A Hecke algebra attached to mod 2 modular forms of level 5

Paul Monsky

Brandeis University, Waltham MA 02454-9110, USA. monsky@brandeis.edu

Abstract

Let $F$ be the element $\sum_{n \text{ odd}, n > 0} x^{n^2}$ of $\mathbb{Z}/2[[x]]$. Set $G = F(x^5)$, $D = F(x) + F(x^{25})$. For $k > 0$, $(k, 10) = 1$, define $D_k$ as follows. $D_1 = D$, $D_3 = D^5/G$, $D_7 = D^2G$, $D_5 = D^4G$; furthermore $D_{k+10} = G^2D_k$.

Using modular forms of level $\Gamma_0(5)$ we show that the space $W$ spanned by the $D_k$ is stabilized by the formal Hecke operators $T_p: \mathbb{Z}/2[[x]] \to \mathbb{Z}/2[[x]]$, $p \neq 2$ or 5. And we determine the structure of the (completed) shallow Hecke algebra attached to $W$. This algebra proves to be a power series ring in $T_3$ and $T_7$ with an element of square 0 adjoined. As Hecke module, $W$ identifies with a certain subquotient of the space of mod 2 modular forms of level $\Gamma_0(5)$, and our Hecke algebra result parallels findings in level 1 (by J.-L. Nicolas and J.-P. Serre) and in level $\Gamma_0(3)$ by us.

1 Some spaces of mod 2 modular forms of level $\Gamma_0(5)$

Nicolas and Serre [3], [4] have proved various results about the action of the Hecke algebra on the space of mod 2 modular forms of level 1. In [1] we gave a variant of their results in level $\Gamma_0(3)$. Here we find close analogues in level $\Gamma_0(5)$.

We first summarize results from [3], [4] just as we did at the start of [1]. There are commuting formal Hecke operations $T_p: \mathbb{Z}/2[[x]] \to \mathbb{Z}/2[[x]]$, one for each odd prime $p$. Here $T_p(\sum c_n x^n) = \sum c_{pn} x^n + \sum c_n x^{pn}$. Let $F$ in $\mathbb{Z}/2[[x]]$ be $\sum_{n \text{ odd}, n > 0} x^{n^2}$. Using modular forms of level 1, Nicolas and Serre show that the $T_p$ stabilize the space spanned by $F, F^3, F^5, F^7, \ldots$ and that the associated (completed) Hecke algebra is a power series ring in $T_3$ and $T_5$. Indeed they make the space into a faithful $\mathbb{Z}/2[[X,Y]]$-module with $X$ and $Y$ acting by $T_3$ and $T_5$, and show that each $T_p$ is multiplication by an element of the maximal ideal $(X,Y)$. 

1

arXiv:1610.07058v1 [math.NT] 22 Oct 2016.
In [1] we took $D$ in $\mathbb{Z}/2[[x]]$ to be $\sum_{(n,6)=1,\ n>0} x^{n^2}$, so that $D = F(x) + F(x^9)$. $W_1$ had a basis consisting of the $D^k$ with $k \equiv 1 \pmod{6}$ and $W_5$ a basis consisting of the $D^k$, $k \equiv 5 \pmod{6}$; $W$ was $W_1 \oplus W_5$. We showed that the $T_p$ with $p \equiv 1 \pmod{6}$ stabilize $W_1$ and $W_5$, while when $p \equiv 5 \pmod{6}$, $T_p(W_1) \subset W_5$ and $T_p(W_5) \subset W_1$. We further showed that $W_1$ has a basis $\{ \eta_{i,j} \}$ “adapted to $T_7$ and $T_{13}$” with $m_{0,0} = D$. We deduced that the (completed shallow) Hecke algebra attached to $W$ is a power series ring in $T_7$ and $T_{13}$ with an element of square 0 adjoined. Though $W$ is a space of mod 2 modular forms of level $\Gamma_0(9)$, it identifies as Hecke-module with a certain subquotient of the space of odd mod 2 modular forms of level $\Gamma_0(3)$.

In the present work we change notation. Now $D = \sum_{(n,10)=1,\ n>0} x^{n^2}$, so that $D = F(x) + F(x^{25})$. Let $G = F(x^5)$. For $k > 0$ with $(k,10) = 1$ define $D_k$ as follows: $D_1 = D$, $D_3 = D^8/G$, $D_7 = D^2G$ and $D_9 = D^4G$, while $D_{k+10} = G^2D_k$. Let $W$ be spanned by the $D_k$. (As $D_k = x^k + \cdots$, these are linearly independent over $\mathbb{Z}/2$.) Then $W = W_a \oplus W_b$ where the $D_k$, $k \equiv 1,3,7,9 \pmod{20}$, are a basis of $W_a$, and the $D_k$, $k \equiv 11,13,17,19 \pmod{20}$ are a basis of $W_b$. We will establish the following analogues to the results of [1].

1. The $T_p$, $p \neq 5$, stabilize $W$. If $p \equiv 1,3,7,9 \pmod{20}$, $T_p$ stabilizes $W_a$ and $W_b$, while if $p \equiv 11,13,17,19 \pmod{20}$, $T_p(W_a) \subset W_b$ and $T_p(W_b) \subset W_a$.

2. Though $W$ is a space of mod 2 modular forms of level $\Gamma_0(25)$, it identifies as Hecke-module with a certain subquotient of the space of odd mod 2 modular forms of level $\Gamma_0(5)$.

3. $W_a$ admits a basis $\{ \eta_{i,j} \}$ adapted to $T_3$ and $T_7$ in the sense of Nicolas and Serre, with $m_{0,0} = D$.

4. The (completed shallow) Hecke algebra attached to $W$ is a power series ring in $T_3$ and $T_7$ with an element of square 0 adjoined.

The proofs of (1) and (2) occupy sections 1 and 2. Some ingredients are the mod 2 level 5 modular equation $(F + G)^6 = FG$ of Theorem 1.12 and the relation $D^{15} + G^4D^3 + G^3 = 0$ of Lemma 2.4.

The proofs of (3) and (4) resemble those of corresponding results in [1]. We identify $W_a$ with a subspace $V'$ of the polynomial ring $\mathbb{Z}/2[w]$, making $D_k$ correspond to $w^k$, and show that under this identification $T_3(D_k)$ corresponds to a certain $P_k$ defined in [2], with $P_{k+80} = w^{80}P_k + w^{20}P_{k+20}$. Lemma 5.5 of [2], which deals with this recursion, gives insight into the action of $T_3$. Suppose in particular that $q$ is a power of 2, and let $W_a(q)$ be spanned by the $D_k$ in $W_a$ with $k < 40q^2$. Using this Lemma 5.5 we find that the kernel of $T_3 : W_a(q) \to W_a(q)$ has dimension at most $2q$. Ideal theory in $\mathbb{Z}[\sqrt{-1}]$, developed in section 4, then shows that this kernel is a space $DI(q)$ of theta-series attached to binary quadratic forms. A study of the action of $T_7$ on $DI(q)$, together with formalism from [1], leads, in section 5, to a proof of (3). And the further study in section 6 of $T_{11} : W_a \to W_b$ and $W_b \to W_a$ gives a
proof of (4).

We begin our proofs by introducing elements $P, E_4, $ and $B$ of $\mathbb{C}[[x]]$. These are the expansions at infinity of classical modular forms of level $\Gamma_0(5)$.

**Definition 1.1** $P = 1 + \cdots$, $E_4 = 1 + \cdots$ and $B = x + \cdots$ are the expansions at infinity of:

1. The normalized weight 2 Eisenstein series for $\Gamma_0(5)$.
2. The normalized weight 4 Eisenstein series of level 1.
3. The normalized weight 4 Eisenstein series, vanishing at infinity, for $\Gamma_0(5)$.

**Remark** One usually views expansions at infinity of modular forms as elements of $\mathbb{C}[[q]]$ where $q = e^{2\pi i z}$. But as in [1] we’ll use the letter $x$ rather than the letter $q$.

**Definition 1.2** $r$ in $\mathbb{Z}/2[[x]]$ is $\sum_{n>0}(x^{n^2} + x^{2n^2} + x^{5n^2} + x^{10n^2})$.

Classical formulae for the coefficients of Eisenstein series show that $P$, $E_4$ and $B$ are in $\mathbb{Z}[[x]]$ with mod 2 reductions 1, 1 and $r$.

**Definition 1.3** $C$ in $\mathbb{C}[[x]]$ is the expansion at infinity of the normalized weight 4 cusp form $(\eta(z)\eta(5z))^4$ for $\Gamma_0(5)$.

Now the expansion of $\eta(z)$ at infinity is $x^{1/24}(an$ element $1 - x - x^2 + \cdots$ of $\mathbb{Z}[[x]])$. We deduce:

**Lemma 1.4** $C$ is in $\mathbb{Z}[[x]]$ and is $x - 4x^2 + \cdots$.

We now show that the mod 2 reduction $\overline{C}$ of $C$ is $r^2 + r$.

**Lemma 1.5** Let $n$ be a positive integer. The number of $(a,b)$ in $\mathbb{Z} \times \mathbb{Z}$ with $a^2 + 5b^2 = 6n$ and $a \equiv b \equiv 3 \pmod{2}$ is 2 mod 4 if $n$ is either a square or $5\cdot$ (an odd square), and 0 mod 4 otherwise.

**Proof** Let $S(n)$ be the set of such $(a,b)$. Then $T : (a,b) \rightarrow (-a,-b)$ and $U : (a,b) \rightarrow \left(\frac{2a - 5b}{3}, \frac{-a - 2b}{3}\right)$ are commuting involutions of $S(a)$. $T$ has no fixed points, while the fixed points of $U$ (resp. $TU$) are of the form $(5k,-k)$ (resp. $(k,k)$). In the first case, $5k^2 = n$ while in the second $k^2 = n$. So we have an action of $\mathbb{Z}/2 \times \mathbb{Z}/2$ on $S(n)$ in which all orbits are of size 4 with the following exceptions. When $n = 5k^2$ there is a size 2 orbit $\pm(5k,-k)$. Where $n = k^2$ there is a size 2 orbit $\pm(k,k)$. The result follows.

**Lemma 1.6** Let $n$ be an integer. The number of $(a,b)$ in $\mathbb{Z} \times \mathbb{Z}$ with $a^2 + 5b^2 = 6n$ and $a \equiv b \equiv 1 \pmod{6}$ is odd if $n$ is an odd square or $5\cdot$ (an odd square), and even otherwise.
We may assume $n \geq 0$. Since $a^2 + 5b^2$ is $2 \mod 4$, there are no such pairs when $n$ is even. For fixed odd $n > 0$ the pairs of Lemma 1.5 come in three types according as $a \equiv b \equiv 1 (6)$, $a \equiv b \equiv 5 (6)$, or $a \equiv b \equiv 3 (6)$. There are as many pairs of the first type as there are of the second. So in view of Lemma 1.5 it suffices to show that the number of pairs of the third type is a multiple of 4. But these pairs come in sets of 4, $(\pm a, \pm b)$. □

**Lemma 1.7** The mod 2 reduction $\bar{C}$ of $C$ is $r^2 + r$.

**Proof** Using the familiar expansion of $\eta(z)$ at infinity we find that $\bar{C} = \left( \sum_{a=1}^{6} a^{2/6} \right) \left( \sum_{b=1}^{6} b^{5b^2/6} \right)$. The coefficient of $x^n$ in this element of $\mathbb{Z}/2[[x]]$ is the mod 2 reduction of the number of $(a, b)$ in $\mathbb{Z} \times \mathbb{Z}$ with $a^2 + 5b^2 = 6n$ and $a \equiv b \equiv 1 (6)$. So by Lemma 1.6, $\bar{C} = \sum_{n \text{ odd}, n > 0} (x^{n^2} + x^{5n^2})$. This is precisely $r^2 + r$. □

**Definition 1.8** If $k \geq 0$ and even, $M_k$ consists of those $f$ in $\mathbb{Z}/2[[x]]$ for which there is a weight $k$ modular form of level $\Gamma_0(5)$ whose expansion at infinity lies in $\mathbb{Z}[[x]]$ and reduces to $f$.

Using multiplication by $E_4$ we see that $M_0 \subset M_4 \subset M_8 \subset \ldots$

**Definition 1.9** $M = \cup M_{4m}$ is “the space of mod 2 modular forms of level $\Gamma_0(5)$.” $M(\text{odd})$ consists of the odd elements of $M$, i.e. those elements lying in $x \cdot \mathbb{Z}/2[[x^2]]$.

Note that $M$ is a subring of $\mathbb{Z}/2[[x]]$. Since the reductions of $E_4$ and $B$ are 1 and $r$, $M \supset \mathbb{Z}/2[r]$. Since $r^2 + r = \sum_{n \text{ odd}, n > 0} (x^{n^2} + x^{5n^2})$ is odd, each $r^{2k}(r^2 + r)$ is in $M(\text{odd})$.

**Theorem 1.10** Fix $m \geq 0$ and suppose $0 \leq i \leq 2m$. Then there is a weight $4m$ modular form $u_i$ of level $\Gamma_0(5)$ whose expansion at infinity has the following properties. It is $x^i + \ldots$, lies in $\mathbb{Z}[[x]]$, and reduces to $r^i$.

**Proof** It suffices to prove this when $m = 1$, so the weight is 4. For $i = 0$ we take $P^2$ whose expansion reduces to 1, while for $i = 1$ we take $B$ whose expansion reduces to $r$. Now $E_4 = 1 + 240x + 2160x^2 + \ldots$, $P^2 = (1 + 6x + 18x^2 + \ldots)^2$ and $B = x + 9x^2 + \ldots$ are expansions at infinity of weight 4 forms of level $\Gamma_0(5)$, and $E_4 - P^2 - 228B = 36x^2 + \ldots$. Also $B - C = 13x^2 + \ldots$, so a $Z$-linear combination of these last two expansions such as $4(\text{first}) - 11(\text{second})$ is $x^2 + \ldots$. And the mod 2 reduction of this linear combination is $B - C$ which is $r^2$ by Lemma 1.7. □

**Theorem 1.11** The $r^i$, $0 \leq i \leq 2m$, are a basis of $M_{4m}$ over $\mathbb{Z}/2$. It follows that $M = \mathbb{Z}/2[r]$. Furthermore the $r^{2k}(r^2 + r)$ are a basis of $M(\text{odd})$ over $\mathbb{Z}/2$.

**Proof** Theorem 1.10 shows that the $r^i$, $0 \leq i \leq 2m$, lie in $M_{4m}$. Now the
are the reductions of the expansions at infinity of ∆(z), so lie in \( M_r \) with the

Recall now that \( G \) is a sum of odd power series. Theorem 1.11 shows that over \( \mathbb{C} \) the elements of \( M_r \) are a basis for the subspace of \( M_{4m} \) consisting of odd power series. \( \square \)

Recall now that \( F \) in \( \mathbb{Z}/2[[x]] \) is \( \sum_{n \text{ odd}, n>0} x^{n^2} \), while \( G = F(x^5) \). We have seen that \( r^2 + r = F + G \).

**Theorem 1.12**

(1) \( F \) and \( G \) lie in \( M_{12} \).
(2) \( G = r^5(r+1), \quad F = r(r+1)^5 \), and \( (F + G)^6 = FG \).

**Proof** Let \( \Delta \) be Ramanujan’s weight 12 level 1 cusp form. Then \( F \) and \( G \) are the reductions of the expansions at infinity of \( \Delta(z) \) and \( \Delta(5z) \), and so lie in \( M_{12} \). Theorem 1.11 shows that \( G \) is a \( Z/2 \)-linear combination of \( r^2 + r, \quad r^4 + r^3 \) and \( r^6 + r^5 \). As \( G = x^5 + \cdots \) it can only be \( r^6 + r^5 \). Then \( F = r^6 + r^5 + r^2 + r = r(r+1)^5 \). The final result is immediate. \( \square \)

**Theorem 1.13** \( M(\text{odd}) \) is spanned by the \( F^iG^j \) with \( i + j \) odd.

**Proof** \( r^2 + r = F + G \), while \( r^4 + r^3 = (r^2 + r)^3 + r^6 + r^5 = (F + G)^3 + G \). Furthermore, \( (r^4 + r^2)(r^{2k+2} + r^{2k+1}) + r^{2k+4} + r^{2k+3} = r^{2k+6} + r^{2k+5} \). Since \( r^4 + r^2 = F^2 + G^2 \), an induction on \( k \) shows that each \( r^{2k+2} + r^{2k+1} \) is a sum of \( F^iG^j \) with \( i + j \) odd. \( \square \)

Suppose now that \( p \) is prime, \( p \neq 2 \) or 5. Then we have commuting formal Hecke operators \( T_p : \mathbb{Z}/2[[x]] \to \mathbb{Z}/2[[x]] \) with \( T_p \) taking \( \sum c_n x^n \) to \( \sum c_{pn} x^n + \sum c_n x^{pn} \).

**Theorem 1.14** The \( T_p \) stabilize \( M \) and \( M(\text{odd}) \). In fact they stabilize the space spanned by the \( r^i \) with \( 0 \leq i \leq 2m \), as well as the space spanned by the \( r^{2i}(r^2 + r) \), \( 0 \leq i \leq m - 1 \).

**Proof** We may assume \( m > 0 \). Consider the \( Z \)-submodule of \( \mathbb{Z}[[x]] \) consisting of those elements of \( Z[[x]] \) that are expansions at infinity of weight \( 4m \) modular form of level \( \Gamma_0(5) \). This module is stabilized by each classical Hecke operator \( T_p : \sum c_n x^n \to \sum c_{pn} x^n + p^{4m-1} \sum c_n x^{pn}, \quad p \neq 5 \). Reducing mod 2 and using Theorem 1.11 we get the result. \( \square \)

**Remark** Multiplication by \( G^2 \) stabilizes \( M(\text{odd}) \). Since \( (F + G)^6 = FG \),
Theorem 1.13 shows that \( M(\text{odd}) \), viewed as \( \mathbb{Z}/2[\mathbb{G}^2] \)-module, is spanned by \( F, F^3, F^5, G, F^2G \) and \( F^4G \). As \( F \) has degree 6 over \( \mathbb{Z}/2(G) \), a basis of \( M(\text{odd}) \) as \( \mathbb{Z}/2[\mathbb{G}^2] \)-module is \( \{ G, F, F^2G, F^3, F^4G, F^5 \} \).

Definition 1.15

(1) \( N2 \subset M(\text{odd}) \) has \( \mathbb{Z}/2[\mathbb{G}^2] \)-basis \( \{ G, F, F^2G, F^3, F^4G \} \).

(2) \( N1 \subset N2 \) has \( \mathbb{Z}/2[\mathbb{G}^2] \)-basis \( \{ G \} \).

Definition 1.16 \( J_1, J_3, J_5, J_7 \) and \( J_9 \) are \( F, F^8/G, G, F^2G \) and \( F^4G \).

\( J_1, J_5, J_7 \) and \( J_9 \) are evidently in \( N2 \). Since \( (F + G)^8 = FG(F + G)^2 \), \( F^8 = G^8 + FG(F + G)^2 \), and \( J_3 = G^7 + F(F + G)^2 \) is also in \( N2 \). Now \( G, F, F^2G, F^3 \) and \( F^4G \) evidently generate the same \( \mathbb{Z}/2[\mathbb{G}^2] \)-module as do \( J_5, J_1, J_7, J_3 \) and \( J_9 \). Consequently:

Theorem 1.17

(1) \( J_1, J_3, J_5, J_7 \) and \( J_9 \) are a \( \mathbb{Z}/2[\mathbb{G}^2] \)-basis of \( N2 \), while \( J_1, J_3, J_7, J_9 \) are a \( \mathbb{Z}/2[\mathbb{G}^2] \)-basis of \( N2/N1 \).

(2) Define \( J_k, k \) odd, \( k > 0 \), by taking \( J_{k+10} \) to be \( G^2 J_k \). Then the \( J_k \) with \( (k, 10) = 1 \) are a \( \mathbb{Z}/2 \)-basis of \( N2/N1 \).

Remarks

(1) The space spanned by the \( F^k \), \( k \) odd and \( > 0 \), is stabilized by the \( T_p \) with \( p \neq 2 \). It follows that \( N1 \) is stabilized by the \( T_p \) with \( p \neq 2 \) or \( 5 \).

(2) One may describe \( N2 \) more elegantly as follows. \( \mathbb{Z}/2(F,G) \) is a degree 6 field extension of \( \mathbb{Z}/2(G) \), and we have a trace map, \( \mathbb{Z}/2(F,G) \to \mathbb{Z}/2(G) \). Using the identity \( (F + G)^6 = FG \) we find that \( F^8, 0 \leq i \leq 4 \), have trace 0, while \( F^5 \) has trace \( G \). So \( N2 \) consists of those elements of \( M(\text{odd}) \) of trace 0. We’ll see in the next section that the \( T_p, p \neq 2 \) or \( 5 \) stabilize not only \( M(\text{odd}) \) and \( N1 \), but also \( N2 \).

2 The spaces \( W, W_a \) and \( W_b \). A decomposition of \( N2/N1 \)

Definition 2.1 \( H = F(x^{25}) = G(x^5) \).

As we noted in section 1, \( D = \sum_{(n,10)=1,\ n>0} x^{n^2} \) is \( F + H \).

Definition 2.2 \( pr : \mathbb{Z}/2[[x]] \to \mathbb{Z}/2[[x]] \) takes \( \sum c_n x^n \) to \( \sum_{(n,5)=1} c_n x^n \).

Since \( G \) lies in \( \mathbb{Z}/2[[x^5]] \), \( pr \) is \( \mathbb{Z}/2[\mathbb{G}] \)-linear and \( pr(\mathbb{N}) = 0 \). The effect of \( pr \) on the \( \mathbb{Z}/2[\mathbb{G}^2] \)-basis \( \{ J_1, J_3, J_7, J_9 \} \) of \( N2/N1 \) is easily described:

Lemma 2.3 \( pr \) takes \( J_1, J_3, J_7, J_9 \) to \( D, D^8/G, D^2G, D^4G \).
Proof \( pr(J_3) = pr(F^8/G) = pr((H^8 + D^8)/G) = pr(D^8/G). \) Since all exponents appearing in \( D \) are prime to 5, the same holds for all exponents appearing in \( D^8/G \) and \( pr(D^8/G) = D^8/G \). The other results have similar proofs. \( \Box \)

Lemma 2.4 \( D^{15} + G^4D^3 + G^5 = 0. \)

Proof \( (F + G)^6 = FG. \) Replacing \( x \) by \( x^5 \) we find that \( (G + H)^6 = GH. \) So \( (D + F + G)^6 = G(D + F). \) Adding \( FG \) to both sides, expanding in powers of \( D \) and dividing by \( D \) we find that \( D^5 + (F + G)^2D^3 + (F + G)^4D = G. \) So if we set \( A = (F + G)^2, \) then:

\[
(1) \quad DA^2 + D^3A + (D^8 + G) = 0.
\]

On the other hand, \( A^3 = (F + G)^6 = FG. \) So \( A^6 = (A + G^2)G^2, \) and:

\[
(2) \quad A^6 + G^2A + G^4 = 0.
\]

We can now eliminate \( A \) from (1) and (2) to get our result. Explicitly, when we multiply (1) by \( DA^4 + D^3A^3 + GA^2 + D^7A, \) (2) by \( D^2, \) and add, all terms involving \( A^6, A^5, A^4 \) or \( A^3 \) drop out, and we find that \( (D^{10} + D^5G + G^2)(A^2 + D^2A) + D^2G^4 = 0. \) Let \( B = A^2 + D^2A. \) Then \( (D^{10} + D^5G + G^2)B = D^2G^4. \) Also, (1) tells us that \( DB = D^5 + G. \) So \( (D^{10} + D^5G + G^2)(D^5 + G) = D^3G^4, \) as desired. \( \Box \)

Multiplying by \( D^5/G^4 \) gives:

Corollary 2.5 \( (D^5/G)^4 + D^5/G = D^8. \)

Definition 2.6 When \( (i, 10) = 1, D_i = pr(J_i). \)

As we’ve seen, \( D_1, D_3, D_7 \) and \( D_9 \) are \( D, D^8/G, D^2G \) and \( D^4G. \) And since \( pr \) is \( Z/2[G^2]-linear, \( D_{i+10} = G^2D_i. \)

Theorem 2.7 The \( D_i \) are linearly independent over \( Z/2. \) So \( pr \) maps \( N2/N1 \) bijectively to the space \( W \) spanned by the \( D_i. \) (Recall that the \( J_k \) with \( (k, 10) = 1 \) are a \( Z/2 \)-basis of \( N2/N1. \))

Proof \( G \) is transcendental over \( Z/2. \) It follows from Lemma 2.4 that \( D \) has degree 15 over \( Z/2(G), \) so that \( D, D^8, D^2 \) and \( D^4 \) are linearly independent over this field. Consequently, \( D_1 = D, D_3 = D^8/G, D_7 = D^2G \) and \( D_9 = D^4G \) are linearly independent over \( Z/2[G^2], \) giving the result. \( \Box \)

Remark \( W \) does not consist of mod 2 modular forms of level 5. In fact the elements of \( W \) “are of level 25.”

We shall see that the \( T_p \) \( (p \neq 2 \) or \( 5 \) as usual) stabilize both \( W \) and \( N2. \) To this end we use a real Dirichlet character \( \chi, \) of modulus 20, to write \( W \) as
a direct sum of $Z/2[G^4]$-submodules, $W_a$ and $W_b$. Then we show that the $T_p$ with $\chi(p) = 1$ stabilize $W_a$ and $W_b$, while those with $\chi(p) = -1$ take $W_a$ to $W_b$ and $W_b$ to $W_a$.

**Definition 2.8** $\chi$ is the mod 20 Dirichlet character taking 1, 3, 7, 9 to 1, and taking 11, 13, 17, 19 to $-1$.

**Definition 2.9** $W_a$ (resp. $W_b$) is the subspace of $W$ spanned by the $D_i$ with $\chi(i) = 1$ (resp. $-1$).

Evidently $W_a$ and $W_b$ are $Z/2[G^4]$-submodules of $W$ with bases $\{D_1, D_3, D_7, D_9\}$ and $\{D_{11}, D_{13}, D_{17}, D_{19}\}$. And $W = W_a \oplus W_b$.

**Lemma 2.10** If $x^n$ appears in $D_k$, $n$ is $k$ or $9k$ mod 40. In particular when $x^n$ appears in $D_k$, $\chi(n) = \chi(k)$.

**Proof** Since $D_{k+10} = G^2D_k$ and all exponents appearing in $G^2$ are 10 mod 40, it suffices to prove the lemma for $k$ in $\{1, 3, 7, 9\}$. Suppose for example $k = 9$, so that $D_k = D^4G$. If $(i, 10) = 1$, $i^2 \equiv 1$ or $9$ mod 40. So all exponents appearing in $D$ are 1 or 9 mod 40, and all exponents in $D^4G$ are $4 + 5 = 9$ or $36 + 5 = 41$ mod 40. The other cases are handled similarly. $\square$

**Definition 2.11**

$p_a : Z/2[[x]] \to Z/2[[x]]$ takes $\sum n x^n$ to $\sum \chi(n) = 1 c_n x^n$.

$p_b : Z/2[[x]] \to Z/2[[x]]$ takes $\sum n x^n$ to $\sum \chi(n) = -1 c_n x^n$.

$p_a$ and $p_b$ are evidently $Z/2[G^4]$-linear. Furthermore:

**Lemma 2.12** $p_a(G^2f)$ and $p_b(G^2f)$ are $G^2p_b(f)$ and $G^2p_a(f)$.

**Proof** We may assume that all the exponents appearing in $f$ are congruent to some fixed $k$ mod 20. Then the exponents in $G^2f$ are congruent to $k + 10$, and we use the fact that $\chi(k + 10) = -\chi(k)$. $\square$

**Lemma 2.13**

If $\chi(k) = 1$, $p_a(J_k) = D_k$ and $p_b(J_k) = 0$.

If $\chi(k) = -1$, $p_a(J_k) = 0$ and $p_b(J_k) = D_k$.

**Proof** Since $pr(J_k) = D_k$, $p_a(J_k) = p_a(D_k)$ while $p_b(J_k) = p_b(D_k)$. Lemma 2.10 then gives the result. $\square$

As $Z/2[G^4]$-module, $N2/N1$ has basis $\{J_1, J_3, J_7, J_9, J_{11}, J_{13}, J_{17}, J_{19}\}$. Evidently $N2/N1 = N2a \oplus N2b$, where $N2a$ and $N2b$ are the $Z/2[G^4]$-submodules with bases $\{J_1, J_3, J_7, J_9\}$ and $\{J_{11}, J_{13}, J_{17}, J_{19}\}$. The $J_k$ with $\chi(k) = 1$ are a $Z/2$-basis of $N2a$; those with $\chi(k) = -1$ are a $Z/2$-basis of $N2b$. Lemma 2.13 now shows that $p_a$ maps $N2/N1$ onto $W_a$ with kernel $N2b$, while $p_b$ maps
Suppose now that $f$ is in $M(\text{odd})/N1$. We'll show that if $p_b(f) = 0$, then $f$ is in $N2a$, while if $p_a(f) = 0$, $f$ is in $N2b$. So in either case, $f$ is in $N2/N1$. This is key to showing that the $T_p$ stabilize $N2$.

Lemma 2.14 $p_a(F(F+G)^4) = p_a(r^8G)$ and $p_b(F(F+G)^4) = p_b(r^8G)$.

Proof $F(F+G)^4 = r(r+1)^5(r^2+r)^4 = (r+1)^8(r^6+r^5) = r^8G + G$. Now apply $p_a$ and $p_b$. □

Lemma 2.15 Let $S = p_a(r^8G)$, $T = p_b(r^8G)$. Then $T = D^5 + G$, $S = D^{10}/G + G$.

Proof Since $r+r^2 = F+G$, $r^8G = G((F+G)^8 + (F+G)^{16} + (F+G)^{32} + \cdots)$. So $pr(r^8G) = G(D^8 + D^{10} + D^{32} + \cdots)$. Now all exponents $n$ appearing in any of $GD^8$, $GD^{32}$, $GD^{128}$, \ldots are 13 or 37 mod 40, while those in any of $GD^{16}$, $GD^{64}$, \ldots are 21 or 69 mod 40. Applying $p_b$ to our identity we find that $T = G(D^8 + D^{32} + D^{128} + \cdots)$. Then $(T/G)^4 + (T/G) = D^8$. So by Corollary 2.5, $T/G$ and $D^5/G$ differ by a constant, and comparing expansions we see that the constant is 1. So $T = D^5 + G$. Finally $S = G(D^{16} + D^{64} + D^{256} + \cdots) = T^2/G$. □

Lemma 2.16

1. $p_a(F(F+G)^4) = D^{10}/G + G$, $p_b(F(F+G)^4) = D^5 + G$.
2. $p_a(FG^2(F+G)^4) = D^5G^2 + G^3$, $p_b(FG^2(F+G)^4) = D^{10}G + G^3$.

Proof Lemmas 2.14 and 2.15 give (1), and Lemma 2.12 yields (2). □

We saw in the remark following the proof of Theorem 1.14 that a basis of $M(\text{odd})$ as $Z/2[G^2]$-module is \{G, F, F^2G, F^3, F^4G, F^5\}. The last five of those elements then give a basis of $M(\text{odd})/N1$. It follows that another $Z/2[G^2]$-basis of $M(\text{odd})/N1$ is \{J_1, J_3, J_7, J_9, F(F+G)^4\}. Then a $Z/2[G^4]$-basis of $M(\text{odd})/N1$ is \{J_1, J_3, J_7, J_9, J_{11}, J_{13}, J_{17}, J_{19}, F(F+G)^4, FG^2(F+G)^4\}.

Theorem 2.17 The kernels of $p_b : M(\text{odd})/N1 \to Z/2[[x]]$ and $p_a : M(\text{odd})/N1 \to Z/2[[x]]$ are N2a and N2b where N2a and N2b have $Z/2[G^4]$-module bases \{J_1, J_3, J_7, J_9\} and \{J_{11}, J_{13}, J_{17}, J_{19}\}.

Proof Consider the 10 element $Z/2[G^4]$-module basis of $M(\text{odd})/N1$ given in the sentence preceding Theorem 2.17. $p_b$ annihilates $J_1, J_3, J_7$ and $J_9$ and sends the last 6 basis elements to $D_{11} = DG^2$, $D_{13} = D^8G$, $D_{17} = D^2G^3$, $D_{19} = D^4G^3$, $D^5 + G$ and $D^{10}G + G^3$; see Lemma 2.16. As we’ve seen, $D$ has degree 15 over $Z/2(G)$, and so $D, D^8, D^2, D^4, D^5 + G$ and $D^{10} + G^2$ are linearly independent over this field. So no non-trivial $Z/2[G^4]$-linear combination of $D_{11}, D_{13}, D_{17}, D_{19}, D^5 + G$ and $D^{10} + G^3$ is zero, and the result for $p_b$ follows.
The result for \( p_a \) is proved similarly. \( \square \)

**Corollary 2.18**

1. If \( \chi(p) = 1 \), \( T_p \) stabilizes \( N2a \) and \( N2b \).
2. If \( \chi(p) = -1 \), \( T_p \) maps \( N2a \) to \( N2b \) and \( N2b \) to \( N2a \).

**Proof** For example suppose \( f \) is in \( N2b \) with \( \chi(p) = -1 \). Then the exponents, \( n \), appearing in (a representative of) \( f \) have \( \chi(n) = -1 \) or \( 0 \). Since \( \chi \) is multiplicative, the exponents appearing in \( T_p \) applied to this representative have \( \chi(n) = 1 \) or \( 0 \). In other words, \( T_p(f) \) is an element of \( M(\text{odd})/N1 \) in the kernel of \( p_b \). By Theorem 2.17, \( T_p(f) \) is in \( N2a \). The other cases are treated similarly. \( \square \)

**Theorem 2.19** If \( p \not\equiv 2 \) or \( 5 \), \( T_p \) stabilizes \( N2 \) and \( W \).

**Proof** If \( h \) is in \( N2 \), the image of \( h \) in \( N2/N1 \) is the sum of an element of \( N2a \) and an element of \( N2b \). By Corollary 2.18, the same holds for the image of \( T_p(h) \) in \( M(\text{odd})/N1 \). So this image is in \( N2/N1 \) and \( h \) is in \( N2 \). Suppose \( f \) is in \( W \). Then \( f = pr(h) \) with \( h \) in \( N2 \). Then \( T_p(h) \) is in \( N2 \), and \( T_p(f) = pr(T_p(h)) \) is in \( W \). \( \square \)

**Corollary 2.20** Suppose \( p \not\equiv 2 \) or \( 5 \), and \( (n, 10) = 1 \). Then \( T_p(D_n) \) is a sum of distinct \( D_k \). In such a decomposition each \( k \) is either \( pn \) or \( 9pn \) mod 40, and in particular \( \chi(k) = \chi(p)\chi(n) \).

**Proof** Since \( D_n \) is in \( W \), so is \( T_p(D_n) \), giving the first result. Also the exponents appearing in \( T_p(D_n) \) are all congruent to \( pn \) or \( 9pn \) mod 40 (by Lemma 2.10 and the definition of \( T_p \)) while those appearing in a \( D_k \) are \( k \) or \( 9k \) mod 40. It follows easily that those \( D_k \) appearing in the sum for which \( k \) is neither congruent to \( pn \) nor to \( 9pn \) mod 40 sum to 0. So there are no such \( k \). \( \square \)

**Remark** Since \( N2/N1 = N2a \oplus N2b \), \( pr : N2/N1 \to Z/2[[x]] \) is 1–1 with image \( W_a \oplus W_b = W \). So \( pr \) gives an identification of the subquotient \( N2/N1 \) of \( M(\text{odd}) \) with \( W \). Now the \( T_p, p \not\equiv 2 \) or \( 5 \), stabilize \( N2/N1 \) and \( W \), and the identification preserves the action of \( T_p \). Corollary 2.20 and this identification are the quoted results (1) and (2) at the beginning of section 1.

We show next that when \( p \equiv 3 \) or \( 7 \) (10), each \( k \) in Corollary 2.20 is \( < n \). (This is also true when \( p \equiv 1 \) or \( 9 \), but this will only be proved in the final section.)

**Definition 2.21** \( v_2 = r^2+r, v_4 = r^4+r^3, v_6 = r^6+r^5, v_{10} = r^{10}+r^9+r^8+r^7, v_{12} = r^{12}+r^{11}+r^{10}+r^9 \).

Note that \( v_2 = F+G, v_4 = (F+G)^3+G, v_6 = G, v_{10} = (F+G)^2G \) and \( v_{12} = (F+G)^4G+(F+G)G^2 \). So \( v_2, v_4, v_6, v_{10} \) and \( v_{12} \) generate the same
$Z/2[G^2]$-submodule of $M(odd)$ as do $G$, $F$, $F^2G$, $F^3$ and $F^4G$; that is to say they generate $N2$. Since $G^2 = r^{12} + r^{10}$, $G^{2s}v_j$ is an element of $N2$ whose degree in $r$ is $12s + j$.

**Lemma 2.22** $T_p(D_{10m+3})$ and $T_p(D_{10m+7})$ are sums of $D_k$ with $k \leq 10m + 7$.

**Proof** $J_7 = F^2G \equiv v_10 \mod N1$. And $J_3 = F^8/G = (F+G)^8/G + G^7 = F(F + G)^2 + G^7$. So mod $N1$, $J_3 + J_7 \equiv (F + G)^3 \equiv v_4$. It follows that $J_{10m+3} = G^{2m}J_3$ and $J_{10m+7} = G^{2m}J_7$ are each congruent mod $N1$ to polynomials in $r$ of degree $\leq 12m + 10$. By Theorem 1.14 the same is true of $T_p(J_{10m+3})$ and $T_p(J_{10m+7})$. (Note also that $J_1 = F \equiv v_2 \mod N1$ while $J_9 + J_{11} = F^4G + FG^2 \equiv v_{12}$.)

Now take an $h$ of degree $\leq 12m + 10$ in $r$ which is congruent mod $N1$ to $T_p(J_{10m+3})$ (or to $T_p(J_{10m+7})$). Since $J_{10m+3}$ and $J_{10m+7}$ are in $N2$, so is $h$. Write $h$ as a sum of distinct $G^{2s}v_i$ with each $i$ in $\{2, 4, 6, 10, 12\}$. The degree in $r$ of $G^{2s}v_i$ is $12s + i$. These degrees are distinct, and since the degree of $h$ is $\leq 12m + 10$, the $s$ appearing in those $G^{2s}v_i$ with $i = 12$ are all $\leq m$, while the remaining $s$ are all $\leq m$. Since $v_2$, $v_4$, $v_6$, $v_{10}$ and $v_{12}$ are congruent mod $N1$ to $J_1$, $J_3 + J_7$, $0$, $J_7$ and $J_9 + J_{11}$, and each of $10m + 1, 10m + 7, 10m + 7, 10(m - 1) + 11$ is $\leq 10m + 7$, each $G^{2s}v_i$ appearing in the sum for $h$ is, mod $N1$, a sum of $J_k$ with $k \leq 10m + 7$. Applying $pr$ to the identity $h = \sum G^{2s}v_i$, noting that $pr$ preserves the action of $T_p$ and that $pr(J_k)$ is either $D_k$ or $0$, we get the result. □

**Lemma 2.23** $T_p(D_{10m+9})$ and $T_p(D_{10m+11})$ are sums of $D_k$ with $k \leq 10m + 11$.

**Proof** $J_{11} = G^2J_1 \equiv G^2v_2 \mod N1$, while $J_9 + J_{11} \equiv v_{12}$. It follows that $J_{10m+9}$ and $J_{10m+11}$ are congruent mod $N1$ to polynomials in $r$ of degree $\leq 12m + 14$. By Theorem 1.14, the same is true of $T_p(J_{10m+9})$ and $T_p(J_{10m+11})$. Now take an $h$ of degree $\leq 12m + 14$ in $r$ which mod $N1$ is $T_p(J_{10m+9})$ (or $T_p(J_{10m+11})$). $h$ is in $N2$ and we write it as a sum of distinct $G^{2s}v_i$, $i$ in $\{2, 4, 6, 10, 12\}$. Arguing as in the proof of Lemma 2.22 we find that the $s$ appearing in the $G^{2s}v_i$ with $i = 2$ are $\leq m + 1$, while the remaining $s$ are $\leq m$, and we continue as in the proof of Lemma 2.22. □

**Theorem 2.24** Suppose $p \equiv 3 \text{ or } 7 \pmod{10}$. When we write $T_p(D_n)$ as a sum of distinct $D_k$, each $k < n$.

**Proof** Suppose $n = 10m + 3$ or $10m + 7$. By Lemma 2.22, $T_p(D_n)$ is a sum of distinct $D_k$, $k \leq 10m + 7$. By Corollary 2.20, each $k \equiv pn$ or $9pn \pmod{10}$ and so is 1 or 9 mod 10. So no $k$ can be $10m + 3$ or $10m + 7$. If $n = 10m + 9$ or $10m + 11$, $T_p(D_n)$ is, by Lemma 2.23, a sum of $D_k$, $k \leq 10m + 11$. Then each $k \equiv pn$ or $9pn \pmod{10}$ and so is 3 or 7 mod 10. So no $k$ is $10m + 9$ or $10m + 11$. Finally, $T_p(D_1) = T_p(D) = 0$. □

We shall write down a linear recursion satisfied by the $T_3(D_n)$, $n \equiv 1, 3, 7, 9 \pmod{20}$.  

11
This recursion, together with some initial condition results, proved with the help of Theorem 2.24 when \( p = 3 \), allow us to relate \( T_3(D_n) \) to a polynomial \( P_n \) appearing in section 5 of [2].

**Lemma 2.25** For \( u \) in \( Z/2[[x]] \), \( T_3(G^16u) = G^16T_3(u) + G^4T_3(G^4u) \).

**Proof** Let \( u \) be the 2-variable polynomial \( A^4 + B^4 + AB \). We have the “level 3 modular equation for \( F \)” \( U(F(x^3), F(x)) = 0 \). Replacing \( x \) by \( x^5 \) shows that \( U(G(x^3), G(x)) = 0 \). Now proceed as in the proof of Lemma 2.19 of [1] (though now we have 4 imbeddings \( \varphi_i \), the first taking \( f(x) \) to \( f(x^3) \), and the others taking \( f(x) \) to \( f(\lambda x^{1/3}) \) where \( \lambda \) runs over the cube roots of 1 in an algebraic closure of \( Z/2 \)). \( \square \)

**Theorem 2.26** The \( T_3(D_n) \) \( n \equiv 1, 3, 7, 9 \ (20) \) satisfy the recursion \( T_3(D_{n+80}) = G^16T_3(D_n) + G^4T_3(D_{n+20}) \). And \( T_3 \) takes

\[
D_1, D_3, D_7, D_9, D_{21}, D_{23}, D_{27}, D_{29}, D_{41}, D_{43}, D_{47}, D_{49}, D_{61}, D_{63}, D_{67}, D_{69}
\]
to:

\[
0, D_1, 0, D_3, D_7, D_9, D_{21}, D_{23}, 0, D_{41}, D_{43} + D_{27}, D_{47} + D_{23}, D_{61} + D_{29} + D_{21}, D_{49} + D_{41}, D_{63} + D_{47} + D_{23}.
\]

**Proof Sketch** Taking \( u = D_9 \) in Lemma 2.25, we get the recursion. I'll calculate \( T_3(D_{47}) \) explicitly, the other 15 initial values being derived in a similar way. By Corollary 2.20 and Theorem 2.24, \( T_3(D_{47}) \) is a \( Z/2 \)-linear combination of \( D_{21} \) and \( D_{29} \). Now \( D_{47} = G^8(D^2G) = (x^{40} + x^{360} + \cdots)(x^2 + x^{18} + x^{98} + \cdots)(x^5 + x^{45} + \cdots) \). So the coefficients of \( x^7, x^{63} \) and \( x^{87} \) in \( D_{47} \) are 0, 1 and 1. It follows that the coefficients of \( x^{21} \) and \( x^{29} \) in \( T_3(D_{47}) \) are each 1. But \( D_{21} = G^4D = x^{21} + x^{29} + \cdots \) while \( D_{29} = x^{29} + \cdots \). It follows that \( T_3(D_{47}) = D_{21} \). \( \square \)

Now let \( w \) be an indeterminate over \( Z/2 \).

**Definition 2.27** \( V' \subset Z/2[w] \) is the space spanned by the \( w^k \) with \( k \equiv 1, 3, 7, 9 \ (20) \).

There is a \( Z/2 \)-linear identification of \( W_a \) with \( V' \) taking \( D_k \) to \( w^k \). Then \( T_3 : W_a \rightarrow W_a \) goes over to a map \( V' \rightarrow V' \) which we'll still call \( T_3 \). Now in section 5 of [2] (see Theorem 5.1, the paragraphs preceding it, and Remark 5.2) we defined certain \( P_k, k \equiv 1, 3, 7, 9 \ (20) \) in \( V' \).

**Theorem 2.28** \( T_3 : V' \rightarrow V' \) takes \( w^k \) to the \( P_k \) of [2] section 5.

**Proof** Let \( A_k = T_3(w^k) \). The recursion of Theorem 2.26 tells us that \( A_{k+80} = w^{80}A_k + w^{20}A_{k+20} \), while Theorem 5.1 of [2] tells us that \( P_{k+80} = w^{80}P_k + w^{20}P_{k+20} \). Putting the initial values in Theorem 2.26 together with Theorem
5.1 of [2] we see that $P_k = A_k$ whenever $k < 80$, $k \equiv 1, 3, 7, 9 \pmod{20}$. The recursions then show that $P_k = A_k$ whenever $k \equiv 1, 3, 7, 9 \pmod{20}$. \hfill \Box

3 Coding a basis of $W_a$. The effect of $T_3$ on the code

Define a total ordering on $N \times N$ as follows. $(c, d)$ “precedes” (or “is earlier than”) $(a, b)$ if $c + d < a + b$ or $c + d = a + b$ and $d < b$.

Consider the space $W_a$ with its basis $\{D_k, k \equiv 1, 3, 7, 9 \pmod{20}\}$. In this section we “code the basis” by identifying it with $N \times N$; $(c, d)^*$ will denote the particular $D_k$ corresponding to $(c, d)$. Under this identification, the total ordering on $N \times N$ given in the last paragraph goes over to a total ordering on our basis, and we use the “precedence” language of the last paragraph and show:

1. $T_3(a, b)^*$ is a sum of $(c, d)^*$ with $c + d < a + b$.
2. If $a > 0$, $T_3(a, b)^* = (a - 1, b)^* + a$ sum of earlier $D_j$.

The hard work in establishing (1) and (2) has already been done in Lemma 5.5 of [2] and Theorem 2.28 of the last section, so most of this section is a summary of results from [2].

Definition 3.1 $g : N \to N$ is the function with $g(2n) = 4g(n)$ and $g(2n + 1) = g(2n) + 1$.

Definition 3.2 $V \subset \mathbb{Z}/2[t]$ is spanned by the $t^k, k$ odd. If $(a, b)$ is in $N \times N$, $[a, b]$ in $V$ is $t^{1+2g(a)+4g(b)}$.

$(a, b) \to [a, b]$ sets up a 1–1 correspondence between $N \times N$ and the monomial basis of $V$. The total ordering of $N \times N$ goes over to a total ordering of the basis. Once again we use the language of “precedence.” We now pass from $V$ to $V'$.

Definition 3.3 If $V'$ is as in Definition 2.27, $\varphi : V \to V'$ is the $\mathbb{Z}/2$-linear bijection with:

- $\varphi(t^{16m+1}) = w^{40m+1}$, $\varphi(t^{16m+3}) = w^{40m+3}$
- $\varphi(t^{16m+5}) = w^{40m+7}$, $\varphi(t^{16m+5}) = w^{40m+21}$
- $\varphi(t^{16m+9}) = w^{40m+9}$, $\varphi(t^{16m+11}) = w^{40m+27}$
- $\varphi(t^{16m+13}) = w^{40m+23}$, $\varphi(t^{16m+15}) = w^{40m+29}$

Definition 3.4 $(a, b)$ in $V'$ is $\varphi[a, b]$. $(a, b)^*$ in $W_a$ is the image of $(a, b)$ under the identification of $V'$ with $W_a$ taking $w^k$ to $D_k$.

Note that $\varphi : V \to V'$ identifies the monomial basis $(t)$ of $V$ with the
monomial basis (in $w$) of $V'$. So Definition 3.4 results in a coding of the basis $\{D_k\}$ of $W_a$.

**Theorem 3.5**

1. $T_3(a,b)^*$ is a sum of $(c,d)^*$ with $c + d < a + b$.
2. If $a > 0$, $T_3(a,b)^* = (a - 1,b)^* + a$ sum of earlier $D_j$.

**Proof** We saw in the last section that $T_3$ stabilizes $W_a$. In view of the identification of $W_a$ with $V'$ it suffices to show that $T_3(a,b)$ is a sum of $(c,d)$ with $c + d < a + b$, and that if $a > 0$, $T_3(a,b) = (a - 1,b) + a$ sum of earlier monomials. Suppose then that $(a,b) = w^k$. By Theorem 2.28, $T_3(a,b)$ is the $P_k$ of [2], Theorem 5.1. So our result is precisely Lemma 5.5 of [2]. $\square$

We will need one further property of our code.

**Theorem 3.6** If $D_i = (c,d)^*$ precedes $D_j = (0,b)^*$, then $i < j$.

**Proof** In view of our identification of $W_a$ with $V'$, it’s enough to show that if $w^i = (c,d)$ precedes $w^j = (0,b)$, then $i < j$.

Now there is the following corresponding result for $V$. If $t^i = [c,d]$ precedes $t^j = [0,b]$ then $i < j$. For $c + d \leq b$, so by Lemma 4.1 of [1], $4g(c) + 4g(d) \leq 4g(b)$. Then $i = 1 + 2g(c) + 4g(d) \leq 1 + 4g(b) = j$, and since $i \neq j$, $i < j$.

We’ll deduce Theorem 3.6 from this result for $V$. Suppose first that $b$ is even, and let $m = g(b/2)$. Then $1 + 4g(b) = 16m + 1$, and $[0,b] = t^{16m+1}$. Write $[c,d]$ as $t^{16m'+r}$ with $r$ in $\{1,3,5,7,9,11,13,15\}$. Since $(c,d)$ precedes $(0,b)$, $[c,d]$ precedes $[0,b]$. By the result of the last paragraph, $16m' + r < 16m + 1$ and so $m' < m$. Now $[0,b] = w^{40m'+1}$ so that $j = 40m + 1$. Similarly, $i \leq 40m' + 29 \leq 40m - 11$, and this is $i < j$. The argument when $b$ is odd is similar. Let $m = g((b - 1)/2)$, so that $g(b) = 4m + 1$, and $[0,b] = t^{16m+5}$. Let $m'$ and $r$ be as in the case of even $b$. Arguing as in the case of even $b$ we find that $16m' + r < 16m + 5$. If $m' < m$ we proceed as in the case of even $b$. If $m' = m$ then $r$ must be 1 or 3. So $(c,d)$ is either $w^{40m+1}$ or $w^{40m+3}$, while $(0,b) = \varphi(t^{16m+5}) = w^{40m+7}$, and once again $i < j$. $\square$

4 **Type a ideals of $\mathbb{Z}[\sqrt{-10}]$ and Gauss-classes**

This section is the counterpart to section 3 of [1]. Fix a power, $q$, of 2. We shall (essentially) use binary quadratic forms of discriminant $-640q^2$ and their associated theta-series to construct a subspace $DI(q)$ of $W_a$ of dimension $2q$, stable under the $T_q$ with $\chi(p) = 1$, and annihilated by $T_3$, and we’ll give a simple description of the action of $T_7$ on $DI(q)$ involving Gaussian composition of
forms. We will not use all primitive positive forms of discriminant \(-640q^2\); the Dirichlet character \(\chi\) of Definition 2.8 may be thought of as a genus character, and we'll only consider forms on which this character takes the value 1. We'll see that the \(SL_2(\mathbb{Z})\)-classes of such forms make up a cyclic group of order \(4q\), and that the class of a form representing 7 is a generator.

As in section 3 of [1], we'll avoid the explicit language of binary forms. Instead we'll consider ideals \(I\) in \(\mathbb{Z}[\sqrt{-10}]\) for which \(\chi(\text{norm}(I)) = 1\). We'll say that such an ideal is “of type \(a\).” We fix a power \(q\) of 2, and introduce an equivalence relation, depending on \(q\), on the type \(a\) ideals. We will call our equivalence relation “Gauss-equivalence,” and the equivalence classes under it “Gauss-classes.”

The class number of \(\mathbb{Z}[\sqrt{-10}]\) is 2, with an ideal of norm 7 representing the non-principal class. We begin by defining Gauss-equivalence for principal ideals \((b + c\sqrt{-10})\) of type \(a\).

Since the norm of \((b + c\sqrt{-10})\) is \(b^2 + 10c^2\), \((b + c\sqrt{-10})\) is of type \(a\) precisely when \((b, 10) = 1\) and \(c\) is even. Note also that the generator of a principal ideal is defined up to multiplication by \(\pm 1\).

**Definition 4.1** Principal type \(a\) ideals \((\alpha)\) and \((\beta)\) are equivalent if there is an integer \(N\) with \((N, 10) = 1\) such that \(N\alpha \equiv \beta \mod 4q\) in the ring \(\mathbb{Z}[\sqrt{-10}]\).

Evidently this does not depend on the choices of generators for the ideals, and is an equivalence relation. Also ideal multiplication makes the set of equivalence classes into a semigroup. Since \((\alpha)(\bar{\alpha}) = (\text{norm}(\alpha))\) which is equivalent to (1), the semigroup is a group.

**Lemma 4.2**

(1) Any principal type \(a\) ideal \((\alpha)\) is equivalent to \((1 + 2d\sqrt{-10})\) for some \(d\).

(2) \((1 + 2c\sqrt{-10})\) and \((1 + 2d\sqrt{-10})\) are equivalent if and only if \(c \equiv d \mod 2q\).

So there are \(2q\) equivalence classes.

**Proof** Write \(\alpha\) as \((b + 2c\sqrt{-10})\). Then \((b, 10) = 1\) and we can choose \(N\) with \((N, 10) = 1\) so that \(Nb \equiv 1 \mod (4q)\). Then \((Na)\) is of type \(a\), and \(Na \equiv 1 + 2Nc\sqrt{-10} \mod 4q\), proving (1). Turning to (2), if \(c \equiv d \mod 2q\) we may take \(N = 1\). Conversely if \(N(1 + 2c\sqrt{-10}) \equiv 1 + 2d\sqrt{-10} \mod 4q\), then \(N \equiv 1 \mod (4q)\). So \(2d \equiv 2Nc \equiv 2c\). \(\square\)

**Theorem 4.3** The order \(2q\) group of classes of principal type \(a\) ideals is cyclic, generated by the class of any \((c + 2d\sqrt{-10})\) with \((c, 10) = 1\) and \(d\) odd.
Proof One argues as in the last few sentences of the proof of Theorem 3.2 of [1].

Now fix a type $a$ non-principal ideal $L$; for example $P = (7, 2 - \sqrt{-10})$. If $I$ is another such ideal, $IL$ is principal of type $a$.

**Definition 4.4** Suppose $I$ and $J$ are type $a$ non-principal. $I$ and $J$ are Gauss equivalent if $IL$ and $JL$ are equivalent in the sense of Definition 4.1.

The definition appears to depend on the choice of $L$. But if one replaces $L$ by $\gamma L$ where $\chi(\text{norm}(\gamma)) = 1$, one finds that the notion of Gauss-equivalence is unchanged. It follows at once that the dependence on $L$ is illusory. One sees further that the Gauss-classes of all type $a$ ideals form a group of order $4q$ under ideal multiplication and that the inverse of $I$ is $\bar{I}$.

**Theorem 4.5** The group of Gauss-classes of type $a$ ideals is cyclic of order $4q$; any class consisting of non-principal ideals is a generator.

**Proof** Let $P = (7, 2 - \sqrt{-10})$. $P$ has norm 7, and is of type $a$. Also, $P^2 = (3 + 2\sqrt{-10})$. By Theorem 4.3, $P^2$ has order $2q$. So $P$ has order $4q$, and the result follows. \(\square\)

**Definition 4.6** If $R$ is a Gauss-class, $\theta(R)$ in $\mathbb{Z}[[x]]$ is $\sum x^{\text{norm}(I)}$, where $I$ runs over the ideals in $R$.

**Definition 4.7**

1. $e$ is the Gauss-class of (1).
2. $AMB$ is the Gauss-class of order 2; that is to say the Gauss-class of $(1 + 2q\sqrt{-10})$.

**Lemma 4.8**

1. The mod 2 reduction of $\theta(e)$ is $D$.
2. $\theta(AMB)$ is in $2\mathbb{Z}[[x]]$, and the mod 2 reduction of $\frac{1}{2}\theta(AMB)$ is $D_{40q^2+1}$.

**Proof** $I$ is in $e$ if and only if $\bar{I}$ is in $e$; also they each make the same contribution to $\theta(e)$. So in calculating $\theta(e)$ mod 2 we only need consider $I$ in $e$ with $\bar{I} = I$. These are just the $(N)$ with $N$ in $\mathbb{Z}$, $(N, 10) = 1$ and $N > 0$, and we get (1). $AMB$ consists of principal ideals. These are of the form $(b+2cq\sqrt{-10})$ with $(b, 10) = 1$, $b > 0$ and $c$ odd. Since $(b + 2cq\sqrt{-10})$ and $(b - 2cq\sqrt{-10})$ make the same contribution to $\theta(AMB)$, $\theta(AMB)$ is in $2\mathbb{Z}[[x]]$. Also, $\frac{1}{2}\theta(AMB)$ is $\sum x^{b^2+40q^2c^2}$, the sum running over all positive $b$ and $c$ with $(b, 10) = 1$ and $c$ odd. Reducing mod 2 we get $DG_{8q^2} = D_{40q^2+1}$. \(\square\)

We next define a Hecke operator $T_p : \mathbb{Z}[[x]] \rightarrow \mathbb{Z}[[x]]$ for each $p$ with $\chi(p) = 1$. 16
Definition 4.9 If $\chi(p) = 1$, $T_p$ is the map $\sum c_n x^n \to \sum c_{pn} x^n + \left(\frac{-10}{p}\right) \sum c_n x^{pn}$. Note that the mod 2 reduction of $T_p$ is our usual mod 2 Hecke operator $T_p : \mathbb{Z}/2[[x]] \to \mathbb{Z}/2[[x]]$.

Remark The motivation for Definition 4.9 is the following. It can be shown that each $\theta(R)$ is the expansion at infinity of a modular form of weight 1 for some $\Gamma_1(N)$, with character $n \mapsto \left(\frac{-10}{n}\right)$. And Definition 4.9 is the standard definition of the Hecke action on such expansions. (But in what follows we won’t use the connection of the $\theta(R)$ with weight 1 modular forms.)

Theorem 4.10 Suppose $\chi(p) = 1$ and $p$ is inert in $\mathbb{Z}[\sqrt{-10}]$. Then $T_p$ annihilates each $\theta(R)$ in $\mathbb{Z}[[x]]$.

Proof $I \to pI$ sets up a 1–1 correspondence between ideals of norm $n$ in $R$ and ideals of norm $p^2n$ in $R$. Also, if $(n,p) = 1$ there are no ideals of norm $pn$ in $R$. Since $\left(\frac{-10}{n}\right) = -1$, the result follows directly from Definition 4.9. □

Theorem 4.11 Suppose $\chi(p) = 1$ and $p$ splits in $\mathbb{Z}[\sqrt{-10}]$, so that $(p) = P \cdot \overline{P}$ with $P \neq \overline{P}$. Then if $R$ is a Gauss-class, $T_p(\theta(R)) = \theta(PR) + \theta(PR)$. (Since $\chi(p) = 1$, $P$ and $\overline{P}$ are type $a$.)

Proof The argument follows that in the proof of Theorem 3.6 of [1], the essential points being the multiplicativity of the norm and unique factorization at the ideal level in $\mathbb{Z}[\sqrt{-10}]$. □

Definition 4.12 $\alpha(R)$ is the mod 2 reduction of $\theta(R)$. $DI(q) \subset \mathbb{Z}/2[[x]]$ is the space spanned by the $\alpha(R)$, as $R$ runs over the $4q$ Gauss-classes of type $a$ ideals.

Now let $C$ be a Gauss-class containing one of the ideals of norm 7. By Theorem 4.5, $C$ generates the group of Gauss-classes of type $a$ ideals.

Theorem 4.13 Let $\alpha_i = \alpha(C^i)$. Then $\alpha_0 = D$, $\alpha_{2q} = 0$, and the $\alpha_i$, $0 \leq i < 2q$ span $DI(q)$.

Proof Since $C$ is a generator, $\alpha_0, \ldots, \alpha_{4q-1}$ span $DI(q)$. By Lemma 4.8, $\alpha_0 = D$ and $\alpha_{2q} = 0$. Finally $I \to \overline{I}$ sets up a 1–1 norm preserving correspondence between the ideals in $C^i$ and the ideals in $C^{4q-i}$, so $\alpha_i = \alpha_{4q-i}$. □

Theorem 4.14
(1) $T_7(\alpha_i) = \alpha_{i-1} + \alpha_{i+1}$ if $0 < i < 2q$. So $T_7$ stabilizes $DI(q)$.
(2) $T_7(D_{4q^2+1}) = \alpha_{2q-1}$.

Proof By Theorem 4.11, $T_7(\theta_i) = \theta_{i-1} + \theta_{i+1}$; reducing mod 2 we get (1). Also $T_7(\theta(AMB)) = \theta_{2q-1} + \theta_{2q+1} = 2\theta_{2q-1}$. Dividing by 2, reducing mod 2
and using Lemma 4.8 we get (2). □

**Definition 4.15** $U_n$ is the element of $Z/2[t]$ with $U_n(t + t^{-1}) = t^n + t^{-n}$. Note that $U_0 = 0$, $U_1(Y) = Y$, and that $U_{n+2}(Y) = Y U_{n+1}(Y) + U_n(Y)$. Furthermore $U_{2n} = U_n^2$, and it follows that $U_q(Y) = Y^q$. Finally $Y$ divides each $U_n(Y)$.

**Lemma 4.16** Let $Y$ be the operator $T_7 : Z/2[[x]] \rightarrow Z/2[[x]]$. Then for $0 \leq i \leq 2q$, $\alpha_{2q-i} = U_i(Y) \cdot (D_{40q^2+1})$.

**Proof** If $i \leq 2q - 2$, Theorem 4.14 and the recursion in Definition 4.15 give:

1. $\alpha_{2q-i-2} = Y(\alpha_{2q-i-1}) + \alpha_{2q-i}$.
2. $U_{i+2}(Y) = Y \cdot U_{i+1}(Y) + U_i(Y)$.

So, by induction on $i$, it suffices to show that $\alpha_{2q}$ and $\alpha_{2q-1}$ are $U_0(Y)(D_{40q^2+1})$ and $U_1(Y)(D_{40q^2+1})$. But Lemma 4.8 and Theorem 4.14 show that $\alpha_{2q} = 0$ and $\alpha_{2q-1} = Y \cdot D_{40q^2+1}$. □

**Theorem 4.17** As $Z/2[Y]$-module, $DI(q)$ is cyclic with generator $\alpha_{2q-1} = Y \cdot D_{40q^2+1}$.

**Proof** $\alpha_{2q-i} = U_i(Y) \cdot D_{40q^2+1}$ for $1 \leq i \leq 2q$. Since $Y$ divides each $U_i(Y)$ we’re done. □

**Theorem 4.18** $Y^{2q-1}(\alpha_{2q-1}) = D$, while $Y^{2q}(\alpha_{2q-1}) = 0$. Also, $DI(q)$ has dimension $2q$ over $Z/2$ and is isomorphic as $Z/2[Y]$-module with $Z/2[Y]/Y^{2q}$.

**Proof** $Y^{2q-1}(\alpha_{2q-1}) = Y^{2q}(D_{40q^2+1}) = U_{2q}(Y) \cdot D_{40q^2+1}$. By Lemma 4.16 this is $\alpha_0 = D$. So $Y^{2q}(\alpha_{2q-1}) = T_7(D) = 0$. It follows that the annihilator of $\alpha_{2q-1}$ in $Z/2[Y]$ is the ideal $(Y^{2q})$. Theorem 4.17 then gives the final assertions. □

**Theorem 4.19** If $p$ is as in Theorem 4.10 then $T_p$ annihilates $DI(q)$. In particular, $X = T_3$ annihilates $DI(q)$.

**Proof** This is immediate from Theorem 4.10 □

5 The action of $T_3$ and $T_7$ on $W_a$

This section is the counterpart to section 4 of [1]. In that paper we defined certain subspaces $W_1$ and $W_5$ of $Z/2[[x]]$; see section 1 of the present paper for a summary. In section 4 of [1] we made $W_5$ into a $Z/2[X,Y]$-module with $X$ and $Y$ acting by $T_7$ and $T_{13}$, and we showed the existence of an “adapted basis” $m_{i,j}$ where $D = \sum_{n>0, (n,0)=1} x^n$ and $m_{0,0} = D^5$. Here we’ll derive a similar result with $W_5$, $T_7$ and $T_{13}$ replaced by $W_a$, $T_3$ and $T_7$. 

18
Since \( \chi(3) = \chi(7) = 1 \), the commuting operators \( T_3 \) and \( T_7 : \mathbb{Z}/2[[x]] \to \mathbb{Z}/2[[x]] \) stabilize \( W_a \); see Corollary 2.20. So one can make \( W_a \) into a \( \mathbb{Z}/2[X,Y] \)-module with \( X \) and \( Y \) acting by \( T_3 \) and \( T_7 \). We shall filter \( W_a \) by finite-dimensional \( \mathbb{Z}/2[X,Y] \)-stable subspaces, \( W_a(q) \), \( q \) running over the powers of \( 2 \).

In the paragraph following Definition 2.27 we constructed an isomorphism between \( W_a \) and a certain subspace \( V' \) of \( \mathbb{Z}/2[w] \). Using this identification we may speak of the “\( w \)-degree” of an element of \( W_a \). Theorem 2.24 shows that the maps \( X \) and \( Y : W_a \to W_a \) lower the \( w \)-degree.

**Definition 5.1** \( W_a(q) \) is the subspace of \( W_a \), of \( \mathbb{Z}/2 \)-dimension \( 8q^2 \), consisting of elements of \( w \)-degree < \( 40q^2 \). (Since \( X \) and \( Y \) lower the \( w \)-degree they stabilize \( W_a(q) \).)

**Theorem 5.2** The space \( DI(q) \) of Definition 4.12, of \( \mathbb{Z}/2 \)-dimension \( 2q \), is a \( \mathbb{Z}/2[X,Y] \)-submodule of \( W_a(q) \) annihilated by \( X \).

**Proof** By Theorems 4.17, 4.18 and 4.19, \( DI(q) \) has \( \mathbb{Z}/2 \)-dimension \( 2q \), is annihilated by \( X \) and as \( \mathbb{Z}/2[Y] \)-module is cyclic generated by \( \alpha_{2q-1} = Y \cdot D_{40q^2+1}. \) So it suffices to show that \( \alpha_{2q-1} \) is in \( W_a(q) \). But \( Y \) lowers the \( w \)-degree. \( \square \)

We’ll use the results of section 3 to show that the kernel of \( X : W_a(q) \to W_a(q) \) is precisely \( DI(q) \). Note that \( g(2q) = 4q^2 \). So in the language of section 3, \( (0,2q) = w^{40q^2+1} \), and so the \( w \)-degree of \( (0,2q)^* \) is \( 40q^2+1 \).

**Lemma 5.3** Suppose \( f \neq 0 \) is in \( W_a(q) \), with \( Xf = 0 \). Write \( f \) as \( (a,b)^* + a \) sum of earlier \( D_i \), as in section 3. Then \( a = 0 \), and \( 0 \leq b < 2q \).

**Proof** If \( a > 0 \), then by Theorem 3.5, \( Xf = (a-1,b)^* + a \) sum of earlier \( D_i \), and so cannot be 0. So \( f = (0,b)^* + a \) sum of earlier \( D_i \). By Theorem 3.6, the \( w \)-degree of \( f \) is the \( w \)-degree of \( (0,b)^* \). If \( b \geq 2q \), then this last \( w \)-degree is \( \geq \) the \( w \)-degree, \( 40q^2+1 \), of \( (0,2q)^* \). So \( f \) cannot be in \( W_a(q) \). \( \square \)

**Theorem 5.4** The kernel of \( X : W_a(q) \to W_a(q) \) is \( DI(q) \).

**Proof** By Lemma 5.3 this kernel has dimension \( \leq 2q \), and we use Theorem 5.2. \( \square \)

**Corollary 5.5** \( DI(1) \subset DI(2) \subset DI(4) \subset \ldots \), and the kernel of \( X : W_a \to W_a \) is the union, \( DI \) of the \( DI(q) \).

**Theorem 5.6** The only elements of \( W_a \) annihilated by \( X \) and \( Y \) are 0 and \( D \).

**Proof** If \( (X,Y)f = 0 \), \( f \) is in \( DI \) by Corollary 5.5, and so is in some \( DI(q) \).
But $DI(q)$, as $Z/2[Y]$-module, is isomorphic to $Z/2[Y]/(Y^{2q})$. It follows that the kernel of $Y : DI(q) \to DI(q)$ has dimension 1 over $Z/2$. □

**Definition 5.7** $S_m$ is the subspace of $W_a$ of dimension $m(m+1)/2$, spanned over $Z/2$ by the $(a,b)^*$ with $a + b < m$.

Note that $S_0 = (0)$ while $S_1$ is spanned by $(0,0)^* = D$. So $X \cdot S_1 = Y \cdot S_1 = S_0$.

**Lemma 5.8** $X : W_a \to W_a$ is onto. In fact $X$ maps $S_{m+1}$ onto $S_m$.

**Proof** By Theorem 3.5, $X \cdot S_{m+1} \subset S_m$, so it suffices to show that the kernel of $X : S_{m+1} \to S_m$ has dimension at most $m + 1$. Suppose $f \neq 0$ is in this kernel. The proof of Lemma 5.3 shows that $f = (0,b)^* + a$ sum of earlier $D_i$, and that the $w$-degree of $f$ is the $w$-degree of $(0,b)^*$. But Theorem 3.6 tells us that every element of $S_{m+1}$ has $w$-degree $\leq$ the $w$-degree of $(0,m)^*$. So $0 \leq b \leq m$, and the result follows. □

**Theorem 5.9** $Y : S_{m+1} \subset S_m$.

**Proof** We argue by induction on $m$, $m = 0$ being clear. Suppose $f$ is in $S_{m+1}$ with $m > 0$. Then $Xf$ is in $S_m$, so by the induction hypothesis, $X(Yf) = Y(Xf)$ is in $S_{m-1}$. By Lemma 5.8, there is an $h$ in $S_m$ with $Xh = XYf$. Then $h + Yf$, being in the kernel of $X$, is $(0,b)^* + a$ sum of earlier $D_i$ for some $b$. Since $h + Yf$ is in $S_{m+1}$, $b \leq m$, and it will suffice to show that $b \neq m$. Suppose on the contrary that $h + Yf = (0,m)^* + a$ sum of earlier $D_i$. Then since $f$ is in $S_{m+1}$ and $Y$ lowers the $w$-degree, the $w$-degree of the left hand side is $< the w$-degree of $(0,m)^*$, giving a contradiction. □

**Lemma 5.10** For each $m$ there is an element of $DI$ of the form $(0,m)^* + a$ sum of earlier $D_i$.

**Proof** Fix $q > m$. Each $f \neq 0$ in $DI(q)$ can be written as $(0,b)^* + a$ sum of earlier $D_i$ for some $b$ with $0 \leq b < 2q$. Since there are only $2q$ choices for $b$, and $DI(q)$ has dimension $2q$, the result follows.

**Lemma 5.11** $DI \cap S_m$ has dimension $m$. Furthermore, $Y$ maps $DI \cap S_{m+1}$ onto $DI \cap S_m$.

**Proof** By Lemma 5.10, $DI \cap S_{m+1} \neq DI \cap S_m$. Now $Y$ maps $DI \cap S_{m+1}$ into $DI \cap S_m$ by Theorem 5.9; Theorem 5.6 shows that the kernel of this map is contained in $\{0, D\}$. So the map is onto, and the dimensions of $DI \cap S_{m+1}$ and $DI \cap S_m$ differ by 1. □

The machinery is now in place to establish the results analogous to those of section 4 of [1]. The arguments are exactly the same as those that were used
to derive Theorems 4.12, 4.14, 4.15, 4.16, 4.17 and Corollary 4.13 of [1].

**Theorem 5.12** Let \( f \) and \( h \) be in \( S_m \) with \( Yf = Xh \). Then there is an \( e \) in \( S_{m+1} \) with \( Xe = f \) and \( Ye = h \).

**Corollary 5.13** There are \( m_{a,b} \) in \( S_{a+b+1} \) such that:

1. \( m_{0,0} = D \).
2. \( X \cdot m_{a,b} = m_{a-1,b} \) or \( 0 \) according as \( a > 0 \) or \( a = 0 \).
3. \( Y \cdot m_{a,b} = m_{a,b-1} \) or \( 0 \) according as \( b > 0 \) or \( b = 0 \).
4. The \( m_{a,b} \) are a \( Z/2 \)-basis of \( W_a \).

**Theorem 5.14** Make \( W_a \) into a \( Z/2[[X,Y]] \)-module with \( X \) and \( Y \) acting by \( T_3 \) and \( T_7 \). (This is possible since \( T_3 \) and \( T_7 \) lower the \( w \)-degree.) Then the action of \( Z/2[[X,Y]] \) on \( W_a \) is faithful.

**Theorem 5.15** If \( \chi(p) = 1 \), \( T_p : W_a \to W_a \) is multiplication by some \( u \) in the ideal \( (X,Y) \) of \( Z/2[[X,Y]] \). In other words, \( T_p \) in its action on \( W_a \) is a power series with 0 constant term in \( T_3 \) and \( T_7 \).

We next prove an analogue to Theorem 4.18 of [1]. Since \( \chi(11) = -1 \), \( T_{11}(W_a) \subset W_b \), \( T_{11}(W_b) \subset W_a \), and \( T_{11}^2 \) stabilizes \( W_a \). We now decompose \( W_a \) into a direct sum of 4 summands. The first is spanned by the \( D_k \) with \( k \equiv 1 \) or 9 (40). For the second, \( k \equiv 3 \) or 27, for the third, \( k \equiv 7 \) or 23, and for the fourth, \( k \equiv 21 \) or 29. By Lemma 2.10, the exponents appearing in elements of the first summand are 1 or 9 mod 40, and corresponding results hold for the other summands.

**Theorem 5.16** \( T_{11}^2 : W_a \to W_a \) is multiplication by \( \lambda^2 \) for some \( \lambda \) in the ideal \( (X,Y) \) of \( Z/2[[X,Y]] \).

**Proof** As in the proofs of Theorem 4.16 and 4.17 of [1] we use the \( Z/2[[X,Y]] \)-linearity of our map to show that it is multiplication by some \( u \) in \( (X,Y) \) and we write \( u \) as \( a + bX + cY + dXY \) with \( a, b, c, d \) in \( Z/2[[X^2,Y^2]] \). Let \( a = \lambda^2 \). We'll show that for each \( h \) in \( W_a \), \( T_{11}^2(h) = \lambda^2 h \). We may assume that \( h \) is in one of the 4 subspaces of the above direct sum decomposition. Suppose for example that it is in the second. Then \( T_{11}^2(h) \) and \( ah \) are sums of \( D_k \), \( k \equiv 3 \) or 27 (40), \( (bX)h \) is a sum of \( D_k \), \( k \equiv 1 \) or 9 (40), \( (cY)h \) is a sum of \( D_k \), \( k \equiv 21 \) or 29 (40) and \( (dXY)h \) is a sum of \( D_k \), \( k \equiv 7 \) or 23 (40). Since \( T_{11}^2(h) = uh \) is the sum of \( \lambda^2 h \), \( (bX)h \), \( (cY)h \) and \( (dXY)h \), and the decomposition is direct, the result follows. \( \square \)

**Lemma 5.17** Write the \( \lambda \) of Theorem 5.16 as \( cX + dY + \cdots \), with \( c \) and \( d \) in \{0, 1\}. Then \( c = d = 1 \).
Proof. On $W_a$, $T_{11}^2 = \lambda^2 = cX^2 + dY^2 + \cdots$. Applying both sides to $D_9$ we find that $0 = cD_1 + dD_1$, while applying both sides to $D_{41}$ shows that $D_1 = dD_1$. □

Theorem 5.18 $T_{11}^2$ maps $S_{m+2}$ onto $S_m$ for all $m$. So $T_{11}^2 : W_a \rightarrow W_a$ is onto.

Proof. Using the explicit description of the action of $T_3$ and $T_7$ on $W_a$ provided by Corollary 5.13 we see that $X^2 + Y^2$ maps $S_{m+2}$ onto $S_m$. Since $T_{11}^2 = X^2 + Y^2 + \cdots$, $T_{11}$ and $X^2 + Y^2$ induce the same map $S_{m+3}/S_{m+2} \rightarrow S_{m+1}/S_m$. So this map is onto for all $m$, and an induction gives the result. □

6 $T_{11} : W_b \rightarrow W_a$ is bijective

Since $\chi(11) = -1$, $T_{11}$ maps $W_a$ to $W_b$ and $W_b$ to $W_a$. In this section we show that $T_{11}(D_k)$ is a sum of $D_i$, $i < k$, and that $T_{11} : W_b \rightarrow W_a$ is bijective. Let $C_k$, $(k, 10) = 1$, be $T_{11}(D_k)$.

Lemma 6.1 If $k < 120$ then:

(a) When $k \equiv 1, 3, 7$ or $9 \pmod{20}$, $C_k$ is a sum of $D_i$, $i < k$.
(b) When $k \equiv 11$ (resp. $19, 13, 17$) mod $20$, $C_k = D_j + a$ sum of $D_i$, $i < j$, where $j = k - 10$ (resp. $k - 10, k - 6, k - 14$).

Proof Sketch Using Corollary 2.20 and Lemmas 2.22 and 2.23 we see that it suffices to prove (a) when $k \equiv 9 \pmod{20}$, i.e. when $k$ is in $\{9, 29, 49, 69, 89, 109\}$. In fact the corresponding $C_k$ are $0, 0, D_{19} + D_{11}, D_{39} + D_{31}, D_{11}$ and $D_{39}$. To calculate $C_{109}$, for example, we use Corollary 2.20 and Lemma 2.23 to see that it is a sum of $D_i$ with each $i$ in $\{31, 39, 71, 79, 111\}$. Examining the expansions of $D_{109}$ and the $D_i$ and arguing as in the proof of Theorem 2.26 we find that $C_{109} = D_{39}$. (b) follows from the more precise results:

(b1) $C_{11}, C_{31}, C_{51}, C_{71}, C_{91}$ and $C_{111}$ are $D_1, D_{21}, D_{41} + D_9, D_{61} + D_{29}, D_{81} + D_{41} + D_9, D_{101} + D_{61} + D_{21}$.

(b2) $C_{19}, C_{39}, C_{59}, C_{79}, C_{99}$ and $C_{119}$ are $D_9, D_{29}, D_{49} + D_9, D_{69} + D_{29}, D_{89} + D_{49} + D_9, D_{109} + D_{69} + D_{29} + D_{21}$.

(b3) $C_{13}, C_{33}, C_{53}, C_{73}, C_{93}$ and $C_{113}$ are $D_7, D_{27} + D_3, D_{47}, D_{67} + D_{43} + D_{27}, D_{87} + D_{47}, D_{107} + D_{83} + D_{67} + D_{43} + D_{27}$.

(b4) $C_{17}, C_{37}, C_{57}, C_{77}, C_{97}$ and $C_{117}$ are $D_3, D_{23} + D_7, D_{43}, D_{63} + D_{47} + D_{23} + D_7, D_{83} + D_{43}, D_{103} + D_{87} + D_{63} + D_{47} + D_{23}$.

To calculate $C_{93}$, for example, we use Corollary 2.20 and Lemma 2.22 to see that it is a sum of $D_i$ where each $i$ is in $\{7, 23, 47, 63, 87\}$. Examining the expansions of $D_{93}$ and the $D_i$ and arguing as in the proof of Theorem 2.26 we find that $C_{93} = D_{87} + D_{47}$. □
**Lemma 6.2** For \( u \) in \( \mathbb{Z}/2[[x]] \), \( T_{11}(uG^{24}) \) is the sum of \( G_{2i}T_{11}(uG^{2j}) \) where \((i, j)\) runs over the 9 pairs \((12, 0), (8, 4), (4, 8), (6, 2), (2, 6), (9, 1), (1, 9), (3, 3), (1, 1)\).

**Proof** We argue as in the proof of Lemma 2.25. Let \( U \) be the 2 variable polynomial \((A + B)^2 + A^6B^2 + A^2B^6 + A^9B + AB^9 + A^3B^3 + AB\). Then \( U(F(x^{11}), F(x)) = 0\); this is the level 11 modular equation for \( F \). Replacing \( x \) by \( x^9 \) we find that \( U(G(x^{11}), G(x)) = 0\). Now let \( L \) be an algebraic closure of \( \mathbb{Z}/2\). We have 12 imbeddings \( \varphi_k : \mathbb{Z}/2[[x]] \rightarrow L[[x^{11}]] \), the first of which takes \( f \) to \( f(x^{11}) \), while each of the others takes \( f \) to \( f(\lambda x^{11}) \) for some \( \lambda \) in \( L \) with \( \lambda^{11} = 1 \). Replacing \( x \) by \( \lambda x^{11} \) in the identity \( U(G(x^{11}), G(x)) = 0 \) and using the symmetry of \( U \) we find that each \( U(\varphi_k(G), G) \) is 0. Squaring and expanding we find that \( \varphi_k(G^{24}) \) is the sum of the \( G^{2i}\varphi_k(G^{2j}) \) where \((i, j)\) runs over the 9 pairs above. Now the definition of \( T_{11} \) shows that if \( f \) is in \( \mathbb{Z}/2[[x]] \), \( T_{11}(f) \) is the sum of the \( \varphi_k(f) \). Multiplying the \( k^{\text{th}} \) of our identities by \( \varphi_k(u) \) and summing we get the result. \( \square \)

**Lemma 6.3** The conclusions (a) and (b) of Lemma 6.1 hold for all \( k \) with \((k, 10) = 1\).

**Proof** We argue by induction on \( k \). For \( k < 120 \), Lemma 6.1 applies. Suppose \( k = n + 120 \) with \( n > 0 \). By Lemma 6.2, \( C_{n+120} \) is a sum of 9 terms each corresponding to one of the 9 pairs \((i, j)\) of the lemma. These terms are \( G_{24}C_n, G_{16}C_{n+40}, G_{8}C_{n+80}, G_{12}C_{n+20}, G_{4}C_{n+60}, G_{18}C_{n+10}, G_{2}C_{n+90}, G_{6}C_{n+30} \) and \( G_{2}C_{n+10} \). The induction hypothesis shows that the term corresponding to \((i, j)\) is a sum of \( D_m \) with \( m < (n + 10j) + 10i \). Since \( i + j \leq 12 \), each \( m < n + 120 \), and in particular (a) holds for \( k \). We turn to (b). For each of the last 6 terms in our sum, \( i + j \leq 10 \). So the corresponding term is a sum of \( D_m \) with \( m < n + 100 \). Now consider the first 3 terms. Suppose for example that \( n \equiv 17 \pmod{20} \). By the induction hypothesis, each of \( G_{24}C_n, G_{16}C_{n+40} \) and \( G_8C_{n+80} \) is \( D_{n+106} + \) a sum of \( D_m \) with \( m < n + 106 \). It follows that \( C_{n+120} \) itself is \( D_{n+106} + \) a sum of \( D_m \) with \( m < n + 106 \). The proof of (b) when \( n \equiv 11, 19 \) or \( 13 \pmod{20} \) is identical. \( \square \)

**Theorem 6.4** If \((k, 10) = 1\), \( T_{11}(D_k) \) is a sum of \( D_i \) with \( i < k \). Furthermore, \( T_{11} : W_b \rightarrow W_a \) is bijective.

**Proof** Lemma 6.3 gives the first result. Also the \( D_k \) where \( k > 0 \) and \( k \equiv 11, 19, 13 \) or \( 17 \pmod{20} \) form a basis of \( W_b \), while the corresponding \( D_{k-10}, D_{k-10}, D_{k-6} \) and \( D_{k-14} \) form a basis of \( W_a \). So Lemma 6.3 gives the second result as well. \( \square \)

**Corollary 6.5** \( T_{11} : W_a \rightarrow W_b \) is onto.

**Proof** By Theorem 5.18, \( T_{11} \) maps the subspace \( T_{11}(W_a) \) of \( W_b \) onto \( W_a \), and we use the last theorem to see that \( T_{11}(W_a) \) is all of \( W_b \). \( \square \)
Corollary 6.6 Let $\lambda$ be as in Theorem 5.16. Then in its action on $W = W_a \oplus W_b$, $T_{11}^2$ is multiplication by $\lambda^2$. (This follows from Corollary 6.5 and Theorem 5.16.)

7 The algebra $\mathcal{O}$ acting on $W_a$

Take $\lambda$ in $(X,Y)$ as in Theorem 5.16, and let $U : W \to W$ be the map $h \to \lambda(X,Y)h + T_{11}(h)$. Since $U$ is $Z/2[[X,Y]]$-linear, and $U^2$ annihilates $W$ (by Corollary 6.6), $W$ has the structure of $Z/2[[X,Y]][\varepsilon]$ module with $\varepsilon^2 = 0, \varepsilon$ acting by $U$, and $X$ and $Y$ by $T_3$ and $T_7$. Let $\mathcal{O}$ be the local ring $Z/2[[X,Y]][\varepsilon]$.

Lemma 7.1 The only element of $W_b$ annihilated by $\varepsilon$ is 0.

Proof Suppose $\varepsilon h_b = 0$, with $h_b$ in $W_b$. Then $T_{11}(h_b) = \lambda(T_3, T_7)h_b$. Since the first of these is in $W_a$ and the second in $W_b$, $T_{11}(h_b) = 0$. By Theorem 6.4, $h_b = 0$. □

In Corollary 5.13 we constructed a $Z/2$-basis $m_{i,j}$ of $W_a$ “adapted to $X = T_3$ and $Y = T_7$.” Since $T_{11} : W_b \to W_a$ is bijective, this basis pulls back under $T_{11}$ to a basis $n_{i,j}$ of $W_b$ “adapted to $T_3$ and $T_7$.”

Theorem 7.2

(1) The $n_{i,j}$ and the $\varepsilon n_{i,j}$ form a $Z/2$-basis of $W$.
(2) $\mathcal{O}$ acts faithfully on $W$.
(3) Each $T_p$, $p \neq 2$ or 5, acts on $W$ by multiplication by some $r + t\varepsilon$ with $r$ and $t$ in $Z/2[[X,Y]]$.

Proof The arguments are just like those giving Theorems 5.2, 5.3 and 5.4 of [1], using the basis $n_{i,j}$ of $W_b$. □

Theorem 7.3

(1) If $\chi(p) = 1$, $T_p : W \to W$ is multiplication by some $t$ in the maximal ideal $(X,Y)$ of $Z/2[[X,Y]]$.
(2) If $\chi(p) = -1$, $T_p : W \to W$ is the composition of $T_{11}$ with multiplication by some $t$ in the maximal ideal $(X,Y)$ of $Z/2[[X,Y]]$.

Proof Suppose $\chi(p) = 1$. By Theorem 5.15, $T_p : W_a \to W_a$ is multiplication by some $t$ in the maximal ideal $(X,Y)$. Since $T_{11} : W_a \to W_b$ is onto, $T_p : W_a \to W_b$ is multiplication by the same $t$, and we get (1). Now $T_{11}$ is multiplication by $\lambda + \varepsilon$. Suppose $\chi(p) = -1$. By Theorem 7.2, $T_p$ is multiplication by some $r + t\varepsilon$ with $r$ and $t$ in $Z/2[[X,Y]]$. Then $T_p + tT_{11}$ is multiplication by $r + \lambda t$. Since
\( T_p + tT_{11} \) and multiplication by \( r + \lambda t \) map \( W_b \) into \( W_a \) and \( W_b \) respectively, 
\( T_p + tT_{11} = 0 \), giving (2). \( \square \)

**Corollary 7.4**  If \( p \neq 2 \) or 5 and \((k, 10) = 1\), then \( T_p(D_k) \) is a sum of \( D_i \) with \( i < k \).

**Proof**  We have seen that this holds when \( p = 3, 7 \) or 11; Theorem 7.3 then gives the general result. \( \square \)

Theorems 7.2 (2) and 7.3 tell us that when we complete the Hecke algebra generated by the \( T_p \) acting on \( W \) with respect to the maximal ideal generated by the \( T_p \), then the completed Hecke algebra we get is just the (non-reduced) local ring \( \mathcal{O} \). This is completely analogous to the results of [1]; see Theorems 5.3 and 5.5 of that paper.

**References**

[1] Monsky P. (2015), “A Hecke algebra attached to mod 2 modular forms of level 3.” arXiv:1508.07523 [math.NT].

[2] Monsky P. (2016), “Variations on a Lemma of Nicolas and Serre.” arXiv:1604.02622 [math.NT].

[3] Nicolas J.-L., Serre J.-P. (2012), “Formes modulaires modulo 2: l’ordre de nilpotence des opérateurs de Hecke.” C. R. Acad. Sci. Paris, Ser. I 350 (7–8) pages 343–348.

[4] Nicolas J.-L., Serre J.-P. (2012), “Formes modulaires modulo 2: structure de l’algèbre de Hecke.” C. R. Acad. Sci. Paris, Ser. I 350 (9–10) pages 449–454.