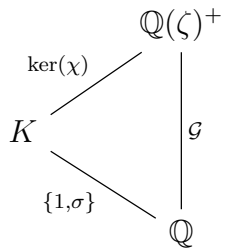
THE ATKIN-LEHNER GROUP OF THE MODULAR CURVE $X_\chi(N)$

CARLOS CASTAÑO-BERNARD

ABSTRACT. Let χ be the quadratic Dirichlet character of conductor N associated with a given real quadratic field K and $X_\chi(N)$ be the modular curve from Shimura's work on $\mathbb{Q}$-curves of conductor 1 over K. We show that the group $\mathcal{W}_\chi$ generated by the Atkin-Lehner automorphisms w_Q of $X_\chi(N)$ is a central extension of an elementary abelian 2-group of rank n. We also prove that w_Q lies in the centre $Z(\mathcal{W}_\chi)$ of $\mathcal{W}_\chi$ if and only if the prime disciminant $p^* > 0$, for each $Q = p^k$ exactly dividing N, with p prime. Assuming $Z(\mathcal{W}_\chi)$ is cyclic, we conjecture that $\mathcal{W}_\chi$ is isomorphic to 2_+^{1+n} or 2_-^{1+n}, if n is even and to the Pauli group $\mathcal{P}_{(n-1)/2}$, if n is odd.

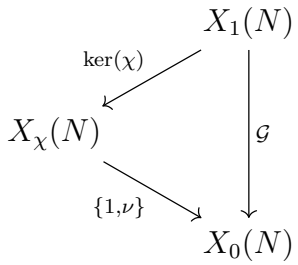
1. INTRODUCTION

1.1. **Statement of the main results.** Let K be a real quadratic field and let $\mathbb{Q}(\zeta)$ be the minimal cyclotomic field that contains K in some fixed algebraic closure of $\mathbb{Q}$. Note K is a subfield of the totally real field $\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta+\zeta^{-1})$ and, assuming that ζ is a primitive N-*th* root of unity, we have a diagram of Galois field extensions



where χ is the primitive quadratic Dirichlet character on the group $\mathcal{G} = (\mathbb{Z}/N\mathbb{Z})^\times/\{-1,1\}$, and σ is the non-trivial automorphism of K. It is well known that $\mathcal{G}$ acts faithfully on the modular curve $X_1(N)$ via the diamond

automorphisms $\langle\cdot\rangle$. Let $X_\chi(N)$ be the modular curve defined by the commutativity of the following diagram of Galois coverings



where ν denotes the projection of $\langle r\rangle$ to $X_\chi(N)$, for any $r \in \mathcal{G}$ such that $r \notin \ker(\chi)$. Let $\mathcal{W}_1$ be the group generated by the Atkin-Lehner automorphisms W_Q of $X_1(N)$, where Q runs through all positive integers that divide N exactly. Let $\mathcal{W}_0$ be the group of Atkin-Lehner involutions of $X_0(N)$, which is an elementary abelian 2-group of rank n, where n is the number of prime divisors of N.

Theorem 1. *For each exact divisor Q of N the projection of W_Q on the curve $X_\chi(N)$ defines a unique automorphism, which we denote w_Q. Let $\mathcal{W}_\chi$ be the group generated by the elements w_Q and assume the natural group homomorphism $\varphi\colon \mathcal{W}_\chi \longrightarrow \mathcal{W}_0$ is not an isomorphism. Then φ fits into the exact sequence*

$$1 \longrightarrow \{1,\nu\} \longrightarrow \mathcal{W}_\chi \xrightarrow{\varphi} \mathcal{W}_0 \longrightarrow 1$$

and ν lies in the centre $Z(\mathcal{W}_\chi)$ of the group $\mathcal{W}_\chi$.

From the work of Hasse [4] we know that the genus field K^* of the quadratic field K may be expressed as the compositum

$$K^* = \mathbb{Q}(\sqrt{p_1^*}, \ldots, \sqrt{p_n^*})$$

where $N = p_1^* \cdots p_n^*$ is the decomposition of the fundamental discriminant N into prime discriminants

$$p^* = \begin{cases} (-1)^{\frac{p-1}{2}} p & \text{if } p \text{ is and odd prime,} \\ -4, \pm 8 & \text{if } p = 2. \end{cases}$$

Theorem 2. *For each prime power p^k that divides exactly N, we have*

$$w_{p^k} \in Z(\mathcal{W}_\chi)$$

if and only if the prime discriminant p^* is positive. In particular, the central extension in Theorem 1 splits if and only the genus field K^* of K is totally real.

Computer calculations in the range $N \leq 31,980$ suggest the following conjecture.

Conjecture 3. *If $\mathcal{W}_\chi$ has cyclic centre, then*

$$\mathcal{W}_\chi \cong \begin{cases} 2_+^{1+n} \text{ or } 2_-^{1+n} & \text{if } n \text{ is even,} \\ \mathcal{P}_{(n-1)/2}, & \text{if } n \text{ is odd.} \end{cases}$$

Here 2_+^{1+n} and 2_-^{1+n} are the two central extensions of an elementary abelian 2-group of rank n and centre of order 2, known as the Hall-Higmann [3] extra-special 2-groups, where n is even. Their representation theory has been studied by Quillen [7] and by Griess [2]. The group $\mathcal{P}_k$ may be defined by letting $\mathcal{P}_1$ be the subgroup of $\mathrm{GL}_2(\mathbb{C})$ generated by the matrices

$$\mathsf{s}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathsf{s}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \mathsf{s}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

which are known from the work of Pauli [6, p. 608], and then let

$$\mathcal{P}_k = \{g_1 \otimes \cdots \otimes g_k \,|\, g_1, \ldots, g_k \in \mathcal{P}_1\} \subset \mathrm{GL}_{2k}(\mathbb{C}),$$

for each $k > 1$. It is a group of cardinality 4^{k+1} known as the Pauli group on k-qubits.

2. The proofs

2.1. **Proof of Theorem 1.** After collecting together some material about modular curves and the Atkin-Leher automorphisms W_Q, we show that they are well-defined on the modular curve $X_\chi(N)$. This is accomplished in Lemma 1, below. Then we show that W_Q^2 is a dimond automorphism and also a central element. This is accomplished in Lemma 2 and in Lemma 3, respectively. Then we proceed to prove Theorem 1.

Let $Y_1(N)$ be the moduli space that classifies ordered pairs (E, P), where E is an elliptic curve over $\mathbb{C}$ and P is a point of order N on E, and let $Y_0(N)$ be the (coarse) moduli space that classifies ordered pairs that classifies ordered pairs (E, E') of elliptic curves E and E' over $\mathbb{C}$ together with a cyclic isogeny $E \longrightarrow E'$ of degree N. As usual, let $X_1(N)$ and $X_0(N)$ denote the corresponding smooth completions. There are natural identifications

$$X_1(N)(\mathbb{C}) \cong \mathfrak{H}^*/\Gamma_1(N)$$

and

$$X_0(N)(\mathbb{C}) \cong \mathfrak{H}^*/\Gamma_0(N),$$

where

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \,|\, a, d \equiv 1 \pmod{N} \right\}$$

and

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,|\, c \equiv 0 \pmod{N} \right\}$$

act on the extended upper half plane $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ via Möbius transformations. The multiplication-by-r-map $P \mapsto [r]P$ induces the diamond automorphism $\langle r \rangle$ of $X_1(N)$, which may be represented by any matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ such that

$$r \equiv d \pmod{N}.$$

From the work of Shimura [8, pp. 169, 172] the group

$$\Gamma_\chi(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \,|\, \chi(d) = 1 \right\}$$

is the congruence subgroup associated to the modular curve $X_\chi(N)$. So there is a natural identification

$$X_\chi(N)(\mathbb{C}) \cong \mathfrak{H}^*/\Gamma_\chi(N).$$

Let Q be a positive integer exactly dividing N. That is, there is positive integer Q' such that $N = QQ'$ and $(Q, Q') = 1$. The matrix

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & Qt \end{pmatrix},$$

where x, y, z, $t \in \mathbb{Z}$ are such that $t \equiv 1 \pmod{Q'}$ and $\det W_Q = Q$, normalises $\Gamma_1(N)$ and thus it uniquely determines an automorphism of $X_1(N)$ we shall denote W_Q.

Lemma 1. *For each Q exactly dividing N the matrix W_Q normalises $\Gamma_\chi(N)$ and hence it uniquely determines an automorphism of $X_1(N)$ which we shall denote w_Q.*

Proof. As in Diamond and Im [1, p. 56], for each Q as above the automorphism $M \mapsto W_Q M W_Q^{-1}$ of the Hecke congruence subgroup $\Gamma_0(N)$ induces the involution α_Q of the group $(\mathbb{Z}/N\mathbb{Z})^\times$ defined by the commutativity of the diagram

$$\begin{array}{ccc} (Z/NZ)^\times & \xrightarrow{\qquad\alpha_Q\qquad} & (Z/NZ)^\times \\ \downarrow & & \downarrow \\ (Z/QZ)^\times \times (Z/Q')^\times & \xrightarrow{id\times(\cdot)^{-1}} & (Z/QZ)^\times \times (Z/Q')^\times \end{array}$$

Composing χ with α_Q gives an even, primitive quadratic Dirichlet character ψ of conductor N. By uniqueness, $\psi = \chi$ and thus

$$\alpha(H) = H,$$

where $H = \mathrm{Ker}(\chi)$. Hence W_Q lies in the normaliser of $\Gamma_\chi(N)$ in $\mathrm{PGL}_2^+(\mathbb{Q})$ (cf. Proposition 2.2 of Im, Jeon, and Kim [5, p. 789]) and the lemma follows. □

Lemma 2. *For each Q that divides N exactly we have*

$$W_Q^2 = \langle d \rangle,$$

for some $d \in \mathcal{G}$.

Proof. Each automorphism w_Q is represented by an Atkin-Lehner matrix

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & Qt \end{pmatrix},$$

where x, y,z, and $t \in \mathbb{Z}$ are such that $\det(W_Q) = Q$. We have

$$\frac{1}{Q} W_Q = \begin{pmatrix} Qx^2 + Q'yz & xy + yt \\ Nxz + Ntz & Qt^2 + Q'yz \end{pmatrix} \in \Gamma_0(N).$$

Therefore

$$w_Q^2 = \langle Qt^2 + Q'yz \rangle$$

and the lemma follows. □

Lemma 3. *If Q_1 and Q_2 are prime powers that exactly divide N, the Atkin-Lehner automorphisms W_{Q_1} and W_{Q_2} satisfy*

$$(W_{Q_1} W_{Q_2})^2 = (W_{Q_2} W_{Q_1})^2.$$

Proof. Let Q_1 and Q_2 be exact divisors of N and for each $i \in \{1, 2\}$ consider the Atkin-Lehner matrix

$$W_{Q_i} = \begin{pmatrix} Q_i x_i & y_i \\ N z_i & Q_i t_i \end{pmatrix}.$$

Clearly

$$\frac{1}{Q_1 Q_2} (W_{Q_1} W_{Q_2})^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

and

$$\begin{aligned} Q_1 Q_2 d = {} & N Q_1^2 x_1 y_2 z_2 t_1 + Q_1^2 Q_2^2 t_1^2 t_2^2 + \\ & N Q_1 Q_2 x_1 x_2 y_2 z_1 + N Q_1 Q_2 y_1 z_2 t_1 t_2 + 2N Q_1 Q_2 y_2 z_1 t_1 t_2 + \\ & N Q_2^2 x_2 y_1 z_1 t_2 + N^2 y_2^2 z_1^2. \end{aligned}$$

Let Q_1' and Q_2' be such that $Q_1 Q_1' = Q_2 Q_2' = N$. Then

$$\begin{aligned} d = {} & Q_1 Q_2' x_1 y_2 z_2 t_1 + Q_1 Q_2 t_1^2 t_2^2 + \\ & N x_1 x_2 y_2 z_1 + N y_1 z_2 t_1 t_2 + 2N y_2 z_1 t_1 t_2 + \\ & Q_1' Q_2 x_2 y_1 z_1 t_2 + Q_1' Q_2' y_2^2 z_1^2 \\ \equiv {} & Q_1 Q_2' x_1 y_2 z_2 t_1 + Q_1 Q_2 t_1^2 t_2^2 + \\ & Q_1' Q_2 x_2 y_1 z_1 t_2 + Q_1' Q_2' y_2^2 z_1^2 \pmod{N} \end{aligned}$$

Assume $Q_1 = p_1^{k_1}$ and $Q_2 = p_2^{k_2}$ are distinct prime powers that divide N exactly and note that

$$Q_1' Q_2' \equiv 0 \pmod{N}.$$

This immediately gives the congruence

$$d \equiv Q_1 Q_2' x_1 y_2 z_2 t_1 + Q_1 Q_2 t_1^2 t_2^2 + Q_1' Q_2 x_2 y_1 z_1 t_2 \pmod{N}$$

and the lemma follows. □

The group $\mathcal{W}_\chi$ is generated by the Atkin-Lehner automorphisms w_Q automorphisms, where $Q = p^k$ runs through the set of prime powers that divide N exactly. Therefore

$$(\alpha\beta)^2 = (\beta\alpha)^2,$$

for all α and $\beta \in \mathcal{W}_\chi$. This is equivalent to the equation

$$\beta\gamma^2\beta^{-1} = \gamma^2,$$

where $\gamma = \alpha\beta$, again for all α and $\beta \in \mathcal{W}_\chi$. In other words, every square is central. Hence $\mathcal{W}_\chi$ is a central extension of an elementary abelian 2-group.

Lemma 2 implies that the exponent of the group $\mathcal{W}_\chi$ is either 2 or 4. Assume that the natural group homomorphism

$$\varphi\colon \mathcal{W}_\chi \longrightarrow \mathcal{W}_0$$

is not an isomorphism. Then the exponent of $\mathcal{W}_\chi$ is 4 and we have $w_Q^2 = \nu$, for some Q exactly dividing N. As all squares in $\mathcal{W}_\chi$ are central, we thus have $\nu \in Z(\mathcal{W}_\chi)$ and Theorem 1 follows.

2.2. **Proof of Theorem 2.** Let Q_1 and Q_2 be distinct prime powers that exactly divide the fundamental discriminant N. First we will prove a lemma that gives a relation satisfied by Atkin-Lehner automorphisms W_{Q_i} on the modular curve $X_1(N)$. Then, by projecting the automorphisms W_{Q_i} to $X_\chi(N)$, we get a corresponding relation for the automorphisms w_{Q_i}. Finally, we apply quadratic reciprocity and its complements to the latter relation and prove Theorem 2.

Lemma 4. *The commutator of the Atkin-Lehner automorphisms W_{Q_1} and W_{Q_2} is a diamond automorphism. More precisely,*

$$[W_{Q_1}, W_{Q_2}] = \langle d \rangle,$$

where the element $d \in \mathcal{G}$ is completely characterised by the three congruences

$$\begin{aligned} d &\equiv 1 \pmod{(Q_1Q_2)'}, \\ d &\equiv Q_2 x_2^2 \pmod{Q_1}, \\ d &\equiv Q_1 t_1^2 \pmod{Q_2}. \end{aligned}$$

Proof. Let W_{Q_1} and W_{Q_1} be as above. A direct calculation shows that

$$W_{Q_1}W_{Q_2}W_{Q_1}^{-1}W_{Q_2}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{\upsilon}\begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where

$$\begin{aligned}
A &= NQ_1Q_2x_1y_1z_2t_2 - NQ_1Q_2x_1x_2y_1z_2 + NQ_1Q_2x_1y_2z_1t_2 - NQ_1Q_2y_1z_2t_1t_2 + \\
&\quad NQ_1^2x_1^2y_2z_2 + NQ_2^2y_1z_1t_2^2 - Q_1^2Q_2^2x_1x_2t_1t_2 - N^2y_1^2z_2^2 \\
B &= NQ_1y_1y_2z_2t_1 - NQ_1x_1y_2^2z_1 - Q_1^2Q_2x_1^2x_2y_2 + Q_1^2Q_2x_1x_2y_2t_1 + \\
&\quad Q_1Q_2^2x_1x_2^2y_1 - Q_1Q_2^2x_1x_2y_1t_2 + NQ_2x_2y_1^2z_2 - NQ_2y_1y_2z_1t_2, \\
C &= NQ_1^2Q_2x_1z_2t_1t_2 - NQ_1^2Q_2z_2t_1^2t_2 - NQ_1Q_2^2x_2z_1t_1t_2 + NQ_1Q_2^2z_1t_1t_2^2 + \\
&\quad N^2Q_1x_1y_2z_1z_2 - N^2Q_1y_1z_2^2t_1 - N^2Q_2x_2y_1z_1z_2 + N^2Q_2y_2z_1^2t_2, \\
D &= NQ_1Q_2x_2y_1z_2t_1 - NQ_1Q_2x_1x_2y_2z_1 + NQ_1Q_2x_2y_2z_1t_1 - NQ_1Q_2y_2z_1t_1t_2 + \\
&\quad NQ_1^2y_2z_2t_1^2 + NQ_2^2x_2^2y_1z_1 - Q_1^2Q_2^2x_1x_2t_1t_2 - N^2y_2^2z_1^2, \\
\upsilon &= NQ_1^2x_1y_2z_2t_1 + NQ_2^2x_2y_1z_1t_2 - Q_1^2Q_2^2x_1x_2t_1t_2 - N^2y_1y_2z_1z_2.
\end{aligned}$$

These five integers are divisible by Q_1Q_2. More precisely,

$$\begin{aligned}
\frac{A}{Q_1Q_2} &= Nx_1y_1z_2t_2 - Nx_1x_2y_1z_2 + Nx_1y_2z_1t_2 - Ny_1z_2t_1t_2 + \\
&\quad Q_1Q_2'x_1^2y_2z_2 + Q_1'Q_2y_1z_1t_2^2 - Q_1Q_2x_1x_2t_1t_2 - Q_1'Q_2'y_1^2z_2^2 \\
\frac{B}{Q_1Q_2} &= Q_2'y_1y_2z_2t_1 - Q_2'x_1y_2^2z_1 - Q_1x_1^2x_2y_2 + Q_1x_1x_2y_2t_1 + \\
&\quad Q_2x_1x_2^2y_1 - Q_2x_1x_2y_1t_2 + Q_1'x_2y_1^2z_2 - Q_1'y_1y_2z_1t_2, \\
\frac{C}{Q_1Q_2} &= NQ_1x_1z_2t_1t_2 - NQ_1z_2t_1^2t_2 - NQ_2x_2z_1t_1t_2 + NQ_2z_1t_1t_2^2 + \\
&\quad NQ_2'x_1y_2z_1z_2 - NQ_2'y_1z_2^2t_1 - NQ_1'x_2y_1z_1z_2 + NQ_1'y_2z_1^2t_2, \\
\frac{D}{Q_1Q_2} &= Nx_2y_1z_2t_1 - Nx_1x_2y_2z_1 + Nx_2y_2z_1t_1 - Ny_2z_1t_1t_2 + \\
&\quad Q_1Q_2'y_2z_2t_1^2 + Q_1'Q_2x_2^2y_1z_1 - Q_1Q_2x_1x_2t_1t_2 - Q_1'Q_2'y_2^2z_1^2 \\
&\equiv -1 \pmod{(Q_1Q_2)'}, \\
\frac{\upsilon}{Q_1Q_2} &= Q_1Q_2'x_1y_2z_2t_1 + Q_1'Q_2x_2y_1z_1t_2 - Q_1Q_2x_1x_2t_1t_2 - Q_1'Q_2'y_1y_2z_1z_2 \\
&= -Q_1x_1t_1 + Q_1Q_2x_1x_2t_1t_2 - Q_2x_2t_2 + Q_1Q_2x_1x_2t_1t_2 + \\
&\quad -Q_1Q_2x_1x_2t_1t_2 - 1 + Q_1x_1t_1 + Q_2x_2t_2 - Q_1Q_2x_1x_2t_1t_2 \\
&= -1.
\end{aligned}$$

Only the congruence and the last equality deserve an explanation. Expanding the product on the left hand side of the equation

$$(Q_1x_1t_1 - Q_1'y_1z_1)(Q_2x_2t_2 - Q_2'y_2z_2) = 1$$

immediately gives

$$Q_1Q_2x_1x_2t_1t_2 \equiv 1 \pmod{(Q_1Q_2)'},$$

which yields

$$\frac{D}{Q_1Q_2} \equiv -1 \pmod{(Q_1Q_2)'}. \tag{1}$$

By making appropriate subtitutions with the help of

$$Q_1'z_1y_1 = -1 + Q_1x_1t_1 \tag{2}$$

and

$$Q_2'z_2y_2 = -1 + Q_2x_2t_2 \tag{3}$$

we get

$$\frac{v}{Q_1Q_2} = -1.$$

The last equation implies that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = -\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_0(N)$$

and thus

$$[W_{Q_1}, W_{Q_2}] = \langle d \rangle.$$

From (1) we immediately have

$$d \equiv 1 \pmod{(Q_1Q_2)'}.$$

By making again appropriate subtitutions with the help of Equation 2 and Equation 3, we get

$$\begin{aligned} d = & -Nx_2y_1z_2t_1 + Nx_1x_2y_2z_1 - Nx_2y_2z_1t_1 + Ny_2z_1t_1t_2 + \\ & Q_1t_1^2 - Q_1Q_2x_2t_1^2t_2 + Q_2x_2^2 - Q_2Q_1x_1x_2^2t_1 + \\ & Q_1Q_2x_1x_2t_1t_2 + Q_1'Q_2'y_2^2z_1^2, \end{aligned}$$

which clearly satisfies the congruences

$$d \equiv Q_2x_2^2 \pmod{Q_1}$$

and

$$d \equiv Q_1t_1^2 \pmod{Q_2},$$

so the lemma follows. □

It follows from the work of Weber [9, p. 322] that the fundamental discriminant N has a unique expression as a product of prime discriminants

$$N = p_1^* \dots p_n^*.$$

Moreover, the primitive character χ may be expressed as a product

$$\chi = \chi_{p_1^*} \cdots \chi_{p_n^*},$$

where

$$\chi_{p_i^*} = \left(\frac{p_i^*}{\cdot}\right)$$

and $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol. To simplify the exposition, assume that $p_1 < p_2 < \dots p_n$. (So that $p_1 = 2$ if and only if N is odd.) The quadratic reciprocity law and its supplements give

$$\chi = \left(\frac{\cdot}{p_1}\right) \dots \left(\frac{\cdot}{p_n}\right), \tag{4}$$

if N is odd and

$$\chi = \chi_{p_1^*}\left(\frac{\cdot}{p_2}\right) \dots \left(\frac{\cdot}{p_n}\right), \tag{5}$$

where χ_{-4} is the non-trivial character modulo 4, χ_8 is the even primitive quadratic character modulo 8, and $\chi_{-8} = \chi_{-4}\chi_8$ is the odd primitive quadratic character modulo 8, otherwise. In order to prove Theorem 2 we divide into cases depending on the first prime discriminant p_1^*, as follows.

Case 1. *The fundamental discriminant N is odd.* In this case Q_1 and Q_2 are distinct odd primes. Lemma 4 implies that

$$\left(\frac{d}{Q}\right) = 1,$$

for each prime divisor Q of N such that $Q \neq Q_1$ and $Q \neq Q_2$,

$$\left(\frac{d}{Q_1}\right) = \left(\frac{Q_1}{Q_2}\right),$$

and

$$\left(\frac{d}{Q_2}\right) = \left(\frac{Q_2}{Q_1}\right).$$

So Equation 4 yields

$$\chi(d) = \left(\frac{d}{Q_1}\right)\left(\frac{d}{Q_2}\right) = \left(\frac{Q_1}{Q_2}\right)\left(\frac{Q_2}{Q_1}\right) = (-1)^{\frac{Q_1-1}{2}\frac{Q_2-1}{2}},$$

where last equality is the quadratic reciprocity law. In other words,

$$w_{Q_1} w_{Q_2} = w_{Q_2} w_{Q_1}$$

if and only if either $Q_1 \equiv 1 \pmod 4$ or $Q_2 \equiv 1 \pmod 4$. In particular, we may conclude that $w_{Q_1} \in Z(\mathcal{W}_\chi)$ if and only if $Q_1 \equiv 1 \pmod 4$ and Theorem 2 follows.

Case 2. *The fundamental discriminant N is even and such that the prime discriminant divisor $p_1^* = -4$.* Suppose that $Q_1 = 4$, so Q_2 is necessarily odd prime. Lemma 4 implies that

$$\left(\frac{d}{Q}\right) = 1,$$

for each odd prime divisor Q of N,

$$\chi_{-4}(d) = \chi_{-4}(Q_2),$$

and

$$\left(\frac{d}{Q_2}\right) = 1.$$

So Equation 5 yields

$$\chi(d) = \chi_{-4}(Q_2).$$

As N is positive and $p_1^* = -4$ is negative, then $\chi_{-4}(Q_2) = -1$, for some odd prime Q_2. Hence $w_{Q_1} \notin Z(\mathcal{W}_\chi)$. The remaining case is Q_1 and Q_2 are both odd primes. But this case may be dealt with in a similar way as in **Case 1** and Theorem 2 follows.

Case 3. *The fundamental discriminant N is even and such that the prime discriminant divisor $p_1^* = \pm 8$.* Suppose that $Q_1 = 4$, so Q_2 is necessarily odd prime. Lemma 4 implies that

$$\left(\frac{d}{Q}\right) = 1,$$

for each odd prime divisor Q of N,

$$\chi_8(d) = \chi_8(Q_2),$$

and

$$\left(\frac{d}{Q_2}\right) = \chi_8(Q_2).$$

Hence $\chi_8(d) = (\frac{d}{Q_2})$. Therefore

$$\chi(d) = \chi_8(d)\chi_8(d) = 1,$$

if $p_1^* > 0$ and

$$\chi(d) = \chi_{-8}(d)\chi_8(d) = \chi_{-4}(d) = \chi_{-4}(Q_2),$$

if $p_1^* < 0$. In the former case, we immediately have $w_{Q_1} \in Z(\mathcal{W}_\chi)$, while in the latter case we argue as in **Case 2** and conclude that $w_{Q_1} \notin Z(\mathcal{W}_\chi)$. Again,

the remaining case is Q_1 and Q_2 are both odd primes. But this case may be dealt with in a similar way as in **Case 1** and Theorem 2 follows.

References

1. F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Conference proceedings,Canadian Mathematical Society, vol. 17, American Mathematical Society, Providence, RI, 1995, pp. 39–133.
2. R. L. Griess, *Automorphisms of extra special groups and nonvanishing degree 2 cohomology*, Pacific Journal of Mathematics **48** (1973), no. 2, 403–422.
3. P. Hall and G. Higman, *On the p-length of p-soluble groups and reduction theorems for Burnside's problem*, Proceedings of the London Mathematical Society **3** (1956), no. 7, 1–42.
4. H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, Journal of the Mathematical Society of Japan **3** (1951), no. 1, 45–51.
5. B. H. Im, D. Y. Jeon, and C. H. Kim, *Normalizers of intermediate congruence subgroups of the hecke subgroups*, Open Mathematics **15** (2017), no. 1, 787–799.
6. W. Pauli, *Zur Quantenmechanik des magnetischen Elektrons*, Zeitschrift für Physik **43** (1927), no. 9, 601–623.
7. D. Quillen, *The Mod 2 Cohomology Rings of Extra-special 2-groups and the Spinor Groups.*, Mathematische Annalen **194** (1971), 197–212.
8. G. Shimura, *Class fields over real quadratic fields in the theory of modular functions*, Several Complex Variables II, Lecture Notes in Mathematics, vol. 185, Springer, Berlin, Heidelberg, 1971, pp. 169–188.
9. H. Weber, *Lehrbuch der Algebra*, vol. 3, F. Vieweg und Sohn, Braunschweig, 1908.

Email address: ccastanobernard@gmail.com