On Galois Representations via Siegel Modular Forms of Genus Two

MICHAEL DETTWEILER †, ULF KÜHN AND STEFAN REITER †

e-mail: michael.dettweiler@iwr.uni-heidelberg.de

We study 4-dimensional Galois representations attached to Siegel modular forms. In some cases we determine the images of the absolute Galois group. This yields Galois realizations over $\mathbb{Q}$ for projective symplectic groups.

1. Introduction

It is well known that to classical modular forms there are attached two-dimensional l-adic representations of the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}} : \mathbb{Q})$, see Deligne [6]. Ribet [15] has studied the images of $G_{\mathbb{Q}}$ and proved that they are almost always "as big as possible". In particular, by considering modular forms of weight 24, he showed that the groups $PSl(2, l^2)$ occur as Galois groups over $\mathbb{Q}$ if $l \neq 47$ and 144169 is a quadratic non-residue modulo l. Reverter and Vila [14] subsequently realized many other groups $PGl(2, l^{2m-1})$ and $PSl(2, l^{2m})$ as Galois groups over $\mathbb{Q}$ by considering modular forms of higher weights.

Results of Weissauer [24] associate four-dimensional Galois representations to Siegel modular forms of genus two (more generally, to any irreducible cuspidal automorphic representation of $GSp(4, \mathbb{A})$, $\mathbb{A}$ being the ring of adeles of $\mathbb{Q}$, whose component at infinity belongs to the holomorphic discrete series, see Theorem 3.1). We study the Galois representations attached to the unique (up to normalization and Galois conjugation) Siegel modular eigenform Υ of weight 28 on the full Siegel modular group $Sp(4, \mathbb{Z})$ which is a cusp form and does not lie in the Maass Spezialschar. The first Fourier coefficients of Υ were determined by Skoruppa [18], [19].

The case of weight 28 is the smallest one where non-Maass, non-Eisenstein eigenforms exist whose Fourier coefficients do not lie completely in $\mathbb{Q}$ (see [18]) – so there is the chance of finding new Galois groups (see Remark 6.3 for details).

We use the following method to determine the image of $G_{\mathbb{Q}}$: We consider the image modulo λ, where λ is a prime of some number field. Then we use the explicitly given characteristic polynomials of the images of the Frobenius elements, combining the results of Weissauer and Skoruppa, to find semisimple elements in the image which do not fit simultaneously into any smaller subgroup than $Sp(4, l^n)$.

† The first and the third author want to thank the Deutsche Forschungsgemeinschaft for financial support.

We show that infinitely many of the groups $PSp(4,l^2)$ and $PGSp(4,l'^3)$ (especially $PSp(4,19^2)$ and $PGSp(4,53^3)$) occur as Galois groups over $\mathbb{Q}$, see Thm 6.2 i) and ii). The corresponding Galois extensions are unramified outside l and l', resp.. An argument similar to a result of Serre-Ribet, see Lemma 2.2, then implies that the corresponding λ-adic inverse images also occur as Galois groups over $\mathbb{Q}$.

We thank Professor Weissauer for providing us with his preprints and for valuable discussions. Further we thank J. Hartmann, J. Klüners, Professor Kramer and Professor Matzat for helpful comments.

2. Lifting modular representations and reducing l-adic representations

In this section we collect some general results about l-adic representations which will be useful later.

Notation 2.1. We denote by $\overline{K}$ an algebraic closure of a field K. By $\mathbb{P}$ we denote the set of primes of $\mathbb{N}$. If $p \in \mathbb{P}$, we denote by Frob_p a Frobenius element of the absolute Galois group $\mathrm{G}_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, see [16]. If E is a number field and λ is a place of E, we denote by E_λ the completion of E with respect to λ. If K is a local field then we denote by O_K (resp. m_K, k_K) its ring of integers (resp. the maximal ideal of O_K, its residue field).

Lemma 2.2. *Let K be a finite extension of $\mathbb{Q}_l$, $l \geq 5$. Suppose that $\mathcal{G}$ is a closed subgroup of $GSp(n, O_K)$ whose image "mod l" contains $Sp(n, O_K/lO_K)$. Then $\mathcal{G}$ contains the group $Sp(n, O_K)$.*

Proof. This is analogous to the proof of Thm. 2.1 of Ribet [15]. The argument of Serre (as given in [15], p. 250) applies, if we can show that the Lie algebra $sp(n,q)$ "mod λ" of $Sp(n,q)$ is generated by nilpotent elements of degree two (here λ denotes an extension of l to K such that $k_K = \mathbb{F}_q$):

By the Cartan decomposition, see [3], we have

$$sp(n,q) = \mathfrak{t} \oplus \sum_{\alpha \in \Omega} \mathfrak{x}_\alpha,$$

where $\mathfrak{t}$ is the Lie algebra of a maximally split torus T, Ω denotes the root system and $\mathfrak{x}_\alpha$ is the root space of α ("mod λ"). Any element of $\mathfrak{x}_\alpha$, $\alpha \in \Omega$, is nilpotent of degree two. Thus it suffices to prove the claim for the elements of $\mathfrak{t}$, which are of the form $\mathrm{diag}(D, -D)$, where $D \in \mathrm{Mat}_{n/2}(q)$ is a diagonal matrix. These elements can be written as

$$\begin{pmatrix} D & 0 \\ 0 & -D \end{pmatrix} = 1/2 \begin{pmatrix} D & D \\ -D & -D \end{pmatrix} + 1/2 \begin{pmatrix} D & -D \\ D & -D \end{pmatrix},$$

where the summands on the right hand side lie in $sp(n,q)$ and are nilpotent of degree two. $\square$

Lemma 2.3. *Let $\tilde{K}$ be a finite extension of $\mathbb{Q}_l$ and $\rho : \mathrm{G}_\mathbb{Q} \mapsto Gl(n, \tilde{K})$ be a continuous representation which is unramified outside a finite set $S \subseteq \mathbb{P}$ of primes. Let $K \subseteq \tilde{K}$ be the field which is generated over $\mathbb{Q}_l$ by the coefficients of the characteristic polynomials* *of all* $\rho(\mathrm{Frob}_p)$, $p \in \mathbb{P} \setminus S$. *Let further*

$$\bar{\ }: O_{\tilde{K}} \longrightarrow k_{\tilde{K}} \subseteq \overline{\mathbb{F}}_l$$

denote the reduction modulo $m_{\tilde{K}}$. *Set* $\mathbb{F}_q = k_K \subseteq k_{\tilde{K}}$. *Then there exists a representation*

$$\hat{\rho} : \mathrm{G}_{\mathbb{Q}} \longrightarrow Gl(n, \mathbb{F}_q),$$

such that ρ *factors through it and*

$$\overline{\det(1 - X \cdot \rho(\mathrm{Frob}_p))} = \det(1 - \overline{X} \cdot \hat{\rho}(\mathrm{Frob}_p)).$$

Proof. By compactness, we can assume that the image of ρ is contained in $Gl(n, O_{\tilde{K}})$. Let $\overline{\rho} : \mathrm{G}_{\mathbb{Q}} \to Gl(n, \overline{\mathbb{F}}_l)$ be the composition of ρ with the reduction modulo $m_{\tilde{K}}$. Let $\overline{\rho}_{ss}$ be the semisimplification of $\overline{\rho}$ in the sense of Serre [16], I-10. The character $\mathrm{tr}(\overline{\rho}_{ss})$ decomposes over $\overline{\mathbb{F}}_l$ into the sum of irreducible characters $\chi_1 + \ldots + \chi_r$. The operation of the standard Frobenius $F : x \mapsto x^q$, permutes the $\chi_1, \ldots, \chi_r$ (it follows from the Brauer-Nesbitt theorem, see [5], Thm 30.16, that $\overline{\rho}_{ss}$ and $\overline{\rho}_{ss}^F$ have the same composition series because the characteristic polynomials of the Frobenius elements $\overline{\rho}_{ss}(\mathrm{Frob}_p)$ remain unchanged). Now the theorem of Lang-Steinberg (see [3], p. 32) implies that $\overline{\rho}_{ss}$ is equivalent to a representation $\hat{\rho} : \mathrm{G}_{\mathbb{Q}} \to Gl(n, \mathbb{F}_q)$. □

3. Galois representations attached to Siegel modular forms

The following theorem will be essential for our considerations:

Theorem 3.1. (Weissauer [24]) *Suppose that* Π *is a unitary cuspidal irreducible automorphic representation of* $GSp(4, \mathbb{A})$ *(*$\mathbb{A}$ *denotes the ring of adeles of* $\mathbb{Q}$*) such that* Π_∞ *belongs to the holomorphic discrete series of weight* (k_1, k_2). *Set* $w := k_1 + k_2 - 3$. *Let* S *denote the set of ramified places of the representation* Π. *Then there exists a number field* E *such that for primes* $p \notin S$ *the local* L*-factor*

$$Q_p(p^{-s}) = L_p(\Pi_p, s - \frac{w}{2}), \quad L_p(X)^{-1} \in E[X],$$

of the degree 4 *spinor* L*-series (suitably normalized) has coefficients in* E, *and such that for any prime number* l *and any extension* λ *of* l *to* E *there exists a four dimensional semisimple Galois representation*

$$\rho_{\Pi,\lambda} : \mathrm{G}_{\mathbb{Q}} \to Gl(4, \overline{E}_\lambda),$$

which is unramified outside $S \cup \{l\}$ *and for* $p \notin S \cup \{l\}$ *the following holds*

$$L_p(\Pi_p, s - \frac{w}{2}) = det(1 - \rho_{\Pi,\lambda}(\mathrm{Frob}_p)p^{-s})^{-1}.$$

First we want to reformulate the above theorem according to our situation:

Let f be a classical Siegel modular form of even weight k on the full Siegel modular group $Sp(4, \mathbb{Z})$ which is a cusp form and a simultaneous eigenform for all Hecke operators $T(n)$, $n \in \mathbb{N}$ (in the notation of Andrianov [1]).

One has a decomposition

$$GSp(4, \mathbb{A}) = GSp(4, \mathbb{Q}) GSp(4, \mathbb{R})^+ \prod_{p<\infty} K_p,$$

where $GSp(4,\mathbb{R})^+$ denotes the subgroup of elements of $GSp(4,\mathbb{R})$ having positive determinant and $K_p := GSp(4,\mathbb{Z}_p)$, see, e.g., Weissauer [23]. One defines an automorphic form $\phi = \phi_f$ on $GSp(4,\mathbb{A})$ via

$$\phi(g) = \phi(\gamma g_\infty k_0) = f(g_\infty(\mathrm{i}\cdot \mathrm{Id}_2)) \cdot \frac{\det(g_\infty(\mathrm{i}\cdot\mathrm{Id}_2))^k}{\det(C\cdot\mathrm{i}\cdot\mathrm{Id}_2 + D)^k},$$

where

$$g_\infty := \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GSp(4,\mathbb{R})^+$$

acts via linear fractional transformations, $\gamma \in GSp(4,\mathbb{Q})$ and $k_0 \in \prod_{p<\infty} K_p$.

Then ϕ gives rise to a cuspidal irreducible automorphic representation $\Pi = \Pi_f$ of $GSp(4,\mathbb{A})$ whose ramification set is empty, see Asgari and Schmidt [2]. Moreover, Π_∞ is in the holomorphic discrete series of weight (k,k) (see [2], [8] or [25]).

We will denote the corresponding Galois representations (given by the above theorem) by $\rho_{f,\lambda}$.

Let λ_n denote the eigenvalue of $T(n)$ and let

$$L_f(s) := \zeta(2s-2k+4)\sum_{n=1}^{\infty}\frac{\lambda_n}{n^s}$$

be the spinor L-function. Then L_f has an Euler product of the form

$$L_f(s) = \prod_{p\in\mathbb{P}} Q_p(p^{-s})^{-1},$$

where Q_p is the following polynomial:

$$\begin{aligned} Q_p(X) &= 1 - \lambda_p X + (\lambda_p^2 - \lambda_{p^2} - p^{2k-4})X^2 - \lambda_p p^{2k-3}X^3 + p^{4k-6}X^4 \qquad (3.1)\\ &= (1-(\lambda_p/2+\sqrt{d_p})X + p^{2k-3}X^2)(1-(\lambda_p/2-\sqrt{d_p})X + p^{2k-3}X^2), \end{aligned}$$

with $d_p = -3/4{\lambda_p}^2 + \lambda_{p^2} + p^{2k-4} + 2p^{2k-3}$, see [18], p. 387.

As a corollary to Theorem 3.1 we get:

Proposition 3.2. *Let f be a Siegel modular form of even weight k on the full Siegel modular group $Sp(4,\mathbb{Z})$ which is a cusp form and a simultaneous eigenform for all Hecke operators $T(n)$, $n\in\mathbb{N}$. Let E be the number field generated over $\mathbb{Q}$ by all the eigenvalues λ_n, $f|T(n) = \lambda_n f$. For any prime number l and any extension λ of l to E there exists a continuous Galois representation*

$$\rho_{f,\lambda} : \mathrm{G}_{\mathbb{Q}} \to Gl(4,\overline{E}_\lambda)$$

such that the following holds: The representation $\rho_{f,\lambda}$ is unramified outside l and

$$\det(\mathrm{Id}_4 - X\cdot\rho_{f,\lambda}(\mathrm{Frob}_p)) = Q_p(X), \quad (p\neq l).$$

If $\rho_{f,\lambda}$ is absolutely irreducible, then the representation $\rho_{f,\lambda}$ is defined over E_λ.

PROOF. All the statements except the last follow immediately from the above discussion. The last statement can be found in [24], App. D (alternatively one could use a result of Carayol [4]). □

Remark 3.3. (i) If Π_f has multiplicity one (that means f is uniquely determined by its weight and its Hecke eigenvalues), the image of $\rho_{f,\lambda}$ is contained in a general symplectic group. See [24], Thm. IV.

ii) In the above proposition, it suffices to adjoin a Hecke eigenvalue of one element $T(p)$ (to obtain the field E) if the characteristic polynomial of $T(p)$ on the space spanned by the Galois translates of f is irreducible over $\mathbb{Q}$. This follows from the existence of a basis of the space of Siegel modular forms of genus two of fixed weight whose elements have Fourier coefficients in $\mathbb{Q}$ (given by Igusa's theorem [9]).

4. Computation of Hecke eigenvalues

As in Skoruppa [18], [19], let

$$\Upsilon = \Upsilon 28 = \sum_{\substack{r,n,m \in \mathbb{Z} \\ r^2-4mn \leq 0 \\ n,m \geq 0}} a(n,r,m) \cdot e^{n \cdot 2\pi i \tau} \cdot e^{r \cdot 2\pi i z} \cdot e^{m \cdot 2\pi i \tau'}, \quad \tau, \tau' \in \mathbb{H},\ z \in \mathbb{C}$$

be the Hecke eigenform of weight 28 which is orthogonal to the space of Klingen-Eisenstein series and the Maass-Spezialschar (an "interesting" form in the notation of [18]).

The Fourier coefficients depend only on the binary quadratic form $nX^2 + rXY + mY^2$, see Andrianov [1]. Skoruppa [19] computed the Fourier coefficients of Υ up to discriminant (of the corresponding quadratic form) -100. Using this, one can compute the values $\lambda_2, \lambda_4, \lambda_3, \lambda_9$ and λ_5, λ_{25}, which determine the polynomials Q_2, Q_3, Q_5 of the previous section (Formula 3.1).

As Υ is a Hecke eigenform we have the following identities, compare to [18], pp. 386-387:

$$\begin{aligned}
\lambda_p a(1,1,1) &= a(p,p,p) + p^{k-2}(1 + (\tfrac{p}{3}))a(1,1,1) \\
\lambda_p a(p,p,p) &= a(p^2,p^2,p^2) + p^{2k-3}a(1,1,1) + p^{k-2}a(1,p,p^2) + \\
&\quad p^{k-2} \textstyle\sum_{\nu \bmod p} a(1+\nu+\nu^2, p(1+2\nu), p^2) \\
\lambda_{p^2} a(1,1,1) &= a(p^2,p^2,p^2) + p^{k-2} \textstyle\sum_{\nu \bmod p: p|1+\nu+\nu^2} a(1+\nu+\nu^2, p(1+2\nu), p^2) + \\
&\quad p^{2k-4}((\tfrac{p}{3}) + (\tfrac{p^2}{3}))a(1,1,1)\ .
\end{aligned}$$

Moreover, since $a(1,3,9) = a(7,15,9) = a(1,1,7)$, $a(1,5,25) = a(21,45,25) = a(1,1,19)$ and $a(3,15,25) = a(7,25,25) = a(13,35,25) = a(3,3,7)$ we get

$$\lambda_2 = \frac{a(2,2,2)}{a(1,1,1)}, \qquad \lambda_4 = \frac{a(4,4,4)}{a(1,1,1)},$$

$$\lambda_3 = \frac{a(3,3,3)}{a(1,1,1)} + 3^{(k-2)}, \qquad \lambda_9 = \frac{\lambda_3 a(3,3,3) - 3 \cdot 3^{(k-2)} a(1,1,7)}{a(1,1,1)} - 3^{(2k-3)},$$

$$\lambda_5 = \frac{a(5,5,5)}{a(1,1,1)}, \qquad \lambda_{25} = \frac{\lambda_5 a(5,5,5) - 3 \cdot 5^{(k-2)} a(3,3,7) - 3 \cdot 5^{(k-2)} a(1,1,19)}{a(1,1,1)} - 5^{(2k-3)}\ .$$

The following Fourier coefficients of Υ of can be found in Skoruppa [19]. Here α denotes some root of the polynomial $x^3 - x^2 - 294086x - 59412960$:

$$
\begin{aligned}
a(1,1,1) &= 1217127393239495995961 7937200\alpha^2 - \\
&\quad 300203565717987213533211 2844312\alpha - \\
&\quad 70266648287313346458671196175512 \\
a(2,2,2) &= 16779845734705316103241389527875 99750\alpha^2 - \\
&\quad 41409262161640179855511924137821 2012691\alpha - \\
&\quad 348800204433658671727420661909312 57658045/2 \\
a(3,3,3) &= 4052867765036230881091727632882 9759765008\alpha^2 - \\
&\quad 99935820719502390960749295062420 70406773384\alpha - \\
&\quad 38770112161368513632700801007362 9284610690936 \\
a(4,4,4) &= 23516157692660337418462509065485 8223519273152\alpha^2 - \\
&\quad 57970607100638211602375544449739 660532651092576\alpha - \\
&\quad 26002926630475951321441608767026 7924851878170 6064 \\
a(5,5,5) &= 78394728033906461782765030942313 953784960201600\alpha^2 - \\
&\quad 19381896022485847701310751066183 248396173872804800\alpha - \\
&\quad 62388108018495387677468460531830 203956953432459 1600 \\
a(1,1,7) &= -52284558237596655158824348611551 189871168\alpha^2 + \\
&\quad 12898733485281936189063574256312 016862462752\alpha + \\
&\quad 14812405484453413048633118857414 2123721611552 \\
a(3,3,7) &= -12288329366640591505065134861374 98432921656 5680\alpha^2 + \\
&\quad 29850125961721250458263024053662 1046492418951 3560\alpha - \\
&\quad 10035375384457495565917755228409 15443221065950 00840 \\
a(1,1,19) &= -12288329366640617801983929133125 59730841076 2800\alpha^2 + \\
&\quad 29850125961721349380946661011468 96613153666927 000\alpha - \\
&\quad 10035375384457147627815816032564 001910750099 2436200
\end{aligned}
$$

Table 4.1: Fourier coefficients of $\Upsilon 28$

Remark 4.1. The polynomial

$$F(x) := x^3 + 137681664x^2 + 4794374687293440x + 4100431555335920025600$$

is the characteristic polynomial of the Hecke operator $T(2)$ on the space spanned by the Galois translates of Υ. This space is exactly the complement of the space spanned by the Klingen-Eisenstein series and the Maass Spezialschar, see [18]. Thus the automorphic representation Π_Υ has multiplicity one.

5. Some results on $GSp(4, q)$

Consider $\beta_1, \beta_2, \eta \in \overline{\mathbb{F}}_q$, such that $\eta^q = \eta$ and such that the following equality holds:

$$\{\beta_1, \eta\beta_1^{-1}, \beta_2, \eta\beta_2^{-1}\} = \{\beta_1{}^q, \eta\beta_1{}^{-q}, \beta_2{}^q, \eta\beta_2{}^{-q}\}.$$

The following table lists (up to conjugation) the tori in $Gl(4, q)$ which are maximal with respect to the condition that their elements have a set of eigenvalues

$$S(t) = \{\beta_1, \eta\beta_1^{-1}, \beta_2, \eta\beta_2^{-1}\}.$$

torus	order	eigenvalues
T_0	$(q-1)^3$	$\{\beta_1, \eta\beta_1^{-1}, \beta_2, \eta\beta_2^{-1}\},\ \beta_i^q = \beta_i$
T_1	$(q+1)^2(q-1)$	$\{\beta_1, \eta\beta_1^{-1}, \beta_2, \eta\beta_2^{-1}\},\ \beta_i^q = \eta\beta_i^{-1}$
T_2	$(q-1)^2(q+1)$	$\{\beta_1, \eta\beta_1^{-1}, \beta_2, \eta\beta_2^{-1}\},\ \beta_1^q = \beta_1,\ \beta_2^q = \eta\beta_2^{-1}$
T_3	$(q^2-1)(q-1)$	$\{\beta_1, \beta_1^q, \eta\beta_1^{-1}, \eta\beta_1^{-q}\},\ \beta_1^{q^2} = \beta_1$
T_4	$(q^2+1)(q-1)$	$\{\beta_1, \beta_1^q, \eta\beta_1^{-1}, \eta\beta_1^{-q}\},\ \beta_1^{q^2} = \eta\beta_1^{-1}$

Table 5.1

Note that these tori are (up to conjugation in $Gl(4,q)$) maximal tori in $GSp(4,q)$ and $CO_4^{\pm}(q)$, resp.. Thus if $S(t) \neq -S(t)$, we get $S(t^\sigma) = \eta^{-1}S(t)$, σ denoting the inverse-transpose map. If $S(t) = -S(t)$, we get $S(t^\sigma) = \eta^{-1}S(t)$ or $S(t^\sigma) = -\eta^{-1}S(t)$.

Remark 5.1. The numbers r_i of irreducible factors (over $\mathbb{F}_q$) of the characteristic polynomial of a regular element of T_i, $i = 0, 1, \ldots, 4$, are 4, 2, 3, 2, 1, respectively. Hence we can uniquely associate to a regular element t (which has a set of eigenvalues $S(t)$ as above) a torus T_i, except in the case $t \sim \mathrm{diag}(\beta, -\eta\beta^{-1}, \eta\beta^{-1}, -\beta)$, $\beta^q = -\eta\beta^{-1}$.

For $\rho_{f,\lambda} : \mathrm{G}_{\mathbb{Q}} \to Gl(4, \overline{E}_\lambda)$ as in Prop. 3.2, let $\mathcal{G} := \mathrm{im}(\rho_{f,\lambda})$. Then, let $\overline{\mathcal{G}}$ be the Zariski closure of $\mathcal{G}$ in $Gl(4, \overline{E}_\lambda)$, $\overline{\mathcal{G}}^0$ be the identity component of $\overline{\mathcal{G}}$ and $\mathcal{G}^0 := \overline{\mathcal{G}}^0 \cap \mathcal{G}$. Let

$$\hat{\rho}_{f,\lambda} : \mathrm{G}_{\mathbb{Q}} \to Gl(4,q),\ \mathbb{F}_q = k_{E_\lambda},$$

be as in Lemma 2.3, G be the image of $\hat{\rho}_{f,\lambda}$ and $G^0 = \hat{\rho}_{f,\lambda}(\rho_{f,\lambda}^{-1}(\mathcal{G}^0))$.

From the list of Taylor [20], bottom of page 298, we deduce that G^0 is contained in one of the groups listed below:

overgroups of G^0	tori	$\lvert\overline{\mathcal{G}}/\overline{\mathcal{G}}^0\rvert$
$CO_4^+(q) = Gl(2,q) \circ Gl_2(q) = \{X \otimes Y \mid X, Y \in Gl(2,q)\}$	T_0, T_1, T_3	≤ 2
$CO_4^-(q) \cong Gl(2,q^2) = \{X \otimes X^{F_q} \mid X \in Gl(2,q^2)\}$	T_2, T_4	≤ 2
$GSp(4,q)$		
$Gl(2,q) = \{\mathrm{diag}(X,X) \mid X \in Gl(2,q)\}$	T_1, T_2	≤ 2
$Gl(2,q) = \{\mathrm{diag}(Y, X, \det(X)Y^{-1}) \mid Y \in Gl_1(q), X \in Gl(2,q)\}$	T_0, T_2	≤ 2
$Gl(2,q) = \{\mathrm{diag}(Y, X, \det(X)Y^{-1}) \mid Y \in GU_1(q), X \in Gl(2,q)\}$	T_1, T_2	≤ 2
$Gl(2,q) \times Gl_1(q) = \{\mathrm{diag}(X, \eta X^\sigma) \mid X \in Gl(2,q), \eta \in \mathbb{F}_q\}$	T_0, T_3	≤ 2
$GU_2(q) \times Gl_1(q) = \{\mathrm{diag}(X, \eta X^\sigma) \mid X \in GU_2(q), \eta \in \mathbb{F}_q\}$	T_1, T_3	≤ 2
$\{(X,Y) \mid X, Y \in Gl(2,q), \det(X) = \det(Y)\}$	T_0, T_1, T_2	≤ 2
$\{(X, X^{F_q}) \mid X \in Gl(2,q^2), \det(X) \in \mathbb{F}_q\}$	T_3, T_4	≤ 2
$T_i, i = 0, \ldots, 4$		≤ 8

Table 5.2

Remark 5.2. Let $s \in N_{Gl(4,q)}(H) \setminus H$, where $H \neq GSp(4,q)$ is one of the groups of the above list. Then s has a pair of eigenvalues $(\beta_1, -\beta_1)$.

PROOF. First, let $s^2 \in CO_4^{\pm}(q)$ and $s \notin CO_4^{\pm}(q)$. Then $s \sim \mathrm{diag}(\beta_1, \beta_2, \eta{\beta_2}^{-1}, -\beta_1)$, ${\beta_1}^2 = \eta \in \mathbb{F}_q, \beta_2 \in \mathbb{F}_{q^2}$ (see Reiter [13]). In any other case $N_{Gl(4,q)}(H)$ is an imprimitive group, where s permutes 2 or 4 blocks. Hence s^2 is not a regular element and the claim follows. □

Proposition 5.3. *Let l be an odd prime such that the residue field $\mathbb{F}_q = k_{E_\lambda}$ is not a prime field and let $G = \mathrm{im}(\hat{\rho}_{f,\lambda})$. Further assume that $\mathbb{F}_q$ is generated over $\mathbb{F}_l$ by the reduced coefficients of the characteristic polynomials of the Frobenius elements. If G contains elements t_0, t_4, resp. t_1, t_4, resp. t_2, t_3, where t_i is contained up to conjugation in the maximal torus T_i (T_i as in Table 5.1) and the element t_i^2 is regular, then $Sp(4,q) \leq G$.*

PROOF. We exclude all the possible overgroups $H \neq GSp(4,q)$ of G^0 (H as in Table 5.2) by considering the maximal tori contained in H, together with Remark 5.2.

To treat the group $GSp(4,q)$ note that the above list contains all maximal subgroups of $GSp(4,q)$ with the possible exception $GSp(4,q_0)$, $q = q_0^r$, r a prime, and maximal subgroups of type S (in the notation of [10]).

The maximal subgroups of type S are exluded by noting that the condition that q is not a prime implies, that one has no maximal subgroups of type S, compare to Mitchell [12].

To exclude the case $GSp(4,q_0)$ note that we can assume by Formula 3.1 and Proposition 3.2 that G is contained in the group $\mathbb{F}_{l^2} \cdot Sp(4,q_0)$. This implies that the compositum of $\mathbb{F}_{l^2}$ and $\mathbb{F}_{q_0}$ is $\mathbb{F}_q$. So we can assume that $[\mathbb{F}_q : \mathbb{F}_{q_0}] = 2$. Now observe that in this case a regular element contained in T_2, resp. T_4, is not contained in the group $\mathbb{F}_{l^2} \cdot Sp(4,q_0)$. □

Proposition 5.4. *Let G be as above. Suppose $Sp(4,q) \leq G$. Then $G/Z(G) = PSp(4,q)$ if m is even and $G/Z(G) = PGSp(4,q)$ if m is odd.*

PROOF. By assumption we get $G/Z(G) = PSp(4,q)$ or $G/Z(G) = PGSp(4,q)$. Let $t_p = \hat{\rho}_{f,\lambda}(\mathrm{Frob}_p)$. Since $G = \langle t_p \mid p \in \mathbb{P} \rangle \leq GSp(4,q)$, we find by Prop. 3.2 that $t_p^\sigma = p^{2k-3} t_p$. Thus if m is even we get $(q-1)_2 > (l-1)_2$. Hence $G \leq Z(Gl(4,q))Sp(4,q)$. Now let m be odd. Then p^{2k-3} is a non square in $\mathbb{F}_q$ if p is a non square in $\mathbb{F}_l$. Assume $(\frac{p}{l}) = 1$ for all $p \in \mathbb{P}$. Then $(\frac{n}{l}) = 1$ for $1 \leq n < l$ odd. Hence $(\frac{n}{l}) = -1$ for $1 \leq n < l$ even. Since $(\frac{4}{l}) = 1$ we have $4 > l$, hence $l = 3$. On the other hand we have $(\frac{5}{3}) = -1$, a contradiction. □

6. The resulting Galois realizations

Definition 6.1. A profinite group G *occurs as Galois group over* $\mathbb{Q}$ if there exists a continuous homomorphism of $\mathrm{G}_{\mathbb{Q}}$ onto G.

Let f be a Siegel modular form of weight k as in Section 3, and let E, λ, and

$$\rho_{f,\lambda} : \mathrm{G}_{\mathbb{Q}} \to Gl(4, \overline{E}_\lambda)$$

be as in Prop. 3.2. If Π_f has multiplicity one, the groups

$$\mathcal{A}_\lambda^k := \{g \in GSp(4, O_{E_\lambda}) \mid \det(g) \in (\mathbb{Z}_l^\times)^{4k-6}\}$$

are natural candidates for the images of $\rho_{f,\lambda}$ by Formula 3.1 and Remark 3.3.

In the following, let $\Upsilon = \Upsilon 28$ be the Hecke eigenform of Section 4. Then $E := \mathbb{Q}(\alpha)$, where α is a root of $x^3 - x^2 - 294086x - 59412960$ (using Remark 3.3 ii) and the irreducibility of $F(x)$ over $\mathbb{Q}$, where $F(x)$ is as in Remark 4.1).

Theorem 6.2. *i) For infinitely many primes numbers l (especially $l = 53$) there exists an extension λ of l to E of inertia degree 3 (i.e. $k_{E_\lambda} \simeq \mathbb{F}_{l^3}$) such that*

$$\rho_{\Upsilon,\lambda}(G_{\mathbb{Q}}) = \mathcal{A}_\lambda^{28}.$$

In particular, the factor groups $PGSp(4, O_{E_\lambda})$ and $PGSp(4, l^3)$ of $\mathcal{A}_\lambda^{28}$ occur as Galois groups over $\mathbb{Q}$. The corresponding Galois extensions of $\mathbb{Q}$ are unramified outside l.

ii) For infinitely many primes numbers l' (especially $l' = 19$) there exists an extension λ' of l' to E of inertia degree 2 such that

$$\rho_{\Upsilon,\lambda'}(G_{\mathbb{Q}}) = \mathcal{A}_{\lambda'}^{28}.$$

In particular, the factor groups $PSp(4, O_{E_{\lambda'}})$ and $PSp(4, l'^2)$ of $\mathcal{A}_{\lambda'}^{28}$ occur as Galois groups over $\mathbb{Q}$. The corresponding Galois extensions of $\mathbb{Q}$ are unramified outside l'.

Proof. (i) Let first $l = 53$. Since 53 does not divide the discriminant of E $(= 5 \cdot 13 \cdot 73693 \cdot 1418741)$ it follows that 53 is unramified. Let λ be an extension of 53 to E. Then, since $F(x)$ modulo λ is irreducible we have $k_{E_\lambda} \simeq \mathbb{F}_{53^3}$.

Let t_p denote the image of a Frobenius element Frob_p under the image of $\hat{\rho}_{\Upsilon,\lambda}$, where $\hat{\rho}_{\Upsilon,\lambda}$ is as in Lemma 2.3. By Lemma 2.3 we get that t_p is contained in $Gl(4, 53^3)$. (By the definition of the polynomials Q_p, E also coincides with the number field which is generated over $\mathbb{Q}$ by the coefficients of the characteristic polynomials of the Frobenii.) Using the results of Section 4 together with Formula (3.1) of Section 3 one sees that

$$\begin{aligned}
Q_2(x) \equiv\ & 4(x^2 + (45\alpha^2 + 19\alpha + 33)x + 28\alpha^2 + 47\alpha + 39) \\
& (x^2 + (48\alpha^2 + 8\alpha + 46)x + 17\alpha^2 + 15\alpha) \bmod \lambda \\
Q_3(x) \equiv\ & 9(x + 39\alpha^2 + 15\alpha + 27)(x + 16\alpha^2 + 28\alpha + 9) \\
& (x + 5\alpha^2 + 5\alpha + 28)(x + 46\alpha^2 + 18\alpha + 39) \bmod \lambda \\
Q_5(x) \equiv\ & 1 + 25(27\alpha^2 + 51\alpha + 52)x + 25(47\alpha^2 + 24 + 26\alpha)x^2 + \\
& 25(29\alpha^2 + 43\alpha + 48)x^3 + 25x^4 \bmod \lambda\ .
\end{aligned}$$

From the list of polynomials $Q_2, Q_3, Q_5 \bmod \lambda$, together with Proposition 3.2 and Lemma 2.3, we deduce that $t_2 \in T_3, t_3 \in T_0, t_5 \in T_4$ and t_3^2, t_5^2 are regular elements. Thus by Proposition 5.3 the group $H := \langle t_2, t_3, t_5 \rangle$ contains the group $Sp(4, 53^3)$; in particular, H is absolutely irreducible. Using the list of the possible overgroups in Section 5 (or by multiplicity one, see Remarks 3.3 i) and 4.1) we find that H is contained in the group $GSp(4, 53^3)$.

Since H is absolutely irreducible, it follows by definition that $\hat{\rho}_{\Upsilon,\lambda}$ is absolutely irreducible. It follows from the construction of $\hat{\rho}_{\Upsilon,\lambda}$ that also $\rho_{\Upsilon,\lambda}$ is absolutely irreducible. Thus the representation $\rho_{\Upsilon,\lambda}$ is defined over E (see Prop. 3.2). Since $H/Z(H)$ contains $PSp(4, l^3)$ it follows $\mathrm{Im}(\rho_{\Upsilon,\lambda}) = \mathcal{A}_\lambda^{28}$, using Lemma 2.2 and $\det(\mathrm{Frob}_p) = p^{4k-6}$. The groups $PGSp(4, O_{E_\lambda})$ and $PGSp(4, l^3)$ are factor groups of $\mathcal{A}_\lambda^{28}$ by Prop. 5.4 and the corresponding Galois extensions are unramified outside l by Prop. 3.2.

We use Cebotarev's density theorem in order to show that analogous statements hold for infinitely many primes l : Let E' be the Galois closure of E and

$$\tilde{Q} := \prod_{i=2,3,5} \cdot \prod_{\sigma \in \mathrm{Gal}(E':\mathbb{Q})} Q_i^\sigma \quad \in \mathbb{Q}[x].$$

Looking at the case $l = 53$ one sees (by applying Cebotarev's density theorem to $\tilde{Q}$) that there are infinitely many primes l of inertia degree 3 in E such that the polynomials $Q_i,\ i = 2, 3, 5$, decompose modulo l as in the 53 case above. Then continue as in the 53 case.

ii) Let first $l' = 19$: We have

$$F(x) \equiv (x + 18)(x^2 + 8x + 17) \bmod l'.$$

Let λ' be the extension of l' to E of inertia degree 2 and let $\alpha \in k_{E_{\lambda'}} = \mathbb{F}_{19^2}$ be a root of $x^2 + 7x + 14$. Then

$$\begin{aligned} Q_2(x) \equiv&\ 1 + 5(17\alpha + 14)x + 5(6 + 13\alpha)x^2 + 5(18\alpha + 7)x^3 + 5x^4 \bmod \lambda' \\ Q_3(x) \equiv&\ 17(x^2 + (\alpha + 8)x + 3)(x^2 + (16\alpha + 4)x + 3) \bmod \lambda' \\ Q_5(x) \equiv&\ 16(x + 9\alpha + 12)(x + 1)(x + 5)(x + 14\alpha + 16) \bmod \lambda' \end{aligned}$$

Thus $t_2 \in T_4, t_3 \in T_1, t_5 \in T_0$. The claim on $l' = 19$ as well as the claim on the infinitely many other l''s follow now analogously as in i). □

Remark 6.3. i) The Galois representations attached to Hecke eigenforms in the Maass Spezialschar are related to two dimensional Galois representations; in particular, they are always reducible, see Weissauer [24], Thm. II. The Fourier coefficients of the non-Maass, non-Eisenstein, Hecke eigenforms of smaller weights lie completely in $\mathbb{Q}$ (see Skoruppa [18]) and thus cannot yield anything new from the inverse Galois theoretic viewpoint (see Malle and Matzat [11], Serre [17] and Völklein [22] for an introduction to the inverse Galois problem), since it is well known that the groups $PGSp(2n, l)$ occur as Galois groups over $\mathbb{Q}$ (e.g. use [11], Thm. I.8.6, together with [13], Satz 6.1, 7.1, as in [11], Ex. I.8.2.).

ii) One can realize symplectic groups $PSp(n, l^m), l$ odd, for a fixed $m \in \mathbb{N}$ (regularly) as Galois groups over $\mathbb{Q}$ if $n > l^m$ (see Dettweiler and Reiter [7], extending results of Thompson and Völklein [21]). It is in general very hard to realize symplectic groups regularly as Galois groups over $\mathbb{Q}$ if n lies below this bound and $m > 1$, because the Hurwitz spaces which parametrize the corresponding families of covers tend to have "few" rational points. This is partly because these Hurwitz spaces are often varieties of general type, partly because of the action of the absolute Galois group on the conjugacy classes via the cyclotomic character (see [11] and [22] for this).

References

1. Andrianov, A.N., *Quadratic forms and Hecke operators*. Berlin: Springer Verlag (1987).
2. Asgari, M., Schmidt, R., Siegel modular forms and representations. *Manuscripta Math.* **104** (2001), No. 2, 173-200.
3. Carter, R., *Finite Groups of Lie Type: Conjugacy classes and complex characters*. New York: Wiley (1985).
4. Carayol, H., Formes modulaires et représentations Galoisiennes à valeurs dans un anneau local complet, in: p-adic Monodromy and the Birch-Swinnerton-Dyer Conjecture (Mazur and Stevens eds.), *Contemp. Math.* **165** (1994), Amer. Math. Soc., 193-236.
5. Curtis, C.W., Reiner, I., *Representation Theory of Finite Groups and Associative Algebras*. New York: Wiley (1962).

6. Deligne, P., Formes modulaires et représentations l-adiques. Seminaires Bourbaki 355, Fevrier 1969, Springer LNM **179** (1971).
7. Dettweiler, M., Reiter, S., An algorithm of Katz and its application to the inverse Galois problem. *Journal of Symb. Comp.* **30** (2000), No. 6, 761-798.
8. Faltings, G., Chai, C.-L., *Degeneration of Abelian Varieties*. Berlin, Heidelberg: Springer Verlag (1990).
9. Igusa, J.-I., On Siegel modular forms of genus two. *Am. J. Math.* **84** (1962), 175-200.
10. Kleidman, P., Liebeck, M., *The subgroup structure of the finite classical groups*. Cambridge University Press (1990).
11. Malle, G., Matzat, B.H., *Inverse Galois theory*. Berlin, Heidelberg: Springer Monographs in Mathematics (1999).
12. Mitchell, H.H., The subgroups of the quaternary abelian linear group. *Trans. AMS* **15** (1914), 379-396.
13. Reiter, S., Galoisrealisierungen klassischer Gruppen. *J. reine angew. Math.* **511** (1999), 193-236.
14. Reverter, A., Vila, N., Some projective linear groups over finite fields as Galois groups over $\mathbb{Q}$. *Contemp. Math., Ed. Fried, M. et al.* **186** (1995), 51-63.
15. Ribet, K.A., On l-adic representations attached to modular forms. *Invent. Math.* **28** (1975), 245-275.
16. Serre, J.-P., *Abelian l-adic Representations and Elliptic Curves.* New York: Addison Wesley (1989).
17. Serre, J.-P., *Topics in Galois Theory*. Boston: Jones and Bartlett (1992).
18. Skoruppa, N.-P., Computations of Siegel modular forms of genus two. *Mathematics of Computation* **58** (1992), 381-398.
19. Skoruppa, N.-P., Siegel Modular Eigenforms of Even Weight on the Full Siegel Modular Group of Genus 2. (1999). Available under http://thor.math.u-bordeaux.fr/ modi/.
20. Taylor, R., On the l-adic cohomology of Siegel threefolds. *Invent. Math.* **114** (1993), 289-310.
21. Thompson, J., Völklein, H., Symplectic groups as Galois groups. *J. Group Theory*. **1** (1998), 1-58.
22. Völklein, H., *Groups as Galois groups.* New York: Cambridge Studies in Advanced Mathematics **53** (1996).
23. Weissauer, R., Differentialformen zu Untergruppen der Siegelschen Modulgruppe zweiten Grades. *J. Reine Angew. Math.* **391** (1988), 100-156.
24. Weissauer, R., Four dimensional Galois representations. Preprint (1993, 2000).
25. Weissauer, R., An application of the hard Lefschetz theorem. Preprint (1993).

M. Dettweiler: IWR, Universität Heidelberg, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany. e-mail: michael.dettweiler@iwr.uni-heidelberg.de.

U. Kühn: Institut für Mathematik, Rudower Chaussee 25, Humboldt-Universität zu Berlin, 10099 Berlin, Germany. e-mail: kuehn@mathematik.hu-berlin.de

S. Reiter: IWR, Universität Heidelberg, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany. e-mail: reiter@iwr.uni-heidelberg.de