Metaplectic Eisenstein Series on GL(3)

Ben Brubaker, Daniel Bump, Solomon Friedberg and Jeffrey Hoffstein

February 14, 2008

This is a companion piece to [2], to be published on the World Wide Web. It consists of two articles.

- The first article, on the Kubota symbol, gives a construction from scratch for the Kubota symbol of degree n on GL(3).
- The second article is a longer version of Section 1 of [2], containing proofs that were shortened for publication.

This work was supported by NSF FRG Grants DMS-0354662, DMS-0353964 and DMS-0354534.

1 The Kubota Symbol

Let F be a global field with ring $\mathfrak{o}$ of integers, and let μ_n denote the group of n-th roots of unity in F. Let $\Gamma(\mathfrak{f})$ be the principal congruence subgroup of $\mathrm{SL}_3(\mathfrak{o})$ consisting of elements that are congruent to the identity modulo $\mathfrak{f}$. The *Kubota symbol* $\kappa : \Gamma(\mathfrak{f}) \longrightarrow \mu_n$ is a character constructed by Bass, Milnor and Serre [1].

We will give a direct construction, obtaining on the way new formulas for the map. We will handle two cases simultaneously.
Case 1: $n = 2$, $F = \mathbb{Q}(i)$, $\mathfrak{o} = \mathbb{Z}[i]$, $\lambda = 1 + i$ and $\mathfrak{f} = \lambda^3\mathfrak{o}$.
Case 2: $n = 3$, $F = \mathbb{Q}(\rho)$ where $\rho = e^{2\pi i/3}$, $\mathfrak{o} = \mathbb{Z}[\rho]$, $\lambda = 1 - \rho$, and $\mathfrak{f} = \lambda^2\mathfrak{o} = 3\mathfrak{o}$.
For these two fields the particular level $\mathfrak{f}$ may be new.

Although we specialize to these particular fields, our formulas should be correct (for some level, with perhaps some other minor modifications) when $n > 1$ is arbitrary, assuming that F is a totally complex field containing the n-th roots of unity such that -1 is an n-th power in F. We specialize to these particular cases since it is convenient that the class number is 1 and the level $\mathfrak{f}$ can be chosen so that the map $\mathfrak{o}^\times \longrightarrow (\mathfrak{o}/\mathfrak{f})^\times$ is surjective.

If c and d are in $\mathfrak{o}$ and $\gcd(d, \mathfrak{f}) = 1$ the *power residue symbol* $\left(\frac{c}{d}\right)$ is defined as follows. First, if c and d are *not* coprime then $\left(\frac{c}{d}\right) = 0$. If $d = p$ is prime, then $\left(\frac{c}{d}\right)$ is the unique n-th root of unity such that

$$c^{(\mathbb{N}p-1)/n} \equiv \left(\frac{c}{p}\right) \bmod p.$$

Finally, if d is not prime, we factor $d = \varepsilon \prod p_i^{k_1}$ where ε is a unit and the p_i are prime, and define $\left(\frac{c}{d}\right) = \prod \left(\frac{c}{p_i}\right)^{k_i}$. Our convention is that $\left(\frac{0}{1}\right) = 1$.

Lemma 1 *If $\lambda \nmid d$ then there exists a unique unit $\varepsilon \in \mathfrak{o}^\times$ such that $\varepsilon\lambda \equiv 1$ modulo $\mathfrak{f}$.*

We will use this fact frequently and without comment.

Proposition 1 *The power residue symbol has the following properties.*
(i) If $\varepsilon \in \mathfrak{o}^\times$ then $\left(\frac{c}{\varepsilon d}\right) = \left(\frac{c}{d}\right)$.
(ii) If $c \equiv c'$ modulo d then $\left(\frac{c}{d}\right) = \left(\frac{c'}{d}\right)$.
(iii) We have $\left(\frac{cc'}{d}\right) = \left(\frac{c}{d}\right)\left(\frac{c'}{d}\right)$.
(iv) We have $\left(\frac{c}{dd'}\right) = \left(\frac{c}{d}\right)\left(\frac{c}{d'}\right)$.
(v) If p is prime (and prime to n) then $\left(\frac{b}{p}\right) = 1$ if and only if b is an n-th power residue modulo p.
(vi) We have $\left(\frac{-1}{d}\right) = 1$.

Proposition 2 (Reciprocity law) *If $c, d \equiv \pm 1$ modulo $\mathfrak{f}$, then*

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

Proposition 3 *(i) Assume that $n = 3$ and $F = \mathbb{Z}[\rho]$. If $d = 1 + 3(m + n\rho)$ then*

$$\left(\frac{\rho}{d}\right) = \rho^{-m-n}, \qquad \left(\frac{\lambda}{d}\right) = \rho^{m}$$

(ii) Assume that $n = 2$ and $F = \mathbb{Z}[i]$. If $d = a + bi \equiv 1$ modulo $\mathfrak{f}$ then

$$\left(\frac{i}{d}\right) = (-1)^{(a-1)/2}, \qquad \left(\frac{\lambda}{d}\right) = (-1)^{(a-3b-1)/4}.$$

Proof These three propositions can all be deduced easily from the discussion of the cubic symbol and its properties in Ireland and Rosen [4]. For the quadratic symbol, one may use results found there for the quartic residue symbol, remembering that the quadratic symbol is the square of the quartic residue symbol. $\square$

Proposition 4 *Suppose that $\lambda \nmid d, d'$ and that $\gcd(c, d) = \gcd(c, d') = 1$. Assume that one of the following three cases applies:*
(i) $d \equiv d'$ modulo $\mathfrak{f}^2$ and $d \equiv d'$ modulo c;
(ii) $d \equiv d'$ modulo $\mathfrak{f}\lambda$, $d \equiv d'$ modulo c and $\gcd(c, \lambda) = 1$;
(iii) c is of the form $\theta\lambda^b$ where θ is a unit and $d \equiv d'$ modulo $\mathfrak{f}^2$.
Then

$$\left(\frac{c}{d}\right) = \left(\frac{c}{d'}\right).$$

Proof Let us write $d = \varepsilon d_0$ and $d' = \varepsilon' d_0'$ where $\varepsilon, \varepsilon'$ are units and $d_0 \equiv d_0' \equiv 1$ modulo $\mathfrak{f}$. We note that since $d \equiv d'$ modulo $\mathfrak{f}$ in each of the 3 cases we have $\varepsilon \equiv \varepsilon'$ modulo $\mathfrak{f}$ which implies that $\varepsilon = \varepsilon'$. Therefore $d_0 \equiv d_0'$ for any modulus such that $d \equiv d'$. Furthermore, $\left(\frac{c}{d}\right) = \left(\frac{c}{d_0}\right)$ and $\left(\frac{c}{d'}\right) = \left(\frac{c}{d_0'}\right)$.

As a result of these observations we may replace d and d' by d_0 and d'_0. In other words, there is no harm in assuming that $d \equiv d'$ modulo $\mathfrak{f}$ and we will assume this.

Let us write $c = c_0\,\theta\,\lambda^u$ where θ is a unit and $c_0 \equiv 1$ modulo $\mathfrak{f}$. Then by the reciprocity law

$$\left(\frac{c}{d}\right) = \left(\frac{\theta\lambda^u}{d}\right)\left(\frac{d}{c_0}\right).$$

In each of the three cases we have $d \equiv d'$ modulo c_0 and so $\left(\frac{d}{c_0}\right) = \left(\frac{d'}{c_0}\right)$. Thus we have only to show that

$$\left(\frac{\theta\lambda^u}{d}\right) = \left(\frac{\theta\lambda^u}{d'}\right).$$

This is true if $d \equiv d'$ modulo $\mathfrak{f}^2$ by Proposition 3, which settles cases (i) and (iii). In case (ii), we have $u = 0$, and the statement follows again from Proposition 3.

□

Let

$$w = \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix}. \tag{1}$$

Then $G = \mathrm{SL}_3$ has an involution defined by

$$^{\iota}g = w \cdot {}^{t}g^{-1} \cdot w.$$

It preserves the group $\Gamma(\mathfrak{f})$ and its subgroup $\Gamma_\infty(\mathfrak{f})$, consisting of the upper triangular matrices in $\Gamma(\mathfrak{f})$. If $g \in \Gamma(\mathfrak{f})$, let $[A_1, B_1, C_1]$ and $[A_2, B_2, C_2]$ be the bottom rows of g and ${}^{\iota}g$, respectively. Then

$$\begin{gathered} (A_1, B_1, C_1) \equiv (A_2, B_2, C_2) \equiv (0, 0, 1) \mod \mathfrak{f}, \\ A_1 C_2 + B_1 B_2 + C_1 A_2 = 0, \\ \gcd(A_1, B_1, C_1) = \gcd(A_2, B_2, C_2) = 1. \end{gathered} \tag{2}$$

We call $A_1, B_1, C_1, A_2, B_2, C_2$ the *invariants* of g. We will refer to (2) as the *Plücker relation*. The invariants depend only on the orbit of g in $\Gamma_\infty(\mathfrak{f})\backslash\Gamma(\mathfrak{f})$.

Proposition 5 *If* $\gcd(A_1, B_1, C_1) = \gcd(A_2, B_2, C_2) = 1$ *and the Plücker relation (2) is satisfied, then we may factor*

$$\begin{aligned} A_1 &= p_1 p_2 q_1 a_1, & A_2 &= q_1 q_2 p_2 a_2, \\ B_1 &= q_1 q_2 r_1 b_1, & B_2 &= p_1 p_2 r_2 b_2, \\ C_1 &= r_1 r_2 p_1 c_1, & C_2 &= r_1 r_2 q_2 c_2, \end{aligned}$$

where

$$\begin{aligned} &\gcd(a_1, b_1) = \gcd(a_1, c_1) = \gcd(a_1, a_2) = \gcd(a_1, b_2) = \gcd(b_1, c_1) = \gcd(b_1, a_2) \\ &= \gcd(b_1, c_2) = \gcd(c_1, b_2) = \gcd(c_1, c_2) = \gcd(a_2, b_2) = \gcd(a_2, c_2) = \gcd(b_2, c_2) \\ &= \gcd(p_1, q_1) = \gcd(p_1, q_2) = \gcd(p_1, r_1) = \gcd(q_2, p_2) = \gcd(q_2, r_2) = \gcd(r_1, p_2) \\ &= \gcd(b_2, q_2) = \gcd(c_1, q_1) = \gcd(c_2, p_2) = 1. \end{aligned}$$

Proof Let Ω be the set of ordered triples (P,Q,R) such that $P|(A_1,B_2)$, $Q|(B_1,A_2)$ and $R|(C_1,C_2)$ and $PQR|\gcd(A_1C_2,B_1B_2,C_1A_2)$. Define a partial order on Ω by $(P,Q,R)\leqslant(P',Q',R')$ if $P|P'$, $Q|Q'$ and $R|R'$. Let (P,Q,R) be a maximal element of Ω, and write $A_1=PA_1'$, $B_1=QB_2'$, $C_1=RC_1'$, $A_2=QA_2'$, $B_2=PB_2'$, $C_2=RC_2'$. Since $PQR|B_1B_2$, we have $R|B_1'B_2'$, so we may factor $R=r_1r_2$ with $r_1|B_1'$ and $r_2|B_2'$; let $B_1'=r_1b_1$ and $B_2'=r_2b_2$. Similarly $P=p_1p_2$ where $C_1'=p_1c_1$ and $A_2'=p_2a_2$, and $Q=q_1q_2$ where $A_1'=q_1a_1$ and $C_2'=q_2c_2$. The maximality of Ω, together with $\gcd(A_1,B_1,C_1)=\gcd(A_2,B_2,C_2)=1$, implies the coprimality conditions of the theorem. $\square$

Proposition 6 *Suppose in the context of Proposition 5 that $A_1\equiv B_1\equiv A_2\equiv B_2\equiv 0$ and $C_1\equiv C_2\equiv 1$ modulo $\mathfrak{f}$. Then we may choose the factorizations so that $r_1\equiv r_2\equiv p_1\equiv q_2\equiv c_1\equiv c_2\equiv 1$ modulo $\mathfrak{f}$ and so that one of the following three cases applies:*

(i) $\mathfrak{f}|b_1$, $\lambda^2|b_2$, $\mathfrak{f}^2|b_1b_2$, $a_1\equiv 1$ and $a_2\equiv -1$ modulo $\mathfrak{f}$;

(ii) $b_1\equiv a_2\equiv 1$ modulo $\mathfrak{f}$ and $\mathfrak{f}|p_2a_1$; or

(iii) $b_2\equiv a_1\equiv 1$ modulo $\mathfrak{f}$ and $\mathfrak{f}|q_1a_2$. We have

$$\left(\frac{b_1}{c_1}\right)\left(\frac{b_2}{c_2}\right)\left(\frac{c_1}{c_2}\right)^{-1}=\begin{cases}\left(\frac{a_1}{c_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{b_2}{a_1}\right)^{-1}=\left(\frac{b_1}{a_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{a_1}{a_2}\right)^{-1} & \textit{in case (i);}\\ \left(\frac{b_1}{c_1}\right)\left(\frac{a_2}{c_2}\right)\left(\frac{b_1}{c_2}\right)^{-1}=\left(\frac{a_1}{b_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{a_1}{a_2}\right)^{-1} & \textit{in case (ii);}\\ \left(\frac{b_2}{c_2}\right)\left(\frac{a_1}{c_1}\right)\left(\frac{b_2}{c_1}\right)^{-1}=\left(\frac{b_1}{a_1}\right)\left(\frac{a_2}{b_2}\right)\left(\frac{a_2}{a_1}\right)^{-1} & \textit{in case (iii).}\end{cases}$$

Proof We first note that it is sufficient to obtain a decomposition in which one of the following is true:

(i') $\mathfrak{f}|b_1$, $\lambda|b_2$, $\mathfrak{f}^2|b_1b_2$, and $\lambda\nmid a_1,a_2$;

(ii') $\lambda\nmid b_1,a_2$ and $\mathfrak{f}|p_2a_1$; or

(iii') $\lambda\nmid b_2,a_1$ and $\mathfrak{f}|q_1a_2$.

Indeed, since $C_1\equiv C_2\equiv 1$ modulo $\mathfrak{f}$, in any decomposition as in Proposition 5 we have automatically that $\lambda\nmid r_1,r_2,p_1,q_2,c_1,c_2$. Now we make use of the fact that if $\lambda\nmid c$ then there exists a unit ε such that $\varepsilon c\equiv 1$ modulo $\mathfrak{f}$ to see that we may adjust r_1,r_2,p_1,q_2,c_1,c_2 by units so that $r_1\equiv r_2\equiv p_1\equiv q_2\equiv 1$ modulo $\mathfrak{f}$, and it follows that $c_1\equiv c_2\equiv 1$ also. There are compensating adjustments, of course, to a_1,a_2,b_1,b_2 but these will be adjusted again. If (i') is satisfied, we may then adjust a_1 and by a unit, with compensating changes to q_1, a_2 and b_2, so that $a_1\equiv 1$ modulo $\mathfrak{f}$. Then, since $a_1c_2+a_2c_1\equiv a_1c_2+b_1b_2+c_1a_2=0$ modulo $\mathfrak{f}$, it follows that $a_2\equiv -1$ modulo $\mathfrak{f}$. The cases (ii') and (iii') are handled similarly.

To establish (i'), (ii') or (iii'), let us denote $\alpha_i=\mathrm{ord}_\lambda(A_i)$ and $\beta_i=\mathrm{ord}_\lambda(B_i)$. Let $r=\mathrm{ord}_\lambda(\mathfrak{f})$; thus $r=2$ if $n=3$ and $r=3$ if $n=2$. Since $\mathfrak{f}|A_1,A_2,B_1,B_2$ we have $\alpha_i\geqslant r$ and $\beta_i\geqslant r$.

Suppose that $\alpha_1>\alpha_2$. Then $\alpha_1=\mathrm{ord}_\lambda(A_1C_2)>\alpha_2=\mathrm{ord}_\lambda(A_2C_1)$

$$\beta_1+\beta_2=\mathrm{ord}_\lambda(-A_1C_2-A_2C_1)=\alpha_2.$$

Now, with Ω as in the proof of Proposition 5, we have $(\lambda^{\beta_2},\lambda^{\beta_1},1)\in\Omega$, and we choose maximal $(P,Q,R)\geqslant(\lambda^{\beta_2},\lambda^{\beta_1},1)$. Then $\lambda^{\beta_2}|p_1p_2$ and since $\lambda\nmid p_1$, we have $\lambda^{\beta_2}|p_2$; similarly $\lambda^{\beta_1}|q_1$. Now a_2 and b_1 are both prime to λ and $\mathfrak{f}|p_2$ so $\mathfrak{f}|p_2a_1$ so we are in case (ii').

The case $\alpha_2>\alpha_1$ similarly leads to case (iii').

We are left with the case where $\alpha_1=\alpha_2$ and β_1 and β_2 are both $\geqslant\alpha_1+1$. Let us write $\alpha_1=2a+\varepsilon$, where $\varepsilon=0$ or 1 and $a>0$. It is easy to see that $a+\varepsilon\geqslant r-1$. Then $(\lambda^{a+\varepsilon},\lambda^a,1)\in\Omega$.

Choosing $(P,Q,R) \geqslant (\lambda^{a+\varepsilon}, \lambda^a, 1)$ we have $\lambda^{a+\varepsilon}|p_2$ and $\lambda^a|q_1$. In fact we have $\lambda^{a+\varepsilon}\|p_2$ and $\lambda^a\|q_1$ since if any larger power of λ than $\lambda^{a+\varepsilon}$ were to divide p_2 then a larger power than $\alpha_1 = 2a+\varepsilon$ would divide $A_1 = p_1p_2q_1a_2$, which is a contradiction; and similarly with q_1. Now it is clear that a_1 and a_2 are both not divisible by λ. Now, since $\lambda \nmid r_1, r_2, p_1, q_2$ (because $\lambda \nmid C_1, C_2$) we have $\lambda^{\beta_1 - a}|b_1$ and $\lambda^{\beta_2-a-\varepsilon}|b_2$. Since $\beta_1 - a \geqslant a+\varepsilon+1 \geqslant r$ and $\beta_2 - a - \varepsilon \geqslant a+1 \geqslant 2$ we have $\mathfrak{f}|b_1$, $\lambda^2|b_2$, $\mathfrak{f}^2|b_1b_2$ and $\lambda \nmid a_1, a_2$. Thus we are in case (i').

It remains to prove the identities for $\left(\frac{b_1}{c_1}\right)\left(\frac{b_2}{c_2}\right)\left(\frac{c_1}{c_2}\right)^{-1}$. Let us tackle case (i) first. Since $a_1c_2 + b_1b_2 + c_1a_2 = 0$ we have

$$\begin{aligned}
\left(\frac{b_1}{c_1}\right)\left(\frac{b_2}{c_2}\right)\left(\frac{c_1}{c_2}\right)^{-1} &= [\text{reciprocity, } c_1 \equiv c_2 \equiv 1 \bmod \mathfrak{f}]\\
\left(\frac{b_1}{c_1}\right)\left(\frac{b_2}{a_1c_2}\right)\left(\frac{c_2}{c_1}\right)^{-1}\left(\frac{b_2}{a_1}\right)^{-1} &= [\text{Prop. 5 (i), } a_1c_2 \equiv -a_2c_1 \bmod b_2 \text{ and } \mathfrak{f}^2]\\
\left(\frac{b_1}{c_1}\right)\left(\frac{b_2}{a_2c_1}\right)\left(\frac{c_2}{c_1}\right)^{-1}\left(\frac{b_2}{a_1}\right)^{-1} &= [\text{multiplicativity}]\\
\left(\frac{b_1b_2}{c_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{c_2}{c_1}\right)^{-1}\left(\frac{b_2}{a_1}\right)^{-1} &= [a_1c_2 \equiv -b_1b_2 \text{ modulo } c_1]\\
\left(\frac{a_1c_2}{c_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{c_2}{c_1}\right)^{-1}\left(\frac{b_2}{a_1}\right)^{-1} &= [\text{multiplicativity}]\\
\left(\frac{a_1}{c_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{b_2}{a_1}\right)^{-1} &= [\text{multiplicativity}]\\
\left(\frac{a_1}{c_1a_2}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{b_2}{a_1}\right)^{-1}\left(\frac{a_1}{a_2}\right)^{-1} &= [\text{reciprocity, } a_1 \equiv c_1a_2 \equiv 1 \bmod \mathfrak{f}]\\
\left(\frac{c_1a_2}{a_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{b_2}{a_1}\right)^{-1}\left(\frac{a_1}{a_2}\right)^{-1} &= [c_1a_2 \equiv -b_1b_2 \bmod a_1]\\
\left(\frac{b_1b_2}{a_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{b_2}{a_1}\right)^{-1}\left(\frac{a_1}{a_2}\right)^{-1} &= \left(\frac{b_1}{a_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{a_1}{a_2}\right)^{-1}.
\end{aligned}$$

Next let us consider case (ii). We have $c_1 \equiv c_2 \equiv b_1 \equiv a_2 \equiv 1$ modulo $\mathfrak{f}$, and we have

$$\begin{array}{rcl}
\left(\frac{b_1}{c_1}\right)\left(\frac{b_2}{c_2}\right)\left(\frac{c_1}{c_2}\right)^{-1} & = & \text{[multiplicativity]} \\
\left(\frac{b_1}{c_1}\right)\left(\frac{b_1 b_2}{c_2}\right)\left(\frac{c_1}{c_2}\right)^{-1}\left(\frac{b_1}{c_2}\right)^{-1} & = & [b_1 b_2 \equiv -a_2 c_1 \text{ modulo } c_2] \\
\left(\frac{b_1}{c_1}\right)\left(\frac{a_2 c_1}{c_2}\right)\left(\frac{c_1}{c_2}\right)^{-1}\left(\frac{b_1}{c_2}\right)^{-1} & = & \text{[multiplicativity]} \\
\left(\frac{b_1}{c_1}\right)\left(\frac{a_2}{c_2}\right)\left(\frac{b_1}{c_2}\right)^{-1} & = & \text{[reciprocity, multiplicativity]} \\
\left(\frac{a_2 c_1}{b_1}\right)\left(\frac{a_2}{c_2}\right)\left(\frac{b_1}{c_2}\right)^{-1}\left(\frac{a_2}{b_1}\right)^{-1} & = & [a_2 c_1 \equiv a_1 c_2 \text{ modulo } b_1, \text{ reciprocity}] \\
\left(\frac{a_1 c_2}{b_1}\right)\left(\frac{a_2}{c_2}\right)\left(\frac{c_2}{b_1}\right)^{-1}\left(\frac{a_2}{b_1}\right)^{-1} & = & \text{[reciprocity, multiplicativity]} \\
\left(\frac{a_1}{b_1}\right)\left(\frac{c_2}{a_2}\right)\left(\frac{a_2}{b_1}\right)^{-1} & = & \text{[reciprocity, multiplicativity]} \\
\left(\frac{a_1}{b_1}\right)\left(\frac{a_1 c_2}{a_2}\right)\left(\frac{a_2}{b_1}\right)^{-1}\left(\frac{a_1}{a_2}\right)^{-1} & = & [a_1 c_2 \equiv b_1 b_2 \bmod a_2] \\
\left(\frac{a_1}{b_1}\right)\left(\frac{b_1 b_2}{a_2}\right)\left(\frac{b_1}{a_2}\right)^{-1}\left(\frac{a_1}{a_2}\right)^{-1} & = & \left(\frac{a_1}{b_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{a_1}{a_2}\right)^{-1}.
\end{array}$$

Case (iii) is similar to (ii). □

Proposition 7 *Suppose that* $\gcd(A_1, B_1, C_1) = \gcd(A_2, B_2, C_2) = 1$, $A_1C_2 + B_1B_2 + C_1A_2 = 0$ *and* $(A_1, B_1, C_1) \equiv (A_2, B_2, C_2) \equiv (0, 0, 1)$ *modulo* $\mathfrak{f}$. *Assume further that* $\gcd(C_1, C_2) = 1$. *Then also* $\gcd(B_1, C_1) = \gcd(B_2, C_2) = 1$. *There exist factorizations*

$$\begin{array}{rr} A_1 = p_2 q_1 A_1', & A_2 = p_2 q_1 A_2', \\ B_1 = q_1 B_1' & B_2 = p_2 B_2', \end{array}$$

where $p_2 q_1 = \gcd(A_1, A_2)$. *We have*

$$\gcd(B_1', A_1') = \gcd(B_2', A_2') = \gcd(A_1', A_2') = \gcd(q_1, C_1) = \gcd(p_2, C_2) = 1 \tag{3}$$

and we may assume that one of the three following cases applies:
(i) $\mathfrak{f}|B_1'$, $\lambda^2|B_2'$, $\mathfrak{f}^2|B_1'B_2'$ *and* $A_1' \equiv -A_2' \equiv 1$ *modulo* $\mathfrak{f}$;
(ii) $B_1' \equiv A_2' \equiv 1$ *modulo* $\mathfrak{f}$ *and* $\mathfrak{f}|p_2 A_1'$; *or*
(iii) $B_2' \equiv A_1' \equiv 1$ *modulo* $\mathfrak{f}$ *and* $\mathfrak{f}|q_1 A_2'$.
We have

$$\left(\frac{B_1}{C_1}\right)\left(\frac{B_2}{C_2}\right)\left(\frac{C_1}{C_2}\right)^{-1} = \begin{cases} \left(\frac{B_1'}{A_1'}\right)\left(\frac{B_2'}{A_2'}\right)\left(\frac{A_1'}{A_2'}\right)^{-1}\left(\frac{q_1}{C_1}\right)\left(\frac{p_2}{C_2}\right) & \text{in case (i);} \\ \left(\frac{A_1'}{B_1'}\right)\left(\frac{B_2'}{A_2'}\right)\left(\frac{A_1'}{A_2'}\right)^{-1}\left(\frac{q_1}{C_1}\right)\left(\frac{p_2}{C_2}\right) & \text{in case (ii);} \\ \left(\frac{B_1'}{A_1'}\right)\left(\frac{A_2'}{B_2'}\right)\left(\frac{A_2'}{A_1'}\right)^{-1}\left(\frac{q_1}{C_1}\right)\left(\frac{p_2}{C_2}\right) & \text{in case (iii).} \end{cases} \tag{4}$$

The assumption that $\gcd(C_1, C_2) = 1$ will be removed in Proposition 10.

Proof The coprimality of B_1 and C_1 follows from the coprimality of C_1 and C_2 since any common prime divisor of B_1 and C_1 divides $-A_1C_2 = B_1B_2 + C_1A_2$, and it cannot divide A_1 since $\gcd(A_1, B_1, C_1) = 1$.

The existence of the a factorization follows from the factorization in Proposition 6 with $A_1' = p_1a_1$, $A_2' = q_2a_2$, $B_1' = q_2b_1$ and $B_2' = p_1b_2$. (We note that every such factorization may be obtained this way.) Since C_1 and C_2 are coprime, we have $r_1 = r_2 = 1$ so $C_1 = p_1c_1$ and $C_2 = q_2c_2$. Using the multiplicativity of the symbol and the reciprocity law, we have

$$\left(\frac{B_1}{C_1}\right)\left(\frac{B_2}{C_2}\right)\left(\frac{C_1}{C_2}\right)^{-1} = \left(\frac{q_2}{p_1}\right)\left(\frac{b_1}{p_1}\right)\left(\frac{b_2}{q_2}\right)\left(\frac{b_1}{c_1}\right)\left(\frac{b_2}{c_2}\right)\left(\frac{c_1}{c_2}\right)^{-1}\left(\frac{q_1}{C_1}\right)\left(\frac{p_2}{C_2}\right).$$

In case (i), we use Proposition 6 to write this

$$\left(\frac{q_2}{p_1}\right)\left(\frac{b_1}{p_1}\right)\left(\frac{b_2}{q_2}\right)\left(\frac{b_1}{a_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{a_1}{a_2}\right)^{-1}\left(\frac{q_1}{C_1}\right)\left(\frac{p_2}{C_2}\right).$$

We have

$$\left(\frac{B_1'}{A_1'}\right)\left(\frac{B_2'}{A_2'}\right)\left(\frac{A_1'}{A_2'}\right)^{-1} = \left(\frac{q_2}{p_1}\right)\left(\frac{b_1}{p_1}\right)\left(\frac{b_2}{q_2}\right)\left(\frac{b_1}{a_1}\right)\left(\frac{b_2}{a_2}\right)\left(\frac{a_1}{a_2}\right)^{-1},$$

and the statement follows. Cases (ii) and (iii) are similar. □

Let Σ be the set of $g \in \Gamma(\mathfrak{f})$ whose invariants A_1, B_1, C_1 and A_2, B_2, C_2 are such that $\gcd(C_1, C_2) = 1$. If $g \in \Sigma$ denote

$$\kappa_0(g) = \left(\frac{B_1}{C_1}\right)\left(\frac{B_2}{C_2}\right)\left(\frac{C_1}{C_2}\right)^{-1}.$$

Let $\Gamma_\infty(\mathfrak{f})$ denote the subgroup of elements of $\Gamma(\mathfrak{f})$ that are upper triangular and unipotent.

Proposition 8 *Suppose that $u \in \Gamma_\infty(\mathfrak{f})$ and that both $g, gu \in \Sigma$. Then $\kappa_0(g) = \kappa_0(gu)$.*

Proof Let $A_1, B_1, C_1, A_2, B_2, C_2$ be the invariants of g, and let $\bar{A}_1, \bar{B}_1, \bar{C}_1, \bar{A}_2, \bar{B}_2, \bar{C}_2$ be the invariants of gu. Writing

$$u = \begin{pmatrix} 1 & u_2 & u_3 \\ & 1 & u_1 \\ & & 1 \end{pmatrix}, \qquad u_4 = u_1u_2 - u_3, \tag{5}$$

we have

$$\begin{aligned} \bar{A}_1 &= A_1, & \bar{A}_2 &= A_2, \\ \bar{B}_1 &= B_1 + u_2A_1, & \bar{B}_2 &= B_2 - u_1A_2, \\ \bar{C}_1 &= C_1 + u_1B_1 + u_3A_1, & \bar{C}_2 &= C_2 - u_2B_2 + u_4A_2. \end{aligned} \tag{6}$$

As in Proposition 7 let

$$\begin{aligned} A_1 &= p_2q_1A_1', & A_2 &= p_2q_1A_2', \\ B_1 &= q_1B_1', & B_2 &= p_2B_2', \end{aligned}$$

where A_1 and A_1' are coprime. Then we may also write

$$\bar{A}_1 = p_2 q_1 \bar{A}_1', \qquad \bar{A}_2 = p_2 q_1 \bar{A}_2',$$
$$\bar{B}_1 = q_1 \bar{B}_1', \qquad \bar{B}_2 = p_2 \bar{B}_2',$$

where

$$\bar{A}_1' = A_1', \qquad \bar{A}_2' = A_2',$$
$$\bar{B}_1' = B_1' + u_2 p_2 A_1', \qquad \bar{B}_2' = B_2' - u_1 q_1 A_2.$$

We note that $C_1 \equiv \bar{C}_1$ modulo q_1 and modulo $\mathfrak{f}^2$ and similarly for C_2, so

$$\left(\frac{q_1}{C_1}\right) = \left(\frac{q_1}{\bar{C}_1}\right), \qquad \left(\frac{p_2}{C_2}\right) = \left(\frac{p_2}{\bar{C}_2}\right).$$

Now suppose we are in case (i) of Proposition 7. Then

$$\kappa_0(g) = \left(\frac{B_1'}{A_1'}\right)\left(\frac{B_2'}{A_2'}\right)\left(\frac{A_1'}{A_2'}\right)^{-1}\left(\frac{q_1}{C_1}\right)\left(\frac{p_2}{C_2}\right).$$

Since $\bar{A}_i' = A_i'$ and $\bar{B}_i' \equiv B_i'$ modulo $\bar{A}_i'$, we may replace A_i' by $\bar{A}_i'$ and B_i' by $\bar{B}_i'$ and obtain $\kappa_0(gu)$.

Next suppose we are in case (ii). Then

$$\kappa_0(g) = \left(\frac{A_1'}{B_1'}\right)\left(\frac{B_2'}{A_2'}\right)\left(\frac{A_1'}{A_2'}\right)^{-1}\left(\frac{q_1}{C_1}\right)\left(\frac{p_2}{C_2}\right).$$

In this case, the handling of the first symbol requires noting that $\mathfrak{f}^2 | u_2 p_2 A_1'$ since $\mathfrak{f} | u_2$ and $\mathfrak{f} | p_2 A_1'$. Hence we may apply Proposition 4 (i) and conclude that

$$\left(\frac{A_1'}{B_1'}\right) = \left(\frac{A_1'}{\bar{B}_1'}\right)$$

so that $\kappa_0(g) = \kappa_0(gu)$. The case (iii) is identical. $\square$

Lemma 2 *Suppose that* $\gcd(A, B, C) = 1$. *Then there exists* λ *such that* $\gcd(A + \lambda B, C) = 1$.

Proof Let $\theta = \gcd(A, B)$, and write $A = \theta A_0$, $B = \theta B_0$ with A_0, B_0 coprime. By the extension to $\mathfrak{o}$ of Dirichlet's theorem on primes in an arithmetic progression, there exists λ such that $\pi = A_0 + \lambda B_0$ is prime, and we may avoid the finite number of primes that divide C. Then $A + \lambda B = \theta\pi$, and both θ and π are prime to C. $\square$

Proposition 9 *If* $g \in \Gamma(\mathfrak{f})$ *then there exists* $u \in \Gamma_\infty(\mathfrak{f})$ *such that* $gu \in \Sigma$.

Proof Let $A_1, B_1, C_1, A_2, B_2, C_2$ be the invariants of g. If u is as in (5) then $\bar{A}_1, \bar{B}_1, \bar{C}_1, \bar{A}_2, \bar{B}_2, \bar{C}_2$ as in (6) are the invariants of gu. First, taking $u_2 = u_3 = u_4 = 0$, Lemma 2 shows that we may choose u_1 such that $\gcd(\bar{A}_1, \bar{C}_1) = 1$; replacing g by another element of $g\,\Gamma_\infty(\mathfrak{f})$ we may therefore assume that $\gcd(A_1, C_1) = 1$.

With this assumption, we now work with $u_1 = u_2 = 0$ and use only u_3. By the extension to $\mathfrak{o}$ of Dirichlet's theorem on primes in an arithmetic progression, we may find u_3 such that $\bar{C}_1 = C_1 + u_3 A_1$ is prime, and we may avoid the finite number of primes that divide $B_1 B_2$. Noting that in the notation of (6) when $u_1 = u_2 = 0$ we have $u_4 = -u_3$, $\gcd(\bar{C}_1, \bar{C}_2) = \gcd(C_1 + u_3 A_1, C_2 - u_3 A_2)$ divides $A_2(C_1 + u_3 A_1) + A_1(C_2 - u_3 A_2) = -B_1 B_2$. Since $\bar{C}_1$ is prime to $B_1 B_2$, this means that $gu \in \Sigma$. $\square$

We may now define the Kubota symbol, which we will eventually prove to be a homomorphism.

Definition 1 *Let $g \in \Gamma(\mathfrak{f})$. Then the Kubota symbol $\kappa(g) = \kappa_0(gu)$, where u is any element of $\Gamma_\infty(\mathfrak{f})$ such that $gu \in \Sigma$.*

The existence of such a u follows from Proposition 9, and the independence of $\kappa_0(gu)$ on the choice of u follows from Proposition 8.

We can now improve the result of Proposition 7 by removing the assumption that $\gcd(C_1, C_2) = 1$.

Proposition 10 *Suppose that $g \in \Gamma(\mathfrak{f})$ has invariants $A_1, B_1, C_1, A_2, B_2, C_2$. Then there exists a factorization*

$$\begin{aligned} A_1 &= p_2 q_1 A_1', & \qquad A_2 &= p_2 q_1 A_2', \\ B_1 &= q_1 B_1', & \qquad B_2 &= p_2 B_2', \end{aligned}$$

where $p_2 q_1 = \gcd(A_1, A_2)$. The coprimality (3) conditions are true, and we may assume that one of the three following cases applies:

(i) $\mathfrak{f} | B_1'$, $\lambda^2 | B_2'$, $\mathfrak{f}^2 | B_1' B_2'$ and $A_1' \equiv -A_2' \equiv 1$ modulo $\mathfrak{f}$;

(ii) $B_1' \equiv A_2' \equiv 1$ modulo $\mathfrak{f}$ and $\mathfrak{f} | p_2 A_1'$; or

(iii) $B_2' \equiv A_1' \equiv 1$ modulo $\mathfrak{f}$ and $\mathfrak{f} | q_1 A_2'$.

We have

$$\kappa(g) = \begin{cases} \left(\frac{B_1'}{A_1'}\right) \left(\frac{B_2'}{A_2'}\right) \left(\frac{A_1'}{A_2'}\right)^{-1} \left(\frac{q_1}{C_1}\right) \left(\frac{p_2}{C_2}\right) & \text{in case (i);} \\ \left(\frac{A_1'}{B_1'}\right) \left(\frac{B_2'}{A_2'}\right) \left(\frac{A_1'}{A_2'}\right)^{-1} \left(\frac{q_1}{C_1}\right) \left(\frac{p_2}{C_2}\right) & \text{in case (ii);} \\ \left(\frac{B_1'}{A_1'}\right) \left(\frac{A_2'}{B_2'}\right) \left(\frac{A_2'}{A_1'}\right)^{-1} \left(\frac{q_1}{C_1}\right) \left(\frac{p_2}{C_2}\right) & \text{in case (iii).} \end{cases}$$

Proof Let $A_1, B_1, C_1, A_2, B_2, C_2$ be the invariants of g, and let $\bar{A}_1, \bar{B}_1, \bar{C}_1, \bar{A}_2, \bar{B}_2, \bar{C}_2$ be the invariants of gu, where u is chosen so that $\gcd(\bar{C}_1, \bar{C}_2) = 1$.

$$\begin{aligned} \bar{A}_1 &= A_1, & \qquad \bar{A}_2 &= A_2, \\ \bar{B}_1 &= B_1 + u_2 A_1, & \qquad \bar{B}_2 &= B_2 - u_1 A_2, \\ \bar{C}_1 &= C_1 + u_1 B_1 + u_3 A_1, & \qquad \bar{C}_2 &= C_2 - u_2 B_2 + u_4 A_2. \end{aligned}$$

By Proposition 7 we may factor

$$\begin{aligned} \bar{A}_1 &= p_2 q_1 \bar{A}_1', & \qquad \bar{A}_2 &= p_2 q_1 \bar{A}_2', \\ \bar{B}_1 &= q_1 \bar{B}_1', & \qquad \bar{B}_2 &= p_2 \bar{B}_2', \end{aligned}$$

where $\gcd(\bar{A}_1', \bar{A}_2') = 1$, and taking

$$\begin{aligned} A_1' &= \bar{A}_1', & A_2' &= \bar{A}_2', \\ B_1' &= \bar{B}_1' - u_2 p_2 \bar{A}_1', & B_2' &= \bar{B}_2' + u_1 q_1 A_2, \end{aligned}$$

we have the required factorization. Proceeding as in Proposition 8 we get

$$\left(\frac{B_1'}{A_1'}\right)\left(\frac{B_2'}{A_2'}\right)\left(\frac{A_1'}{A_2'}\right)^{-1}\left(\frac{q_1}{C_1}\right)\left(\frac{p_2}{C_2}\right) = \left(\frac{\bar{B}_1'}{\bar{A}_1'}\right)\left(\frac{\bar{B}_2'}{\bar{B}_2'}\right)\left(\frac{\bar{B}_1'}{\bar{B}_2'}\right)^{-1}\left(\frac{q_1}{\bar{C}_1}\right)\left(\frac{p_2}{\bar{C}_2}\right)$$

in case (i), and since the right-hand side is $\kappa_0(gu) = \kappa(g)$, we are done in this case; the other cases are similar. □

Proposition 11 *If $g \in \Gamma(\mathfrak{f})$, then we may obtain a factorization as in Proposition 5 where $r_1 \equiv r_2 \equiv p_1 \equiv q_2 \equiv c_1 \equiv c_2 \equiv 1$ modulo $\mathfrak{f}$. In this case*

$$\begin{aligned} \kappa(g) = &\left(\frac{q_1}{p_1}\right)\left(\frac{q_2}{p_1}\right)\left(\frac{r_1}{p_1}\right)\left(\frac{p_2}{q_2}\right)\left(\frac{p_2}{r_1}\right)\left(\frac{p_2}{r_2}\right)\left(\frac{q_1}{r_1}\right)\left(\frac{q_1}{r_2}\right)\left(\frac{r_2}{q_2}\right) \\ &\left(\frac{b_1}{p_1}\right)\left(\frac{b_2}{q_2}\right)\left(\frac{q_1}{c_1}\right)\left(\frac{p_2}{c_2}\right)\left(\frac{r_1}{a_1}\right)\left(\frac{r_2}{a_2}\right) \\ &\times \left(\frac{b_1}{c_1}\right)\left(\frac{b_2}{c_2}\right)\left(\frac{c_1}{c_2}\right)^{-1}. \end{aligned} \tag{7}$$

Proof Given any factorization as in Proposition 5 we may adjust r_1, r_2, p_1, q_1 by units, with compensating changes in a_i, b_i, c_i so that $r_1 \equiv r_2 \equiv p_1 \equiv q_2 \equiv c_1 \equiv c_2 \equiv 1$.

It follows from the proof of Proposition 6 that there exists a particular factorization of this type in which cases (i), (ii) or (iii) of that proposition applies. Moreover, passing to such a factorization from an arbitrary one involves replacing b_1, q_1, p_2, b_2 by αb_1, $\alpha^{-1} q_1$, αp_2, $\alpha^{-1} b_2$ for some $\alpha \in F^\times$, and it may be checked easily that such a change does not alter (7). Therefore we may assume that cases (i), (ii) or (iii) applies.

Let

$$\begin{aligned} A_1' &= p_1 a_1, & A_2' &= q_2 a_2, \\ B_1' &= q_2 r_1 b_1, & B_2' &= p_1 r_2 b_2. \end{aligned}$$

This factorization satisfies the conditions of Proposition 10, and we may use one of the expressions from that Proposition. Expanding the symbols, using reciprocity when necessary, together with the identify from Proposition 6 gives (7). □

Theorem 1 *Suppose that $g \in \Gamma(\mathfrak{f})$ has invariants $A_1, B_1, C_1, A_2, B_2, C_2$. Then there exists a factorization*

$$\begin{aligned} C_1 &= r_1 r_2 C_1' & C_2 &= r_1 r_2 C_2' \\ B_1 &= r_1 B_1', & B_2 &= r_2 B_2', \end{aligned}$$

where $r_1 \equiv r_2 \equiv C_1' \equiv C_2' \equiv 1$ modulo $\mathfrak{f}$, and $\gcd(C_1, C_1') = 1$. We have

$$\gcd(B_1', C_1') = \gcd(B_2', C_2') = \gcd(A_1, r_1) = \gcd(A_2, r_2) = 1$$

and

$$\kappa(g) = \left(\frac{B_1'}{C_1'}\right)\left(\frac{B_2'}{C_2'}\right)\left(\frac{C_1'}{C_2'}\right)^{-1}\left(\frac{A_1}{r_1}\right)\left(\frac{A_2}{r_2}\right). \tag{8}$$

Proof The existence of such a factorization may be proved directly very easily, or alternatively follows from Proposition 5, on taking

$$\begin{aligned} B_1' &= q_1q_2b_1, & B_2' &= p_1p_2b_2, \\ C_1' &= p_1c_1, & C_2' &= q_2c_2. \end{aligned}$$

We need to know that every such factorization arises from Proposition 6 in this way, which we may see by taking any $(P, Q, R) \geqslant (1, 1, r_1r_2)$ in the proof of Proposition 6. Once the factorization of Proposition 6 is obtained, we may adjust p_1 and q_2 by units so that $r_1 \equiv r_2 \equiv p_1 \equiv q_2 \equiv c_1 \equiv c_2 \equiv 1$ modulo $\mathfrak{f}$. Plugging in these expressions for B_1', B_2', C_1', C_2', as well as $A_1 = p_1p_2q_1a_1$ and $A_2 = q_1q_2p_2a_2$, into the right-hand side of (8) then expanding and using the reciprocity law, we obtain (7), proving (8). □

Proposition 12 *Suppose that $g \in \Gamma(\mathfrak{f})$ and let*

$$h = \begin{pmatrix} p & q & \\ r & s & \\ & & 1 \end{pmatrix} \in \Gamma(\mathfrak{f}).$$

Then $\kappa(gh) = \kappa(g)\,\kappa(h)$.

Proof We prove this first under the assumption (to be removed later) that $g \in \Sigma$. Thus let $A_1, B_1, C_1, A_2, B_2, C_2$ be the invariants of g, and let $A_1'', B_1'', C_1'', A_2'', B_2'', C_2''$ be the invariants of $g'' = gh$. Our assumption on g is that $\gcd(C_1, C_2) = 1$.

We find that

$$\begin{aligned} sA_1'' - rB_1'' &= A_1, & (9)\\ sB_2'' + rC_2'' &= B_2, & (10)\\ sC_2 - qB_2 &= C_2''. & (11) \end{aligned}$$

The following identities are also easily established:

$$\begin{aligned} pC_1A_2 &= -A_1''C_2 - B_1B_2'', & (12)\\ qC_1A_2 &= -B_1''C_2 + B_1C_2'', & (13)\\ rC_1A_2 &= -A_1''B_2 + A_1B_2'', & (14)\\ sC_1A_2 &= -B_1''B_2 - A_1C_2''. & (15) \end{aligned}$$

As in Theorem 1 let us factor

$$\begin{aligned} B_1'' &= r_1B_1', & B_2'' &= r_2B_2', \\ C_1'' &= r_1r_2C_1', & C_2'' &= r_1r_2C_2', \end{aligned}$$

where $r_1 \equiv r_2 \equiv C_1' \equiv C_2' \equiv 1$ modulo $\mathfrak{f}$ and $\gcd(C_1', C_2') = 1$. The fact that $g \in \Sigma$ implies that $\gcd(B_2'', C_2'') = \gcd(B_2, C_2) = 1$ and so $r_2 = 1$. Thus by Theorem 1

$$\kappa(gh) = \left(\frac{B_1'}{C_1'}\right)\left(\frac{B_2'}{C_2'}\right)\left(\frac{C_1'}{C_2'}\right)^{-1}\left(\frac{A_1''}{r_1}\right).$$

Note that r_1 divides $C_1'' = C_1$ and so it is prime to C_2 and B_1. Next we prove that

$$\left(\frac{B_1'}{C_1'}\right)\left(\frac{C_1'}{C_2'}\right)^{-1} = \left(\frac{B_1}{C_1}\right)\left(\frac{C_1}{C_2}\right)^{-1}\left(\frac{B_1}{r_1}\right)^{-1}\left(\frac{C_2}{r_1}\right). \tag{16}$$

By (13) we have $qC_1'A_2 = -B_1'C_2 + B_1C_2'$. Thus

$$\left(\frac{B_1'}{C_1'}\right)\left(\frac{C_1'}{C_2'}\right)^{-1} = \left(\frac{B_1'C_2}{C_1'}\right)\left(\frac{C_1'}{C_2'}\right)^{-1}\left(\frac{C_2}{C_1'}\right)^{-1} = \left(\frac{B_1C_2'}{C_1'}\right)\left(\frac{C_1'}{C_2'}\right)^{-1}\left(\frac{C_2}{C_1'}\right)^{-1} = \left(\frac{B_1}{C_1'}\right)\left(\frac{C_2}{C_1'}\right)^{-1}.$$

Now (16) follows, using reciprocity (again), since $C_1 = C_1'' = r_1C_1'$.

Let us factor $s = \sigma d$, $C_2'' = d\gamma_2''$ with $\sigma \equiv d \equiv \gamma_2'' \equiv 1$ modulo $\mathfrak{f}$ and $\gcd(\sigma, \gamma_2'') = 1$. We have $C_2'' = sC_2 - qB_2$ and since $\gcd(s, q) = 1$, d divides B_2; write $B_2 = d\beta_2$. Now since $C_2'' = r_1C_2'$ we may factor $d = d_1d_2$, with $r_1 = \rho_1 d_1$ and $C_2' = d_2\gamma_2'$. This factorization may be chosen so that $\gcd(\rho_1, d_2) = 1$, and $d_1 \equiv d_2 \equiv 1$ modulo $\mathfrak{f}$. We note that $\gamma_2'' = \rho_1\gamma_2'$. We now show that

$$\left(\frac{B_2'}{C_2'}\right) = \left(\frac{r}{s}\right)\left(\frac{B_2}{C_2}\right)\left(\frac{r}{d}\right)^{-1}\left(\frac{d}{C_2}\right)^{-1}\left(\frac{\rho_1}{\sigma}\right)\left(\frac{B_2'}{d_2}\right)\left(\frac{\beta_2}{\rho_1}\right)^{-1}. \tag{17}$$

By (10) and (11) we have

$$\begin{aligned} \sigma B_2'' + r\gamma_2'' &= \beta_2, && (18)\\ \sigma C_2 - q\beta_2 &= \gamma_2'' && (19) \end{aligned}$$

Using (18) we have

$$\left(\frac{B_2'}{C_2'}\right) = \left(\frac{B_2'}{d_2}\right)\left(\frac{B_2'}{\gamma_2'}\right) = \left(\frac{B_2'}{d_2}\right)\left(\frac{\sigma B_2'}{\gamma_2'}\right)\left(\frac{\sigma}{\gamma_2'}\right)^{-1} = \left(\frac{B_2'}{d_2}\right)\left(\frac{\beta_2}{\gamma_2'}\right)\left(\frac{\sigma}{\gamma_2'}\right)^{-1}.$$

Note that $\gcd(\beta_2, \gamma_2'') = 1$. Indeed by (19) any prime dividing both γ_2'' and β_2 would divide either σ (impossible since σ and γ_2'' are coprime) or C_2 (impossible since B_2 and C_2 are coprime). Therefore

$$\begin{aligned} \left(\frac{B_2'}{C_2'}\right) = \left(\frac{B_2'}{d_2}\right)\left(\frac{\beta_2}{\gamma_2''}\right)\left(\frac{\beta_2}{\rho_1}\right)^{-1}\left(\frac{\sigma}{\gamma_2'}\right)^{-1} &= \text{[by (19) and Proposition 4 (i)]}\\ \left(\frac{B_2'}{d_2}\right)\left(\frac{\beta_2}{\sigma}\right)\left(\frac{\beta_2}{C_2}\right)\left(\frac{\beta_2}{\rho_1}\right)^{-1}\left(\frac{\sigma}{\gamma_2'}\right)^{-1} &= \text{[by (18), reciprocity]}\\ \left(\frac{B_2'}{d_2}\right)\left(\frac{r}{\sigma}\right)\left(\frac{\gamma_2''}{\sigma}\right)\left(\frac{\beta_2}{C_2}\right)\left(\frac{\beta_2}{\rho_1}\right)^{-1}\left(\frac{\gamma_2'}{\sigma}\right)^{-1}, & \end{aligned}$$

and (17) follows. Since $\kappa(h) = \left(\frac{r}{s}\right)$, and since we are assuming that $g \in \Sigma$, we now have

$$\frac{\kappa(gh)}{\kappa(g)\,\kappa(h)} = \left(\frac{B_1'}{C_1'}\right)\left(\frac{B_2'}{C_2'}\right)\left(\frac{C_1'}{C_2'}\right)^{-1}\left(\frac{A_1''}{r_1}\right)\left(\frac{B_1}{C_1}\right)^{-1}\left(\frac{B_2}{C_2}\right)^{-1}\left(\frac{C_1}{C_2}\right)\left(\frac{r}{s}\right)^{-1},$$

which by (16) and (17) equals

$$\left(\frac{B_1}{r_1}\right)^{-1}\left(\frac{C_2}{r_1}\right)\left(\frac{r}{d}\right)^{-1}\left(\frac{d}{C_2}\right)^{-1}\left(\frac{\rho_1}{\sigma}\right)\left(\frac{B_2'}{d_2}\right)\left(\frac{\beta_2}{\rho_1}\right)^{-1}\left(\frac{A_1''}{r_1}\right).$$

We will show that this equals 1. By (9), d_1 divides A_1, say $A_1 = d_1\alpha_1$ so (9) implies

$$\sigma d_2 A_1'' - r\rho_1 B_1' = \alpha_1. \tag{20}$$

Since $\gcd(\rho_1, d_2) = 1$ and $r_1 = \rho_1 d_1$ our previous expression equals

$$\left(\frac{B_1}{r_1}\right)^{-1}\left(\frac{C_2}{r_1}\right)\left(\frac{r}{d}\right)^{-1}\left(\frac{d}{C_2}\right)^{-1}\left(\frac{B_2'}{d_2}\right)\left(\frac{\beta_2}{\rho_1}\right)^{-1}\left(\frac{d_2}{\rho_1}\right)^{-1}\left(\frac{\sigma d_2 A_1''}{\rho_1}\right)\left(\frac{A_1''}{d_1}\right).$$

Using (20), $r_1 = \rho_1 d_1$ and $\alpha_1 C_2 + d_2 B_1 \beta_2 + \rho_1 C_1' A_2 = 0$, this reduces to

$$\left(\frac{B_1}{d_1}\right)^{-1}\left(\frac{C_2}{d_1}\right)\left(\frac{B_2'}{d_1}\right)^{-1}\left(\frac{A_1''}{d_1}\right)\cdot\left(\frac{r}{d}\right)^{-1}\left(\frac{C_2}{d}\right)^{-1}\left(\frac{B_2'}{d}\right)$$

The product of the first four four is 1 by (12), together with the fact that $B_2' = B_2''$. The product of the last four factors is 1 by (10).

The result is now proved under the assumption that $g \in \Sigma$. Replacing g by gh and h by h^{-1} and noting that $\kappa(h^{-1}) = \kappa(h)^{-1}$, we have also proved the result under the assumption that $gh \in \Sigma$. We may remove this assumption by the following considerations. By Proposition 9 there exists

$$u = \begin{pmatrix} 1 & u_2 & u_3 \\ & 1 & u_1 \\ & & 1 \end{pmatrix} \in \Gamma_\infty(\mathfrak{f})$$

such that $ghu \in \Sigma$, and by definition $\kappa(gh) = \kappa(ghu)$. Now $hu = u'h'$ where

$$u' = \begin{pmatrix} 1 & & pu_3 + qu_1 \\ & 1 & ru_3 + su_1 \\ & & 1 \end{pmatrix}, \qquad h' = \begin{pmatrix} p & q + u_2 p & \\ r & s + u_2 r & \\ & & 1 \end{pmatrix}.$$

Thus the case that we have just settled shows that $\kappa(gh) = \kappa(gu')\,\kappa(h') = \kappa(g)\,\kappa(h')$. But

$$\kappa(h') = \left(\frac{r}{s + u_2 r}\right) = \left(\frac{r}{s}\right) = \kappa(h)$$

by Proposition 4 (i), and we are done. □

Lemma 3 *Let G and H be a groups, S a generating subset of G that is closed under the inverse map of G. Assume that $\chi : G \longrightarrow H$ is a map such that $\chi(gx) = \chi(g)\,\chi(x)$ for all $x \in S$, $g \in G$. Then χ is a homomorphism.*

Proof By induction if $x_1, \cdots, x_N \in S$ we have $\chi(x_1 \cdots x_N) = \chi(x_1) \cdots \chi(x_N)$, and since every element of G can be written in this form, the statement follows. $\square$

Theorem 2 *The map $\kappa : \Gamma(\mathfrak{f}) \longrightarrow \mu_n$ is a homomorphism.*

Proof We may take S to be the subset of g of the three forms

$$\begin{pmatrix} p & q & \\ r & s & \\ & & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & & \\ & p & q \\ & r & s \end{pmatrix}, \qquad \begin{pmatrix} 1 & u_2 & u_3 \\ & 1 & u_1 \\ & & 1 \end{pmatrix}.$$

We have proved that $\kappa(gx) = \kappa(g)$ when x is of the first or third form. For the second type of element, we may deduce this from the first type by applying the involution. The result now follows from Lemma 3. $\square$

2 Some Exponential Sums

In this Section, $\mathfrak{o}$ will be the ring of integers in a totally complex number field F. We assume that $\mathfrak{o}^\times$ contains the group μ_n of n-th roots of unity, and that -1 is an n-th power in $\mathfrak{o}^\times$. We assume that there is given an ideal $\mathfrak{f}$ of $\mathfrak{o}$ such that

$$d \equiv c \equiv 1 \bmod \mathfrak{f}, \quad \gcd(d, c) = 1 \qquad \Rightarrow \qquad \left(\frac{c}{d}\right) = \left(\frac{d}{c}\right). \tag{21}$$

We also assume that if $d \equiv d' \equiv 1$ modulo $\mathfrak{f}$ then

$$d \equiv d' \bmod \mathfrak{f}^2 \text{ and } d \equiv d' \bmod c \quad \Rightarrow \quad \left(\frac{c}{d}\right) = \left(\frac{c}{d'}\right). \tag{22}$$

Note that this condition is satisfied in the two cases of Section 1 by Proposition 4.

We embed $F \longrightarrow F_\infty$, the product of the archimedean completions of F. Let $\psi : F_\infty \longrightarrow \mathbb{C}$ be a nontrivial additive character. We assume that the conductor of ψ is precisely $\mathfrak{o}$ that is, $\psi(x\mathfrak{o}) = 1$ if and only if $x \in \mathfrak{o}$.

The exponential sums that we describe are analogs of classical Gauss sums, and they will be evaluated in terms of Gauss sums. Some of what we will prove about the H-sums proved in this Section (particularly the multiplicativity) are analogous to properties of the Gauss sums, so this is the place to discuss the Gauss sums, even though they won't be used until the next Section. If $c \equiv 1$ modulo $\mathfrak{f}$ let

$$g(m, c) = \sum_{d \bmod c} \left(\frac{d}{c}\right) \psi\left(\frac{md}{c}\right). \tag{23}$$

Also, let $\phi(c)$ be the cardinality of $(\mathfrak{o}/(c))^\times$.

Proposition 13 *The Gauss sum has the following properties.*
(i) We have

$$g(m, cc') = \left(\frac{c}{c'}\right)\left(\frac{c'}{c}\right) g(m, c)\, g(m, c'), \qquad \text{if } c, c' \text{ are coprime;}$$

(ii) We have

$$g(am, c) = \left(\frac{a}{c}\right)^{-1} g(m, c) \qquad \text{if } a, c \text{ are coprime;}$$

(iii) Suppose that p is prime. The Gauss sum $g(p^k, p^l)$ is zero unless either $l = k + 1$ or $k \geqslant l$ and $n|l$. If $n|l$ then

$$g(p^k, p^l) = \begin{cases} 0 & \text{if } k < l - 1; \\ -\mathbb{N}p^k & \text{if } k = l - 1; \\ \phi(p^l) & \text{if } k \geqslant l. \end{cases}$$

(iv) If $n \nmid l$ then $|g(p^{l-1}, p^l)| = \mathbb{N}p^{l-\frac{1}{2}}$.
(v) If $k, k + b > 0$ and $n|b$ then $g(p^{k+b}, p^{l+b}) = \mathbb{N}p^b \, g(p^k, p^l)$.

Let C_1 and C_2 be elements of $\mathfrak{o}$ that are congruent to 1 modulo $\mathfrak{f}$, and let m_1, $m_2 \in \mathfrak{o}$. We define

$$H(C_1, C_2; m_1, m_2) = \sum_{\substack{A_1, B_1 \bmod C_1 \\ A_2, B_2 \bmod C_2 \\ \gcd(A_1, B_1, C_1) = 1 \\ \gcd(A_2, B_2, C_2) = 1 \\ A_1 \equiv B_1 \equiv A_2 \equiv B_2 \equiv 0 \bmod \mathfrak{f} \\ A_1 C_2 + B_1 B_2 + C_1 A_2 \equiv 0 \bmod C_1 C_2}} \left(\frac{B_1'}{C_1'}\right) \left(\frac{B_2'}{C_2'}\right) \left(\frac{C_1'}{C_2'}\right)^{-1} \left(\frac{A_1}{r_1}\right) \left(\frac{A_2}{r_2}\right) \psi\left(\frac{m_1 B_1}{C_1} + \frac{m_2 B_2}{C_2}\right),$$

where we have chosen a factorization

$$\begin{aligned} C_1 &= r_1 r_2 C_1' & \qquad C_2 &= r_1 r_2 C_2' \\ B_1 &= r_1 B_1', & B_2 &= r_2 B_2', \end{aligned}$$

where $r_1 \equiv r_2 \equiv C_1' \equiv C_2' \equiv 1$ modulo $\mathfrak{f}$, and $\gcd(C_1, C_1') = 1$.

Remark 1 The summation is more correctly written

$$\sum_{\substack{B_1 \bmod C_1 \\ B_2 \bmod C_2 \\ B_1 \equiv B_2 \equiv 0 \bmod \mathfrak{f}}} \quad \sum_{\substack{A_1 \bmod C_1 \\ A_2 \bmod C_2 \\ \gcd(A_1, B_1, C_1) = 1 \\ \gcd(A_2, B_2, C_2) = 1 \\ A_1 \equiv A_2 \equiv 0 \bmod \mathfrak{f} \\ A_1 C_2 + B_1 B_2 + C_1 A_2 \equiv 0 \bmod C_1 C_2}} . \tag{24}$$

The reason that this way of writing the sum is correct is that if B_1 is changed to $B_1 + tC_1$ then the terms of the inner sum are permuted, with a compensating change $A_2 \longrightarrow A_2 - tB_2$. We will check this in the proof of the following Proposition.

Proposition 14 *The sum $H(C_1, C_2; m_1, m_2)$ is well-defined.*

Proof First, it must be checked that for fixed $A_1, B_1, C_1, A_2, B_2, C_2$ the expression is independent of the factorization. We do this in two steps. First, with C_1' and C_2' fixed, we might vary the factorization by changing r_1 and r_2, with compensating changes to B_1' and B_2':

$$\begin{aligned} r_1 &\longrightarrow \alpha r_1, & B_1' &\longrightarrow \alpha^{-1} B_1', \\ r_2 &\longrightarrow \alpha^{-1} r_2, & B_2' &\longrightarrow \alpha B_2'. \end{aligned}$$

Here $\alpha \in F^\times$ must be such that $\alpha r_1, \alpha^{-1} r_2, \alpha^{-1} B_1', \alpha B_2'$ as well as r_1, r_2, B_1', B_2' are integral, and $\alpha^{-1} B_1', \alpha B_2' \in \mathfrak{f}$. Writing α as a fraction, this may be done in two steps; first we consider the case where α is integral, dividing r_2 and B_1'; then we take α^{-1} to be integral, dividing r_1 and B_2'. The two steps are identical, so we only check the first; thus α is an integer dividing $\gcd(r_2, B_1')$. Since $r_1 \equiv 1$ modulo $\mathfrak{f}$, and αr_1 is to satisfy the same congruence, we have $\alpha \equiv 1$ modulo $\mathfrak{f}$. This variable change multiplies the symbol in the definition of H by

$$\left(\frac{\alpha}{C_1'}\right)^{-1} \left(\frac{\alpha}{C_2'}\right) \left(\frac{A_1}{\alpha}\right) \left(\frac{A_2}{\alpha}\right)^{-1} = \left(\frac{A_2 C_1'}{\alpha}\right)^{-1} \left(\frac{A_1 C_2'}{\alpha}\right),$$

where we have used (21). Now $A_2 C_1' \equiv A_1 C_1'$ modulo both $\mathfrak{f}^2$ and α, since both $\mathfrak{f}^2$ and α divide $B_1' B_2'$, so the symbol is unchanged. One must also check invariance under

$$\begin{aligned} C_1' &\longrightarrow \varepsilon C_1', & C_2' &\longrightarrow \varepsilon C_2', \\ r_1' &\longrightarrow \varepsilon^{-1} r_1, & B_1' &\longrightarrow \varepsilon B_1', \end{aligned}$$

with r_2 and B_2' unchanged, where ε is a unit $\equiv 1$ modulo $\mathfrak{f}$. This is straightforward as a consequence of reciprocity and the invariance of $\left(\frac{c}{d}\right)$ when d is changed by a unit.

The next thing that must be checked is that in (24) the inner sum over A_1 and A_2 does not depend on the choice of A_1 and A_2 modulo C_1 and C_2 respectively. This follows from Proposition 1 (ii) since r_1 and r_2 both divide C_1 and C_2.

Lastly, it must be checked is that the sum is invariant under $B_1 \longrightarrow B_1 + tC_1$ and $A_2 \longrightarrow A_2 - tB_2$. This variable change corresponds to $B_1' \longrightarrow B_1' + t r_2 C_1'$, with no changes in r_1, r_2 and B_2, and it is easy to check using Proposition 1 (ii) that the sum is unchanged. This proves the assertion in Remark 1 that the terms of the inner sum are permuted when B_1 is changed modulo C_1. There is a similar verification for $B_2 \longrightarrow tC_2$ and $A_1 \longrightarrow A_1 - tB_1$. $\square$

Proposition 15 *If* $\gcd(C_1 C_2, C_1' C_2') = 1$ *with* $C_1 \equiv C_2 \equiv C_1' \equiv C_2' \equiv 1$ *modulo* $\mathfrak{f}$*, then*

$$H(C_1 C_1', C_2 C_2'; m_1, m_2) = \left(\frac{C_1}{C_1'}\right)^2 \left(\frac{C_2}{C_2'}\right)^2 \left(\frac{C_1}{C_2'}\right)^{-1} \left(\frac{C_2}{C_1'}\right)^{-1} H(C_1, C_2; m_1, m_2)\, H(C_1', C_2'; m_1, m_2).$$

Proof Let $p, p' \in \mathfrak{o}$ such that $pC_1C_2 + p'C_1'C_2' = 1$. Let B_1, A_1 be given modulo C_1 and B_2, A_2 modulo C_2 such that $A_1 \equiv B_1 \equiv A_2 \equiv B_2 \equiv 0$ modulo $\mathfrak{f}$, $\gcd(A_1, B_1, C_1) = \gcd(A_2, B_2, C_2) = 1$ and $A_1 C_2 + B_1 B_2 + C_1 A_2 \equiv 0$ modulo $C_1 C_2$, and let similar data B_1', A_1' modulo C_1'. Let

$$\begin{aligned} c_1 &= C_1 C_1', & c_2 &= C_2 C_2', \\ b_1 &= p' C_1'^2 C_2' B_1 + p C_1^2 C_2 B_1', & b_2 &= p' C_1' C_2'^2 B_2 + p C_1 C_2^2 B_2', \\ a_1 &= p' C_1'^2 C_2' A_1 + p C_1^2 C_2 A_1' & a_2 &= p' C_1' C_2'^2 A_2 + p C_1 C_2^2 A_2'. \end{aligned}$$

Then b_1, a_1 and b_2, a_2 run through the residue classes modulo c_1 and c_2 respectively such that $a_1c_2 + b_1b_2 + c_1a_2 \equiv 0$ modulo c_1c_2 and $\gcd(a_1, b_1, c_1) = \gcd(a_2, b_2, c_2) = 1$, and we may use these to parametrize the sum $H(c_1, c_2; m_1, m_2)$. We show that we can choose factorizations

$$\begin{aligned} C_1 &= r_1r_2\hat{C}_1, & C_2 &= r_1r_2\hat{C}_2, \\ B_1 &= r_1\hat{B}_1, & B_2 &= r_2\hat{B}_2, \\ C_1' &= r_1'r_2'\hat{C}_1', & C_2' &= r_1'r_2'\hat{C}_2', \\ B_1' &= r_1'\hat{B}_1', & B_2' &= r_2'\hat{B}_2', \\ c_1 &= R_1R_2\hat{c}_1, & c_2 &= R_1R_2\hat{c}_2, \\ b_1 &= R_1\hat{b}_1, & b_2 &= R_2\hat{b}_2, \end{aligned}$$

such that $r_i \equiv r_i' \equiv R_i \equiv 1$ modulo $\mathfrak{f}$ and $\gcd(C_1, C_2) = \gcd(\hat{C}_1', \hat{C}_2') = \gcd(c_1, c_2) = 1$ and

$$\begin{aligned} \left(\frac{\hat{b}_1}{\hat{c}_1}\right)\left(\frac{\hat{b}_2}{\hat{c}_2}\right)\left(\frac{\hat{c}_1}{\hat{c}_2}\right)^{-1}\left(\frac{a_1}{R_1}\right)\left(\frac{a_2}{R_2}\right) &= \\ \left(\frac{\hat{B}_1}{\hat{C}_1}\right)\left(\frac{\hat{B}_2}{\hat{C}_2}\right)\left(\frac{\hat{C}_1}{\hat{C}_2}\right)^{-1}\left(\frac{A_1}{r_1}\right)\left(\frac{A_2}{r_2}\right)\left(\frac{\hat{B}_1'}{\hat{C}_1'}\right)\left(\frac{\hat{B}_2'}{\hat{C}_2'}\right)\left(\frac{\hat{C}_1'}{\hat{C}_2'}\right)^{-1}\left(\frac{A_1'}{r_1'}\right)\left(\frac{A_2'}{r_2'}\right)& \\ \times\left(\frac{C_1}{C_1'}\right)^2\left(\frac{C_2}{C_2'}\right)^2\left(\frac{C_1}{C_2'}\right)^{-1}\left(\frac{C_2}{C_1'}\right)^{-1}&. \end{aligned} \tag{25}$$

We first choose the factorizations of the C_i and C_i', then take $R_1 = r_1r_1'$, $R_2 = r_2r_2'$,

$$\begin{aligned} \hat{c}_1 &= \hat{C}_1\hat{C}_1', & \hat{c}_2 &= \hat{C}_2\hat{C}_2', \\ \hat{b}_1 &= r_1'^2r_2'^3p'\hat{C}_1'^2\hat{C}_2'\hat{B}_1 + pr_1^2r_2^3\hat{C}_1^2\hat{C}_2\hat{B}_1', & \hat{b}_2 &= p'r_1'^3r_2'^2\hat{C}_1'\hat{C}_2'^2\hat{B}_2 + pr_1^3r_2^2\hat{C}_1\hat{C}_2^2\hat{B}_2'. \end{aligned}$$

We will show that

$$\begin{aligned} \left(\frac{\hat{b}_1}{\hat{c}_1}\right) &= \left(\frac{r_2\hat{C}_1\hat{B}_1'}{\hat{C}_1'}\right)\left(\frac{r_2'\hat{C}_1'\hat{B}_1}{\hat{C}_1}\right), & \left(\frac{\hat{b}_2}{\hat{c}_2}\right) &= \left(\frac{r_1'\hat{C}_2'\hat{B}_2}{\hat{C}_2}\right)\left(\frac{r_1\hat{C}_2\hat{B}_2'}{\hat{C}_2'}\right), \\ \left(\frac{a_1}{R_1}\right) &= \left(\frac{r_1'r_2'\hat{C}_1'A_1}{r_1}\right)\left(\frac{r_1r_2\hat{C}_1A_1'}{r_1'}\right), & \left(\frac{a_2}{R_2}\right) &= \left(\frac{r_1'r_2'\hat{C}_2'A_2}{r_2}\right)\left(\frac{r_1r_2\hat{C}_2A_2'}{r_2'}\right). \end{aligned} \tag{26}$$

We begin by noting that

$$\left(\frac{\hat{b}_1}{\hat{c}_1}\right) = \left(\frac{pr_1^2r_2^3\hat{C}_1^2\hat{C}_2B_1'}{\hat{C}_1'}\right)\left(\frac{r_1'^2r_2'^3p'\hat{C}_1'^2\hat{C}_2'\hat{B}_1}{\hat{C}_1}\right)$$

and since $pr_1^2r_2^2\hat{C}_1\hat{C}_2 + p'r_1'^2r_2'^2\hat{C}_1'\hat{C}_2' = 1$, one may simplify both factors to obtain the first identity. The others are similar. Now substituting (26) into the left-hand side of (25) and simplifying one (using the reciprocity law) obtains the result. $\square$

Proposition 16 *Suppose that* $\gcd(m_1'm_2', C_1C_2) = 1$. *Then*

$$H(C_1, C_2; m_1m_1', m_2m_2') = \left(\frac{m_1'}{C_1}\right)^{-1}\left(\frac{m_2'}{C_2}\right)^{-1} H(C_1, C_2; m_1, m_2)$$

Proof This is much easier than the multiplicativity of Proposition 15, and we leave it to the reader. $\square$

We now prove the main theorem of [2], giving fuller details than we had space for in that paper. IWe will make use of strict Gelfand-Tsetlin patterns of the form

$$\mathfrak{T} = \left\{ \begin{array}{ccccc} l_1+l_2+2 & & l_2+1 & & 0 \\ & a & & b & \\ & & c & & \end{array} \right\}. \tag{27}$$

For each such $\mathfrak{T}$ define

$$G(\mathfrak{T}) = g(p^{a-b-1}, p^{c-b})\; g(p^{l_2}, p^b)\, g(p^{l_1+b}, p^{a+b-l_2-1}) \tag{28}$$

unless $a = l_2+1$; in the latter case we modify the definition and write

$$G\left(\left\{ \begin{array}{ccccc} l_1+l_2+2 & & l_2+1 & & 0 \\ & l_2+1 & & b & \\ & & c & & \end{array} \right\}\right) = \mathbb{N}p^b\, g(p^{a-b-1}, p^{c-b})\; g(p^{l_2}, p^b). \tag{29}$$

Note that the pattern $\mathfrak{T}$ with $a = b = l_2+1$ is not strict, and will be omitted from our summations. Thus $a-b-1 \geqslant 0$.

If $\mathfrak{T}$ is as in (27), let $k(\mathfrak{T}) = (a+b-l_2-1, c)$. Let $k_1(\mathfrak{T}) = a+b-l_2-1$ and $k_2(\mathfrak{T}) = c$.

Theorem 3 *Let l_1, l_2 be nonnegative integers. Then*

$$\sum_{k_1,k_2} H(p^{k_1}, p^{k_2}; p^{l_1}, p^{l_2})\, \mathbb{N}p^{-k_1 s_1 - k_2 s_2} = \sum_{\mathfrak{T}} G(\mathfrak{T})\, \mathbb{N}p^{-k_1(\mathfrak{T})s_1 - k_2(\mathfrak{T})s_2},$$

where the summation is over all strict Gelfand-Tsetlin patterns $\mathfrak{T}$ of the form (27).

Proof Let us denote $k(\mathfrak{T}) = (a+b-l_2-1, c)$. Let $\Upsilon(k_1,k_2;l_1,l_2)$ be the set of all $\mathfrak{T}$ of the form (27) such that $k(\mathfrak{T}) = (k_1,k_2)$. Evidently what must be proved is that

$$H(k_1,k_2;l_1,l_2) = H'(k_1,k_2;l_1,l_2) \tag{30}$$

where

$$H'(k_1,k_2;l_1,l_2) = \sum_{\mathfrak{T}\in\Upsilon(k_1,k_2;l_1,l_2)} G(\mathfrak{T}).$$

Lemma 4 *Let*

$$\mathfrak{T} = \left\{ \begin{array}{ccccc} l_1+l_2+2 & & l_2+1 & & 0 \\ & a & & b & \\ & & c & & \end{array} \right\}$$

be a Gelfand-Tsetlin pattern. Assume that

$$\begin{aligned} l_2 &\geqslant b, \\ c+l_2+1 &\geqslant a, \\ c-2a+l_1+2l_2+2 &\geqslant b. \end{aligned} \tag{31}$$

Let

$$\begin{aligned} a' &= c - a + l_1 + l_2 + 2, \\ b' &= a - l_2 - 1, \\ c' &= a + b - l_2 - 1, \end{aligned}$$

and

$$\mathfrak{T}' = \left\{ \begin{array}{ccccc} l_1 + l_2 + 2 & & l_1 + 1 & & 0 \\ & a' & & b' & \\ & & c' & & \end{array} \right\}.$$

Then $\mathfrak{T}'$ is also a Gelfand-Tsetlin pattern and $G(\mathfrak{T}) = G(\mathfrak{T}')$. The hypothesis (31) is always satisfied if $k_2 = c$ is greater than $k_1 = a + b - l_2 - 1$.

Proof It is straightforward to check that (31) implies that $\mathfrak{T}'$ is a Gelfand-Tsetlin pattern. It is also easy to check that that $k_2 > k_1$ implies (31).

We turn to the proof that $G(\mathfrak{T}) = G(\mathfrak{T}')$. First suppose that $a > l_2 + 1$. We note that our assumptions imply that $a' > l_1 + 1$. Assuming (31) we must show that

$$\begin{aligned} g(p^{a-b-1}, p^{c-b})\; g(p^{l_2}, p^b)\, g(p^{l_1+b}, p^{a+b-l_2-1}) &= \\ g(p^{c-2a+l_1+2l_2+2}, p^b)\, g(p^{l_1}, p^{a-l_2-1})\, g(p^{a-1}, p^c). & \end{aligned}$$

Since we are assuming $l_2 \geqslant b$ and $c - 2a + 2l_1 + l_2 + 2 \geqslant b$ both sides vanish unless $n|b$. We therefore assume $n|b$. Since

$$g(p^{l_2}, p^b) = g(p^b, p^b) = g(p^{c-2a+2l_1+l_2+2}, p^b) \tag{32}$$

so we must show that

$$g(p^{a-b-1}, p^{c-b})\, g(p^{l_1+b}, p^{a+b-l_2-1}) = g(p^{a-1}, p^c) g(p^{l_1}, p^{a-l_2-1})\,.$$

This follows since $n|b$ implies that

$$g(p^{a-1}, p^c) = \mathbb{N}p^b\, g(p^{a-b-1}, p^{c-b}) \tag{33}$$

and

$$g(p^{l_2+b}, p^{a+b-l_1-1}) = \mathbb{N}p^b\, g(p^{l_2}, p^{a-l_1-1}).$$

If $a = l_2 + 1$ then what we must show is that

$$\begin{aligned} \mathbb{N}p^b\, g(p^{a-b-1}, p^{c-b})\; g(p^{l_2}, p^b) &= \\ g(p^{c-2a+l_1+2l_2+2}, p^b)\, g(p^{l_1}, p^{a-l_2-1})\, g(p^{a-1}, p^c). & \end{aligned}$$

Again both sides vanish unless $n|b$, which we assume, and proceeding as before, the statement now follows from (32) and (33), together with the fact that $g(p^{l_1}, p^{a-l_2-1}) = 1$. $\square$

Lemma 4 gives a bijection $\Upsilon(k_1, k_2; l_1, l_2) \longrightarrow \Upsilon(k_2, k_1; l_2, l_1)$ when $k_2 > k_1$; since the bijection preserves $G(\mathfrak{T})$, this means that the right-hand side of (30) satisfies

$$H'(p^{k_1}, p^{k_2}; p^{l_1}, p^{l_2}) = H'(p^{k_2}, p^{k_1}; p^{l_2}, p^{l_1})$$

when $k_2 > k_1$; on the other hand it is evident from the definition that

$$H(p^{k_1}, p^{k_2}; p^{l_1}, p^{l_2}) = H(p^{k_2}, p^{k_1}; p^{l_2}, p^{l_1}) \tag{34}$$

for all k_1 and k_2. Hence we are reduced to proving the Theorem when $k_1 \geqslant k_2$.

Lemma 5 *If $k_1 > k_2$, then*

$$H(p^{k_1}, p^{k_2}; p^{l_1}, p^{l_2}) = \sum_{i=\max(0,k_2-l_2-1)}^{\min(k_2,k_2-k_1+l_1+1)} g(p^i, p^i)\; g(p^{l_2}, p^{k_2-i})\; g(p^{l_1+k_2-i}, p^{k_1}).$$

Proof We note that since $g(p^a, p^b) = 0$ if $a < b-1$, the statement is equivalent to

$$H(p^{k_1}, p^{k_2}; p^{l_1}, p^{l_2}) = \sum_{i=0}^{k_2} g(p^i, p^i)\; g(p^{l_2}, p^{k_2-i})\; g(p^{l_1+k_2-i}, p^{k_1}) \tag{35}$$

since any terms in this sum with $i < k_2 - l_2 - 1$ or $i > k_2 - k_1 + l_1 + 1$ contribute zero. We prove (35).

In the definition of H, we have $r_1 r_2 = p^{k_2}$ and we can take $C_1' = p^{k_1-k_2}$, $C_2' = 1$. Thus

$$H(p^{k_1}, p^{k_2}; p^{l_1}, p^{l_2}) = \sum_{\substack{A_1, B_1 \bmod p^{k_1} \\ A_2, B_2 \bmod p^{k_2} \\ \gcd(A_1, B_1, p) = \gcd(A_2, B_2, p) = 1 \\ A_1 p^{k_2} + B_1 B_2 + A_2 p^{k_1} \equiv 0 \bmod p^{k_1+k_2}}} \left(\frac{B_1'}{p^{k_1-k_2}}\right) \left(\frac{A_1}{r_1}\right) \left(\frac{A_2}{r_2}\right) \psi\left(\frac{B_1 p^{l_1}}{p^{k_1}} + \frac{B_2 p^{l_2}}{p^{k_2}}\right). \tag{36}$$

It is understood that A_1, A_2, B_1 and B_2 are always chosen to be divisible by the conductor $\mathfrak{f}$; we will omit this condition from all summations since it really plays no role in the computation. We break the sum up into 3 pieces: (1) $\gcd(B_2, p) = 1$, (2) p^i exactly divides B_2 with $1 \leqslant i < k_2$, and (3) $p^{k_2} | B_2$.

First we consider the contribution where $\gcd(B_2, p) = 1$. Here $r_2 = 1$, $r_1 = p^{k_2}$, and from the Plücker relation, $B_1 \equiv 0 \mod p^{k_2}$. After replacing B_1 by $p^{k_2} B_2'$ and dropping the prime, we get

$$\sum_{\substack{A_1 \bmod p^{k_1},\ B_1 \bmod p^{k_1-k_2} \\ A_2, B_2 \bmod p^{k_2} \\ \gcd(B_2, p) = \gcd(A_1, p) = 1 \\ A_1 + B_1 B_2 + A_2 p^{k_1-k_2} \equiv 0 \bmod p^{k_1}}} \left(\frac{B_1}{p^{k_1-k_2}}\right) \left(\frac{A_1}{p^{k_2}}\right) \psi\left(\frac{B_1 p^{l_1}}{p^{k_1-k_2}} + \frac{B_2 p^{l_2}}{p^{k_2}}\right). \tag{37}$$

We may use the Plücker relation to determine A_1. The sum becomes

$$\sum_{\substack{B_1 \bmod p^{k_1-k_2} \\ A_2, B_2 \bmod p^{k_2} \\ \gcd(B_2, p) = \gcd(A_2 p^{k_1-k_2} + B_1 B_2, p) = 1}} \left(\frac{B_1}{p^{k_1-k_2}}\right) \left(\frac{A_2 p^{k_1-k_2} + B_1 B_2}{p^{k_2}}\right) \psi\left(\frac{B_1 p^{l_1}}{p^{k_1-k_2}} + \frac{B_2 p^{l_2}}{p^{k_2}}\right).$$

Since $k_1 > k_2$ we may replace the condition $\gcd(A_2 p^{k_1-k_2} + B_1 B_2, p) = 1$ by just $\gcd(B_1, p) = 1$, and we also have $\left(\frac{A_2 p^{k_1-k_2} + B_1 B_2}{p^{k_2}}\right) = \left(\frac{B_1 B_2}{p^{k_2}}\right)$. The summand is independent of A_2, and we may drop this summation to obtain

$$\mathbb{N}p^{k_2} \sum_{\substack{B_1 \bmod p^{k_1-k_2} \\ B_2 \bmod p^{k_2} \\ \gcd(B_1 B_2, p) = 1}} \left(\frac{B_1}{p^{k_1}}\right) \left(\frac{B_2}{p^{k_2}}\right) \psi\left(\frac{B_1 p^{l_1}}{p^{k_1-k_2}} + \frac{B_2 p^{l_2}}{p^{k_2}}\right).$$

Now we may drop the leading factor of $\mathbb{N}p^{k_2}$ by summing B_2 over p^{k_1} instead of $p^{k_1-k_2}$. Hence we obtain

$$g(p^{l_2},p^{k_2})\,g(p^{l_1+k_2},p^{k_1}).$$

This is the contribution $i=0$ in (35).

Next, we have the contributions where p^i exactly divides B_2 for some i, $1\leqslant i<k_2$. Note that $B_1\equiv 0 \mod p^{k_2-i}$. We have $r_2=p^i$, $r_1=p^{k_1-i}$. After writing $B_1=p^{k_2-i}B_1'$, $B_2=p^iB_2'$ and dropping the primes from the notation, the sum becomes

$$\sum_{\substack{A_1 \bmod p^{k_1},\ B_1 \bmod p^{k_1-k_2+i}\\ A_2 \bmod p^{k_2},\ B_2 \bmod p^{k_2-i}\\ \gcd(A_1,p)=\gcd(B_2,p)=\gcd(A_2,p)=1\\ A_1+B_1B_2+A_2p^{k_1-k_2}\equiv 0 \bmod p^{k_1}}} \left(\frac{B_1}{p^{k_1-k_2}}\right)\left(\frac{A_1}{p^{k_2-i}}\right)\left(\frac{A_2}{p^i}\right)\psi\left(\frac{B_1p^{l_1}}{p^{k_1-k_2+i}}+\frac{B_2p^{l_2}}{p^{k_2-i}}\right). \tag{38}$$

Next we use the Plücker relation to eliminate A_1. The sum is

$$\sum_{\substack{B_1 \bmod p^{k_1-k_2+i}\\ A_2 \bmod p^{k_2},\ B_2 \bmod p^{k_2-i}\\ \gcd(B_2,p)=\gcd(A_2,p)=1\\ \gcd(B_1B_2,p)=1}} \left(\frac{B_1}{p^{k_1-k_2}}\right)\left(\frac{B_1B_2}{p^{k_2-i}}\right)\left(\frac{A_2}{p^i}\right)\psi\left(\frac{B_1p^{l_1}}{p^{k_1-k_2+i}}+\frac{B_2p^{l_2}}{p^{k_2-i}}\right).$$

The A_2 sum gives zero unless $n|i$; since the i contribution in (35) is also zero unless $n|i$ due to the factor $g(p^i,p^i)$, we may now assume that $n|i$. The A_2 sum produces $\phi(p^{k_2})=\mathbb{N}p^{k_2-i}\,g(p^i,p^i)$ and the B_2 sum produces $g(p^{l_2},p^{k_2-i})$. We obtain

$$\mathbb{N}p^{k_2-i}\,g(p^i,p^i)\,g(p^{l_2},p^{k_2-i})\sum_{B_1 \bmod p^{k_1-k_2+i}}\left(\frac{B_1}{p^{k_1-i}}\right)\psi\left(\frac{B_1p^{l_1}}{p^{k_1-k_2+i}}\right).$$

We can absorb the $\mathbb{N}p^{k_2-i}$ into the summation by extending the summation to the larger modulus p^{k_1}. Since $n|i$, we may also write $\left(\frac{B_1}{p^{k_1-i}}\right)=\left(\frac{B_1}{p^{k_1}}\right)$ and obtain the i-th term in (35).

Finally, we have the contribution when $p^{k_2}|B_2$. We have $r_1=1$ and $r_2=p^{k_2}$. We may take $B_2=0$ in the sum. We obtain

$$\sum_{\substack{A_1,B_1 \bmod p^{k_1}\\ A_2 \bmod p^{k_2}\\ \gcd(A_1,B_1,p)=\gcd(A_2,p)=1\\ A_1+p^{k_1-k_2}A_2\equiv 0 \bmod p^{k_1}}} \left(\frac{B_1}{p^{k_1-k_2}}\right)\left(\frac{A_2}{p^{k_2}}\right)\psi\left(\frac{B_1p^{l_1}}{p^{k_1}}\right). \tag{39}$$

We may use the Plücker relation to eliminate A_1, which is divisible by p. The sum is therefore

$$\sum_{\substack{B_1 \bmod p^{k_1}\\ A_2 \bmod p^{k_2}\\ \gcd(B_1,p)=\gcd(A_2,p)=1}} \left(\frac{B_1}{p^{k_1-k_2}}\right)\left(\frac{A_2}{p^{k_2}}\right)\psi\left(\frac{B_1p^{l_1}}{p^{k_1}}\right) =$$

$$g(p^{k_2},p^{k_2})\sum_{\substack{B_1 \bmod p^{k_1}\\ \gcd(B_1,p)=1}}\left(\frac{B_1}{p^{k_1-k_2}}\right)\psi\left(\frac{B_1p^{l_1}}{p^{k_1}}\right).$$

Note that $g(p^{k_2},p^{k_2})=0$ unless $n|k_2$, in which case $\left(\frac{B_1}{p^{k_1-k_2}}\right)=\left(\frac{B_1}{p^{k_1}}\right)$. Hence this contribution is $g(p^{k_2},p^{k_2})\,g(p^{l_1},p^{k_1})$, which is the contribution of $i=k_2$ in (35). $\square$

Now suppose that $k_1>k_2$. Then given an integer i we consider

$$\mathfrak{T}=\left\{\begin{array}{ccccc} l_1+l_2+2 & & l_2+1 & & 0\\ & a & & b & \\ & & c & & \end{array}\right\},\qquad \begin{array}{l} a=k_1-k_2+i+l_2+1,\\ b=k_2-i,\\ c=k_2.\end{array}$$

A necessary and sufficient condition for this to be a Gelfand-Tsetlin pattern is that

$$\max(0,k_2-l_2-1)\leqslant i\leqslant\min(k_2,k_2+l_1+1-k_1).$$

This gives a complete enumeration of $\Upsilon(k_1,k_2;l_1,l_2)$. We have $a-b-1\geqslant c-b$ and so

$$\begin{aligned} G(\mathfrak{T})=g(p^{c-b},p^{c-b})\;g(p^{l_2},p^b)\,g(p^{l_1+b},p^{a+b-l_2-1}) &= \\ g(p^i,p^i)\;g(p^{l_2},p^{k_2-i})\;g(p^{l_1+k_2-i},p^{k_1}). \end{aligned}$$

In this case, the result now follows from Lemma 5.

It remains for us to handle the case $k_1=k_2$.

Lemma 6 *We have*

$$\begin{aligned} H(p^k,p^k;p^{l_1},p^{l_2}) &= \\ \sum_{i=\max(0,k-l_1-1)}^{\min(k-1,l_2+1)} g(p^{l_2},p^i)\;g(p^{l_1+i},p^k)\;g(p^{l_2+k-2i},p^{k-i}) & \\ +\left\{\begin{array}{ll} \mathbb{N}p^k\,g(p^k,p^k) & \textit{if } k\leqslant l_2;\\ 0 & \textit{if } k>l_2. \end{array}\right. & \end{aligned}$$

Proof As in the proof of Lemma 5 we may replace the range of summation with $\sum_{i=0}^{k-1}$since the fact that $g(p^a,p^b)=0$ when $a<b-1$ implies that any additional terms are zero. Now using (34) it is equivalent to prove

$$\begin{aligned} H(p^k,p^k;p^{l_1},p^{l_2}) &= \\ \sum_{i=0}^{k-1} g(p^{l_1},p^i)\;g(p^{l_2+i},p^k)\;g(p^{l_1+k-2i},p^{k-i}) & \\ +\left\{\begin{array}{ll} \mathbb{N}p^k\,g(p^k,p^k) & \text{if } k\leqslant l_1;\\ 0 & \text{if } k>l_1, \end{array}\right. & \end{aligned}\tag{40}$$

which has the advantage that we may reuse parts of the proof of Lemma 5. It is possible that $l_1+k-2i<0$ but if this occurs the meaning of $g(p^{l_1+k-2i},p^{k-i})$ can be assigned arbitrarily since then $i>l_1+1$, and the first Gauss sum will be zero.

We start with (36) and break the sum up as in Lemma 5.

First let us consider the contribution when $\gcd(B_2,p)=1$. This is still given by (37). Since B_1 is chosen modulo 1 it is arbitrary, and we take $B_1=p$. We may omit the summation over A_2 since it is determined by A_1 and B_2. We obtain

$$\sum_{\substack{A_1 \bmod p^k \\ B_2 \bmod p^{k_2} \\ \gcd(B_2,p)=\gcd(A_1,p)=1}} \left(\frac{A_1}{p^k}\right) \psi\left(\frac{B_2 p^{l_2}}{p^k}\right).$$

The A_1 summation produces $g(p^k,p^k) = g(p^{l_1+k},p^k)$, which is zero unless $n|k$. Assuming this the B_2 sum gives $g(p^{l_2},p^k)$ and we get the $i=0$ contribution in (40).

Next let us consider the contribution when $p^i \| B_2$ with $0 < i \leqslant k-1$. This is given by (38). We can use the Plücker relation to eliminate A_1. Moreover, we can extend the summations of B_1 and B_2 to the larger modulus p^k, dividing by $\mathbb{N}p^{-k}$ to compensate for overcounting. We obtain

$$\mathbb{N}p^{-k} \sum_{\substack{B_1 \bmod p^k \\ A_2, B_2 \bmod p^k \\ \gcd(B_2,p)=\gcd(A_2,p)=1 \\ \gcd(B_1B_2+A_2,p)=1}} \left(\frac{A_2+B_1B_2}{p^{k-i}}\right)\left(\frac{A_2}{p^i}\right) \psi\left(\frac{B_1 p^{l_1}}{p^i} + \frac{B_2 p^{l_2}}{p^{k-i}}\right).$$

We make the variable change $B_1 \longmapsto B_2^{-1}(B_1 - A_2)$, where the inverse is modulo p^k. This produces

$$\mathbb{N}p^{-k} \sum_{\substack{B_1 \bmod p^k \\ A_2, B_2 \bmod p^k \\ \gcd(B_2,p)=\gcd(A_2,p)=1 \\ \gcd(B_1,p)=1}} \left(\frac{B_1}{p^{k-i}}\right)\left(\frac{A_2}{p^i}\right) \psi\left(\frac{B_2^{-1}(B_1-A_2) p^{l_1}}{p^i} + \frac{B_2 p^{l_2}}{p^{k-i}}\right).$$

Next we replace B_1 and A_2 by B_1B_2 and A_2B_2, respectively to get

$$\mathbb{N}p^{-k} \sum_{\substack{B_1 \bmod p^k \\ A_2, B_2 \bmod p^k \\ \gcd(B_2,p)=\gcd(A_2,p)=1 \\ \gcd(B_1,p)=1}} \left(\frac{B_1}{p^{k-i}}\right)\left(\frac{A_2}{p^i}\right)\left(\frac{B_2}{p^k}\right) \psi\left(\frac{(B_1-A_2) p^{l_1}}{p^i} + \frac{B_2 p^{l_2}}{p^{k-i}}\right).$$

The B_2 sum produces $g(p^{l_2+i},p^k)$, and the A_2 sum gives $\mathbb{N}p^{k-i} g(p^{l_1},p^i)$. Thus we arrive at

$$\mathbb{N}p^{-i}\, g(p^{l_2+i},p^k)\, \mathbb{N}p^{k-i} g(p^{l_1},p^i) \sum_{\substack{B_1 \bmod p^k \\ \gcd(B_1,p)=1}} \left(\frac{B_1}{p^{k-i}}\right) \psi\left(\frac{B_1 p^{l_1}}{p^i}\right).$$

But $g(p^{l_1},p^i)$ is nonzero only when $i \leqslant l_1+1$. In this case $l_2+k-2i > 0$ and

$$\mathbb{N}p^{-i} \sum_{\substack{B_1 \bmod p^k \\ \gcd(B_1,p)=1}} \left(\frac{B_1}{p^{k-i}}\right) \psi\left(\frac{B_1 p^{l_1}}{p^i}\right) = g(p^{l_2+k-2i},p^{k-i}).$$

Thus we arrive at the contribution $g(p^{l_1},p^i)\, g(p^{l_2+i},p^k)\, g(p^{l_1+k-2i},p^{k-i})$.

It remains for us to discuss the contribution when $p^k|B_2$. We start with (39). The A_1 sum is irrelevant since $A_1 \equiv -A_2$ modulo p^k. As $p \nmid A_2$, this implies that the condition $\gcd(A_1, B_1, p) = 1$ may also be dropped. Now the summation over B_1 produces a factor of p^k if $k \leqslant l_1$, and zero otherwise; and the summation over A_2 produces a factor of $g(p^k, p^k)$. $\square$

Assume that $k_1 = k_2 = k$. Given an integer i, consider

$$\mathfrak{T} = \left\{ \begin{array}{ccccc} l_1 + l_2 + 2 & & l_2 + 1 & & 0 \\ & a & & b & \\ & & c & & \end{array} \right\}, \qquad \begin{array}{l} a = k - i + l_2 + 1, \\ b = i, \\ c = k. \end{array}$$

A necessary and sufficient condition for this to be a Gelfand-Tsetlin pattern is that

$$\max(0, k - l_1 - 1) \leqslant i \leqslant \max(k, l_2 + 1),$$

and this gives a complete enumeration of $\Upsilon(k, k; l_1, l_2)$. We assume first that $i < k$. In this case we have

$$\begin{aligned} G(\mathfrak{T}) = g(p^{a-b-1}, p^{c-b})\ g(p^{l_2}, p^b)\, g(p^{l_1+b}, p^{a+b-l_2-1}) \\ g(p^{l_2+k-2i}, p^{k-i})\, g(p^{l_2}, p^i)\, g(p^{l_1+i}, p^k), \end{aligned}$$

and these terms account for the first summation in Lemma 6. If $k \leqslant l_2 + 1$ there is one more term with $i = k$. Using (29), this accounts for the last term in Lemma 6, and the Theorem is proved. $\square$

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} $(n \geq 2)$. *Inst. Hautes Études Sci. Publ. Math.*, (33):59–137, 1967.

[2] B. Brubaker, D. Bump, S. Friedberg, and J. Hoffstein. Weyl group multiple Dirichlet series III: Twisted unstable A_r.

[3] D. Bump. *Automorphic forms on* $\mathrm{GL}(3, R)$, volume 1083 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1984.

[4] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.