J. Math. Kyoto Univ. (JMKYAZ)
45-4 (2005), 807–829

On the Hecke operator U(p)

By

Siegfried Böcherer
(with an appendix by Ralf Schmidt)

Introduction

The operator $U(p)$ is a familiar tool in the theory of elliptic modular forms (introduced by Hecke in [5]). It can be defined in the same way on holomorphic Siegel modular forms of degree n for the congruence subgroups $\Gamma_0(N) := \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{Sp}(n,\mathbb{Z}) \mid c \equiv 0\ (N) \right\}$; the action of $U(p)$ on the Fourier expansion of such a modular form f is given by

$$f = \sum_T a(T) e^{2\pi i \mathrm{tr}(TZ)} \longmapsto f \mid U(p) = \sum_T a(pT) e^{2\pi i \mathrm{tr}(TZ)};$$

here T runs over all symmetric half integral positive semidefinite matrices of size n and Z is an element of Siegel's upper half space. To be more precise, let us denote by $[\Gamma_0(N), k, \chi]$ the space of Siegel modular forms of weight k with respect to the group $\Gamma_0(N)$ and the nebentypus character χ. Then $U(p)$ maps this space into itself (if $p \mid N$) and maps it into $[\Gamma_0(\frac{N}{p}), k, \chi]$ if $p^2 \mid N$ and χ is defined modulo $\frac{N}{p}$. It is clear from the theory of old- and newforms (for $n = 1$) that we can expect a nontrivial kernel for $U(p)$ if $p^2 \mid N$ and χ is defined modulo $\frac{N}{p}$.

The injectivity of $U(p)$ for $p^2 \mid N$ and χ not defined modulo $\frac{N}{p}$ can be proved along the classical lines (see Section 6). The main purpose of the present note is to show that $U(p)$ is injective for $p \mid\mid N$ (see Section 3). This will be done in a purely algebraic manner by studying the properties (invertibility) of the double coset $\Gamma_0(p) \cdot \begin{bmatrix} 0_n & -\mathbf{1}_n \\ \mathbf{1}_n & 0_n \end{bmatrix} \cdot \Gamma_0(p)$ in the abstract Hecke algebra associated to the pair $(\Gamma_0(p), \mathrm{Sp}(n,\mathbb{Z}))$ and its analogue over the finite field $\mathbb{F}_p$; to include the case of nontrivial nebentypus χ we will have to work with a slightly smaller group $\Gamma_1(p)$.

The results of this paper are motivated (and are used in a crucial way) in our investigation of the basis problem for Siegel modular forms with level [2].

Received March 2, 2005

Of course the operator $U(p)$ can be defined also for other types of congruence subgroups. The Iwahori subgroup is of particular interest; in this case there is a well established structure theory for the Hecke algebra (in terms of generators and relations). In an appendix to this paper, Ralf Schmidt will give a proof for the injectivity in this framework.

Acknowledgements. I want to thank M. Ueda and H. Yoshida for helpful discussions on the topics of this paper. In particular, Ueda patiently explained to me the cases $n = 1$ and $n = 2$. Essential parts of this paper were written during two stays in Japan in 2004 (at Nara Women University and Rikkyo University). The hospitality of M. Ueda and F. Sato and their universities is gratefully acknowledged. It is my pleasure to thank Ralf Schmidt for generously sharing his insight about Hecke operators with me and for providing the appendix.

Contents

1. The Hecke algebra

We fix a prime $p \neq 2$ and also a subgroup G of $\mathbb{F}_p^\times$ of index κ; then we define a subgroup Γ^G of $\mathrm{Sp}(n,\mathbb{Z})$ by

$$\Gamma^G := \left\{ g = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \mid C \equiv 0_n,\, \det(D) \bmod p \in G \right\}$$

As important special cases we mention

$$\Gamma^{\mathbb{F}_p^\times} = \{g \in \mathrm{Sp}(n,\mathbb{Z}) \mid C \equiv 0 \bmod p\} \qquad \text{(usually called } \Gamma_0(p)),$$
$$\Gamma^{\{1\}} = \{g \in \Gamma_0(p) \mid \det(D) \equiv 1 \bmod p\} \qquad \text{(usually called } \Gamma_1(p)).$$

In any case Γ^G is a normal subgroup of $\Gamma_0(p)$ with factor group isomorphic to $\mathbb{F}_p^\times/G$. We study the abstract Hecke-algebra over $\mathbb{C}$ associated to the pair $(\Gamma^G, \mathrm{Sp}(n,\mathbb{Z}))$; by definition, this is the set of all finite linear combinations of double cosets $\Gamma^G \cdot g \cdot \Gamma^G$ with $g \in \mathrm{Sp}(n,\mathbb{Z})$, equipped with the usual structure of a Hecke algebra. This algebra is isomorphic in a natural way to the $\mathbb{C}$–Hecke algebra $\mathcal{H}_p^G$ for the Hecke pair $(\Gamma_p^G, \mathrm{Sp}(n,\mathbb{F}_p))$, where

$$\Gamma_p^G = \left\{ \begin{bmatrix} A & B \\ 0 & D \end{bmatrix} \in \mathrm{Sp}(n,\mathbb{F}_p) \mid \det(D) \in G \right\},$$

and we prefer to work with this realization. We will often use that the group

$$\mathrm{GL}(n,G) := \{u \in \mathrm{GL}(n,\mathbb{F}_p) \mid \det(u) \in G\}$$

can be embedded into Γ_p^G via

$$\iota_n : \begin{cases} \mathrm{GL}(n,G) & \longrightarrow & \Gamma_p^G \\ D & \longmapsto & \begin{bmatrix} D^{-t} & 0 \\ 0 & D \end{bmatrix} \end{cases};$$

in particular, we may embed $\mathrm{SL}(n,\mathbb{F}_p)$ in this way. To describe the Hecke algebra, we need some special elements: For $a \in \mathbb{F}_p^\times/G$ and $0 \le i \le n$ we denote by $\tau(a,i)$ the double coset

$$\Gamma_p^G\, W(a,i)\, \Gamma_p^G = \Gamma_p^G\, \widetilde{W(a,i)}\, \Gamma_p^G,$$

where the elements $W(a,i)$ are defined by

$$W(a,i) = \begin{cases} \begin{bmatrix} 0_i & 0 & -C^{-t} & 0 \\ 0 & \mathbf{1}_{n-i} & 0 & 0_{n-i} \\ C & 0 & 0_i & 0 \\ 0 & 0_{n-i} & 0 & \mathbf{1}_{n-i} \end{bmatrix} & \text{for} \quad i \ge 1 \\ \begin{bmatrix} D^{-t} & 0_n \\ 0_n & D \end{bmatrix} & \text{for} \quad i = 0 \end{cases}$$

The $\widetilde{W(a,i)}$ are defined similarly by $\widetilde{W(a,0)} = W(a,0)$ and for $i > 0$

$$\widetilde{W(a,i)} = \begin{bmatrix} \mathbf{1}_{n-i} & 0 & 0_{n-i} & 0 \\ 0 & 0_i & 0 & -C^{-t} \\ 0_{n-i} & 0 & \mathbf{1}_{n-i} & 0 \\ 0 & C & 0 & 0_i \end{bmatrix}.$$

Here C and D are any matrices in $\mathrm{GL}(i,\mathbb{F}_p)$ and $\mathrm{GL}(n,\mathbb{F}_p)$ respectively with $\det(C) = a$ and $\det(D) = a$. We can change C or D to UCV and UDV with $U,V \in \mathrm{GL}(i,G)$ (resp. $U,V \in \mathrm{GL}(n,G)$); therefore the double coset $\tau(a,i)$ does not depend on the choice of C or D. We may even assume that C and D are of type

$$C = \mathrm{diag}(1,\dots,1,a,1\dots,1) \quad \text{and} \quad D = \mathrm{diag}(1,\dots,1,a,1\dots1)$$

with the a at any position convenient for us. In our applications, we will mainly be concerned with the cases

$$G = \mathbb{F}^\times, \qquad G = (\mathbb{F}_p^\times)^2, \qquad G = \{1\}.$$

To formulate our result simultaneously for these cases, we allow G to be arbitrary; to do so, we have to distinguish two cases:

Case I: G contains a quadratic non-residue.
Case II: $G \subset (\mathbb{F}_p^\times)^2$.

Furthermore, we denote by ϵ a quadratic non-residue in $\mathbb{F}_p^\times$.

Proposition 1.1. *Let G be a subgroup of index κ in $\mathbb{F}_p^\times$. Then a complete set of representatives of the double classes in the Hecke algebra $\mathcal{H}_p^G$ is given by*

Case I: $\{\tau(a,0)\,,\,\tau(a,n)\ \mid\ a \in \mathbb{F}_p^\times/G\}\ \cup\ \{\tau(1,i)\ \mid\ 1 \le i \le n-1\}$

Case II: $\{\tau(a,0)\,,\,\tau(a,n)\ \mid\ a \in \mathbb{F}_p^\times/G\}\ \cup\ \{\tau(1,i)\,,\tau(\epsilon,i)\ \mid\ 1 \le i \le n-1\}$

In particular, $\mathcal{H}_p^G$ is an algebra of dimension $2\kappa+n-1$ in case I *and dimension $2\kappa+2n-2$ in case* II.

Proof. For a given double coset $\Gamma_p^G \cdot g \cdot \Gamma_p^G$ with $g = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \mathrm{Sp}(n, \mathbb{F}_p)$ we will exhibit an explicit representative. For g as above the double coset $\Gamma_p^G g \Gamma_p^G$ depends only on the "second row" (C, D) of g. We may change this second row by

$$(C,D) \longmapsto (UCV^{-t}, UDV) \qquad (U, V \in \mathrm{GL}(n,G))$$
$$(C,D) \longmapsto (C, D+CT) \qquad (T = T^t \in \mathbb{F}_p^{(n,n)})$$

without changing the double coset. Therefore we may assume that C is of the form $C = \begin{bmatrix} c_1 & 0 \\ 0 & 0 \end{bmatrix}$, where $c_1 \in \mathrm{GL}(i, \mathbb{F}_p)$ with $i = \mathrm{rank}(C)$. By choosing T appropriately, D can be chosen to be of type $D = \begin{bmatrix} 0 & 0 \\ d_3 & d_4 \end{bmatrix}$; the product $C \cdot D^t$ has to be symmetric, hence we also have $d_3 = 0$. Therefore the double cosets in our Hecke algebra are parametrized by

$$\bigcup_{i=0}^{n} \left\{ \begin{bmatrix} & * & & * \\ c_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & d_4 \end{bmatrix} \mid c_1 \in \mathrm{GL}(i, \mathbb{F}_p),\ d_4 \in \mathrm{GL}(n-i, \mathbb{F}_p) \right\} / \sim$$

with two such pairs (c_1, d_4) and (c_1', d_4') being equivalent iff there exist $U, V \in \mathrm{GL}(n, G)$ such that

$$\begin{bmatrix} c_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & d_4 \end{bmatrix} = \left[U \cdot \begin{bmatrix} c_1' & 0 \\ 0 & 0 \end{bmatrix} \cdot V^{-t},\, U \cdot \begin{bmatrix} 0 & 0 \\ 0 & d_4' \end{bmatrix} \cdot V \right].$$

Clearly we only have to consider pairs with the same i. The "extreme cases" $i = 0$ and $i = n$ are easy: The pairs $(0_n, d)$ and $(0_n, d')$ are equivalent iff $\det(d) \cdot G = \det(d') \cdot G$; the pairs $(c, 0_n)$ and $(c', 0_n)$ are equivalent iff $\det(c) \cdot G = \det(c') \cdot G$.

The "mixed cases" ($1 \leq i \leq n-1$) are more delicate: First it is easy to see that we only need to consider

$$U = \begin{bmatrix} u_1 & 0 \\ 0 & u_4 \end{bmatrix}, \qquad V = \begin{bmatrix} v_1 & 0 \\ 0 & v_4 \end{bmatrix}$$

with $u_1, v_1 \in \mathrm{GL}(i, \mathbb{F}_p)$, $u_4, v_4 \in \mathrm{GL}(n-i, \mathbb{F}_p)$ with the extra condition

$$\det(u_1)\det(u_4) \in G\,, \qquad \det(v_1)\det(v_4) \in G.$$

We may now assume without loss of generality that $d_4 = d_4' = \mathbf{1}_{n-i}$. Then U and V must satisfy $u_4 v_4 = \mathbf{1}_{n-i}$; together with the extra conditions from above this gives

$$\det(u_1)\det(v_1) \in G.$$

For fixed i with $1 \leq i \leq n-1$ the double cosets are then parametrized by elements $c \in \mathrm{GL}(i, \mathbb{F}_p)$, subject to an equivalence relation

$$c \sim c' \iff c' = u \cdot c \cdot v$$

with $u, v \in \mathrm{GL}(i, \mathbb{F}_p)$ and $\det(u) \cdot \det(v) \in G$. We may assume that both c and c' are diagonal matrices of type

$$c = \mathrm{diag}(\lambda, 1, \ldots, 1)\,, \qquad c' = \mathrm{diag}(\lambda', 1, \ldots, 1).$$

Then c is equivalent to c' iff $\lambda = \frac{u}{v} \cdot \lambda'$ with $u, v \in \mathbb{F}_p$ with $u \cdot v \in G$. This means

$$\lambda' = u^2 \cdot g \cdot \lambda$$

for an appropriate $u \in \mathbb{F}_p^\times$, $g \in G$. So for fixed i there is exactly one equivalence class if G contains a quadratic non-residue, and two equivalence classes if $G \subset \mathbb{F}_p^2$. □

Remark 1.

a) The $\tau(a, 0)$ are invertible elements of the Hecke algebra $\mathcal{H}_p^G$; these double cosets consist of just one left or right coset.

b) For $i > 0$ we have

$$\begin{aligned} \tau(a, 0) \cdot \tau(b, i) &= \tau(ab, i), \\ \tau(b, i) \cdot \tau(a, 0) &= \tau(ba^{-1}, i). \end{aligned}$$

These equations imply that

$$\tau(a\lambda^2, 0) - \tau(a, 0)$$

is a left and right zero divisor in the Hecke algebra, provided that $\lambda^2 \notin G$. Also, by considering the case $i = n$, we see that the Hecke algebra $\mathcal{H}_p^G$ is not commutative if $(\mathbb{F}_p^\times)^2 \not\subset G$.

c) In the case $(\mathbb{F}_p^\times)^2 \subset G$ the Hecke algebra is commutative, because

$$g \longmapsto \hat{g} := \begin{bmatrix} \mathbf{1}_n & 0_n \\ 0_n & \mathbf{1}_n \end{bmatrix} \cdot g^{-1} \cdot \begin{bmatrix} \mathbf{1}_n & 0_n \\ 0_n & \mathbf{1}_n \end{bmatrix}$$

defines an anti-involution of the Hecke pair with

$$\Gamma \cdot \hat{g} \cdot \Gamma = \Gamma \cdot g \cdot \Gamma$$

(one can choose representatives of the double cosets in such a way!).

d) We can choose representatives for the left cosets in $\tau(1,n)$ in a particularly nice way (which does not depend on the group G at all). Clearly

$$\begin{bmatrix} 0_n & -\mathbf{1}_n \\ \mathbf{1}_n & 0_n \end{bmatrix}^{-1} \cdot \Gamma_p^G \cdot \begin{bmatrix} 0_n & -\mathbf{1}_n \\ \mathbf{1}_n & 0_n \end{bmatrix} \cap \Gamma_p^G = \left\{ \begin{bmatrix} A & 0_n \\ 0_n & D \end{bmatrix} \in \mathrm{Sp}(n, \mathbb{F}_p) \mid \det(D) \in G \right\},$$

and therefore a complete set of representatives for the left cosets of $\tau(1,n)$ is given by

$$\left\{ \begin{bmatrix} 0_n & -\mathbf{1}_n \\ \mathbf{1}_n & 0_n \end{bmatrix} \cdot \begin{bmatrix} \mathbf{1}_n & T \\ 0_n & \mathbf{1}_n \end{bmatrix} \mid T = T^t \in \mathbb{F}_p^{n,n} \right\}.$$

We call these representatives the "standard representatives" of $\tau(1,n)$.

Remark 2. The number γ_i of left cosets in $\tau(a,i)$ equals

$$\gamma_i = \delta_i \cdot p^{in+\frac{i}{2}-\frac{1}{2}i^2} \cdot \frac{\prod_{j=i+1}^{n}(1-p^{-j})}{\prod_{j=1}^{n-i}(1-p^{-j})}$$

with

$$\delta_i = \begin{cases} 1 & \text{if } \; i=0,\, i=n, \\ [\mathbb{F}^\times : \sqrt{G}] & \text{if } \; 0<i<n, \end{cases}$$

where $\sqrt{G} := \{x \in \mathbb{F}_p^\times \mid x^2 \in G\}$.

Proof. Clearly this number does not depend on $a \in \mathbb{F}_p^\times$, so we assume $a = 1$. Furthermore, only the case $0 < i < n$ needs attention ($i = 0$ is trivial, $i = n$ is covered in Remark 1d)). We write Γ for Γ_p^G in the sequel. The number of left cosets in $\Gamma W(1,i)\Gamma$ is then equal to the group index

$$[\Gamma : W(1,i)^{-1}\Gamma W(1,i) \cap \Gamma].$$

The subgroup

$$W(1,i)^{-1}\Gamma\, W(1,i) \cap \Gamma$$

consists of those elements $\begin{bmatrix} A & B \\ 0_n & D \end{bmatrix}$ with the extra properties (besides $\det(D) \in G$)

$$b_1 = 0, \qquad d_3 = 0, \qquad \det(d_1) \cdot \det(d_4)^{-1} \in G,$$

where we decompose D as $D = \begin{bmatrix} d_1 & d_2 \\ d_3 & d_4 \end{bmatrix}$ with d_1 of size i (and similarly for B). Note that the last of these three conditions comes from the fact that we have to consider elements $W(1,i)^{-1} \cdot \gamma \cdot W(1,i)$ with $\gamma \in \Gamma$. Therefore

$$\gamma_i = p^{\frac{i(i+1)}{2}} \cdot [\mathrm{GL}(n,G) : P_i(G)],$$

where

$$P_i(G) := \left\{ \begin{bmatrix} d_1 & d_2 \\ 0 & d_4 \end{bmatrix} \mid \det(d_1)\det(d_4) \in G\,,\, \det(d_1)\det(d_4)^{-1} \in G \right\}.$$

An elementary calculation shows that indeed

$$[\mathrm{GL}(n,G) : P_i(G)] = [\mathbb{F}_p^\times : \sqrt{G}] \cdot [\mathrm{GL}(n,\mathbb{F}_p) : P_i(\mathbb{F}_p)].$$

Therefore we get

$$\begin{aligned} \gamma_i &= \delta_i \cdot p^{\frac{i(i+1)}{2}} \cdot \frac{\#\mathrm{GL}(n,\mathbb{F}_p)}{p^{i(n-i)}\#\mathrm{GL}(i,\mathbb{F}_p) \cdot \#\mathrm{GL}(n-i,\mathbb{F}_p)} \\ &= \delta_i \cdot p^{\frac{i(i+1)}{2} - i(n-i)} \cdot \frac{p^{n^2} \cdot \prod_{j=1}^n (1-p^{-j})}{p^{i^2} \cdot \prod_{j=1}^i (1-p^{-j}) \cdot p^{(n-i)^2} \cdot \prod_{k=1}^{n-i}(1-p^{-k})}. \end{aligned}$$

□

2. The endomorphism ψ_n

We define an endomorphism of $\mathcal{H}_p^G$ as a vector space by

$$\psi_n : \left\{ \begin{array}{ccc} \mathcal{H}_p^G & \longrightarrow & \mathcal{H}_p^G \\ x & \longmapsto & \tau(1,n) \cdot x \end{array} \right. .$$

By a standard reasoning of linear algebra, $\tau(1,n)$ is a (left and right) invertible element of the algebra $\mathcal{H}_p^G$, if ψ_n is an invertible endomorphism.

Proposition 2.1. *The determinant of the endomorphism ψ_n is different from zero. In particular, $\tau(1,n)$ is an invertible element of the Hecke algebra $\mathcal{H}_p^G$.*

Proof. We use the standard representatives for the left cosets in $\tau(1,n)$. To write down $\tau(1,n) \cdot \tau(1,i)$ explicitly as a linear combination of the $\tau(a,j)$ it is enough to determine the double cosets to which

$$M := \begin{bmatrix} 0_n & -\mathbf{1}_n \\ \mathbf{1}_n & T \end{bmatrix} \cdot W(1,i) = \begin{bmatrix} & * & & * \\ -t_1 & 0 & -\mathbf{1}_i & t_2 \\ -t_2^t & \mathbf{1}_{n-i} & 0 & t_4 \end{bmatrix}$$

belongs. Clearly, t_2 and t_4 are irrelevant for this; we may assume that both are zero. We assume that t_1 is of rank r with $0 \le r \le i$. Then there is a

$V \in \mathrm{SL}(i, \mathbb{F}_p)$ with $V \cdot (-t_1) \cdot V^t = \begin{bmatrix} 0 & 0 \\ 0 & s \end{bmatrix}$ with s of (maximal) rank r. For $U := \begin{bmatrix} V & 0 \\ 0 & \mathbf{1}_{n-i} \end{bmatrix} \in \mathrm{SL}(n, \mathbb{F}_p)$ we get

$$\left(U \cdot \begin{bmatrix} t_1 & 0 \\ 0 & \mathbf{1}_{n-i} \end{bmatrix} \cdot U^t \, , U \cdot \begin{bmatrix} -\mathbf{1}_i & 0 \\ 0 & 0 \end{bmatrix} \cdot U^{-1} \right) = \left(\begin{bmatrix} 0 & 0 & \\ 0 & s & \\ & & \mathbf{1}_{n-i} \end{bmatrix} , \begin{bmatrix} -\mathbf{1}_i & 0 \\ 0 & 0 \end{bmatrix} \right).$$

The rightmost block matrix may be changed into $\begin{bmatrix} -\mathbf{1}_{i-r} & 0 \\ 0 & 0 \end{bmatrix}$ by changing this block matrix modulo a multiple of s. The minus sign can be moved to the first block. Therefore M is in the same double coset as

$$\widetilde{W}(n-i+r, L),$$

where L is any matrix of size $n-i+r$ with

$$\det(L) = (-1)^{i-r} \det(s).$$

Then the product matrix M is in the same double coset as

$$\begin{bmatrix} D^{-t} & 0 \\ 0 & D \end{bmatrix} \cdot \begin{bmatrix} & * & * & \\ 0 & 0 & \mathbf{1}_{i-r} & 0 \\ 0 & \mathbf{1}_{n-i+r} & 0 & 0 \end{bmatrix}$$

with

$$D = \begin{bmatrix} -\mathbf{1}_{i-r} & & \\ & s & \\ & & \mathbf{1}_{n-i} \end{bmatrix}.$$

So we finally see that

$$\Gamma_p^G M \Gamma_p^G = \tau((-1)^{i-r} \det(s), n-i+r).$$

To determine the multiplicities, we have to count the number of left cosets which occur in the consideration above and belong to a fixed double coset $\tau(a, j)$. We get a contribution only for $j \geq n-i$. In the case $r = 0$, i.e. $j = n-i$, only $a = (-1)^i$ occurs; its multiplicity is

$$p^{\frac{(n-i)(n-i+1)}{2}} \cdot p^{i(n-i)} \frac{\gamma_i}{\gamma_{n-i}}. \tag{2.1}$$

Here the p–powers at the beginning come from the t_2 and t_4 components of T. The other "extreme case" is $r = i$, i.e. $j = n$. The multiplicity of $\tau(a, n)$ (with $a \in \mathbb{F}_p^\times / G$) is

$$p^{\frac{(n-i)(n-i+1)}{2}} \cdot p^{i(n-i)} \cdot \sum_{b \in \mathbb{F}_p^\times, \, bG = aG} c_{ii}(b) \frac{\gamma_i}{\gamma_n}. \tag{2.2}$$

Here, for $b \in \mathbb{F}_p^\times$,

$$\begin{aligned} c_{ii}(b) &:= \#\{X \in \mathbb{F}_p^{(i,i)} \mid X = X^t\,,\, \det(X) = b\} \\ &= \frac{\#\mathrm{SL}(i, \mathbb{F}_p)}{\#\mathrm{SO}(T)(\mathbb{F}_p)}. \end{aligned}$$

Here T is any symmetric matrix of size i with $\det(T) = b$; the number $\#\mathrm{SO}(T)$ is well-known ([10]):

$$\#\mathrm{SO}(T) = p^{\frac{i(i-1)}{2}} \cdot \begin{cases} (1 - \epsilon(T)p^{-\frac{i}{2}}) \prod_{k=1}^{\frac{i}{2}-1}(1 - p^{2k-i}) & \text{if } i \text{ even,} \\ \prod_{k=1}^{\frac{(i-1)}{2}}(1 - p^{2k-i-1}) & \text{if } i \text{ odd;} \end{cases}$$

here we put $\epsilon(T) = \left(\frac{(-1)^{\frac{i}{2}} \det(T)}{p}\right)$.

It remains the case $n - i < j < n$ with $a = 1$ (Case I) or $a \in \{1, \epsilon\}$ (Case II). In case I we get for the multiplicity of $\tau(1, n - i + r)$

$$p^{\frac{(n-i)(n-i+1)}{2}} \cdot p^{i(n-i)} \cdot c_{r,i} \cdot \frac{\gamma_i}{\gamma_{n-i+r}} \tag{2.3}$$

with

$$c_{r,i} = \#\{X \in \mathbb{F}_p^{(i,i)} \mid X = X^t,\, \mathrm{rank}(X) = r\},$$

and in the case II (with $a \in \{1, \epsilon\}$)

$$p^{\frac{(n-i)(n-i+1)}{2}} \cdot p^{i(n-i)} \cdot c_{r,i}((-1)^{i-r}a)\frac{\gamma_i}{\gamma_{n-i+r}} \tag{2.4}$$

with (for $0 < l < k$)

$$\begin{aligned} c_{l,k}(a) &:= \#\{X \in \mathbb{F}_p^{(k,k)} \mid X = X^t,\, \mathrm{rank}(X) = l,\, d(X) = a\} \\ &= \frac{\#\mathrm{GL}(k, \mathbb{F}_p)}{p^{l(k-l)} \cdot \#\mathrm{GL}(k - l, \mathbb{F}_p) \cdot \#\mathrm{O}(S)(\mathbb{F}_p)} \end{aligned}$$

Here S is any symmetric matrix of size l with $\det(S) = a$; we denote by $d(X)$ the determinant (or discriminant) of the quadratic space $V(S)/\mathrm{rad}(V(S))$, where $V(X)$ denotes the quadratic space associated with X and $\mathrm{rad}(V(S))$ its radical (note, however, that $d(X)$ is well defined only up to a square factor in $\mathbb{F}_p^\times$).

To make case I also completely explicit, we just mention that

$$c_{r,i} = c_{r,i}(1) + c_{r,i}(\epsilon).$$

Some caution is necessary here: In $c_{kk}(a)$ we have a condition on the determinant, whereas in $c_{lk}(a)$ for $l < k$ there is only a condition on the discriminant (which is only defined modulo squares). With these informations at hand, we can write the product $\tau(1, n) \cdot \tau(a, i)$ explicitly as linear combinations of the basis elements as given in Proposition 1.1. We do not need the full information here, but we emphasize that

$$\tau(1,n)\cdot\tau(a,i)=p^{\frac{(n-i)(n-i+1)}{2}}\cdot p^{i(n-i)}\cdot\frac{\gamma_i}{\gamma_{n-i}}\cdot\tau((-1)^i\cdot a,n-i)+\dots \tag{2.5}$$

where $\dots$ involves only the $\tau(b,j)$ with $j>n-i$. If we describe the endomorphism ψ in terms of a matrix with respect to the basis

$$\tau(a_1,0),\dots,\tau(a_\kappa,0),\ \tau(1,1),\tau(\epsilon,1),\dots\tau(1,n-1),$$
$$\tau(\epsilon,n-1),\ \tau(a_1,n),\dots,\tau(a_\kappa,n),$$

where $a_1,\dots a_\kappa$ run over representatives of $\mathbb{F}^\times/G$ (this is for case II; in case I we should omit the elements with ϵ), then this matrix has the shape

$$\Psi_n=\begin{bmatrix} & & & X_n\\ & & x_{n-1} & *\\ & \iddots & & \vdots\\ & x_1 & & \\ X_0 & & \dots & *\end{bmatrix}.$$

Here $X_0=\mathbf{1}_\kappa$ and $X_n=\gamma_n\cdot Y_n$, where Y_n is a matrix of size κ, describing the permutation in $\mathbb{F}_p^\times/G$ induced by multiplication with $(-1)^n$. For $1\le j\le n-1$ we have (with $n-i=j$) in case I

$$\begin{aligned}x_j&=p^{\frac{(n-i)(n-i+1)}{2}}\cdot p^{i(n-i)}\frac{\gamma_i}{\gamma_{n-i}}\\&=p^{in-\frac{i^2}{2}+\frac{i}{2}},\end{aligned}$$

and in case II

$$\begin{aligned}x_j&=p^{\frac{(n-i)(n-i+1)}{2}}\cdot p^{i(n-i)}\frac{\gamma_i}{\gamma_{n-i}}\cdot y_j\\&=p^{in-\frac{i^2}{2}+\frac{i}{2}}\cdot y_j,\end{aligned}$$

where y_j is a 2×2-matrix describing the permutation in $1,\epsilon$ given by multiplication with $(-1)^j$. In particular, the determinant of ψ_n is different from zero. □

Remark 3. In our calculations above, we have determined *all* the entries of the matrix Ψ_n. To obtain the result of the proposition, only the (somewhat simpler) calculation of the entries of $X_0,X_n,x_1,\dots,x_{n-1}$ was necessary (together with the fact that the upper triangular part of Ψ_n is zero).

3. The operator $U(p)$

Now we switch back to a global setting, i.e., we work now with subgroups of $\mathrm{Sp}(n,\mathbb{Z})$ of level p; the connection between the two settings is given by the natural homomorphism

$$\pi:\mathrm{Sp}(n,\mathbb{Z})\longrightarrow\mathrm{Sp}(n,\mathbb{F}_p).$$

Whenever possible, we still use the same notations as in the previous sections, denoting any representative of $\pi^{-1}(g)$ also by g; in particular, we use in this section the symbol $\tau(1,n)$ for the double coset $\Gamma^G \cdot \begin{bmatrix} 0_n & -\mathbf{1}_n \\ \mathbf{1}_n & 0_n \end{bmatrix} \cdot \Gamma^G$ in $\mathrm{Sp}(n,\mathbb{Z})$ (and similarly for the other $\tau(a,j)$).

For standard notations about Siegel modular forms and their Hecke operators we refer the reader to [1], [4]. We just recall that for any congruence subgroup Γ of $\mathrm{Sp}(n,\mathbb{Z})$ and any (holomorphic) Siegel modular form $F : \mathbb{H}_n \longmapsto \mathbb{C}$ of degree n and weight k for Γ we can define the action of a double coset $\Gamma \cdot g \cdot \Gamma$ with $g \in \mathrm{GSp}(n,\mathbb{Q})^+$ (the "+" indicating positive multiplier) by

$$F \longmapsto F \Big| \Gamma \cdot g \cdot \Gamma := \sum_i F \Big|_k g_i \qquad (\Gamma \cdot g \cdot \Gamma = \sqcup_i \Gamma \cdot g_i);$$

here, for $h = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ the slash-operator is defined by

$$(f \mid_k g)(Z) = \det(g)^{\frac{k}{2}} \det(CZ+D)^{-k} f((AZ+B)(CZ+D)^{-1}). \tag{3.1}$$

Using the special representatives from Remark 1d) this means for $\Gamma = \Gamma^G$

$$\begin{aligned} F \mid \tau(1,n) &= \sum_T F \mid_k \begin{bmatrix} 0_n & -\mathbf{1}_n \\ \mathbf{1}_n & T \end{bmatrix} \\ &= \sum_T F \mid_k \begin{bmatrix} 0_n & -\mathbf{1}_n \\ p\mathbf{1}_n & 0_n \end{bmatrix} \cdot \begin{bmatrix} \mathbf{1}_n & T \\ 0_n & p\mathbf{1}_n \end{bmatrix} \\ &= p^{\frac{n(n+1)}{2} - \frac{nk}{2}} \times F \mid W_p \mid U(p). \end{aligned} \tag{3.2}$$

Here W_p denotes the involution of Fricke type

$$F \longrightarrow F \mid W_p := F \mid_k \begin{bmatrix} 0_n & -\mathbf{1}_n \\ p \cdot \mathbf{1}_n & 0_n \end{bmatrix}, \tag{3.3}$$

and $U(p)$ is the operator defined by the action of the double coset $\Gamma \begin{bmatrix} \mathbf{1}_n & 0_n \\ 0_n & p\mathbf{1}_n \end{bmatrix} \Gamma$. On the Fourier expansion of F this operator is given by

$$F = \sum_T a(T) e^{2\pi i \mathrm{tr}(TZ)} \longmapsto \sum_T a(pT) e^{2\pi i \mathrm{tr}(TZ)}.$$

The element $\tau(1,n)$ being invertible in the Hecke algebra $\mathcal{H}_p^G$, and W_p normalizing the group Γ^G, we obtain:

Theorem 3.1. *On any space of Siegel modular forms for a group Γ^G of level p the operator $U(p)$ is injective.*

This clearly implies, in particular, that $U(p)$ is injective on spaces of modular forms for the Hecke type subgroup $\Gamma_0(p)$ with nebentypus χ (with any Dirichlet character χ mod p). The case of nebentypus will be investigated in more detail in the next section.

4. The case of nontrivial nebentypus

Let χ be a character of $\mathbb{F}_p^\times$; whenever convenient, we tacitly identify χ with a Dirichlet character mod p or a character of $\Gamma_0(p)$ or of the quotient group $\Gamma_0(p)/\Gamma_1(p)$.

We consider now the case $G = \{1\}$, i.e., our group is $\Gamma_1(p)$. From the considerations of the previous sections it is clear that $W_pU(p)$ satisfies a relation of degree $(p-1)\cdot n$ on the space of Siegel modular forms of weight k for $\Gamma_1(p)$; as in [4] we call this space $[\Gamma_1(p), k]$. We want to get more precise informations in the case of modular forms with nebentypus. The space $[\Gamma_1(p), k]$ decomposes as

$$[\Gamma_1(p), k] = \oplus_\chi [\Gamma_0(p), k, \chi], \tag{4.1}$$

where χ runs over all Dirichlet characters modulo p and

$$\begin{aligned}&[\Gamma_0(p), k, \chi]\\ &\quad = \left\{ f \in [\Gamma_1(p)] \;\middle|\; f\mid_k M = \chi(\det(D))f \text{ for all } M = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \Gamma_0(p) \right\}.\end{aligned}$$

A modular form $f \in [\Gamma_0(p), k, \chi]$ can then be identified with an element of $[\Gamma_1, k]$ with the additional property

$$f\mid_k \tau(a, 0) = \chi(a)\cdot f \qquad (a \in \mathbb{F}_p^\times).$$

Here $\tau(a, 0)$ should be identified with (any) matrix M from $\Gamma_0(p)$ satisfying

$$M \equiv \begin{bmatrix} D^{-t} & 0 \\ 0 & D \end{bmatrix} \mod p$$

with $\det(D)$ congruent to a modulo p. We denote by $T(a, i)$ the endomorphism of $[\Gamma_1(p), k]$ induced by the double coset $\tau(a, i)$. The commutation rule from Remark 1 b) then implies that the Hecke operator $T(a, i)$ satisfies (for any $F \in [\Gamma_0(p), k, \chi]$, any $a, b \in \mathbb{F}_p^\times$ and any $i > 0$)

$$\begin{aligned} F \mid T(a, i)T(b, 0) &= F \mid T(ab^{-1}, i)\\ &= F \mid T(b^{-1}, 0) \mid T(a, i)\\ &= \chi(b^{-1})F \mid T(a, i).\end{aligned}$$

This shows that (for $i > 0$) the endomorphism $T(a, i)$ of $[\Gamma_1(p), k]$ induces a homomorphism from $[\Gamma_0(p), k, \chi]$ to $[\Gamma_0(p), k, \overline{\chi}]$, which we denote by $T(a, i)_\chi$.

The case $1 \le i \le n-1$ exhibits a special phenomenon: In the equation above, $T(ab^{-1}, i)$ depends only on the square class of ab^{-1}. Therefore, we have at the same time (for any $\lambda \in \mathbb{F}^\times$)

$$F \mid T(a,i)T(b,0) = \chi(\lambda^2 b^{-1}) \cdot F \mid T(a,i).$$

We conclude then that for $1 \le i \le n-1$ and a nonquadratic character χ, the endomorphism $T(a,i)_\chi$ is zero on $[\Gamma_0(p), k, \chi]$. On the other hand, it follows from Proposition 1.1 that $\tau(1,n) \cdot \tau(1,n)$ is a linear combination of the $\tau(a,j)$. We claim that in the corresponding expression for $T(1,n)_\chi^2$ only the contribution of $T((-1)^n, 0)_\chi$ can survive. The reason is that all the $T(a,j)_\chi$ with $1 \le j \le n-1$ are zero anyway and the $T(a,n)_\chi$ would change the nebentypus character from χ to $\overline{\chi}$. (An alternative –more explicit– reasoning is also possible here: by the calculations of Section 2 we can write $T(1,n)_\chi^2$ explicitly as linear combinations of the $T(1,j)_\chi$, using $T(a,j)_\chi = \chi(a) \cdot T(1,j)_\chi$; an inspection of the coefficients –using orthogonality relations for characters– shows that their coefficients are indeed zero for $j > 0$).

We summarize these considerations as

Proposition 4.1. *Assume that χ is a nonquadratic character mod p. Then the Hecke operators $T(a,i)_\chi$ satisfy the relations*

$$\begin{aligned} T(a,i)_\chi &= 0 \qquad \textit{for } 1 \le i \le n-1, \\ T(1,n)_\chi^2 &= \chi(-1)^n \cdot p^{\frac{n(n+1)}{2}}. \end{aligned}$$

This means in particular, that the operator $W_p U(p)$ satisfies

$$(W_p U(p))^2 = \chi(-1)^n p^{nk - \frac{n(n+1)}{2}}.$$

This relation is well known for elliptic modular forms, see e.g. [7], where it occurs implicitly in the (stronger) results of §4.6.

We now consider the case of a nontrivial quadratic character χ mod p. We go back to the setting of Section 2 with $G = (\mathbb{F}_p^\times)^2$. We recall the multiplication rule (with $a \in \{1, \epsilon\}$)

$$\tau(1,n) \cdot \tau(a,i) = \alpha(i) \cdot \tau((-1)^i \cdot a, n-i) + \sum_{b \in \{1,\epsilon\}, r > 0} \alpha(b,i,r) \cdot \tau(b, n-i+r)$$

with coefficients $\alpha(i)$, $\alpha(b,i,r)$, which can be read off from Section 2. The dependence of the coefficients $\alpha(b,i,r)$ on b comes from counting the elements in $\mathrm{O}(S)(\mathbb{F}_p)$, where S is any symmetric matrix of size r with discriminant $(-1)^{i-r}b$. These numbers do not depend on b at all if r is odd. With this observation at hand, we pass to the quotient Hecke algebra

$$\overline{\mathcal{H}}_{p,\chi} := \mathcal{H}_p^G / \mathcal{I},$$

where $\mathcal{I}$ is the ideal generated by

$$\{\tau(a,0) - \chi(a)\tau(1,0) \mid a = 1, \epsilon\}.$$

Then $\overline{\mathcal{H}}_{p,\chi}$ is a $\mathbb{C}$–vector space of dimension n with basis given by the equivalence classes of the $\tau(1,i)$, which we will call $\overline{\tau(i)}$. The multiplication rule above then becomes

$$\begin{aligned}\overline{\tau(n)}\cdot\overline{\tau(i)} &= \alpha(i)\cdot\overline{\tau(n-i)}+\sum_{r>0}\left(\alpha(1,i,r)-\alpha(\epsilon,i,r)\right)\overline{\tau(n-i+r)}\\ &= \alpha(i)\cdot\overline{\tau(n-i)}+\sum_{\substack{r>0\\ r\text{ even}}}\left(\alpha(1,i,r)-\alpha(\epsilon,i,r)\right)\overline{\tau(n-i+r)}.\end{aligned}$$

In particular, multiplication with $\overline{\tau(n)}$ leaves the subspace

$$\overline{\mathcal{H}}_{p,\chi}^{\text{even}} := \mathbb{C}\{\overline{\tau(l)}\mid l \text{ even}\}$$

invariant if n is even. In the case of odd n, the same property holds for multiplication with $\overline{\tau(n)}^2$. Let (for n even) $\mathcal{P}=\sum_t \lambda_t X^t$ be the characteristic polynomial of this multiplication by $\overline{\tau(n)}$ on $\overline{\mathcal{H}}_{p,\chi}^{\text{even}}$; in particular, $\sum_t \lambda_t \overline{\tau(n)}^t\cdot\overline{\tau(0)}=0$; with $\overline{\tau(0)}$ being the unit element in the Hecke algebra $\overline{\mathcal{H}}_{p,\chi}$, we then get $\mathcal{P}(\overline{\tau(n)})=0$, now as an identity in the algebra $\overline{\mathcal{H}}_{p,\chi}$. From this and a similar reasoning in the case of odd n we obtain

Proposition 4.2. *Let χ be a nontrivial character mod p. Then $\overline{\tau(n)}$ satisfies a polynomial relation of degree $\frac{n}{2}+1$ if n is even. In the case of odd n, we get a polynomial relation of degree $\frac{n+1}{2}$ for $\overline{\tau(n)}^2$.*

Remark 4. The statement above was formulated in terms of an abstract Hecke algebra. If we define (for $f\in[\Gamma_0(p),k,\chi]$ and $G=(\mathbb{F}_p^\times)^2$)

$$f\mid T(i)_\chi := \chi(a)\mid \Gamma^G W(i,a)\Gamma^G,$$

then this is independent of the choice of $a\in\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ and defines an endomorphism of $[\Gamma_0(p),k,\chi]$. Clearly, $\overline{\tau(i)}\longmapsto T(i)_\chi$ defines a homomorphism from $\overline{\mathcal{H}}_{p,\chi}$ to the endomorphism ring of $[\Gamma_0(p),k,\chi]$, and we obtain that $T(n)_\chi$ satisfies a relation of degree $\frac{n}{2}+1$ if n is even and $T(n)_\chi^2$ satisfies a relation of degree $\frac{n+1}{2}$ if n is odd.

5. Examples

We start with two general remarks, which are helpful in understanding the examples below.

Remark 5. In the case $G=\mathbb{F}_p$ the mapping ψ_n always has the eigenvalue $p^{\frac{n(n+1)}{2}}$ with eigenvector $\phi_n:=\sum_{i=0}^n\tau(1,i)$. As a union of double cosets, ϕ_n equals $\mathrm{Sp}(n,\mathbb{F}_p)$; multiplication with the elements of $\tau(1,n)$ just permutes the elements of $\mathrm{Sp}(n,\mathbb{F}_p)$; the eigenvalue is then equal to the number of left cosets in $\tau(1,n)$.

Remark 6. Here we consider the case $G = (\mathbb{F}_p^\times)^2$ and a nontrivial quadratic character mod p. The case $p \equiv 3 \bmod 4$ is more complicated than $p \equiv 1 \bmod 4$. There are two reasons, which both bring up sign changes in the formulas for the matrix $\overline{\psi}_{n,\chi}$ (when compared with the formulas for the case $p \equiv 1 \bmod 4$). The first reason is the change from $a \in \{1, \epsilon\}$ to $(-1)^{i-r} \cdot a$ in the formulas of Section 2. The second reason is the quadratic residue symbol $\left(\frac{(-1)^{\frac{r}{2}} \det(S)}{p}\right)$, which occurs in the formula for $\#\mathrm{O}(S)(\mathbb{F}_p)$ (with S a symmetric matrix of even size r).

Then (for $0 \le i, j \le n$) there are polynomials α_{ij} and β_{ij} such that the entries of the matrix $\overline{\psi}_{n,\chi}$ are given by $\alpha_{ij}(p)$ for $p \equiv 1 \bmod 4$ and by $\beta_{ij}(p)$ for $p \equiv 3 \bmod 4$. They satisfy (with $j = n - i + r$)

$$\beta_{ij}(p) = (-1)^{i+\frac{r}{2}} \alpha_{ij}(p).$$

Example 5.1.[*1] $n = 2$, $G = \mathbb{F}_p^\times$. The matrix ψ_2 is then a 3×3 matrix:

$$\psi_2 = \begin{bmatrix} & & p^3 \\ & p^2 & p^2(p-1) \\ 1 & p^2 - 1 & p^2(p-1) \end{bmatrix}.$$

The characteristic polynomial is

$$(X - p)(X + p)(X - p^3).$$

These eigenvalues also occur in [11].

Example 5.2. $n = 3$, $G = \mathbb{F}_p^\times$

$$\psi_3 = \begin{bmatrix} & & & p^6 \\ & & p^5 & p^6 - p^5 \\ & p^3 & p^5 - p^3 & p^6 - p^5 \\ 1 & p^3 - 1 & (p^3 - 1)p^2 & p^2(p-1)(p^3-1) \end{bmatrix}.$$

The characteristic polynomial is

$$(X - p^6)(X - p^2)(X + p^3)^2,$$

the minimal polynomial however is of degree 3 (this is *not* explained by our general statements!).

Example 5.3. $n = 3$, χ the nontrivial quadratic character mod p with $p \equiv 1$ modulo 4. We study the matrix for the multiplication by $\overline{\tau(3)}$ in $\overline{\mathcal{H}}_{p,\chi}$, reasonably called $\overline{\psi}_{n,\chi}$:

[*1] This example was shown to me by Professor Ueda; he obtained it by a method, which is somewhat different from the one in Section 2.

$$\overline{\psi}_{3,\chi} = \begin{bmatrix} & & & p^6 \\ & & p^5 & 0 \\ & p^3 & 0 & p^5 - p^4 \\ 1 & 0 & p(p^3-1) & 0 \end{bmatrix}.$$

The characteristic polynomial is

$$(X^2 - p^9)(X^2 - p^5).$$

It is a polynomial in X^2 of degree 2 in accordance with Proposition 4.2. For $p \equiv 3 \bmod 4$ the characteristic polynomial is then (for $n = 3$) equal to

$$(X^2 + 9) \cdot (X^2 + p^5),$$

and the minimal polynomial is again of degree 3.

Example 5.4. $n = 4$ and χ a nontrivial quadratic character. Then

$$\overline{\psi}_{4,\chi} = \begin{bmatrix} & & & & p^{10} \\ & & & \chi(-1)p^9 & 0 \\ & & p^7 & 0 & \chi(-1)(p^9 - p^8) \\ & \chi(-1)p^4 & 0 & p^8 - p^5 & 0 \\ 1 & 0 & \chi(-1)p(p^3-1)(p^2+1) & 0 & p^4(p-1)(p^3-1) \end{bmatrix}$$

For $p \equiv 1 \bmod 4$ this gives the characteristic polynomial

$$(X - p^8)^2(X + p^5)^2(X - p^4).$$

The minimal polynomial is of degree 3 as predicted by Proposition 4.2. For $p \equiv 3 \bmod 4$ we obtain the same characteristic polynomial and minimal polynomial.

Remark 7. We can write down (for $G = \mathbb{F}_p^\times$) an explicit expression for the inverse $\tau(n)^{-1}$ in the form

$$\sum x_i \cdot \tau(i),$$

where the x_i are the entries of the first column in the matrix ψ_n^{-1}. A similar statement holds for the inverse of $\overline{\tau(n)}^{-1}$ in the case of a nontrivial character. From this one can also deduce an explicit expression for the inverse of the operator $U(p)$.

6. On not square-free cases

Injectivity of $U(p)$ does not hold in general on $[\Gamma_0(M), k, \chi]$ if $p^2 \mid M$. The situation is much better if the conductor of χ is sufficiently large. To illustrate this, we consider the case $M = p^N$ with $N \geq 2$ (the generalization to $M = p^N \cdot M'$ with M coprime to p is then straightforward).

Proposition 6.1. *The operator $U(p)$ is injective on $[\Gamma_0(p^N), k, \chi]$ provided that $N \geq 2$ and χ is primitive mod p^N.*

Proof (adopted from Theorem 3 in [8]). For integral symmetric matrices L and C of size n we start from the commutation rule

$$\begin{bmatrix} \mathbf{1}_n & L \\ 0_n & p \cdot \mathbf{1}_n \end{bmatrix} \cdot \begin{bmatrix} \mathbf{1}_n & 0_n \\ p^{N-1} \cdot C & \mathbf{1}_n \end{bmatrix}$$
$$= \underbrace{\begin{bmatrix} \mathbf{1}_n + p^{N-1} \cdot L \cdot C & -p^{N-2} \cdot L \cdot C \cdot L \\ p^N \cdot C & \mathbf{1}_n - p^{N-1} \cdot C \cdot L \end{bmatrix}}_{\in \Gamma_0(p^N)} \cdot \begin{bmatrix} \mathbf{1}_n & L \\ 0_n & p \cdot \mathbf{1}_n \end{bmatrix}.$$

Suppose now that we have $f \in [\Gamma_0(p^N), k, \chi]$ with $f \mid U(p) = 0$. Then we get for all C

$$0 = p^{\frac{n(n+1)}{2} - \frac{nk}{2}} \cdot (f \mid U(p)) \mid_k \begin{bmatrix} \mathbf{1}_n & 0_n \\ p^{N-1} \cdot C & \mathbf{1}_n \end{bmatrix}$$
$$= \sum_L f \mid_k \begin{bmatrix} \mathbf{1}_n & L \\ 0_n & p \cdot \mathbf{1}_n \end{bmatrix} \cdot \begin{bmatrix} \mathbf{1}_n & 0_n \\ p^{N-1} \cdot C & \mathbf{1}_n \end{bmatrix}$$
$$= \sum_L \chi(\det(\mathbf{1}_n - p^{N-1} \cdot C \cdot L)) f \mid_k \begin{bmatrix} \mathbf{1}_n & L \\ 0_n & p \cdot \mathbf{1}_n \end{bmatrix}.$$

We use the elementary formula

$$\chi(\det(\mathbf{1}_n - p^{N-1} \cdot C \cdot L)) = \chi(1 - p^{N-1} \mathrm{tr}(C \cdot L)).$$

Then we put

$$\xi = \chi(1 - p^{N-1})$$

and observe that ξ is a primitive p-th root of unity; moreover,

$$\chi(\det(\mathbf{1}_n - p^{N-1} \cdot C \cdot L)) = \chi(1 - p^{N-1} \mathrm{tr}(C \cdot L)) = \xi^{\mathrm{tr}(C \cdot L)}.$$

For all symmetric integral C we have

$$0 = \sum_L \xi^{tr(C \cdot L)} f \mid \begin{bmatrix} \mathbf{1}_n & L \\ 0_n & p \cdot \mathbf{1}_n \end{bmatrix}.$$

The functions

$$\xi_L : \begin{cases} \mathrm{Sym}^n(\mathbb{F}_p) & \longrightarrow & \mathbb{C}^\times \\ C & \longmapsto & \xi^{\mathrm{tr}(C \cdot L)} \end{cases}$$

with $L \in \mathrm{Sym}^n(\mathbb{F}_p)$ make up the set of characters of the additive group $(\mathrm{Sym}^n(\mathbb{F}_p), +)$. The linear independence of pairwise different characters then implies $f = 0$. □

7. Final remarks

• The case $p = 2$ was excluded above mainly to keep the formulation simple. The main results (in particular the injectivity of $U(2)$) can be obtained along the same lines.

• Most considerations of Sections 1 and 2 work over an arbitrary finite field (not just $\mathbb{F}_p$).

• It is clear that with a slightly more complicated notation, the results above also hold true for any level N with $p \mid\mid N$ (instead of prime level).

• For relations of our considerations with the representation theory of finite groups (in particular $\mathrm{Ind}_P^{\mathrm{Sp}(n,\mathbb{F}_p)}(\chi \circ \det)$, where P is the Siegel parabolic subgroup), we refer to [11] and much more generally [6].

• Related questions for Iwahori subgroups were considered in [9], [11] for the case of Sp(2); a proof for the injectivity of $U(p)$ in the Iwahori case is given in the appendix.

8. Appendix: The case of Iwahori subgroups (by Ralf Schmidt)

In this appendix we shall give a different approach to the injectivity of the Hecke operator $U(p)$, which uses the structure theory of Iwahori–Hecke algebras. However, we will not obtain the more refined results of the previous sections.

Invertibility in the Iwahori–Hecke algebra

Let F be a p–adic field, $\mathfrak{o}$ its ring of integers, $\mathfrak{p}$ the maximal ideal, and ϖ a generator of $\mathfrak{p}$. Let G denote the algebraic F–group $\mathrm{GSp}(n) = \{g \in \mathrm{GL}(2n) : {}^t gJg = \lambda(g)J \text{ for some } \lambda(g) \in \mathrm{GL}(1)\}$, where $J = \begin{bmatrix} & \mathbf{1}_n \\ \mathbf{1}_n & \end{bmatrix}$. Conjugation with

$$c = \begin{bmatrix} J_n & \\ & \mathbf{1}_n \end{bmatrix}, \qquad \text{where } J_n = \begin{bmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{bmatrix}$$

provides an isomorphism of G with the more symmetric version of the symplectic group that is defined using the symplectic form $\begin{bmatrix} & J_n \\ -J_n & \end{bmatrix}$. The *Iwahori subgroup* $I \subset G(\mathfrak{o})$ consists of all matrices g such that cgc^{-1} is upper triangular mod $\mathfrak{p}$. The *Atkin–Lehner element*

$$u = \begin{bmatrix} & -J_n \\ \varpi J_n & \end{bmatrix} \tag{8.1}$$

normalizes I. The *Iwahori–Hecke algebra* $\mathcal{I}$ is the convolution algebra of left and right I–invariant functions $G(F) \to \mathbb{C}$. The simple Weyl group elements are

$$s_i = c \begin{bmatrix} \mathbf{1}_{i-1} & & & & & & \\ & 0 & 1 & & & & \\ & 1 & 0 & & & & \\ & & & \mathbf{1}_{2n-2i-2} & & & \\ & & & & 0 & 1 & \\ & & & & 1 & 0 & \\ & & & & & & \mathbf{1}_{i-1} \end{bmatrix} c^{-1}, \qquad i = 1, \dots, n-1,$$

and

$$s_n = c \begin{bmatrix} \mathbf{1}_{n-1} & & & \\ & 0 & 1 & \\ & -1 & 0 & \\ & & & \mathbf{1}_{n-1} \end{bmatrix} c^{-1}.$$

These elements generate the spherical Weyl group of $\mathrm{GSp}(n)$, which has $2^n n!$ elements. The elements $s_1, \dots, s_{n-1}$ generate the Weyl group of $\mathrm{GL}(n)$. The (infinite) affine Weyl group is generated by the s_i and $s_0 := us_nu^{-1}$. Let e be the characteristic function of I (the identity element in $\mathcal{I}$), η the characteristic function of uI and e_i the characteristic function of Is_iI. Then the Iwahori–Hecke algebra is known to be generated by η and the e_i, $i = 1, \dots, n$. The relation

$$e_i^2 = (q-1)e_i + qe, \qquad q = \#\mathfrak{o}/\mathfrak{p}, \tag{8.2}$$

shows that each e_i is invertible in $\mathcal{I}$, the inverse being $q^{-1}e_i - (1-q^{-1})e$. More generally we have:

Lemma 8.1. *For any element $g \in G(F)$, the characteristic function of IgI is invertible as an element of $\mathcal{I}$.*

Proof. This is well known; see [3]. We recall the argument. After multiplying with powers of the Atkin–Lehner element η, we may assume that $\det(g) \in \mathfrak{o}^*$. By general structure theory,

$$\{h \in G(F) : \det(h) \in \mathfrak{o}^*\} = \bigsqcup_{w \in W} IwI,$$

where W is the affine Weyl group. Hence we may assume that g is a Weyl group element. Choose a representation $g = s_{i_1} \cdot \ldots \cdot s_{i_m}$ of minimal length, where each s_{i_j} is one of the simple reflections from above. Then the length of $s_{i_1} \cdot \ldots \cdot s_{i_j}$ is j. The multiplication rules in the Hecke algebra show that, for any Weyl group element w, if the length of ws_i is greater than the length of w, then

$$\mathrm{char}(IwI) \cdot \mathrm{char}(Is_iI) = \mathrm{char}(Iws_iI).$$

Consequently $\mathrm{char}(IgI) = \mathrm{char}(Is_{i_1}I) \cdot \ldots \cdot \mathrm{char}(Is_{i_m}I) = e_{i_1} \cdot \ldots \cdot e_{i_m}$ is a product of invertible elements. $\square$

The invertibility of the $U(p)$ operator on spaces of modular forms will follow from this lemma, but we have to clarify the relation between local and global Hecke algebras.

The case of trivial nebentypus

For a positive integer N let $\Gamma_I(N) \subset \mathrm{Sp}(n, \mathbb{Z})$ be the global analogue of the Iwahori subgroup. Since $\Gamma_I(N) \subset \Gamma_0(N)$, we have $[\Gamma_I(N), k] \supset [\Gamma_0(N), k]$. On the bigger space we have the Hecke operator $\Gamma_I(N)\mathrm{diag}(\mathbf{1}_n, p\mathbf{1}_n)\Gamma_I(N)$, and on the smaller space we have the Hecke operator $\Gamma_0(N)\mathrm{diag}(\mathbf{1}_n, p\mathbf{1}_n)\Gamma_0(N)$. It is easy to see that the inclusion induces a bijection

$$\Gamma_I(N)\backslash(\Gamma_I(N)\begin{bmatrix}\mathbf{1}_n & \\ & p\mathbf{1}_n\end{bmatrix}\Gamma_I(N)) \cong \Gamma_0(N)\backslash(\Gamma_0(N)\begin{bmatrix}\mathbf{1}_n & \\ & p\mathbf{1}_n\end{bmatrix}\Gamma_0(N)).$$

Hence both Hecke operators coincide on the smaller space. We shall denote both operators by $U(p)$. Our goal is to show that $U(p)$ is injective if $p||N$, and it is enough to show this for the Iwahori case.

Let $F \in [\Gamma_I(N), k]$. Let $\mathbb{A}$ be the ring of adeles of $\mathbb{Q}$. We shall associate to F a function on the adelic group $G(\mathbb{A})$, as follows. Let $K_p = G(\mathbb{Z}_p)$ for $p \nmid N$ and $K_p = I(p)$, the local Iwahori subgroup at p, for $p|N$. By strong approximation, and since the determinant function on the local groups K_p is onto $\mathbb{Z}_p^*$, we have $G(\mathbb{A}) = G(\mathbb{Q})G(\mathbb{R})^+\prod_{p<\infty} K_p$, where $G(\mathbb{R})^+$ stands for those elements of $G(\mathbb{R})$ with positive multiplier. Given $g \in G(\mathbb{A})$, write $g = \rho g_\infty \kappa$ according to this decomposition, where $\kappa \in \prod_{p<\infty} K_p$. We define $\Phi = \Phi_f$ by $\Phi(g) = (F|_k g_\infty)(I)$, where $I = i\mathbf{1}_{2n}$ and

$$(F|_k h)(Z) = \lambda(h)^k \det(CZ + D)^{-k} F(h\langle Z\rangle) \qquad \text{for } h = \begin{bmatrix} A & B \\ C & D\end{bmatrix} \in G(\mathbb{R})^+$$

(note the slight difference with the definition (3.1)). Then Φ is a well-defined function $G(\mathbb{A}) \to \mathbb{C}$ and satisfies $\Phi(\rho g \kappa) = \Phi(g)$ for $\rho \in G(\mathbb{Q})$ and $\kappa \in \prod_{p<\infty} K_p$. We obtain an isomorphism of $[\Gamma_I(N), k]$ with a (finite-dimensional) space $\mathcal{A}_I(N, k)$ of adelic functions.

Let $g \in M(2n, \mathbb{Z})$ be a matrix with non-zero determinant. The double coset $\Gamma_I(N)g\Gamma_I(N)$ in the Hecke algebra for $\Gamma_I(N)$ defines an endomorphism of $[\Gamma_I(N), k]$. Locally, we fix a prime number p and let I be the Iwahori subgroup in $G(\mathbb{Z}_p)$. Let $\mathcal{I}$ be the Iwahori–Hecke algebra at p, consisting of left and right I invariant functions on $G(\mathbb{Q}_p)$. Assuming that $p||N$, the Iwahori–Hecke algebra acts on $\mathcal{A}_I(N, k)$, and the following diagram is commutative.

$$\begin{array}{ccc} [\Gamma_I(N), k] & \xrightarrow{\sim} & \mathcal{A}_I(N, k) \\ {\scriptstyle \Gamma_I(N)g\Gamma_I(N)}\downarrow & & \downarrow{\scriptstyle \mathrm{char}(Ig^{-1}I)} \\ [\Gamma_I(N), k] & \xrightarrow{\sim} & \mathcal{A}_I(N, k) \end{array} \tag{8.3}$$

For the injectivity of $U(p)$ on $[\Gamma_I(N), k]$ it is therefore enough to show that the characteristic function of $I\mathrm{diag}(\mathbf{1}_n, p^{-1}\mathbf{1}_n)I$ is invertible in $\mathcal{I}$. But this is just a special case of Lemma 8.1. To summarize:

Proposition 8.1. *Let N be a positive integer and p a prime number with $p||N$.*

i) *The operator* $U(p) = \Gamma_I(N)\begin{bmatrix}\mathbf{1}_n & \\ & p\mathbf{1}_n\end{bmatrix}\Gamma_I(N)$ *on* $[\Gamma_I(N), k]$ *is injective.*

ii) *The operator* $U(p) = \Gamma_0(N)\begin{bmatrix}\mathbf{1}_n & \\ & p\mathbf{1}_n\end{bmatrix}\Gamma_0(N)$ *on* $[\Gamma_0(N), k]$ *is injective.*

Both operators $U(p)$ coincide on the smaller space $[\Gamma_0(N), k]$.

Non-trivial nebentypus

The case of non-trivial nebentypus is slightly more difficult. For notational simplicity we shall assume that $N = p$ is a prime number. As mentioned in (4.1) we have $[\Gamma_1(p), k] = \oplus_\chi[\Gamma_0(p), k, \chi]$, where χ runs through all Dirichlet characters mod p. The endomorphism $U(p) = \Gamma_1(p)\mathrm{diag}(\mathbf{1}_n, p\mathbf{1}_n)\Gamma_1(p)$ of $[\Gamma_1(p), k]$ leaves each of the subspaces $[\Gamma_0(p), k, \chi]$ invariant. Similarly as before we shall prove that $U(p)$ is invertible by switching to a smaller congruence subgroup. Define $\Gamma_{I_1}(p)$ to be the subgroup of $\Gamma_I(p)$ consisting of matrices whose diagonal elements are congruent 1 mod p. Then $\Gamma_{I_1}(p) \subset \Gamma_1(p)$, and therefore $[\Gamma_{I_1}(p), k] \supset [\Gamma_1(p), k]$. On the bigger space we have the operator $U(p) = \Gamma_{I_1}(p)\mathrm{diag}(\mathbf{1}_n, p\mathbf{1}_n)\Gamma_{I_1}(p)$. The notation is unambigous since the restriction of this $U(p)$ to $[\Gamma_1(p), k]$ coincides with the previously defined $U(p)$. This follows because the inclusion induces a bijection

$$\Gamma_{I_1}(p)\backslash(\Gamma_{I_1}(p)\begin{bmatrix}\mathbf{1}_n & \\ & p\mathbf{1}_n\end{bmatrix}\Gamma_{I_1}(p)) \cong \Gamma_1(p)\backslash(\Gamma_1(p)\begin{bmatrix}\mathbf{1}_n & \\ & p\mathbf{1}_n\end{bmatrix}\Gamma_1(p)),$$

which is easy to check. Note that both groups $\Gamma_1(p)$ and $\Gamma_{I_1}(p)$ are normalized by the Atkin–Lehner element $\begin{bmatrix} & -J_n \\ pJ_n & \end{bmatrix}$.

The local analogue of the congruence subgroup $\Gamma_{I_1}(p)$ is the subgroup I_1 of the Iwahori subgroup $I \subset G(\mathfrak{o})$ consisting of matrices whose diagonal elements are in $1 + \mathfrak{p}$. However, I_1 is not suitable for lifting modular forms to adelic functions, since the multiplier map on I_1 is not onto $\mathfrak{o}^*$. We therefore define $\tilde{I}_1$ as the group generated by I_1 and elements $\mathrm{diag}(a\mathbf{1}_n, \mathbf{1}_n)$, $a \in \mathfrak{o}^*$.

As before an element $F \in [\Gamma_{I_1}(p), k]$ can then be lifted to an adelic function Φ, which is invariant on the right under $\tilde{I}_1(p)$. We get a space of adelic functions $\widetilde{\mathcal{A}}_1(p, k)$. Let $\widetilde{\mathcal{I}}_1$ (resp. $\mathcal{I}_1$) be the Hecke algebra consisting of left and right $\tilde{I}_1$ invariant (resp. I_1 invariant) functions on $\mathrm{GSp}(2n, \mathbb{Q}_p)$. Then $\widetilde{\mathcal{A}}_1(p, k)$ is a representation space for $\widetilde{\mathcal{I}}_1$, but not for $\mathcal{I}_1$. We shall slightly enlarge $\widetilde{\mathcal{A}}_1(p, k)$ to obtain a space on which $\mathcal{I}_1$ acts. Namely, let V be the space of functions on $G(\mathbb{A})$ spanned by *all* right translates of functions in $\widetilde{\mathcal{A}}_1(p, k)$ by elements of $G(\mathbb{Q}_p)$. Then V is a smooth representation of $G(\mathbb{Q}_p)$. Let $\mathcal{A}_1(p, k)$ be the subspace of I_1 invariant functions. Then $\mathcal{I}_1$ acts on $\mathcal{A}_1(p, k)$, and $\widetilde{\mathcal{A}}_1(p, k)$ is a (not necessarily invariant) subspace. Let $g = \begin{bmatrix}\mathbf{1}_n & \\ & p\mathbf{1}_n\end{bmatrix}$. Since $\tilde{I}_1 g \tilde{I}_1/\tilde{I}_1 \simeq I_1 g I_1/I_1$ we get a commutative diagram

(8.4)
$$\begin{array}{ccccc}
[\Gamma_{I_1}(p), k] & \xrightarrow{\sim} & \widetilde{\mathcal{A}}_1(p, k) & \longrightarrow & \mathcal{A}_1(p, k) \\
{\scriptstyle U(p)=\Gamma_{I_1}(p)g\Gamma_{I_1}(p)}\downarrow & & \downarrow{\scriptstyle \mathrm{char}(\tilde{I}_1 g^{-1}\tilde{I}_1)} & & \downarrow{\scriptstyle \mathrm{char}(I_1 g^{-1} I_1)} \\
[\Gamma_{I_1}(p), k] & \xrightarrow{\sim} & \widetilde{\mathcal{A}}_1(p, k) & \longrightarrow & \mathcal{A}_1(p, k)
\end{array}$$

It is therefore enough to show that $\mathrm{char}(I_1 g^{-1} I_1)$ is invertible in $\mathcal{I}_1$. We do not have a complete structure theorem for $\mathcal{I}_1$, but consider the sub-algebra $\widehat{\mathcal{I}}_1$ generated by the elements $\hat{e}_i = \mathrm{char}(I_1 s_i I_1)$, where the s_i are the simple reflections defined above, and by $\hat{\eta} = \mathrm{char}(uI_1)$, where u is the Atkin–Lehner element. It is easily checked that for the $\hat{e}_i$ we have the same quadratic relation (8.2) as for the $e_i \in \mathcal{I}$. In fact, we can define an isomorphism of vector spaces $\mathcal{I} \longrightarrow \widehat{\mathcal{I}}_1$ by sending the characteristic function of $Iu^m wI$ to the characteristic function of $I_1 u^m w I_1$. Note here that each double coset IhI has a unique representative of the form $u^m w$ with $m \in \mathbb{Z}$ and a Weyl group element w. This isomorphism sends e_i to $\hat{e}_i$ and η to $\hat{\eta}$, and it is an exercise to show that the map is an isomorphism of algebras (in fact, $I_1 w I_1 / I_1 \simeq IwI/I$ for each $w \in W$). It therefore follows from Lemma 8.1 that $\mathrm{char}(I_1 g^{-1} I_1)$ is invertible in $\widehat{\mathcal{I}}_1$, and then also in $\mathcal{I}_1$. We summarize:

Proposition 8.2. *Let N be a positive integer and p a prime number with $p||N$.*

i) *The operator* $U(p) = \Gamma_{I_1}(N) \begin{bmatrix} \mathbf{1}_n & \\ & p\mathbf{1}_n \end{bmatrix} \Gamma_{I_1}(N)$ *on* $[\Gamma_{I_1}(N), k]$ *is injective.*

ii) *The operator* $U(p) = \Gamma_1(N) \begin{bmatrix} \mathbf{1}_n & \\ & p\mathbf{1}_n \end{bmatrix} \Gamma_1(N)$ *on* $[\Gamma_1(N), k]$ *is injective. Both operators $U(p)$ coincide on the smaller space* $[\Gamma_1(N), k]$.

Remark on Atkin–Lehner elements. On the space $[\Gamma_0(p), k]$ the element $W_p = \begin{bmatrix} & -\mathbf{1}_n \\ p\mathbf{1}_n & \end{bmatrix}$ defined in (3.3) has the same effect as the Atkin–Lehner element $u_p = \begin{bmatrix} & -J_n \\ pJ_n & \end{bmatrix}$. In the Iwahori approach to injectivity of $U(p)$ we were forced to work with u_p, since this element normalizes Iwahori-type subgroups while W_p does not.

Kunzenhof 4b
79117 Freiburg
Germany
e-mail: boecherer@t-online.de

Department of Mathematics
University of Oklahoma
Norman, OK 73019-0315
USA
e-mail: rschmidt@math.ou.edu

References

[1] A. Andrianov, *Quadratic Forms and Hecke Operators*, Springer, 1987.

[2] S. Böcherer, H. Katsurada and R. Schulze-Pillot, *The basis problem for Siegel modular forms of large weight and square-free level*, in preparation.

[3] A. Borel, *Admissible representations of a semisimple group over a local field with vectors fixed by an Iwahori subgroup*, Invent. Math **35** (1976), 233–259.

[4] E. Freitag, *Siegelsche Modulfunktionen*, Springer, 1983.

[5] E. Hecke, *Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung* II, Math. Ann. **114** (1937), 316–351 (Mathematische Werke Nr. 36).

[6] R. B. Howlett and G. I. Lehrer, *Induced cuspidal representations and generalized Hecke rings*, Invent. Math. **58** (1980), 37–64.

[7] T. Miyake, *Modular Forms*, Springer, 1989.

[8] A. Ogg, *On eigenvalues of Hecke operators*, Math. Ann. **179** (1969), 101–108.

[9] R. Schmidt, *Iwahori-spherical representations of GSp*(2) *and Siegel modular forms of degree* 2 *with square-free level*, to appear in J. Math. Soc. Japan.

[10] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen* I, Ann. of Math. **36** (1935), 527–606.

[11] H. Yoshida, *On representations of finite groups in the space of Siegel modular forms and theta series*, J. Math. Kyoto Univ. **28** (1988), 343–372.