PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A
MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

The Arithmetic Theory of Local Galois Gauss Sums for Tame Characters

A. Frohlich and M. J. Taylor

Phil. Trans. R. Soc. Lond. A 1980 **298**, 141-181
doi: 10.1098/rsta.1980.0242

THE ARITHMETIC THEORY OF LOCAL GALOIS GAUSS SUMS FOR TAME CHARACTERS

By A. FRÖHLICH,† F.R.S., and M. J. TAYLOR‡

† *King's College, Strand, London WC2R 2LS*

‡ *Queen Mary College, Mile End Road, London E1 4NS*

(*Received* 22 *August* 1979)

CONTENTS

	PAGE
Introduction	141
1. Basic results and statement of the main theorems	144
2. Properties of conductors, resolvents and characteristics	151
3. Definition of τ and immediate consequences	156
4. Proof of theorem 4	161
5. l-characters	161
6. Inductivity	167
7. Uniqueness	175
8. Real-valued characters	177
References	181

The constants in the functional equation of the Artin L-function can be written as products of local root numbers and these in turn are defined in terms of local Galois Gauss sums. It is the arithmetic behaviour of the latter which is determined here in the tame case. In particular their ideal values are described by local resolvents, and two types of basic congruences are established. It is also shown that for a given local field the tame Galois Gauss sums can be characterized within that field by their arithmetic properties. In addition a new local proof for inductivity in the tame case is obtained.

Introduction

The constants in the functional equation of the Abelian L-functions can in a natural manner be written as products of local factors, defined in terms of Gauss sums (see Tate's thesis published in Cassels & Fröhlich (1967)). The existence of a similar local decomposition of the constants in the functional equation of the Artin L-functions is equivalent to the existence of local constants for not necessarily Abelian characters of local Galois groups which coincide with the classical ones in the Abelian case and behave well under character induction. (There is a more general problem for Weil groups, but we restrict ourselves to Galois groups.)

This problem was originally stated by Hasse (1954) and Dwork (1956) obtained a solution modulo ± 1. The first to arrive at a complete solution was Langlands. His proof was based on some new results in representation theory and on some deep and difficult manipulations with local Gauss sums. Langland's proof has not actually been published. A shorter proof, going via the existence of global constants, is due to Deligne (1973), and a variant of Deligne's proof was given in Tate's (1977) Durham lectures. It is these notes of Tate's which can serve best for the discussion of the background to our paper.

We shall actually formulate everything in terms of the local Galois Gauss sums $\tau(\chi)$ first introduced by Martinet (1977). They are connected with the local root numbers $W(\chi)$ (i.e. the local factors of the Artin constants) by the equation

$$W(\chi) = \tau(\bar{\chi})/N\mathfrak{f}(\chi)^{\frac{1}{2}}.$$

Here χ is a not necessarily Abelian character of a local Galois group, $\bar{\chi}$ its complex conjugate, $\mathfrak{f}(\chi)$ the conductor and $N\mathfrak{f}(\chi)^{\frac{1}{2}}$ the positive square root of its absolute norm. Given $N\mathfrak{f}(\chi)$, whose determination is a relatively easier problem, the root numbers $W(\chi)$ and the Galois Gauss sums $\tau(\chi)$ determine each other. In fact however, while the knowledge of the $W(\chi)$ does not entail that of the other two constants, that of the $\tau(\chi)$ does. Indeed $N\mathfrak{f}(\chi)^{\frac{1}{2}}$ is the modulus $|\tau(\chi)| = |\tau(\bar{\chi})|$ and so $W(\chi)$ is the projection of $\tau(\bar{\chi})$ on the unit circle. This is the first reason for our preference for the Galois Gauss sum. The second one lies in its direct connection with the classical (Abelian) Gauss sum, which had played such an important rôle in many arithmetic contexts and which was used to define the local Abelian constants in the first place. Our third reason is that – as will be seen – the underlying arithmetic properties attach naturally to the $\tau(\chi)$ rather than the $W(\chi)$. Finally it is the $\tau(\chi)$ which lie at the basis of the connection with global Galois module structure (Fröhlich 1976) and with local Hermitian Galois module structure (Fröhlich 1977).

As indicated in the title we are concerned only with tame characters of Galois groups (although a few of our results obviously generalize). These are the Galois Gauss sums which can be viewed as a generalization of Gauss sums for finite fields. Our first aim is to derive their fundamental arithmetic properties, as regards prime ideal decomposition, absolute values, Galois action and congruence behaviour. The original motivation which first led to these, previously unknown, arithmetic properties was the connection with Galois module structure of algebraic integers, and indeed almost every theorem on Galois Gauss sums has its module theoretic implications. The original point of view here was mainly global, whereas the actual results on Galois Gauss sums are essentially local ones, properly to be studied in the local context and of independent interest in themselves, besides their direct application to local Hermitian Galois module structure.

One aspect of our theory is the connection with certain other functions of Galois characters – e.g. 'norm resolvents' and the 'characteristic' – to be defined. Indeed we suspect that the formal properties found here apply, *mutatis mutandis*, to a much wider range of arithmetic character functions.

Our second aim is an internal characterization of the $\tau(\chi)$ over a given local field K, without reference to induction, i.e. to transition to extension fields of K. The theorem of Langlands – Deligne essentially describes the $\tau(\chi)$ over K in terms of the $\tau(\chi)$ restricted to Abelian χ over E, E running through all extension fields of K. The computation of the $\tau(\chi)$ thus requires the knowledge of the structure of the E^*, the multiplicative group of E, for all such E. Here we shall in fact prove that the $\tau(\chi)$, for Galois characters χ over K, are uniquely determined by their intrinsic properties in terms of absolute values, ideals, congruences etc., together with the explicit formula for Abelian characters over K only. The interesting aspect of this lies in the treatment of the non-Abelian characters.

We take the Abelian theory for granted, as developed in the classical paper of Davenport & Hasse (1935). Following Stickelberger they gave an internal arithmetic description in the Abelian case and we are doing the same in the non-Abelian one. In fact our congruence theorems are strongly non-Abelian, and are much weaker for Abelian characters. They could of course be supplemented by the Abelian congruence theorems in the Davenport & Hasse paper rather than by the explicit Abelian formulae. Whatever method one adopts the local Galois Gauss sums are uniquely described in terms of the one given field K.

In the original version of this paper we took for granted the existence of inductive Galois Gauss sums, as established by Langlands and Deligne. We realized subsequently that our approach via the arithmetic properties provided a new method of actually producing local Galois Gauss sums and so local root numbers $W(\chi)$ with the required inductive behaviour. This then is our third aim. In this context our approach is different from that outlined in the preceding paragraphs. We now consider all tame Galois characters over all tame extensions of K and extend the classical Gauss sum to non-Abelian characters, the extended function being inductive in degree zero. Unfortunately our proof applies only to tame characters, but as far as these are concerned it is different from either Langlands's or Deligne's. In particular – compared with Deligne's – it is entirely local.

We assume nothing beyond general algebraic number theory, up to and including local class field theory and the theory of Gauss sums of finite fields as presented in the Davenport & Hasse paper. Beyond that our theory is self contained. All required definitions (i.e. conductors etc.) will be stated, and all theorems will in principle be deduced from these. 'In principle' means that we allow ourselves references to the available literature as a guide to the reader of how to derive a stated result from our given definitions.

In §1 we give the basic definitions and state the main theorems. §2 deals with properties of certain auxiliary objects to be introduced. The proofs then follow in §§3–7. In §8 we give an application to the general theory of real valued characters. It was this special case which first led to a study of the constants (Fröhlich & Queyrut 1971; Armitage 1972; and Fröhlich 1974).

Tame local constants have also – in a different context – recently been studied by Macdonald (in preparation), who has established a relation with the representations of finite general linear groups.

Notation

The symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ have the usual meaning: the set of natural numbers, the ring of integers and the fields of rational, real and complex numbers. $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are the ring of p-adic integers and the field of p-adic numbers respectively, and $\overline{\mathbb{Q}}_p$ is a fixed algebraic closure of $\mathbb{Q}_p$. For $r > 0$, $\mathbb{F}_{p^r}$ is the finite field of p^r elements.

If S is a ring, S^* is the multiplicative group of its invertible elements. If Γ is a finite group, $S\Gamma$ is the group ring of Γ over S. For the purposes of this paper a local field k is a field between $\mathbb{Q}_p$ and $\overline{\mathbb{Q}}_p$ which is of finite degree over $\mathbb{Q}_p$. The ring of integers of k is $\mathfrak{O}_k$, the non-zero prime ideal of k is $\mathfrak{p}_k$ and the residue class field of $\mathfrak{O}_k$ is $\tilde{k}(=\mathfrak{O}_k/\mathfrak{p}_k)$.

Further notation will be introduced as it is required.

1. Basic results and statement of main theorems

Let K be a finite extension of $\mathbb{Q}_p$. We consider tame continuous characters α of K^* such that (i) for some $n \in \mathbb{N}$, $\alpha^n = \epsilon$, the identity character of K^*, (ii) the restriction of α to $\mathfrak{O}_K^*$ is lifted from a character of $\tilde{K}^*$; by abuse of notation we shall also call this residue class character α. These characters α of K^* form a multiplicative group $X(K)$.

If $\alpha | \mathfrak{O}_K^*$ is trivial, then α is non-ramified, i.e. α may be viewed as a character of $K^*/\mathfrak{O}_K^*$, and thus of the group of fractional ideals of $\mathfrak{O}_K$. In this case we define the conductor $\mathfrak{f}(\alpha) = \mathfrak{O}_K$, and the Abelian Gauss sum $\tau^{ab}(\alpha)$ to be

$$\tau^{ab}(\alpha) = \alpha(D_K)^{-1}, \tag{1.1.a}$$

where D_K is the different of $K/\mathbb{Q}_p$.

If $\alpha | \mathfrak{O}_K^*$ is non-trivial, then the conductor $\mathfrak{f}(\alpha) = \mathfrak{p}_k$ and the Abelian Gauss sum $\tau^{ab}(\alpha)$ is

$$\tau^{ab}(\alpha) = \sum_u \alpha(uc^{-1})\, \psi_K(uc^{-1}). \tag{1.1.b}$$

Here (i) the sum extends over a set of representatives u of $\tilde{K}^*$ in $\mathfrak{O}_K^*$, (ii) $c \in K$ is chosen such that $c\mathfrak{O}_K = \mathfrak{p}_K D_K$, (iii) ψ_K is the canonical additive character of K given by $\psi_K = \psi_p \circ t_{K/\mathbb{Q}_p}$, where $t_{K/\mathbb{Q}_p}$ is the trace, and ψ_p is the homomorphism of the additive group of $\mathbb{Q}_p$ into $\mathbb{C}^*$ with $\mathbb{Z}_p \subset \ker(\psi_p)$ and $\psi_p(p^s) = e^{2\pi i p^s}$ for $s \in \mathbb{Z}$.

It can easily be verified that $\tau^{ab}(\alpha)$ is independent of the particular choice of c and of choice of representatives u.

Now let N/K be a tame (i.e. at most tamely ramified) normal extension of local fields. We consider representations T of the Galois group $\Gamma = \mathrm{Gal}(N/K)$ over $\mathbb{C}$, and their associated characters χ viewed as functions $\Gamma \to \mathbb{C}$, where $\chi(\gamma) = \mathrm{trace}\,(T(\gamma))$, for all $\gamma \in \Gamma$. The additive group generated by the characters is called the group of virtual characters of Γ and it will be denoted by $R(N/K)$. If L/K is also a tame normal extension with $L \supset N$, then lifting representations of characters from the quotient group $\mathrm{Gal}(N/K)$ of $\mathrm{Gal}(L/K)$ to $\mathrm{Gal}(L/K)$ yields an embedding $R(N/K) \to R(L/K)$, and we denote the direct limit of the $R(N/K)$ by $R(K)$. We shall view $R(K)$ as the union of the $R(N/K)$; its elements are the tame Galois characters over K.

In defining functions on $R(K)$ we have, of course, to be careful to ensure that definitions are independent of choice of extension N.

If in the above $\mathbb{C}$ is replaced by $\overline{\mathbb{Q}}_p$, we analogously get p-adic characters $\chi\colon \Gamma \to \overline{\mathbb{Q}}_p$, and groups $R^{(p)}(N/K)$, $R^{(p)}(K)$. Alternatively we may consider directly the continuous representations T of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ (endowed with the Krull topology) either over $\mathbb{C}$, or, over $\overline{\mathbb{Q}}_p$ (both $\mathbb{C}$ and $\overline{\mathbb{Q}}_p$ being viewed as discrete groups), and where $\ker(T)$ contains the 'first' or 'wild' ramification groups. We then view $R(K)$ and $R^{(p)}(K)$ as the additive groups of the corresponding virtual characters.

An Abelian character $\phi \in R(K)$ is an actual character of degree one. We shall identify such a ϕ with the associated homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K) \to \mathbb{C}^*$. The Abelian characters form a multiplicative group $R(K)^{ab}$.

The Artin map of local class field theory yields an isomorphism

$$A\colon R(K)^{ab} \xrightarrow{\sim} X(K). \tag{1.2}$$

Similarly for p-adic Abelian characters the Artin map yields an isomorphism $R^{(p)}(K)^{ab} \xrightarrow{\sim} X^{(p)}(K)$.

Now let L/K be a tame extension of local fields. Induction of characters yields homomorphisms of additive groups

$$\mathrm{Ind}_K^L\colon\begin{cases}R(L)\to R(K),\\ R(L)^0\to R(K)^0,\end{cases}$$

where $R(K)^0$ is the subgroup of $R(K)$ of virtual characters of degree zero. We have similar homomorphisms for $R^{(p)}(L)$ and $R^{(p)}(L)^0$.

For a given local field k, let R_k (resp. $R_k^{(p)}$) be the union of the groups $R(K)$ (resp. $R^{(p)}(K)$) where K runs through the tame extensions of k of finite degree. In the sequel, K, L, N are always local fields which are tame over k.

THEOREM 1. *There is a function*

$$\tau\colon R_k\to\mathbb{C}^*$$

with the following properties:

(i) *For all K/k, $\tau\colon R(K)\to\mathbb{C}^*$ is a homomorphism of groups, i.e.* $\tau(\chi+\theta)=\tau(\chi)\,\tau(\theta)$.

(ii) *If $\phi\in R(K)^{ab}$ then*

$$\tau(\phi)=\tau^{ab}(A\phi)\quad(\text{cf. }(1.1),\ (1.2)).$$

(iii) *τ is inductive in degree zero, i.e. if $L\supset K$, $\chi\in R(L)^0$, then*

$$\tau(\mathrm{Ind}_K^L\,\chi)=\tau(\chi).$$

$\tau(\chi)$ is called the (local) Galois Gauss sum of χ.

As stated in the introduction, our approach is independent of previous work on non-Abelian local constants, and therefore proofs will be given for all theorems stated in this section, in outline at least.

Later we shall see that theorem 1 is essentially the tame case of the Langlands theorem on the existence of local constants.

Remark. Brauer induction ensures the uniqueness of τ (see Serre 1971, p. 96, exercise 2).

Note now that the values of Galois characters lie in $\overline{\mathbb{Q}}$. Thus $\Omega=\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on characters by $(\chi^\omega)(\gamma)=(\chi(\gamma))^\omega$, for $\chi\in R(K)$, $\gamma\in\mathrm{Gal}\,(\overline{\mathbb{Q}}_p/K)$, $\omega\in\Omega$. Again by (1.1), theorem 1 and Brauer induction we may view τ as a function $R_k\to\overline{\mathbb{Q}}^*$. In order to describe the action of Ω on τ we need the canonical homomorphism $u\colon\Omega\to\mathbb{Z}_p^*$ given by the action of Ω on the p-primary subgroup μ_{p^∞} of μ, the group of roots of unity in $\overline{\mathbb{Q}}$. If $\omega\in\Omega$ and $m\in\mathbb{Z}$ with $u_p(\omega)\cdot m\equiv 1\bmod p^n$, then $(\mathrm{e}^{2\pi i p^{-n}})^\omega=\mathrm{e}^{2\pi i m p^{-n}}$.

Observe that if χ is a Galois character corresponding to a representation T of $\Gamma=\mathrm{Gal}\,(N/K)$, then the map $\gamma\mapsto\mathrm{Det}\,(T(\gamma))=\det_\chi(\gamma)$ defines an Abelian character $\det_\chi$. The map $\chi\mapsto\det_\chi$ extends to a homomorphism of groups

$$\det\colon R(K)\to R(K)^{ab}.$$

Now we have (cf. Fröhlich 1975, theorem 4).

THEOREM 2. *For all $\chi\in R_k$ and for all $\omega\in\Omega$,*

$$\tau(\chi^{\omega^{-1}})^\omega=\tau(\chi)\cdot A\det_\chi(u_p(\omega)).$$

Theorem 2 will be proved in §3.

Now let $\chi\in R(K)$ correspond to a representation $T\colon\Gamma\to GL_m(\mathbb{C})$, where $\Gamma=\mathrm{Gal}\,(N/K)$. Let V be an m-dimensional $\mathbb{C}$ vector space which is viewed as a Γ-module via T. Let $I=I(N/K)$ be the inertia group of Γ. We define the conductor of χ, $\mathfrak{f}(\chi)$, to be

$$\mathfrak{f}(\chi) = \mathfrak{p}_K^{\dim(V)-\dim(V^I)}. \tag{1.3}$$

The norm conductor $N\mathfrak{f}(\chi)$ is the absolute norm of the ideal $\mathfrak{f}(\chi)$, i.e. the order of $\mathfrak{O}_K/\mathfrak{f}(\chi)$. It is clear that the map $\chi \mapsto N\mathfrak{f}(\chi)$ extends, by $\mathbb{Z}$-linearity, to a homomorphism of $R(K)$ into the multiplicative group of positive rationals.

THEOREM 3. (i) *For all* $\chi \in R(K)$, $|\tau(\chi)| = N\mathfrak{f}(\chi)^{\frac{1}{2}}$ (*the positive square root of* $N\mathfrak{f}(\chi)$).
(ii) *If* $\xi \in R(K)^{ab}$ *and if* ξ *is non-ramified* (*i.e. if* $A\xi$ *is non-ramified*), *then for all* $\chi \in R(K)$

$$\tau(\xi\chi) = \tau(\chi)\,\tau(\xi)^{\deg(\chi)}\cdot A\xi(\mathfrak{f}(\chi))^{-1}.$$

Theorem 3 will be proved in §3.

Remark. The definition of $\tau^{ab}(\alpha)$ and theorems 1–3 extend to the wild case. Indeed, given theorem 1, the proofs of theorems 2 and 3 in the general case are the same as for tame characters.

If $z \in \mathbb{C}$, then uniquely we can write

$$z = |z|\,r(z).$$

We define

$$W(\chi) = r(\tau(\bar{\chi})), \tag{1.4}$$

where $\bar{\chi}$ is the complex conjugate of χ. Then we have

COROLLARY. *The maps* $\chi \mapsto N\mathfrak{f}(\chi)^{\frac{1}{2}}$, $\chi \mapsto W(\chi)$ *are additive on* $R(K)$ *and are inductive on* $R(K)^0$.

This corollary, together with the explicit formulae for Abelian characters (theorem 1 (ii)), ensures that $W(\chi)$ coincides with the Langlands constant, as described in Tate's (1977) notes, for Abelian characters and in degree zero, hence generally.

The next three theorems introduce some entirely new properties of the local Galois Gauss sums. Their global analogues are closely related to the theory of global Galois module structure (see Fröhlich 1976).

We first have to introduce the notion of a local resolvent. Let $T: \Gamma \to GL_m(\overline{\mathbb{Q}}_p)$ be a representation of $\Gamma = \mathrm{Gal}\,(N/K)$ with character χ. We extend T to an algebra map from $M_k(\overline{\mathbb{Q}}_p\,\Gamma)$ (the $k \times k$ matrices with entries in $\overline{\mathbb{Q}}_p\,\Gamma$) to the ring $M_{mk}(\overline{\mathbb{Q}}_p)$. The map $g \mapsto \mathrm{Det}\,T(g)$ is a homomorphism $GL_k(\overline{\mathbb{Q}}_p\,\Gamma) \to \overline{\mathbb{Q}}_p^*$ which only depends on the character χ of T and which we denote by Det_χ. This definition extends to virtual characters by $\mathbb{Z}$-linearity. (Note that the restriction of Det_χ to Γ, when $k = 1$, is the p-adic analogue to the homomorphism $\det_\chi: \Gamma \to \mathbb{C}^*$ defined earlier.)

Next we observe that, because N/K is tame, N/K has a normal integral basis, i.e. $\mathfrak{O}_N$ is a free $\mathfrak{O}_K\,\Gamma$-module on one generator. For an outline of the proof of this fact see Noether (1934). Let a be such a generator. For $\chi \in R^{(p)}(N/K)$ the element resolvent $(a|\chi)_{N/K}$ is defined by

$$(a|\chi)_{N/K} = \mathrm{Det}_\chi\,(\sum_{\gamma \in \Gamma} a^\gamma \cdot \gamma^{-1}). \tag{1.5}$$

Let $\overline{U}_p$ be the group of units in the ring of integers of $\overline{\mathbb{Q}}_p$. The quotient group $\overline{\mathbb{Q}}_p^*/\overline{U}_p$ may be viewed as the group of p-adic fractional ideals. We shall show that the fractional ideal

$$P(\chi) = ((a|\chi)_{N/K}) \tag{1.6}$$

is independent of the choice of both a and N. First we observe that any other free generator b of $\mathfrak{O}_N$ over $\mathfrak{O}_K\,\Gamma$ is of the form a^g for $g \in \mathfrak{O}_K\,\Gamma^*$. One verifies immediately from (1.5) that

$$(a^g|\chi)_{N/K} = (a|\chi)_{N/K}\,\mathrm{Det}_\chi\,(g),$$

and clearly $\mathrm{Det}_\chi\,(g) \in \overline{U}_p$.

Now let $L\supset N$ with L/K tame and normal, and let c be a free generator of $\mathfrak{O}_L$ over $\mathfrak{O}_K\Sigma$ (where $\Sigma=\mathrm{Gal}\,(L/K)$). It is easily seen that the trace $t_{L/N}(c)$ is a free generator of $\mathfrak{O}_N$ over $\mathfrak{O}_K\Gamma$ and that

$$(t_{L/N}(c)|\chi)_{N/K}=(c|\chi)_{L/K},$$

for $\chi\in R^{(p)}(N/K)\subset R^{(p)}(L/K)$.

The Galois group $\Omega_p=\mathrm{Gal}\,(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts both on $R^{(p)}(K)$ and also (trivially) on $\overline{\mathbb{Q}}_p^*/\overline{U}_p$. In particular if $\omega\in\mathrm{Gal}\,(\overline{\mathbb{Q}}_p/K)$ then with a and χ as above one verifies that

$$(a|\chi^{\omega^{-1}})^{\omega}_{N/K}=(a|\chi)_{N/L}\,\mathrm{det}_{\chi}\,(\omega),$$

where det_{χ} is now interpreted p-adically. Thus

$$P(\chi^{\omega^{-1}})^{\omega}=P(\chi).$$

Let $\{\sigma\}$ be a right transversal of $\mathrm{Gal}\,(\overline{\mathbb{Q}}_p/K)$ in Ω_p. Then the 'norm' of $P(\chi)$

$$\mathcal{N}_{K/\mathbb{Q}_p}P(\chi)=\prod_{\sigma}P(\chi^{\sigma^{-1}})^{\sigma}=\prod_{\sigma}P(\chi^{\sigma^{-1}}) \tag{1.7}$$

is a well-defined p-adic fractional ideal.

Now let h be a field embedding $\overline{\mathbb{Q}}\hookrightarrow\overline{\mathbb{Q}}_p$ which extends $\mathbb{Q}\hookrightarrow\mathbb{Q}_p$. Then h induces isomorphisms $R(K)\xrightarrow{h}R^{(p)}(K)$, $R_k\xrightarrow{h}R_k^{(p)}$. If $\chi\in R(K)$ then $\tau(\chi)^h\in\overline{\mathbb{Q}}_p^*$ determines a unique p-adic fractional ideal $(\tau(\chi)^h)$. We then have

Theorem 4. (*Local resolvent–Gauss sum theorem*). *For all such embeddings h*

$$(\tau(\chi)^h)=\mathcal{N}_{K/\mathbb{Q}_p}P(\chi^h).$$

Theorem 4 will be proved in §4.

Remark. This is the local analogue of the global, or rather semi-local theorem, which lies at the foundation of the global Galois module structure theory in Fröhlich (1976) (see also Fröhlich's forthcoming book). The global result can also be deduced from our local one and this in fact is the most satisfactory approach.

For subsequent use we have to introduce some notation for congruences in $\overline{\mathbb{Q}}$. Let l be a prime number. We denote the radical of the ideal l in the ring of all algebraic integers by $\mathfrak{L}_l$. The congruence $a\equiv b \bmod l^r\mathfrak{L}_l$ $(r\geqslant 0)$ for algebraic integers a and b means that in any number field F containing a and b, for any prime ideal $\mathfrak{L}$ of F above l, we have a congruence $a\equiv b\bmod l^r\mathfrak{L}$.

Let l again be a prime number. Let $\Gamma=\mathrm{Gal}\,(N/K)$, and define

$$\ker d_{l,\,N/K}=\{\chi\in R(N/K)\,|\,\chi(\gamma)=0\quad\text{if}\quad(\mathrm{order}(\gamma),l)=1\}.$$

In fact $\ker d_{l,\,N/K}$ is the kernel of 'reduction mod l' i.e. of the Brauer decomposition map on the characters of Γ. It is easily verified that if $L\supset N$ with L/K tame and normal then $\ker d_{l,\,N/K}=R(N/K)\cap\ker d_{l,\,L/K}$. The union of the groups $\ker d_{l,\,N/K}$ thus forms a sub-group, $\ker d_l$ say, of $R(K)$ and $\ker d_l\cap R(N/K)=\ker d_{l,\,N/K}$.

After these preparatory remarks we now define a function on Galois characters which we shall call the non-ramified characteristic. This function has been defined previously, for quite different reasons, by Deligne (1973, (5.1)).

Let $\chi\in R(K)$ be irreducible. We put

$$n(\chi)=\chi\quad\text{if}\quad\mathfrak{f}(\chi)=\mathfrak{O}_K,$$

$$n(\chi)=0\quad\text{if}\quad\mathfrak{f}(\chi)\neq\mathfrak{O}_K.$$

By $\mathbb{Z}$-linearity we extend n to an endomorphism of $R(K)$, for every K. This is possible, and is uniquely so, because the irreducible characters are free generators of the Abelian group $R(K)$. $n(\chi)$ is the non-ramified part of χ. Now we put

$$y(\chi) = (-1)^{\deg(n(\chi))} \cdot A\,\mathrm{det}_{n(\chi)}(\mathfrak{p}_K). \tag{1.8}$$

Here $\deg(n(\chi))$ is the degree of $n(\chi)$, and $A\,\mathrm{det}_{n(\chi)}(\mathfrak{p}_K)$ is well-defined as $A\,\mathrm{det}_{n(\chi)}$ is non-ramified. $y(\chi)$ is called the non-ramified characteristic of χ.

Recall that μ is the group of roots of unity in $\overline{\mathbb{Q}}$ and that $\Omega = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

THEOREM 5. (i) *$y \in \mathrm{Hom}_\Omega(R(K), \mu)$ for all K, and $y(\chi) = 1$ if both $\mathrm{det}_{n(\chi)} = \epsilon$ the identity character and* $\deg(n(\chi)) \equiv 0 \bmod (2)$.

(ii) *y is inductive, i.e. for all $L \supset K$ and for all $\phi \in R(L)$,*

$$y(\mathrm{Ind}_K^L \phi) = y(\phi).$$

(iii) If $\chi \in \ker d_l$, *then*

$$y(\chi) \equiv \tau(\chi) \bmod \mathfrak{L}_l.$$

Parts (i) and (ii) of theorem 5 are proved in §2, and part (iii) is proved at the end of §6.

Remark 1. It is property (iii) which is the crucial one. Its global version, a consequence of the local one, again has important consequences in Galois module structure (see Cassou-Noguès 1978; Fröhlich 1976; and also Cassou-Noguès 1979).

Remark 2. In an earlier paper (Fröhlich 1976, §11) one of us had introduced functions y_l on $\ker d_l$, one for each prime l, satisfying a congruence of the type given in (iii). Subsequently Philippe Cassou-Noguès proved as a consequence of a general result in character theory that these y_l could be 'fitted together'. Here we have a direct proof of this result.

For the final result in this group of theorems we introduce the notion of an l-character. Let l again be a prime number. An l-character is a (tame) Galois character which appears as a character of $\mathrm{Gal}(N/K) = \Gamma$ where Γ is a group of l-power order. Note that if $l = p$, then all such characters are necessarily non-ramified. We first state the result for the case when l is odd.

THEOREM 6 (*a*). *Let l be an odd prime number and let χ be an irreducible non-Abelian l-character. Then*

$$\tau(\chi - \mathrm{det}_\chi) \equiv A\,\mathrm{det}_\chi(\deg(\chi))^{-1} \quad \bmod (l).$$

Remark 1. See Taylor's (1977) paper (and also Fröhlich, in preparation) for the consequences in Galois module structure of this congruence.

Remark 2. Theorem 6 (*a*) corresponds to the local root number identity

$$W(\chi) = A\,\mathrm{det}_\chi(\deg(\chi))\, W(\mathrm{det}_\chi)$$

for χ an irreducible, non-Abelian l-character (Taylor 1977).

For $l = 2$ the congruences are more complicated and we have to introduce a number of ancillary functions and discuss various types of 2-character.

First let $p \equiv -1 + 2^{N-1} \bmod (2^N)$, with $N \geqslant 3$. Let B be the set of characters of $\mathbb{F}_{p^2}^*$ of order 2^N. Choose $d \in \mathbb{F}_{p^2}^*$ such that $d \notin \mathbb{F}_p^*$, $d^2 \in \mathbb{F}_p^*$.

For $\beta \in B$ we put

$$\lambda = \lambda(\beta) = \sum_{x \in \mathbb{F}_p} \beta(1 + xd). \tag{1.10}$$

Let η be a primitive 2^N-th root of unity.

Proposition 1. (i) *$\lambda(\beta)$ is independent of the choice of d.*

(ii) *For all such β*

$$\lambda(\beta) \equiv \mathrm{i} \bmod (2(\eta-1)^{-1}),$$

$$\lambda(\beta) \not\equiv \mathrm{i} \bmod (2)$$

i.e.

$$\lambda(\beta) \equiv \mathrm{i}(\eta+1)/(\eta-1) \bmod (2).$$

Moreover the residue class of $\lambda(\beta)$ mod $2(\eta-1)$, and hence mod $2\mathfrak{L}_2$ is independent of β. We denote this residue class by Λ_p.

(iii) *$\lambda(\beta) \in \mathbb{Q}(\eta-\eta^{-1})$ and $\lambda(\beta)\cdot\overline{\lambda(\beta)} = p$.*

Remark. On fixing $\eta = \mathrm{e}^{\pi \mathrm{i}/2^{N-1}}$, we get

$$\mathrm{i}(\eta+1)/(\eta-1) = \cot(\pi/2^N)$$

and so we may choose $\Lambda_p = \pm\cot(\pi/2^N) \bmod 2\mathfrak{L}_2$, with the appropriate choice of sign.

Question. Is there some other arithmetic property of p which allows us to determine Λ_p among the two possible choices given above, i.e. other than by congruences mod $2(\eta-1)$?

We now wish to describe the set of prime divisors $\mathfrak{p}$ of p in $\mathbb{Q}(\eta)$ which divide $\lambda(\beta)$. Let $\pi_\mathfrak{p}$ be a surjection of the ring of integers of $\mathbb{Q}(\eta)$ onto $\mathbb{F}_{p^2}$ with kernel $\mathfrak{p}$. Then for some $s \in \mathbb{Z}$ we have $\pi_\mathfrak{p}\cdot\beta(x) = x^s$ for all $x \in \mathbb{F}^*_{p^2}$. This then determines s uniquely up to the substitution $s \mapsto sp$ (achieved by composing $\pi_\mathfrak{p}$ with the Frobenius of p), and modulo congruences mod (p^2-1). We now choose $0 < s < p^2-1$. Let $\beta \in B$. Clearly s is odd. If we view the $\{\beta\circ\pi_\mathfrak{p}\}$ as automorphisms of $\langle\eta\rangle$ in the natural way, then they are distinct. So by counting we obtain a bijection between primes $\mathfrak{p}|(p)$ and pairs of residue classes s, sp mod $\mathbb{Z}/2^N\mathbb{Z}$, with s odd. For such an s, $\mathfrak{p}_s$ has the obvious meaning.

Put $s = 2m+1$ and write

$$L_s = \sum_{\substack{0<j\leqslant m\\ p-1|j}} \binom{2m+1}{2j}(-1)^j, \tag{1.11}$$

where the $\binom{2m+1}{2j}$ are the usual binomial coefficients.

We consider the set of orbits of $(\mathbb{Z}/2^N\mathbb{Z})^*$ under multiplication by p. In the sequel let S be a set of representatives of these orbits, in the interval $0 < s < p^2-1$. Then we have

Proposition 2. (i) *$(\lambda(\beta)) = \prod'_s \mathfrak{p}_s$, where the product extends over those $s \in S$ with $p|L_s$. This property, together with the congruence $\lambda(\beta) \equiv \Lambda_p \bmod 2\mathfrak{L}_2$ and the equation $\lambda(\beta)\,\overline{\lambda(\beta)} = p$, determines $\lambda(\beta)$ uniquely.*

(ii) *Writing $\lambda(\beta) = a + b(\eta-\eta^{-1})$ with $a, b \in \mathbb{Q}(\eta^2+\eta^{-2})$, we have*

$$a = \Sigma^+\beta(1+xd), \quad b(\eta-\eta^{-1}) = \Sigma^-\beta(1+xd),$$

where Σ^+, Σ^- are summed over the squares, and non-squares respectively among the elements $\{1+xd\}$.

Question. Is every algebraic integer $\lambda \in \mathbb{Q}(\eta-\eta^{-1})$ with the property that $\lambda\bar{\lambda} = p$ and $\lambda \equiv \Lambda_p$ mod $2\mathfrak{L}_2$ of the form $\lambda = \lambda(\beta)$?

We have to introduce a further symbol. For each $N \geqslant 2$ and for all $m \in \mathbb{Z}$ with $m \equiv \pm 1 \bmod (2^N)$, we define a symbol ν_N by

$$\nu_N(m) = \begin{cases} 1 & \text{if} \quad m \equiv \pm 1 \bmod (2^{N+1}), \\ -1 & \text{if} \quad m \equiv \pm 1 + 2^N \bmod (2^{N+1}). \end{cases}$$

ν_N is thus a restricted residue class character.

Now we return to the general situation considered earlier, with $\Gamma = \mathrm{Gal}\,(N/K)$ a 2-group. Le I be the inertia sub-group of Γ. We shall assume Γ to be non-Abelian. We will say that Γ *acts by inversion* on I, if for some $\pi : \Gamma \to \langle \pm 1 \rangle$ we have

$$\gamma^{-1}\sigma\gamma = \sigma^{\pi(\gamma)}$$

for all $\gamma \in \Gamma$ and for all $\sigma \in I$.

If χ is an irreducible non-Abelian 2-character in $R(K)$, then we say that χ is of *inversion type* if χ is in some $R(N/K)$ where $\Gamma = \mathrm{Gal}\,(N/K)$ acts by inversion. Also, if χ is of inversion type then $\deg(\chi) = 2$, and if χ is faithful on Γ then $N\mathfrak{p}_K \equiv -1 \bmod (2^N)$ where 2^N is the order of the inertia group.

Theorem 6 (*b*). *Let χ be an irreducible, non-Abelian 2-character in $R(K)$.*

(i) *If χ is of inversion type, then*

$$\tau(\chi) \equiv \tau(\det_\chi)\, \nu_N(N\mathfrak{p}_K)\, A \det_\chi(\mathfrak{p}_K)^{-1} \bmod 2\mathfrak{L}_2.$$

(ii) *If χ is not of inversion type and $N\mathfrak{p}_K \equiv 1 \bmod (4)$, then*

$$\tau(\chi) \equiv -\tau\,(\det_\chi)\left(\frac{2}{p}\right)^{(\tilde{K}:\mathbb{F}_p)} A \det_\chi(\deg(\chi))^{-1} \bmod 2\mathfrak{L}_2.$$

(iii) *If χ is not of inversion type and $N\mathfrak{p}_K \equiv -1 \bmod (4)$, then*

$$\tau(\chi) \equiv -\tau\,(\det_\chi)\, \Lambda_p^{(K:\mathbb{F}_p)} A \det_\chi(\deg(\chi))^{-1} \bmod 2\mathfrak{L}_2.$$

Theorem 6, parts (*a*) and (*b*), will be proved in § 5.

Finally we give an internal characterization of the homomorphism $\tau : R(k) \to \overline{\mathbb{Q}}^*$, in terms of the properties stated in theorems 2–6 without reference to Galois Gauss sums in extension fields of k, i.e. without reduction to the Abelian case via Brauer induction. The aim is to characterize τ over k purely by arithmetic properties. Indeed one can see fairly easily that the properties of theorems 2–4 already determine τ uniquely modulo a homomorphism $R(k) \to \mu$ commuting with Ω-action. The main object of study is the sub-group of $R(k)$ generated by the irreducible non-Abelian characters, or some other suitable complement in $R(k)$ of the additive sub-group generated by $R(k)^{ab}$. Indeed, although some of our characterizations do extend to $R(k)^{ab}$, the results are much stronger in the non-Abelian case, and anyway, the job for Abelian characters had already been done (Davenport & Hasse 1935, § 4). Accordingly we shall allow here the explicit formulae (1.1) for Abelian characters as part of our description.

Let $S(k)$ be the kernel of $\det : R(k) \to R(k)^{ab}$, i.e. $S(k)$ is the sub-group of virtual characters χ with $\det_\chi = \epsilon$. Clearly $S(k)$, together with $R(k)^{ab}$, generates $R(k)$.

Theorem 7. *The homomorphism $\tau : R(k) \to \overline{\mathbb{Q}}^*$ is the unique homomorphism such that*

(i) *for $\phi \in R(k)^{ab}$, $\tau(\phi) = \tau^{ab}(\phi)$;*

(ii) *the various equations of theorems* 2, 3, 4, 5 (iii) *and* 6, *all hold when their domains of definition are restricted to $S(k)$.*

Remark 1. Theorem 7 remains true if we replace $S(k)$ by the smaller subgroup,

$$\ker(\det) \cap \ker(\deg),$$

of virtual characters with determinant ϵ and degree zero. (The point being that this subgroup is inductive.)

Remark 2. It also suffices to restrict requirement (i) to the values of $\tau(\phi)$, where ϕ runs through the Abelian l-characters for all primes l, and, in (ii), we require theorem 3 (ii) only for Abelian non-ramified l-characters for all primes l.

2. Properties of conductors, resolvents and characteristics

In § 3 we shall give a definition of τ in terms of Abelian characters and a canonical non-ramified induction theorem, for irreducible characters. In order to prove theorems 2, 4 and 5 we must first establish certain basic properties for the functions mentioned in the title of this section.

2 (a). Let $L \supset K$. For the identity character ϵ_L of Gal $(\overline{\mathbb{Q}}_p/L)$, we have $\mathfrak{f}(\epsilon_L) = 1$. If $\chi \in R(L)$ then

$$\mathfrak{f}(\mathrm{Ind}_K^L \chi) = N_{L/K}\,\mathfrak{f}(\chi)\,\mathfrak{d}(L/K)^{\deg(\chi)}.$$

(Here $N_{L/K}$ is the relative norm and $\mathfrak{d}(L/K)$ is the relative discriminant.)

The proof of 2 (a) follows immediately from the definition (1.3) of $\mathfrak{f}(\chi)$, and from the standard formula

$$\mathfrak{d}(L/K) = \mathfrak{p}_K^{f(e-1)},$$

where f and e are the residue class degree, and the ramification index, respectively.

2 (b). If $\phi \in R(K)^{ab}$, then $\mathfrak{f}(\phi) = \mathfrak{f}(A\phi)$.

(This is part of local class field theory.)

In preparation for subsequent use we shall introduce some further notation and recall various results from local class field theory. Let L/K be an extension of local fields, and let N be a normal extension of K which contains L. We put

$$\Gamma = \mathrm{Gal}\,(N/K), \quad \Delta = \mathrm{Gal}\,(N/L). \tag{2.1}$$

We denote by $\rho_{L/K}$ the signature of the permutation representation of Γ on the cosets Γ/Δ. Clearly this only depends on L and K. It is an Abelian character of order 1 or 2, and explicitly

$$\rho_{L/K} = \det{}_{\epsilon_*}, \quad \epsilon_* = \mathrm{Ind}_K^L\,\epsilon_L.$$

Next we denote by $V_{L/K}$ the co-transfer map $V_{L/K}: R^{ab}(L) \to R^{ab}(K)$. From local class field theory we know that the diagram

$$\begin{tikzcd}
R^{ab}(K) \arrow[r, "A"] & X(K) \\
R^{ab}(L) \arrow[u, "V_{L/K}"] \arrow[r, "A"] & X(L) \arrow[u]
\end{tikzcd} \tag{2.2}$$

commutes, where the right hand column is induced by the inclusion map $K^* \hookrightarrow L^*$. Similarly we have a further commutative diagram

$$\begin{tikzcd} R^{ab}(K) \arrow[r, "A"] \arrow[d, "\mathrm{Res}"'] & X(K) \arrow[d, "N_{L/K}"] \\ R^{ab}(L) \arrow[r, "A"] & X(L) \end{tikzcd} \tag{2.3}$$

where the left hand column is character restriction and the right hand column is the co-norm (induced by $N_{L/K}: L^* \rightarrow K^*$).

We now consider the non-ramified characteristic defined in §1.

Theorem 5 (i) is obvious.

Proof of theorem 5 (ii). We keep the notation of (2.1), and we use the following description of $n(\chi)$ (the non-ramified part of χ). Let V be a Γ-module with character χ and let I be the inertia sub-group of Γ. Then $n(\chi)$ is the character of the Γ sub-module of elements of V fixed by I, V^I say.

For the proof of theorem 5 (ii) we may assume χ to be an irreducible character of Δ. In view of the solubility of local Galois groups, by transitivity of induction we may assume that $[L:K] = l$, a prime number.

First if $n(\chi) = 0$, then $(\chi|_{I\cap\Delta}, \epsilon_{I\cap\Delta}) = 0$, and so by Mackey's restriction formula (Serre 1971, 7.1) $(\mathrm{Ind}_\Gamma^\Delta \chi|_I, \epsilon_I) = 0$ hence $n\,(\mathrm{Ind}_\Gamma^\Delta \chi) = 0$, thus

$$y(\chi) = 1 = y\,(\mathrm{Ind}_\Gamma^\Delta \chi).$$

Now we assume $n(\chi) = \chi$, so that, as χ is irreducible, χ must be Abelian.

Suppose, first, that L/K is totally ramified. By Mackey's restriction formula

$$\begin{aligned}(\mathrm{Ind}_\Gamma^\Delta \chi|_I, \epsilon_I) &= (\mathrm{Ind}_I^{I\cap\Delta} \chi|_{I\cap\Delta}, \epsilon_I) \\ &= (\mathrm{Ind}_I^{I\cap\Delta} \epsilon_{I\cap\Delta}, \epsilon_I) = 1.\end{aligned}$$

Thus $n(\mathrm{Ind}_\Gamma^\Delta \chi) = \phi$, an Abelian character which extends χ (by Frobenius reciprocity). As $N_{L/K}\,\mathfrak{p}_L = \mathfrak{p}_K$, by the commutativity of (2.3), $A\phi(\mathfrak{p}_K) = A\chi(\mathfrak{p}_L)$. Because $\deg(\phi) = 1 = \deg(\chi)$, we have now shown that $y(\chi) = y(\mathrm{Ind}_\Gamma^\Delta \chi)$.

Next we take L/K to be non-ramified. Then $n(\mathrm{Ind}_\Gamma^\Delta \chi) = \mathrm{Ind}_\Gamma^\Delta \chi\ (= \chi_*$ say), and $\det_{\chi_*} = \rho_{L/K} \cdot V_{L/K}\,\chi$. As L/K is non-ramified, by the commutativity of (2.2),

$$A \det_{\chi_*}(\mathfrak{p}_K) = A\rho_{L/K}(\mathfrak{p}_K) \cdot A\chi(\mathfrak{p}_L),$$

whence

$$y(\chi_*) = A\chi(\mathfrak{p}_L)\,[A\rho_{L/K}(\mathfrak{p}_K)\,(-1)^l].$$

If $l = 2$, $A\rho_{L/K}$ is quadratic and non-ramified, and hence takes the value -1 on $\mathfrak{p}_K$; while if $l \neq 2$ then $\rho_{L/K} = \epsilon_K$.

In both cases the expression in brackets takes the value -1, and this completes the proof.

Next, we consider resolvents. Global analogues to the results we state here are proved in §§4, 5 and 6 of Fröhlich (1976).

2 (c). With the notation introduced in § 1, preceding theorem 4, for $\chi \in R^{(p)}(L)$

$$\mathscr{N}_{K/\mathbb{Q}_p} P(\mathrm{Ind}_K^L \chi) = \mathscr{N}_{L/\mathbb{Q}_p} P(\chi) \cdot N_{K/\mathbb{Q}_p} \mathfrak{d}(L/K)^{\frac{1}{2}\deg(\chi)}.$$

(To justify the exponent $\frac{1}{2}\deg(\chi)$ recall that we are working in the group of all fractional ideals, i.e. $\overline{\mathbb{Q}}_p^*/\overline{U}_p$, and this group is divisible.)

2 (d). Let $\chi \in R^{(p)}(N/K)$, let $N \supset L \supset K$ with L/K unramified and let χ' be the restriction of χ to Gal (N/L). Then $P(\chi) = P(\chi')$.

As an immediate corollary to 2 (d) we have:

2 (e). Let χ, $\phi \in R^{(p)}(N/K)$. If their restrictions to the inertia subgroup coincide, then $P(\chi) = P(\phi)$.

2 (f). Let $\phi \in R^{(p)}(K)$ be an Abelian character of order prime to p. Suppose that for all $u \in \mathfrak{D}_K^*$

$$A\phi(u) \equiv u^{-(N\mathfrak{p}_K - 1)s} \bmod \mathfrak{p}_K$$

with $0 \leqslant s < 1$, $s \in [1/(N\mathfrak{p}_K - 1)]\,\mathbb{Z}$. Such an s exists as the order of the restriction of $A\phi$ to $\mathfrak{D}_K^*$ divides $N\mathfrak{p}_K - 1$, hence K^* contains the values of $A\phi$ on $\mathfrak{D}_K^*$, and so the map $u \mapsto A\phi(u)$ defines an endomorphism of $(\mathfrak{D}_K/\mathfrak{p}_K)^*$. Clearly s is unique. Then our result is that

$$P(\phi) = \mathfrak{p}_K^s$$

and we recall that in our language a power of $\mathfrak{p}_K$ by a rational exponent makes sense.

Proof of 2 (c). Let $\Gamma = \mathrm{Gal}\,(N/K)$, $\Delta = \mathrm{Gal}\,(L/K)$. We shall show the identity

$$(a|\mathrm{Ind}_K^L \chi) \equiv \prod_{\sigma} (b|\chi^{\sigma^{-1}})^{\sigma} \cdot \mathfrak{d}(L/K)^{\frac{1}{2}\deg(\chi)} \bmod \overline{U}_p \tag{2.4}$$

where a (resp. b) is a free generator of $\mathfrak{D}_N$ over $\mathfrak{D}_K\Gamma$ (resp. $\mathfrak{D}_L\Delta$) and where $\{\sigma\}$ is a right transversal of Δ in Γ. (Applying $\mathscr{N}_{K/\mathbb{Q}_p}$ then yields 2 (c).)

Let $q = (\Gamma : \Delta)$ and let $\{c_i\}_{i=1}^q$ be a basis of $\mathfrak{D}_L$ over $\mathfrak{D}_K$. Let $\{w_i\}$ be a basis of $\mathfrak{D}_N$ over $\mathfrak{D}_K\Delta$ (such a basis exists because $\mathfrak{D}_N$ is $\mathfrak{D}_K\Gamma$ free!). Suppose that $T: \Delta \to GL_n(\overline{\mathbb{Q}}_p)$ is a representation of Δ with character χ. As in § 1 we extend to an algebra homomorphism $T: M_q(\overline{\mathbb{Q}}_p\Delta) \to M_{nq}(\overline{\mathbb{Q}}_p)$.

We denote by w the element of $M_q(\mathbb{Q}_p\Delta)$ whose (σ, i) entry is

$$\sum_{\delta \in \Delta} w_i^{\delta\sigma}\delta^{-1}.$$

Suppose now that we consider a second basis $\{w_i'\}$ of $\mathfrak{D}_N$ over $\mathfrak{D}_K\Delta$, giving rise to a matrix w'. Clearly $w_i' = \Sigma_j w_j \lambda_{ji}$, where $(\lambda_{ji}) \in GL_q(\mathfrak{D}_K\Delta)$, and one checks then that

$$\mathrm{Det}_\chi(w') = \mathrm{Det}_\chi(w)\,\mathrm{Det}_\chi(\lambda_{ij}), \tag{2.5}$$

i.e.

$$\mathrm{Det}_\chi(w') \equiv \mathrm{Det}_\chi(w) \bmod \overline{U}_p.$$

We now make the first of two special choices of $\{w_i\}$. We put $w_i = c_i b$. Then we have

$$\Sigma w_i^{\delta\sigma}\delta^{-1} = c_i^\sigma \Sigma b^{\delta\sigma}\delta^{-1}$$

and so

$$w = \mathrm{diag}\,(\Sigma b^{\delta\sigma}\delta^{-1})_{(\sigma)}(c_i^\sigma)_{(i,\sigma)}.$$

Taking the image under T, and taking determinants, we get

$$\mathrm{Det}_\chi(w) = \mathscr{N}_{L/K}(b|\chi)\,\det(c_i^\sigma)^{\deg(\chi)}.$$

So because $\det(c_i^\sigma)^2\mathfrak{O}_K = \mathfrak{d}(L/K)$, we see that as fractional ideals

$$\mathrm{Det}_\chi(w) = \mathscr{N}_{L/K}(b|\chi)\,\mathfrak{d}(L/K)^{\frac{1}{2}\deg(\chi)}.$$

We now make a second choice of $\{w_i\}$. Namely we set $\{w_i\} = \{a^{\sigma^{-1}}\}$. Then w becomes

$$(\sum_\delta a^{\theta^{-1}\delta\sigma}\,\delta^{-1})_{(\sigma,\,\theta)}.$$

So now by (2.5) it is enough to show that there is a representation $T_*: \Gamma \rightarrow GL_{nq}(\overline{\mathbb{Q}}_p)$ with character $\mathrm{Ind}_K^L\,\chi$, such that $T_*(\Sigma a^\gamma\gamma^{-1}) = T(w)$ (for then $\det(\{a^{\theta^{-1}}\}) = (a|\,\mathrm{Ind}_K^L\,\chi)$ as required).

We may view $\oplus_{r=1}^n\,\overline{\mathbb{Q}}_p$ as a Δ module via T. We then view $\oplus_\sigma\oplus_r\overline{\mathbb{Q}}_p\,\sigma$ as a Γ module in the obvious way. (This module then has character $\mathrm{Ind}_K^L\,\chi$.) Thus it is enough to note that

$$\begin{aligned}\sigma\Sigma a^\gamma\gamma^{-1} &= \Sigma a^{\gamma\sigma}\gamma^{-1}\\ &= \sum_\theta\sum_\delta a^{\theta^{-1}}\delta^{-1}\theta.\end{aligned}$$

Proof of 2 (d). With the same notation as above we are required to prove

$$(a|\chi) \equiv (b|\chi|_\Delta) \bmod \overline{U}_p. \tag{2.6}$$

Consider the ring of Δ maps from Γ to $\mathfrak{O}_N$, $\mathrm{Map}_\Delta(\Gamma, \mathfrak{O}_N)$. This is a Γ-module by stipulating that $g^\gamma(\gamma') = g(\gamma\gamma')$, for $g \in \mathrm{Map}_\Delta(\Gamma, \mathfrak{O}_N)$, $\gamma, \gamma' \in \Gamma$.

The algebra $\mathfrak{O}_N \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$ is an $\mathfrak{O}_L$ Γ-module, where Γ acts on the first factor and $\mathfrak{O}_L$ on the second. We have a homomorphism of rings and Γ-modules

$$\eta: \mathfrak{O}_N \otimes \mathfrak{O}_L \rightarrow \mathrm{Map}_\Delta(\Gamma, \mathfrak{O}_N)$$

given by $\eta(\Sigma x \otimes y)\ (\gamma) = \Sigma x^\gamma y$. We see that η is given by restricting the algebra isomorphism

$$N \otimes_K L \cong \mathrm{Map}_\Delta(\Gamma, N).$$

Thus in the first place η is injective. Moreover, L/K being non-ramified, $\mathfrak{O}_N \otimes \mathfrak{O}_L$ is a maximal order. Thus, its image under η is a maximal order contained in the order $\mathrm{Map}_\Delta(\Gamma, \mathfrak{O}_N)$. In other words η is surjective and so is an isomorphism.

We now make $\mathrm{Map}_\Delta(\Gamma, \mathfrak{O}_N)$ into an $\mathfrak{O}_L$-module via η (through multiplication on the second factor of $\mathfrak{O}_N \otimes \mathfrak{O}_L$). This preserves the Γ-structure of $\mathrm{Map}_\Delta(\Gamma, \mathfrak{O}_N)$, so that it is now an $\mathfrak{O}_L$ Γ-module.

We have our injection of $\mathfrak{O}_L$ Γ-modules ξ: $\mathrm{Map}_\Delta(\Gamma, \mathfrak{O}_N) \hookrightarrow \mathfrak{O}_N\Gamma$ given by $\xi(g) = \Sigma g(\gamma)\,\gamma^{-1}$.

Consider $f_b \in \mathrm{Map}_\Delta(\Gamma, \mathfrak{O}_N)$ defined by

$$f_b(\gamma) = \begin{cases} b^\gamma & \text{if} \quad \gamma \in \Delta,\\ 0 & \text{if} \quad \gamma \notin \Delta.\end{cases}$$

Then f_b is seen to be a free generator of $\mathrm{Map}_\Delta(\Gamma, \mathfrak{O}_N)$ over $\mathfrak{O}_L\Gamma$. Thus for some $\lambda \in \mathfrak{O}_L\Gamma^*$, as $\eta(a \otimes 1)$ is also a free generator,

$$\eta(a \otimes 1)\cdot\lambda = f_b,$$

so taking images under ξ

$$(\sum_{\gamma\in\Gamma} a^\gamma\gamma^{-1})\,\lambda = \sum_{\delta\in\Delta} b^\delta\delta^{-1}.$$

(2.6) now follows on applying Det_χ to both sides, since $\mathrm{Det}_\chi(\lambda) \in \overline{U}_p$.

Proof of 2 (*d*). The proof falls into two parts. We first assume that K contains the values of ϕ and establish the result under this hypothesis. Then we reduce from the general case to this special case.

So suppose K contains all the nth roots of unity, where ϕ is of order n. Thus ϕ is faithful of order n on Gal (N/K) for some Kummer extension N of K, and the elements $x \in K$ with $x^{\gamma} = x\phi(\gamma)$ for all $\gamma \in \mathrm{Gal}\,(N/K)$ form a one-dimensional K-subspace N_{ϕ} of N. By linearity, extend the surjective homomorphism v: $K^* \to \mathbb{Z}$ given by valuation to a homomorphism v: $N^* \to \mathbb{Q}$, which is trivial on $\mathfrak{O}_N^*$. It is clear that the values of v on $N^* \cap N_{\phi} = N_{\phi}^*$ form a coset in $\mathbb{Q} \bmod \mathbb{Z}$. Let s be the least non-negative one of these values (so that $0 \leqslant s < 1$). Observe then that the $\mathfrak{O}_K$-module $\mathfrak{O}_N \cap N_{\phi}$ is free of rank one, and an element $x \in N_{\phi}^*$ is a generator precisely when $v(x) = s$.

Now let a be a free generator of $\mathfrak{O}_N$ over $\mathfrak{O}_K$ Gal (N/K). Then indeed $(a|\chi)$ is a free generator of $\mathfrak{O}_N \cap N_{\phi}$ over $\mathfrak{O}_K$. Hence $v(a|\chi) = s$, i.e.

$$P(\phi) = \mathfrak{p}_K^s. \tag{2.7}$$

We now have to show that s satisfies the given congruence conditions. For this we have to use the properties of the local norm residue symbol. In the sequel we denote the Artin map onto Galois groups of Abelian extensions by A. Let u be a unit of $\mathfrak{O}_K$ and let x be a generator of $N_{\phi} \cap \mathfrak{O}_N$. Then $x^n = \pi^r w$, where π is a given element of K with $\pi\mathfrak{O}_K = \mathfrak{p}_K$ and w a unit. This implies that $r = ns$. Writing $\sqrt[n]{u} = y$, we have

$$\begin{aligned} A\phi(u) &= x^{A(u)}x^{-1} = \left(\frac{\pi^r w, u}{\mathfrak{p}}\right)_n \quad (\text{definition of } (-)_n) \\ &= \left(\frac{\pi, u}{\mathfrak{p}}\right)_n^r \quad \left(\text{multiplicativity and } \left(\frac{w, u}{\mathfrak{p}}\right)_n = 1\right) \\ &= \left(\frac{u, \pi}{\mathfrak{p}}\right)_n^{-r} \quad (\text{skew-symmetry}) \\ &= (y^{A(\pi)}y^{-1})^{-r} \quad (\text{definition}) \\ &\equiv y^{-r(N\mathfrak{p}_K-1)} \bmod \mathfrak{p}_K \quad (\text{as } A(\pi) \text{ is a Frobenius}) \\ &\equiv u^{-s(N\mathfrak{p}_K-1)} \bmod \mathfrak{p}_K \quad (\text{as } r = ns). \end{aligned}$$

This then establishes the result in the Kummer case.

In the general case let $L = K(\phi)$ be the field obtained from K by adjoining the values of ϕ, and suppose that

$$A\phi(u) \equiv u^{-(N\mathfrak{p}_K-1)s} \bmod \mathfrak{p}_K$$

for all $u \in \mathfrak{O}_K^*$, with $0 \leqslant s < 1$. Trivially L contains the values of Res ϕ, the restriction of ϕ to Galois groups over L. But by the commutativity of (2.3)

$$A\,\mathrm{Res}\,\phi(u) = A\phi(N_{L/K}\,u)$$

for $u \in L^*$, and as L/K is non-ramified

$$N_{L/K}(u) \equiv u^{(N\mathfrak{p}_L-1)/(N\mathfrak{p}_K-1)} \bmod \mathfrak{p}_L.$$

Therefore $$A\,\mathrm{Res}\,\phi(u) \equiv u^{-(N\mathfrak{p}_L-1)\,s} \bmod \mathfrak{p}_L.$$

So that, as we are now in the Kummer case,

$$P\,(\mathrm{Res}\,\phi) = \mathfrak{p}_L^s.$$

Again as L/K is non-ramified we have in the first place that $\mathfrak{p}_L = \mathfrak{p}_K$, and in the second place, by 2 (d), that $P(\phi) = P(\operatorname{Res}\phi)$. Thus indeed

$$P(\phi) = \mathfrak{p}_K^s.$$

3. Definition of τ and immediate consequences

Throughout this section we consider a fixed tame, normal extension N/K with Galois group Γ and with inertia group I. Thus Γ/I and I are both cyclic.

3 (a). (i) One knows (for instance by an easy generalization of 8.2 in Serre (1971)) that if χ is an irreducible character of Γ, then there exists a subgroup Σ of Γ, $\Sigma \supset I$, and an Abelian character ϕ of Σ such that χ is induced from ϕ, i.e. $\chi = \operatorname{Ind}_\Gamma^\Sigma \phi$. χ determines Σ uniquely and determines ϕ uniquely to within the substitution $\phi \mapsto {}^\gamma\phi$, for $\gamma \in \Gamma$, where ${}^\gamma\phi(\delta) = \phi(\gamma^{-1}\delta\gamma)$.

(ii) By Mackey's irreducibility criterion (Serre 1971, 7.4), if Δ is a normal subgroup of Γ and if ϕ is an Abelian character of Δ, then $\operatorname{Ind}_\Gamma^\Delta \phi$ is irreducible if, and only if, ${}^{\gamma_1}\phi = {}^{\gamma_2}\phi$ implies $\gamma_1 \equiv \gamma_2$ mod Δ, for $\gamma_i \in \Gamma$ (i.e. if, and only if, Δ is the stabilizer of ϕ).

With χ a given irreducible character of Γ, we let $L = N^\Sigma$ be the fixed field of the sub-group Σ associated to χ by 3 (a) (i); so that $\chi = \operatorname{Ind}_K^L(\phi)$, $\phi \in R^{ab}(N/L)$. We now define

$$\tau(\chi) = \tau_{N/K}(\chi) = \tau^{ab}(A\phi)\, A\rho_{L/K}(D_K). \tag{3.1}$$

Note that $\rho_{L/K} = \rho_{L/K}^{-1}$, since it has order two. Here $\rho_{L/K} = \det \epsilon_*$, $\epsilon_* = \operatorname{Ind}_K^L \epsilon_L$. (Note that as $\Sigma \supset I$, L/K is non-ramified and hence $\rho_{L/K}$ is non-ramified.) We have, of course, to verify first that $\tau^{ab}(A\phi) = \tau^{ab}(A{}^\gamma\phi)$. This is immediate because $A{}^\gamma\phi(x) = A\phi(x^\gamma)$ for $x \in L^*$, while on the other hand the additive character ψ_L is Γ-invariant, i.e. $\psi_L(x^\gamma) = \psi_L(x)$. (Now use the definition of τ^{ab} given in (1.1).) Secondly we have to verify that if $N' \supset N$ with N'/K tame and normal, then indeed $\tau_{N'/K}(\chi) = \tau_{N/K}(\chi)$. This is obvious.

We now extend the definition of τ to all of $R(N/K)$ by additivity; so that for $\chi, \theta \in R(N/K)$

$$\tau(\chi + \theta) = \tau(\chi) \cdot \tau(\theta). \tag{3.2}$$

Our logical procedure is then as follows. We prove theorems 2–4 (in §§ 3 and 4) directly from our definitions. We also establish part of the inductivity of τ (parts (i) and (ii) of theorem 1 already being obvious from our definitions). We use this to derive a weak version of theorem 5 (iii), the remainder of theorem 5 having been already established in § 2. In § 5 we prove theorem 6. Then in § 6 we complete the proofs of inductivity for τ and of theorem 5. Finally, § 7 contains the proof of theorem 7 (the uniqueness theorem).

We now describe certain results for Abelian Gauss sums which were established by Davenport & Hasse (1935). We shall then interpret these results in terms of τ^{ab}.

Let K be a local field, and let $\psi_{\tilde{K}}$ be the canonical additive character of the residue class field $\tilde{K}$ given by

$$\psi_{\tilde{K}}(x) = \exp\{2\pi i \operatorname{tr}_{\tilde{K}}(x)/p\}.$$

Let $\alpha \in X(K)$. As remarked previously α defines a character of $\tilde{K}^*$ which we also denote by α. We put

$$G(\alpha) = \begin{cases} -\sum\limits_{x \in \tilde{K}^*} \alpha(x)\, \psi_{\tilde{K}}(x) & \text{if } \alpha \text{ is ramified,} \\ \quad 1 & \text{if } \alpha \text{ is non-ramified.} \end{cases} \tag{3.3}$$

Let $\tilde{F}/\tilde{K}$ be an extension of finite fields. Then $\alpha \circ N_{\tilde{F}/\tilde{K}}$ defines a character of $\tilde{F}^*$. From (0.8) of Davenport & Hasse (1935) we have

$$G(\alpha \circ N_{\tilde{F}/\tilde{K}}) = G(\alpha)^{[\tilde{F}:\tilde{K}]}. \tag{3.4}$$

Let β also be an Abelian character of $\tilde{K}^*$, with order m. Then from (0.9_1) of Davenport & Hasse

$$\prod_{i=1}^{m} G(\alpha\beta^i) = \alpha^m(m^{-1})\, G(\alpha^m) \prod_{i=1}^{m} G(\beta^i). \tag{3.5}$$

We now interpret G and (3.4) and (3.5) in terms of τ^{ab}. Let M be the maximal non-ramified extension of $\mathbb{Q}_p$ contained in K. Let $\alpha \in X(K)$ be ramified. By (1.1)

$$\tau^{ab}(\alpha) = \Sigma\alpha(uc^{-1})\, \psi_K(uc^{-1}),$$

where u is summed through a set of representatives of $\mathfrak{O}_M^* \operatorname{mod} \mathfrak{p}_M$. Thus $\psi_K(uc^{-1}) = \psi_M(u \operatorname{tr}_{K/M}(c^{-1}))$, and because

$$\operatorname{tr}_{K/M}(D_K^{-1}\mathfrak{p}_K^{-1}) = D_M^{-1}\mathfrak{p}_M^{-1} = p^{-1}\mathfrak{O}_M$$

we can, without loss of generality, assume $\operatorname{tr}_{K/M}(c^{-1}) = p^{-1}$.

So now we have shown that for ramified $\alpha \in X(K)$

$$\tau^{ab}(\alpha) = -\alpha(c^{-1})\, G(\alpha), \tag{3.6}$$

where c is chosen such that both $c\mathfrak{O}_K = \mathfrak{p}_K D_K$ and $\operatorname{tr}_{K/M}(c^{-1}) = p^{-1}$.

Now let L/K be an non-ramified extension of local fields. Let c be as in (3.6); then $c\mathfrak{O}_L = \mathfrak{p}_K D_K \mathfrak{O}_L = \mathfrak{p}_L D_L$. So, for ramified $\alpha \in X(K)$, as for (3.6) we have

$$\begin{aligned} \tau^{ab}(\alpha \circ N_{L/K}) &= -\alpha \circ N_{L/K}(c^{-1})\, G(\alpha \circ N_{L/K}) && \text{by (3.4)} \\ &= -(\alpha(c^{-1})\, G(\alpha))^{(L:K)} \end{aligned}$$

so that

$$\tau^{ab}(\alpha \circ N_{L/K}) = \tau^{ab}(\alpha)^{(L:K)} \cdot (-1)^{(L:K)+1}. \tag{3.7}$$

Let $\beta \in X(K)$ have order m, and assume that in fact β has order m on $\tilde{K}^*$. Let $\alpha \in X(K)$ and assume that α^m is ramified. Then for each integer i

$$\tau^{ab}(\alpha\beta^i) = -\alpha\beta^i(c^{-1})\, G(\alpha\beta^i)$$

so by (3.5)

$$\begin{aligned} \prod_{i=1}^{m} \tau^{ab}(\alpha\beta^i) &= \prod_{i=1}^{m} -\alpha\beta^i(c^{-1})\, G(\alpha\beta^i) \\ &= \alpha^m(m^{-1})\, \alpha^m(c^{-1})\, G(\alpha^m) \prod_i (-G(\beta^i)\, \beta^i(c^{-1})). \end{aligned}$$

But β^i is genuinely ramified for all such i except $i = m$ when $G(\beta^m) = 1 = \tau^{ab}(\beta^m)$, and so we have

$$\prod_{i=1}^{m} \tau^{ab}(\alpha\beta^i) = \alpha^m(m^{-1})\, \tau^{ab}(\alpha^m) \prod_{i=1}^{m} \tau^{ab}(\beta^i). \tag{3.8}$$

Proof of theorem 3 (i). Throughout χ and ϕ are as in (3.1). It will clearly suffice to establish the theorem for irreducible such χ, as both $|\tau(\chi)|$ and $N\mathfrak{f}(\chi)^{\frac{1}{2}}$ are additive in χ. The proof that for $\alpha \in X(L)$

$$|\tau^{ab}(\alpha)| = |G(\alpha)| = N\mathfrak{f}(\alpha)^{\frac{1}{2}}$$

is classical and will not be repeated (see (0.4) in Davenport & Hasse).

Now use 2 (*a*) and 2 (*b*) to deduce that $N\mathfrak{f}(\chi)^{\frac{1}{2}} = N\mathfrak{f}(A\phi)^{\frac{1}{2}}$ (note that $\mathfrak{d}(L/K) = \mathfrak{O}_K$).

Proof of theorem 3 (ii). Again by additivity in χ, we assume that χ is an irreducible character. Now $\chi = \mathrm{Ind}_{\Gamma}^{\Sigma}(\phi)$. So by Frobenius reciprocity $\xi\chi = \mathrm{Ind}_{\Gamma}^{\Sigma}(\phi\xi|_{\Sigma})$ and $\xi\chi$ is irreducible. From (3.1)

$$\tau(\chi) = \tau^{ab}(A\phi)\, A\rho_{L/K}(D_K),$$
$$\tau(\xi\chi) = \tau^{ab}(A(\phi\xi|_{\Sigma}))\, A\rho_{L/K}(D_K).$$

It follows immediately from (1.1) that

$$\tau^{ab}(\phi\xi|_{\Sigma}) = \begin{cases} \tau^{ab}(A\phi)\, \tau^{ab}(A\xi|_{\Sigma}) & \text{if } \phi \text{ non-ramified,} \\ \tau^{ab}(A\phi)\, \tau^{ab}(A\xi|_{\Sigma})\, A\xi|_{\Sigma}\,(\mathfrak{p}_L^{-1}) & \text{otherwise.} \end{cases}$$

But by the commutativity of (2.3) $A\xi|_{\Sigma} = (A\xi) \circ N_{L/K}$. Thus

$$\tau^{ab}(A\xi|_{\Sigma}) = \xi(D_K)^{-(L:K)} = \tau^{ab}(\xi)^{\deg(\chi)}$$

and if ϕ is ramified $\qquad A\xi|_{\Sigma}(\mathfrak{p}_L) = \xi(\mathfrak{p}_K)^{(L:K)} = \xi(\mathfrak{f}(\chi)).$

Theorem 3 (ii) is now shown.

Proof of theorem 2. One shows first that for $x \in L$, $\omega \in \Omega$, we have $\psi_L(x)^{\omega} = \psi_L(x \cdot u_p\, \omega^{-1})$. It follows that, for $\alpha \in X(L)$ and ramified, by (1.1)

$$\begin{aligned} \tau^{ab}(\alpha^{\omega^{-1}})^{\omega} &= \Sigma\alpha(uc^{-1})\, \psi_L(u \cdot c^{-1} \cdot u_p\, \omega^{-1}), \\ &= \alpha(u_p\, \omega)\, \Sigma\alpha(u \cdot c^{-1} \cdot u_p\, \omega^{-1})\, \psi_L(u \cdot c^{-1} \cdot u_p\, \omega^{-1}), \\ &= \alpha(u_p\, \omega)\, \tau^{ab}(\alpha). \end{aligned}$$

While if α is non-ramified

$$\tau^{ab}(\alpha^{\omega^{-1}})^{\omega} = \alpha(D_K)^{-1} = \tau^{ab}(\alpha) = \tau^{ab}(\alpha)\, \alpha(u_p\, \omega).$$

By additivity it is enough to prove theorem 2 for irreducible $\chi = \mathrm{Ind}_K^L\, \phi$. Because $(A\phi)^{\omega^{-1}} = A(\phi^{\omega^{-1}})$, from (3.1) (by observing that $\rho_{L/K}$ takes values in ± 1)

$$\begin{aligned} \tau(\chi^{\omega^{-1}})^{\omega} &= \tau^{ab}(A\phi^{\omega^{-1}})^{\omega} \rho_{L/K}(D_K) \\ &= \tau^{ab}(A\phi) \cdot A\phi(u_p\, \omega) \cdot \rho_{L/K}(D_K) \quad \text{by the above} \\ &= \tau(\chi)\, A\phi(u_p\, \omega). \end{aligned}$$

Now $\det_{\chi} = V_{L/K}\, \phi \cdot \rho_{L/K}$, thus

$$(A \det_{\chi})\,(u_p\, \omega) = (AV_{L/K}\, \phi)\,(u_p\, \omega)\, \rho_{L/K}(u_p\, \omega).$$

But by (2.2) $(AV_{L/K}\, \phi)(u_p\, \omega) = A\phi(u_p\, \omega)$, and $\rho_{L/K}(u_p\, \omega) = 1$ because $\rho_{L/K}$ is non-ramified. Hence the result.

3 (*b*). If F is a non-ramified extension of K, and $\chi \in R(F)$, then

$$\tau\,(\mathrm{Ind}_K^F\, \chi) = A\rho_{F/K}(D_K)^{\deg(\chi)} \cdot \tau(\chi).$$

In particular τ is inductive for non-ramified extensions and degree zero virtual characters.

Proof. Without loss of generality we may assume that $F \subset N$, $F = N^{\Delta}$ with $\Delta \supset I$. For any $G \supset F$ we have the formula

$$A\rho_{F/K}(D_K)^{\deg(\chi)[G:F]} A\rho_{G/F}(D_F)^{\deg(\chi)} = A\rho_{G/K}(D_K)^{\deg(\chi)}.$$

This is a special case of the formula for the determinant of an induced character, which gives $\rho_{G/K} = \rho_{F/K}^{[G:F]} V\rho_{G/F}$. So by transitivity of induction we may suppose that $[K:F] = l$, a prime number. Also, by additivity, we suppose that χ is an irreducible character of Δ. We have

$$\chi = \operatorname{Ind}_F^E \phi, \tag{3.9}$$

where $E = N^{\Omega}, I \subset \Omega \subset \Delta$ and $\phi \in R^{ab}(N/E)$. We put $\xi = \operatorname{Ind}_K^E \phi$, and we let Σ be the stabilizer of ϕ in Γ, i.e. $\Sigma = \{\gamma \in \Gamma | {}^{\gamma}\phi = \phi\}$. Let $L = N^{\Sigma}$. Clearly $\Sigma \cap \Delta = \Omega$.

Case 1. $\Sigma = \Omega$. Then by 3 (*a*) ξ is irreducible, and so, by our definition of τ, we must show that

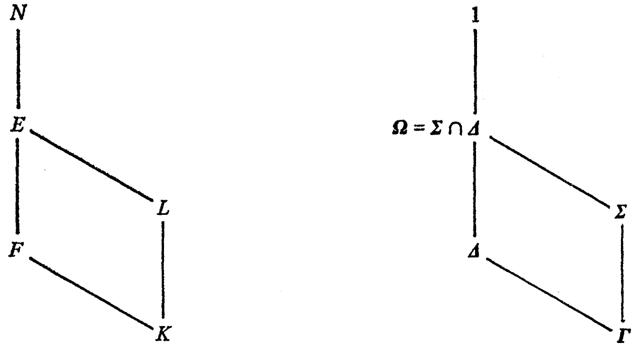
$$\tau^{ab}(A\phi)\, A\rho_{L/K}(D_K) = A\rho_{F/K}(D_K)^{[L:F]}\cdot A\rho_{L/F}(D_F)\,\tau^{ab}(A\phi).$$

Note that $D_F = D_K\,\mathfrak{D}_F$. The above equation then follows from (2.2) and the identity

$$V_{F/K}\,\rho_{L/F}\cdot\rho_{F/K}^{[L:F]} = \rho_{L/K} \tag{3.10}$$

which is a special case of the equation for the determinant of an induced character.

Case 2. $\Sigma \neq \Omega$ (i.e. $\Delta\Sigma = \Gamma$). We have the following diagrams of fields and their Galois groups:



In view of the definition of Σ, and the fact that $(E:L) = l$, the Abelian character ϕ of Ω has l distinct extensions $\{\phi_i\}_{i=1}^{l}$ to Σ. If $\{\theta_i\}$ are the distinct Abelian characters of Σ/Ω inflated to Σ, then we can write $\phi_i = \phi_1\,\theta_i$. We have

$$\operatorname{Ind}_L^E \phi = \sum_{i=1}^{l} \phi_i. \tag{3.11}$$

Moreover Σ is the stabilizer of each ϕ_i in Γ, so that by 3 (*a*) the $\operatorname{Ind}_K^L \phi_i$ are all irreducible. So

$$\xi = \operatorname{Ind}_K^F \chi = \sum_{i=1}^{l} \operatorname{Ind}_K^L \phi_i$$

and hence
$$\tau(\xi) = A\rho_{L/K}(D_K)^l \prod_i \tau^{ab}(A\phi_i).$$

Using (3.10) and its analogue for the tower of fields $E \supset F \supset K$, we see that we have to prove the equation

$$\tau(\phi) = \prod_i \tau^{ab}(A\phi_1\,\theta_i)\cdot A\rho_{E/L}(D_L). \tag{3.12}$$

If ϕ *is non-ramified* then $\tau(\phi) = A\phi(D_E)^{-1} = AV_{L/E}\,\phi(D_L)^{-1}$ (by (2.2)) and so

$$\prod_i \tau^{ab}(A\phi_1\,\theta_i) = \prod_i A\phi_1\,\theta_i(D_L)^{-1} = \det_{\phi_*}(D_L)^{-1},$$

where $\phi_* = \operatorname{Ind}_L^E \phi$. Hence (3.12) follows by the formula for the determinant of an induced character.

If ϕ is ramified, then because the θ_i are non-ramified, by theorem 3 (ii),

$$\tau^{ab}(A\phi_1\,\theta_i) = \tau^{ab}(A\phi_1)\,A\theta_i(\mathfrak{p}_L D_L)^{-1}.$$

Now $\mathrm{Ind}_L^E\,\epsilon_E = \Sigma_i\,\theta_i$; so by taking determinants, $\Pi_i\,\theta_i = \rho_{E/L}$. The right hand side in (3.12) is now $\tau^{ab}(A\phi_1)^l A\rho_{E/L}(\mathfrak{p}_L)$, and of course $A\rho_{E/L}(\mathfrak{p}_L) = (-1)^{l+1}$.

On the other hand, $\phi_1|_\Omega = \phi$; so by the commutativity of (2.3), $A\phi = A\phi_1 \circ N_{E/L}$. Hence, we are required to show

$$\tau^{ab}(A\phi_1 \circ N_{E/L}) = (-1)^{1+[E:L]}\tau^{ab}(A\phi_1)^{(E:L)},$$

which is a particular case of the identity (3.7).

We denote by $H_l(N/K)$ the subgroup of $R(N/K)$ which is generated by virtual characters of Γ of the form $\mathrm{Ind}_\Gamma^\Sigma(\phi_1-\phi_2)$ where $\Sigma \supset I$ and ϕ_1, ϕ_2 are Abelian with $\phi_1-\phi_2 \in \ker d_l$. Clearly $H_l(N/K) \subset \ker d_l$. We shall now derive a weak form of theorem 5 (iii), namely

3 (c). If $\chi \in H_l(N/K)$, then

$$\tau(\chi) \equiv y(\chi) \bmod \mathfrak{L}_l.$$

Proof. One sees easily that $H_l(N/K)$ is in fact generated by virtual characters $\mathrm{Ind}_\Gamma^\Sigma(\phi-\phi')$, where ϕ, ϕ' are Abelian, where ϕ' has order prime to l and $\phi^{-1}\phi'$ has l-power order. By theorem 5 (ii) and 3 (b), it suffices to prove 3 (c) under hypothesis that $\Sigma = \Gamma$, i.e. that $\chi = \phi-\phi'$ (with ϕ, ϕ' as above).

Note that always $A\phi(x) \equiv A\phi'(x) \bmod \mathfrak{L}_l$. If first ϕ', and hence ϕ, is genuinely ramified, then it follows immediately that

$$\tau(\phi) \equiv \tau(\phi') \bmod \mathfrak{L}_l, \quad y(\phi-\phi') = 1.$$

If $l \neq p$, then $\tau(\phi)$ and $\tau(\phi')$ are units at $\mathfrak{L}_l$, and hence $\tau(\phi-\phi') \equiv 1 \bmod \mathfrak{L}_l$. On the other hand, if $p = l$ then $\phi^{-1}\phi'$ is non-ramified, hence $\tau(\phi) = A\phi^{-1}\phi'(D_K\mathfrak{p}_K)\,\tau(\phi')$, and so again we have $\tau(\phi-\phi') \equiv 1 = y(\phi-\phi')$.

Next if both ϕ and ϕ' are non-ramified, then

$$\tau(\phi-\phi') = A\phi(D_K)^{-1}A\phi'(D_K) \equiv 1 \bmod \mathfrak{L}_l,$$

while
$$y(\phi-\phi') = A\phi(\mathfrak{p}_K)\,A\phi'(\mathfrak{p}_K)^{-1} \equiv 1 \bmod \mathfrak{L}_l.$$

Finally, if ϕ' is non-ramified, but ϕ genuinely ramified, then writing $A\phi = \alpha$, $A\phi' = \alpha'$, $\alpha = \alpha'\alpha''$ (so that α'' has l-power order) we get

$$\begin{aligned}\tau(\phi) &= \alpha(c)^{-1}\Sigma\alpha''(u)\,\psi_K(c^{-1}u)\\ &\equiv \alpha'(c)^{-1}\Sigma\psi_K(c^{-1}u) \bmod \mathfrak{L}_l\\ &\equiv -\alpha'(c^{-1}) = -A\phi'(\mathfrak{p}_K)^{-1}\tau(\phi') \bmod \mathfrak{L}_l\\ &\equiv y(\phi-\phi')\,\tau(\phi') \bmod \mathfrak{L}_l.\end{aligned}$$

Here we have used the fact that $x \mapsto \psi_K(c^{-1}x)$ is a non-trivial character on the additive group $\mathfrak{O}_K/\mathfrak{p}_K$; whence

$$0 = \psi_K(c^{-1}\cdot 0) + \Sigma\psi_K(c^{-1}u) = 1 + \Sigma\psi_K(c^{-1}u).$$

Now we observe that in this situation we must have $l \neq p$, so that $\tau(\phi)$ and $\tau(\phi')$ are units at $\mathfrak{L}_l$, and it follows then that

$$\tau(\phi-\phi') \equiv y(\phi-\phi') \bmod \mathfrak{L}_l.$$

4. Proof of theorem 4

To begin with the notation is the same as that of § 3. Let h be an embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$. Because both $\mathcal{N}_{K/\mathbb{Q}_p} P(\chi^h)$ and $(\tau(\chi)^h)$ are additive in χ, we may assume that χ is irreducible where, as in 3 (a), $\chi = \mathrm{Ind}_K^L \phi$, $\phi \in R^{ab}(N/L)$, $L = N^{\Sigma}$, $I \subset \Sigma$.

By (3.1) $(\tau(\chi)^h) = (\tau(\phi)^h)$, and by 2 ($c$) $\mathcal{N}_{K/\mathbb{Q}_p}(P(\chi^h)) = \mathcal{N}_{L/\mathbb{Q}_p}(P(\phi^h))$. We may thus assume that $\chi = \phi \in R^{ab}(N/K)$.

Now write $\phi = \phi_1 \phi_2$, where ϕ_1 has order prime to p and ϕ_2 has p-power order. Because N/K is tame, ϕ_2 must be non-ramified. Hence by theorem 3 (ii) $(\tau(\phi_1 \phi_2)^h) = (\tau(\phi_1)^h)$. On the other hand, by 2 (e), $\mathcal{N}_{K/\mathbb{Q}_p} P(\phi_1 \phi_2) = \mathcal{N}_{K/\mathbb{Q}_p} P(\phi_1)$. We may now assume that $\phi = \phi_1$ is of order prime to p.

To evaluate $\mathcal{N}_{K/\mathbb{Q}_p} P(\phi^h)$, let M be the maximal non-ramified extension of $\mathbb{Q}_p$ in K, and let $\{\sigma\}$ be a right transversal of Gal $(\overline{\mathbb{Q}}_p/K)$ in Gal $(\overline{\mathbb{Q}}_p/M)$. This extends to a right transversal $\{\sigma\omega^{-j}\}$ in Gal $(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, where ω acts as the Frobenius on M, and where $j = 0, \ldots, m-1$ with $N\mathfrak{p}_K = p^m$.

Let β be the restriction of $A\phi^h$ to $\mathfrak{O}_K^*$. The values of β lie in M, and so $\beta^{\omega^j \sigma^{-1}} = \beta^{\omega^j} = \beta^{p^j}$. Therefore $\phi^{h\omega^j\sigma^{-1}}$ differs from ϕ^{hp^j} by a non-ramified character. Hence from 2 (e), and using the fact that fractional ideals are fixed under Gal $(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, we deduce that

$$P(\phi^{h\omega^j\sigma^{-1}})^{\sigma\omega^{-j}} = P(\phi^{hp^j}). \tag{4.1}$$

If now $0 \leqslant s < 1$, and

$$\beta(u) \equiv u^{-s(p^m-1)} \bmod \mathfrak{p}_K$$

then applying 2(f) to α^{p^j}, we get

$$P(\phi^{hp^j}) = \mathfrak{p}_K^{\{p^js\}}, \quad 0 \leqslant \{p^js\} < 1, \quad \{p^js\} \equiv p^js \bmod \mathbb{Z}. \tag{4.2}$$

Now $[K:M] = e$, where $\mathfrak{p}_K^e = (p)$. Thus by (4.1), (4.2),

$$\mathcal{N}_{K/\mathbb{Q}_p} P(\phi^h) = \prod_{j=0}^{m-1} P(\phi^{hp^j}) = \mathfrak{p}_K^{e\Sigma_{j=0}^{m-1}\{p^js\}} = (p)^{\Sigma},$$

where Σ stands for $\Sigma_{j=0}^{m-1}\{p^js\}$.

By the Stickelberger formula for $(\tau(\phi)^h)$ (see Coates 1977, theorem 3.6 and lemma 3.7) this coincides with $(\tau(\phi)^h)$.

5. l-characters

Throughout this section l is a prime number. Indeed, because all p-characters are necessarily non-ramified, we shall without loss of generality assume $l \neq p$.

5 (a). Let $E \supset F \supset F_0$ be local fields where E/F_0 is cyclic and tame of degree l for $l \neq 2$ (resp. of degree 4 when $l = 2$), and where $[E:F] = l$.

Let $\alpha \in X(E)$ have l-power order and let $\alpha|_{F^*}$ be genuinely ramified. Then

$$\tau^{ab}(\alpha) \equiv \tau^{ab}(\alpha|_{F^*})\,\alpha(l)^{-1} \begin{cases} \bmod (l) & \text{if} \quad l \neq 2, \\ \bmod 2\mathfrak{L}_2 & \text{if} \quad l = 2. \end{cases}$$

We shall need

Lemma 1. *Let L/M be a tame extension of local fields. Then* $\mathfrak{p}_L D_L = \mathfrak{p}_M D_M \mathfrak{O}_L$
(This is easily checked.)

Proof of 5(*a*). The group Gal(E/F_0), $= \langle\gamma\rangle$ say, acts in the natural way on the dual of $\tilde{E}^*$. In particular, when we view α as a residue class character of $\tilde{E}^*$,

$$^{\gamma}\alpha = \alpha^{r+al^s},$$

where $a = 0$ or $(a, l) = 1$, where $r = 1$, $s \geqslant 1$ for l odd, and where, if $l = 2$, $r = \pm 1$ with $s \geqslant 2$ when $a \neq 0$.

Thus if $x \in \mathfrak{O}_{\tilde{E}}^*$, then
$$\sum_{\delta\in\langle\gamma\rangle} \alpha(x^\delta) = \sum_{\delta} {}^{\delta}\alpha(x) = \sum_k \alpha(x)^{(r+al^s)^k}$$
for $k = 1, 2, \ldots, l$ if $l \neq 2$, $k = 1, 2, 3, 4$ if $l = 2$.

It is now an easy matter of verification that
$$\sum_{\delta\in\langle\gamma\rangle} \alpha(x^\delta) \equiv 0 \quad \begin{Bmatrix} \operatorname{mod}(l) & l \neq 2, \\ \operatorname{mod} 2\mathfrak{L}_2 & l = 2. \end{Bmatrix} \tag{5.1}$$

For example, if l is odd, then either $\alpha(x^\delta) = \alpha(x)$ for all δ, or, $\alpha(x) \neq \alpha(x^\delta) = \alpha(x)^{1+al^s}$, with $(a, l) = 1$. In the first case the sum is just $l\alpha(x)$. In the second case we must have $\alpha(x)^{l^{s+1}} = 1$ as $^{\gamma^l}\alpha(x) = \alpha(x)$, and then we just get $\alpha(x)$ times the sum of all lth roots of unity, and this is zero. An analogous result holds for $l = 2$, where, however, more cases can occur.

From (1.1) we have
$$\tau^{ab}(\alpha) = \Sigma\alpha(uc^{-1})\,\psi_E(uc^{-1}),$$
where by lemma 1 we may choose $c \in F_0^*$. Thus if the image of u in $\tilde{E}$ does not lie in $\tilde{F}$, then for all $\delta \in \langle\gamma\rangle$, $\psi_E(u^\delta c^{-1}) = \psi_E(uc^{-1})$ and the classes of u^δ in $\tilde{E}$ are distinct. So we see that the sum for $\tau^{ab}(\alpha)$ contains a term
$$\sum_\delta \alpha(u^\delta c^{-1})\,\psi_E(u^\delta c^{-1}) = \alpha(c^{-1})\,\psi_E(uc^{-1}) \sum_\delta \alpha(u^\delta),$$
which by (5.1) satisfies the required congruences. Therefore
$$\begin{aligned} \tau^{ab}(\alpha) &= \sum_{u\in\mathfrak{O}_F^* \operatorname{mod} \mathfrak{p}_F} \alpha(uc^{-1})\,\psi_F(luc^{-1}) \\ &= \alpha(l)^{-1}\tau^{ab}(\alpha|_{F^*}). \end{aligned}$$

From now on we shall use the notation of §3, and where we now, moreover, assume $\Gamma =$ Gal(N/K) to have order a power of l. Throughout χ is an irreducible non-Abelian character of Γ induced by an Abelian character ϕ of a sub-group Σ containing I. We put $L = N^\Sigma$ and $\alpha = A\phi$. Moreover, in the case $l = 2$ we let F be the non-ramified quadratic extension of K, so that $F \subseteq L$. We shall also assume that $\alpha|_I$ is faithful. σ denotes a generator of I and ω a generator of Γ modulo I, thus, without loss of generality, a Frobenius element.

We write
$$\left.\begin{aligned} l^N = \operatorname{order}(\sigma), \quad l^m &= \operatorname{order}(\omega) \operatorname{mod} \Sigma, \\ \omega^{-1}\sigma\omega &= \sigma^{r+al^t}, \end{aligned}\right\} \tag{5.2}$$
i.e.
$$\left.\begin{aligned} \operatorname{order}(\alpha|_{\mathfrak{O}_L^*}) &= l^N, \\ ^{\omega}\alpha(x) = \alpha(x)^{r+al^t} \quad &\text{for} \quad x \in \mathfrak{O}_L^*. \end{aligned}\right\} \tag{5.2a}$$
If l is odd, then here we have
$$r = 1, \quad (a, l) = 1, \quad t \geqslant 1, \quad t+m = N, \tag{5.3}$$
while if $l = 2$, then we have either
$$\omega \text{ acts by } \textit{inversion}, \text{ i.e. } a = 0, \quad r = -1, \quad m = 1, \quad N \geqslant 2, \tag{5.3a}$$
or
$$r = \pm 1, \quad (a, 2) = 1, \quad t \geqslant 2, \quad t+m = N. \tag{5.3b}$$

Further, as $\omega^{-1}\sigma\omega = \sigma^{N\mathfrak{p}_K}$, we get

$$N\mathfrak{p}_K \equiv r + al^t \bmod (l^N). \tag{5.4}$$

One now verifies, e.g. by computing the transfer of σ from Γ to Σ, that

$$\text{order } (\alpha|_{\mathfrak{o}^*_K}) = \text{order } (V_{L/K}\,\phi|_I) = \left\{\begin{matrix} l^t \text{ if either } l \neq 2, \text{ or, } l = 2 \text{ and } r = 1, \\ 2 \text{ if } l = 2,\ r = -1,\ \omega \text{ does } \textit{not} \text{ act by inversion,} \\ 1 \text{ if } \omega \text{ acts by inversion.} \end{matrix}\right\} \tag{5.5}$$

Similarly one shows that if $\Sigma \subset \Omega \subset \Gamma$, $[\Omega:\Sigma] = l$, if $M = N^\Omega$, and further if in the case $l = 2$ we also have $M \supseteq F$, then

$$\text{order } (\alpha|_{\mathfrak{o}^*_M}) = \text{order } (V_{L/M}\,\phi|_I) = l^{N-1}. \tag{5.6}$$

As the order of ω mod Ω is l^{m-1}, all the assertions (5.2)–(5.5) on ϕ apply equally to $V_{L/M}\,\phi$ with the *same* r, a and t and with N and m replaced by $N-1$ and $m-1$. Note that if $l = 2$ and ω acts by inversion no such field M exists.

5 (b) (i). If l is odd, then

$$\tau^{ab}(\alpha) \equiv \tau^{ab}(\alpha|_{K^*})\,\alpha\,(\deg{(\chi)})^{-1} \bmod (l).$$

(ii) If $l = 2$ and ω does not act by inversion, then

$$\tau^{ab}(\alpha) \equiv \tau^{ab}(\alpha|_{F^*})\,\alpha(\tfrac{1}{2}\deg{(\chi)})^{-1} \bmod 2\mathfrak{L}_2.$$

Proof. By repeated applications of 5 (a), using (5.5) and (5.6).

For odd l theorem 6 (a) now follows immediately. By (3.1) $\tau(\chi) = \tau^{ab}(\alpha)$, and $\alpha|_{K^*} = AV_{L/K}\,\phi = A\det_\chi$. So from now on we shall assume $l = 2$.

Now let $\beta \in X(F)$ have 2-power order. We let $F = K(d)$ with $d^2 \in K^*$, $d \in \mathfrak{O}^*_F$. Then, by lemma 1, we can choose $c \in K^*$ with $c\mathfrak{O}_F = \mathfrak{p}_F D_F = \mathfrak{p}_K D_K \mathfrak{O}_F$. We have

$$\tau^{ab}(\beta) = \beta(c^{-1})\,[(\sum_a \beta(a)\,\psi_K(2ac^{-1}))\sum_b \beta(1+bd) + \beta(d)\sum_a \beta(a)],$$

where b (resp. a) runs through a complete set of representatives of $\tilde{K}$ (resp. $\tilde{K}^*$).

If first $\beta|_{\mathfrak{o}^*_K}$ is trivial then $\Sigma_a \beta(a) = N\mathfrak{p}_K - 1$, $\Sigma_a \beta(a)\,\psi_K(2ac^{-1}) = -1$, and, because d, $\{1+bd\}_b$ represent each coset of $\tilde{F}^*/\tilde{K}^*$ exactly once, we have

$$\sum_b \beta(1+bd) = -\beta(d).$$

Thus

$$\tau^{ab}(\beta) = \beta|_{K^*}(D_K\mathfrak{p}_K)^{-1}N\mathfrak{p}_K\,\beta(d). \tag{5.7}$$

In the remaining case when $\beta|_{\mathfrak{o}^*_K}$ is non-trivial, $\Sigma_a \beta(a) = 0$, and

$$\beta(c^{-1})\sum_a \beta(a)\,\psi_K(2ac^{-1}) = \beta(2)^{-1}\tau^{ab}(\beta|_{K^*}).$$

Hence

$$\tau^{ab}(\beta) = \beta(2)^{-1}\tau^{ab}(\beta|_{K^*})\sum_b \beta(1+bd). \tag{5.8}$$

We shall first complete the proof of the part of theorem 6 (b) dealing with action by inversion. Now let $\beta = \alpha$ be as given. By (5.5) $\alpha|_{K^*}$ is non-ramified, and it is clear that $A\rho_{F/K}$ is non-ramified. So since $A\det_\chi = A\rho_{F/K}\,AV_{F/K}\,\phi = A\rho_{F/K}\,\alpha\,|_{K^*}$, we deduce that $A\det_\chi$ is non-ramified, so we have

$$\tau(\chi) = \tau^{ab}(\alpha)\,A\rho_{F/K}(D_K),$$

$$\tau(\det_\chi) = \alpha|_{K^*}(D_K)\,A\rho_{F/K}(D_K).$$

Hence
$$\tau(\chi) = \tau(\det_\chi)\,\alpha|_{K^*}(D_K)\,\tau^{ab}(\beta)$$
$$= \tau(\det_\chi)\,\alpha|_{K^*}(\mathfrak{p}_K)^{-1}N\mathfrak{p}_K{\cdot}\alpha(d) \qquad \text{by (5.7).}$$

Now we know that
$$\alpha|_{K^*}(\mathfrak{p}_K)^{-1} = A\det_\chi(\mathfrak{p}_K)^{-1}A\rho_{F/K}(\mathfrak{p}_K)^{-1}$$
$$= -A\det_\chi(\mathfrak{p}_K)^{-1}$$
and by (5.4), $N\mathfrak{p}_K \equiv 1 \bmod (4)$. Therefore
$$\tau(\chi) \equiv \tau(\det_\chi)\,A\det_\chi(\mathfrak{p}_K)^{-1}\alpha(d) \bmod (4). \tag{5.9}$$

Now d satisfies a congruence $\qquad d \equiv x^{(N\mathfrak{p}_K+1)/2^s} \bmod \mathfrak{p}_F$

for $s = 1$, but not for $s = 0$. If then the order of $\alpha|_{\mathfrak{O}_F^*}$ is 2^N, as assumed, we have
$$\alpha(d) = (-1)^{(N\mathfrak{p}_K+1)/2^N},$$
i.e.
$$\alpha(d) = \nu_N(N\mathfrak{p}_K),$$
ν_N having been defined in § 1 preceding the statement of theorem 6 (*b*). This, in conjunction with (5.9), completes the proof of this part of the theorem.

Now we consider the case when ω does not act by inversion. As always, χ is the irreducible character induced by ϕ, and $\alpha = A\phi$. We shall show that mod $2\mathfrak{L}_2$
$$\tau^{ab}(\alpha) \equiv \alpha\,(\deg(\chi))^{-1}\,\tau^{ab}\,(\alpha|_{K^*})\left(\frac{2}{N\mathfrak{p}_K}\right) \quad \text{if} \quad N\mathfrak{p}_K \equiv 1 \bmod (4), \tag{5.10a}$$
$$\tau^{ab}(\alpha) \equiv \alpha\,(\deg(\chi))^{-1}\,\tau^{ab}(\alpha|_{K^*})\,A_p^{[\tilde{K}:\mathbb{F}_p]} \quad \text{if} \quad N\mathfrak{p}_K \equiv -1 \bmod (4), \tag{5.10b}$$
where A_p is the residue class defined in proposition 1. Now $A\det_\chi = A\rho_{L/K}{\cdot}\alpha|_{K^*}$, so by (5.5) $\det_\chi$ is ramified and
$$\tau(\det_\chi) = \tau^{ab}(\alpha|_{K^*})\,A\rho_{L/K}(D_K)\,A\rho_{L/K}(\mathfrak{p}_K)$$
$$= -\tau^{ab}(\alpha|_{K^*})\,A\rho_{L/K}(D_K),$$
while by (3.1)
$$\tau(\chi) = \tau^{ab}(\alpha)\,A\rho_{L/K}(D_K).$$
This, in conjunction with (5.10), yields the result of theorem 6 (*b*). (We must also take into account the fact that $A\det_\chi(\deg(\chi)) = \alpha(\deg(\chi))$, because, as $A\rho_{L/K}$ is non-ramified, $A\rho_{L/K}(\deg(\chi)) = 1$).

Now by 5 (*b*) (ii) and repeated applications of (5.6) we see moreover that (5.10) follows from the special case $m = 1$, $L = F$. So from now on we again assume that $L = F$.

First we consider the sub-case where $N\mathfrak{p}_K \equiv 1 \bmod (4)$. We shall show
$$\tau^{ab}(\alpha) \equiv \alpha(2)^{-1}\left(\frac{2}{N\mathfrak{p}_K}\right)\tau^{ab}(\alpha|_{K^*}) \bmod 2\mathfrak{L}_2. \tag{5.11}$$
Indeed, by (5.3*b*), order$(\alpha)] = 2^{t+1}$ and, by (5.4), $N\mathfrak{p}_K \equiv 1 + 2^t \bmod (2^{t+1})$. For any $b \in \mathfrak{O}_K$
$$\alpha(1-bd) = \alpha((1+bd)^\omega) = \alpha(1+bd)^{N\mathfrak{p}_K},$$
that is
$$\alpha(1-bd) = \begin{cases} \alpha(1+bd) & \text{if} \quad \left(\dfrac{1+bd}{\mathfrak{p}_F}\right)_2 = 1, \\ -\alpha(1+bd) & \text{if} \quad \left(\dfrac{1+bd}{\mathfrak{p}_F}\right)_2 = -1. \end{cases}$$

Thus $\Sigma\alpha(1+bd) = 1+2\Sigma^{+}\alpha(1+bd)$, where Σ^{+} is the sum over a half-system $\pm b \bmod \mathfrak{p}_K$, $b \notin \mathfrak{p}_K$ so that $(1+bd)$ is a quadratic residue. Hence, mod $2\mathfrak{L}_2$, we have

$$\Sigma\alpha(1+bd) \equiv 1+g,$$

where g is the number of non-zero classes $b \bmod \mathfrak{p}_K$ with $\left(\dfrac{1+bd}{\mathfrak{p}_F}\right)_2 = 1.$

Observe that $\tilde{K}^* \subset \tilde{F}^{*2}$. Precisely half of the elements $\{1+bd\}_{b\neq 0}$, 1, d are quadratic residues. 1 clearly is, and, as $r = +1$, d is a non-residue. Therefore $g = \frac{1}{2}(N\mathfrak{p}_K+1)-1 = \frac{1}{2}(N\mathfrak{p}_K-1)$. Hence, as $N\mathfrak{p}_K \equiv 1 \bmod (4)$,

$$1+g \equiv \left(\frac{2}{N\mathfrak{p}_K}\right) \bmod (4),$$

and thus $\Sigma\alpha(1+bd) \equiv \left(\dfrac{2}{N\mathfrak{p}_K}\right) \bmod 2\mathfrak{L}_2$. This, in conjunction with (5.8), yields (5.11).

Next we assume that $N\mathfrak{p}_K \equiv -1 \bmod (4)$. We have to show that

$$\sum_b \alpha(1+bd) = \Lambda_p^{[\tilde{K}:\mathbb{F}_p]}. \tag{5.12}$$

We reduce the proof to the case $K = \mathbb{Q}_p$. In view of (5.4), $N\mathfrak{p}_K = p^f$, f odd. Thus we can find an Abelian character α_0 of F_0, the non-ramified quadratic extension of $\mathbb{Q}_p$, with the property that when α and α_0 are viewed as residue class characters

$$\alpha = \alpha_0 \circ N_{\tilde{F}/\tilde{F}_0}.$$

Thus by restriction $\alpha|_{\tilde{K}^*} = \alpha_0|\mathbb{F}_p^* \circ N_{\tilde{K}/\mathbb{F}_p}$. Choose $c \in K^*$ so that $c\mathfrak{D}_K = \mathfrak{p}_K D_K$ and $\mathrm{tr}_{K/M}(c^{-1}) = p^{-1}$ (where M is the maximal non-ramified extension in K). Then, by (3.6)

$$\begin{aligned} \tau^{ab}(\alpha) &= -\alpha(c^{-1})\, G(\alpha) \\ &= -\alpha(c^{-1})\, G(\alpha_0)^{(\tilde{K}:\mathbb{F}_p)} \quad \text{by} \quad (3.4). \end{aligned}$$

Similarly
$$\tau^{ab}(\alpha|_{K^*}) = -\alpha(c^{-1})\, G(\alpha_0|_{\mathbb{F}_p^*})^{(\tilde{K}:\mathbb{F}_p)},$$

and so we have
$$\frac{\tau^{ab}(\alpha)}{\tau^{ab}(\alpha|_{K^*})} = \left(\frac{G(\alpha_0)}{G(\alpha|_{\mathbb{F}_p^*})}\right)^{(\tilde{K}:\mathbb{F}_p)} = \left(\frac{\tau^{ab}(\alpha_0)}{\tau^{ab}(\alpha_0|_{\mathbb{Q}_p^*})}\right)^{(\tilde{K}:\mathbb{F}_p)}.$$

Trivially we see $\alpha(2) = \alpha_0(2)^{(\tilde{K}:\mathbb{F}_p)}$. Therefore by (5.8) and the corresponding formula for α_0 we get

$$\Sigma\alpha(1+bd) = (\Sigma\alpha_0(1+b_0 d_0))^{[\tilde{K}:\mathbb{F}_p]} \tag{5.13}$$

with the obvious notation on the right hand side.

So now it remains to establish (5.12) in the case $K = \mathbb{Q}_p$ and to prove propositions 1 and 2. As in § 1, we write

$$\lambda(\alpha) = \Sigma\alpha(1+bd),$$

where now $K = \mathbb{Q}_p$ and F is the non-ramified quadratic extension of $\mathbb{Q}_p$. By (5.8), $\lambda(\alpha)$ is certainly independent of the choice of d (i.e. proposition 1 (i) holds). We shall assume that $d^2 \equiv -1 \bmod (p)$. Moreover, to fix the notation, we write

$$p \equiv -1+2^{N-1} \bmod (2^N), \quad N \geqslant 3$$

and η is always a primitive 2^Nth root of unity. Further, we shall now work with the actual elements of $\mathbb{F}_{p^2}$, and the symbols b, d etc. should be viewed in this way. In particular, α will now be viewed as a character of $\mathbb{F}_{p^2}^*$.

Multiplication by an element u of $\mathbb{F}^*_{p^2}$ replaces the set consisting of d and the $1+bd$ by a set yd, $\{y_b(1+bd)\}$, where y, $y_b \in \mathbb{F}^*_p$. (This is because d, $\{1+bd\}$ are a set of representatives of the cosets $\mathbb{F}^*_{p^2}/\mathbb{F}^*_p$). As α takes only values ± 1 on $\mathbb{F}^*_p$, we see that

$$\alpha(u)\,[\sum_b \alpha(1+bd)+\alpha(d)] \equiv [\sum_b \alpha(1+bd)+\alpha(d)] \bmod (2),$$

and choosing $\alpha(u) = \eta$ we conclude that

$$(\lambda(\alpha)+\alpha(d))\,(\eta-1) \equiv 0 \bmod (2).$$

But $\alpha(d) = \pm\mathrm{i}$, whence

$$\lambda(\alpha) \equiv \mathrm{i} \bmod (2(\eta-1)^{-1}). \tag{5.14}$$

Next note that

$$\alpha(1-bd) = \alpha(1+bd)^{-1+2^{N-1}} = \bar{\alpha}(1+bd)\,\theta(1+bd),$$

where θ is the quadratic character of $\mathbb{F}^*_{p^2}$. Taking complex conjugates we get

$$\bar{\lambda}(\alpha) = \Sigma\bar{\alpha}(1-bd) = \Sigma\alpha(1+bd)\,\theta(1+bd),$$

and so

$$\begin{aligned} \lambda(\alpha)+\bar{\lambda}(\alpha) &= 2\Sigma^{+}\alpha(1+bd), \\ \lambda(\alpha)-\bar{\lambda}(\alpha) &= 2\Sigma^{-}\alpha(1+bd), \end{aligned} \tag{5.15}$$

where Σ^{+}, Σ^{-} are sums over those b for which $1+bd$ is a square, a non-square, respectively, in $\mathbb{F}^*_{p^2}$.

Now because $\mathbb{F}^*_p \subset \mathbb{F}^*_{p^2}$, exactly half of the set d, $\{1+bd\}_b$ are squares. But d is a square, hence the sum Σ^{-} has $\frac{1}{2}(p+1)$ terms, each congruent to $1 \bmod (\eta-1)$. Thus $\Sigma^{-}\alpha(1+bd) \equiv 0 \bmod (\eta-1)$, and hence

$$\lambda(\alpha)-\bar{\lambda}(\alpha) \equiv 0 \bmod (2(\eta-1)). \tag{5.16}$$

Now suppose, for a contradiction, that $\lambda = \lambda(\alpha) \equiv \mathrm{i} \bmod (2)$. Then put $\lambda-\mathrm{i} = 2\xi$, for an integer ξ in $\mathbb{Q}(\eta)$. Then

$$(\lambda-\mathrm{i})-(\overline{\lambda-\mathrm{i}}) = 2(\xi-\bar{\xi}) \equiv 0 \bmod (2(\eta-1)),$$

and so by (5.16) $2\mathrm{i} \equiv 0 \bmod (2(\eta-1))$, which is a contradiction. Therefore

$$\left.\begin{aligned} &\lambda \not\equiv \mathrm{i} \bmod (2), \\ \text{i.e.}\quad &\lambda \equiv \mathrm{i}\left(1+\frac{2}{\eta-1}\right) = \mathrm{i}\left(\frac{\eta+1}{\eta-1}\right) \bmod (2). \end{aligned}\right\} \tag{5.17}$$

As before Λ_p denotes the residue class of $\lambda(\beta) \bmod 2\mathfrak{L}_2$, i.e. $\Lambda_p \equiv \pm\mathrm{i}(\eta-1)/(\eta+1)$ $(= \pm \cot\,(\pi/2^N)) \bmod 2\mathfrak{L}_2$, with suitable choice of sign.

We next wish to show that the class Λ_p of $\lambda(\alpha) \bmod 2\mathfrak{L}_2$ does not depend on the choice of α. As the other characters of $\mathbb{F}^*_{p^2}$ of order 2^N are precisely the conjugates α^{ω} of α under the action of Gal $(\mathbb{Q}(\eta)/\mathbb{Q})$, and as $\lambda(\alpha^{\omega}) = \lambda(\alpha)^{\omega}$, it suffices to prove that

$$\lambda \equiv \lambda^{\omega} \bmod (2(\eta-1)). \tag{5.18}$$

We do this without ramification theory. Because we already have (5.16), it suffices to establish (5.18) for Galois automorphisms ω, so that

$$\eta^{\omega} = \eta^{e}, \quad e = 1+2^{r} \bmod (2^{r+1}), \quad r \geqslant 2.$$

One then verifies quickly that

$$\left(\frac{\eta+1}{\eta-1}\right)^{\omega} \equiv \left(\frac{\eta+1}{\eta-1}\right) \bmod (2(\eta-1)),$$

and in view of the form of Λ_p this proves (5.18).

(5.10) and proposition 1 (apart from (iii)) have now been established. For the moment let δ be the element of Gal $(\mathbb{Q}(\eta)/\mathbb{Q})$ with $\eta^{\delta} = -\eta^{-1}$. Then δ is the Frobenius of p in $\mathbb{Q}(\eta)/\mathbb{Q}$ and so $\alpha(1+bd)^{\omega} = \alpha(1-bd)$. Hence $\lambda(\alpha)^{\omega} = \lambda(\alpha) \in \mathbb{Q}(\eta-\eta^{-1})$, and so $\lambda(\alpha)$ is of the form

$$\lambda(\alpha) = a+b(\eta-\eta^{-1}),$$

where a, b are integers of the maximal real subfield $\mathbb{Q}(\eta^2+\eta^{-2})$ of $\mathbb{Q}(\eta-\eta^{-1})$. By (5.7) and theorem 3 (i) we have $\lambda(\alpha)\,\overline{\lambda(\alpha)} = p$ (which is proposition 1 (iii)). Clearly

$$2a = \lambda+\bar{\lambda},$$

$$2b(\eta-\eta^{-1}) = \lambda-\bar{\lambda},$$

yielding, by (5.14), the expressions for a and b given in proposition 2 (ii).

We now prove proposition 2 (i). For the first part expand $(1+bd)^{s}$ by the binomial theorem and then sum over all b. The result then follows by use of the congruence mod (l)

$$\sum_{b} b^{r} \equiv \begin{cases} 0 & \text{if} \quad p-1 \nmid r, \\ -1 & \text{if} \quad p-1 \mid r. \end{cases}$$

Because p is completely split in $\mathbb{Q}(\eta-\eta^{-1})$, and because $\lambda(\alpha)\,\overline{\lambda(\alpha)} = p$ is the value of $\lambda(\alpha)$ under the norm from $\mathbb{Q}(\eta-\eta^{-1})$ to $\mathbb{Q}(\eta^2+\eta^{-2})$, we see that precisely half the primes $\mathfrak{p}$ above p divide $\lambda(\alpha)$. However, since $\lambda(\alpha)\,\overline{\lambda(\alpha)} = p$, $\lambda(\alpha)$ is divisible only by primes above p, and so the result is established.

Finally, to establish uniqueness, observe that the given value of the ideal $(\lambda(\alpha))$ determines $\lambda(\alpha)$ up to a unit, and then the norm equation $\overline{\lambda(\alpha)}\,\lambda(\alpha) = p$ up to a root of unity in $\mathbb{Q}(\eta-\eta^{-1})$, and, finally, the congruence mod $2(\eta-1)$ fixes the root of unity.

6. Inductivity

Our procedure is as follows. We always work in the context of a given extension N/K. After establishing inductivity modulo roots of unity in 6 (a), we first prove the inductivity of τ for all N/K, with Gal $(N/K) = \Gamma$ Abelian. Hereafter, we shall work with the induction hypothesis that inductivity holds for all Galois extensions N'/K' with $[N':K'] < [N:K]$.

As in §3 we use the notation

$$\Gamma = \mathrm{Gal}\,(N/K), \quad \Delta < \Gamma, \quad F = N^{\Delta}. \tag{6.1}$$

For inductivity we have to show that for all $\chi \in R(N/F)$

$$\tau(\mathrm{Ind}_K^F\,\chi) = \tau(\chi)\,\tau(\mathrm{Ind}_K^F\,\epsilon_F)^{\deg(\chi)}. \tag{6.2}$$

6 (a). $\tau(\chi)\,\tau(\mathrm{Ind}_K^F\,\epsilon_F)^{\deg(\chi)}\,\tau(\mathrm{Ind}_K^F\,\chi)^{-1}$ is a root of unity.

Proof. For short we denote the expression in 6 (a), by $\mu(\chi)$. By theorem 2 (proved in §3), as applied to complex conjugation ω, $\tau(\mathrm{Ind}_K^F\,\epsilon_F)^{\omega} = \pm\tau(\mathrm{Ind}_K^F\,\epsilon_F)$. This, in conjunction with theorem 3 (i), yields

$$\pm\tau(\mathrm{Ind}_K^F\,\epsilon_F)^2 = N\mathfrak{f}(\mathrm{Ind}_K^F\epsilon_F) = N\mathfrak{d}(F/K).$$

Now it follows from theorem 4, and from the inductive property of norm resolvents (2 (c)), that $\mu(\chi)$ is a unit. By theorem 3 (i) and 2 (a) we see that $|\mu(\chi)| = 1$. But from theorem 2, $\mu(\chi)^{\omega} = \mu(\chi^{\omega})\,\mu'$ for some root of unity μ'; whence $|\mu(\chi)^{\omega}| = 1$ for all $\omega \in \Omega$. This implies that $\mu(\chi)$ is a root of unity.

Note that in (6.2), if F/K is non-ramified, then

$$\tau(\mathrm{Ind}_K^F \epsilon_F) = A\rho_{F/K}(D_K)$$

and so we know by 3(*b*) that (6.2) holds in this case. In view of the solubility of Γ, by the transitivity of induction, we may always assume that

$$[\Gamma : \Delta] = l \quad \text{(a prime number)}, \tag{6.3}$$

and, by what we have said previously, we can also assume

$$F/K \text{ is totally ramified.} \tag{6.4}$$

Lemma 2. *With notation as above let ξ be an Abelian character of* Gal(N/K), *and suppose $\xi|_\Delta$ is ramified. Then* $\tau(\xi|_\Delta) = A\xi^{-l}(l)\,\tau(\xi^l)$.

Proof. Choose $c \in K$ such that $c\mathfrak{D}_K = D_K\mathfrak{p}_K$, then by lemma 1

$$\tau(\xi|_\Delta) = \sum_u A\xi|_\Delta(uc^{-1})\,\psi_F(uc^{-1}),$$

where the sum is taken over a set of representatives u of $\mathfrak{D}_F$ *mod* $\mathfrak{p}_F$. Indeed, because F/K is totally ramified, we can choose the u to lie in K. Also, by the commutativity of (2.3), $A\xi|_\Delta = A\xi \circ N_{F/K}$; thus we have

$$\begin{aligned}\tau(\xi|_\Delta) &= \sum_u A\xi(uc^{-1})^l\psi_K(luc^{-1})\\ &= A\xi^l(l^{-1})\,\tau(\xi^l).\end{aligned}$$

6(*b*). (6.2) holds if Γ is Abelian.

Proof. We may assume χ to be an Abelian character (by additivity). If $\{\alpha_i\}_{i=0}^{l-1}$ are the distinct Abelian characters of $\Gamma/\Delta = \mathrm{Gal}(F/K)$, with $\alpha_0 = \epsilon_K$ say, then

$$\mathrm{Ind}_K^F \epsilon_F = \sum_{i=0}^{l-1} \alpha_i,$$

$$\mathrm{Ind}_K^F \chi = \sum_{i=0}^{l-1} \xi\alpha_i,$$

where ξ is some Abelian character with $\xi|_\Delta = \chi$. Thus we must show

$$\prod_{i=0}^{l-1} \tau(\xi\alpha_i) = \tau(\xi|_\Delta) \prod_{i=0}^{l-1} \tau(\alpha_i). \tag{6.5}$$

First, if χ is ramified, then (6.5) follows immediately from lemma 2 and (3.8). On the other hand, if χ is non-ramified, then we can choose (uniquely) ξ to be non-ramified. We then have

$$\begin{aligned}\tau(\xi|_\Delta) = A\xi(N_{F/K}D_F)^{-1} &= A\xi(N_{F/K}(\mathfrak{p}_F^{l-1}D_K))^{-1}\\ &= A\xi(\mathfrak{p}_K^{l-1}D_K^l)^{-1}.\end{aligned}$$

Also, trivially, $$\tau(\xi\alpha_0) = A\xi(D_K)^{-1} = A\xi(D_K)^{-1}\tau(\alpha_0)$$

while by theorem 3 (ii) for $0 < i < l$

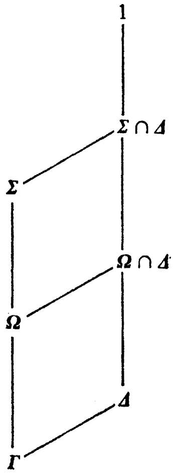
$$\tau(\xi\alpha_i) = A\xi(D_K)^{-1}A\xi(\mathfrak{p}_K^{-1})\,\tau(\alpha_i).$$

One may now verify (6.5) directly.

From now on we assume (6.2) to hold when N, F, K are replaced by any triplet of fields N', F', K' with $[N':K'] < [N:K]$. Clearly, by additivity, it will suffice to take χ irreducible, and also, if convenient, we may assume that the representations associated with χ are faithful on Γ.

6 (*c*). It suffices to prove (6.2) under the further hypothesis that χ is Abelian.

Proof. We let Σ (resp. Ω) be the centralizer of I (resp. $I \cap \Delta$) in Γ. Thus we have a tower of Galois groups:



(6.6)

As in 3 (*a*), we put $\chi = \mathrm{Ind}^{\Delta}_{\Lambda}\,\phi$, where ϕ is an Abelian character of Λ and $\Lambda \supset \Delta \cap I$. Because $\mathrm{Ind}^{\Delta}_{\Gamma}\,\chi$ can be assumed faithful on Γ, we may assume ϕ to be faithful on $\Delta \cap I$. On the other hand, because χ is irreducible, we must have that Λ is the centralizer of $\Delta \cap I$ in Δ, namely $\Omega \cap \Delta$.

If, first, ϕ is non-ramified, then because χ is irreducible we must have $\Omega \cap \Delta = \Delta$, and $\phi = \chi$; thus χ is Abelian.

So now suppose ϕ is genuinely ramified (so that $\Delta \cap I \neq \{1\}$). We put $\theta = \mathrm{Ind}^{\Omega\cap\Delta}_{\Omega}\,\phi$. Then by our non-ramified induction formula in 3 (*b*)

$$\tau(\mathrm{Ind}^{\Omega}_{\Gamma}\,\theta) = \tau(\theta)\,\tau(\mathrm{Ind}^{\Omega}_{\Gamma}\,\epsilon_{\Omega})^{l}.$$

If $\Omega = \Gamma$, then again $\Omega \cap \Delta = \Delta$, i.e. χ is Abelian. Otherwise, we may apply our induction hypothesis to θ and Ω and get

$$\tau(\theta) = \tau(\mathrm{Ind}^{\Omega\cap\Delta}_{\Omega}\,\phi) = \tau(\phi)\,\tau(\mathrm{Ind}^{\Omega\cap\Delta}_{\Omega}\,\epsilon_{\Omega\cap\Delta}).$$

We are required to show that

$$\tau(\mathrm{Ind}^{\Delta}_{\Gamma}\,\chi) = \tau(\chi)\,\tau(\mathrm{Ind}^{\Delta}_{\Gamma}\,\epsilon_{\Delta})^{\deg\chi},$$

i.e.

$$= \tau(\phi)\,\tau(\mathrm{Ind}^{\Omega\cap\Delta}_{\Delta}\,\epsilon_{\Omega\cap\Delta})\,\tau(\mathrm{Ind}^{\Delta}_{\Gamma}\,\epsilon_{\Delta})^{\deg\chi},$$

and since $\mathrm{Ind}^{\Omega}_{\Gamma}\,\theta = \mathrm{Ind}^{\Delta}_{\Gamma}\,\chi$ it is enough to show that

$$\tau(\mathrm{Ind}^{\Omega\cap\Delta}_{\Omega}\,\epsilon_{\Omega\cap\Delta})\,\tau(\mathrm{Ind}^{\Omega}_{\Gamma}\,\epsilon_{\Omega})^{l} = \tau(\mathrm{Ind}^{\Omega\cap\Delta}_{\Delta}\,\epsilon_{\Omega\cap\Delta})\,\tau(\mathrm{Ind}^{\Delta}_{\Gamma}\,\epsilon_{\Delta})^{\deg\chi}.$$

Clearly all four characters in this expression factor through the proper quotient of Γ, $\Gamma/\Delta \cap I$. So, by induction hypothesis, the above equation follows from (6.2) on evaluating $\tau(\mathrm{Ind}^{\Omega\cap\Delta}_{\Gamma}\,\epsilon_{\Omega\cap\Delta})$, inducing first through Ω and secondly through Δ.

So now we are in the situation where χ is Abelian, $[\Gamma:\Delta] = l$ and F/K is totally ramified. We are required to show (6.2). We remark that, because $[\Delta,\Delta] \subset \Delta \cap I$ and because we may assume $\chi|_{\Delta\cap I}$ to be faithful, Δ is Abelian. As before Σ is the centralizer of I in Γ, and we have a tower of the fields and Galois groups

$$\begin{tikzcd} & N, \{1\} \arrow[dd, dash] \\ F, \Delta \arrow[ur, dash] \arrow[dd, dash] & \\ & L, \Sigma \\ K, \Gamma \arrow[ur, dash] & \end{tikzcd} \qquad (6.7)$$

If $\Sigma = \Gamma$, then Γ is Abelian and this case was dealt with in 6(*b*). Hence we shall assume that $\Sigma \neq \Gamma$, and so that $\Sigma \cap \Delta \neq \Delta$.

For a finite group X, we denote by X_l an l-Sylow group.

6(*d*). Suppose that $(I \cap \Delta)_l = 1$, i.e. we have a decomposition $I = (I \cap \Delta) \times I_l$. Then Γ/Σ is of order f, $f > 1$, $f \mid l-1$, and this group acts faithfully on I_l. Let θ_0 be the unique Abelian character of Γ such that $\theta_0|_{I_l} = \epsilon_{I_l}$, $\theta_0|_\Delta = \chi$, and let $\{\alpha_i\}_{i=0}^{l-1}$ be the Abelian characters of Σ such that the $\alpha_i|_{I_l}$ are the distinct non-trivial Abelian characters of I_l and so that $\alpha_i|_{\Delta\cap\Sigma} = \epsilon_{\Delta\cap\Sigma}$. Define $\beta_i = \alpha_i \cdot \theta_0|_\Sigma$ $(i = 1, \ldots, l-1)$. Finally let α_i, $i = 1, \ldots, (l-1)f^{-1}$, represent the distinct orbits of the $\{\alpha_i\}$ under the action of Γ/Σ. Then the characters

$$\phi_i = \operatorname{Ind}_\Gamma^\Sigma \alpha_i$$

for $i = 1, \ldots, (l-1)f^{-1}$, are irreducible and distinct. Similarly the characters

$$\theta_i = \operatorname{Ind}_\Gamma^\Sigma (\alpha_i \cdot \theta_0|_\Sigma), \quad i = 1, \ldots, (l-1)f^{-1}$$

are irreducible and distinct. Finally, we have

$$\operatorname{Ind}_\Gamma^\Delta \epsilon_\Delta = \epsilon_\Gamma + \sum_{i=1}^{(l-1)f^{-1}} \phi_i,$$

$$\operatorname{Ind}_\Gamma^\Delta \chi = \theta_0 + \sum_{i=1}^{(l-1)f^{-1}} \theta_i.$$

Proof. As $\Gamma = \Delta I$, and as both Δ and I are Abelian, Γ centralizes $\Delta \cap I$; thus Σ, the centralizer of I, is the centralizer of I_l. Hence Γ/Σ acts faithfully on the group I_l (of order l), and so, as $\Sigma \neq \Gamma$, $f > 1$ and $f \mid l-1$. Dually Γ/Σ acts faithfully on the $\alpha_i|I_l$, and hence, in turn, on the α_i. Thus, by 3(*a*), the characters ϕ_i are irreducible, and the ϕ_i, $i = 1, \ldots, (l-1)f^{-1}$ are the distinct ones among them. The same reasoning applies to the $\alpha_i \cdot \theta_0|_\Sigma$ and the θ_i, so yielding our assertions.

Finally, θ_0 is Abelian, hence irreducible and distinct from the θ_i $(i > 0)$. Now by Frobenius reciprocity

$$(\operatorname{Ind}_\Gamma^\Delta \epsilon_\Delta, \phi_i) = ((\operatorname{Ind}_\Gamma^\Delta \epsilon_\Delta)|_\Sigma, \alpha_i),$$

where (,) is the standard inner product on the group of characters. The right hand side is 1, since by Mackey's restriction formula

$$\operatorname{Ind}_\Gamma^\Delta \epsilon_\Delta|_\Sigma = \operatorname{Ind}_\Sigma^{\Sigma\cap\Delta} \epsilon_{\Sigma\cap\Delta} = \epsilon_\Sigma + \sum_{i=1}^{l-1} \alpha_i.$$

Likewise $$(\mathrm{Ind}_{\Gamma}^{\Delta}\epsilon_{\Delta}, \epsilon_{\Gamma}) = (\epsilon_{\Delta}, \epsilon_{\Gamma}|_{\Delta}) = (\epsilon_{\Delta}, \epsilon_{\Delta}) = 1.$$

Thus, by comparing degrees,
$$\mathrm{Ind}_{\Gamma}^{\Delta}\epsilon_{\Delta} = \epsilon_{\Gamma} + \sum_{i=1}^{(l-1)f^{-1}} \phi_i.$$

By Frobenius reciprocity
$$\begin{aligned}\mathrm{Ind}_{\Gamma}^{\Delta}\chi &= \theta_0\,\mathrm{Ind}_{\Gamma}^{\Delta}\epsilon_{\Delta} = \theta_0(\epsilon_{\Gamma} + \sum_i \phi_i) \\ &= \theta_0 + \sum_i \mathrm{Ind}_{\Gamma}^{\Delta}(\alpha_i\cdot\theta_0|_{\Sigma}) = \theta_0 + \sum_i \theta_i,\end{aligned}$$
and so 6 (*d*) is now shown.

6 (*e*). If $(I \cap \Delta)_l = \{1\}$, then (6.2) holds.

Proof. Let $g = (l-1)f^{-1}$. Using 6 (*d*) and cancelling a factor $A\rho_{L/K}(D_K)^g$ from both sides, we see that (6.2) is equivalent to
$$\tau(\theta_0|_{\Delta}) \prod_{i=1}^{g} \tau(\alpha_i) = \tau(\theta_0) \prod_{i=1}^{g} \tau(\alpha_i\,\theta_0|_{\Sigma}). \tag{6.8}$$

First suppose that $\chi = \theta_0|_{\Delta}$ is non-ramified. Then θ_0 is non-ramified, and so
$$\tau(\theta_0) = A\theta_0(D_K)^{-1}, \tau(\theta_0|_{\Delta}) = A\theta_0(N_{F/K}\,D_F)^{-1} = A\theta_0(D_K^l\,\mathfrak{p}_K^{l-1})^{-1},$$
since $D_F = \mathfrak{p}_F^{l-1}D_K$. Also
$$\tau(\alpha_i\cdot\theta_0|_{\Sigma}) = \tau(\alpha_i)\,A\theta_0(N_{L/K}(D_L\,\mathfrak{p}_L))^{-1} = \tau(\alpha_i)\,A\theta_0(D_K\,\mathfrak{p}_K)^{-f}.$$

On collecting all the factors, (6.8) is seen to hold. So now we assume that χ is ramified. Then some prime q (different from l and p) divides the order of $\chi|_{I\cap\Delta}$.

First we show that
$$\tau(\theta_0|_{\Delta}) \equiv \tau(\theta_0)^l \bmod \mathfrak{L}_l. \tag{6.9}$$

Now by lemma 2 $$\tau(\theta_0|_{\Delta}) = A\theta_0^{-l}(l)\,\tau(\theta_0^l),$$

while by the binomial theorem, with the usual notation,
$$\tau(\theta_0)^l \equiv \Sigma A\theta_0^l(uc^{-1})\,\psi_K(lc^{-1}u) \bmod \mathfrak{L}_l,$$
i.e. $$\equiv A\theta_0^{-l}(l)\,\tau(\theta_0^l) \bmod \mathfrak{L}_l.$$
This proves (6.9).

Next we apply 3 (*c*) to $\alpha_i - \epsilon_{\Sigma}$ and $\alpha_i\cdot\theta_0|_{\Sigma} - \theta_0|_{\Sigma}$, and we obtain
$$\tau(\alpha_i) \equiv -1, \quad \tau(\alpha_i\,\theta_0|_{\Sigma}) \equiv \tau(\theta_0|_{\Sigma}) \bmod \mathfrak{L}_l. \tag{6.10}$$

Now by (3.7), $\tau(\theta_0|_{\Sigma}) = (-1)^{1+f}\tau(\theta_0)^f$. From this equation and from (6.9) and (6.10) we conclude that the two sides in (6.8) are congruent mod $\mathfrak{L}_l$. We shall also show that they are congruent mod $\mathfrak{L}_q$, i.e. that
$$\tau(\theta_0|_{\Delta}) \prod_{i=1}^{g} \tau(\alpha_i) \equiv \tau(\theta_0) \prod_{i=1}^{g} \tau(\alpha_i\cdot\theta_0|_{\Sigma}) \bmod \mathfrak{L}_q. \tag{6.11}$$

By 6 (*a*) the quotient of the two sides in (6.8) is thus a root of unity which is congruent to 1 mod $\mathfrak{L}_l$ and mod $\mathfrak{L}_q$. Hence this root of unity is 1, which yields 6 (*e*).

It remains then to establish (6.11). Let $\theta_0 = \theta_0'\,\theta_0''$, where θ_0'' has q-power order and θ_0' has order prime to q. Then $\chi' = \theta_0'|_{\Delta}$ and the α_i are all characters of Γ/I_q, and so, because $I_q \neq \{1\}$, by our induction hypothesis (6.8) will hold if θ_0 is replaced throughout by θ_0'. However, by 3 (*c*), we have congruences mod $\mathfrak{L}_q$

$$\tau(\alpha_i \cdot \theta_0|_\Sigma) \equiv \tau(\alpha_i \cdot \theta_0'|_\Sigma),$$

$$\tau(\theta_0) \equiv d\tau(\theta_0') \quad \text{and} \quad \tau(\theta_0|_\Delta) \equiv d\tau(\theta_0'|_\Delta),$$

where

$$d = \begin{cases} 1 & \text{if} \quad \theta_0' \text{ is ramified,} \\ -A\theta_0'(\mathfrak{p}_F)^{-1} & \text{if} \quad \theta_0' \text{ is non-ramified.} \end{cases}$$

(6.11) is now immediate, and so 6 (*e*) is now shown.

6 (*f*). Suppose now that $(I \cap \Delta)_l \neq \{1\}$. Then Γ/Σ is of order l and acts trivially on all Sylow groups I_q for $q \neq l$. A generator ω of $\Gamma \bmod \Sigma$ acts on a generator σ of I_l via

$$\omega^{-1}\sigma\omega = \sigma^{1+al^t}, \quad (a, l) = 1, \quad \sigma^{l^{t+1}} = 1,$$

when l is odd, or, if $l = 2$ with $t \geqslant 2$; while if $l = 2$ with $\sigma^4 = 1$, then

$$\omega^{-1}\sigma\omega = \sigma^{-1}.$$

Let $\{\alpha_i\}$ be the non-trivial Abelian characters of $\Sigma/\Sigma \cap \Delta$, viewed as characters of I, and let α_i' be the extension of α_i to Γ such that $\alpha_i'|_\Delta = \epsilon_\Delta$ (recall that by the above $\Gamma/\Delta \cap I$ is Abelian!). Then

$$\mathrm{Ind}_\Gamma^\Delta \epsilon_\Delta = \sum_{i=1}^{l-1} \alpha_i' + \epsilon_\Gamma.$$

Further, if β is an Abelian character of Σ such that $\beta|_{\Delta \cap \Sigma} = \chi|_{\Delta \cap \Sigma}$, then

$$\mathrm{Ind}_\Gamma^\Delta \chi = \mathrm{Ind}_\Gamma^\Sigma \beta$$

and this character is irreducible.

Proof. Both Δ and I, and hence $\Gamma = \Delta \cdot I$, commute with $\Delta \cap I$, hence with I_l^l and with all Sylow groups I_q (for $q \neq l$). So now the cyclic group Γ/Σ acts faithfully on I_l and trivially on I_l^l; thus $(\Gamma : \Sigma) = l$. It now follows easily that

$$\omega^{-1}\sigma\omega = \sigma^{1+al^t}, \quad (a, l) = 1, \ t \geqslant 1,$$

where order $(\sigma) = l^{t+1}$. In particular, if $l = 2$ and $t = 1$, then σ has order 4 and $\omega^{-1}\sigma\omega = \sigma^{-1}$.

The formula for $\mathrm{Ind}_\Gamma^\Delta \epsilon_\Delta$ is immediate as the α_i' are the distinct, non-trivial, Abelian characters of Γ/Δ. Next recall that $\chi|_{I \cap \Delta} = \beta|_{I \cap \Delta}$ is faithful; hence $\beta|_I$ is faithful and so Σ is the stabilizer of β. Therefore, by 3 (*a*), $\mathrm{Ind}_\Gamma^\Sigma \beta$ is irreducible. Now by Frobenius reciprocity

$$(\mathrm{Ind}_\Gamma^\Delta \chi, \mathrm{Ind}_\Gamma^\Sigma \beta) = (\mathrm{Ind}_\Gamma^\Delta \chi|_\Sigma, \beta)$$

and the right-hand side is 1 since, by Mackey's restriction formula,

$$(\mathrm{Ind}_\Gamma^\Delta \chi)|_\Sigma = \mathrm{Ind}_\Sigma^{\Delta \cap \Sigma} (\beta|_{\Sigma \cap \Delta}) = \beta + \sum_i \beta\alpha_i.$$

So because $\mathrm{Ind}_\Gamma^\Delta \chi$ and $\mathrm{Ind}_\Gamma^\Sigma \beta$ have the same degree, with the latter being irreducible, we deduce $\mathrm{Ind}_\Gamma^\Delta \chi = \mathrm{Ind}_\Gamma^\Sigma \beta$.

6 (*g*). If $(I \cap \Delta)_l \neq \{1\}$, and if for some prime q $(\neq l)$ $\Delta_q \neq \{1\}$, then (6.2) holds.

Proof. We are required to prove that

$$\tau(\chi) \prod_{i=1}^{l-1} \tau(\alpha_i') = \tau(\beta) A \rho_{L/K}(D_K). \tag{6.12}$$

Let $\chi = \chi'\chi''$, $\beta = \beta'\beta''$, where χ'', β'' have q-power order and χ', β' have order prime to q. Then χ', β' are still ramified being non-trivial on $(I \cap \Delta)_l \neq \{1\}$, and we are again in the situation described in 6 (f). Hence, by our induction hypothesis (applied to Γ/Δ_q), the analogue of (6.12) holds for χ', β' in place of χ and β. Further, by 3 (c), we have congruences mod $\mathfrak{L}_q$

$$\tau(\chi) \equiv \tau(\chi'), \quad \tau(\beta) \equiv \tau(\beta'),$$

whence we deduce that the two sides of (6.12) are congruent mod $\mathfrak{L}_q$.

Using the argument used previously (based on 6 (a)) we shall establish (6.12) by showing that the two sides are also congruent mod $\mathfrak{L}_l$.

So now let $\chi = \chi^*\chi^{**}$, $\beta = \beta^*\beta^{**}$, where χ^{**}, β^{**} have l-power order and χ^*, β^* have order prime to l. Let $I = I_l \times I^*$. Because χ and β coincide on $I \cap \Delta$, they will coincide on I^*, and so χ^* and β^* are either both ramified or both non-ramified.

First, we assume that they are both non-ramified. Then, by 3 (c), we get that mod $\mathfrak{L}_l$

$$\tau(\chi) \equiv -A\chi^*(\mathfrak{p}_F)^{-1}\tau(\chi^*) \equiv -A\chi^*(\mathfrak{p}_F D_F)^{-1},$$
$$\tau(\beta) \equiv -A\beta^*(\mathfrak{p}_L)^{-1}\tau(\beta^*) \equiv -A\beta^*(\mathfrak{p}_L D_L)^{-1}.$$

Now χ^* and β^* are both Abelian characters of the Abelian groups $\Delta/\Delta \cap I_l$ and $\Sigma/\Delta \cap I_l$ which coincide on their intersection inside the Abelian group $\Gamma/\Delta \cap I_l$. Hence they have a common extension ϕ^* to this latter group. So by (2.3) and lemma 1

$$A\beta^*(\mathfrak{p}_L D_L) = A\phi^*(N_{L/K}\mathfrak{p}_L D_L) = A\phi^*(\mathfrak{p}_K D_K)^l,$$
$$A\chi^*(\mathfrak{p}_F D_F) = A\phi^*(N_{F/K}\mathfrak{p}_F D_F) = A\phi^*(\mathfrak{p}_K D_K)^l;$$

thus we have $\tau(\chi) \equiv \tau(\beta) \bmod \mathfrak{L}_l$.

Now if $l \neq 2$, $A\rho_{L/K}(D_K) = 1$, $\tau(\alpha_i)' \equiv -1 \bmod \mathfrak{L}_l$ and so $\Pi_{i=1}^{l-1}\tau(\alpha_i') \equiv 1 \bmod \mathfrak{L}_l$; while if $l = 2$, then

$$A\rho_{L/K}(D_K) \equiv 1 \equiv \tau(\alpha_i') \bmod \mathfrak{L}_l.$$

Thus we obtain the required congruence mod $\mathfrak{L}_l$ when χ^* and β^* are non-ramified.

So next assume that χ^* and β^* are both ramified. Let ϕ^* be the common extension of χ^* and β^* to Γ, as above. We have

$$\mathrm{Ind}_\Gamma^\Delta \chi^* = \phi^* + \sum_{i=1}^{l-1} \phi^*\alpha_i'.$$

So, since all these characters are characters of the Abelian group Γ/I_l, by 6 (b) we have

$$\tau(\chi^*) \prod_{i=1}^{l-1} \tau(\alpha_i') = \tau(\phi^*) \prod_{i=1}^{l-1} \tau(\phi^*\alpha_i).$$

Hence, by 3 (c),
$$\tau(\chi^*) \prod_{i=1}^{l-1} \tau(\alpha_i') \equiv \tau(\phi^*)^l \bmod \mathfrak{L}_l. \tag{6.13}$$

But by (3.7), because $(-1)^{1+l} \equiv 1 \bmod (l)$,

$$\tau(\beta^*) \equiv \tau(\phi^*)^l \bmod \mathfrak{L}_l,$$

and also
$$A\rho_{L/K}(D_K) \equiv 1 \bmod \mathfrak{L}_l.$$

Thus, by 3 (c), the respective sides of (6.13) are congruent mod $\mathfrak{L}_l$ to those of (6.12). Hence we have the required congruence mod $\mathfrak{L}_l$, which completes the proof of 6 (g).

6 (h). If $\Delta = \Delta_l$, and $(I \cap \Delta)_l \neq \{1\}$ then (6.2) holds.

Proof. Again we have to show (6.12), and now Γ is a group of l-power order. First take l odd. As $\mathrm{Ind}_\Gamma^\Delta \chi = \mathrm{Ind}_\Gamma^\Xi \beta$, we have the two expressions for the determinant of this character

$$V_{F/K}\chi \cdot \rho_{F/K} = V_{L/K}\beta \cdot \rho_{L/K}, \quad \text{i.e. } V_{F/K}\chi = V_{L/K}\beta \quad \text{as} \quad \rho_{F/K} = \rho_{L/K} = \epsilon_K$$

(since l odd). By theorem 6 (a) and by 3 (b), we see that

$$\tau(\beta) = \tau(\mathrm{Ind}_\Gamma^\Xi \beta) \equiv \tau(V_{F/K}\chi)\, A\chi(l)^{-1} \bmod (l).$$

But, as F/K is totally ramified,

$$\begin{aligned} \tau(\chi) = \tau^{ab}(A\chi) &= \Sigma A\chi(uc^{-1})\, \psi_L(uc^{-1}) \\ &= A\chi(l^{-1})\, \tau^{ab}(A\chi|_{K^*}) \\ &= A\chi(l)^{-1}\tau(V_{F/K}\chi), \end{aligned}$$

and so $\tau(\chi) \equiv \tau(\beta) \bmod (l)$. Trivially $A\rho_{L/K}(D_K) = 1$; also the α_i' occur in complex conjugate pairs and by 3 (c) $\tau(\alpha_i') \equiv -1 \bmod \mathfrak{L}_l$. Thus $\tau(\alpha_i')\,\tau(\overline{\alpha}_i') = 1 \bmod \mathfrak{L}_l$. But by theorems 2 and 3 the left-hand side is $N\mathfrak{f}(\alpha_i')$, an integer. Hence $\tau(\alpha_i')\,\tau(\overline{\alpha}_i') \equiv 1 \bmod (l)$. So now we can conclude that the quotient of the two sides in (6.12) is congruent to $1 \bmod (l)$. But by 6 (a) this quotient is a root of unity so, since $l \neq 2$, the quotient is 1.

From now on then we take $l = 2$, and we consider separately two cases. First we shall assume that

$$\mathrm{Ind}_\Gamma^\Delta \chi = \mathrm{Ind}_\Gamma^\Xi \beta (= \phi \text{ say}),$$

is of inversion type; so that by 6 (f) $\beta|_I$ has order 4. From (5.4) $N\mathfrak{p}_K \equiv -1 \bmod (4)$, and, by the quadratic reciprocity law,

$$\nu_2(N\mathfrak{p}_K) = \left(\frac{2}{N\mathfrak{p}_K}\right)_Q = \left(\frac{2}{\mathfrak{p}_K}\right) = A\alpha_1'(2).$$

From theorem 6 (b) part (i), we get that mod 2 $\mathfrak{L}_2$

$$\begin{aligned} A\alpha_1'(2)\,\tau(\det_\phi)\,A\det_\phi(\mathfrak{p}_K)^{-1} &\equiv \tau(\phi) \\ &\equiv \tau(\beta)\,A\rho_{L/K}(D_K). \end{aligned} \tag{6.14}$$

On the other hand, because F/K is totally ramified, as usual we have

$$\begin{aligned} \tau(\chi) = \tau^{ab}(A\chi) &= \Sigma A\chi(uc^{-1})\,\psi_K(2uc^{-1}) \\ &= A\chi(2)^{-1}\tau^{ab}(A\chi|_K) = AV_{F/K}\chi(2)^{-1}\tau(V_{F/K}\chi). \end{aligned} \tag{6.15}$$

Since $V_{F/K}\chi = \alpha_1' \cdot \det_\phi$, with $\det_\phi$ non-ramified, by theorem 3 (ii) we have

$$\begin{aligned} \tau(\chi)\,\tau(\alpha_1') &= A\alpha_1'(2)^{-1}\tau(\det_\phi)\,A\det_\phi(\mathfrak{p}_K)^{-1}\tau(\alpha_1')^2 \\ &\equiv \tau(\beta)\,A\rho_{L/K}(D_K)\,\tau(\alpha_1')^2 \bmod 2\mathfrak{L}_2 \qquad \text{by (6.14).} \end{aligned}$$

But from theorems 2 and 3 we see that

$$\tau(\alpha_1')^2 \equiv \left(\frac{-1}{N\mathfrak{p}_K}\right) N\mathfrak{p}_K \equiv 1 \bmod (4).$$

So, indeed, by 6 (a), (6.12) holds in this case.

We are left with the case when $\phi = \mathrm{Ind}_K^F \chi$ is not of inversion type. By 6 (f) and (5.4), $N\mathfrak{p}_K \equiv 1 \bmod (4)$, and, by theorem 6 ($b$) part (ii),

$$\begin{aligned}\tau(\beta)\, A\rho_{L/K}(D_K) &= \tau(\phi)\\ &\equiv -\tau(\det_\phi)\, A\det_\phi(2)^{-1}\left(\frac{2}{N\mathfrak{p}_K}\right) \bmod 2\mathfrak{L}_2.\end{aligned}$$

On the other hand, as above in (6.15) we obtain

$$\begin{aligned}\tau(\chi) &= A\alpha_1'(2)^{-1} A\det_\phi(2)^{-1}\tau(\det_\phi)\,\tau(\alpha_1')\, J(\alpha_1', \det_\phi)^{-1}\\ &= \left(\frac{2}{N\mathfrak{p}_K}\right) A\det_\phi(2)^{-1}\tau(\det_\phi)\,[\tau(\alpha_1')\, J(\alpha_1', \det_\phi)^{-1}].\end{aligned}$$

Here
$$\begin{aligned}J(\alpha_1', \det_\phi) &= \frac{\tau(\alpha_1')\,\tau(\det_\phi)}{\tau(\alpha_1' \det_\phi)}\\ &= \sum_{\substack{x+y\equiv 1 \bmod \mathfrak{p}_K\\ xy \not\equiv 0 \bmod \mathfrak{p}_K}} A\alpha_1'(x)\, A\det_\phi(y)\end{aligned}$$

is the Jacobi sum (Davenport & Hasse 1935, (0.6)). (Note it is crucial in the last equation that α_1', $\det_\phi$ and $\alpha_1' \det_\phi = V_{F/K}\chi$ are all ramified. For $V_{F/K}\chi$ and α_1' this is immediate as F/K is totally ramified. Also $\det_\phi = V_{L/K}\beta\cdot\rho_{L/K}$ is ramified as $\rho_{L/K}$ is non-ramified and $V_{L/K}\beta$ is ramified by (5.5)). Hence

$$\frac{\tau(\beta)\, A\rho_{L/K}(D_K)}{\tau(\chi)\,\tau(\alpha_1')} \equiv -\frac{J(\alpha_1', \det_\phi)}{\tau(\alpha_1')^2} \bmod 2\mathfrak{L}_2.$$

As before we see that $\tau(\alpha_1')^2 \equiv 1 \bmod (4)$. To complete the proof, we note that

$$\begin{aligned}J(\alpha_1', \det_\phi) &= \Big(\sum_{y\not\equiv 0,1\, \mathfrak{p}_K} [A\alpha_1'(1-y)+1]\det_\phi(y)\Big)+1\\ &= 2\Big(\sum_{\substack{y\not\equiv 0,1\\ A\alpha_1'(y)=1}} A\det_\phi(y)\Big)+1,\\ &\equiv 2\left(\frac{N\mathfrak{p}_K-3}{2}\right)+1 \bmod 2\mathfrak{L}_2\\ &\equiv -1 \bmod 2\mathfrak{L}_2,\end{aligned}$$

as the number of $y \not\equiv 0$, 1 which are squares mod $\mathfrak{p}_K$ is $\frac{1}{2}(N\mathfrak{p}_K-3)$, and since $N\mathfrak{p}_K \equiv 1 \bmod (4)$. This completes the proof of 6 (h), and so the inductivity of τ is now shown.

Proof of theorem 5 (iii). This now follows straight away from theorem 5 parts (i) and (ii), from theorem 1, from the weak version of 5 (iii) already proved (in 3 (c)), as applied to the Abelian case, and from the fact that $\ker d_{l,\Gamma}$ is generated by virtual characters induced from virtual characters $\alpha_1-\alpha_2$ of sub-groups Δ of Γ with α_1, α_2 Abelian and $\alpha_1-\alpha_2 \in \ker d_{l,\Delta}$ (Deligne 1973, proposition 1.8).

7. Uniqueness

Throughout this section we consider a homomorphism $g\colon R(k) \to \overline{\mathbb{Q}}^*$, such that

(i) $g(\alpha) = \tau^{ab}(A\alpha)$ for $\alpha \in R^{ab}(k)$,

(ii) $g|_{S(k)}$ satisfies the same equations as $\tau|_{S(k)}$ given in theorems 2–4, 5 (iii) and 6. (Recall that $S(k) = \ker(\det\colon R(k) \to R^{ab}(k))$.

We put $\mu(\chi) = \tau(\chi)\, g(\chi)^{-1}$. Our aim is to prove that $\mu(\chi) = 1$ for all $\chi \in R(k)$. Clearly μ is additive and $\mu(\alpha) = 1$ for Abelian characters α. It thus suffices to prove that $\mu(\chi) = 1$ for non-Abelian irreducible χ.

7 (*a*). $\mu(\chi^{\omega}) = \mu(\chi)^{\omega}$ for all $\omega \in \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$, and $\mu(\chi)$ is a root of unity.

Proof. Clearly $S(k)$ and $R^{ab}(k)$ generate $R(k)$. Thus, by conditions (i) and (ii) on g, and by theorems 2–4 as applied to $\tau|_{R(k)^{ab}}$, g will in fact satisfy the same equations as τ as given in theorems 2, 3 and 4 for the whole of $R(k)$.

By theorem 2 it now follows that $\mu(\chi^{\omega}) = \mu(\chi)^{\omega}$. From theorem 4 we see that $\mu(\chi)$ is always a unit, and by theorem 3 (i) $|\mu(\chi)^{\omega}| = 1$, for all $\omega \in \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$. Hence $\mu(\chi)$ is indeed a root of unity.

We shall now work inside $R(N/k)$ for some given normal tame extension field N/k. Because $\mu(\chi) = 1$ whenever $\mathrm{Gal}\,(N/k)$ is Abelian, inductively we shall assume the hypothesis of uniqueness to hold for $R(N'/k)$ whenever N'/k is normal and $[N':k] < [N:k]$. More precisely we shall assume that $\mu(\chi) = 1$ whenever χ is not faithful on Γ.

In the sequel let χ be a faithful irreducible non-Abelian character of $\Gamma = \mathrm{Gal}\,(N/k)$. Let $\chi = \mathrm{Ind}_{\Gamma}^{\Sigma}\alpha$, where α is an Abelian character of a subgroup Σ containing the inertia group I. Because χ is faithful, $\alpha|_I$ is faithful and because the commutator group $[\Sigma, \Sigma] \subset I$, Σ is Abelian.

7 (*b*). If Γ is an l-group, then $\mu(\chi) = 1$.

Proof. Indeed $\chi - \det_{\chi} \in S(k)$, so by theorem 6, which gives formulae for the values of τ (and whence of g) on $\chi - \det_{\chi}$, we see that $\mu(\chi - \det_{\chi}) \equiv 1 \bmod (l)$ (resp. mod $2\mathfrak{L}_2$) if $l \neq 2$ (resp. $l = 2$). Since all roots of unity are distinguished mod (l) if $l \neq 2$ and mod $2\mathfrak{L}_2$ if $l = 2$, we deduce $\mu(\chi - \det_{\chi}) = 1$. Now $\det_{\chi}$ is an Abelian character, so that $\mu(\det_{\chi}) = 1$. Hence we see that $\mu(\chi) = 1$.

7 (*c*). If the order of Σ has two distinct prime divisors, l and q say, then $\mu(\chi) = 1$.

Proof. Let $\alpha = \alpha_l \alpha_q \alpha^*$, where α is an Abelian character of l-power order, α_q one of q-power order and α^* one of order prime to lq. Let

$$\chi^{(l)} = \mathrm{Ind}_{\Gamma}^{\Sigma}(\alpha_q\alpha^*), \quad \chi^{(q)} = \mathrm{Ind}_{\Gamma}^{\Sigma}(\alpha_l\alpha^*), \quad \chi^{(0)} = \mathrm{Ind}_{\Gamma}^{\Sigma}(\alpha^*).$$

Then $\chi - \chi^{(l)}, \chi^{(q)} - \chi^{(0)} \in \ker d_l$, and applying the same reasoning for $\ker d_q$, we see that $\phi = \chi - \chi^{(l)} - \chi^{(q)} + \chi^{(0)}$ is an element of $\ker d_l \cap \ker d_q \cap S(k)$. (The inclusion in $S(k)$ follows by evaluating $\det_{\phi} = V_{\Sigma/L}(\alpha_l\alpha_q\alpha^* \cdot (\alpha_q\alpha^*)^{-1}(\alpha_l\alpha^*)^{-1}\alpha^*) = \epsilon_{\Gamma}$.) By theorem 5 (iii), we get

$$\mu(\phi) \equiv 1 \bmod \mathfrak{L}_l, \quad \mu(\phi) \equiv 1 \bmod \mathfrak{L}_q.$$

Hence $\mu(\phi) = 1$. But $\chi^{(l)}, \chi^{(q)}$ and $\chi^{(0)}$ are faithful on proper quotient groups of Γ, hence, by induction hypothesis, $\mu(\chi^{(l)}) = \mu(\chi^{(q)}) = \mu(\chi^{(0)}) = 1$, and so we see $\mu(\chi) = 1$.

We are now left with the case when Σ has l-power order, but when Γ does not have l-power order. We now consider this situation in the following:

7 (*d*). Suppose that Σ has l-power order and that Γ/Σ has a sub-group Ξ of order $m > 1$, prime to l which acts faithfully on $I\ (= I_l)$. Then $\mu(\chi) = 1$.

Proof. We remark that because $\mathrm{Aut}\,(I_2)$ is a 2-group we must have $l \neq 2$.

The Abelian l-group Σ is a module over the integral group ring $\mathbb{Z}_l\Xi$ (where Ξ acts via conjugation). Because $m \mid l-1$, and because $\mathbb{Z}_l^*$ contains the $(l-1)$st roots of unity, Σ splits up into a sum of one-dimensional modules. We let B (resp. A) be the sum of the one-dimensional modules with trivial (resp. non-trivial) action. As Ξ acts trivially on Σ/I, we see that $A \subset I$, and, since Ξ acts on I with no fixed points except 1, we see that $A = I$ and so we have a decomposition

$$\Sigma = I \times B. \qquad (7.1)$$

We may write $\alpha = \beta\phi$, where $\beta|_B = \epsilon$, $\phi|_I = \epsilon$. Thus ϕ is the restriction to Σ of a non-ramified character ϕ' of Γ. Now let $\xi = \mathrm{Ind}_\Gamma^\Sigma \beta$. By Frobenius reciprocity $\chi = \phi' \cdot \xi$, and by theorem 3 (ii), we see that $\mu(\chi) = \mu(\xi)$. If $B \neq \{1\}$, then ξ is a character of a proper quotient of Γ and so $\mu(\xi) = 1$, and hence $\mu(\chi) = 1$.

So now we assume that $B = \{1\}$. The action of Γ/Σ on I yields a dual action on the powers of α, and in fact – denoting the field of values of α by $\mathbb{Q}(\alpha)$ – we have an injective group homomorphism

$$j\colon \Gamma/\Sigma \to \mathrm{Gal}\,(\mathbb{Q}(\alpha)/\mathbb{Q})$$

given by

$$\alpha(\sigma^\omega) = \alpha(\sigma)^{j(\omega)}.$$

This implies that $\mathbb{Q}(\chi) \subset \mathbb{Q}(\alpha)^{\mathrm{Im}\,(j)}$. Because $\mathrm{Im}\,(j)$ possesses a subgroup of order m prime to l, $m > 1$, the only lth root of unity in $\mathbb{Q}(\alpha)^{\mathrm{Im}\,(j)}$, and hence in $\mathbb{Q}(\chi)$, is 1.

If $\epsilon_* = \mathrm{Ind}_\Gamma^\Sigma \epsilon$, we see that $\det_{\chi-\epsilon_*} = V_{\Sigma/\Gamma}\,\alpha$ is a character of l-power order with values in $\mathbb{Q}(\chi) = \mathbb{Q}(\chi - \epsilon_*)$, hence $\det_{\chi-\epsilon_*} = \epsilon_\Gamma$. Thus we see $\chi - \epsilon_* \in \ker d_l \cap S(k)$, and so, by theorem 5 (iii)

$$\mu(\chi - \epsilon_*) \equiv 1 \bmod \mathfrak{L}_l.$$

But, by 7 (*a*), $\mu(\chi - \epsilon_*) \in \mathbb{Q}(\chi - \epsilon_*)$, which possesses no l-power roots of unity except 1. So, because roots of unity of order prime to l are distinguished mod $\mathfrak{L}_l$, $\mu(\chi - \epsilon_*) = 1$ and thus $\mu(\chi) = 1$, since ϵ_* is a character of a proper quotient of Γ.

8. Real-valued characters

In this section we study the subgroup of real-valued virtual characters of $R(K)$, which we denote by $R_{\mathbb{R}}(K)$. Throughout this section we shall assume p to be odd. (The case $p = 2$ is easier, but different.) Modulo the group of virtual characters of the form $\phi + \bar\phi$ ($\bar\phi$ being the complex conjugate of ϕ), $R_{\mathbb{R}}(K)$ is generated by irreducible real valued characters (see Serre 1971, 13.2). Let Δ be a finite group. A representation T of Δ, and the corresponding character ϕ, are called dihedral (resp. quaternion) if there exist generators σ, ω of Δ mod ker T, such that

$$T(\sigma) = \begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix}, \quad T(\omega) = \begin{cases} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{(dihedral)}, \\[1ex] \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \text{(quaternion)}, \end{cases}$$

where η is a primitive mth root of unity for $m > 2$.

Again we adopt the notations used in previous sections. In particular $\Gamma = \mathrm{Gal}\,(N/K)$.

Proposition 3. *Let χ be an irreducible real-valued character of Γ. Then either* (i) *χ is Abelian* (i.e. *χ is quadratic or $\chi = \epsilon_\Gamma$*), *or* (ii) *there exists a subgroup $\Delta, I \subset \Delta$ and a character ϕ of Δ, which is either dihedral or quaternion, so that $\chi = \mathrm{Ind}_\Gamma^\Delta \phi$. χ determines Δ uniquely and determines ϕ uniquely up to conjugacy, i.e. to within the substitution $\phi \mapsto {}^\gamma\phi$ for $\gamma \in \Gamma$. Conversely, characters of the form $\chi = \mathrm{Ind}_\Gamma^\Delta \phi$, where Δ is the stabilizer of ϕ and where ϕ is dihedral or quaternion, are both real valued and irreducible.*

Proof. We use the earlier result 3 (*a*). Let $\chi = \mathrm{Ind}_\Gamma^\Sigma \alpha$, with $\Sigma \supset I$ and α an Abelian character of Σ. As χ is real valued, we also have $\chi = \mathrm{Ind}_\Gamma^\Sigma \bar\alpha$ whence there exists $\omega \in \Gamma$ with ${}^\omega\alpha = \bar\alpha = \alpha^{-1}$. Clearly ${}^{\omega^2}\alpha = \alpha$, i.e. $\omega^2 \in \Sigma$. We now take $\Delta = \langle \Sigma, \omega \rangle$. Because ${}^\omega\alpha = \bar\alpha$ we see that $\ker \alpha \lhd \Delta$. We choose $\sigma \in \Sigma$ with image a generator of the cyclic group $\Sigma/\ker\alpha$. Then ω and σ generate Δ mod $\ker\alpha$, and now we put $\eta = \alpha(\sigma)$. The remainder of the proposition is now immediate.

If χ is an irreducible real-valued non-Abelian character we adopt the following notation. With Σ and Δ as in the proof of the previous proposition we write $N^{\Sigma} = L$ and $N^{\Delta} = E$. We say that χ is of dihedral type (resp. of quaternion type) if the character ϕ (as above) is of dihedral type (resp. of quaternion type). There is a simple criterion for distinguishing between dihedral and quaternion type. Recall that $\det_{\phi} = \rho_{L/E} \cdot V_{L/E}\, \alpha$ is now non-ramified.

Proposition 4. *Let χ be irreducible, real valued and non-Abelian. Then either* (i) *χ is of quaternion type and* $\det_{\chi} = \epsilon_{\Gamma}$, *so that in particular* $A \det_{\chi}(\mathfrak{p}_K) = 1$, *or* (ii) *$\chi$ is of dihedral type and* $A \det_{\chi}(\mathfrak{p}_K) = -1$; *in particular* $\det_{\chi} \neq \epsilon_{\Gamma}$.

Proof. This is clearly true if $K = E$, i.e. if $\chi = \phi$. But, as $\deg(\phi) = 2$, from the general formula for the determinant of an induced character we get $\det_{\chi} = V_{E/K} \det_{\phi} \cdot \rho_{E/K}^{\deg(\phi)}$, i.e.

$$\det_{\chi} = V_{E/K} \det_{\phi}. \tag{8.1}$$

Since E/K is non-ramified, $\mathfrak{O}_E \mathfrak{p}_K = \mathfrak{p}_E$, and so by (2.2) we conclude that

$$A \det_{\chi}(\mathfrak{p}_K) = A \det_{\phi}(\mathfrak{p}_E). \tag{8.2}$$

The result is now immediate.

We shall be specifically interested in values of τ on real valued virtual characters with determinant ϵ_{Γ}, or, which is the same, on virtual characters of the form $\chi - \det_{\chi}$, where χ is real valued.

Theorem 8. (i) *If χ is a real-valued virtual character, then the Artin conductor $\mathfrak{f}(\chi - \det_{\chi})$ is the square of an ideal (in K), and $\tau(\chi - \det_{\chi})$ is a rational number and a 2-adic unit.*

(ii) *Let $u(\chi) = \pm 1$ be such that*

$$u(\chi) \equiv \tau(\chi - \det_{\chi}) \bmod (4).$$

Then
$$u(\chi)\left(\frac{-1}{N\mathfrak{f}(\chi - \det_{\chi})^{\frac{1}{2}}}\right) = W(\chi - \det_{\chi}) = \operatorname{sign}(\tau(\chi - \det_{\chi})),$$

where $W(\chi - \det_{\chi})$ is the local root number defined in (1.4).

Also $u(\chi)$ is given by the following:

(*a*) *If χ is irreducible non-Abelian, and if e_{χ} denotes the order of $I/\ker(\chi|_I)$, then*

$$\begin{aligned} u(\chi) &= -\left(\frac{-1}{N\mathfrak{p}_K}\right)^{\frac{1}{2}\deg(\chi)} A \det_{\chi}(\mathfrak{p}_K) && \text{if} \quad e_{\chi} \equiv 1 \bmod (2), \\ &= A \det_{\chi}(\mathfrak{p}_K) && \text{if} \quad e_{\chi} \equiv 2 \bmod (4), \\ &= A \det_{\chi}(\mathfrak{p}_K)\, \nu_N(N\mathfrak{p}_K) && \text{if} \quad e_{\chi} \equiv 0 \bmod (4), \\ & && \text{where} \quad 2^N \| e_{\chi}. \end{aligned}$$

(*b*) *If $\chi = \phi + \bar{\phi}$, then*

$$u(\chi) = A \det_{\phi}(-1)\left(\frac{-1}{N\mathfrak{f}(\phi)}\right).$$

(*c*) *If χ is Abelian, then* $u(\chi) = 1$.

(*d*) *For any real-valued virtual characters χ, ξ*

$$u(\chi + \xi)/u(\chi)\, u(\xi) = [\det_{\chi}, \det_{\xi}],$$

where for real Abelian characters α, β

$$[\alpha, \beta] = \begin{cases} 1 & \text{if} \quad \alpha \text{ or } \beta \text{ is } \epsilon, \\ A \det_{\alpha}(-1) & \text{if} \quad \alpha\beta = \epsilon, \\ -1 & \text{if} \quad \alpha, \beta, \alpha\beta \text{ are all different from } \epsilon. \end{cases}$$

Remark 1. It is clear now that for real-valued χ, with $\det_\chi = \epsilon$, the Galois Gauss sum is determined uniquely by either (1*a*) the modulus equation $|\tau(\chi)| = N\mathfrak{f}(\chi)^{\frac{1}{2}}$ (see theorem 3 (i)), or (1*b*) the ideal equation $(\tau(\chi)) = (\mathcal{N}_{K/\mathbb{Q}_p} P(\chi))$, and, in addition, either (2*a*) the congruence $\tau(\chi) \equiv u(\chi) \bmod (4)$, or (2*b*) the 'congruence at infinity' sign $(\tau(\chi)) = W(\chi)$.

Also, from the equation

$$W(\chi) = u(\chi)\left(\frac{-1}{|\tau(\chi)|}\right),$$

we see that the above theorem determines not only $u(\chi)$, but also $W(\chi)$.

Remark 2. It is clear from the above theorem that the restriction of τ to real-valued characters of trivial determinant may be viewed as a function into any ring in which p is a unit.

Proof. If first χ is an actual character, then we re-word the definition of $\mathfrak{f}(\chi)$. Let n_χ be the number of eigenvalues, distinct from 1, of a fixed generator of I under the representation associated with χ. Then $\mathfrak{f}(\chi) = \mathfrak{p}_K^{n_\chi}$. As χ is real valued, the non-real eigenvalues occur in complex conjugate pairs, and so $n_{\det_\chi} \equiv n_\chi \bmod (2)$. Thus we see $\mathfrak{f}(\chi - \det_\chi)$ is a square.

Observe that for any virtual characters χ, ξ we have

$$\chi - \det_\chi + \xi - \det_\xi = (\chi + \xi - \det_{\chi+\xi}) + (\det_\xi \det_\chi - \det_\chi - \det_\xi).$$

Now for quadratic Abelian characters α, β,

$$\mathfrak{f}(\alpha\beta - \alpha - \beta) = 1$$

if at least one of α, β is non-ramified, and

$$\mathfrak{f}(\alpha\beta - \alpha - \beta) = \mathfrak{p}_K^{-2}$$

otherwise.

So if χ is a virtual character, choose an actual character ξ such that $\chi + \xi$ is an actual character. By the above $\mathfrak{f}(\chi - \det_\chi + \xi - \det_\xi)$ and $\mathfrak{f}(\xi - \det_\xi)$ are squares, whence $\mathfrak{f}(\chi - \det_\chi)$ is a square.

Because $\chi - \det_\chi$ is real valued and has determinant ϵ, we conclude from theorem 2 that $\tau(\chi - \det_\chi)$ is a real number. So because by theorem 3 (i) $|\tau(\chi - \det_\chi)| = N\mathfrak{f}(\chi - \det_\chi)^{\frac{1}{2}}$ and because $N\mathfrak{f}(\chi - \det_\chi)^{\frac{1}{2}}$ is rational, we deduce that $\tau(\chi - \det_\chi)$ is rational and moreover as p is odd $\tau(\chi - \det_\chi)$ must be a 2-adic unit.

The first part of theorem 8 (ii) is immediate since

$$N\mathfrak{f}(\chi - \det_\chi)^{\frac{1}{2}}\left(\frac{-1}{N\mathfrak{f}(\chi - \det_\chi)}\right) \equiv 1 \bmod (4).$$

Now suppose that, as in proposition 3, $\chi = \operatorname{Ind}_K^E \phi$, $\phi = \operatorname{Ind}_E^L \alpha$, where ϕ is either a dihedral or a quaternion character. Then

$$\tau(\chi) = \tau(\phi)\, A\rho_{E/K}(D_E)^2 = \tau(\phi)$$

and by (8.1)

$$\begin{aligned}\tau(\det_\chi) &= \tau(V_{E/K} \det_\phi) = AV_{E/K} \det_\phi(D_K)^{-1}\\ &= A \det_\phi(D_E)^{-1} = \tau(\det_\phi).\end{aligned}$$

Thus

$$\tau(\chi - \det_\chi) = \tau(\phi - \det_\phi). \tag{8.3}$$

The argument leading up to (5.7), in the case when β was a 2-character, still applies with $A\alpha$ in place of β, and we get

$$\tau(\alpha) = AV_{L/E}\,\alpha(\mathfrak{p}_E)^{-1}\tau(V_{L/E}\,\alpha)\, N\mathfrak{p}_E\, A\alpha(d),$$

where $L = E(d)$ and $d^2 \in \mathfrak{O}_E^*$. This yields

$$\tau(\phi - \det_\phi) = -N\mathfrak{p}_E \cdot A \det_\phi(\mathfrak{p}_E)^{-1} A\alpha(d). \tag{8.4}$$

If $e_\phi(=e_\chi) \equiv 0 \bmod (4)$, then $N\mathfrak{p}_E \equiv -1 \bmod (4)$ and, as in 5 (*b*), we see that $\alpha(d) = \nu_N(N\mathfrak{p}_E)$, where $2^N \| e_\chi$. This then gives

$$\tau(\phi - \det_\phi) \equiv A \det_\phi(\mathfrak{p}_E)^{-1} \nu_N(N\mathfrak{p}_E) \bmod 2\mathfrak{L}_2.$$

In this case, because $N\mathfrak{p}_E = N\mathfrak{p}_K^{[E:K]} \equiv -1 \bmod (4)$, we see that $[E:K]$ is odd. Thus $\nu_N(N\mathfrak{p}_E) = \nu_N(N\mathfrak{p}_K)$, and so, by (8.2) and (8.3), we obtain the required result for this case.

If now $e_\chi \equiv 2 \bmod (4)$, then easily we have $\alpha(d) = -\left(\frac{-1}{N\mathfrak{p}_E}\right)$, and so, by (8.4) and (8.3),

$$\tau(\phi - \det_\phi) \equiv A \det_\phi(\mathfrak{p}_E) = A \det_\chi(\mathfrak{p}_K).$$

Hence, by (8.2), we obtain the required result.

If e_χ is odd, then $\alpha(d) = 1$ and, as always, $N\mathfrak{p}_E = N\mathfrak{p}_K^{\frac{1}{2}\deg(\chi)}$. So again, by (8.2), (8.3), and (8.4), we are done.

To show part (*b*), we observe that from theorem 2 and theorem 3 (*i*)

$$N\mathfrak{f}(\phi) = \tau(\phi + \overline{\phi})\, A \det_\phi(-1).$$

Part (*c*) is trivial since for Abelian χ

$$\tau(\chi - \det_\chi) = \tau(0) = 1.$$

For part (*d*) we evaluate $\tau(\alpha)\,\tau(\beta)\,\tau(\alpha\beta)^{-1}$ and show it is equal to $[\alpha, \beta]$. If α or β is ϵ the result is clear. If $\alpha\beta = \epsilon$, then $\alpha = \beta$, and so the result follows from part (*b*). Finally, if $\alpha, \beta, \alpha\beta$ are different from ϵ, then one of them, α say, is non-ramified. So, by theorem 3 (ii), the quotient is $A\alpha(\mathfrak{p}_K) = -1$, and similarly if β, or $\alpha\beta$, is non-ramified.

Lastly as
$$(\chi + \xi - \det_{\chi+\xi}) - (\chi - \det_\chi) - (\xi - \det_\xi) = \det_\chi + \det_\xi - \det_{\chi+\xi}$$
we obtain the remaining equation by the additivity of τ.

Remark 1. Instead of looking at virtual characters of determinant ϵ, one could have considered the group of real-valued virtual characters of determinant ϵ and degree zero. This group behaves better with respect to induction. The question of values of τ is the same, because we always have that
$$\tau(\phi) = \tau(\phi - \deg(\phi)\cdot\epsilon).$$

Remark 2. One can also determine explicitly the values of $\tau(\alpha)$, for α real and Abelian. The non-ramified case presents no problem. For ramified α, choose $c \in K^*$ as in (3.6), so that

$$\tau(\alpha) = -A\alpha(c^{-1})\, G(A\alpha).$$

Viewing $A\alpha$ as a residue class character of $\tilde{K}^*$, we see that $A\alpha$ is given by composing the Legendre symbol $\left(\frac{-}{p}\right)$ with $N_{\tilde{K}/\mathbb{F}_p}$. So by (3.4)

$$G(A\alpha) = G\left(\left(\frac{-}{p}\right)\right)^{(K:\mathbb{F}_p)}.$$

It is a classical result (see, for instance, Borevich & Shafarevich 1967) that

$$G\left(\left(\frac{-}{p}\right)\right) = \left(\left(\frac{-1}{p}\right)p\right)^{\frac{1}{2}}$$

(with the positive or positive imaginary square root). Thus

$$\tau(\alpha) = -A\alpha(c^{-1})\left(\left(\frac{-1}{p}\right)p\right)^{\frac{1}{2}[K:\mathbb{F}_p]}.$$

So if $[\tilde{K}:\mathbb{F}_p] \equiv 0 \bmod (2)$, then $\tau(\chi)$ is rational for all (tame) real-valued χ, and $W(\chi) = \pm 1$.

References

Armitage, J. V. 1972 Zeta functions with a zero at $s = \frac{1}{2}$. *Invent. Math.* **15**, 199–207.

Borevich, Z. I. & Shafarevich, I. R. 1967 *Number theory*, 2nd edn. London: Academic Press.

Cassels, J. W. S. & Fröhlich, A. (eds.) 1967 *Algebraic number theory*. London: Academic Press.

Cassou-Noguès, Ph. 1978 Quelques théorèmes de base normale d'entiers, *Annls Inst. Fourier, Grenoble*, **28** (3), 1–33.

Cassou-Noguès, Ph. 1979 Structure Galoisienne des anneaux d'entiers. *Proc. Lond. Math. Soc.* **38**, 545–576.

Coates, J. 1977 *p*-adic *L*-functions and Iwasawa's theory. In *Algebraic Number fields* (ed. A. Fröhlich). London: Academic Press.

Davenport, H. & Hasse, H. 1935 Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *J. reine agnew. Math.* **172**, 151–182.

Deligne, P. 1973 Les constantes des equations fonctionelles des fonctions L. *Modular forms in one variable II*, Lecture Notes in Mathematics, vol. 349, pp. 501–597.

Dwork, B. 1956 On the Artin root number. *Am. J. Math.* **78**, 444–472.

Fröhlich, A. 1974 Artin root numbers, conductors and representations for generalized quaternion groups. *Proc. Lond. Math. Soc.* **28**, 402–438.

Fröhlich, A. 1975 Resolvents and trace form. *Proc. Camb. Phil. Soc.* **78**, 185–210.

Fröhlich, A. 1976 Arithmetic and Galois module structure for tame extensions, *J. reine agnew. Math.* **286/7**, 380–440.

Fröhlich, A. 1977 Symplectic local constants and hermitian Galois module structure. In *Algebraic number theory* (ed. S. Iyanaga). Tokyo, Japan: Society for the promotion of science.

Fröhlich, A. *Galois module structure of rings of integers*. Ergebnisse: Springer. (In preparation.)

Fröhlich, A. & Queyrut, J. 1971 On the functional equation of the Artin *L*-function for characters of real representations. *Invent. Math.* **14**, 173–183.

Hasse, H. 1954 Artinsche Führer, Artinsche *L*-Funktionen and Gaussche Summen über endlich algebraischen Zahlkörpern. *Acta Salamantioensia*.

Macdonald, I. G. Zeta functions attached to finite general linear groups. (In preparation.)

Martinet, J. 1977 Character theory and Artin *L*-functions. In *Algebraic number fields* (ed. A. Fröhlich). London: Academic Press.

Noether, E. 1932 Normalbasis bei Körpern ohne höhere Verzweigung. *J. reine agnew. Math.* **167**, 147–152.

Serre, J.-P. 1971 *Représentations linéaires des groupes finis*, 2nd edn. Paris: Hermann.

Tate, J. 1977 Local constants. In *Algebraic number fields* (ed. A. Fröhlich). London: Academic Press.

Taylor, M. J. 1979 Adams operations, local root numbers and the Galois module structure of rings of integers. *Proc. Lond. Math. Soc.* **39** (3), 147–175.