COMPOSITIO MATHEMATICA

E. THOMAS
A. T. VASQUEZ

Rings of Hilbert modular forms

Compositio Mathematica, tome 48, nº 2 (1983), p. 139-165
<http://www.numdam.org/item?id=CM_1983__48_2_139_0>

COMPOSITIO MATHEMATICA, Vol. 48, Fasc. 2, 1983, pag. 139–165

RINGS OF HILBERT MODULAR FORMS*

E. Thomas and A.T. Vasquez

1. Introduction

Let G be the Hilbert modular group for a totally real number field K of degree n. Thus, $G = \mathrm{PSL}_2(\mathfrak{o})$, where $\mathfrak{o}$ is the ring of integers for K. (We allow the case $n = 1$, with $K = Q$ and $\mathfrak{o} = Z$). By means of the n distinct embeddings of K into the real numbers R, G acts on H^n, where H denotes the complex upper half plane; see [7] for details. A holomorphic function $f: H^n \to C$ is called a *modular form* of *weight* $2k$ if:

$$f(g \cdot z) = J(g,z)^{-k} f(z) \text{ for all } g \in G \text{ and } z \in H^n. \tag{1.1}$$

Here $J(g,z)$ is the Jacobian of the transformation g at z – i.e., if g is represented by a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and if $z = (z_1, \ldots, z_n)$, then

$$J(g,z) = \prod_{i=1}^{n} (c^{(i)} z_i + d^{(i)})^{-2},$$

where, for x in K, $x^{(i)}$ denotes the image of x by the i^{th} embedding of K in R. (If $n = 1$, we also must assume that f is "holomorphic at the cusp"). We set

$$(M_G)_k = \text{complex vector space of modular forms of weight } 2k,$$
$$M_G = \sum_{k \geq 0} (M_G)_k, \text{ with } (M_G)_0 = C.$$

Thus M_G is a (finitely generated) algebra over C.

* Research supported by grants from the National Science Foundation.

0010-437X/83/02/0139–27$0.20

PROBLEM 1: *For a given number field K determine the structure of the ring of modular forms M_G.*

When $n = 1$ ($K = Q$), it is a classical result that M_G is a polynomial ring:

$$M_G = C[E_2, E_3]$$

where E_i is an Eisenstein series of weight $2i$ ($i = 2, 3$). When $n = 2$, only some scattered results have been obtained. We adopt the following notation: if K is a real quadratic number field of discriminant D, we write $M(D)$ instead of M_G. The following rings $M(D)$ have been determined [5], [8], [9]:

$$\begin{aligned} M(5) &= C[X_1, X_3, X_5, X_{10}]/(R_{20}) \\ M(8) &= C[X_1, X_2, X_3, X_7]/(R_{14}) \\ M(13) &= C[X_1, X_2, X_3, Y_3, X_4]/(R_6, R_8). \end{aligned} \tag{1.2}$$

Here the X's and Y's are generators and the R's are relations, with weight twice the subscript. These rings are all examples of "complete intersection" rings, see Section 5 for definition. On the other hand van der Geer [4] has determined the ring $M(24)$, and this turns out not to be a complete intersection (see Section 6). As a step towards Problem 1, we ask: *for which discriminants D is the ring M(D) a complete intersection*? Our result is:

THEOREM 1: *If $D \neq 12$, then $M(D)$ is a complete intersection ring if, and only if, $D = 5$, 8 or 13.*

REMARK: From the results in Section 6 it seems likely that $M(12)$ is also a complete intersection. Specifically, we have:

CONJECTURE 1: $M(12) = C[X_1, X_2, X_3, Y_3, X_4]/(R'_6, R'_8)$.

Suppose now that Γ is a subgroup of G (n arbitrary). We then have the notion of a modular form for Γ – simply require that (1.1) holds only for all $\gamma \in \Gamma$ – and hence we obtain the algebra of modular forms M_Γ. In particular suppose that Γ is the principal congruence subgroup associated to a proper ideal $\mathfrak{A}$ in $\mathfrak{o}$. (See §7). Such a subgroup is torsion free provided $\mathfrak{A}^2 \neq (2)$ or (3). If K is a real quadratic number field of discriminant D, we write $M(D, \mathfrak{A})$ for M_Γ. Hirzebruch [8] has proved that the ring $M(5, (2))$ is a complete intersection: specifically,

$$M(5,(2)) = C[X_1, X_2, X_3, X_4, X_5]/(S, T) \tag{1.3}$$

where $\deg X_i = 2$, $\deg S = 4$, $\deg T = 8$.

Our result is

THEOREM 2: *Let K be a real quadratic number field of discriminant D, and let $\mathfrak{A}$ be a proper ideal in $\mathfrak{o}$ with $\mathfrak{A}^2 \neq (2)$ or (3). If $(D, \mathfrak{A}) \neq (8,(2))$, then $M(D, \mathfrak{A})$ is a complete intersection ring if, and only if, $(D, \mathfrak{A}) = (5,(2))$.*

REMARK: It seems likely that $M(8,(2))$ is also a complete intersection ring, with structure as follows:

CONJECTURE 2:
$M(8,(2)) = C[X_1, X_2, X_3, X_4, X_5, X_6, X_7]/(R_1, R_2, R_3, R_4)$,
where $\deg X_i = 2$, $\deg R_i = 4$.

These two theorems suggest that we look for weaker structures than complete intersections for the rings M_Γ. For example, every complete intersection ring is Gorenstein and every Gorenstein ring is Cohen–Macaulay. (We are using the definitions in [12]). It is not known whether or not M_G (or more generally, M_Γ) is always Cohen–Macaulay. When $n = 2$, we have the following result. (In general we will say that a subgroup Γ of a modular group G is of *modular type* if either $\Gamma = G$ or Γ is a torsion free subgroup of finite index).

THEOREM 3: *Let Γ be a subgroup of modular type for a real quadratic number field. If M_Γ is Cohen–Macaulay, then it is also Gorenstein.*

We now consider Problem 1 for totally real cubic number fields, i.e., $n = 3$. Our result here is:

THEOREM 4: *Let Γ be a subgroup of modular type for a totally real cubic number field. Then, the ring M_Γ is never Gorenstein.*

As indicated above this shows, in particular, that M_Γ is never a complete intersection ring.

The paper is organized as follows. In §2 we describe the formula of Shimizu, which gives the dimension of the space of "cusp" forms. Using this, in §3 we construct a rational function $\mu_\Gamma(t)$ for each group Γ. We define the notion of a "palindromic function" in §4 and give there the proofs of Theorems 3 and 4, using properties of $\mu_\Gamma(t)$.) Finally, we discuss complete intersection rings in §5, give the proof of Theorem 1 in §6 and that of Theorem 2 in §7.

2. The Formula of Shimizu

The results of the preceding section are proved by studying the properties of a certain rational function $\mu_\Gamma(t)$ associated with the ring M_Γ. This function is defined using results of Shimizu, which we now explain.

With each graded, finitely generated algebra A over the complex numbers we associate a formal power series (the "Hilbert series") by:

$$\alpha(t) = \sum_{i=0}^{\infty} (\dim_C A_i) t^i,$$

where $A = \sum_{i=0}^{\infty} A_i$. Since A is finitely generated, $\alpha(t)$ is in fact a rational function, i.e., an element of $Q(t)$ (see [1]). Thus with each subgroup Γ of modular type we associate, in a canonical way, a rational function $\mu_\Gamma(t)$, taking $A = M_\Gamma$. To calculate $\mu_\Gamma(t)$ we must know the integers $\dim_C(M_\Gamma)_k$, $k \geq 1$. These follow from the work of Shimizu [11], for $k > 1$, and Freitag [3], $k = 1$.

The vector space $(M_\Gamma)_k$ contains a subspace $(C_\Gamma)_k$, the space of "cusp forms" of weight $2k$ (see [11]). In fact,

$$\dim(M_\Gamma)_k = \dim(C_\Gamma)_k + h \qquad (\dim = \dim_C), \tag{2.1}$$

where h denotes the number of "cusps" of Γ. By Shimizu ([11], Theorem 11) we have:

(2.2) *Let K be a totally real number field of degree n, and let Γ be a subgroup of modular type, with $[G:\Gamma] = e$. Then, for $k \geq 2$,*

$$\dim(C_\Gamma)_k = \frac{(-1)^n(2k-1)^n e}{2^{n-1}} \cdot \zeta_K(-1) + w + \sum_\tau a(\tau)\gamma_k(\tau).$$

Here ζ_K is the Dedekind zeta function of K, while w is a rational number (see below) arising from the cusps of Γ. The remaining terms in (2.2) come from the fixed points of Γ. With each fixed point x we associate an $(n+1)$-tuple, τ, of positive integers (called a type): $\tau = (r; q_1, \ldots, q_n)$. Here r is the order of the isotropy group, Γ_x, at x, while $(q_1, \ldots, q_n)$ describe the representation of the (cyclic) group Γ_x on C^n, relative to a choice of generator. We say that a type is "proper" if $q_1 = 1$ and $0 < q_i < r$, for $i > 1$. We show in §2 of [14] that with each fixed point of Γ we can associate a unique proper type. Two fixed points x and x' are called "equivalent" if there is γ in Γ such that $x' = \gamma x$. The number of equivalence classes of fixed points for Γ is finite; moreover, equivalent fixed points have the same proper type. We set

$a(\tau)$ = number of equivalence classes of fixed points with proper type τ.

Finally, for $k \geq 0$, we define (see [6], [11] and [15]):

$$\gamma_k(\tau) = \frac{1}{r} \sum_{\substack{\zeta^r = 1 \\ \zeta \neq 1}} \prod_{i=1}^{n} \frac{\zeta^{kq_i}}{1 - \zeta^{q_i}} \qquad (\tau = (r; q_1, \ldots, q_n)). \tag{2.3}$$

In (2.2) the summation is over the finite set of proper types τ with $a(\tau) \neq 0$. Note that:

(2.4) If Γ is torsion free, then $a(\tau) = 0$ for all τ.

Also, as noted by Shimizu [11]:

(2.5) If K has a unit of negative norm (e.g., if n odd), then $w = 0$.

In §1 we are concerned only with $n = 2$ and 3; thus, by (2.5) we need only calculate the number w for $n = 2$. For this we define the *arithmetic genus* of Γ, $\chi(\Gamma)$.

Let $Y_\Gamma = H^n/\Gamma$, the quotient space of H^n by Γ. By Blumenthal and Maass, one can compactify Y_Γ by adding on h points so that the resulting compact space, $\hat{Y}_\Gamma$, is a projective variety (h = number of cusps of Γ). Let Z_Γ be a non-singular model for $\hat{Y}_\Gamma$. Since any two such models are birationally equivalent and since the arithmetic genus χ is a birational invariant, we obtain an invariant that depends only upon Γ if we set:

$$\chi(\Gamma) = \chi(Z_\Gamma).$$

By Freitag [3] and Hammond ([6], page 41), using the fact that $p_g + 1 = \chi$, we obtain:

(2.6) *Let Γ be a subgroup of modular type for a real quadratic number field K. Then,*

$$w = \chi(\Gamma) - \tfrac{1}{2}e\zeta_K(-1) - \sum_{\tau} a(\tau)\gamma_0(\tau).$$

We stress that (2.6) holds whether or not K has a unit of negative norm. For $k \geq 0$ set

$$\omega_k(\tau) = \gamma_k(\tau) - \gamma_0(\tau).$$

Combining (2.2) and (2.6) we obtain:

(2.7) *Let Γ be a subgroup of modular type for a real quadratic field K, with $[G:\Gamma] = e$. Then, for $k \geq 2$,*

$$\dim(C_\Gamma)_k = 2ek(k-1)\cdot\zeta_K(-1) + \chi(\Gamma) + \sum_\tau a(\tau)\omega_k(\tau).$$

For $n = 2$ and 3 we now give explicit calculations of the (rational) numbers $\gamma_k(\tau)$ and $\omega_k(\tau)$, for all proper types that occur. We start with $n = 2$; for $k \geq 0$ define integers δ_k, ε_k by the generating functions:

$$\sum_{k=0}^{\infty} \delta_k t^k = t^2/(1-t^3), \qquad \sum_{k=0}^{\infty} \varepsilon_k t^k = t^2(2 + t + 2t^2)/(1-t^5). \tag{2.8}$$

Using the results of Prestel [10], we prove:

(2.9) THEOREM: *For real quadratic numbers fields there are eight proper types of fixed points for the modular group. For each such proper type the value of $\omega_k(\tau)$ is as follows:*

$\omega_k(\tau) = 0$, *if* $\tau = (2;1,1), (3;1,2), (4;1,1), (4;1,3), (6;1,5)$,
$\omega_k(3;1,1) = -\delta_k/3$,
$\omega_k(5;1,2) = \omega_k(5;1,3) = -\varepsilon_k/5$.

We precede the proof with the following simple result.

(2.10) LEMMA: *If the number $\gamma_k(\tau)$ is constant for all k, then $\omega_k(\tau) = 0$, all k. In particular, if $\tau = (r;1,r-1)$, then $\omega_k(\tau) = 0$, all k.*

This follows at once from (2.3) and the definition of $\omega_k(\tau)$.

Proof of (2.9): Prestel shows ([10], page 207) that the eight proper types given in (2.9) are the only ones that occur for real quadratic fields. By Lemma (2.10) $\omega_k(\tau) = 0$, for $\tau = (2;1,1), (3;1,2), (4;1,3)$ and $(6;1,5)$. By (2.3), $\gamma_k(4;1,1) = 1/16$ (all k), and so again by (2.10), $\omega_k(4;1,1) = 0$. By (2.3), for $k \equiv 0, 1 \bmod 3$, $\gamma_k(3;1,1) = 1/9$; while if $k \equiv 2 \bmod 3$, $\gamma_k(3;1,1) = -2/9$. This gives the value indicated above for $\omega_k(3;1,1)$. Similarly, we find that $\gamma_k(5;1,2) = \gamma_k(5;1,3)$; and that for $k \equiv 0, 1 \bmod 5$, $\gamma_k(5;1,2) = 1/5$; if $k \equiv 2, 4 \bmod 5$, $\gamma_k(5;1,2) = -1/5$; and if $k \equiv 3 \bmod 5$, $\gamma_k(5;1,2) = 0$. Thus we obtain the values indicated for $\omega_k(5;1,2)$ and $\omega_k(5;1,3)$; this completes the proof.

We now prove the analogous result for $n = 3$; of course, by (2.5), we now work directly with the $\gamma_k(\tau)$'s. For $k \geq 0$ define integers ϕ_k, ψ_k, θ_k and ξ_k by:

$$\sum_{k\geq 0} \phi_k t^k = (1+t)^{-1}, \qquad \sum_{k\geq 0} \psi_k t^k = (1-t)(1-t^3)^{-1}$$
$$\sum_{k\geq 0} \theta_k t^k = (1-t+t^2+t^3-t^5-t^6)(1-t^7)^{-1} \tag{2.11}$$
$$\sum_{k\geq 0} \xi_k t^k = (1-t+9t^2+t^3-t^4+t^6-t^7-9t^8)(1-t^9)^{-1}.$$

Note that in the second, third and fourth functions $(1-t)$ is common to numerator and denominator.

Our result is:

(2.12) THEOREM: *For totally real cubic number fields seven proper types of fixed points occur for the modular group. For each such proper type the value of $\gamma_k(\tau)$ is given as follows*:

$$\begin{array}{ll} \gamma_k(2;1,1,1) = \phi_k/16, & \\ \gamma_k(3;1,1,1) = 0, & \psi_k(3;1,1,2) = \psi_k/9 \\ \gamma_k(7;1,2,4) = 0, & \psi_k(7;1,2,3) = \theta_k/7 \\ \gamma_k(9;1,4,7) = \psi_k/3, & \psi_k(9;1,2,5) = \xi_k/27. \end{array}$$

The fact that only these seven types occur (up to an equivalence relation) is proved in [14], §2. For each type the value of γ_k is then a standard calculation and is left to the reader. For the case $r = 9$ it is useful to note that if ζ is a 9$^{\text{th}}$ root of unity then $\zeta^6 + \zeta^3 + 1 = 0$. Also, if discriminant $K > 81$, only the first three types occur, see [16].

Using (2.9) and (2.12) we rewrite (2.2) and (2.7). Suppose that K is a real quadratic field with discriminant D; define a number s_D by:

$$s_D = \begin{cases} 1/6, & \text{if } D \not\equiv 0 \bmod 3 \\ 4/15, & \text{if } D > 12 \text{ and } D \equiv 3 \bmod 9 \\ 1/3, & \text{if } D = 12 \text{ or } D \equiv 6 \bmod 9. \end{cases} \tag{2.13}$$

Also, if Γ is any subgroup of modular type (n arbitrary), we set, for $r \geq 2$,

(2.14) $a_r(\Gamma)$ = number of equivalence classes of fixed points x of Γ, with $|\Gamma_x| = r$.

For $n = 2$ the numbers a_r have been calculated by Prestel [10], and for $n = 3$ by Weisser [16].

Let δ_k and ε_k be the integers defined in (2.8). We prove:

(2.15) THEOREM: *Let K be a real quadratic number field with discriminant D and Γ a subgroup of modular type, with $[G:\Gamma] = e$. Then, for $k \geq 2$,*

$$\dim(C_\Gamma)_k = 2ek(k-1)\cdot\zeta_K(-1) + \chi(\Gamma) - s_D\delta_k a_3(\Gamma) - a_5(\Gamma)\varepsilon_k/5.$$

PROOF: By (2.9) we see that the only proper types we need consider in (2.7) are (3; 1, 1), (5; 1, 2) and (5; 1, 3). By [9], page 207, we find that:

$$a(3;1,1) = 3s_D a_3(\Gamma), \qquad a(5;1,2) + a(5;1,3) = a_5(\Gamma).$$

Thus the theorem follows from (2.7) and (2.9).

REMARK: If $D > 5$, then $a_5(\Gamma) = 0$, while if Γ is torsion free $a_3(\Gamma) = a_5(\Gamma) = 0$.

We now rewrite (2.2) using Theorem (2.12). Let ϕ_k, ψ_k, θ_k and ξ_k be the integers defined in (2.11). We prove:

(2.16) THEOREM: *Let Γ be a subgroup of modular type for a totally real cubic number field K. Then, for $k \geq 2$,*

$$\dim(C_\Gamma)_k = -\frac{(2k-1)^3 e}{4}\cdot\zeta_K(-1) + a_2\phi_K/16 + (a_3 + a_9)\psi_k/12 + 3a_7\theta_k/28 + a_9\xi_k/36.$$

Here $a_r = a_r(\Gamma)$ and $e = [G:\Gamma]$.

The proof follows at once from (2.2), together with (2.12) and the frequencies with which the various types occur, as shown in Theorem (2.11) of [14].

3. Rational Functions

We now use the results of §2, especially Theorems (2.15) and (2.16), to calculate explicitly the rational function $\mu_\Gamma(t)$ associated to the ring of modular forms M_Γ. After some preliminary remarks we do out in detail the case $n = 2$; the proofs for $n = 3$ are quite similar and so are only sketched.

We study $\mu_\Gamma(t)$ by means of an analogous function derived from the cusp forms. For this define

$$\sigma_\Gamma(t) = \sum_{k=0}^{\infty} \dim(C_\Gamma)_k t^k,$$

where we set $(C_\Gamma)_0 = C$. Thus, by (2.1), we have:

$$\mu_\Gamma(t) = \sigma_\Gamma(t) + ht(1-t)^{-1}, \tag{3.1}$$

where h = number of cusps for Γ. Thus $\sigma_\Gamma(t)$ is also a rational function; we first calculate this, and then obtain $\mu_\Gamma(t)$ by (3.1).

Notice that in (2.2) (and its variants in §2), we are not given $\dim(C_\Gamma)_1$. For this we need a result of Freitag [3].

(3.2) *Let Γ be a subgroup of modular type for a totally real number field of degree n. Then,*

$$\dim(C_\Gamma)_1 = (-1)^n(\chi(\Gamma) - 1).$$

We now have all the facts necessary to calculate $\sigma_\Gamma(t)$. We begin with a useful observation.

(3.3) LEMMA: *Let $\alpha(t) = \sum_{k=0}^{\infty} A_k t^k$ be a formal power series with rational coefficients. Suppose there is a polynomial $f(t)$ in $Q[t]$, of degree m, and a positive integer N such that*

$$A_k = f(k), \text{ for all } k \geq N.$$

Then,

$$\alpha(t) = g(t)(1-t)^{-(m+1)} + h(t),$$

where $g(t), h(t) \in Q[t]$, with $\deg g = m$, $\deg h = N - 1$.

The proof is standard and is left to the reader.

THE CASE $n = 2$. We begin by assuming that $D > 5$; the case $D = 5$ is handled below.

(3.4) THEOREM: *Let K be a real quadratic number field with discriminant D, and let $\mu_G(t)$ be the rational function given by the Hilbert series for the ring of Hilbert modular forms M_G. Suppose that $D > 5$. Then,*

$$\mu_G(t) = (\textstyle\sum_1^6 B_i t^i)(1 - t)^{-2}(1 - t^3)^{-1},$$

where

$$\begin{aligned}
B_0 &= B_6 = 1\\
B_1 &= B_5 = \chi + h - 3\\
B_2 &= B_4 = 4\zeta_K(-1) - \chi - sa_3 - h + 3\\
B_3 &\quad\;\; = 4\zeta_K(-1) + 2sa_3 - 2.
\end{aligned}$$

Here $\chi = \chi(G)$, h = *class number of* K, $s = s_D$ (*see* (2.13)).

PROOF: We begin with the more general situation of a subgroup Γ of modular type, with $[G:\Gamma] = e$. By (2.15), (2.8) and (3.3) we see that $\sigma_\Gamma(t)$ has the following form (we use here the fact that $a_5 = 0$, since $D > 5$):

$$\sigma_\Gamma(t) = g(t)(1 - t)^{-3} + h(t) + bt^2(1 - t^3)^{-1}, \tag{3.5}$$

where $\deg g = 2$, $\deg h = 1$ and b is a constant. Putting everything over a common denominator we find that

$$\sigma_\Gamma(t) = f(t)(1 - t)^{-2}(1 - t^3)^{-1}, \quad \deg f = 6. \tag{3.6}$$

But by (2.15) and (3.2) we know the terms through degree 6 on the left hand side of (3.6). If we set $S_i = \dim(C_\Gamma)_i$, we find:

$$\begin{aligned}
S_0 &= 1\\
S_1 &= \chi - 1\\
S_2 &= 4e\zeta + \chi - sa_3\\
S_3 &= 12e\zeta + \chi\\
S_4 &= 24e\zeta + \chi\\
S_5 &= 40e\zeta + \chi - sa_3\\
S_6 &= 60e\zeta + \chi.
\end{aligned}$$

Here $\chi = \chi(\Gamma)$, $s = s_D$, $a_3 = a_3(\Gamma)$ and $\zeta = \zeta_K(-1)$. Multiplying through by $(1 - t)^2(1 - t^3)$, in (3.6), and solving for $f(t)$, we obtain:

$$f(t) = \textstyle\sum_1^6 A_i t^i, \tag{3.7}$$

where

$$\begin{aligned}
A_0 &= A_6 = 1\\
A_1 &= A_5 = \chi - 3\\
A_2 &= A_4 = 4e\zeta_K(-1) - \chi - sa_3 + 3\\
A_3 &\quad\;\; = 4e\zeta_K(-1) + 2sa_3 - 2.
\end{aligned}$$

Taking $e = 1$ (i.e., $\Gamma = G$) in (3.7) and adding on the term $ht(1-t)^{-1}$, see (3.1), we obtain (3.4). Notice that (3.7) continues to hold when Γ is torsion free, even for $D = 5$, since in this case we also have $a_5 = 0$ (as well as $a_3 = 0$).

Sippose now that $\Gamma = G$ and $D = 5$. We now must adjust (3.5) by adding on a term $ct^2(2 + t + 2t^2)/(1 - t^5)$, where c is a constant, see (2.8) and (2.15). Thus, (3.6) changes to:

$$\sigma_G(t) = f(t)(1-t)^{-1}(1-t^3)^{-1}(1-t^5)^{-1}, \quad \deg f = 10.$$

But by (2.15) we can calculate the numbers S_i for $0 \leq i \leq 10$. We find: $S_0 = 1$; $S_1 = S_2 = 0$; $S_3 = S_4 = 1$; $S_5 = 2$; $S_6 = S_7 = 3$; $S_8 = 4$; $S_9 = 5$; $S_{10} = 7$. Solving for $f(t)$ and adding on the term $t(1-t)^{-1}$ ($h = 1$, for $D = 5$), we obtain:

(3.8) ADDENDUM: *Let K be the real quadratic field with discriminant* 5, *and let G be the Hilbert modular group for K. Then,*

$$\mu_G(t) = (1 + t^{10})(1-t)^{-1}(1-t^3)^{-1}(1-t^5)^{-1}.$$

Suppose now that Γ is a torsion free subgroup of G, with index e. As noted above (3.7) continues to hold in this case by taking $a_3 = 0$. One readily checks that, in this case, the polynomial $f(t)$ in (3.7) factors over the integers, with $1 + t + t^2$ as a factor. Since this is also a factor of the denominator polynomial given in (3.6), we have the following result.

(3.9) COROLLARY: *Let K be a real quadratic number field and Γ a torsion free subgroup of the Hilbert modular group. Then,*

$$\mu_\Gamma(t) = (1 + B_1 t + B_2 t^2 + B_3 t^3 + t^4)(1-t)^{-3},$$

where $B_1 = B_3 = \chi + h - 4$, $B_2 = 2(2e\zeta_K(-1) - \chi - h + 3)$.

THE CASE $n = 3$. We begin by assuming that discriminant K $(= D)$ is greater than 81.

(3.10) THEOREM: *Let K be a totally real cubic number field with discriminant* > 81. *Then,*

$$\mu_G(t) = \left(\sum_1^8 B_i t^i\right)(1-t)^{-2}(1-t^2)^{-1}(1-t^3)^{-1},$$

where

$$
\begin{aligned}
B_0 &= B_8 = 1 \\
B_1 &= h - \chi - 1, \\
B_2 &= \tfrac{1}{4}[-25\zeta_K(-1) + 3a_2/4 + 2a_3/3] - 2 - h, \\
B_3 &= \tfrac{1}{4}[-71\zeta_K(-1) - 3a_2/4 + a_3/3] + 1 - h, \\
B_4 &= \tfrac{1}{2}[-47\zeta_K(-1) + a_2/4 - 2a_3/3] + 2, \\
B_5 &= B_3 + 2h, \\
B_6 &= B_2 + 2h, \\
B_7 &= -(h + \chi + 1).
\end{aligned}
$$

Here $a_r = a_r(G)$, $h =$ *class number of* K *and* $\chi = \chi(G)$.

PROOF: Suppose that Γ is a subgroup of modular type, with $[G:\Gamma] = e$. We assume that $a_7(\Gamma) = a_9(\Gamma) = 0$; e.g., either take $e > 1$ or $D > 81$ (see [16]). Then, using the functions given in (2.11), together with (2.16) and (3.3), we obtain:

$$\sigma_\Gamma(t) = f(t)(1-t)^{-2}(1-t^2)^{-1}(1-t^3)^{-1}, \quad \deg f = 8. \tag{3.11}$$

We compute the left hand side of (3.11) through degree 8 by (2.1): if we set $S_k = \dim(C_\Gamma)_k$, $k \geq 0$, then

$$
\begin{aligned}
&S_0 = 1, \quad S_1 = 1 - \chi, && S_2 = \tfrac{1}{4}(27x + y), \\
&S_3 = \tfrac{1}{4}(125x - y + z), && S_4 = \tfrac{1}{4}(343x + y - z), \\
&S_5 = \tfrac{1}{4}(729x - y), && S_6 = \tfrac{1}{4}(1331x + y + z), \\
&S_7 = \tfrac{1}{4}(2197x - y), && S_8 = \tfrac{1}{4}(3375x + y),
\end{aligned} \tag{3.12}
$$

where $x = -\zeta_K(-1)$, $y = a_2/4$ and $z = a_3/3$.

Solving for $f(t) = \sum_1^8 A_i t^i$, we find:

$$
\begin{aligned}
&A_0 = A_8 = 1, \quad A_1 = A_7 = \tfrac{1}{4}(x - y - z) - 1, \\
&A_2 = A_6 = \tfrac{1}{4}(25x + 3y + 2z) - 2, \\
&A_3 = A_5 = \tfrac{1}{4}(71x - 3y + z) + 1, \\
&A_4 = \tfrac{1}{2}(47x + y - 2z) + 2.
\end{aligned} \tag{3.13}
$$

If we now take $e = 1$ ($\Gamma = G$) and add on the term $ht(1-t)^{-1}$, we obtain $\mu_G(t)$ as given in (3.10). This completes the proof.

By the same method one also computes $\mu_G(t)$ when $D = 49$ or 81. The results are as follows; we omit the details.

(3.14) ADDENDUM: *Let* K *be the totally real cubic number field with discriminant* D:

(i) *If* $D = 49$, *then*

$$\mu_G(t) = \frac{(1+t^4+3t^5+5t^6+4t^7+3t^8+3t^9+3t^{10}+2t^{11}-2t^{13}+t^{14})}{(1-t)(1-t^2)(1-t^3)(1-t^7)}.$$

(ii) *If* $D = 81$, *then*:

$$\mu_G(t) = \\ = \frac{(1-t+t^2+t^3+t^4+6t^5+4t^6-2t^7+4t^8+6t^9-t^{10}+3t^{11}+3t^{12}-3t^{13}+t^{14})}{(1-t)^2(1-t^2)(1-t^9)}.$$

When K is a Galois cubic number field the coefficients $B_1, \dots, B_4$ are readily calculated using the tables in [16]. We illustrate this below for Galois fields of small discriminant.

(3.15) TABLE: *Coefficients* $B_1, \dots, B_4$ *for* $\mu_G(t)$

Discriminant K	h	χ	B_1	B_2	B_3	B_4
13^2	1	1	-1	2	4	10
19^2	1	1	-1	6	18	22
31^2	1	-1	1	59	163	222
37^2	1	0	0	45	123	164
43^2	1	-5	5	159	448	598

Suppose finally that Γ is a torsion free subgroup of G, with finite index e, K a totally real cubic number field. Then $a_r = 0$, all r, and so $\chi = \chi(\Gamma) = \frac{1}{4}e\zeta_K(-1)$. Thus, in (3.13), we find:

$$A_1 = A_7 = -\chi - 1, \qquad A_2 = A_6 = -25\chi - 2,$$
$$A_3 = A_5 = -71\chi + 1, \qquad A_4 = -94\chi + 2.$$

Therefore the polynomial $f(t)$ in (3.11) factors into

$$(1+t)^2(1+t+t^2)(\textstyle\sum_1^4 C_i t^i),$$

where $C_0 = C_4 = 1$, $C_1 = C_3 = -(\chi + 4)$, $C_2 = 6 - 22\chi$.

Consequently, we obtain:

(3.16) COROLLARY: *Let* Γ *be a torsion free subgroup of* G, *as above. Set* $\chi = \chi(\Gamma)$, $h =$ *number of cusps for* Γ. *Then,*

$$\mu_\Gamma(t) = (\textstyle\sum_1^5 B_i t^i)(1-t)^{-4},$$

where

$$\begin{aligned} &B_0 = B_5 = 1, \\ &B_1 = -(\chi + 3 - h), \quad B_4 = B_1 - 2h, \\ &B_2 = 2 - 23\chi - 3h, \quad B_3 = B_2 + 6h. \end{aligned}$$

We give three examples below: in each case Γ is the principal congruence subgroup (see §7) associated to a prime ideal $\mathfrak{p}$. (See [14], (1.7) for details.)

(3.17) TABLE: *Coefficients B_1 and B_2 for $\mu_\Gamma(t)$*

discriminant K	norm $\mathfrak{p}$	h	χ	B_1	B_2
7^2	7	8	-2	7	24
13^2	5	6	-5	8	99
19^2	11	12	-165	174	3761

4. Palindromic Functions

Let $f(t)$ be an element of the rational functional field $Q(t)$. We will say that f is *Palindromic* (a P-function) if, for some integer e, $t^e f(t^{-1}) = f(t)$. Similarly, we call f a *Q-function* if $f(-t)$ is a P-function. Finally, an *R-function* is one that is either P or Q.

The following facts are immediate consequences of the definitions.

(4.1) *If $f(t)$ and $g(t)$ are R-functions, then so is $f \cdot g(t)$.*

(The multiplication rule is: $P \cdot P = Q \cdot Q = P$, $P \cdot Q = Q$).

(4.2) *If $f(t)$ is an R-function then so is $1/f(t)$, with the same value of R.*

If an R-function is in fact a polynomial (in $Q[t]$ or $Z[t]$), we call it an *R-polynomial.* We now consider factorization of such polynomials. Define an integer, ± 1, as follows:

$$\varepsilon_R = \begin{cases} +1, & \text{if } R = P \\ -1, & \text{if } R = Q \end{cases}$$

(4.3) LEMMA: *Let $f(t)$ be an R-polynomial of odd degree. Then,*

$$f(t) = (1 + \varepsilon_R t) g(t),$$

where $g(t)$ is a P-polynomial.

The proof follows at once from the definitions and (4.1), (4.2).

(4.4) LEMMA: *Suppose that $f(t)$ is a P-polynomial of even degree such that ε $(= \pm 1)$ is a root. Then,*

$$f(t) = (1 - \varepsilon t)^2 g(t),$$

where $g(t)$ is a P-polynomial.

PROOF: Since ε is a root of $f(t)$, $f(t) = (1 - \varepsilon t)h(t)$, where $h(t)$ is an R-polynomial with $\varepsilon_R = -\varepsilon$. Thus, by (4.3),

$$h(t) = (1 + \varepsilon_R t)g(t) = (1 - \varepsilon t)g(t),$$

which proves the lemma.

We use these ideas to prove the theorems in §1. With each subgroup Γ of modular type ($n = 2, 3$) we associate a polynomial with integer coefficients, $\beta_\Gamma(t)$, as follows:

(4.5) *$\beta_\Gamma(t)$ is the polynomial in the numerator of $\mu_\Gamma(t)$, as given in* (3.4), (3.8), (3.9), (3.10), (3.14) *and* (3.16).

Thus, in the notation of §3,

$$\beta_\Gamma(t) = \textstyle\sum_1^r B_i t^i,$$

where r is 6 in (3.4), 10 in (3.8), 4 in (3.9), 8 in (3.10), 14 in (3.14) and 5 in (3.16).

We now prove Theorems 3 and 4. Let Γ be a subgroup of modular type, as above. By [12], page 481, and by the results of §3 it follows that the algebra M_Γ has Krull dimension $n + 1$, $n = 2, 3$. Therefore, by [13], page 71, we obtain:

(4.6) *Let Γ be a subgroup of modular type for a totally real number field of degree* 2 *or* 3. *If the ring M_Γ is Gorenstein, then $\beta_\Gamma(t)$ is a P-polynomial. Conversely, if M_Γ is Cohen–Macaulay and $\beta_\Gamma(t)$ is a P-polynomial, then M_Γ is Gorenstein.*

PROOF OF THEOREM 3: By (3.4), (3.8) and (3.9), $\beta_\Gamma(t)$ is always a P-polynomial, and so Theorem 3 follows at once from (4.6).

PROOF OF THEOREM 4: Since h is always a positive integer, it follows from (3.10), (3.14) and (3.16) that $\beta_\Gamma(t)$ is never a P-polynomial. Thus, by (4.6), M_Γ is never Gorenstein.

5. Complete Intersections

Let R be a graded Noetherian algebra. We say that a sequence $\theta_1, \ldots, \theta_r$ of elements of R is a *regular sequence*, if each θ_i is homogeneous of positive degree and θ_i is not a zero-divisor modulo $(\theta_1, \ldots, \theta_{i-1})$ for $i = 1, \ldots, r$. We say that a graded algebra A (over C) is a *complete intersection* if

$$A \approx C[X_1, \ldots, X_s]/(\theta_1, \ldots, \theta_r), \tag{5.1}$$

where $\theta_1, \ldots, \theta_r$ is a regular sequence (see [13]).

By Stanley ([12], p. 505) we have:

(5.2) *Suppose that A is a complete intersection, as above, with* $\deg X_i = d_i$ *and* $\deg \theta_j = e_j$. *Then,*

$$\alpha(t) = [\textstyle\prod_1^r (1 - t^{e_j})]\prod_1^s (1 - t^{d_i})^{-1}.$$

For the rest of the paper we suppose that K is a real quadratic number field of discriminant D and that Γ is a subgroup of modular type for K. Let $\beta_\Gamma(t)$ be the polynomial in $Z[t]$ defined in (4.5). Thus, by §3:

(5.3) *If $\Gamma = G$ and $D > 5$, then* $\deg \beta_\Gamma = 6$; *if $\Gamma = G$ and $D = 5$,* $\deg \beta_\Gamma = 10$; *finally, if $\Gamma \neq G$,* $\deg \beta_\Gamma = 4$.

Note that in all three cases the denominator of $\mu_\Gamma(t)$ has the form given in (5.2). Thus, by (5.2), we have the following important fact, the key to proving Theorems 1 and 2.

(5.4) PROPOSITION: *Let Γ be a subgroup of modular type for the real quadratic number field K. If M_Γ is a complete intersection ring, then $\beta_\Gamma(t)$ factors completely into a product of cyclotomic polynomials.*

In the next section we use (5.4) to prove Theorem 1, while in §7 we use it to prove Theorem 2.

6. Proof of Theorem 1

For this section we take $\Gamma = G$ ($n = 2$), and if discriminant $K = D$, we write $\beta_D(t)$ for $\beta_\Gamma(t)$ and $\mu_D(t)$ for $\mu_\Gamma(t)$. By (5.4) we will prove Theorem 1 in the "only if" direction by showing:

(6.1) PROPOSITION: *If $D > 13$, then the polynomial $\beta_D(t)$ does not factor into a product of cyclotomic polynomials.*

The proof proceeds in two steps. We first show that if $\beta_D(t)$ factors into cyclotomic polynomials, then $13 < D \leq 41$. And we then show, by explicit calculation, that for the 9 values of D in this interval, $\beta_D(t)$ does not so factor.

The proof hinges on the following two elementary facts. Let

$$\beta_D(t) = \textstyle\sum_1^6 B_i t^i$$

where the B_i's are given in (3.4). Set $a_3 = a_3(G)$, $\zeta = \zeta_K(-1)$, and $s = s_D$.

(6.2) PROPOSITION:

$$a_3 = \frac{B_3 + 2 - (B_1 + B_2)}{3s}$$

$$2\zeta = \tfrac{1}{6}(B_3 + 2(B_1 + B_2 + 1)).$$

The proof follows at once from (3.4). We now use the specific calculation of ζ given by Siegel (see [7], page 192):

$$2\zeta_K(-1) = \frac{1}{30} \sum_{\substack{k \in Z, k^2 < D \\ k^2 \equiv D \bmod 4}} \sigma_1\left(\frac{D - k^2}{4}\right)$$

where $\sigma_1(m)$ is the sum of the divisors of m. Since $\sigma_1(m) \geq 1 + m$, one readily shows:

(6.4) LEMMA: *Let K be a real quadratic field with discriminant D.*

(i) *Suppose that $D \equiv 1 \bmod 4$, and let r be the largest integer such that $D > 4r(r - 1) + 1$. Then,*

$$2\zeta_K(-1) \geq \frac{1}{15}\left[r\left(\frac{D + 3}{4} - \frac{(r^2 - 1)}{3}\right) - 1\right].$$

(ii) *Suppose that* $D = 4d$, *with* $d \equiv 2$, $3 \bmod 4$; *let* r *be the largest integer such that* $d > 4r^2$. *Then,*

$$2\zeta_K(-1) \geq \frac{1}{30}\left[(2r+1)\left((d+1) - \frac{r(r+1)}{3}\right) - 2\right].$$

REMARK: The lower bound can be achieved, e.g. $D = 5, 13, 29, 53$.

By the lemma, and the table on page 200 of [7], we have:

(6.5) COROLLARY:
(i) *If* $D > 37$, $2\zeta_K(-1) \geq 7/3$.
(ii) *If* $D > 57$, $2\zeta_K(-1) > 8/3$.
(iii) *If* $D > 153$, $2\zeta_K(-1) > 32/3$.

We now prove, using (6.2) and (6.5):

(6.6) PROPOSITION: *If the polynomial* $\beta_D(t)$ *factors into a product of cyclotomic polynomials, then* $D \leq 41$.

We begin by showing that λ_1 $(= 1 - t)$ does not divide $\beta_D(t)$ and that if λ_2 $(= 1 + t)$ divides $\beta_D(t)$, then $D \leq 41$. Suppose λ_1 divides $\beta_D(t)$, i.e., $\beta_D(1) = 0$. Then, $B_3 + 2(B_1 + B_2 + 1) = 0$, which implies by (6.2) that $2\zeta = 0$. But this is impossible, and so $\lambda_1 \nmid \beta_D(t)$. Suppose then that $\lambda_2 | \beta_D(t)$, i.e., that $\beta_D(-1) = 0$. Thus, $B_3 = 2(B_2 - B_1 + 1)$, and so by (6.2) we obtain:

$$a_3 = \frac{B_2 - 3B_1 + 4}{3s}, \quad 2\zeta = \tfrac{2}{3}(B_2 + 1). \tag{6.7}$$

But a_3 is a positive integer (it is a multiple of a class number), and so:

$$3B_1 < B_2 + 4. \tag{6.8}$$

Since $\beta_D(t)$ is a P-polynomial (see (3.4)), $(\lambda_2)^2$ divides β_D, by (4.4). Suppose then that $\beta_D(t) = (1 + t)^2\phi$, where ϕ factors into cyclotomic polynomials. (See list below.) If ϕ is cyclotomic of degree 4, then the coefficients (B_1, B_2) of $\beta_D(t)$ can only have the following values: $(3, 4)$, $(2, 1)$, $(1, 0)$ or $(2, 0)$. By (6.8), only the pair $(1, 0)$ is possible – but then by (6.7) and (6.5), $D \leq 37$.

On the other hand, suppose that $\phi = (\deg 2) \times (\deg 2)$, so that

$$\beta_D(t) = (1 + 2t + t^2)(1 + at + t^2)(1 + bt + t^2),$$

where $a, b = 0, \pm 1, 2$, with $a \leq b$. Then,

$$B_1 = 2 + a + b, \quad B_2 = 2a + 2b + ab + 3,$$

and so by (6.8), $a + b \leq ab$. Thus, there are only four possibilities for the pair (a, b):

(a,b)	(B_1, B_2)	$2\zeta_K(-1)$
(2,2)	(6,15)	32/3
(0,0)	(2,3)	8/3
(−1,0)	(1,1)	4/3
(−1,−1)	(0,0)	2/3

By (6.5), in the third and fourth cases above we again have $D \leq 37$. Thus to complete our analysis of the possible factor $(\lambda_2)^2$, we need only show that $2\zeta = 32/3$ or $8/3$ is not possible if $D > 41$. (Note that for $D = 41$, $2\zeta = 8/3$). By page 200 of [7] and by (6.5), we see that if $2\zeta = 8/3$ and $D > 41$, then $D \leq 57$ and $D \equiv 1 \bmod 4$. The only possibilities are $D = 53$ or 57, and for these one easily checks, by (6.3), that $2\zeta \neq 8/3$. Similarly, if $2\zeta = 32/3$, then $D \equiv 1 \bmod 4$ and $D \leq 153$. Using (6.3), one readily shows that $D \geq 97$. One now simply checks the 15 cases, $97 \leq D \leq 153$, $D \equiv 1 \bmod 4$, and finds that for D in this range, $2\zeta \neq 32/3$. Thus, we have shown:

(6.9) *If $\beta_D(t)$ factors into cyclotomic polynomials, with λ_2 a factor, then $D \leq 41$ and the coefficients (B_1, B_2) of $\beta_D(t)$ must be one of the following*: (1,0), (1,1), (0,0).

We now prove (6.6) under the supposition that $\beta_D(t)$ factors into a product of cyclotomic polynomials with degree greater than one. For convenience we list below all such polynomials.

(6.10) TABLE: *Cyclotomic polynomials*

degree 2	degree 4
$\lambda_3 = t^2 + t + 1$	$\lambda_5 = t^4 + t^3 + t^2 + t + 1$
$\lambda_4 = t^2 + 1$	$\lambda_8 = t^4 + 1$
$\lambda_6 = t^2 - t + 1$	$\lambda_{10} = t^4 - t^3 + t^2 - t + 1$
	$\lambda_{12} = t^4 - t^2 + 1$

degree 6

$$\begin{aligned}
\lambda_7 &= t^6 + t^5 + t^4 + t^3 + t^2 + t + 1\\
\lambda_9 &= t^6 + t^3 + 1\\
\lambda_{14} &= t^6 - t^5 + t^4 - t^3 + t^2 - t + 1\\
\lambda_{18} &= t^6 - t^3 + 1
\end{aligned}$$

Suppose first that $\beta_D(t)$ is simply a cyclotomic polynomial of degree 6. By taking the coefficients B_1, B_2 and B_3 for the four polynomials above and inserting these into (6.2), one finds that $2\zeta < 7/3$, and so by (6.5), $D \leq 41$, as stated in (6.6).

We suppose next that $\beta_D(t)$ is a product of a cyclotomic polynomial of degree two and one of degree four. We list below, using (6.10), the possible values of B_1, B_2 and B_3 that could then arise.

(6.11) TABLE: *Values of* (B_1, B_2, B_3) *if* $\beta_D(t) = (\text{degree } 2) \times (\text{degree } 4)$

$(2,3,3)$	$(1,1,0)$	$(0,1,-1)$
$(1,2,2)$	$(0,1,0)$	$(1,0,-1)$
$(0,1,1)$	$(-1,1,0)$	$(-1,2,-2)$
$(-1,0,1)$	$(0,0,0)$	$(-2,3,-3)$

The first triple, $(2,3,3)$, when substituted into (6.2), gives $a_3 = 0$, which is impossible. On the other hand, for the remaining triples we clearly have $B_3 + 2(B_1 + B_2 + 1) < 14$, and so by (6.2), $2\zeta < 7/3$. Thus, by (6.5), $D \leq 41$, as claimed.

To complete the proof of (6.6) we are left with showing that if $\beta_D(t)$ factors into a product of three cyclotomic polynomials, each of degree two, then $D \leq 41$. Again we list below the values of B_1, B_2 and B_3 that can occur.

(6.12) TABLE: *Values of* (B_1, B_2, B_3) *if* $\beta_D(t) = (\text{degree } 2) \times (\text{degree } 2) \times (\text{degree } 2)$

$(3,6,7)$	$(0,3,0)$	$(-1,3,-2)$
$(2,4,4)$	$(0,2,0)$	$(-2,4,-4)$
$(1,3,2)$	$(-1,2,-1)$	$(-3,6,-7)$
$(1,2,1)$		

Note that for the first two triples – $(3,6,7)$ and $(2,4,4)$ – we obtain, by (6.2), $a_3 = 0$, which is impossible. On the other hand, for the remaining eight triples we obtain as above (by (6.2)), $2\zeta < 7/3$, and so $D \leq 41$ as required.

This completes the proof of Proposition (6.6).

Thus to prove Theorem 1 in the "only if" direction, we are left with showing that if $13 < D \leq 41$, then $\beta_D(t)$ does not factor into a product of cyclotomic polynomials. We list below the coefficients B_1, B_2, B_3 that occur, for $13 < D \leq 41$. The data on the left hand side of the Table comes from [7], pages 200 and 239, and [2], page 422.

(6.13) TABLE: *Coefficients of* $\beta_D(t)$, *for* $13 < D \leq 41$.

D	2ζ	χ	h	a_3	s	B_1	B_2	B_3
17	2/3	1	1	2	1/6	−1	2	0
21	2/3	1	1	5	4/15	−1	1	2
24	1	1	1	3	1/3	−1	2	2
28	4/3	1	1	4	1/6	−1	3	2
29	1	2	1	6	1/6	0	1	2
33	2	1	1	3	1/3	−1	4	4
37	5/3	2	1	8	1/6	0	2	4
40	7/3	2	2	4	1/6	1	3	4
41	8/3	2	1	2	1/6	0	5	4

Here we have used (3.4) to calculate the B_i's.

In the proof of (6.6) we showed that $\lambda_1 \nmid \beta_D(t)$ and that if $\lambda_2 \mid \beta_D(t)$, then $(B_1, B_2) = (1,0)$, $(1,1)$ or $(0,0)$. Since these values do not occur in the above Table, we see that neither λ_1 nor λ_2 divides $\beta_D(t)$. Also, by comparing (6.10) and (6.13) we find that $\beta_D(t)$ is not a cyclotomic polynomial of degree 6. The remaining possibility is that $\beta_D(t)$ factors into a product of a cyclotomic polynomial of degree 2 and one of degree 4 or two others of degree 2. However, by comparing (6.13) with (6.11) and (6.12) we find that neither of these factorizations occurs. This completes the proof of Proposition (6.1) which, in turn, proves Theorem 1 in the "only if" direction.

To complete the proof of Theorem 1 we now show that for $D = 5$, 8 and 13, $M(D)$ is a complete intersection ring. This is clear when $D = 5$ and 8 since, by (1.2), these rings have only a single relation. One can verify directly that $M(13)$ is a complete intersection, using the specific calculations given in [5]. This completes the proof of Theorem 1.

We complete the section by giving the evidence for Conjecture 1. For this we need the rational function $\mu_{12}(t)$.

(6.14) PROPOSITION:

$$\mu_{12}(t) = (1 - t^6)(1 - t^8)(1 - t)^{-1}(1 - t^2)^{-1}(1 - t^3)^{-2}(1 - t^4)^{-1}.$$

Note that this is the correct rational function for $M(12)$ to have the structure given in Conjecture 1.

PROOF: As in (6.8) we give the B_i's for $\mu_{12}(t)$, along with the data necessary for the computation.

D	2ζ	χ	h	a_3	s	B_1	B_2	B_3
12	1/3	1	1	2	1/3	-1	1	0

We find that $\mu_{12}(t) = \lambda_6 \cdot \lambda_8 \cdot (1-t)^{-2}(1-t^3)^{-1}$. Multiplying through by $\lambda_1 \cdot \lambda_2 \cdot \lambda_3 \cdot (1-t^4)$ we obtain the form of $\mu_{12}(t)$ given in (6.14).

7. Proof of Theorem 2

Let Γ be a torsion free, normal subgroup of the modular group for a real quadratic field K. As in (4.5), set $\beta_\Gamma(t) = 1 + B_1 t + B_2 t^2 + B_1 t^3 + t^4$, where by (3.9),

$$B_1 = h + \chi - 4, \qquad B_2 = 2(2e\zeta - \chi - h + 3). \tag{7.1}$$

Here $\chi = \chi(\Gamma)$, h = number of cusps for Γ and $\zeta = \zeta_K(-1)$. To show that M_Γ is not a complete intersection ring it suffices (by (5.4)) to show that $\beta_\Gamma(t)$ cannot be factored into a product of cyclotomic polynomials.

Set $E = 2B_1 + B_2 + 2$. By (7.1) and (2.6) we have:

$$E = 4e\zeta = 8(\chi - w). \tag{7.2}$$

Since e and ζ are both positive, so is E. We prove:

(7.3) LEMMA: *If all units in K have positive norm and if the discriminant of K is ≤ 29, then $E \equiv 0 \bmod 4$. If K has a unit of negative norm, then $E \equiv 0 \bmod 8$.*

PROOF: Since G has torsion of order 2 and 3, and since Γ is torsion free and normal, we must have $e \equiv 0 \bmod 6$, say $e = 6f$. Suppose now that K has no unit of negative norm and that $D \leq 29$. By [2], page 422, we see that $D = 12$, 21, 24 or 28; and so by page 200 of [7], $2\zeta = N/3$, where $1 \leq N \leq 4$. Thus, $E = 4e\zeta = 4fN \equiv 0 \bmod 4$. On the other hand if K has a unit of negative norm, then by (2.5), $w = 0$. Hence, by (7.2), $E = 8\chi \equiv 0 \bmod 8$, since χ is an integer. This completes the proof.

To prove Theorem 2 we will show:

(7.4) PROPOSITION: *$\beta_\Gamma(t)$ factors into a product of cyclotomic polynomials if, and only if,* $(D, \mathfrak{A}) = 5, (2))$ *or* $(8, (2))$.

We devote the rest of the section to the proof. Note first that $(1 - t)$ does not divide $\beta_\Gamma(t)$. For if $\beta_\Gamma(1) = 0$, then $E = 0$, which is impossible as noted above. Also, $\beta_\Gamma(t)$ cannot be a cyclotomic polynomial of degree 4. For by (6.10) we see that the integer E for these polynomials has the value 5, 2 or 1. We note below that this implies $D \leq 29$, and hence (7.3) would give a contradiction.

Suppose then that

$$\beta_\Gamma(t) = (1 + at + t^2)(1 + bt + t^2), \tag{7.5}$$

where $a, b = 0, \pm 1, 2$, $a \leq b$. For each such pair (a, b),

$$E = ab + 2(a + b + 2),$$

and so $E \leq 16$. By (7.2), $2\zeta = E/2e = E/12f \leq 4/3$. Thus by (6.5) and page 200 of [7], we have $D \leq 29$, as required above. Using (7.3), we see that if $\beta_\Gamma(t)$ factors as in (7.5), then $E = 4$, 8, 12 or 16. Also, for $D \leq 29$, $2\zeta = 1/15$, 1/6, 1/3, 2/3, 1 or 4/3. Since $e = E/4\zeta$ by (7.2), and since $e \equiv 0 \bmod 6$, we find that

$$e = 6,\ 12,\ 18,\ 24,\ 48,\ 60 \text{ or } 120, \tag{7.6}$$

noting that $E \equiv 0 \bmod 8$, when $2\zeta = 1/15$ or 1/6.

In fact we will show:

(7.7) LEMMA: *If $\beta_\Gamma(t)$ factors as in* (7.5), *with Γ a torsion free principal congruence subgroup, then e (the index of Γ in G) is one of* 6, 12, 48 *or* 60.

We give the proof shortly. Using (7.7), the values of E given above (4, 8, 12, 16), and the fact that $2\zeta = E/2e$, we list below all possible pairs (e, D) that can arise, with $D \leq 29$ and $\beta_\Gamma(t)$ factoring as in (7.5). If K has a unit of negative norm ($D = 5$, 8, 13, 17), we also list the value of χ $(= E/8)$ and the number of cusps, h $(= B_1 + 4 - \chi)$; see (7.1) and (7.2). For the calculation of h note that if $E = 16$, then $B_1 = 4$ (with $B_2 = 6$), while if $E = 8$, then $B_1 = B_2 = 2$.

(7.8)

E	e	2ζ	D	χ	h
4	6	1/3	12		
8	6	2/3	17	1	5
8	6	2/3	21		
12	6	1	24		
16	6	4/3	28		
8	12	1/3	12		
8	12	1/3	13	1	5
16	12	2/3	17	2	6
16	12	2/3	21		
16	48	1/6	8	2	6
8	60	1/15	5	1	5

Now let $\mathfrak{A}$ be a proper ideal in $\mathfrak{o}$ (= ring of integers in K), and set

$$\hat{\Gamma} = \text{Ker}[SL_2(\mathfrak{o}) \to SL_2(\mathfrak{o}/\mathfrak{A})].$$

$\hat{\Gamma}$ acts effectively on H^2 provided $-1 \notin \hat{\Gamma}$, i.e., $2 \notin \mathfrak{A}$. We define

$$\Gamma = \Gamma(D, \mathfrak{A}) = \begin{cases} \hat{\Gamma}, & \text{if } 2 \notin \mathfrak{A} \\ \hat{\Gamma}/\{\pm 1\}, & \text{if } 2 \in \mathfrak{A}. \end{cases}$$

Thus Γ is a normal subgroup of G, which we call the principal congruence subgroup associated to $\mathfrak{A}$ (see [4], §1). Moreover, Γ is torsion free provided

$$\mathfrak{A}^2 \neq (2) \text{ or } (3). \tag{7.9}$$

For the rest of the section we will take Γ to be the principal congruence subgroup associated to a proper ideal $\mathfrak{A}$ satisfying (7.9).

We now take up the proof of (7.4) with Γ as above. In passing, we prove (7.7).

PROOF OF (7.4): The key to the proof is the fact that the index e can be computed from the ideal $\mathfrak{A}$ (see [4], §1). Namely,

$$e = c \cdot N(\mathfrak{A})^3 \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-2}), \tag{7.10}$$

where $N(\ )$ denotes the norm and where the product is over all prime ideals $\mathfrak{p}$ dividing $\mathfrak{A}$. The number c is given by:

$$c = \begin{cases} 1, & \text{if } 2 \in \mathfrak{A} \\ \frac{1}{2}, & \text{if } 2 \notin \mathfrak{A}. \end{cases} \tag{7.11}$$

Similarly we can calculate h, the number of cusps of Γ ([4], §1):

$$hu = e/N(\mathfrak{A}), \tag{7.12}$$

where u denotes the index in the group of all units of the subgroup of those units congruent to 1 mod $\mathfrak{A}$. (We use here the fact that for those fields given in table (7.8), the class number is 1).

From now on assume that $\beta_\Gamma(t)$ factors as in (7.5). We consider separately the two cases $c = \frac{1}{2}$ and $c = 1$. Suppose first that $c = \frac{1}{2}$, i.e. $2 \notin \mathfrak{A}$. Thus, 2 does not divide $N(\mathfrak{A})$. It follows readily from (7.10) that if $N(\mathfrak{A}) \geq 7$, then $e > 120$. Thus by (7.6), $N(\mathfrak{A}) = 3$ or 5; in either case, $\mathfrak{A}$ is then prime. By (7.10), if $N(\mathfrak{A}) = 3$ then $e = 12$, and so by (7.8), $D = 12$, 13, 17 or 21. If $D = 12$ or 21 then $3 | D$ and so $(3) = \mathfrak{A}^2$; but this is ruled out by (7.9). Suppose then that $D = 13$ or 17; by (7.8) we then have $h = 5$ or 6, and so by (7.12), $u = 12/3h = 4/h$, which is impossible. Thus, $N(\mathfrak{A}) \neq 3$. If $N(\mathfrak{A}) = 5$, then $e = 60$ and so $D = 5$ and $h = 5$. Thus by (7.12), $u = 60/5 \cdot 5$, which again is impossible. Thus, if $\beta_\Gamma(t)$ factors as in (7.5), we must have $c \neq \frac{1}{2}$.

Suppose then that $c = 1$; i.e., 2 is in $\mathfrak{A}$. We distinguish four cases: (i) $\mathfrak{A} \cdot \mathfrak{A}' = (2)$, $N(\mathfrak{A}) = 2$, $\mathfrak{A} \neq \mathfrak{A}'$; (ii) $\mathfrak{A} = (2) = \mathfrak{p} \cdot \mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$; (iii) $\mathfrak{A} = (2) = \mathfrak{p}^2$; (iv) $\mathfrak{A} = (2)$, $\mathfrak{A}$ prime.

In case (i), since $\mathfrak{A}$ is prime, $e = 6$ by (7.10). Thus, $D = 12$, 17, 21, 24, 28. When D is even, $(2) = \mathfrak{p}^2$, which contradicts the assumption made in (i). Also, if $D = 21$, then by [2], page 236, 2 remains prime, again a contradiction. Finally, if $D = 17$, then $h = 5$, and so by (7.12) we have $u = 3/5$, which is impossible. Thus case (i) is ruled out.

In case (ii), $N(\mathfrak{A}) = 4$ and so $e = 36$. Since this value of e does not occur in (7.6), case (ii) is also not possible.

Consider then case (iii): again $N(\mathfrak{A}) = 4$, and we find $e = 48$, which by (7.8) implies that $D = 8$. Thus $(D, \mathfrak{A}) = (8, (2))$, one of the two cases given in (7.4).

Finally, in case (iv), since $\mathfrak{A}$ is prime and $N(\mathfrak{A}) = 4$, we obtain $e = 60$, and so $D = 5$. Consequently, we obtain the other example mentioned in (7.4), $(5, (2))$.

To complete the proof of (7.4), and hence of Theorem 2, we are left with showing that if $(D, \mathfrak{A}) = (5, (2))$ or $(8, (2))$, then $\beta_\Gamma(t)$ does factor as given in (7.5). Before proving this, we note that the only values of e found using (7.10) (in the list of possible values given in (7.6)) are 6, 12, 48 and 60, which proves (7.7).

Suppose then that $D = 5$ and $\mathfrak{A} = (2)$. Since $D \equiv 5 \bmod 8$, $\mathfrak{A}$ is prime ([2], page 236). Thus by (7.10), with $c = 1$, $e = 60$. By (7.2), since $2\zeta_K(-1) = 1/15$, $\chi = 1$. Finally one readily computes that $u = 3$, and so by (7.12)

$$h = 60/4 \cdot 3 = 5.$$

Therefore, by (3.9), $B_1 = B_2 = 2$, and so

$$\mu_\Gamma(t) = (1+t)^2(1+t^2)(1-t)^{-3} = (1-t^2)(1-t^4)(1-t)^{-5}.$$

Similarly, if $D = 8$ and $\mathfrak{A} = (2)$, we obtain: $e = 48$, $u = 2$, $h = 6$ and $\chi = 2$. Thus, $B_1 = 4$ and $B_2 = 6$, which gives:

$$\mu_\Gamma(t) = (1+t)^4(1-t)^{-3} = (1-t^2)^4(1-t)^{-7}.$$

Thus (7.4) is proved and hence Theorem 2. Note that for $(D, \mathfrak{A}) = (5,(2))$ the function μ_Γ obtained above agrees with (1.3); moreover, if $(D, \mathfrak{A}) = (8,(2))$, μ_Γ is consistent with Conjecture 2.

REFERENCES

[1] M.F. Atiyah and I.G. Macdonald: Introduction to Commutative Algebra, Addison–Wesley, Reading, Mass., 1969.

[2] Z.I. Borevich and I.R. Shafarevich: Number Theory, Academic Press, New York, 1969.

[3] E. Freitag: Lokale und globale invarianten der Hilbertschen modulgruppe, Invent. Math. 17 (1972), 106–134.

[4] G. van der Geer: Hilbert modular forms for the field $Q(\sqrt{6})$, Math. Ann. 233 (1978), 163–179.

[5] G. van der Geer and D. Zagier: The Hilbert modular group for the field $Q(\sqrt{13})$, Invent. Math. 42 (1977), 93–133.

[6] W. Hammond: The Hilbert modular surface of a real quadratic field, Math. Ann. 200 (1973), 25–45.

[7] F. Hirzebruch: Hilbert modular surfaces, L'Enseignement Math. 19 (1974), 182–281.

[8] F. Hirzebruch: Hilbert's modular group for the field $Q(\sqrt{5})$ and the cubic diagonal surface of Clebsch and Klein, Russian Math. Surveys 31 (1976), 96–110.

[9] F. Hirzebruch: The ring of Hilbert modular forms for real quadratic number fields of small discriminant, Lecture Notes in Math. (vol. 627), Springer-Verlag, Berlin, 1977.

[10] A. Prestel: Die elliptische Fixpunte der Hilbertschen Modulgruppe, Math. Ann. 117 (1968), 181–209.

[11] H. Shimizu: On discontinuous groups operating on the product of upper half planes, Ann. of Math. 77 (1963), 33–71.

[12] R.P. Stanley: Invariants of finite groups and their applications to combinatorics, Bull. A.M.S. (new series) 1 (1979), 443–594.

[13] R.P. STANLEY: Hilbert functions of graded algebras, Advances in Mathematics 28 (1978), 57–83.
[14] E. THOMAS and A. VASQUEZ: Chern numbers of Hilbert modular varieties, J. für r. und ang. Math. 324 (1981), 192–210.
[15] M.-F. VIGNÉRAS: Invariants numériques des groupes de Hilbert, Math. Ann. 224 (1976), 189–215.
[16] D. WEISSER: The arithmetic genus of the Hilbert modular variety and the elliptic fixed points of the Hilbert modular group, Math. Ann. 257 (1981), 9–22.

(Oblatum 18-IV-1981)

Current addresses:

E. Thomas
Department of Mathematics
University of California
Berkeley, CA 94720
U.S.A.

A. Vasquez
Graduate School CUNY
33 W. 42nd St.
New York, NY 10036
U.S.A.