ANNALES DE L'INSTITUT FOURIER

MARTIN J. TAYLOR

Galois module structure of rings of integers

Annales de l'institut Fourier, tome 30, nº 3 (1980), p. 11-48

<http://www.numdam.org/item?id=AIF_1980__30_3_11_0>

Ann. Inst. Fourier, Grenoble
30, 3 (1980), 11-48

GALOIS MODULE STRUCTURE OF RINGS OF INTEGERS

by Martin J. TAYLOR (*)

1. Introduction.

Let E/F be a tame Galois extension of number fields with $\mathrm{Gal}(E/F) = \Gamma$. The ring of integers of E, $\mathcal{O}_E$, is a module over the integral group ring $\mathbf{Z}\Gamma$. In [11], E. Noether outlined a proof that E/F being tame implies that $\mathcal{O}_E$ is a locally free $\mathcal{O}_F\Gamma$ module. Hence $\mathcal{O}_E$ is a locally free $\mathbf{Z}\Gamma$ module with rank equal to the degree of F over the field of rationals $\mathbf{Q}$.

We let $\mathrm{Cl}(\mathbf{Z}\Gamma)$ denote the locally free classgroup of $\mathbf{Z}\Gamma$, and we denote the class of $\mathcal{O}_E$ in $\mathrm{Cl}(\mathbf{Z}\Gamma)$ by $(\mathcal{O}_E)$. In [5], A. Fröhlich made the following remarkable conjecture:

CONJECTURE. – *If* $F = \mathbf{Q}$, *then* $(\mathcal{O}_E)^2 = 1$. *He has since conjectured that* $(\mathcal{O}_E)^2 = 1$, *for arbitrary base field* F.

The main result of this paper is to show.

THEOREM 1. – *If all the prime divisors of* $[E:F]$ *are unramified in* $E/\mathbf{Q}$, *then* $(\mathcal{O}_E)^4 = 1$.

Remark 1. – The condition that the prime divisors of $[E:F]$ be unramified in $E/\mathbf{Q}$ is, of course, stronger than the condition that E/F be tame.

(*) Part of the work in this paper was done whilst I received financial support from the C.N.R.S. and the kind hospitality of the University of Besançon.

Remark 2. – There is an excellent sketch of our proof of Theorem 1 in A. Fröhlich's forthcoming book [4].

Remark 3. – J. Martinet was the first to show that there exist tame Galois extensions $E/\mathbf{Q}$ so that $(\mathcal{O}_E) \neq 1$. A. Fröhlich and Ph. Cassou-Noguès have since proved a series of results which demonstrate that the question of whether $(\mathcal{O}_E)$ is 1, or, not, is intimately related to the sign of the root numbers of irreducible symplectic characters of $\mathrm{Gal}(E/\mathbf{Q})$ (cf. [3] and [1]).

Remark 4. – In the course of the proof of Theorem 1, the local root number will be seen to play a very special role (instead of using the local Galois Gauss sum which is the usual tool). This special role of root numbers is particularly interesting and is, as yet, far from understood.

COROLLARY 1. – *Let* E/F *be as in Theorem 1, and suppose further that* $[E:F]$ *is odd, then* $\mathcal{O}_E$ *is a free* $\mathbf{Z}\Gamma$ *module of rank* $[F:\mathbf{Q}]$.

Proof. – From the corollary to Theorem 2 in [15], we know that the order of $(\mathcal{O}_E)$ divides the Artin exponent of the group Γ (cf. [15] or [8] for the definition of the Artin exponent). By 1.6 of [8], we know that the Artin exponent of Γ divides the group order $|\Gamma|$. So it is immediate from Theorem 1 that $(\mathcal{O}_E) = 1$, i.e. $\mathcal{O}_E$ is a stably free $\mathbf{Z}\Gamma$-module.

However, because $|\Gamma|$ is odd, the rational group algebra $\mathbf{Q}\Gamma$ satisfies the Eichler condition, i.e. no simple component of $\mathbf{Q}\Gamma$ is a totally definite quaternion algebra. So, by Jacobinski's Cancellation Theorem (cf. section 3 of [6] for instance), we know that $\mathbf{Z}\Gamma$ possesses the cancellation property, and thus $\mathcal{O}_E$ is a free $\mathbf{Z}\Gamma$-module.

COROLLARY 2. – *Let* $F = \mathbf{Q}$ *and suppose that the extension* E/F *is of* ℓ*-power degree, for some odd prime number* ℓ. *Then* $\mathcal{O}_E$ *is a free* $\mathbf{Z}\Gamma$*-module.*

I should like to express my warmest thanks to A.Fröhlich for numerous discussions and suggestions concerning this work.

2. Definitions and preliminary results.

Firstly, we set up our notation and recall various results on class groups. Our main source of reference is [3].

For a rational prime number ℓ, $\mathbf{Z}_\ell$ is the ring of rational ℓ-adic integers and $\mathbf{Q}_\ell$ is the rational ℓ-adic field. If ℓ is the infinite rational prime, we define $\mathbf{Z}_\ell = \mathbf{Q}_\ell = \mathbf{R}$, the field of real numbers.

For any number field M, we denote the ring of integers of M by $\mathfrak{O}_M$. It ℓ is a rational prime number, we define

$$M_\ell = M \otimes_{\mathbf{Q}} \mathbf{Q}_\ell\,, \ \mathfrak{O}_{M_\ell} = \mathfrak{O}_M \otimes_{\mathbf{Z}} \mathbf{Z}_\ell\,;$$

whilst if ℓ is the infinite rational prime, we put $\mathfrak{O}_{M_\ell} = M_\ell = M \otimes_{\mathbf{Q}} \mathbf{R}$. For a ring R, we denote the group of units by R^*.

Let $\overline{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in the field of complex numbers $\mathbf{C}$, and let μ be the group of roots of unity in $\overline{\mathbf{Q}}$. For any number field M, we define $\Omega_M = \mathrm{Gal}(\overline{\mathbf{Q}}/M)$, and

$$\overline{\mathbf{Q}}_\ell = \varinjlim_{M\subset\overline{\mathbf{Q}}} M_\ell \qquad U(\overline{\mathbf{Q}}_\ell) = \varinjlim_{M\subset\overline{\mathbf{Q}}} \mathfrak{O}^*_{M_\ell}\,.$$

Then $\Omega_{\mathbf{Q}}$ acts on $\overline{\mathbf{Q}}_\ell$ and $U(\overline{\mathbf{Q}}_\ell)$ in the natural way. Note that we can identify $\overline{\mathbf{Q}}_\ell$ with $\overline{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$.

If S is a finite set of rational primes, then we put

$$U_S(\overline{\mathbf{Q}}) = \prod_{\ell\in S} U(\overline{\mathbf{Q}}_\ell)\,.$$

We shall denote the Jacobson radical of $\mathfrak{O}_{M_\ell}$ by $\mathfrak{R}_{\ell,M}$ and we put $\mathfrak{R}_\ell = \varinjlim_{M\subset\overline{\mathbf{Q}}} \mathfrak{R}_{\ell,M}$.

J(M) (resp. U(M)) will denote the group of ideles of M (resp. group of unit ideles of M), and we put

$$J(\overline{\mathbf{Q}}) = \varinjlim_{M\subset\overline{\mathbf{Q}}} J(M) \qquad U(\overline{\mathbf{Q}}) = \varinjlim_{M\subset\overline{\mathbf{Q}}} U(M)\,.$$

For an element $x \in J(\overline{\mathbf{Q}})$, we let $(x)_\ell$ denote the image of x under the projection $J(\overline{\mathbf{Q}}) \longrightarrow \overline{\mathbf{Q}}_\ell$. If q is a positive integer then $M(q)$ denotes the number field obtained by adjoining a primitive q^{th} root of unity of M.

Let E/F be a Galois extension of number fields, let $\mathfrak{p}$ be a prime of F and let $\mathfrak{q}$ be a prime of E above $\mathfrak{p}$. We denote the decomposition group (resp. the inertia group) of $\mathfrak{q}$ in E/F by

$\Delta_{\mathfrak{q}}$ (resp. $T_{\mathfrak{q}}$). As previously, we put $\Gamma = \mathrm{Gal}(E/F)$. For each virtual character χ of Γ we have the local root number $W(\chi_{\mathfrak{p}})$ and the local Galois Gauss sum $\tau(\chi_{\mathfrak{p}})$. These two terms will be defined in section 4. However, for a more complete description see [14] and [10].

For a finite group Γ, R_Γ is the ring of virtual characters of Γ. Suppose that Δ is a sub-group of Γ. Then we have induction and restriction homomorphisms

$$\mathrm{Ind}_\Delta^\Gamma : R_\Delta \longrightarrow R_\Gamma ,$$
$$\mathrm{Res}_\Gamma^\Delta : R_\Gamma \longrightarrow R_\Delta .$$

For $\chi \in R_\Gamma$ we shall frequently write $\chi|_\Delta$ in place of $\mathrm{Res}_\Gamma^\Delta(\chi)$. We denote by $V_\Delta^\Gamma : \mathrm{Hom}_{\mathbf{Z}}(\Delta, \mu) \longrightarrow \mathrm{Hom}_{\mathbf{Z}}(\Gamma, \mu)$ the co-transfer homomorphism.

Suppose that $\pi : \Gamma \longrightarrow \Sigma$ is a surjective group homomorphism. Then composition with π yields the inflation homomorphism $\mathrm{Inf}_\Sigma^\Gamma : R_\Sigma \longrightarrow R_\Gamma$.

If $\chi \in R_\Gamma$, then $\mathbf{Q}(\chi)$ is the number field obtained by adjoining the values of χ to $\mathbf{Q}$. We let $\Omega_{\mathbf{Q}}$ acts on R_Γ in the natural way (i.e. by action on values). We define $\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, J(\mathbf{Q}))$ to be the subgroup of those $f \in \mathrm{Hom}(R_\Gamma, J(\overline{\mathbf{Q}}))$ such that $f(\chi^\omega) = f(\chi)^\omega$ for all $\omega \in \Omega_{\mathbf{Q}}$ and all $\chi \in R_\Gamma$. We let $\mathrm{Hom}_{\Omega_{\mathbf{Q}}}^+(R_\Gamma, J(\overline{\mathbf{Q}}))$ be the subgroup of such homomorphisms which take totally positive values on all symplectic characters of Γ.

Let χ be a character of Γ which is afforded by a representation $T : \Gamma \longrightarrow GL_n(\overline{\mathbf{Q}})$. We let $\det_\chi$ be the abelian character given by $\gamma \longmapsto \det(T(\gamma))$, for $\gamma \in \Gamma$. For each rational prime ℓ we extend T to a homomorphism of algebras $T : \mathbf{Q}_\ell \Gamma \longrightarrow M_n(\overline{\mathbf{Q}}_\ell)$. Then, for $\alpha \in \mathbf{Q}_\ell\Gamma^*$, we define $\mathrm{Det}(\alpha) \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, \overline{\mathbf{Q}}_\ell^*)$ to be the homomorphism given by $\mathrm{Det}(\alpha)(\chi) = \det(T(\alpha))$. (Then we extend $\mathrm{Det}(\alpha)$ to virtual characters of Γ by $\mathbf{Z}$-linearity).

We let $U(\mathbf{Z}\Gamma) = \prod_p \mathbf{Z}_p\Gamma^*$, $U_S(\mathbf{Z}\Gamma) = \prod_{p \in S} \mathbf{Z}_p\Gamma^*$. Here the first direct product is taken over all rational primes p, and the second direct product extends over all p in the finite set S. Det then extends in the natural way to homomorphisms

$$\mathrm{Det} : U(\mathbf{Z}\Gamma) \longrightarrow \mathrm{Hom}_{\Omega_{\mathbf{Q}}}^+(R_\Gamma, U(\overline{\mathbf{Q}})),$$
$$\mathrm{Det} : U_S(\mathbf{Z}\Gamma) \longrightarrow \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, U_S(\overline{\mathbf{Q}})).$$

Following Appendix I.10 of [3], we are now able to give A. Fröhlich's description of $\mathrm{Cl}(\mathbf{Z}\Gamma)$

$$\mathrm{Cl}(\mathbf{Z}\Gamma) \simeq \frac{\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathrm{J}(\overline{\mathbf{Q}}))}{\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \overline{\mathbf{Q}}^*)\,\mathrm{Det}(\mathrm{U}(\mathbf{Z}\Gamma))}\,. \tag{2.1}$$

Here we view $\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \overline{\mathbf{Q}}^*)$ as a sub-group of $\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathrm{J}(\overline{\mathbf{Q}}))$ via the diagonal embedding $\overline{\mathbf{Q}}^* \hookrightarrow \mathrm{J}(\overline{\mathbf{Q}})$. Now we consider the "kernel group" $\mathrm{D}(\mathbf{Z}\Gamma) \subset \mathrm{Cl}(\mathbf{Z}\Gamma)$, which, for our purposes, we may regard as being defined by the isomorphism

$$\mathrm{D}(\mathbf{Z}\Gamma) \simeq \frac{\mathrm{Hom}^+_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathrm{U}(\overline{\mathbf{Q}}))}{\mathrm{Hom}^+_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathcal{O}^*_{\overline{\mathbf{Q}}})\,\mathrm{Det}(\mathrm{U}(\mathbf{Z}\Gamma))} \tag{2.2}$$

where $\mathcal{O}^*_{\overline{\mathbf{Q}}} = \varinjlim_{\mathrm{M}\subset\overline{\mathbf{Q}}} \mathcal{O}^*_{\mathrm{M}}$. For a natural module theoretic interpretation of $\mathrm{D}(\mathbf{Z}\Gamma)$ see Appendix II of [3].

Let p be a finite rational prime which is co-prime to the group order $|\Gamma|$, then $\mathbf{Z}_p\Gamma$ is a maximal order, and so

$$\mathrm{Det}(\mathbf{Z}_p\Gamma^*) = \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathrm{U}(\overline{\mathbf{Q}}_p)).$$

On the other hand, if p is the infinite rational prime, it follows that by the Hasse-Schilling norm theorem

$$\mathrm{Det}(\mathbf{R}\Gamma^*) = \mathrm{Hom}^+_{\mathrm{G}(\mathbf{C}/\mathbf{R})}(\mathrm{R}_\Gamma, \mathbf{C}^*).$$

Let S now denote the set of (finite) rational prime divisors of $|\Gamma|$. Then, by the above work and from (2.2), we have

$$\mathrm{D}(\mathbf{Z}\Gamma) \simeq \frac{\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathrm{U_S}(\overline{\mathbf{Q}}))}{\mathrm{Hom}^+_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathcal{O}^*_{\overline{\mathbf{Q}}})\,\mathrm{Det}(\mathrm{U_S}(\mathbf{Z}\Gamma))}\,. \tag{2.3}$$

We now proceed to describe an element of $\mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathrm{U_S}(\overline{\mathbf{Q}}))$ which represents the class $(\mathcal{O}_\mathrm{E})^4$ under (2.3).

The fact that $(\mathcal{O}_\mathrm{E}) \in \mathrm{D}(\mathbf{Z}\Gamma)$ was first conjectured by J. Martinet, and was subsequently proved by A. Fröhlich (cf. Theorem 11 of [3]). Because E/F is tame, by Noether's theorem loc cit., $\mathcal{O}_\mathrm{E}$ is a locally free $\mathcal{O}_\mathrm{F}\Gamma$ module. Thus, by weak approximation, we can choose $a \in \mathrm{E}$ so that for all $\ell \in \mathrm{S}$

$$\mathcal{O}_\mathrm{E} \otimes_\mathbf{Z} \mathbf{Z}_\ell = a\,\mathcal{O}_\mathrm{F}\Gamma \otimes_\mathbf{Z} \mathbf{Z}_\ell\,.$$

Let $\{\sigma_i\}$ be a right transversal of $\Omega_\mathrm{F}\backslash\Omega_\mathbf{Q}$. We define

$$\mathrm{A} = \prod_i \Big(\sum_{\gamma\in\Gamma} a^{\gamma\sigma_i}\gamma^{-1} \Big). \tag{2.4}$$

We let $f_{\mathrm{E}} \in \mathrm{Hom}\,(\mathrm{R}_\Gamma\,,\ \prod_{\ell \in \mathrm{S}} \mathbf{Q}_\ell^*)$ be that homomorphism given by

$$(f_{\mathrm{E}}(\chi))_\ell = [\mathrm{Det}(\mathrm{A}_\ell)\,(\chi)\,(\tau(\chi)^{-1})_\ell]^4 \tag{2.5}$$

for $\chi \in \mathrm{R}_\Gamma$. From Theorem 2 of [3], we know that

$$f_{\mathrm{E}} \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma\,, \mathrm{U}_{\mathrm{S}}(\overline{\mathbf{Q}}))$$

and moreover, by (9.4) of [3], f_{E} represents the class of $(\mathcal{O}_{\mathrm{E}})^4$ under (2.3).

Let $\hat{\mathrm{E}}$ be the normal closure of E in $\overline{\mathbf{Q}}$; so that $\mathrm{A}_\ell \in \mathcal{O}_{\hat{\mathrm{E}}} \otimes \mathbf{Z}_\ell$. Indeed, because by hypothesis $\mathrm{E}/\mathbf{Q}$ is unramified at each $\ell \in \mathrm{S}$, from Corollary 2 to Proposition 1.2 of [3], we know that $\mathrm{Det}(\mathrm{A}_\ell)\,(\chi)$ is a unit for all $\chi \in \mathrm{R}_\Gamma$. Consequently we deduce that for each $\ell \in \mathrm{S}$

$$\mathrm{A}_\ell \in (\mathcal{O}_{\hat{\mathrm{E}}}\Gamma \otimes \mathbf{Z}_\ell)^*\,. \tag{2.6}$$

We now make certain adjustments to the homomorphism f_{E}. In [16] we showed that, if E/F is unramified at all $\ell \in \mathrm{S}$, then the homomorphism $v_{\mathrm{E}} \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mathrm{U}_{\mathrm{S}}(\overline{\mathbf{Q}}))$ given by $(v_{\mathrm{E}}(\chi))_\ell = (\mathrm{N}f(\chi))_\ell$, for $\ell \in \mathrm{S}$, represents the trivial class under (2.3). (Here $\mathrm{N}f(\chi)$ is the absolute norm of the Artin conductor $f(\chi)$ of χ). Trivially then, $(\mathcal{O}_{\mathrm{E}})^4$ is also represented by $f_{\mathrm{E}}\, v_{\mathrm{E}}^2$, and, from definition (7.2) in [10], we see that for all $\chi \in \mathrm{R}_\Gamma$, $\ell \in \mathrm{S}$

$$\begin{aligned}(f_{\mathrm{E}}(\chi)\,.\,v_{\mathrm{E}}(\chi)^2)_\ell &= \mathrm{Det}(\mathrm{A}_\ell)\,(\chi)^4\ \ (\tau(\chi)^{-4}\,\mathrm{N}f(\chi)^2)_\ell\\ &= \mathrm{Det}(\mathrm{A}_\ell)\,(\chi)^4\ \ (\mathrm{W}(\chi)^4)_\ell\,.\end{aligned} \tag{2.7}$$

In section 5 we will show

THEOREM 2. – *Let* E, F *and* Γ *be as given in Theorem 1. Then we can find a number field* K *so that*

(i) $\mathrm{K}/\mathbf{Q}$ *is abelian.*

(ii) $\mathrm{K}/\mathbf{Q}$ *is unramified at each* $\ell \in \mathrm{S}$.

(iii) *For each prime* $\mathfrak{P}$ *of* F *and for each* $\ell \in \mathrm{S}$, *there exists* $z_{\mathfrak{p},\ell} \in (\mathcal{O}_{\mathrm{K}}\mathrm{T}_{\mathfrak{p}} \otimes \mathbf{Z}_\ell)^*$ *and* $y_{\mathfrak{p}} \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Gamma, \mu)$ *so that*

$$(\mathrm{W}(\chi_{\mathfrak{p}})^4)_\ell = (y_{\mathfrak{p}}^4(\chi))_\ell\,\mathrm{Det}(z_{\mathfrak{p},\ell})\,(\chi) \tag{2.8}$$

for all $\chi \in \mathrm{R}_\Gamma$. *Further, it is immediate that we can choose* $z_{\mathfrak{p},\ell} = y_{\mathfrak{p}} = 1$ *for almost all* $\mathfrak{p}$.

Remark. – Despite its rather technical appearance Theorem 2 is very much the heart of the matter !

Now, from (2.7) and the above theorem, we see that $(\mathcal{O}_E)^4$ is represented by the homomorphism whose ℓ-component is $(\prod_{\mathfrak{p}} y_{\mathfrak{p}})_\ell \operatorname{Det}(A_\ell^4 \prod_{\mathfrak{p}} z_{\mathfrak{p},\ell})$ where the two products are taken over the primes $\mathfrak{p}$ which are ramified in $E/\mathbf{Q}$. So, because

$$\prod y_{\mathfrak{p}} \in \operatorname{Hom}_{\Omega_{\mathbf{Q}}}(R_\Gamma, \mu),$$

the class $(\mathcal{O}_E)^4$ is represented by $\prod_{\ell \in S} \operatorname{Det}(A_\ell^4 \prod_{\mathfrak{p}} z_{\mathfrak{p},\ell})$, the direct product being taken over $\ell \in S$. For brevity we now put $B_\ell = A_\ell^4 \prod_{\mathfrak{p}} z_{\mathfrak{p},\ell}$. By (2.6) and Theorem 2, we know that $B_\ell \in (\mathcal{O}_{\hat{E}K}\Gamma \otimes \mathbf{Z}_\ell)^*$.

However, we also know that $\operatorname{Det}(B_\ell)$ commutes with $\Omega_{\mathbf{Q}}$-action. Hence, for $\omega \in \Omega_{\mathbf{Q}}$ and $\chi \in R_\Gamma$,

$$\operatorname{Det}(B_\ell^\omega)(\chi) = [\operatorname{Det}(B_\ell)(\chi^{\omega^{-1}})]^\omega = \operatorname{Det}(B_\ell)(\chi)$$

$$\text{i.e.} \quad \operatorname{Det}(B_\ell^\omega) = \operatorname{Det}(B_\ell).$$

In Theorem 1 of [17], it is shown that for any number field L which is unramified at ℓ, if $x \in (\mathcal{O}_L\Gamma \otimes \mathbf{Z}_\ell)^*$ has the property that $\operatorname{Det}(x) = \operatorname{Det}(x^\omega)$ for all $\omega \in \Omega_{\mathbf{Q}}$, then

$$\operatorname{Det}(x) \in \operatorname{Det}((\mathcal{O}_L\Gamma \otimes \mathbf{Z}_\ell^*)^{\Omega_{\mathbf{Q}}}) = \operatorname{Det}(\mathbf{Z}_\ell\Gamma^*).$$

Thus we have shown that $\operatorname{Det}(B_\ell) \in \operatorname{Det}(\mathbf{Z}_\ell\Gamma^*)$, and so $(\mathcal{O}_E)^4$ is represented by an element of $\prod_{\ell \in S} \operatorname{Det}(\mathbf{Z}_\ell\Gamma^*)$. From this we conclude that $(\mathcal{O}_E)^4 = 1$.

We now describe the structure of the remainder of this paper. In section 3 we give various congruences for local grouprings of a cyclic group. In section 4 we define the local root number and introduce a certain adjusted root number. In section 5 we give the proof of Theorem 2, and, lastly, in section 6 we prove various lemmas concerning local root numbers which are stated in section 4.

3. Determinantal congruences.

In this section we describe various higher congruences for group rings of cyclic groups. These will play a crucial role in the proof of

Theorem 2 in section 5. However, it is also felt that these relations are of independent interest, and they could, perhaps, be used to throw further light on the structure of classgroups of cyclic groups.

Once and for all we fix a prime $\mathfrak{q}$ of E and a rational prime ℓ dividing $|\Gamma|$. From now on, therefore, we will omit the subscript $\mathfrak{q}$ on $T_{\mathfrak{q}}$ and $\Delta_{\mathfrak{q}}$.

Let $T = C_n$ be the cyclic group of order n. Suppose that the ℓ-Sylow subgroup of T has order ℓ^v – we denote it by C_{ℓ^v}. Then, if $n = m\,\ell^v$, C_m is the unique subgroup in C_n of order m.

We denote by $\mathbf{Z}_\ell[\zeta_s]$ the ring $\mathbf{Z}_\ell \otimes_{\mathbf{Z}} \mathcal{O}_{\mathbf{Q}(s)}$. We have an isomorphism of rings $\mathbf{Z}_\ell C_n \simeq \underset{s|m}{\otimes} \mathbf{Z}_\ell[\zeta_s]\, C_{\ell^v}$. For any number field K satisfying property (ii) of Theorem 2, we have the corresponding isomorphism

$$\mathcal{O}_{K_\ell} C_n \cong \oplus\, (\mathcal{O}_{K_\ell} \otimes_{\mathbf{Z}_\ell} \mathbf{Z}_\ell[\zeta_s]\, C_{\ell^v}). \tag{3.1}$$

Here $\Omega_{\mathbf{Q}}$ acts on the $\mathcal{O}_{K_\ell}$ component of each side. We let R_s be the free abelian group on those abelian characters of C_n whose restriction to C_n have order exactly s. Then, by (3.1), we have an isomorphism

$$\frac{\mathrm{Hom}_{\Omega_K}(R_{C_n}, U(\overline{\mathbf{Q}}_\ell))}{\mathrm{Det}(\mathcal{O}_{K_\ell} C_n^*)} \longrightarrow \underset{s|m}{\oplus} \frac{\mathrm{Hom}_{\Omega_K}(R_s, U(\overline{\mathbf{Q}}_\ell))}{\mathrm{Det}(\mathcal{O}_{K_\ell} \otimes \mathbf{Z}_\ell[\zeta_s]\, C_{\ell^v}^*}.$$

After a certain stage, by a "faithfulness argument", we shall be able to concentrate on the special case $s = m$. So, with this in mind, we now proceed to study the quotient group

$$\frac{\mathrm{Hom}_{\Omega_K}(R_m, U(\overline{\mathbf{Q}}_\ell))}{\mathrm{Det}(\mathcal{O}_{K_\ell} \otimes \mathbf{Z}_\ell[\zeta_m]\, C_{\ell^v}^*)}.$$

Let ξ'_s be an abelian character of C_m, with order exactly s, and let φ be a faithfull abelian character of C_{ℓ^v}. We define

$$\varphi_i = \varphi^{\ell^{v-i}} \qquad \xi_{s,i} = \xi'_s \otimes \varphi_i \tag{3.2}$$

and, for brevity, we will denote $\xi_{m,i}$ by ξ_i. We remark that for $z \in \mathcal{O}_{K_\ell} \otimes \mathbf{Z}_\ell[\zeta_m]\, C_{\ell^v}^*$, $\mathrm{Det}(z)$ is completely determined by specifying the values $\mathrm{Det}(z)\,(\xi_i)$ for $0 \leqslant i \leqslant v$.

Again, for the sake of brevity, we will write $\mathcal{O}(m\ell^i)$ for the ring of integers of $K(m\ell^i)_\ell$. Let $\mathbf{f}$ be the (unique) Frobenius of

ℓ in $K(n)/\mathbf{Q}(\ell^v)$ and let $N_{i/i-1} : K(m\ell^i) \longrightarrow K(m\ell^{i-1})$ be the norm map.

Now we shall assume that $v > 0$. We define homomorphisms

$$S^0_{i-1} : \mathrm{Hom}_{\Omega_K}(R_m, U(\overline{\mathbf{Q}}_\ell)) \longrightarrow U(\overline{\mathbf{Q}}_\ell)$$

for $0 < i \leqslant v$, via

$$S^0_{i-1}(h) = \begin{cases} N_{i/i-1}(h(\xi_i))\, h(\xi_{i-1})^{-\mathrm{f}} & \text{for } i > 1, \\ N_{1/0}(h(\xi_1))\, h(\xi_0)^{1-\mathrm{f}} & \text{for } i = 1, \end{cases}$$

where $h \in \mathrm{Hom}_{\Omega_K}(R_m, U(\overline{\mathbf{Q}}_\ell))$. More generally, for $0 \leqslant j \leqslant i \leqslant v-1$, we define *maps* $S^j_{i-1} : \mathrm{Hom}_{\Omega_K}(R_m, U(\overline{\mathbf{Q}}_\ell)) \longrightarrow \overline{\mathbf{Q}}_\ell$ in the following inductive manner. We put

$$S^1_{i-1}(h) = \left(\frac{S^0_{i-1}(h) - 1}{\ell}\right)^\ell - \left(\frac{S^0_{i-2}(h) - 1}{\ell}\right)^\mathrm{f}$$

for each $i > 1$, and then inductively, for $i - 1 \geqslant j \geqslant 2$, we put

$$S^j_{i-1}(h) = \left(\frac{S^{j-1}_{i-1}(h)}{\ell}\right)^\ell - \left(\frac{S^{j-1}_{i-2}(h)}{\ell}\right)^\mathrm{f}.$$

PROPOSITION 1. – *Let* $z \in \mathcal{O}(m)\, C^*_{\ell^v}$. *Then, for*

$$0 \leqslant j \leqslant i - 1 \leqslant v - 1,$$

$$S^j_{i-1}(\mathrm{Det}(z)) \equiv \begin{cases} 1 \mod(\ell) & \text{if } j = 0, \\ 0 \mod(\ell) & \text{if } j > 0. \end{cases}$$

Before proving the proposition we need a lemma.

LEMMA 4. – *Let* ζ_ℓ *be a primitive* ℓ^{th} *root of unity, and let* $X_1, \ldots, X_{\ell^v}$ *be* ℓ^v *algebraically independent indeterminates. Then*

$$\prod_{\alpha=1}^{\ell} \Big(\sum_{j=1}^{\ell^v} X_j \zeta_\ell^{\alpha j}\Big) = \sum_j X_j^\ell + \ell f(X_1, \ldots, X_{\ell^v})$$

for some $f(X_1, \ldots, X_{\ell^v}) \in \mathbf{Z}[X_1, \ldots, X_{\ell^v}]$.

Proof. – We observe that, by the binomial theorem, the expression on the left is congruent to

$$\sum_j X_j^\ell \mod (1 - \zeta_\ell)\, \mathbf{Z}[\zeta_\ell, X_1, \ldots, X_{\ell^v}].$$

However, by Galois theory, the left hand side belongs to $\mathbf{Z}[X_1, \ldots, X_{\ell v}]$ hence the congruence holds $\bmod \ell \mathbf{Z}[X_1, \ldots, X_{\ell v}]$, which establishes the lemma.

We now proceed with the proof of the proposition. Let $C_{\ell v} = \langle c \rangle$ and suppose $z = \Sigma\, a_j c^j \in \mathcal{O}(m)\, C^*_{\ell v}$ with $a_j \in \mathcal{O}(m)$. In the above lemma we make the substitution $X_j = a_j \varphi_i(c^j)$. Then, for $i > 1$,

$$N_{i/i-1}(\varphi_i(z)) = \Sigma\, a_j^\ell \varphi_i(c^{j\ell}) + \ell\, \varphi_i(f(a_1 c, \ldots, a_{\ell v})$$

and similarly

$$N_{1/0}(\varphi_1(z))\, \varphi_0(z) = \Sigma\, a_j^\ell + \ell\, \varphi_1(f(a_1 c, \ldots, a_{\ell v}).$$

So now we define $b \in \mathcal{O}(m)\, C_{\ell v}$, by

$$b = \sum_j \left(\frac{a_j^\ell - a_j^{\mathsf{f}}}{\ell}\right) c^{j\ell} + f(a_1 c, \ldots, a_{\ell v}).$$

Then it follows that for all $i > 1$

$$N_{i/i-1}(\varphi_i(z)) - \varphi_{i-1}(z)^{\mathsf{f}} = \varphi_i(\ell b)$$

and further, when $i = 1$,

$$N_{1/0}(\varphi_1(z))\, \varphi_0(z) - \varphi_0(z)^{\mathsf{f}} = \varphi_1(\ell b).$$

We now introduce the ring homomorphism

$$\psi : \mathcal{O}(m)\, C_{\ell v} \longrightarrow \mathcal{O}(m)\, C_{\ell v - 1}$$

given by $\psi(\Sigma\, d_j c^j) = \Sigma\, d_j c^{\ell j}$, where $d_\ell \in \mathcal{O}(m)$. Now we put $b^{(0)} = 1 + \ell b\,.\,(\psi(z^{\mathsf{f}}))^{-1}$. Note that since z is a unit in $\mathcal{O}(m)\, C_{\ell v}$, $\psi(z^{\mathsf{f}})$ is also a unit, and thus $b^{(0)} \in 1 + \ell \mathcal{O}(m)\, C_{\ell v}$ (here f acts on $\mathcal{O}(m)\, C_{\ell v}$, by fixing the elements of $C_{\ell v}$). It is now immediate that for all $i > 0$, $S^0_{i-1}(\mathrm{Det}(z)) = \varphi_i(b^{(0)})$.

Now we define

$$b^{(1)} = \left(\frac{b^{(0)} - 1}{\ell}\right)^{\ell} - \left(\frac{\psi(b^{(0)}) - 1}{\ell}\right)^{\mathsf{f}}$$

and inductively, for $i > 1$, we put

$$b^{(j)} = \left(\frac{b^{(j-1)}}{\ell}\right)^{\ell} - \left(\frac{\psi(b^{(j-1)})}{\ell}\right)^{\mathsf{f}}.$$

Then, by an elementary induction argument on j, using the fact that, for $i > 0$, $\varphi_{i-1} = \varphi_i \circ \psi$, we obtain that

$$S^{j}_{i-1}(\mathrm{Det}(z)) = \varphi_i(b^{(j)}),$$

for all $0 \leqslant j \leqslant i-1 < v$. However, by repeated application of the Binomial theorem we see that $b^{(j)} \in \ell\, \mathcal{O}(m)\, C_{\ell^v}$ for each j, and thus the proposition is shown.

LEMMA 5. – *Let* $v \geqslant 2$, *let* $z \in \mathcal{O}(m)\, C^*_{\ell^v}$, *and suppose that for each* i, $0 \leqslant i-1 < v-1$, $S^0_{i-1}(\mathrm{Det}(z)) = 1$; then

$$S^0_{v-1}(\mathrm{Det}(z)) \in 1 + \ell(1-\zeta_\ell)\, \mathcal{O}(n\ell^{-1}).$$

Proof. – From Proposition 1, we know that

$$S^0_{v-1}(\mathrm{Det}(z)) = 1 + \ell\alpha,$$

for some $\alpha \in \mathcal{O}(n\ell^{-1})$. To each prime $\mathfrak{L}_i$ of $K(n\ell^{-1})$ which lies above ℓ, we associate the standard (additive) valuation ν_i (such that ν_i maps $K(n\ell^{-1})$ onto $\mathbf{Z}$). From the definition of S^{v-1}_{v-1}, and using the fact that $S^0_{i-1}(\mathrm{Det}(z)) = 1$ for $i-1 < v-1$, we obtain that for $v > 1$

$$S^{v-1}_{v-1}(\mathrm{Det}(z)) = \alpha^{\ell^{v-1}} \,.\, \ell^{-[(\ell^{v-1}-1)(\ell-1)^{-1}-1]}\,.$$

Whilst by Proposition 1, we know that $S^{v-1}_{v-1}(\mathrm{Det}(z)) \equiv 0 \bmod(\ell)$, and hence, for each i, $\ell^{v-1} \,.\, \nu_i(\alpha) \geqslant \nu_i(1-\zeta_\ell)\,(\ell^{v-1}-1)$.

Now suppose, for a contradiction, that $\alpha \notin (1-\zeta_\ell)\, \mathcal{O}(n\ell^{-1})$. Then for some i, $\nu_i(\alpha) \leqslant \nu_i(1-\zeta_\ell) - 1$,

i.e. $$\ell^{v-1}\nu_i(\alpha) \leqslant \ell^{v-1}\nu_i(1-\zeta_\ell) - \ell\nu_i(1-\zeta_\ell),$$
$$< (\ell^{v-1}-1)\,\nu_i(1-\zeta_\ell).$$

Thus we obtain a contradiction, and so the lemma is shown.

LEMMA 6. – *For* $i > 1$,

$$N_{i/i-1}(1 + (1-\zeta_\ell)\, \mathcal{O}(m\ell^i)) = 1 + \ell(1-\zeta_\ell)\, \mathcal{O}(m\ell^{i-1}).$$

Proof. – Let φ, ψ denote the Herbrand functions of the extension $K(m\ell^i)/K(m\ell^{i-1})$, let t denote the so-called "jump number" for this extension, and let ν be the standard valuation attached to some prime of $K(m\ell^i)$ which lies above ℓ (cf. page 91 of [12] for details). We know that $t = \nu((1-\zeta_\ell)(1-\zeta_{\ell^i})^{-1})$, $\varphi(t) = t = \psi(t)$, and so the lemma follows immediately from Corollary 3 on page 93 of [12].

4. Local root numbers.

In this section we first define the local root number (following the treatment given by Tate in [16]). We then define an adjusted local root number and establish certain basic results for it. Then, at the end of this section, we cite six lemmas, whose proof will be given in section 6.

Throughout the remainder of this paper we shall refer to finite extensions of $\mathbf{Q}_p$ (resp. of $\mathbf{R}$) as non-Archimedean fields (resp. as Archimedean fields).

Let $E_{\mathfrak{q}}/F_{\mathfrak{p}}$ be an arbitrary Galois extension of Archimedean or non-Archimedean fields with $\mathrm{Gal}(E_{\mathfrak{q}}/F_{\mathfrak{p}}) = \Delta$. Langlands, and later Deligne in [2], showed that for each Galois group Δ there exists a unique homomorphism, called the local root number, $W_\Delta : R_\Delta \longrightarrow \bar{\mathbf{Q}}^*$, with the property that

(i) Let $\Lambda \subset \Delta$ and suppose $\chi \in R_\Lambda$ with $\chi(1) = 0$, i.e. χ is of degree zero, then

$$W_\Delta(\mathrm{Ind}_\Lambda^\Delta(\chi)) = W_\Lambda(\chi).$$

(ii) Suppose restriction of automorphism induces a surjection of Galois groups $\Delta \longrightarrow \Omega$, and let $\chi \in R_\Omega$, then

$$W_\Delta(\mathrm{Inf}_\Omega^\Delta(\chi)) = W_\Omega(\chi).$$

(iii) Let χ be an abelian character of Δ, and suppose

(a) $F_{\mathfrak{p}}$ *is Archimedean*

Then $W_\Delta(\chi) = 1$ if $F_{\mathfrak{p}}$ is complex,

$$W_\Delta(\chi) = \begin{cases} 1 & \text{if } F_{\mathfrak{p}} \text{ is real, } \chi \text{ trivial,} \\ -i & \text{if } F_{\mathfrak{p}} \text{ is real, } \chi \text{ non-trivial.} \end{cases}$$

(Here i is the square root of -1).

(b) $F_{\mathfrak{p}}$ *is non-Archimedean*

Let $\mathfrak{q}$ (resp. $\mathfrak{p}$) be the maximal ideal of the ring of integers of $E_{\mathfrak{q}}$ (resp. $F_{\mathfrak{p}}$). We denote the different of $F_{\mathfrak{p}}$ by $D_{F_{\mathfrak{p}}}$, and we choose $c \in F_{\mathfrak{p}}$ so that $c\mathcal{O}_{F_{\mathfrak{p}}} = D_{F_{\mathfrak{p}}} f(\chi)$. We let $\psi_{F_{\mathfrak{p}}}$ be the canonical additive character of $F_{\mathfrak{p}}$, given by the composite

$$\mathrm{F}_{\mathfrak{p}} \xrightarrow{\mathrm{Tr}_{\mathrm{F}}/\mathbf{Q}_p} \mathbf{Q}_p \longrightarrow \mathbf{Q}_p/\mathbf{Z}_p \hookrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow \mathbf{R} \xrightarrow{e^{2\pi i}} \mathbf{C}^*$$

(Note that for $\Lambda \subset \Delta$, we shall frequently write ψ_Λ in place of $\psi_{\mathrm{E}_{\mathfrak{q}}^{\Lambda}}$, the canonical additive character of $\mathrm{E}_{\mathfrak{q}}^{\Lambda}$).

If χ is unramified, we set $\mathrm{W}_\Delta(\chi) = \chi(\mathrm{D}_{\mathrm{F}_{\mathfrak{p}}})$.

If χ is genuinely ramified, we set

$$\mathrm{W}_\Delta(\chi) = \mathrm{N}f(\chi)^{-1/2} \sum_{u \in \mathcal{O}^*_{\mathrm{F}_{\mathfrak{p}}} \bmod f(\chi)} \chi(u^{-1}c)\, \psi_{\mathrm{F}_{\mathfrak{p}}}(uc^{-1}).$$

(We view χ as a character of $\mathrm{F}_{\mathfrak{p}}^*$, via composition with the local Artin map, in the usual way).

We remark that $\mathrm{W}_\Delta(\chi)$ is then defined for all virtual characters χ by Brauer's induction theorem (cf. Example 2, page 96 [13]).

Globalisation. – Suppose E/F is a Galois extension of number fields, with $\Gamma = \mathrm{Gal}(\mathrm{E}/\mathrm{F})$. Let $\mathfrak{p}$ be a prime of F and let $\mathfrak{q}$ be a prime of E above $\mathfrak{p}$. If $\chi \in \mathrm{R}_\Gamma$, χ yields a character of the decomposition group $\mathrm{Gal}(\mathrm{E}_{\mathfrak{q}}/\mathrm{F}_{\mathfrak{p}})$. We put $\mathrm{W}(\chi_{\mathfrak{p}}) = \mathrm{W}_{\Delta_{\mathfrak{q}}}(\chi \mid_{\Delta_{\mathfrak{q}}})$ (which is defined by the above work). Then we have that $\mathrm{W}(\chi) = \prod_{\mathfrak{p}} \mathrm{W}(\chi_{\mathfrak{p}})$ where $\mathrm{W}(\chi)$ is the Artin root number of χ, and where the product extends over all primes of F.

We now define an "adjusted" local root number W^*. (W^* is in many ways similar to the adjusted root number ϵ_0 introduced in (5.1) of [2]. First though, we state without proof the following elementary result:

LEMMA 7. – *Let* $\mathrm{E}_{\mathfrak{q}}/\mathrm{F}_{\mathfrak{p}}$ *be a tame Galois extension of non-Archimedean fields, then* $\mathfrak{q}\,\mathrm{D}_{\mathrm{E}_{\mathfrak{q}}} = \mathfrak{p}\,\mathrm{D}_{\mathrm{F}_{\mathfrak{p}}}\,\mathcal{O}_{\mathrm{E}_{\mathfrak{q}}}$.

From now on we will always assume the extension $\mathrm{E}_{\mathfrak{q}}/\mathrm{F}_{\mathfrak{p}}$ to be both tame and Galois. We fix $c \in \mathrm{F}_{\mathfrak{p}}$ so that $c\,\mathcal{O}_{\mathrm{F}_{\mathfrak{p}}} = \mathfrak{p}\,\mathrm{D}_{\mathrm{F}_{\mathfrak{p}}}$. For each subgroup Σ of Δ, we define $y_\Sigma \in \mathrm{Hom}_{\Omega_{\mathbf{Q}}}(\mathrm{R}_\Sigma, \mu)$, by stipulating that for each irreducible character φ of Σ

$$y_\Sigma(\varphi) = \begin{cases} -\varphi(\mathrm{D}_{\mathrm{E}_{\mathfrak{q}}^{\Sigma}})^{-1} & \text{if } \varphi \text{ unramified}, \\ \det_\varphi(c^{-1}) & \text{otherwise}. \end{cases} \tag{4.1}$$

Remark. – y_Σ is closely related to the non-ramified characteristic homomorphism introduced in [7].

For each $\Sigma \subset \Delta$, we define

$$W_{\Sigma}^{*}(\varphi) = y_{\Sigma}(\varphi)\, W_{\Sigma}(\varphi) \tag{4.2}$$

for $\varphi \in R_{\Sigma}$, where $W_{\Sigma}(\varphi)$ is the local root number of φ, defined previously. Frequently, when there is no danger of confusion, the subscript Σ will be omitted on W and W^*. The crucial property of W^* is:

LEMMA 8. – *Let ν be an unramified abelian character of Δ, then, for each $\chi \in R_{\Delta}$, $W^*(\chi) = W^*(\nu\chi)$.*

Proof. – From page 115 of [14], we derive that

$$W(\nu\chi) = W(\nu)^{\chi(1)}\, W(\chi)\, \nu(f(\chi)).$$

Now, if χ is irreducible and genuinely ramified,

$$W(\nu\chi) = W(\nu)^{\chi(1)}\, W(\chi)\, \nu(\mathfrak{p})^{\chi(1)} = y_{\Delta}(\chi - \nu\chi)\, W(\chi)$$

as is required. On the other hand, if χ is irreducible and unramified, then the result is immediate.

Now let α be an abelian character of the inertia group T, and let χ_{α} be any irreducible character of Δ which occurs in $\mathrm{Ind}_{T}^{\Delta}(\alpha)$. Such irreducible characters differ only by a multiple of an unramified abelian character. So from Lemma 8, $W^*(\chi_{\alpha})$ depends only on α, and not on the particular choice of χ_{α}.

For the sake of clarity it will be convenient to introduce the following notation. With the terminology of (3.2), we shall write $W^*(\chi_{s,i})$ (resp. $W^*(\chi_i)$) in place of $W^*(\chi_{\xi s,i})$ (resp. $W^*(\chi_{\xi i})$).

Because both T and $\mathrm{Ker}(\alpha)$ are normal in Δ, and because by our hypotheses on K, $K \cap \mathbf{Q}(\alpha) = \mathbf{Q}$, conjugation induces a homomorphism of groups $\rho_{\alpha} : \Delta_{/T} (= \Xi$, say$) \longrightarrow \mathrm{Gal}(K(\alpha)/K)$ given by $(\alpha(c))^{\rho_{\alpha}(\delta)} = \alpha(\delta^{-1} c \delta)$, for $c \in T$, $\delta \in \Delta$. We will denote the kernel of the composite homomorphism $\Delta \longrightarrow \Xi \longrightarrow \mathrm{Gal}(K(\alpha)/K)$ by H_{α}, and we put $\Sigma_{\alpha} = \Delta/H_{\alpha}$. Equivalently

$$H_{\alpha} = \mathrm{Ker}(\Delta \longrightarrow \mathrm{Aut}(T/\mathrm{Ker}(\alpha))).$$

This interchange between local Galois groups and "cyclotomic" Galois groups will be absolutely crucial in the sequel.

(4.3) From now on we shall view Σ_α as a sub-group of $\mathrm{Gal}(\mathrm{K}(\alpha)/\mathrm{K})$. Again, for the sake of brevity, it will be convenient to write $\Sigma_{s,i}$, $\mathrm{H}_{s,i}$, Σ_i, H_i in place of $\Sigma_{\xi_{s,i}}$, $\mathrm{H}_{\xi_{s,i}}$, Σ_{ξ_i}, H_{ξ_i}, respectively.

For a finite abelian group G, we denote the ℓ-Sylow sub-group of G by G_ℓ, and we let G' be the unique direct complement of G_ℓ in G.

(4.4) We write $\mathrm{A}_{s,i} = \mathrm{K}(\xi_{s,i})$, $\mathrm{A}_i = \mathrm{K}(\xi_i)$, and we let $\mathrm{B}_{s,i}$ (resp. B_i) be the subfield of $\mathrm{A}_{s,i}$ (resp. A_i) which is fixed by $\Sigma_{s,i}$ (resp. by Σ_i). Then by use of Mackey's restriction formula (cf. 7.3 of [13]), we obtain that

$$\mathrm{B}_{s,i} = \mathrm{A}_{s,i}^{\Sigma_{s,i}} = \mathrm{K}(\chi_{s,i}|_{\mathrm{T}}).$$

(4.6) The inertia group of the primes above ℓ in the extension $\mathrm{A}_i/\mathrm{B}_i$ is easily calculated from the action of Σ_i on T. To be more precise, the inertia sub-group of Σ_i is made up of those elements which act trivially on T'.

For the remainder of this section K satisfies conditions (i) and (ii) of Theorem 2 and also we assume that $\mathrm{K} \supseteq \mathbf{Q}(p)$.

LEMMA 9. – $\mathrm{W}^*(\chi_{s,i})$ *is a unit in the integers of* $(\mathrm{B}_{s,i})_\ell$, *and further, for* $\omega \in \Omega_{\mathbf{Q}(p)}$ $\mathrm{W}^*(\chi_{s,i}^\omega)^2 = \mathrm{W}^*(\chi_{s,i})^{2\omega}$.

Proof. – We know that $\chi_{s,i} = \mathrm{Ind}_{\mathrm{H}_{s,i}}^{\Delta}(\check{\xi}_{s,i})$, for some abelian character $\check{\xi}_{s,i}$ which extends $\xi_{s,i}$. From the inductivity of local root numbers in degree zero we deduce that $\mathrm{W}_\Delta(\chi_{s,i})^2 = \mathrm{W}_{\mathrm{H}_{s,i}}(\check{\xi}_{s,i}^\gamma)^2$ for each $\gamma \in \Delta$, where $\check{\xi}_{s,i}^\gamma$ is the abelian character obtained by composing $\check{\xi}_{s,i}$ with conjugation by γ. Hence, for all $\sigma \in \Sigma_{s,i}$

$$\mathrm{W}(\chi_{s,i})^2 = \begin{cases} \chi(\mathrm{D}_{\mathrm{F}}\ )^2 & \text{if } \chi \text{ is unramified}, \\ \mathrm{N}f(\chi_{s,i})^{-1}\Big(\sum\limits_u \check{\xi}_{s,i}(u^{-1})\,\psi_{\mathrm{H}_{s,i}}(uc^{-1})\Big)^{2\sigma}\check{\xi}_{s,i}^{v}(c^2) & \text{otherwise.}\end{cases}$$

Here the sum extends over a set of representatives of the units of $\mathrm{E}_{\mathfrak{q}}^{\mathrm{H}_{s,i}}$ modulo $\mathfrak{q} \cap \mathrm{E}_{\mathfrak{q}}^{\mathrm{H}_{s,i}}$. Note that because $\check{\xi}_{s,i}|_{\mathrm{T}} = \xi_{s,i}$, it follows that the $\check{\xi}_{s,i}(u) \in \xi_{s,i}(\mathrm{T})$.

Now, in the unramified case $\mathrm{W}^*(\chi_{s,i})^2 = 1$, whilst in the remaining case, by local class field theory,

$$y_\Delta(\chi)^2 = \det_\chi(c)^{-2} = \mathrm{V}_{\mathrm{H}_{s,i}}^{\Delta}\,\check{\xi}_{s,i}(c^{-2}) = \check{\xi}_{s,i}(c^{-2}).$$

Thus, by the above, we see that $W^*(\chi_{s,i})^2 \in \mathbf{Q}(p, \xi_{s,i})^{\Sigma_{s,i}}$, which, by (4.5), is a subfield of $B_{s,i}$.

Further, it is clear from the above that for $\omega \in \Omega_{\mathbf{Q}(p)}$,

$$W(\chi_{s,i}^{\omega})^2 = W(\check{\xi}_{s,i})^2 = W(\check{\xi}_{s,i})^{2\omega} = W(\chi_{s,i})^{2\omega},$$

whilst $y_\Delta(\chi_{s,i}^{\omega}) = y_\Delta(\chi_{s,i})^{\omega}$, because y_Δ commutes with $\Omega_{\mathbf{Q}}$ action. So indeed we obtain the equation $W^*(\chi_{s,i}^{\omega})^2 = W^*(\chi_{s,i})^{2\omega}$.

Finally, we must show that $W^*(\chi_{s,i})$ is an ℓ-unit. However, by the above work $Nf(\chi_{s,i})\,W(\chi_{s,i})^2$ is an algebraic integer, whilst from Proposition 4.1 of [10], we know that $Nf(\chi_{s,i})\,W(\chi_{s,i})^2$ divides $Nf(\chi_{s,i})^2$ which, in turn, is an ℓ-unit, since all prime divisors of the group order of Γ are unramified in E/F.

In the remainder of this section, we state various results which relate $W^*(\chi_{i+1})$ and $W^*(\chi_i)$. First though, we must introduce further notation.

For $i > 0$, the surjection of Galois groups

$$\mathrm{Gal}(A_i/K) \longrightarrow \mathrm{Gal}(A_{i-1}/K)$$

induces a surjection $\Sigma_i \longrightarrow \Sigma_{i-1}$. We put $q = \mathrm{Card}(\mathrm{Ker}(\Sigma_1 \longrightarrow \Sigma_0))$,

$$\text{if } \ell \neq 2,\quad r = \mathrm{Sup}\,\{i \geqslant 1 \mid \mathrm{Ker}(\Sigma_i \longrightarrow \Sigma_1) = \{1\},$$

$$\text{if } \ell = 2,\quad u = \mathrm{Sup}\,\{i \geqslant 1 \mid |\mathrm{Ker}\,(\Sigma_i \longrightarrow \Sigma_1)| \leqslant 2\}.$$

Because $\mathrm{Ker}(\Sigma_1 \longrightarrow \Sigma_0)$ is a subgroup of the automorphism group of the ℓ^{th} roots of unity, we see that $q \mid \ell - 1$, and so, in particular $(q, \ell) = 1$. Further, we see that if $\ell \neq 2$, then r is the largest integer so that Σ_r acts tamely at ℓ. (As far as I know the integer u has no such neat interpretation).

The following result is an elementary exercise in the theory of automorphisms of cyclic groups – consequently we shall omit the proof.

LEMMA 10. –

(i) *Let* $\ell \neq 2$ *and suppose* $\ell \mid (H_0 : H_i)$ (i.e. $i > r$), *then for all* $k > i$, $(H_{k-1} : H_k) = \ell$.

(ii) *Let* $\ell = 2$ *and suppose* $4 \mid (H_0 : H_i)$ (i.e. $i > u$), *then for all* $k > i$, $(H_{k-1} : H_k) = 2$.

Recall that $\mathbf{f} \in \Omega_{\mathbf{Q}}$ has the property that its restriction to $K(|T'|)$ is the Frobenius for the primes above ℓ, whilst the restriction to $\mathbf{Q}(|T_\ell|)$ is trivial.

LEMMA 11. –

(i) *Let* $\ell \neq 2$, *then* $W^*(\chi_1)^2 \equiv W^*(\chi_0)^{2q} \bmod \mathfrak{N}_\ell$ *and*

$$N_{B_1/B_0}(W^*(\chi_1)^4) = W^*(\chi_0)^{4(\mathbf{f}-1)}.$$

(ii) *Let* $\ell = 2$, *then* $W^*(\chi_1)^2 \equiv W^*(\chi_0)^2 \bmod \mathfrak{N}_2$ *and*

$$W^*(\chi_1)^4 = W^*(\chi_0)^{4(\mathbf{f}-1)}.$$

LEMMA 12. –

(i) *Let* $\ell \neq 2$ *and suppose* $r \geqslant i > 1$, *then*

$$N_{i/i-1}(W^*(\chi_i)^4) = W^*(\chi_{i-1})^{4\mathbf{f}}$$

(ii) *Let* $\ell = 2$, *let* $i > 1$ *and suppose that* $H_{i-1} = H_i$, *then*

$$N_{i/i-1}(W^*(\chi_i)^4) = W^*(\chi_{i-1})^{4\mathbf{f}},$$

and further, if $(H_0 : H_i) > 1$, *then*

$$N_{i/i-1}(W^*(\chi_i)^2) = W^*(\chi_{i-1})^{2\mathbf{f}}.$$

LEMMA 13. –

(i) *Let* $\ell \neq 2$ *and suppose* $i > r$, *then* $W^*(\chi_i)^4 = W^*(\chi_{i-1})^{4\mathbf{f}}$.

(ii) *Let* $\ell = 2$ *and suppose* $(H_{i-1} : H_i) = 2$, *then*

$$W^*(\chi_i)^4 = W^*(\chi_{i-1})^{4\mathbf{f}}.$$

LEMMA 14. – *Let* $\Phi \subset \Psi \subset \Delta$, *suppose that* Φ *is normal in* Ψ *with* Ψ/Φ *abelian, and let* $\varphi \in R_\Phi$.

(i) *If the ramification index in* $E_{\mathfrak{q}}^\Phi / E_{\mathfrak{q}}^\Psi$ *is odd, then*

$$W^*(\mathrm{Ind}_\Phi^\Psi(\varphi))^2 = W^*(\varphi)^2.$$

(ii) *If* $(\Psi : \Phi) = 2$ *and if* $E_{\mathfrak{q}}^\Phi / E_{\mathfrak{q}}^\Psi$ *is totally ramified, then*

$$W^*(\mathrm{Ind}_\Phi^\Psi(\varphi))^2 = (-1)^{\frac{\mathbf{N}\mathbf{P}-1}{2}\cdot\varphi(1)}\, W^*(\varphi)^2$$

where $\mathbf{P}$ *is the maximal ideal of the ring of integers of* $E_{\mathfrak{q}}^\Psi$.

LEMMA 15 (Hasse-Davenport). – *Let* $\Phi \subset \Psi \subset \Delta$, *let*

$$\Phi \cap T = \Psi \cap T$$

and let ψ *be an abelian character of* Ψ, *then*

$$W^*(\psi)^{2(\Psi:\Phi)} = W^*(\psi|_\Phi)^2 .$$

For the statement of the last in our series of lemmas, we suppose that $v = r$ if $\ell \neq 2$ and that $v = u$ if $\ell = 2$ (where $|T_\ell| = \ell^v$ as per the notation of section 3). We let M be the subfield of E fixed by H_v. Because ξ_v is faithful on T and because Δ is metacyclic, we know that E_q/M is an abelian extension.

Let $(-, E_q/M)$ be the Artin symbol attached to the extension E_q/M. We define T, $\overline{T} \in \mathbf{Z}[\zeta_p]\,T$ by

$$T = \sum_u (u, E_q/M)\, \psi_M(uc^{-1})$$

$$\overline{T} = \sum_u (u^{-1}, E_q/M)\, \psi_M(-uc^{-1})$$

where both sums extend over a set of representatives of $\mathcal{O}_M^*$ mod $\mathfrak{p}\mathcal{O}_M$.

LEMMA 16. – *With notation as above, let* $\beta \in R_{H_0}$ *and let* $\alpha \in R_{H_v}$, *then*

$$\mathrm{Det}(\overline{T}\,T^{-1})(\beta) = W^*(\beta)^{2(H_0:H_v)},$$

$$\mathrm{Det}(\overline{T}\,T^{-1})(\alpha) = W^*(\alpha)^2 .$$

Lemmas 11 to 16 will be proved in section 6.

5. Proof of theorem 2.

We keep the notation of previous sections. We shall consider number fields K such that

(5.1a) $K/\mathbf{Q}$ is abelian and unramified at primes in S.

(5.1b) $K \supset \mathbf{Q}(p)$, for all primes p which ramify in E/F.

(5.1c) The residue classfields of K at primes $\ell \in S$ are "big enough" (in a sense which will be made more precise later).

For the existence of such fields K satisfying (5.1c) cf. § 2, Ch. X of [9].

As previous $\mathfrak{l}$ is a chosen prime in S, and $\mathfrak{p}$ is a fixed prime of F. We now state a theorem which we will firstly show implies Theorem 2, and then we will prove that theorem.

THEOREM 3. – *We can find a number field* K *(as in (5.1)) and homomorphisms* $t^{(s)} \in \mathrm{Hom}_{\Omega_K}(R_s, U(\overline{\mathbf{Q}}_{\mathfrak{l}}))$ *for each* $s \mid m$, *with the property that*

(1) *For each* i, $0 \leqslant i \leqslant v$, *and for all* $s \mid m$

$$N_{A_{s,i}/B_{s,i}}(t^{(s)}(\xi_{s,i})) = (W^*(\chi_{s,i})^4)_{\mathfrak{l}}.$$

(2) *For* $1 < i$

$$N_{i/i-1}(t^{(s)}(\xi_{s,i})) = t^{(s)}(\xi_{s,i-1})^{\mathfrak{f}},$$

and

$$N_{1/0}(t^{(s)}(\xi_{s,1})) = t^{(s)}(\xi_{s,0})^{\mathfrak{f}-1}.$$

(3)
$$t^{(s)} \in \mathrm{Det}(\mathcal{O}_{K_{\mathfrak{l}}} \otimes \mathbf{Z}[\zeta_s]\, C^*_{\mathfrak{l}^v}).$$

Now, because $R_T \cong \bigoplus_{s \mid m} R_s$, we may view

$$\oplus\, t^{(s)} \in \mathrm{Hom}_{\Omega_K}(R_T, U(\overline{\mathbf{Q}}_{\mathfrak{l}})).$$

We put $g = \oplus\, t^{(s)}$.

PROPOSITION 2. – *If* g *is as given by Theorem 3, then for* $\chi \in R_\Delta$ $\mathrm{Ind}_T^\Delta(g)(\chi)$ $(= g(\chi|_T)) = (W^*(\chi)^4)_{\mathfrak{l}}$.

Proof. – By $\mathbf{Z}$-linearity it is sufficient to show that for each pair (s, i), $\mathrm{Ind}_T^\Delta(g)(\chi_{s,i}) = (W^*(\chi_{s,i})^4)_{\mathfrak{l}}$.

Now,

$$\mathrm{Ind}_T^\Delta(g)\,(\chi_{s,i}) = g(\chi_{s,i}|_T)$$

by Mackey's restriction theorem,

$$= g\Big(\sum_{\sigma \in \Sigma_{s,i}} \xi_{s,i}^{\sigma}\Big)$$

since g commutes with Ω_K action,

$$= N_{A_{s,i}/B_{s,i}}(g(\xi_{s,i}))$$

by definition of g

$$= N_{A_{s,i}/B_{s,i}}(t^{(s)}(\xi_{s,i}))$$

by (1)

$$= (W^*(\chi_{s,i})^4)_{\mathfrak{l}}.$$

Now we show that Theorem 3 implies Theorem 2. By part (3) of Theorem 3 we may suppose that $t^{(s)} = \mathrm{Det}(z_s)$, for $z_s \in \mathcal{O}_{K_\ell} \otimes \mathbf{Z}[\zeta_s] C^*_{\ell v}$. We suppose that under the isomorphism (3.1), $z_{\mathfrak{p},\ell} \longmapsto \oplus z_s$. Then, by Proposition 2, for $\varphi \in R_\Delta$,

$$(W^*(\varphi)^4)_\ell = \mathrm{Ind}_T^\Delta(g)(\varphi) = g(\varphi|_T) = \mathrm{Det}(z_{\mathfrak{p},\ell})(\varphi|_T) = \mathrm{Det}(z_{\mathfrak{p},\ell})(\varphi).$$

However, for $\chi \in R_\Gamma$,

$$\begin{aligned}(W(\chi_{\mathfrak{p}})^4)_\ell &= (W(\chi|_\Delta)^4)_\ell,\\ &= (y_\Delta(\chi|_\Delta)^4 \cdot W^*(\chi|_\Delta)^4)_\ell,\\ &= (\mathrm{Ind}_\Delta^\Gamma(y_\Delta)(\chi))_\ell \,\mathrm{Det}(z_{\mathfrak{p},\ell})(\chi),\end{aligned}$$

and so, if we write $y = \mathrm{Ind}_\Delta^\Gamma(y_\Delta)$ we obtain Theorem 2.

Remark. – In the above proof that Theorem 3 implies Theorem 2, it is not apparent why we impose condition (2) on the t's. In fact, this condition will play a crucial role when we use an induction argument to demonstrate the existence of the t-homomorphisms.

Now we set out to prove Theorem 3. By factoring out in Δ by subgroups of T and by arguing by induction on $|\Delta|$, we may assume that $t^{(s)}$ exists in Theorem 3 for all $s\,|\,m$, $s \neq m$. So now we have to produce $t^{(m)}$. For brevity, we write t in place of $t^{(m)}$. Moreover, because Theorem 3 is easily seen to be trivial if $v = 0$, we may assume $v \geqslant 1$. (For, if $v = 0$, we need only find $x \in U_\ell(A_{s,0})$ so that $N_{A_{s,0}/B_{s,0}}(x) = (W^*(\chi_0)^4)_\ell$, and then put $t(\xi_0) = x$. The existence of such an x is clear because $A_{s,0}/B_{s,0}$ is unramified at ℓ).

Let C_ℓ be the unique subgroup of T with order ℓ. Then, by considering the quotient group Δ/C_ℓ and by arguing inductively on the group order of Δ, we may, if we wish, assume that we have values $t(\xi_0), \dots, t(\xi_{v-1})$ which satisfy properties (1) and (2) for $i < v$ and so that for some $\overline{w} \in \mathcal{O}_{K_\ell} \otimes \mathbf{Z}[\zeta_m]\,(C_{\ell v}/C_\ell)^*$

$$t(\xi_i) = \mathrm{Det}(\overline{w})(\xi_i)$$

for all $i < v$, where we view ξ_i as a character of T/C_ℓ in the natural way. Equivalently we can assume the existence of $\overline{z} \in \mathcal{O}(m)\,(C_{\ell v}/C_\ell)^*$, so that $t(\xi_i) = \varphi_i(\overline{z})$.

For any $x \in U(\overline{\mathbf{Q}}_\ell)$, we can write x uniquely in the form $x = x_{(1)} x_{(\ell)}$, where $x_{(\ell)} \equiv 1 \bmod \mathfrak{R}_\ell$ and where $x_{(1)}$ is of finite order prime to ℓ. For $t \in \mathrm{Hom}_{\Omega_K}(\mathrm{R}_m, \mathrm{U}(\mathbf{Q}_\ell))$ we have the corresponding decomposition $t = t_{(1)} t_{(\ell)}$. For brevity we will write $\mathrm{W}^*_{(\ell)}$ (resp. $\mathrm{W}^*_{(1)}$) in place of $(\mathrm{W}^*_\ell)_{(\ell)}$ (resp. $(\mathrm{W}^*_\ell)_{(1)}$). (As usual W^*_ℓ is the projection of the adjusted local root number homomorphism into $\mathrm{U}(\overline{\mathbf{Q}}_\ell)$).

The proof of Theorem 3 for the prime $\ell = 2$, whilst in many ways parallel to the case when ℓ is odd, is sufficiently singular to warrant special treatment. So, first we prove Theorem 3 when $\ell \neq 2$ and then, afterwards, we deal with the case $\ell = 2$.

Proof of Theorem 3 when $\ell \neq 2$. –

Step 1. In this first step, we establish the existence of the homomorphism $t_{(1)}$ required for Theorem 3.

Since $\mathrm{A}_0 = \mathrm{K}(m)$, from (5.1c) we know that $(\mathrm{A}_0)_\ell/(\mathrm{B}_0)_\ell$ is completely split, and so we have an isomomorphism of rings

$$(\mathrm{A}_0)_\ell \simeq \Pi\, (\mathrm{B}_0)_\ell \tag{5.2}$$

where we view $(\mathrm{B}_0)_\ell$ as being diagonally embedded in the right hand side. By Lemma 9 $\mathrm{W}^*(\chi_0)^2 \in \mathrm{B}_0$, and so, for each $\omega \in \Omega_\mathrm{K}$ and each i, $0 \leqslant i \leqslant v$, we define $t_{(1)}(\xi_i^\omega) \in (\mathrm{A}_0)_\ell$, so that under (5.2) $t_{(1)}(\xi_i^\omega) \longmapsto (\mathrm{W}^*_{(1)}(\chi_0)^4 \times 1 \ldots \times 1)^\omega$.

Note that if $\xi_i^\omega = \xi_i$, then ω fixes the whole of $\mathrm{A}_i (= \mathrm{K}(\xi_i))$ and hence ω fixes the subfield A_0. This then shows that each $t_{(1)}(\xi^\omega)$ is well-defined, and that $t_{(1)}(\xi^\omega) = t_{(1)}(\xi)^\omega$ for $\omega \in \Omega_\mathrm{K}$.

We must now show that $t_{(1)}$ satisfies the corresponding properties to (1), (2) and (3). Namely we must show:

For each i, $0 \leqslant i \leqslant v$

$$\mathrm{N}_{\mathrm{A}_i/\mathrm{B}_i}(t_{(1)}(\xi_i)) = (\mathrm{W}_{(1)}(\chi_i)^4)_\ell\,. \tag{1}$$

For $1 < i$

$$\mathrm{N}_{i/i-1}(t_{(1)}(\xi_i)) = t_{(1)}(\xi_{i-1})^{\mathrm{f}}\,, \tag{2}$$

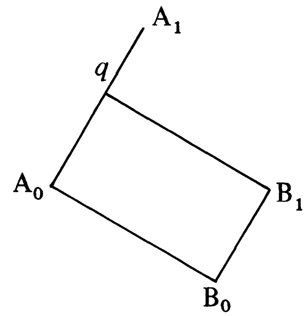
and

$$\mathrm{N}_{1/0}(t_{(1)}(\xi_1)) = t_{(1)}(\xi_0)^{\mathrm{f}-1}\,.$$

$$t_{(1)} \in \mathrm{Det}(\mathcal{O}_{\mathrm{K}_\ell} \otimes \mathbf{Z}[\zeta_m]\, \mathrm{C}^*_{\ell v})\,. \tag{3}$$

It is immediate from our definition of $t_{(1)}$ above that $t_{(1)} \doteq \mathrm{Det}(t_{(1)}(\xi_0))$. (By Lemma 9, $t_{(1)}(\xi_0) \in \mathcal{O}^*_{(\mathrm{A}_0)_\ell}$ and so we view $t_{(1)} \in \mathrm{Det}(\mathcal{O}_{K_\ell} \otimes \mathbf{Z}[\zeta_m]^*)$ as explained at the beginning of section 3). Now we must establish properties (1) and (2).

If $i = 1$, we have a diagram of fields



Recall that $q = (\mathrm{H}_0 : \mathrm{H}_1)$ and so

$$\begin{aligned} \mathrm{N}_{\mathrm{A}_1/\mathrm{B}_1}(t_{(1)}(\xi_1)) &= \mathrm{N}_{\mathrm{A}_0/\mathrm{B}_0}(t_{(1)}(\xi_0))^q \\ &= (\mathrm{W}^*_{(1)}(\chi_0)^{4q})_\ell \end{aligned}$$

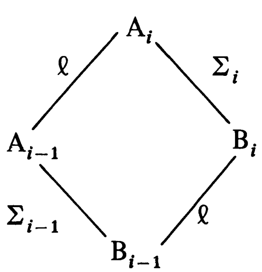
by Lemma 11 (i) $\qquad = (\mathrm{W}^*_{(1)}(\chi_1)^4)_\ell$.

Lastly, it is immediate that, since $t_{(1)}(\xi_1) = t_{(1)}(\xi_0)$,

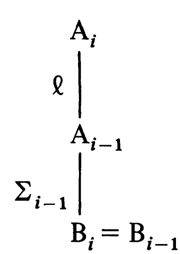
$$\mathrm{N}_{\mathrm{A}_1/\mathrm{A}_0}(t_{(1)}(\xi_1)) = t_{(1)}(\xi_0)^{\ell-1} = t_{(1)}(\xi)^{\mathfrak{f}-1} .$$

So now, we suppose that $i > 1$. By using Lemma 10, we see that, according as $v > r$, or, $v = r$, $(\mathrm{H}_{i-1} : \mathrm{H}_i) = \ell$, or, $\mathrm{H}_{i-1} = \mathrm{H}_i$. Thus we have a diagram of fields

If $\mathrm{H}_i = \mathrm{H}_{i-1}$



If $(\mathrm{H}_{i-1} : \mathrm{H}_i) = \ell$



If $\mathrm{H}_{i-1} = \mathrm{H}_i$

$$\mathrm{N}_{i/i-1}(t_{(1)}(\xi_i)) = t_{(1)}(\xi_i)^\ell = t_{(1)}(\xi_i)^{\mathfrak{f}} = t_{(1)}(\xi_{i-1})^{\mathfrak{f}} .$$

Hence, property (2) is established.

Inductively, we may suppose that

$$W^*_{(1)}(\chi_{i-1})^4 = N_{A_{i-1}/B_{i-1}}(t_{(1)}(\xi_{i-1})).$$

Since $t_{(1)}(\xi_i) = t_{(1)}(\xi_{i-1})$, $W^*_{(1)}(\chi_{i-1})^4 = N_{A_i/B_i}(t_{(1)}(\xi_i))$.

However, from Lemma 12 (i), we deduce that

$$W^*_{(1)}(\chi_{i-1})^{4f} = N_{i/i-1}(W^*_{(1)}(\chi_i)^4),$$

and so, by the total ramification of ℓ in A_i/A_{i-1},

$$= W^*_{(1)}(\chi_i)^{4\ell} = W^*_{(1)}(\chi_i)^{4f}.$$

Hence, we see that $W^*_{(1)}(\chi_i) = W^*_{(1)}(\chi_{i-1})$, and we obtain that

$$N_{A_i/B_i}(t_{(1)}(\xi_i)) = W^*_{(1)}(\chi_i)^4.$$

This now establishes property (1).

If $(H_{i-1} : H_i) = \ell$

That property (2) holds is proved in exactly the same way as above. To verify property (1) we may suppose, inductively, that

$$W^*_{(1)}(\chi_{i-1})^4 = N_{A_{i-1}/B_{i-1}}(t_{(1)}(\xi_{i-1})).$$

From the diagram of fields, using the fact that $t_{(1)}(\xi_i) = t_{(1)}(\xi_{i-1})$, we have

$$\begin{aligned} N_{A_i/B_i}(t_{(1)}(\xi_i)) &= N_{A_{i-1}/B_{i-1}}(t_{(1)}(\xi_{i-1}))^{\ell} \\ &= W^*_{(1)}(\chi_{i-1})^{4f} \\ \text{by Lemma 13 (i)} \qquad &= W^*_{(1)}(\chi_i)^4. \end{aligned}$$

This now completes step 1.

Step 2. In this step of the proof of Theorem 3, we establish the existence of homomorphism $t_{(\ell)}$, for the special case when $v = r$. So now we want to define $t_{(\ell)}(\xi_i)$, for $0 \leqslant i \leqslant v$, so that

$$N_{A_i/B_i}(t_{(\ell)}(\xi_i)) = W^*_{(\ell)}(\chi_i)^4 \tag{1}$$

$$N_{i/i-1}(t_{(\ell)}(\xi_i)) = t_{(\ell)}(\xi_{i-1})^{f} \quad \text{for} \quad i > 1, \tag{2}$$

and $N_{1/0}(t_{(\ell)}(\xi_1)) = t_{(\ell)}(\xi_0)^{f-1}$.

$$t_{(\ell)} \in \mathrm{Det}(\mathcal{O}_{K_\ell} \otimes \mathbf{Z}[\zeta_m]\, C^*_{\ell v}). \tag{3}$$

We remark that (3) automatically implies that $t_{(\ell)}$ commutes with Ω_K action.

Recall that $\mathcal{O}(m)$ denotes the integers of $K(m)_\ell$. We now make certain observations concerning the group ring $\mathcal{O}(m)\,C_{\ell^v}$. For any $z \in \mathcal{O}(m)\,C_{\ell^v}^*$, we can write z uniquely in the form $z = z_{(1)} z_{(\ell)}$, where $z_{(1)}$ has finite order prime to ℓ, and $z_{(\ell)}$ lies in the pro-ℓ-Sylow subgroup of $\mathcal{O}(m)\,C_{\ell^v}^*$. Because $q\,(=(H_0 : H_1))$ is prime to ℓ, raising to the q^{th} power yields an automorphism of this pro-ℓ-Sylow subgroup. We will denote the inverse of this automorphism by $z \longmapsto z^{q^{-1}}$.

The ring isomorphism $(A_0)_\ell \simeq \Pi\,(B_0)_\ell$ of (5.2) induces an isomorphism

$$(A_0)_\ell C_{\ell^v} \simeq \Pi\,(B_0)_\ell C_{\ell^v}\,. \tag{5.3}$$

Here, as usual, we regard $(B_0)_\ell C_{\ell^v}$ as being diagonally embedded in the right hand side. Suppose that under the composite homomorphism

$$\begin{array}{ccccc} K_\ell T & \xrightarrow{\xi'_m} & (A_0)_\ell C_{\ell^v} & \longrightarrow & \Pi\,(B_0)_\ell C_{\ell^v} \\ (\overline{T}\,T^{-1})_{(\ell)}^{2q^{-1}} & \longrightarrow & s & \longrightarrow & \prod_j s_j\,, \end{array} \tag{5.4}$$

where $T, \overline{T}$ are the elements given in Lemma 16 of section 4, and where we write $(\overline{T}\,T^{-1})_{(\ell)}$ in place of $((\overline{T}\,T^{-1})_\ell)_{(\ell)}$. Recall that ξ'_m is a faithful abelian character of $T' = C_m$, that φ_i is a certain abelian character of order ℓ^i on $T_\ell = C_{\ell^v}$, and $\xi_i = \xi'_m \otimes \varphi_i$ (cf. section 3).

For each i, we let $\check{\xi}_i$ denote an abelian character of H_i which extends the character ξ_i of T. Then

$$\varphi_i(s) = \xi_i((\overline{T}\,T^{-1})_{(\ell)}^{2q^{-1}}) = \check{\xi}_{i|H_v}((\overline{T}\,T^{-1})_{(\ell)}^{2q^{-1}}),$$

by Lemma 16 $\qquad = W_{(\ell)}^*(\check{\xi}_{i|H_v})^{4q^{-1}}\,.$

Next, observe that by Lemma 15

$$W_{(\ell)}^*(\check{\xi}_{i|H_v})^4 = W_{(\ell)}^*(\check{\xi}_i)^{4(H_i:H_v)},$$

by Lemma 14 $\qquad = W_{(\ell)}^*(\chi_i)^{4(H_i:H_v)}\,.$

Moreover, since we know $v = r$, $H_v = H_1$, and thus we have now shown

$$\varphi_i(s) = \begin{cases} W_{(\ell)}^*(\chi_0)^4 & \text{if } i = 0, \\ W_{(\ell)}^*(\chi_i)^{4q^{-1}} & \text{if } i > 0. \end{cases} \tag{5.5}$$

Originally, all we could say was that $s \in (\mathrm{A}_0)_{\mathfrak{Q}} \mathrm{C}^*_{\mathfrak{Q}^v}$. However, we have now shown that $\varphi_i(s) \in \mathrm{B}_0(\mathfrak{Q}^i)_{\mathfrak{Q}}$ for all i, $0 \leqslant i \leqslant v$ (since by Lemma 9, $\mathrm{W}^*(\chi_i)^2 \in \mathrm{B}_i \subset \mathrm{B}_0(\mathfrak{Q}^i)$). So we can deduce that in fact $s \in (\mathrm{B}_0)_{\mathfrak{Q}} \mathrm{C}_{\mathfrak{Q}^v}$ (cf. 1.5 of [17]). This then implies that, in (5.4), the s_j are all equal. For $\omega \in \Omega_{\mathrm{K}}$, we define $t_{(\mathfrak{Q})}(\xi_i^{\omega})$ in $(\mathrm{A}_i)_{\mathfrak{Q}}$, so that under the isomorphism induced by (5.3)

$$t_{(\mathfrak{Q})}(\xi_i^{\omega}) \longmapsto (\varphi_i(s_1) \times 1 \ldots \times 1). \tag{5.6}$$

It then follows immediately that $t_{(\mathfrak{Q})} \in \mathrm{Det}(\mathcal{O}_{\mathrm{K}_{\mathfrak{Q}}} \otimes \mathbf{Z}[\zeta_m]\, \mathrm{C}^*_{\mathfrak{Q}^v})$, and so property (3) holds.

Now we consider $\mathrm{N}_{\mathrm{A}_i/\mathrm{B}_i}(t_{(\mathfrak{Q})}(\xi_i))$, in order to establish property (1). We let G_i be the subfield of A_i fixed by the Galois group $\mathrm{H}_0/\mathrm{H}_i (\subset \Sigma_i)$. Because $v = r$, we know that $\mathrm{H}_v = \mathrm{H}_1$, and so we obtain a diagram of fields

$$\begin{tikzcd}
 & \mathrm{A}_i \arrow[dl, dash] \arrow[dr, dash, "q"] & & \\
\mathrm{A}_1 \arrow[dr, dash, "q"'] & & \mathrm{G}_i \arrow[dl, dash] \arrow[dr, dash] & \\
 & \mathrm{G}_1 \arrow[dl, dash] \arrow[dr, dash] & & \mathrm{B}_i \arrow[dl, dash] \\
\mathrm{G}_0 = \mathrm{A}_0 \arrow[dr, dash, "\Sigma_0"'] & & \mathrm{B}_1 & \\
 & \mathrm{B}_0 \arrow[ur, dash] & &
\end{tikzcd}$$

In particular $\mathfrak{Q}$ is totally ramified in $\mathrm{A}_i/\mathrm{G}_i$ and, by (5.1c), $\mathfrak{Q}$ is completely split in $\mathrm{G}_i/\mathrm{B}_i$. Thus, with abuse of notation,

$$\mathrm{N}_{\mathrm{A}_i/\mathrm{B}_i}(t_{(\mathfrak{Q})}(\xi_i)) = \mathrm{N}_{\mathrm{G}_i/\mathrm{B}_i}(\mathrm{N}_{\mathrm{A}_i/\mathrm{G}_i}(\varphi_i(s_1)) \times 1 \ldots \times 1) = \mathrm{N}_{\mathrm{A}_i/\mathrm{G}_i}(\varphi_i(s_1)).$$

However, by (5.5) and using the fact that, from Lemma 9, $\mathrm{W}^*(\chi_i)^2 \in \mathrm{B}_i$, we deduce $\mathrm{N}_{\mathrm{A}_i/\mathrm{B}_i}(t_{(\mathfrak{Q})}(\xi_i)) = \mathrm{W}^*_{(\mathfrak{Q})}(\chi_i)^4$, for all i, $0 \leqslant i \leqslant v$. This then establishes property (2).

We now consider property (1). From (5.5) and (5.6) we obtain

$$t_{(\mathfrak{Q})}(\xi_i) = \begin{cases} \mathrm{W}^*_{(\mathfrak{Q})}(\chi_0)^4 \times 1 \ldots \times 1 & \text{if } i = 0, \\ \mathrm{W}^*_{(\mathfrak{Q})}(\chi_i)^{4q^{-1}} \times 1 \ldots \times 1 & \text{if } i > 0. \end{cases} \tag{5.7}$$

Suppose first that $i = 1$. Then, by Lemma 11 (i),

$$\mathrm{N}_{\mathrm{B}_1/\mathrm{B}_0}(\mathrm{W}^*_{(\ell)}(\chi_1)^4) = \mathrm{W}^*_{(\ell)}(\chi_0)^{4(\mathrm{f}-1)}$$

so that

$$\mathrm{N}_{1/0}(\mathrm{W}^*_{(\ell)}(\chi_1)^4) = \mathrm{W}^*_{(\ell)}(\chi_0)^{4q(\mathrm{f}-1)}.$$

Hence, by (5.7), $\mathrm{N}_{1/0}(t_{(\ell)}(\xi_1)) = t_{(\ell)}(\xi_0)^{\mathrm{f}-1}$.

So now we suppose that $i > 1$. Again from Lemma 12 (i)

$$\mathrm{N}_{i/i-1}(\mathrm{W}^*_{(\ell)}(\chi_i)^4) = \mathrm{W}^*_{(\ell)}(\chi_{i-1})^{4\mathrm{f}},$$

and so by (5.7)

$$\mathrm{N}_{i/i-1}(t_{(\ell)}(\xi_i)) = t_{(\ell)}(\xi_{i-1})^{\mathrm{f}}$$

which completes step 2.

Step 3. In this, the last step in the proof of Theorem 3, we establish the existence of the homomorphism $t_{(\ell)}$, for the case when $v > r$.

As explained earlier, we may assume inductively that

$$t_{(\ell)}(\xi_0), \ldots, t_{(\ell)}(\xi_{v-1})$$

are already defined and that there exists $\bar{z} \in \mathcal{O}_{\mathrm{K}(m)_\ell}(\mathrm{C}_{\ell^v}/\mathrm{C}_\ell)^*$ so that $t_{(\ell)}(\xi_i) = \varphi_i(\bar{z})$. We must find $t_{(\ell)}(\xi_v)$ such that (1) and (2) hold at $i = v$, and so that (3) holds. As previous, we know we have a diagram of fields

$$\begin{array}{c} \mathrm{A}_v \\ | \\ \mathrm{A}_{v-1} \\ | \\ \mathrm{B}_{v-1} = \mathrm{B}_v . \end{array}$$

(5.8) First we show that if property (2) holds for $i = v$, then, necessarily, property (1) must hold for $i = v$. Clearly

$$\mathrm{N}_{\mathrm{A}_v/\mathrm{B}_v}(t_{(\ell)}(\xi_v)) = \mathrm{N}_{\mathrm{A}_{v-1}/\mathrm{B}_{v-1}}(\mathrm{N}_{i/i-1}(t_{(\ell)}(\xi_v)))$$

further, as property (2) holds by hypothesis,

$$= \mathrm{N}_{\mathrm{A}_{v-1}/\mathrm{B}_{v-1}}(t_{(\ell)}(\xi_{v-1})^{\mathrm{f}})$$

by our induction hypothesis

$$= \mathrm{W}^*_{(\ell)}(\chi_{v-1})^{4\mathrm{f}}$$

from Lemma 13 (i) $\quad = W^*_{(\ell)}(\chi_v)$

as is required.

By enlarging K if necessary (preserving (5.1a) and (5.1b)), it is clear that we can find $x \in (A_v)_\ell$ so that

$$N_{v/v-1}(x) = t_{(\ell)}(\xi_{v-1})^{\mathrm{f}}. \tag{5.9}$$

Our aim is to find such an x with the additional property that there exists $z \in \mathcal{O}(m)\, C^*_{\ell^v}$ so that

$$z \longmapsto \bar{z} \text{ under } \mathcal{O}(m)\, C^*_{\ell^v} \longrightarrow \mathcal{O}(m)\,(C_{\ell^v}/C_\ell)^*, \tag{5.10a}$$

$$\varphi_v(z) = x. \tag{5.10b}$$

(For then we can set $t_{(\ell)}(\xi_v) = x$ and we are done).

Using the results of section 3, we now find such an x. We pick any $z \in \mathcal{O}(m)\, C^*_{\ell^v}$ so that $z \longmapsto \bar{z}$, under the quotient homomorphism. We know from property (2) of $t_{(\ell)}$ that

$$S^0_{i-1}(t_{(\ell)}) = 1 \quad \text{for all} \quad i < v, \tag{5.11}$$

consequently, by (5.10a),

$$S^0_{i-1}(\mathrm{Det}(z)) = 1 \quad \text{for all} \quad i < v. \tag{5.12}$$

Thus, as $v > r \geqslant 1$, from Lemma 5 of section 3 we have

$$S^0_{v-1}(\mathrm{Det}(z)) \in 1 + \ell(1 - \zeta_\ell)\, \mathcal{O}(m\ell^{v-1}). \tag{5.13}$$

So, from (5.10a) and (5.9)

$$\begin{aligned} S^0_{v-1}(\mathrm{Det}(z)) &= S^0_{v-1}(\mathrm{Det}(z)) \,.\, N_{v/v-1}(x)^{-1}\, t_{(\ell)}(\xi_{v-1})^{\mathrm{f}} \\ &= N_{v/v-1}(\varphi_v(z)) \,.\, \varphi_{v-1}(z)^{-\mathrm{f}} \,.\, N_{v/v-1}(x^{-1}) \,.\, t_{(\ell)}(\xi_{v-1})^{\mathrm{f}} \\ &= N_{v/v-1}(\varphi_v(z)\, x^{-1}). \end{aligned}$$

Whence, by (5.13), we obtain that

$$N_{v/v-1}(\varphi_v(z)\, x^{-1}) \in 1 + \ell(1 - \zeta_\ell)\, \mathcal{O}(m\ell^{v-1}).$$

However, by Lemma 6 of section 3, we see that, after multiplying x by an element of $\mathrm{Ker}(N_{v/v-1})$ (which, of course, still preserves (5.9)), we may assume that $\varphi_v(z)\, x^{-1} \in 1 + (1 - \zeta_\ell)\, \mathcal{O}(m\ell^v)$. So now, if c generates C_{ℓ^v}, we may choose

$$z' \in 1 + (1 - c^{\ell^{v-1}})\, \mathcal{O}(m)\, C_{\ell^v},$$

so that $\varphi_v(z') = \varphi_v(z^{-1})\, x$.

Then, trivially, $\varphi_i(z') = 1$, for all $i < v$, and so we obtain

$$\varphi_i(zz') = \begin{cases} x & \text{if } i = v, \\ t_\ell(\xi_i) & \text{if } i < v. \end{cases}$$

It is now immediate that if, for $\omega \in \Omega_K$, we put $t_{(\ell)}(\xi_v^\omega) = x^\omega$, then $t_{(\ell)} \in \mathrm{Det}(\mathcal{O}_{K_\ell} \otimes \mathbf{Z}[\zeta_m]\, C^*_{\ell v})$. Further, by (5.9), $t_{(\ell)}$ satisfies property (2), and whence, by (5.8), also property (1). This then completes our proof of Theorem 3 when $\ell \neq 2$.

Proof of Theorem 3 when $\ell = 2$. –

Step 1. Again, in this the first step, we establish the existence of the homomorphism $t_{(1)}$. As for the case $\ell \neq 2$, we define $t_{(1)}(\xi_i^\omega) \in (A_0)_2$ for all i, $0 \leqslant i \leqslant v$, so that under the isomorphism (5.2), $t_{(1)}(\xi_i^\omega) \mapsto (W^*_{(1)}(\chi_0)^4 \times 1 \ldots \times 1)^\omega$.

As before, we are required to show that $t_{(1)}$ satisfies properties (1), (2) and (3). The proof that they are satisfied is entirely analagous to the case $\ell \neq 2$, and so is omitted.

Step. 2. In this step we establish the existence of $t_{(2)}$ when $v = u$. The proof for this case is in someways similar to step 2 when $\ell \neq 2$. We recall that our aim is to find $t_{(2)}$ so that (1), (2) and (3) hold (as listed in step (2) when $\ell \neq 2$).

We define $\delta = 2\,(H_0 : H_v)^{-1}$ ($\geqslant 1$!). We suppose that under the composite homomorphism

(5.13) $K_2 T \xrightarrow{\xi'_m} (A_0)_2 C_{2^v} \xrightarrow{\sim} \Pi (B_0)_2 C_{2^v}$

$(\overline{T}\, T^{-1})^\delta_{(2)} \longrightarrow S \longrightarrow \Pi S_j$.

Here T, $\overline{T}$ are the elements given in Lemma 16 and we write $(\overline{T}\, T^{-1})_{(2)}$ in place of $((\overline{T}\, T^{-1})_2)_{(2)}$.

Again, $\check{\xi}_i$ denotes an abelian character of H_i which extends ξ_i. Then

$$\varphi_i(S) = \xi_i((\overline{T}\, T^{-1})^\delta_{(2)}) = \check{\xi}_{i|H_v}((\overline{T}\, T^{-1})^\delta_{(2)})$$

which by Lemma 16

$$= W^*_{(2)}(\check{\xi}_{i|H_v})^{2\delta}$$

and from Lemma 15

$$W^*(\check{\xi}_{i|H_v})^2 = W^*(\check{\xi}_i)^{2(H_i : H_v)}.$$

So, by Lemma 14, we obtain

$$W^*(\check{\xi}_{i|H_v})^2 = W^*(\chi_i)^{4(H_0:H_i)^{-1}} .$$

Thus we have shown that

$$\varphi_i(S) = W^*_{(2)}(\chi_i)^{4(H_0:H_i)^{-1}} . \tag{5.14}$$

Originally we only knew that $S \in (A_0)_2 C^*_{2^v}$, but now we have shown that $\varphi_i(S) \in (B_0(2^i))_2$ for all i, $0 \leqslant i \leqslant v$ (since, by Lemma 9, $W^*(\chi_i)^2 \in B_i \subset B_0(2^i))$. Thus we may deduce that in fact $S \in (B_0)_2 C^*_{2^v}$ (cf. [17]), and consequently, in (5.13), all the S_j are equal.

For $\omega \in \Omega_K$, we define $t_{(2)}(\xi_i^\omega) \in (A_i)_2$, so that under the isomorphism induced by (5.13),

$$t_{(2)}(\xi_i^\omega) = (\varphi_i(S) \times 1 \ldots \times 1)^\omega . \tag{5.15}$$

It is immediate that $t_{(2)} \in \mathrm{Det}(\mathcal{O}_{K_2} \otimes \mathbf{Z}[\zeta_m]\, C^*_{2^v})$, so that property (3) holds. Now we consider $N_{A_i/B_i}(t_{(2)}(\xi_i))$, in order to establish property (1).

Let G_i be the subfield of A_i which is fixed by the Galois group H_0/H_i. Then G_i is the maximal subextension of A_i, containing B_i, which is unramified at ℓ, and we have a diagram of fields

$$\begin{tikzcd}[column sep=small]
 & A_i \arrow[d, dash, "(H_0:H_i)"] & \\
 & G_i \arrow[dl, dash] \arrow[dr, dash] & \\
A_0 \arrow[dr, dash] & & B_i \arrow[dl, dash] \\
 & B_0 &
\end{tikzcd}$$

With abuse of notation we have,

$$\begin{aligned} N_{A_i/B_i}(t_{(2)}(\xi_i)) &= N_{G_i/B_i}(N_{A_i/G_i}(\varphi_i(S)) \times 1 \ldots \times 1) \\ &= N_{A_i/G_i}(\varphi_i(S)) \end{aligned}$$

by (5.14) $$= W^*_{(2)}(\chi_i)^4 ,$$

since, by Lemma 9, $W^*(\chi_i)^2 \in B_i$.

This establishes property (1). We now show property (2). Suppose first that $i = 1$. Then, because a cyclic group of order two has trivial automorphism group, $H_0 = H_1$, and so from Lemma 11 (ii),

$$W^*_{(2)}(\chi_1)^4 = W^*_{(2)}(\chi_0)^{4(\mathrm{f}-1)}.$$

By (5.14) and (5.15) we obtain $t_{(2)}(\xi_1) = t_{(2)}(\xi_0)^{\mathrm{f}-1}$, as is required.

Secondly, we suppose that $i > 1$ and that $H_i = H_{i-1}$. Then, from Lemma 12 (ii), $N_{i/i-1}(W^*_{(2)}(\chi_i)^4) = W^*_{(2)}(\chi_{i-1})^{4\mathrm{f}}$. Further, by the same lemma, we know that if $(H_0 : H_i) > 1$ (i.e. if $(H_0 : H_i) = 2$ since by hypothesis $v = u$), then $N_{i/i-1}(W^*_{(2)}(\chi_i)^2) = W^*_{(2)}(\chi_{i-1})^{2\mathrm{f}}$.

Thus, by (5.14) and (5.15), we see that, regardless of whether $H_0 = H_i$, or, $(H_0 : H_i) = 2$, $N_{i/i-1}(t_{(2)}(\xi_i)) = t_{(2)}(\xi_{i-1})^{\mathrm{f}}$ as is required.

Lastly, we suppose that $(H_{i-1} : H_i) = 2$. From Lemma 13 (ii)

$$W^*_{(2)}(\chi_i)^4 = W^*_{(2)}(\chi_{i-1})^{4\mathrm{f}}, \tag{5.16}$$

and so, by (5.14) and (5.15), using the fact that $(H_0 : H_i) = 2$,

$$N_{i/i-1}(t_{(2)}(\xi_i)) = N_{i/i-1}(W^*_2(\chi_i)^2 \times 1 \ldots \times 1).$$

However, as $(H_{i-1} : H_i) = 2$, it is clear that $B_i = B_{i-1}$, and so, by Lemma 9 ,

$$N_{i/i-1}(t_{(2)}(\xi_i)) = (W^*_{(2)}(\chi_i)^4 \times 1 \ldots \times 1)$$

by (5.16)

$$= (W^*_{(2)}(\chi_{i-1})^{4\mathrm{f}} \times 1 \ldots \times 1).$$

Moreover, because $v = u$, we must have that $(H_0 : H_{i-1}) = 1$ and so, by (5.14) and (5.15), we obtain $N_{i/i-1}(t_{(2)}(\xi_i)) = t_{(2)}(\xi_{i-1})^{\mathrm{f}}$.

This now establishes property (2) and so completes our proof of step (2).

Step 3. In this the last step we are required to establish the existence of $t_{(2)}$ when $v > u$. The proof is exactly the same as in step (3) for the case when ℓ is odd, and so the details are omitted.

6. Proofs of Lemmas.

In this section we give proofs of Lemmas 11 to 16. We start by proving Lemma 14.

Proof of Lemma 14. – By the transitivity of induction, we can, without loss of generality, assume that $(\Psi : \Phi)$ is a prime number, and by linearity we can assume that φ is irreducible. From the inductivity of local root numbers on degree zero virtual characters, we derive that $W(\mathrm{Ind}_\Phi^\Psi(\varphi))\, W(\rho_{\Psi/\Phi})^{-\varphi(1)} = W(\varphi)$, where $\rho_{\Psi/\Phi}$ is the regular character of the quotient group Ψ/Φ inflated to Ψ.

In case (i) of the lemma, by pairing conjugate characters, we may deduce that $W(\rho_{\Psi/\Phi})$ is ± 1 (cf. Corollary 1 to Theorem 1 in [14]).

In case (ii), we let α be the unique ramified abelian character of E_q^Φ/E_q^Ψ. Then $W(\rho_{\Psi/\Phi}) = W(\alpha)$, and from Corollary 1 to Theorem 1 in [14] $W(\alpha)^2 = \alpha(-1) = (-1)^{\frac{NP-1}{2}}$.

So now it is sufficient to show that when $(\Psi : \Phi)$ is prime and Φ is normal in Ψ, $y_\Psi(\mathrm{Ind}_\Phi^\Psi(\varphi))^2 = y_\Phi(\varphi)^2$. We prove this result by considering the possible different cases.

Let D_Ψ (resp. D_Φ) denote the different of E_q^Ψ (resp. E_q^Φ) and let P (resp. Q) be the maximal ideal of the ring of integers of E_q^Ψ (resp. E_q^Φ).

1) *Suppose φ is genuinely ramified.* – Then, as all the irreducible characters in $\mathrm{Ind}_\Phi^\Psi(\varphi)$ are genuinely ramified, we obtain

$$\begin{aligned} y_\Psi(\mathrm{Ind}_\Phi^\Psi(\varphi))^2 &= \det(\mathrm{Ind}_\Phi^\Psi(\varphi))\,(c^2), \\ &= V_\Phi^\Psi \varphi(c^2), \\ \text{by local class field theory} \qquad &= \varphi(c^2) = y_\Phi(\varphi)^2 . \end{aligned}$$

2) *Suppose φ is unramified with E_q^Φ/E_q^Ψ unramified.* – Then all the irreducible characters occuring in $\mathrm{Ind}_\Phi^\Psi(\varphi)$ are unramified and so

$$y_\Psi(\mathrm{Ind}_\Phi^\Psi(\varphi))^2 = \det(\mathrm{Ind}_\Phi^\Psi(\varphi))\,(D_\Psi)^2 = V_\Phi^\Psi\varphi(D_\Psi)^2,$$

by local class field theory $= \varphi(D_\Phi)^2 = y_\Phi(\varphi)^2$.

3) *Suppose φ is unramified with E_q^Φ/E_q^Ψ totally ramified.* – Let φ' be the unique unramified abelian character of Ψ which extends φ. First we consider the decomposition of the character $\mathrm{Ind}_\Phi^\Psi(\epsilon_\Phi)$. We may write $\mathrm{Ind}_\Phi^\Psi(\epsilon_\Phi) = \epsilon_\Psi + \sum_i n_i\theta_i$ with the θ_i distinct irreducible characters and with $n_i > 0$. By Frobenius reciprocity,

$(\epsilon_\Psi, \mathrm{Ind}_\Phi^\Psi(\epsilon_\Phi)) = 1$, so that $\theta_i \neq \epsilon_\Psi$ for each i. However, by Mackey's restriction theorem, $\mathrm{Ind}_\Phi^\Psi(\epsilon_\Phi)|_T$ is just the regular character of the unique quotient of T with order ℓ. Hence, all the θ_i are genuinely ramified. By a further application of Frobenius reciprocity we have $\mathrm{Ind}_\Phi^\Psi(\varphi) = \varphi \cdot \mathrm{Ind}_\Phi^\Psi(\epsilon_\Phi) = \varphi' + \Sigma\, n_i \varphi' \cdot \theta_i$, and, as φ' is unramified and abelian, the $\varphi'\theta_i$ are all genuinely ramified and irreducible. Thus,

$$\begin{aligned} y(\mathrm{Ind}_\Phi^\Psi(\varphi))^2 &= \varphi'(\mathrm{D}_\Psi)^2 \prod_i \det_{n_i\theta_i\varphi'}(c^2) \\ &= \varphi'(\mathrm{D}_\Psi)^2 \det_{\mathrm{Ind}_\Phi^\Psi(\varphi)}(c^2) \cdot \varphi'(c^{-2}) \\ &= \varphi'(\mathrm{P})^{-2}\, \mathrm{V}_\Phi^\Psi \varphi(c^2). \end{aligned}$$

But, by local class field theory, $\mathrm{V}_\Phi^\Psi \varphi(c^2) = \varphi(c^2)$ and $\varphi'(\mathrm{P}) = \varphi$ (Norm P) $= \varphi(\mathrm{Q})$, (since $\varphi'|_\Phi = \varphi$). Thus we obtain

$$y(\mathrm{Ind}_\Phi^\Psi(\varphi))^2 = \varphi(c\mathrm{Q}^{-1})^2 = \varphi(\mathrm{D}_\Phi)^2 = y(\varphi)^2$$

as we require.

Proof of Lemma 15. – We follow the proof given in § 5 of [2]. By Lemma 14, we know that $\mathrm{W}^*(\psi_{|\Phi})^2 = \mathrm{W}^*(\mathrm{Ind}_\Phi^\Psi(\psi_{|\Phi}))^2$. However, $\mathrm{Ind}_\Phi^\Psi(\psi_{|\Phi})$ splits up into a sum of $(\Psi : \Phi)$ distinct abelian characters, all of which differ from ψ only by a multiple of an unramified abelian character. The result then follows by Lemma 8.

LEMMA 17. – *Let* ξ_i *be the abelian character of* T *defined previously. Let* $\Phi \subset \Psi \subset \Delta$ *with* $(\Psi : \Phi) = \ell$ *and with* $\mathrm{E}_\mathfrak{q}^\Phi/\mathrm{E}_\mathfrak{q}^\Psi$ *totally ramified. Suppose that* $\xi_{i|\mathrm{T}\cap\Phi}$ *extends to an abelian character* λ_i *of* Φ. *Then, if* $i \geqslant 1$, $\xi_{i-1|\mathrm{T}\cap\Psi}$ *extends to an abelian character* μ_{i-1} *of* Ψ *(resp. if* $i = 0$, *then* $\xi_{0|\mathrm{T}\cap\Psi}$ *extends to an abelian character* μ_{-1} *of* Ψ*) and* $\mathrm{W}^*(\lambda_i)^2 = \mathrm{W}^*(\mu_{i-1})^{2\mathrm{f}}$.

Proof. – We may suppose that λ_i is ramified, otherwise the result is immediate. Let Q (resp. P) be the maximal ideal of the ring of integers of $\mathrm{E}_\mathfrak{q}^\Phi$ (resp. $\mathrm{E}_\mathfrak{q}^\Psi$). Then

$$\mathrm{W}^*(\lambda_i) = \mathrm{NQ}^{-1/2}\, \Sigma\, \lambda_i(u)\, \psi_\Psi(uc^{-1})$$

where u is summed through the units of $\mathrm{E}_\mathfrak{q}^\Phi$ mod Q. However, as $\mathrm{E}_\mathfrak{q}^\Phi/\mathrm{E}_\mathfrak{q}^\Psi$ is totally ramified, we can choose u to be a set of representatives of the units of $\mathrm{E}_\mathfrak{q}^\Psi$ mod P. So, by local class field theory,

$$\begin{aligned} W^*(\lambda_i)^2 &= NP^{-1}(\Sigma\, V_\Phi^\Psi \lambda_i(u)\, \psi_\Psi(\ell u c^{-1}))^2 \\ &= NP^{-1}(\Sigma\, V_\Phi^\Psi \lambda_i^{f^{-1}}(u)\, \psi_\Psi(u c^{-1}))^{2f} \\ &= W^*(V_\Phi^\Psi \lambda_i^{f^{-1}})^{2f}\,. \end{aligned}$$

So, it is sufficient to show that ξ_{i-1} and $V_\Phi^\Psi \lambda_i^{f^{-1}}$ agree on $T \cap \Psi$. For brevity, we put $\Psi' = \Psi \cap T$, $\Phi' = \Phi \cap T$.

Because $(\Psi : \Phi) = (\Psi' : \Phi') = \ell$, we see that for $\sigma \in \Psi'$ $V_\Phi^\Psi \lambda_i(\sigma) = V_{\Phi'}^{\Psi'}(\lambda_{i|\Phi'})(\sigma)$ and, because Ψ' is abelian,

$$V_\Phi^\Psi \lambda_i(\sigma) = \lambda_i(\sigma^\ell) = \xi_i(\sigma^\ell) = \xi_{i-1}^f(\sigma)$$

as is required.

In proving the next three lemmas, we shall suppose that the group extension

$$1 \longrightarrow T \longrightarrow \Delta \longrightarrow \Xi \longrightarrow 1 \tag{6.1}$$

is split. There is no loss of generality in making this assumption. For, if the extension is not split, we can find a tame extension $J \supset E_q \supset F_\mathfrak{p}$ with $\mathrm{Gal}(J/F_\mathfrak{p}) = \overline{\Delta}$, where $\overline{\Delta}$ is split with respect to the corresponding exact sequence, and where the extension J/E_q is unramified. We would then prove the corresponding results for $J/F_\mathfrak{p}$ and use the fact that W^* is inflative, so long as W_Δ^* and $W_{\overline{\Delta}}^*$ are obtained from W_Δ and $W_{\overline{\Delta}}$ by the same $c \in F_\mathfrak{p}^*$. So now we choose θ in Δ so that $\Delta = \langle \theta, T \rangle$ and $\langle \theta \rangle \cap T = \{1\}$. It will be convenient to always choose our abelian character $\check{\xi}_i$ of H_i, which extends ξ_i, to be trivial on $\theta^{(\Delta:H_i)}$. Then $\check{\xi}_i$ is uniquely defined.

Proof of Lemma 11. – We firstly show that

$$W^*(\chi_1)^2 \equiv W^*(\chi_0)^{2(H_0:H_1)} \bmod \mathfrak{R}_\ell\,.$$

We know that $\chi_i = \mathrm{Ind}_{H_i}^\Delta(\check{\xi}_i)$ for $i = 0, 1$, and from Lemma 11.1 of [3] (or, by straight-forward computation), because $\check{\xi}_{0|H_1} \equiv \check{\xi}_1 \bmod \mathfrak{R}_\ell$,

$$W^*(\mathrm{Ind}_{H_1}^\Delta(\check{\xi}_{0|H_1} - \check{\xi}_1))^2 = W^*(\check{\xi}_{0|H_1} - \check{\xi}_1)^2 \equiv 1 \bmod \mathfrak{R}_\ell\,.$$

Now we observe that, by Lemma 15

$$W^*(\mathrm{Ind}_{H_1}^\Delta(\check{\xi}_{0|H_1}))^2 = W^*(\check{\xi}_{0|H_1})^2 = W^*(\check{\xi}_0)^{2(H_0:H_1)} = W^*(\chi_0)^{2(H_0:H_1)}\,.$$

Let T^{ℓ} denote the subgroup of T formed by the ℓ^{th} powers of elements in T, and put $P = \langle \theta^{(\Delta:H_0)}, T^{\ell} \rangle$. Then, by Lemma 14, $W^*(\mathrm{Ind}_P^{\Delta}(\check{\xi}_{0|P}))^4 = W^*(\check{\xi}_{0|P})^4$ and, by Lemma 17, on putting $\Psi = H_0$, $\Phi = P$, $\lambda_0 = \check{\xi}_{0|P}$, $\mu_{-1} = \check{\xi}_0$, we obtain

$$W^*(\check{\xi}_{0|P})^4 = W^*(\check{\xi}_0)^{4f} = W^*(\chi_0)^{4f}. \tag{6.2}$$

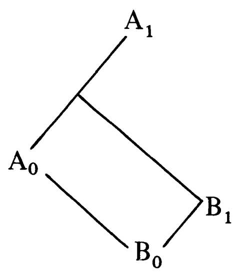
On the other hand, we claim that,

$$\mathrm{Ind}_P^{\Delta}(\check{\xi}_{0|P}) = \chi_0 + \sum_{\omega} \chi_1^{\omega} \tag{6.3}$$

where ω is summed through $\mathrm{Gal}(B_1/B_0)$. Clearly to show (6.3), it is enough to establish

$$\mathrm{Ind}_P^{H_0}(\check{\xi}_{0|P}) = \check{\xi}_0 + \sum_{\omega} \mathrm{Ind}_{H_1}^{H_0}(\check{\xi}_1^{\omega}). \tag{6.4}$$

We know by Frobenius reciprocity that $(\mathrm{Ind}_P^{H_0}(\check{\xi}_{0|P}), \check{\xi}_0) = 1$. Moreover, because H_0/H_1 identifies as the Galois group of A_1/B_1A_0,



we see that the various $\mathrm{Ind}_{H_1}^{H_0}(\check{\xi}_1^{\omega})$, for $\omega \in \mathrm{Gal}(B_1/B_0)$, are all irreducible and distinct. Also, for each such ω, by a double application of Frobenius reciprocity,

$$(\mathrm{Ind}_P^{H_0}(\check{\xi}_{0|P}), \mathrm{Ind}_{H_1}^{H_0}(\check{\xi}_1^{\omega})) = (\check{\xi}_{0|P\cap H_1}, \check{\xi}^{\omega}_{1|P\cap H_1}) = 1.$$

Thus, by counting degrees, (6.4), and whence (6.3), is established. So now we have

$$\begin{aligned} W^*(\mathrm{Ind}_P^{\Delta}(\xi_{0|P}))^4 &= W^*(\chi_0)^4 \prod_{\omega} W^*(\chi_1^{\omega})^4 \\ &= W^*(\chi_0)\, N_{B_1/B_0}(W^*(\chi_1)^4) \end{aligned}$$

since, by Lemma 9, for such ω, $W^*(\chi_1^{\omega})^2 = W^*(\chi_1)^{2\omega}$. From this, together with (6.2), we obtain,

$$N_{B_1/B_0}(W^*(\chi_1))^4 = W^*(\chi_0)^{4(f-1)}.$$

Proof of Lemma 12. – By hypothesis $H_i = H_{i-1}$. We put $P = \langle \theta^{(\Delta:H_i)}, T^{\ell} \rangle$. From Lemma 14 we know that

$$W^*(\check{\xi}_{i|P})^4 = W^*(\mathrm{Ind}_P^{H_i}(\check{\xi}_{i|P}))^4$$

and, by Frobenius reciprocity, it is easily seen that

$$\mathrm{Ind}_P^{H_i}(\check{\xi}_{i|P}) = \sum_{\omega \in \mathrm{Gal}(A_i/A_{i-1})} \check{\xi}_i^{\omega}.$$

However, by Lemma 9, we know that for such ω,

$$W^*(\check{\xi}_i^{\omega})^2 = W^*(\check{\xi}_i)^{2\omega},$$

and so we deduce that

$$W^*(\check{\xi}_{i|P})^4 = N_{i/i-1}(W^*(\check{\xi}_i)^4)$$

which by Lemma 14

$$= N_{i/i-1}(W^*(\chi_i)^4).$$

Moreover, we remark that if $\ell = 2$ and $(H_0 : H_1) > 1$, then the absolute norm of the maximal ideal of the ring of integers of $E_q^{H_i}$ is congruent to 1 mod (4) (because it is a square). So, using Lemma 14 (ii) and arguing as above, we may derive that,

$$W^*(\check{\xi}_{i|P})^2 = N_{i/i-1}(W^*(\chi_i)^2).$$

On the other hand, applying Lemma 17, putting $\Psi = H_i$, $\Phi = P$, $\mu_{i-1} = \check{\xi}_{i-1}$, $\lambda_i = \check{\xi}_{i|P}$, we obtain $W^*(\check{\xi}_{i|P})^2 = W^*(\check{\xi}_{i-1})^{2f}$.

Because $H_i = H_{i-1}$, applying Lemma 14 we obtain,

$$W^*(\check{\xi}_{i|P})^2 = W^*(\chi_{i-1})^{2f}.$$

Thus we have now shown that $N_{i/i-1}(W^*(\chi_i)^4) = W^*(\chi_{i-1})^{4f}$. Moreover, if $\ell = 2$ with $(H_0 : H_i) = 2$, then we have shown $N_{i/i-1}(W^*(\chi_i)^2) = W^*(\chi_{i-1})^{2f}$.

Proof of Lemma 13. – We put $P = \langle \theta^{(\Delta:H_{i-1})}, T^{\ell} \rangle$ and we let let η_i be an abelian character of P which extends $\check{\xi}_{i|H_i \cap P}$. (Such a character exists because H_{i-1} acts trivially on ξ_{i-1}, and whence trivially on $\xi_{i|T^{\ell}}$). By a double application of Frobenius reciprocity, we obtain that

$$(\mathrm{Ind}_P^{H_{i-1}}(\eta_i), \mathrm{Ind}_{H_i}^{H_{i-1}}(\check{\xi}_i)) = (\eta_{i|P\cap H_i}, \xi_{i|P\cap H_i}) = 1.$$

But $\mathrm{Ind}_{H_i}^{H_{i-1}}(\check{\xi}_i)$ is irreducible, and so, because both characters in the left hand side of (6.5) have the same degree (namely ℓ), we deduce that $\mathrm{Ind}_{\mathrm{P}}^{\mathrm{H}_{i-1}}(\eta_i) = \mathrm{Ind}_{\mathrm{H}_i}^{\mathrm{H}_{i-1}}(\check{\xi}_i)$. Hence $\chi_i = \mathrm{Ind}_{\mathrm{P}}^{\Delta}(\eta_i)$, and of course, as usual, we know that $\chi_k = \mathrm{Ind}_{\mathrm{H}_k}^{\Delta}(\check{\xi}_k)$ for $k = i$, $i-1$. So, from Lemma 14, we have $\mathrm{W}^*(\chi_i)^4 = \mathrm{W}^*(\eta_i)^4$.

Moreover, applying Lemma 17 with $\Psi = \mathrm{H}_{i-1}$, $\Phi = \mathrm{P}$, $\check{\mu}_{i-1} = \check{\xi}_{i-1}$, $\lambda_i = \eta_i$, we obtain $\mathrm{W}^*(\check{\xi}_{i-1})^{4\mathrm{f}} = \mathrm{W}^*(\eta_i)^4$ and, using $\mathrm{W}^*(\chi_{i-1})^4 = \mathrm{W}^*(\check{\xi}_{i-1})^4$, we deduce that

$$\mathrm{W}^*(\chi_i)^4 = \mathrm{W}^*(\eta_i)^4 = \mathrm{W}^*(\chi_{i-1})^{4\mathrm{f}}$$

as is required.

Proof of Lemma 16. – We suppose then that $\alpha \in \mathrm{R}_{\mathrm{H}_v}$. As explained prior to the statement of Lemma 16, H_v is an abelian group, and so, without loss of generality, we may take α to be an abelian character. Then the statement that $\alpha(\overline{\mathrm{T}}\,\mathrm{T}^{-1}) = \mathrm{W}^*(\alpha)^2$ follows straight from the definition of $\mathrm{W}(\alpha)$ and $\mathrm{W}^*(\alpha)$, once we have observed that $\mathrm{W}(\alpha)\,\overline{\mathrm{W}(\alpha)} = 1$ and further, that if α is unramified, then $\alpha(\mathrm{T}) = \alpha(\overline{\mathrm{T}}) = \Sigma\, \psi_{\mathrm{M}}(uc^{-1}) = -1$. (Because $\psi_{\mathrm{M}}(*c^{-1})$ induces a non-trivial additive character on the group $\mathcal{O}_{\mathrm{M}} \bmod \mathfrak{p}$).

So now we suppose that $\beta \in \mathrm{R}_{\mathrm{H}_0}$. In order to show

$$\mathrm{Det}(\overline{\mathrm{T}}\,\mathrm{T}^{-1})\,(\beta) = \mathrm{W}^*(\beta)^{2(\mathrm{H}_0:\mathrm{H}_v)},$$

by linearity it is sufficient to assume that β is irreducible. We note that because $v = r$ if $\ell \neq 2$ (resp. $v = u$ if $\ell = 2$), β is either abelian, or, of the form $\mathrm{Ind}_{\mathrm{H}_v}^{\mathrm{H}_0}(\xi)$, for some abelian character ξ of H_v.

First we suppose that β is abelian. We put $\alpha = \beta|_{\mathrm{H}_v}$. Then $\beta(\overline{\mathrm{T}}\,\mathrm{T}^{-1}) = \alpha(\overline{\mathrm{T}}\,\mathrm{T}^{-1})$, so that by the first part of this proof

$$\beta(\overline{\mathrm{T}}\,\mathrm{T}^{-1}) = \mathrm{W}^*(\alpha)^2 = \mathrm{W}^*(\beta|_{\mathrm{H}_v})^2$$

and by Lemma 15

$$= \mathrm{W}^*(\beta)^{2(\mathrm{H}_0:\mathrm{H}_v)}$$

as is required. So now, lastly, we suppose β is non-abelian with $\beta = \mathrm{Ind}_{\mathrm{H}_v}^{\mathrm{H}_0}(\xi)$. By Mackey's restriction theorem, $\beta|_{\mathrm{H}_v} = \sum_{\eta} \xi^{\eta}$ where η is summed through a transversal of H_v in H_0. (Here ξ^{η} denotes the composition of ξ with conjugation by η). Hence, as $\overline{\mathrm{T}}, \mathrm{T}$ lie in $\mathbf{Z}[\zeta_p]\,\mathrm{T} \subset \mathbf{Z}[\zeta_p]\,\mathrm{H}_v$,

$$\mathrm{Det}(\overline{\mathrm{T}}\,\mathrm{T}^{-1})\,(\beta) = \prod_{\eta} \xi^{\eta}(\overline{\mathrm{T}}\,\mathrm{T}^{-1}).$$

However, by the first part of this proof,

$$\xi^\eta(\overline{T}\,T^{-1}) = W^*(\xi^\eta)^2$$

which by Lemma 14 $$= W^*(\mathrm{Ind}_{H_v}^{H_0}(\xi^\eta))^2 = W^*(\beta)^2.$$

Thus we obtain that $\mathrm{Det}(\overline{T}\,T^{-1})\,(\beta) = W^*(\beta)^{2(H_0:H_v)}$ which completes the proof of the lemma.

BIBLIOGRAPHY

[1] Ph. CASSOU-NOGUES, Quelques théorèmes de base normale d'entiers, *Ann. Inst. Fourier,* 28, 3 (1978), 1-33.

[2] P. DELIGNE, Les constantes des équations fonctionnelles des fonctions L, Modular forms in one variable III, *Lecture Notes in Mathematics,* 349 (1973), 501-597.

[3] A. FRÖHLICH, Arithmetic and Galois module structure for tame extensions, *J. reine und angew. Math.*, 286/287 (1976), 380-440.

[4] A. FRÖHLICH, To appear in the Springer Ergebnisse series.

[5] A. FRÖHLICH, Galois module structure, Algebraic Number Fields, (Proc. Durham Symposium), Academic Press, 1977, London.

[6] A. FRÖHLICH, Locally free modules over arithmetic orders, *J. reine angew. Math.,* 274/5 (1975), 112-124.

[7] A. FRÖHLICH and M.J. TAYLOR, The arithmetic theory of local Galois Gauss sums for tame characters, to appear in the *Philosophical Transactions of the Royal Society.*

[8] T.Y. LAM, Artin exponents of finite groups, *J. Algebra,* 9 (1968), 94-119.

[9] S. LANG, Algebraic number theory, Addison-Wesley (1970).

[10] J. MARTINET, Character theory and Artin L-functions, Algebraic Number fields, (Proc. Durham Symposium), Academic Press, (1977), London.

[11] E. NOETHER, Normalbasis bei Körpern ohne höhere Verzweigung, *J. reine angew. Math.,* 167 (1932), 147-152.

[12] J.P. SERRE, Corps locaux, Hermann, Paris, 1968.

[13] J.P. SERRE, Représentations linéaires des groupes finis, 2nd ed., Hermann, Paris, 1971.

[14] J. TATE, Local constants, Algebraic Number Fields, (Proc. Durham Symposium), Academic Press, London, 1977.

[15] M.J. TAYLOR, Galois module structure of relative abelian extensions, *J. reine angew. Math.*, 303/4 (1978), 97-101.

[16] M.J. TAYLOR, On the self-duality of a ring of integers as a Galois module, *Inventiones Mathematicae,* 46 (1978), 173-177.

[17] M.J. TAYLOR, A logarithmic description of locally free classgroups of finite groups, to appear in the *Journal of Algebra.*

Manuscrit reçu le 25 janvier 1980.

Martin J. TAYLOR,
Queen Mary College
London (G.B.)
&
Université de Besançon (France).