IRREDUCIBLE SPACES OF MODULAR UNITS

DAVID E. ROHRLICH

Fix a prime $p \geqslant 7$, put $G = \mathrm{PSL}(2, \mathbb{F}_p)$, and write U for the multiplicative group of modular units of level p. We shall determine the irreducible subspaces of the natural representation of G on U/U^p. The outcome of the calculation can be described as follows: Every irreducible nontrivial representation of G over $\mathbb{F}_p$ occurs with multiplicity one in the maximal semisimple subspace of the "noncongruence part" of U/U^p (to be defined). Apart from the formulation and some slight differences arising from the choice of group ($\mathrm{PSL}(2, \mathbb{F}_p)$ instead of $\mathrm{GL}(2, \mathbb{F}_p)/\{\pm 1\}$), the result is already in Gross [2]. Presumably one can give conditions as in [6] and [7] which ensure that the unit group remains large after descent and specialization to a number field, but this problem will not be addressed here.

For the sake of perspective, it is useful to recall that the natural representation of G on the space of modular forms of weight 2 and level p was decomposed into irreducibles in two papers of Hecke [3], [4]. As one would expect, most of the work in these papers goes into decomposing the space of cusp forms, but it is actually the space of Eisenstein series – dealt with by Hecke in a few lines – which has some bearing on the present note. The reason is simple: if $f \in U$ then $(d \log f)/dz$ is an Eisenstein series of weight 2 and level p. In fact the space of all such Eisenstein series is simply $\mathbb{C} \otimes_{\mathbb{Z}} (d \log U)/dz$. Furthermore, since the kernel of $f \mapsto (d \log f)/dz$ is the subgroup of constant functions $\mathbb{C}^\times \subset U^p$, we see that U/U^p is isomorphic as an $\mathbb{F}_p[G]$-module to $\mathbb{F}_p \otimes_{\mathbb{Z}} (d \log U)/dz$. Thus the representation of G on U/U^p arises via tensor product with $\mathbb{F}_p$ from a G-stable $\mathbb{Z}$-form of the space of Eisenstein series. It follows that the semisimplification of U/U^p can be computed directly from Hecke's decomposition of the space of Eisenstein series into irreducibles.

But the structure of U/U^p itself is another matter. To determine whether a given irreducible constituent of U/U^p actually occurs as a subspace we must turn to the work of Kubert and Lang [5], which reduces the problem to an elementary exercise. The present note is nothing more than a solution to the exercise: but however trite, it is nonetheless a heartfelt acknowledgment of an enormous personal debt to Serge Lang. I would also like to acknowledge the help provided by the referee of [7], whose suggestion for simplifying the proof of Proposition 7 of [7] turned out to be an essential ingredient of the present work.

1. The module of parameters

The $\mathbb{Z}[G]$-module M introduced below is a first approximation to the domain of the Kubert-Lang map parametrizing U. Our goal is to decompose the associated representation of G on the vector space $V = M/pM$ over $\mathbb{F}_p$.

1.1. Preliminaries. The irreducible representations of G in characteristic p can be classified using a single invariant: their dimension. Indeed for each integer k satisfying $0 \leqslant k \leqslant (p-1)/2$ there is an absolutely irreducible representation σ_k of G over $\mathbb{F}_p$ of dimension $2k+1$, and σ_k is unique up to isomorphism. Furthermore every irreducible representations of G in characteristic p is isomorphic to some σ_k. In order to work with an explicit model we shall take σ_k to be the $(2k)$th symmetric power of the tautological two-dimensional projective representation of G. Then the space of σ_k consists of binary homogeneous polynomials $f(x, y)$ of degree $2k$ over $\mathbb{F}_p$, and the action of G is given by the formula

$$(\sigma_k(g)f)(x, y) = f(ax + cy, bx + dy), \tag{1}$$

where g is the image in G of the element

$$\tilde{g} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{2}$$

of $\mathrm{SL}(2, \mathbb{F}_p)$.

Put $R = \mathbb{F}_p^2 \smallsetminus \{(0, 0)\}$. We define M to be the free $\mathbb{Z}$-module of rank $(p^2 - 1)/2$ consisting of functions $m : R \to \mathbb{Z}$ such that $m(-r) = m(r)$ for $r \in R$. An action of G on M is given by the formula

$$(g \cdot m)(r) = m(r\tilde{g}), \tag{3}$$

where $\tilde{g}$ is either of the two lifts of g to $\mathrm{SL}(2, \mathbb{F}_p)$ and $r\tilde{g}$ is the product of the 1×2 row vector r and the matrix $\tilde{g}$. Of course this action is formally the same as (1), except that m is now an even function $R \to \mathbb{Z}$ rather than a homogeneous polynomial over $\mathbb{F}_p$.

Given a field F, put $V_F = F \otimes_{\mathbb{Z}} M$ and extend the action (3) by linearity to a representation τ_F of G on V_F. We can identify V_F with the vector space of dimension $(p^2 - 1)/2$ over F consisting of even functions $m : R \to F$, and then the action of G is again formally the same as in (1) and (3). We are primarily interested in the case $F = \mathbb{F}_p$, and in this case we write V_F and τ_F simply as V and τ.

1.2. Irreducible constituents. Write B for the image in G of the upper triangular subgroup of $\mathrm{SL}(2, \mathbb{F}_p)$ and $N \subset B$ for the image of the strictly upper triangular subgroup (i. e. the subgroup defined by the conditions $c = 0$, $a = d = 1$ in (2)). We denote the trivial one-dimensional character of any group by 1, leaving both the group and the implicit field of scalars to be inferred from context. In the following proposition, for example, 1 is the trivial one-dimensional character of N with values in F, and $\mathrm{ind}_N^G 1$ is the representation of G over F which it induces.

Proposition 1. $\tau_F \cong \mathrm{ind}_N^G 1$.

Proof. Take the space of $\mathrm{ind}_N^G 1$ to consist of functions $f : G \to F$ satisfying $f(ng) = f(g)$ for $n \in N$ and $g \in G$, with G acting by right translation. As we have already noted, V_F is also a space of functions, namely the space of even functions $m : R \to F$. Furthermore, given f in the space of $\mathrm{ind}_N^G 1$ we obtain an element $m_f \in V_F$ by setting $m_f(r) = f(g)$ if $e\tilde{g} = \pm r$, where e is the row vector $(0, 1) \in R$. The map $f \mapsto m_f$ is redily verified to be G-equivariant and injective, and its domain and range both have dimension $(p^2 - 1)/2$. □

We now take $F = \mathbb{F}_p$ and compute the semisimplification of τ:

Proposition 2. *The multiplicity of σ_k as a constituent of τ is* 1 *if $k = 0$ or $k = (p - 1)/2$ and* 2 *if $1 \leqslant k \leqslant (p - 3)/2$.*

Proof. Given $t \in \mathbb{F}_p^\times$, let $a(t)$ denote the image in B of the diagonal matrix with diagonal entries t, t^{-1}. The map $t \mapsto a(t)$ induces an isomorphism of quotient groups $\mathbb{F}_p^\times/\{\pm 1\} \cong B/N$, and we can compose the inverse of this isomorphism with even powers of the Teichmüller character $\omega : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ to obtain characters of B. More precisely, we define $\xi_k : B \to \mathbb{Q}_p^\times$ $(0 \leqslant k \leqslant (p-3)/2)$ by setting

$$\xi_k(a(t)n) = \omega(t)^{2k} \qquad (t \in \mathbb{F}_p^\times,\ \ n \in N).$$

Then $\mathrm{ind}_N^B 1 \cong \oplus_{k=0}^{(p-3)/2} \xi_k$, whence Proposition 1 and the identification $\mathrm{ind}_N^G 1 = \mathrm{ind}_B^G(\mathrm{ind}_N^B 1)$ give

$$\tau_{\mathbb{Q}_p} \cong \oplus_{k=0}^{(p-3)/2} \pi_k \tag{4}$$

with $\pi_k = \mathrm{ind}_B^G \xi_k$ (cf. formula (22) of [3]). We remark that $\pi_0 \cong 1 \oplus \eta$ with an absolutely irreducible representation η of dimension p over $\mathbb{Q}_p$, while if $p \equiv 1 \bmod 4$ then $\pi_{(p-1)/4}$ decomposes over $\overline{\mathbb{Q}}_p$ as the direct sum of two inequivalent irreducible representations ζ and ζ' of dimension $(p+1)/2$. Apart from these exceptions, the direct summands in (4) are absolutely irreducible (although not distinct, as $\pi_k \cong \pi_{(p-1-2k)/2}$ for $1 \leqslant k \leqslant (p-3)/2$).

Put $\mathcal{M} = \mathbb{Z}_p \otimes_{\mathbb{Z}} M$. Then $\mathcal{M}$ is a G-stable $\mathbb{Z}_p$-lattice in $V_{\mathbb{Q}_p}$ and $V = \mathbb{F}_p \otimes \mathcal{M}$. Hence the semisimplification of V can be read from (4) and the mod-p decomposition numbers of G. These decomposition numbers are implicit in Brauer-Nesbitt [1] (p. 590) and explicitly computed in Srinivasan [8] (pp. 107 − 108). In applying [8], note that for $n = 1$ her $\Phi(r_0)$ and $\varphi(r_0)$ coincide. Hence taking $r_0 = 2k$ in formula (3.5) of [8], we find that the character of our π_k coincides on p-regular conjugacy classes with the sum of the Brauer characters of our σ_k and $\sigma_{(p-1-2k)/2}$. In the first instance this conclusion holds only when $1 \leqslant k \leqslant (p-3)/2$ and $k \neq (p-1)/4$, but in fact it holds also when $k = 0$ (by the first three lines on p. 108 of [8]) and when $k = (p-1)/4$ (by formula (3.7) of [8]). The upshot is that in all cases, the semisimplification of the reduction modulo p of π_k coincides with $\sigma_k \oplus \sigma_{(p-1-2k)/2}$. Hence the proposition follows from (4). □

1.3. Irreducible subspaces and quotient spaces. Next we determine the multiplicity of σ_k as a quotient representation of τ. Given representations α and β of a group H on vector spaces W_α and W_β over a field F, write $\mathrm{Hom}_{F[H]}(\alpha, \beta)$ for $\mathrm{Hom}_{F[H]}(W_\alpha, W_\beta)$.

Proposition 3. *For $0 \leqslant k \leqslant (p-1)/2$,*

$$\dim_{\mathbb{F}_p} \mathrm{Hom}_{\mathbb{F}_p[G]}(\tau, \sigma_k) = 1.$$

Proof. Proposition 1 and Frobenius reciprocity give

$$\mathrm{Hom}_{\mathbb{F}_p[G]}(\tau, \sigma_k) \cong \mathrm{Hom}_{\mathbb{F}_p[N]}(1, \mathrm{res}_N^G \sigma_k).$$

Now N is generated by the element u corresponding to the choices $a = b = d = 1$ and $c = 0$ in (2), so it suffices to see that the subspace of vectors fixed by $\sigma_k(u)$ is one-dimensional. Let A be the matrix of $\sigma_k(u)$ relative to the ordered basis $x^{2k}, x^{2k-1}y, \ldots, y^{2k}$, and let a_{ij} be the (i,j)-entry of A for $1 \leqslant i, j \leqslant 2k+1$. Using (1) to write $(\sigma_k(u)f)(x,y) = f(x, x+y)$, one readily verifies that A is upper triangular, that $a_{ii} = 1$ for all i, and that $a_{i,i+1} \neq 0$ for $1 \leqslant i \leqslant k$. It follows that the Jordan normal form of A consists of a single Jordan block, whence x^{2k} is the unique eigenvector of $\sigma_k(u)$ up to scalar multiples. □

A similar statement holds for subrepresentations:

Proposition 4. *For $0 \leqslant k \leqslant (p-1)/2$,*

$$\dim_{\mathbb{F}_p} \operatorname{Hom}_{\mathbb{F}_p[G]}(\sigma_k, \tau) = 1.$$

Proof. In view of Proposition 3 it suffices to see that both σ_k and τ are self-dual. The self-duality of σ_k follows from the fact that irreducible representations of G over $\mathbb{F}_p$ are determined up to isomorphism by their dimension. The self-duality of τ follows from the fact that the symmetric bilinear form

$$\langle m, m' \rangle = \sum_{r \in R'} m(r) m'(r) \qquad (m, m' \in V) \tag{5}$$

is nondegenerate and G-invariant. □

1.4. Homogeneous components. Recall that $\mathcal{M} = \mathbb{Z}_p \otimes_{\mathbb{Z}} M$ and that $\omega : \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ is the Teichmüller character. We shall view the elements of $\mathcal{M}$ as even functions $m : R \to \mathbb{Z}_p$. We define $\mathcal{M}^{(k)}$ to be the $\mathbb{Z}_p$-submodule of $\mathcal{M}$ consisting of those m such that

$$m(tr) = \omega(t)^{2k} m(r)$$

for $t \in \mathbb{F}_p^\times$ and $r = (r_1, r_2) \in R$, where $tr = (tr_1, tr_2)$. The linear operators $e^{(k)} : \mathcal{M} \to \mathcal{M}$ given by

$$(e^{(k)} m)(r) = \frac{1}{p-1} \sum_{t \in \mathbb{F}_p^\times} \omega^{-(k)}(t) m(tr) \tag{6}$$

$(0 \leqslant k \leqslant (p-3)/2)$ form a family of orthogonal idempotents projecting $\mathcal{M}$ onto the respective submodules $\mathcal{M}^{(k)}$ and summing to the identity, so we have

$$\mathcal{M} = \oplus_{k=0}^{(p-3)/2} \mathcal{M}^{(k)}. \tag{7}$$

In fact (7) is a decomposition into $\mathbb{Z}_p[G]$-submodules, because the idempotents $e^{(k)}$ commute with the action of G. Hence the space of τ likewise decomposes into G-stable subspaces:

$$V = \oplus_{k=0}^{(p-3)/2} V^{(k)} \tag{8}$$

with $V^{(k)} = \mathbb{F}_p \otimes_{\mathbb{Z}_p} \mathcal{M}^{(k)}$. Let $\tau^{(k)}$ denote the representation of G on $V^{(k)}$.

Proposition 5. *If $1 \leqslant k \leqslant (p-3)/2$ then $\tau^{(k)}$ has a unique irreducible subrepresentation and a unique irreducible quotient representation, and they are equivalent to σ_k and $\sigma_{(p-1-2k)/2}$ respectively. On the other hand, $\tau^{(0)} \cong \sigma_0 \oplus \sigma_{(p-1)/2}$.*

Proof. The first point is that the free $\mathbb{Z}_p$-module $\mathcal{M}^{(k)}$ has rank $p+1$. Indeed for each of the $p+1$ lines ℓ through the origin in $\mathbb{F}_p^2$, fix an element $r_\ell \in R$ which spans ℓ, and define a function $f_{\ell,k} \in \mathcal{M}^{(k)}$ by

$$f_{\ell,k}(r) = \begin{cases} \omega(t)^{2k} & \text{if } r = tr_\ell \text{ with } t \in \mathbb{F}_p^\times \\ 0 & \text{if } r \notin \ell. \end{cases}$$

For fixed k the $p+1$ functions $f_{\ell,k}$ have pairwise disjoint supports and are therefore linearly independent over $\mathbb{Z}_p$. Hence $\mathcal{M}^{(k)}$ has rank at least $p+1$. But $\mathcal{M}$ has rank $(p+1)(p-1)/2$, so we deduce from (7) that $\mathcal{M}^{(k)}$ has rank exactly $p+1$, as claimed.

It follows that $V^{(k)}$ has dimension $p+1$ over $\mathbb{F}_p$. But an irreducible representation of G over $\mathbb{F}_p$ has dimension $\leqslant p$, so $V^{(k)}$ has a *proper* irreducible subspace and hence at least two irreducible constituents. On the other hand, V has exactly $p-1$ irreducible constituents (Proposition 2), so we deduce from (8) that $V^{(k)}$ has exactly two constituents.

To identify these constituents up to isomorphism, we introduce a $\mathbb{Z}[G]$-submodule $\mathcal{N}_k$ of $\mathcal{M}$ for $0 \leqslant k \leqslant (p-3)/2$. Given $m \in \mathcal{M}$, let $\overline{m} : R \to \mathbb{F}_p$ denote the reduction of m modulo p. We define $\mathcal{N}_k \subset \mathcal{M}$ to be the submodule consisting of all m such that $\overline{m}$ coincides with a binary homogeneous polynomial of degree $2k$ over $\mathbb{F}_p$. Strictly speaking, we should say "coincides with the function $R \to \mathbb{F}_p$ defined by" such a polynomial, but the distinction is moot: a homogeneous polynomial of degree $< p$ which vanishes on R is zero. Thus the map $m \mapsto \overline{m}$ determines an embedding of $\mathcal{N}_k/(\mathcal{N}_k \cap p\mathcal{M})$ into the space of σ_k. In fact this embedding is surjective and hence a G-isomorphism, because any even function $R \to \mathbb{F}_p$ can be lifted to an even function $R \to \mathbb{Z}_p$.

Now put $\mathcal{N}_k^{(l)} = e^{(l)}\mathcal{N}_k$ $(0 \leqslant l \leqslant (p-3)/2)$. It is readily verified that if $l \neq k$ then the image of $\mathcal{N}_k^{(l)}$ under $m \mapsto \overline{m}$ is $\{0\}$. On the other hand, we have just seen that the map $m \mapsto \overline{m}$ gives a G-isomorphism of $\mathcal{N}_k/(\mathcal{N}_k \cap p\mathcal{M})$ onto the space of σ_k. It follows that the domain of this G-isomorphism can be replaced by $\mathcal{N}_k^{(k)}/(\mathcal{N}_k^{(k)} \cap p\mathcal{M}^{(k)})$. But the latter can be viewed as a G-stable subspace $W^{(k)}$ of $V^{(k)}$, and the representation of G on $W^{(k)}$ is therefore equivalent to σ_k. Furthermore, we have seen that $V^{(k)}$ has exactly two irreducible constituents, so the quotient $V^{(k)}/W^{(k)}$ is also irreducible. Since its dimension is $(p+1)-(2k+1) = p-2k$, we deduce that the quotient representation is equivalent to $\sigma_{(p-1-2k)/2}$. In summary, the representation of G on $W^{(k)}$ and on $V^{(k)}/W^{(k)}$ is equivalent to σ_k and to $\sigma_{(p-1-2k)/2}$ respectively.

To see that $\tau^{(0)} \cong \sigma_0 \oplus \sigma_{(p-1)/2}$, we observe that the set of indices k satisfying $1 \leqslant k \leqslant (p-3)/2$ is stable under $k \mapsto (p-1-2k)/2$. It follows that σ_0 and $\sigma_{(p-1)/2}$ occur as constituents of $V^{(k)}$ if and only if $k = 0$. On the other hand, σ_0 and $\sigma_{(p-1)/2}$ occur not merely as constituents but as subrepresentations of τ (Proposition 4). It follows that they occur as subrepresentations of $\tau^{(0)}$, whence $\tau^{(0)} \cong \sigma_0 \oplus \sigma_{(p-1)/2}$.

Finally, suppose that $1 \leqslant k \leqslant (p-3)/2$. If W is an irreducible subspace of $V^{(k)}$ then the representation of G on W is equivalent to an irreducible constituent of $\tau^{(k)}$, hence either to σ_k or to $\sigma_{(p-1-2k)/2}$. But if $W \neq W^{(k)}$ then the first possibility is excluded, because σ_k occurs as a subrepresentation of τ with multiplicity one (Proposition 4). As for the second possibility, it coincides with the first (and is therefore excluded when $W \neq W^{(k)}$) if $k = (p-1)/4$. Otherwise it is excluded by Proposition 4 again, because $\sigma_{(p-1-2k)/2}$ already occurs as a subrepresentation of $\tau^{((p-1-2k)/2)}$, and the spaces $V^{((p-1-2k)/2)}$ and $V^{(k)}$ are linearly independent. We conclude that $W^{(k)}$ is the unique irreducible subspace of $V^{(k)}$, and since $V^{(k)}$ has just two irreducible constituents it follows that $V^{(k)}/W^{(k)}$ is the unique irreducible quotient. □

2. The quadratic relations

To move a step closer to U we turn from M to the $\mathbb{Z}[G]$-submodule Q of M defined by the "quadratic relations" of Kubert and Lang. As before, our primary concern is the representation of G on the associated vector space over $\mathbb{F}_p$, which is now the space $V' = Q/pQ$.

2.1. Preliminaries. To define Q, recall that given $m \in M$ we write $\overline{m} : R \to \mathbb{F}_p$ for the reduction of m modulo p. We will also let N denote the $\mathbb{Z}[G]$-submodule of M consisting of all n for which $\overline{n}$ has the form

$$\overline{n}(r) = ar_1^2 + br_1r_2 + cr_2^2 \tag{9}$$

with $a, b, c \in \mathbb{F}_p$, where $r = (r_1, r_2)$. Since N is a $\mathbb{Z}$-form of the $\mathbb{Z}_p[G]$-module previously denoted $\mathcal{N}_1$, it might be more logical to denote it N_1, but for simplicity we omit the subscript (and thereby void our previous convention that N is the subgroup of G corresponding to strictly upper triangular matrices). We define Q to consist of those $m \in M$ such that

$$\sum_{r \in R} \overline{m}(r)\overline{n}(r) = 0 \tag{10}$$

for all $n \in N$.

It is immediate from this description that Q contains pM. Thus M/Q is a quotient of the finite-dimensional vector space $V = M/pM$ over $\mathbb{F}_p$. In fact since Q is defined by the vanishing of three linearly independent linear forms on M/pM (namely those corresponding to the choices $(a, b, c) = (1, 0, 0)$, $(0, 1, 0)$, and $(0, 0, 1)$ in (9) and (10)) we see that M/Q has dimension three over $\mathbb{F}_p$. In particular Q has finite index in M, so by the Brauer-Nesbitt theorem, the representation τ' of G on the space $V' = Q/pQ$ has the same semisimplification as τ. In other words, Proposition 2 holds with τ replaced by τ'. However Proposition 5 must be modified slightly.

2.2. Homogeneous components, Put $\mathcal{Q} = \mathbb{Z}_p \otimes_{\mathbb{Z}} Q$. Then $\mathcal{Q}$ is stable under $e^{(k)}$ (cf. (6), (9), and (10)). Hence

$$\mathcal{Q} = \oplus_{k=0}^{(p-3)/2} \mathcal{Q}^{(k)}$$

with $\mathcal{Q}^{(k)} = e^{(k)}\mathcal{Q}$. Thus putting ${V'}^{(k)} = \mathcal{Q}^{(k)}/p\mathcal{Q}^{(k)}$ we have

$$V' = \oplus_{k=0}^{(p-3)/2} {V'}^{(k)}, \tag{11}$$

a decomposition of V' into G-stable subspaces. Let ${\tau'}^{(k)}$ denote the representation of G on ${V'}^{(k)}$.

Proposition 6. *If $1 \leqslant k \leqslant (p-5)/2$ then ${\tau'}^{(k)}$ has a unique irreducible subrepresentation and a unique irreducible quotient representation, and they are equivalent to σ_k and $\sigma_{(p-1-2k)/2}$ respectively. On the other hand, ${\tau'}^{(0)} \cong \sigma_0 \oplus \sigma_{(p-1)/2}$ and ${\tau'}^{((p-3)/2)} \cong \sigma_1 \oplus \sigma_{(p-3)/2}$.*

Proof. Suppose first that $k \neq (p-3)/2$. We claim that $\mathcal{M}^{(k)} \subset \mathcal{Q}$, whence $\mathcal{M}^{(k)} = \mathcal{Q}^{(k)}$. To see this, take $m \in \mathcal{M}^{(k)}$ and $n \in N$, and write

$$\sum_{r \in R} \overline{m}(r)\overline{n}(r) = \sum_{\ell \in \Lambda} \sum_{r \in R \cap \ell} \overline{m}(r)\overline{n}(r),$$

where Λ is the set of lines through the origin in $\mathbb{F}_p^2$. For each $\ell \in \Lambda$ choose a vector $r_\ell \in R$ spanning ℓ. Then the inner sum on the right-hand side can be written as a sum over $t \in \mathbb{F}_p^\times$, with $r = tr_\ell$. The homogeneity of $\overline{m}$ and $\overline{n}$ then gives

$$\sum_{r \in R} \overline{m}(r)\overline{n}(r) = \sum_{\ell \in \Lambda} \overline{m}(r_\ell)\overline{n}(r_\ell) \sum_{t \in \mathbb{F}_p^\times} t^{2k+2}.$$

Since $k \neq (p-3)/2$ the exponent of t on the right-hand side is $< p-1$ and consequently the inner sum is 0. Thus $\mathcal{M}^{(k)} \subset \mathcal{Q}$ and $\mathcal{M}^{(k)} = \mathcal{Q}^{(k)}$, as claimed.

It follows that if $k \neq (p-3)/2$ then ${\tau'}^{(k)} \cong \tau^{(k)}$, whence the assertions at hand reduce to those of Proposition 5. To handle the remaining case $k = (p-3)/2$, we recall that τ and τ' have isomorphic semisimplifications and are direct sums of their respective homogeneous components $\tau^{(k)}$ and ${\tau'}^{(k)}$. Since ${\tau'}^{(k)} \cong \tau^{(k)}$ for $k \neq (p-3)/2$, we deduce that the semisimplifictions of ${\tau'}^{((p-3)/2)}$ and $\tau^{((p-3)/2)}$ are likewise isomorphic. Thus by Proposition 5, ${\tau'}^{((p-3)/2)}$ has exactly two irreducible constituents, namely $\sigma_{(p-3)/2}$ and σ_1.

Now $\mathcal{M}$ and $\mathcal{Q}$ are also the direct sums of their homogeneous components $\mathcal{M}^{(k)}$ and $\mathcal{Q}^{(k)}$, and we have seen that the vector space $\mathcal{M}/\mathcal{Q} = M/Q$ has dimension three over $\mathbb{F}_p$ (cf. (9) and (10)) while $\mathcal{M}^{(k)} = \mathcal{Q}^{(k)}$ for $k \neq (p-3)/2$. Consequently $\mathcal{M}^{((p-3)/2)}/\mathcal{Q}^{((p-3)/2)}$ is also three-dimensional over $\mathbb{F}_p$, as is therefore the subspace $Y = p\mathcal{M}^{((p-3)/2)}/p\mathcal{Q}^{((p-3)/2)}$ of ${V'}^{((p-3)/2)}$. Since ${\tau'}^{((p-3)/2)}$ has just the two irreducible constituents σ_1 and $\sigma_{(p-3)/2}$ of dimensions 3 and $p-2$ respectively, we deduce that the representation of G on Y is σ_1. Thus σ_1 is a subrepresentation of ${\tau'}^{((p-3)/2)}$ and $\sigma_{(p-3)/2}$ is the corresponding quotient representation.

It remains to see that σ_1 is also a quotient representation of ${\tau'}^{((p-3)/2)}$, whence $\sigma_{(p-3)/2}$ is a subrepresentation and ${\tau'}^{((p-3)/2)} \cong \sigma_1 \oplus \sigma_{(p-3)/2}$. To this end, consider the bilinear pairing $\prec *, * \succ : Q \times N \to \mathbb{Z}$ given by

$$\prec m, n \succ = \frac{1}{p} \sum_{r \in R} m(r) n(r) \qquad\qquad (m \in Q, \quad n \in N).$$

Write L for the $\mathbb{Z}[G]$-submodule of Q consisting of those m such that

$$\prec m, n \succ \equiv 0 \pmod{p}$$

for all $n \in N$. Put $\mathcal{L} = \mathbb{Z}_p \otimes_{\mathbb{Z}} L$. Then $\mathcal{L}$ is stable under $e^{(k)}$, so putting $\mathcal{L}^{(k)} = e^{(k)}\mathcal{L}$ we have

$$\mathcal{L} = \oplus_{k=0}^{(p-3)/2} \mathcal{L}^{(k)}.$$

We claim that $\mathcal{L}^{((p-3)/2)}$ contains $p\mathcal{Q}^{((p-3)/2)}$ and that the quotient space $Z = \mathcal{Q}^{((p-3)/2)}/\mathcal{L}^{((p-3)/2)}$ of ${V'}^{(p-3)/2}$ is of positive dimension $\leqslant 3$. An immediate consequence of the claim is that the representation of G on Z is equivalent to σ_1, so verifying the claim will complete the proof.

It is immediate from the definitions that L contains pQ and hence that $\mathcal{L}$ contains $p\mathcal{Q}$. On the other hand, $\mathcal{L}$ does not contain $p\mathcal{M}$: for if $m \in M$ is the function taking the value 1 on $(\pm 1, 0)$ and 0 elsewhere then $\prec pm, n \succ \not\equiv 0 \bmod p$ for any $n \in N$ satisfying (9) with $a \neq 0$. It follows that for some k with $0 \leqslant k \leqslant (p-3)/2$ we have $p\mathcal{M}^{(k)} \not\subset \mathcal{L}^{(k)}$. But we have seen that $p\mathcal{Q} \subset \mathcal{L}$ and that $p\mathcal{Q}^{(k)} = p\mathcal{M}^{(k)}$ for $k \neq (p-3)/2$. Hence $\mathcal{L}^{((p-3)/2)}$ does not contain $p\mathcal{M}^{((p-3)/2)}$, and we deduce that $\mathcal{L}^{((p-3)/2)}/p\mathcal{Q}^{((p-3)/2)}$ is a subspace of ${V'}^{((p-3)/2)}$ of positive codimension. On the other hand, the codimension is $\leqslant 3$, because the subspace is defined by the vanishing of three linear forms on ${V'}^{((p-3)/2)}$ (namely the forms $m + p\mathcal{Q}^{((p-3)/2} \mapsto \prec m, n \succ$ with n as in (9) and $(a, b, c) = (1, 0, 0)$, $(0, 1, 0)$, and $(0, 0, 1)$). Our claim follows. $\square$

3. The Kubert-Lang map

Now let H denote the complex upper half-plane. Given a matrix $\tilde{\gamma} \in \mathrm{SL}(2,\mathbb{Z})$, we identify its image $\gamma \in \mathrm{PSL}(2,\mathbb{Z})$ with the fractional linear transformation of H defined by γ. Thus if f is a function on H and $\tilde{\gamma}$ is the right-hand side of (2) then $f \circ \gamma$ is the function $z \mapsto f((az+b)/(cz+d))$. As usual, $\Gamma(p)$ denotes the subgroup of $\mathrm{SL}(2,\mathbb{Z})$ defined by the conditions $a \equiv d \equiv 1$ and $b \equiv c \equiv 0 \bmod p$, and the group that we are denoting U – namely the multiplicative group of modular units of level p – consists of modular functions for $\Gamma(p)$ which are holomorphic and nowhere vanishing on H. We make U into a $\mathbb{Z}[G]$-module via the action

$$g \cdot f = f \circ \gamma^{-1} \qquad (g \in G, \ \ f \in U),$$

where $\gamma \in \mathrm{PSL}(2,\mathbb{Z})$ is any lift of g. The resulting representation of G on the vector space $V'' = U/U^p$ over $\mathbb{F}_p$ will be denoted τ''.

Given $a \in p^{-1}\mathbb{Z}^2$ with $a \neq (0,0)$, define the Siegel function g_a as in [5], p. 29. For $r \in R$ we put $f_r = g_a^{12}$, where $a \in p^{-1}\mathbb{Z}^2$ is chosen so that r coincides with the residue class of pa modulo $p\mathbb{Z}^2$. Since a can be replaced by any element of the coset $a+\mathbb{Z}^2$, the function g_a^{12} is determined only up to multiplication by a pth root of unity ([5], p. 28, Formula K2), but the coset f_rU^p is uniquely determined by r because U^p contains $\mathbb{C}^\times$. Furthermore, if $m \in Q$ then the function

$$f^m := \prod_{r \in R} f_r^{m(r)}$$

belongs to U ([5], p. 76, Theorem 5.2). Hence the assignment $m + pQ \mapsto f^mU^p$ defines an $\mathbb{F}_p$-linear map $\Phi : V' \to V''$.

Proposition 7. *The map Φ is surjective with one-dimensional kernel, and it intertwines τ' with τ''.*

Proof. The argument echos the proof of Proposition 0 of [7], which in turn merely assembles a number of results from [5]. Let us at least recall the relevant citations: The surjectivity of Φ follows from [5], p. 83, Theorem 1.3, because p is prime to 12 and thus the map $fU^p \mapsto f^{12}U^p$ is an automorphism of U/U^p. That the kernel of Φ is one-dimensional follows from the surjectivity, because V' has dimension $(p^2-1)/2$ over $\mathbb{F}_p$ while V'' has dimension $(p^2-3)/2$ ([5], p. 42, Theorem 3.2). Finally, the G-equivariance of Φ follows from [5], p. 27, Formula K1. □

Put $V''^{(k)} = \Phi(V'^{(k)})$, so that

$$V'' = \oplus_{k=0}^{(p-3)/2} V''^{(k)},$$

and let $\tau''^{(k)}$ denote the representation of G on $V''^{(k)}$.

Proposition 8. *If $1 \leqslant k \leqslant (p-5)/2$ then $\tau''^{(k)}$ has a unique irreducible subrepresentation and a unique irreducible quotient representation, and they are equivalent to σ_k and $\sigma_{(p-1-2k)/2}$ respectively. On the other hand, $\tau''^{(0)} \cong \sigma_{(p-1)/2}$ and $\tau''^{((p-3)/2)} \cong \sigma_1 \oplus \sigma_{(p-3)/2}$.*

Proof. Combine Propositions 6 and 7 and observe that V' has exactly one G-stable subspace of dimension one. □

We conclude with some remarks which will lead to a slight reformulation of Proposition 8. Since $p \geqslant 7$, the two direct summands of $\tau''^{((p-3)/2)}$ are inequivalent, so there is a unique subspace $W''^{((p-3)/2)}$ of $V''^{((p-3)/2)}$ on which the representation of G is equivalent to $\sigma_{(p-3)/2}$. We shall refer to the subspace

$$V''_{\mathrm{nc}} = \left(\oplus_{k=0}^{(p-5)/2} V''^{(k)}\right) \oplus W''^{((p-3)/2)}$$

of V'' as the *noncongruence part* of V''. The *congruence part* of V'' is the unique subspace V''_{c} of $V''^{((p-3)/2)}$ on which the representation of G is equivalent to σ_1. Thus

$$V'' = V''_{\mathrm{nc}} \oplus V''_{\mathrm{c}}. \tag{12}$$

To explain the terminology, let $\mathfrak{K}$ be the field of modular functions for $\Gamma(p)$ and let $\mathfrak{K}^{\mathrm{cc}}$ be the "congruence closure" of $\mathfrak{K}$, in other words the union of the modular function fields for all congruence subgroups of $\mathrm{SL}(2,\mathbb{Z})$. Given any subspace W of V'', we write $\mathfrak{K}_W$ for the Kummer extension of $\mathfrak{K}$ obtained by adjoining the pth roots of all $f \in U$ such that $fU^p \in W$. (Note that $\mathfrak{K}^{\times p} \cap U = U^p$, so that we can apply Kummer theory with $\mathfrak{K}^\times/\mathfrak{K}^{\times p}$ replaced by U/U^p: in particular, $[\mathfrak{K}_W : \mathfrak{K}] = |W|$.) We claim that

$$\mathfrak{K}_{V''} \cap \mathfrak{K}^{\mathrm{cc}} = \mathfrak{K}_{V''_{\mathrm{c}}}. \tag{13}$$

Together, (12) and (13) justify the designation "noncongruence part" for V''_{nc}.

To prove (13), we recall from the proof of Proposition 6 that the subspace of $V'^{((p-3)/2)}$ on which G acts via σ_1 is pM/pQ (strictly speaking we should identify this subspace as $p\mathcal{M}^{((p-3)/2)}/p\mathcal{Q}^{((p-3)/2)}$, not pM/pQ, but $\mathcal{M}^{(k)} = \mathcal{Q}^{(k)}$ for $k \neq (p-3)/2$). Thus $\Phi(pM/pQ) = V''_{\mathrm{c}}$. It follows (see [7], Proposition 2, p. 12) that $\mathfrak{K}_{V''_{\mathrm{c}}}$ is the field of modular functions for $\Gamma(p^2)$, whence the right-hand side of (13) is contained in the left-hand side. For the reverse inclusion, put

$$\Gamma = \{\gamma \in \mathrm{SL}(2,\mathbb{Z}) : f \circ \gamma = f \text{ for all } f \in \mathfrak{K}_{V''} \cap \mathfrak{K}^{\mathrm{cc}}\}.$$

Then the field of modular functions for Γ is the left-hand side of (13). In particular, since the left-hand side of (13) is a subfield of $\mathfrak{K}^{\mathrm{cc}}$ it follows that Γ is a congruence subgroup. But the least common multiple of the cusp amplitudes of Γ divides p^2, because the field $\mathfrak{K}_{V''}$ is generated over $\mathfrak{K}$ by pth roots of elements of $\mathfrak{K}$. Thus the Wohlfahrt level of Γ divides p^2, and since Γ is a congruence subgroup its Wohlfahrt level equals its congruence level by the Fricke-Wohlfahrt theorem [9]:

$$\Gamma(p^2) \subset \Gamma. \tag{14}$$

Taking modular function fields of the two sides of (14) reverses the inclusion and thus gives the inclusion of the left-hand side of (13) in the right-hand side.

Now put $W''^{(0)} = V''^{(0)}$, and for $1 \leqslant k \leqslant (p-5)/2$ let $W''^{(k)}$ be the unique irreducible subspace of $V''^{(k)}$. Then the maximal semisimple subspace of V''_{nc} is $\oplus_{k=0}^{(p-3)/2} W''^{(k)}$, and we obtain:

Proposition 9. *The representation of G on the maximal semisimple subspace of V''_{nc} is equivalent to $\oplus_{k=1}^{(p-1)/2}\sigma_k$.*

References

[1] R. Brauer and C. Nesbitt, *On the modular characters of groups,* Ann. of Math. **42** (1941), 556 – 590.

[2] B. H. Gross, *Representation theory and the cuspidal group of $X(p)$,* Duke Math. J. **54** (1987), 67 – 75.

[3] E. Hecke, *Über ein Fundamentalproblem aus der Theorie der elliptischen Modulfunktionen,* Abh. Math. Sem. Hamb. **6** (1928), 235 – 257 (= *Math. Werke* # 28, 525 – 547).

[4] E. Hecke, *Über das Verhalten der Integrale 1. Gattung bei Abbildungen, insbesondere in der Theorie der elliptischen Modulfunktionen,* Abh. Math. Sem. Hamb. **8** (1930), 271 – 281 (= *Math. Werke* # 29, 548 – 558).

[5] D. S. Kubert and S. Lang, *Modular Units*, Springer-Verlag, Grundlehren Math. Wissen. vol. 244, 1981.

[6] Á. Lozano-Robledo, *On the surjectivity of Galois representations attached to elliptic curves over number fields*, Acta Arith. **117** (2005), 283 – 291.

[7] D. E. Rohrlich, *Modular units and the surjectivity of a Galois representation,* J. of Number Thy. **107** (2004), 8 – 24.

[8] B. Srinivasan, *On the modular characters of the special linear group* $SL(2, p^n)$, Proc. London Math. Soc. **14** (1964), 101 –114.

[9] K. Wohlfahrt, *An extension of F. Klein's level concept,* Ill. J. Math. **8** (1964), 529 – 535.

Department of Mathematics and Statistics, Boston University, Boston, MA 02215
E-mail address: `rohrlich@math.bu.edu`