ON THE EXPERIMENTAL VERIFICATION OF THE ARTIN CONJECTURE FOR 2-DIMENSIONAL ODD GALOIS REPRESENTATIONS OVER $\mathbb{Q}$. LIFTINGS OF 2-DIMENSIONAL PROJECTIVE GALOIS REPRESENTATIONS OVER $\mathbb{Q}$.

IAN KIMING

1. Introduction.

1.1. Consider equivalence classes of 2-dimensional, irreducible, continuous, odd Galois representations over $\mathbb{Q}$:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$$

with Artin conductor $N \in \mathbb{N}$ and determinant character $\det \rho = \varepsilon$. Here, $\mathbb{C}$ has the discrete topology and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has the natural topology as a profinite group so that 'continuous' implies 'having finite image'. The determinant character ε is the character on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ obtained by composing ρ with the determinant homomorphism:

$$\det : \mathrm{GL}_2(\mathbb{C}) \to \mathbb{C}^{\times}.$$

Then ε is a character on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with class field theoretic conductor dividing N. By class field theory we may identify ε with a Dirichlet character modulo N; that ρ is *odd* then means that $\varepsilon(-1) = -1$.

It is conjectured that these equivalence classes are in 1-1 correspondence with the normalized newforms $f(z)$ of weight 1 and nebentypus ε on the congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ \middle| \ c \equiv 0 \quad (N) \right\}$$

(see for example [10] for definitions). More explicitly, one expects that if the Artin L-series of ρ (which depends only on the equivalence class of ρ) is:

$$(*) \qquad L(s,\rho) = \sum_{n=1}^{\infty} a_n n^{-s} \ , \quad \mathrm{Re}(s) > 1,$$

then:

$$(**) \qquad f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \ , \quad \mathrm{Im}(z) > 0,$$

should be a (normalized) newform of weight 1 on $\Gamma_0(N)$ with nebentypus ε. This can also be expressed in this way: The Artin L-series of ρ should be the Hecke L-series of the corresponding newform $f(z)$.

Now, a theorem of Deligne and Serre (cf. [4]) states that if $f(z)$ is a normalized newform on $\Gamma_0(N)$ of weight 1 and nebentypus ε with Fourier expansion at ∞ as in $(**)$, then there is a Galois representation ρ as above with Artin L-series as in $(*)$. A classical theorem of Hecke (cf. for example [10], chap. 4) then implies that this L-series, enlarged by the usual Γ-factor, has a holomorphic continuation to the whole complex plane, i.e. it satisfies the Artin conjecture. With this, a theorem of Weil (cf. [16], [9] or [10]) shows that the above conjecture conjunctively for all Galois representations of the above type is equivalent to the Artin conjecture for these representations. We also see that the existence, for given N and ε, of the above-mentioned conjectural (set-theoretic) 1-1 correspondence implies the existence of a 1-1 correspondence with 'preservation of L-functions' as in $(*)$, $(**)$.

1.2. ρ is a Galois representation of the above type, we may consider its projectivisation:

$$\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{PGL}_2(\mathbb{C})$$

obtained by composing ρ with the canonical homomorphism $\mathrm{GL}_2(\mathbb{C}) \rightarrow \mathrm{PGL}_2(\mathbb{C})$. As a finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$ the image of $\bar{\rho}$ is a priori either isomorphic to a cyclic group, a dihedral group, to the alternating group A_4, to the symmetric group S_4, or to the alternating group A_5, where however the cyclic case is excluded since ρ was required to be irreducible. We shall distinguish these cases by saying that ρ is of dihedral, A_4- , S_4- or A_5-type, respectively. Now, if ρ is of dihedral type, then one may by class field theory show that ρ is associated to a newform of weight 1 as in 1.1, i.e. its L-series is the L-series of such a modular form. By results of Langlands and Tunnell (cf. [8] and [15]) this is also the case if ρ is of A_4- or S_4-type. Hence the question of whether ρ is in this way associated to a newform of weight 1 is only interesting in case that ρ is of A_5-type. If this is the case, the above-mentioned methods of associating to ρ a newform of weight 1 fail completely, and so the question of displaying at least *examples* of representations of A_5-type whose Artin L-series are L-series of newforms of weight 1 arises. Up till now there was in the literature only 1 such example, namely the example of J.P. Buhler (cf. [3]). How could we produce such examples in a systematic way? Conceptually, there is a simple way of doing that:

Suppose that we are given a natural number N and a Dirichlet character ε with $\varepsilon(-1) = -1$. Denote by $S_1^{\mathrm{new}}(N, \varepsilon)$ the complex vector space generated by the newforms of weight 1 and nebentypus ε on $\Gamma_0(N)$, and by $d(N, \varepsilon)$ the number of equivalence classes of 2-dimensional, complex, irreducible, continuous, odd representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with Artin conductor N and determinant character ε. The above-mentioned theorem of Deligne and Serre then tells us that:

$$\dim S_1^{\mathrm{new}}(N, \varepsilon) \leq d(N, \varepsilon),$$

and that if we have equality here, all of these representations are associated with newforms of weight 1 as in 1.1 (and so the enlarged L-series of these representations as well of their 'twists' by 1-dimensional characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ will have holomorphic continuations to the whole complex plane, i.e. they will satisfy the Artin conjecture). If we do not have equality, the Artin conjecture is false.

Hence we should ask ourselves how one can determine the number $\dim S_1^{\mathrm{new}}(N, \varepsilon)$ and $d(N, \varepsilon)$ for given N and ε. The problem of determining $d(N, \varepsilon)$ will be considered in sections 2, 3 and 4 below. For the rest of this section, we shall briefly show

how the problem of computing $\dim S_1^{\mathrm{new}}(N,\varepsilon)$ can be reduced to analogous 'higher weight' problems.

1.3. Let k and N be natural numbers and let ε be a Dirichlet character mod N with $\varepsilon(-1)=(-1)^k$. The complex vector space $S_k(N,\varepsilon)$ of cusp forms of weight k and nebentypus ε on $\Gamma_0(N)$ has a basis consisting of forms all of whose Fourier coefficients (at ∞) are integers; for $k\geq 2$ this follows from [14], Th. 3.52, and for $k=1$ it follows from the considerations below. Call any such basis an 'integral basis'.

Clearly, if one can find an integral basis for $S_1(N,\varepsilon)$, then one can also determine the subspace generated by the oldforms in it, and hence one can compute $\dim S_1^{\mathrm{new}}(N,\varepsilon)$. In order to find such a basis we can, as a first shot, use the well-known trick (cf. [13] or [3], chap. 6) of multiplying with modular forms without a common zero (neither in the upper half plane nor at any cusp):

Let p be a prime number such that N is divisible by $2p$, if $p\equiv 3\ (4)$, or divisible by $4p$, if $p\equiv 1\ (4)$; if no such prime number exists, replace N by a suitable multiple for which there does. Consider the Eisenstein series:

$$E_p(z)=-\frac{1}{2}h+\sum_{n=1}^{\infty}\left(\sum_{d|n}\chi_{-p}(d)\right)e^{2\pi i n z},\quad \mathrm{Im}(z)>0,$$

where χ_{-p} is the character of the quadratic field $\mathbb{Q}(\sqrt{-p})$ and h its class number. The function $E_p(z)$ is a modular form of weight 1 and nebentypus χ_{-p} on $\Gamma_0(M)$, where:

$$M=\begin{cases} p\ , & \text{if } p\equiv 3 \quad (4)\\ 4p\ , & \text{if } p\equiv 1\quad (4)\end{cases}$$

Consider furthermore the theta-series:

$$\theta_2(z)=\sum_{m=-\infty m\equiv 1\quad (2)}^{\infty} e^{\pi i m^2 z/4}\ ,\quad \mathrm{Im}(z)>0;$$

it is a modular form of weight $\frac{1}{2}$ on $\Gamma_0(2)$ with the multiplier-system:

$$(+)\qquad v_2\left(\begin{pmatrix} a & b\\ c & d\end{pmatrix}\right)=\left(\frac{c}{d}\right)_* e^{\pi i(d-1+bd)/4},\quad \text{for}\quad \begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma_0(2),$$

where:

$$\left(\frac{c}{d}\right)_*=\left(\frac{c}{|d|}\right)\sigma(c,d),$$

with:

$$\sigma(c,d)=\begin{cases} -1, & \text{if } c<0 \text{ and } d<0\\ 1, & \text{otherwise.}\end{cases}$$

Cf. [11], p. 269. We conclude that θ_2^8 is a modular form of weight 4 on $\Gamma_0(2)$ with trivial nebentypus. Now, θ_2 vanishes only at the cusp ∞ (cf. [11], p. 23) and E_p is non-zero at ∞. Consequently, the map:

$$S_1(N,\varepsilon)\to S_2(N,\varepsilon\chi_{-p})\times S_5(N,\varepsilon)$$

given by:

$$f\mapsto (f\cdot 2E_p, f\theta_2^8),$$

maps $S_1(N,\varepsilon)$ isomorphically onto the subspace:

$$V\leq S_2(N,\varepsilon\chi_{-p})\times S_5(N,\varepsilon)$$

consisting of pairs (f_1, f_2) with:

$$(++) \qquad f_1\theta_2^8 = f_2 \cdot 2E_p \quad \text{in} \quad S_6(N, \varepsilon\chi_{-p}).$$

Since the equation (++) is equivalent to a linear system of equations involving (finitely many) Fourier coefficients of the forms f_1 and f_2, it is clear that if we know how to obtain integral bases for the spaces $S_2(N, \varepsilon\chi_{-p})$ and $S_5(N, \varepsilon)$, then the problem of computing $\dim S_1(N, \varepsilon)$ or even obtaining an integral basis for the space $S_1(N, \varepsilon)$ is reduced to a question in linear algebra. An algorithm for obtaining an integral basis for a space $S_k(\cdot, \cdot)$, where $k \geq 2$, will be described in IV and V.

1.4. The algorithm described in 1.3 is of course general but has the disadvantage of requiring the construction of an integral basis for a space of cusp forms of weight 5, which may be computationally unmanageable for interesting cases. Here we shall show that in some favorable cases there is an algorithm which only involves computation in a space of cusp forms of weight 2. In this subsection we shall assume that N is a natural number of the form:

$$N = 2^{s+1}mn \ ,$$

where m and n are coprime natural numbers which are both odd and square free, and

$$s \geq \begin{cases} 1\ , & n \equiv 3 \quad (4) \\ 2\ , & n \equiv 1 \quad (4). \end{cases}$$

Define the function $g_{s,n}$ by:

$$g_{s,n}(z) = \theta_2(2^s z)\theta_2(2^s nz)\ , \quad \mathrm{Im}(z) > 0\ ,$$

where θ_2 is the theta-function considered in 1.3. Recall that if f is a non-zero holomorphic modular form of some weight and with a multiplier-system on some subgroup Γ in $\mathrm{SL}_2(\mathbb{Z})$ of finite index and ζ is a cusp of Γ, then f has a well-defined *order* at ζ with respect to Γ (cf. [11], p. 12). This order depends only on the equivalence class of ζ with respect to Γ .

Lemma 1. *The function $g_{s,n}$ is a modular form on $\Gamma_0(2^{s+1}mn)$ of weight 1 and nebentypus χ_{-n}, where χ_{-n} is the character of the quadratic field $\mathbb{Q}(\sqrt{-n})$. It vanishes only at cusps (equivalent to a cusp) of the form:*

$$-(2^{s+1}kl)^{-1}, \quad \text{with} \quad k \mid m\ , l \mid n\ ,$$

and its order at such a cusp $-(2^{s+1}kl)^{-1}$ is:

$$2^{s-3} \cdot \frac{m}{k} \cdot \left(\frac{n}{l} + l\right) \ .$$

Proof. For information (equivalence classes, widths) on the cusps of groups $\Gamma_0(N)$ we refer to [11], pp. 241–251.

Let us start by noting that the cusps $-(2^{s+1}kl)^{-1}$, where k and l run independently through the divisors of m and n respectively, are mutually inequivalent under $\Gamma_0(2^{s+1}mn)$. Here we have used the fact that m and n are coprime.

We shall use the usual notation $\Gamma(\mu, \nu)$ for the congruence subgroup:

$$\Gamma(\mu, \nu) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ \mid \ c \equiv 0 \quad (\mu)\ , b \equiv 0 \quad (\nu) \right\}.$$

Recall that θ_2 is a holomorphic modular form of weight $\frac{1}{2}$ on $\Gamma_0(2)$ with the multiplier system v_2 given in 1.3 by (+).

Let us now fix k and l with $k \mid m$, $l \mid n$. The cusp $-(2k)^{-1}$ is equivalent to ∞ under $\Gamma_0(2)$, and with respect to $\Gamma(2m, 2^s)$ it has width $2^s \cdot \frac{m}{k}$. Since θ_2 has order $\frac{1}{8}$ with respect to $\Gamma_0(2)$ at ∞, we conclude that θ_2 has order $2^{s-3} \cdot \frac{m}{k}$ at $-(2k)^{-1}$ with respect to $\Gamma(2m, 2^s)$. Acting with the matrix:

$$\begin{pmatrix} 2^s & 0 \\ 0 & 1 \end{pmatrix}$$

on $\theta_2(z)$, we find that $\theta_2(2^s z)$ is a form on $\Gamma_0(2^{s+1}m)$ which has order $2^{s-3} \cdot \frac{m}{k}$ at the cusp $-(2^{s+1}k)^{-1}$. (Use for example a reasoning along the lines of the argument on p. 248 in [11]).

The cusps $-(2^{s+1}k)^{-1}$ and $-(2^{s+1}kl)^{-1}$ are equivalent under $\Gamma_0(2^{s+1}m)$ with width $\frac{m}{k}$. Since $-(2^{s+1}kl)^{-1}$ has width $\frac{mn}{kl}$ with respect to $\Gamma_0(2^{s+1}mn)$, we conclude that $\theta_2(2^s z)$ has order $2^{s-3} \cdot \frac{mn}{kl}$ at the cusp $-(2^{s+1}kl)^{-1}$ with respect to $\Gamma_0(2^{s+1}mn)$.

Using the fact that m and n are coprime and m is square free, we find that $-(2^{s+1}k)^{-1}$ and $-\frac{n}{l} \cdot (2^{s+1}k)^{-1}$ are equivalent under $\Gamma_0(2^{s+1}m)$:

Put $\alpha = \frac{n}{l}$, $\beta = 2^{s+1}k$ and $M = 2^{s+1}m$. Choose $u, v \in \mathbb{Z}$ such that:

$$-\beta u - \alpha v = 1,$$

and $\mu, \nu \in \mathbb{Z}$ such that:

$$\nu\beta + \mu \cdot \frac{M}{\beta} = \beta - 1 - v \ .$$

Then the matrix:

$$\begin{pmatrix} -\alpha & u \\ \beta & v \end{pmatrix} \begin{pmatrix} 1 & \nu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \beta - 1 & 1 \\ -\beta & -1 \end{pmatrix}$$

belongs to $\Gamma_0(M)$ and it maps $-\frac{1}{\beta}$ to $-\frac{\alpha}{\beta}$.

Now, the cusp $-(2^{s+1}k)^{-1}$ has width $\frac{m}{k}$ with respect to $\Gamma_0(2^{s+1}m)$ and the cusp $-\frac{n}{l} \cdot (2^{s+1}k)^{-1}$ has width $\frac{m}{k} \cdot l$ with respect to $\Gamma(2^{s+1}m, n)$. Since $\theta_2(2^s z)$ has order $2^{s-3} \cdot \frac{m}{k}$ at $-(2^{s+1}k)^{-1}$ with respect to $\Gamma_0(2^{s+1}m)$, we find that $\theta_2(2^s z)$ has order $2^{s-3} \cdot \frac{m}{k} \cdot l$ at $-\frac{n}{l}(2^{s+1}k)^{-1}$ with respect to $\Gamma(2^{s+1}m, n)$. Acting on $\theta_2(2^s z)$ with the matrix:

$$\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix},$$

we then find that $\theta_2(2^s nz)$ is a form on $\Gamma_0(2^{s+1}mn)$ which has order $2^{s-3} \cdot \frac{m}{k} \cdot l$ at $-(2^{s+1}kl)^{-1}$.

Consequently, $g_{s,n}$ is a modular form of weight 1 on $\Gamma_0(2^{s+1}mn)$. Given the multiplier v_2 of θ_2, one easily finds that the multiplier of $g_{s,n}$ is:

$$v\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \left(\frac{n}{|\delta|}\right) \cdot (-1)^{\frac{\delta-1}{2} + \frac{n+1}{2} \cdot 2^{s-1}\beta\delta},$$

for $\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) \in \Gamma_0(2^{s+1}mn)$. Using the assumption that $s \geq 2$ if $n \equiv 1 \ (4)$, we find that this value is:

$$\left(\frac{n}{|\delta|}\right) \cdot (-1)^{\frac{\delta-1}{2}} \ ,$$

and this is precisely $\chi_{-n}(\delta)$. Hence $g_{s,n}$ is a form of weight 1 and nebentypus χ_{-n} on $\Gamma_0(2^{s+1}mn)$.

Let us compute the sum of the orders of $g_{s,n}$ with respect to $\Gamma_0(2^{s+1}mn)$ at the cusps $(2^{s+1}kl)^{-1}$, where k and l run independently through the divisors of m and n respectively. Using the fact that m and n are coprime and both square free, we find that this sum is:

$$\begin{aligned} \sum_{k|m}\sum_{l|n} 2^{s-3} \cdot \frac{m}{k} \cdot \left(\frac{n}{l} + l\right) &= 2^{s-2} \sum_{k|m}\sum_{l|n} \frac{mn}{kl} \\ &= 2^{s-2} mn \prod_{p|mn} \left(1 + \frac{1}{p}\right) \ , \end{aligned}$$

where the product is over all prime divisors of mn. Since mn is odd, we see that this sum is precisely $\frac{1}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(2^{s+1}mn)]$. Hence we may conclude that $g_{s,n}$ vanishes *only* at the above cusps. □

If now ε is a Dirichlet character modulo N with $\varepsilon(-1) = -1$, the above lemma tells us that multiplication by $g_{s,n}$ maps $S_1(N, \varepsilon)$ isomorphically onto the subspace of $S_2(N, \varepsilon\chi_{-n})$ consisting of forms which vanish at any cusp $-(2^{s+1}kl)^{-1}$, where $k \mid m$, $l \mid n$, with order greater than:

$$2^{s-3} \cdot \frac{m}{k} \cdot \left(\frac{n}{l} + l\right).$$

Let us now fix divisors $k \mid m$, $l \mid n$, and consider the 'Atkin-Lehner operator' (cf. [1]):

$$W_{N,kl} = \begin{pmatrix} \frac{mn}{kl} & b \\ -N & \frac{mn}{kl} d \end{pmatrix} \ ,$$

where b and d are such that:

$$\frac{mn}{kl} d + 2^{s+1} klb = 1.$$

(Such numbers b and d exist since mn is an odd, square free number). Now, $\varepsilon\chi_{-n}$ is a Dirichlet character mod N, and so we have $\varepsilon\chi_{-n} = \chi_1\chi_2$, where χ_1 and χ_2 are Dirichlet characters mod $\frac{mn}{kl}$ and mod $2^{s+1}kl$ respectively. Acting with $W_{N,kl}$ on modular forms gives us an isomorphism:

$$S_2(N, \varepsilon\chi_{-n}) \quad \xrightarrow{\sim} \quad S_2(N, \overline{\chi_1}\chi_2).$$

Since we have:

$$W_{N,kl} = \begin{pmatrix} 1 & b \\ -2^{s+1}kl & \frac{mn}{kl} d \end{pmatrix} \begin{pmatrix} \frac{mn}{kl} & 0 \\ 0 & 1 \end{pmatrix} \ ,$$

and since $\det W_{N,kl} = \frac{mn}{kl}$, which is precisely the width of the cusp $-(2^{s+1}kl)^{-1}$ with respect to $\Gamma_0(N)$, we find that a form $f \in S_2(N, \varepsilon\chi_{-n})$ has order greater than:

$$2^{s-3} \cdot \frac{m}{k} \cdot \left(\frac{n}{l} + l\right) \quad \text{at} \quad -(2^{s+1}kl)^{-1}$$

if and only if the first $2^{s-3} \cdot \frac{m}{k} \cdot \left(\frac{n}{l} + l\right)$ Fourier coefficients at ∞ (counting from the coefficient of $e^{2\pi i z}$) of $f|W_{N,kl}$ are 0.

Thus it is clear that if we have an algorithm for finding integral bases for spaces of cusp forms of weight 2, and as we noted above such an algorithm will be given in IV and V, together with an algorithm for determining the action of the above 'Atkin-Lehner operators', then we have in certain favorable cases (and in fact in all cases to be considered in VI) an algorithm for computing $\dim S_1(N, \varepsilon)$ (and in fact for determining an integral basis for $S_1(N, \varepsilon)$). The question of determining the action of the 'Atkin-Lehner operators' will be considered in IV (and in VI).

2. Liftings of 2-dimensional projective Galois representations over $\mathbb{Q}$

We return to the discussion of 1.2 and in particular to the question of determining the number $d(N, \varepsilon)$, i.e. the number of equivalence classes of irreducible representations:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$$

with Artin conductor N and determinant character ε. In the following we do not assume that the representations are odd, i.e. we do not require $\varepsilon(-1) = -1$. Given the representation ρ, we may consider its projectivisation:

$$\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{C}).$$

We now want to reverse this situation, i.e. to consider $\bar{\rho}$ as being given and ask for 'liftings' of $\bar{\rho}$, where by a lifting of $\bar{\rho}$ we shall understand a representation ρ as above whose projectivisation is $\bar{\rho}$. According to a theorem of Tate, such liftings always exist. Our prime concern is now of course to obtain information on the Artin conductors and determinant characters of such liftings. We want to ask the following question: Given $\bar{\rho}$ as above, what are the possible pairs (N, ε), where $N \in \mathbb{N}$ and ε is a Dirichlet character modulo N, such that $\bar{\rho}$ has a lifting with Artin conductor N and determinant (character) ε? For each occurring pair (N, ε) one also wants to know its 'multiplicity', i.e. the number of inequivalent liftings of $\bar{\rho}$ with Artin conductor N and determinant ε.

Given an answer to this question, we can reduce the problem of enumerating all (irreducible) Galois representations:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$$

with given Artin conductor, N, and determinant, to a question in geometry of numbers: For if ρ has Artin conductor N, then the *minimal* Artin conductor of a lifting of the associated projective representation $\bar{\rho}$ will certainly be $\leq N$, and this gives, as will become clear from the following, an explicit bound for the discriminant $D(K/\mathbb{Q})$, where K is the fixed field of the kernel of $\bar{\rho}$. The finitely many possibilities for K can thus, at least in principle, be found by geometry of numbers.

Let us now return to the situation where the projective representation $\bar{\rho}$ is given. Now, if ρ is any lifting of $\bar{\rho}$, then the other liftings of $\bar{\rho}$ are $\rho \otimes \chi$, where χ runs through the characters of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The determinant of $\rho \otimes \chi$ is:

$$\det(\rho \otimes \chi) = \det(\rho) \cdot \chi^2,$$

hence it is clear that we can answer the above question, if we can point to *one* lifting ρ, with such precision that we may determine $\det(\rho)$ and the Artin conductor of every 'twist' $\rho \otimes \chi$. Let us now localize the question by choosing for each prime number p a place of $\overline{\mathbb{Q}}$ over p; let D_p resp. I_p be the associated decomposition resp. inertia group. The restriction $\bar{\rho}_p$ of $\bar{\rho}$ to D_p can be viewed as a projective representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. The following theorem of Tate is now helpful.

Theorem. *(Tate, cf. [13]) Let $\bar{\rho}$ be a projective representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Assume that for each prime number p there is a given lifting r_p of $\bar{\rho}_p$. Assume further that r_p is unramified (i.e. $r_p(I_p) = 1$) for all but finitely many p. Then there is a lifting ρ of $\bar{\rho}$ such that:*

$$\rho \mid I_p = r_p \mid I_p \quad \text{for all } p,$$

and ρ is unique.

Given $\bar{\rho}$, the restriction $\bar{\rho}_p$ is unramified for almost all p, and one knows that there is always a system (r_p) of liftings of $\bar{\rho}_p$ satisfying the requirements of the theorem, cf. [13]. In the situation of the theorem the determinant of ρ is given, once one knows its restriction to I_p for all p, and this restriction is $\det(r_p) \mid I_p$. Viewing via local class field theory the character $\det(r_p)$ as a character of $\mathbb{Q}_p^\times$, this restriction is simply the restriction of $\det(r_p)$ to the group of units of $\mathbb{Z}_p$. Furthermore, if χ is a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then we may by global class field theory view χ as an idele class character and consider its restriction χ_p to $\mathbb{Q}_p^\times$ for every p. The Artin conductor of $\rho \otimes \chi$ is the product of the Artin conductors of $r_p \otimes \chi_p$ for all p. (Note that these latter conductors depend only on the restriction of r_p to I_p.)

Concerning the question of equivalence of twists $\rho \otimes \chi$ in case ρ is 2-dimensional, one must know for what characters χ the representations ρ and $\rho \otimes \chi$ are equivalent. If χ is non-trivial this can only happen, if $\mathrm{Im}(\bar{\rho})$ is a dihedral group, and this case can be completely analyzed, as will become clear from the following, by use of the well-known theorem of Mackey concerning induced representations. Thus, we shall not pursue this question further.

It is now clear that we can answer the above question once we have solved the following problem.

Problem: Let p be a prime number and let $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{PGL}_2(\mathbb{C})$ be a (continuous) representation. Determine for some lifting ρ of $\bar{\rho}$ the following:

(1) the restriction of $\det(\rho)$ to the group of units of $\mathbb{Z}_p$, viewing $\det(\rho)$ as a character of $\mathbb{Q}_p^\times$,

(2) the Artin conductor of $\rho \otimes \chi$, where χ runs through all characters of $\mathbb{Q}_p^\times$.

(ρ has to be chosen to be unramified, if $\bar{\rho}$ is unramified.)

This problem will be solved in the following two sections.

Given $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{PGL}_2(\mathbb{C})$, let us consider the finite extension $M/\mathbb{Q}_p$ which is cut out by $\bar{\rho}$, i.e. M is the fixed field of the kernel of $\bar{\rho}$. For the Galois group $G = \mathrm{Gal}(M/\mathbb{Q}_p)$ we have a priori the following possibilities:

(a) G is a cyclic group,

(b) G is a dihedral group,

(c) G is isomorphic to A_4 or S_4,

since G is a finite, solvable subgroup of $\mathrm{PGL}_2(\mathbb{C})$.

Here, we may dispose of case (a) immediately: If G is a cyclic group, then $\bar{\rho}$ is given by a character χ_0 of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, and the liftings of $\bar{\rho}$ are the representations:

$$\rho(\chi) : g \mapsto \begin{pmatrix} \chi_0(g)\chi(g) & 0 \\ 0 & \chi(g) \end{pmatrix},$$

where χ runs through all characters of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. The determinant of $\rho(\chi)$ is $\chi_0\chi^2$ and its Artin conductor is the product of the conductors of $\chi_0\chi$ and χ.

The cases (b) and (c) will be considered in sections 3 and 4 respectively. As the proofs are somewhat technical we shall merely give the main points; details will appear elsewhere. For case (c) there is already essential information available: Building upon [17], the *minimal* conductor of a lifting of $\bar{\rho}$ was determined by Buhler and Zink, cf. [3] and [18]. In fact, the conductors of twists $\rho \otimes \chi$, where ρ is a lifting of $\bar{\rho}$ with minimal conductor, were determined in [18]. Hence, in this case our problem is to complement these works by discussing the associated determinant characters.

Let us now introduce the following notation. If p is a prime number and $M/\mathbb{Q}_p$ a finite extension, let O_M denote the ring of integers in M, $\wp_M$ its prime ideal, π_M a prime element of $\wp_M$, $U_M^0 = U_M$ the group of units of O_M and for $i \in \mathbb{N}$ let U_M^i denote the group of 1-units of level $\geq i$. Let E_M denote the group of roots of unity in $M^\times$ of order prime to p, and let for l a prime number $\mu_{l^\infty}(M)$ be the group of roots of unity in $M^\times$ of l-power order. The extension of M obtained by adjoining the p'th roots of units will be denoted by $M(\mu_p)$. Finally, denote by $\wp_M^{c_M(\chi)}$ the (class field theoretic) conductor of χ, if χ is a character of $M^\times$; for convenience, we shall refer to $c_M(\chi)$ as the conductor of χ.

3. The dihedral case

Consider a projective representation:

$$\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{PGL}_2(\mathbb{C})$$

of dihedral type, i.e. the extension $M/\mathbb{Q}_p$ cut out by $\bar{\rho}$ has Galois group isomorphic to:

$$D_n = \langle \sigma, \tau \mid \sigma^2 = \tau^n = 1 , \sigma\tau\sigma^{-1} = \tau^{-1} \rangle$$

for some $n \geq 2$. We want to recall a few elementary facts, for which the reader is referred to [13], about this situation. The field M contains a quadratic extension $L/\mathbb{Q}_p$ corresponding to the cyclic subgroup $\langle \tau \rangle$ of D_n. (There is exactly 1 such quadratic extension in M (i.e. such that M/L is cyclic) if $n \geq 3$, and if $n = 2$ we let L denote any of the 3 quadratic extensions in M.) The Galois group of M/L is then cyclic of order n, so that the restriction of $\bar{\rho}$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$ is given by a character χ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$. Conversely, if $L/\mathbb{Q}_p$ is a given quadratic extension and χ is a non-trivial character of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$, then the field M cut out by χ is Galois over $\mathbb{Q}_p$ with dihedral Galois group if and only if $\chi \circ \mathrm{Ver}_{L/\mathbb{Q}_p}$ vanishes, where $\mathrm{Ver}_{L/\mathbb{Q}_p}$ denotes the transfer. If this condition is fulfilled, χ then gives rise to a unique projective representation $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{PGL}_2(\mathbb{C})$ of dihedral type. Any lifting ρ of $\bar{\rho}$ has (up to equivalence) the form:

$$\rho = \mathrm{Ind}_{L/\mathbb{Q}_p}(\psi),$$

where $\mathrm{Ind}_{L/\mathbb{Q}_p}$ means induction from $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, and where ψ is a character of $\mathrm{Gal}\overline{\mathbb{Q}}_p/L)$ with:

$$\psi(\sigma g \sigma^{-1}) = \chi(g)\psi(g), \quad g \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/L),$$

where σ denotes any element of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) - \mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$. The Artin conductor of ρ is:

$$A(\rho) = D(L/\mathbb{Q}_p) N_{L/\mathbb{Q}_p}\left(\wp_L^{c_L(\psi)}\right),$$

where $D(L/\mathbb{Q}_p)$ is the discriminant of $L/\mathbb{Q}_p$ and $N_{L/\mathbb{Q}_p} : L \to \mathbb{Q}_p$ the norm, and its determinant is:

$$\det(\rho) = \varepsilon \cdot (\psi \circ \mathrm{Ver}_{L/\mathbb{Q}_p}),$$

where ε is the quadratic character corresponding to $L/\mathbb{Q}_p$. Furthermore, if φ is a character of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, then:

$$\rho \otimes \varphi = \mathrm{Ind}_{L/\mathbb{Q}_p}(\psi) \otimes \varphi = \mathrm{Ind}_{L/\mathbb{Q}_p}(\psi \cdot \; res \; (\varphi)),$$

where res is the restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$.

Viewing χ and ψ as characters of $L^\times$ and φ as a character of $\mathbb{Q}_p^\times$, we now see (by class field theory) that the problem of section 2 amounts to the following:

Given a quadratic extension $L/\mathbb{Q}_p$ and a character χ of $L^\times$ which vanishes on $\mathbb{Q}_p^\times$, determine for a character ψ of $L^\times$ such that:

$$(*) \qquad \psi\left(\frac{\sigma x}{x}\right) = \chi(x) \quad \text{for all } x \in L^\times,$$

where σ denotes the generator of $\mathrm{Gal}(L/\mathbb{Q}_p)$, the following:

(1) the restriction of ψ to the group of units of $\mathbb{Z}_p$,

and

(2) the conductor of $\psi \cdot (\varphi \circ N_{L/\mathbb{Q}_p})$, where φ runs through the characters of $\mathbb{Q}_p^\times$.

This is done by theorem 1 below together with the remarks following it. We have chosen to state and prove a slightly more general result, because this costs little extra effort and because we want to make it clear what sort of problems one would have to solve, if one wanted to consider the situation for an arbitrary p-adic ground field.

Proposition 1. *Suppose that l is a prime number, that $K/\mathbb{Q}_p$ is a finite extension and that $K^\times$ contains the l'th roots of unity. Let L/K be a Galois extension with Galois group $G \cong \mathbb{Z}/\mathbb{Z}l$, and let σ be a generator of G. Denote by $\sigma - 1$ the endomorphism $x \mapsto x^{-1}\sigma x$ of $L^\times$.*

(1) *Let $i \in \mathbb{N}$. An element $x \in K^\times$ belongs to $(L^x)^{\sigma-1} U_L^i$ if and and only if $x^p \in N_{L/K}(U_L^i)$.*

(2) *Suppose that L/K is unramified. Then: $(U_L^i)^{\sigma-1} \le U_L^i$ for all $i \in \mathbb{N}$, and the homomorphism:*

$$U_L^i/U_K^iU_L^{i+1} \to U_L^i/U_L^{i+1}$$

induced by $\sigma - 1$ is injective.

(3) *Suppose that L/K is ramified with ramification groups:*

$$G = G_0 = \ldots = G_t \ne G_{t+1} = 0$$

(where t is a non-negative integer).

If $i \in \mathbb{N}$ with $l \mid i$, we have: $(U_L^i)^{\sigma-1} \le U_L^{i+t+1}$.

If $i \in \mathbb{N}$ with $l \nmid i$, then: $(U_L^i)^{\sigma-1} \le U_L^{i+t}$, and the homomorphism:

$$U_L^i/U_L^{i+1} \to U_L^{i+t}/U_L^{i+t+1}$$

induced by $\sigma - 1$ is an isomorphism.

Proof. (1) This is a trivial consequence of Hilbert's theorem 90.

(2) Clearly, $\sigma - 1$ maps U_L^i into itself for all $i \in \mathbb{N}$. Choose $\pi = \pi_K$ as a prime element of L. If $u \in U_L^i - U_L^{i+1}$ and $u^{-1}\sigma u \in U_L^{i+1}$, then choose $a \in E_L$ such that u is represented by $1 + a\pi^i$ modulo U_L^{i+1}. One then finds:

$$\frac{\sigma(1 + a\pi^i)}{1 + a\pi^i} \equiv 1 + (\sigma a - a)\pi^i \mod \wp_L^{2i},$$

whence a is not a unit. One deduces $a \in K^\times$ and so $u \in U_K^iU_L^{i+1}$.

(3) Suppose that L/K is wildly ramified, i.e. $t > 0$, i.e. $l = p$. Let π be a prime element for L. Then:

$$\sigma\pi = \pi + u\pi^{t+1},$$

where u is a unit, since $\sigma \in G_t - G_{t+1}$. If $i \in \mathbb{N}$ and $b \in O_L$, then as $\sigma b \equiv b \mod \wp_L^{t+1}$ one easily finds:

$$\frac{\sigma(1 + b\pi^i)}{1 + b\pi^i} \equiv 1 + iu(\sigma b)\pi^{i+t} \mod \wp_L^{i+t+1}.$$

From this the assertions follow immediately.

The case $t = 0$ is similar, but simpler. □

We want to consider the situation of proposition 1 in the case that $K = \mathbb{Q}_p(\mu_p)$ and $l = p$, i.e. L/K is a Galois extension with Galois group $G \cong \mathbb{Z}/\mathbb{Z}p$. Let σ be a generator of G. Recall that the group of 1-units of K has a basis, as a $\mathbb{Z}_p$-module, of the form:

$$\zeta, \eta_2, \ldots, \eta_p\ ,$$

whereζ is a primitive p'th root of unity and η_i has level exactly i (i.e. $\eta_i \in U_K^i - U_K^{i+1}$) for $i = 2, \ldots, p$ (cf. [7] pp. 246–247). Here, and in what follows, we suppose that a choice of the elements $\eta_2, \ldots, \eta_p$ has been fixed. Put:

$$U_K' = \langle \eta_2, \ldots, \eta_p \rangle\ .$$

Let χ be a character of $L^\times$ which vanishes on $K^\times$. Let $c = 1$ if χ is unramified and $c = c_L(\chi)$ otherwise.

Suppose first that L/K is ramified with $t = p - 1$, where t is defined as in proposition 1, and that χ is wildly ramified, i.e. $c > 1$. Let the integer a be such that $c \equiv a(p)$ and $1 \leq a \leq p$. Using [12], chapter 5, one finds:

$$U_K^{\frac{1}{p}(c-a)+p} = N_{L/K}(U_L^{c+p-1}),$$

so that if $u \in U_K'$ with $u^p \in U_K^{\frac{1}{p}(c-a)+p}$, then there is $x \in L^\times$ such that:

$$u \equiv \frac{\sigma x}{x} \mod U_L^{c+p-1}.$$

If $x, y \in L^\times$ and:

$$\frac{\sigma x}{x} \equiv \frac{\sigma y}{y} \mod U_L^{c+p-1},$$

put $z = x/y$. Then $z^{-1}\sigma z \in U_L^{c+p-1}$, and since $c \geq 1$, we see that $z \in K^\times U_L^1$. If $z \in K^\times$, then $\chi(x) = \chi(y)$. Otherwise, choose $i \in \mathbb{N}$ largest possible such that $z \in K^\times U_L^i$. Then $p \nmid i$, since $U_L^j \leq K^\times U_L^{j+1}$, if $p \mid j$. So, proposition 1 gives that $z^{-1}\sigma z \notin U_L^{i+p}$; as $z^{-1}\sigma z \in U_L^{c+p-1}$, we have $i \geq c = c_L(\chi)$, hence $\chi(z) = 1$. Since $\eta_2, \ldots, \eta_p$ form a basis of U_K', we infer the existence of a character ψ_2 on U_K' satisfying the following requirements: For $i = 2, \ldots, p$ let $s_i \geq 1$ be smallest possible such that:

$$\eta_i^{p^{s_i}} \in U_K^{\frac{1}{p}(c-a)+p},$$

and let $x_i \in L^\times$ be such that:

$$\eta_i^{p^{s_i-1}} \equiv \frac{\sigma x_i}{x_i} \mod U_L^{c+p-1}.$$

The requirements are then:

$$\psi_2(\eta_i^{p^{s_i-1}}) = \chi(x_i)\ , \quad i = 2, \ldots, p.$$

We let ψ_2 denote any such character. One easily sees, that ψ_2 has the following property: If $u \in U_K'$ and $x \in L^\times$ are such that:

$$u \equiv \frac{\sigma x}{x} \mod U_L^{c+p-1},$$

then:

$$\psi_2(u) = \chi(x).$$

Suppose then that L/K is unramified. By a similar, but simpler argument, one now infers the existence of a character ψ_2 on U_K' satisfying: Let for $i = 2, \ldots p$ the integer $s_i \geq 1$ be smallest possible such that:

$$\eta_i^{p^{s_i}} \in U_L^c.$$

Then there are $x_i \in L^\times$ such that:

$$\eta_i^{p^{s_i-1}} \equiv \frac{\sigma x_i}{x_i} \mod U_L^c\ , \quad i = 2, \ldots, p,$$

and the requirements are:

$$\psi_2(\eta_i^{p^{s_i-1}}) = \chi(x_i)\ , \quad i = 2, \ldots, p.$$

Denote by ψ_2 any such character. One finds that ψ_2 has the property: If $u \in U_K'$ and $x \in L^\times$ are such that:

$$u \equiv \frac{\sigma x}{x} \mod U_L^c,$$

then:

$$\psi_2(u) = \chi(x).$$

Theorem 1. *Suppose that l and p are prime numbers, and that K is a finite extension of $\mathbb{Q}_p$ containing the l'th roots of unity. Let L/K be a Galois extension with Galois group $G \cong \mathbb{Z}/\mathbb{Z}l$ and let σ be a generator of G. If L/K is unramified, put $t = 0$. If L/K is ramified, we denote by $t \geq 0$ the break in the ramification filtration of G:*

$$G = G_0 = \ldots = G_t \neq G_{t+1} = 0.$$

If $l = p$, we make the assumption that $K = \mathbb{Q}_p(\mu_p)$, and furthermore that $t \geq p-1$, if L/K is ramified.

Let χ be a non-trivial character on $L^\times$ which vanishes on $K^\times$. Let $\alpha \in K^\times$ be such that $L = K(\alpha^{1/l})$, and let the primitive l'th root of unity be such that:

$$\sigma\alpha^{1/l} = \zeta\alpha^{1/l}.$$

Let ψ_1 be a character of $\mu_{l^\infty}(K)$ satisfying the following requirements:

$$\begin{array}{rlll} \psi_1 = 1\ , & \text{if} \quad L \neq K(\sqrt{-1}) & \text{and} & \chi(\alpha^{1/l}) = 1\ , \\ \psi_1(\zeta) = \chi(\alpha^{1/l})\ , & \text{if} \quad L \neq K(\sqrt{-1}) & \text{and} & \chi(\alpha^{1/l}) \neq 1\ , \\ \psi_1 = 1\ , & \text{if} \quad L = K(\sqrt{-1}) & \text{and} & \chi(1+\sqrt{-1}) = 1\ , \\ \psi_1(-1) = \chi(1+\sqrt{-1})^2\ , & \text{if} \quad L = K(\sqrt{-1}) & \text{and} & \chi(1+\sqrt{-1}) \neq 1\ . \end{array}$$

(Note that if also $L = K(\beta^{1/l})$, then $\chi(\alpha^{1/l}) \neq 1 \Longleftrightarrow \chi(\beta^{1/l}) \neq 1$.)

Define:

$$c = \begin{cases} 1, & \textit{if } \chi \textit{ is unramified} \\ c_L(\chi), & \textit{if } \chi \textit{ is ramified} \end{cases}$$

If $l \neq p$, let U'_K be U^1_K , and put $U'_K = \langle \eta_2, \ldots, \eta_p \rangle$ if $l = p$. Let ψ_2 be the trivial character on U'_K, if either $l \neq p$ or if $l = p$ and L/K is ramified with either $t \geq p$ or ($t = p-1$ and $c = 1$). Otherwise, i.e. if $l = p$ and L/K is either unramified of ramified with ($t = p-1$ and $c > 1$), let ψ_2 be a character on U'_K of the type described immediately after proposition 1.

Finally, denote by U_0 the group of roots of unity in $K^\times$ of order prime to lp.

Then there exists a character ψ on $L^\times$ such that:

(i) $$\psi\left(\frac{\sigma x}{x}\right) = \chi(x) \quad \textit{for all } x \in L^\times$$

(ii) $$\psi(\langle \pi_L \rangle U_0) = 1$$

(iii) $$\psi \mid \mu_{l^\infty}(K) = \psi_1$$

(iv) $$\psi \mid U'_K = \psi_2$$

and

(v) $$c_L(\psi) = c + t.$$

Furthermore, if φ is a character of $K^\times$ and $N_{L/K}$ denotes the norm map $L^\times \to K^\times$, then:

$$c_L(\psi \cdot (\varphi \circ N_{L/K})) = \max\left\{c+t\ , c_L(\varphi \circ N_{L/K})\right\}\ ,$$

and for the number $c_L(\varphi \circ N_{L/K})$:

$$c_L(\varphi \circ N_{L/K}) = c_K(\varphi)\ , \quad \textit{if } L/K \quad \textit{is unramified}$$

and if L/K is ramified:

$$\begin{array}{rcll} c_L(\varphi \circ N_{L/K}) & = & lc_K(\varphi) + (1-l)t + 1\ , & \quad \textit{if } c_K(\varphi) \geq t+2\ , \\ c_L(\varphi \circ N_{L/K}) & \leq & t+1\ , & \quad \textit{if } c_K(\varphi) \leq t+1. \end{array}$$

Proof. Using the fact that if $\xi \in (L^\times)^{\sigma-1} \cap \mu_{l^\infty}(L)$, then $N_{L/K}(\xi) = 1$ and:

$$\sigma\xi = \zeta^a \xi \quad \text{with} \quad a \not\equiv 0 \quad (l), \quad \text{if} \quad \xi \notin K^\times,$$

one easily finds:

$$(*) \qquad (L^\times)^{\sigma-1} \cap \mu_{l^\infty}(L) = \begin{cases} \langle\sqrt{-1}\rangle, & \text{if} \quad L = K(\sqrt{-1}) \\ \langle\zeta\rangle, & \text{otherwise} \end{cases}$$

Define the character ψ_0 on $(L^\times)^{\sigma-1}$ by:

$$\psi_0\left(\frac{\sigma x}{x}\right) = \chi(x) \quad \text{for} \quad x \in L^\times;$$

this is well-defined since χ vanishes on $K^\times$. It now follows from $(*)$ and the definition of ψ_1 that there is a character on $(L^\times)^{\sigma-1}\mu_{l^\infty}(L)$ whose restriction to $(L^\times)^{\sigma-1}$ and $\mu_{l^\infty}(K)$ respectively is ψ_0 and ψ_1 respectively.

If $y \in (L^\times)^{\sigma-1}\mu_{l^\infty}(L) \cap U'_K$, then:

$$y^l = N_{L/K}(y) \in \mu_{l^\infty}(K) \cap U'_K = \{1\}.$$

So, if $l \neq p$ we have $y = 1$, since y is a 1-unit. If $l = p$, it also follows that $y = 1$, since $y \in U'_K$ and U'_K is torsion free for $l = p$.

We deduce the existence of a character on $(L^\times)^{\sigma-1}\mu_{l^\infty}(L)U'_K$ whose restriction to $(L^\times)^{\sigma-1}$, $\mu_{l^\infty}(K)$ and U'_K respectively is ψ_0, ψ_1 and ψ_2 respectively. We fix one such character and denote it by abuse of notation by ψ_0.

Denote by i_0 the smallest non-negative integer such that:

$$U_L^{i_0} \cap (L^\times)^{\sigma-1} \leq \mathrm{Ker}(\psi_0).$$

We claim that:

$$(**) \qquad i_0 = c + t.$$

Note that $i_0 \geq 1$, because $(L^\times)^{\sigma-1} \leq U_L^0$ and because ψ_0 cannot be trivial on $(L^\times)^{\sigma-1}$ since χ is non-trivial.

Let us show $(**)$ in the case where L/K is unramified and χ is wildly ramified. Then $c + t = c_L(\chi) + t$. We note that $c \not\equiv 1\ (l)$. This follows once we note that if $i \in \mathbb{N}$ is divisible by l, then:

$$U_L^i \leq K^\times U_L^{i+1}.$$

There is an $x \in U_L^{c-1}$ with $\chi(x) \neq 1$. Now proposition 1 gives that $x^{-1}\sigma x \in U_L^{c-1+t} - U_L^{c+t}$, since $c-1$ is not divisible by l. Hence $i_0 \geq c+t$. On the other hand, suppose that $x \in L^\times$ is such that $x \notin K^\times$ and $x^{-1}\sigma x \in U_L^{c+t}$. Let i be largest possible such that $l \nmid i$ and such that there is a $y \in U_L^i$ with $x \equiv y \bmod K^\times$. Then $y \notin U_L^{i+1}$; for if $l \nmid i+1$, this is clear, and otherwise there is a $y_1 \in U_L^{i+2}$ with $y \equiv y_1 \bmod K^\times$ and $l \nmid i+2$. As $l \nmid i$, proposition 1 gives that $x^{-1}\sigma x = y^{-1}\sigma y \notin U_L^{i+t+1}$. So: $i \geq c$, whence $\chi(x) = \chi(y) = 1$. We conclude that $i_0 \leq c+t$.

The proof of $(**)$ in the other cases, i.e. L/K unramified or L/K ramified but χ unramified, is similar but simpler.

Concerning the norm map $N_{L/K} : \times \to K^\times$ we note the following: If L/K is unramified, then:

$$N_{L/K}(U_L^i) = U_K^i \quad \text{for all} \quad i \geq 0,$$

and if L/K is ramified, we have:

$$N_{L/K}(U_L^{lx+(1-l)t+1}) = \ldots = N_{L/K}(U_L^{lx+(1-l)t+l}) = U_K^{x+1} \quad \text{for} \quad x \geq t,$$

and

$$N_{L/K}(U^{x+1}) \leq U_K^{x+1} \quad \text{for} \quad 0 \leq x \leq t,$$

cf. [12], V. From this, the remarks in the statement of the theorem about the number $c_L(\varphi \circ N_{L/K})$ for a character φ of $K^\times$ immediately follow.

We now claim that:

$$(***) \qquad \langle \pi_L \rangle U_0 U_L^{i_0} \cap (L^\times)^{\sigma-1} \mu_{l^\infty}(L) U'_K \leq \mathrm{Ker}(\psi_0)\ .$$

The rest of the theorem follows from $(***)$. For if $(***)$ holds, then we know from harmonic analysis that there is a character ψ on the locally compact group $L^\times$ whose restriction to the compact group $(L^\times)^{\sigma-1}\mu_{l^\infty}(L)U'_K$ is ψ_0 and which vanishes on the closed subgroup $\langle \pi_L \rangle U_0 U_L^{i_0}$. If ψ is any such character, then ψ satisfies (i), (ii), (iii), and (iv) in the statement of the theorem and $c_L(\psi)$ is at the most $i_0 = c+t$. Furthermore, by definition of i_0 there is an $x \in U_L^{i_0-1} \cap (L^\times)^{\sigma-1}$ with $\psi(x) \neq 1$. Hence $c_L(\psi)$ is exactly i_0. If φ is any character on $K^\times$, then $\varphi \circ N_{L/K}$ vanishes on $(L^\times)^{\sigma-1}$ and in particular $(\varphi \circ N_{N/L})(x) = 1$. It follows that:

$$c_L(\psi \cdot (\varphi \circ N_{L/K})) = \max\left\{c_L(\psi)\ , c_L(\varphi \circ N_{L/K})\right\}.$$

Concerning the proof of $(***)$:

Suppose that $y \in \langle \pi_L \rangle U_0 U_L^{i_0} \cap (L^\times)^{\sigma-1}\mu_{l^\infty}(L)U'_K$. As $y \in (L^\times)^{\sigma-1}\mu_{l^\infty}(L)U'_K$, y is a unit, so that we can write:

$$y = u_0 u = \frac{\sigma x}{x} \cdot \xi u_1,$$

with $u_0 \in U_0$, $u \in U_L^{i_0}$, $x \in L^\times$, $\xi \in \mu_{l^\infty}(L)$ and $u_1 \in U'_K$. Then $N_{L/K}(y) = N_{L/K}(\xi)u_1^l$, so there is an $s \in \mathbb{N}$ such that:

$$N_{L/K}(y)^{l^s} \quad \text{is a 1-unit.}$$

On the other hand, $N_{L/K}(y) = u_0^l N_{L/K}(u)$, hence:

$$u_0^{l^{s+1}} \quad \text{is a 1-unit.}$$

Since u_0 is a root of unity of order prime to lp, we deduce:

$$u_0 = 1.$$

One now splits the discussion up into 4 cases: ($l \neq p$ or $l = p$) and (L/K unramified or L/K ramified). Let us for example consider the case $l = p$ and L/K ramified. We have $K = \mathbb{Q}_p(\mu_p)$ which has ramification index $e = p - 1$ over $\mathbb{Q}_p$. Since the 1-units $\eta_2, \ldots, \eta_p$ have level $> \frac{e}{p-1}$, it follows that if $\lambda \in U_K'$ has level exactly i, then λ^p has level exactly $i + e$. Choose a such that $1 \leq a \leq p$ and $c \equiv a$ (p), and put $w = \frac{1}{p}(c - a) + t$. Now,

$$N_{L/K}(\xi)u_1^p = N_{L/K}(u) \in N_{L/K}(U_L^{c+t}) = U_K^{w+1},$$

and so $N_{L/K}(\xi)$ and u_1^p both belong to U_K^{w+1}. As $N_{L/K}(\xi)$ is a power of ζ, we must have $N_{L/K}(\xi) = 1$, so $\xi \in (L^\times)^{\sigma-1}$. Consequently, there is $x_0 \in L^\times$ such that:

$$y = u = \frac{\sigma x_0}{x_0} \cdot u_1.$$

Suppose first that $t \geq p$ or ($t = p - 1$ and $c = 1$). In both cases we have:

$$t \geq p - \frac{p - a}{p - 1},$$

and this gives:

$$u_1 \in U_K^{w+1-e} \leq U_L^{p(w+1-e)} \leq U_L^{c+t},$$

hence $x_0^{-1}\sigma x_0 \in U_L^{c+t}$. We then deduce that $x_0 \in K^\times U_L^c$. For, since $c \geq 1$, we must have $x_0 \in K^\times U_L^1$, so if $x_0 \notin K^\times$ we choose i largest possible such that $x_0 \in K^\times U_L^i$; then $p \nmid i$, and proposition 1 gives $\frac{\sigma x_0}{x_0} \notin U_L^{i+t+1}$, hence $i \geq c$.

We then get:

$$\psi_0(y) = \chi(x_0)\psi_0(u_1) = \psi_2(u_1) = 1,$$

since ψ_2 is trivial.

Suppose then that $t = p - 1$ and $c > 1$. Now,

$$u_1^{-1} \equiv \frac{\sigma x_0}{x_0} \mod U_L^{c+t},$$

so from the properties of ψ_2 we obtain:

$$\psi_0(y) = \chi(x_0)\psi_2(u_1) = \chi(x_0)\chi(x_0^{-1}) = 1.$$

□

Remark 1. *As is clear from the proof of theorem 1, there is, in the setting of theorem 1 for an arbitrary ground field K (containing the l'th roots of unity), always a character ψ on $L^\times$ such that $\psi(x^{-1}\sigma x) = \chi(x)$ for all $x \in \times$ and such that $c_L(\chi) = c + t$ in the notation of the theorem. A special case of this result was given in [3] but without a discussion of the possible behaviour of the restriction of ψ to $K^\times$. It is also clear from the above proof, that the explicit construction of a possible choice of this restriction depends in the general case on a detailed knowledge of the structure of the 1-unit group of K and in particular on the structure of the quotients U_K^1/U_K^i for $i \in \mathbb{N}$. It is also clear that a possible ψ for the case $p \neq 2$, $K = \mathbb{Q}_p(\mu_p)$, and L/K wildly ramified with $t < p - 1$ may be constructed, but we have avoided that since it is unnecessary for our purposes.*

Remark 2. *The value $c+t$ is the smallest possible value of $c_L(\psi)$ if ψ is a character on $L^\times$ with $\psi(x^{-1}\sigma x) = \chi(x)$ for all $x \in L^\times$; this follows immediately from the definition of $i_0(= c+t)$ in the proof of the theorem.*

Remark 3. *The value of $c_L(\psi\cdot(\varphi\circ N_{L/K}))$, where ψ is as in the theorem and φ is a character on $K^\times$, is computed immediately alone from the knowledge of $c_K(\varphi)$. This is clear if L/K is unramified or if L/K is ramified and $c_K(\varphi)\geq t+2$; if L/K is ramified and $c_K(\varphi)\leq t+1$, we get:*

$$c_L(\psi\cdot(\varphi\circ N_{L/K})) = c_L(\psi) = c+t,$$

since then $c_L(\varphi\circ N_{L/K})\leq 1+t$ and $c\geq 1$.

Remark 4. *From the remarks preceding proposition 1 it is clear that the problem of section 1 for representations of dihedral type is solved by theorem 1 once we explicate the character ψ_2 in the cases where it is not a priori trivial. There are 3 such cases: $K=\mathbb{Q}_2$ and $L=\mathbb{Q}_2(\sqrt{\alpha})$, where α is $-3,-1$ or 3, and χ is a character on $L^\times$ vanishing on $\mathbb{Q}_2^\times$ such that χ is wildly ramified if α is -1 or 3. In all 3 cases U_K' is the group generated by 5, and a few simple computations now reveal that we can choose for ψ_2 any character on $\langle 5\rangle$ satisfying the following:*

Let c be defined as in theorem 1.

<u>If $\alpha=-3$:</u> Put $\psi_2=1$ if $c\leq 2$. If $c\geq 3$, we require:

$$\psi_2\left(5^{2^{c-3}}\right) = \chi(1+\eta\cdot 2^{c-1}),$$

where η is a primitive 3'rd root of unity.

<u>If $\alpha=-1$ or $\alpha=3$:</u> Here L/K is wildly ramified and since $c>1$, the number $c=c_L(\chi)$ must be even. Put $\psi_2=1$ if $c=2$. If $c\geq 4$, we require:

$$\psi_2\left(5^{2^{\frac{1}{2}c-2}}\right) = \chi(1+\pi^{c-1}),$$

where π is any prime element of L.

4. The 'primitive' case

Let p be a prime number and $K/\mathbb{Q}_p$ a finite extension. Let us consider a projective representation:

$$\bar\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_p/K) \to \mathrm{PGL}_2(\mathbb{C}) ,$$

such that $\mathrm{Im}(\bar\rho)$ is isomorphic to A_4 or S_4. We want to recall a few facts concerning this situation; we refer to [3] or [18].

First, we must necessarily have $p=2$, cf. [3], pp. 18–20.

Let M denote the fixed field of $\mathrm{Ker}(\bar\rho)$, and put $G=\mathrm{Gal}(M/K)$ so that $\bar\rho$ is given by an embedding of G in $\mathrm{PGL}_2(\mathbb{C})$. The group G contains a unique normal subgroup V isomorphic to the Klein 4-group, and we have G/V either cyclic of order 3 or isomorphic to S_3. Let L denote the fixed field of V. Then M/L is totally, wildly ramified, and L/K is at the most tamely ramified. If $G\cong S_4$, the quadratic extension K_0/K contained in L must then be unramified, and since L/K is not abelian, L/K_0 is tamely ramified of degree 3. Let e denote the ramification index of L/K, so that e is 1 or 3. Since V has no proper subgroup which is normal in G, we see that the ramification groups for M/L are all either V or 0; define $t \geq 1$ such that:

$$V = V_0 = \ldots = V_t \neq V_{t+1} = 0$$

is the sequence of ramification groups for M/L.

For every lifting ρ of $\bar{\rho}$ the restriction of ρ to $\mathrm{Gal}(\overline{\mathbb{Q}}_2/M)$ has the form:

$$\rho(g) = \begin{pmatrix} \chi(g) & 0 \\ 0 & \chi(g) \end{pmatrix},$$

where χ is a character of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/M)$; we refer to χ as the *central character* of the lifting ρ. The Artin conductor $\wp_K^{a(\rho)}$ is related to the conductor of χ by:

$$(\flat) \qquad a(\rho) = \frac{1}{2e}(c_M(\chi) + 3t + 4e - 1).$$

The representation $\bar{\rho}$ has a lifting ρ with central character χ such that:

$$(\flat\flat) \qquad c_M(\chi) = 3t + 1, \quad \text{hence} \quad a(\rho) = \frac{3}{e}t + 2,$$

and $\wp_K^{3t/e+2}$ is the minimal value of the Artin conductor of a lifting of $\bar{\rho}$. Furthermore, if ρ is a lifting with this minimal Artin conductor and χ is its central character, then there is an $u \in U_M^{3t}$ with:

$$(\flat\flat\flat) \qquad N_{M/K}(u) = 1 \quad \text{and} \quad \chi(u) \neq 1.$$

Here, $(\flat)$ and $(\flat\flat)$ are the principal statements of [3], chap. 2, and [18], section 3. The existence of $u \in U_M^{3t}$ with $(\flat\flat\flat)$ follows from the proof of minimality of $3t+1$ in $(\flat\flat)$, cf. [18], section 3.

Now we want to study the norm map $N_{M/K} : M \to K$. Let W be a subgroup of V of order 2 and let L_0 be the fixed field of W. It is easy to see that the ramification groups for M/L_0 and L_0/L are the following:

$$W = W_0 = \ldots = W_t \neq W_{t+1} = 0,$$

and

$$(V/W) = (V/W)_0 = \ldots = (V/W)_t \neq (V/W)_{t+1} = 0.$$

We conclude that:

$$U_{L_0}^{x+1} = N_{M/L_0}(U_M^{2x-t+1}) = N_{M/L_0}(U_M^{2x-t+2}) \quad \text{for } x \geq t,$$

and

$$U_{L_0}^{x} \geq N_{M/L_0}(U_M^{x}) \quad \text{for } 1 \leq x \leq t,$$

and similarly for L_0/L, cf. [12], chap. 5. Hence:

$$\begin{aligned} U_L^{x+1} &= N_{M/L}(U_M^{i}) \qquad \text{for } 4x - 3t + 1 \leq i \leq 4x - 3t + 4\ , \text{ if } x \geq t\ , \\ U_L^{x} &\geq N_{M/L}(U_M^{x}) \qquad \text{if } 1 \leq x \leq t\ . \end{aligned}$$

Using again [12], chap. 5, we furthermore obtain:

$$U_K^{x+1} = N_{L/K}(U_L^{ex+a}) \quad \text{for } x \geq 0, \quad 1 \leq a \leq e.$$

Combined with the above, we find for $1 \le a \le e$:

$$(\natural) \qquad U_K^{x+1} = N_{M/K}(U_M^i) \quad \text{for} \quad 4ex - 3t + 4a - 3 \le i \le 4ex - 3t + 4e,$$

if $ex \ge t - a + 1$, $x \ge 0$, and

$$(\natural\natural) \qquad U_K^{x+1} \ge N_{M/K}(U_M^{ex+a}) \quad \text{if} \quad 0 \le x \le \frac{t-a}{e}.$$

We conclude that if φ is a character on $K^\times$ with conductor $c_K(\varphi) = c$, then:

$$(\sharp) \qquad c_M(\varphi \circ N_{M/K}) \le ec - e + 1, \quad \text{if} \quad c \le \frac{t-1}{e} + 1,$$

and

$$(\sharp\sharp) \qquad c_M(\varphi \circ N_{M/K}) = 4ec - 3t - 4e + 1, \quad \text{if} \quad c \ge \frac{t+1}{e} + 1,$$

since in the latter case: $c - 2 \ge \frac{1}{e}(t - e + 1)$ and $c - 1 \ge \frac{t}{e}$ so that:

$$U_K^c = N_{M/K}(U_M^{4ec-3t-4e+1}),$$

and

$$U_K^{c-1} = N_{M/K}(U_M^{4ec-3t-4e}).$$

Using the above it is now easy to prove the following proposition which is a reformulation of a result due to E.-W. Zink (see [18]).

Proposition 2. *Let $\bar\rho : \mathrm{Gal}(\overline{\mathbb{Q}_2}/K) \to \mathrm{PGL}_2(\mathbb{C})$ be a representation with $\mathrm{Im}(\bar\rho)$ isomorphic to A_4 or S_4. If ρ is any lifting of $\bar\rho$ with minimal Artin conductor, then for any character φ of $K^\times$ we have, retaining the above notation, for the exponent $a(\rho \otimes \varphi)$ of the Artin conductor of $\rho \otimes \varphi$:*

$$\begin{aligned} a(\rho \otimes \varphi) &= \tfrac{3}{e}t + 2 \qquad \textit{for} \quad c_K(\varphi) \le \frac{3t}{2e} + 1 \ , \\ a(\rho \otimes \varphi) &= 2c_K(\varphi) \qquad \textit{for} \quad c_K(\varphi) \ge \frac{3t}{2e} + 1 \ . \end{aligned}$$

Proof. Let ρ be any lifting of $\bar\rho$ with minimal Artin conductor $\wp_K^{3t/e+2}$ and let χ be the central character of ρ. Let φ be a character of $K^\times$ and put $c = c_K(\varphi)$. Now, $\rho \otimes \varphi$ is also a lifting of $\bar\rho$ and its central character is:

$$\chi \cdot (\varphi \circ N_{M/K}).$$

According to ($\flat\flat$) and ($\flat\flat\flat$) above, we have $c_M(\chi) = 3t+1$ and there is an $u \in U_M^{3t}$ with $N_{M/K}(u) = 1$ and $\chi(u) \ne 1$. So, $\chi \cdot (\varphi \circ N_{M/K})$ does not vanish on u, and from this we conclude that:

$$c_M(\chi \cdot (\varphi \circ N_{M/K})) = \max\left\{3t + 1 \ , c_M(\varphi \circ N_{M/K})\right\}.$$

Suppose that $c \ge \frac{3t}{2e} + 1$. We claim that $c \ge \frac{t+1}{e} + 1$. This is clear if $t \ge 2$. If $t = e = 1$, then $c \ge 3 = 1 + \frac{2}{e}$, and if $t = 1, e = 3$, then $\frac{2}{e} + 1 < 2 \le c$. From ($\sharp\sharp$) we conclude that:

$$c_M(\varphi \circ N_{M/K}) = 4ec - 3t - 4e + 1 \ge 3t + 1,$$

hence $c_M(\chi(\varphi \circ N_{M/K})) = 4ec - 3t - 4e + 1$,and:

$$a(\rho \otimes \varphi) = \frac{1}{2e}(c_M(\chi(\varphi \circ N_{M/K})) + 3t + 4e - 1) = 2c.$$

Suppose then that $c \leq \frac{3t}{2e} + 1$. If $c > \frac{t-1}{e} + 1$, then $e(c-1) \geq t$, so that according to (♮):

$$U_K^c = N_{M/K}(U_M^{4ec-3t-4e+1}),$$

whence:

$$c_M(\varphi \circ N_{M/K}) \leq 4ec - 3t - 4e + 1 \leq 3t + 1.$$

If $c \leq \frac{t-1}{e} + 1$, then (♯) gives:

$$c_M(\varphi \circ N_{M/K}) \leq ec - e + 1 \leq t < 3t + 1.$$

So, $c_M(\chi \cdot (\varphi \circ N_{M/K})) = c_M(\chi) = 3t + 1$ in any case, and $a(\rho \otimes \varphi) = \frac{3}{e}t + 2$. □

We shall now restrict the discussion to the ground field $K = \mathbb{Q}_2$. We know, see [17], that $M/\mathbb{Q}_2$ is a finite extension with Galois group isomorphic to A_4 or S_4 if and only if M is one of the following 4 fields.

$$M_1 = \mathbb{Q}_2\left(\zeta_7\ , \sqrt{1+2\zeta_7}\ , \sqrt{1+2\zeta_7^2}\ , \sqrt{1+2\zeta_7^4}\right),$$

where ζ_7 is a primitive 7'th root of unity; put:

$$L = \mathbb{Q}_2(\zeta_3, \pi),$$

where ζ_3 is a primitive 3'rd root of unity and $\pi^3 = 2$, and let α be the automorphism of L with $\alpha\pi = \zeta_3\pi$; define then:

$$M_i = L\left(\sqrt{x_i}\ , \sqrt{\alpha x_i}\ , \sqrt{\alpha^2 x_i}\right) \quad \text{for} \quad i = 2, 3, 4,$$

where $x_2 = 3(1+\pi)(1+\pi^2)$, $x_3 = 3(1+\pi)$ and $x_4 = 1 + \pi^2$. We have:

$$\mathrm{Gal}(M_1/\mathbb{Q}_2) \cong A_4 \quad \text{and} \quad \mathrm{Gal}(M_i/\mathbb{Q}_2) \cong S_4 \quad \text{for} \quad i = 2, 3, 4.$$

In the above notation we have the values $e = 1, 3, 3, 3$ and $t = 1, 5, 5, 1$ respectively for the extensions $M_i/\mathbb{Q}_2$, $i = 1, 2, 3, 4$ respectively.

The following theorem solves the problem of section 2 for 2-dimensional, projective Galois representations over $\mathbb{Q}_2$ of type A_4 or S_4.

Theorem 2. *Let $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}_2}/\mathbb{Q}_2) \rightarrow \mathrm{PGL}_2(\mathbb{C})$ be a representation such that $\mathrm{Gal}(M/\mathbb{Q}_2)$ is isomorphic to A_4 or S_4, where M is the fixed field of $\mathrm{Ker}(\bar{\rho})$. Then $\bar{\rho}$ has a lifting ρ such that its determinant character $\varepsilon = \det(\rho)$, viewed as a character of $\mathbb{Q}_2^\times$, and the Artin conductors $2^{a(\rho\otimes\varphi)}$ of the twist $\rho \otimes \varphi$, where φ is any character of $\mathbb{Q}_2^\times$ with conductor $c = c_{\mathbb{Q}_2}(\varphi)$, satisfy the following.*

I. *If $M = M_1$: $\varepsilon(-1) = -1$, $\varepsilon(5) = 1$, and:*

$$a(\rho \otimes \varphi) = \begin{cases} 5 & \text{for } c \leq 2 \\ 2c & \text{for } c \geq 3\ . \end{cases}$$

II. *If $M = M_2$: $\varepsilon(-1) = -1$, $\varepsilon(5) = 1$, and:*

$$a(\rho \otimes \varphi) = \begin{cases} 7 & \textit{for } c \leq 3 \\ 2c & \textit{for } c \geq 4 \ . \end{cases}$$

III. *If $M = M_3$: $\varepsilon(-1) = \varepsilon(5) = 1$, and:*

$$a(\rho \otimes \varphi) = \begin{cases} 7 & \textit{for } c \leq 3 \\ 2c & \textit{for } c \geq 4 \ . \end{cases}$$

IV. *If $M = M_4$: $\varepsilon(-1) = \varepsilon(5) = 1$, and:*

$$a(\rho \otimes \varphi) = \begin{cases} 3 & \textit{for } c \leq 1 \\ 2c & \textit{for } c \geq 2 \ . \end{cases}$$

Proof. Let ρ be a lifting of $\bar{\rho}$ with minimal conductor and let χ be its central character. Hence $c_M(\chi) = 3t + 1$, where $t = 1, 5, 5, 1$ respectively if $M = M_i$, $i = 1, 2, 3, 4$ respectively. The restriction of $\det(\rho)$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_2/M)$ is given by:

$$\det(\rho)(g) = \begin{pmatrix} \chi(g) & 0 \\ 0 & \chi(g) \end{pmatrix} \ , \quad g \in \mathrm{Gal}(\overline{\mathbb{Q}}_2/M) \ ,$$

hence, if $\varepsilon = \det(\rho)$ is viewed as a character of $\mathbb{Q}_2^\times$ and χ as a character of $M^\times$, we have:

$$(\dagger) \qquad \varepsilon \circ N_{M/\mathbb{Q}_2} = \chi^2 \ .$$

We must determine the restriction of ε to the group of (1-)units of $\mathbb{Q}_2$. Now, the image of the norm map $M^\times \to \mathbb{Q}_2^\times$ coincides with the image of the norm $M_0^\times \to \mathbb{Q}_3^\times$, where $M_0/\mathbb{Q}_2$ is the maximal abelian extension contained in M, and since M_0 is in any case unramified, we have $N_{M/\mathbb{Q}_2}(U_M) = U_{\mathbb{Q}_2}$. Hence it suffices to study the behaviour of χ^2 on U_M. Now, if χ^2 is trivial on U_M, then ε is unramified, hence $\varepsilon = \psi^2$ for some unramified character ψ on $\mathbb{Q}_2^\times$. Then $\rho \otimes \psi^{-1}$ still has minimal conductor and the square of its central character is 1. By replacing ρ by $\rho \otimes \psi^{-1}$ if necessary, we may assume that if χ^2 is non-trivial, it is non-trivial on U_M .

Now, the minimal order among the orders of central characters of liftings of $\bar{\rho}$ is $4, 4, 2, 2$ respectively for the cases $M = M_i$, $i = 1, 2, 3, 4$ respectively, cf. [18], section 2, or [2], where it is shown how to compute this order using a criterion of Serre. Let ρ_1 be a lifting of $\bar{\rho}$ whose central character χ_1 has this minimal order. There is a character ψ of $\mathbb{Q}_2^\times$ such that:

$$\rho = \rho_1 \otimes \psi \ ,$$

if ψ is viewed as a character of $\mathrm{Gal}(\overline{\mathbb{Q}}_2, /\mathbb{Q}_2)$, and this means:

$$(\dagger\dagger) \qquad \chi = \chi_1 \cdot (\psi \circ N_{M/\mathbb{Q}_2}) \ .$$

One now proceeds with an individual discussion in each of the 4 cases $M = M_i$, $i = 1, 2, 3, 4$. Let us for example consider the case:

<u>$M = M_3$:</u> Suppose that χ^2 is non-trivial. Then χ^2 is non-trivial on U_M, and since ($\dagger\dagger$) gives:

$$\chi^2 = \psi^2 \circ N_{M/\mathbb{Q}_2},$$

because $\chi_1^2 = 1$, we deduce that ψ^2 is non-trivial on $U_{\mathbb{Q}_2}$. Since $\psi^2(-1) = 1$, we then see that ψ^2 has conductor at least 3. Then (♯♯) above gives:

$$c_M(\chi^2) = c_M(\chi^2 \circ N_{M/\mathbb{Q}_2}) = 12c_{\mathbb{Q}_2}(\psi^2) - 26 \geq 10,$$

which is impossible: If $u \in U_M^8$, then $u^2 \in U_M^{16}$, and since $c_M(\chi) = 3t + 1 = 16$, we have $c_M(\chi^2) \leq 8$. Hence $\chi^2 = 1$, and $\varepsilon(-1) = \varepsilon(5) = 1$.

The statements about the Artin conductor of the twists $\rho \otimes \varphi$ follow immediately from proposition 2 because ρ is a lifting with minimal Artin conductor. □

5. Examples

5.1. We shall now illustrate the preceding 3 sections with some examples which will be analyzed further in VI.

Denote for square free $n \in \mathbb{Z}$ by χ_n the character of the quadratic field $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$.

We will enumerate irreducible Galois representations:

$$(\ddagger) \qquad \rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$$

with Artin conductor N and determinant character ε in the following cases:

$$\begin{array}{llll} N = p \ , & \varepsilon = \chi_{-p} & \text{with} & p \in \{487, 751, 887, 919, 2083\}, \\ N = 4p \ , & \varepsilon = \chi_{-p} & \text{with} & p \in \{487, 751, 887, 919\}, \\ & & \text{and} & \\ N = 2^5 p \ , & \varepsilon = \chi_{-p} & \text{with} & p \in \{73, 193\}. \end{array}$$

Note that the numbers 73, 193, 487, 751, 887, 919 and 2083 are prime numbers.

We shall fix the following notation. The symbol ρ denotes a representation (‡). If ρ is such a representation, we denote by $\bar{\rho}$ the associated projective representation, by $K/\mathbb{Q}$ the extension cut out by $\bar{\rho}$, and for a prime number l by G_l the (isomorphism class of the) image under $\bar{\rho}$ of some decomposition group over l. Also, N and ε denote the Artin conductor and determinant character of ρ respectively.

In the following we shall occasionally make use of the following simple principle: Suppose that G is the absolute Galois group of a number field L (finite extension of $\mathbb{Q}$), that V is a finite-dimensional complex vector space and that:

$$R : G \to \mathrm{Aut}(V)$$

is a continuous representation. If M/L is the Galois extension cut out by R and M_0/L is a cyclic subextension, then the class field theoretic conductor of M_0/L divides the Artin conductor of R. This follows from the corresponding local statement:

Lemma 2. *Suppose that p is a prime number, $L/\mathbb{Q}_p$ a finite extension, M/L a finite Galois extension with Galois group G, N a normal subgroup of G with G/N cyclic, M_0 the fixed field of N in M, and that:*

$$R : G \to \mathrm{Aut}(V)$$

is a finite-dimensional, faithful complex representation. Then the conductor of M_0/L divides the Artin conductor of R.

Proof. Let:

$$G \geq G_0 \geq G_1 \geq \ldots \geq G_i \geq \ldots$$

be the chain of ramification groups in G and let g_i denote the order of G_i. Define the numbers t, s_j and d_j such that:

$$\begin{array}{lll} \text{codim } V^{G_i} = d_0 \ , & i = 0, \ldots, s_1 & , \\ \vdots & & \\ \text{codim } V^{G_i} = d_t \ , & i = s_t + 1, \ldots, s_{t+1} & , \\ \text{codim } V^{G_i} = d_{t+1} = 0 \ , & i \geq s_{t+1} + 1 & , \end{array}$$

where $d_0 > d_1 > \ldots > d_t > d_{t+1} = 0$, and where V^{G_i} means the space of fixed points of G_i in V. Letting $\varphi_{M/L}$ denote the Herbrand function of M/L, the Artin conductor of R is by definition $\wp_K^{a(R)}$ where we have with $s_0 = -1$:

$$\begin{aligned} a(R) &= \sum_{j=0}^{t} \sum_{i=s_j+1}^{s_{j+1}} d_j \cdot \frac{g_i}{g_0} \\ &= d_0 \sum_{i=0}^{s_1} \frac{g_i}{g_0} + \sum_{j=1}^{t} d_j \cdot \left(\sum_{i=0}^{s_{j+1}} \frac{g_i}{g_0} - \sum_{i=0}^{s_j} \frac{g_i}{g_0} \right) \\ &= d_0 + d_0 \varphi_{M/L}(s_1) + \sum_{j=1}^{t} d_j \left(\varphi_{M/L}(s_{j+1}) - \varphi_{M/L}(s_j) \right) \\ &= d_0 + \sum_{j=1}^{t+1} (d_{j-1} - d_j) \varphi_{M/L}(s_j) \ . \end{aligned}$$

Let c be the largest integer with $(G/N)_c \neq 1$. Then the conductor of M_0/L is $\wp_L^{\gamma}$ with:

$$\gamma = 1 + \varphi_{M_0/L}(c).$$

If $\delta \in \mathbb{R}$ with $\delta > s_{t+1}$ then:

$$V^{G_\delta} = V \ ,$$

and so $G_\delta = 1$, since R is faithful. Thus:

$$1 = (G_\delta N)/N = (G/N)_{\varphi_{M/M_0}(\delta)} \ ,$$

and so $c < \varphi_{M/M_0}(\delta)$; hence $c \leq \varphi_{M/M_0}(s_{t+1})$. Then:

$$\varphi_{M_0/L}(c) \leq \varphi_{M_0/L} \left(\varphi_{M/M_0}(s_{t+1}) \right) = \varphi_{M/L}(s_{t+1}),$$

i.e.:

$$\gamma \leq 1 + \varphi_{M/L}(s_{t+1}) \leq d_0 + d_t \varphi_{M/L}(s_{t+1}) \leq a(R).$$

□

5.2. Let us now consider representations ρ of A_5-type with $N = 2^\alpha p$, where $\alpha = 0, 2$ or 5, p is an odd prime number, and $\varepsilon = \chi_{-p}$.

First, since p is odd the group G_p must be dihedral or cyclic. However, if G_p were dihedral, then $\bar{\rho}$ would not have a lifting for which the p-part of its conductor were p; this is an immediate consequence of theorem 1 of section 3. Hence G_p is cyclic, and since ε is quadratic, G_p is cyclic of order 2. As p is odd, we then find that the p-part of the discriminant of a 'root field' of K, i.e. a subfield of K of degree 5 over $\mathbb{Q}$, is p^2.

If $\alpha = 0$, we should then look for A_5-fields K for which the discriminant of as root field is p^2. Note that we must have $p \equiv 3 \ (4)$. Table 1, which will be discussed in II, reveals that for $p \leq 2083$ there is exactly 1 such field K, namely the splitting field of the polynomial:

$$x^5 + 8x^3 + 7x^2 + 172x + 53 \ ;$$

here, $p = 2083$. The splitting field of this polynomial over $\mathbb{Q}_{2083}$ is:

$$\mathbb{Q}_{2083}(\sqrt{-2083}).$$

Using the theorem of Tate mentioned in section 2, we find that each of the 2 projective representations (corresponding to the 2 different embeddings $A_5 \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$) associated with this field has a lifting with conductor 2083 and determinant character χ_{-2083}. Any such lifting may be twisted, without changing conductor or determinant, with a quadratic character with conductor dividing 2083, i.e. with 1 or χ_{-2083}. We conclude then that there are exactly 4 (inequivalent) representations ρ of A_5-type with $N = 2083$ and $\varepsilon = \chi_{-2083}$. (The analysis of representations with prime conductor is by the way well-known, cf. [13]).

Let us then proceed with the case $\alpha = 2$ and $p \equiv 3 \ (4)$. A priori the group G_2 is cyclic of order 2, dihedral of order 4 or 6, or isomorphic to A_4. Since $\varepsilon = \chi_{-p}$ has conductor p, the cyclic case is excluded. Since $\alpha = 2$, one finds that the dihedral group of order 4 and A_4 are also excluded. So, G_2 must be dihedral of order 6, i.e. it corresponds to the tamely ramified extension of order 3 of the unramified quadratic extension of $\mathbb{Q}_2$. This gives the contribution 2^2 to the discriminant of a root field of K. Accordingly, we must in this case look for A_5-fields K for which the discriminant of a root field is $2^2 \cdot p^2$, where p is a prime number $\equiv 3 \ (4)$.Table 1 shows that for $p \leq 1041$ there are exactly 4 such fields, namely: for $p = 487, 751, 887, 919$ the splitting field of the polynomial:

$$\begin{aligned} &x^5 - 7x^3 - 17x^2 + 18x + 73 \ , \\ &x^5 - 8x^3 + 10x^2 + 160x + 128, \\ &x^5 + 10x^3 + 10x^2 + 44x + 56 \ , \\ &x^5 - 8x^3 + 28x^2 - 40x + 48 \ , \end{aligned}$$

respectively. In each case one finds that the splitting field of the polynomial over $\mathbb{Q}_2$ is indeed the tamely ramified extension of degree 3 of $\mathbb{Q}_2(\sqrt{5})$. Over $\mathbb{Q}_p$ the splitting field is $\mathbb{Q}_p(\sqrt{p})$ in the cases $p = 751, 887$ or 919, and it is $\mathbb{Q}_p(\sqrt{-p})$ for $p = 487$. Using the theorem of Tate and theorem 1 above, we find in each case that any of the 2 projective representations associated with K lifts to a representation with $N = 4p$ and $\varepsilon = \chi_{-p}$, and that any such lifting can be twisted, without changing conductor or determinant, with a quadratic character with conductor dividing p.

We conclude that for $p = 487, 751, 887$ or 919 there are exactly 4 representations of A_5-type with $N = 4p$ and $\varepsilon = \chi_{-p}$.

We then turn to the case $\alpha = 5$, $\varepsilon = \chi_{-p}$. Again, the group G_2 is either cyclic or order 2, dihedral of order 4 or 6, or isomorphic to A_4, but here none of these possibilities can be a priori excluded. We only find, using theorem 1 and the condition $\alpha = 5$, some restrictions if G_2 has order 4. Working through the various cases, one finds that the 2-part of the discriminant of a root field of K is in any case bounded by 2^6. Consequently, we want to look for A_5-fields for which the discriminant of a root field is $2^\beta \cdot p^2$, where p is a prime number and $\beta \leq 6$. Table 1 shows that for $p = 73$ or $p = 193$ there is exactly 1 such field, namely:

$$\text{for } p = 73 \text{ the splitting field of:} \quad x^5 + 2x^3 - 4x^2 - 2x + 4 \ ,$$

$$\text{for } p = 193 \text{ the splitting field of:} \quad x^5 + 10x^3 - 26x^2 + 11x + 30 \ .$$

In both cases, $\beta = 6$, and the splitting field over $\mathbb{Q}_2$ is the unique A_4-extension of $\mathbb{Q}_2$; over $\mathbb{Q}_p$ the splitting field is $\mathbb{Q}_p(\sqrt{-p})$. Using theorem 2 of section 4, we find in both cases ($p = 73$ or $p = 193$) that any of the 2 projective representations associated with the splitting field of the polynomial has a lifting with conductor $2^5 \cdot p$ whose determinant character is quadratic with conductor $2^2 \cdot p$; this determinant character is thus χ_{-p}. It follows furthermore from theorem 2 that any such lifting can be twisted, without changing the conductor or determinant, with a quadratic character with conductor dividing $2^2 \cdot p$. There are 4 such characters, namely $1, \chi_{-1}, \chi_p$ and χ_{-p}, and so we conclude that there are for $p = 73$ and for $p = 193$ precisely 8 representations ρ of A_5-type with $N = 2^5 \cdot p$ and $\varepsilon = \chi_{-p}$.

5.3. We shall now find the representations of A_4- or S_4-type where (N, ε) is one of the possibilities mentioned in 5.1. The A_4-case may be dealt with quickly, since it is impossible for a simple reason: Suppose that ρ is an A_4-type representation. The projective kernel field K then contains a cyclic Galois extension $L/\mathbb{Q}$ of degree 3. There exists an odd prime number l which ramifies in L. The group G_l is not isomorphic to A_4 since l is odd, and as a subgroup of A_4 it must then be cyclic of order 3. It follows that the determinant character of ρ has order divisible by 3. Since $\varepsilon^2 = 1$ in any of our cases, the A_4-case will not occur.

Let us then turn to representations of S_4-type. If ρ is a representation of S_4-type, then the projective kernel field K contains a unique Galois extension $L/\mathbb{Q}$ with Galois group isomorphic to S_3. Let $M/\mathbb{Q}$ denote the quadratic extension in L. Since we require ρ to have conductor of the form $2^\alpha p$ (where p is one of the prime numbers $73, 193, 487, 751, 887, 919, 2083$), we see that $L/\mathbb{Q}$, and thus $M/\mathbb{Q}$ is unramified outside $\{2, p\}$; for $p = 2083$, we have that $L/\mathbb{Q}$ is unramified outside $\{p\}$, since we require ρ to have conductor p in this case. In the other cases, 2 is either ramified or decomposed in $M/\mathbb{Q}$ which means that L/M must be unramified over 2. Since we require the determinant character of ρ to be χ_{-p}, we find as in the preceding subsection that L/M is also unramified over p. Hence L/M is an unramified Galois extension of degree 3 and so the class number of M must be divisible by 3. The class numbers h of the quadratic fields $\mathbb{Q}(\sqrt{a})$ which a priori (recall the lemma of section 5.1) are candidates for M are given by the following table:

a	h	a	h	a	h	a	h
-1	1	-919	19	751	1	$-2 \cdot 73$	16
-2	1	-2083	7	887	1	$2 \cdot 73$	2
-73	4	2	1	919	1	$-2 \cdot 193$	20
-193	4	73	1	2083	1	$2 \cdot 193$	2
-487	7	193	1				
-751	15	487	1				
-887	29						

So, we only have to consider the case:

$$M = \mathbb{Q}(\sqrt{-751}),$$

and here there does in fact exist a unique S_3-extension of $\mathbb{Q}$ containing M, namely the splitting field L of the polynomial:

$$x^3 - 11x - 15 \ .$$

Now we have to ask whether L can be embedded in an S_4-extension of $\mathbb{Q}$ unramified outside $\{2, 751\}$. This is in fact possible as follows from the table in [6]: The splitting field of the polynomial:

$$x^4 + 6x^3 + 13x^2 + 11x + 1$$

is an S_4-extension $K/\mathbb{Q}$ ramified only over 751; the discriminant of a quartic subfield of K is -751, and K is unique with these properties. As is well-known (cf. [13]) or easily seen, this means that there are exactly 2 representations ρ with $N = 751$ and $\varepsilon = \chi_{-751}$. Now, using the method of [2] one may verify that this field K is in fact the only possibility even if we allow K/L to be ramified over 2: We consider the elliptic curve:

$$E : y^2 = x^3 - 11x - 15$$

over $\mathbb{Q}$. Its conductor is $N_E = 2 \cdot 751$ and its discriminant is $\Delta_E = -2^4 \cdot 751$. Now, from [2] we know that S_4-extensions $K/\mathbb{Q}$ containing the above S_3-extension $L/\mathbb{Q}$ are given by elements:

$$\varphi \in \mathrm{H}^1\left(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}})_2\right) \setminus \{0\} \ .$$

One may further show, cf. [5], that if we want to produce representations ρ with conductor of the form $2^\alpha \cdot 751$, then it suffices to consider non-trivial elements φ in the Selmer group $S_{\{2\}}(E, \mathbb{Q})_2$. This group can be determined by an algorithm of Birch and Swinnerton-Dyer, and one finds that it has order 2, generated by $\delta(P)$, where $P = \left(\frac{17}{4}, \frac{31}{8}\right)$ is a rational point on E, and δ is the natural injection:

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{H}^1\left(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}})_2\right) \ .$$

The corresponding S_4-extension of $\mathbb{Q}$ is then obtained by adjoining to $\mathbb{Q}$ the x-coordinates of points $Q \in E(\overline{\mathbb{Q}})$ with $2Q = P$. One finds then that this S_4-extension is the splitting field of the polynomial:

$$x^4 - 17x^3 + 22x^2 + 307x + 376 \ ,$$

which of course is the same field as is obtained from the table in [6].

5.4. Finally, we shall briefly discuss representations ρ of dihedral type in the cases listed in 5.1. These are most easily obtained by global means, and let us recall how (cf. [13]): Any representation ρ of dihedral type has the form:

$$\rho = \mathrm{Ind}(\psi),$$

where ψ is a character on $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$, where $M/\mathbb{Q}$ is some quadratic extension, with $\sigma \cdot \psi \neq \psi$ for a (any) element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which does not belong to $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$, and where Ind means induction from $\mathrm{Gal}(\overline{\mathbb{Q}}/M)$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If ψ is viewed as a character on the idele classes of M, then the determinant character of ρ, viewed as a character on the idele classes of $\mathbb{Q}$, is:

$$\det(\rho) = \omega \cdot (\psi \mid C_{\mathbb{Q}}),$$

where ω is the quadratic character of $M/\mathbb{Q}$ and $\psi \mid C_{\mathbb{Q}}$ means restriction of ψ to the idele classes of $\mathbb{Q}$. The Artin conductor of ρ is:

$$|D(M/\mathbb{Q})| \cdot N_{M/\mathbb{Q}}\left(c_M(\psi)\right),$$

where $D(M/\mathbb{Q})$ is the discriminant of $M/\mathbb{Q}$ and $c_M(\psi)$ is the (class field theoretic) conductor of ψ. If $\rho_i = \mathrm{Ind}(\psi_i)$, $i = 1, 2$, are 2 such representations where ψ_i are characters on the idele classes of the *same* quadratic field $M/\mathbb{Q}$, then ρ_1 and ρ_2 are equivalent if and only if:

$$\text{either} \quad \psi_1 = \psi_2 \quad \text{or} \quad \psi_1 = \sigma \cdot \psi_2 \quad (\sigma \text{ as above}).$$

The case of dihedral type representations with prime conductor p is well-known, cf. [13], and we shall not reproduce the simple arguments, but merely state the facts:

We must have $p \equiv 3\ (4)$ and with the above notation it suffices to consider the field $M = \mathbb{Q}(\sqrt{-p})$. The non-trivial automorphism σ of this extension $M/\mathbb{Q}$, considered as acting on characters of the class group of M, fixes only the trivial character. The class number h of M is thus odd, and we obtain precisely $\frac{1}{2}(h-1)$ inequivalent representations of dihedral type with conductor p. The determinant character of any of these representations is χ_{-p}. Consequently, we have for $p = 487, 751, 887, 919, 2083$ exactly $3, 7, 14, 9, 3$ representations of dihedral type with conductor p and determinant character χ_{-p}, respectively.

Let us then consider representations of dihedral type with conductor $4p$ and determinant χ_{-p}, where p is an odd prime number $\equiv 3\ (4)$. A priori, we have 2 possibilities for the field M: $M = \mathbb{Q}(\sqrt{p})$ or $M = \mathbb{Q}(\sqrt{-p})$. However, if $M = \mathbb{Q}(\sqrt{p})$, then the character ψ would have to be unramified with an *odd* restriction to the idele classes of $\mathbb{Q}$, which is easily seen to be impossible (for example by computing the appropriate ray class number). If $M = \mathbb{Q}(\sqrt{-p})$ with $p \equiv 7\ (8)$, then 2 decomposes:

$$(2) = \wp_1\wp_2 \quad \text{in} \quad M\ ;$$

since the ray class numbers of M corresponding to the cycles (2), $\wp_1^2$ and $\wp_2^2$ all coincide with the class number of M, this case is excluded. (By the way, if $p \equiv 3\ (8)$, 2 is inert in M, and one finds that the ray class number corresponding to the cycle (2) is 3 times the class number h of M, and that we have exactly h

representations of dihedral type with conductor $4p$ and determinant χ_{-p}). Hence, if $p = 487, 751, 887$, or 919, there are no representations of dihedral type with conductor $4p$ and determinant χ_{-p} (and there are precisely 7 such representations if $p = 2087$).

Suppose now that p is a prime number $\equiv 1 \pmod 8$, and let us ask for dihedral-type representations with $N = 2^5 \cdot p$ and $\varepsilon = \chi_{-p}$. Keeping the above notation, the field M must be one of the following:

$$\mathbb{Q}(\sqrt{\pm 2}),\ \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{\pm 2 \cdot p}),\ \mathbb{Q}(\sqrt{\pm p}).$$

If M is one of the fields $\mathbb{Q}(\sqrt{\pm 2})$,$\mathbb{Q}(\sqrt{\pm 2 \cdot p})$, then 2 ramifies:

$$(2) = \wp^2 \quad \text{in} \quad M,$$

and the p-part of the conductor of the character ψ should be $\wp^2$. But then the conductor of $\psi \mid C_{\mathbb{Q}}$ would certainly not be divisible by 2^3, which would be required by these cases. If $M = \mathbb{Q}(\sqrt{-p})$, then 2 is again ramified in M: $(2) = \wp^2$, but now the character ψ should have conductor $\wp^3$ and trivial restriction to $C_{\mathbb{Q}}$; this is easily seen to be impossible (consider the restriction of ψ to $M_{\wp}^{\times}$). Similarly, the case $M = \mathbb{Q}(\sqrt{-1})$ is excluded. If then finally $M = \mathbb{Q}(\sqrt{p})$, then 2 decomposes in M:

$$(2) = \wp_1 \wp_2,$$

and $\psi \mid C_{\mathbb{Q}}$ should be χ_{-p}. The norm of the conductor of ψ should be 2^5 and so there are various possibilities for the conductor of ψ. Suppose for example that ψ has conductor $\wp_1^3 \wp_2^2$ and consider the restrictions:

$$\psi_i = \psi \mid M_{\wp_i}^{\times}\ , \quad i = 1, 2\ .$$

Note that $M_{\wp_i} = \mathbb{Q}_2$. Then ψ_1 cannot be trivial on all elements of the type $1 + b \cdot 2^2 + \ldots$; for otherwise there would be an element:

$$u = 1 + 2 + b \cdot 2^2 + \ldots$$

with $\psi_1(u) = -1$. Since ψ_2 has conductor $\wp_2^2$ we would also have $\psi_2(u) = -1$. We then see that the restriction $\psi \mid C_{\mathbb{Q}}$ would be trivial on $\mathbb{Q}_2^{\times}$ which is impossible. So, there is an element $y = 1 + b \cdot 2^2 + \ldots$ with $\psi_1(y) \neq 1$. Since ψ_2 has conductor $\wp_2^2$ we conclude that $\psi \mid C_{\mathbb{Q}}$ has conductor divisible by 2^3, which is impossible. The other possibilities for the conductor of ψ are similarly excluded.

We conclude that if p is a prime number $\equiv 1 \pmod 8$, then there are no dihedral type representations with conductor $2^5 \cdot p$ and determinant character χ_{-p}. This holds then in particular for $p = 73$ and for $p = 193$.

Let us then finally, for use in VI, note the following fact: If $p = 73$ or $p = 193$, then there is at least 1 dihedral-type representation with conductor $2^2 \cdot p$ and determinant character χ_{-p}. This follows, as one may easily verify in both of these cases, because the ideal class group of $\mathbb{Q}(\sqrt{-p})$ is cyclic of order 4 and contains an ideal class which is not invariant under the action of the non-trivial automorphism of $\mathbb{Q}(\sqrt{-p})/\mathbb{Q}$.

References

[1] Atkin, J. Lehner: 'Hecke operators on $\Gamma_0(m)$.' Math. Ann. **185** (1970), 134–160.
[2] P. Bayer, G. Frey: 'Galois representations of octahedral type and 2-coverings of elliptic curves.' Math. Z. **207** (1991), 395–408.
[3] J. P. Buhler: 'Icosahedral Galois Representations.' Lecture Notes in Mathematics **654**, Springer-Verlag 1978.
[4] P. Deligne, J.-P. Serre: 'Formes modulaires de poids 1.' Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530.
[5] G. Frey: 'Construction and arithmetic applications of modular forms of low weight.' CRM Proc. Lecture Notes **4** (1994), 1–21.
[6] H.J. Godwin: 'On quartic fields of signature one with small discriminant.' Quart. J. Math. Oxford Ser. (2) **8** (1957), 214–222.
[7] H. Hasse: 'Number Theory.' Grundlehren der mathematischen Wissenschaften **229**, Springer-Verlag, 1980.
[8] R.P. Langlands: 'Base change for $GL(2)$.' Annals of Mathematics Studies **96**, Princeton University Press, 1980.
[9] W. Li: 'On converse theorems for $GL(2)$ and $GL(1)$.' Amer. J. Math. 103 (1981), 851–885.
[10] T. Miyake: 'Modular Forms.' Springer Verlag, 1989.
[11] H. Petersson: 'Modulfunktionen und quadratische Formen.' Ergebnisse der Mathematik und ihrer Grenzgebiete **100**, Springer Verlag, 1982.
[12] J.-P. Serre: 'Local Fields.' Graduate Texts in Mathematics **67**, Springer Verlag, 1979.
[13] J.-P. Serre: 'Modular forms of weight one and Galois representations.' In: A. Fröhlich: Algebraic Number Fields. Academic Press 1977.
[14] G. Shimura: 'Introduction to the arithmetic theory of automorphic functions.' Princeton University Press, 1971.
[15] Tunnell: 'Artin's conjecture for representations of octahedral type.' Bull. Amer. Math. Soc. (N.S.) **5** (1981), 173–175.
[16] A. Weil: 'Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen.' Math. Ann. **168** (1967), 149–156.
[17] A. Weil: 'Exercises dyadiques.' Invent. Math. **27** (1974), 1–22.
[18] E.-W. Zink: 'Ergänzungen zu Weils Exercises dyadiques.' Math. Nachr. 92 (1979), 163–183.

kiming@math.ku.dk

Dept. of math., Univ. of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark.