

Werk

Titel: Inventiones Mathematicae

Verlag: Springer

Jahr: 1981

Kollektion: Mathematica

Werk Id: PPN356556735_0063

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN356556735_0063 | LOG_0010

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

On Fröhlich's Conjecture for Rings of Integers of Tame Extensions[★]

M.J. Taylor

Queen Mary College, Mile End Road, London E1 4NS, England and
E.R.A. C.N.R.S. no. 070654, F-25030 Besançon, Cedex, France

Introduction and Results

Let M/N be a tame Galois extension of number fields with $\Gamma = \text{Gal}(M/N)$. By Noether's theorem (cf. [N]) we know that the ring of integers of M , $\mathfrak{O}_M$, is a locally free $\mathbb{Z}\Gamma$ module. For a character χ of Γ , we let $A(s, \chi)$ be the "extended" Artin L -function associated to χ (cf. [M2]). Then

$$\begin{aligned} A(s, \chi) &\text{ satisfies a functional equation} \\ A(s, \chi) &= W(\chi) A(1-s, \bar{\chi}) \end{aligned}$$

where $\bar{\chi}$ is the complex conjugate of χ . The constant $W(\chi)$ is called the Artin root number of χ .

In [M1] J. Martinet showed that $\mathfrak{O}_M$ is not always a free $\mathbb{Z}\Gamma$ -module when $N = \mathbb{Q}$ and when Γ is a quaternion group of order 8. Subsequently, in [F5], A. Fröhlich showed that the class of $\mathfrak{O}_M$, in this special case, is determined by the sign of the Artin root number of the irreducible symplectic character of Γ .

We now return to the general case and let $Cl(\mathbb{Z}\Gamma)$ be the class group of locally free $\mathbb{Z}\Gamma$ -modules. Given a locally free $\mathbb{Z}\Gamma$ -module X , we denote its class by (X) . Philippe Cassou-Noguès defined a class $t(W)$ in $Cl(\mathbb{Z}\Gamma)$ which is defined solely in terms of the values of Artin root numbers of symplectic characters (this class will be defined in §2). After numerous computations by Fröhlich et al. (cf. [F6], [C], [T3] for instance), Fröhlich conjectured the result given below which we prove in this paper.

Theorem 1. $(\mathfrak{O}_M) = t(W)$, and so in particular

- (a) as the Artin root numbers of symplectic characters are ± 1 , $(\mathfrak{O}_M)^2 = 1$.
- (b) the only obstructions to the vanishing of the class of $\mathfrak{O}_M$, are the signs of the Artin root numbers of symplectic characters.

Corollary. If further $|\Gamma|$ is odd then $\mathfrak{O}_M$ is a free $\mathbb{Z}\Gamma$ -module.

[★] The work for this paper was done whilst I received financial support from the C.N.R.S. and the kind hospitality of the University of Besançon.

Proof. As Γ is of odd order, it has no irreducible symplectic characters (cf. 8.1 of [S]). Thus we deduce firstly that $(\mathfrak{D}_M)=1$ and secondly that the group algebra $\mathbb{Q}\Gamma$ satisfies the Eichler condition i.e. no simple component of $\mathbb{Q}\Gamma$ is a totally definite quaternion algebra. So, by Jacobinski's Cancellation theorem, (cf. Sect. 3 of [F3] for example) we know that $\mathbb{Z}\Gamma$ possesses the cancellation property, and thus $\mathfrak{D}_M$ is a free $\mathbb{Z}\Gamma$ -module.

Remark. For example of groups where $t(W)$ is not 1 see §14 of [F1], [F6] and [C].

In Sect. 2 we give Fröhlich's description of $Cl(\mathbb{Z}\Gamma)$ and of his representative for $(\mathfrak{D}_M)$. Then, using an important new logarithmic approach given in [T1], we explain the strategy of the proof. It is of particular interest that in the proof, when we apply this logarithmic method to the Gauss sum homomorphism, we obtain remarkably simple and beautiful results (cf. Theorem 5). Sections 9 and 10 of this paper are, in essence, concerned with checking the torsion that is thrown away by the logarithm.

I would like to express my warmest thanks to A. Fröhlich for the interest he has shown and the encouragement he has given me in my research.

1. Notation

$\mathbb{Q}$ is the field of rationals and $\mathbb{Z}$ is the ring of integers. $\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in the field of complex numbers. For a number field $L \subset \bar{\mathbb{Q}}$, we write $\Omega_L = \text{Gal}(\bar{\mathbb{Q}}/L)$ and we denote the ring of integers of L by $\mathfrak{D}_L$. If l is a rational prime number, then we let $\mathbb{Q}_l$ be the field of l -adic numbers and $\mathbb{Z}_l$ be the ring of l -adic integers. We write $L_l = L \otimes_{\mathbb{Q}} \mathbb{Q}_l$ and $\mathfrak{D}_{L_l} = \mathfrak{D}_L \otimes_{\mathbb{Z}} \mathbb{Z}_l$. We denote the Jacobson radical of $\mathfrak{D}_{L_l}$ by $\mathfrak{r}_{L_l}$ and we put

$$U_l = \varinjlim_{L \subset \bar{\mathbb{Q}}} \mathfrak{D}_{L_l}^* \quad \mathfrak{L}_l = \varinjlim_{L \subset \bar{\mathbb{Q}}} \mathfrak{r}_{L_l}.$$

Then U_l and $\mathfrak{L}_l$ are $\Omega_{\mathbb{Q}}$ -modules in the natural way. Likewise we define $\bar{\mathfrak{D}}^* = \varinjlim \mathfrak{D}_L^*$. If S is a finite set of rational prime numbers we define $U_S = \prod_{l \in S} U_l$.

Suppose now that Γ is an arbitrary finite group. We denote the Grothendieck group of virtual characters of Γ by R_{Γ} . We shall always denote the identity character of Γ by ε_{Γ} . If $\chi \in R_{\Gamma}$, then it is well known that the central function $\psi^n(\chi)$, which is defined by $\psi^n(\chi)(\gamma) = \chi(\gamma^n)$, for $\gamma \in \Gamma$ and n a positive integer, is in fact a virtual character of Γ (cf. 9.1 of [S] for instance). The $\psi^n: R_{\Gamma} \rightarrow R_{\Gamma}$ are known as the Adams operations.

Now let Δ be a sub-group of Γ . Then we have the induction and restriction homomorphisms

$$\text{Ind}_{\Delta}^{\Gamma}: R_{\Delta} \rightarrow R_{\Gamma} \quad \text{Res}_{\Delta}^{\Gamma}: R_{\Gamma} \rightarrow R_{\Delta}.$$

If Δ is normal in Γ and if α is an abelian character of Δ , then for $\gamma \in \Gamma$ we denote by α^{γ} the abelian character given by $\alpha^{\gamma}(\delta) = \alpha(\gamma\delta\gamma^{-1})$, for $\delta \in \Delta$.

Next we suppose we are given a surjection $u: \Gamma \rightarrow \Sigma$. Then composition with u yields an injection $\text{Inf}_\Sigma^F: R_\Sigma \rightarrow R_\Gamma$, which we call inflation from Σ to Γ . Let $\text{ver}_\Gamma^\Sigma: \Gamma^{ab} \rightarrow \Sigma^{ab}$ be the transfer from $\Gamma^{ab} (= \Gamma/[\Gamma, \Gamma])$ to Σ^{ab} . Dually, if α is an abelian character of Σ , we may view α as a character of Σ^{ab} , compose this with ver_Γ^Σ and inflate from Γ^{ab} to Γ . We denote the resulting character (the co-transfer of α) by $v_\Sigma^F \alpha$.

If χ is a character of Γ we denote by $L(\chi)$ the field obtained by adjoining to L the values of χ . Similarly, if m is a positive integer, then $L(m)$ is the field obtained by adjoining the m^{th} roots of unity to L .

Next we choose a rational prime l , and we denote by $\text{Hom}_{\Omega_L}(R_\Gamma, U_l)$ the group of homomorphisms from R_Γ to U_l which commute with Ω_L action. Here we view Ω_L as acting on R_Γ value-wise.

Let χ be a character of Γ which is afforded by a representation $T: \Gamma \rightarrow GL_n(F)$. We denote by $\det(\chi)$ or $\det_\chi$, the abelian character given by composing T with the determinant homomorphism $GL_n(F) \rightarrow F^*$. We then extend $\det$ to a group homomorphism on R_Γ by $\mathbb{Z}$ -linearly and we extend T to a ring homomorphism

$$T: \mathfrak{D}_{L_l} \Gamma \rightarrow M_n(L \cdot F \otimes_{\mathbb{Q}} \mathbb{Q}_l).$$

Then, for any $x \in \mathfrak{D}_{L_l} \Gamma^*$, we write

$$\text{Det}(x)(\chi) = \det(T(x)).$$

It is immediate that the right-hand side depends only on the character of T . In this way we view $\text{Det}(x)$ as a homomorphism from R_Γ to U_l . From Proposition 1.4 of [F1] we know that $\text{Det}(x)$ commutes with Ω_L action. We denote the resulting sub-group of $\text{Hom}_{\Omega_L}(R_\Gamma, U_l)$, obtained by the various $\text{Det}(x)$, by $\text{Det}(\mathfrak{D}_{L_l} \Gamma^*)$. Indeed, it is easily seen that $\text{Det}(\mathfrak{W}^*) = \text{Hom}_{\Omega_L}(R_\Gamma, U_l)$, where $\mathfrak{W}$ is a maximal order of $L_l \Gamma$ which contains $\mathfrak{D}_{L_l} \Gamma^*$, and so, in particular, the sub-group $\text{Det}(\mathfrak{D}_{L_l} \Gamma^*)$ is of finite index in $\text{Hom}_{\Omega_L}(R_\Gamma, U_l)$.

More generally, if S is a finite set of rational prime numbers, then we put $\text{Det}(\mathfrak{D}_{L_S} \Gamma^*) = \prod_{l \in S} \text{Det}(\mathfrak{D}_{L_l} \Gamma^*)$.

Next we consider certain functorial properties of the Det -groups. We suppose $\Delta \subset \Gamma$, then from Appendices VII and VIII of [F1] we have homomorphisms

$$\text{Ind}_\Delta^F: \text{Det}(\mathfrak{D}_{L_l} \Delta^*) \rightarrow \text{Det}(\mathfrak{D}_{L_l} \Gamma^*),$$

$$\text{Res}_F^\Delta: \text{Det}(\mathfrak{D}_{L_l} \Gamma^*) \rightarrow \text{Det}(\mathfrak{D}_{L_l} \Delta^*),$$

where explicitly for $x \in \mathfrak{D}_{L_l} \Delta^*$, $y \in \mathfrak{D}_{L_l} \Gamma^*$, $\chi \in R_\Gamma$, $\phi \in R_\Delta$,

$$\text{Ind}_\Delta^F(\text{Det}(x))(\chi) = \text{Det}(x)(\text{Res}_F^\Delta \chi),$$

$$\text{Res}_F^\Delta(\text{Det}(y))(\phi) = \text{Det}(y)(\text{Ind}_\Delta^F \phi).$$

Let $R_{\mathbb{Q}}(\Gamma)$ be the sub-ring of R_Γ which is generated by those characters of Γ which can be realised over $\mathbb{Q}$. Following an idea of Swan, Ullom showed that

$\text{Det}(\mathfrak{D}_{L_l} \Gamma^*)$ is an $R_{\mathbb{Q}}(\Gamma)$ -module via the rule that for $\theta \in R_{\mathbb{Q}}(\Gamma)$, $\chi \in R_{\Gamma}$, $x \in \mathfrak{D}_{L_l} \Gamma^*$

$$(\theta \cdot \text{Det}(x))(\chi) = \text{Det}(x)(\chi\theta).$$

(For proof that this multiplication preserves $\text{Det}(\mathfrak{D}_{L_l} \Gamma^*)$ see [U] or [F4]).

Lastly we remark that throughout this paper we shall refer to finite field extensions of $\mathbb{Q}_l$ as local fields (of residual characteristic l).

2. Classgroups and Strategy of Proof

Let $\mathfrak{M}$ be any maximal order in $\mathbb{Q}\Gamma$ which contains $\mathbb{Z}\Gamma$, and let $Cl(\mathfrak{M})$ be the locally free classgroup of $\mathfrak{M}$. Then extension of scalars induces a homomorphism $Cl(\mathbb{Z}\Gamma) \rightarrow Cl(\mathfrak{M})$. We shall denote the kernel of this homomorphism by $D(\mathbb{Z}\Gamma)$. It is well known that $D(\mathbb{Z}\Gamma)$ is independent of the particular choice of $\mathfrak{M}$. Our reason for introducing $D(\mathbb{Z}\Gamma)$, is that, following a conjecture of Martinet, Fröhlich showed that $(\mathfrak{D}_M) \in D(\mathbb{Z}\Gamma)$, i.e. $\mathfrak{D}_M$ becomes stably free over $\mathfrak{M}$. We now proceed to give Fröhlich's description of $D(\mathbb{Z}\Gamma)$ (cf. Appendix 11.2 of [F1]).

Let $\text{Hom}_{\Omega_{\mathbb{Q}}^+}(R_{\Gamma}, \bar{\mathfrak{D}}^*)$ be that sub-group of $\Omega_{\mathbb{Q}}$ -homomorphisms from R_{Γ} to $\bar{\mathfrak{D}}^*$, whose values on symplectic characters are totally positive. Let S be the set of prime divisors of $|\Gamma|$. We view $\text{Hom}_{\Omega_{\mathbb{Q}}^+}(R_{\Gamma}, \bar{\mathfrak{D}}^*)$ as a sub-group of $\text{Hom}_{\Omega_{\mathbb{Q}}}(R_{\Gamma}, U_S)$ via the diagonal embedding $\bar{\mathfrak{D}}^* \hookrightarrow U_S$. Then

$$(2.1) \quad D(\mathbb{Z}\Gamma) \cong \frac{\text{Hom}_{\Omega_{\mathbb{Q}}}(R_{\Gamma}, U_S)}{\text{Det}(\mathbb{Z}_S \Gamma^*) \cdot \text{Hom}_{\Omega_{\mathbb{Q}}^+}(R_{\Gamma}, \bar{\mathfrak{D}}^*)}.$$

We now wish to introduce a homomorphism which represents the class $(\mathfrak{D}_M)$ under the above isomorphism (cf. (9.4) of [F1]).

By Noether's theorem loc. cit. we can find $a \in \mathfrak{D}_M$ so that for all $l \in S$

$$a \cdot \mathfrak{D}_{N_l} \Gamma = \mathfrak{D}_{M_l}.$$

Let $\hat{M}$ be the normal closure of $M/\mathbb{Q}$ in $\bar{\mathbb{Q}}$, and let $\{\sigma\}$ be a right transversal of Ω_N in $\Omega_{\bar{\mathbb{Q}}}$. Then we define $A \in \mathfrak{D}_{\hat{M}} \Gamma$ by

$$(2.2) \quad A = \prod_{\sigma} \left(\sum_{\gamma \in \Gamma} a^{\gamma\sigma} \gamma^{-1} \right).$$

(The particular order in which the above product is taken will be irrelevant in all our uses of the element A).

Next we define $W': R_{\Gamma} \rightarrow \pm 1$ by stipulating that for irreducible χ in R_{Γ}

$$W'(\chi) = \begin{cases} W(\chi) & \text{if } \chi \text{ is symplectic,} \\ 1 & \text{otherwise.} \end{cases}$$

By Theorem 9 of [F1], $W'(\chi^{\omega}) = W'(\chi)^{\omega}$ for all $\chi \in R_{\Gamma}$, $\omega \in \Omega_{\mathbb{Q}}$. We define the class $t(W)$ to be that class in $D(\mathbb{Z}\Gamma)$ represented under (2.1) by the image of W' under $\bar{\mathfrak{D}}^* \hookrightarrow U_S$. Let $\tau_{\Gamma}: R_{\Gamma} \rightarrow \bar{\mathbb{Q}}^*$ be the Galois Gauss sum homomorphism associated

to the extension M/N (cf. [M2] for the definition, and also §3). We may write $\tau_F = \prod_{\mathfrak{p}} \tau_{F, \mathfrak{p}}$, where the product is taken over all prime ideals $\mathfrak{p}$ of N . This makes sense as the local Gauss sum $\tau_{F, \mathfrak{p}} = 1$ for almost all $\mathfrak{p}$. We let $u: R_F \rightarrow \bar{\mathbb{Q}}^*$ be the homomorphism $u = \text{Det}(A) \cdot W' \cdot \tau_F^{-1}$. From Theorem 2 of [F1] we know that u commutes with $\Omega_{\mathbb{Q}}$ -action and that the values of u are units at S . Thus, if we identify u with the homomorphism obtained by projecting its values into U_S , we see $u \in \text{Hom}_{\Omega_{\mathbb{Q}}}(R_F, U_S)$. Then, by (9.4) of [F1], we have the crucial result that u represents $(\mathfrak{D}_M)$ under (2.1).

We now explain how we shall prove Theorem 1.

We identify A with its image under $\mathfrak{D}_M \Gamma \hookrightarrow \prod_{l \in S} \mathfrak{D}_{M_l} \Gamma$.

In the same way, if K is a number field which contains $\tau_{F, \mathfrak{p}}$, and if l is fixed we shall identify $\tau_{F, \mathfrak{p}}(\chi)$ with its image in K_l . Thus, for each prime $\mathfrak{p}$ of N , $\tau_{F, \mathfrak{p}}$ takes global values, but, henceforth, we consider these values semi-locally.

In §3 for each prime ideal $\mathfrak{p}$ of N we will construct $\Omega_{\mathbb{Q}}^+$ homomorphisms $y'_{\mathfrak{p}}$ from R_F to the group of roots of unity in $\bar{\mathbb{Q}}$. For a rational prime p we put $y'_p = \prod_{\mathfrak{p}|p} y'_{\mathfrak{p}}$.

In §3–12 we show

Theorem 2. *For each $l \in S$.*

(a) *There exists a Galois extension $E/\mathbb{Q}$ (with $\text{Gal}(E/\mathbb{Q})$ denoted by Λ) so that*

$$y'_l{}^{-1} \text{Det}(A) \prod_{\mathfrak{p}|l} \tau_{F, \mathfrak{p}}^{-1} = \text{Det}(z)$$

for some $z \in \prod_{\mathfrak{Q}|l} \mathfrak{D}_{E_{\mathfrak{Q}}}^{P_{\mathfrak{Q}}} \Gamma^*$. Here $\mathfrak{Q}$ runs through the primes of E above l and $P_{\mathfrak{Q}}$ is the wild inertia group of $\mathfrak{Q}$ in $E/\mathbb{Q}$.

(b) *Now suppose $\mathfrak{p} \nmid l$ and put $K = \mathbb{Q}(p)$, where $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Then $y'_{\mathfrak{p}} \tau_{F, \mathfrak{p}} \in \text{Det}(\mathfrak{D}_{K_l} \Gamma^*)$.*

Moreover, if p is non ramified in $M/\mathbb{Q}$, then $\tau_{F, \mathfrak{p}} = y'_{\mathfrak{p}} = 1$.

We can show, with aid of this result, how we can obtain Theorem 1.

By enlarging if necessary, without loss of generality we may assume E to contain the p^{th} roots of unity for all primes p different from l and ramified in $M/\mathbb{Q}$. By Theorem 2, if we write $y''^{-1} = \prod_{\mathfrak{p}} y'_{\mathfrak{p}}$ then the l component of $W'^{-1} \cdot y'' \cdot u$ equals $\text{Det}(z)$ for some $z = \prod_{\mathfrak{Q}} z_{\mathfrak{Q}}$ with $z_{\mathfrak{Q}} \in \text{Det}(\mathfrak{D}_{E_{\mathfrak{Q}}}^{P_{\mathfrak{Q}}} \Gamma^*)$. Moreover we know this to be an $\Omega_{\mathbb{Q}}$ -homomorphism, and so for all $\chi \in R_F$, $\omega \in \Omega_{\mathbb{Q}}$

$$\text{Det}(z)(\chi^{\omega}) = (\text{Det}(z)(\chi))^{\omega} = \text{Det}(z^{\omega})(\chi^{\omega}).$$

Thus $\text{Det}(z) = \text{Det}(z^{\omega})$, i.e. $\text{Det}(z)$ is fixed by all $\omega \in \Omega_{\mathbb{Q}}$. Hence in particular, each $\text{Det}(z_{\mathfrak{Q}})$ is fixed by the decomposition group of $\mathfrak{Q}$ in $E/\mathbb{Q}$. So, as $z_{\mathfrak{Q}}$ has tame coefficients in $E_{\mathfrak{Q}}$, by Theorem 6 in §12, $\text{Det}(z_{\mathfrak{Q}}) = \text{Det}(x)$ for some $x \in \mathbb{Z}_l \Gamma^*$. Furthermore, because $\Lambda = \text{Gal}(E/\mathbb{Q})$ transitively permutes the primes of E above l and because $\text{Det}(z)$ is Λ -fixed, we deduce that $\text{Det}(z)$ is the same as

$$\text{Det}(x \times \dots \times x) \in \text{Det}\left(\prod_{\mathfrak{Q}} \mathfrak{D}_{E_{\mathfrak{Q}}} \Gamma^*\right), \quad \text{i.e. } \text{Det}(z) \in \text{Det}(\mathbb{Z}_l \Gamma^*).$$

Repeating this argument at each $l \in S$, we have shown that the homomorphism $W'^{-1} \cdot y'' \cdot u$ represents the trivial class under (2.1). However, y'' lies in the denominator in the right hand side of (2.1), and so W' and u represent the same class i.e.

$$(\mathfrak{D}_M) = t(W).$$

3. The Local Galois Gauss Sums and Characters

Let M'/N' be a Galois extension of local fields of residual characteristic p , and let $\Gamma' = \text{Gal}(M'/N')$. We denote by $\tau_{\Gamma'}$ the local Galois Gauss sum associated to the extension M'/N' , as defined by Martinet in [M2]. We recall that $\tau_{\Gamma'}$ has the following four properties:

$$(3.1) \quad \text{For } \chi, \psi \in R_{\Gamma'}, \tau_{\Gamma'}(\chi + \psi) = \tau_{\Gamma'}(\chi) \cdot \tau_{\Gamma'}(\psi).$$

$$(3.2) \quad \text{If } \Delta' \subset \Gamma', \text{ and if } \chi \in R_{\Delta'} \text{ is of degree zero, then}$$

$$\tau_{\Delta'}(\chi) = \tau_{\Gamma'}(\text{Ind}_{\Delta'}^{\Gamma'} \chi).$$

$$(3.3) \quad \text{If } M' \supset L \supset N' \text{ with } L/N' \text{ Galois and } \Lambda = \text{Gal}(L/N'); \text{ then for } \theta \in R_{\Lambda},$$

$$\tau_{\Lambda}(\theta) = \tau_{\Gamma'}(\text{Inf}_{\Lambda}^{\Gamma'} \theta).$$

$$(3.4) \quad \text{If } \chi \text{ is an abelian character, then } \tau_{\Gamma'}(\chi) \text{ is defined explicitly via:}$$

χ *Non-ramified*. Let $D_{N'}$ be the different of $N'/\mathbb{Q}_p$, then $\tau_{\Gamma'}(\chi) = \chi(D_{N'})^{-1}$, where we view χ as an abelian character of N'^* via the local Artin symbol.

χ *Genuinely Ramified*. We choose $c \in N'$ so that $c\mathfrak{D}_{N'} = \mathfrak{f} \cdot D_{N'}$, where $\mathfrak{f}$ is the conductor of χ when viewed as a character on N'^* . We let $\psi_{N'}$ be the canonical additive character of N' given by the composite:

$$N' \xrightarrow{Tr_{N'/\mathbb{Q}_p}} \mathbb{Q}_p \rightarrow \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{e^{2\pi i}} \mathbb{C}^*.$$

Then we have

$$\tau_{\Gamma'}(\chi) = \sum_u \chi(uc^{-1}) \psi_N(uc^{-1})$$

where the sum is taken over a set of representatives of $\mathfrak{D}_{N'}^* \bmod \mathfrak{f}$. It is readily verified that $\tau_{\Gamma'}(\chi)$ is independent of the choice of representatives u and of the choice of generator c .

Next we define the non-ramified character $y_{\Gamma'}: R_{\Gamma'} \rightarrow \mu$. This homomorphism was first introduced by Deligne in [D], and was subsequently developed in [FT]. We define $y_{\Gamma'}$ on irreducible characters of Γ' by

$$y_{\Gamma'}(\chi) = \begin{cases} (-1) \cdot \chi(\mathfrak{p}_{N'}) & \text{if } \chi \text{ is non-ramified,} \\ 1 & \text{otherwise.} \end{cases}$$

Here $\mathfrak{p}_{N'}$ is the maximal ideal of $\mathfrak{D}_{N'}$. We then extend $y_{\Gamma'}$ to the whole of $R_{\Gamma'}$ by $\mathbb{Z}$ -linearity. It is a triviality that $y_{\Gamma'}$ is 1 on symplectic characters and commutes with $\Omega_{\mathbb{Q}}$ -action.

Lemma 3.5. *Let M'/N' be a tame extension of local fields, then*

$$\mathfrak{p}_{M'} D_{M'} = \mathfrak{p}_{N'} D_{N'} \cdot \mathfrak{D}_{M'}.$$

(This is elementary.)

From now on we suppose all our local extensions to be tame over the chosen base field N' .

Proposition 3.6. *Let $\Delta' \subset \Gamma'$, and let $\phi \in R_{\Delta'}$, then*

$$y_{\Delta'}(\phi) = y_{\Gamma'}(\text{Ind}_{\Delta'}^{\Gamma'} \phi)$$

(For proof see Theorem 5(ii) in [FT]).

Let l be a rational prime number, and let $\text{Ker } d_{l, \Gamma'}$ be the $R_{\Gamma'}$ ideal of virtual characters which vanish on those elements of Γ' of order prime to l . The crucial property of $y_{\Gamma'}$ (c.f. Theorem 5(iii), [FT]) is that

Proposition 3.7. *For each prime number l ,*

$$\tau_{\Gamma'}(\chi) \equiv y_{\Gamma'}(\chi) \pmod{\mathfrak{L}_l}$$

for all $\chi \in \text{Ker } d_{l, \Gamma'}$.

While, as per Proposition III.2 in the Appendix of [F1], we can show

Proposition 3.8. *Let L be any number field and let $x \in \mathfrak{D}_{L, l} \Gamma'^*$. Then for all $\chi \in \text{Ker } d_{l, \Gamma'}$*

$$\text{Det}(x)(\chi) \equiv 1 \pmod{\mathfrak{L}_l}.$$

We now define an adjusted local Galois Gauss Sum $\tau_{\Gamma'}^*$ which has good properties both with respect to $\text{Ker } d_l$ and with respect to restriction to the inertia group I of Γ' .

Once and for all we choose $c \in N'$ so that $c \mathfrak{D}_{N'} = \mathfrak{p}_{N'} D_{N'}$. Let K'/N' be tame, let $K' \supset L \supset N'$ with K'/L Galois and $\Delta' = \text{Gal}(K'/L)$. We choose $\delta_c \in \Delta'$ to be any element of Δ' whose image in Δ'^{ab} coincides with the image of c under the Artin symbol of the maximal abelian subextension of K'/L . Then we define

$$(3.9) \quad \tau_{\Delta'}^* = \tau_{\Delta'} \cdot y_{\Delta'}^{-1} \cdot \text{Det}(\delta_c).$$

The main properties of $\tau_{\Delta'}^*$ are given by:

Proposition 3.10. (i) *For any $\chi \in R_{\Gamma'}$, $\tau_{\Gamma'}^*(\chi)$ is a unit outside p .*

(ii) *For $\omega \in \Omega_{\mathbb{Q}(p)}$*

$$\tau_{\Gamma'}^*(\chi^\omega) = \tau_{\Gamma'}^*(\chi)^\omega.$$

(iii) *If v is a non-ramified abelian character of Γ' , then for $\chi \in R_{\Gamma'}$*

$$\tau_{\Gamma'}^*(v\chi) = \tau_{\Gamma'}^*(\chi).$$

(iv) If χ is an irreducible character of Γ' , then $\tau_{\Gamma'}^*(\chi) \in \mathbb{Q}(p)(\chi|_I)$.

(v) For each rational prime number l , $\tau_{\Gamma'}^*(\chi) \equiv 1 \pmod{\mathfrak{L}_l}$, for any $\chi \in \text{Ker } d_{l, \Gamma'}$.

Proof. (ii) is an immediate consequence of A. Fröhlich's Galois action formula for $\tau_{\Gamma'}$, since $y_{\Gamma'}$ and $\text{Det}(\delta_c)$ commute with $\Omega_{\mathbb{Q}}$ action (cf. [F2]). (v) is an immediate consequence of Propositions 3.7 and 3.8.

To prove the three remaining parts, by $\mathbb{Z}$ -linearity, we may assume χ to be irreducible. Because I and Γ'/I are both cyclic, we can write $\chi = \text{Ind}_{\Delta'}^{\Gamma'} \alpha$, where Δ' contains the inertia group I and α is an abelian character of Δ' .

From the inductivity of $\tau_{\Gamma'}$ in degree zero, we deduce

$$(3.11) \quad \tau_{\Gamma'}(\chi) = \tau_{\Delta'}(\alpha) \cdot \tau_{\Gamma'}(\rho_{\Gamma'/\Delta'})$$

where $\rho_{\Gamma'/\Delta'}$ is the regular character of Γ'/Δ' inflated to Γ' . Moreover, as $\rho_{\Gamma'/\Delta'}$ is made up entirely of non-ramified characters

$$\tau_{\Gamma'}(\rho_{\Gamma'/\Delta'}) = \tau_{\Gamma'}(\det(\rho_{\Gamma'/\Delta'})) = \pm 1.$$

Now from (3.4), $\tau_{\Gamma'}(\alpha)$ is an algebraic integer and by Theorem 3(i) of [FT], $\tau_{\Gamma'}(\alpha)$ divides a power of p if α is genuinely ramified, while of course $\tau_{\Gamma'}(\alpha)$ is a root of unity if α is non-ramified. So, as $y_{\Gamma'}$ and $\text{Det}(\delta_c)$ are root of unity valued, we have shown (i).

Now we show (iii) and (iv). Because $\det_{\chi} = v_{\Delta'}^{\Gamma'} \alpha \cdot \det(\rho_{\Gamma'/\Delta'})$, by local class field theory

$$\det_{\chi}(c) = \alpha(c) \cdot \det(\rho_{\Gamma'/\Delta'})(c).$$

So, by (3.11),

$$y_{\Gamma'}(\chi) \tau_{\Gamma'}^*(\chi) = y_{\Delta'}(\alpha) \tau_{\Delta'}^*(\alpha) \cdot \det(\rho_{\Gamma'/\Delta'})(c) \cdot \tau_{\Gamma'}(\det(\rho_{\Gamma'/\Delta'})).$$

But by Proposition 3.6 $y_{\Gamma'}(\chi) = y_{\Delta'}(\alpha)$, while we see that if $(\Gamma': \Delta')$ is odd $\det(\rho_{\Gamma'/\Delta'})$ is trivial, and if $(\Gamma': \Delta')$ is even then $\det(\rho_{\Gamma'/\Delta'})$ is the non-trivial, non-ramified character of order 2. Using this one verifies

$$\det(\rho_{\Gamma'/\Delta'})(c) \cdot \tau_{\Gamma'}(\det(\rho_{\Gamma'/\Delta'})) = (-1)^{(\Gamma': \Delta') + 1}$$

and whence

$$(3.12) \quad \tau_{\Gamma'}^*(\chi) = \tau_{\Delta'}^*(\alpha) \cdot (-1)^{(\Gamma': \Delta') + 1}.$$

So, if α is ramified,

$$(3.13) \quad \tau_{\Gamma'}^*(\chi) = (-1)^{(\Gamma': \Delta') + 1} \left(\sum_{u \bmod \mathfrak{p}_{L'}} \alpha(u) \psi_{\Delta'}(uc^{-1}) \right)$$

where $\psi_{\Delta'}$ is the canonical additive character of the subfield fixed by Δ' . We now show (iii) and (iv) in this case.

Γ'/Δ' identifies as a sub-group Σ of $\text{Gal}(\mathbb{Q}(\alpha|_I)/\mathbb{Q})$ via conjugation. That this homomorphism is injective is an immediate consequence of Mackey's Irreducibility Criterion. Now, since

$$\psi_{\Delta'}(u^{\gamma} c^{-1}) = \psi_{\Delta'}(u^{\gamma} c^{-\gamma}) = \psi_{\Delta'}(uc^{-1})$$

for all $\gamma \in \Gamma'$, we see that $\tau_{\mathcal{A}'}^*(\alpha)$ is fixed by the subgroup Λ of Σ which fixes $\mathbb{Q}(p)$. Now, by elementary Galois theory,

$$(\mathbb{Q}(p)(\alpha|_I))^{\Lambda} = \mathbb{Q}(p) \cdot \mathbb{Q}(\alpha|_I)^{\Sigma}.$$

On the other hand, using Mackey's Restriction Theorem $\chi|_I = \sum_{\sigma \in \Sigma} (\alpha|_I)^{\sigma}$, and so it is easily verified that

$$\mathbb{Q}(\alpha|_I)^{\Sigma} = \mathbb{Q}(\chi|_I).$$

Thus (iv) is shown. Now let v be as in the statement of the proposition. Then by (3.12), (3.13) and Frobenius reciprocity

$$\begin{aligned} \tau_{\mathcal{A}'}^*(v\chi) &= \tau_{\mathcal{A}'}^*(\alpha \cdot v|_{\mathcal{A}'}) \cdot (-1)^{(\Gamma': \mathcal{A}') + 1} \\ &= (-1)^{(\Gamma': \mathcal{A}') + 1} \cdot \sum \alpha(u) \psi_{\mathcal{A}'}(uc^{-1}) \end{aligned}$$

since $v|_{\mathcal{A}'}$ is non-ramified and so trivial on the units u . This establishes (iii) when α is genuinely ramified.

Now we take α non-ramified. Then by the definition of τ^*

$$\tau_{\mathcal{A}'}^*(\alpha) = -\alpha(\mathfrak{p}_{N'})^{-1} \cdot \alpha(c) \cdot \alpha(D_{N'})^{-1} = -1$$

and so (iii) and (iv) are immediate in this case. The proposition is now shown.

Theorem 2(a) will be proved in Sect. 11. We now turn our attention to Theorem 2(b) and so from now on until the end of § 10 we fix a prime p different from l .

Theorem 3. *With the above notation, and putting $K = \mathbb{Q}(p)$, we have $\tau_{\mathcal{A}'}^* \in \text{Det}(\mathfrak{D}_{K_l} \Gamma'^*)$.*

Now we show that Theorem 3 implies Theorem 2(b). Let M, N and Γ be as in Sect. 2. Let $\mathfrak{p}$ be a prime of N , let $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, and let $\mathfrak{q}$ be a prime ideal of $\mathfrak{D}_M$ above $\mathfrak{p}$. We denote the decomposition group of $\mathfrak{q}$ in Γ , by $\Gamma_{\mathfrak{q}}$. In the above theorem we put $M' = M_{\mathfrak{q}}$, $N' = N_{\mathfrak{p}}$, $\Gamma' = \Gamma_{\mathfrak{q}}$. Then, by the definition of $\tau_{\Gamma, \mathfrak{p}}$, for each $\chi \in R_{\Gamma'}$,

$$\tau_{\Gamma, \mathfrak{p}}(\chi) = \tau_{\Gamma'}(\chi|_{\Gamma'}) = y_{\Gamma'}(\chi|_{\Gamma'}) \text{Det}(\delta_c)(\chi|_{\Gamma'})^{-1} \cdot \tau_{\Gamma'}^*(\chi|_{\Gamma'}).$$

Now let $\tilde{y}: R_{\Gamma'} \rightarrow \mu$ be the homomorphism $y_{\Gamma'}^{-1} \text{Det}(\delta_c)$. Because $\det_{\chi} = \varepsilon_{\Gamma'}$ for all symplectic characters χ of Γ' , we see that $\tilde{y}$ is also an $\Omega_{\mathbb{Q}}^+$ homomorphism. Let $\text{Ind}_{\Gamma'}^{\Gamma}(\tilde{y})$ be that $\Omega_{\mathbb{Q}}^+$ -homomorphism obtained by composing $\tilde{y}$ with restriction from $R_{\Gamma'}$ to R_{Γ} . Because symplectic characters restrict to symplectic characters, we deduce that $\text{Ind}_{\Gamma'}^{\Gamma}(\tilde{y})$ is in turn an $\Omega_{\mathbb{Q}}^+$ -homomorphism.

By the above theorem we know $\tau_{\mathcal{A}'}^* = \text{Det}(x_l)$ for each $l \in S$. Thus we have shown

$$\tau_{\Gamma, \mathfrak{p}} = \text{Ind}_{\Gamma'}^{\Gamma}(\tilde{y}) \cdot \text{Ind}_{\Gamma'}^{\Gamma}(\text{Det}(\prod_{l \in S} x_l)).$$

This establishes Theorem 2(b) in the case when p is ramified in $M/\mathbb{Q}$; while if p is non-ramified, we put $\tau_{\Gamma, \mathfrak{p}} = y'_{\mathfrak{p}} = 1$ and the result is immediate.

Henceforward we shall always be working locally at a fixed p , and so from now on we shall omit the primes on M , N and Γ , i.e. in the sequel, M/N is a tame Galois extension of local fields of residual characteristic p .

Types of 2-character

Let $H \subset \Gamma$ be a 2-group, let I be the inertia sub-group of H and let χ be an irreducible character of degree 2 of H . We can write $\chi = \text{Ind}_\Delta^H \alpha$, with $\Delta \supset I$ and α an abelian character of Δ .

Let $\mathfrak{p}_H$ (resp. $\mathfrak{p}_I$) be the maximal ideal of the ring of integers of the fixed field of H (resp. of I) and let $\xi \in H$ have the same image as Frobenius in H/I . Then ξ acts by raising to the power $N\mathfrak{p}_H \bmod \mathfrak{p}_I$. Now by Mackey's irreducibility criterion we know that $\alpha^\xi|_I \neq \alpha$, and thus raising to the power $N\mathfrak{p}_H$ is a non-trivial automorphism of order 2 on $\alpha|_I$. Let 2^r be the order of $\alpha|_I$. We distinguish between three cases

Type 1. If $N\mathfrak{p}_H \equiv 1 \pmod{(4)}$, then we say χ is of semi-abelian type. (Thus, in particular, $N\mathfrak{p}_H \equiv 1 + 2^{r-1} \pmod{(2^r)}$.)

Type 2. If $N\mathfrak{p}_H \equiv -1 \pmod{(2^r)}$, then we say χ is of inversion type.

Type 3. If $N\mathfrak{p}_H \equiv -1 + 2^{r-1} \pmod{(2^r)}$ with $r \geq 3$, then we say χ is of semi-dihedral type.

Note that type of χ is of course solely determined by $\chi|_I$. It is also clear that if χ is of inversion type, then, as $N\mathfrak{p}_H$ necessarily has order 2 mod (2^{r+1}) , we can find an irreducible character $\tilde{\chi}$ of degree 2, of a 2-power tame extension of H (i.e. of a tame Galois group of 2-power order possessing H as quotient) with $\tilde{\alpha}^2|_I = \alpha|_I$ and with $\tilde{\chi}$ of either inversion or semi-dihedral type, according as $N\mathfrak{p}_H = -1(2^{r+1})$ or $N\mathfrak{p}_H \equiv -1 + 2^r \pmod{(2^{r+1})}$.

4. Logarithms

In this section we recall various results from [T1]. Let $L/\mathbb{Q}$ be a finite abelian extension which is non-ramified at l , and let H be a finite group of l -power order, say $|H| = l^m$. We denote by F the Frobenius of l in the extension $L(l^m)/\mathbb{Q}(l^m)$, and we write $\mathfrak{B} = \mathfrak{D}_L \otimes_{\mathbb{Z}} \mathbb{Z}_l$. We define $\mathfrak{a}$ to be the commutator ideal $\sum_{\gamma \in [H, H]} \mathfrak{B}H(1 - \gamma)$, i.e. $\mathfrak{a} = \text{Ker}(\mathfrak{B}H \rightarrow \mathfrak{B}H^{ab})$. We define $\psi^l: \mathfrak{B}H \rightarrow \mathfrak{B}H$ to be the $\mathfrak{B}$ -linear map induced by $\gamma \mapsto \gamma^l$. Then, for r in $\mathfrak{r}_H$, the Jacobson radical of $\mathfrak{B}H$, we define the map Ω_1 via

$$(4.1) \quad \Omega_1(1-r) = -l \sum_{n=1}^{\infty} \frac{r^n}{n} + \sum_{n=1}^{\infty} \frac{\psi^l(r^n)^F}{n} \in \mathfrak{B}H \otimes \mathbb{Q}_l.$$

(That this series converges l -adically is shown in [T1]). Further, let $\mathfrak{C}_H$ denote the set of conjugacy classes of H and let $\phi_H: L \otimes \mathbb{Q}_l H \rightarrow L \otimes \mathbb{Q}_l \mathfrak{C}_H$ be the $L \otimes \mathbb{Q}_l$ linear-map induced by associating to $\gamma \in H$ its conjugacy class in $\mathfrak{C}_H$. We view

$\theta \in R_H$ as functions on $\mathfrak{C}_H$, and whence on $L \otimes \mathbb{Q}_l \mathfrak{C}_H$, by stipulating that $\theta(\phi_H(\gamma)) = \theta(\gamma)$. We define $\mathfrak{L}_H = \phi_H \circ \mathfrak{L}_1$. In [T1] it is shown that $\mathfrak{L}_H: 1 + \mathfrak{r}_H \rightarrow \mathfrak{B}\mathfrak{C}_H \otimes \mathbb{Q}_l$ is a group homomorphism and that for $\theta \in R_H$,

$$(4.2) \quad \theta(\mathfrak{L}_H(1-r)) = \log(\text{Det}(1-r)(l\theta) \cdot \text{Det}(1-r)(\psi^l\theta)^{-F}).$$

Because such θ span the dual of $\mathfrak{B}\mathfrak{C}_H \otimes \mathbb{Q}_l$, we see that $\text{Ker}(\mathfrak{L}_H) \supset \text{Ker}(\text{Det}|_{1+\mathfrak{r}_H})$, and whence there exists a unique homomorphism v_H which makes the triangle below commute:

$$\begin{array}{ccc} 1 + \mathfrak{r}_H & \xrightarrow{\mathfrak{L}_H} & \mathfrak{B}\mathfrak{C}_H \otimes \mathbb{Q}_l \\ \text{Det} \searrow & & \nearrow v_H \\ & \text{Det}(1 + \mathfrak{r}_H) & \end{array}$$

In fact, because the index $(\text{Hom}_{\Omega_L}(R_H; U_l): \text{Det}(1 + \mathfrak{r}_H))$ is finite and, because the image space of v_H is uniquely divisible, we can extend v_H in a unique way to $\text{Hom}_{\Omega_L}(R_H, U_l)$, and moreover, by (4.2), for $h \in \text{Hom}_{\Omega_L}(R_H, U_l)$ we know

$$(4.3) \quad \theta(v_H(h)) = \log(h(l\theta) \cdot h(-\psi^l\theta)^F).$$

We now quote various further properties of v_H from [T1] (cf. Proposition 3.1 and Theorem 4.23)

$$(4.4.a) \quad v_H(\text{Det}(\mathfrak{B}H^*)) = v_H(\text{Det}(1 + \mathfrak{r}_H)) \subseteq l\mathfrak{B}\mathfrak{C}_H$$

$$(4.4.b) \quad v_H(\text{Det}(1 + \mathfrak{a})) = l\phi_H(\mathfrak{a})$$

$$(4.4.c) \quad \text{Ker}(v_H) \cap \text{Det}(1 + \mathfrak{a}) = \{1\}.$$

Let $\mathfrak{T}$ be the torsion sub-group of $\text{Hom}_{\Omega_L}(R_H, U_l)$. From Proposition 3.11 of [T1] we know that $\text{Det}(1 + \mathfrak{r}_H) \cap \text{Ker}(v_H) = \mathfrak{T} \cap \text{Det}(1 + \mathfrak{r}_H)$.

Thus, as $\text{Hom}_{\Omega_L}(R_H, U_l)$ is of finite index over $\text{Det}(1 + \mathfrak{r}_H)$, we see

$$(4.5) \quad \text{Ker}(v_H) = \mathfrak{T}.$$

Lastly in this section we show:

Proposition 4.6. *Let I be a cyclic group of l -power order, let c be an element of order l in I , and let $\mathfrak{r}_I$ be the Jacobson radical of $\mathfrak{B}I$; then*

$$\mathfrak{L}_1(1 + (1-c)\mathfrak{B}I) \supset l(1-c)\mathfrak{r}_I.$$

Proof. First observe that by the Binomial theorem, because $c^l = 1$, $(1-c)^l = l(1-c)\lambda$, for some $\lambda \in \mathbb{Z}\langle c \rangle$.

Now choose $x \in \mathfrak{r}_I$. Because $\psi^l(1-c) = 0$ and using the above binomial result, it is easily verified that

$$\mathfrak{L}_1(1 - (1-c)x) = -l(1-c)(x + \lambda x^l + yx)$$

where $y \in (1-c)\mathfrak{B}I$. Hence as $x \in \mathfrak{r}_I$, we can write

$$\mathfrak{L}_1(1 - (1-c)x) = -l(1-c)x + l(1-c)xy'$$

with $y' \in r_I$. So, as $r_I^i \rightarrow 0$ l -adically as $i \rightarrow \infty$ (by the Binomial theorem), on using a standard approximation argument we obtain the result. (Note here we use the fact that as $\mathfrak{C}_I$ identifies with I , $\mathfrak{Q}_1$ itself is a group homomorphism).

5. Reduction to $\mathbb{Q}$ -Elementary Groups

In this section we show that it is sufficient to show Theorem 3 for $\mathbb{Q}$ -elementary groups. As always we view l as being fixed and we shall write $K = \mathbb{Q}(p)$ and $\mathfrak{A} = \mathfrak{S}_K \otimes_{\mathbb{Z}} \mathbb{Z}_l$.

By Brauer's Induction Theorem (cf. 12.6 of [S]) we can find $\mathbb{Q}$ -elementary sub-groups Δ_i of Γ and virtual $\mathbb{Q}$ -characters θ_i of Δ_i so that

$$\varepsilon_{\Gamma} = \sum_i \text{Ind}_{\Delta_i}^{\Gamma} \theta_i.$$

Then, by Frobenius reciprocity, for each $\chi \in R_{\Gamma}$, we have

$$\tau_{\Gamma}^*(\chi) = \prod_i \tau_{\Gamma}^*(\text{Ind}_{\Delta_i}^{\Gamma}(\chi|_{\Delta_i} \cdot \theta_i)).$$

While by Proposition 3.6, by the inductivity of τ_{Γ} in degree zero, and using the fact that for any $\phi \in R_{\Delta_i}$

$$\det(\text{Ind}_{\Delta_i}^{\Gamma} \phi) = v_{\Delta}^{\Gamma} \det(\phi) \cdot \det(\rho_i)^{\phi(1)}$$

we obtain

$$(5.1) \quad \tau_{\Gamma}^*(\text{Ind}_{\Delta_i}^{\Gamma} \phi) = \tau_{\Delta_i}^*(\phi) \tau_{\Gamma}(\rho_i)^{\phi(1)} \cdot \text{Det}(\delta_c^{\phi(1)})(\rho_i)$$

where we denote $\text{Ind}_{\Delta_i}^{\Gamma}(\varepsilon_{\Delta_i})$ by ρ_i . However, by Fröhlich's Galois action formula for τ_{Γ} (cf. [F2]), we know $\tau_{\Gamma}(\rho_i - \det \rho_i) \in \mathbb{Q}$; while from the definition of τ_{Γ} on abelian characters we know $\tau_{\Gamma}(\det \rho_i) \in K$, and further, by Proposition 3.10(i), it is a unit outside p . Thus if we put

$$u_i = \tau_{\Gamma}(\rho_i) \text{Det}(\delta_c)(\rho_i) (= \pm \tau_{\Gamma}(\rho_i)),$$

then

$$\tau_{\Gamma}^*(\chi) = \prod_i \tau_{\Delta_i}^*(\theta_i \cdot \chi|_{\Delta_i}) \text{Det}(u_i)(\theta_i \cdot \chi|_{\Delta_i}).$$

Consequently, with the notation of Sect. 2, if we suppose that $\tau_{\Delta_i}^* = \text{Det}(z_i)$ for some $z_i \in \mathfrak{A}\Delta_i^*$, then

$$\begin{aligned} \tau_{\Gamma}^*(\chi) &= \prod_i (\theta_i \cdot \text{Det}(z_i \cdot u_i))(\chi|_{\Delta_i}) \\ &= \prod_i \text{Ind}_{\Delta_i}^{\Gamma}(\theta_i \cdot \text{Det}(z_i \cdot u_i))(\chi) \end{aligned}$$

and so

$$\tau_{\Gamma}^* = \prod_i \text{Ind}_{\Delta_i}^{\Gamma}(\theta_i \cdot \text{Det}(z_i u_i)) \in \text{Det}(\mathfrak{A}\Gamma^*).$$

(5.2) Thus we have shown that in order to establish Theorem 3 it is sufficient to take Γ to be $\mathbb{Q}$ -elementary.

In Sects. 6–8 we shall show

Proposition 5.3. *For each $\mathbb{Q}$ - q -elementary sub-group Δ of Γ , with q different from l , there exists an integer k so that*

$$\tau_{\Delta}^{*l^k} \in \text{Det}(\mathfrak{A}\Delta^*).$$

Proposition 5.4. *Theorem 3 holds for all $\mathbb{Q}$ - l -elementary sub-groups of Γ .*

We now show that these two propositions yield the theorem. Arguing as above and using the fact that for some m prime to l , there exist $\mathbb{Q}$ - l -elementary sub-groups of $\Gamma\Delta'_j$ and virtual $\mathbb{Q}$ -characters θ'_j of Δ'_j such that

$$m\varepsilon_{\Gamma} = \sum_j \text{Ind}_{\Delta'_j}^{\Gamma}(\theta'_j)$$

(cf. 12.6 of [S]), we deduce that by Proposition 5.4

$$\tau_{\Gamma}^{*m} \in \text{Det}(\mathfrak{A}\Gamma^*),$$

and this result holds for arbitrary Γ . In particular it holds for the various subgroups Δ of Γ in Proposition 5.3, and so for such Δ we obtain $\tau_{\Delta}^* \in \text{Det}(\mathfrak{A}\Delta^*)$. This, in conjunction with Proposition 5.4, yields (5.2) as was required.

Lastly in this section we note that by Proposition 3.10(ii)

$$(5.5) \quad \tau_{\Gamma}^* \in \text{Hom}_{\Omega_K}(R_{\Gamma}, U_l)$$

where as usual we view the values of τ_{Γ}^* as being embedded in U_l .

6. $\mathbb{Q}$ - q -Elementary Groups

As in the previous section we put $K = \mathbb{Q}(p)$ and $\mathfrak{A} = \mathfrak{D}_K \otimes \mathbb{Z}_l$.

We let Γ be a $\mathbb{Q}$ - q -elementary group and so we may identify Γ with a semi-direct product $(C \times C') \rtimes P$, where P is a q -sub-group ($q \neq l$) and where C (resp. C') is normal and cyclic of l -power order (resp. of order prime to lq). We put $\Gamma' = C' \rtimes P$ and we shall view Γ' as a quotient of Γ . Since the kernel of the ring homomorphism $u: \mathfrak{A}\Gamma \rightarrow \mathfrak{A}\Gamma'$, induced by $\Gamma \rightarrow \Gamma'$, is contained in the Jacobson radical of $\mathfrak{A}\Gamma$, we see that $X \in \mathfrak{A}\Gamma$ is a unit if, and only if, $u(X)$ is a unit in $\mathfrak{A}\Gamma'$.

If $u_1: \mathfrak{A}\Gamma^* \rightarrow \mathfrak{A}\Gamma'^*$, $u_2: \text{Det}(\mathfrak{A}\Gamma^*) \rightarrow \text{Det}(\mathfrak{A}\Gamma'^*)$ are the natural homomorphisms induced by u , then we have a commutative diagram

$$\begin{array}{ccc} \mathfrak{A}\Gamma^* & \xrightarrow{u_1} & \mathfrak{A}\Gamma'^* \\ \downarrow & & \downarrow \\ \text{Det}(\mathfrak{A}\Gamma^*) & \xrightarrow{u_2} & \text{Det}(\mathfrak{A}\Gamma'^*) \end{array}$$

Now by the above u_1 is surjective, so, because the vertical maps are surjective, u_2 is also surjective.

Since $(l, |\Gamma'|) = 1$, we know that $\mathfrak{A}\Gamma'$ is a maximal order and so it is immediate that

$$\tau_{\Gamma'}^* \in \text{Det}(\mathfrak{A}\Gamma'^*) (= \text{Hom}_{\Omega_K}(R_{\Gamma'}, U_l)).$$

We choose $z' \in \mathfrak{A}\Gamma^*$ with the property that $\tau_F^* = \text{Det}(z')$. Next we choose $z \in \mathfrak{A}\Gamma^*$ so that $u_1(z) = z'$, and we put

$$H(\mathfrak{Q}_l) = \text{Hom}_{\Omega_K}(R_\Gamma, 1 + \mathfrak{Q}_l).$$

Proposition 6.1. $\tau_F^* \text{Det}(z)^{-1} \in H(\mathfrak{Q}_l)$.

Proof. Let χ be an irreducible character of Γ . By 8.2 and 8.5 of [S], we can find $\Delta \supset C \times C'$ and α an abelian character of Δ so that $\chi = \text{Ind}_\Delta^F \alpha$.

Let α' be the l -free part of α . We define $\chi' = \text{Ind}_\Delta^F(\alpha')$. Then χ' is inflated from Γ' and $\chi - \chi' \in \text{Ker } d_{l, \Gamma}$.

Now by Proposition 3.8

$$\text{Det}(z)(\chi) \equiv \text{Det}(z)(\chi') \pmod{\mathfrak{Q}_l}$$

and by passing to the quotient Γ'

$$\begin{aligned} \text{Det}(z)(\chi') &= \text{Det}(z')(\chi') \\ &= \tau_{F'}^*(\chi') = \tau_F^*(\chi'). \end{aligned}$$

Moreover, by Proposition 3.10(v) since $\chi - \chi' \in \text{Ker } d_{l, \Gamma}$,

$$\tau_F^*(\chi) \equiv \tau_F^*(\chi') \pmod{\mathfrak{Q}_l},$$

thus we see that for all $\theta \in R_\Gamma$

$$\tau_F^*(\theta) \equiv \text{Det}(z)(\theta) \pmod{\mathfrak{Q}_l}$$

as was required.

Now we prove Proposition 5.3.

By the above proposition

$$\tau_F^* \in H(\mathfrak{Q}_l) \cdot \text{Det}(\mathfrak{A}\Gamma^*),$$

so, because $H(\mathfrak{Q}_l)$ is a pro- l -group and because $\text{Det}(\mathfrak{A}\Gamma^*)$ is of finite index in $\text{Hom}_{\Omega_K}(R_\Gamma, U_l)$, we obtain Proposition 5.3.

7. $\mathbb{Q}$ - l -Elementary Groups

As previous $K = \mathbb{Q}(p)$ and $\mathfrak{A} = \mathfrak{O}_K \otimes \mathbb{Z}_l$. In this section we assume Γ to be a $\mathbb{Q}$ - l -elementary group and so we identify Γ with a semi-direct product $C \rtimes P$ where P is an l -subgroup and C is a normal cyclic group of order prime to l . Thus we have an isomorphism of rings

$$\mathbb{Z}_l C \cong \prod_{m \mid |C|} \mathbb{Z}[\zeta_m] \otimes \mathbb{Z}_l$$

where ζ_m denotes a primitive m^{th} root of unity. This in turn, by tensoring, yields a ring isomorphism

$$(7.1) \quad \mathfrak{A}\Gamma \cong \prod_m \mathfrak{A}_m \circ P$$

where $\mathfrak{A}_m = \mathfrak{A} \otimes \mathbb{Z}[\zeta_m]$ and $\mathfrak{A}_m \circ P$ is the corresponding twisted group ring.

Let $\mathfrak{x}$ be a chosen abelian character of C of order n . P acts via conjugation on C and thus we obtain an action of P on $\mathfrak{x}(C)$, the group of n^{th} roots of unity. We let H be the kernel of this action and we put $\Delta = C \rtimes H$, $A = \Gamma/\Delta$. (Observe that H and A both depend on the order of the chosen character $\mathfrak{x}$).

Definition. $R_\Gamma^{(n)}$ (resp. $R_\Delta^{(n)}$) is the sub-group of R_Γ (resp. R_Δ) generated by those irreducible characters of Γ (resp. of Δ) whose restriction to C is made up of abelian characters of order n .

It is immediate that every irreducible character of Γ (resp. of Δ) belongs to some $R_\Gamma^{(m)}$ (resp. $R_\Delta^{(m)}$). Alternatively we can view $R_\Gamma^{(n)}$ as the group of virtual representations of $\mathbb{Q}(n) \circ P$ as a $\mathbb{Q}$ algebra. The direct decomposition (7.1) induces

$$\text{Det}(\mathfrak{A}\Gamma^*) \cong \prod_m \text{Det}(\mathfrak{A}\Gamma^*)|_{R_\Gamma^{(m)}}$$

and in the same way we have

$$\text{Det}(\mathfrak{A}\Delta^*) \cong \prod_m \text{Det}(\mathfrak{A}\Delta^*)|_{R_\Delta^{(m)}}.$$

For the sake of brevity we shall write $\tau_{\Delta(n)}^*$ and $\tau_{\Gamma(n)}^*$ in place of $\tau_\Gamma^*|_{R_\Gamma^{(n)}}$ and $\tau_\Delta^*|_{R_\Delta^{(n)}}$. It is clear from the above work that in order to establish Proposition 5.4 it is sufficient to show $\tau_{\Gamma(n)}^* \in \text{Det}(\mathfrak{A}\Gamma^*)|_{R_\Gamma^{(n)}}$, for each n . From now on we shall view the character $\mathfrak{x}$ as being fixed.

Using techniques introduced in §5 of [T1], we now reduce the problem to that of showing $\tau_{\Delta(n)}^* \in \text{Det}(\mathfrak{A}\Delta^*)|_{R_\Delta^{(n)}}$.

Let $\mu: \text{Hom}_{\Omega_K}(R_\Gamma^{(n)}, U_l) \rightarrow \text{Hom}_{\Omega_K}(R_\Delta^{(n)}, U_l)$ be the restriction homomorphism given by induction of character, i.e. if $f \in \text{Hom}_{\Omega_K}(R_\Gamma^{(n)}, U_l)$, and $\chi \in R_\Delta^{(n)}$, then

$$\mu(f)(\chi) = f(\text{Ind}_\Delta^\Gamma(\chi)).$$

It is easily seen that Ind_Δ^Γ maps $R_\Delta^{(n)}$ onto $R_\Gamma^{(n)}$ (cf. 8.2 of [S]) and so μ is injective. Because A -conjugate characters of Δ induce to the same character of Γ it is immediate that $\text{Im}(\mu) \subseteq \text{Hom}_{\Omega_K}(R_\Delta^{(n)}, U_l)^A$ where as usual the superscript A denotes the points fixed by A .

From Proposition 5.14 of [T1] we know that

$$\mu(\text{Det}(\mathfrak{A}\Gamma^*)|_{R_\Gamma^{(n)}}) = (\text{Det}(\mathfrak{A}\Delta^*)|_{R_\Delta^{(n)}})^A.$$

Thus we now have a commutative diagram

$$(7.2) \quad \begin{array}{ccc} \text{Hom}_{\Omega_K}(R_\Gamma^{(n)}, U_l) & \xhookrightarrow{\mu} & \text{Hom}_{\Omega_K}(R_\Delta^{(n)}, U_l)^A \\ \uparrow & & \uparrow \\ \text{Det}(\mathfrak{A}\Gamma^*)|_{R_\Gamma^{(n)}} & \xrightarrow{\sim} & (\text{Det}(\mathfrak{A}\Delta^*)|_{R_\Delta^{(n)}})^A. \end{array}$$

We are now required to show that $\mu(\tau_{\Gamma(n)}^*) \in (\text{Det}(\mathfrak{A}\Delta^*)|_{R_\Delta^{(n)}})^A$. However, as per (5.1), for any $\chi \in R_\Delta^{(n)}$

$$\mu(\tau_{\Gamma(n)}^*)(\chi) = \tau_{\Gamma(n)}^*(\text{Ind}_\Delta^\Gamma(\chi)) = \tau_{\Delta(n)}^*(\chi) \text{Det}(\text{Det}(\delta_c)(\rho) \tau_\Gamma(\rho))(\chi)$$

and so, since $\text{Det}(\text{Det}(\delta_c)(\rho)\tau_r(\rho)) \in \text{Det}(\mathfrak{A}^*)$, it is enough to show that $\tau_{A(n)}^* \in (\text{Det}(\mathfrak{A}A^*)|_{R_A^{(n)}})^A$. So in fact now we are reduced to showing

$$(7.3) \quad \tau_{A(n)}^* \in \text{Det}(\mathfrak{A}A^*)|_{R_A^{(n)}}.$$

We now wish to pass from homomorphisms on $R_A^{(n)}$, to homomorphisms on R_H . Then, because H is an l -group, we will be able to apply the integral logarithmic techniques of [T1]. We will denote the number field $K(n)$, by L , and the ring $\mathfrak{O}_L \otimes \mathbb{Z}_l$ by $\mathfrak{B}$.

F will denote the Frobenius of l in $L/\mathbb{Q}$. We define the non-canonical homomorphism for $\sigma \in \text{Gal}(K/\mathbb{Q})$

$$v_\sigma: \text{Hom}_{\Omega_K}(R_A^{(n)}, U_l) \rightarrow \text{Hom}_{\Omega_L}(R_H, U_l)$$

by stipulating that for $\chi \in R_H$, $f \in \text{Hom}_{\Omega_K}(R_A^{(n)}, U_l)$

$$(v_\sigma f)(\chi) = f(\mathfrak{x}^\sigma \cdot \chi).$$

Let $\{\sigma\}$ run through a set of embeddings of $K \cap \mathbb{Q}(n)$ over $\mathbb{Q}$. We define $\tilde{v}$ to be the direct product of the v_σ .

Here $\mathfrak{x} \cdot \chi$ is interpreted as a virtual character in $R_A^{(n)}$, in the natural way. Indeed, because every irreducible character in $R_A^{(n)}$ can be uniquely written in the form $\mathfrak{x}^\theta \cdot \chi$, with $\theta \in \text{Gal}(\mathbb{Q}(\mathfrak{x})/\mathbb{Q})$ and χ an irreducible character of H , it is clear that $\tilde{v}$ is an isomorphism.

Now we consider $\tilde{v}(\text{Det}(\mathfrak{A}A^*)|_{R_A^{(n)}})$. We shall also denote by $\mathfrak{x}$ the algebra homomorphism $\mathfrak{x}: \mathfrak{A}A \rightarrow \prod_\sigma \mathfrak{B}H$, which is induced by the characters $\mathfrak{x}^\sigma$. We

remark that $\mathfrak{B}H$ is the standard group ring of H over $\mathfrak{B}$, since by definition H acts trivially on the values of $\mathfrak{x}$. Let $b \in \mathfrak{A}A$ and let T be a representation of H with character χ . Then $T \circ \mathfrak{x}^\sigma$ is a representation with character $\mathfrak{x}^\sigma \cdot \chi$. So by definition

$$v_\sigma(\text{Det}(b))(\chi) = \text{Det}(T(\mathfrak{x}^\sigma(b))) = \text{Det}(\mathfrak{x}^\sigma(b))(\chi).$$

Thus, as $\mathfrak{x}(\mathfrak{A}A^*) = \prod_\sigma \mathfrak{B}H^*$ we see that

$$\tilde{v}(\text{Det}(\mathfrak{A}A^*)|_{R_A^{(n)}}) = \prod_\sigma \text{Det}(\mathfrak{B}H^*),$$

and hence we obtain a commutative diagram

$$\begin{array}{ccc} \text{Hom}_{\Omega_K}(R_A^{(n)}, U_l) & \xrightarrow{\sim} & \prod_\sigma \text{Hom}_{\Omega_L}(R_H, U_l) \\ \uparrow & & \uparrow \\ \text{Det}(\mathfrak{A}A^*)|_{R_A^{(n)}} & \xrightarrow{\sim} & \prod_\sigma \text{Det}(\mathfrak{B}H^*). \end{array}$$

So, in order to show (7.3), it is sufficient to prove for each σ

$$(7.4) \quad v_\sigma(\tau_{A(n)}^*) \in \text{Det}(\mathfrak{B}H^*).$$

For the sake of notation, by writing $\mathfrak{x}$ in place of $\mathfrak{x}^\sigma$ we can assume $\sigma=1$, and we write v in place of v_1 . In the sequel, for brevity, we will write $\check{\tau}_{\Delta(n)}$ for $v(\tau_{\Delta(n)}^*)$.

Indeed, by factoring out by $\text{Ker}(\mathfrak{x})$ (which is normal in Δ), one sees that there is no loss of generality in assuming $\mathfrak{x}$ to be faithful on C . Thus we take the semi-product in Δ to be direct. Let I' be the inertia subgroup of Δ , let $I=I' \cap H$ and let $\mathfrak{D}_I$ be the subset of $\mathfrak{C}_H$ given by conjugacy classes of elements of I . Because H/I and I are both cyclic, by composing our extension with a sufficiently large unramified, l -power extension of $\mathbb{Q}_p$, we can assume the exact sequence

$$1 \rightarrow I \rightarrow H \rightarrow H/I \rightarrow 1$$

to be split. (For then we will have proved (7.4) with an “enlarged” H , and whence, by passing to the quotient, for H also).

Similarly, if $l=2$ and if H has an irreducible character of inversion type, then, arguing as in the last part of §3, we can enlarge H to ensure H has a character of semi-dihedral type. (This is a technical trick which will simplify subsequent arguments enormously.)

In the next section we will prove the following two propositions *without* using the hypothesis that H is “large enough” in the sense that H satisfies the above two properties.

Proposition 7.5. $v_H(\check{\tau}_{\Delta(n)} \in l\mathfrak{B}\mathfrak{D}_I$.

Proposition 7.6. *There exists $T' \in \mathfrak{B}I^*$ with the property that for all abelian characters χ in R_H ,*

$$\check{\tau}_\Delta(\chi) = \text{Det}(T')(\chi).$$

Now by Proposition 7.6 and by (4.3), we know that $\theta(v_H(\check{\tau}_{\Delta(n)} \cdot \text{Det}(T')^{-1}))=0$ for all abelian characters θ of H . Thus we deduce that

$$v_H(\check{\tau}_{\Delta(n)} \cdot \text{Det}(T')^{-1}) \in \phi_H(\mathfrak{a}) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

In order to show (7.4) we will need the following embellishment of Proposition 7.5.

Proposition 7.7. *There exists $z \in (1 + \mathfrak{a}) \cap \mathfrak{B}I$, so that*

$$v_H(\check{\tau}_{\Delta(n)} \cdot \text{Det}(T')^{-1}) = v_H(\text{Det}(z)).$$

First we need the following:

Lemma 7.8. *Suppose $[H, H]$ is non-trivial and let c be an element of $[H, H]$ of order l . We define*

$$\mathfrak{g} = (1 - c)\mathfrak{B}H = \text{Ker}(\mathfrak{B}H \rightarrow \mathfrak{B}H/\langle c \rangle).$$

Then

$$\phi_H(\mathfrak{g}) \cap \mathfrak{B}\mathfrak{D}_I = \phi_H((1 - c)\mathfrak{B}I).$$

Proof. Because c is central in H , c acts in a well-defined way on $\mathfrak{C}_H$ via multiplication, and in particular ϕ_H commutes with this multiplication. We

distinguish between 3 types of conjugacy class in H . Type 1: Those fixed by c -multiplication, Type 2: Those not fixed by c -multiplication and not in $\mathfrak{D}_I$, Type 3: Otherwise.

So now let $y \in \mathfrak{B}\mathfrak{C}_H$ with $(1-c)y \in \mathfrak{B}\mathfrak{D}_I$, and explicitly let

$$y = \Sigma^{(1)} b_{c_1} c_1 + \Sigma^{(2)} b_{c_2} c_2 + \Sigma^{(3)} b_{c_3} c_3$$

where $b_{c_i} \in \mathfrak{B}$ and the index above the summand denotes the type summed. We shall show we can take $y \in \mathfrak{B}\mathfrak{D}_I$. Clearly $(1-c)c_1 = 0$ for all conjugacy classes of type 1. Further, as $\mathfrak{D}_I$ is closed under c multiplication and as $(1-c)y \in \mathfrak{B}\mathfrak{D}_I$, $(1-c)\Sigma^{(2)} b_{c_2} c_2 = 0$. Thus we obtain

$$(1-c)y = (1-c)\Sigma^{(3)} b_{c_3} c_3,$$

as we required.

Proof of Proposition 7.7. We prove the result by arguing by induction on the order of $[H, H]$. Clearly if $[H, H] = 1$, then the result is a triviality. So let Z be the subgroup of order l in $[H, H]$ (recall that the latter group is contained in I and as such is cyclic). We write $\bar{H} = H/Z$, and in general, for an object associated to H , we denote the image under a homomorphism induced by $H \rightarrow \bar{H}$, by the adjunction of $\bar{}$.

So, by our induction hypothesis, we know

$$(7.9) \quad v_H(\check{\tau}_{\bar{A}(n)} \text{Det}(\bar{T}')^{-1}) = v_H(\text{Det}(\bar{z}))$$

for some $\bar{z} \in (1 + \bar{a}) \cap \mathfrak{B}\bar{I}$. We may now choose $z \in \mathfrak{B}I$ so that $z \mapsto \bar{z}$. As $\bar{z} \in 1 + \bar{a}$ it is immediate that $z \in 1 + a$. Let c generate Z . Then, with the notation of Lemma 7.8, by (7.9) we know

$$X = v_H(\check{\tau}_{\bar{A}(n)} \text{Det}(T'z)^{-1}) \in \text{Ker}(L\mathfrak{C}_H \rightarrow L\mathfrak{C}_{\bar{H}}) \otimes \mathbb{Q}_l.$$

We denote $\text{Ker}(L\mathfrak{C}_H \rightarrow L\mathfrak{C}_{\bar{H}})$ by Y . The kernel of $LH \rightarrow L\mathfrak{C}_H$ (resp. $L\bar{H} \rightarrow L\mathfrak{C}_{\bar{H}}$), A_H (resp. $A_{\bar{H}}$) say, is $\sum_{\gamma, \delta \in H} L(\gamma - \delta^{-1}\gamma\delta)$ (resp. $\sum_{\bar{\gamma}, \bar{\delta} \in \bar{H}} L(\bar{\gamma} - \bar{\delta}^{-1}\bar{\gamma}\bar{\delta})$). So, because A_H maps onto $A_{\bar{H}}$, on applying the snake lemma to the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & (1-c)LH & \longrightarrow & LH & \longrightarrow & L\bar{H} \longrightarrow 0 \\ & & \downarrow & & \downarrow \phi_H & & \downarrow \phi_H \\ 0 & \longrightarrow & Y & \longrightarrow & L\mathfrak{C}_H & \longrightarrow & L\mathfrak{C}_{\bar{H}} \longrightarrow 0 \end{array}$$

we obtain $Y = (1-c)L\mathfrak{C}_H$. By the above and Proposition 7.5, $X \in \phi_H(\mathfrak{g}) \otimes \mathbb{Q}_l \cap l\mathfrak{B}\mathfrak{D}_I$. Moreover, arguing as above, we can also show $\phi_H(\mathfrak{g}) = \text{Ker}(\mathfrak{B}\mathfrak{C}_H \rightarrow \mathfrak{B}\mathfrak{C}_{\bar{H}})$. Hence $\phi_H(\mathfrak{g})$ is a direct factor of $\mathfrak{B}\mathfrak{C}_H$ (as a $\mathfrak{B}$ -module), so that $\phi_H(\mathfrak{g}) \otimes \mathbb{Q}_l \cap l\mathfrak{B}\mathfrak{C}_H = l\phi_H(\mathfrak{g})$ thus $X \in l\phi_H(\mathfrak{g}) \cap l\mathfrak{B}\mathfrak{D}_I$, and so by Lemma 7.8,

$$v_H(\check{\tau}_{\bar{A}(n)} \cdot \text{Det}(T'z)^{-1}) \in l\phi_H((1-c)\mathfrak{B}I).$$

Moreover, as c is an element of order l in the cyclic commutator group $[H, H]$, there exist $\alpha, \beta \in H$ so that $c = \alpha\beta\alpha^{-1}\beta^{-1}$. Indeed, as H/I is cyclic, we can

suppose $\beta \in I$. Now we note that

$$\phi_H((1-c)\beta) = \phi_H(\beta - \alpha\beta\alpha^{-1}) = 0,$$

so because $(1-c)\beta$ generates the abelian group $(1-c)\mathfrak{B}I/(1-c)r_I$, we have shown

$$\phi_H((1-c)\mathfrak{B}I) = \phi_H((1-c)r_I).$$

Hence, for some $a \in (1-c)r_I$, we have

$$v_H(\check{\tau}_{A(m)} \cdot \text{Det}(T'z)^{-1}) = l\phi_H(a).$$

By Proposition 4.6 we can find $x \in \mathfrak{B}I$ so that $\mathfrak{Q}_1(1+(1-c)x) = la$, and so taking ϕ_H of both sides, we obtain

$$v_H(\text{Det}(1+(1-c)x)) = l\phi_H(a) = v_H(\check{\tau}_{A(m)} \cdot \text{Det}(T'z)^{-1})$$

which gives the required result.

We recall that the aim of this section is to show (7.4), assuming Propositions 7.5 and 7.6. It follows immediately from Proposition 7.7 and from (4.5), that for some $t \in \mathfrak{T}$

$$(7.10) \quad \check{\tau}_{A(m)} = t \cdot \text{Det}(T'z),$$

and, of course by Proposition 7.6, t is trivial on all abelian characters of H . We wish to show $t=1$. In order to show this we need:

Theorem 4. *Let χ be an irreducible character of H . Then $\chi = \text{Ind}_{\Phi}^H(\alpha)$ for some sub-group Φ of H , containing I , with α an abelian character of Φ .*

I. *If $\chi(1) > 2$, then we let Ψ be the unique sub-group of H containing Φ so that $(\Psi : \Phi) = l$ and we write $v\alpha = v_{\Phi}^{\Psi}(\alpha)$ and $\chi' = \text{Ind}_{\Psi}^H(v\alpha)$. Then order $(v\alpha|_I) < \text{order}(\alpha|_I)$,*

$$(Ia) \quad \tau_A^*(\mathfrak{x}\chi) \tau_A^*(\mathfrak{x}\chi')^{-F} \equiv 1 \pmod{2\mathfrak{Q}_2} \quad \begin{array}{ll} \text{if } l \neq 2, \\ \text{if } l = 2, \end{array}$$

and for $x \in \mathfrak{B}I^*$

$$(Ib) \quad \text{Det}(x)(\chi) \text{Det}(x)(\chi')^{-F} \equiv 1 \pmod{2\mathfrak{Q}_2} \quad \begin{array}{ll} \text{if } l \neq 2, \\ \text{if } l = 2. \end{array}$$

II. *If $\chi(1) = 2$ and if χ is of semi-abelian type, then there exists a sub-group Ψ of H so that $(H : \Psi) = (I : I \cap \Psi) = 2$ and an abelian character λ of Ψ so that $\chi = \text{Ind}_{\Psi}^H(\lambda)$. We write $v\lambda = v_{\Psi}^H(\lambda)$ and $\chi' = \text{Ind}_{\Psi}^H(\lambda^2)$. Then $v\lambda(\sigma) = \lambda(\sigma^2)$ for $\sigma \in I$,*

$$(IIa) \quad \tau_A^*(\mathfrak{x}\chi) \cdot \tau_A^*(\mathfrak{x} \cdot v\lambda)^{-F} = \tau_A^*(\mathfrak{x}\chi') \tau_A^*(\mathfrak{x} \cdot v\lambda^2)^{-F}$$

and for $x \in \mathfrak{B}I^*$ we have the congruence mod $2\mathfrak{Q}_2$

$$(IIb) \quad \text{Det}(x)(\chi) \text{Det}(x)(v\lambda)^{-F} \equiv \text{Det}(x)(\chi') \text{Det}(x)(v\lambda^2)^{-F}.$$

III. If $\chi(1)=2$ and if χ is of inversion type, then there exists an irreducible character $\tilde{\chi}$ of either inversion or semi-dihedral type on H , with $\tilde{\chi} = \text{Ind}_{\Phi}^H(\tilde{\alpha})$ and $\tilde{\alpha}^2|_I = \alpha|_I$. Then for some $\omega \in \Omega_{\mathbb{Q}}$ which fixes L (pointwise)

$$(IIIa) \quad \tau_A^*(\mathfrak{x}\tilde{\chi} + \mathfrak{x}\tilde{\chi}^{\omega}) \tau_A^*(\mathfrak{x}\chi)^{-F} \equiv 1 \pmod{4}$$

and for $x \in \mathfrak{B}I^*$

$$(IIIb) \quad \text{Det}(x)(\tilde{\chi} + \tilde{\chi}^{\omega}) \cdot \text{Det}(x)(\chi)^{-F} \equiv 1 \pmod{2\Omega_2}.$$

IV. If $\chi(1)=2$ and if χ is of semi-dihedral type, we put $E=L(\alpha|_I)$. For any abelian character ϕ of Φ , we write ϕ_* for $\text{Ind}_{\Phi}^H\phi$, and furthermore we will write ε_* in place of $(\varepsilon_{\Phi})_*$. Let 2^r be the order of $\alpha|_I$. Then we have the following congruences mod(4),

$$(IVa) \quad \begin{aligned} & 2^{1-r} \text{Tr}_{E/L}(\tau_A^*(\mathfrak{x}\chi)) - \tau_A^*(\mathfrak{x}\det_{\chi})^F \\ & \equiv \sum_{\phi} \tau_A^*(\mathfrak{x}\phi_*) \cdot 2^{1-r} - \tau_A^*(\mathfrak{x}\det_{\varepsilon_*})^F \end{aligned}$$

and for $x \in \mathfrak{B}I^*$

$$(IVb) \quad \begin{aligned} & 2^{1-r} \text{Tr}_{E/L}(\text{Det}(x)(\chi)) - \text{Det}(x)(\det_{\chi})^F \\ & \equiv \sum_{\phi} \text{Det}(x)(\phi_*) \cdot 2^{1-r} - \text{Det}(x)(\det_{\varepsilon_*})^F. \end{aligned}$$

Here the sums on the right hand side extend over abelian characters of $I/\text{Ker}(\alpha^2|_I)$ extended to Φ (arbitrarily). Further both sides in IVa are divisible by 2.

We shall prove parts (a) of this theorem in §9 and parts (b) in §10.

Our aim now is to show that for irreducible χ on H $t(\chi)=1$, using the above result. We shall argue by induction on the index $(I: \text{Ker}(\chi|_I))$. First though, we note that by Proposition 7.6, $t(\chi)=1$ if χ is abelian. This starts our induction.

So now we suppose that χ is irreducible of degree 2. (If $l \neq 2$, of course this is vacuous). First we take χ to be of semi-abelian type. Then by IIa and IIb we deduce

$$t(\chi)t(v\lambda)^{-F} \equiv t(\chi')t(v\lambda^2)^{-F} \pmod{2\Omega_2}.$$

Since $v\lambda|_{I \cap \Psi} = \lambda^2|_{I \cap \Psi}$, then by our induction hypothesis,

$$t(v\lambda) = t(\chi') = t(v\lambda^2) = 1.$$

And so, since the torsion elements of U_2 are all distinguished mod $2\Omega_2$, we deduce $t(\chi)=1$, as we required.

Now we take χ to be of inversion or of semi-dihedral type. It is immediate that $\mathfrak{x} \cdot \text{Ind}_{\Phi}^H(\alpha - \varepsilon_{\Phi}) \in \text{Ker } d_2$, and so by Proposition 3.8 and Proposition 3.10(v)

$$t(\text{Ind}_{\Phi}^H(\alpha - \varepsilon)) \equiv 1 \pmod{\Omega_2}.$$

However, $\text{Ind}_{\Phi}^H(\varepsilon_{\Phi})$ is the sum of two abelian characters and so we deduce that

$$(7.11) \quad t(\chi) \equiv 1 \pmod{\mathfrak{Q}_2}$$

and thus $t(\chi)$ is of 2-power order.

Now we observe that $\tau_A^*(\mathfrak{x}\chi)$ and $\text{Det}(\mathfrak{B}I^*)(\chi)$ are both contained in $L(\chi|_I) \otimes \mathbb{Q}_2$, (cf. Proposition 3.10(iv)). Whence, because the only roots of unity in $\mathbb{Q}(\chi|_I)$ are seen to be ± 1 , we see that $t(\chi)$ has order at most 2.

Next we specialise to the case when χ is of inversion type only. We let $\tilde{\chi}$ be as in the theorem above. From IIIa and IIIb we deduce that

$$t(\tilde{\chi} + \tilde{\chi}^{\omega}) \equiv t(\chi)^F \pmod{2\mathfrak{Q}_2}.$$

Since $\tilde{\tau}$ and the elements of $\text{Det}(\mathfrak{B}H^*)$ are Ω_L homomorphisms, we know that $t(\tilde{\chi}^{\omega}) = t(\tilde{\chi})^{\omega}$, and further, as ω fixes L with $t(\tilde{\chi})$ of order 2, we know $t(\tilde{\chi})^{\omega} = t(\tilde{\chi})$. But a priori, as $\tilde{\chi}$ is of inversion or semi-dihedral type, $t(\tilde{\chi})^2 = 1$, and so we deduce $t(\chi) = 1$.

Now we take χ to be of semi-dihedral type. Then by IVb we know that $\text{mod}(4)$

$$\begin{aligned} & 2^{1-r} \cdot \text{Tr}_{E/L}(t^{-1}\tilde{\tau}_A(\chi)) - t^{-1}\tilde{\tau}_A(\det_{\chi})^F \\ & \equiv \sum_{\phi} t^{-1}\tilde{\tau}_A(\phi_*) 2^{1-r} - t^{-1}\tilde{\tau}_A(\det(\varepsilon_*))^F. \end{aligned}$$

However, by our induction hypothesis we know that $t(\phi_*) = 1$; while

$$t(\det_{\chi}) = t(\det(\varepsilon_*)) = 1$$

since t is known to be trivial on abelian characters. Now we subtract the above congruence from IVa and we obtain:

$$2^{1-r} \cdot \text{Tr}_{E/L}((t(\chi)^{-1} - 1)\tilde{\tau}_A(\chi)) \equiv 0 \pmod{4}.$$

However, we have already seen that the two torsion of $(L(\chi|_I) \otimes \mathbb{Q}_2)^*$ is the same as that of $(L \otimes \mathbb{Q}_2)^*$, and so we obtain

$$2^{1-r} \cdot (t(\chi)^{-1} - 1) \cdot \text{Tr}_{E/L}(\tilde{\tau}_A(\chi)) \equiv 0 \pmod{4}.$$

Moreover, because the left hand side of IVa is known to be divisible by 2, while $\tau_A^*(\mathfrak{x} \det_{\chi})$ is a 2-unit, we must have that $2^{1-r} \cdot \text{Tr}_{E/L}(\tilde{\tau}_A(\chi))$ is a 2-unit, and so from the above we deduce $t(\chi) = 1$, as we required.

Lastly we suppose that χ has degree > 2 . Then by Ia and Ib we obtain the congruence

$$t(\chi)t(\chi')^{-F} \equiv 1 \pmod{2\mathfrak{Q}_2}^{(l)} \quad \begin{array}{ll} \text{if } l \neq 2, \\ \text{if } l = 2. \end{array}$$

However, we know that $\text{Ker}(\chi'|_I) \supseteq \text{Ker}(\chi|_I)$ and so, by our induction hypothesis, we deduce that $t(\chi') = 1$ and whence $t(\chi) = 1$.

8. Logarithm of the Gauss Sum Homomorphism

Our notation is the same as in the previous section.

Let A be the maximal abelian sub-group of Δ which contains both C and I , and let $\Sigma = A \cap H$. Let D (resp. G) be the subfield of M fixed by A (resp. Δ). Following [T2] we define $T_1 \in \mathbb{Z}[\zeta_p]A$ by

$$T_1 = \sum_{u \bmod^* p_D} (u, M/D) \psi_D(u c^{-1})$$

and, denoting the maximal abelian extension of G in M by M^{ab} ,

$$T_2 = \sum_{v \bmod^* p_G} (v, M^{ab}/G) \psi_G(v c^{-1}).$$

(Here $(-, M/D)$, $(-, M^{ab}/G)$ are the normal Artin symbols).

For $x, y \in \mathbb{Q}^*$, we shall say $x \sim y$ if xy^{-1} is a root of unity.

Proposition 8.1. (i) For all $\alpha \in R_{A^{ab}}, \beta \in R_A$

$$\text{Det}(T_2)(\alpha) = \tau_{A^{ab}}^*(\alpha) = \tau_A^*(\alpha),$$

(ii) For all $\chi \in R_A$

$$\text{Det}(T_1)(\beta) = \tau_A^*(\beta).$$

$$\text{Det}(T_1)(\chi) \sim \tau_A^*(\chi)^{(A:A)}.$$

Proof. First we show part (i) for T_2 and A^{ab} (the proof for T_1 and A being the same). Clearly it is enough to establish the result when α is an abelian character. If α is genuinely ramified then the equation follows immediately from the definition of the Galois Gauss Sum on abelian characters. So now we suppose α to be non-ramified. In the proof of Proposition 3.10 we showed that for such α , $\tau_A^*(\alpha) = -1$. However, because α is non-ramified

$$\text{Det}(T_2)(\alpha) = \sum_v \psi_G(v c^{-1}).$$

Thus, as $\psi_G(- \cdot c^{-1})$ defines a non-trivial additive character on $\mathfrak{D}_G \bmod \mathfrak{p}_G$, we see that the right hand side is -1 as required.

Now we show (ii). By $\mathbb{Z}$ -linearity we may assume χ to be irreducible. Thus we can write $\chi = \text{Ind}_\Omega^A(\beta)$ with $\Omega \supset A$ and β an abelian character of Ω . So since $T_1 \in \mathfrak{A}_A$,

$$\text{Det}(T_1)(\chi) = \text{Det}(T_1)(\chi|_A)$$

and by Mackey's restriction formula

$$= \prod_{\gamma \in A/\Omega} \text{Det}(T_1)(\beta^\gamma|_A).$$

Now from part (i) we know

$$\text{Det}(T_1)(\beta^\gamma|_A) = \tau_A^*(\beta^\gamma|_A)$$

and by (0.8) in $[DH]$

$$\tau_A^*(\beta^\gamma|_A) \sim \tau_\Omega^*(\beta^\gamma)^{(\Omega:A)}.$$

Moreover, by the inductivity of τ in degree zero, together with the fact that $I' \subset \Omega$, $\tau_A^*(\chi) = \tau_A^*(\text{Ind}_\Omega^A \beta^\gamma) \sim \tau_\Omega^*(\beta^\gamma)$, which establishes part (ii).

To obtain the element T' required for Proposition 7.6, we choose any $x \in \mathfrak{U}I'$ so that $x \mapsto T_2$ under the algebra homomorphism $\mathfrak{U}A \rightarrow \mathfrak{U}A^{ab}$. We note that x is necessarily a unit because the kernel of this homomorphism is contained in the Jacobson radical of $\mathfrak{U}A$ and because by Proposition 8.1 and Proposition 3.10(i) T_2 is itself a unit in $\mathfrak{U}A^{ab}$. We then let $T' = \mathfrak{x}(x)$ in $\mathfrak{B}H$, and we have now established Proposition 7.6.

Corollary 8.2. *Let $S \in \mathfrak{B}\Sigma$ be the image of T_1 under the composite $\mathfrak{U}A \hookrightarrow \mathfrak{U}A \xrightarrow{x} \mathfrak{B}H$, then*

$$v_H(\text{Det}(S)) = (\Delta : A) v_H(\check{\tau}_{\Delta(n)}).$$

Proof. By part (ii) of the above proposition $\text{Det}(S)^{-1} \check{\tau}^{(\Delta:A)}$ is torsion valued on R_H and whence lies in $\text{Ker}(v_H)$.

As a result of this corollary, in order to prove Proposition 7.5 it is enough to show that

$$(8.3) \quad v_H(\text{Det}(S)) \in l(\Delta : A) \mathfrak{B} \mathfrak{D}_I.$$

Our aim now is to calculate $v_H(\text{Det}(S))$. To achieve this we first calculate $v_\Sigma(\text{Det}(S))$ by means of a standard Fourier Inversion technique, and then we use the commutative diagram

$$\begin{array}{ccccc} \mathfrak{B}\Sigma^* & \longrightarrow & \text{Det}(\mathfrak{B}\Sigma^*) & \xrightarrow{v_\Sigma} & l\mathfrak{B}\mathfrak{C}_\Sigma \\ \downarrow & & \downarrow & & \downarrow \eta \\ \mathfrak{B}H^* & \longrightarrow & \text{Det}(\mathfrak{B}H^*) & \xrightarrow{v_H} & l\mathfrak{B}\mathfrak{C}_H. \end{array}$$

Here η is the $\mathfrak{B}$ -linear map induced by $\Sigma \hookrightarrow H$.

Theorem 5. *Let $v_\Sigma(\text{Det}(S)) = \sum_{\sigma \in \Sigma} S_\sigma \sigma$, with $S_\sigma \in \mathfrak{B} \otimes \mathbb{Q}_l$. (Note that because Σ is abelian, Σ identifies with $\mathfrak{C}_\Sigma$).*

- (a) *If $\sigma \notin I$, then $S_\sigma = 0$.*
- (b) *If $I \neq \{1\}$, $S_1 = \frac{l-1}{2} \log N \mathfrak{p}_D$.*
- (c) *If $1 \neq \langle \sigma \rangle \not\subseteq I$, then $S_\sigma = 0$.*
- (d) *If $\langle \sigma \rangle = I$, then $S_\sigma \in l\mathfrak{B}$.*
- (e) *For any $\gamma \in H$, $S_{\sigma\gamma} = S_\sigma$.*

Proof. By the standard orthogonality result for abelian characters,

$$|\Sigma| S_\sigma = \sum_{\theta \in \hat{\Sigma}} \theta(v_\Sigma(\text{Det}(S))) \theta(\sigma^{-1}).$$

Here $\hat{\Sigma}$ denotes the multiplicative group of abelian characters of Σ . By (4.3),

$$\begin{aligned}\theta(v_{\Sigma}(\text{Det}(S))) &= \log(\text{Det}(S)(l\theta)) \\ &\quad - \log(\text{Det}(S)(\psi^l(\theta))^F)\end{aligned}$$

by Proposition 8.1(i) $\text{Det}(S) = \check{\tau}_{A(n)}$, so that

$$\theta(v_{\Sigma}(\text{Det}(S))) = \log(\tau_A^*(l\mathfrak{x}\theta) \cdot \tau_A^*(-\mathfrak{x}\psi^l(\theta))^F)$$

and so we obtain

$$(8.4) \quad |\Sigma|S_{\sigma} = \sum_{\theta} \log(\tau_A^*(l\mathfrak{x}\theta) \cdot \tau_A^*(-\mathfrak{x}\psi^l(\theta))^F) \theta(\sigma^{-1}).$$

Now we prove part (a); so let $\sigma \notin I$ and choose a non-ramified abelian character α of Σ which is non-trivial on σ . By Proposition 3.10(iii),

$$\begin{aligned}\tau_A^*(l\mathfrak{x}\theta\alpha) &= \tau_A^*(l\mathfrak{x}\theta), \\ \tau_A^*(\mathfrak{x} \cdot \psi^l(\theta\alpha)) &= \tau_A^*(\mathfrak{x}\theta^l\alpha^l) = \tau_A^*(\mathfrak{x}\theta^l).\end{aligned}$$

Hence writing $\theta\alpha$ for θ in (8.4), we get

$$|\Sigma|S_{\sigma} = \sum_{\theta} \log(\tau_A^*(l\mathfrak{x}\theta) \cdot \tau_A^*(-\mathfrak{x}\theta^l)^F) \theta\alpha(\sigma^{-1})$$

and so $|\Sigma|S_{\sigma} = \alpha(\sigma)|\Sigma|S_{\sigma}$, which implies $S_{\sigma} = 0$ because $\alpha(\sigma) \neq 1$.

Next we consider the case when $1 \neq \langle \sigma \rangle \subseteq I$. Let μ' be the group of abelian characters of I of order $\leq l$, and let $\{\mu_i\}_i^l = 1$ be extensions to Σ of the characters in μ' . Then, because each $\mu_i(\sigma) = 1$, we see that

$$l|\Sigma|S_{\sigma} = \sum_{\theta} \sum_i \log(\tau_A^*(l\mathfrak{x}\theta\mu_i) \tau_A^*(-\mathfrak{x}\theta^l\mu_i^l)^{-F}) \theta(\sigma^{-1}).$$

Now from (0.9₁) of [DH] (cf. also (3.8) of [FT]) and by pairing conjugate characters

$$\tau_A^*(\sum_i \mathfrak{x}\theta\mu_i) \tau_A^*(-\mathfrak{x}^l \cdot \theta^l) \sim N \mathfrak{p}_D^{\frac{l-1}{2}}$$

while by the Galois action formula for Gauss sums

$$\tau_A^*(\mathfrak{x}^l\theta^l) \sim \tau_A^*(\mathfrak{x}\theta^l)^F.$$

So, because μ_i^l is non-ramified, we can write the coefficient for $\theta(\sigma^{-1})$ as

$$\log(\tau_A^*(\sum_i l\mathfrak{x}\theta\mu_i - l\mathfrak{x}^l\theta^l))$$

and hence we obtain

$$l|\Sigma|S_{\sigma} = \sum_{\theta} \frac{l(l-1)}{2} \log N \mathfrak{p}_D \cdot \theta(\sigma^{-1}) = 0.$$

The calculation for S_1 – when $I \neq \{1\}$, so that μ' has order l – is now immediate. Namely by the above

$$l|\Sigma|S_1 = |\Sigma| \cdot \frac{l(l-1)}{2} \log N \mathfrak{p}_D.$$

In order to prove (e), we observe that by (8.4)

$$\begin{aligned} |\Sigma|S_{\sigma^\gamma} &= \sum_{\theta} \log(\tau_A^*(l\mathfrak{x}\theta) \tau_A^*(\mathfrak{x}\theta^l)^{-F}) \theta(\sigma^{-\gamma}) \\ &= \sum_{\theta} \log(\tau_A^*(l\mathfrak{x}\theta) \cdot \tau_A^*(\mathfrak{x}\theta^l)^{-F}) \theta^{\gamma^{-1}}(\sigma^{-1}). \end{aligned}$$

However, for each $\chi \in R_A$, we know $\tau_A(\mathfrak{x}\chi^\gamma) = \tau_A(\mathfrak{x}\chi)$ (by the inductivity of τ). Thus we obtain that $|\Sigma|S_{\sigma^\gamma} = |\Sigma|S_\sigma$.

It now remains to prove (d). This is an immediate consequence of (4.4.a) (writing Σ in place of H). Theorem 5 is now shown.

Next we calculate the value

$$v_H(\text{Det}(S)) = \eta(v_\Sigma(\text{Det}(S)))$$

(recall η is the map $\mathfrak{B}\mathfrak{C}_\Sigma \rightarrow \mathfrak{B}\mathfrak{C}_H$ induced by $\Sigma \hookrightarrow H$). We shall suppose $v_H(\text{Det}(S)) = \sum_{c \in \mathfrak{C}_H} t_c c$.

From Theorem 5 we see that $t_c = 0$, except when $c = 1$ or when c is the conjugacy class of a generator of I . For the case $c = 1$, because 1 in $\mathfrak{C}_\Sigma$ is the only conjugacy class to map to 1 in $\mathfrak{C}_H$, we see that, providing $I \neq \{1\}$,

$$t_1 = \frac{l-1}{2} \log N \mathfrak{p}_D.$$

Now as D/G is non-ramified, $N \mathfrak{p}_D = N \mathfrak{p}_G^{(A:A)}$, and so, as $\frac{l-1}{2} \cdot \log N \mathfrak{p}_G$ is always l divisible, we see that $t_1 \in l(\Delta:A)\mathbb{Z}_l$. (Note we have used $\log(\mathbb{Z}_2^*) = 4\mathbb{Z}_2$ here). The singular case $c = 1$ when $I = \{1\}$ is a special case of the second case, namely when c is the conjugacy class of a generator of I . So now we suppose $\langle \sigma \rangle = 1$. Because H/Σ acts faithfully on I , the elements $\{\sigma^\gamma\}_{\gamma \in H/\Sigma}$ are all distinct. Hence, by Theorem 5(e)

$$t_c = (\Delta:A)S_\sigma$$

while by part (d) of the theorem $S_\sigma \in l\mathfrak{B}$. Thus indeed we have shown $v_H(\text{Det}(S)) \in l(\Delta:A)\mathfrak{B}\mathfrak{C}_H$, as required to show Proposition 7.5.

9. Gauss Sum Congruences

In this section we prove Ia, IIa, IIIa and IVa. We preserve the notation of Sect. 7.

For subgroups Φ, Ψ of H we write $\Phi' = C \times \Phi$, $\Psi' = C \times \Psi$. If $\chi \in R_\Phi$, then we denote by $\mathfrak{x}\chi$ the external product of characters, i.e. for $(c, \phi) \in C \times \Phi$

$$\mathfrak{x}\chi(c, \phi) = \mathfrak{x}(c) \cdot \chi(\phi).$$

More generally if $\Psi \subset \Phi$, then we see that the maps on R_Φ and R_Ψ defined by external product with $\mathfrak{x}$ commute with restriction and induction. On the other hand if θ is an abelian character of Ψ then we see that

$$\nu_{\Psi'}^{\Phi'}(\mathfrak{x}\theta) = \mathfrak{x}^{(\Phi:\Psi)} \cdot \nu_\Psi^\Phi \theta.$$

Proof of Ia. Arguing as in 5.1 of [FT], we obtain the congruence

$$\tau_\Phi(\mathfrak{x}\alpha) \tau_{\Psi'}(\mathfrak{x} \cdot \nu\alpha)^{-F} \equiv 1 \pmod{2^{\mathfrak{e}_2}} \begin{matrix} (l) & \text{if } l \neq 2, \\ & \text{if } l = 2. \end{matrix}$$

In fact this congruence is proved only for the case when $\mathfrak{x} = 1$ and under the hypothesis that $\nu\alpha$ is genuinely ramified. We shall show $\nu\alpha$ is genuinely ramified below, and we remark that the argument in [FT] extends trivially to $\mathfrak{x}$, because H acts trivially on $\mathfrak{x}$.

Now, by the inductivity in degree zero of τ , we know

$$\begin{aligned} \tau_\Delta(\mathfrak{x}\chi) &= \tau_\Phi(\mathfrak{x}\alpha) \tau_\Delta(\rho_{\Delta/\Phi'}) \\ \tau_\Delta(\mathfrak{x}\chi') &= \tau_{\Psi'}(\mathfrak{x} \cdot \nu\alpha) \tau_\Delta(\rho_{\Delta/\Psi'}) \end{aligned}$$

where $\rho_{\Delta/\Phi'}$ and $\rho_{\Delta/\Psi'}$ are the regular characters of Δ/Φ' and Δ/Ψ' inflated to Δ . We note that

$$\tau_\Delta(\rho_{\Delta/\Phi'}) = \det(\rho_{\Delta/\Phi'})(D_G) = \det(\rho_{\Delta/\Psi'})(D_G) = \tau_\Delta(\rho_{\Delta/\Psi'})$$

and so we obtain

$$\tau_\Delta(\mathfrak{x}\chi) \tau_\Delta(\mathfrak{x}\chi')^{-F} \equiv 1 \pmod{2^{\mathfrak{e}_2}} \begin{matrix} (l) & \text{if } l \neq 2, \\ & \text{if } l = 2. \end{matrix}$$

Similarly we see that

$$\begin{aligned} \det(\mathfrak{x}\chi) &= \mathfrak{x}^{(H:\Phi)} (\nu_\Phi^H \alpha \cdot \det(\text{Ind}_\Phi^H \varepsilon_\Phi)) \\ &= \mathfrak{x}^{(H:\Psi)^F} (\nu_\Psi^H (\nu\alpha) \cdot \det(\text{Ind}_\Psi^H \varepsilon_\Psi)) = \det(\mathfrak{x}\chi')^F, \end{aligned}$$

and so in order to show Ia it will be sufficient to show $y_\Delta(\mathfrak{x}\chi) = y_\Delta(\mathfrak{x}\chi') = 1$. But since χ is non-abelian and irreducible, it is clear that $y_\Delta(\mathfrak{x}\chi) = 1$. Now choose $\delta \in \Psi \setminus \Phi$. Then by Mackey's criterion we know $\alpha^\delta|_I \neq \alpha|_I$. We let $\text{ord}(\alpha|_I) = l'$, and $u \in \mathbb{Z}_l^*$ is chosen so that $\alpha^\delta|_I = \alpha^u|_I$. Then it is immediate that u has order $l \bmod^*(l')$ and that $u \equiv 1 \pmod{l}$. Moreover, if $l = 2$, we know that u is a square since $(H:\Psi) \geq 2$; hence $u \equiv 1 \pmod{8}$. Thus we can deduce

$$\begin{aligned} (9.1) \quad u &\equiv 1 + al'^{-1} \pmod{l'} \quad \text{with } (a, l) = 1, \\ r &\geq 2 \quad \text{if } l \neq 2, \\ r &\geq 4 \quad \text{if } l = 2. \end{aligned}$$

It is now easily calculated that for $\sigma \in I$

$$(9.2) \quad v\alpha(\sigma) = \prod_{i=1}^l \alpha(\sigma)^{u_i} \equiv \alpha'(\sigma) \pmod{l}.$$

In particular $v\alpha|_I$ has order l^{r-1} and so $v\alpha$ is genuinely ramified, whence $y_A(x\chi') = 1$. We assume H is a 2-group from now on. Before proving IIa we need the following:

Lemma 9.3. *Let $B \subset A \subset H$ with $(A:B) = (A \cap I : B \cap I) = 2$, let $A' = C \times A$, $B' = C \times B$, let β be a genuinely ramified abelian character of B and let μ be the non-trivial abelian character of A' with kernel B' . Then*

$$\tau_A^*(x \cdot \text{Ind}_B^A \beta) = \tau_{A'}^*(x \cdot v_B^A \beta)^F \tau_{A'}^*(\mu).$$

Proof. Since $x \cdot \text{Ind}_B^A(\beta) = \text{Ind}_{B'}^{A'}(x \cdot \beta)$ and because τ is inductive in degree zero

$$\begin{aligned} \tau_{A'}(x \cdot \text{Ind}_B^A \beta) &= \tau_{A'}(\text{Ind}_{B'}^{A'}(x \cdot \beta)) \\ &= \tau_{B'}(x \beta) \tau_{A'}(\mu) \\ &= \tau_{A'}(\mu) \sum x \beta(uc^{-1}) \psi_{B'}(uc^{-1}) \end{aligned}$$

where u runs through a set of representatives of the units in $N^{B'}$ modulo the prime. However, as $N^{B'}/N^{A'}$ is totally ramified we can choose the u to lie in $N^{A'}$. Thus by local classfield theory

$$\tau_{A'}(x \cdot \text{Ind}_B^A \beta) = \tau_{A'}(\mu) \sum v_B^{A'}(x \beta)(uc^{-1}) \psi_{A'}(2uc^{-1})$$

and so because $v_B^{A'}(x \beta) = x^2 \cdot v_B^A \beta$

$$\tau_{A'}(x \cdot \text{Ind}_B^A \beta) = \tau_{A'}(\mu) \tau_{A'}(x \cdot v_B^A \beta)^F.$$

Moreover, as tame inertia groups are cyclic and $(A \cap I : B \cap I) = (A:B)$, ver_B^A maps inertia group onto inertia group, and thus $v_B^A \beta$ is genuinely ramified. Hence

$$y_{A'}(x \cdot \text{Ind}_B^A \beta) = y_{A'}(\mu) = y_{A'}(x \cdot v_B^A \beta) = 1,$$

while it is elementary that

$$\det(x \cdot \text{Ind}_B^A \beta) = \mu \cdot x^{(A:B)} \cdot v_B^A \beta = \mu \cdot x^F \cdot v_B^A \beta.$$

Putting together the above equations for τ , y and $\det$ then gives the required equation for τ^* .

Proof of IIa. Recall that in §7 we assumed the exact sequence

$$(9.4) \quad 1 \rightarrow I \rightarrow H \rightarrow H/I \rightarrow 1$$

to be split. So, with the notation of Theorem 4, we choose Ψ to be a sub-group of H so that $(H:\Psi) = (I:I \cap \Psi) = 2$. Because H/I acts trivially on $\alpha|_{I_2}$ (since χ is of semi-abelian type), we may extend $\alpha|_{\Psi \cap \Phi}$ to an abelian character λ of Ψ . Now,

by a double application of Frobenius reciprocity and by Mackey's restriction formula

$$\begin{aligned}\langle \text{Ind}_{\Psi}^H \lambda, \text{Ind}_{\Phi}^H \alpha \rangle &= \langle \lambda, \text{Ind}_{\Phi \cap \Psi}^{\Psi} (\alpha|_{\Phi \cap \Psi}) \rangle \\ &= \langle \lambda|_{\Phi \cap \Psi}, \alpha|_{\Phi \cap \Psi} \rangle = 1\end{aligned}$$

and so, because $\text{Ind}_{\Phi}^H(\alpha) = \chi$ is irreducible of degree 2, we deduce $\chi = \text{Ind}_{\Psi}^H(\lambda)$. By Lemma 9.3

$$\tau_A^*(x\chi) \tau_A^*(x \cdot v\lambda)^{-F} = \tau_A^*(\mu)$$

where μ is the non-trivial abelian character of Δ/Ψ' inflated to Δ . Because χ is of semi-abelian type, $\text{order}(\lambda|_{I \cap \Psi}) \geq 4$, and so in particular λ^2 is genuinely ramified. Thus, arguing in the same way, we get

$$\tau_A^*(x\chi') \tau_A^*(xv\lambda^2)^{-F} = \tau_A^*(\mu),$$

which then establishes IIa. Lastly, we note that because $(I:I \cap \Psi) = (H:\Psi) = 2$, we can choose $\{1, \sigma\}$ as a transversal of H/Ψ , where σ generates I . So by the usual definition of the transfer $v_{\Psi}^H \lambda(\sigma) = \lambda(\sigma^2)$, as we required.

Proof of IIIa. Again, since (9.4) is split, we can choose $\Psi \subset \Phi$ so that $(\Phi:\Psi) = (I:I \cap \Psi) = 2$. We define $\theta = \text{Ind}_{\Psi}^H(\tilde{\alpha}|_{\Psi})$, where $\tilde{\alpha}$ is an abelian character of Φ so that $\tilde{\alpha}^2|_I = \alpha|_I$. (The existence of such an $\tilde{\alpha}$ is guaranteed by our hypothesis on H in § 7). As previous we put $\tilde{\chi} = \text{Ind}_{\Phi}^H \tilde{\alpha}$. It is then immediate that $\theta = \tilde{\chi} + \tilde{\chi}\mu$, where μ is a genuinely ramified quadratic abelian character of Δ . Thus, if $\omega \in \Omega_{\mathbb{Q}}$ is such that ω fixes $L(\alpha|_I)$ but not $L(\tilde{\alpha}|_I)$, then $\tilde{\chi}^{\omega} = \text{Ind}_{\Phi}^H \tilde{\alpha}^{\omega}$ and $\tilde{\chi}\mu = \text{Ind}_{\Phi}^H(\tilde{\alpha} \cdot \mu|_{\Phi})$, and, by the definition of ω , the restrictions to the inertia group I of $\tilde{\alpha}^{\omega}$ and $\tilde{\alpha} \cdot \mu|_{\Phi}$ coincide. So we deduce that $\tilde{\chi}^{\omega}$ and $\tilde{\chi}\mu$ differ only by a multiple of a non-ramified abelian character. Hence by Proposition 3.10 (iii)

$$(9.5) \quad \tau_A^*(x\theta) = \tau_A^*(x\tilde{\chi} + x\tilde{\chi}\mu)$$

and similarly for $x \in \mathfrak{B}I^*$

$$(9.6) \quad \text{Det}(x)(\theta) = \text{Det}(x)(\tilde{\chi} + \tilde{\chi}^{\omega}).$$

By the inductivity of Gauss sums in degree zero, we know

$$\begin{aligned}(9.7) \quad \tau_A(x\theta) &= \tau_{\Phi}(x \cdot \text{Ind}_{\Psi}^{\Phi}(\tilde{\alpha}|_{\Psi})) \tau_A(v)^2 \\ \tau_A(x\chi) &= \tau_{\Phi}(x\alpha) \tau_A(v) = -v(c^{-1}) \tau_{\Phi}(x\alpha)\end{aligned}$$

where v is the non-trivial, non-ramified abelian character of Δ . Further, as α and $\tilde{\alpha}$ are both genuinely ramified, $y(x\theta) = y(x\chi) = 1$. Moreover, it is easily calculated that

$$\det(x\theta) = v_{\Phi}^{\Delta}(\det(x \text{Ind}_{\Psi}^{\Phi}(\tilde{\alpha}|_{\Psi}))),$$

whence by local classfield theory

$$\det(x\theta)(c) = \det(x \text{Ind}_{\Psi}^{\Phi}(\tilde{\alpha}|_{\Psi}))(c).$$

Similarly,

$$\det(\mathfrak{x}\chi) = \mathfrak{x}^2 \cdot v_{\Phi}^H(\alpha) \cdot v$$

and

$$\det(\mathfrak{x}\chi)(c) = \mathfrak{x}^2(c) \cdot v(c) \cdot \alpha(c).$$

Thus, as $\mathfrak{x}^F = \mathfrak{x}^2$, from (9.7)

$$\tau_{\Delta}^*(\mathfrak{x}\theta) \tau_{\Delta}^*(\mathfrak{x}\chi)^{-F} = -\tau_{\Phi}^*(\mathfrak{x} \cdot \text{Ind}_{\Psi}^{\Phi}(\tilde{\alpha}|_{\Psi})) \tau_{\Phi}^*(\mathfrak{x}\alpha)^{-F}.$$

Because $\tilde{\alpha}|_{\Psi}$ is ramified, we can apply Lemma 9.3, and we obtain

$$\tau_{\Phi}^*(\mathfrak{x} \cdot \text{Ind}_{\Psi}^{\Phi}(\tilde{\alpha}|_{\Psi})) = \tau_{\Phi}^*(\mathfrak{x} \cdot v_{\Psi}^{\Phi}(\tilde{\alpha}|_{\Psi}))^F \tau_{\Phi}^*(v_1)$$

where v_1 is the non-trivial abelian character of Φ'/Ψ' inflated to Φ . However, it is immediate that $v_{\Psi}^{\Phi}(\tilde{\alpha}|_{\Psi}) = \tilde{\alpha}^2$, and since $\tilde{\alpha}^2|_I = \alpha|_I$, by Proposition 3.10(iii)

$$\tau_{\Phi}^*(\mathfrak{x} \cdot v_{\Psi}^{\Phi}(\tilde{\alpha}|_{\Psi})) = \tau_{\Phi}^*(\mathfrak{x}\alpha)$$

and so we have now shown

$$\tau_{\Delta}^*(\mathfrak{x}\theta) \tau_{\Delta}^*(\mathfrak{x}\chi)^{-F} = -\tau_{\Phi}^*(v_1).$$

Let v_2 be a ramified quadratic abelian character of Δ , then by (0.8) of [DH] we know

$$(-\tau_{\Delta}^*(v_2))^2 = -\tau_{\Phi}^*(v_1).$$

But clearly $\tau_{\Delta}^*(v_2) \equiv 1 \pmod{2}$, since v_2 is of order 2. Thus $\tau_{\Delta}^*(v_2)^2 \equiv 1 \pmod{4}$, and so IIIa is established.

Proof of IVa. For any positive integer s we write I_s for the group of 2^s -th powers I^{2^s} . In particular I_r is the kernel of $\alpha|_I$. Let η be any abelian character of Φ/I_r inflated to Φ . We denote the non-trivial abelian character of Δ with kernel Φ' by μ . By the inductivity of τ in degree zero

$$\tau_{\Delta}(\mathfrak{x} \cdot \text{Ind}_{\Phi}^H \eta) = \tau_{\Phi}(\mathfrak{x}\eta) \tau_{\Delta}(\mu)$$

and by Frobenius reciprocity and Proposition 3.6

$$y_{\Delta}(\mathfrak{x} \cdot \text{Ind}_{\Phi}^H \eta) = y_{\Phi}(\mathfrak{x}\eta)$$

while $y_{\Delta}(\mu) = 1$, since μ is non-ramified of order 2. Next we observe that

$$\det(\mathfrak{x} \cdot \text{Ind}_{\Phi}^H \eta) = \det(\text{Ind}_{\Phi}^{\Delta} \mathfrak{x}\eta) = v_{\Phi}^{\Delta}(\mathfrak{x}\eta) \cdot \mu,$$

then, piecing the above work together, we have

$$\tau_{\Delta}^*(\mathfrak{x} \cdot \text{Ind}_{\Phi}^H \eta) = \tau_{\Phi}^*(\mathfrak{x}\eta) \cdot \tau_{\Delta}^*(\mu) = -\tau_{\Phi}^*(\mathfrak{x}\eta).$$

Moreover, we know that

$$(9.8) \quad \tau_{\Phi}^*(\mathfrak{x} \cdot \eta) = \sum_u \mathfrak{x}\eta(u) \psi_{\Phi}(uc^{-1}).$$

Here u is summed over a set of representatives of the integers of the fixed field of Φ' , J say, modulo the maximal ideal $\mathfrak{p}_J$ of $\mathfrak{O}_J$, and ψ_Φ is the canonical additive character associated to this field. Let k_J (resp. k_G) be the residue class field of $\mathfrak{O}_J$ (resp. $\mathfrak{O}_G$). We recall that as χ is of semi-dihedral type $|k_G| \equiv -1 + 2^{r-1} \pmod{2^r}$ with $r \geq 3$. Thus $k_J = k_G(\delta)$ where δ is a square root of -1 . In the sequel it will be convenient to view the abelian characters $\mathfrak{x}\eta|_{I'}$ as characters of k_J^* .

In particular note that if $\text{order}(\eta|_{I'}) < 2^r$, then $\varepsilon_C \eta|_{I'}$ viewed as a residue class character and restricted to k_G^* is trivial (i.e. $v_\Phi^A \varepsilon_C \eta$ is unramified). For brevity we put $\mathfrak{x}_1 = \mathfrak{x}\varepsilon_\Phi$, $\mathfrak{x}_2 = \mathfrak{x}\varepsilon_H$.

Let X be the set $\{1 + b\delta\}$, for all $b \in k_G$. By (9.8), because $k_J^* = k_G^* \cdot X \cup k_G^* \cdot \delta$,

$$(9.9) \quad \tau_\Phi^*(\mathfrak{x}\eta) = \left(\sum_a \mathfrak{x}\eta(a) \psi_G(2ac^{-1}) \right) \left(\sum_{x \in X} \mathfrak{x}\eta(x) + \sum_a \mathfrak{x}\eta(a\delta) \right)$$

where a is summed over the elements of k_G^* .

Lemma 9.10. (i) $2^{1-r} \cdot \text{Tr}_{E/L}(\tau_\Phi^*(\mathfrak{x}\alpha)) \equiv \tau_A^*(\mathfrak{x} \cdot v_\Phi^H \alpha)^F \left(\sum_{x' \in X'} \mathfrak{x}_1(x') \right) \pmod{4}$ where x' is summed over the sub-set X' of X made up of those elements of X which are 2^{r-1} -powers in k_J^* .

$$(ii) \quad \sum_\phi \tau_\Phi^*(\mathfrak{x}\phi) = \tau_A^*(\mathfrak{x}_2)^F \left(\sum_{x' \in X'} \mathfrak{x}_1(x') \right) \cdot 2^{r-1}$$

where, as previous, ϕ is summed over the abelian characters of I/I_{r-1} extended to Φ .

Proof. If ζ is a 2^r -th root of unity of order > 2 , then $\text{Tr}_{E/L}(\zeta) = 0$, while of course $2^{1-r} \text{Tr}_{E/L}(\pm 1) = \pm 1$. Now we observe that $(v_\Phi^H \alpha)|_I$ is of order 2 and so, by Proposition 3.10(iv), $\tau_A^*(\mathfrak{x} \cdot v_\Phi^H \alpha) \in L$. Thus, on putting $\eta = \alpha$ in (9.9) and applying $2^{1-r} \text{Tr}_{E/L}$, we see that the lefthand side of part (i) of the lemma is equal to

$$\tau_A^*(\mathfrak{x} v_\Phi^H \alpha)^F \left(\sum_{x' \in X'} \mathfrak{x}\alpha(x') \right).$$

However, if $x' \in X'$ is a 2^{r-1} -st power but not a 2^r -th power in k_J^* , then x'^f is distinct from x' and $\mathfrak{x}\alpha(x'^f) = \mathfrak{x}\alpha(x')$ (Here f is the Frobenius of k_J/k_G). Thus

$$\sum_{x'} \mathfrak{x}\alpha(x') \equiv \sum_{x'} \mathfrak{x}_1(x') \pmod{4}.$$

Now we consider (9.9) when η is some ϕ . As was explained prior to (9.9), the $v_\Phi^A(\varepsilon_C \phi)$ are all non-ramified, so that

$$\tau_\Phi^*(\mathfrak{x}\phi) = \tau_A^*(\mathfrak{x}_2)^F \left(\sum_{x \in X} \mathfrak{x}\phi(x) \right) + \left(\sum_a \mathfrak{x}_1(a) \right) \mathfrak{x}\phi(\delta).$$

We now sum this equation over ϕ . By a standard orthogonality result for abelian characters

$$\sum_\phi \sum_{x \in X} \mathfrak{x}\phi(x) = 2^{r-1} \cdot \sum_{x' \in X'} \mathfrak{x}\phi(x')$$

and similarly, as δ is not a 2^{r-1} -st power in k_J , $\sum_\phi \mathfrak{x}\phi(\delta) = 0$. The lemma is now shown.

We now prove IVa. By the work prior to (9.8), on putting $\eta = \alpha$,

$$2^{1-r} Tr_{E/L}(\tau_{\mathcal{A}}^*(\mathfrak{x} \cdot \text{Ind}_{\Phi}^H \alpha)) = -2^{1-r} Tr_{E/L}(\tau_{\Phi}^*(\mathfrak{x} \alpha))$$

which by part (i) of the above lemma

$$\equiv -\tau_{\mathcal{A}}^*(\mathfrak{x} \cdot v_{\Phi}^H \alpha)^F \left(\sum_{x'} \mathfrak{x}_1(x') \right) \text{mod}(4).$$

Thus the lefthand side in the statement of IVa, Y say, satisfies the congruence mod(4)

$$Y \equiv -\tau_{\mathcal{A}}^*(\mathfrak{x} \det_{\chi})^F - \tau_{\mathcal{A}}^*(\mathfrak{x} v_{\Phi}^H \alpha) \left(\sum_{x'} \mathfrak{x}_1(x') \right).$$

However, $\det_{\chi} = v_{\Phi}^H \alpha \cdot \mu$ with μ non-ramified. So, by Proposition 3.10(iii)

$$\tau_{\mathcal{A}}^*(\mathfrak{x} \cdot \det_{\chi}) = \tau_{\mathcal{A}}^*(\mathfrak{x} \cdot v_{\Phi}^H \alpha)$$

and hence

$$Y \equiv -\tau_{\mathcal{A}}^*(\mathfrak{x} \cdot \det_{\chi})^F (1 + \sum \mathfrak{x}_1(x')) \text{mod}(4).$$

Now we consider the righthand side in the statement of IVa (which we denote by Z). Again, by the work prior to (9.8)

$$\sum_{\phi} \tau_{\mathcal{A}}^*(\mathfrak{x} \cdot \phi_{*}) 2^{1-r} = -\sum_{\phi} \tau_{\Phi}^*(\mathfrak{x} \phi) \cdot 2^{1-r}.$$

So, by part (ii) of Lemma 9.10

$$Z = -\tau_{\mathcal{A}}^*(\mathfrak{x}_2)^F \left(\sum_{x'} \mathfrak{x}_1(x') \right) - \tau_{\mathcal{A}}^*(\mathfrak{x} \cdot \det_{e_*})^F,$$

thus as $\det_{e_*}$ is non-ramified

$$= -\tau_{\mathcal{A}}^*(\mathfrak{x}_2)^F (1 + \sum_{x'} \mathfrak{x}_1(x')).$$

Hence, in order to show $Y \equiv Z \text{mod}(4)$, it is enough to show

$$(9.11) \quad 1 \equiv \sum_{x'} \mathfrak{x}_1(x') \text{mod}(2),$$

$$(9.12) \quad \tau_{\mathcal{A}}^*(\mathfrak{x}_2) \equiv \tau_{\mathcal{A}}^*(\mathfrak{x} \cdot \det_{\chi}) \text{mod}(2).$$

Now (9.12) is an immediate consequence of the fact that $\det_{\chi}|_I$ is of order 2. While (9.11) follows from the fact that X' breaks up into $\{1\}$ and orbits of order 2 under the Frobenius f , together with the observation that $\mathfrak{x}_1(x'^f) = \mathfrak{x}_1(x')$.

10. Determinantal Congruences

In this section we prove Ib, IIb, IIIb and IVb of Theorem 4. First we show:

Lemma 10.1. *Let $\{X_i\}_{i \in \mathfrak{J}}$ be algebraically independent (commuting) indeterminates for some finite index set $\mathfrak{J}$, and let $\{\zeta_i\}$ be l -th roots of unity. Then for*

some $f \in \mathbb{Z}[\dots X_i \dots]$,

$$\prod_{j=1}^l (\Sigma X_i \zeta_i^j) = \Sigma X_i^l + lf.$$

Proof. It is immediate that the left hand side is congruent to ΣX_i^l modulo $(1 - \zeta_l)\mathbb{Z}[\zeta_l, \dots X_i \dots]$ (where ζ_l is a primitive l -th root of unity). However, by Galois theory, the left hand side belongs to $\mathbb{Z}[\dots X_i \dots]$, and thus the congruence holds mod $l\mathbb{Z}[\dots X_i \dots]$, as required.

Proof of Ib. Let $I = \langle \sigma \rangle$ and let $x \in \mathfrak{B}I^*$. We are required to show

$$\text{Det}(x)(\chi) \cdot \text{Det}(x)(\chi')^{-F} \equiv 1 \pmod{2^{\varrho_2}} \quad \begin{array}{ll} \text{if } l \neq 2, \\ \text{if } l = 2. \end{array}$$

So, by Mackey's restriction formula, this is equivalent to showing

$$(10.2) \quad \prod_{\gamma \in H/\Psi} [(\prod_{\delta \in \Psi/\Phi} \alpha^{\delta\gamma}(x)) v \alpha^{\gamma}(x)^{-F}] \equiv 1 \pmod{2^{\varrho_2}}.$$

First we consider the product $\prod_{\delta} \alpha^{\delta}(x)$. Suppose $x = \sum_{i=1}^{|I|} x_i \sigma^i$, with $x_i \in \mathfrak{B}$. In the above lemma we put $X_i = x_i \alpha(\sigma^i)$ and for a chosen $\delta \in \Psi \setminus \Phi$, $\zeta_i = \alpha(\sigma^{-i}) \alpha^{\delta}(\sigma^i)$. Then, with the notation of the proof of Ia, we have

$$\begin{aligned} \zeta_i^j &= (\alpha(\sigma^{-1}) \alpha^{\delta}(\sigma))^{ij} = \alpha(\sigma)^{(u-1)ij} \\ &= \alpha(\sigma)^{(u^j-1)i} = \alpha(\sigma^{-i}) \alpha^{\delta^j}(\sigma^i) \end{aligned}$$

and whence $X_i \zeta_i^j \mapsto x_i \alpha^{\delta^j}(\sigma^i)$. Thus we obtain

$$\sum_{j=1}^l \alpha^{\delta^j}(x) \equiv \Sigma x_i^l \alpha^l(\sigma^i) \pmod{l}$$

and so by (9.2)

$$(10.3) \quad \equiv v \alpha(x)^F \pmod{l}.$$

Next we observe that H/Φ acts faithfully via conjugation on $\alpha(I)$ and whence identifies as a sub-group of $\text{Gal}(L(\alpha|_I)/L)$. (Note the fact that H/Φ acts faithfully on $\alpha(I)$ is a consequence of Mackey's Irreducibility Criterion). Similarly, H/Φ maps into $\text{Gal}(L(v\alpha|_I)/L)$, and, because

$$v\alpha(\sigma) = \alpha(\sigma^N)$$

for $N = \sum_{j=1}^l u^j$, we deduce that the diagram below commutes:

$$\begin{array}{ccc} H/\Phi & \xhookrightarrow{\rho} & \text{Gal}(L(\alpha|_I)/L) \\ \parallel & & \downarrow \\ H/\Phi & \xrightarrow{v\rho} & \text{Gal}(L(v\alpha|_I)/L). \end{array}$$

(Here the right and vertical arrow is restriction of automorphism). So by (10.3)

$$\prod_{\gamma \in H/\Psi} \left(\left[\prod_{j=1}^l \alpha^{\delta_j}(x) \right] v \alpha(x)^{-F} \right)^{\rho(\gamma)} = \prod_{\gamma \in H/\Psi} (1 + l\beta)^{\rho(\gamma)}$$

for some integer β of $L(\alpha|_I) \otimes \mathbb{Q}_l$. This then gives the result if l is odd.

If $l=2$, since $L(\alpha|_I)/L$ is totally ramified, $\beta^{\rho(\gamma)} \equiv \beta \pmod{\mathfrak{Q}_2}$ and thus, as $(H:\Psi)$ is even, we obtain (10.2) in this case as well.

Proof of IIb. Let $\psi^2: \mathfrak{B}I \rightarrow \mathfrak{B}I$ be the $\mathfrak{B}$ -linear ring homomorphism induced by $\sigma^i \rightarrow \sigma^{2i}$. Since $(I:I \cap \Psi) = (H:\Psi) = 2$, we can choose $\{1, \sigma\}$ as a transversal of H/Ψ and so, for any abelian character β of Ψ

$$(10.4) \quad v_{\Psi}^H \beta(\sigma) = \beta(\sigma^2).$$

Also, by Mackey restriction,

$$(\text{Ind}_{\Psi}^H \beta)|_I = \text{Ind}_{\Psi \cap I}^I (\beta|_{\Psi \cap I}) = \beta' + \beta' \mu$$

where μ is the non-trivial abelian character of I of order 2 and β' is an extension of $\beta|_{\Psi \cap I}$ to I .

As previous we take $x = \sum x_i \sigma^i \in \mathfrak{B}I^*$ and we apply Lemma 10.1 making the substitutions $X_i \mapsto x_i \sigma^i$, $\zeta_i = (-1)^i$. So we obtain

$$\text{Det}(x)(\text{Ind}_{\Psi}^H \beta) = \beta'(x) \cdot \beta' \mu(x) = (\sum x_i \beta'(\sigma^i)) (\sum x_i \beta'(\sigma^i) (-1)^i)$$

by the lemma

$$= \sum x_i^2 \beta'(\sigma^{2i}) + 2\beta' f(\dots x_i \sigma^i \dots).$$

So by (10.4) we now have

$$\frac{\text{Det}(x)(\text{Ind}_{\Psi}^H \beta)}{\text{Det}(x)(v_{\Psi}^H \beta)^F} = 1 + 2\beta' \left[\frac{f(\dots x_i \sigma^i \dots) + \sum \frac{1}{2}(x_i^2 - x_i^F) \sigma^{2i}}{\psi^2(x)^F} \right]$$

and furthermore as $x \in \mathfrak{B}I^*$, $\psi^2(x)^F \in \mathfrak{B}I^*$. To obtain IIb we first put $\beta = \lambda$ and then $\beta = \lambda^2$. The result is then a consequence of the congruence $\lambda \equiv \lambda^2 \pmod{\mathfrak{Q}_2}$.

Proof of IIIb. We keep the notation of the proof of IIIa. By (9.6)

$$\text{Det}(x)(\tilde{\chi} + \tilde{\chi}^{\omega}) = \text{Det}(x)(\theta)$$

which by Mackey restriction

$$= \text{Det}(x) \left(\sum_{\gamma \in H/\Phi} \tilde{\alpha}^{\gamma}|_I + \tilde{\alpha}^{\gamma} \mu|_I \right).$$

So we are required to show

$$(10.5) \quad \prod_{\gamma \in H/\Phi} (\tilde{\alpha}^{\gamma}(x) \cdot \tilde{\alpha}^{\gamma} \mu(x) \cdot \alpha^{\gamma}(x)^{-F}) \equiv 1 \pmod{2\mathfrak{Q}_2}.$$

Recall μ is a ramified quadratic abelian character of Δ and that $\tilde{\alpha}$ has the property

$$(10.6) \quad \tilde{\alpha}^2|_I = \alpha|_I.$$

Now we apply Lemma 10.1, making the substitution $X_i \mapsto x_i \sigma^i$, $\zeta_i = (-1)^i$. Then, as in the proof of IIb, we obtain

$$\tilde{\alpha}^\gamma(x) \tilde{\alpha}^\gamma \mu(x) = \sum x_i^2 \tilde{\alpha}^\gamma(\sigma^{2i}) + 2\tilde{\alpha}^\gamma(f(\dots x_i \sigma^i \dots))$$

and so by (10.6)

$$\frac{\tilde{\alpha}^\gamma(x) \cdot \tilde{\alpha}^\gamma \mu(x)}{\alpha^\gamma(x)^F} = 1 + 2\tilde{\alpha}^\gamma \left[\frac{f(\dots x_i \sigma^i \dots) + \sum \frac{1}{2}(x_i^2 - x_i^F) \sigma^{2i}}{\psi^2(x)^F} \right]$$

(10.5) is then a consequence of the congruence $\tilde{\alpha} \equiv \tilde{\alpha}^\gamma \pmod{\Omega_2}$.

Proof of IVb. For ease of notation we suppose that $\alpha|_I$ is faithful on I . (We can assume this by passing to the quotient group $H/\text{Ker}(\alpha|_I)$). As previous let $x = \sum x_i \sigma^i \in \mathfrak{B}I^*$. To prove IVb we shall show

$$(10.7) \quad 2^{1-r} \text{Tr}_{E/L}(\text{Det}(x)(\chi)) \\ = \sum x_i^2 (-1)^i + \sum_{\substack{i \equiv j \pmod{2^{r-1}} \\ i > j}} 2x_i x_j (-1)^{(i-j)2^{1-r}+j},$$

$$(10.8) \quad 2^{1-r} \sum_{\phi} \text{Det}(x)(\phi_*) = \sum x_i^2 + \sum_{\substack{i \equiv j \pmod{2^{r-1}} \\ i > j}} 2x_i x_j.$$

First we show that (10.7) and (10.8) together imply IVb, then we give their proof.

It is readily calculated that

$$\det_{\chi}(\sigma) = -1 \quad \det_{e_*}(\sigma) = 1$$

and thus

$$\text{Det}(x)(\det_{\chi})^F = \sum x_i^F (-1)^i,$$

$$\text{Det}(x)(\det_{e_*})^F = \sum x_i^F.$$

IVb is then an immediate consequence of the congruences

$$\pm 2x_i x_j \equiv 2x_i x_j \pmod{4},$$

$$\pm (x_i^2 - x_i^F) \equiv (x_i^2 - x_i^F) \pmod{4}.$$

Suppose now that β is any abelian character of Φ . Then, by Mackey restriction, $\text{Det}(x)(\text{Ind}_{\Phi}^H \beta) = \beta(x) \beta(x^\xi)$, where $\xi \in H \setminus \Phi$. However,

$$(10.9) \quad x x^\xi = \sum x_i^2 \sigma^{(1+\xi)i} + \sum_{i \neq j} x_i x_j \sigma^{i+j\xi}.$$

Note that if $2^{r-1} \nmid i$, then $\text{Tr}_{E/L}(\alpha(\sigma^i)) = 0$, whilst if $2^{r-1} | i$, $\text{Tr}_{E/L}(\alpha(\sigma^i)) = 2^{r-1} \alpha(\sigma^i)$.

Now, because χ is of semi-dihedral type with $\alpha|_I$ faithful, we know $\sigma^\xi = \sigma^{-1+2^{r-1}}$. Thus, when we apply α to (10.9) and follow this by $Tr_{E/L}$, the only cross terms which give a non-zero contribution are those pairs (i, j) with $i \equiv j \pmod{2^{r-1}}$, and furthermore the sign of this term is $(-1)^{(i-j)2^{1-r}+j}$.

Now as $i \equiv j \pmod{2^{r-1}}$, we deduce that

$$(i-j)2^{1-r}+j \equiv (j-i)2^{1-r}+i \pmod{2}$$

and so the sign of the (i, j) and (j, i) terms are the same. (10.7) is now shown.

(10.8) follows immediately from (10.9) and the standard orthogonality result

$$\sum_{\phi} \phi(\sigma^i) = \begin{cases} 0 & \text{if } 2^{r-1} \nmid i, \\ 2^{r-1} & \text{if } 2^{r-1} \mid i. \end{cases}$$

11. Proof of Theorem 2(a)

Let E denote the compositum of the normal closure of $M/\mathbb{Q}$ with the cyclotomic field $\mathbb{Q}(|I|)$ and let $A = \text{Gal}(E/\mathbb{Q})$, $\Theta = \text{Gal}(E/N)$.

Let A and a be as given in (2.2). We define the homomorphism $y_p: R_r \rightarrow \mu$ for each prime p of N above l as follows. Let Δ be a decomposition group of p in M/N ; then, with the notation of (3.9), we put

$$y_p = \text{Ind}_\Delta^F(y_\Delta^{-1} \text{Det}(\delta_c)).$$

Here, as always, induction of homomorphism corresponds to composition with restriction. Then, exactly as in the proof in §3 that Theorem 3 implies Theorem 2(b), we see that y_p is an $\Omega_{\mathbb{Q}}^+$ homomorphism.

Now we write $\tau_{F,p}^*$ for $\text{Ind}_\Delta^F(\tau_\Delta^*)$, where τ_Δ^* is the adjusted Galois Gauss sum at p defined in (3.9). We choose an extension $\bar{E}$ of $\mathbb{Q}_l$ and a dense embedding $h: E \rightarrow \bar{E}$. We shall write h exponentially. Let $\bar{\mathfrak{Q}}$ be the maximal ideal of the ring of integers $\bar{E}$ and let $\mathfrak{Q}$ be the inverse image of h on $\bar{\mathfrak{Q}}$. We say that $\mathfrak{Q}$ is the prime associated to h . Multiplication on the left (resp. right) gives the usual action of A (resp. $\text{Gal}(\bar{E}/\mathbb{Q}_l)$) on embeddings of E into $\bar{E}$.

We denote the maximal tame extension of $\mathbb{Q}_l$ in $\bar{E}$ by T and we put $D = \text{Gal}(\bar{E}/\mathbb{Q}_l)$, $P = \text{Gal}(\bar{E}/T)$.

In order to establish Theorem 2(a) we will show

$$(11.1) \quad (\text{Det}(A) \prod_{p|l} \tau_{F,p}^*)^h \in \text{Det}(\mathfrak{S}_T \Gamma^*).$$

Next we recall Fröhlich's norm operator (cf. [F1] Appendix VI for more details). Let $\bar{E} \supset G \supset L$. Then we have the homomorphism

$$\mathcal{N}_{G/L}: \text{Det}(\mathfrak{S}_G \Gamma^*) \rightarrow \text{Det}(\mathfrak{S}_L \Gamma^*)$$

given by

$$\mathcal{N}_{G/L}(\text{Det}(x)) = \prod_{\sigma} \text{Det}(x^{\sigma})$$

where σ runs through a transversal of $\text{Gal}(\bar{E}/G) \setminus \text{Gal}(\bar{E}/L)$. Equivalently, for $\chi \in R_\Gamma$, we see that $\mathcal{N}_{G/L}$ corresponds to the usual trace or co-transfer map

$$\mathcal{N}_{G/L} \text{Det}(x)(\chi^h) = \prod_{\sigma} \text{Det}(x)(\chi^{h\sigma^{-1}})^{\sigma}.$$

Let $\bar{E} \supset M' \supset N'$ and let M'/N' be tame. Then, because P is normal in D , we can find a transversal of $\text{Gal}(\bar{E}/N') \setminus D$ of the form $\{\pi_{i,j} \omega_j\}$, where for each j $\{\pi_{i,j}\}$ is a transversal of $\text{Gal}(\bar{E}/M') \cap P \setminus P$. We call such a transversal a distinguished transversal of $N'/\mathbb{Q}_l$ with respect to M' . The vital property of such transversals is that for $x \in \mathfrak{S}_{M'} \Gamma^*$, then $\prod_i \text{Det}(x^{\pi_{i,j}})$ lies in the image of the norm operator from $\text{Det}(\mathfrak{S}_{M'} \Gamma^*)$ to $\text{Det}(\mathfrak{S}_{M'}^P \Gamma^*)$, and so

$$(11.2) \quad \prod_{i,j} \text{Det}(x^{\pi_{i,j} \omega_j}) \in \text{Det}(\mathfrak{S}_T \Gamma^*).$$

Now let $\{\sigma\}$ be the right transversal of $\Theta \setminus A$ given in (2.2). Then, by associating to σ the prime of N below that of σh , we can split up the transversal into equivalence classes $C(\mathfrak{p})$ for each prime $\mathfrak{p}$ of N above l . Thus the $(\sigma h)|_N$ for $\sigma \in C(\mathfrak{p})$ are the distinct embeddings of N into $\bar{E}$ associated to the prime $\mathfrak{p}$.

Now we choose a prime $\mathfrak{p}$ of N above l and we fix a $\sigma_0 \in C(\mathfrak{p})$. We write M' , N' for the closure of $M^{\sigma_0 h}$, $N^{\sigma_0 h}$ in $\bar{E}$. Then the $\{(\sigma h)|_N\}$ for $\sigma \in C(\mathfrak{p})$ are the same as $\{(\sigma_0 h \delta|_N)\}$ where δ runs through a right transversal of $\text{Gal}(\bar{E}/N') \setminus D$. Consequently, by multiplying the σ on the left by elements of Θ , we can assume that the sets of embeddings $\{\sigma h\}$ and $\{\sigma_0 h \delta\}$ coincide with $\{\delta\}$ a distinguished transversal of $N'/\mathbb{Q}_l$ with respect to M' . By abuse of notation we say that the partial transversal $C(\mathfrak{p})$ is distinguished at $\mathfrak{p}$. So now we assume our transversal of $\Theta \setminus A$ to be so that $C(\mathfrak{p})$ is distinguished at $\mathfrak{p}$ for all $\mathfrak{p}$ above l . Thus, to sum up, for our chosen h , in general we alter A as given in (2.2), since we change the transversal of $\Theta \setminus A$. However, such a change in transversal alters $\text{Det}(A)$ only by some $\text{Det}(\gamma)$ for $\gamma \in \Gamma$ (cf. Proposition 1.5 of [F1]), and so indeed it will be sufficient to prove (11.1) with this altered transversal (which we still denote by $\{\sigma\}$). In fact we prove the stronger result that for each $\mathfrak{p}$

$$(11.3) \quad (\text{Det}(\prod_{\sigma \in C(\mathfrak{p})} (\Sigma a^{\gamma \sigma} \gamma^{-1})) \cdot \tau_{T,\mathfrak{p}}^{*-1})^h \in \text{Det}(\mathfrak{S}_T \Gamma^*).$$

From now on we fix $\mathfrak{p}$. Let I be the inertia group of $\mathfrak{p}$ in M/N and let $b \in M$ give a normal integral basis of M over M^I at $\mathfrak{p}$. By Theorem 6, §4 [F1], we know that for some $B_1 \in \mathfrak{S}_{M^I} \Gamma^*$

$$(11.4) \quad \Sigma a^{\gamma \sigma_0 h} \gamma^{-1} = (\Sigma_{\alpha \in I} b^{\alpha \sigma_0 h} \alpha^{-1}) \cdot B_1.$$

Now we put

$$A_{\mathfrak{p}} = \prod_{\sigma \in C(\mathfrak{p})} (\Sigma a^{\gamma \sigma h} \gamma^{-1}) \quad \text{and} \quad C = \prod_{\sigma \in C(\mathfrak{p})} (\Sigma b^{\alpha \sigma h} \alpha^{-1}).$$

Then, by (11.2), because the $\sigma \in C(\mathfrak{p})$ form a distinguished partial transversal,

$$\text{Det}(C) \in \text{Det}(\mathfrak{D}_T I) \cap \text{Det}(T I^*) \quad \text{and} \quad \text{Det}(A_{\mathfrak{p}}) = \text{Det}(C) \text{Det}(B)$$

for some $B \in \mathfrak{D}_T I^*$.

(11.5) Next we put $t = \tau_{\Delta}^{*h}$ (with τ_{Δ}^* as given previously in this section). By Theorem 4 in [FT] we know that $\text{Det}(C)t^{-1}$ takes unit values on R_{Δ} . So, in order to prove (11.3), we show

Proposition 11.6. $\text{Det}(C)t^{-1} \in \text{Ind}_I^{\Delta}(\text{Det}(\mathfrak{D}_T I^*)).$

Proof. Let $e = |I|$. By construction E , and whence also T , contains both the e and l -th roots of unity. By tameness we know $(e, l) = 1$, and so the map $z \mapsto \prod_{\phi} \text{Det}(z)(\phi^h)$ induces an isomorphism of rings

$$(11.7) \quad \mathfrak{D}_T I \xrightarrow{\sim} \prod_{\phi} \mathfrak{D}_T$$

where the direct product extends over the distinct abelian characters $\phi: I \rightarrow E^*$.

Let $m|e$ and put $\mathfrak{D}_m = \prod'_{\phi} \mathfrak{D}_T$ where now the direct product runs over those ϕ of order m . By tameness I is cyclic and so conjugation by Δ induces an action on I and whence on $\phi(I)$. So, if ϕ has order m , we obtain a homomorphism from Δ to $\text{Aut}(\phi(I))$. We denote the kernel (resp. the image) by H_m (resp. Σ_m).

Let χ be an irreducible character of Δ . Then, as Δ is metacyclic, we can write $\chi = \text{Ind}_{H_m}^{\Delta} \check{\phi}$ for some abelian character $\check{\phi}$ with $\check{\phi}|_I$ of order m . Conversely, by extending a given ϕ of order m to H_m and inducing to Δ , we obtain an irreducible character χ of Δ , and χ is unique up to a multiple of a non-ramified abelian character of Δ . Thus, by Proposition 3.10(iii), $t(\chi^h)^{-1} \text{Det}(C)(\chi^h)$ is a function of ϕ alone. By Proposition 3.10(iv) it takes values in T and by (11.5) it is unit valued. Thus we have constructed a homomorphism $X: R_I \rightarrow \mathfrak{D}_T^*$ given by

$$(11.8) \quad X(\phi^h) = t(\chi^h)^{-1} \text{Det}(C)(\chi^h).$$

Moreover for $\delta \in \Delta$ clearly $\check{\phi}^{\delta}$ and $\check{\phi}$ induce to the same character of Δ , and so we see that X , when restricted to abelian characters of order m , is Σ_m fixed. Consequently, because the isomorphism (11.7) is completely split, we can find $z_m \in \mathfrak{D}_m^*$ so that

$$(11.9) \quad \prod_{\beta \in \Sigma_m} z_m(\phi^{\beta h}) = X(\phi^h)$$

for all abelian characters ϕ of order m . Let $z \in \mathfrak{D}_T I^*$ map to $\prod_m z_m$ under (11.7).

We assert that on R_{Δ} , $t^{-1} \text{Det}(C) = \text{Det}(z)$. By $\mathbb{Z}$ -linearity it is sufficient to show that, with the above notation, for each irreducible character χ of $\Delta (= \text{Ind}_{H_m}^{\Delta} \check{\phi})$, as above say),

$$(11.10) \quad t^{-1}(\chi^h) \text{Det}(C)(\chi^h) = \text{Det}(z)(\chi^h).$$

By Mackey restriction

$$\begin{aligned}\mathrm{Det}(z)(\chi^h) &= \mathrm{Det}(z)(\chi^h|_I) \\ &= \prod_{\delta \in H_m \setminus \Delta} z(\phi^{\delta h}) = \prod_{\beta \in \Sigma_m} z(\phi^{\beta h})\end{aligned}$$

which by (11.9) is $X(\phi^h)$, and so by (11.8) the result is shown.

12. Fixed Point Theorem

In this section we prove:

Theorem 6. *Let l divide $|\Gamma|$ and let $L/\mathbb{Q}_l$ be a tame, finite Galois extension. We put $\Delta = \mathrm{Gal}(L/\mathbb{Q}_l)$ and we view $\mathrm{Det}(\mathfrak{D}_L \Gamma^*)$ as a Δ -module by the rule $\mathrm{Det}(z) \cdot \delta = \mathrm{Det}(z^\delta)$ for $z \in \mathfrak{D}_L \Gamma^*$, $\delta \in \Delta$.*

Then

$$(12.1) \quad \mathrm{Det}(\mathfrak{D}_L \Gamma^*)^\Delta = \mathrm{Det}(\mathfrak{D}_L^\Delta \Gamma^*),$$

where the superscript Δ denotes points fixed by Δ .

Proof. Let I denote the inertia group of Δ . As a first step towards proving (12.1) we will show

$$(12.2) \quad \mathrm{Det}(\mathfrak{D}_L \Gamma^*)^I = \mathrm{Det}(\mathfrak{D}_L^I \Gamma^*).$$

Because $\mathfrak{D}_L^I$ maps onto $\mathfrak{D}_L$ modulo the maximal ideal $\mathfrak{l}$ of $\mathfrak{D}_L$, we see that

$$\mathrm{Det}(\mathfrak{D}_L \Gamma^*) = \mathrm{Det}(\mathfrak{D}_L^I \Gamma^*) \mathrm{Det}(1 + \mathfrak{l} \mathfrak{D}_L \Gamma).$$

So, on taking fixed points

$$(12.3) \quad \mathrm{Det}(\mathfrak{D}_L \Gamma^*)^I = \mathrm{Det}(\mathfrak{D}_L^I \Gamma^*) \mathrm{Det}(1 + \mathfrak{l} \mathfrak{D}_L \Gamma)^I.$$

Now, as in the previous section, we have Fröhlich's norm operator

$$\mathcal{N}_I: \mathrm{Det}(\mathfrak{D}_L \Gamma^*) \rightarrow \mathrm{Det}(\mathfrak{D}_L^I \Gamma^*)$$

given by $\mathcal{N}_I(\mathrm{Det}(x)) = \prod_{\sigma \in I} \mathrm{Det}(x^\sigma)$. Thus, if $\mathrm{Det}(x)$ is I -fixed, then the norm of $\mathrm{Det}(x)$ is $\mathrm{Det}(x)^{|I|}$. Moreover, as $\mathrm{Det}(1 + \mathfrak{l} \mathfrak{D}_L \Gamma)$ is a pro- l -group and because $(|I|, l) = 1$ we see that the norm is just an automorphism on $\mathrm{Det}(1 + \mathfrak{l} \mathfrak{D}_L \Gamma)^I$. This shows

$$\mathrm{Det}(1 + \mathfrak{l} \mathfrak{D}_L \Gamma)^I \subseteq \mathrm{Det}(\mathfrak{D}_L^I \Gamma^*)$$

and this, together with (12.3), gives (12.2).

Finally, to show (12.1) we must now show

$$\mathrm{Det}(\mathfrak{D}_L^I \Gamma^*)^{\Delta/I} = \mathrm{Det}(\mathfrak{D}_L^\Delta \Gamma^*)$$

and this is Theorem 1.1 of [T1].

Appendix of Certain Notation Introduced

Γ -global Galois group upto §3; thereafter a local Galois group. From §3 to §10 $\mathfrak{p}$ is fixed prime ideal, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, and l is a fixed prime different from p .

$K = \mathbb{Q}(p)$ (the p -th cyclotomic field).

$\mathfrak{A} = \mathfrak{O}_K \otimes \mathbb{Z}_l$.

From §7 to §10 χ is a chosen abelian character of $C(\subset \Gamma)$ with order n , $L = K(\chi)$, $\mathfrak{B} = \mathfrak{O}_L \otimes \mathbb{Z}_l$.

F is the Frobenius of l in $L(|H|)/\mathbb{Q}(|H|)$

$\tau, \tau^*, y, \text{Ker}(d_l)$ are defined in §3.

$v_H, \phi_H, \mathfrak{C}_H, r_H, \mathfrak{T}$ are defined in §4.

$H, I, \mathfrak{D}_I, \tilde{\tau}$ are defined in §7.

References

- [C] Cassou-Noguès, Ph.: Quelques théorèmes de base normale d'entiers, *Ann. Inst. Fourier*, **28**, 1–33 (1978)
- [DH] Davenport, H., Hasse, H.: Die Nullstellen der Kongruenzetafunktionen in gewissen zyklischen Fällen. *J. reine und angew. Math.* **172**, 151–182 (1935)
- [D] Deligne, P.: Les constantes des équations fonctionnelles des fonctions L , *Modular Forms in one variable*, *Lecture Notes in Mathematics* **349**, 501–597 (1973)
- [F1] Fröhlich, A.: Arithmetic and Galois module structure for tame extensions, *J. reine angew. Math.* **286**, 380–440 (1976)
- [F2] Fröhlich, A.: Resolvents and trace form, *Proc. Camb. Phil. Soc.* **78**, 185–210 (1975)
- [F3] Fröhlich, A.: Locally free modules over arithmetic orders, *J. reine angew. Math.* **274**, 112–124 (1975)
- [F4] Fröhlich, A.: Classgroups, in particular Hermitian classgroups, in press (1980)
- [F5] Fröhlich, A.: Artin root numbers and normal integral bases for quaternion fields, *Invent. Math.* **17**, 143–166 (1972)
- [F6] Fröhlich, A.: Module Invariants and root numbers for quaternion fields of degree $4l'$, *Proc. Camb. Phil. Soc.* **76**, 393–399 (1974)
- [FT] Fröhlich, A., Taylor, M.J.: The arithmetic theory of local Galois Gauss sums for tame characters, *Philosophical Transactions of the Royal Society* **298**, 141–181 (1980)
- [M1] Martinet, J.: Modules sur l'algèbre du groupe quaternionien, *Ann. Sci. Ecole Norm. Sup.* **4**, 229–308 (1971)
- [M2] Martinet, J.: Character theory and Artin L -functions, *Algebraic Number Fields (Proc. Durham Symposium)*, London: Academic Press 1977
- [N] Noether, E.: Normalbasis bei Körpern ohne höhere Verzweigung, *J. reine angew. Math.* **167**, 147–152 (1932)
- [S] Serre, J.-P.: *Représentations linéaires des groupes finis*, 2nd edition. Paris: Hermann 1971
- [T1] Taylor, M.J.: A logarithmic approach to classgroups of integral group rings, *J. Algebra*, **66**, 321–353 (1980)
- [T2] Taylor, M.J.: Galois module structure of relative abelian extensions, *J. reine angew. Math.* **303**, 97–101 (1978)
- [T3] Taylor, M.J.: Adams operations, local root numbers and the Galois module structure of rings of integers, *Proc. L.M.S. (3)*, **39**, 147–175 (1979)
- [U] Ullom, S.: Character action on the classgroup of Fröhlich, informal report

