

# GALOIS REPRESENTATIONS OF DIHEDRAL TYPE OVER $\mathbb{Q}_p$ .

PEDER FREDERIKSEN, IAN KIMING

ABSTRACT. We give a complete classification of 2-dimensional complex Galois representations of dihedral type over a local field  $\mathbb{Q}_p$ , including their conductors and determinants on inertia. This explicit classification complements earlier works [2], [5] on these types of representations.

## 1. INTRODUCTION.

**1.1. Notation.** Throughout the paper the following notation will be used:  $p$  denotes a prime number. Except in section 1.2,  $k$  is a finite extension of  $\mathbb{Q}_p$ . Additionally:

$G_k$	:	the absolute Galois group of $k$
$c(\rho)$	:	for a continuous complex representation $\rho$ of $G_k$ , the valuation of the Artin conductor of $\rho$
$U_k$	:	for a finite extension $k/\mathbb{Q}_p$ the group of units of $k$
$U_k^{(s)}$	:	for a finite extension $k/\mathbb{Q}_p$ the group of units of $k$ of level $\geq s$
$K = \mathbb{Q}_p(\sqrt{d})$	:	a quadratic extension of $\mathbb{Q}_p$
$\sigma$	:	the non-trivial automorphism of $K/\mathbb{Q}_p$
$\chi$	:	a complex character of $K^\times$ vanishing on $\mathbb{Q}_p^\times$
$(\cdot, \cdot)$	:	the local symbol in $\mathbb{Q}_p$

We allow ourselves the implicit use of local class field theory. Thus for instance, a character  $\chi$  as above may also be viewed as a character on  $G_K$ .

**1.2. Lifting projective Galois representations.** Suppose that  $k$  is an algebraic number field with absolute Galois group  $G_k$ . In studying 2-dimensional (irreducible) continuous complex representations of  $G_k$  the following question is of interest, cf. [2], [7], [5]: Given a continuous *projective* representation

$$\rho_0 : G_k \longrightarrow \mathrm{PGL}_2(\mathbb{C}),$$

find for all lifts  $\rho : G_k \rightarrow \mathrm{GL}_2(\mathbb{C})$  the determinant  $\det \rho$  and the Artin conductor of  $\rho$ . Now, as any lift has the shape  $\rho \otimes \phi$  with  $\rho$  any fixed lift and  $\phi$  a character of  $G_k$ , and as  $\det(\rho \otimes \phi) = \det \rho \cdot \phi^2$ , one might hope to accomplish this by finding one particular lift  $\rho$  for which the following data can be determined:

- (1) The determinant  $\det \rho$ , and
- (2) For any character  $\phi$  of  $G_k$ , the Artin conductor of  $\rho \otimes \phi$  can be determined solely from the knowledge of the Artin conductor of  $\phi$ .

We might then informally refer to such a lift  $\rho$  as a ‘good lift’ of  $\rho_0$ . It is not at all clear whether good lifts exist generally, but at least in case  $k$  has class number 1 –

and thus in particular if  $k = \mathbb{Q}$  – one knows, cf. again [2], [7], [5], that the problem of finding a good lift can be reduced to the following local problem: Consider the completion  $k_{\mathfrak{p}}$  of  $k$  at a (finite) prime  $\mathfrak{p}$ . Given a projective representation

$$\rho_{0,\mathfrak{p}} : G_{k_{\mathfrak{p}}} \longrightarrow \mathrm{PGL}_2(\mathbb{C})$$

find for *some* lift  $\rho_{\mathfrak{p}}$  the following:

- (1) The restriction of the determinant  $\det \rho_{\mathfrak{p}}$  to the inertia of  $G_{k_{\mathfrak{p}}}$ , i.e. the restriction  $\det \rho_{\mathfrak{p}}|_{U_{k_{\mathfrak{p}}}}$  when viewing  $\det \rho$  as a character on  $k_{\mathfrak{p}}^{\times}$ , and
- (2) For any character  $\phi_{\mathfrak{p}}$  of  $G_{k_{\mathfrak{p}}}$ , an algorithm computing the Artin conductor of  $\rho_{\mathfrak{p}} \otimes \phi_{\mathfrak{p}}$  solely from the Artin conductor of  $\phi_{\mathfrak{p}}$ .

We might then also refer to such a lift  $\rho_{\mathfrak{p}}$  as a ‘good lift’ of  $\rho_{0,\mathfrak{p}}$ .

Building upon and completing previous investigations [9], [2], [10] of this local problem, in [5] we constructed good lifts under conditions of some generality, and in particular in all cases where  $k_{\mathfrak{p}}$  is a  $p$ -adic field  $\mathbb{Q}_p$ . Perhaps somewhat surprisingly the case of *dihedral* type projective representations, i.e. projective representations whose (finite) image is isomorphic to a dihedral group, turns out to be especially complicated to analyze. Let us then briefly recall the precise shape of the problem in the (local) dihedral case.

**1.3. Galois representations of dihedral type.** For convenience, let us now shift notation so that  $k$  is now a finite extension of some  $\mathbb{Q}_p$ . Suppose that

$$\rho_0 : G_k \longrightarrow \mathrm{PGL}_2(\mathbb{C})$$

is a continuous representation of dihedral type. If  $L/k$  is the extension cut out by  $\rho$  then  $L$  contains a quadratic subextension  $K/k$  such that  $L/K$  is cyclic ( $K$  is unique if  $[L : k] > 4$ ). By the structure theory for ramification groups in  $G_k$  we see that  $L/K$  is necessarily ramified unless possibly when  $[L : k] = 4$ ; in the latter case however, there are 3 possible choices of  $K$  and we can choose  $K$  so that  $L/K$  is ramified. We now recall the following facts for which the reader is referred to [7] (or the introduction of [5]):

We have

$$(\rho_0)|_{G_K} \sim \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix},$$

with  $\chi$  a ramified character of  $K^{\times}$  vanishing on  $k^{\times}$ . Conversely, if  $\chi$  is such a character there exists a projective representation  $\rho_0$  behaving in this way. Any lift  $\rho$  of  $\rho_0$  has shape:

$$\rho = \mathrm{Ind}_K^k(\psi)$$

where  $\mathrm{Ind}_K^k$  means induction from  $G_K$  to  $G_k$ , and where  $\psi$  is a character of  $K^{\times}$  (viewed as a character of  $G_K$ ) such that

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

where  $\sigma$  denotes the non-trivial automorphism of  $K/k$ . For such a lift  $\rho$  one has

$$\det \rho = \omega \cdot (\psi|_{k^{\times}})$$

with  $\omega$  the quadratic character of  $k^{\times}$  corresponding to  $K/k$  by local class field theory, and the Artin conductor of  $\rho \otimes \phi$  for a character  $\phi$  of  $k^{\times}$  viewed as a character of  $G_k$  is:

$$D(K/k) \cdot N_{K/k}(\mathfrak{P}^{c(\psi \cdot (\phi \circ N_{K/k}))})$$

with  $D(K/k)$  the discriminant,  $N_{K/k}$  the norm map,  $\mathfrak{P}$  the prime ideal of  $K$ , and  $c(\psi \cdot (\phi \circ N_{K/k}))$  the exponent of the conductor of  $\psi \cdot (\phi \circ N_{K/k})$  as a character of  $K^\times$ .

Accordingly, the local problem mentioned in the previous subsection amount in the dihedral case to the following: Given a (ramified) character  $\chi$  of  $K^\times$  vanishing on  $k^\times$ , find a character  $\psi$  of  $K^\times$  such that

- (1)  $\psi\left(\frac{\sigma x}{x}\right) = \chi(x)$ , for  $x \in K^\times$ ,
- (2) The restriction  $\psi|_{U_k}$  is known, and
- (3) For any character  $\phi$  of  $k^\times$  the number  $c(\psi \cdot (\phi \circ N_{K/k}))$  can be computed solely from the knowledge of the conductor of  $\phi$ .

As we mentioned above a solution to this problem was given in some generality in [5]. However, the solution given there was in terms of various data attached to  $\chi$ . One may wish for an additional level of explicitness for particular ground fields  $k$ , more precisely for a classification of the possible  $\chi$ 's, the determination of the needed data attached to them, and the explication of the solution of [5] for each possible  $\chi$ . For applications (to global Galois representations over  $\mathbb{Q}$ ), this is particularly desirable in the cases where  $k$  is a field  $\mathbb{Q}_p$ , and is precisely what we carry out in the next section. This first involves a detailed analysis of units in quadratic extensions of a field  $\mathbb{Q}_p$  where we can base ourselves on [3]. The result is Proposition 1 below classifying the possible  $\chi$ 's as above together with certain crucial data. Secondly, we have to apply the results of [5] for each of these  $\chi$  in order to produce explicit good lifts in each case. The results are found in Theorem 1.

Finally, and again because of applications to global Galois representations over  $\mathbb{Q}$ , one can also ask for a reformulation of these results in such a way that they can be readily applied to a practical situation where one really only starts with a concrete polynomial whose splitting field is the field cut out by the projective representation  $\rho_0$ . One would then like to know how to apply the results of the next section when given essentially only this polynomial. In principle, this problem can be solved through use of explicit local reciprocity maps. In the final section we shall however show – for the special cases of  $\rho_0$ 's of type  $V_4$  or  $D_4$  – that one can give an answer on the basis of the results of the next section and certain ad hoc arguments from the theory of embedding problems. We have focused on the  $V_4$  and  $D_4$  cases because these are the most difficult among these cases one would encounter studying Galois representations over  $\mathbb{Q}$  of one the complicated types  $A_4$ ,  $A_5$ , and  $S_4$  (in fact, all other cases can be handled immediately using only the results of the next section, but we we will not show this in detail).

## 2. GOOD LIFTS.

**Proposition 1.** *Consider a quadratic extension  $K = \mathbb{Q}_p(\sqrt{d})$  of  $\mathbb{Q}_p$ .*

- (1) *The structure of the abelian group  $K^\times/\mathbb{Q}_p^\times$  is  $\cong A_0 \times A_1 \times A_2$  where the isomorphism class of the  $A_i$  as well as (topological) generators  $a_i$  for the  $A_i$  are given by the following table.*

$p$	$d$	$A_0 \cong$	$A_1 \cong$	$A_2 \cong$	$a_0$	$a_1$	$a_2$
2	-3	$\mathbb{Z}/\mathbb{Z}3$	$\mathbb{Z}/\mathbb{Z}2$	$\mathbb{Z}_2$	$\epsilon$	$\sqrt{d}$	$-1 + 2\sqrt{d}$
2	3	1	$\mathbb{Z}/\mathbb{Z}2$	$\mathbb{Z}_2$	1	$\sqrt{d}$	$1 - \sqrt{d}$
2	-1	1	$\mathbb{Z}/\mathbb{Z}4$	$\mathbb{Z}_2$	1	$1 - \sqrt{d}$	$-1 + 2\sqrt{d}$
2	$\equiv 2 \pmod{4}$	1	$\mathbb{Z}/\mathbb{Z}2$	$\mathbb{Z}_2$	1	$\sqrt{d}$	$1 + \sqrt{d}$
$\neq 2$	$p \nmid d$	1	$\mathbb{Z}/\mathbb{Z}(p+1)$	$\mathbb{Z}_p$	1	$\zeta$	$1 + p\sqrt{d}$
$\neq 2, 3$	$p \mid d$	$\mathbb{Z}/\mathbb{Z}2$	1	$\mathbb{Z}_p$	$\sqrt{d}$	1	$1 + \sqrt{d}$
3	3	$\mathbb{Z}/\mathbb{Z}2$	1	$\mathbb{Z}_3$	$\sqrt{d}$	1	$1 + \sqrt{d}$
3	-3	$\mathbb{Z}/\mathbb{Z}2$	$\mathbb{Z}/\mathbb{Z}3$	$\mathbb{Z}_3$	$\sqrt{d}$	$\epsilon$	$1 + 3\sqrt{d}$

where  $\epsilon$  and  $\zeta$  denote a primitive root of unity of order 3 and  $(p^2 - 1)$ , respectively.

(2) Suppose that  $\chi$  is a character of  $K^\times/\mathbb{Q}_p^\times$ , and write  $\chi = \chi'\chi''$  where  $\chi'$  has order prime to  $p$ , whereas the order of  $\chi''$  is a power of  $p$ . Then,

$$c(\chi) = \max\{c(\chi'), c(\chi'')\},$$

and  $c(\chi') = 1$ , except if  $p \neq 2$ ,  $p \mid d$ , and  $\chi'$  is a character of  $A_0$  extended to  $K^\times/\mathbb{Q}_p^\times$ , in which case  $c(\chi') = 0$ .

If  $\chi$  has  $p$ -power order we may write  $\chi = \chi_1\chi_2$  with  $\chi_i$  a character of  $p$ -power order on  $A_i$  extended to  $K^\times/\mathbb{Q}_p^\times$ . Let the order of  $\chi_i$  be  $p^{s_i}$ ,  $i = 1, 2$ . Then  $c(\chi)$  is given by the following table.

$p$	$d$	$c(\chi)$
2	-3	$2s_1$ , for $s_2 = 0$ $s_2 + 2$ , for $s_2 \geq 1$
2	3	0, for $s_1 = 0, s_2 \leq 1$ 2, for $s_1 = 1, s_2 = 2$ 4, for $(s_1 = 1, s_2 \leq 1)$ or $(s_1 = 0, s_2 = 2)$ $2s_2$ , for $s_2 \geq 3$
2	-1	0, for $s_1 \leq 1, s_2 = 0$ 2, for $s_1 = 2, s_2 = 0$ $2s_2 + 2$ , for $s_2 \geq 1$
2	$\equiv 2 \pmod{4}$	$2s_2$
$\neq 2$	$p \nmid d$	0, for $s_2 = 0$ $s_2 + 1$ , for $s_2 \geq 1$
$\neq 2, 3$	$p \mid d$	$2s_2$
3	3	$2s_2$
3	-3	$2s_1$ , for $s_2 = 0$ $2s_2 + 2$ , for $s_2 \geq 1$

*Proof.* The proof is based on results of Halter-Koch who in [3] gave an explicit set of (topological) generators of the 1-unit group of a quadratic extension  $K = \mathbb{Q}_p(\sqrt{d})$  of  $\mathbb{Q}_p$ , including their orders mod  $\mathfrak{p}^s$  for any  $s$  ( $\mathfrak{p}$  the maximal ideal of the ring of integers in  $K$ ). We have to complement this by discussing the full group  $K^\times$ , and in particular the shape of elements of  $\mathbb{Q}_p^\times$  when written in terms of the chosen generators. We shall give details of this discussion only in the cases  $p = 2$  and  $d = 3$ . The discussion in each of the other cases is similar but simpler.

So, suppose that  $p = 2$  and  $d = 3$ . As prime element of  $K$  we choose  $\pi := 1 - \sqrt{d}$ . According to [3], as a basis for  $U_K^{(1)}$  as a  $\mathbb{Z}_2$ -module, one may choose:

$$-1, \quad \eta_{11} := \sqrt{d}, \quad \eta_{13} := -1 + 2\sqrt{d},$$

where we have used the notation of [3]. Thus, any element of  $K^\times$  has a unique representation of the form:

$$(*) \quad \pm \pi^n \eta_{11}^u \eta_{13}^v$$

with  $n \in \mathbb{Z}$  and  $u, v \in \mathbb{Z}_2$ .

Let us consider the action of the non-trivial automorphism  $\sigma$  on such representations. First, we have

$$\sigma \eta_{11} = -\eta_{11},$$

and

$$\sigma \eta_{13} = -\eta_{11}^{2a} \eta_{13}^{-1},$$

with a 2-adic integer  $a$ ; the last expression is found by noting that the norm of  $\eta_{13}$ , which is  $-11$ , has a representation of form  $-3^a$  in  $\mathbb{Q}_2$  (and that  $3 = \eta_{11}^2$ ). As the norm of  $\pi$  is  $-2$  we have

$$\sigma \pi = \xi \pi,$$

if  $\xi$  is the unit  $\xi := -2 \cdot \pi^{-2}$  of norm 1. For the expansion of the unit  $\xi$ :

$$\xi = (-1)^\alpha \eta_{11}^{\beta'} \eta_{13}^\beta$$

we necessarily have

$$\beta' = -a\beta, \quad \text{and} \quad \beta \text{ a 2-adic unit};$$

here, the first claim follows from the fact that  $\xi$  has norm 1, whereas the second is verified by actually computing the beginning of the 2-adic expansion of  $\beta \in \mathbb{Z}_2$ .

We can now compute that an element  $(*)$  belongs to  $\mathbb{Q}_2$  if and only if

$$\alpha n + u + v \equiv 0 \pmod{2}, \quad -a\beta n + 2av = 0, \quad \text{and} \quad \beta n - 2v = 0.$$

As  $\beta$  is a unit, the integer  $n$  must then be even and  $v = \beta \cdot n/2$ ; thus, the conditions are equivalent to:

$$n \equiv 0 \pmod{2}, \quad u + v \equiv 0 \pmod{2}, \quad \text{and} \quad v = \beta \cdot n/2.$$

We see that elements of  $\mathbb{Q}_2^\times$  have unique representations of form

$$\pm (\pi^2 \eta_{11} \eta_{13}^\beta)^m \cdot \eta_{11}^{2b}$$

with  $m \in \mathbb{Z}$ ,  $b \in \mathbb{Z}_2$ . That the structure of  $K^\times / \mathbb{Q}_2^\times$  is as stated (with  $a_1 = \eta_{11}$ ,  $a_2 = \pi$ ) now follows readily.

Suppose then that  $\chi$  is a continuous complex character of  $K^\times / \mathbb{Q}_2^\times$ . The first statements of (2) are trivial to check, so we have only to verify the entries of the table in (2).

Assume then that  $\chi$  is of 2-power order and write  $\chi = \chi_1 \chi_2$  as in the last part of the statement of (2).

Now, if we use the information in [3] on the orders of the units  $\eta_{11}$  and  $\eta_{13} \pmod{\mathfrak{p}^s}$ ,  $s \geq 0$ , we deduce:

$$c(\chi) = 0 \Leftrightarrow \chi(\eta_{11}) = \chi(\eta_{13}) = 1,$$

and

$$c(\chi) \leq 2s + 2 \Leftrightarrow \chi(\eta_{13})^{2^s} = 1,$$

for  $s \geq 0$ . We used here that  $\chi$  vanishes on  $\mathbb{Q}_2^\times$ . As

$$\chi(\eta_{13})^{-\beta} = \chi_1(a_1) \cdot \chi_2(a_2)^2$$

with a 2-adic unit  $\beta$ , we deduce (using that  $\chi(a_1)$  is of order  $\leq 2$ )

$$\begin{aligned} c(\chi) = 0 &\Leftrightarrow \chi(a_1) = \chi(a_2)^2 = 1 \Leftrightarrow s_1 = 0, s_2 \leq 1, \\ c(\chi) \leq 2 &\Leftrightarrow \chi(a_1)\chi(a_2)^2 = 1 \Leftrightarrow (s_1 = 0, s_2 \leq 1) \quad \text{or} \quad (s_1 = 1, s_2 = 2), \\ c(\chi) \leq 4 &\Leftrightarrow \chi(a_2)^4 = 1 \Leftrightarrow s_2 \leq 2, \\ c(\chi) \leq 2s &\Leftrightarrow s_2 \leq s, \end{aligned}$$

for  $s \geq 2$ . Noting that  $c(\chi)$  is necessarily an even number in the present case, the formulas for  $c(\chi)$  result immediately.  $\square$

**Theorem 1.** *Suppose that  $\rho_0 : G_{\mathbb{Q}_p} \rightarrow \text{PGL}_2(\mathbb{C})$  is a continuous representation of dihedral type. Let  $K = \mathbb{Q}_p(\sqrt{d})$  be a quadratic extension such that the fixed field of  $\text{Ker} \rho_0$  is ramified and cyclic over  $K$ . Then  $(\rho_0)|_{G_K}$  has shape*

$$(\rho_0)|_{G_K} \sim \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix},$$

with  $\chi$  a ramified character of  $K^\times$  vanishing on  $\mathbb{Q}_p^\times$ .

In each case define  $\chi_i$  as the restriction of  $\chi$  to the  $\langle a_i \rangle$ ,  $i = 1, 2$ , of Proposition 1. Define also  $c := c(\chi)$  according to the recipe of the Proposition.

Suppose that  $\delta$  is any continuous complex character of  $U_{\mathbb{Q}_p}$  satisfying the following requirements:  $\delta$  is trivial on roots of unity of odd order, and in addition:

If  $p = 2$ :

$p$	$d$	$\delta(-1)$	$\delta(5)$
2	-3	$\chi_1(a_1)$	$\chi_2(a_2)$
2	3	$-\chi_1(a_1)$	$\chi_1(a_1)\chi_2(a_2)^2$ , if $c \geq 4$ 1, otherwise
2	-1	$-\chi_1(a_1)^2$	$\chi_2(a_2)$ , if $c \geq 4$ 1, otherwise
2	2, -6	$\chi_1(a_1)$	-1
2	-2, 6	$-\chi_1(a_1)$	-1

If  $p \neq 2$ :  $\delta$  is trivial on the 1-units, and

$p$	$d$	$\delta(-1)$
$\neq 2$	$p \nmid d$	$\chi_1(a_1)^{\frac{p+1}{2}}$
$\neq 2$	$p \mid d$	$(-1)^{\frac{p-1}{2}} \cdot \chi(a_0)$

Then there exists a lift  $\rho : G_{\mathbb{Q}_p} \rightarrow \text{GL}_2(\mathbb{C})$  of  $\rho_0$  with the following properties.

- (1) The restriction  $(\det \rho) | U_{\mathbb{Q}_p}$  is  $\delta$ .
- (2) If  $\phi : G_{\mathbb{Q}_p} \rightarrow \mathbb{C}^\times$  is a character of conductor  $p^\gamma$ , then the valuation of the Artin conductor  $c(\rho \otimes \phi)$  of  $\rho \otimes \phi$  is given as follows:

$p$	$d$	$c(\rho \otimes \phi)$
2	-3	$2 \cdot \max\{c, \gamma\}$
2	-1, 3	$c + 3$ , for $\gamma \leq 2$ $\max\{c + 3, 2\gamma + 2\}$ , for $\gamma \geq 3$
2	$\pm 2, \pm 6$	$c + 5$ , for $\gamma \leq 3$ $\max\{c + 5, 2\gamma + 2\}$ , for $\gamma \geq 4$
$\neq 2$	$p \nmid d$	$2 \cdot \max\{c, \gamma\}$
$\neq 2$	$p \mid d$	$c + 1$ , for $\gamma \leq 1$ $\max\{c + 1, 2\gamma + 2\}$ , for $\gamma \geq 2$

*Proof.* The proof is based on the Theorem 1 of [5]. As recalled in the introduction 1.3, any lift  $\rho$  of  $\rho_0$  has shape  $\text{Ind}_{K/\mathbb{Q}_p}(\psi)$  where  $\psi$  is a character on  $K^\times$  satisfying

$$(\#) \quad \psi\left(\frac{\sigma x}{x}\right) = \chi(x), \quad x \in K^\times.$$

For such a lift  $\rho$  the determinant  $\det \rho$ , when viewed as a character of  $\mathbb{Q}_p^\times$ , is given by:

$$(\#\#) \quad \det \rho = \omega \cdot (\psi|_{\mathbb{Q}_p^\times})$$

with  $\omega$  the character  $\mathbb{Q}_p^\times \rightarrow \{\pm 1\}$  corresponding to the extension  $K/\mathbb{Q}_p$  via class field theory.

Theorem 1 of [5] is an existence statement: What is proved — under conditions more general than the above setting — is the existence of a character  $\psi$  as above (#) with the following special properties: If  $\rho := \text{Ind}_{K/\mathbb{Q}_p}(\psi)$  then the Artin conductor of any twist  $\rho \otimes \phi$  of  $\rho$  by a character  $\phi$  of  $G_{\mathbb{Q}_p}$  can be explicitly given. Also, the restriction of  $\psi$  to the units  $U_{\mathbb{Q}_p}$  of  $\mathbb{Q}_p$  is described so that also  $(\det \rho)|_{U_{\mathbb{Q}_p}}$  can be analyzed via (##). We shall now apply and further explicate these results to the various cases listed in Proposition 1.

So, in the situation under consideration we let  $\psi$  be a character on  $K^\times$  whose existence is assured by Theorem 1 of [5]. Put  $\rho := \text{Ind}_{K/\mathbb{Q}_p}(\psi)$ . If then  $\phi$  is a character on  $G_{\mathbb{Q}_p}$  of conductor  $p^\gamma$ , then the number  $c(\rho \otimes \phi)$  is given as follows: Define the non-negative integer  $t$  to be 0 if  $K/\mathbb{Q}_p$  is unramified, and otherwise let  $t$  be the break in the ramification filtration of  $G := \text{Gal}(K/\mathbb{Q}_p)$ :

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

In the latter case the discriminant of  $K/\mathbb{Q}_p$  is  $p^{t+1}$  as  $K/\mathbb{Q}_p$  is then totally ramified and cyclic of prime order 2 (cf. [8], V, §3). According to Theorem 1 of [5] we have then, denoting by  $N_{K/\mathbb{Q}_p}(\cdot)$  the norm map, that

$$c(\rho \otimes \phi) = 2 \max\{c, \gamma\}, \quad \text{if } K/\mathbb{Q}_p \text{ is unramified}$$

and

$$c(\rho \otimes \phi) = t + 1 + \max\{c + t, c(\phi \circ N_{K/\mathbb{Q}_p})\}, \quad \text{if } K/\mathbb{Q}_p \text{ is ramified}$$

where in the latter case we have for the exponent  $c(\phi \circ N_{K/\mathbb{Q}_p})$  of the conductor of the character  $\phi \circ N_{K/\mathbb{Q}_p}$ :

$$c(\phi \circ N_{K/\mathbb{Q}_p}) = \begin{cases} 2\gamma - t + 1, & \text{if } \gamma \geq t + 2 \\ \leq t + 1, & \text{if } \gamma \leq t + 1 \end{cases}$$

whence

$$c(\rho \otimes \phi) = \begin{cases} c + 2t + 1, & \text{if } \gamma \leq t + 1 \\ \max\{c + 2t + 1, 2\gamma + 2\}, & \text{if } \gamma \geq t + 2. \end{cases}$$

Computing the number  $t$  in the various cases we arrive at the stated table for the number  $c(\rho \otimes \phi)$ .

Let us then turn to a discussion of  $(\det \rho)|_{U_{\mathbb{Q}_p}}$ . Let  $U'_{\mathbb{Q}_p}$  be the group of units generated by 5 if  $p = 2$ , and otherwise let it denote the full group of 1-units of  $\mathbb{Q}_p$ . The statement of Theorem 1 of [5] specializes to the following: For any choice of complex characters  $\psi_2$  on  $U'_{\mathbb{Q}_p}$  and  $\psi_1$  on the group  $\mu_{2^\infty}(\mathbb{Q}_p)$  of roots of unity of 2-power order in  $\mathbb{Q}_p$ , satisfying certain requirements to be explained below, there is a character  $\psi$  on  $K^\times$  satisfying all of the above, is trivial on roots of unity of odd order, and satisfies in addition:

$$\psi|_{\mu_{2^\infty}(\mathbb{Q}_p)} = \psi_1, \quad \psi|_{U'_{\mathbb{Q}_p}} = \psi_2.$$

The requirements on the character  $\psi_2$  is first that it be trivial if  $p \neq 2$ , or if  $p = 2$  but  $t \geq 2$ . In the remaining cases, i.e.  $p = 2$  and  $d \in \{-1, \pm 3\}$ , we may choose for  $\psi_2$  any character satisfying the following:

Suppose that  $p = 2$ ,  $d = -3$ : Let  $\epsilon$  be the 3'rd root of unity  $(-1 + \sqrt{d})/2$ . If  $c = c(\chi) \leq 2$ , we have from Proposition 1 that  $\chi_2$  is trivial. In that case we require  $\psi_2$  to be trivial. Otherwise the requirement is:

$$\psi_2(5)^{2^{c-3}} = \chi(1 + \epsilon \cdot 2^{c-1})$$

which we claim is satisfied if we require

$$\psi_2(5) = \chi_2(a_2)$$

where  $a_2 := -1 + 2\sqrt{d}$  as in Proposition 1. This follows once we note by easy induction on  $j$  that

$$a_2^{-2^j} \cdot (1 + \epsilon \cdot 2^{j+2}) \in U_K^{(j+3)}$$

so that the requirement on  $\psi_2$  is

$$\psi_2(5)^{2^{c-3}} = \chi(1 + \epsilon \cdot 2^{c-1}) = \chi_2(a_2)^{2^{c-3}}.$$

Suppose then that  $p = 2$  and  $d \in \{-1, 3\}$ : In both of these cases we choose  $\pi := 1 - \sqrt{d}$  as prime element for  $K$ . Notice that  $c(\chi)$  is now necessarily an even number, as  $K/\mathbb{Q}_2$  is now ramified. If  $c = c(\chi) < 4$  we require  $\psi_2$  to be trivial. So, assume  $c \geq 4$ . Then the requirement is

$$\psi_2(5)^{2^{c/2-2}} = \chi(1 + \pi^{c-1}).$$

Now, let us consider the unit  $\eta := -1 + 2\sqrt{d}$  and note by induction on  $j$  that

$$\eta^{-2^j} \cdot (1 + \pi^{2j+3}) \in U_K^{(2j+4)}$$

which shows that our requirement is

$$\psi_2(5)^{2^{c/2-2}} = \chi(\eta)^{2^{c/2-2}}.$$



As the number  $\chi(\eta)^{2^{c/2-2}} = \chi(1 + \pi^{c-1})$  is necessarily  $-1$ , our requirement is satisfied whenever  $\psi_2$  is chosen so that

$$\psi_2(5) = \chi(\eta)^\beta$$

with a 2-adic unit  $\beta$ .

If then  $d = -1$  we have  $a_2 = \eta$ , and we may choose for  $\psi_2$  any character with  $\psi_2(5) = \chi(a_2) = \chi_2(a_2)$ .

If on the other hand  $d = 3$  we have  $a_2 = \pi$ , and as noted in the proof of Proposition 1 we have

$$\pi^2 \equiv a_1^{-1} \eta^\beta \pmod{\mathbb{Q}_2^\times}$$

for a certain 2-adic unit  $\beta$ . Hence, we may choose for  $\psi_2$  any character satisfying

$$\psi_2(5) = \chi_1(a_1) \chi_2(a_2)^2.$$

We can now immediately verify the stated values of  $\delta(5)$  in the various cases.

Let us then turn to a discussion of the character  $\psi_1$ . We will first notice that the proof of Theorem 1 of [5] reveals that we can choose for  $\psi_1$  the restriction  $\tilde{\psi}_1|_{\mathbb{Q}_p^\times}$  where  $\tilde{\psi}_1$  is any character on the group  $\mu_{2^\infty}(K)$  of roots of unity of 2-power order in  $K$  satisfying

$$\tilde{\psi}_1(y) = \chi(x) \quad \text{whenever} \quad y = \frac{\sigma x}{x} \in (K^\times)^{\sigma-1} \cap \mu_{2^\infty}(K).$$

Also, it is shown in that proof that we have

$$(K^\times)^{\sigma-1} \cap \mu_{2^\infty}(K) = \begin{cases} \langle \sqrt{-1} \rangle, & \text{if } K = \mathbb{Q}_p(\sqrt{-1}) \\ \langle -1 \rangle, & \text{otherwise.} \end{cases}$$

So, if  $K \neq \mathbb{Q}_p(\sqrt{-1})$  we have  $\psi_1 = \tilde{\psi}_1$  for which the requirement is

$$\tilde{\psi}_1(-1) = \chi(\sqrt{d}),$$

as  $-1 = \frac{\sigma\sqrt{d}}{\sqrt{d}}$ .

If on the other hand  $K = \mathbb{Q}_p(\sqrt{-1})$  we have  $\mu_{2^\infty}(\mathbb{Q}_p) = \{\pm 1\}$ . We note that  $\sqrt{-1} = \frac{\sigma(1-\sqrt{-1})}{1-\sqrt{-1}}$  and so we choose for  $\tilde{\psi}_1$  any character satisfying  $\tilde{\psi}_1(\sqrt{-1}) = \chi(1 - \sqrt{-1})$ . Then  $\psi_1$  is determined by the requirement

$$\psi_1(-1) = \tilde{\psi}_1(-1) = \tilde{\psi}_1^2(\sqrt{-1}) = \chi((1 - \sqrt{-1})^2) = \chi(-2\sqrt{-1}) = \chi(\sqrt{d}).$$

It is now a trivial matter to verify the stated values for  $\delta(-1)$ ; notice in case  $p \neq 2$ ,  $p \nmid d$  that we have with  $\zeta$  a primitive  $(p^2 - 1)$ 'st root of unity, that

$$\sqrt{d} \equiv \zeta^{\frac{p+1}{2}} \pmod{\mathbb{Q}_p^\times}$$

(as these elements both satisfy the equation  $\sigma x = -x$ ).

This finishes the proof of the Theorem.  $\square$

## 3. FURTHER EXPLICATION IN SPECIAL CASES.

The results of the previous section give a general explicit classification of dihedral type projective representations  $\rho_0 : G_{\mathbb{Q}_p} \rightarrow \mathrm{PGL}_2(\mathbb{C})$  together with information on their lifts to linear representations which is sufficiently explicit for the purposes described in the introduction 1. However, one may wish for an even more explicit description: One that would allow the immediate construction of algorithms computing the relevant lifting data more or less directly from a polynomial over  $\mathbb{Q}_p$  whose splitting field is the field cut out by  $\rho_0$ . Such an additional level of explicitness is in principle achievable through use of explicit reciprocity laws in local class field theory: These would allow the explicit description of the character  $\chi$  of Proposition 1 and Theorem 1 directly from a polynomial as above.

In this final section we shall however give an alternative answer in 2 central and especially problematic cases, namely those cases where the Galois group of the extension cut out by  $\rho_0$  is isomorphic to either  $V_4$  or  $D_4$ . Understanding these cases is important in connection with the problem of lifting global representations of  $S_4$ -type over  $\mathbb{Q}$ , — a problem that has been much studied in the literature. The local cases — in particular the  $D_4$ -case — are difficult for  $p = 2$  mainly because there are many different such representations.

Our additional explication of the lifting theory in these cases is based on the results of the previous section. One essential new point is a reinterpretation of the character  $\psi_1$  occurring in the proof of Theorem 1 which will lead to another way of computing this character ‘directly’ from the extension  $L/\mathbb{Q}_p$  cut out by  $\rho_0$ .

In this section we shall use the following additional notation:  $L/\mathbb{Q}_p$  is an extension with  $G := \mathrm{Gal}(L/\mathbb{Q}_p)$  dihedral of order 4 or 8, i.e.  $G \cong V_4$  or  $G \cong D_4$ . We let  $K = \mathbb{Q}_p(\sqrt{d})$  be a quadratic field contained in  $L$  such that  $L/K$  is cyclic and ramified (such a  $K$  always exists as is easily seen).

Choosing an embedding  $G \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$  gives us a representation  $\rho_0$  as above. In the  $D_4$ -case there are 2 inequivalent choices of this embedding, but it is immaterial for the discussion and the result below which one we choose. With this  $\rho_0$  we are in the setting of Theorem 1 with a ramified character  $\chi$  on  $K^\times$  such that

$$(\rho_0)|_{G_K} \sim \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix}.$$

We can then also retain all other notation from Proposition 1 and Theorem 1.

Our goal in this section is to recompute the data given in Theorem 1 (using among other things Theorem 1 itself) when  $L$  is given explicitly as a radical extension of  $\mathbb{Q}_p$ . I.e., we shall give for one particular lift  $\rho$  of  $\rho_0$  first the restriction  $(\det \rho)|_{U_{\mathbb{Q}_p}} =: \delta$ , and secondly the valuation  $c(\rho \otimes \phi)$  of the Artin conductor of  $\rho \otimes \phi$  for any character  $\phi : G_{\mathbb{Q}_p} \rightarrow \mathbb{C}^\times$  of conductor  $p^\gamma$ .

We shall need the following consequence of a theorem due to B. Perrin-Riou, cf. Théorème 5 of [6]. The theorem applies generally to the case of a dihedral extension of a  $p$ -adic field but we will of course only need it in the  $V_4$  and  $D_4$  cases.

**Lemma 1.** (cf. Théorème 5 of [6]). *In the above situation we have  $\chi(\sqrt{d}) = 1$  if and only if  $L$  can be embedded in a dihedral extension of degree  $2 \cdot [L : \mathbb{Q}_p]$  cyclic over  $K$ .*

*Proof.* An immediate consequence of Théorème 5 of [6] is that the stated embedding problem is solvable if and only if  $\sqrt{d} \in K$  is a norm from  $L$ . As the kernel of  $\chi$  consists precisely of the elements  $K^\times$  that are norms from  $L$ , the claim follows.  $\square$

**3.1.  $V_4$  cases.** Assume now that  $G \cong V_4$ .

The discussion of this case is basically trivial if  $p \neq 2$ : By Proposition 1, there is only one such field  $L$  and  $K/\mathbb{Q}_p$  is the unramified quadratic extension. We have  $c(\chi) = 1$ , and Theorem 1 shows that  $c(\rho \otimes \phi) = 2 \cdot \max\{1, \gamma\}$ , and that we may choose for  $\delta$  any character on  $U_{\mathbb{Q}_p}$  which is trivial on 1-units and on roots of unity of odd order and satisfies:

$$\delta(-1) = \begin{cases} 1 & , \text{ if } p \equiv 3 \pmod{4} \\ -1 & , \text{ if } p \equiv 1 \pmod{4}. \end{cases}$$

The last statement follows because the character  $\chi$  is necessarily non-trivial on  $a_1$  whence  $\chi(a_1) = -1$ .

Let us the proceed with a discussion of the 7 cases with  $G \cong V_4$  for  $p = 2$ .

**Proposition 2.** *Retaining all of the above notation, we have for the 7 extensions  $L/\mathbb{Q}_2$  of  $V_4$ -type lifts  $\rho$  of the attached  $\rho_0$  with the properties summarized in the following table:*

$K$	$L$	$(\det \rho)(-1)$	$(\det \rho)(5)$	$c(\rho \otimes \phi)$
$\mathbb{Q}_2(\sqrt{-3})$	$\mathbb{Q}_2(\sqrt{-3}, \sqrt{-1})$	-1	1	4, if $\gamma \leq 2$ $2\gamma$ , if $\gamma \geq 3$
$\mathbb{Q}_2(\sqrt{-3})$	$\mathbb{Q}_2(\sqrt{-3}, \sqrt{2})$	-1	-1	6, if $\gamma \leq 3$ $2\gamma$ , if $\gamma \geq 4$
$\mathbb{Q}_2(\sqrt{-3})$	$\mathbb{Q}_2(\sqrt{-3}, \sqrt{-2})$	1	-1	6, if $\gamma \leq 3$ $2\gamma$ , if $\gamma \geq 4$
$\mathbb{Q}_2(\sqrt{3})$	$\mathbb{Q}_2(\sqrt{3}, \sqrt{\pm 2})$	1	-1	7, if $\gamma \leq 2$ $2\gamma + 2$ , if $\gamma \geq 3$
$\mathbb{Q}_2(\sqrt{2})$	$\mathbb{Q}_2(\sqrt{2}, \sqrt{-1})$	-1	-1	7, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
$\mathbb{Q}_2(\sqrt{6})$	$\mathbb{Q}_2(\sqrt{6}, \sqrt{-1})$	-1	-1	7, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$

*Proof.* We give the details for the case  $K = \mathbb{Q}_2(\sqrt{-3})$ ,  $L = \mathbb{Q}_2(\sqrt{-3}, \sqrt{2})$ . The other cases are handled in a similar fashion. In this case, the valuation of the conductor of  $L/K$  is 3. Proposition 1 then tells us that  $\chi_2$  is non-trivial of order 2. Theorem 1 then gives  $(\det \rho)(5) = -1$  and the stated value for  $c(\rho \otimes \phi)$ .

Concerning the value  $(\det \rho)(-1)$  let us recall that this is  $\omega(-1)\psi_1(-1)$  where  $\omega$  is the quadratic character of  $\mathbb{Q}_2^\times$  corresponding to  $K/\mathbb{Q}_2$ , and  $\psi_1$  is the character occurring in the proof of Theorem 1. Let us also recall from that proof that  $\psi_1(-1) = \chi(\sqrt{d})$ . Combining this with the above Lemma 1, as well as with the general well-known result (cf. for instance [4] or Lemma 2 below) that a  $V_4$ -extension  $\mathbb{Q}_2(\sqrt{d}, \sqrt{a})$  can be embedded in a  $D_4$ -extension cyclic over  $\mathbb{Q}_2(\sqrt{d})$  if and only if  $(a, -d) = 1$ , we deduce in our present case:

$$(\det \rho)(-1) = (-3, -1) \cdot (2, 3) = -1.$$

$\square$

3.2.  $D_4$  cases. Assume now that  $G \cong D_4$ .

In this case also the discussion is essentially trivial if  $p \neq 2$ : Proposition 1 shows that there exists a dihedral extension  $L/\mathbb{Q}_p$  of order 8 only if  $p \equiv 3 \pmod{4}$ , and in that case there is precisely one such; for an attached projective representation  $\rho_0$  Theorem 1 reveals that we have a lift  $\rho$  with the properties:  $\det \rho$  vanishes on 1-units and roots of unity of odd order, and

$$\det \rho(-1) = (-1)^{\frac{p+1}{4}}.$$

The number  $c(\rho \otimes \phi)$  equals  $2 \cdot \max\{1, \gamma\}$ .

Let us then turn to the more complicated case  $p = 2$ . Before stating the theorem we shall first need some general facts about  $D_4$ -extensions:

**Lemma 2.** *Let  $k$  be a field of characteristic  $\neq 2$ . A biquadratic extension  $k(\sqrt{d}, \sqrt{a})$  can be embedded in a  $D_4$ -extension cyclic over  $k(\sqrt{d})$  if and only if  $(a, -d) = 1$ , i.e. if and only if the equation*

$$x^2 - ay^2 = ad$$

has a solution  $x, y \in k$ . If this is the case then the solutions  $L/k$  to this embedding problem are precisely given by the fields

$$(b) \quad L = k \left( \sqrt{d}, \sqrt{q(x + y\sqrt{a})} \right)$$

where  $q$  runs through  $k^\times$ .

If  $L$  as in (b) is a  $D_4$ -extension then  $L$  can be embedded in a  $D_8$ -extension cyclic over  $k(\sqrt{d})$  if and only if

$$(a, 2)(2qx, -d) = 1 \quad \text{in case } x \neq 0,$$

and if and only if

$$(a, 2) = 1 \quad \text{in case } x = 0.$$

Here, the symbol  $(\cdot, \cdot)$  denotes the usual Brauer symbol over  $k$ .

*Proof.* The first part of the statement is well-known; it can be obtained as a trivial reformulation of Theorem 5 of [4].

For the second part of the statement we need Theorem 6 of [4]. To apply that theorem we need to reshape the square roots generating  $L$  a bit: If  $x \neq 0$  we find that

$$L = k \left( \sqrt{u}, \sqrt{u-1}, \sqrt{2q'(u + \sqrt{u})} \right)$$

where

$$q' := \frac{y^2 qa}{2x}, \quad u := \frac{x^2}{y^2 a};$$

if on the other hand  $x = 0$  then  $k(\sqrt{d}) = k(\sqrt{-1})$ , and we find

$$L = k \left( \sqrt{u}, \sqrt{-1}, \sqrt{2q'\sqrt{u}} \right)$$

with

$$q' := \frac{yq}{2}, \quad u := a.$$

Applying now Theorem 6 of [4] the second part of the statement immediately follows.  $\square$

**Theorem 2.** *The following table lists the  $D_4$ -extensions  $L/\mathbb{Q}_2$  together with the following information: The number  $d$  is such that the quadratic field  $K = \mathbb{Q}_2(\sqrt{d})$  is the (uniquely determined) quadratic sub-extension over which  $L$  is cyclic.*

*Each extension  $L$  gives rise to a projective representation  $\rho_0 : G_{\mathbb{Q}_2} \rightarrow \mathrm{PGL}_2(\mathbb{C})$  by choosing an embedding  $\mathrm{Gal}(L/\mathbb{Q}_2) \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$ . Then there exists a lifting of  $\rho_0$  to a linear representation  $\rho$  with the properties stated in the table for the determinant  $\delta := \det \rho$  and for the exponents of the Artin conductors of a twist of  $\rho$  by a character  $\phi : G_{\mathbb{Q}_2} \rightarrow \mathbb{C}^\times$  of conductor  $2^\gamma$ .*

*The symbol  $i$  denotes a complex 4'th root of unity.*

$d$	$L$	$\delta(-1)$	$\delta(5)$	$c(\rho \otimes \phi)$
-3	$\mathbb{Q}_2(\sqrt{-3}, \sqrt{2 + \sqrt{-2}})$	1	$i$	8, if $\gamma \leq 4$ $2\gamma$ , if $\gamma \geq 5$
-3	$\mathbb{Q}_2(\sqrt{-3}, \sqrt{-(2 + \sqrt{-2})})$	-1	$i$	8, if $\gamma \leq 4$ $2\gamma$ , if $\gamma \geq 5$
-2	$\mathbb{Q}_2(\sqrt{-2}, \sqrt{1 + \sqrt{-1}})$	-1	-1	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
-2	$\mathbb{Q}_2(\sqrt{-2}, \sqrt{3(1 + \sqrt{-1})})$	1	-1	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
2	$\mathbb{Q}_2(\sqrt{2}, \sqrt{3 + \sqrt{3}})$	-1	-1	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
2	$\mathbb{Q}_2(\sqrt{2}, \sqrt{-(3 + \sqrt{3})})$	1	-1	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
6	$\mathbb{Q}_2(\sqrt{6}, \sqrt{3 + \sqrt{-1}})$	-1	-1	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
6	$\mathbb{Q}_2(\sqrt{6}, \sqrt{2(3 + \sqrt{-1})})$	1	-1	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
-6	$\mathbb{Q}_2(\sqrt{-6}, \sqrt{2 + 2\sqrt{-2}})$	1	-1	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
-6	$\mathbb{Q}_2(\sqrt{-6}, \sqrt{-(2 + 2\sqrt{-2})})$	-1	-1	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
-1	$\mathbb{Q}_2(\sqrt{-1}, \sqrt{\sqrt{2}})$	-1	$i$	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
-1	$\mathbb{Q}_2(\sqrt{-1}, \sqrt{3\sqrt{2}})$	-1	$i$	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
-1	$\mathbb{Q}_2(\sqrt{-1}, \sqrt{\sqrt{3}})$	1	1	5, if $\gamma \leq 2$ $2\gamma + 2$ , if $\gamma \geq 3$
-1	$\mathbb{Q}_2(\sqrt{-1}, \sqrt{2\sqrt{3}})$	1	-1	7, if $\gamma \leq 2$ $2\gamma + 2$ , if $\gamma \geq 3$
-1	$\mathbb{Q}_2(\sqrt{-1}, \sqrt{\sqrt{6}})$	1	$i$	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
-1	$\mathbb{Q}_2(\sqrt{-1}, \sqrt{2\sqrt{6}})$	1	$i$	9, if $\gamma \leq 3$ $2\gamma + 2$ , if $\gamma \geq 4$
3	$\mathbb{Q}_2(\sqrt{3}, \sqrt{2 + \sqrt{-1}})$	-1	-1	7, if $\gamma \leq 2$ $2\gamma + 2$ , if $\gamma \geq 3$
3	$\mathbb{Q}_2(\sqrt{3}, \sqrt{2(2 + \sqrt{-1})})$	1	1	5, if $\gamma \leq 2$ $2\gamma + 2$ , if $\gamma \geq 3$

*Proof.* It is well-known that there are exactly 18  $D_4$ -extensions of  $\mathbb{Q}_2$ , and also what they actually look like: See for instance [1]. One finds this list by applying Lemma 2: We have to find the biquadratic extensions  $\mathbb{Q}_2(\sqrt{d}, \sqrt{a})$  for which  $(a, -d) = 1$ ; for such an extension, the  $D_4$ -extensions containing it which are cyclic over  $\mathbb{Q}_2(\sqrt{d})$  are then given by the fields  $L = \mathbb{Q}_2\left(\sqrt{d}, \sqrt{q(x + y\sqrt{a})}\right)$  where  $(x, y)$  is a solution to the equation  $x^2 - ay^2 = ad$ , and  $q$  runs through  $\mathbb{Q}_2^\times$ ; one sees immediately that we get exactly 2 distinct fields  $L$ , by choosing  $q \in \{1, u\}$  where  $u$  is such that the numbers

$$1, d, a, ad, u, ud, ua, uad$$

is a full system of representatives for the square classes in  $\mathbb{Q}_2^\times$ .

Given now any such field  $L = \mathbb{Q}_2\left(\sqrt{d}, \sqrt{q(x + y\sqrt{a})}\right)$ , we compute the exponent  $c$  of the conductor of the cyclic extension  $L/\mathbb{Q}_2(\sqrt{d})$ . Once an embedding  $\text{Gal}(L/\mathbb{Q}_2)$  – and thus a projective representation  $\rho_0$  – has been chosen we have  $c = c(\chi)$  where  $\chi$  is the character of  $G_{\mathbb{Q}_2(\sqrt{d})}$  such that  $(\rho_0)|_{G_{\mathbb{Q}_2(\sqrt{d})}} \sim \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix}$ . Interpreting  $\chi$  as a character of  $K^\times$  with  $K := \mathbb{Q}_2(\sqrt{d})$  we are then in the situation of Theorem 1. Theorem 1 then gives us a ‘good’ lifting  $\rho$  but we have to determine the quantities  $\chi_1(a_1)$  and  $\chi_2(a_2)$  of the theorem in order to get the desired data for the lift  $\rho$  (in the case  $d = -1$ , knowledge of  $\chi_1(a_1)^2$  and  $\chi_2(a_2)$  will do). To do this, we first claim – and this must be verified individually in each case – that we can determine from Proposition 1 the order  $2^{s_2}$  of  $\chi_2$  solely from knowledge of  $c(\chi)$  and the fact that  $\chi$  has order 4. Secondly, the number  $\chi_1(a_1)$  can be determined thus: Except in case  $d = -1$  we have  $\chi_1(a_1) = \chi(\sqrt{d})$ ; if  $d = -1$  we have  $\chi_1(a_1)^2 = \chi(\sqrt{d})$ . So, it is clear that all the desired data for the lift  $\rho$  can be determined by Theorem 1 if we can compute  $\chi(\sqrt{d})$ . However, combining Lemmas 1 and 2 we find:

$$\chi(\sqrt{d}) = \begin{cases} (a, 2)(2qx, -d), & \text{if } x \neq 0 \\ (a, 2), & \text{if } x = 0. \end{cases}$$

Let us give the details for  $d = -3$ . The arguments in the other cases run similarly. For  $d = -3$  we have the 2 fields

$$L = \mathbb{Q}_2\left(\sqrt{-3}, \sqrt{q(2 + \sqrt{-2})}\right)$$

with  $q = \pm 1$ . In both cases we find  $c = 4$ . Proposition 1 then reveals that  $s_2 = 2$ , i.e. that  $\chi_2$  has order 4. So, by Theorem 1 the number  $\delta(5)$  is a complex 4'th root of unity. The theorem also immediately gives the number  $c(\rho \otimes \phi)$ . We find

$$\delta(-1) = \chi(\sqrt{-3}) = (-2, 2)(2q \cdot 2, 3) = (q, 3) = \begin{cases} 1, & \text{for } q = 1 \\ -1, & \text{for } q = -1. \end{cases}$$

□

**Remark 1.** *There are 2 inequivalent embeddings  $D_4 \hookrightarrow \text{PGL}_2(\mathbb{C})$ . One can easily verify that switching between these in the setting of Theorem 2 has the only effect of changing the sign of the complex 4'th root of unity  $i$  wherever it occurs in the table.*

## REFERENCES

- [1] P. Bayer, A. Rio: 'Dyadic exercises for octahedral extensions.' *J. Reine Angew. Math.* **517** (1999), 1–17.
- [2] J. P. Buhler: 'Icosahedral Galois representations', *Lecture Notes in Mathematics* **654**, Springer, 1978.
- [3] F. Halter-Koch: 'Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern.' *J. Number Theory* **4** (1972), 70–77.
- [4] I. Kiming: 'Explicit classification of some 2-extensions of a field of characteristic different from 2.' *Canad. J. Math.* **42** (1990), 825–855.
- [5] I. Kiming: 'On the liftings of 2-dimensional projective Galois representations over  $\mathbb{Q}$ .' *J. Number Theory* **56** (1996), 12–35.
- [6] B. Perrin-Riou: 'Plongement d'une extension diédrale dans une extension diédrale ou quaternionienne.' *Ann. Inst. Fourier (Grenoble)* **30** (1980), no. 4, 19–33.
- [7] J.-P. Serre: 'Modular forms of weight one and Galois representations.' *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pp. 193–268. Academic Press, London, 1977.
- [8] J.-P. Serre: 'Local Fields.' *Graduate Texts in Mathematics* **67**, Springer-Verlag, 1979.
- [9] A. Weil: 'Exercices dyadiques.' *Invent. Math.* **27** (1974), 1–22.
- [10] E.-W. Zink: 'Ergänzungen zu Weils Exercises dyadiques.' *Math. Nachr.* **92** (1979), 163–183.

P.F: H:S INSTITUTE OF PREVENTIVE MEDICINE, KOMMUNEHOSPITALET, 1399 COPENHAGEN K, DENMARK, EMAIL: PF@IPM.HOSP.DK

I.K.: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COPENHAGEN, UNIVERSITETSPARKEN 5, 2100 COPENHAGEN Ø, DENMARK, EMAIL: KIMING@MATH.KU.DK