Q}(\sqrt{5})$.
(1) If $p \geq 5$ is a prime number such that $p \equiv 3 \pmod 4$, then

$$A_{\mathbb{F}_p}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_p\big[\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{15}\big]/(\tilde{A}_p(\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}) - 1, \tilde{C}_p(\tilde{J}_2, \tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{15}))$$

(2)

$$A_{\mathbb{F}_3}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_3\big[\tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{15}\big]/(\tilde{C}_p)$$
$$A_{\mathbb{F}_2}(\Gamma_{\mathbb{K}}) \cong \mathbb{F}_2\big[\tilde{J}_6, \tilde{J}_{10}, \tilde{J}_{12}, \tilde{J}_{15}\big]/(\tilde{J}_6^2 + \tilde{J}_{10}^2, \tilde{J}_{15}^2 + \tilde{J}_{10}^3 + \tilde{J}_{12}^2).$$

References

[1] Baily, W. L., Jr.: Automorphic forms with integral Fourier coefficients. In *Several Complex Variables, I (Proc. Conf., Univ. of Maryland, College Park, Md., 1970)*, pp. 1-8. Springer Verlag, 1970.

[2] Baily, W. L., Jr.: Theorems on the finite generation of algebras of modular forms. *Amer. J. Math.* **104** (1982), 645–682.

[3] Goren, E. Z.: Hilbert modular forms modulo p^m: the unramified case. *J. Number Theory* **90** (2001), 341–375.

[4] Goren, E. Z.: *Lectures on Hilbert modular varieties and modular forms. CRM Monograph series* **14**. American Mathematical Society, Providence, RI, 2002.

[5] Nagaoka, S.: On the ring of Hilbert modular forms over $\mathbb{Z}$. *J. Math. Soc. Japan* **35** (1983), 589–608.

[6] Nagaoka, S.: On Hilbert modular forms with integral Fourier coefficients. *Abh. Math. Sem. Univ. Hamburg* **56** (1986), 157–168.

[7] Nagaoka, S.: Note on mod p Siegel modular forms. *Math. Z.* **235** (2000), 405–420.

[8] Serre, J.-P.: Formes modulaires et fonctions zêta p-adiques. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, 191–268. Lecture Notes in Math. **350**. Springer Verlag, Berlin, 1973.

[9] Swinnerton-Dyer, H. P. F.: On l-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, 1–55. Lecture Notes in Math. **350**. Springer Verlag, Berlin, 1973.

Recibido: 19 de septiembre de 2003

Shoyu Nagaoka
Department of Mathematics
Kinki University
Higashi-Osaka
Osaka 577-8502, Japan
nagaoka@math.kindai.ac.jp