ON THE LIFTINGS OF 2-DIMENSIONAL PROJECTIVE GALOIS REPRESENTATIONS OVER $\mathbb{Q}$.

IAN KIMING

Abstract. We show how the problem of determining the possible Artin conductors and determinant characters of liftings of a given 2-dimensional (irreducible) projective Galois representation over $\mathbb{Q}$ can be reduced to certain analogous local problems, and we solve those problems. By this, the problem of determining all irreducible representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{C})$ with prescribed Artin conductor and determinant character is effectively reduced to a question in geometry of numbers.

1. Introduction and motivation

Given a 2-dimensional, continuous representation:

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

where $\mathbb{C}$ has the discrete topology so that 'continuous' implies 'having finite image', we may consider its projectivisation:

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

obtained by composing ρ with the canonical projection $\mathrm{GL}_2(\mathbb{C}) \to \mathrm{PGL}_2(\mathbb{C})$. Sometimes, and in particular in connection with investigations of the conjectural correspondence between 2-dimensional, continuous, irreducible, 'odd' Galois representations over $\mathbb{Q}$ and modular forms of weight 1 on congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, it is of interest to reverse this situation, i.e. to consider $\bar{\rho}$ as being given and ask for 'liftings' of $\bar{\rho}$ that is, representations ρ as above whose projectivisation is $\bar{\rho}$ (cf. for example: [1], [2], [5]). According to a theorem of Tate, such liftings always exist. Of particular interest is the knowledge of the Artin conductors and determinant characters of the liftings, where by the determinant character $\det(\rho)$, of a lifting ρ we understand the character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ obtained by composing ρ with the determinant:

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

The class field theoretic conductor of $\det(\rho)$ divides the Artin conductor $a(\rho)$ of ρ, so that $\det(\rho)$ may be viewed as a Dirichlet character modulo $a(\rho)$. Hence, one wants to address 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. [5]) 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. [5]. 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.)

The purpose of this note is to solve this problem.

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 2 and 3 respectively. In section 2 we shall consider a somewhat more general problem, which is analogous to the above problem in case (b). A specialization, which is given in the second part of Theorem 1 of section 2, gives however a complete solution to the above problem for the case (b); see the discussion at the beginning of section 2.

For case (c) there is already essential information available: Building upon [6], the *minimal* conductor of a lifting of $\bar{\rho}$ was determined by Buhler and Zink, cf. [2] and [7]. In fact, the conductors of twists $\rho \otimes \chi$, where ρ is a lifting of $\bar{\rho}$ with minimal conductor, were determined in [7]. 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.

2. 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 [5], 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 1 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 $\mathbb{Q}_p^\times$.

We have found it profitable to consider a slightly more general problem: Suppose that K is a finite extension of $\mathbb{Q}_p$, l is a prime number and L/K is a Galois extension with Galois group $\mathbb{Z}/\mathbb{Z}l$ generated by σ. Suppose further that χ is a character of $L^\times$ vanishing on $K^\times$. Determine for a character ψ satisfying $(*)$ the answers to (1) and (2) above.

A solution to this problem has, along lines completely analogous to the above discussion, applications to the study of liftings of projective, l-dimensional representations:

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{PGL}_l(\mathbb{C})$$

for which the image in $\mathrm{PGL}_l(\mathbb{C})$ is a finite group of the type: $< \sigma > \ltimes < \tau >$, where τ has order n, σ has order l and:

$$\sigma\tau\sigma^{-1} = \tau^a,$$

where a is an integer in $(\mathbb{Z}/\mathbb{Z}n)^\times$ such that:

$$n \quad \text{divides} \quad 1 + a + \ldots + a^{l-1}.$$

The dihedral case above corresponds to $l = 2$, $a = -1$.

This more general problem will be considered in the first part of Theorem 1 below under certain assumptions on the ground field K. In case $l = 2$, these assumptions are true if $K = \mathbb{Q}_p$ for some p, so that the specialization $l = 2$ of the first part of Theorem 1 gives, according to the above discussion, a complete and explicit solution to case (b) of the problem considered in the introduction. This solution is given in the second part of Theorem 1.

First, we need the following simple proposition.

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: $(U_L^i)^{\sigma-1} \leq U_L^i$ 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:*

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

(where t is a non-negative integer).

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

If $i \in \mathbb{N}$ with $l \nmid i$, then: $(U_L^i)^{\sigma-1} \leq U_L^{i+t}$, 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) We may choose $\pi = \pi_K$ as a prime element of L. It is trivial that $\sigma - 1$ maps U_L^i into itself for all $i \in \mathbb{N}$. Let $i \in \mathbb{N}$ and let $u \in U_L^i - U_L^{i+1}$ be such that $u^{-1}\sigma u \in U_L^{i+1}$. Modulo U_L^{i+1} the element u is represented by $1 + a\pi^i$ for some $a \in E_L$. Now, $\frac{\sigma(1+a\pi^i)}{1+a\pi^i} \equiv (1 + (\sigma a)\pi^i)(1 - a\pi^i) \equiv 1 + (\sigma a - a)\pi^i \bmod \wp_L^{2i}$, hence $\sigma a - a$ is not a unit. Then $\frac{\sigma a}{a} - 1$ is also not a unit, so $\frac{\sigma a}{a}$ is a 1-unit. Since $\frac{\sigma a}{a} \in E_L$, we deduce $\frac{\sigma a}{a} = 1$, i.e. $a \in K^\times$, and thus $u \in U_K^i U_L^{i+1}$.

(3) Clearly, $\sigma - 1$ maps U_L^i into itself for all i. Suppose first that $t = 0$, i.e. L/K is tamely ramified, i.e. $l \neq p$. It follows that we can choose a prime element π of L such that:

$$\sigma\pi = \zeta\pi,$$

ζ is a primitive l'th root of unity. Let $i \in \mathbb{N}$ and $u \in U_L^i - U_L^{i+1}$. Modulo U_L^{i+1} we can represent n by $1 + a\pi^i$ for some $a \in E_L$. Now, as σ acts trivially on a we get:

$$\frac{\sigma(1 + a\pi^i)}{1 + a\pi^i} \equiv (1 + a\zeta^i\pi^i)(1 - a\pi^i) \equiv 1 + a(\zeta^i - 1)\pi^i \bmod \wp_L^{2i} \ .$$

Since $\zeta^i - 1$ is a unit if and only if $l \nmid i$, our claims follow immediately in this case.

Suppose then that L/K is wildly ramified, i.e. $t > 0$, i.e. $l = p$. Let π be a prime element for L. We have:

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

where u is a unit, since $\sigma \in G_t - G_{t+1}$. If now $i \in \mathbb{N}$ and $b \in O_L$, then:

$$\begin{aligned} \sigma(1 + b\pi^i) &= 1 + (\sigma b)(\pi + u\pi^{t+1})^i \\ &\equiv 1 + (\sigma b)\pi^i + iu(\sigma b)\pi^{i+t} \bmod \wp_L^{i+t+1} \ , \end{aligned}$$

since $t \geq 1$. As $\sigma b \equiv b \bmod \wp_L^{t+1}$, we obtain:

$$\begin{aligned} \frac{\sigma(1 + b\pi^i)}{1 + b\pi^i} &\equiv (1 + (\sigma b)\pi^i + iu(\sigma b)\pi^{i+t}) \sum_{k=0}^{\infty} (-1)^k b^k \pi^{ik} \\ &\equiv 1 + iu(\sigma b)\pi^{i+t} + \sum_{k=1}^{\infty} (-1)^{k-1} b^{k-1} (\sigma b - b)\pi^{ik} \\ &\equiv 1 + iu(\sigma b)\pi^{i+t} \bmod \wp_L^{i+t+1} \ . \end{aligned}$$

It follows that $(U_L^i)^{\sigma-1} \leq U_L^{i+t}$ for all i, that $(U_L^i)^{\sigma-1} \leq U_L^{i+t+1}$, if $p \mid i$, and that the homomorphism:

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

induced by $\sigma - 1$ is injective if $p \nmid i$. If $p \nmid i$, every element of U_L^{i+t} can modulo U_L^{i+t+1} be represented by an element of the form $1 + iu(\sigma b)\pi^{i+t}$, this homomorphism is also surjective. □

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. [3] 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 [4], 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. (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:

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

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

Define:

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

If $l \neq p$, let U_K' be U_K^1 , 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*) $$\psi\left(\frac{\sigma x}{x}\right) = \chi(x) \quad \text{for all } x \in L^\times$$

(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 $c_L(\varphi \circ N_{L/K})$:

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

and if L/K is ramified:

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

(2). *Retaining the notation of (1), consider the situation of (1) for $l = 2$, so that K is a finite extension of $\mathbb{Q}_p$, L/K a quadratic extension, and χ a character on $L^\times$ which vanishes on $K^\times$. The assumptions of (1) then simply mean that $K = \mathbb{Q}_2$ if $p = 2$.*

Furthermore, the character ψ_2 may be explicated as follows.

If $p \neq 2$, or if $p = 2$ and L/K ramified but χ unramified, ψ_2 is trivial.

Otherwise we have $p = 2$, so that $K = \mathbb{Q}_2$, and $L = \mathbb{Q}_2(\sqrt{\alpha})$ where α is -3, -1 or 3 and χ is (wildly) ramified if α is -1 or 3. Then U'_K is the group generated by 5 and for ψ_2 we may choose any character on $< 5 >$ satisfying the following.

If $\alpha = -3$: Then $L = \mathbb{Q}_2(\epsilon)$, where ϵ is a primitive 3'rd root of unity. Put $\psi_2 = 1$ if $c \leq 2$. If $c \geq 3$, we require:

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

If $\alpha = -1$ or $\alpha = 3$: Here $L/\mathbb{Q}_2$ is wildly ramified, and since χ is ramified we have $c = c_L(\chi) > 1$. Then c is an even number. Let π be a prime element of L (for example $1 + \sqrt{\alpha}$). Put $\psi_2 = 1$ if $c = 2$. If $c \geq 4$, we require:

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

Proof. (1). We shall first show that:

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

For, if $\xi \in (L^\times)^{\sigma-1} \cap \mu_{l^\infty}(L)$, then $N_{L/K}(\xi) = 1$. So, if $\xi \in K^\times$, we get $\xi^l = 1$, hence $\xi \in \langle \zeta \rangle$. If $\xi \notin K^\times$, we have:

$$\sigma\xi = \zeta^a \xi \quad \text{for some} \quad a \not\equiv 0 \quad (l).$$

Then:

$$1 = N_{L/K}(\xi) = \xi^l \zeta^{a \cdot \frac{l(l-1)}{2}},$$

and so $l = 2$, since otherwise $\xi^l = 1$. But then: $\xi^2 = \zeta^{-1} = -1$, i.e. $\xi \in \langle\sqrt{-1}\rangle$ and $L = K(\sqrt{-1})$. On the other hand we clearly have $\zeta \in (L^\times)^{\sigma-1}$, and if $L = K(\sqrt{-1})$ then:

$$\sqrt{-1} = \frac{\sigma(1-\sqrt{-1})}{1-\sqrt{-1}}.$$

This establishes $(*)$.

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

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

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:

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

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.

If L/K is unramified, then χ must be ramified, since χ vanishes on $K^\times$. Hence: $c = c_L(\chi)$. Clearly, $\sigma - 1$ has kernel E_K on E_L. Proposition 1 then implies that $x^{-1}\sigma x \in U_L^i \Rightarrow x \in K^\times U_L^i$, for $i \geq 0$. So: $i_0 \leq c$. If $c = 1$, we must then have $i_0 = 1$. Otherwise there is an $x \in U_L^{c-1}$ with $\chi(x) \neq 1$. Then $x \notin K^\times U_L^c$, and so proposition 1 gives: $x^{-1}\sigma x \in U_L^{c-1} - U_L^c$. So: $i_0 \geq c$.

If L/K is ramified, then $E_L = E_K$ and so χ is either unramified of wildly ramified. Suppose that χ is unramified. Then $c + t = 1 + t$. Since $\chi(\pi_L) \neq 1$ and $\pi_L^{-1}\sigma\pi_L \in U_L^t - U_L^{t+1}$, we have $i_0 \geq 1 + t$. On the other hand, we now see that proposition 1 implies: $x^{-1}\sigma x \in U_L^{1+t} \Rightarrow x \in K^\times U_L^1$. So: $i_0 \leq 1 + t$.

Suppose finally that L/K is ramified and that 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 $y \equiv y_1$ mod $K^\times$ 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 $i_0 \leq c+t$.

By this, $(**)$ is established.

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

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

and if L/K is ramified, we have:

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

and

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

cf. [4], chapter 5. From this, the remarks in the statement of (1) 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 (1) 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:

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

We shall now demonstrate $(***)$.

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:

$$u_0 = 1.$$

We now split the discussion up into 4 cases.

I. Suppose first that $l \neq p$. Then $U'_K = U^1_K$, $t = 0$ and $i_0 = c$. Now, $N_{L/K}(u) = N_{L/K}(\xi)u_1^l$, so $N_{L/K}(\xi) \in \mu_{l^\infty}(K) \cap U^1_K = \{1\}$, and as we have seen this gives $\xi \in (L^\times)^{\sigma-1}$. Then $u_1 \in N_{L/K}(U^c_L)$, since $l \neq p$.

Ia. If L/K is unramified, we get:

$$u_1 \in N_{L/K}(U^c_L) = U^c_K \leq U^c_L,$$

and so $\frac{\sigma x}{x} \cdot \xi \in (L^\times)^{\sigma-1} \cap U^c_L$, hence

$$\psi_0(y) = \psi_0\left(\frac{\sigma x}{x}\xi\right)\psi_0(u_1) = \psi_2(u_1) = 1,$$

since ψ_2 is trivial.

Ib. If L/K is ramified, choose a such that $1 \leq a \leq l$ and $c \equiv a \ (l)$. Then:

$$u_1 \in N_{L/K}(U^c_L) = U_K^{\frac{c-a}{l}+1} \leq U^{c-a+l}_L \leq U^c_L,$$

and as in **Ia** we deduce that $\psi_0(y) = 1$.

IIa. Suppose now that $l = p$ and L/K is unramified. Then $\mu_{p^\infty}(L) = \mu_{p^\infty}(K) = \langle\zeta\rangle \leq (L^\times)^{\sigma-1}$ so that we can write:

$$y = u = \frac{\sigma x_0}{x_0} \cdot u_1 \quad \text{for some } x_0 \in L^\times.$$

Then $u_1^{-1} \equiv \frac{\sigma x_0}{x_0} \mod U^c_L$, since $u \in U^{i_0}_L = U^c_L$, and so $\psi_2(u_1) = \chi(x_0)^{-1}$, hence: $\psi_0(y) = \chi(x_0)\psi_2(u_1) = 1$.

IIb.

Suppose then finally that $l = p$ and that L/K is 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,

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

and so $N_{L/K}(\xi)$ and u_1^p both belong to U^{w+1}_K. 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:

$$u_1 \in U^{w+1-e}_K \leq U^{p(w+1-e)}_L \leq U^{c+t}_L,$$

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:

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

This finishes the proof of $(***)$ and of (1) of the theorem.

(2). For $p = 2$ the special assumptions on K and L are: $K = \mathbb{Q}_2$ and $t \geq 1$ if L/K is ramified; but here the last assumption is vacuous since there are no tamely ramified extensions of $\mathbb{Q}_2$.

If $p \neq 2$, or if $p = 2$ and $L/\mathbb{Q}_2$ is ramified but χ unramified, then (1) implies that ψ_2 may be chosen to be trivial.

Otherwise, $p = 2$ and $L = \mathbb{Q}_2(\sqrt{\alpha})$ where α is -3, -1 or 3. Here we may explicate ψ_2 as a character on $< 5 >$ by going through the procedure given before the statement of Theorem 1.

Notice first that:

$$5^{2^s} \equiv 1 + 2^{s+2} \mod 2^{s+3},$$

if s is a non-negative integer.

Suppose that $\alpha = -3$: Then $L/\mathbb{Q}_2$ is unramified, i.e. $L = \mathbb{Q}_2(\epsilon)$, where ϵ is a 3'rd root of unity. We have $\sigma\epsilon = \epsilon^2$, where σ is the non-trivial automorphism of $L/\mathbb{Q}_2$. The requirement on ψ_2 is that:

$$\psi_2(5^{2^{s-1}}) = \chi(x) \ ,$$

where $s \geq 1$ is smallest possible such that:

$$5^{2^s} \in U_L^c \ ,$$

and $x \in L^\times$ is such that:

$$5^{2^{s-1}} \equiv \frac{\sigma x}{x} \mod U_L^c.$$

If $c \leq 2$ we have $s = 1$ and may choose $x = 1$; hence $\psi_2 = 1$.

If $c \geq 3$ we have $s = c-2$. Since $\epsilon^2 + \epsilon + 1 = 0$ we have:

$$5^{2^{c-3}}(1 + \epsilon \cdot 2^{c-1}) \equiv (1 + 2^{c-1})(1 + \epsilon \cdot 2^{c-1}) \equiv 1 + \epsilon^2 \cdot 2^{c-1} \mod U_L^c,$$

so that we may choose $x = 1 + \epsilon \cdot 2^{c-1}$; the requirement on ψ_2 is then:

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

Suppose that $\alpha = -1$ or $\alpha = 3$: Here $L/\mathbb{Q}_2$ is ramified so that χ is assumed to be ramified. Then $c = c_L(\chi)$, which must be even, since χ vanishes on $\mathbb{Q}_2^\times$. The number t is 1 in both cases. If π is a prime element of L, we have then:

$$\sigma\pi = \pi + u\pi^2,$$

where σ is the non-trivial automorphism of $L/\mathbb{Q}_2$ and u a (1-)unit. Now, the requirement on ψ_2 is that:

$$\psi_2(5^{2^{s-1}}) = \chi(x),$$

where $s \geq 1$ is smallest possible such that:

$$5^{2^s} \in U_{\mathbb{Q}_2}^{\frac{1}{2}c+1},$$

and $x \in L^\times$ is such that:

$$5^{2^{s-1}} \equiv \frac{\sigma x}{x} \mod U_L^{c+1}.$$

If $c = 2$, we have $s = 1$ and we may choose $x = 1$; hence $\psi_2 = 1$.

If $c \geq 4$, we have $s = \frac{1}{2}c - 1$ and:

$$5^{2^{\frac{1}{2}c-2}}(1 + \pi^{c-1}) \equiv 1 + \pi^{c-1} + \pi^c \equiv 1 + \pi^{c-1} + u(c-1)\pi^c$$

$$\equiv 1 + (\sigma\pi)^{c-1} \mod U_L^{c+1},$$

since $u(c-1)$ is a 1-unit. Hence we may choose $x = 1+\pi^{c-1}$, and so the requirement on ψ_2 is:

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

This finishes the proof of (2) of the theorem. □

Remark 1. *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 2. *Notice that one of the non-trivial and essential points of Theorem 1 is the fact that $c_L(\psi \cdot (\varphi \circ N_{L/K}))$, where ψ is as in the theorem and φ is a character on $K^\times$, can be computed alone from the knowledge of c, t and $c_K(\varphi)$. For if L/K is unramified, we have $c_L(\varphi \circ N_{L/K}) = c_K(\varphi)$ and so:*

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

If L/K is ramified and $c_K(\varphi) \geq t + 2$, we have:

$$c_L(\psi \cdot (\varphi \circ N_{L/K})) = \max\{c + t, l \cdot c_K(\varphi) + (1 - l)t + 1\};$$

and finally, if L/K is ramified and $c_K(\varphi) \leq t+1$, then $c_L(\varphi \circ N_{L/K}) \leq t+1 \leq c+t$, and so:

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

In particular, (2) of Theorem 1 gives a complete solution to 'case (b)' of the problem considered in the introduction.

3. 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 [2] or [7].

First of all, we must necessarily have $p = 2$, cf. [2], 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 [2], chap. 2, and [7], 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. [7], 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. [4], chap. 5. Hence:

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

Using again [4], 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 $1 \leq a \leq e$:

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

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

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

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

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

and

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

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

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

and

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

The next result is due to E.-W. Zink (see [7]), but we shall restate and reprove the result in order to make a few points more explicit.

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 $\rho \otimes \varphi$:*

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

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 (♭♭) and (♭♭♭) above, we have $c_M(\chi) = 3t+1$ and there is an $u \in U_M^{3t}$ with $N_{M/K}(u) = 1$ and $\chi(u) \neq 1$. 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 $c \geq \frac{3t}{2e} + 1$. We claim that $c \geq \frac{t+1}{e} + 1$. This is clear if $t \geq 2$. If $t = e = 1$, then $c \geq 3 = 1 + \frac{2}{e}$, and if $t = 1, e = 3$, then $\frac{2}{e} + 1 < 2 \leq c$. From (♯♯) we conclude that:

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

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 [6], 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 1 for 2-dimensional, projective Galois representations over $\mathbb{Q}_2$ of type A_4 or S_4.

Theorem 2. *Let $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2) \to \mathrm{PGL}_2(\mathbb{C})$ 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:*

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

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

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

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

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

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. [7], section 2, or [1], 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:

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

We now split the discussion up into 4 cases.

$\underline{M = M_1}$: From (♮) above we get:

$$U^2_{\mathbb{Q}_2} = N_{N/\mathbb{Q}_2}(U^5_M) \ ,$$

and since $c_M(\chi) = 3t + 1 = 4$, we deduce from (†) that $\varepsilon(5) = 1$. On the other hand, χ^2 must be non-trivial, hence non-trivial on U_M, so ε is non-trivial on $U_{\mathbb{Q}_2}$. Hence, $\varepsilon(-1) = -1$.

$\underline{M = M_2}$: Here, (♮) above gives:

$$U^2_{\mathbb{Q}_2} = N_{M/\mathbb{Q}_2}(U^9_M).$$

Now, if $u \in U^8_M$ then $u^2 \in U^{16}_M$, and since $c_M(\chi) = 3t+1 = 16$, we find $c_M(\chi^2) \leq 8$. We deduce that $\varepsilon(5) = 1$. As in the preceding case we then find that $\varepsilon(-1) = -1$.

$\underline{M = M_3}$: Suppose that χ^2 is non-trivial. Then χ^2 is non-trivial on U_M, and since (††) 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:

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

which is impossible, because we have $c_M(\chi^2) \leq 8$ as in the case $M = M_2$. Hence $\chi^2 = 1$, and $\varepsilon(-1) = \varepsilon(5) = 1$.

$\underline{M = M_4}$: If χ^2 were non-trivial, then ψ^2 would have conductor at least 3, and (††) combined with (♯♯) above would give:

$$c_M(\chi^2) = c_M(\psi^2 \circ N_{M/\mathbb{Q}_2}) = 12 c_{\mathbb{Q}_2}(\psi^2) - 4 \geq 32,$$

contradicting $c_M(\chi) = 3t + 1 = 4$. Hence $\chi^2 = 1$, and $\varepsilon(-1) = \varepsilon(5) = 1$.

This finishes the proof of the theorem, since the statements about the Artin conductors of the twists $\rho \otimes \varphi$ follow immediately from proposition 2 because ρ is a lifting with minimal Artin conductor. □

References

[1] P. Bayer, G. Frey: 'Galois representations of octahedral type and 2-coverings of elliptic curves.' Math. Z. **207** (1991), 395–408.
[2] J. P. Buhler: 'Icosahedral Galois Representations.' Lecture Notes in Mathematics **654**, Springer-Verlag 1978.
[3] H. Hasse: 'Number Theory.' Grundlehren der mathematischen Wissenschaften **229**, Springer-Verlag, 1980.
[4] J.-P. Serre: 'Local Fields.' Graduate Texts in Mathematics **67**, Springer Verlag, 1979.
[5] J.-P. Serre: 'Modular forms of weight one and Galois representations.' In: A. Fröhlich: Algebraic Number Fields. Academic Press 1977.
[6] A. Weil: 'Exercises dyadiques.' Invent. Math. **27** (1974), 1–22.
[7] 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.