D. Bump, S. Friedberg and J. Hoffstein
Nagoya Math. J.
Vol. 119 (1990), 173-188

THE KUBOTA SYMBOL FOR $Sp(4, \mathbf{Q}(i))$[1)]

DANIEL BUMP, SOLOMON FRIEDBERG
AND
JEFFREY HOFFSTEIN

§ 1. Introduction

Following eariler work of Kubota and Mennicke, the major work of Bass, Milnor and Serre [1] constructed characters of congruence subgroups of the modular subgroups of $SL(n)$ and $Sp(2n)$ over a totally complex number field, which are related to the power residue symbol. They do not obtain the lowest possible level of these Kubota characters, nor does it appear possible to modify their arguments to extend the characters to the lowest possible level.

It is important for applications, such as our paper [2], that precise formulae for the Kubota symbol be available. The formulae are simplest if the ground field contains the fourth roots of unity, and so we will work over the field $\mathbf{Q}(i)$. We shall give here a construction of the Kubota symbol for $Sp(4)$ over this field, independent of the work of Bass, Milnor and Serre, with precise formulae for the symbol, and a proof of its multiplicativity. We will construct the symbol over a larger congruence subgroup of $Sp(4, \mathbf{Z}[i])$ than that afforded by the results of Bass Milnor and Serre. Because of this feature, our results do not follow from those of Bass, Milnor and Serre.

Since we wrote this paper, we were surprised to discover that it may actually be possible to extend the symbol to a character of an even larger congruence subgroup, $\Gamma(2)$ of $Sp(4, \mathbf{Z}[i])$. (We have not proved this, but it appears likely to be true.) The formulas which we give for the symbol are not valid without modification for that group, but it is likely that our method can be adapted to extend the symbol to that larger group. However, our results are adequate for the purposes of [2].

It should be mentioned that Johnson and Millson [3] have recently

Received August 25, 1989.
[1)] This work was supported by grants from the NSF.

investigated the theta multipliers for $Sp(2n, \mathbf{Z})$. See also Stark [4] and Styer [5].

To state the main result, let us introduce the following notation. Let $\mathcal{O} = \mathbf{Z}[i]$, $\lambda = 1 + i$, and $M = (\lambda^3)$. Let $Sp(4, \mathcal{O})$ denote the subgroup of $SL(4, \mathcal{O})$ consisting of matrices g satisfying $gJ^tg = J$, where

$$J = \begin{pmatrix} & & & -1 \\ & & -1 & \\ & 1 & & \\ 1 & & & \end{pmatrix}.$$

Let $\Gamma(M)$ denote the subgroup of $Sp(4, \mathcal{O})$ of matrices congruent to the identity modulo M, and let $\Gamma_P(M)$ be the subgroup of $\Gamma(M)$ of matrices having 2×2 block form $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$.

If $\gamma = (\gamma_{ij})$ is any square matrix of degree four, let $A_{ij} = A_{ij}(\gamma)$ denote the $(3, 4) \times (i, j)$ minor $\gamma_{3i}\gamma_{4j} - \gamma_{4i}\gamma_{3j}$. The A_{ij} are called the *invariants* (or *Plücker coordinates*) of γ.

Observe that if $\gamma, \gamma' \in \Gamma(M)$, then $A_{ij}(\gamma) = A_{ij}(\gamma')$ if and only if $\Gamma_P(M)\gamma = \Gamma_P(M)\gamma'$, so that the cosets of $\Gamma_P(M)\backslash\Gamma(M)$ are parametrized by these invariants (see Proposition 2.2 below for a more precise statement).

We shall construct a character κ: $\Gamma(M) \to \{\pm 1\}$, which is trivial on the subgroup $\Gamma_P(M)$. We shall give an explicit formula for $\kappa(\gamma)$ in terms of the invariants A_{ij} and the quadratic resdue symbol. The main result is

THEOREM 1.1. *There exists a unique character* κ: $\Gamma(M) \to \{\pm 1\}$ *such that if* $\gamma \in \Gamma(M)$ *has invariants* A_{ij}, *then assuming that* A_{24} *and* A_{34} *are coprime, we have*

$$\kappa(\gamma) = \left(\frac{A_{24}}{A_{34}}\right). \tag{1.1}$$

We will also give more complicated formulae for $\kappa(\gamma)$ in terms of the invariants which are valid even if A_{24} and A_{34} are not coprime.

§ 2. Preliminaries

We begin by collecting some facts on the arithmetic of $\mathcal{O}$. Recall that every ideal in $\mathcal{O}$ which is prime to M has a unique generator which is congruent to 1 modulo M. Such a generator is called *primitive*. If p is a prime ideal other than (λ), we shall also use the same letter p to

denote its unique primitive generator.

Let a, b be coprime elements of $\mathcal{O}$ such that λ does not divide b. Let (a/b) be the usual quadratic symbol. We have the following properties:

PROPOSITION 2.1. *The quadratic symbol satisfies*

(a) $(a/b) = \pm 1$ *if* a *and* b *are coprime, zero otherwise;*

(b) *If* p *is prime and if* $p \nmid a$, *then* $(a/p) = 1$ *or* -1 *according as the congruence* $x^2 \equiv a \bmod p$ *is or is not solvable;*

(c) $(aa'/b) = (a/b)(a'/b)$;

(d) $(a/bb') = (a/b)(a/b')$;

(e) *If* $\varepsilon \in \mathcal{O}^\times$, *then* $(a/\varepsilon b) = (a/b)$;

(f) *If* $a \equiv a' \bmod b$, *then* $(a/b) = (a'/b)$;

(g) *If* a *and* b *are primitive, then* $(a/b) = (b/a)$;

(h) *If* $a = A + Bi$ *is primitive, where* A, B *are rational integers so that* $A \equiv 1 \bmod 2$, $A - 1 \equiv B \bmod 4$, *then*

$$\left(\frac{i}{a}\right) = (-1)^{(1/4)(A^2+B^2-1)}, \quad \text{and} \quad \left(\frac{\lambda}{a}\right) = (-1)^{(1/4)(A-B-B^2-1)}.$$

(i) *If* $b \equiv b' \bmod a$ *and* $b \equiv b' \bmod \lambda^5$, *then* $(a/b) = (a/b')$.

(j) *If* $b \equiv b' \bmod a$ *and* $\lambda^4 \mid a$, *then* $(a/b) = (a/b')$.

Also, let us collect some facts concerning the invariants A_{ij}. For any $\gamma \in Sp(4, \mathcal{O})$, the invariants satisfy

$$A_{14} = -A_{23}, \tag{2.1}$$

$$A_{12}A_{34} - A_{13}A_{24} - A_{14}^2 = 0, \tag{2.2}$$

and

$$\gcd(A_{12}, A_{13}, A_{24}, A_{34}) = 1. \tag{2.3}$$

Indeed, (2.1) holds since γ is symplectic. Also (2.2) follows from (2.1) and the "Plücker relation" $A_{12}A_{34} - A_{13}A_{24} + A_{14}A_{23} = 0$, which is valid for the invariants of any matrix, symplectic or not. To prove (2.3), note that since γ is an integral unimodular matrix, so is the six by six matrix $\wedge^2\gamma$ of γ in the exterior square representation, and so the bottom row of this matrix is unimodular, i.e. $\gcd(A_{12}, A_{13}, A_{24}, A_{34}, A_{14}, A_{23}) = 1$. However by (2.1) and (2.2) any divisor of (2.3) would also divide A_{14} and A_{23}. Thus we have (2.3).

If $\gamma \in \Gamma(M)$, then in addition

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

$$A_{12}, A_{13}, A_{14}, A_{23}, A_{24} \equiv 0 \bmod M, \qquad A_{34} \equiv 1 \bmod M. \tag{2.4}$$

Conversely, we have

PROPOSITION 2.2. *Suppose $A_{ij} \in \mathcal{O}$ satisfy* (2.1), (2.2), (2.3) *and* (2.4). *Then there exists a unique coset in $\Gamma_P(M)\backslash\Gamma(M)$ with these invariants.*

One can give an explicit formula for a coset representative. For this, and the details of the proof, see [2].

§ 3. The Kubota symbol

First we give a formula for $\kappa(\gamma)$ which is valid even without the assumption that $\gcd(A_{24}, A_{34}) = 1$.

PROPOSITION 3.1. *Let $\gamma \in \Gamma(M)$ have invariants A_{ij} satisfying* (2.2), (2.3) *and* (2.4). *Let b be the primitive generator of the ideal* $\gcd(A_{34}, A_{13}, A_{24})$. *Choose a factorization $b = b'b''$ with b', b'' primitive such that $b' \mid A_{24}$ and $b'' \mid A_{13}$. Let $b = v\beta^2$, $b' = v'\beta'^2$, $b'' = v''\beta''^2$ such that v, v', v'' are squarefree and primitive. Factor $v = v_1v_2'' = v_1'v_2$ where v_1, v_2'', v_1' and v_2 are primitive, $v_1 \mid A_{24}$, $\gcd(v_2'', A_{24}) = 1$, $v_2 \mid A_{13}$, $\gcd(v_1', A_{13}) = 1$. Then $v_2'' \mid v''$ and $v_1' \mid v'$, so let $v'' = v_1''v_2''$, $v' = v_1'v_2'$. Let $A_{13} = b''A_{13}'$, $A_{24} = b'A_{24}'$, $A_{34} = bA_{34}''$, $A_{14} = v\beta A_{14}'$, so that*

$$A_{12}A_{34}'' - A_{13}'A_{24}' = vA_{14}'^2. \tag{3.1}$$

Then

$$\begin{aligned} \gcd(v_1'', A_{12}) &= \gcd(v_1, A_{34}'') = \gcd(v_2'', A_{24}') \\ &= \gcd(v_1, A_{13}') = \gcd(A_{24}', A_{34}'') = 1. \end{aligned} \tag{3.2}$$

Thus

$$\kappa(\gamma) = \left(\frac{A_{12}}{v_1''}\right)\left(\frac{A_{34}''}{v_1}\right)\left(\frac{A_{24}'}{v_2''}\right)\left(\frac{A_{13}'}{v_1}\right)\left(\frac{A_{24}'}{A_{34}''}\right) \tag{3.3}$$

is defined. Moreover, the expression (3.3) *is independent of the factorization $b = b'b''$.*

Proof. To show that $\gcd(v_1'', A_{12}) = 1$, observe that any prime common divisor of v_1'', A_{12} would divide $A_{12}, A_{13}, A_{24}, A_{34}$, contradicting (2.3). To show that $\gcd(v_1, A_{34}'') = 1$, observe that a common divisor would divide $A_{13}'A_{24}' = A_{12}A_{34}'' - vA_{14}'^2$, yet $A_{34}'', A_{13}'A_{24}'$ are coprime. In fact, this proves the stronger relation

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

$$\gcd(v, A''_{34}) = 1 . \tag{3.4}$$

To prove that $\gcd(v_1, A'_{13}) = 1$, note that a common divisor would divide $A_{12}A''_{34} = A'_{13}A'_{24} + vA'^2_{14}$, and so by (3.4) would divide A_{12}. Thus a common factor of v_1, A'_{13} would divide A_{12}, A_{13}, A_{24}, A_{34}, contradicting (2.3). The remaining two assertions of (3.2) are obvious.

To prove that the expression (3.3) is independent of the factorization $b = b'b''$, suppose $b = c'c''$, c', c'' primitive, $c' \mid A_{24}$, $c'' \mid A_{13}$, and let w'' be the primitive squarefree part of c''. Let $w'' = w''_1 v''_2$, $A_{13} = c''B'_{13}$, $A_{24} = c'B'_{24}$. We must show that

$$\left(\frac{A_{12}}{v''_1}\right)\left(\frac{A''_{34}}{v_1}\right)\left(\frac{A'_{24}}{v''_2}\right)\left(\frac{A'_{13}}{v_1}\right)\left(\frac{A'_{24}}{A''_{34}}\right) = \left(\frac{A_{12}}{w''_1}\right)\left(\frac{A''_{34}}{v_1}\right)\left(\frac{B'_{24}}{v''_2}\right)\left(\frac{B'_{13}}{v_1}\right)\left(\frac{B'_{24}}{A''_{34}}\right). \tag{3.5}$$

There exist primitive μ, ν where $\nu \mid \gcd(A'_{24}, B'_{13}, c'', b')$, $\mu \mid \gcd(A'_{13}, B'_{24}, c', b'')$ such that $b' = \nu\mu^{-1}c'$, $b'' = \mu\nu^{-1}c''$, $B'_{13} = \mu\nu^{-1}A'_{13}$, $B'_{24} = \nu\mu^{-1}A'_{24}$, and v''_1 equals $\mu\nu w''_1$ times a square, so the left side of (3.5) equals the right side, times a factor which equals

$$\left(\frac{A_{12}}{\mu\nu}\right)\left(\frac{\mu\nu}{v''_2}\right)\left(\frac{\mu\nu}{v_1}\right)\left(\frac{\mu\nu}{A''_{34}}\right) = \left(\frac{A_{12}A''_{34}}{\mu\nu}\right)\left(\frac{v}{\mu\nu}\right),$$

where we have invoked quadratic reciprocity. Every prime factor which divides $\mu\nu$ divides $A'_{13}A'_{24}$, so (3.1) implies (3.5).

PROPOSITION 3.2. *In the notation of Proposition* 3.1,

$$\begin{aligned}\gcd(v'_2, A_{12}) = \gcd(v_2, A''_{34}) = \gcd(v_1, A''_{13}) = \gcd(v_2, A'_{24}) \\ = \gcd(A'_{13}, A''_{34}) = 1 .\end{aligned} \tag{3.6}$$

Moreover the value of

$$\left(\frac{A_{12}}{v'_2}\right)\left(\frac{A''_{34}}{v_2}\right)\left(\frac{A'_{13}}{v'_1}\right)\left(\frac{A'_{24}}{v_2}\right)\left(\frac{A'_{13}}{A''_{34}}\right) \tag{3.7}$$

is independent of the factorization $b = b'b''$, *and equals* $\kappa(\gamma)$.

Proof. The proofs of (3.6), and the independence of (3.7) of the factorization $b = b'b''$ are exactly similar to the corresponding assertions in Proposition 3.1. We will verify that (3.7) equals $\kappa(\gamma)$.

By using (3.1), the ratio of (3.3) to (3.7) may be expressed as

$$\left(\frac{A_{12}}{v_1''v_2'}\right)\left(\frac{A_{34}''}{vv_1v_2}\right)\left(\frac{A_{13}'}{v_1v_1'}\right)\left(\frac{A_{24}'}{v_2v_2''}\right). \tag{3.8}$$

Observe that $v_1v_2v_1'v_2''$ and $v_1v_1'v_1''v_2'$ are squares and

$$\gcd(v_2'', v_1') = \gcd(v_1, v_2'') = \gcd(v_2, v_1') = 1,$$

so that the set S of primes dividing any one of $v_1'', v_2', v_1, v_2, v_1', v_2''$ may be partitioned into $S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \cup S_6 \cup S_7$ (disjoint) where

$p \mid v_1, v_2, v_1''$,	$p \nmid v_1', v_2'', v_2'$	if $p \in S_1$;
$p \mid v_1, v_2, v_2'$,	$p \nmid v_1', v_2'', v_1''$	if $p \in S_2$;
$p \mid v_1, v_1', v_1'', v_2'$,	$p \nmid v_2, v_2''$	if $p \in S_3$;
$p \mid v_1, v_1'$,	$p \nmid v_2, v_2'', v_1'', v_2'$	if $p \in S_4$;
$p \mid v_2, v_2''$,	$p \nmid v_1, v_1', v_1'', v_2'$	if $p \in S_5$;
$p \mid v_2, v_2'', v_1'', v_2'$,	$p \nmid v_1, v_1'$	if $p \in S_6$;
$p \mid v_1'', v_2'$,	$p \nmid v_1, v_2, v_1', v_2''$	if $p \in S_7$.

We may evaluate (3.8) by computing separately the contributions from $p \in S_i$, $i = 1, \cdots, 7$. Thus (3.8) equals

$$\left[\prod_{p \in S_1, S_2} \left(\frac{A_{12}A_{34}''}{p}\right)\left(\frac{A_{13}'A_{24}'}{p}\right)\right]\left[\prod_{\substack{i=3 \\ p \in S_i}}^{7} 1\right].$$

If $p \in S_1$ or S_2, $p \mid v$ and so the first product is one by (3.1). This completes the proof of Proposition 3.2.

PROPOSITION 3.3. *Let $\gamma \in \Gamma(M)$ have invariants A_{ij} satisfying* (2.2), (2.3) *and* (2.4). *Let c be a generator of the ideal $\gcd(A_{24}, A_{12}A_{34})$. Factor $c = c'c''$ where $c'' \mid A_{12}$, and $c' \mid A_{34}$ is primitive. Let $c = u\delta^2$, $c' = u'\delta'^2$, $c'' = u''\delta''^2$, where u, u', u'' are squarefree and u' is primitive. Factor $u = u_1u_2'' = u_1'u_2$ where $u_1 \mid A_{34}$ is primitive, $(u_2'', A_{34}) = 1$, $u_2 \mid A_{12}$, $(u_1', A_{12}) = 1$. Then $u_2'' \mid u''$, $u_1' \mid u'$, so let $u'' = u_1''u_2''$, $u' = u_1'u_2'$. Then $\lambda \nmid u_1, u_1', u_2', u_1''$,*

$$\begin{aligned}\gcd(u_1'', A_{13}) &= \gcd(u_1, A_{24}'') = \gcd(u_2'', A_{34}') \\ &= \gcd(u_1, A_{12}') = \gcd(A_{34}', A_{24}'') = 1\end{aligned} \tag{3.9}$$

and

$$\kappa(\gamma) = \left(\frac{A_{13}}{u_1''}\right)\left(\frac{A_{24}''}{u_1}\right)\left(\frac{u_2''}{A_{34}'}\right)\left(\frac{A_{12}'}{u_1}\right)\left(\frac{A_{24}''}{A_{34}'}\right). \tag{3.10}$$

Proof. It is clear that $\lambda \nmid u_1, u_1', u_2'$. Since $u_1u_1'u_2'u_1''$ is a square, it follows that $\lambda \nmid u_1''$. The proof of (3.9) is similar to the proof of (3.2). An

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

argument similar to the proof of (3.5) shows that the right-hand side of (3.10) is independent of the choice of factorization $c = c'c''$ (and the other minor choices involved). To compare (3.10) to (3.3), we may therefore assume that $b' = c'$ is the primitive generator of the ideal $\gcd(A_{24}, A_{34})$, so $u' = v'$. Then $A'_{34} = b''A''_{34}$, $A'_{24} = c''A''_{24}$. The ratio of (3.10) to (3.3) is

$$\left(\frac{A_{12}}{v''_1}\right)\left(\frac{A''_{34}}{v_1}\right)\left(\frac{A'_{24}}{v''_2}\right)\left(\frac{A'_{13}}{v_1}\right)\left(\frac{A'_{24}}{A''_{34}}\right)\left(\frac{A_{13}}{u''_1}\right)\left(\frac{A''_{24}}{u_1}\right)\left(\frac{u''_2}{A'_{34}}\right)\left(\frac{A'_{12}}{u_1}\right)\left(\frac{A''_{24}}{A_{24}}\right).$$

Replacing A_{12}, A'_{24}, A'_{34} and A_{13} by $c''A'_{12}$, $c''A''_{24}$, $b''A''_{34}$ and $b''A'_{13}$, and performing obvious simplifications, this equals

$$\left(\frac{A'_{12}}{v''_1}\right)\left(\frac{A''_{34}}{v_1}\right)\left(\frac{A''_{24}}{v''_1}\right)\left(\frac{A'_{13}}{v_1}\right)\left(\frac{A'_{13}}{u''_1}\right)\left(\frac{A''_{24}}{u_1}\right)\left(\frac{u''_1}{A''_{34}}\right)\left(\frac{A_{12}}{u_1}\right) = \left(\frac{A''_{34}A'_{13}}{v_1u''_1}\right)\left(\frac{A''_{24}A_{12}}{v''_1u_1}\right). \tag{3.11}$$

It is easy to see that $v_1u''_1v''_1u_1$ is a square and that $(u''_1, v''_1) = 1$. As in the proof that (3.8) equals one, one shows that (3.11) equals one by case-by-case consideration of the primes dividing any of v_1, u''_1, v''_1, u_1. The cases of concern are

$$\begin{aligned} &p \mid v_1, v''_1, && p \nmid u''_1, u_1, \\ &p \mid v_1, u_1, && p \nmid u''_1, v''_1, \\ &p \mid u''_1, u_1, && p \nmid v_1, v''_1. \end{aligned}$$

We have $A'_{12}A''_{34} - A'_{13}A''_{24} = w(A'_{14})^2$ where A'_{14} is an integer, and w is the squarefree part of bc''. It may be verified that in each of the three cases above, $p \mid w$, so that

$$\left(\frac{A''_{34}A'_{13}}{p}\right) = \left(\frac{A''_{24}A_{12}}{p}\right)$$

so there is no contribution. In the other two cases,

$$\begin{aligned} &p \mid v_1, u''_1, && p \nmid v''_1, u_1 \\ &p \mid u_1, v''_1, && p \nmid u''_1, v_1 \end{aligned}$$

it is obvious that there is no contribution. This completes the proof of Proposition 3.3.

PROPOSITION 3.4. *Let γ, $\delta \in \Gamma(M)$ have invariants A_{ij}, B_{ij} respectively, where $A_{34} = B_{34}$, $A_{12} = B_{12}$, $A_{13} = B_{24}$, $A_{24} = B_{13}$, and $A_{14} = B_{14}$. Then $\kappa(\gamma) = \kappa(\delta)$.*

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

Proof. This follows by comparing the statements of Propositions 3.1 and 3.2.

We would like to show that the Kubota symbol agrees with (A_{24}/A_{34}) as in the statement of Theorem 1.1. It is convenient to prove slightly more.

PROPOSITION 3.5. *Let $\gamma \in \Gamma(M)$ have invariants A_{ij}. Let b' be the primitive generator of the ideal $\gcd(A_{24}, A_{34})$, and let $A_{24} = b'A'_{24}$. Assume that A'_{24} and A_{34} are coprime. Let $b' = v'\beta'^2$ where v' is primitive and squarefree. Then v' and A_{12} are coprime, and*

$$\kappa(\gamma) = \left(\frac{A_{12}}{v'}\right)\left(\frac{A'_{24}}{A_{34}}\right).$$

Proof. Suppose p is a prime dividing v' and A_{12}. Then $p \mid A_{34}, A_{24}, A_{12}$ so by (2.3) $p \nmid A_{13}$. In the notation of Proposition 3.1, let b'' be the primitive generator of the ideal $\gcd(A_{13}, A_{34}b'^{-1})$. Then $p \mid v'$ and $p \nmid v''$ so $p \mid v$. Now $A'_{13}A'_{24} \equiv A_{12}A''_{34} \bmod v$ which is a contradiction since $p \mid A_{12}$, $p \nmid A'_{13}A'_{24}$. Thus $(A_{12}, v') = 1$. Using (3.3), $\kappa(\gamma)(A_{12}/v')(A'_{24}/A_{34})$ simplifies to

$$\left(\frac{A_{12}}{v'_1v''_1v_2}\right)\left(\frac{A''_{34}}{v_1}\right)\left(\frac{A'_{13}A'_{24}}{v_1}\right) = \left(\frac{A_{12}}{v_1v'_1v''_1v_2}\right)$$

since $A'_{13}A'_{24} \equiv A_{12}A''_{34} \bmod v_1$. This equals 1 since $v_1v'_1v''_1v_2$ is a square.

We trun now to the proof of Theorem 1.1. Let $\hat{\Gamma}$ be the subgroup of $Sp(4, \mathcal{O})$ consisting of matrices $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ where $B \equiv C \equiv 0 \bmod M$ and $\det(A)$, $\det(D)$ are primitive. Let $\hat{\Gamma}_P$ be the subgroup where $C \equiv 0$. Clearly $\Gamma(M) \subset \hat{\Gamma}$ and $\Gamma_P(M) = \Gamma(M) \cap \hat{\Gamma}_P$.

PROPOSITION 3.6. *The natural map $\Gamma_P(M)\backslash\Gamma(M) \to \hat{\Gamma}_P\backslash\hat{\Gamma}$ is a bijection.*

Proof. Clearly it is an injection. On the other hand, if $\gamma \in \hat{\Gamma}$ the invariants of γ satisfy the hypotheses of Theorem 2.5 of [2], and so the coset $\hat{\Gamma}_P\gamma$ contains a representative in $\Gamma(M)$. Thus the natural map is surjective.

We have pointed out that κ is actually a function on $\Gamma_P(M)\backslash\Gamma(M)$. Thus Proposition 3.7 implies that κ may be regarded as a function on $\hat{\Gamma}$. Theorem 1.1 will follow from Proposition 3.5 and the following stronger

THEOREM 3.7. *κ is a character of $\hat{\Gamma}$.*

Let Σ be the set of $\gamma \in \hat{\Gamma}$ whose invariants satisfy $\gcd(A_{24}, A_{34}) = 1$. Let

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

$$\hat{\Gamma}_0 = \{\gamma \in \hat{\Gamma} \mid \kappa(\gamma) = \kappa(\gamma^{-1}) \text{ and } \kappa(\gamma'\gamma) = \kappa(\gamma')\kappa(\gamma) \text{ if } \gamma' \in \hat{\Gamma}\},$$
$$\hat{\Gamma}_1 = \{\gamma \in \hat{\Gamma} \mid \kappa(\gamma) = \kappa(\gamma^{-1}) \text{ and } \kappa(\gamma'\gamma) = \kappa(\gamma')\kappa(\gamma) \text{ if } \gamma' \in \hat{\Gamma},\ \gamma'\gamma \in \Sigma\}.$$

Evidently $\hat{\Gamma}_0$ is a subgroup of $\hat{\Gamma}$ and κ is a character of $\hat{\Gamma}_0$. We have $\hat{\Gamma}_0 \subseteq \hat{\Gamma}_1 \subseteq \hat{\Gamma}$. It is not *a priori* clear that $\hat{\Gamma}_1$ is a subgroup of $\hat{\Gamma}$, but in fact we will eventually prove that $\hat{\Gamma}_0 = \hat{\Gamma}_1 = \hat{\Gamma}$.

LEMMA 3.8. *The element*

$$w_2 = \begin{pmatrix} & -1 & & \\ 1 & & & \\ & & & 1 \\ & & -1 & \end{pmatrix}$$

of $\hat{\Gamma}$ *lies in* $\hat{\Gamma}_0$.

In fact, this is simply a restatement of Proposition 3.4.

LEMMA 3.9. *If* $t \in M$ *then*

$$\gamma = \begin{pmatrix} 1 & & & \\ & 1 & t & \\ & & 1 & \\ & & & 1 \end{pmatrix} \in \hat{\Gamma}_0.$$

Proof. Suppose γ' has invariants A_{ij}, and $\gamma'\gamma$ has invariants B_{ij}. Then $B_{12} = A_{12}$, $B_{24} = A_{24}$, $B_{14} = A_{14}$, $B_{13} = A_{13} + tA_{12}$, $B_{34} = A_{34} + tA_{24}$. To prove that $\kappa(\gamma'\gamma) = \kappa(\gamma')$ (whence $\gamma \in \hat{\Gamma}_0$ since $\kappa(\gamma) = 1$), it is convenient to use Proposition 3.3, to which we refer for notation. We have, by Proposition 3.3

$$\kappa(\gamma') = \left(\frac{A_{13}}{u_1''}\right)\left(\frac{A_{24}''}{u_1}\right)\left(\frac{u_2''}{A_{34}'}\right)\left(\frac{A_{12}'}{u_1}\right)\left(\frac{A_{24}''}{A_{34}'}\right)$$
$$\kappa(\gamma'\gamma) = \left(\frac{B_{13}}{u_1''}\right)\left(\frac{A_{24}''}{u_1}\right)\left(\frac{u_2''}{B_{34}'}\right)\left(\frac{A_{12}'}{u_1}\right)\left(\frac{A_{24}''}{B_{34}'}\right)$$

in which $B_{34}' = A_{34}' + tc''A_{24}''$. Thus $B_{34}' \equiv A_{34}' \bmod \lambda^6 A_{24}''$ which by Proposition 2.1 (i) implies that

$$\left(\frac{u_2''}{A_{34}'}\right) = \left(\frac{u_2''}{B_{34}'}\right), \qquad \left(\frac{A_{24}''}{A_{34}'}\right) = \left(\frac{A_{24}''}{B_{34}'}\right).$$

Also, clearly $(A_{13}/u_1'') = (B_{13}/u_1'')$ and so the two symbols $\kappa(\gamma')$ and $\kappa(\gamma'\gamma)$ are equal. Thus $\gamma \in \hat{\Gamma}_0$.

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

LEMMA 3.10. *If* $u \in M$ *then*

$$\gamma = \begin{pmatrix} 1 & & u & \\ & 1 & & u \\ & & 1 & \\ & & & 1 \end{pmatrix} \in \hat{\Gamma}_1 .$$

Proof. Let $\gamma' \in \hat{\Gamma}$, $\gamma'\gamma \in \Sigma$. Then if γ', $\gamma'\gamma$ have invariants A_{ij}, B_{ij} respectively, then $B_{12} = A_{12}$, $B_{13} = A_{13}$, $B_{24} = A_{24}$, $B_{14} = A_{14} + uA_{12}$ and $B_{34} = A_{34} + 2uA_{14} + u^2A_{12}$. We are assuming B_{24}, B_{34} to be coprime. Thus $\kappa(\gamma'\gamma) = (B_{24}/B_{34})$ while $\kappa(\gamma')$ is given by Proposition 3.1, to which we refer for notation. We have

$$\kappa(\gamma'\gamma) = \left(\frac{A'_{24}}{A''_{34}}\right)\left(\frac{A'_{24}}{A''_{34}B_{34}}\right)\left(\frac{v'}{B_{34}}\right).$$

Now

$$\begin{aligned} A''_{34}B_{34} &= A''_{34}A_{34} + 2uA''_{34}A_{14} + u^2A_{12}A''_{34} \\ &\equiv A''_{34}A_{34} + 2uA''_{34}A_{14} + u^2vA'^2_{14} \bmod u^2A'_{24} . \end{aligned}$$

The right side in this congruence equals $v(\beta A''_{34} + uA'_{14})^2$ and so by Proposition 2.1 (i)

$$\left(\frac{A'_{24}}{A''_{34}B_{34}}\right) = \left(\frac{A'_{24}}{v}\right).$$

It follows in particular from the preceding congruence that v, A'_{24} are coprime. Observe that v_1 and v''_1 divide A_{24}, so $v_1v''_1$ and B_{34} are coprime. As $v_1v'_1v''_1v'_2 = v_1v''_1v'_1$ is a square, it follows that

$$\left(\frac{v'}{B_{34}}\right) = \left(\frac{v_1v''_1}{B_{34}}\right) = \left(\frac{B_{34}}{v_1v''_1}\right) = \left(\frac{A_{12}}{v_1v''_1}\right)\left(\frac{A_{12}B_{34}}{v_1v''_1}\right).$$

Now $A_{12}B_{34} \equiv (A_{14} + uA_{12})^2 \bmod A_{24}$, and since $v_1, v''_1 \mid A_{24}$ it follows that

$$\kappa(\gamma'\gamma) = \left(\frac{A'_{24}}{v_1v''_2}\right)\left(\frac{A_{12}}{v_1v''_1}\right)\left(\frac{A'_{24}}{A''_{34}}\right).$$

Now $A_{12}A''_{34} \equiv A'_{24}A'_{13} \bmod v_1$ and so

$$\kappa(\gamma'\gamma) = \left(\frac{A_{12}}{v''_1}\right)\left(\frac{A''_{34}}{v_1}\right)\left(\frac{A'_{24}}{v''_2}\right)\left(\frac{A'_{13}}{v_1}\right)\left(\frac{A'_{24}}{A''_{34}}\right) = \kappa(\gamma')$$

by Proposition 3.1. Since $\kappa(\gamma) = 1$, this proves that $\gamma \in \hat{\Gamma}_1$.

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

LEMMA 3.11. *Let $A, B, C, D \in \mathcal{O}$, with A and D coprime. Then there exists $\rho \in \mathcal{O}$ such that $A + \rho B$ and $C + \rho D$ are coprime.*

Proof. If $D = 0$ we may take $\rho = 0$. Assume then that $D \neq 0$. Observe that if μ is a solution to $\gcd(A + \mu BD,\ C + \mu D^2) = 1$, then $\rho = \mu D$ is a solution to $\gcd(A + \rho B,\ C + \rho D) = 1$. Thus we may assume that every prime which divides D also divides B. Let d be the greatest common divisor of C and D. By Dirichlet's Theorem on Primes in an Arithmetic Progression, there exist infinitely many ρ such that $C + \rho D = pd$ where p is prime. Since every prime dividing d divides B, and since $\gcd(A, d) = 1$, we have $\gcd(A + \rho B, d) = 1$. Thus either $A + \rho B$, $C + \rho D$ are coprime or $p \mid A + \rho B$. It is sufficient to show that $p \mid A + \rho B$ can occur for only finitely many ρ. If $p \mid A + \rho B$ then $(A + \rho B)/(C + \rho D) = \sigma/d$ where $\sigma \in \mathcal{O}$. Solving for ρ,

$$\rho = \frac{C\sigma - AD}{-D\sigma + Bd}. \tag{3.12}$$

However, as σ runs through $\mathcal{O}$, the right side of (3.12) remains bounded, hence there are only finitely many possible σ.

Let $U(M)$ be the subgroup of $\hat{\Gamma}$ of all

$$\begin{pmatrix} 1 & & u & v \\ & 1 & t & u \\ & & 1 & \\ & & & 1 \end{pmatrix}, \qquad t, u, v \in M. \tag{3.13}$$

PROPOSITION 3.12. *If $\gamma \in \hat{\Gamma}$, there exists $\gamma' \in U(M)$ such that $\gamma\gamma' \in \Sigma$.*

Proof. If γ has invariants A_{ij} and γ' is the matrix in (3.13), then $\gamma\gamma'$ has invariants B_{ij} where $B_{34} = A_{34} - vA_{13} + tA_{24} + (u^2 - tv)A_{12} + 2uA_{14}$, $B_{24} = A_{24} - vA_{12}$, and $B_{12} = A_{12}$. Since $\gcd(A_{34}, A_{13}, A_{24}, A_{12}, A_{14}) = 1$, we may clearly arrange that B_{34} and B_{12} are coprime. We may then further adjust using v along with $t = u = 0$ by Lemma 3.11.

LEMMA 3.13. $U(M) \subset \hat{\Gamma}_0$.

Proof. First let us show that $U(M) \subset \hat{\Gamma}_1$. The matrix (3.13) may be factored as

$$\begin{pmatrix} 1 & & t & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} w_2 \begin{pmatrix} 1 & & v & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} w_2^{-1} \begin{pmatrix} 1 & & u & \\ & 1 & & u \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

where the first four matrices lie in $\hat{\Gamma}_0$ by Lemmas 3.8 and 3.9, and the fourth is in $\hat{\Gamma}_1$ by Lemma 3.10. Hence each matrix (3.13) lies in $\hat{\Gamma}_1$.

Now to prove that $U(M) \subset \hat{\Gamma}_0$, let $\gamma' \in \hat{\Gamma}$, $\gamma \in U(M)$. By Proposition 3.12, there exists $\gamma'' \in U(M)$ such that $\gamma'\gamma\gamma'' \in \Sigma$. Since $\gamma\gamma'' \in \hat{\Gamma}_1$ (as we have just proved), $\kappa(\gamma') = \kappa(\gamma'\gamma\gamma'')$. Now as $\gamma'' \in \hat{\Gamma}_1$, $\kappa(\gamma'\gamma\gamma'') = \kappa(\gamma'\gamma)$. It follows that $\gamma \in \hat{\Gamma}_0$.

LEMMA 3.14. *If* $e, f, g, h \in \mathcal{O}$, $eh - fg \equiv 1 \bmod M$ *then*

$$\gamma = \begin{pmatrix} e & f & & \\ g & h & & \\ & & e & -f \\ & & -g & h \end{pmatrix} \in \hat{\Gamma}_0 .$$

Proof. Observe that by Proposition 3.5, $\kappa(\gamma) = 1$. First let us prove that $\gamma \in \hat{\Gamma}_1$. Suppose that $\gamma' \in \hat{\Gamma}$, $\gamma'\gamma \in \Sigma$. If $\gamma', \gamma'\gamma$ have invariants A_{ij}, B_{ij} respectively, then $B_{12} = A_{12}$, $B_{13} = e^2A_{13} - 2egA_{14} - g^2A_{24}$, $B_{24} = h^2A_{24} + 2fhA_{14} - f^2A_{13}$, $B_{14} = (eh + fg)A_{14} - efA_{13} + ghA_{14}$, $B_{34} = A_{34}$. We are assuming B_{24}, B_{34} are coprime. Thus

$$\kappa(\gamma'\gamma) = \left(\frac{B_{24}}{B_{34}}\right).$$

We will compare this to $\kappa(\gamma')$ which is given by Proposition 3.1.

$$\left(\frac{B_{24}}{B_{34}}\right) = \left(\frac{B_{24}}{v_1}\right)\left(\frac{B_{24}}{v_2''}\right)\left(\frac{B_{24}}{A_{34}''}\right).$$

Since $u_1 \mid A_{24}, A_{14}$, $(B_{24}/v_1) = (A_{13}/v_1) = (A_{13}'/v_1)(v''/v_1)$. Also, since $v_2'' \mid A_{13}, A_{14}$, $(B_{24}/u_2'') = (A_{24}/v_2'') = (A_{24}'/v_2'')(v'/v_2'')$. Now $A_{24}'B_{24} \equiv v'(h\beta'A_{24}' - fA_{14}'')^2 \bmod A_{34}''$ where A_{14}'' is defined by $A_{14} = v'\beta'A_{14}''$. It is integral because $b' \mid A_{14}^2$. Since $\gcd(A_{24}'B_{24}, A_{34}'') = 1$ this proves that v', A_{34}'' are coprime and

$$\left(\frac{B_{24}}{A_{34}''}\right) = \left(\frac{v'}{A_{34}''}\right)\left(\frac{A_{24}'}{A_{34}''}\right).$$

Thus

$$\kappa(\gamma'\gamma) = \left(\frac{A_{13}'}{v_1}\right)\left(\frac{v''}{v_1}\right)\left(\frac{A_{24}'}{v_2''}\right)\left(\frac{v'}{v_2''}\right)\left(\frac{v'}{A_{34}''}\right)\left(\frac{A_{24}'}{A_{34}''}\right).$$

Now since $v_1'' \mid A_{24}$, $A_{12}A_{34}'' \equiv vA_{14}''^2 \bmod v_1''$ so bearing in mind that $v_1v_1''v'$ is a square,

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

$$\left(\frac{v'}{A''_{34}}\right) = \left(\frac{A''_{34}}{v_1}\right)\left(\frac{A''_{34}A_{12}}{v''_1}\right)\left(\frac{A_{12}}{v''_1}\right) = \left(\frac{A''_{34}}{v_1}\right)\left(\frac{v}{v''_1}\right)\left(\frac{A_{12}}{v''_1}\right).$$

Thus by Proposition 3.1

$$\kappa(\gamma'\gamma) = \kappa(\gamma')\left(\frac{v''}{v'_1}\right)\left(\frac{v'}{v''_2}\right)\left(\frac{v}{v''_1}\right).$$

Now

$$\left(\frac{v''}{v_1}\right)\left(\frac{v'}{v''_2}\right)\left(\frac{v}{v''_1}\right) = \left(\frac{v_1}{v''_1}\right)\left(\frac{v_1}{v''_2}\right)\left(\frac{v'_1}{v''_2}\right)\left(\frac{v'_2}{v''_2}\right)\left(\frac{v_1}{v''_1}\right)\left(\frac{v''_1}{v''_2}\right) = 1$$

since $v_1v'_1v''_1v'_2$ is a square. Thus $\kappa(\gamma'\gamma) = \kappa(\gamma')$, proving that $\gamma \in \hat{\Gamma}_1$.

Now let us prove more precisely that $\gamma \in \hat{\Gamma}_0$. If $\gamma' \in \hat{\Gamma}$ is no longer assumed to be such that $\gamma'\gamma \in \Sigma$, nevertheless by Proposition 3.12 there exists $\gamma'' \in U(M)$ such that $\gamma'\gamma\gamma'' \in \Sigma$. Now by Lemma 3.13, $\kappa(\gamma'\gamma) = \kappa(\gamma'\gamma\gamma'')$ $= \kappa(\gamma'(\gamma\gamma''\gamma^{-1})\gamma)$ and since $\gamma \in \hat{\Gamma}_1$, this equals $\kappa(\gamma'(\gamma\gamma''\gamma^{-1}))$. Now $\gamma\gamma''\gamma^{-1} \in U(M)$, so by Lemma 3.13 again this equals $\kappa(\gamma')$. This proves that $\gamma \in \hat{\Gamma}_0$.

LEMMA 3.15. *If $t, u, r \in M$ then*

$$\gamma = \begin{pmatrix} 1 & & & \\ & 1 & & \\ u & t & 1 & \\ r & u & & 1 \end{pmatrix} \in \hat{\Gamma}_0.$$

Proof. Let $\gamma' \in \hat{\Gamma}$ have invariants A_{ij}. Then $\gamma'\gamma$ has invariants B_{ij} where $B_{12} = A_{12} + tA_{13} - rA_{24} + (u^2 - tr)A_{34} + 2uA_{14}$, $B_{13} = A_{13} - rA_{34}$, $B_{24} = A_{24} + tA_{34}$, $B_{14} = A_{14} + uA_{34}$, $B_{34} = A_{34}$. In Proposition 3.1, the factors v, v_1, v''_2, v'' and v_1 are unchanged from the A_{ij} to the B_{ij}, which makes the comparison of $\kappa(\gamma')$ and $\kappa(\gamma'\gamma)$ simple. Since $v''_1 \mid A_{13}, A_{24}, A_{34}, A_{14}$, we have $A_{12} \equiv B_{12} \bmod v''_1$ and so

$$\left(\frac{B_{12}}{v''_1}\right) = \left(\frac{A_{12}}{v''_1}\right).$$

As $v''_2 \mid A_{34}$, $\gcd(v''_2, b') = 1$, so $B'_{24} \equiv A'_{24} \bmod v''_2$ and so

$$\left(\frac{B'_{24}}{v''_2}\right) = \left(\frac{A'_{24}}{v''_2}\right).$$

Let us show that $v_1 \mid b'$. Since v_1 is squarefree, it is sufficient to show that each prime p dividing v_1 divides b'. If $p \mid v'$, then clearly $p \mid b'$. On the other hand, if $p \nmid v'$, since $v_1v''_1v'$ is a square, $p \mid v''_1$. Now $p \mid v_1, v''_1$ so

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

$p \mid A_{34}$, A_{24}, A_{13} so by (2.3) $p \nmid A_{12}$. Also by (3.2), $p \nmid A''_{34}$. As $p \mid v$, $A'_{13}A'_{24} \equiv A_{12}A''_{34} \bmod p$, so $p \nmid A'_{24}$. Now $p \mid A_{24}$, $p \nmid A'_{24}$, so $p \mid b'$ in this case also. Thus $v_1 \mid b'$. Now $B'_{13} = A_{13} - rb'A''_{34}$ and so $B'_{13} \equiv A'_{13} \bmod v_1$. Thus

$$\left(\frac{B'_{13}}{v_1}\right) = \left(\frac{A'_{13}}{v_1}\right).$$

Clearly

$$\left(\frac{A''_{34}}{v_1}\right) = \left(\frac{B''_{34}}{v_1}\right), \qquad \left(\frac{A'_{24}}{A''_{34}}\right) = \left(\frac{B'_{24}}{B''_{34}}\right)$$

and so each symbol in (3.3) equals the corresponding symbol in the corresponding formula for $\kappa(\gamma'\gamma)$. Thus $\kappa(\gamma'\gamma) = \kappa(\gamma')$ and so $\gamma \in \hat{\Gamma}_0$.

The following lemma contains the heart of the proof.

LEMMA 3.16. *If* $p, q, r, s \in \mathcal{O}$, $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod M$, $ps - qr = 1$, *then*

$$\gamma = \begin{pmatrix} 1 & & & \\ & p & q & \\ & r & s & \\ & & & 1 \end{pmatrix} \in \hat{\Gamma}_0.$$

Proof. First let us show that $\gamma \in \hat{\Gamma}_1$. Let $\gamma' \in \hat{\Gamma}$, $\gamma'\gamma \in \Sigma$. Let $\gamma', \gamma'\gamma$ have invariants A_{ij}, B_{ij} respectively. We have $B_{24} = pA_{24} + rA_{34}$, $B_{34} = qA_{24} + sA_{34}$. Our hypothesis that $\gcd(B_{24}, B_{34}) = 1$ implies that $\gcd(A_{24}, A_{34}) = 1$, and so $\gamma' \in \Sigma$. Now

$$\kappa(\gamma') = \left(\frac{A_{24}}{A_{34}}\right), \qquad \kappa(\gamma) = \left(\frac{r}{s}\right), \qquad \kappa(\gamma'\gamma) = \left(\frac{B_{24}}{B_{34}}\right)$$

so what we must prove is that

$$\left(\frac{B_{24}}{B_{34}}\right) = \left(\frac{r}{s}\right)\left(\frac{A_{24}}{A_{34}}\right). \tag{3.14}$$

Let d be the primitive generator of the ideal $\gcd(s, B_{34})$. Let $s = ds'$, $B_{34} = dB'_{34}$. Note that d, s', B'_{34} are all primitive. Since $A_{24} = sB_{24} - rA_{34}$, $d \mid A_{24}$. Let $A_{24} = dA'_{24}$. Now

$$B_{24} \equiv rA_{34} \quad \bmod A_{24} \tag{3.15}$$

$$B'_{34} \equiv s'A_{34} \quad \bmod \lambda^3 A'_{24} \tag{3.16}$$

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

$$A'_{24} = s'B_{24} - rB'_{34}\,. \tag{3.17}$$

Now

$$\left(\frac{B_{24}}{B_{34}}\right) = \left(\frac{s'}{B'_{34}}\right)\left(\frac{s'B_{24}}{B'_{34}}\right)\left(\frac{B_{24}}{d}\right).$$

Using (3.17) and (3.15) to rewrite the second and third symbols on the right, this equals

$$\left(\frac{s'}{B'_{34}}\right)\left(\frac{A'_{34}}{B'_{34}}\right)\left(\frac{r}{d}\right)\left(\frac{A_{34}}{d}\right).$$

Now observe that $\lambda^3 \mid A'_{34}$. Thus by Proposition 2.1 (i) we may use (3.16) to evaluate the second symbol and obtain

$$\left(\frac{s'}{B'_{34}}\right)\left(\frac{A'_{24}}{s'}\right)\left(\frac{A'_{24}}{A_{34}}\right)\left(\frac{r}{d}\right)\left(\frac{A_{34}}{d}\right) = \left(\frac{s'}{B'_{34}}\right)\left(\frac{r}{s'}\right)\left(\frac{B'_{34}}{s'}\right)\left(\frac{A'_{24}}{A_{34}}\right)\left(\frac{r}{d}\right)\left(\frac{A_{34}}{d}\right),$$

where we have used (3.17) again. Now using the quadratic reciprocity law (Proposition 2.1 (g)) to invert the third and last symbols on the right, we obtain (3.14). This proves that $\gamma \in \hat{\Gamma}_1$.

To deduce from this that $\gamma \in \hat{\Gamma}_0$, let $\gamma' \in \hat{\Gamma}$. We are no longer assuming that $\gamma' \in \Sigma$. Now there exists, by Proposition 3.12, a $\gamma_1 \in U(M)$ such that $\gamma'\gamma\gamma_1 \in \Sigma$. Now we may write $\gamma\gamma_1 = \gamma_2\gamma_3$, where $\gamma_2 \in \hat{\Gamma}_0$, $\gamma_3 \in \hat{\Gamma}_1$, $\kappa(\gamma_2) = 1$ and $\kappa(\gamma_3) = \kappa(\gamma)$. Indeed, if

$$\gamma_1 = \begin{pmatrix} 1 & & b & c \\ & 1 & a & b \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

let

$$\gamma_2 = \begin{pmatrix} 1 & -rb & pb & c \\ & 1 & & pb \\ & & 1 & rb \\ & & & 1 \end{pmatrix}, \qquad \gamma_3 = \begin{pmatrix} 1 & & & \\ & p & q + ap & \\ & r & s + ar & \\ & & & 1 \end{pmatrix}.$$

It follows from Lemmas 3.13 and 3.14 that $\gamma_2 \in \hat{\Gamma}_0$, and clearly $\kappa(\gamma_2) = 1$. It has just been established that $\gamma_3 \in \hat{\Gamma}_1$, and by Proposition 2.1 (i) we have

$$\kappa(\gamma_3) = \left(\frac{r}{s + ar}\right) = \left(\frac{r}{s}\right) = \kappa(\gamma)\,.$$

https://doi.org/10.1017/S0027763000003184 Published online by Cambridge University Press

Now $\kappa(\gamma'\gamma) = \kappa(\gamma'\gamma\gamma_1) = \kappa(\gamma'\gamma_2\gamma_3) = \kappa(\gamma'\gamma_2)\kappa(\gamma_3)$ since $\gamma'\gamma_2\gamma_3 \in \Sigma$ and $\gamma_3 \in \hat{\Gamma}_1$. This equals $\kappa(\gamma')\kappa(\gamma)$, where $\gamma \in \hat{\Gamma}_0$.

The proof of Theorem 3.7 (and hence Theorem 1.1) is now nearly complete. It is easily checked that the matrices in Lemmas 3.13, 3.14, 3.15 and 3.16 generate $\hat{\Gamma}$. Thus the group $\hat{\Gamma}_0$ equals $\hat{\Gamma}$; since κ is a character on $\hat{\Gamma}_0$ it is a character on $\hat{\Gamma}$.

References

[1] H. Bass, J. Milnor and J.-P. Serre, Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)., Publ. Math. IHES, **33** (1967), 59–137.

[2] D. Bump, S. Friedberg and J. Hoffstein, Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives, Ann. of Math., **131** (1990), 53–127.

[3] D. Johnson and J. Millson, Modular Lagrangians and the theta multiplier, Preprint (1988).

[4] H. Stark, On the transformation formula for the symplectic theta function and applications, J. Fac. Sci. Univ. Tokyo, **29** (1982), 1–12.

[5] R. Styer, Prime determinant matrices and the symplectic theta function, Amer. J. Math., **106** (1984), 645–664.

D. Bump
Department of Mathematics
Stanford University
Stanford, CA 94305, U.S.A.

S. Friedberg
Department of Mathematics
The University of California at Santa Cruz
Santa Cruz, CA 95064, U.S.A.

J. Hoffstein
Department of Mathematics
Brown University
Providence, RI 02912, U.S.A.