A

THE LOCAL THEORY OF ROOT NUMBERS

by

AARON WAN

A dissertation submitted to the Graduate Faculty in Mathematics
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy, The City University of New York

2004

UMI Number: 3115301

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

01/22/04 Carlos J. Moreno

Date — Carlos Moreno, Chair of Examining Committee

01/22/04 Alvany Rocha

Date — Alvany Rocha, Executive Officer

Raymond Hoobler

Kenneth Kramer

Melvyn Nathanson

Lucien Szpiro

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Acknowledgements

I am grateful to my advisor Carlos Moreno, who has been extremely patient with me and very generous in sharing his ideas, insights and knowledge for more than six years. He is truely a model of great mentor and teacher that I wish to emulate.

I would like to thank Raymond Hoobler, Kenneth Kramer, Melvyn Nathanson and Lucien Szpiro, who have served in my supervisory committee, for their encouragements, professional advices and all the helpful conversations. I would like to extend my thanks to the faculty members and friends at the Graduate Center and to my colleagues at LaGuardia Community College for the heartfelt supports over the years.

I also want to express my deep appreciation to my parents, Helen and Michael. They have shown a lot of faith in me, even in the occasions when I question myself seriously. A special thank goes to my brother Alex, whose presence has helped ease the difficult times during the course of my graduate study.

Finally, I must acknowledge all the sacrifices Joanna Tam has made for me in the last two years. Without her care, understanding and comfort, this thesis would not be possible.

Contents

0 Introduction

This thesis is a contribution to the theory of local root numbers. We use Deligne's proof of Langlands' determination of the kernel of Brauer induction for solvable groups to derive directly the existence of local root numbers. In this introduction, after laying out the basic definitions and notations, we will recall briefly the history of the problem, particularly Langlands' Yale manuscript of 1971. In the last section, we describe the main objectives of the thesis.

The Problem and its History.

Let F be a number field. A constant that appears in the functional equation of the L-series associated with a representation V of the Weil group W_F is traditionally known as the root number. Its value depends on V. (In contrast, the choice of an additive character, together with a Haar measure, of the completion F_v of F at a prime v also affects the "local" root number. See [4].) The problem of existence and uniqueness of the global (resp. local) root number for every finite dimensional representation of W_F (resp. W_{F_v}) was initiated and completed by the work of Hecke, Artin, Brauer, Hasse, Tate, Dwork, Langlands and Deligne. Therefore, given a representation ρ of a "global" Galois group G, we have, as special cases of the theory for Weil groups, the Artin root number $W(\rho)$ as well as its local counterpart $W(\rho_v)$ where v is a prime of the fixed field of G. Moreover, $W(\rho)$ is equal to the product $\prod W(\rho_v)$ over all the primes[1]. By modifying the global argument due to Deligne, Tate [23] has shown that $W(\rho_v)$ is well defined without the machinery of Weil groups. We will adhere to this idea, approaching $W(\rho)$ and $W(\rho_v)$ within the Galois setting.

Let K be a finite normal extension of the number field F and G be the Galois group $Gal(K/F)$. A representation ρ of G is a homomorphism from G to the group $GL_n(V)$ consisting of automorphisms of the n-dimensional vector space V. Suppose V^* is the dual of V. Then the contragradient of ρ is a representation $\hat{\rho}\colon G \to GL_n(V^*)$ defined by $\hat{\rho}(g)(h) = h \circ \rho^{-1}(g)$ where $g \in G$ and $h \in V^*$. Given a prime v of F, let w be a prime of K lying above v (i.e. $w|v$) and G_w be the decomposition group of w. If the

[1]This is called the local decomposition of $W(\rho)$.

restriction of ρ to G_w is denoted by ρ_w, we shall see that both the local L-function and the local root number stay constant on the set $\{ \rho_w \mid w|v \}$. This permits the identification of ρ_v with any one of the representations in $\{ \rho_w \mid w|v \}$. Now, we are in position to define the local L-function for ρ_v.

(i) v is finite. If I_w stands for the inertia group of w, let V^{I_w} be the subspace of V on which every automorphism in $\rho(I_w)$ is the identity map 1. Because I_w is normal in G_w, we conclude $\rho(g)(V^{I_w}) = V^{I_w}$ for all $g \in G_w$. Meanwhile, G_w/I_w is isomorphic to the Galois group of the residue class field extension. Under this group isomorphism, there exists $\sigma_w \in G_w$ which is sent to the automorphism $x \to x^{N(v)}$, where $N(v)$ equals the cardinality of the residue class field of F with respect to v. Consequently, for any complex number s, $1-N(v)^{-s}\rho(\sigma_w)$ is a linear map from V^{I_w} to itself and is insensitive (on the subspace V^{I_w}) to the choice of σ_w. Since the determinant (of any matrix realization) of $1 - N(v)^{-s}\rho(\sigma_w)$ remains invariant when we change the prime w above v, let us write this determinant as follows

$$det\Big[1 - N(v)^{-s}\rho_v(\sigma_v)\Big]$$

and define the local L-function, whose value could be ∞, by

$$L_v(\rho_v, s) = \frac{1}{det\left[1 - N(v)^{-s}\rho_v(\sigma_v)\right]} .$$

(ii) v is infinite and F_v is the field of complex numbers.

$$L_v(\rho_v, s) = \left[2(2\pi)^{-s}\ \Gamma(s)\right]^n .$$

Recall that n equals the dimension of the representation ρ_v and that s is a complex variable.

(iii) v is infinite and F_v is the field of real numbers. Given $w|v$, the decomposition group G_w is either trivial or cyclic of order 2. Let σ_w be the generator for G_w. Then the automorphism $\rho(\sigma_w)$ decomposes the vector space V into a direct sum $V_+ \oplus V_-$ where

$$V_+ = \left\{x \in V \mid \rho(\sigma_w)(x) = x\right\}$$

and

$$V_- = \left\{x \in V \mid \rho(\sigma_w)(x) = -x\right\} .$$

This is because $\rho(\sigma_w)^2 = \rho(\sigma_w^2) = \rho(1) = 1$. We define

$$L_v(\rho_v, s) = \left[\pi^{-s/2}\ \Gamma\left(\frac{s}{2}\right)\right]^{dim\ V_+} \left[\pi^{-(s+1)/2}\ \Gamma\left(\frac{s+1}{2}\right)\right]^{dim\ V_-} .$$

Here $dim\, V_+$ and $dim\, V_-$ are the dimensions of the respective subspaces, and they are independent of the prime w chosen.

Now, the global (Artin) L-function $L(\rho, s)$ for ρ is the product of the local L-functions over all the primes of F. This global L-function is analytic at s whose real part is greater than one. Moreover, $L(\rho, s)$ is an additive and inductive function over F in the sense of Tate [21] (see 2.3.2, p.11).

Suppose L is a finite extension of K such that L/F is Galois. Then ρ can be interpreted as a representation of $Gal(L/F)$ via the natural homomorphism $proj : Gal(L/F) \to Gal(K/F)$. The corresponding Artin L-function $L(\rho \circ proj\, , s)$ is in fact the same as $L(\rho, s)$. Consequently, with $\overline{F}$ an algebraic closure of F, the L-function is well defined for all finite dimensional complex representations of $Gal(\overline{F}/F)$.

Meanwhile, we may assume the representation $\rho : Gal(K/F) \to GL_n(V)$ is faithful i.e. ρ has trivial kernel. When $dim\, V = 1$, this means K/F is cyclic. $L(\rho, s)$ in this case is known as the abelian L-function. Composing ρ with the Artin reciprocity map, we obtain an idele class character χ, whose Hecke's L-series possesses a meromorphic continuation in the entire complex plane $\mathbf{C}$. If D denotes the discriminant of the number field F and $N(f(\chi))$ denotes the absolute norm of the conductor of χ, then it is a special case of Hecke's result [11] that

$$L(\chi, s) \;=\; L(\rho, s) \;=\; \prod_v L_v(\rho_v, s)$$

is a meromorphic function on $\mathbf{C}$ and satisfies the functional equation

$$L(\chi, s) \;=\; W(\chi)\left[|D| \cdot N(f(\chi))\right]^{(1-2s)/2} L(\chi^{-1}, 1-s) \qquad (F.E.).$$

According to Tate's proof [22] of $(F.E.)$, the above constant $W(\chi)$ is a product (over all primes v in F) of local constants $W(\chi_v)$. Here χ_v is the composition of χ with the inclusion map i_v from $F_v^\times$ to the idele group of F. Let us now recall the explicit formulas [23] for $W(\chi_v)$.

Definition of the abelian root number.

(i) v is finite. Suppose π_{F_v} is a uniformizing parameter of F_v, O_{F_v} is the ring of integers for F_v, P_{F_v} is the maximal ideal in O_{F_v}, U_{F_v} is the unit group of O_{F_v}, ψ_F is the canonical additive character (see [23], p.91) of F_v, d is the order of the absolute different of F_v, and m is the conductor of χ_v i.e. the smallest nonnegative integer such that

χ_v annihilates $U_{F_v}^m = 1 + P_{F_v}^m$.

$$W(\chi_v) = N(P_{F_v}^m)^{-1/2} \sum_{x \in U_{F_v}/U_{F_v}^m} \chi_v^{-1}\left(\frac{x}{\pi_{F_v}^{m+d}}\right) \psi_F\left(\frac{x}{\pi_{F_v}^{m+d}}\right) .$$

In particular, for $m = 0$, we have $W(\chi_v) = \chi_v(\pi_{F_v}^d)$.

(ii) v is infinite and F_v is the field of complex numbers.

$$W(\chi_v) = 1 .$$

In fact, because the idele class character χ shares the same finite image with ρ, the (quasi) character χ_v is always trivial.

(iii) v is infinite and F_v is the field of real numbers.

$$W(\chi_v) = \begin{cases} 1 & \text{when } \chi_v = 1 . \\ -i & \text{otherwise.} \end{cases}$$

Again, $x/|x|$ is the only possible non-trivial χ_v due to the finiteness of $\chi_v(F_v^\times)$.

In terms of the one dimensional representation ρ of $G(K/F)$, the above functional equation $(F.E.)$ can be restated:

$$L(\rho, s) = W(\rho)\, A(\rho)^{(1-2s)/2}\, L(\hat{\rho}, 1-s)$$

where the Artin root number $W(\rho)$ is defined to be $\prod_v W(\chi_v)$ and the constant $A(\rho)$ is the product of $|D|$ and the absolute norm of the Artin conductor[2] of ρ.

The composition of the Artin reciprocity map and i_v, under which the image of $F_v^\times$ coincides with the decomposition group for a prime lying above v, is called the local reciprocity map θ_v. It can be constructed in the purely local setting (see Serre [20].) Because $\chi_v = \rho_v \circ \theta_v$, the natural definition

$$W(\rho_v) = W(\chi_v)$$

shows that the root number also exists as a purely local object when the representation is one dimensional. We are justified to call $W(\chi_v)$ the local root number because it appears in Tate's local functional equation. (See Tate [22].) Moreover, the above definition of $W(\rho_v)$ readily yields the local decomposition of $W(\rho)$. (See footnote 1.)

The proof of the meromorphic continuation and the functional equation for all Artin L-functions is credited to Brauer, who used his induction theorem

[2] The equality between the Artin conductor of ρ and the conductor of the idele class character χ is due to Artin.

to reduce the problem to the one dimensional case. It follows that the Artin root number is defined for every finite dimensional complex representation of $Gal(\overline{F}/F)$. Let us conclude the global theory here by a remark on the constant $A(\rho)$ in the functional equation for $L(\rho, s)$. When ρ has dimension $n > 1$, this constant is really the product of $|D|^n$ and the absolute norm of the Artin conductor of ρ; otherwise $A(\rho)$ would not be inductive.

Regarding the local theory of root numbers, the immediate focus is on generalizing $W(\chi_v)$ when v is finite. Dwork built upon Artin's idea of extending functions originally defined on one dimensional representations of local Galois groups (see [6], § 1, p.445) and showed that the constant $W(\chi_v)^2\chi_v(-1)$ (instead of $W(\chi_v)$) has an analogue for higher dimensional representations of $Gal(\overline{F_v}/F_v)$, which is inductive over F_v. (See [6], § 3, Theorem 5′, p.462.) Consequently, he obtained a local decomposition for the square of the Artin root number. Nonetheless, his work leading to this result bears the most significance. Specifically, Dwork found the generators for the kernel of Brauer induction in the supersolvable case and proved an arithmetic result [5] (referred to by Langlands as the 1st and 2nd identities) that established the existence and uniqueness of the root number for a representation of any nilpotent local Galois group.

Weil's proof of the converse theorem for classical modular forms makes use of the twisting properties of the global root numbers in the functional equations for the Dirichlet L-functions (see Weil [24], Theorem 1, p.152). Motivated by this idea of Weil, Langlands established the existence of certain extraordinary representation in Jacquet-Langlands [13](p.240) from a detailed knowledge of the local root numbers, part of which he developed separately in the Yale manuscript [16]. Primarily, Langlands' manuscript completes the local theory of root numbers with his determination of the generators for the kernel of Brauer induction in the solvable case (which had eluded Dwork who eventually resorted to a global analytic argument in [6], § 2, p.453) and with the introduction of his λ-constant:

Theorem (Langlands [17]).[3] *Suppose* F *is a local field. It is possible in*

[3] Our version is a special case of Langlands' original statement. For simplicity, we have used the canonical additive character for the local field F.

exactly one way to assign to each finite extension E *of* F *a complex number* $\lambda_{E/F}$ *and to each isomorphism class* ω *of representations of* $Gal(\overline{E}/E)$ *a complex number* $\varepsilon(\omega)$ *such that*

(a) *if* ω *is one dimensional, then* $\varepsilon(\omega) = W(\omega)$ *, Tate's root number.*

(b) ε *is additive over* E *.*

(c) *if* $Ind_{E/F}(\omega)$ *denotes the isomorphism class of the induced representation of* $Gal(\overline{E}/F)$ *by* ω *, then*

$$\varepsilon(\,Ind_{E/F}\,(\omega)\,) \;=\; (\lambda_{E/F})^{\,dim\,\omega}\cdot\varepsilon(\omega)$$

where $dim\,\omega$ *stands for the dimension of* ω *.*

There are four fundamental identities critical to Langlands' proof of the above theorem. The 1st and 2nd identities had already been discovered by Dwork. The last two, which amount to the tame case and the wild case respectively of a single identity, are Langlands' pivotal insight. Unfortunately, the lengthy verification of Dwork's identities in [16] is fragmentary. To the best of my knowledge, the remaining sources for the proof of these two identities by

Dwork are Lakkis [14] and the unpublished thesis of Dwork. However, neither includes the completed argument for the 2nd identity. (The completed argument for the 1st identity appears in chapter 3 of Dwork's thesis.) As commented by Langlands in his collected works [17], if one accepts the two identities of Dwork, the proof of the above theorem in [16] is complete.

By abandoning the purely local approach in [16], Deligne found a proof of Langlands' theorem which avoids the difficulties that arise from verifying the fundamental root number identities. His comparatively short argument [4] (pp.35-47) has been modified by Tate into a proof that is applicable to the framework originally used by Dwork and Hasse to extend $W(\chi_v)$. The key to Deligne's proof is the behavior of root numbers under twisting by character (see [4], 4.6, p.39). In addition, Deligne is able to separate the theory of λ-constants from his proof by formulating the local theory of root numbers in terms of virtual representations (see [23], § 2, p.101). This has suggested a simplification in Langlands' local proof.

As elegant as the argument in Deligne [4] is, it still depends on the existence and the analytic properties of the global Artin root numbers[4]. From the perspective of Langlands, a satisfactory local proof of his theorem remains an open problem [17], and this thesis results from an attempt to make progress in this direction.

Before we describe the contents of the thesis, which is based on Langlands' original local approach, let us give an overview of Langlands' unpublished[5] manuscript [16].

Langlands' Yale Manuscript.

The original Langlands' manuscript, according to the table of contents, consisted of 21 paragraphs (Chapters), an introductory section, and an appendix. Of these §§0,2,3,4,5,6,7,14,15,16,17,18, and 19, were typeset and readily available from the Library at Yale. Except for § 10, which is missing, the rest of the paragraphs were available in hand written form from Langlands. Presently all the paragraphs originally available (except for Chapter

[4]So does Dwork's analytic method.

[5]The manuscript was neither published nor reviewed officially, but it currently appears at the web site www.sunsite.ubc.ca/DigitalMathArchive/Langlands/

10) have been set in Tex and are available in the collected works of Langlands [17].

The introductory chapter (§0) of Langlands' manuscript recalls the definition of Artin L-functions, states the functional equation and gives the definition of root numbers. The problem of expressing this root number as a product of local ε-factors arises as a generalization of Tate's local decomposition of the corresponding root number for abelian L-functions [22]. The existence and uniqueness of such local ε-factors (Theorem A) forms the principal result of the manuscript. As pointed out by Tate ([21], p.17), it is important to note that Langlands' version of the abelian local constant $\Delta(\chi_F, \psi_F)$ is not always consistent with that which appears in the literature. In the following $\Delta(\chi_F, \psi_F)$ is the root number of χ_F as given by Langlands.

After laying out the notation for Weil groups and reviewing some of their basic properties (chapter 1), Langlands reformulates Theorem A: given a relation in the kernel of Brauer induction, there corresponds to it an analogous relation among root numbers, up to some λ-factors. The existence and uniqueness of these λ-factors (Theorem 2.1) make it possible to define the

ε-factor in Theorem A by means of Brauer's theorem. To derive Theorem A from Theorem 2.1, one must verify certain tansitivity and non-vanishing properties for the λ-factors (chapter 4). For this purpose, Langlands developes in chapter 3 his lemmas of induction, which bear the overall structure of the inductive proof of Theorem 2.1.

In essence, the lemmas of induction determine when a family of extensions inside a local Galois extension K/F coincides with the complete lattice of subextensions of K/F. From a group theoretic viewpoint, these lemmas of induction reveal that cyclic groups and solvable semi-direct products are the building blocks for all local Galois groups.

Langlands uses the lemmas of induction to prove the transitivity, the non-vanishing property, as well as the uniqueness of λ-factors (cf. Theorem 2.1) in chapter 4. As for the existence of λ-factors (cf.Theorem 2.1), he argues inductively on the degree of the Galois extension K/F, assuming that the λ-factors are already well-defined on subextensions of smaller degree. The entire induction comprises 14 chapters in the manuscript (from chapter 6 to chapter 19).

Another significant application of the lemmas of induction appears in chapter 6 where Langlands defines the Herbrand function for finite separable extensions, generalizing the well known results in local class field theory (see Serre [20, chapter IV and V]). This Herbrand function together with the norm map help derive relations between the conductors of quasi-characters in the four root number identities that constitute Langlands' four main lemmas. In addition to the Herbrand function, a natural filtration for local Weil groups is also defined in chapter 6, analogous to the upper numbering filtration for local Galois group from the perspective of the Herbrand's theorem and the local reciprocity map.

One group theoretic component of the inductive argument for Theorem 2.1 is lemma 15.1 (see also lemma 1.11 in Deligne [4]). Its corresponding root number identity (lemma 15.3) ties up the four main lemmas in the manuscript. When applied to the trivial quasi-character, this root number identity then yields a definition of the λ-factor (lemma 16.2), which satisfies the transitivity formula given the induction hypothesis of theorem 2.1.

Based on a pure group theoretic argument equivalent to (in the Galois setting) Deligne's lemma 1.13.2 [4], Langlands further reduces the proof of the existence part in Theorem 2.1 to that of a special case (lemma 17.1) with additional constraints on the quasi-characters. In fact, Theorem A holds if and only if lemma 17.1 does. As a general strategy of proving lemma 17.1, Langlands writes his representations in terms of inflations (so that the induction hypothesis of Theorem 2.1 can be applied) and establishes the prescribed root number identities (to be combined with the induction hypothesis of Theorem 2.1).

Lemma 18.1 demonstrates the above strategy when the Galois group $Gal(K/F)$ is nilpotent. Because such a Galois group has a non-trivial center and so do its subgroups and quotients, the induction hypothesis of Theorem 2.1 together with the first and second root number identities already suffice to prove lemma 17.1 for the nilpotent case (given the definition of λ-factors in chapter 16). According to Langlands' own commentary, the first part of lemma 18.1, whose proof is independent of Theorem 2.1 and its induction hypothesis, may be of interest beyond the purposes of the manuscript (see [17]).

Beyond the nilpotent case, the tensor product between two induced representations must be analyzed carefully. Lemma 19.2 serves this purpose. An elegant approach to lemma 19.2 can also be found in Deligne [4]. The remainder of the proof of lemma 17.1 (when $Gal(K/F)$ is not nilpotent) splits into two cases. With Langlands' four main lemmas and the induction hypothesis of Theorem 2.1, these two cases are dealt with using lemmas 19.1 and 19.2.

The first three main lemmas are reduced to identities between ordinary Gauss sums, when the field extensions are not wildly ramified and the quasi-characters all have conductors less than or equal to one. Granted the result of Stickelberger (lemma 7.1), Langlands establishes in chapter 7 three identities between ordinary Gauss sums that are equivalent to some special cases of his main lemmas. Particularly, the Hasse-Davenport relation, proved in lemma 7.7, corresponds to the 1st identity, while lemma 7.8 and lemma 7.9 correspond to the 3rd identity (lemma 13.3) and the 2nd identity (lemma 12.1) respectively.

Langlands decomposes his root number Δ $(= \Delta(\chi, \psi))$ of a wildly ramified quasi-character χ_F on $F^\times$ into three factors Δ/Δ_1, Δ_2 and Δ_3 in order to facilitate the proof of his four main lemmas, and the definitions of Δ_1, Δ_2 and Δ_3 appear in chapter 8. Once Δ/Δ_1 is fixed, lemma 8.1 shows that Δ_2 depends only on a certain parameter β. The rest of chapter 8 studies the relationship between this β for quasi-character χ_F and its counterpart for the composition $\chi_F \circ N_{E/F}$ when E is a finite separable extension of F (for technical reasons Langlands needs only the case that E/F is a totally ramified abelian extension whose ramification filtration has only one jump). The main results are stated by means of the map $P^*_{E/F}$ (see lemma 8.2 and lemma 8.10), but the critical steps in the proof of the main result are summarized in lemma 8.9 and lemma 8.11 respectively.

Langlands turns to Δ_3 in chapter 9. According to lemma 8.1, Δ_3 is significant only when the conductor of χ_F is odd. In view of lemma 9.3, Langlands reduces the analysis of Δ_3 to that of Dwork's delta sum defined on the residue class field (see Dwork [5], Chap. 2). The first half of this chapter is devoted to some basic properties of the delta sum and their implications for Δ_3. The second half (starting from lemma 9.7) consists of a delicate result that relates Δ_3 for χ_F to its counterpart for the composition $\chi_F \circ N_{K/F}$

where K/F is a totally ramified Galois extension of prime degree $\neq 2$.

Chapter 10, which accounts for the verification of the 1st identity, is missing. Fortunately, its completed proof due originally to Dwork can be found in his thesis (see [5], chap. 3).

Chapter 11 of Langlands' manuscript elaborates the theory of Artin-Schreier extension. Its presentation, modeled on that of Lakkis [14], originates from Dwork's proof of the 2nd identity (lemma 12.1). A totally and wildly ramified cyclic extension of degree p is characterized as an Artin-Schreier extension if the unique jump in the ramification filtration is not divisible by p (lemma 11.2). If Z_p denotes the cyclic group of prime order p, then a totally ramified Galois extension K/F with $Gal(K/F) = Z_p \oplus Z_p$ contains $p+1$ Artin Schreier subextension K/L_i. Given a root θ of an Artin-Schreier equation that generates K/L_i, the norm and the trace of θ satisfy a sharp congruence when p is odd (lemma 11.8). Since every element in K can be expressed as a polynomial in θ, analogous congruences involving the norm and the trace of monomials in θ are obtained as well (lemma 11.9). These congruences, which have only been partially verified by

Langlands, are crucial ingredients for the basic result in chapter 11. However, Langlands never formally stated this basic result in the manuscript (see Lakkis [14], Hilfsaatz 18).

Suppose L_1 and L_2 are distinct cyclic extensions of prime degree ℓ over a local field F. Under the premises of the second main lemma, the 2nd identity (lemma 12.1) relates the root number of a quasi-character χ_{L_1} on $L_1^\times$ to the root number of a quasi-character χ_{L_2} on $L_2^\times$. In the case that both χ_{L_1} and χ_{L_2} have large conductors compared with the conductor of the extension, Langlands proves the 2nd identity by means of character twisting. Specifically, a quasi-character χ_F on $F^\times$ is constructed in lemma 12.3 (resp. lemma 12.4) so that the product $\chi_{L_i}^{-1} \cdot (\chi_F \circ N_{L_i/F})$ has the minimum conductor for $i = 1, 2$. It follows that the root number of χ_{L_i} and the root number of $\chi_F \circ N_{L_i/F}$ differ by a multiple of some character value of $\chi_{L_i}^{-1} \cdot (\chi_F \circ N_{L_i/F})$, when the conductor of χ_{L_1} is twice the size of this minimum conductor. By applying the 1st identity to the root number of $\chi_F \circ N_{L_i/F}$, Langlands is able to reduce the proof of the 2nd identity in this case to checking the character values of χ_{L_1} and χ_{L_2} on the ground field F. However, when the conductor of χ_{L_1} is comparable to the size of the minimum conductor, the proof of the 2nd identity in chapter 12 remains incomplete.

Langlands' 3rd identity first appears in chapter 13 (the third main lemma) and to some extent generalizes the 1st identity. Suppose C is a non-trivial abelian normal subgroup of a semi-direct product $H \cdot C = Gal(K/F)$ such that every non-trivial normal subgroup of $Gal(K/F)$ contains C. If E is the fixed field of H, then the 3rd identity relates the root number of a quasi-character χ_F on $F^\times$ to the root number of $\chi_F \circ N_{E/F}$. Langlands establishes this identity for tamely ramified K/F in lemma 13.3. His proof is divided according to the conductor m of χ_F, but earlier results from chapter 6 and chapter 7 readily yield the conductor relation (responsible for reducing lemma 13.3 to an identity for Δ_1 factors) as well as the identity when m is less than or equal to one. For the case $m > 1$, Langlands follows the scheme developed in chapter 8 and chapter 9, comparing the respective Δ_2 and Δ_3 factors of the root numbers in the 3rd identity.

Regarding the 3rd identity for wildly ramified K/F (lemma 14.1), Langlands again starts with the conductor relation and then proves lemma 14.1

when χ_F is either unramified or tamely ramified. For the wild case (i.e. $m > 1$), he considers the quotient ρ between the two sides of the 3rd identity and shows that this quotient ρ is simultaneously an ℓ-th root of unity and an n-th root of unity where ℓ and n are relatively prime. Specifically, he reduces the remaining proof of lemma 14.1 to the proof of four subsequent lemmas in chapter 14 each of which asserts that ρ lies in certain cyclotomic fields. The first two lemmas (14.2 and 14.3) are largely devoted to various comparisons between the respective Δ_2 and Δ_3 of the root numbers according to different combinations of the conductor m and the length of the ramification filtration for $Gal(K/F)$. In contrast, the last two lemmas (14.4 and 14.5) use the main group theoretic result in chapter 15 as well as the induction hypothesis of Theorem 2.1.

This concludes our review of Langlands' manuscript.

Contents of Thesis.

Langlands' main theorem associates a unique root number to each representation of a local Galois group. Langlands' original proof in [16] depends on the theory of local Weil groups. Our aim is to provide a simpler local proof by limiting the use of Weil groups. In addition, our local proof incorporates a number of ideas already used by Deligne in his global analytic proof, particularly the elimination of the theory of λ-constants and Deligne's characterization of the kernel of Brauer induction for solvable groups. As in Langlands' original proof, we base our derivation on three fundamental root number identities. We provide detailed verification for these.

Chapter one introduces the notations, conventions and definitions needed to state Deligne's version of the kernel of Brauer induction for solvable groups (theorem 1.4.1). For completeness we include the proof of lemmas 1.2.3 and 1.2.5 omitted in Deligne's presentation

Chapter two begins with the definition of local root numbers based on a variation of Brauer induction. The Main Theorem of the thesis is also stated and a number of preliminary properties of root numbers are established.

Chapter three recalls the statement of the three fundamental root number identities (see section 3.1) and provides the inductive proof of The Main Theorem (sections 3.2 and 3.3). When the local Galois group G in our Main

Theorem is not nilpotent, we must appeal to the theory of Weil groups. An effort has been made to clarify the role of Weil groups in the local proof of Langlands' theorem.

Chapter four contains the proofs of the three fundamental root number identities (section 4.2 for the 1st identity, section 4.3 for the 2nd identity and section 4.4 for the 3rd identity). Despite the importance of making available the completed verification of these identities, we have decided to present their proofs in the case that all field extensions are not wildly ramified and to remark on the wild case at the conclusion of each identity.

In Appendix A we have collected the basic results from the Dwork-Lamprecht theory (Theorems A.1, A.2 and A.3). In Appendix B we have given concrete examples of the form of the 2nd and the 3rd identities.

CHAPTER ONE

1 The Kernel of Brauer Induction

Let ρ be a finite dimensional representation (over the complex numbers $\mathbf{C}$) of a finite group G . Then Brauer's induction theorem states that

$$\rho \;=\; \sum_i n_i \, Ind_{H_i}^G(\chi_i)$$

where the sum on the right hand side is finite, the coefficient n_i is an integer, H_i is an elementary subgroup of G and $\chi_i \in Hom(H_i, \mathbf{C}^\times)$.

However, n_i , H_i , χ_i are not uniquely determined by ρ . In other words, there exist relations:

$$\sum_i n_i \, Ind_{H_i}^G(\chi_i) \;=\; 0 \; .$$

Our goal in this chapter is to describe Deligne's characterization of such relations.

1.1 Some basic definitions

While most notations here are adopted from Deligne [4] and Serre [19], let me point out that our symbol α^y is defined differently. Also, by a character of a group we always mean a one dimensional representation. i.e. a homomorphism from the group to the unit circle S^1.

$R(G)$ denotes the free abelian group generated by isomorphism classes V_j of irreducible representations of a finite group G. Elements of $R(G)$ are called virtual representations.

The dimension of a virtual representation $v = \sum_j m_j V_j$ is given by

$$dim\, v = \sum_j m_j\, dim(V_j) \qquad \text{where } dim(V_j) \text{ is the degree of } V_j .$$

$R_+(G)$ denotes the free abelian group generated by a basis that consists of G-conjugacy classes of ordered pairs (H, χ), where χ is a character of a subgroup H in G.

$b_G : R_+(G) \to R(G)$ is the induction map defined by

$$b_G(H, \chi) = Ind_H^G(\chi)$$

In this context, Brauer's theorem states that b_G is surjective. We call $R \in R_+(G)$ a relation if $b_G(R) = 0$.

$res : R_+(G) \rightarrow R_+(H)$ is defined, whenever H is a subgroup in G, by

$$res(A,\alpha) = \sum_{s \in H\backslash G/A} (H \cap sAs^{-1} , \alpha^{s^{-1}})$$

where s are representatives of the (A,H) double cosets of G and $\alpha^{s^{-1}}$ is a character of the subgroup sAs^{-1} defined by $\alpha^{s^{-1}}(x) = \alpha(s^{-1}\, x\, s)$.

$infl : R_+(G/H) \rightarrow R_+(G)$ is the pullback map. If $H \triangleleft G$ and $proj : G \rightarrow G/H$ is the canonical projection map, then we define

$$infl(A,\alpha) = (proj^{-1}(A) , \alpha \circ proj)$$

$R_+(G)$ is endowed with a multiplication which turns it into a ring and b_G into a ring homomorphism. Suppose α is a character of a subgroup A in G. For $y \in G$, let $A^y = y\,A\,y^{-1}$ and $\alpha^y(a) = \alpha(y\,a\,y^{-1})$. Then we define

$$(A,\alpha)\cdot(B,\beta) = \sum_{\substack{(x,y) \in \\ (G/A \times G/B)/G}} (A^x \cap B^y , \alpha^{x^{-1}} \cdot \beta^{y^{-1}})$$

where the sum is indexed by the equivalence classes of the G-action on the cartesian product $G/A \times G/B$.

1.2 Preliminary lemmas

Besides the relevant group theoretic claims that appear in Deligne [4], we have also included in this section several facts about representation theory that are used frequently later on.

Lemma 1.2.1 (cf. Deligne [4, 1.9.5 p.12]). With the notations in 1.1, we have two commutative diagrams:

$$
\begin{array}{ccc}
R_+(H) & \overset{i}{\hookrightarrow} & R_+(G) \\
b_H \downarrow & & \downarrow b_G \\
R(H) & \overset{Ind_H^G}{\longrightarrow} & R(G)
\end{array}
\qquad\qquad
\begin{array}{ccc}
R_+(G) & \overset{res}{\longrightarrow} & R_+(H) \\
b_G \downarrow & & \downarrow b_H \\
R(G) & \overset{Res_H}{\longrightarrow} & R(H)
\end{array}
$$

where Ind_H^G, Res_H are the usual induction and restriction, and i stands for the inclusion map.

Lemma 1.2.2 (cf. Deligne [4, 1.9.6 p.12]). If $r \in R_+(G)$, then by definition $res(r) \cdot (H,\chi) \in R_+(H)$ and

$$i(\, res(r) \cdot (H,\chi)\,) = r \cdot (H,\chi)\,.$$

Here i is the inclusion map in lemma 1.2.1.

Lemma 1.2.3 (cf. Deligne [4, Lemma 1.11 p.13]). Suppose $G = H{\cdot}C$ such that C is an abelian normal subgroup of G. Let χ be a character of H. Then there exists a character μ belonging to C^*, the character group of C, that satisfies $\chi|_{H\cap C} = \mu|_{H\cap C}$. Because G acts on C^* by conjugation, if G_μ is the stabilizer of μ, we can define a character $\{\chi,\mu\}$ on G_μ by

$$\{\chi,\mu\}(h\,c) \;=\; \chi(h)\cdot\mu(c) \quad \text{for } h \in H\cap G_\mu \;\text{ and }\; c \in C\,.$$

With C^*/G a set of representatives of the orbits of the above G - action on C^*,

$$Ind_H^G(\chi) \;=\; \sum_{\substack{\mu \in C^*/G \\ \chi|_{H\cap C}=\mu|_{H\cap C}}} Ind_{G_\mu}^G(\{\chi,\mu\})$$

Lemma 1.2.4 (cf. Deligne [4, Lemma 1.13.1 (1) p.15]). If G is abelian and χ is a character of subgroup $H \subseteq G$, then

$$Ind_H^G(\chi) \;=\; \sum_{\substack{\varphi \in G^* \\ \varphi|_H = \chi}} \varphi$$

where G^* again denotes the character group of G.

Lemma 1.2.5 (cf. Deligne [4, Lemma 1.13.2 p.15]). Let C be an abelian normal subgroup of G. Then G acts on the character group $C*$

by conjugation. Suppose T is a fixed set of representatives of the orbits of this G-action. If $\sum_i n_i Ind_{H_i}^{G}(\chi_i) = 0$ where $n_i \in \mathbf{Z}$, $H_i \supseteq C$ and $\chi_i|_C \in T$ for all i, then with a fixed $\mu \in T$, we have

$$\sum_{\chi_i|_C = \mu} n_i Ind_{H_i}^{G_\mu}(\chi_i) = 0$$

Notice the condition $\chi_i|_C = \mu$ assures $H_i \subseteq G_\mu$, the stabilizer of μ.

Lemma 1.2.6 (cf. Deligne [4, Theorem 1.13 (a_i) p.16]). If Z is the center of G, then the following belongs to $ker(b_{HZ})$, the kernel of b_{HZ}.

$$(H,\chi) - \sum_{\chi'|_H = \chi} (HZ,\chi')$$

Lemma 1.2.7 (A generalization of 1.2.5). Let K be a normal subgroup of G. Then G acts on $K^* = Hom(K,\mathbf{C}^\times)$. Let T be a fixed set of representatives of the orbits of this G-action. Given $\mu \in T$, the stabilizer of μ with respect to the G-action is denoted by G_μ. Suppose $\sum_i n_i Ind_{H_i}^{G}(\chi_i) = 0$ such that each subgroup H_i contains K and χ_i is a character of H_i satisfying $\chi_i|_K \in T$. Then for a fixed $\mu \in T$, we have

$$\sum_{\chi_i|_K = \mu} n_i Ind_{H_i}^{G_\mu}(\chi_i) = 0$$

Lemma 1.2.8 (cf. Langlands [16, Lemma 19.2]). Let A and B be fields lying between K and F where K/F is a Galois extension. If χ_A and χ_B are characters of the Galois groups $Gal(K/A)$ and $Gal(K/B)$ respectively, then there exist subfields $A_1, \ldots, A_M$, $B_1, \ldots, B_M$ and characters $\chi_{A_1}, \ldots, \chi_{A_M}$, $\chi_{B_1}, \ldots, \chi_{B_M}$ together with a collection of automorphisms

$$\{\sigma_1, \ldots, \sigma_M\} = Gal(K/A)\backslash Gal(K/F)/Gal(K/B)$$

representing the $(Gal(K/B)$, $Gal(K/A))$ double cosets of $Gal(K/F)$, so that for $\ell = 1, \ldots, M$, the subfield A_ℓ stays between K and A, the subfield B_ℓ stays between K and B, χ_{A_ℓ} is a character of $Gal(K/A_\ell)$ and χ_{B_ℓ} is a character of $Gal(K/B_\ell)$. In addition, we have the following five properties:

(1) If we write $\sigma_\ell(A_\ell)$ as ${A_\ell}^{\sigma_\ell}$, then $B_\ell = {A_\ell}^{\sigma_\ell}$.

In fact, $Gal(K/A_\ell) = Gal(K/A) \cap {\sigma_\ell}^{-1} Gal(K/B) \sigma_\ell$

and $Gal(K/B_\ell) = Gal(K/B) \cap \sigma_\ell Gal(K/A) {\sigma_\ell}^{-1}$.

(2) $(\chi_{B_\ell})^{\sigma_\ell} = \chi_{A_\ell}$ where the G-action is the usual conjugation.

(3) $$\left\{Ind_{Gal(K/A)}^{Gal(K/F)}\ (\chi_A)\right\} \otimes \left\{\ Ind_{Gal(K/B)}^{Gal(K/F)}\ (\chi_B)\right\}$$

$$= \ \sum_{\ell} Ind_{Gal(K/A_\ell)}^{Gal(K/F)}\ (\chi_{A_\ell})\ .$$

$$\left\{Ind_{Gal(K/A)}^{Gal(K/F)}\ (\chi_A)\right\} \otimes \left\{\ Ind_{Gal(K/B)}^{Gal(K/F)}\ (\chi_B)\right\}$$

$$= \ \sum_{\ell} Ind_{Gal(K/B_\ell)}^{Gal(K/F)}\ (\chi_{B_\ell})\ .$$

(4) $$\left\{Ind_{Gal(K/A)}^{Gal(K/F)}\ (\chi_A - 1)\right\} \otimes \left\{\ Ind_{Gal(K/B)}^{Gal(K/F)}\ (\chi_B)\right\}$$

$$= \ \sum_{\ell} \left[Ind_{Gal(K/A_\ell)}^{Gal(K/F)}\ (\chi_{A_\ell} - 1) \ - \ Ind_{Gal(K/A_\ell)}^{Gal(K/F)}\ ((\chi_{B_\ell/B})^{\sigma_\ell} - 1)\right]$$

$$= \ \sum_{\ell} \left[Ind_{Gal(K/B_\ell)}^{Gal(K/F)}\ (\chi_{B_\ell} - 1) \ - \ Ind_{Gal(K/B_\ell)}^{Gal(K/F)}\ (\chi_{B_\ell/B} - 1)\right]$$

where $\chi_{B_\ell/B}$ denotes the restricted character $\chi_B|_{Gal(K/B_\ell)}$.

(5) If $\alpha \ = \ Res_{Gal(K/A)}\left(Ind_{Gal(K/B)}^{Gal(K/F)}\ (\chi_B)\right)$

$$\beta \ = \ Res_{Gal(K/B)}\left(Ind_{Gal(K/A)}^{Gal(K/F)}\ (\chi_A)\right)$$

$$\gamma = Res_{Gal(K/B)}\left(Ind_{Gal(K/A)}^{Gal(K/F)}\ (1)\right)$$

then

$$\chi_B \otimes \beta = \sum{}_{\ell}\ Ind_{Gal(K/B_\ell)}^{Gal(K/B)}\ (\chi_{B_\ell})$$

$$\chi_B \otimes \gamma = \sum{}_{\ell}\ Ind_{Gal(K/B_\ell)}^{Gal(K/B)}\ (\chi_{B_\ell/B})$$

$$\chi_A \otimes \alpha = \sum{}_{\ell}\ Ind_{Gal(K/A_\ell)}^{Gal(K/A)}\ (\chi_{A_\ell})\ .$$

Moreover,

$$(\chi_A - 1) \otimes \alpha = \sum_{\ell} \left\{ Ind_{Gal(K/A_\ell)}^{Gal(K/A)}\ (\chi_{A_\ell} - 1) - Ind_{Gal(K/A_\ell)}^{Gal(K/A)}\ ((\chi_{B_\ell/B})^{\sigma_\ell} - 1) \right\}$$

$$(\beta - \gamma) \otimes \chi_B = \sum_{\ell} \left\{ Ind_{Gal(K/B_\ell)}^{Gal(K/B)}\ (\chi_{B_\ell} - 1) - Ind_{Gal(K/B_\ell)}^{Gal(K/B)}\ (\chi_{B_\ell/B} - 1) \right\}\ .$$

Lemma 1.2.9 (An application of lemma 1.2.11). If a relation R belongs to $ker(b_{G/A})$, the kernel of the homomorphism $b_{G/A}$, then $infl(R) \in ker(b_G)$. Conversely, if all the characters within a relation in $ker(b_G)$ annihilate $A \lhd G$, then that relation comes from a relation in $ker(b_{G/A})$ via *infl*.

Lemma 1.2.10 (cf. Langlands [16, Lemma 13.2]). Suppose χ is a character of a Galois group $Gal(K/E) \subseteq Gal(K/F)$, where K , E , F are finite extensions of a p-adic number field. For any $g \in Gal(K/F)$, let χ^g be a character of $g^{-1}Gal(K/E)g$ defined by $\chi^g(x) = \chi(g\,x\,g^{-1})$. If $W(\chi)$ and $W(\chi^g)$ denote the abelian root numbers of the respective characters, then $W(\chi) = W(\chi^g)$.

Lemma 1.2.11. Let G be any group, finite or infinite, with subgroup H of finite index. If χ is a character of H whose kernel contains a subgroup $A \lhd G$, then $Ind_H^G(\chi)$ comes from (is an inflation of) a representation of G/A via the canonical projection $proj : G \to G/A$. In fact $proj$ enables the identification between $Ind_H^G(\chi)$ and $Ind_{H/A}^{G/A}(\chi)$.

Lemma 1.2.12. Suppose K is a finite Galois extension of a local field F. Let $Gal(K/F)$, $W_{K/F}$ be the corresponding Galois group and relative Weil group (see Tate [21]). Then the exact sequence

$$1 \to K^{\times} \to W_{K/F} \to Gal(K/F) \to 1$$

implies that $Ind_{Gal(K/E)}^{Gal(K/F)}(\chi)$ can be inflated to $Ind_{W_{K/E}}^{W_{K/F}}(\chi)$. In other words, considered as a representation of $W_{K/F}$ via the surjection $W_{K/F} \to Gal(K/F)$ in the exact sequence, the first induced representation is equal to the second.

1.3 Proving the preliminary lemmas

Proof of lemma 1.2.1 The diagram on the left is commutative due to the transitivity of induction. i.e. $Ind_A^G(\alpha) = Ind_H^G(Ind_A^H(\alpha))$ if $(A, \alpha) \in R_+(H)$.

To see that the diagram on the right is also commutative, recall the formula (Serre [19, Proposition 22 in 7.4, p.58])

$$Res_H\,(\,Ind_A^G\,(\alpha)\,) \;=\; \sum_{s\,\in\,H\backslash G/A} Ind^H_{(H\cap sAs^{-1})}\,(\alpha^{s^{-1}}) \qquad (1.3a)$$

where the index s ranges over the representatives for the double cosets of G and the character $\alpha^{s^{-1}}$ is defined as in 1.1. ||

Proof of lemma 1.2.2 It is sufficient to consider the case when r =

$(A\,,\,\alpha)$ i.e. r is a basis element of $R_+(G)$. From our definition in 1.1

$$(A,\alpha)\cdot(H,\chi) \;=\; \sum_{\substack{(x,y)\,\in \\ (G/A\;\times\;G/H)/G}} (A^x \cap H^y\;,\;\alpha^{x^{-1}}\cdot\chi^{y^{-1}})$$

Let's choose the representatives $(x,y)\;\in\;(G/A\;\times\;G/H)/G$ such that y is always equal to 1. In fact, $s\mapsto(s,1)$ yields a bijection between $H\backslash G/A$ and $(G/A\;\times\;G/H)/G$. On the other hand, in $R_+(H)$ the product

$$res(A,\alpha)\cdot(H,\chi) \;=\; \sum_{s\,\in\,H\backslash G/A} (H\cap sAs^{-1}\;,\;\alpha^{s^{-1}}\cdot\chi\,)$$

So, as an element of $R_+(G)$, $res(A,\alpha)\cdot(H,\chi)\;=\;(A,\alpha)\cdot(H,\chi)$.||

Proof of lemma 1.2.3 Let us first relate the dimensions (degrees) of the representations on both sides. Consider the restriction

$$Res_C\,(\,Ind_H^{HC}\,(\chi)\,) \;=\; \sum_{s\,\in\,C\backslash HC/H} Ind_{(C\,\cap\,sHs^{-1})}^{C}\,(\chi^{s^{-1}}) \;=\; Ind_{(H\,\cap\,C)}^{C}\,(\chi)$$

Since C is abelian, we can apply lemma 1.2.4 (proved separately), and this restriction becomes

$$Res_C\,(\,Ind_H^{HC}\,(\chi)\,) \;=\; \sum_{\substack{\mu\,\in\,C^* \\ \mu|_{C\cap H}\,=\,\chi|_{C\cap H}}} \mu \qquad (1.3b)$$

Now, observe that each representation $Ind_{(HC)_\mu}^{HC}\;(\{\chi,\mu\})$ is irreducible by Mackey's criterion. Moreover, distinct representatives in $C^*/(HC)$ yield distinct irreducible $Ind_{(HC)_\mu}^{HC}(\{\chi,\mu\})$. Suppose $\nu \neq \mu^g$ for any $g \in HC$. By $(1.3a)$ and the Frobenius reciprocity (see Serre [19, 7.2, Theorem 13, p.56],

$$\langle\, Ind_{(HC)_\nu}^{HC}(\{\chi,\nu\})\,,\, Ind_{(HC)_\mu}^{HC}(\{\chi,\mu\})\,\rangle_G$$

$$= \sum_{s\,\in\,(HC)_\nu\backslash(HC)/(HC)_\mu} \langle\,\{\chi,\nu\}\,,\,\{\chi,\mu\}^{s^{-1}}\,\rangle_{(HC)_\nu\,\cap\,s[(HC)_\mu]s^{-1}}$$

Because $C \subseteq (HC)_\nu \cap s[(HC)_\mu]s^{-1}$ and we have $\{\chi,\nu\} = \nu \neq \mu^{s^{-1}} = \{\chi,\mu\}^{s^{-1}}$ on C, the above sum must be zero.

Furthermore, $Ind_{(HC)_\mu}^{HC}(\{\chi,\mu\})$ is a irreducible component of $Ind_H^{HC}(\chi)$.

$$\langle\, Ind_H^{HC}(\chi)\,,\, Ind_{(HC)_\mu}^{HC}(\{\chi,\mu\})\,\rangle_G = \langle\, Ind_{(HC)_\mu\cap H}^{(HC)_\mu}(\chi)\,,\,\{\chi,\mu\}\,\rangle_{(HC)_\mu}$$

$$= \langle\,\chi\,,\,\{\chi,\mu\}\,\rangle_{(HC)_\mu\,\cap\,H}$$

$$= 1$$

according to Frobenius reciprocity and $(1.3a)$. Therefore

$$\sum_{\substack{\mu\,\in\,C^*/(HC)\\ \mu|_{H\cap C}\,=\,\chi|_{H\cap C}}} Ind_{(HC)_\mu}^{HC}(\{\chi,\mu\})$$

is a subrepresentation of $Ind_H^{HC}(\chi)$.

On the other hand, the representation $Ind_{(HC)_\mu}^{HC}(\{\chi, \mu\})$ has degree $\frac{|HC|}{|(HC)_\mu|}$. This is precisely the cardinality of the orbit containing μ under the HC-action. So the above subrepresentation is actually equal to $Ind_H^{HC}(\chi)$ as they share the same dimension by $(1.3b)$. ||

Proof of lemma 1.2.4 Since G is abelian, its center Z is equal to the entire group G. So lemma 1.2.4 follows from lemma 1.2.6.

Proof of lemma 1.2.5 See the proof of lemma 1.2.7. Simply replace the normal subgroup K in lemma 1.2.7 by C.

Proof of lemma 1.2.6 It is equivalent to proving

$$Ind_H^{HZ}(\chi) = \sum_{\substack{\chi' \in (HZ)^* \\ \chi'|_H = \chi}} \chi'$$

if $(HZ)^*$ is the character group of HZ. We can construct one χ' prescribed as above. The restricion $\chi|_{H \cap Z}$ can be extended to a character μ of Z because Z is abelian and the restriction map from the character group of Z to the character group of $H \cap Z$ is surjective. On HZ, we define $\chi_o'(h\,z) = \chi(h)\mu(z)$. This is a well-defined group homomorphism. In addition, notice that $H \lhd HZ$ and HZ/H is abelian. If $\varphi_1, \ldots, \varphi_n$ denote all the characters of HZ/H, then by viewing them as characters of HZ we have

$$\sum_{\substack{\chi' \in (HZ)^* \\ \chi'|_H = \chi}} \chi' = \chi_o' \cdot \varphi_1 +, \ldots + \chi_o' \cdot \varphi_n$$

Consequently, for $x \in HZ$

$$\sum_{\substack{\chi' \in (HZ)^* \\ \chi'|_H = \chi}} \chi'(x) = \begin{cases} |HZ/H| \cdot \chi(x) & \text{for } x \text{ belonging to } H \\ 0 & \text{otherwise} \end{cases}$$

but the trace of the induced representation $Ind_H^{HZ}(\chi)$ has exactly the same values. ||

Proof of lemma 1.2.7 Suppose

$$\sum_i n_i Ind_{H_i}^G(\chi_i) = \sum_{\mu \in T} \sum_{\chi_i|_K = \mu} n_i Ind_{H_i}^G(\chi_i) = 0$$

Notice that if $\mu = \chi_i|_K \neq \chi_j|_K = \nu$, then by the Frobenius reciprocity (Serre [19, 7.2, Theorem 13, p.56])

$$\langle\, Ind_{H_i}^G(\chi_i)\ ,\ Ind_{H_j}^G(\chi_j)\,\rangle_G = \langle\, \chi_i\ ,\ Res_{H_i}(\,Ind_{H_j}^G(\chi_j)\,)\,\rangle_{H_i}$$

which is equal to

$$\sum_{s \in H_i \backslash G/H_j} \langle \chi_i \ , \ Ind^{H_i}_{(H_i \cap sH_js^{-1})} (\chi_j^{s^{-1}}) \rangle_{H_i} \ = \sum_{s \in H_i \backslash G/H_j} \langle \chi_i \ , \ \chi_j^{s^{-1}} \rangle_{(H_i \cap sH_js^{-1})}$$

The last sum must be zero because $\chi_i \neq \chi_j^{s^{-1}}$ on the normal subgroup $K \subseteq H_i \cap sH_js^{-1}$. As a result, for any fixed $\mu \in T$, we conclude

$$0 \ = \ \langle \underbrace{\sum_{\nu \in T} \sum_{\chi_i|_K = \nu} n_i Ind^G_{H_i}(\chi_i)}_{\sum_i n_i Ind^G_{H_i}(\chi_i) \ = \ 0} \ , \ \sum_{\chi_i|_K = \mu} n_i Ind^G_{H_i}(\chi_i) \rangle_G$$

$$= \ \langle \sum_{\chi_i|_K = \mu} n_i Ind^G_{H_i}(\chi_i) \ , \ \sum_{\chi_i|_K = \mu} n_i Ind^G_{H_i}(\chi_i) \rangle_G$$

In other words,

$$\sum_{\chi_i|_K = \mu} n_i Ind^G_{H_i}(\chi_i) \ = \ 0$$

which means

$$\sum_{\chi_i|_K = \mu} n_i \, Res_{G_\mu} (Ind^G_{H_i}(\chi_i)) \ = \ 0$$

Consequently

$$\sum_{\chi_i|_K = \mu} n_i \, (\sum_{t \in G_\mu \backslash G/H_i} \cdot \, Ind^{G_\mu}_{(G_\mu \cap tH_it^{-1})} (\chi_i^{t^{-1}})) \ = \ 0$$

Since $\chi_i|_K = \mu$ implies $G_\mu \supseteq H_i$,

$$\sum_{\chi_i|_K = \mu} n_i \underbrace{\left\{ Ind^{G_\mu}_{H_i}(\chi_i) \ + \sum_{1 \neq t \in G_\mu \backslash G/H_i} Ind^{G_\mu}_{(G_\mu \cap tH_it^{-1})} (\chi_i^{t^{-1}}) \right\}}_{\sigma_i} \ = \ 0$$

Let us simplify the notation by writing this sum on the left hand side as $\sum_{\chi_i|_K = \mu} n_i \sigma_i$. We then consider the scalar product

$$\langle \sum_{\chi_i|_K = \mu} n_i \sigma_i \, , \sum_{\chi_j|_K = \mu} n_j \, Ind_{H_j}^{G_\mu} (\chi_j) \rangle_{G_\mu} = 0 \qquad (1.3c)$$

Now,

$$\langle \, Ind_{(G_\mu \cap tH_it^{-1})}^{G_\mu} (\chi_i^{t^{-1}}) \, , \, Ind_{H_j}^{G_\mu} (\chi_j) \rangle_{G_\mu} = 0 \qquad \text{for all } t \neq 1$$

because the left hand side can be rewritten, by means of the Frobenius reciprocity and $(1.3a)$, as

$$\sum_{r \in H_j \backslash G_\mu / (G_\mu \cap tH_it^{-1})} \langle \, Ind_{H_j \cap r(G_\mu \cap tH_it^{-1})r^{-1}}^{H_j} (\chi_i^{t^{-1}})^{r^{-1}} \, , \, \chi_j \rangle_{H_i}$$

which is equal to

$$\sum_{r \in H_j \backslash G_\mu / (G_\mu \cap tH_it^{-1})} \langle \, (\chi_i^{t^{-1}})^{r^{-1}} \, , \, \chi_j \rangle_{H_j \cap r(G_\mu \cap tH_it^{-1})r^{-1}}$$

Observe that $\langle (\chi_i^{t^{-1}})^{r^{-1}} \, , \, \chi_j \rangle \neq 0$ if and only if the two characters coincide on $H_j \cap r(G_\mu \cap tH_it^{-1})r^{-1}$. However $K \subseteq H_j \cap r(G_\mu \cap tH_it^{-1})r^{-1}$, and $(\chi_i^{t^{-1}})^{r^{-1}} = \chi_j$ on K means $(r \cdot t) \in G_\mu$. This is impossible as r is already in G_μ and $t \neq 1$. Hence, expanding the scalar product in (1.3c), we obtain

$$\langle \sum_{\chi_j|_K = \mu} n_j \, Ind_{H_j}^{G_\mu} (\chi_j) \, , \sum_{\chi_j|_K = \mu} n_j \, Ind_{H_j}^{G_\mu} (\chi_j) \rangle_{G_\mu} = 0$$

Lemma 1.2.7 is now established. ||

Proof of lemma 1.2.8 Let us introduce some abbreviations to simplify the subsequent notations.

$$\begin{array}{rclcrclcrcl} G_F &=& Gal(K/F) &,& G_A &=& Gal(K/A) &,& G_B &=& Gal(K/B) \\ \varrho &=& Ind_{G_A}^{G_F}(\chi_A) &,& \sigma &=& Ind_{G_B}^{G_F}(\chi_B) &,& \tau &=& Ind_{G_A}^{G_F}(1) \\ \alpha &=& Res_{G_A}(\sigma) &,& \beta &=& Res_{G_B}(\varrho) &,& \gamma &=& Res_{G_B}(\tau) \end{array}$$

For future reference, note that the bijection $G_F \stackrel{s^{-1}}{\rightarrow} G_F$, which sents s to its inverse, maps a set of representatives for the (G_B, G_A) double cosets of G_F into a set of representatives for the (G_A, G_B) double cosets of G_F . In other words,

$$G_A \backslash G_F / G_B \stackrel{s^{-1}}{\rightarrow} G_B \backslash G_F / G_A$$

Also, let M be the total number of double cosets in either one of these decompositions.

Now, given a set of representatives $G_B \backslash G_F / G_A$ and $\sigma_\ell \in G_B \backslash G_F / G_A$, we define

$$G_{A_\ell} = Gal(K/A_\ell) = G_A \cap \sigma_\ell^{-1} G_B \sigma_\ell$$

and

$$G_{B_\ell} \;=\; Gal(K/B_\ell) \;=\; G_B \,\cap\, \sigma_\ell \, G_A \, \sigma_\ell^{-1}$$

It follows that

$$\sigma_\ell \, G_{A_\ell} \, \sigma_\ell^{-1} \;=\; \underbrace{\sigma_\ell \, Gal(K/A_\ell) \, \sigma_\ell^{-1}}_{Gal(K/A_\ell^{\sigma_\ell})} \;=\; Gal(K/B_\ell) \;=\; G_{B_\ell}$$

Hence, ${A_\ell}^{\sigma_\ell} = B_\ell$ and we have property (1). As $(\chi_B)^{\sigma_\ell}$ is a character defined on $\sigma_\ell^{-1} \, G_B \, \sigma_\ell$, let

$$\varphi_{A_\ell} \;=\; (\chi_B)^{\sigma_\ell}|_{G_{A_\ell}}$$

Similarly, define

$$\varphi_{B_\ell} \;=\; (\chi_A)^{\sigma_\ell^{-1}}|_{G_{B_\ell}}$$

We see that

$$\beta \;=\; \sum_{\sigma_\ell \,\in\, G_B \backslash G_F / G_A} Ind_{G_{B_\ell}}^{G_B} \, (\varphi_{B_\ell})$$

Moreover, due to the bijection s^{-1},

$$\alpha \;=\; \sum_{s \,\in\, G_A \backslash G_F / G_B} Ind_{G_A \,\cap\, sG_B s^{-1}}^{G_A} \, (\, (\chi_B)^{s^{-1}} \,) \;=\; \sum_{\sigma_\ell \,\in\, G_B \backslash G_F / G_A} Ind_{G_{A_\ell}}^{G_A} \, (\varphi_{A_\ell}) \tag{1.3d}$$

Now, if we define $\chi_{B_\ell} = (\chi_B|_{G_{B_\ell}}) \cdot \varphi_{B_\ell}$ and $\chi_{A_\ell} = (\chi_A|_{G_{A_\ell}}) \cdot \varphi_{A_\ell}$ and $\chi_{B_\ell/B} = \chi_B|_{G_{B_\ell}}$, then

$$\beta \otimes \chi_B = \chi_B \otimes \beta = \sum_{\ell=1}^{M} Ind_{G_{B_\ell}}^{G_B} \, (\underbrace{(\chi_B|_{G_{B_\ell}}) \cdot \varphi_{B_\ell}}_{\chi_{B_\ell}}) \tag{1.3e}$$

and

$$\chi_A \otimes \alpha = \sum_{\ell=1}^{M} Ind_{G_{A_\ell}}^{G_A} \, (\underbrace{(\chi_A|_{G_{A_\ell}}) \cdot \varphi_{A_\ell}}_{\chi_{A_\ell}}) \tag{1.3f}$$

Furthermore

$$\gamma \otimes \chi_B = \chi_B \otimes \gamma = \sum_{\ell=1}^{M} Ind_{G_{B_\ell}}^{G_B} \, (\underbrace{\chi_B|_{G_{B_\ell}}}_{\chi_{B_\ell/B}})$$

When this is combined with (1.3e) ,

$$(\beta - \gamma) \otimes \chi_B = \sum_{\ell=1}^{M} \left\{ Ind_{G_{B_\ell}}^{G_B} \, (\chi_{B_\ell} - 1) \; - \; Ind_{G_{B_\ell}}^{G_B} \, (\chi_{B_\ell/B} - 1) \right\}$$

In addition, (1.3d) and (1.3f) yield

$$(\chi_A - 1) \otimes \alpha = \sum_{\ell=1}^{M} \left\{ Ind_{G_{A_\ell}}^{G_A} \, (\chi_{A_\ell} - 1) \; - \; Ind_{G_{A_\ell}}^{G_A} \, (\varphi_{A_\ell} - 1) \right\} \tag{1.3g}$$

and we have all of property (5) once it is shown that $\varphi_{A_\ell} = (\chi_{B_\ell/B})^{\sigma_\ell}$.

Because $G_{B_\ell} = \sigma_\ell \, G_{A_\ell} \, \sigma_\ell^{-1}$,

$$\varphi_{A_\ell} = (\chi_B)^{\sigma_\ell}|_{G_{A_\ell}} = (\chi_B|_{G_{B_\ell}})^{\sigma_\ell} = (\chi_{B_\ell/B})^{\sigma_\ell} \tag{1.3h}$$

Meanwhile, by inducing $(1.3e)$ and $(1.3f)$, we can obtain property (3). In particular, compare

$$\varrho \otimes \sigma \;=\; Ind_{G_B}^{G_F}(\beta \otimes \chi_B) \;=\; \sum_{\ell=1}^{M} Ind_{G_{B_\ell}}^{G_F}(\chi_{B_\ell})$$

with

$$\varrho \otimes \sigma \;=\; Ind_{G_A}^{G_F}(\chi_A \otimes \alpha) \;=\; \sum_{\ell=1}^{M} Ind_{G_{A_\ell}}^{G_F}(\chi_{A_\ell})$$

On the other hand

$$\tau \otimes \sigma \;=\; Ind_{G_B}^{G_F}(\gamma \otimes \chi_B) \;=\; \sum_{\ell=1}^{M} Ind_{G_{B_\ell}}^{G_F}(\chi_{B_\ell/B})$$

Together with property (3), this implies

$$(\varrho - \tau) \otimes \sigma \;=\; \sum_{\ell=1}^{M} \left\{ Ind_{G_{B_\ell}}^{G_F}(\chi_{B_\ell}) - Ind_{G_{B_\ell}}^{G_F}(\chi_{B_\ell/B}) \right\}$$

which is equal to

$$\sum_{\ell=1}^{M} \left\{ Ind_{G_{B_\ell}}^{G_F}(\chi_{B_\ell} - 1) \;-\; Ind_{G_{B_\ell}}^{G_F}(\chi_{B_\ell/B} - 1) \right\}$$

So we obtain one half of property (4). Induce $(1.3g)$ to produce the other half.

$$\left\{ Ind_{G_A}^{G_F}(\chi_A - 1) \right\} \otimes \sigma \;=\; \sum_{\ell=1}^{M} \left\{ Ind_{G_{A_\ell}}^{G_F}(\chi_{A_\ell} - 1) \;-\; Ind_{G_{A_\ell}}^{G_F}(\varphi_{A_\ell} - 1) \right\}$$

Now (1.3h) completes property (4). At last we proceed to verify property (2).

$$\underbrace{(\chi_A |_{G_{A_\ell}}) \cdot \varphi_{A_\ell}}_{\chi_{A_\ell}} = (\chi_A |_{G_{A_\ell}}) \cdot (\chi_{B_\ell/B})^{\sigma_\ell}$$

$$= \left[(\chi_A |_{G_{A_\ell}})^{\sigma_\ell^{-1}} \cdot \chi_{B_\ell/B} \right]^{\sigma_\ell}$$

$$= \left[\underbrace{((\chi_A)^{\sigma_\ell^{-1}} |_{G_{B_\ell}})}_{\varphi_{B_\ell}} \cdot \chi_{B_\ell/B} \right]^{\sigma_\ell}$$

$$= (\chi_{B_\ell})^{\sigma_\ell}$$

Lemma 1.2.8 is proved. ||

Proof of lemma 1.2.9 Suppose $R = \sum_i n_i \, (H_i/A \, , \, \chi_i') \in ker(b_{G/A})$. Then

$$\sum_i n_i \, Ind_{H_i/A}^{G/A} \, (\chi_i') = 0$$

If $proj : H_i \to H_i/A$ is the canonical projection, we define a character χ_i of H_i by $\chi_i = \chi_i' \circ proj$. According to 1.2.11

$$\sum_i n_i \, Ind_{H_i}^{G} \, (\chi_i) = 0$$

which implies that $infl(R) \in ker(b_G)$. Conversely, let $\sum_i n_i \, (H_i, \chi_i) \in$

$ker(b_G)$ such that $\chi_i|_A = 1$ for all i. This means

$$\sum_i n_i \, Ind_{H_i}^{G}(\chi_i) = 0$$

Moreover, we can consider the representation $\sum_i n_i Ind_{H_i/A}^{G/A}(\chi_i')$, which must be zero by lemma 1.2.11. In other words,

$$R = \sum_i n_i \, (H_i/A \, , \, \chi_i') \in ker(b_{G/A})$$

but $infl(R) = \sum_i n_i \, (H_i, \chi_i)$. ||

Proof of lemma 1.2.10 Recall that to define the root number for a character χ of a Galois group $Gal(K/E)$, we first converts χ into a character on $E^\times$ via the reciprocity map $E^\times \to Gal(K/E)^{ab}$. Therefore if we interpret χ^g as a character defined on $g^{-1}(E^\times)$, then according to the functoriality of the reciprocity map

$$\chi^g(x) = \chi \circ g(x) \quad \text{for all } x \text{ belonging } g^{-1}(E^\times)$$

By definition (see Tate [23]), for $m > 0$,

$$W(\chi) = N(P_E{}^m)^{-1/2} \sum_{x \in U_E/U_E^m} \chi^{-1}\Big(\frac{x}{\pi_E{}^{d+m}}\Big) \, \psi_{E/F}\Big(\frac{x}{\pi_E{}^{d+m}}\Big)$$

where π_E is a uniformizing parameter of the local field E, m is the conductor of χ, U_E is the unit group of the ring of integer of E, d is the order of the absolute different of the field E, $\psi_{E/F} = \psi_F \circ Tr_{E/F}$ is the composition of the trace $Tr_{E/F}$ with the canonical additive character of F (see Tate [23]), $N({P_E}^m)$ is the m-th power of the cardinality of the residue class field for E. If P_E denotes the maximal ideal in the ring of integers of F, recall that

$$U_E^i = 1 + P_E^i \qquad \text{for } i > 0$$

yield a filtration of the unit group U_E. Because $g^{-1}(U_E^i) = U_{g^{-1}(E)}^i$, the conductor of χ is the same as that of χ^g. Also, we can take $\pi_{g^{-1}(E)} = g^{-1}(\pi_E)$ to be our uniformizing parameter of $g^{-1}(E)$. Notice that the order of the absolute different of $g^{-1}(E)$ is again d because E and $g^{-1}(E)$ are algebraically as well as analytically isomorphic. Meanwhile, let us rewrite the above sum on the right hand side of the definition as

$$\sum_{\substack{g^{-1}(x) \in \\ U_{g^{-1}(E)}/U^m_{g^{-1}(E)}}} (\chi^g)^{-1}\left(\frac{g^{-1}(x)}{g^{-1}(\pi_E)^{d+m}}\right) \psi_{E/F}\left(\frac{x}{{\pi_E}^{d+m}}\right)$$

Observe that

$$Tr_{g^{-1}(E)/F}\left(\frac{g^{-1}(x)}{g^{-1}(\pi_E)^{d+m}}\right) = Tr_{E/F}\left(\frac{x}{\pi_E{}^{d+m}}\right)$$

which implies

$$\psi_{g^{-1}(E)/F}\left(\frac{g^{-1}(x)}{g^{-1}(\pi_E)^{d+m}}\right) = \psi_{E/F}\left(\frac{x}{\pi_E{}^{d+m}}\right)$$

So the sum

$$\sum_{\substack{g^{-1}(x) \in \\ U_{g^{-1}(E)}/U^m_{g^{-1}(E)}}} (\chi^g)^{-1}\left(\frac{g^{-1}(x)}{g^{-1}(\pi_E)^{d+m}}\right) \psi_{g^{-1}(E)/F}\left(\frac{g^{-1}(x)}{g^{-1}(\pi_E)^{d+m}}\right)$$

is equal to

$$\sum_{x \in U_E/U_E^m} \chi^{-1}\left(\frac{x}{\pi_E{}^{d+m}}\right) \psi_{E/F}\left(\frac{x}{\pi_E{}^{d+m}}\right)$$

Replace all $g^{-1}(x)$ by y for the sake of clarity. We see that $W(\chi) = W(\chi^g)$ because the constant $N(P_E{}^m)^{-1/2}$ is just the reciprocal of the absolute value of the sum in our definition.

As for the case $m = 0$, we note that χ^g must annihilate $g^{-1}(U_E) = U_{g^{-1}(E)}$. Hence,

$$W(\chi) = \chi(\pi_E^d) = \chi^g(\pi_{g^{-1}(E)}^d) = W(\chi^g)$$

and lemma 1.2.10 is completed. ||

Proof of lemma 1.2.11 As $\chi|_A = 1$, we can interpret χ as a character of G/A. So $Ind_{H/A}^{G/A}(\chi)$ makes sense. Being a homomorphism from G/A to the group of $[G:H]$ by $[G:H]$ invertible matrices over the complex numbers, this induced representation satisfies (see Serre [19, 3.3])

$$\text{The trace of } \underbrace{\left(Ind_{H/A}^{G/A}(\chi) \right)(x\,A)}_{\text{matrix}} = \sum_{\substack{g \in (H/A)\backslash(G/A) \\ (g x g^{-1}) A \in H/A}} \chi(g x g^{-1})$$

On the other hand, $Ind_{H/A}^{G/A}(\chi)$ defines a representation of G via the canonical projection $G \to G/A$, but this representation of G coincides with $Ind_H^G(\chi)$ according to the formula

$$\text{The trace of } \left(Ind_H^G(\chi) \right)(x) = \sum_{\substack{g \in H\backslash G \\ g x g^{-1} \in H}} \chi(g\,x\,g^{-1})$$

Notice the conditions under the two sums are equivalent. ||

Proof of lemma 1.2.12 It follows from the exact sequence that $W_{K/F}/K^\times \simeq Gal(K/F)$. So if $F \subseteq E \subseteq K$ and χ is a character of $Gal(K/E)$, then

$$Ind_{Gal(K/E)}^{Gal(K/F)}(\chi) = Ind_{W_{K/E}/K^\times}^{W_{K/F}/K^\times}(\chi)$$

Viewed as a representation of $W_{K/F}$ via the surjection $W_{K/F} \to Gal(K/F)$, $Ind_{W_{K/E}/K^\times}^{W_{K/F}/K^\times}(\chi)$ coincides with $Ind_{W_{K/E}}^{W_{K/F}}(\chi)$ according to lemma 1.2.11. ||

1.4 The kernel of Brauer induction

In this section, we state Deligne's characterization of the kernel of Brauer induction. Any new notation or definition introduced here will not be required for the subsequent chapters.

For a character χ of G, the group homomorphism from $R_+(G)$ to itself defined by the multiplication of (G, χ) is called torsion by χ. It is worth noting the formula for such multiplication

$$\left[\sum_i n_i \, (H_i, \varphi_i) \right] \cdot (G, \chi) \quad = \quad \sum_i n_i \, (H_i \, , \, \varphi_i \cdot (\chi \,|_{H_i}))$$

Because

$$b_G(H_i \, , \, \varphi_i \cdot (\chi \,|_{H_i})) \quad = \quad Ind_{H_i}^G \, (\varphi_i \cdot (\chi \,|_{H_i})) \quad = \quad \left\{ Ind_{H_i}^G \, (\varphi_i) \right\} \otimes \chi$$

the torsion homomorphism preserves the kernel of b_G. Henceforth, torsion by χ is abbreviated to $\cdot_G \, \chi$.

Also, given $H \subseteq G$, the inclusion map from $R_+(H)$ to $R_+(G)$ is denoted by i. Notice that the kernel of b_H is mapped into the kernel of of b_G under i according to lemma 1.2.1.

Theorem 1.4.1 (Deligne, Langlands). *If G is solvable, then the kernel of $b_G : R_+(G) \to R(G)$, as an additive group, is generated by the following three types of relation.*

Type I *: Let A be a cyclic group of prime order and A^* be its character group. By lemma 1.2.4*

$$S = (\{1\}, 1) - \sum_{\varphi \in A^*} (A, \varphi)$$

is a relation in $ker(b_A)$, the kernel of b_A. We say that a relation R in $ker(b_G)$ is of type I if there exists a subgroup $B \subseteq G$ with a cyclic quotient isomorphic to A such that $R = i\,(infl(S) \cdot_B \chi)$ for some character $\chi \in B^*$.

Type II *: Let A be a central extension of the direct sum of two cyclic groups with prime order ℓ. i.e. the center of A contains a subgroup Z satisfying* *the exact sequence*

$$1 \to Z \to A \to Z_\ell \oplus Z_\ell \to 1$$

Let H_1 , H_2 *be distinct subgroups of* A *containing* Z , *so that* H_1/Z , H_2/Z *are both cyclic of prime order* ℓ . *Under this circumstance,* H_1 , H_2 *must be abelian and* $H_1 \cap H_2 = Z$. *For any* $\chi_1 \in H_1^*$ *whose restriction to* Z *cannot be extended to a character of* A , *it follows from lemma 1.2.3*

$$S = (H_1 , \chi_1) - (H_2 , \mu)$$

belongs to $ker(b_A)$, *where* $\chi_1 |_Z = \mu |_Z$. *We say that a relation* R *in* $ker(b_G)$ *is of type II if there exists a subgroup* $B \subseteq G$ *with a nilpotent quotient isomorphic to* A *such that* $R = i\,(\,infl(S) \cdot_B \chi\,)$ *for some character* $\chi \in B^*$.

Type III : *Let* A *be a semidirect product of* H *by* C (*i.e.* $A = H \cdot C$ *and* $H \cap C = \{1\}$) *with*

(a) $H \neq \{1\}$

(b) C *is a non-trivial abelian normal subgroup of* A .

(c) C *is minimal in the sense that* C *contains no normal subgroup of* A *other than* $\{1\}$ *and* C *.*

In particular, we have $H \not\supseteq C$ *. For any character* $\varphi \in H^*$

$$S = (H, \varphi) - \sum_{\mu \in C^*/A} (A_\mu, \{\varphi, \mu\})$$

belongs to $ker(b_A)$ *according to lemma 1.2.3. We say that a relation* R *in* $ker(b_G)$ *is of type III if there exists a subgroup* $B \subseteq G$ *with a quotient isomorphic to* A *such that* $R = i\,(infl(S) \cdot_B \chi)$ *for some character* $\chi \in B^*$ *.*

We are not going to reproduce the proof of theorem 1.4.1 here, but Deligne's idea in that proof will be adapted to establish the main theorem in chapter 3.

CHAPTER TWO

2 Properties of the Local Root Number

Recall a variation of Brauer's theorem[1]:

Every element $v \in R(G)$ of dimension zero can be expressed as a linear combination of virtual representations of the form $Ind_H^G(\chi - 1)$ with integer coefficients, where H is an elementary subgroup of G with character χ.

We now extend the notion of root number from the abelian case to higher dimensional representations of a local Galois group. Let K be a finite Galois extension of a local field F. For us, a local field means finite extension of a p-adic number field. If ρ is a representation of the Galois group $G = Gal(K/F)$ with dimension $dim\,\rho$, then by the above theorem of Brauer

$$\rho - (dim\,\rho) \cdot 1 = \sum_i n_i \, Ind_{H_i}^G(\chi_i - 1)$$

We define the root number for ρ as follows.

[1] A proof can be found at the end of this chapter

Definition of the root number. Keeping ρ , χ_i , n_i as above, we define

$$W(\rho) = \prod_i W(\chi_i)^{n_i}$$

where each $W(\chi_i)$ is the abelian root number of the character χ_i .

It is important to remark that the validity of this definition depends on our main theorem (see below), whose proof constitutes the next chapter.

The main theorem. *Given* $\sum_i n_i Ind_{H_i}^G (\chi_i - 1) = 0$ *such that each* χ_i *is a non-trivial character of* H_i *with abelian root number* $W(\chi_i)$ *, we have*

$$\prod_i W(\chi_i)^{n_i} = 1 .$$

Meanwhile, we accept that the definition of $W(\rho)$ is legitimate and proceed to derive some basic properties of the root number.

Theorem 2.0.1. *If we assume the above main theorem and define for any given local Galois group* G *a function* ε_G *from* $R(G)$ *to the non-zero complex numbers by*

$$\varepsilon_G (\sum_j m_j V_j) = \prod_j W(V_j)^{m_j}$$

where each V_j is an irreducible representation of G, then

(0) for any representation ρ of G with a decomposition $\sum m_j V_j$ into direct sum of irreducible components, we have

$$W(\rho) \;=\; \varepsilon_G\,(\sum_j m_j\, V_j) \;=\; \prod_j W(V_j)^{m_j}$$

In other words, ε_G extends our definition of root number to the entire group $R(G)$ of virtual representations. Hence we will identify $\varepsilon_G\,(\rho)$ with $W(\rho)$ in the rest of 2.0.1.

(1) for any pair of representations ρ_1, ρ_2 of G,

$$\varepsilon_G\,(\rho_1 + \rho_2) \;=\; \varepsilon_G\,(\rho_1) \cdot \varepsilon_G\,(\rho_2)$$

In fact, the same holds when ρ_1, ρ_2 are replaced by virtual representations in $R(G)$.

(2) given a normal subgroup H in G and a representation ρ of G/H,

$$\varepsilon_{G/H}\,(\rho) \;=\; \varepsilon_G\,(\rho \circ proj)$$

Here we interpret ρ as a homomorphism from G/H to the group of $dim\,\rho \times dim\,\rho$ invertible matrices, and $proj : G \to G/H$ denotes the canonical projection.

(3)

$$\varepsilon_G\,(Ind_H^G\,v) \;=\; \varepsilon_H\,(v)$$

for any subgroup $H \subseteq G$ *and any* $v \in R(H)$ *of dimension zero.*

(4) whenever ρ *is a 1-dimensional representation of* G *,* $\varepsilon_G\,(\rho)$ *coincides with the abelian root number for* ρ *.*

Proof. Because $\sum_j m_j\,(dim\,V_j) \;=\; dim\,\rho$, we have

$$\rho \;-\; (dim\,\rho)\cdot 1 \;=\; \sum_j m_j\,(V_j \;-\; (dim\,V_j)\cdot 1)$$

Suppose that for each j

$$V_j \;-\; (dim\,V_j)\cdot 1 \;=\; \sum_{k_j} s_{k_j}\,Ind_{E_{k_j}}^G\,(\alpha_{k_j} - 1)$$

Then, not only

$$W(V_j) \;=\; \prod_{k_j} W(\alpha_{k_j})^{s_{k_j}}$$

but also

$$\rho \;-\; (dim\,\rho)\cdot 1 \;=\; \sum_j m_j \sum_{k_j} s_{k_j}\,Ind_{E_{k_j}}^G\,(\alpha_{k_j} - 1)$$

By our definition of root number

$$W(\rho) = \prod_j \Big\{ \underbrace{\prod_{k_j} W(\alpha_{k_j})^{s_{k_j}}}_{W(V_j)} \Big\}^{m_j} = \varepsilon_G \, (\sum_j m_j \, V_j)$$

This proves (0) .

As we can identify $\varepsilon_G \, (\rho)$ with $W(\rho)$ according to (0) ,

$$W(\rho_1 + \rho_2) = W(\rho_1) \cdot W(\rho_2)$$

is equivalent to (1) . However, this equality is immediate from our definition of root number. The same assertion with respect to virtual representations follows directly from the definition of ε_G . As a result, ε_G is a group homomorphism. In particular, given $v \in R(G)$, we have

$$\varepsilon_G(-v) = \varepsilon_G(v)^{-1}$$

(2) is a consequence of Brauer's theorem for G/H , lemma 1.2.11 and the definition of abelian root number.

As for (3) , because of Brauer's theorem and (1) above, it is sufficient to prove that

$$\varepsilon_G \, (Ind_H^G \, (\alpha - 1) \,) = \varepsilon_H \, (\alpha - 1) \qquad (2.0a)$$

if α is a character of H .

Applying Brauer's theorem, we obtain

$$Ind_H^G(\alpha) \ - \ [G:H]\cdot 1 \ = \ \sum_t d_t \, Ind_{A_t}^G(\nu_t - 1) \qquad (2.0b)$$

and

$$Ind_H^G(1) \ - \ [G:H]\cdot 1 \ = \ \sum_\ell e_\ell \, Ind_{B_\ell}^G(\mu_\ell - 1) \qquad (2.0c)$$

.

Together with (0) and (1) ,

$$\varepsilon_G\,(\,Ind_H^G(\alpha-1)\,) \ = \ \frac{\varepsilon_G\,(\,Ind_H^G(\alpha)\,)}{\varepsilon_G\,(\,Ind_H^G(1)\,)} \ = \ \frac{W(\,Ind_H^G(\alpha)\,)}{W(\,Ind_H^G(1)\,)} \ = \ \frac{\prod_t W(\nu_t)^{d_t}}{\prod_\ell W(\mu_\ell)^{e_\ell}} \qquad (2.0d)$$

On the other hand, subtract (2.0c) from (2.0b) . We conclude $Ind_H^G(\alpha-1)$ is equal to

$$Ind_H^G(\alpha) \ - \ Ind_H^G(1) \ = \ \sum_t d_t \, Ind_{A_t}^G(\nu_t - 1) \ - \ \sum_\ell e_\ell \, Ind_{B_\ell}^G(\mu_\ell - 1)$$

Therefore

$$Ind_H^G(\alpha - 1) \ - \ \sum_t d_t \, Ind_{A_t}^G(\nu_t - 1) \ + \ \sum_\ell e_\ell \, Ind_{B_\ell}^G(\mu_\ell - 1) \ = \ 0$$

Then by the main theorem,

$$\frac{W(\alpha)\cdot\prod_\ell W(\mu_\ell)^{e_\ell}}{\prod_t W(\nu_t)^{d_t}} = 1$$

which is equivalent to

$$W(\alpha) = \frac{\prod_t W(\nu_t)^{d_t}}{\prod_\ell W(\mu_\ell)^{e_\ell}}$$

Compare this with $(2.0d)$. We see that

$$\varepsilon_G\,(Ind_H^G\,(\alpha - 1)\,) = W(\alpha) \tag{3'}$$

$$= \frac{W(\alpha)}{W(1)}$$

$$= \frac{\varepsilon_H\,(\alpha)}{\varepsilon_H\,(1)}$$

The last equality, and consequently $(2.0a)$, hold provided that we have (4) . However, when applied to characters like α , our definition of root number indeed yields the abelian root number, as

$$\alpha - (dim\,\alpha)\cdot 1 = Ind_H^H\,(\alpha - 1)$$

Due to (0), this final argument successfully completes (4), and theorem 2.0.1 is proved. ||

Theorem 2.0.2 : *Property* (1) *and property* (4) *in theorem 2.0.1 together with* (3′) *in the above proof uniquely determine the function* ε_G . *In other words, any function on* $R(G)$ *satisfying these three properties must be the same as* ε_G .

Proof: Let $v \in R(G)$. By (4),

$$\varepsilon_G(v) = \frac{\varepsilon_G(v)}{W(1)^{\dim v}} = \frac{\varepsilon_G(v)}{\varepsilon_G(1)^{\dim v}}$$

which is equal to $\varepsilon_G(v - (\dim v)\cdot 1)$ because of (1). Now, according to Brauer's theorem

$$v - (\dim v)\cdot 1 = \sum_i n_i \, Ind_{H_i}^G(\chi_i - 1)$$

So

$$\varepsilon_G(v) = \varepsilon_G\Big(\sum_i n_i \, Ind_{H_i}^G(\chi_i - 1)\Big)$$

It follows from (1) and (3′) that

$$\varepsilon_G(v) = \prod_i W(\chi_i)^{n_i}$$

This shows that the value of $\varepsilon_G(v)$ is determined by the three properties.

||

Theorem 2.0.3. *Let χ be an unramified character of $G = Gal(K/F)$. In other words, χ annihilates the inertia group G_o. If ρ is a representation of G and $f(\rho)$ is the Artin conductor of ρ, then*

$$W(\chi \otimes \rho) = \chi(\sigma_{K/F})^{f(\rho)} \cdot W(\chi)^{dim\,\rho} \cdot W(\rho)$$

where $\sigma_{K/F}$ denotes the Frobenius automorphism in G/G_o.

Proof. First we verify the formula for the case $dim\,\rho = 1$. Both χ and ρ can be regarded as characters of $F^\times$ via the reciprocity map in this case. By the definition of abelian root number, if π_F is a uniformizing parameter of F and $m = f(\rho)$ is the conductor of the character ρ (as well as that of $\chi \otimes \rho$), then

$$W(\chi \otimes \rho) = \chi(\pi_F)^m \cdot W(\chi) \cdot W(\rho) \qquad (2.0e)$$

Because π_F is sent to the Frobenius automorphism in G/G_o under the reciprocity map, theorem 2.0.3 for $dim\,\rho = 1$ is proved.

Let $dim\,\rho > 1$. According to Brauer's theorem

$$\rho \;-\; (dim\,\rho)\cdot 1 \;=\; \sum_i n_i Ind_{H_i}^{G}\,(\alpha_i - 1) \qquad (2.0f)$$

Tensor both sides with χ.

$$(\chi \otimes \rho) \;-\; (\,dim\,\rho\,)\,\chi \;=\; \sum_i n_i\,\{\chi \otimes Ind_{H_i}^{G}\,(\alpha_i - 1)\}$$

Since $dim\,(\chi \otimes \rho) \;=\; dim\,\rho$, we can write

$$\Big\{\,(\chi \otimes \rho) \;-\; (\,dim\,(\chi \otimes \rho)\,)\cdot 1\,\Big\} \;-\; (\,dim\,\rho\,)\,\Big\{\chi - 1\Big\}$$

$$=\; \sum_i n_i \Big\{\,Ind_{H_i}^{G}\,(\,(\chi\,|_{H_i})\cdot\alpha_i \;-\; 1) \;-\; Ind_{H_i}^{G}\,(\,(\chi\,|_{H_i}) - 1\,)\,\Big\}$$

So $(\chi \otimes \rho) \;-\; (\,dim\,(\chi \otimes \rho)\,)\cdot 1$ is equal to

$$(\,dim\,\rho\,)\,\Big\{\chi - 1\Big\} \;+\; \sum_i n_i \Big\{\,Ind_{H_i}^{G}\,(\,(\chi\,|_{H_i})\cdot\alpha_i \;-\; 1) \;-\; Ind_{H_i}^{G}\,(\,(\chi\,|_{H_i}) - 1\,)\,\Big\}$$

It follows from our definition of root number that

$$W(\chi \otimes \rho) \;=\; W(\chi)^{\,dim\,\rho} \prod_i \left\{\frac{W(\,(\chi\,|_{H_i})\cdot\alpha_i\,)}{W(\,(\chi\,|_{H_i})\,)}\right\}^{n_i}$$

If $H_i = Gal(K/E_i)$ and π_{E_i} is a uniformizing parameter of E_i, then (2.0e) implies

$$W(\chi \otimes \rho) = W(\chi)^{\dim \rho} \prod_i \left\{ \frac{\chi \circ N_{E_i/F}(\pi_{E_i})^{f(\alpha_i)} \cdot W(\chi\,|_{H_i}) \cdot W(\alpha_i)}{W(\,(\chi\,|_{H_i})\,)} \right\}^{n_i}$$

As a result,

$$W(\chi \otimes \rho) = W(\chi)^{\dim \rho} \prod_i \{ \chi \circ N_{E_i/F}(\pi_{E_i})^{f(\alpha_i)} \}^{n_i} \cdot \underbrace{\prod_i \{ W(\alpha_i) \}^{n_i}}_{W(\rho)}$$

Notice $W(\rho) = \prod W(\alpha_i)^{n_i}$ because of (2.0f). Hence it remains to show that

$$\chi(\sigma_{K/F})^{f(\rho)} = \prod_i \{ \chi \circ N_{E_i/F}(\pi_{E_i})^{f(\alpha_i)} \}^{n_i}$$

Here the notation χ has been abused in an obvious way. Precisely, we identify $\sigma_{K/F} \in G/G_o$ with the uniformizing parameter π_F by means of the reciprocity map.

$$\chi(\pi_F)^{f(\rho)} = \prod_i \{ \chi(\pi_F{}^{\mathrm{f}_{E_i/F}})^{f(\alpha_i)} \}^{n_i}$$

where $\mathrm{f}_{E_i/F}$ is the residue class field degree. So it is sufficient to prove that

$$f(\rho) = \sum_i n_i \, \mathrm{f}_{E_i/F} \, f(\alpha_i) \tag{2.0g}$$

Let a_G denote the Artin representation of G. By definition of the Artin conductor (see [2, chapter VI, 4.3]),

$$f(\rho) = \langle a_G , \rho \rangle_G = \langle a_G , \rho - (dim\, \rho) \cdot 1 \rangle_G$$

and $(2.0f)$ implies

$$f(\rho) = \langle a_G , \sum_i n_i Ind_{H_i}^G (\alpha_i - 1) \rangle_G$$

According to Frobenius reciprocity

$$f(\rho) = \sum_i n_i \left[\langle a_G |_{H_i} , \alpha_i \rangle_{H_i} - \langle a_G |_{H_i} , 1 \rangle_{H_i} \right]$$

Now recall a formula for the restriction of the Artin representation:

Lemma 2.0.4 [20]. *Given a Galois extension K/F, let $\lambda_{E/F}$ be the order of the discriminant of the subextension E/F i.e. $F \subseteq E \subseteq K$ and let $\mathrm{f}_{E/F}$ be the residue class field degree. If r_H , a_H are the regular representation and the Artin representation of the Galois group $H = Gal(K/E)$ respectively, then the restriction to H of the Artin representation a_G of $Gal(K/F)$ is*

$$a_G |_H = \lambda_{E/F} \cdot r_H + \mathrm{f}_{E/F} \cdot a_H$$

Proof. Recall that the order of the different $d_{K/F}$ is related to the cardinality of the ramification group G_i by the formula [2, chapter 1 § 9, proposition 4, p.36]

$$d_{K/F} = \sum_{i=0}^{\infty} (|G_i| - 1)$$

Together with the definition of a_G (see Serre [20, chapter VI, § 2]), this implies

$$dim\, a_G = \mathfrak{f}_{K/F} \cdot d_{K/F} \qquad (2.0h)$$

When $h \in H$ is not the identity element, it follows from the definition of Artin representation that

$$tr(\, a_G(h)\,) = \mathfrak{f}_{E/F} \cdot tr(\, a_H(h)\,)$$

Here we regard a_G (resp. a_H) as a homomorphism from G (resp. H) to the group of $dim\, a_G \times dim\, a_G$ (resp. $dim\, a_H \times dim\, a_H$) invertible matrices over the complex numbers and tr denotes the trace of a matrix. For $h = 1$, $(2.0h)$ shows

$$tr(\, a_G(1)\,) = \mathfrak{f}_{K/F} \cdot d_{K/F}$$

So it remains to show

$$\mathrm{f}_{K/F} \cdot d_{K/F} \;=\; \lambda_{E/F} \cdot \underbrace{[K:E]}_{|H|} \;+\; \mathrm{f}_{E/F} \cdot (\mathrm{f}_{K/E} \cdot d_{K/E})$$

but this is the transitivity formula for discriminant [20, chapter III, § 4] in disguise. ||

Suppose λ_i is the order of the discriminant of E_i/F. Then it is a consequence of the above lemma that

$$f(\rho) \;=\; \sum_i n_i \,[\,(\,\lambda_i \;+\; \mathrm{f}_{E_i/F} \cdot f(\alpha_i)\,) \;-\; \lambda_i\,]$$

which yields (2.0g) and therefore theorem 2.0.3. ||

At the beginning of this chapter, a variation of Brauer's theorem has been used. We will now give a proof of that statement, taking for granted the original Brauer induction theorem in chapter 1 (consult Serre [19, chapter 10] for its proof). First of all, let us recall some elementary facts about nilpotent groups.

There are two equivalent definitions of nilpotent group, both of which are useful to us. Let G be a finite group. If A , B are normal subgroups of

G, let $[A, B]$ be the subgroup of G generated by commutators $aba^{-1}b^{-1}$ where $a \in A$ and $b \in B$. Observe that $[A, B]$ is also normal in G. Now, we define a sequence of subgroups G^i recursively as follows: $G^1 = G$ and $G^{i+1} = [G, G^i]$.

Definition 1 : *A finite group G is called nilpotent if there exists an integer n such that $G^n = \{1\}$.*

Because $G^{i+1} = [G, G^i]$, we note that G^i/G^{i+1} is contained in the center of G/G^{i+1}. Therefore the above definition is equivalent to

Definition 2 : *If there exists a sequence*

$$G = A_o \supset A_1 \supset, \dots, \supset A_n = \{1\}$$

of normal subgroups of G so that A_i/A_{i+1} is in the center of G/A_{i+1} for $n > i \geq 0$, then G is said to be nilpotent.

Abelian groups and *p*-groups provide abundant examples of nilpotent group. It follows from either definition that every subgroup of a nilpotent group must also be nilpotent. Moreover, any quotient of a nilpotent group remains nilpotent. Given $G \neq \{1\}$, the non-trivial subgroup A_{n-1} stays inside the center of G. In other words, all nilpotent groups have non-trivial center. Finally, we prove by induction on the order of G that

Claim I. *If H is a proper subgroup of a nilpotent group G, then the normalizer*

$$N(H) = \{ g \in G \mid gHg^{-1} = H \}$$

cannot equal H.

Proof. In the case the non-trivial center Z of G is not a subgroup of H, we conclude that $HZ \subseteq N(H)$; otherwise we apply the induction hypothesis to G/Z. ||

The following lemma appears as an exercise in Serre [19]. It is equivalent to the Brauer's theorem at the beginning of this chapter if we identify Serre's notation $f(1)$ with the dimension of the virtual representation f.

Lemma. *Each $f \in R(G)$ with $f(1) = 0$ is a $\mathbf{Z}$-linear combination of virtual representations of the form $Ind_E^G(\alpha - 1)$, where E is an elementary* *subgroup of* G *and* $\alpha \in Hom(E, \mathbf{C}^{\times})$ *.*

Proof. Remember that a subgroup E of G is called elementary if there exists a prime p so that E is a direct product of a p-group and a cyclic group of order prime to p. This definition is independent of G. With $R(G)$ the free abelian group generated by the isomorphism classes of irreducible representations of G, here are two of its subgroups that will be relevant to us.

$$R'_o(G) = \text{Subgroup generated by elements of the form } Ind_E^G(\alpha - 1)$$

$$R'(G) = \mathbf{Z} + R'_o(G)$$

We claim that $R(G) = R'(G)$ is a necessary and sufficient condition for the lemma to hold. Given $f \in R(G) = R'(G)$, if $f(1) = 0$, then $f \in R'_o(G)$ by definition, and we obtain the above lemma. Conversely, let 1_G be the trivial character of G. For every $f \in R(G)$, the virtual representation $f - f(1) \cdot 1_G$ has dimension zero, and the lemma asserts that $f - f(1) \cdot 1_G \in R'_o(G)$. This means $f \in \mathbf{Z} + R'_o(G) = R'(G)$. So we can conclude $R(G) = R'(G)$.

It is also immediate that for any subgroup H of G, the group homomorphism Ind_H^G maps $R'_o(H)$ into $R'_o(G)$ because elementary subgroups of H remain elementary in G.

Claim II. *If G is elementary, then we have $R(G) = R'(G)$.*

Proof. First, let us remark on the behavior of Ind_H^G when $H \triangleleft G$ and G/H is abelian. By lemma 1.2.4 and lemma 1.2.11,

$$Ind_H^G(1) = \sum_{\substack{\varphi \in G^* \\ \varphi|_H = 1}} \varphi$$

Here G^* is the character group of G. If we write

$$Ind_H^G(1) = [G:H]\cdot 1_G + \sum_{\substack{\varphi \in G^* \\ \varphi|_H = 1}} (\varphi - 1_G)$$

then it becomes clear that Ind_H^G maps $R'(H)$ into $R'(G)$.

Now, suppose Y is the set of all maximal subgroups of G. (H is maximal if there is no subgroup K satisfying $H \subset K \subset G$. We will exclude G from Y.) Recall from claim I that the normalizer $N(H)$ for each $H \in Y$ cannot be H, which means that $H \triangleleft G$ as H is maximal. As a result, G/H is a non-trivial group with no proper subgroup. In other words, it is cyclic of prime order. Therefore, the previous remark on Ind_H^G applies to all $H \in Y$. i.e. Ind_H^G maps $R'(H)$ into $R'(G)$ for all $H \in Y$.

We are in the position to prove claim II by induction on the order of G. When $|G| = 1$, both $R(G)$, $R'(G)$ are isomorphic to $\mathbf{Z}$. Let $|G| > 1$. Then it follows from the Brauer induction theorem in chapter 1 that $R(G)$ is generated by one dimensional representations of G together with elements in $Ind_H^G(R(H))$ where $H \in Y$. Meanwhile, the induction hypothesis implies $R(H) = R'(H)$ for all $H \in Y$. So $Ind_H^G(R(H)) = Ind_H^G(R'(H)) \subseteq R'(G)$. In addition, since G is elementary, we conclude that for every one dimensional representation (i.e. character) φ of G

$$\varphi = 1_G + (\varphi - 1_G) \in \mathbf{Z} + R_o'(G) = R'(G)$$

In summary, $R(G) = R'(G)$. ||

Having established the above claim, we proceed to the general case when G is not necessarily elementary. Suppose X is the set of all elementary subgroups of G. According to the Brauer's induction theorem in chapter 1,

$$1_G = \sum_{E \in X} Ind_E^G(f_E) \qquad \text{where } f_E \in R(E).$$

Given $\rho \in R(G)$, let $\rho_E = f_E \otimes Res_E(\rho)$, where Res_E denotes the usual restriction map from $R(G)$ to $R(E)$. Then

$$\sum_{E \in X} Ind_E^G(\rho_E) = \sum_{E \in X} Ind_E^G(f_E) \otimes \rho = 1_G \otimes \rho = \rho$$

In case $\rho(1) = 0$, it follows that $\rho_E(1) = 0$ and $\rho_E \in R_o'(E)$ by claim II. However, remember Ind_E^G maps $R_o'(E)$ into $R_o'(G)$. Hence

$$\rho(1) = 0 \implies \rho = \sum_{E \in X} Ind_E^G(\rho_E) \in R_o'(G)$$

and we arrive at the lemma, which is equivalent to $R'(G) = R(G)$ as pointed out before. ||

CHAPTER THREE

3 Root Number Identities

In this chapter we prove the main theorem stated earlier, using the three fundamental root number identities discussed in section 3.1. First we assume the local Galois group $Gal(K/F)$ is nilpotent. Section 3.2 establishes the main theorem for this particular case. When $Gal(K/F)$ is not nilpotent, we need the extra dimension in Weil group to complete the argument. So a Weil group version of the main theorem is formulated and proved in section 3.3. We end the chapter with Tate's outline [23] of how to extend the definition of root number to the context of Weil groups.

Unless we state otherwise, all the fields are finite extensions of a p-adic number field. i.e. they are local fields. We will say that a field X is a *subfield* of a field extension B/A if $A \subseteq X \subseteq B$. Such X is called *proper* in case it is neither A nor B. Throughout this chapter, by a quasi-character on the multiplicative group of a local field F we mean a continuous homomorphism from $F^{\times}$ to the non-zero complex numbers. The root number for a quasi-character φ will be denoted by $W(\varphi)$. It is defined by the same formula given in the introduction. (See definition of the abelian root number.)

3.1 Three fundamental identities

There are three root number identities that mirror the generators of the kernel of Brauer induction in theorem 1.4.1. In some sense special cases of the main theorem, these identities are the subject of the next chapter and will not be proved here.

For any abelian Galois extension E/F and quasi-character φ on $F^\times$,

$$W(\varphi \circ N_{E/F}) \prod_{\mu \in S(E/F)} W(\mu) = \prod_{\mu \in S(E/F)} W(\varphi \cdot \mu)$$

where $S(E/F)$ consists of characters of $F^\times$ which annihilate the norm group $N_{E/F}(E^\times)$. **This is our 1st identity.**

As a demonstration, we assume φ has finite order for the moment and translate the 1st identity into a special case of our main theorem. First,

Lemma 3.1.1. Let $G = Gal(K/F)$ be abelian and G^* be its character group. If χ is a character of $H = Gal(K/E) \subseteq G$, then

$$W(\chi) \prod_{\substack{\varphi' \in G^* \\ \varphi'|_H = 1}} W(\varphi') = \prod_{\substack{\varphi \in G^* \\ \varphi|_H = \chi}} W(\varphi)$$

follows from the 1st identity.

Proof. Let us identify χ as a character of $E^\times$ and φ, φ' as characters of $F^\times$ via the reciprocity map. Then $\varphi \circ N_{E/F} = \chi$. Moreover, if we fix one such φ, all others in G^* with the same restriction $\varphi|_H = \chi$ will be of the form $\varphi \cdot \varphi'$. Finally, each φ' can be interpreted as a character of $Gal(E/F)$ and therefore identified with some μ in $S(E/F)$. ||

Conversely, if we start with an abelian extension E/F and a quasi-character φ of finite order, then the kernel of φ must be a norm group $N_{B/F}(B^\times)$ such that B/F is cyclic. So the field K defined to be the composition $E \cdot B$ is abelian over F. As in lemma 3.1.1, let $G = Gal(K/F)$ and $H = Gal(K/E)$. Via the reciprocity map, φ can be regarded as a character of G. Suppose we define $\chi = \varphi|_H$. It is a consequence of lemma 1.2.4 that

$$Ind_H^G(\chi - 1) - \Big\{ \sum_{\substack{\varphi \in G^* \\ \varphi|_H = \chi}} (\varphi - 1) - \sum_{\substack{\varphi' \in G^* \\ \varphi'|_H = 1}} (\varphi' - 1) \Big\} = 0$$

Hence we expect from the main theorem

$$W(\chi) \prod_{\substack{\varphi' \in G^* \\ \varphi'|_H = 1}} W(\varphi') = \prod_{\substack{\varphi \in G^* \\ \varphi|_H = \chi}} W(\varphi)$$

which is the 1st identity as explained in the proof of lemma 3.1.1. In this sense, we say the 1st identity is derived from a special case of the main theorem.

We proceed to state the other two root number identities.

Suppose $G = Gal(K/F)$ is the direct sum $Z_\ell \oplus Z_\ell$ of two cyclic group of prime order ℓ. Let χ_K be a character of $K^\times$ such that $\chi_K \circ \sigma = \chi_K$ for each $\sigma \in G$ and $\chi_K \neq \chi_F \circ N_{K/F}$ for each character χ_F of $F^\times$. Given two distinct subfields L_1, L_2 of K/F, both of which have degree ℓ over F, if χ_{L_1} and χ_{L_2} are characters of $L_1^\times$ and $L_2^\times$ respectively satisfying

$$\chi_{L_1} \circ N_{K/L_1} = \chi_K = \chi_{L_2} \circ N_{K/L_2}$$

then

$$W(\chi_{L_1}) \prod_{\mu \in S(L_1/F)} W(\mu) = W(\chi_{L_2}) \prod_{\mu' \in S(L_2/F)} W(\mu')$$

where $S(L_i/F)$ consists of characters of $F^\times$ annihilating $N_{L_i/F}(L_i^\times)$. **This is the 2nd identity.**

Finally, let $G = Gal(K/F)$ be a semi-direct product $H \cdot C$ such that

(a) $H \neq \{1\}$

(b) C is a non-trivial abelian normal subgroup which is contained in every non-trivial normal subgroup of G.

Suppose $C = Gal(K/L)$ and $H = Gal(K/E)$. Consider the G-action on C^*, the character group of C, by conjugation. If T is a set of representatives of the orbits of this G-action, we denote the stabilizer of $\mu \in T$ by $G_\mu = Gal(K/F_\mu)$. Notice that a representative μ determines G_μ up to a conjugacy class. Moreover, we have $G_\mu = (G_\mu \cap H) \cdot C$ and a character μ' of G_μ defined by

$$\mu'(h\,c) = \mu(c) \qquad \text{where } h \in G_\mu \cap H \text{ and } c \in C$$

In other words, μ' extends μ. Now for any quasi-character χ on $F^\times$,

$$W(\chi \circ N_{E/F}) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu') \quad = \quad W(\chi) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\, \mu' \cdot (\chi \circ N_{F_\mu/F})\,)$$

This is the 3rd identity. Here we interpret μ' as a character of $F_\mu^\times$ via the reciprocity map.

3.2 The existence of local root numbers

By a local Galois group we mean the Galois group of a finite Galois extension over a local field. Recall from chapter 2

The main theorem:

Let G be a local Galois group. Given $\sum_i n_i Ind_{H_i}^G(\chi_i - 1) = 0$ such that each n_i is an integer and each χ_i is a character of H_i with abelian root number $W(\chi_i)$, we have $\prod_i W(\chi_i)^{n_i} = 1$.

Its proof is broken into three parts: the abelian case, the nilpotent case and the general case. Section 3.2 addresses the first two cases, while the proof of the general case appears in section 3.3. We will assume all three root number identities in 3.1 throughout the remainder of chapter 3. First,

Theorem 3.2.0. *If G is abelian, then the 1st identity implies the main theorem.*

Proof. Let $(H,\chi) \in R_+(G)$. By lemma 1.2.4, we conclude that

$$Ind_H^G(\chi) \quad = \quad \sum_{\substack{\varphi \in G^* \\ \varphi|_H = \chi}} \varphi$$

or equivalently,

$$(H,\chi) \; - \; \sum_{\varphi|_H = \chi} (G,\varphi)$$

belongs to $ker(b_G)$, the kernel of the ring homomorphism b_G in 1.1.

In particular, the following belongs to $ker(b_G)$.

$$(H,\chi) - (H,1) \; - \sum_{\varphi|_H = \chi} (G,\varphi) \; + \sum_{\varphi'|_H = 1} (G,\varphi')$$

Since G is abelian, both φ and φ' exist, and the number of φ is equal to the number of φ'. Therefore,

$$(H,\chi) - (H,1) \; - \sum_{\varphi|_H = \chi} \left[(G,\varphi) - (G,1)\right] \; + \sum_{\varphi'|_H = 1} \left[(G,\varphi') - (G,1)\right]$$

is in $ker(b_G)$. Meanwhile, according to lemma 3.1.1, the 1st identity asserts that

$$\frac{\mathrm{W}(\chi) \prod_{\varphi'|_{\mathrm{H}} = 1} \mathrm{W}(\varphi')}{\prod_{\varphi|_{\mathrm{H}} = \chi} \mathrm{W}(\varphi)} \; = \; 1 \, .$$

Now we put this observation into the perspective of our main theorem. Suppose $\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right] \in ker(b_G)$. We have already seen that

$$\underbrace{\sum_i n_i \left\{ (H_i, \chi_i) - (H_i, 1) - \sum_{\varphi_i|_{H_i} = \chi_i} \left[(G, \varphi_i) - (G, 1)\right] + \sum_{\varphi'_i|_{H_i} = 1} \left[(G, \varphi'_i) - (G, 1)\right] \right\}}_{R}$$

is in $ker(b_G)$. Let us denote this relation by R . Just as before, the 1st identity implies

$$\prod_i \left\{ \frac{W(\chi_i) \prod_{\varphi'_i|_{H_i} = 1} W(\varphi'_i)}{\prod_{\varphi_i|_{H_i} = \chi_i} W(\varphi_i)} \right\}^{n_i} = 1$$

due to lemma 3.1.1.

So, to complete the proof of theorem 3.2.0, we must show

$$\prod_i \left\{ \frac{\prod_{\varphi_i|_{H_i} = \chi_i} W(\varphi_i)}{\prod_{\varphi'_i|_{H_i} = 1} W(\varphi'_i)} \right\}^{n_i} = 1 \tag{3.2a}$$

As both R and $\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right]$ belong to $ker(b_G)$, their difference $\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right] - R$ stays inside the kernel as well.

$$\sum_i n_i \left\{ \sum_{\varphi_i|_{H_i} = \chi_i} \left[(G, \varphi_i) - (G, 1)\right] - \sum_{\varphi'|_{H_i} = 1} \left[(G, \varphi'_i) - (G, 1)\right] \right\} \in ker(b_G)$$

which means

$$\sum_i n_i \left\{ \sum_{\varphi_i|_{H_i} = \chi_i} (\varphi_i - 1) - \sum_{\varphi'|_{H_i} = 1} (\varphi'_i - 1) \right\} = 0$$

However, being irreducible characters of G, all the φ_i and φ'_i constitute a **C**-linearly independent set of class functions (see Serre [19, 2.5]). Consequently the exponents of $W(\varphi_i)$ on the left hand side of $(3.2a)$ must add up to zero, and so are the exponents of $W(\varphi'_i)$. We have proved $(3.2a)$ and hence theorem 3.2.0. ||

With the abelian case established, the next two theorems complete the nilpotent case.

Theorem 3.2.1. *If G is nilpotent, then the 1st and the 2nd identity imply the main theorem.*

Proof. Because G is nilpotent, its center Z is non-trivial. Assume $\sum_i n_i \Big[(H_i, \chi_i) - (H_i, 1)\Big] \in ker(b_G)$. It follows from lemma 1.2.6 that

$$(H_i, \chi_i) - (H_i, 1) - \sum_{\chi'_i|H_i = \chi_i} (H_i Z, \chi'_i) + \sum_{\varphi_i|H_i = 1} (H_i Z, \varphi_i)$$

is in $ker(b_{H_i Z})$. Consequently,

$$\sum_i n_i \left\{ \sum_{\chi'_i|H_i = \chi_i} (H_i Z, \chi'_i) - \sum_{\varphi_i|H_i = 1} (H_i Z, \varphi_i) \right\}$$

must belong to $ker(b_G)$.

Moreover, because there exists at least one χ_i' as explained in the proof of lemma 1.2.6, the number of χ_i' is equal to the number of φ_i. Thus we have

$$\sum_i n_i \underbrace{\left\{ \sum_{\chi_i'|_{H_i} = \chi_i} \Big[(H_iZ,\chi_i') - (H_iZ,1)\Big] - \sum_{\varphi_i|_{H_i} = 1} \Big[(H_iZ,\varphi_i) - (H_iZ,1)\Big] \right\}}_{S_i}$$

belongs to $ker(b_G)$.

Let $\sum_i n_i S_i$ represent this last relation. Then

$$\sum_i n_i \Big[(H_i,\chi_i) - (H_i,1)\Big] = \sum_i n_i S_i + \sum_i n_i \left\{ \underbrace{\Big[(H_i,\chi_i) - (H_i,1)\Big] - S_i}_{T_i} \right\}$$

If T_i denotes $\Big[(H_i,\chi_i) - (H_i,1)\Big] - S_i$ on the right hand side of the above equality, we claim that

Claim. $T_i \in ker(b_{H_iZ})$ *implies*

$$\frac{\mathrm{W}(\chi_i) \prod_{\varphi_i|_{\mathrm{H_i}} = 1} \mathrm{W}(\varphi_i)}{\prod_{\chi_i'|_{\mathrm{H_i}} = \chi_i} \mathrm{W}(\chi_i')} = 1\,.$$

Proof. Notice that not only is $ker(\chi_i)$ normal in H_i, it is also a normal subgroup of H_iZ. According to lemma 1.2.9, T_i comes from a similar relation in $ker(b_{H_iZ/ker(\chi_i)})$ via the map *infl*. However, the quotient $H_iZ/ker(\chi_i)$ is abelian because the commutator subgroup $[H_iZ, H_iZ] =$

$[H_i, H_i] \subseteq ker(\chi_i)$. Hence theorem 3.2.0 applies, and our claim follows, as the abelian root number is insensitive to *infl* . ||

As a result of the above claim,

$$\prod_i \left\{ \frac{W(\chi_i) \prod_{\varphi_i|_{H_i} = 1} W(\varphi_i)}{\prod_{\chi_i'|_{H_i} = \chi_i} W(\chi_i')} \right\}^{n_i} = 1 .$$

So it remains to prove that

$$\prod_i \left\{ \frac{\prod_{\chi_i'|_{H_i} = \chi_i} W(\chi_i')}{\prod_{\varphi_i|_{H_i} = 1} W(\varphi_i)} \right\}^{n_i} = 1 \qquad (3.2b).$$

Because $\sum_i n_i S_i \in ker(b_G)$, this particular identity $(3.2b)$, and therefore theorem 3.2.1, follow from

Theorem 3.2.2. *If G is nilpotent with non-trivial center Z and we have $\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right] \in ker(b_G)$ such that $Z \subseteq H_i$ for all i, then*

$$\prod_i W(\chi_i)^{n_i} = 1$$

Proof. We are going to prove theorem 3.2.2 by induction on $|G/Z|$. When the order of G/Z is 1, theorem 3.2.0 applies. Hence, let us assume

$|G/Z| > 1$. Because G is nilpotent, so is G/Z. By the definition of nilpotent group (see chapter 2), there exists a normal subgroup G_1 of G such that G_1/Z is non-trivial and is contained in the center of G/Z. Select a subgroup C from G_1 with $Z \subset C$ and $|C/Z| = l$ a prime. Then C must be abelian as C modulo its own center is isomorphic to a quotient of C/Z which is cyclic. Moreover, being in the center of G/Z, the quotient C/Z is normal in G/Z, and therefore $C \lhd G$. Consequently, G contains an abelian normal subgroup C that is central modulo Z with $[C:Z] = l$ a prime.

Suppose theorem 3.2.2 holds for any nilpotent group G such that $k \geq |G/Z|$. Given G with $|G/Z| = k+1$, we consider the following relation in $ker(b_{H_iC})$, which is obtained from lemma 1.2.3.

$$(H_i, \chi_i) - (H_i, 1) - \left\{ \sum_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_{H_i \cap C} = \mu|_{H_i \cap C}}} ((H_iC)_\mu, \{\chi_i, \mu\}) - \sum_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_{H_i \cap C} = 1}} ((H_iC)_{\mu'}, \{1, \mu'\}) \right\} \qquad (3.2c)$$

It is understood that if $H_i \supseteq C$, then the brace at the end is equal to $(H_i, \chi_i) - (H_i, 1)$, or equivalently $(3.2c)$ becomes zero.

Suppose C is not contained in H_i. On one hand,

$$\sum_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_{H_i \cap C} = \mu|_{H_i \cap C}}} ((H_iC)_\mu, 1) - \sum_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_{H_i \cap C} = 1}} ((H_iC)_{\mu'}, 1)$$

can be viewed as an element of $R_+((H_iC)/C)$; on the other hand, the virtual representation

$$\sigma = \sum_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_{H_i \cap C} = \mu|_{H_i \cap C}}} Ind_{(H_iC)_\mu}^{H_iC}(1) - \sum_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_{H_i \cap C} = 1}} Ind_{(H_iC)_{\mu'}}^{H_iC}(1)$$

has dimension zero because the relation (3.2c) implies $\sigma = Ind_{H_i}^{H_iC}(\chi_i) - Ind_{H_i}^{H_iC}(1)$. It follows from lemma 1.2.11 and Brauer's theorem (chapter 2) that

$$\sigma = \sum_j m_{ij}\, Ind_{K_{ij}}^{H_iC}(\alpha_{ij} - 1)$$

where all K_{ij} contain C and all α_{ij} annihilate C.

In the case C is already inside H_i, we notice that the virtual representation $\sigma = 0$. So, K_{ij} and α_{ij} exist only when C is not contained in H_i.

Other than this exceptional case ($H_i \supseteq C$), we see that

$$\sum_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_{H_i \cap C} = \mu|_{H_i \cap C}}} ((H_iC)_\mu, 1) - \sum_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_{H_i \cap C} = 1}} ((H_iC)_{\mu'}, 1)$$

$$- \sum_j m_{ij} \left[(K_{ij}, \alpha_{ij}) - (K_{ij}, 1)\right]$$

is a relation in $ker(b_{H_iC})$, and due to (3.2c), so is

$$(H_i, \chi_i) - (H_i, 1) - \left\{M_i - N_i\right\} - \sum_j m_{ij} \left[(K_{ij}, \alpha_{ij}) - (K_{ij}, 1)\right] \qquad (3.2d)$$

if

$$M_i = \sum_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_{H_i \cap C} = \mu|_{H_i \cap C}}} \left[(\,(H_iC)_\mu\,,\ \{\chi_i, \mu\}\,) - (\,(H_iC)_\mu\,,\ 1\,)\right]$$

and

$$N_i = \sum_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_{H_i \cap C} = 1}} \left[(\,(H_iC)_{\mu'}\,,\ \{1, \mu'\}\,) - (\,(H_iC)_{\mu'}\,,\ 1\,)\right]$$

In the case $H_i \supseteq C$, the above relation (3.2d) can be adopted. Simply take $M_i = (H_i, \chi_i) - (H_i, 1)$ and $N_i = 0$. Also the terms involving K_{ij} do not exist in this case as explained before.

Now, given $\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right] \in ker(b_G)$ with $Z \subseteq H_i$, we can conclude that both

$$\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right] - \sum_i n_i \left\{M_i - N_i\right\} - \sum_{i,j} n_i m_{ij} \left[(K_{ij}, \alpha_{ij}) - (K_{ij}, 1)\right]$$

and

$$\sum_i n_i \left\{M_i - N_i\right\} + \sum_{i,j} n_i m_{ij} \left[(K_{ij}, \alpha_{ij}) - (K_{ij}, 1)\right]$$

belong to $ker(b_G)$.

These two relations in $ker(b_G)$ will be dealt with separately.

First, C is contained in the subgroups $(H_iC)_\mu$ and $(H_iC)_{\mu'}$ which appear in the sums M_i and N_i respectively. Also all $K_{ij} \supseteq C$ by construction. Hence, the identity

$$\left\{ \prod_i \left[\frac{\prod_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_{H_i\cap C} = \mu|_{H_i\cap C}}} W(\{\chi_i, \mu\})}{\prod_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_{H_i\cap C} = 1}} W(\{1, \mu'\})} \right]^{n_i} \right\} \prod_{i,j} W(\alpha_{ij})^{n_i m_{ij}} = 1 \qquad (3.2e)$$

comes from the second relation $\sum_i n_i \left\{M_i - N_i\right\} + \sum_{i,j} n_i m_{ij} \left[(K_{ij}, \alpha_{ij}) - (K_{ij}, 1)\right]$ according to the following claim whose proof appears at the end of this section.

Claim I. *If* $\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right] \in ker(b_G)$ *such that* $C \subseteq H_i$, then the induction hypothesis of theorem 3.2.2 implies $\prod_i W(\chi_i)^{n_i} = 1$.

Next, we look at the first relation,

$$\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right] - \sum_i n_i \left\{M_i - N_i\right\} - \sum_{i,j} n_i m_{ij} \left[(K_{ij}, \alpha_{ij}) - (K_{ij}, 1)\right]$$

We have already seen earlier (cf. (3.2*d*)) that

$$(H_i, \chi_i) - (H_i, 1) - \left\{M_i - N_i\right\} - \sum_j m_{ij} \left[(K_{ij}, \alpha_{ij}) - (K_{ij}, 1)\right]$$

belongs to $ker(b_{H_iC})$. So, the identity

$$\frac{\mathrm{W}(\chi_i) \prod_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_{H_i \cap C} = 1}} \mathrm{W}(\{1, \mu'\})}{\prod_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_{H_i \cap C} = \mu|_{H_i \cap C}}} W(\{\chi_i, \mu\}) \ \prod_j W(\alpha_{ij})^{m_{ij}}} = 1 \qquad (3.2f)$$

results from the induction hypothesis if $G \neq H_iC$, as we assume $Z \subseteq H_i$.

In the case $G = H_iC$, we need a more specific description of subgroups K_{ij} as well as their characters α_{ij}, which have been constructed by means of Brauer's theorem such that

$$\sum_j m_{ij} \, Ind_{K_{ij}}^{H_iC} (\alpha_{ij} - 1)$$

$$= \underbrace{\sum_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_{H_i \cap C} = \mu|_{H_i \cap C}}} Ind_{(H_iC)_\mu}^{H_iC} (1)}_{P} - \underbrace{\sum_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_{H_i \cap C} = 1}} Ind_{(H_iC)_{\mu'}}^{H_iC} (1)}_{Q}$$

where all K_{ij} contain C and all α_{ij} annihilate C. To simplify the notation, we write this defining property of K_{ij} and α_{ij} as

$$P - Q = \sum_j m_{ij} \, Ind_{K_{ij}}^{H_iC} (\alpha_{ij} - 1) \qquad (3.2g)$$

Since K_{ij} and α_{ij} exist only when C is not contained in H_i, let us assume that $H_i \not\supseteq C$. Taking into account $Z \subseteq H_i$ and $[C:Z] = l$ a prime, we can conclude that $H_i \cap C = Z$. As a result, the number of μ' in the second sum Q on the left hand side of $(3.2g)$ with the condition $\mu' \mid_{H_i \cap C} = 1$ must be exactly l. These μ' form a cyclic group of prime order l and their respective stabilizers $(H_iC)_{\mu'}$ are all identical. On contrary, in the first sum P on the left hand side of $(3.2g)$, we observe the number of such character $\mu \in C^*/(H_iC)$ is either 1 or l. To summarize,

Claim II. *Assume $H_i \not\supseteq C$. Then the sum Q consists of l terms and we have $H_iC = (H_iC)_{\mu'}$, while the sum P either contains l terms or just contain one term, according to whether $[H_iC : (H_iC)_\mu]$ equals one or l.*

We defer the proof just as in claim I. The above claim yields two scenarios. If P contains l terms, then $[H_iC : (H_iC)_\mu] = 1$ and $P - Q = 0$. So K_{ij} and α_{ij} are redundant. The relation $(3.2d)$ is reduced to

$$(H_i, \chi_i) - (H_i, 1) \quad - \left\{ \underbrace{\sum_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_Z = \mu|_Z}} \Big[(H_iC, \{\chi_i, \mu\}) - (H_iC, 1)\Big]}_{M_i} \right.$$

$$- \underbrace{\sum_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_Z = 1}} \Big[(H_iC, \{1, \mu'\}) - (H_iC, 1)\Big]}_{N_i} \Bigg\}$$

If P contains just one term, then $[H_iC : (H_iC)_\mu] = l$ and

$$P - Q = Ind_{(H_iC)_\mu}^{H_iC}(1) - l(1)$$

To determine K_{ij} and α_{ij} in this second scenario, we rewrite the right hand side of the above equality by

Claim III. *The stabilizer $(H_iC)_\mu$ is normal in H_iC. Moreover, we obtain the decomposition*

$$Ind_{(H_iC)_\mu}^{H_iC}(1) = \sum_{\substack{\tau \in (H_iC)^* \\ \tau|_{(H_iC)_\mu}=1}} \tau$$

where $(H_iC)^*$ stands for the character group of H_iC.

Pending the proof at the end, we apply this claim to rewrite

$$P - Q = \sum_{\substack{\tau \in (H_iC)^* \\ \tau|_{(H_iC)_\mu}=1}} (\tau - 1)$$

Compare $\sum_{\substack{\tau \in (H_iC)^* \\ \tau|_{(H_iC)_\mu}=1}} (\tau - 1)$ with the right hand side of $(3.2g)$. It follows that we can take $K_{ij} = H_iC$ and $\alpha_{ij} = \tau$ with $m_{ij} = 1$.

Then the relation (3.2*d*) becomes

$$(H_i,\chi_i)-(H_i,1) \;-\; \Bigg\{ \underbrace{\Big[\big((H_iC)_\mu\,,\,\{\chi_i,\mu\}\big)-\big((H_iC)_\mu\,,\,1\big)\Big]}_{M_i}$$

$$-\underbrace{\sum_{\substack{\mu'\,\in\, C^*/(H_iC)\\ \mu'|_Z\,=\,1}}\Big[(H_iC,\{1,\mu'\})-(H_iC,1)\Big]\Bigg\}}_{N_i} \;-\; \sum_{\substack{\tau\,\in\,(H_iC)^*\\ \tau|_{(H_iC)_\mu}=1}}\Big[(H_iC,\tau)-(H_iC,1)\Big]$$

Our goal is to establish the same root number identity (3.2*f*) from the relation (3.2*d*) for the case $G = H_iC$. So far, we have seen the relation (3.2*d*), which belongs to $ker(b_{H_iC})$, in three different forms:

Case 1 $C \subseteq H_i$. Then we may set $M_i = (H_i,\chi_i) - (H_i,1)$ and $N_i = 0$. In this case (3.2*d*) is zero, and identity (3.2*f*) is a triviality.

Case 2 $C \nsubseteq H_i$ **and** $[H_iC : (H_iC)_\mu] = 1$. Then (3.2*d*) is reduced to

$$(H_i,\chi_i)-(H_i,1) \;-\; \Bigg\{ \underbrace{\sum_{\substack{\mu\,\in\, C^*\\ \chi_i|_Z\,=\,\mu|_Z}}\Big[(H_iC,\{\chi_i,\mu\})-(H_iC,1)\Big]}_{M_i}$$

$$-\underbrace{\sum_{\substack{\mu'\,\in\, C^*\\ \mu'|_Z\,=\,1}}\Big[(H_iC,\{1,\mu'\})-(H_iC,1)\Big]\Bigg\}}_{N_i}$$

Case 3 $C \not\subseteq H_i$ **and** $[H_iC : (H_iC)_\mu] = l$. Then the relation $(3.2d)$ becomes

$$(H_i, \chi_i) - (H_i, 1) - \Bigg\{ \underbrace{\Big[((H_iC)_\mu, \{\chi_i, \mu\}) - ((H_iC)_\mu, 1)\Big]}_{M_i}$$

$$- \underbrace{\sum_{\substack{\mu' \in C^* \\ \mu'|_Z = 1}} \Big[(H_iC, \{1, \mu'\}) - (H_iC, 1)\Big]}_{N_i} \Bigg\} - \sum_{\substack{\tau \in (H_iC)^* \\ \tau|_{(H_iC)_\mu} = 1}} \Big[(H_iC, \tau) - (H_iC, 1)\Big]$$

Fortunately, our next claim, which will be proved later, shows that the induction hypothesis will handle all but one extreme case.

Claim IV. *The fact that* C *is central modulo* Z *implies* $H_i \lhd G = H_iC$. *In addition,* $A = \bigcap_{g \in G} g\, ker(\chi_i)\, g^{-1}$ *is not only a normal subgroup of* $G = H_iC$ *but also a normal subgroup of* $(H_iC)_\mu$.

According to lemma 1.2.9, we can now conclude that the relation $(3.2d)$ in $ker(b_{H_iC})$ comes from a similar relation in $ker(b_{H_iC/A})$ regardless of case 1, 2 or 3. With $G = H_iC$, let us denote the center of G/A by $Z(G/A)$. Then

$$|G/Z| \geq |G|/|ZA| = |G/A|/|(ZA)/A| \geq |G/A|/|Z(G/A)|$$

The first inequality from the left is strict unless $A \subseteq Z$, and the last inequality is strict unless $(ZA)/A = Z(G/A)$. Consequently, applying the induction hypothesis to the relation in $ker(b_{H_iC/A})$, which is inflated to $(3.2d)$, yields the identity $(3.2f)$, unless both $A \subseteq Z$ and $Z/A = Z(G/A)$ are true.

It remains to consider the extreme case in which all of the followings hold

(i) $G = H_iC$

(ii) $C \not\subseteq H_i$

(iii) $A \subseteq Z$

(iv) $Z/A = Z(G/A)$

First of all we note that $G/A = (H_iC)/A$ is equal to $(H_i/A)\cdot(C/A)$. This product does make sense because the subgroup $A \subseteq Z = H_i \cap C$ is normal in G and $C/A \triangleleft G/A$. Also, we have $H_i/A \cap C/A = Z/A$. Besides, it follows from claim IV that $H_i/A \triangleleft G/A$. As a matter of fact, since

$$A = \bigcap_{g \in G} g \; ker(\chi_i) \; g^{-1} = \underbrace{\bigcap_{g \in G} ker(\chi_i^{g^{-1}}) \supseteq [H_i, H_i]}_{H_i \lhd G \text{ by claim IV}} \tag{3.2h}$$

we see that the commutator subgroup $[H_i/A \;,\; H_i/A]$ must be trivial, and therefore H_i/A is abelian. In addition, if $\chi_i(z) = 1$ with $z \in Z$, then, by the definition of A, we notice z must be inside A. Hence the quotient Z/A is cyclic.

Recall that in case 2, we have $C \nsubseteq H_i$ and $[H_iC : (H_iC)_\mu] = 1$. Suppose $\mu \in C^*$ such that $\chi_i \mid_Z = \mu \mid_Z$. Then given $h \in H_i$ and $c \in C$,

$$\mu(hch^{-1}) = \mu(c) \implies 1 = \mu(hch^{-1}c^{-1})$$

Because the two subgroups H_i and C are normal in H_iC and the intersection $H_i \cap C$ coincides with Z, the commutator $hch^{-1}c^{-1}$ always stay inside Z. As explained above, it follows from the definition of A that

$$\mu(hch^{-1}) = \mu(c) \implies 1 = \mu(hch^{-1}c^{-1}) \implies hch^{-1}c^{-1} \in A$$

(3.2*i*)

Since (3.2*h*) confirms H_i/A is abelian, (3.2*i*) means that the premise $[H_iC : (H_iC)_\mu] = 1$ in case 2 implies H_i is central modulo A. Now, adding condition (iii) and condition (iv) , we see that H_i is central modulo A if and only if $H_i/A = Z/A$, which contradicts the assumption $| G/Z | > 1$. In other words, case 2 can be handled solely by the induction hypothesis, while (iii) and (iv) only occur in case 3.

In summary, by assuming (i) , (ii) , (iii) and (iv) , we can conclude that

(a) $G/A = (H_i/A) \cdot (C/A)$.

(b) $H_i/A \cap C/A = Z/A$.

(c) H_i/A is an abelian normal subgroup of $(H_iC)/A$.

(d) $ker(\chi_i |_Z) = A$.

(e) $[H_iC : (H_iC)_\mu] = l$ (case 3).

Claim V. *Suppose* $G = H_iC$ *and* $C \not\subseteq H_i$. *If*

$$A = \bigcap_{g \in G} g\, ker(\chi_i)\, g^{-1}$$

is a subgroup of Z *such that* Z/A *coincides with the center of* G/A *, then* $(3.2f)$ *is the same as the 2nd identity.*

Once claim V is proved, $(3.2f)$ follows from $(3.2d)$, regardless of whether $G = H_iC$ or not.

Now, for each i , we have established a root number identity $(3.2f)$. Take the product of these root number identities over all i .

$$\prod_i \left\{ \frac{W(\chi_i) \prod_{\substack{\mu' \in C^*/(H_iC) \\ \mu'|_{H_i \cap C} = 1}} W(\{1, \mu'\})}{\prod_{\substack{\mu \in C^*/(H_iC) \\ \chi_i|_{H_i \cap C} = \mu|_{H_i \cap C}}} W(\{\chi_i, \mu\}) \ \prod_j W(\alpha_{ij})^{m_{ij}}} \right\}^{n_i} = 1$$

Multiply the above identity by $(3.2e)$. We arrive at the result of theorem 3.2.2 and subsequently that of theorem 3.2.1 as well. ||

To complete the proof of theorem 3.2.2, we now verify claim I, II, III, IV and V.

Claim I. If $\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right] \in ker(b_G)$ *such that* $C \subseteq H_i$,

then the induction hypothesis of theorem 3.2.2 implies $\prod_i W(\chi_i)^{n_i} = 1$.

Proof of claim I. Because the abelian root numbers are insensitive to the G-action according to lemma 1.2.10, we can select an element from each G-conjugacy class $(H_i, \chi_i) - (H_i, 1)$ so that lemma 1.2.5 can be applied to $\sum_i n_i \left[Ind_{H_i}^G(\chi_i) - Ind_{H_i}^G(1)\right] = 0$. In other words, we must assure

$$\chi_i|_C \neq \chi_j|_C \quad \text{if and only if} \quad \chi_i|_C \neq (\chi_j^g)|_C \quad \text{for all } g \in G .$$

Fix a complete set T of representatives of the G-orbits that contains $\chi_i|_C$ for all i . Given a fixed non-trivial $\mu \in T$,

$$\sum_{\chi_i|_C = \mu} n_i \, (H_i, \chi_i)$$

belongs to $ker(b_{G_\mu})$ according to lemma 1.2.5. Similarly, we can conclude that

$$\sum_{\chi_i|_C = 1} n_i \left[(H_i, \chi_i) - (H_i, 1)\right] - \sum_{\chi_i|_C \neq 1} n_i \, (H_i, 1)$$

is a relation in $ker(b_G)$. Indexed as above,

$$\sum_{\chi_i|_C = \mu} n_i \, Ind_{H_i}^{G_\mu}(1)$$

and

$$\sum_{\chi_i|_C \neq 1} n_i \, Ind_{H_i}^{G}(1) \ .$$

are virtual representations of dimension zero. By lemma 1.2.11, they are inflations of similar virtual representations of G_μ/C and G/C respectively. So, the Brauer's theorem in chapter 2 produces subgroups $V_{s_\mu} \supseteq C$ and characters λ_{s_μ} annihilating C such that

$$\sum_{s_\mu} d_{s_\mu} \, Ind_{V_{s_\mu}}^{G_\mu}(\lambda_{s_\mu} - 1) \quad = \quad \begin{cases} \sum_{\chi_i|_C = \mu} n_i Ind_{H_i}^{G_\mu}(1) & \mu \neq 1 \\ -\sum_{\chi_i|_C \neq 1} n_i Ind_{H_i}^{G}(1) & \mu = 1 \end{cases}$$

As a result, for all $\mu \in T$

$$\sum_{\chi_i|_C = \mu} n_i \left[(H_i, \chi_i) - (H_i, 1)\right] + \underbrace{\sum_{s_\mu} d_{s_\mu} \left[(V_{s_\mu}, \lambda_{s_\mu}) - (V_{s_\mu}, 1)\right]}_{J_\mu} \quad \in \; ker(b_{G_\mu}) \tag{3.2j}$$

If we let

$$J_\mu \;=\; \sum_{s_\mu} d_{s_\mu} \left[(V_{s_\mu}, \lambda_{s_\mu}) - (V_{s_\mu}, 1)\right]$$

then $\sum_{\mu \in T} J_\mu \in ker(b_G)$. In fact, $\sum_{\mu \in T} J_\mu$ as an element of $R_+(G)$ turns out to be zero. It follows that

$$\prod_{\mu \in T} \prod_{s_\mu} W(\lambda_{s_\mu})^{d_{s_\mu}} \;=\; 1 \tag{3.2k}$$

Now we return to the key relation $(3.2j)$. Because the kernel $ker(\mu)$ of μ is normal in G_μ, lemma 1.2.9 says that $(3.2j)$ comes from a similar relation in $ker(b_{G_\mu/ker(\mu)})$ via $infl$. We will show that the induction hypothesis applies to such a relation in $ker(b_{G_\mu/ker(\mu)})$ (a preimage of $(3.2j)$ under $infl$).

Given $g \in G_\mu$, the diagram below is commutative.

$$\begin{array}{ccc} C/ker(\mu) & \overset{\mu}{\rightarrow} & S^1 \\ gxg^{-1} \downarrow & & \nearrow \mu \\ & C/ker(\mu) & \end{array}$$

Here S^1 stands for the unit circle in the complex plane. Therefore, $C/ker(\mu)$ stays inside the center of $G_\mu/ker(\mu)$, which will be denoted by $Z(G_\mu/ker(\mu))$. In particular,

$$|\,(G_\mu/ker(\mu))\;/\;(C/ker(\mu))\,| \;\geq\; |\,(G_\mu/ker(\mu))\;/\;Z(G_\mu/ker(\mu))\,| \;.$$

On the other hand

$$|\,G/Z\,| \;\geq\; |\,G_\mu/Z\,| \;>\; |\,G_\mu/C\,| \;=\; |\,(G_\mu/ker(\mu))\;/\;(C/ker(\mu))\,|$$

So the induction hypothesis applies to relations in $ker(b_{G_\mu/ker(\mu)})$, and yields

$$\prod_{\chi_i|_C=\mu} W(\chi_i)^{n_i} \prod_{s_\mu} W(\lambda_{s_\mu})^{d_{s_\mu}} = 1$$

Hence,

$$\prod_{\mu \in T} \left\{ \prod_{\chi_i|_C=\mu} W(\chi_i)^{n_i} \prod_{s_\mu} W(\lambda_{s_\mu})^{d_{s_\mu}} \right\} = 1$$

or equivalently,

$$\left\{ \prod_{i} W(\chi_i)^{n_i} \right\} \left\{ \prod_{\mu \in T} \prod_{s_\mu} W(\lambda_{s_\mu})^{d_{s_\mu}} \right\} = 1 .$$

Dividing this by $(3.2k)$, we obtain the claim. ||

Claim II. Assume $H_i \not\supseteq C$. *Then the sum* Q *consists of* l *terms and we have* $H_iC = (H_iC)_{\mu'}$, *while the sum* P *either contains* l *terms or just contain one term, according to whether* $[H_iC : (H_iC)_\mu]$ *equals one or* l .

Proof of claim II. Because, $[C : Z] = l$ and H_i contains Z , the characters in C^* that annihilate $H_i \cap C = Z$ form a cyclic group of prime order l . Let σ be a generator of this cyclic subgroup of C^* . Then $\langle \sigma \rangle$ is closed under the conjugation by $G = H_iC$. In other words,

$$(\sigma^k)^g \,|_{H_i \cap C} = 1 \qquad \text{for all } g \in G .$$

Under this G-action, $\langle \sigma \rangle$ is divided into equivalence classes, each of which has $[G : G_{\sigma^k}]$ number of elements. However $\sigma^g = \sigma$ means $(\sigma^k)^g = \sigma^k$ for all k. In addition, any $\sigma^k \neq 1$ is a generator of $\langle \sigma \rangle$. It follows $G_\sigma = G_{\sigma^k}$ as long as $0 < k < l$, and we only need to examine one stabilizer G_σ. Since C is abelian, it is sufficient to consider the same action by H_i. Recall that C is central modulo Z. So, given $h \in H_i$ and $x \in C$, we have

$$\sigma(hxh^{-1}) = \sigma(xhzh^{-1})$$

where $h^{-1}x^{-1}hx = z \in Z$. Hence

$$\sigma(hxh^{-1}) = \sigma(xhz\,h^{-1}) = \sigma(xhh^{-1}z) = \sigma(xz) = \sigma(x)$$

and this implies $G = G_\sigma$. Now it is immediate that the sum Q consists of l terms because we have $H_iC = (H_iC)_{\mu'}$.

As for the sum P, let us fix one such μ. Then the others are of the form $\mu\,\sigma^k$. As we have seen already, $G = G_{\sigma^k}$. Thus, $G_\mu = G_{(\mu\,\sigma^k)}$ for all k, which means $[G : G_\mu]$ divides the prime l. Consequently, $[G : G_\mu]$ either equals 1 or l, and P either contains l terms or just contain one term. $\|$

Claim III. The stabilizer $(H_iC)_\mu$ *is normal in* H_iC *. Moreover, we obtain the decomposition*

$$Ind_{(H_iC)_\mu}^{H_iC}(1) = \sum_{\substack{\tau \in (H_iC)^* \\ \tau|_{(H_iC)_\mu} = 1}} \tau$$

where $(H_iC)^*$ *stands for the character group of* H_iC *.*

Proof of claim III. The statement is trivial if $[H_iC : (H_iC)_\mu] = 1$. Hence we can assume $H_i \not\supseteq C$. According to claim II, it remains to prove claim III for $[H_iC : (H_iC)_\mu] = l$. Because $C \subsetneq (H_iC)_\mu$, let us consider $h(H_iC)_\mu h^{-1}$ with $h \in H_i$. In fact,

$$h(H_iC)_\mu h^{-1} = (H_iC)_{(\mu^{h^{-1}})} .$$

Notice that $\mu^{h^{-1}}|_Z = \mu|_Z$. So $\mu^{h^{-1}} = \sigma\mu$ for some $\sigma \in C^*$ such that $\sigma|_Z = 1$. Just as the argument in the proof of claim II, we have $H_iC = (H_iC)_\sigma$, which implies $(H_iC)_\mu = (H_iC)_{(\sigma\mu)}$. Therefore

$$(H_iC)_\mu = (H_iC)_{(\mu^{h^{-1}})} = h(H_iC)_\mu h^{-1}$$

and $(H_iC)_\mu \triangleleft H_iC$. It follows that $(H_iC)/(H_iC)_\mu$ is cyclic of prime order l . By lemma 1.2.4,

$$Ind_{(H_iC)_\mu/(H_iC)_\mu}^{(H_iC)/(H_iC)_\mu}(1) = \sum_{\tau \in ((H_iC)/(H_iC)_\mu)^*} \tau .$$

If τ is interpreted as a character of $(H_iC)^*$ via the canonical projection $proj : H_iC \to (H_iC)/(H_iC)_\mu$, then lemma 1.2.11 asserts that

$$Ind_{(H_iC)_\mu}^{H_iC}(1) = \sum_{\substack{\tau \in (H_iC)^* \\ \tau|_{(H_iC)_\mu} = 1}} \tau .$$

Claim III is now established. ||

Claim IV. The fact that C *is central modulo* Z *implies* $H_i \lhd G = H_iC$ *. In addition,* $A = \bigcap_{g \in G} g\, ker(\chi_i)\, g^{-1}$ *is not only a normal subgroup of* $G = H_iC$ *but also a normal subgroup of* $(H_iC)_\mu$ *.*

Proof of claim IV. It is enough to show $c(H_i)c^{-1} \subseteq H_i$ for all $c \in C$. Given $h \in H_i$ and $c \in C$, there exists $z \in Z$ such that

$$c\,h = h\,c\,z$$

because C is central modulo Z. So

$$c\,h\,c^{-1} = h\;c\,z\,c^{-1} = h\,z\,c\,c^{-1} = h\,z$$

which belongs to H_i as we assume $Z \subseteq H_i$.

To prove the second statement, we will show $\mu(xyx^{-1}y^{-1}) = 1$ for $x \in A$ and $y \in C$. Notice from the definition of A that $A \subseteq H_i$ and that there exists $x' \in ker(\chi_i)$ such that $y^{-1}x'y = x^{-1}$. Meanwhile, because $H_i \lhd H_iC$, we have $xyx^{-1}y^{-1} \in Z$. So

$$\mu(xyx^{-1}y^{-1}) = \chi_i(xyx^{-1}y^{-1}) = \chi_i(xyy^{-1}x'yy^{-1}) = \chi_i(xx') = 1 .$$

In other words,

$$\mu(xyx^{-1}) = \mu(y)$$

and A is a subgroup of $(H_iC)_\mu$. By its definition, A must be normal in $(H_iC)_\mu$ as well. ||

Claim V. Suppose $G = H_iC$ *and* $C \not\subseteq H_i$. *If* $A = \bigcap_{g \in G} g\,ker(\chi_i)\,g^{-1}$ *is a subgroup of* Z *such that* Z/A *coincides with the center of* G/A, *then* $(3.2f)$ *is the same as the 2nd identity.*

Proof of claim V. With the four premises, we have already seen that

(a) G/A is the semi-direct product of (H_i/A) and (C/A) .

(b) $H_i/A \cap C/A = Z/A$, the center of G/A.

(c) H_i/A is an abelian normal subgroup of G/A

(d) $ker(\chi_i|_Z)$, the kernel of the restricted character $\chi_i|_Z$, is A .

(e) $(H_iC)_\mu$ is a normal subgroup of index l in H_iC .

Let us first show that $[H_i : Z] = l$.

Consider a bilinear map $u : H_i \times C \longrightarrow Z$ defined by $u(h, c) = hch^{-1}c^{-1}$. Since either $h \in Z$ or $c \in Z$ means $u(h,c) = 1$, we may define $\overline{u} : H_i/Z \times C/Z \longrightarrow Z$ with the same formula $\overline{u}(hZ, cZ) = hch^{-1}c^{-1}$. Suppose c_oZ is a generator of the cyclic group C/Z . Then, due to fact (b) and (c) above, we conclude that $u(h, c_o) \in A$ if and only if $h \in Z$. In other words, $\overline{u}(hZ, c_oZ)$ is an injective homomorphism from H_i/Z to Z/A. Recall $ker(\chi_i|_Z) = A$. This means Z/A is cyclic, and therefore H_i/Z is also cyclic. Notice that $\overline{u}(hZ, c_oZ)^l = 1$ as C/Z has order l. Consequently, H_i/Z is cyclic of prime order l.

With $[H_i : Z] = l$, we note that the subgroup H_i is abelian. Moreover,

$$[H_iC : C] = [H_i : Z] = l \ .$$

Because $(H_iC)_\mu \supseteq C$ and $[H_iC : (H_iC)_\mu] = l$, it follows from

$$l = [H_iC : C] = [H_iC : (H_iC)_\mu]\,[(H_iC)_\mu : C]$$

that $(H_iC)_\mu = C$. As a result, relation (3.2d) becomes

$$(H_i, \chi_i) - (H_i, 1) - \Bigg\{ \underbrace{\big[(C, \mu) - (C, 1)\big]}_{M_i}$$

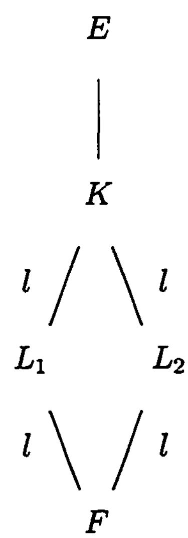
$$- \underbrace{\sum_{\substack{\mu' \in C^* \\ \mu'|_Z = 1}} \Big[(H_iC, \{1, \mu'\}) - (H_iC, 1)\Big]}_{N_i} \Bigg\} - \sum_{\substack{\tau \in (H_iC)^* \\ \tau|_C = 1}} \Big[(H_iC, \tau) - (H_iC, 1)\Big] \tag{3.2l}$$

(cf. case 3), and the identity $(3.2f)$ is reduced to

$$\frac{W(\chi_i) \prod_{\substack{\mu' \in C^* \\ \mu'|_Z = 1}} W(\{1, \mu'\})}{W(\mu) \prod_{\substack{\tau \in (H_iC)^* \\ \tau|_C = 1}} W(\tau)} = 1 .$$

Now, we must show that this is precisely the 2nd identity in 3.1.

Let $H_iC = Gal(E/F)$, $Z = Gal(E/K)$, $H_i = Gal(E/L_1)$ and $C = Gal(E/L_2)$.



(3.2m).

Because $C \not\subseteq H_i$, the fixed fields L_1 and L_2 are distinct. Moreover, $H_i \triangleleft H_iC$ implies $[H_iC : H_i] = [C : Z] = l$.

Since $\tau \in (H_iC)^*$ satisfying $\tau|_C = 1$, it can be seen as a character of the Galois group $Gal(L_2/F)$. Via the reciprocity map, we conclude that $\tau \in S(L_2/F)$. Similarly, $\{1, \mu'\} \in (H_iC)^*$ is trivial on H_i by definition. So $\{1, \mu'\}$ can be seen as a character of the Galois group $Gal(L_1/F)$. Via the reciprocity map, we have $\{1, \mu'\} \in S(L_1/F)$. It remains to check the other premises leading to the 2nd identity.

Remember μ has been chosen such that

$$\chi_i|_Z = \mu|_Z \qquad (3.2n).$$

If χ_i and μ are interpreted as characters of $L_1^\times$ and $L_2^\times$ respectively by means of the reciprocity map, then $(3.2n)$ is translated into $\chi_i \circ N_{K/L_1} = \mu \circ N_{K/L_2}$. Let us identify χ_{L_1} with χ_i and identify χ_{L_2} with μ. We will also denote the character $\chi_i \circ N_{K/L_1}$ of $K^\times$ by χ_K.

In view of diagram $(3.2m)$, the Galois group $Gal(K/F)$ is a direct product of $Gal(K/L_1)$ and $Gal(K/L_2)$. Suppose $\sigma_j \in Gal(K/L_j)$ for $j = 1$ or 2. Then

$$\chi_K \circ \sigma_j = (\chi_{L_j} \circ N_{K/L_j}) \circ \sigma_j = \chi_{L_j} \circ (N_{K/L_j} \circ \sigma_j) = \chi_{L_j} \circ N_{K/L_j} = \chi_K$$

from which we obtain $\chi_K \circ \sigma = \chi_K$ for all $\sigma \in Gal(K/F)$.

Finally, $\chi_K \neq \chi_F \circ N_{K/F}$ for all quasi-characters χ_F on $F^\times$. If on contrary such χ_F exists, then it must annihilate the norm group $N_{E/F}(E^\times)$ because $\chi_K = \chi_i \circ N_{K/L_1}$ annihilates $N_{E/K}(E^\times)$. In other words, χ_F can be regarded as a character of the Galois group $Gal(E/F)$ such that

$$\chi_F\,|_Z = \chi_i\,|_Z = \mu\,|_Z$$

Consequently, the restriction $\chi_F\,|_C$ must be equivalent to μ under the (H_iC)-action on C^* as (3.2l) indicates the sum M_i collapses to $\left[(C,\mu) - (C,1)\right]$. In particular, the stabilizer of $\chi_F\,|_C$ is a conjugate of the stabilizer of μ. However, the stabilizer of $\chi_F\,|_C$ equals H_iC. This contradicts the fact that $[H_iC : (H_iC)_\mu] = l$.

We have successfully verified all the premises for the 2nd identity, and claim V is now proved. ||

3.3 Representations of the Weil group

Having proved theorem 3.2.0 and theorem 3.2.1, we are in a position to tackle the general case. The next theorem completes the proof of our main theorem in 3.2 and extends the theory to the context of Weil group.

Let $G = Gal(K/F)$ be a local Galois group. Recall the relative Weil group for K/F is an extension of G by the multiplicative group of K i.e.

$$1 \longrightarrow K^\times \longrightarrow W_{K/F} \longrightarrow G \longrightarrow 1$$

is exact. Analoguous to $R(G)$, the group $R(W_{K/F})$ is free abelian generated by isomorphism classes of irreducible representations of $W_{K/F}$.

Theorem 3.3.1. *With the above notations,*

(i) G is solvable, and the main theorem in section 3.2 holds.

(ii) if $\sum_j m_j Ind_{W_{K/E_j}}^{W_{K/F}}(\chi_{E_j} - 1) \in R(W_{K/F})$ is equal to zero, then

$$\prod_j W(\chi_{E_j})^{m_j} = 1$$

where E_j is a subfield of K/F and χ_{E_j} is a quasi-character on $E_j^\times$ of finite order for each j.

(iii) given any abelian normal subgroup $C = Gal(K/L)$ of G and any finite order quasi-character χ_E on the multiplicative group of a subfield E of K/F satisfying $\chi_E \circ N_{K/E} = \chi_F \circ N_{K/F}$ for some

quasi-character χ_F *on* $F^\times$ *, there are subfields* F_s *of* L/F *and quasi-characters* χ_{F_s} *on* $F_s^\times$ *of finite order such that*

1) $\chi_{F_s} \circ N_{K/F_s}$ *is either* $\chi_E \circ N_{K/E}$ *or* 1 *.*

2) for some integers a_s *, we have*

$$Ind_{W_{K/E}}^{W_{K/F}}(\chi_E - 1) \;=\; \sum_s a_s Ind_{W_{K/F_s}}^{W_{K/F}}(\chi_{F_s} - 1) \;.$$

3) with a_s *as above*

$$W(\chi_E) \;=\; \prod_s W(\chi_{F_s})^{a_s} \,.$$

For notational simplicity, we will abbreviate the composition $\chi_E \circ N_{K/E}$ to $\chi_{K/E}$, the composition $\chi_F \circ N_{K/F}$ to $\chi_{K/F}$, and $\chi_{F_s} \circ N_{K/F_s}$ to χ_{K/F_s} .

Proof. We prove theorem 3.3.1 by induction on $|G| = [K:F]$. Suppose the order of G is 1. The assertion $\prod_i W(\chi_i)^{n_i} = 1$ in the main theorem becomes a triviality since $\chi_i = 1$ for all i . As for statement (ii) , we may assume each χ_{E_j} is non-trivial since $W(1) = 1$. Compare the conductors of χ_{E_j} . Suppose m is the largest among these conductors. Then the restriction of χ_{E_j} to the unit group U_F of the ring of integers of F can be viewed as irreducible characters of the finite quotient U_F/U_F^m . Therefore, $\sum_j m_j(\chi_{E_j} - 1) = 0$ implies $m_j = 0$ for such j whose χ_{E_j} is not unramified. So it remains to prove the finite product $\prod_j W(\chi_{E_j})^{m_j} = 1$ in the case every χ_{E_j} is unramified. Let ℓ be the least common multiple of the orders of χ_{E_j}. Then each χ_{E_j} can be regarded as a non-trivial irreducible character of the finite cyclic group of order ℓ. Consequently, $\sum_j m_j(\chi_{E_j} - 1) = 0$ implies $m_j = 0$ for all j. Regarding statement (iii), we simply take $F_s = E = F$ and $\chi_{F_s} = \chi_E$.

Now suppose statement (i), (ii) and (iii) hold for all local Galois groups with order less than or equal to I. This is the **induction hypothesis of theorem 3.3.1**. Let $|Gal(K/F)| = I + 1$.

To prove statement (i), we consider the following two possibilities separately.

Case 1: $H_i \neq G$ *for all* i.

Case 2: $H_i = G$ *for some* i.

Let us handle case 1 first. Since theorem 3.2.1 together with theorem 3.2.2

yield (i) when G is nilpotent, we can assume that G is not nilpotent. According to Brauer's induction theorem, the trivial character of $G = Gal(K/F)$ can be expresssed

$$1 = \sum_{k=1}^{N} e_k \, Ind_{Gal(K/F_k)}^{Gal(K/F)} \, (\chi_{F_k}) \ .$$

Notice that G is not nilpotent implies $F_k \neq F$ for all k. Let $V_k = Gal(K/F_k)$ and

$$S = (G, 1) - \sum_{k=1}^{N} e_k \, (V_k, \chi_{F_k}) \ .$$

Then $S \in R_+(G)$. Lemma 1.2.1 shows that $res(S) \in R_+(H_i)$ is a relation in the kernel $ker(b_{H_i})$ of b_{H_i} for all i, and therefore so is the product $res(S) \cdot \big[(H_i, \chi_i) - (H_i, 1)\big]$. When multiplied out, this product can be written as a sum in the form of

$$\sum_n a_{i,n} \big[(A_{i,n}, \alpha_{i,n}) - (A_{i,n}, 1)\big] \ .$$

Consequently,

$$0 = b_{H_i}\Big(res(S) \cdot \big[(H_i, \chi_i) - (H_i, 1)\big]\Big) = \sum_n a_{i,n} \, Ind_{A_{i,n}}^{H_i} \, (\alpha_{i,n} - 1)$$

to which the induction hypothesis of theorem 3.3.1 applies as $H_i \neq G$ for all i. Hence,

$$\prod_n W(\alpha_{i,n})^{a_{i,n}} = 1 \tag{3.3a}$$

for all i.

In fact, if we write $(H_i, \chi_i) - (H_i, 1)$ as

$$S \cdot \Big[(H_i, \chi_i) - (H_i, 1)\Big] + \sum_{k=1}^{N} e_k (V_k, \chi_{F_k}) \cdot \Big[(H_i, \chi_i) - (H_i, 1)\Big]$$

it follows from lemma 1.2.2 that

$$(H_i, \chi_i) - (H_i, 1) = \sum_n a_{i,n} \Big[(A_{i,n}, \alpha_{i,n}) - (A_{i,n}, 1)\Big] + \sum_{k=1}^{N} e_k R_{i,k} \tag{3.3b}$$

where $R_{i,k}$ stands for the product $(V_k, \chi_{F_k}) \cdot \Big[(H_i, \chi_i) - (H_i, 1)\Big]$.

We can argue just as above for $R_{i,k}$. Particularly, let us multiply out $(V_k, \chi_{F_k}) \cdot res\Big(\Big[(H_i, \chi_i) - (H_i, 1)\Big]\Big) \in R_+(V_k)$, and suppose

$$(V_k, \chi_{F_k}) \cdot res\Big(\Big[(H_i, \chi_i) - (H_i, 1)\Big]\Big) = \sum_y d_{i,k,y} \Big[(B_{i,k,y}, \beta_{i,k,y}) - (B_{i,k,y}, 1)\Big]$$

Summing such equalities over i, we have

$$(V_k, \chi_{F_k}) \cdot res\Big(\sum_i n_i \Big[(H_i, \chi_i) - (H_i, 1)\Big]\Big)$$

$$= \sum_i \sum_y n_i \, d_{i,k,y} \left[(B_{i,k,y}, \beta_{i,k,y}) - (B_{i,k,y}, 1) \right] .$$

Because $res\Big(\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1) \right] \Big) \in ker(b_{V_k})$, so is

$$\sum_i \sum_y n_i \, d_{i,k,y} \left[(B_{i,k,y}, \beta_{i,k,y}) - (B_{i,k,y}, 1) \right] .$$

In other words,

$$\sum_i \sum_y n_i \, d_{i,k,y} \, Ind_{B_{i,k,y}}^{V_k} (\beta_{i,k,y} - 1) = 0 .$$

Since $F_k \neq F$ implies $V_k \neq G$, the induction hypothesis yields

$$\prod_i \prod_y W(\beta_{i,k,y})^{n_i \, d_{i,k,y}} = 1 \qquad (3.3c).$$

Meanwhile, summing $(3.3b)$ over i produces

$$\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1) \right] = \sum_i \sum_n n_i \, a_{i,n} \left[(A_{i,n}, \alpha_{i,n}) - (A_{i,n}, 1) \right] + \sum_{k=1}^{N} e_k \left\{ \sum_i n_i \, R_{i,k} \right\} .$$

By lemma 1.2.2, we see that

$$\sum_i n_i \, R_{i,k} = \sum_i \sum_y n_i \, d_{i,k,y} \left[(B_{i,k,y}, \beta_{i,k,y}) - (B_{i,k,y}, 1) \right] .$$

As a result, $\sum_i n_i \left[(H_i, \chi_i) - (H_i, 1)\right]$ is equal to

$$\sum_i \sum_n n_i \, a_{i,n} \left[(A_{i,n}, \alpha_{i,n}) - (A_{i,n}, 1)\right]$$

$$+ \sum_{k=1}^{N} e_k \left\{ \sum_i \sum_y n_i \, d_{i,k,y} \left[(B_{i,k,y}, \beta_{i,k,y}) - (B_{i,k,y}, 1)\right] \right\} .$$

Observe that each term in the above sums is a basis element of $R_+(G)$. Therefore,

$$\prod_i W(\chi_i)^{n_i} = \left\{ \prod_i \left[\prod_n W(\alpha_{i,n})^{a_{i,n}} \right]^{n_i} \right\} \left\{ \prod_{k=1}^{N} \left[\prod_i \prod_y W(\beta_{i,k,y})^{n_i \, d_{i,k,y}} \right]^{e_k} \right\} .$$

Now, it follows from (3.3a) and (3.3c) that the products within square brackets on the right hand side are trivial. So $\prod_i W(\chi_i)^{n_i} = 1$, and case 1 is completed.

Let us proceed to case 2. Just as in the previous case, we will assume G is not nilpotent. Suppose $H_i = G$ for some i. By a variation of Brauer's theorem (see chapter 2),

$$Ind_{H_i}^{G} (\chi_i - 1) = \chi_i - 1 = \sum_j m_j \, Ind_{D_j}^{G} (\zeta_j - 1)$$

such that m_j is an integer and ζ_j is a character of $D_j \neq G$ for each j.

Once it is shown

$$W(\chi_i) \;=\; \prod_j W(\zeta_j)^{m_j}$$

we can replace those terms in the original sum $\sum_i \; n_i\, Ind_{H_i}^G(\chi_i - 1)$ of the form $\chi_i - 1$ by the corresponding $\sum_j \; m_j\, Ind_{D_j}^G(\zeta_j - 1)$ in order to turn case 2 into case 1 which we proved earlier. Particularly,

$$\sum_i n_i\, Ind_{H_i}^G\,(\chi_i - 1) \;=\; \sum_{H_i \neq G} n_i\, Ind_{H_i}^G\,(\chi_i - 1) \;+\; \sum_{H_i = G} n_i\,(\chi_i - 1)\;.$$

which can be written

$$\sum_{H_i \neq G} n_i\, Ind_{H_i}^G\,(\chi_i - 1) \;+\; \sum_{H_i = G} n_i \left\{ \sum_j m_j\, Ind_{D_j}^G\,(\zeta_j - 1) \right\}$$

where the index j may depend on i. If $\sum_i \; n_i\, Ind_{H_i}^G(\chi_i - 1) \;=\; 0$, then

$$1 \;=\; \prod_{H_i \neq G} W(\chi_i)^{n_i} \prod_{H_i = G} \left\{ \prod_j W(\zeta_j)^{m_j} \right\}^{n_i}$$

by case 1. Hence the following lemma will complete case 2.

Lemma. *Suppose* $G \;=\; Gal(K/F)$ *of order* $I + 1$ *is not nilpotent and* χ_i *is a character of* $H_i \;=\; G$ *. If*

$$\chi_i - 1 \;=\; \sum_j m_j\, Ind_{D_j}^G\,(\zeta_j - 1)$$

for some integers m_j *and characters* ζ_j *of* $D_j \neq G$ *, then the induction hypothesis of theorem 3.3.1 together with the 3rd identity imply*

$$W(\chi_i) = \prod_j W(\zeta_j)^{m_j} .$$

Proof. Let C be an abelian normal subgroup which is non-trivial and minimal in the sense that C has no non-trivial subgroup that is normal in G, other than C itself. Because G is solvable, such C must exist. Specifically the sequence

$$G \supset [G,G] \supset \big[[G,G] , [G,G] \big] \supset \cdots$$

terminates. So the last non-trivial group in the sequence will be an abelian normal subgroup of G. It is possible to choose a minimal subgroup C within this last non-trivial group in the sequence.

Let $D_j = Gal(K/E_j)$ and $C = Gal(K/L)$. If $\chi_i - 1$ is regarded as an element of $R(W_{K/F})$ via the surjective homomorphism $W_{K/F} \to Gal(K/F)$, then by lemma 1.2.12

$$\chi_i - 1 = \sum_j m_j \, Ind_{W_{K/E_j}}^{W_{K/F}} (\zeta_j - 1) .$$

In the case $D_j \supseteq C$ for all j, we have $L \supseteq E_j \supseteq F$, and the above equality implies that as an element of $R(W_{L/F})$

$$\chi_i - 1 = \sum_j m_j \, Ind_{W_{L/E_j}}^{W_{L/F}} (\zeta_j - 1)$$

in view of lemma 1.2.11 and the surjection $W_{K/F} \to W_{L/F}$.

Because L/F is a Galois extension and $I \geq |Gal(L/F)|$, the induction hypothesis of theorem 3.3.1 yields $W(\chi_i) = \prod_j W(\zeta_j)^{m_j}$. This proves the claim below.

Claim I. *With the notations in the lemma, suppose we have* $\chi_i - 1 = \sum_j m_j Ind_{D_j}^{G} (\zeta_j - 1)$ *such that* $D_j \supseteq C$ *for all* j *. Then it follows from the induction hypothesis of theorem 3.3.1 that* $W(\chi_i) = \prod_j W(\zeta_j)^{m_j}$.

Now we assume $D_j \not\supseteq C$ for some j . By lemma 1.2.3,

$$(D_j, \zeta_j) - (D_j, 1) - \left\{ \sum_{\substack{\mu \in C^*/(D_jC) \\ \zeta_j|_{D_j \cap C} = \mu|_{D_j \cap C}}} ((D_jC)_\mu, \{\zeta_j, \mu\}) - \sum_{\substack{\mu' \in C^*/(D_jC) \\ \mu'|_{D_j \cap C} = 1}} ((D_jC)_{\mu'}, \{1, \mu'\}) \right\}$$

is a relation in $ker(b_{D_jC})$. Consequently, the virtual representation

$$\sigma = \sum_{\substack{\mu \in C^*/(D_jC) \\ \zeta_j|_{D_j\cap C} = \mu|_{D_j\cap C}}} Ind_{(D_jC)_\mu}^{D_jC}(1) - \sum_{\substack{\mu' \in C^*/(D_jC) \\ \mu'|_{D_j\cap C} = 1}} Ind_{(D_jC)_{\mu'}}^{D_jC}(1)$$

has dimension zero. Since both $(D_jC)_\mu$ and $(D_jC)_{\mu'}$ contain C, the above σ is an inflation of a similar virtual representation of the quotient D_jC/C, and the theorem of Brauer in chapter 2 together with lemma 1.2.11 assert that

$$\sigma = \sum_s q_{j,s}\, Ind_{T_{j,s}}^{D_jC}\,(\nu_{j,s} - 1)$$

for some $T_{j,s} \supseteq C$ and characters $\nu_{j,s}$ trivial on C. As a result, if we set

$$M_j = \sum_{\substack{\mu \in C^*/(D_jC) \\ \zeta_j|_{D_j\cap C} = \mu|_{D_j\cap C}}} \Big[\,((D_jC)_\mu, \{\zeta_j, \mu\}) - ((D_jC)_\mu, 1)\,\Big]$$

and

$$N_j = \sum_{\substack{\mu' \in C^*/(D_jC) \\ \mu'|_{D_j\cap C} = 1}} \Big[\,((D_jC)_{\mu'}, \{1, \mu'\}) - ((D_jC)_{\mu'}, 1)\,\Big]$$

then

$$(D_j, \zeta_j) - (D_j, 1) - \Big\{M_j - N_j\Big\} - \sum_s q_{j,s}\Big[\,(T_{j,s}, \nu_{j,s}) - (T_{j,s}, 1)\,\Big] \tag{3.3d}$$

is a relation in $ker(b_{D_jC})$.

Let us rewrite $\chi_i - 1 = \sum_j m_j Ind^G_{D_j}(\zeta_j - 1)$ in our lemma using the above relation (3.3*d*). Whenever $D_j \not\supseteq C$, we replace the corresponding term $Ind^G_{D_j}(\zeta_j - 1)$ by

$$\sum_{\substack{\mu \in C^*/(D_jC) \\ \zeta_j|_{D_j\cap C} = \mu|_{D_j\cap C}}} Ind^G_{(D_jC)_\mu}(\{\zeta_j,\mu\} - 1) - \sum_{\substack{\mu' \in C^*/(D_jC) \\ \mu'|_{D_j\cap C} = 1}} Ind^G_{(D_jC)_{\mu'}}(\{1,\mu'\} - 1) + \sum_s q_{j,s}\, Ind^G_{T_{j,s}}(\nu_{j,s} - 1) \ .$$

Notice that $(D_jC)_\mu$, $(D_jC)_{\mu'}$ and $T_{j,s}$ all contain C. Therefore claim I applies, and

$$W(\chi_i) = \prod_{D_j\supseteq C} W(\zeta_j)^{m_j} \prod_{D_j\not\supseteq C} \left\{ \frac{\prod_{\substack{\mu \in C^*/(D_jC) \\ \zeta_j|_{D_j\cap C} = \mu|_{D_j\cap C}}} W(\{\zeta_j,\mu\})}{\prod_{\substack{\mu' \in C^*/(D_jC) \\ \mu'|_{D_j\cap C} = 1}} W(\{1,\mu'\})} \prod_s W(\nu_{j,s})^{q_{j,s}} \right\}^{m_j} .$$

To complete the proof of our lemma, it remains to show that for $D_j \not\supseteq C$,

$$W(\zeta_j) = \frac{\prod_{\substack{\mu \in C^*/(D_jC) \\ \zeta_j|_{D_j\cap C} = \mu|_{D_j\cap C}}} W(\{\zeta_j,\mu\})}{\prod_{\substack{\mu' \in C^*/(D_jC) \\ \mu'|_{D_j\cap C} = 1}} W(\{1,\mu'\})} \prod_s W(\nu_{j,s})^{q_{j,s}} \qquad (3.3e).$$

In case $D_jC \neq G$, the induction hypothesis of 3.3.1 applies to the relation (3.3*d*) and yields identity (3.3*e*). Henceforth we can assume $D_jC = G$.

Observe that $D_j \cap C \lhd D_jC$. Since C is minimal by construction, $D_j \not\supseteq C$ then implies $D_j \cap C = \{1\}$. Consequently the relation (3.3d) becomes

$$(D_j, \zeta_j) - (D_j, 1) - \underbrace{\sum_{\mu \in C^*/G} \Big[((D_jC)_\mu, \{\zeta_j, \mu\}) - ((D_jC)_\mu, 1) \Big]}_{M_j}$$

$$+ \underbrace{\sum_{\mu \in C^*/G} \Big[((D_jC)_\mu, \{1, \mu\}) - ((D_jC)_\mu, 1) \Big]}_{N_j} .$$

Notice $T_{j,s}$ and $\nu_{j,s}$ are redundant. In fact, the representation σ , from which $T_{j,s}$ and $\nu_{j,s}$ are defined via Brauer's theorem, is equal to zero when $D_j \cap C = \{1\}$.

As a result, we have

$$Ind_{D_j}^{G}(\zeta_j - 1) - \sum_{\mu \in C^*/G} \Big\{ Ind_{(D_jC)_\mu}^{G}(\{\zeta_j, \mu\} - 1) - Ind_{(D_jC)_\mu}^{G}(\{1, \mu\} - 1) \Big\} = 0$$

which can be inflated to

$$Ind_{W_{K/E_j}}^{W_{K/F}}(\zeta_j - 1) - \sum_{\mu \in C^*/G} \Big\{ Ind_{W_{K/F_{j,\mu}}}^{W_{K/F}}(\{\zeta_j, \mu\} - 1) - Ind_{W_{K/F_{j,\mu}}}^{W_{K/F}}(\{1, \mu\} - 1) \Big\} = 0 \qquad (3.3f)$$

according to lemma 1.2.12, if $(D_jC)_\mu = Gal(K/F_{j,\mu})$.

Recall that the centralizer of a subgroup consists of element(s) in G that commutes with everything within that subgroup. If there exists a non-trivial normal subgroup of D_j lying inside the centralizer of C, then this non-trivial normal subgroup, denoted by $Gal(K/U)$, is also normal in D_jC. Meanwhile, $(D_jC)_\mu$ contains the centralizer of C. Therefore E_j and $F_{j,\mu}$ are subfields of the Galois extension U/F. By lemma 1.2.11, $(3.3f)$ is an inflation of

$$Ind_{W_{U/E_j}}^{W_{U/F}}(\zeta_j - 1) - \sum_{\mu \in C^*/G} \left\{ Ind_{W_{U/F_{j,\mu}}}^{W_{U/F}}(\{\zeta_j, \mu\} - 1) - Ind_{W_{U/F_{j,\mu}}}^{W_{U/F}}(\{1, \mu\} - 1) \right\} = 0$$

to which the induction hypothesis of theorem 3.3.1 can be applied because $I \geq |Gal(U/F)|$.

Hence,

$$W(\zeta_j) \prod_{\mu \in C^*/G} \left\{ \frac{W(\{1,\mu\})}{W(\{\zeta_j,\mu\})} \right\} = 1$$

or equivalently

$$W(\zeta_j) = \prod_{\mu \in C^*/G} \left\{ \frac{W(\{\zeta_j,\mu\})}{W(\{1,\mu\})} \right\}.$$

This is identity $(3.3e)$ because $D_j \cap C = \{1\}$ means $T_{j,s}$ and $\nu_{j,s}$ are redundant.

We may now assume $D_jC = G$ and there is no non-trivial normal subgroup of D_j lying inside the centralizer of C. (It follows immediately that $D_j \not\supseteq C$ and that $D_j \cap C = \{1\}$.)

Claim II. With C abelian and normal in $D_jC = G$, if there is no non-trivial normal subgroup of D_j lying inside the centralizer of C, then C is its own centralizer.

Proof. Let A be the centralizer of C. Then, being an abelian group, $C \subseteq A$. In fact, $(A \cap D_j) \cdot C \subseteq A$. On the other hand, given $h \in A$ we can write $h = dc$ for some $d \in D_j$ and some $c \in C$. This means $d = hc^{-1} \in A$. So it is possible to conclude that $(A \cap D_j) \cdot C = A$. In addition, with $x \in A \cap D_j$, $d \in D_j$ and $c \in C$,

$$dxd^{-1}c = dxd^{-1}cdd^{-1} = dd^{-1}cdxd^{-1} = cdxd^{-1} .$$

(The equality in the middle holds because x commutes with $d^{-1}cd \in C$.) In other words, dxd^{-1} commutes with all $c \in C$. Therefore, $dxd^{-1} \in A \cap D_j$, which implies $A \cap D_j \lhd D_j$. However, D_j contains no non-trivial normal subgroup lying in A. So we must have $A \cap D_j = \{1\}$. Now it follows from $(A \cap D_j) \cdot C = A$ that $C = A$. $\|$

Suppose $H \triangleleft G$ such that $H \not\supseteq C$. Then $H \cap C$ is abelian and normal in G. Since C is minimal, this means $H \cap C = \{1\}$ which implies that H is contained in the centralizer A of C. By claim II, $H \subseteq C$. So we conclude $H = H \cap C = \{1\}$.

In summary, we have $D_j C = G$, $D_j \cap C = \{1\}$ and C is contained in every non-trivial normal subgroup of G. Because G is not nilpotent, $D_j \neq \{1\}$. Let S^1 be the unit circle in the complex plane, if we define $\theta_j : D_j C \to S^1$ by $\theta_j(d\,c) = \zeta_j(d)$, then θ_j is well-defined and it is a character of $D_j C$. Moreover, the fact $\zeta_j = \theta_j \mid_{D_j}$ is translated into $\zeta_j = \theta_j \circ N_{E_j/F}$ when we view ζ_j and θ_j as characters of $E_j^\times$ and $F^\times$ respectively. In addition, examining the character values on $(D_j C)_\mu = (D_j \cap (D_j C)_\mu) \cdot C$ reveals that $\{\zeta_j, \mu\} = \{1, \mu\} \cdot (\theta_j \mid_{(D_j C)_\mu})$. Therefore, under the condition $D_j \cap C = \{1\}$, identity (3.3e)

$$W(\zeta_j) = \prod_{\mu \in C^*/G} \left\{ \frac{W(\{\zeta_j, \mu\})}{W(\{1, \mu\})} \right\}$$

is exactly the 3rd identity, and our lemma is proved. ||

Case 2 is now completed, and we have shown that statement (i) is true when

$|Gal(K/F)| \;=\; I+1\,.$

Next, we prove statement (iii) by elaborating on the argument at the end of the proof of statement (i). Let $C \;=\; Gal(K/L)$ be an abelian normal subgroup of G. If $C \;=\; \{1\}$, then (iii) becomes a triviality as E itself is contained in $L = K$. By the same argument, the case $C \subsetneq Gal(K/E)$ is equally trivial. So we will assume $C \neq \{1\}$ and $C \not\subseteq Gal(K/E)$.

In the case $E \cap L \neq F$, the order of $Gal(K/E \cap L)$ is less than or equal to I, and $\chi_E \circ N_{K/E} \;=\; (\chi_F \circ N_{(E\cap L)/F}) \circ N_{K/(E\cap L)}$. Hence the induction hypothesis of theorem 3.3.1 implies that there are subfields F_s of $L/(E\cap L)$ and quasi-characters χ_{F_s} on $F_s{}^{\times}$ such that

$$Ind_{W_{K/E}}^{W_{K/(E\cap L)}}(\chi_E - 1) \;=\; \sum_s a_s Ind_{W_{K/F_s}}^{W_{K/(E\cap L)}}(\chi_{F_s} - 1)$$

which means

$$Ind_{W_{K/(E\cap L)}}^{W_{K/F}}\left(Ind_{W_{K/E}}^{W_{K/(E\cap L)}}(\chi_E - 1)\right) = \sum_s a_s Ind_{W_{K/(E\cap L)}}^{W_{K/F}}\left(Ind_{W_{K/F_s}}^{W_{K/(E\cap L)}}(\chi_{F_s} - 1)\right) .$$

Moreover,

$$W(\chi_E) \;=\; \prod_s W(\chi_{F_s})^{a_s}.$$

Notice that the induction hypothesis has already assured χ_{K/F_s} is either $\chi_{K/E}$ or 1.

Suppose now $E \cap L = F$. Let us abbreviate the composition $\chi_F \circ N_{E/F}$ to $\chi_{E/F}$. Because $\chi_{K/E}$ is equal to $\chi_{K/F}$, the character $\chi_E \cdot {\chi_{E/F}}^{-1}$ annihilates the norm group $N_{K/E}(K^\times)$. In fact, $\chi_E \cdot {\chi_{E/F}}^{-1}$ annihilates $N_{K'/E}(K'^\times)$ where K' is the fixed field of the commutator subgroup of $Gal(K/E)$ [2, proposition 4, p.143]. Consequently, $\chi_E \cdot {\chi_{E/F}}^{-1}$ can be identified, via the reciprocity map, with a character θ_E of the Galois group $Gal(K/E) = H$. We will abuse the notation and write $\chi_E = \theta_E \cdot \chi_{E/F}$, interpreting θ_E as a character of $E^\times$. By lemma 1.2.3

$$Ind_H^G(\theta_E) = \sum_{\substack{\mu \in C^*/G \\ \theta_E|_{H\cap C} = \mu|_{H\cap C}}} Ind_{G_\mu}^G(\{\theta_E, \mu\}) .$$

Similarly

$$Ind_H^G(1) = \sum_{\substack{\mu' \in C^*/G \\ \mu'|_{H\cap C} = 1}} Ind_{G_{\mu'}}^G(\{1, \mu'\}) .$$

It follows from lemma 1.2.12 that the first of these equalities can be inflated to

$$Ind_{W_{K/E}}^{W_{K/F}}(\theta_E) = \sum_{\substack{\mu \in C^*/G \\ \theta_E|_{H\cap C} = \mu|_{H\cap C}}} Ind_{W_{K/F_\mu}}^{W_{K/F}}(\{\theta_E, \mu\})$$

where $G_\mu = Gal(K/F_\mu)$. Inflate the second equality accordingly, and let $G_{\mu'} = Gal(K/F_{\mu'})$.

Since lemma 1.2.12 is based on the surjection $W_{K/E} \to Gal(K/E)$ which forms part of a commutative diagram

$$\begin{array}{ccccccc} W_{K/E} & \longrightarrow & Gal(K/E) & \xrightarrow{proj.} & Gal(K/E)^{ab} & \xrightarrow{\theta_E} & S^1 \\ \text{proj.} \downarrow & & & \nearrow & & & \\ (W_{K/E})^{ab} & = & W_{E/E} & \simeq & E^\times & & \end{array}$$

with the reciprocity map $E^\times \to Gal(K/E)^{ab}$, we can conclude that

$$\begin{aligned} Ind_{W_{K/E}}^{W_{K/F}}(\chi_E) &= \left\{ Ind_{W_{K/E}}^{W_{K/F}}(\theta_E) \right\} \otimes \chi_F \\ &= \sum_{\substack{\mu \in C^*/G \\ \theta_E|_{H\cap C} = \mu|_{H\cap C}}} Ind_{W_{K/F_\mu}}^{W_{K/F}}(\{\theta_E, \mu\} \cdot \chi_{F_\mu/F}) . \end{aligned}$$

This last equality is due to a commutative diagram (that relates the reciprocity map ${F_\mu}^\times \longrightarrow {G_\mu}^{ab}$ to the surjection $W_{K/F_\mu} \longrightarrow G_\mu$) analogous to the one above and the fact

$$\begin{array}{ccccc} & {F_\mu}^\times & \xrightarrow{\simeq} & (W_{K/F_\mu})^{ab} \\ N_{F_\mu/F} & \downarrow & & \downarrow \\ & F^\times & \xrightarrow{\simeq} & (W_{K/F})^{ab} \end{array}$$

Subtracting the equation

$$Ind_{W_{K/E}}^{W_{K/F}}(1) = \sum_{\substack{\mu' \in C^*/G \\ \mu'|_{H\cap C} = 1}} Ind_{W_{K/F_{\mu'}}}^{W_{K/F}}(\{1, \mu'\})$$

from above, we obtain

$$\begin{aligned} Ind_{W_{K/E}}^{W_{K/F}}(\chi_E - 1) &= \sum_{\substack{\mu \in C^*/G \\ \theta_E|_{H\cap C} = \mu|_{H\cap C}}} Ind_{W_{K/F_\mu}}^{W_{K/F}}(\{\theta_E, \mu\} \cdot \chi_{F_\mu/F}) \\ &\quad - \sum_{\substack{\mu' \in C^*/G \\ \mu'|_{H\cap C} = 1}} Ind_{W_{K/F_{\mu'}}}^{W_{K/F}}(\{1, \mu'\}) . \end{aligned}$$

It is important to remark that both F_μ and $F_{\mu'}$ are subfields of L/F. In fact, because G_μ and $G_{\mu'}$ contain the centralizer of C, if L' denotes the fixed field of this centralizer, then F_μ and $F_{\mu'}$ are subfields of L'/F. Moreover, $C \lhd G$ implies the centralizer of C is also normal. This means L'/F is a Galois extension. Therefore, the representation

$$\sigma = \sum_{\substack{\mu \in C^*/G \\ \theta_E|_{H\cap C} = \mu|_{H\cap C}}} Ind_{G_\mu}^{G}(1) - \sum_{\substack{\mu' \in C^*/G \\ \mu'|_{H\cap C} = 1}} Ind_{G_{\mu'}}^{G}(1)$$

which has dimension zero, is an inflation of a similar virtual representation of $G/Gal(K/L')$. According to the variation of Brauer's theorem in chapter 2 and lemma 1.2.11,

$$\sigma = \sum_t d_t \, Ind_{K_t}^{G}(\alpha_t - 1) \tag{3.3g}$$

for some K_t containing $Gal(K/L')$ and character α_t annihilating $Gal(K/L')$.

Let $K_t = Gal(K/F_t)$. By lemma 1.2.12, $(3.3g)$ is inflated to

$$\sum_{\substack{\mu \in C^*/G \\ \theta_E|_{H\cap C} = \mu|_{H\cap C}}} Ind_{W_{K/F_\mu}}^{W_{K/F}}(1) - \sum_{\substack{\mu' \in C^*/G \\ \mu'|_{H\cap C} = 1}} Ind_{W_{K/F_{\mu'}}}^{W_{K/F}}(1) = \sum_t d_t \, Ind_{W_{K/F_t}}^{W_{K/F}}(\alpha_t - 1)$$

where the subfields F_t are contained in L', the fixed field of the centralizer of C. As a result,

$$\begin{aligned} Ind_{W_{K/E}}^{W_{K/F}}(\chi_E - 1) = & \sum_{\substack{\mu \in C^*/G \\ \theta_E|_{H\cap C} = \mu|_{H\cap C}}} Ind_{W_{K/F_\mu}}^{W_{K/F}}(\{\theta_E, \mu\} \cdot \chi_{F_\mu/F} - 1) \\ & - \sum_{\substack{\mu' \in C^*/G \\ \mu'|_{H\cap C} = 1}} Ind_{W_{K/F_{\mu'}}}^{W_{K/F}}(\{1, \mu'\} - 1) \\ & + \sum_t d_t \, Ind_{W_{K/F_t}}^{W_{K/F}}(\alpha_t - 1) \end{aligned} \qquad (3.3h).$$

Moreover, as a character of $F_\mu^{\times}$ (via the reciprocity map $F_\mu^{\times} \longrightarrow G_\mu^{ab}$), $\{\theta_E, \mu\}$ satisfies $\{\theta_E, \mu\} \circ N_{K/F_\mu} = 1$. Therefore,

$$\left(\{\theta_E, \mu\} \cdot \chi_{F_\mu/F}\right) \circ N_{K/F_\mu} = \chi_{K/E} \,.$$

Similarly, we conclude that $\{1, \mu'\} \circ N_{K/F_{\mu'}} = 1$ and $\alpha_t \circ N_{K/F_t} = 1$. Now, to complete the argument for statement (*iii*), it remains to show

$$W(\chi_E) = \frac{\prod_{\substack{\mu \in C^*/G \\ \theta_E|_{H\cap C} = \mu|_{H\cap C}}} W\left(\{\theta_E, \mu\} \cdot \chi_{F_\mu/F}\right)}{\prod_{\substack{\mu' \in C^*/G \\ \mu'|_{H\cap C} = 1}} W\left(\{1, \mu'\}\right)} \prod_t W(\alpha_t)^{d_t} \qquad (3.3i).$$

If the composite $EL \neq K$, or equivalently $H \cap C \neq \{1\}$, then E, F_μ, $F_{\mu'}$, F_t are subfields of $(EL)/F$. As $E \cap L = F$ implies $HC = G$, we note $H \cap C \lhd G$. So $(EL)/F$ is a Galois extension, and according to lemma 1.2.11, $(3.3h)$ is an inflation of

$$\begin{aligned} Ind_{W_{(EL)/E}}^{W_{(EL)/F}} (\chi_E - 1) = & \sum_{\substack{\mu \in C^*/G \\ \theta_E|_{H\cap C} = \mu|_{H\cap C}}} Ind_{W_{(EL)/F_\mu}}^{W_{(EL)/F}} \left(\{\theta_E, \mu\} \cdot \chi_{F_\mu/F} - 1\right) \\ & - \sum_{\substack{\mu' \in C^*/G \\ \mu'|_{H\cap C} = 1}} Ind_{W_{(EL)/F_{\mu'}}}^{W_{(EL)/F}} \left(\{1, \mu'\} - 1\right) \\ & + \sum_t d_t \, Ind_{W_{(EL)/F_t}}^{W_{(EL)/F}} (\alpha_t - 1) \end{aligned}$$

to which the induction hypothesis of theorem 3.3.1 applies because $I \geq |Gal(EL/F)|$. Thus $(3.3i)$ follows from this equality. Similarly, if $H = Gal(K/E)$ contains a non-trivial normal subgroup $H_1 = Gal(K/K_1)$ lying in the centralizer of C, then $H_1 \lhd HC = G$. Again, since E, F_μ, $F_{\mu'}$, F_t are subfields of K_1/F, just as before $(3.3h)$ is an inflation of

$$\begin{aligned} Ind_{W_{K_1/E}}^{W_{K_1/F}}(\chi_E - 1) \;=\; & \sum_{\substack{\mu \,\in\, C^*/G \\ \theta_E|_{H\cap C} \,=\, \mu|_{H\cap C}}} Ind_{W_{K_1/F_\mu}}^{W_{K_1/F}}\left(\{\theta_E, \mu\}\cdot \chi_{F_\mu/F} - 1\right) \\ & - \sum_{\substack{\mu' \,\in\, C^*/G \\ \mu'|_{H\cap C} \,=\, 1}} Ind_{W_{K_1/F_{\mu'}}}^{W_{K_1/F}}\left(\{1, \mu'\} - 1\right) \\ & + \sum_t d_t \, Ind_{W_{K_1/F_t}}^{W_{K_1/F}}(\alpha_t - 1) \; . \end{aligned}$$

Hence the induction hypothesis of theorem 3.3.1 applies, and we have $(3.3i)$.

From now on, we can assume $HC = G$ such that $H \cap C = \{1\}$ and H contains no non-trivial normal subgroup lying in the centralizer of C. In this case, the characters α_t in $(3.3h)$ are redundant by definition, and their abelian root numbers do not appear in $(3.3i)$.

Claim III. *With these assumptions, the quasi-character* χ_F *in statement (iii) can be chosen such that* $\chi_E = \chi_{E/F}$. *If we further assume that* C *is* *minimal in the sense that C contains no proper abelian normal subgroup of G, then (3.3i) is reduced to either the 1st identity or the 3rd identity.*

Proof. We have already seen that there exists a character θ_E of $H = Gal(K/E)$ such that, when viewed as a character of $E^\times$ under the reciprocity map, θ_E satisfies $\chi_E = \theta_E \cdot \chi_{E/F}$. Because $H \cap C = \{1\}$, every element in $HC = G$ can be expressed uniquely as a product hc for some $h \in H$ and some $c \in C$. So it is possible to define a character θ_F of G by $\theta_F(hc) = \theta_E(h)$. When this character θ_F is viewed as a character of $F^\times$, it follows from the definition of θ_F that $\theta_F \circ N_{E/F} = \theta_E$. Therefore, $\chi_E = \theta_{E/F} \cdot \chi_{E/F}$, which means $\chi_E = (\theta_F \cdot \chi_F) \circ N_{E/F}$.

Suppose $D \triangleleft G$ such that $D \not\supseteq C$. Then $D \cap C$ must be abelian and normal in G. However C is assumed to be minimal, which means $D \cap C = \{1\}$. So, given $d \in D$ and $c \in C$, we have $dcd^{-1}c^{-1} = 1$. This implies D stays inside the centralizer of C. Now recall from claim II that the centralizer of C in HC is equal to C itself, as long as H contains no non-trivial normal subgroup lying in the centralizer of C. As a consequence, $D \subseteq C$. In fact, $\{1\} = D \cap C = D$.

To summarize, we have $HC = G$, $H \cap C = \{1\}$ and that C is contained in every non-trivial normal subgroup of G. Moreover, with $\chi_E = \chi_{E/F}$, (3.3i) is reduced to

$$W(\chi_{E/F}) = \prod_{\mu \in C^*/G} \frac{W(\{1, \mu\} \cdot \chi_{F_\mu/F})}{W(\{1, \mu\})} .$$

This is equal to the 3rd identity when $H \neq \{1\}$ and is equal to the 1st identity when $H = \{1\}$. ||

Complementary to the above claim, let us consider the case when $HC = G$, $H \cap C = \{1\}$ and C is not minimal. Then there exists a non-trivial abelian normal subgroup C_o contained in C, but $C_o \neq C$. This means that $HC_o \neq G$ as $H \cap C = \{1\}$. Suppose $HC_o = Gal(K/F')$. Notice $\chi_{K/E} = (\chi_F \circ N_{F'/F}) \circ N_{K/F'}$. Moreover, the abelian subgroup $C_o = Gal(K/L_o)$ is normal in HC_o. So the induction hypothesis of theorem 3.3.1 asserts that there are subfields F_s' of L_o/F' and quasi-characters $\chi_{F_s'}$ satisfying $\chi_{K/F_s'} = 1$ or $\chi_{K/F_s'} = \chi_{K/E}$ such that

$$Ind_{W_{K/E}}^{W_{K/F'}} (\chi_E - 1) = \sum_s a_s \, Ind_{W_{K/F_s'}}^{W_{K/F'}} (\chi_{F_s'} - 1)$$

with

$$W(\chi_E) \;=\; \prod_s W(\chi_{F_s'})^{a_s} \qquad (3.3j).$$

As a result,

$$Ind_{W_{K/F'}}^{W_{K/F}} \left(Ind_{W_{K/E}}^{W_{K/F'}} (\chi_E - 1) \right) \;=\; \sum_s a_s \, Ind_{W_{K/F'}}^{W_{K/F}} \left(Ind_{W_{K/F_s'}}^{W_{K/F'}} (\chi_{F_s'} - 1) \right) .$$

Combine this equality with $(3.3h)$. We observe that, under our assumption $H \cap C \;=\; \{1\}$, the sum

$$\sum_s a_s \, Ind_{W_{K/F'}}^{W_{K/F}} \left(Ind_{W_{K/F_s'}}^{W_{K/F'}} (\chi_{F_s'} - 1) \right) \;=\; \sum_s a_s \, Ind_{W_{K/F_s'}}^{W_{K/F}} (\chi_{F_s'} - 1)$$

is equal to

$$\sum_{\mu \in C^*/G} Ind_{W_{K/F_\mu}}^{W_{K/F}} (\{\theta_E , \mu\} \cdot \chi_{F_\mu/F} \;-\; 1) \;-\; \sum_{\mu \in C^*/G} Ind_{W_{K/F_\mu}}^{W_{K/F}} (\{1 , \mu\} \;-\; 1) \;.$$

Because F_s' and F_μ are subfields of the Galois extension L_o/F, this is an inflation of

$$\sum_s a_s \, Ind_{W_{L_o/F_s'}}^{W_{L_o/F}} (\chi_{F_s'} - 1) \;=\; \sum_{\mu \in C^*/G} Ind_{W_{L_o/F_\mu}}^{W_{L_o/F}} (\{\theta_E , \mu\} \cdot \chi_{F_\mu/F} \;-\; 1)$$
$$-\; \sum_{\mu \in C^*/G} Ind_{W_{L_o/F_\mu}}^{W_{L_o/F}} (\{1 , \mu\} \;-\; 1)$$

according to lemma 1.2.11.

As $I \geq |Gal(L_o/F)|$, the induction hypothesis of theorem 3.3.1 yields

$$\prod_s W(\chi_{F_s'})^{a_s} = \prod_{\mu \in C^*/G} \frac{W(\{\theta_E, \mu\} \cdot \chi_{F_\mu/F})}{W(\{1, \mu\})} .$$

Now (3.3*i*) is a consequence of this equality together with (3.3*j*), and we succeed in showing that statement (*iii*) is true when $|Gal(K/F)| = I + 1$.

Finally we return to statement (*ii*). Given

$$\sum_j m_j \, Ind_{W_{K/E_j}}^{W_{K/F}} (\chi_{E_j} - 1) = 0$$

such that every quasi-character χ_{E_j} has finite order, let B be a field extension of K satisfying the two conditions below.

(1) B/F is a Galois extension of finite degree.

(2) Each χ_{E_j} annihilates the norm group $N_{B/E_j}(B^\times)$ and as a result can be interpreted as a character of the Galois group $Gal(B/E_j)$.

By lemma 1.2.11, we have

$$\sum_j m_j \, Ind_{W_{B/E_j}}^{W_{B/F}} (\chi_{E_j} - 1) = 0$$

which is an inflation (via the surjection $W_{B/F} \longrightarrow Gal(B/F)$) of

$$\sum_j m_j \, Ind_{Gal(B/E_j)}^{Gal(B/F)} (\chi_{E_j} - 1) \; = \; 0 \qquad (3.3k)$$

due to lemma 1.2.11 and the commutative diagram below. (This diagram indicates that χ_{E_j}, as a character of W_{B/E_j} via the top row of horizontal arrows, annihilates $B^\times$, the kernel of $W_{B/E_j} \longrightarrow Gal(B/E_j)$.)

$$\begin{array}{ccccccccc}
W_{B/E_j} & \xrightarrow{proj.} & \overbrace{W_{E_j/E_j}}^{(W_{B/E_j})^{ab}} & \simeq & E_j^\times & \xrightarrow{proj.} & E_j^\times/N_{B/E_j}(B^\times) & \xrightarrow{\chi_{E_j}} & S^1 \\
\downarrow & & & \searrow & & \nearrow \text{isomorphism} & & & \\
Gal(B/E_j) & \xrightarrow{proj.} & & & Gal(B/E_j)^{ab} & & & &
\end{array}$$

Let $G' = Gal(B/F)$ and $G_o' = Gal(B/K)$. Because of lemma 1.2.10, the action on χ_{E_j} by $Gal(B/F)$ does not alter the conclusion of statement (ii). So, without loss of generality we may assume that lemma 1.2.7 applies to $(3.3k)$ with the normal subgroup G_o' in G'. Given a fixed character χ_K in a set of representatives $(G_o')^*/G'$, if

$$Gal(B/F_{\chi_K}) = \{\sigma \in G' \mid \chi_K^\sigma = \chi_K\}$$

then

$$\sum_{\chi_{E_j}|_{G_o'} = \chi_K} m_j \, Ind_{Gal(B/E_j)}^{Gal(B/F_{\chi_K})} (\chi_{E_j}) \;=\; 0$$

for $\chi_K \neq 1$, and

$$\sum_{\chi_{E_j}|_{G_o'} = 1} m_j \, Ind_{Gal(B/E_j)}^{Gal(B/F)} (\chi_{E_j} - 1) \;-\; \sum_{\chi_{E_j}|_{G_o'} \neq 1} m_j \, Ind_{Gal(B/E_j)}^{Gal(B/F)} (1) \;=\; 0$$

for $\chi_K = 1$.

Also notice that $F_{\chi_K} \subseteq K$ because given any $x, \sigma \in G_o'$, we have

$$\chi_K^{\sigma}(x) \;=\; \chi_K(\sigma x \sigma^{-1}) \;=\; \chi_K(\sigma) \cdot \chi_K(x) \cdot \chi_K(\sigma)^{-1} \;=\; \chi_K(x) \,.$$

Consequently, with a fixed $\chi_K \neq 1$, the representations

$$\sum_{\chi_{E_j}|_{G_o'} = \chi_K} m_j \, Ind_{Gal(B/E_j)}^{Gal(B/F_{\chi_K})} (1)$$

and

$$\sum_{\chi_{E_j}|_{G_o'} \neq 1} m_j \, Ind_{Gal(B/E_j)}^{Gal(B/F)} (1)$$

which must have dimension zero according to above, are inflations of similar representations of $Gal(K/F_{\chi_K})$ and $Gal(K/F)$ respectively. Hence, the variation of Brauer's theorem (in chapter 2) and lemma 1.2.11 imply that there exist subfields K_s of K/F_{χ_K} and characters α_s of $Gal(B/K_s)$ satisfying $\alpha_s|_{G_o'} = 1$ such that

$$\sum_{\chi_{E_j}|_{G_o'} = \chi_K} m_j \, Ind_{Gal(B/E_j)}^{Gal(B/F_{\chi_K})} (1) \;=\; \sum_s d_s \, Ind_{Gal(B/K_s)}^{Gal(B/F_{\chi_K})} (\alpha_s - 1)$$

for $\chi_K \neq 1$, and

$$- \sum_{\chi_{E_j}|_{G_o'} \neq 1} m_j \, Ind_{Gal(B/E_j)}^{Gal(B/F)} (1) \;=\; \sum_s d_s \, Ind_{Gal(B/K_s)}^{Gal(B/F)} (\alpha_s - 1)$$

otherwise.

Therefore, no matter χ_K is trivial or not, we have

$$\sum_{\chi_{E_j}|_{G_o'} = \chi_K} m_j \, Ind_{Gal(B/E_j)}^{Gal(B/F_{\chi_K})} (\chi_{E_j} - 1) + \sum_s d_s \, Ind_{Gal(B/K_s)}^{Gal(B/F_{\chi_K})} (\alpha_s - 1) \;=\; 0 \qquad (3.3l).$$

Apply lemma 1.2.12 followed by lemma 1.2.11. $(3.3l)$ yields

$$\sum_{\chi_{E_j}|_{G_o'} = \chi_K} m_j \, Ind_{W_{K/E_j}}^{W_{K/F_{\chi_K}}} (\chi_{E_j} - 1) \;+\; \sum_s d_s \, Ind_{W_{K/K_s}}^{W_{K/F_{\chi_K}}} (\alpha_s - 1) \;=\; 0 \qquad (3.3m).$$

In case $F_{\chi_K} \neq F$, the order of $Gal(K/F_{\chi_K})$ is less than or equal to I and the induction hypothesis of theorem 3.3.1 asserts

$$\prod_{\chi_{E_j}|_{G_o'} = \chi_K} W(\chi_{E_j})^{m_j} \prod_s W(\alpha_s)^{d_s} = 1 \qquad (3.3n).$$

On the other hand, our definition of K_s and α_s shows that

$$\prod_{\chi_K \in (G_o')^*/G'} \prod_s W(\alpha_s)^{d_s} = 1$$

where the index s depends on character χ_K. This last equality can be deduced from statement (i) as well, if we consider

$$\sum_{\chi_K \in (G_o')^*/G'} \sum_s d_s \, Ind_{Gal(K/K_s)}^{Gal(K/F)} (\alpha_s - 1) = 0$$

which is a consequence of $(3.3l)$, $(3.3k)$, lemma 1.2.11 together with the fact that $K_s \subseteq K$ and $\alpha_s|_{G_o'} = 1$.

As a result, once $(3.3n)$ is established for every χ_K in $(G_o')^*/G'$, we can form the product of $(3.3n)$ over all $\chi_K \in (G_o')^*/G'$

$$\left\{ \prod_{\substack{\chi_K \in \\ (G_o')^*/G'}} \prod_{\chi_{E_j}|_{G_o'} = \chi_K} W(\chi_{E_j})^{m_j} \right\} \underbrace{\left\{ \prod_{\substack{\chi_K \in \\ (G_o')^*/G'}} \prod_s W(\alpha_s)^{d_s} \right\}}_{\substack{\text{equals 1} \\ \text{according to above}}} = 1$$

and conclude that

$$\prod_j W(\chi_{E_j})^{m_j} = 1 .$$

So, in order to complete the proof of statement (*ii*), it is sufficient to verify (3.3*n*) when $F_{\chi_K} = F$.

Claim IV. *Suppose* $F_{\chi_K} = F$. *Then* $ker(\chi_K) = Gal(B/M)$ *is normal in* G', *and the cyclic group* $Gal(M/K)$ *is in the center of* $Gal(M/F)$.

Proof. Recall that $G'_o \triangleleft G'$. If $\sigma \in G'$ and $x \in ker(\chi_K)$, then

$$\chi_K(\sigma\, x\, \sigma^{-1}) = \chi_K(x) = 1$$

because $\chi_K^\sigma = \chi_K$ when $F_{\chi_K} = F$. Now let us interpret χ_K as a character of the cyclic group $Gal(M/K)$. Notice $Gal(M/K) \triangleleft Gal(M/F)$ and $\chi_K^b = \chi_K$ if $b \in Gal(M/F)$ i.e. given $a \in Gal(M/K)$, $b \in Gal(M/F)$, we have $\chi_K(b\, a\, b^{-1}) = \chi_K(a)$. Hence it follows that $b\, a\, b^{-1}\, a^{-1} = 1$. This means $Gal(M/K)$ is in the center of $Gal(M/F)$. ||

An immediate consequence of the above claim is that $Gal(M/F)$ is nilpotent if $Gal(K/F)$ is nilpotent. Therefore, theorem 3.2.1 can be applied to

$$\sum_{\chi_{E_j}|_{G_o'} = \chi_K} m_j \, Ind_{Gal(M/E_j)}^{Gal(M/F)} (\chi_{E_j} - 1) \; + \; \sum_s d_s \, Ind_{Gal(M/K_s)}^{Gal(M/F)} (\alpha_s - 1) \; = \; 0$$

which comes from $(3.3l)$ by means of lemma 1.2.11 as $\alpha_s|_{Gal(B/K)} = 1$ for all s and $Gal(B/M) = ker(\chi_K) = ker(\chi_{E_j}|_{Gal(B/K)}) \subseteq ker(\chi_{E_j})$ for those χ_{E_j} that appears in $(3.3l)$. So we have $(3.3n)$ whenever $F_{\chi_K} = F$ and $Gal(K/F)$ is nilpotent.

Henceforth we assume $F_{\chi_K} = F$ and $Gal(K/F)$ is not nilpotent. Then Brauer's theorem claims that $K_s \neq F$ for all s. Because $Gal(K/F)$ is always solvable, it contains a non-trivial abelian normal subgroup $C = Gal(K/L)$.

If E_j and K_s that appears in $(3.3l)$ are all subfields of L/F, then according to lemma 1.2.11, $(3.3m)$ is an inflation of

$$\sum_{\chi_{E_j}|_{G_o'} = \chi_K} m_j \, Ind_{W_{L/E_j}}^{W_{L/F}} (\chi_{E_j} - 1) \; + \; \sum_s d_s \, Ind_{W_{L/K_s}}^{W_{L/F}} (\alpha_s - 1) \; = \; 0$$

Since $I \geq |Gal(L/F)|$, the above equality and the induction hypothesis of theorem 3.3.1 yield $(3.3n)$. Generalizing this argument, we obtain

Claim V. *If the finite sum* $\sum_j m_j \, Ind_{W_{K/E_j}}^{W_{K/F}} (\chi_{E_j} - 1) \;=\; 0$ *with every* E_j *contained in the fixed field of a non-trivial abelian normal subgroup of* $Gal(K/F)$, *then* $\prod_j W(\chi_{E_j})^{m_j} \;=\; 1$ *follows from the induction hypothesis of theorem 3.3.1.*

Now suppose E_j and K_s are not necessarily subfields of L/F. Let us interpret χ_K as a character of $K^\times$ via the isomorphism $K^\times / N_{M/K}(M^\times) \simeq Gal(M/K)$ and consider two possible scenarios:

(a) χ_K *is equal to* $\chi_F \circ N_{K/F}$ *for some quasi-character* χ_F *on* $F^\times$.

(b) *There is no quasi-character* χ_F *on* $F^\times$ *satisfying* $\chi_F \circ N_{K/F} \;=\; \chi_K$.

Observe that, as a character of $K_s^\times$ via the reciprocity map, α_s always annihilate the norm group $N_{K/F}(K^\times)$ by construction. So, in view of the commutative diagram

$$\begin{array}{ccccc} W_{K/K_s} & \overset{proj.}{\longrightarrow} & \overbrace{W_{K_s/K_s}}^{(W_{K/K_s})^{ab}} \;\simeq\; {K_s}^\times & & \\ \downarrow & & \searrow \quad\quad \downarrow \text{ reciprocity map} & & \\ Gal(K/K_s) & \overset{proj.}{\longrightarrow} & Gal(K/K_s)^{ab} & \overset{\alpha_s}{\longrightarrow} & S^1 \end{array}$$

if (a) is true, then statement (*iii*) together with claim V show that (3.3m) implies (3.3n); otherwise notice (b) means $E_j \neq F$. Moreover, we recall $K_s \neq F$ for all s when $Gal(K/F)$ is not nilpotent. Under this circumstance, our next claim deduces (3.3n) from (3.3m) and therefore completes the proof of (3.3n) for all χ_K in $(G'_o)^*/G'$.

Claim VI. *Suppose $Gal(K/F)$ is not nilpotent. Given*

$$\sum_j m_j \, Ind_{W_{K/E_j}}^{W_{K/F}} (\chi_{E_j} - 1) \;=\; 0$$

such that $E_j \neq F$ and χ_{E_j} has finite order for all j, the induction hypothesis of theorem 3.3.1 implies $\prod_j W(\chi_{E_j})^{m_j} \;=\; 1$.

Proof. Again let P be a field extension of K so that

(1) P/F is a Galois extension of finite degree.

(2) χ_{E_j} annihilates the norm group $N_{P/E_j}(P^\times)$. In other words, χ_{E_j} can be interpreted as a character of the Galois group $Gal(P/E_j)$.

Remember the trivial character of $Gal(K/F)$ can be expressed

$$1 \;=\; \sum_{k=1}^{N} e_k \, Ind_{Gal(K/F_k)}^{Gal(K/F)} (\chi_{F_k}) \ .$$

Because $Gal(K/F)$ is not nilpotent, Brauer's theorem further concludes that $F_k \neq F$ for all k. By lemma 1.2.11, the above equality can be inflated into

$$1 = \sum_{k=1}^{N} e_k \, Ind_{Gal(P/F_k)}^{Gal(P/F)} \, (\chi_{F_k}) \qquad (3.3o).$$

Now we invoke lemma 1.2.8 with $G = Gal(P/F)$, $A = E_j$, $B = F_k$, $\chi_A = \chi_{E_j}$, $\chi_B = \chi_{F_k}$.

We denote the corresponding subfields A_ℓ and B_ℓ in lemma 1.2.8 by

$A_\ell = E_{j,k,\ell}$, $B_\ell = F_{j,k,\ell}$ for $M_{j,k} \geq \ell \geq 1$, and there are characters $\chi_{A_\ell} = \chi_{E_{j,k,\ell}}$, $\chi_{B_\ell} = \chi_{F_{j,k,\ell}}$ defined on $Gal(P/E_{j,k,\ell})$ and $Gal(P/F_{j,k,\ell})$ respectively.

Observe from property (1) of lemma 1.2.8 that $A_\ell = E_{j,k,\ell}$ and $B_\ell = F_{j,k,\ell}$ are in fact subfields of K/F. Moreover, being representatives of the $(Gal(P/F_k), Gal(P/E_j))$ double cosets of $Gal(P/F)$, the automorphisms $\sigma_\ell \in Gal(P/E_j)\backslash Gal(P/F)/Gal(P/F_k)$, when restricted to K, are distinct.

By property (5) of lemma 1.2.8, if

$$\alpha_{j,k} = Res_{Gal(P/E_j)} \left(Ind_{Gal(P/F_k)}^{Gal(P/F)} \, (\chi_{F_k}) \right)$$

$$\beta_{j,k} = Res_{Gal(P/F_k)} \left(Ind_{Gal(P/E_j)}^{Gal(P/F)} \, (\chi_{E_j}) \right)$$

$$\beta_{j,k} = Res_{Gal(P/F_k)} \left(Ind_{Gal(P/E_j)}^{Gal(P/F)} \, (\chi_{E_j}) \right)$$

$$\gamma_{j,k} \;=\; Res_{Gal(P/F_k)}\left(Ind_{Gal(P/E_j)}^{Gal(P/F)}\,(1)\right)$$

then $(\chi_{E_j}-1)\otimes\alpha_{j,k}$ is equal to

$$\sum_{\ell=1}^{M_{j,k}} \underbrace{\left\{ Ind_{Gal(P/E_{j,k,\ell})}^{Gal(P/E_j)}\,(\chi_{E_{j,k,\ell}}-1) \;-\; Ind_{Gal(P/E_{j,k,\ell})}^{Gal(P/E_j)}\,((\chi_{F_{j,k,\ell}/F_k})^{\sigma_\ell}-1)\right\}}_{U_{j,k,\ell}}$$

and $(\beta_{j,k}-\gamma_{j,k})\otimes\chi_{F_k}$ is equal to

$$\sum_{\ell=1}^{M_{j,k}} \underbrace{\left\{ Ind_{Gal(P/F_{j,k,\ell})}^{Gal(P/F_k)}\,(\chi_{F_{j,k,\ell}}-1) \;-\; Ind_{Gal(P/F_{j,k,\ell})}^{Gal(P/F_k)}\,(\chi_{F_{j,k,\ell}/F_k}-1)\right\}}_{V_{j,k,\ell}}$$

where character $\chi_{F_{j,k,\ell}/F_k}$ denotes the restriction $\chi_{F_k}|_{Gal(P/F_{j,k,\ell})}$.

Let us abbreviate the above two sums to $\sum_\ell U_{j,k,\ell}$ and $\sum_\ell V_{j,k,\ell}$ respectively.

Now, according to $(3.3o)$,

$$\sum_{k=1}^{N} e_k\,\alpha_{j,k} \;=\; Res_{Gal(P/E_j)}\left(\sum_{k=1}^{N} e_k Ind_{Gal(P/F_k)}^{Gal(P/F)}\,(\chi_{F_k})\right) \;=\; 1\ .$$

On the other hand, by lemma 1.2.11 $\sum_j m_j\, Ind_{W_{K/E_j}}^{W_{K/F}}\,(\chi_{E_j}-1) \;=\; 0$ can be inflated to $\sum_j m_j\, Ind_{W_{P/E_j}}^{W_{P/F}}\,(\chi_{E_j}-1) \;=\; 0$ which then yields

$$\sum_j m_j\, Ind_{Gal(P/E_j)}^{Gal(P/F)}\,(\chi_{E_j}-1) \;=\; 0$$

because of the following commutative diagram.

$$\begin{array}{ccc} W_{P/E_j} \xrightarrow{proj.} (W_{P/E_j})^{ab} = W_{E_j/E_j} & \simeq & {E_j}^{\times} \\ \downarrow & & \downarrow \text{proj.} \\ Gal(P/E_j) \xrightarrow{proj.} Gal(P/E_j)^{ab} & \simeq & {E_j}^{\times}/N_{P/E_j}(P^{\times}) \xrightarrow{\chi_{E_j}} S^1 \end{array}$$

(3.3p).

The above homomorphism $W_{P/E_j} \to Gal(P/E_j)$ is a surjection, which forms part of an exact sequence in lemma 1.2.12. It confirms that the character χ_{E_j} annihilates $P^{\times} \subseteq W_{P/E_j}$.

As a result,

$$\sum_j m_j(\beta_{j,k} - \gamma_{j,k}) = Res_{Gal(P/F_k)} \Big(\sum_j m_j \, Ind_{Gal(P/E_j)}^{Gal(P/F)} (\chi_{E_j} - 1) \Big) = 0 \; .$$

We can therefore conclude that for all j, $\chi_{E_j} - 1$ is equal to

$$(\chi_{E_j} - 1) \otimes \Big\{ \sum_{k=1}^{N} e_k \, \alpha_{j,k} \Big\} = \sum_{k=1}^{N} e_k \Big\{ (\chi_{E_j} - 1) \otimes \alpha_{j,k} \Big\} = \sum_{k=1}^{N} \sum_{\ell=1}^{M_{j,k}} e_k \, U_{j,k,\ell}$$

and for $N \geq k \geq 1$,

$$\Big\{ \sum_j m_j(\beta_{j,k} - \gamma_{j,k}) \Big\} \otimes \chi_{F_k} = \sum_j m_j \Big\{ (\beta_{j,k} - \gamma_{j,k}) \otimes \chi_{F_k} \Big\} = \sum_j \sum_{\ell=1}^{M_{j,k}} m_j \, V_{j,k,\ell}$$

is zero. Apply lemma 1.2.12 followed by lemma 1.2.11. We obtain

$$\chi_{E_j} - 1 = \sum_{k=1}^{N} \sum_{\ell=1}^{M_{j,k}} e_k \left\{ Ind_{W_{K/E_{j,k,\ell}}}^{W_{K/E_j}} (\chi_{E_{j,k,\ell}} - 1) \right.$$
$$\left. - Ind_{W_{K/E_{j,k,\ell}}}^{W_{K/E_j}} ((\chi_{F_{j,k,\ell}/F_k})^{\sigma_\ell} - 1) \right\}$$

as well as

$$0 = \sum_{j} \sum_{\ell=1}^{M_{j,k}} m_j \left\{ Ind_{W_{K/F_{j,k,\ell}}}^{W_{K/F_k}} (\chi_{F_{j,k,\ell}} - 1) \right.$$
$$\left. - Ind_{W_{K/F_{j,k,\ell}}}^{W_{K/F_k}} (\chi_{F_{j,k,\ell}/F_k} - 1) \right\} .$$

It is legitimate to apply lemma 1.2.11 because in (3.3p) the canonical projection $W_{P/E_j} \to (W_{P/E_j})^{ab} = W_{E_j/E_j}$ factors through W_{K/E_j}. We can argue similarly for $\chi_{E_{j,k,\ell}}$, $\chi_{F_{j,k,\ell}}$, $\chi_{F_{j,k,\ell}/F_k}$, $(\chi_{F_{j,k,\ell}/F_k})^{\sigma_\ell}$.

Now, recall that $F_k \neq F$ and $E_j \neq F$. In other words, both $|Gal(K/F_k)|$ and $|Gal(K/E_j)|$ are less than or equal to I . So the induction hypothesis of theorem 3.3.1 yields

$$W(\chi_{E_j}) = \prod_{k=1}^{N} \prod_{\ell=1}^{M_{j,k}} \left\{ \frac{W(\chi_{E_{j,k,\ell}})}{W({\chi_{F_{j,k,\ell}/F_k}}^{\sigma_\ell})} \right\}^{e_k}$$

for all j and

$$1 = \prod_{j} \prod_{\ell=1}^{M_{j,k}} \left\{ \frac{W(\chi_{F_{j,k,\ell}})}{W(\chi_{F_{j,k,\ell}/F_k})} \right\}^{m_j} \qquad (3.3q)$$

for $N \geq k \geq 1$.

Consequently,

$$\prod_j W(\chi_{E_j})^{m_j} = \prod_j \left\{ \prod_{k=1}^{N} \prod_{\ell=1}^{M_{j,k}} \left\{ \frac{W(\chi_{E_{j,k,\ell}})}{W(\,(\chi_{F_{j,k,\ell}/F_k})^{\sigma_\ell}\,)} \right\}^{e_k} \right\}^{m_j}$$

$$= \prod_j \prod_{k=1}^{N} \prod_{\ell=1}^{M_{j,k}} \left\{ \frac{W(\chi_{E_{j,k,\ell}})}{W(\,(\chi_{F_{j,k,\ell}/F_k})^{\sigma_\ell}\,)} \right\}^{e_k\, m_j}$$

$(3.3r)$.

Meanwhile, property (2) of lemma 1.2.8 asserts that $(\chi_{F_{j,k,\ell}})^{\sigma_\ell} = \chi_{E_{j,k,\ell}}$.

Hence lemma 1.2.10 implies

$$W(\chi_{E_{j,k,\ell}}) = W(\,(\chi_{F_{j,k,\ell}})^{\sigma_\ell}\,) = W(\chi_{F_{j,k,\ell}})$$

Similarly,

$$W(\,(\chi_{F_{j,k,\ell}/F_k})^{\sigma_\ell}\,) = W(\chi_{F_{j,k,\ell}/F_k})$$

Substitute these into $(3.3r)$. We have

$$\prod_j W(\chi_{E_j})^{m_j} = \prod_j \prod_{k=1}^{N} \prod_{\ell=1}^{M_{j,k}} \left\{ \frac{W(\chi_{F_{j,k,\ell}})}{W(\chi_{F_{j,k,\ell}/F_k})} \right\}^{e_k\, m_j}$$

$$= \prod_{k=1}^{N} \prod_j \prod_{\ell=1}^{M_{j,k}} \left\{ \frac{W(\chi_{F_{j,k,\ell}})}{W(\chi_{F_{j,k,\ell}/F_k})} \right\}^{e_k\, m_j}$$

$$= \prod_{k=1}^{N} \left\{ \prod_{j} \prod_{\ell=1}^{M_{j,k}} \left\{ \frac{W(\chi_{F_{j,k,\ell}})}{W(\chi_{F_{j,k,\ell}/F_k})} \right\}^{m_j} \right\}^{e_k} .$$

Now, our claim follows from $(3.3q)$. ||

With the above claim, identity $(3.3n)$ is proved for all χ_K. As explained before, when $|Gal(K/F)| = I + 1$, statement (ii) is a direct consequence of $(3.3n)$. This completes the proof of theorem 3.3.1. ||

3.4 Generalization of the epsilon factor

Following Tate [23], we now outline how to define the root number for a representation of the absolute Weil group W_F, so that the root number coincides with our definition in chapter 2 whenever the representation is of Galois type (see Tate [23]). Specifically there exists a function ε_F on the free abelian group $R(W_F)$ generated by irreducible representations of W_F which satisfies (1) and (3) in theorem 2.0.1. We recall that each representation of an absolute Weil group can be factored through some relative Weil group.

To obtain such ε_F, we first define $\varepsilon_F(\phi)$ for irreducible ϕ. Deligne [4] has proved that every irreducible ϕ takes the form $(\rho \circ u) \otimes |\ |_F^s$ where ρ is a representation of some local Galois group $Gal(E/F)$, u is the chain of surjective homomorphisms $W_F \to W_{E/F} \to Gal(E/F)$ and $|\ |_F$ is the normalized absolute value of the local field F . Let us define

$$\varepsilon_F(\phi) \;=\; |\pi_F^{f(\rho) + d \cdot dim\, \rho}|_F^s \cdot W(\rho)$$

such that π_F is a uniformizing parameter of F , $f(\rho)$ is the Artin conductor, d is the order of the absolute different of F and $W(\rho)$ is the root number defined in chapter 2. Due to property (2) in theorem 2.0.1, we may regard ρ as a representation of $Gal(\overline{F}/F)$, where $\overline{F}$ is an algebraic closure of F . The corresponding u is the homomorphism $W_F \to Gal(\overline{F}/F)$.

Theorem 3.4.0. Our definition of $\varepsilon_F(\phi)$ for irreducible ϕ is insensitive to different decompositions of ϕ into a finite component $(\rho \circ u)$ and an infinite component $|\ |_F^s$.

Proof. If

$$(\rho_1 \circ u) \otimes |\ |_F^{s_1} \;=\; (\rho_2 \circ u) \otimes |\ |_F^{s_2}$$

then its equivalence

$$(\rho_1 \circ u) = (\rho_2 \circ u) \otimes |\ |_F^{s_2 - s_1}$$

indicates that the quasi-character $|\ |_F^{s_2 - s_1}$ must send $W_F^{ab} \simeq F^\times$ to a finite image within the unit circle S^1. This means $s_2 - s_1$ is a rational multiple of $2\pi i/\ln(|\pi_F|_F)$. So $|\ |_F^{s_2 - s_1}$ is in fact an unramified character of $F^\times$. We apply theorem 2.0.3 with an appropriate Galois extension K over F and a character χ corresponding to $|\ |_F^{s_2 - s_1}$ under the reciprocity map.

$$\begin{aligned} W(\rho_2 \otimes |\ |_F^{s_2 - s_1}) &= (|\pi_F|_F^{s_2 - s_1})^{f(\rho_2)} \cdot W(|\ |_F^{s_2 - s_1})^{dim \rho_2} \cdot W(\rho_2) \\ &= |\pi_F^{f(\rho_2) + d \cdot dim\, \rho_2}|_F^{s_2 - s_1} \cdot W(\rho_2) \\ &= \frac{|\pi_F^{f(\rho_2) + d \cdot dim\, \rho_2}|_F^{s_2} \cdot W(\rho_2)}{|\pi_F^{f(\rho_2) + d \cdot dim\, \rho_2}|_F^{s_1}} . \end{aligned}$$

Here we have abused the notation $|\ |_F^{s_2 - s_1}$, using it not only as a quasi-character on $F^\times$ but also as the corresponding unramified character χ of the Galois group $Gal(\overline{F}/F)$. Strictly speaking, $\chi \circ u = |\ |_F^{s_2 - s_1}$.

On the other hand, because u is surjective,

$$\rho_1 = \rho_2 \otimes |\ |_F^{s_2 - s_1} \qquad (3.4a).$$

So

$$W(\rho_1) \;=\; W(\rho_2 \otimes |\;|_F^{s_2 - s_1}) \;=\; \frac{|\pi_F^{f(\rho_2) + d \cdot dim\, \rho_2}|_F^{s_2} \cdot W(\rho_2)}{|\pi_F^{f(\rho_2) + d \cdot dim\, \rho_2}|_F^{s_1}}$$

and we can conclude

$$|\pi_F^{f(\rho_1) + d \cdot dim\, \rho_1}|_F^{s_1} \cdot W(\rho_1) \;=\; |\pi_F^{f(\rho_2) + d \cdot dim\, \rho_2}|_F^{s_2} \cdot W(\rho_2) \qquad (3.4b)$$

provided that $dim\, \rho_1 = dim\, \rho_2$ and $f(\rho_1) = f(\rho_2)$.

Claim I. Let ρ, χ be representations of a local Galois group $G = Gal(K/F)$. If in addition χ is an unramified character, then $f(\rho \otimes \chi) = f(\rho)$.

Proof. Use Brauer's induction theorem to write

$$\rho \;=\; \sum_i n_i\, Ind_{H_i}^G\, (\alpha_i) \;.$$

Then

$$\rho \otimes \chi \;=\; \sum_i n_i\, Ind_{H_i}^G\, (\, \alpha_i \cdot (\chi\, |_{H_i})\,) \;.$$

Therefore

$$f(\rho \otimes \chi) \;=\; \sum_i n_i \,\langle\, a_G \;,\; Ind_{H_i}^G\, (\, \alpha_i \cdot (\chi\, |_{H_i})\,)\,\rangle_G \;.$$

By Frobenius reciprocity

$$f(\rho \otimes \chi) \;=\; \sum_i n_i \,\langle\, a_G\, |_{H_i} \;,\; \alpha_i \cdot (\chi\, |_{H_i})\,\rangle_{H_i} \;.$$

According to lemma 2.0.4, if $H_i = Gal(K/E_i)$ and λ_i is the order of the discriminant of E_i/F, then

$$f(\rho \otimes \chi) = \sum_i n_i \left[\lambda_i + \mathrm{f}_{E_i/F} \cdot f(\, \alpha_i \cdot (\chi\,|_{H_i})\,) \right]$$

$$= \sum_i n_i \left[\lambda_i + \mathrm{f}_{E_i/F} \cdot f(\alpha_i) \right]$$

as it is immediate from the definition of the conductor for a character that $f(\, \alpha_i \cdot (\chi\,|_{H_i})\,) = f(\alpha_i)$. Now, we use lemma 2.0.4 once again to conclude that $\sum_i n_i \,[\, \lambda_i + \mathrm{f}_{E_i/F} \cdot f(\alpha_i)\,] = f(\rho)$, and the claim is established. ||

Notice that $(3.4a)$ already implies $dim\, \rho_1 = dim\, \rho_2$. Together with claim I, we have proved $(3.4b)$ and therefore theorem 3.4.0. ||

Having defined $\varepsilon_F(\phi)$ for irreducible ϕ, we extend the function ε_F "linearly" to obtain the root number for all virtual representations of W_F. Thus ε_F satisfies property (1) in theorem 2.0.1 automatically. Moreover this ε_F is consistent with ε_G in chapter 2. Given a representation ρ of $G = Gal(K/F)$, consider its decomposition $\sum_j m_j V_j$ into a direct sum of irreducible representations. If u denotes the chain of surjective homomorphisms $W_F \to W_{K/F} \to Gal(K/F)$, then the Weil group representation

$V_j \circ u$ must be irreducible too. Hence

$$\varepsilon_F(\rho \circ u) \;=\; \prod_j \varepsilon_F(V_j \circ u)^{m_j} \;=\; \underbrace{\prod_j W(V_j)^{m_j} \;=\; \varepsilon_G(\rho)}_{\text{theorem 2.0.1}} \qquad (3.4c).$$

Similarly, we extend the dimension *dim* and the conductor f to all virtual representations by linearity. For irreducible $\phi = (\rho \circ u) \otimes |\,|_F^s$, the dimension of ϕ is given by $dim\,\rho$ and the conductor of ϕ is that of ρ.

Theorem 3.4.1. (A generalization of theorem 2.0.3.) If v is a virtual representation of W_F, then

$$\varepsilon_F(v \otimes |\,|_F^s) = |\pi_F^{f(v)+d\cdot dim\,v}|_F^s \cdot \varepsilon_F(v) = (|\pi_F|_F^s)^{f(v)} \cdot \varepsilon_F(|\,|_F^s)^{dim\,v} \cdot \varepsilon_F(v)\ .$$

Proof. The formula follows directly from the definition of $\varepsilon_F(v)$, $dim\,v$ and $f(v)$ for virtual representation. ||

Finally, we verify that ε_F satisfies property (3) in theorem 2.0.1. For notational simplicity, given any finite extension E over a local field F, the induction $Ind_{W_E}^{W_F}$ will be abbreviated to $Ind_{E/F}$.

Theorem 3.4.2. If ϕ is an irreducible representation of W_E, then

$$\varepsilon_F\Big(Ind_{E/F}\,(\phi - (dim\,\phi)\cdot 1)\Big) = \varepsilon_E\Big(\phi - (dim\,\phi)\cdot 1\Big) .$$

Proof: Let n be the degree of E/F. Suppose $\phi = (\rho \circ u) \otimes |\;|_E^s$, where ρ is a representation of a local Galois group $H = Gal(B/E)$ and u is the chain of homomorphisms $W_E \to W_{B/E} \to Gal(B/E)$. We may select B so that B/F is also Galois. Observe that

$$Ind_{E/F}\,(\phi) = Ind_{E/F}\,(\rho \circ u) \otimes |\;|_F^s .$$

If d_F, d_E are the respective orders of the absolute different of F and the absolute different of E, then by theorem 3.4.1 $\varepsilon_F(Ind_{E/F}\,(\phi))$ is equal to

$$|\pi_F^{f(Ind_{E/F}\,(\rho \circ u)) + d_F \cdot dim\,(Ind_{E/F}\,(\rho \circ u))}|_F^s \cdot \varepsilon_F(Ind_{E/F}\,(\rho \circ u)) .$$

Let G be the Galois group $Gal(B/F)$ and u' be the chain of homomorphisms $W_F \to W_{B/F} \to Gal(B/F)$. It follows from lemma 1.2.11 that

$$Ind_{E/F}\,(\rho \circ u) = \Big(Ind_H^G\,(\rho)\Big) \circ u' .$$

According to (3.4c), we have

$$\varepsilon_F\Big(\Big(Ind_H^G\,(\rho)\Big) \circ u'\Big) = \varepsilon_G\Big(Ind_H^G\,(\rho)\Big) .$$

Moreover, it can be shown from the definition that

$$dim\Big(\big(Ind_H^G(\rho) \big) \circ u' \Big) \;=\; dim\Big(Ind_H^G(\rho) \Big) \;.$$

In fact, for any representation σ of G

$$dim(\, \sigma \circ u' \,) \;=\; dim(\, \sigma \,) \qquad (3.4d).$$

Similarly

$$f\Big(\big(Ind_H^G(\rho) \big) \circ u' \Big) \;=\; f\Big(Ind_H^G(\rho) \Big)$$

and in general

$$f(\, \sigma \circ u' \,) \;=\; f(\, \sigma \,) \qquad (3.4e).$$

Therefore

$$\varepsilon_F\Big(Ind_{E/F}(\phi) \Big) \;=\; |\pi_F^{f(\, Ind_H^G(\rho)\,) + d_F \cdot dim\,(\, Ind_H^G(\rho)\,)}|_F^s \cdot \varepsilon_G\left(Ind_H^G(\rho) \right)$$

which means

$$\varepsilon_F\Big(Ind_{E/F}(\phi \;-\; (dim\,\phi)\cdot 1) \Big)$$

$$=\; |\pi_F^{f(\, Ind_H^G(\rho)\,) + d_F \cdot dim\,(\, Ind_H^G(\rho)\,)}|_F^s \cdot \varepsilon_G\left(Ind_H^G(\rho \;-\; (dim\,\phi)\cdot 1) \right) .$$

Now, recall from (3) in theorem 2.0.1 that $\varepsilon_G\left(Ind_H^G(\rho \;-\; (dim\,\phi)\cdot 1) \right) =$ $\varepsilon_H\left(\rho \;-\; (dim\,\phi)\cdot 1\right)$.

On the other hand $\varepsilon_E(\rho \circ u) = \varepsilon_H(\rho)$ by (3.4c), while theorem 3.4.1 yields

$$\varepsilon_E(\phi) = |\pi_E^{f(\rho \circ u) + d_E \cdot dim(\rho \circ u)}|_E^s \cdot \varepsilon_E(\rho \circ u) .$$

In summary, $\varepsilon_F\Big(Ind_{E/F}(\phi - (dim\,\phi)\cdot 1)\Big)$ is equal to

$$\frac{|\pi_F^{f(Ind_H^G(\rho)) + d_F \cdot dim(Ind_H^G(\rho))}|_F^s}{|\pi_E^{f(\rho \circ u) + d_E \cdot dim(\rho \circ u)}|_E^s} \cdot \varepsilon_E\Big(\phi - (dim\,\phi)\cdot 1\Big) .$$

Analogous to (3.4d) and (3.4e), we have

$$f(\rho \circ u) = f(\rho)$$

and

$$dim(\rho \circ u) = dim(\rho) .$$

So, to establish theorem 3.4.2, it remains to show

$$\frac{|\pi_F^{f(Ind_H^G(\rho)) + d_F \cdot dim(Ind_H^G(\rho))}|_F^s}{|\pi_E^{f(\rho) + d_E \cdot dim(\rho)}|_E^s} = 1 .$$

If $s = 0$, the above equality is a triviality; otherwise this is equivalent to proving

$$f(\,Ind_H^G\,(\rho)\,)\;+\;d_F\cdot dim\,(\,Ind_H^G\,(\rho)\,)\;=\;[\,f(\,\rho\,)\;+\;d_E\cdot dim\,(\,\rho\,)\,]\cdot \mathrm{f}_{E/F} \tag{3.4f}$$

because $|\pi_E|_E \;=\; |\pi_F|_F^{\mathrm{f}_{E/F}}$, where $\mathrm{f}_{E/F}$ is the residue class field degree.

For the finite extension E/F, let $\lambda_{E/F}$ be the order of the discriminant, $d_{E/F}$ be the order of the different, $e_{E/F}$ be the ramification index, and n be the degree. Then lemma 2.0.4 implies

$$\begin{aligned} & f(\,Ind_H^G\,(\rho)\,)\;+\;d_F\cdot dim\,(\,Ind_H^G\,(\rho)\,) \\ =\;& \lambda_{E/F}\cdot dim\,\rho\;+\;\mathrm{f}_{E/F}\cdot f(\rho)\;+\;d_F\cdot n\cdot(dim\,\rho) \\ =\;& \mathrm{f}_{E/F}\cdot d_{E/F}\cdot dim\,\rho\;+\;\mathrm{f}_{E/F}\cdot f(\rho)\;+\;d_F\cdot n\cdot(dim\,\rho) \\ =\;& [\,f(\rho)\;+\;(d_{E/F}\;+\;d_F\cdot e_{E/F})\cdot dim\,\rho\,]\cdot \mathrm{f}_{E/F}\;. \end{aligned}$$

Now the transitivity formula (see chapter III, §4, proposition 8 in Serre [20]) for the different yields (3.4f), and theorem 3.4.2 is proved. ||

For any virtual representation v of W_E with dimension zero, rewrite its decomposition $\sum_j m_j\,\phi_j$ into a direct sum of irreducible representations as follows.

$$v \;=\; \sum_j m_j\, \phi_j \;=\; \sum_j m_j \left(\phi_j \;-\; (\mathit{dim}\,\phi)\cdot 1\right) \;.$$

Then by theorem 3.4.2

$$\begin{aligned} \varepsilon_E\big(v\big) \;&=\; \sum_j m_j\, \varepsilon_E\big(\phi_j \;-\; (\mathit{dim}\,\phi)\cdot 1\big) \\ &=\; \sum_j m_j\, \varepsilon_F\Big(\, \mathit{Ind}_{E/F}\,(\phi_j \;-\; (\mathit{dim}\,\phi)\cdot 1)\,\Big) \\ &=\; \varepsilon_F\Big(\, \mathit{Ind}_{E/F}\,(v)\,\Big) \;. \end{aligned}$$

This is precisely property (3) in theorem 2.0.1.

CHAPTER FOUR

4 The Three Fundamental Identities

This chapter assembles comments and proofs of the three fundamental identities in 3.1. We will present a detailed argument for the tame case (in the sense that all field extensions are tamely ramified) of each identity and remark on what we know about the wild case (i.e. not tame). In an effort to streamline the discussion, some of the general results on abelian root number due to Dwork and Lamprecht (Theorem A.1, A.2, and A.3) have been relocated to the appendix. We begin this chapter with a theorem in section 4.1 that relates root number of a tame quasi-character to ordinary Gauss sum over a finite field. Then section 4.2 to 4.4 look at the three fundamental identities in order. As a reminder, all the fields in this chapter are finite extensions of a p-adic number field Q_p, i.e. they are local fields.

First we fix some notations. For any local field F,

π_F is a uniformizing parameter of F

O_F is the ring of integers of F

$P_F = \pi_F \cdot O_F$ is the maximal ideal of O_F

$U_F = O_F - P_F$ is the unit group of O_F

$U_F^n = 1 + P_F^n$ for $n \geq 1$ and U_F^0 is understood to be just U_F.

$k_F = O_F / P_F$ is the residue class field of F

p is the characteristic of k_F

$N(P_F) = |k_F|$ is the cardinality of the residue class field k_F

F_p is the finite field with p elements

$\mathrm{f} = [k_F : F_p]$ is the residue class field degree of F/Q_p

d is the order of the absolute different of F

λ is the additive map from Q_p to the rationals satisfying two conditions:

(a) The denominator of $\lambda(x)$ is always a power of p.

(b) $\lambda(x) - x$ is a p-adic integer.

$\psi_F = e^{2\pi i\,(\lambda \circ Tr_{F/Q_p})}$ is the canonical additive character of F.

$\zeta = e^{2\pi i/p}$ is a primitive p - th root of unity

F_o is the maximal subfield of F that is unramified over Q_p

O_{F_o} is the ring of integers of F_o

There are occasions in the proof of the identities that a particular choice of the uniformizing parameter simplifies the argument. The following theorem offers one choice that we will use repeatedly.

Theorem 4.0.1. *If K/F is a totally and tamely ramified Galois extension of prime degree n, then there exists a uniformizing parameter π_F of F such that all the roots of the polynomial*

$$x^n + (-1)^n \pi_F$$

are uniformizing parameters of K.

Proof. Since K/F is totally ramified, if $\tilde{\pi}_K$ is a unformizing parameter of K, then $N_{K/F}(\tilde{\pi}_K)$ will be a uniformizing parameter of F. Hence we can choose $\pi_F \in N_{K/F}(K^\times)$. Let K' be the splitting field over F of the Eisenstein polynomial

$$f(x) = x^n + (-1)^n \pi_F$$

The fact that K/F is a totally and tamely ramified Galois extension implies F contains all the n-th roots of unity (see [2, chapter 1, § 8]). So K' must be a totally ramified Galois extension of degree n over F. Moreover all the roots of $f(x)$ are uniformizing parameters of K'. To complete the proof of theorem 4.0.1, we only have to show that the two fields K and K' coincide. First, as K'/F is also tamely ramified,

$$N_{K'/F}(U^1_{K'}) \;=\; U^1_F \;=\; N_{K/F}(U^1_K)$$

Moreover, observe that $U_F/U^1_F \;\simeq\; k_F^\times$, being cyclic, contains a unique subgroup of index n. As a result,

$$N_{K'/F}(U_{K'}) \;=\; N_{K/F}(U_K)$$

According to our choice, $\pi_F \;=\; N_{K/F}(\widetilde{\pi}_K)$ for some uniformizing parameter $\widetilde{\pi}_K$ of K. On the other hand, if $\pi_{K'}$ is a root of $f(x)$, then

$$\pi_F \;=\; N_{K'/F}(\pi_{K'})$$

In other words,

$$N_{K'/F}(\,(K')^\times) \;=\; \langle \pi_F \rangle \cdot N_{K'/F}(U_{K'}) \;=\; \langle \pi_F \rangle \cdot N_{K/F}(U_K) \;=\; N_{K/F}(K^\times)$$

Here $\langle \pi_F \rangle$ denotes the cyclic group $\{ \pi_F^m \mid m \text{ is an integer} \}$. Now we can conclude that $K' = K$ and the theorem is proved. ||

An immediate consequence of theorem 4.0.1 is that given a totally and tamely ramified Galois extension K/F of prime degree n, we can select uniformizing parameters π_K, π_F for K and F respectively such that

$$\pi_F = N_{K/F}(\pi_K) = (-1)^{n+1} \pi_K^n$$

4.1 Abelian root numbers and Gauss sums

By a tame quasi-character χ on $F^\times$ we mean $\chi(U_F^1) = \{1\}$ but $\chi(U_F) \neq \{1\}$. Restricted to the unit group U_F, such quasi-character χ can be identified with a character of $k_F^\times = U_F/U_F^1$.

Theorem 4.1.1. *If χ is a tame quasi-character on $F^\times$ with root number $W(\chi)$, then $N(P_F)^{1/2}\, W(\chi)$ is given by*

$$\sum_{x \in U_F/U_F^1} \chi^{-1}\left(\frac{x}{\pi_F^{d+1}}\right) \psi_F\left(\frac{x}{\pi_F^{d+1}}\right) = -\chi(t\, \pi_F^{d+1})\, G_{\mathfrak{f}}(\chi^{-1}) ,$$

where

$$G_{\mathfrak{f}}(\chi) \;=\; -\sum_{x \,\in\, k_F^\times} \chi(x)\,\zeta^{\,Tr_{k_F/F_p}(x)}$$

is the ordinary Gauss sum over the residue class field k_F *with* $p^{\mathfrak{f}}$ *elements*

and

$$t \;=\; Tr_{F/F_o}\left(\frac{p}{\pi_F^{d+1}}\right)$$

is a unit in O_{F_o} *.*

Proof. The additive character $\psi_F\left(x/\pi_F^{d+1}\right)$ is a character of the residue class field $k_F = O_F/P_F$. So there exists $t \in k_F$ such that

$$\psi_F\left(\frac{x}{\pi_F^{d+1}}\right) \;=\; \zeta^{\,Tr_{k_F/F_p}(t\,x)} \qquad \text{for all } x \in k_F\,.$$

See [22, § 2.2, lemma 2.2.1]. This parameter t can be made more explicit. Notice that given $x \in O_F$,

$$Tr_{F/Q_p}\left(\frac{p\,x}{\pi_F^{d+1}}\right) \quad \text{is a } p\text{-adic integer.}$$

In fact, because π_F^d is also the different of F/F_o ,

$$Tr_{F/F_o}\left(\frac{p\,x}{\pi_F^{d+1}}\right) \;\in\; O_{F_o}\;.$$

It follows that

$$\lambda \circ Tr_{F/Q_p}\left(\frac{x}{\pi_F^{d+1}}\right) \;=\; \lambda\left(\frac{1}{p}\; Tr_{F/Q_p}\left(\frac{p\,x}{\pi_F^{d+1}}\right)\right)$$

$$= \lambda\left(\frac{1}{p}\ Tr_{F_o/Q_p}\left[Tr_{F/F_o}\left(\frac{p\,x}{\pi_F^{d+1}}\right)\right]\right)$$

$$= \lambda\left(\frac{1}{p}\ Tr_{k_F/F_p}\left[Tr_{F/F_o}\left(\frac{p\,x}{\pi_F^{d+1}}\right)\right]\right)$$

as $k_F \simeq O_{F_o}/(p \cdot O_{F_o})$. Via this isomorphism, we can select y from O_{F_o} satisfying

$$x \equiv y \mod P_F \ .$$

This means

$$\lambda \circ Tr_{F/Q_p}\left(\frac{x}{\pi_F^{d+1}}\right) = \lambda \circ Tr_{F/Q_p}\left(\frac{y}{\pi_F^{d+1}}\right) .$$

However,

$$\lambda \circ Tr_{F/Q_p}\left(\frac{y}{\pi_F^{d+1}}\right) = \lambda\left(\frac{1}{p}\ Tr_{\,k_F/F_p}\left[y \cdot Tr_{F/F_o}\left(\frac{p}{\pi_F^{d+1}}\right)\right]\right) .$$

Therefore

$$\psi_F\left(\frac{x}{\pi_F^{d+1}}\right) = e^{2\pi i\left(\lambda \circ Tr_{F/Q_p}\left(x/\pi_F^{d+1}\right)\right)} = \zeta^{Tr\ k_F/F_p\left[x \cdot Tr_{F/F_o}\left(p/\pi_F^{d+1}\right)\right]}$$

$$(4.1a).$$

Observe that $Tr_{F/F_o}\left(p/\pi_F^{d+1}\right)$ belongs to O_{F_o} and we may take

$$t = Tr_{F/F_o}\left(\frac{p}{\pi_F^{d+1}}\right)$$

which must be a unit in O_{F_o} because $\psi_F\left(x/\pi_F^{d+1}\right)$ is non-trivial on k_F.

To complete the proof, consider

$$G_{\mathfrak{f}}(\chi^{-1}) \;=\; -\sum_{x \in k_F^{\times}} \chi^{-1}(x)\, \zeta^{\,Tr_{k_F/F_p}(x)} \;.$$

Since $t \neq 0$, multiplication by t is a bijection from k_F to itself. So

$$-\,G_{\mathfrak{f}}(\chi^{-1}) \;=\; \sum_{x \in k_F^{\times}} \chi^{-1}(t\,x)\, \zeta^{\,Tr_{k_F/F_p}(t\,x)}$$

By $(4.1a)$,

$$-\,\chi(t)\, G_{\mathfrak{f}}(\chi^{-1}) \;=\; \sum_{x \in k_F^{\times}} \chi^{-1}(x)\, \psi_F\!\left(\frac{x}{\pi_F^{d+1}}\right) \;.$$

Recall that the inclusion map $U_F \hookrightarrow O_F$ induces the group isomorphism $U_F/U_F^1 \;\simeq\; k_F^{\times}$. Consequently,

$$-\,\chi(t\,\pi_F^{d+1})\, G_{\mathfrak{f}}(\chi^{-1}) \;=\; \sum_{x \in U_F/U_F^1} \chi^{-1}\!\left(\frac{x}{\pi_F^{d+1}}\right) \psi_F\!\left(\frac{x}{\pi_F^{d+1}}\right) \;.$$

This equality and the definition of $W(\chi)$ establish theorem 4.1.1. ||

When K/F is a tamely ramified Galois extension, Frohlich and Taylor [8] have shown that theorem 4.1.1 is a special case of an analogous result for all tamely ramified irreducible representations of $Gal(K/F)$ (see [8], (3.1), p.156).

Theorem 4.1.1 suggests that the familiar identities between ordinary Gauss sums (Evans [7, §§ 2 – 3]) can be translated into root number identities. This is in fact a principal goal of the subsequent sections.

4.2 The first identity

We begin with theorem 4.2.1 which reduces the proof of the 1st identity to that of the following **special case**:

For any Galois extension E/F of prime degree and quasi-character φ on $F^\times$,

$$W(\varphi \circ N_{E/F}) \prod_{\mu \in S(E/F)} W(\mu) = \prod_{\mu \in S(E/F)} W(\varphi \cdot \mu)$$

where $S(E/F)$ consists of characters of $F^\times$ which annihilate the norm group $N_{E/F}(E^\times)$.

Theorem 4.2.1. *This special case implies the 1st identity in 3.1.*

Proof. Let E/F be an abelian extension. We are going to argue inductively. For $[E:F] = 1$, both sides of the identity collapse into $W(\varphi)$. Suppose the 1st identity is true for $[E:F]$ less than or equal to I. Given an abelian extension E/F of degree $I+1$, it contains a subfield L such that E/L is cyclic of prime degree. Since the case $L = F$ is a triviality, let us assume that $[L:F] > 1$. Then the above special case of the 1st identity asserts

$$W((\varphi \circ N_{L/F}) \circ N_{E/L}) \prod_{\mu \in S(E/L)} W(\mu) = \prod_{\mu \in S(E/L)} W((\varphi \circ N_{L/F}) \cdot \mu) \tag{4.2a}$$

Observe that $\nu \in S(E/F)$ implies $\nu \circ N_{L/F} \in S(E/L)$. In fact, for each $\mu \in S(E/L)$, there are exactly $[L:F]$ such ν satisfying

$$\nu \circ N_{L/F} = \mu$$

because among the $[E:F]$ characters in $S(E/F)$ we have $[L:F]$ of them annihilating the norm group $N_{L/F}(L^{\times})$. The induction hypothesis shows

$$W((\varphi \circ N_{L/F}) \cdot \mu) = W((\varphi \cdot \nu) \circ N_{L/F}) = \frac{\prod_{\tau \in S(L/F)} W(\varphi \cdot \nu \cdot \tau)}{\prod_{\tau \in S(L/F)} W(\tau)} .$$

Similarly we have

$$W(\mu) = W(\nu \circ N_{L/F}) = \frac{\prod_{\tau \in S(L/F)} W(\nu \cdot \tau)}{\prod_{\tau \in S(L/F)} W(\tau)} .$$

By substituting these into $(4.2a)$, we obtain

$$W((\varphi \circ N_{L/F}) \circ N_{E/L}) \cdot \prod_{\mu \in S(E/L)} \left\{ \frac{\prod_{\tau \in S(L/F)} W(\nu \cdot \tau)}{\prod_{\tau \in S(L/F)} W(\tau)} \right\}$$

$$= \prod_{\mu \in S(E/L)} \left\{ \frac{\prod_{\tau \in S(L/F)} W(\varphi \cdot \nu \cdot \tau)}{\prod_{\tau \in S(L/F)} W(\tau)} \right\}$$

which simplifies to

$$W(\varphi \circ N_{E/F}) \prod_{\mu \in S(E/L)} \prod_{\tau \in S(L/F)} W(\nu \cdot \tau) = \prod_{\mu \in S(E/L)} \prod_{\tau \in S(L/F)} W(\varphi \cdot \nu \cdot \tau) .$$

As both μ and τ vary, the corresponding $\nu \cdot \tau$ exhaust the characters in $S(E/F)$. Hence we arrive at the 1st identity for $[E:F] = I+1$. ||

We will first prove the identity by assuming E/F is unramified. Then we deal with the case when E/F is tamely ramified. Because of theorem 4.2.1, it is sufficient to do these for prime degree $[E:F]$.

Theorem 4.2.2. *Suppose E/F is an unramified Galois extension of prime degree ℓ. Let φ be a quasi-character on $F^\times$. If $S(E/F)$ consists of characters of $F^\times$ that annihilate the norm group $N_{E/F}(E^\times)$, then*

$$W(\varphi \circ N_{E/F}) \prod_{\mu \in S(E/F)} W(\mu) = \prod_{\mu \in S(E/F)} W(\varphi \cdot \mu) \qquad (4.2b).$$

Proof. Because E/F is unramified,

$$N_{E/F}(U_E^n) = U_F^n \qquad \text{for all } n \geq 0 \qquad (4.2c).$$

We conclude that $\varphi \circ N_{E/F}$ and φ share the same conductor which will be denoted by m.

If $m = 0$, then $(4.2b)$ becomes

$$\varphi \circ N_{E/F}(\pi_F^d) \prod_{\mu \in S(E/F)} \mu(\pi_F^d) = \prod_{\mu \in S(E/F)} \varphi(\pi_F^d)\, \mu(\pi_F^d)$$

since $(4.2c)$ implies that all $\mu \in S(E/F)$ are unramified. Thus it remains to show

$$\varphi \circ N_{E/F}(\pi_F^d) = \varphi(\pi_F^d)^{\ell}$$

but this is immediate as $N_{E/F}(\pi_F^d) = (\pi_F^d)^{\ell}$.

Now, let us assume $m > 0$. Again, because $\mu \in S(E/F)$ must be unramified, the definition of root number yields

$$W(\varphi \cdot \mu) = \mu(\pi_F^{d+m})\, W(\varphi) .$$

As a result, (4.2b) follows if we can prove

$$W(\varphi \circ N_{E/F}) = W(\varphi)^{\ell} \prod_{\mu \in S(E/F)} \mu(\pi_F^m) .$$

Claim I. *If* E/F *is an unramified Galois extension of prime degree* ℓ *, then*

$$\prod_{\mu \in S(E/F)} \mu(\pi_F) = (-1)^{(\ell-1)} .$$

Proof. Let μ_o be a non-trivial character of the Galois group $Gal(E/F)$. Then its order is ℓ, and μ_o generates the entire character group of $Gal(E/F)$. Thus

$$\prod_{\mu \in S(E/F)} \mu(\pi_F) = \mu_o(\pi_F)^{\frac{\ell(\ell-1)}{2}} .$$

For ℓ odd, $\mu_o(\pi_F)^{\frac{\ell(\ell-1)}{2}} = (\mu_o(\pi_F)^{\ell})^{\frac{\ell-1}{2}} = 1$ because μ_o has order ℓ.

For $\ell = 2$, $\mu_o(\pi_F)^{\frac{\ell(\ell-1)}{2}} = -1$ because μ_o is an unramified character of order 2.

So we have the claim. ||

According to this claim, the proof of theorem 4.2.2 can be completed by showing that

$$W(\varphi \circ N_{E/F}) \;=\; W(\varphi)^{\ell}\,(-1)^{(\ell-1)\,m} \qquad (4.2d).$$

Claim II. *When* $m = 1$, (4.2d) *is a consequence of the Hasse-Davenport relation [7, p.200].*

Proof. Recall the isomorphism

$$U_F/U_F^1 \;\rightarrow\; (U_F \cdot U_E^1)/U_E^1$$

induced by the inclusion $U_F \hookrightarrow (U_F \cdot U_E^1) \subset U_E$. Because φ is tame, $\varphi|_{U_F}$ can be interpreted as a character of $(U_F \cdot U_E^1)/U_E^1 \simeq k_F^\times$, which is denoted by φ as well. Let χ be a character of $k_E^\times$ with order $p^{\mathrm{f}\ell} - 1$. Here $\mathrm{f} = [k_F : F_p]$. Then, restricted to $k_F^\times$, the character χ has order exactly $p^{\mathrm{f}} - 1$. So there exists an integer α such that

$$\chi^{\alpha} \;=\; \varphi^{-1} \qquad \text{on } (U_F \cdot U_E^1)/U_E^1 \;.$$

Now we invoke the **Hasse-Davenport relation** (see Evans [7, fomula (6), p.200]). If $q = p^{\mathrm{f}}$, then

$$G_{\mathrm{f}\ell}\left((\chi^{\alpha})^{\frac{q^{\ell}-1}{q-1}} \right) \;=\; G_{\mathrm{f}}(\chi^{\alpha})^{\ell} \;.$$

Here the notation is consistent with that in theorem 4.1.1.

On the other hand, we observe that

$$N_{E/F}(x) \equiv x^{\frac{q^{\ell}-1}{q-1}} \quad mod\ P_E \qquad \text{for } x \in U_E \ .$$

Therefore $x^{\frac{q^{\ell}-1}{q-1}} \in (U_F \cdot U_E^1)$, and we have

$$(\varphi \circ N_{E/F})^{-1} = (\chi^{\alpha})^{\frac{q^{\ell}-1}{q-1}} \qquad \text{on } U_E/U_E^1 \ .$$

(Recall $N_{E/F}$ maps U_E/U_E^1 into $(U_F \cdot U_E^1)/U_E^1$.)

By theorem 4.1.1 and the Hasse-Davenport relation,

$$\frac{N(P_E)^{1/2}\ W(\varphi \circ N_{E/F})}{-\varphi \circ N_{E/F}\left(t'\,\pi_F^{d+1}\right)} = \left(\frac{N(P_F)^{1/2}\ W(\varphi)}{-\varphi\left(t\,\pi_F^{d+1}\right)}\right)^{\ell} \qquad (4.2e)$$

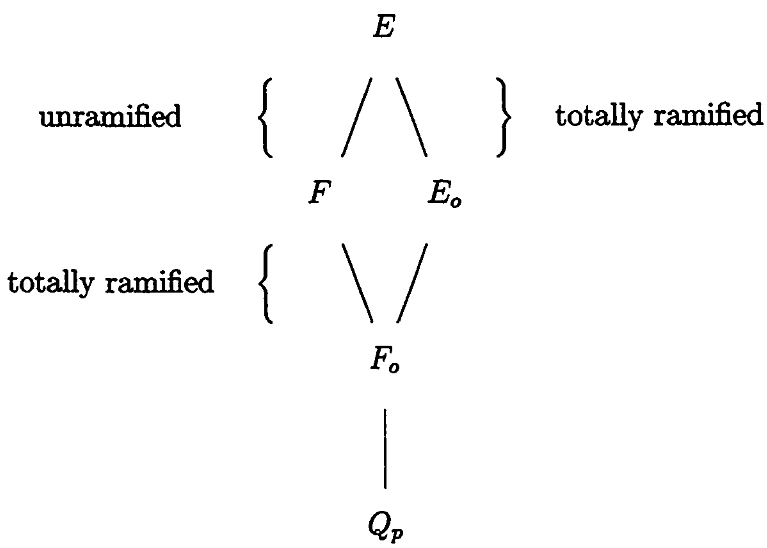
where

$$t' = Tr_{E/E_o}\left(p/\pi_F^{d+1}\right)$$
$$t = Tr_{F/F_o}\left(p/\pi_F^{d+1}\right) \ .$$

Since E/F is unramified, $[k_E : k_F] = \ell$. In other words, $N(P_E) = N(P_F)^{\ell}$. So our claim is proved once we verify that $t' = t$.

From the diagram below, the fact that E_o/Q_p is unramified means that

$[E_o : F_o] = [E : F]$. Moreover, $F \cap E_o = F_o$, while the composite FE_o, unramified over F of degree ℓ, must coincide with E.



(4.2f).

Consequently, we can conclude

$$Tr_{E/E_o}\left(p/\pi_F^{d+1}\right) = Tr_{F/F_o}\left(p/\pi_F^{d+1}\right)$$

and claim II is proved. ||

It remains to establish (4.2d) for $m > 1$. We will consider the following two cases separately.

Case 1 : *m is even. i.e. $m = 2 \cdot d_{(\varphi)}$ for some integer $d_{(\varphi)} > 0$.*

Case 2 : *m is odd. i.e.* $m = 1 + 2 \cdot d_{(\varphi)}$ *for some integer* $d_{(\varphi)} > 0$.

Recall that m is the common conductor of φ and $\varphi \circ N_{E/F}$.

Let us handle **case 1** first. By theorem A.1 (see appendix)

$$W(\varphi \circ N_{E/F}) = (\varphi \circ N_{E/F})^{-1}(\, c(\varphi_{E/F})\,) \;\; \psi_E(\, c(\varphi_{E/F})\,) \qquad (4.2g)$$

where $c(\varphi_{E/F}) \in P_E^{-\,(d+m)}$ satisfies

$$\varphi \circ N_{E/F}\,(1+x) = \psi_E\,(\, c(\varphi_{E/F})\, x\,) \qquad \text{for all } x \in P_E^{d_{(\varphi)}} \, .$$

Since E/F is unramified, theorem A.2 part (b) says we may take

$$c(\varphi_{E/F}) = c \qquad (4.2h)$$

if $c \in P_F^{-\,(d+m)}$ is the parameter in theorem A.1 for φ .

Now, (4.2g) can be rewritten

$$W(\varphi \circ N_{E/F}) = (\varphi \circ N_{E/F})^{-1}(c) \;\; \psi_E(c) = \varphi^{-1}(c)^{\,\ell} \;\; \psi_F(c)^{\,\ell} = W(\varphi)^{\,\ell}.$$

This is exactly (4.2d) because $(-1)^{(\ell-1)\, 2\cdot d_{(\varphi)}} = 1$.

Next we turn to **case 2**. Recall from theorem A.1 that there exist $c(\varphi_{E/F})$ and c such that

$$(\varphi \circ N_{E/F})\,(1+x) \;=\; \psi_E\,(\,c(\varphi_{E/F})\,x\,) \qquad \text{for } x \in P_E^{1+d_{(\varphi)}}$$

and

$$\varphi\,(1+x) \;=\; \psi_F\,(c\,x) \qquad \text{for } x \in P_F^{1+d_{(\varphi)}} \;.$$

Just as in case 1, $(4.2h)$ holds because of theorem A.2 part (b).

To establish $(4.2d)$ in case 2, we will rely on theorem A.3 which is sensitive to the parity of the residue class field characteristic p. Hence our argument will depend on p as well, but first we make a relevant observation arising from $(4.2h)$. Given $\delta \in F$ of order $d_{(\varphi)}$, let us choose $\eta \in O_{F_o}$ so that

$$\psi_F(c\,\delta^2\,x)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\;Tr_{k_F/F_p}(\eta\,x)\right) \qquad \text{for } x \in O_F \;.$$

Then, for any $x \in O_E$

$$\psi_F(\,c\,\delta^2\,Tr_{E/F}(x)\,)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\;Tr_{k_F/F_p}(\,\eta\;Tr_{E/F}(x)\,)\right)$$

which implies

$$\psi_E(c\,\delta^2\,x)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\;Tr_{k_E/F_p}(\eta\,x)\right) \qquad (4.2i).$$

Claim III. *If the characteristic* p *of* k_F *is odd and* $m = 1 + 2 \cdot d_{(\varphi)}$ *, then part* (a) *of theorem A.3 produces* (4.2*d*) .

For notational simplicity, let us abbreviate the composition $\varphi \circ N_{E/F}$ to $\varphi_{E/F}$. Also we reserve f for the residue class field degree $[k_F : F_p]$.

Proof. With the previously selected c , δ and η , we apply part (a) of theorem A.3 to $\varphi_{E/F}$. Because of (4.2h) and (4.2i) , we can conclude

$$W(\varphi_{E/F}) \;=\; \varphi_{E/F}^{-1}(c)\;\psi_E(c)\;\;\psi_E\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\,\eta}{P_E}\right)(-1)^{\ell \mathrm{f}\text{-}1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\,\right)^{\ell \mathrm{f}} \tag{4.2j}$$

where $\gamma \in O_{E_o}$ satisfies

$$\varphi_{E/F}^{-1}(1 + \delta\,x)\,\psi_E(c\,\delta\,x) \;=\; \psi_E\Big(\,c\,\delta^2\,\Big(\frac{x^2}{2} + \gamma\,x\Big)\Big) \qquad \text{for all } x \in O_E\,.$$

We will show that it is possible to choose γ from O_{F_o} . In fact, suppose $\gamma\,'$ is an element in O_{F_o} such that

$$\varphi^{-1}(1 + \delta\,x)\,\psi_F(c\,\delta\,x) \;=\; \psi_F\,\Big(\,c\,\delta^2\,\Big(\frac{x^2}{2} + \gamma\,'\,x\Big)\Big) \qquad \text{for all } x \in O_F\,.$$

Then, given any $x \in O_E$, $\varphi_{E/F}^{-1}(1 + \delta x)\, \psi_E(c\,\delta\, x)$ is equal to

$$\varphi^{-1}(\,1 + \delta\, Tr_{E/F}(x)\,)\; \varphi^{-1}(\,1 + \delta^2\, Tr^{(2)}_{E/F}(x)\,)\; \psi_F(\,c\,\delta\, Tr_{E/F}(x)\,)$$

$$= \psi_F\left(c\,\delta^2\left(\frac{Tr_{E/F}(x)^2}{2} + \gamma'\, Tr_{E/F}(x)\right)\right)\; \varphi^{-1}(\,1 + \delta^2\, Tr^{(2)}_{E/F}(x)\,)$$

$$= \psi_F\left(c\,\delta^2\left(\frac{Tr_{E/F}(x)^2}{2} + \gamma'\, Tr_{E/F}(x)\right)\right)\; \psi_F\,(\,c\,\delta^2\, Tr^{(2)}_{E/F}(x)\,)^{-1}$$

$$= \psi_F\left(c\,\delta^2\left(\frac{Tr_{E/F}(x^2)}{2} + \gamma'\, Tr_{E/F}(x)\right)\right)$$

$$= \psi_E\left(c\,\delta^2\left(\frac{x^2}{2} + \gamma'\, x\right)\right)$$

because of two observations:

1. $N_{E/F}(1 + \delta\, x) \equiv (\,1 + \delta\, Tr_{E/F}(x)\,)(\,1 + \delta^2\, Tr^{(2)}_{E/F}(x)\,) \mod P_F^m$

   where $Tr^{(2)}_{E/F}(x)$ denotes the second elementary symmetric function.

2. $Tr_{E/F}(x)^2 = Tr_{E/F}(x^2) + 2\, Tr^{(2)}_{E/F}(x)$.

In summary, we may take

$$\gamma = \gamma' \in O_{F_o} .$$

As a result, $(4.2j)$ can now be written

$$W(\varphi_{E/F}) = \varphi^{-1}(c)^{\ell}\, \psi_F(c)^{\ell} \left(\psi_F\!\left(c\,\delta^2\, \frac{\gamma^2}{2}\right)^{-1}\right)^{\ell} \left(\frac{-2\,\eta}{P_E}\right) (-1)^{\ell f - 1} \left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\ell f}.$$

Moreover, notice that ℓ is odd implies

$$\left(\frac{-2\,\eta}{P_E}\right) = \left(\frac{-2\,\eta}{P_F}\right) = \left(\frac{-2\,\eta}{P_F}\right)^{\ell}$$

while

$$\left(\frac{-2\,\eta}{P_E}\right) = 1 = \left(\frac{-2\,\eta}{P_F}\right)^{2}$$

when $\ell = 2$.

Therefore $W(\varphi_{E/F})$ is equal to

$$\left[\ \varphi^{-1}(c)\ \psi_F(c)\ \ \psi_F\!\left(c\,\delta^2\,\frac{\gamma^2}{2}\right)^{-1}\left(\frac{-2\,\eta}{P_F}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}\ \right]^{\ell}(-1)^{\ell-1}.$$

By part (a) of theorem A.3, the expression inside the square brackets is precisely $W(\varphi)$, and we are able to conclude that

$$W(\varphi_{E/F}) = W(\varphi)^{\ell}\,(-1)^{\ell-1}$$

which is equivalent to $(4.2d)$ as $m = 1 + 2 \cdot d_{(\varphi)}$. Claim III is now established. ||

The next claim complements the one we just proved. It will complete case 2 and consequently theorem 4.2.2.

Claim IV. *If the characteristic* p *of* k_F *is 2 and* $m = 1 + 2 \cdot d_{(\varphi)}$, *then part* (b) *and part* (c) *of theorem A.3 produces* (4.2d) .

Again, we abbreviate the composition $\varphi \circ N_{E/F}$ to $\varphi_{E/F}$. Recall that f still denotes the residue class field degree $[k_F : F_p]$.

Proof. We apply theorem A.3 part (b) to $\varphi_{E/F}$. With c , δ and η as before, (4.2h) and (4.2i) together imply

$$W(\varphi_{E/F}) \;=\; \varphi_{E/F}^{-1}(c)\ \psi_E(c)\ \Delta \left(\frac{1+i}{\sqrt{2}}\right)^{\ell \mathrm{f}} (-1)^{\ell \mathrm{f}-1} \tag{4.2k}$$

where the Δ factor stands for

$$(-i)^{\,Tr_{k_E/F_p}(\gamma)}\ (-1)^{Tr^{(2)}_{k_E/F_p}(\gamma)}$$

and $\gamma \in O_{E_o}$ satisfies

$$\varphi_{E/F}^{-1}(1 + \beta\,\delta\,x)\,\psi_E(c\,\beta\,\delta\,x) \;=\; i^{\,Tr_{k_E/F_p}(x)}\ (-1)^{Tr^{(2)}_{k_E/F_p}(x)}\ (-1)^{\,Tr_{k_E/F_p}(\gamma\,x)}$$

for all $x \in O_E$. Recall that $\beta \in O_F$ is chosen so that $\beta^2 \equiv \eta^{-1} \mod P_F$.

Now, we are going to show that γ can be chosen from O_{F_o} . For all $x \in O_E$,

$$\varphi_{E/F}^{-1}(1 + \beta\,\delta\,x)\,\psi_E(c\,\beta\,\delta\,x)$$

$$= \varphi^{-1}(\,1 + \beta\,\delta\,Tr_{E/F}(x)\,)\;\varphi^{-1}(\,1 + \eta^{-1}\,\delta^2\,Tr^{(2)}_{E/F}(x)\,)\;\psi_F(\,c\,\beta\,\delta\,Tr_{E/F}(x)\,)$$

because $N_{E/F}(1 + \beta\,\delta\,x) \equiv (\,1 + \beta\,\delta\,Tr_{E/F}(x)\,)(\,1 + \beta^2\,\delta^2\,Tr^{(2)}_{E/F}(x)\,)$ modulo P_F^m. Again, $Tr^{(2)}_{E/F}(x)$ is the second elementary symmetric function.

Let $\gamma\,'$ be an element in O_{F_o} such that for all $x \in O_F$,

$$\varphi^{-1}(1 + \beta\,\delta\,x)\,\psi_F(c\,\beta\,\delta\,x) = i^{\,Tr_{k_F/F_p}(x)}\;(-1)^{Tr^{(2)}_{k_F/F_p}(x)}\;(-1)^{Tr_{k_F/F_p}(\gamma'\,x)}\;.$$

Then we see

$$\varphi_{E/F}^{-1}(1 + \beta\,\delta\,x)\,\psi_E(c\,\beta\,\delta\,x)\;\varphi(\,1 + \eta^{-1}\,\delta^2\,Tr^{(2)}_{E/F}(x)\,)$$

$$= i^{\,Tr_{k_F/F_p}(\,Tr_{E/F}(x)\,)}\;(-1)^{Tr^{(2)}_{k_F/F_p}(\,Tr_{E/F}(x)\,)}\;(-1)^{Tr_{k_F/F_p}(\,\gamma'\,Tr_{E/F}(x)\,)}$$

$$= i^{\,Tr_{k_E/F_p}(x)}\;(-1)^{Tr^{(2)}_{k_F/F_p}(\,Tr_{k_E/k_F}(x)\,)}\;(-1)^{Tr_{k_E/F_p}(\gamma'\,x)}\;.$$

Meanwhile, we recall from the definition of c that

$$\varphi(\,1 + \eta^{-1}\,\delta^2\,Tr^{(2)}_{E/F}(x)\,) = \psi_F(c\,\eta^{-1}\,\delta^2\,Tr^{(2)}_{E/F}(x)\,)$$

$$= (-1)^{Tr_{k_F/F_p}(\, Tr^{(2)}_{k_E/k_F}(x)\,)} \, .$$

As a result, we can conclude

$$\varphi^{-1}_{E/F}(1 + \beta\,\delta\, x)\,\psi_E(c\,\beta\,\delta\, x) \;=\; i^{\,Tr_{k_E/F_p}(x)}\;(-1)^{Tr^{(2)}_{k_E/F_p}(x)}\;(-1)^{\,Tr_{k_E/F_p}(\gamma'\, x)}$$

because $Tr^{(2)}_{k_F/F_p}(\,Tr_{k_E/k_F}(x)\,) + Tr_{k_F/F_p}(\,Tr^{(2)}_{k_E/k_F}(x)\,) \;=\; Tr^{(2)}_{k_E/F_p}(x)$.

To summarize, it is possible to take

$$\gamma \;=\; \gamma' \;\in\; O_{F_o} \, .$$

Consequently, the Δ factor in $(4.2k)$ becomes

$$\Big[\, i^{\,Tr_{k_F/F_p}(\ell\,\gamma)}\;(-1)^{Tr^{(2)}_{k_F/F_p}(\ell\,\gamma) + Tr_{k_F/F_p}(\frac{\ell(\ell-1)}{2}\,\gamma^2)}\,\Big]^{-1}.$$

Apply part (c) of theorem A.3. We obtain

$$(-i)^{\,Tr_{k_E/F_p}(\gamma)}\;(-1)^{Tr^{(2)}_{k_E/F_p}(\gamma)} \;=\; \Big[\Big(\, i^{\,Tr_{k_F/F_p}(\gamma)}\;(-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)}\,\Big)^{\ell}\,\Big]^{-1}$$

$$=\; \Big(\,(-i)^{\,Tr_{k_F/F_p}(\gamma)}\;(-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)}\,\Big)^{\ell}.$$

Substitute into $(4.2k)$. It follows that $W(\varphi_{E/F})$ is equal to

$$\Big(\,\varphi^{-1}(c)\;\psi_F(c)\;\;(-i)^{\,Tr_{k_F/F_p}(\gamma)}\;(-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)}\,\Big(\frac{1+i}{\sqrt{2}}\Big)^{\mathrm{f}}\,(-1)^{\mathrm{f}-1}\,\Big)^{\ell}\,(-1)^{\ell-1} \, .$$

Due to part (*b*) of theorem A.3,

$$W(\varphi) \;=\; \varphi^{-1}(c)\;\psi_F(c)\;\;(-i)^{\,Tr_{k_F/F_p}(\gamma)}\;(-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)}\left(\frac{1+i}{\sqrt{2}}\right)^{\mathrm{f}}(-1)^{\mathrm{f}-1}\;.$$

Hence we have (4.2*d*) and the claim is proved. ||

Now case 2 is established. (4.2*d*) remains true for all $m > 1$. Because (4.2*b*) is a consequence of (4.2*d*) when $m > 0$, we have completed the proof of theorem 4.2.2. ||

After proving the 1st identity when E/F is unramified, we turn to the tamely ramified case in the next theorem. Again it is sufficient to focus on prime degree $[E:F]$ due to theorem 4.2.1.

Theorem 4.2.3. *If E/F is a totally and tamely ramified Galois extension of prime degree ℓ, then the 1st identity* (4.2*b*) *holds.*

Proof. Without loss of generality, we may assume the conductor $m(\varphi)$ of the quasi-character φ is the smallest among $\left\{\, m(\varphi{\cdot}\mu) \;\mid\; \mu \in S(E/F) \,\right\}$. Then

For $m(\varphi)$ less than or equal to one, the two quasi-characters $\varphi \circ N_{E/F}$ and

φ *share the same conductor.*

(4.2*l*)

We divide the proof of theorem 4.2.3 according to $m(\varphi)$, the conductor of φ . Unramified quasi-characters are dealt with first, followed by tamely ramified quasi-characters. When φ is wildly ramified, our argument is sensitive to the parity of $m(\varphi)$, the degree ℓ , as well as the residue class field characteristic p . Hence we have arranged **case 1(a) , (b)** and **case 2(a) , (b) , (c)** to address all possible combinations of $m(\varphi)$, ℓ and p .

Given $m(\varphi) = 0$, we have

$$W(\varphi \cdot \mu) = \varphi(\pi_F^{d+1})\, W(\mu) \qquad \text{for all non-trivial } \mu \in S(E/F)\,.$$

So $(4.2b)$ is equivalent to

$$W(\varphi \circ N_{E/F}) = \varphi(\pi_F^{d})\, \varphi(\pi_F^{d+1})^{\,\ell-1}\ .$$

Notice that $\varphi \circ N_{E/F}$ must be unramified as well. Moreover, because E/F is totally and tamely ramified, the order of the absolute different of E is $\ell - 1 + \ell d$. If we select the uniformizing parameters $\pi_F\,, \pi_E$ such that

$N_{E/F}(\pi_E) = \pi_F$, then (4.2b) becomes

$$\varphi(\pi_F^{\ell-1+\ell d}) = \varphi(\pi_F^{d})\,\varphi(\pi_F^{d+1})^{\,\ell-1}$$

which is self-evident. Therefore, when E/F is totally and tamely ramified, we have (4.2b) for $m(\varphi) = 0$.

Henceforth, our uniformizing parameters for E and F are chosen so that

$$\pi_F = N_{E/F}(\pi_E) = (-1)^{\,\ell+1}\,\pi_E^{\ell} .$$

See theorem 4.0.1.

Next we suppose that $m(\varphi) = 1$. Then $m(\varphi \circ N_{E/F}) = 1$, as noted above in (4.2$l$). Hence φ , $\varphi \circ N_{E/F}$ and all the non-trivial μ are tame. Let f be the residue class field degree $[k_F : F_p]$. Now, we recall the **distribution formula** for ordinary Gauss sums:

$$1 = \frac{\varphi^{-\ell}(\ell)}{G_{\mathfrak{f}}(\varphi^{-\ell})} \prod_{\mu \in S(E/F)} \frac{G_{\mathfrak{f}}(\varphi^{-1}\cdot\mu^{-1})}{G_{\mathfrak{f}}(\mu^{-1})} .$$

See Evans [7, formula (7), p.200].

Before converting this into a root number identity, we point out the following.

Analogous to the above formula,

$$1 \;=\; \frac{1}{N(P_F)} \prod_{\mu \in S(E/F)} \frac{N(P_F)}{N(P_F)^{\,m(\mu)}}$$

can be verified readily. It is equally immediate that $N(P_E) = N(P_F)$. Moreover, the inclusion $U_F \hookrightarrow U_E$ induces an isomorphism $U_F/U_F^1 \simeq U_E/U_E^1$. So the root number $W(\varphi \circ N_{E/F})$ becomes

$$N(P_E)^{-1/2} \sum_{x \,\in\, U_F/U_F^1} (\varphi \circ N_{E/F})^{-1}\left(\frac{x}{\pi_E^{(\ell-1+\ell d)\,+\,1}}\right) \psi_E\left(\frac{x}{\pi_E^{(\ell-1+\ell d)\,+\,1}}\right)$$

which is the same as $\varphi^{\,\ell}(\ell)\, W(\varphi^{\,\ell})$ because $\pi_F = (-1)^{\,\ell+1}\, \pi_E^{\ell}$ and multiplication by the unit $\ell^{-1}(-1)^{\,(\ell+1)(d+1)}$ yields a bijection from U_F/U_F^1 to itself.

Together with theorem 4.1.1, we can now obtain from the distribution formula that

$$\frac{1}{-\,\varphi^{\,-\ell}(t\,\pi_F^{d+1})\;W(\varphi \circ N_{E/F})} \prod_{\mu \in S(E/F)} \frac{(-1)^{m(\mu)}\,\mu(t\,\pi_F^{d+1})\;W(\varphi\cdot\mu)}{-\,(\varphi\cdot\mu)(t\,\pi_F^{d+1})\;W(\mu)}$$

is equal to one. Here,

$$t \;=\; Tr_{F/F_\circ}\left(\frac{p}{\pi_F^{d+1}}\right).$$

In other words, we have (4.2*b*) once it is shown that

$$1 \;=\; \frac{1}{-\,\varphi^{-\ell}(t\,\pi_F^{d+1})} \prod_{\mu \in S(E/F)} \frac{(-1)^{m(\mu)}\,\mu(t\,\pi_F^{d+1})}{-\,(\varphi\cdot\mu)(t\,\pi_F^{d+1})}.$$

Simplifying the product over $S(E/F)$ yields

$$\prod_{\mu \in S(E/F)} \frac{(-1)^{m(\mu)}\,\mu(t\,\pi_F^{d+1})}{-\,(\varphi\cdot\mu)(t\,\pi_F^{d+1})} \;=\; \frac{1}{-\,\varphi(t\,\pi_F^{d+1})^{\,\ell}}\,.$$

Hence (4.2*b*) holds in the case $m(\varphi) = 1$ with E/F tamely ramified.

The following lemma on the j-th elementary symmetric function $Tr^{(j)}_{E/F}$ will be important to the subsequent argument in the proof of theorem 4.2.3.

Lemma 4.2.4 : *Let* $\lfloor x \rfloor$ *be the largest integer among integers less than or equal to* x *. Then for* $\ell - 1 \geq j \geq 1$ *we have*

$$Tr^{(j)}_{E/F}\left(P_E^m\right) \;\subseteq\; P_F^{\left\lfloor \frac{jm\,+\,(\ell-1)}{\ell} \right\rfloor}$$

provided that E/F *is a totally and tamely ramified Galois extension of prime degree* ℓ *.*

Proof: The case $j = 1$ is a well known result (see for example [20, chapter V, § 3, p.83]). For $j > 1$, the higher elementary symmetric function

$Tr^{(j)}_{E/F}(x)$ can be expressed as a sum of traces. In fact, if

$$V = \left\{ S \subset Gal(E/F) \;\middle|\; S \text{ contains exactly } j \text{ elements.} \right\}$$

then

$$Tr^{(j)}_{E/F}(x) = \sum_{\{\sigma_{i_1}, \dots, \sigma_{i_j}\} \in V} Tr_{E/F}\left(\frac{\sigma_{i_1}(x)\,\sigma_{i_2}(x)\,\dots\,\sigma_{i_j}(x)}{\ell} \right)$$

which yields the lemma since the residue class field characteristic p does not divide ℓ. ||

Having established (4.2b) for both unramified and tame φ when E/F is tamely ramified, we are now in the position to examine the case $m(\varphi) > 1$. The argument is splitted into five subcases. **Case 1(a)** , **case 1(b)** together prove (4.2b) for $m(\varphi)$ even and greater than one, while **case 2(a)** , **case 2(b)** , **case 2(c)** account for the odd $m(\varphi)$ greater than one. To simplify the notation in the rest of the proof, let us abbreviate $\varphi \circ N_{E/F}$ to $\varphi_{E/F}$.

Case 1 : *Let* E/F *be totally and tamely ramified of prime degree* ℓ. *We assume* $m(\varphi)$ *is even and greater than one. The proof of* (4.2b) *in this case is divided into*

(a) $\ell \neq 2$.

(b) $\ell = 2$.

Theorem A.1 part (c) and theorem A.2 are both valid in case 1 because $m(\varphi) > 1$ and E/F is tamely ramified. We will show that theorem A.1 together with theorem A.2 suffice to yield case 1(a). As for case 1(b), we will depend on not only theorem A.1, theorem A.2 but also part (a) of theorem A.3.

We first assume $\ell \neq 2$. Let $d_{(\varphi)}$ be the positive integer $\frac{m(\varphi)}{2}$. By theorem A.2 part (a),

$$m(\varphi_{E/F}) = \ell(m(\varphi) - 1) + 1$$

which in this case is a positive even number. Also if $c \in P_F^{-(d + m(\varphi))}$ such that

$$\varphi(1 + x) = \psi_F(cx) \qquad \text{for } x \in P_F^{d_{(\varphi)}}$$

then according to part (c) of theorem A.2, the same c satisfies

$$\varphi_{E/F}(1 + x) = \psi_E(cx) \qquad \text{for } x \in P_E^{d_{(\varphi_{E/F})}}$$

where $m(\varphi_{E/F}) = 2 \cdot d_{(\varphi_{E/F})}$. Hence it follows from part (a) of theorem A.1 that

$$W(\varphi_{E/F}) = \varphi_{E/F}^{-1}(c)\, \psi_E(c) = W(\varphi)^{\ell}.$$

On the other hand, recall from part (c) of theorem A.1

$$W(\varphi \cdot \mu) = W(\varphi) \cdot \mu^{-1}(c)$$

for all $\mu \in S(E/F)$. Therefore

$$\prod_{\mu \in S(E/F)} W(\varphi \cdot \mu) = W(\varphi)^{\ell} \prod_{\mu \in S(E/F)} \mu^{-1}(c) .$$

Given any non-trivial $\mu_o \in S(E/F)$, notice

$$\prod_{\mu \in S(E/F)} \mu^{-1}(c) = \mu_o(c)^{\frac{\ell(\ell-1)}{2}} = 1 \qquad (4.2m)$$

because ℓ is odd. As a result, the claim below completes case 1(a).

Claim V. If E/F is a Galois extension of prime degree $\ell \neq 2$, then

$$\prod_{\mu \in S(E/F)} W(\mu) = 1 .$$

Proof. As it is stated, the claim actually holds when E/F is unramified, although this case does not concern us here in the proof of theorem 4.2.3.

In fact, the above argument that produces (4.2m) handles the claim for unramified E/F as well. Let E/F be totally ramified and u be the jump in the ramification filtration of $G = Gal(E/F)$ i.e.

$$G = G_o = \ldots = G_u \neq G_{u+1} = \{1\} .$$

Then $m(\mu) = u + 1$ for all non-trivial $\mu \in S(E/F)$. By definition,

$$W(\mu) = N(P_F^{u+1})^{-1/2} \sum_{x \in U_F/U_F^{u+1}} \mu^{-1}\left(\frac{x}{\pi_F^{d+u+1}}\right) \psi_F\left(\frac{x}{\pi_F^{d+u+1}}\right) .$$

Because $x \mapsto -x$ induces a bijection from the finite group U_F/U_F^{u+1} to itself, we conclude that the complex conjugate of $W(\mu)$ equals

$$\overline{W(\mu)} = \mu(-1)\, W(\mu^{-1}) .$$

Recall $\ell \neq 2$ is the order of every non-trivial μ. Hence $1 = \mu(-1)^{\ell} = \mu(-1)$. In other words,

$$\overline{W(\mu)} = W(\mu^{-1})$$

which is equal to $W(\mu)^{-1}$ as $|W(\mu)| = 1$ (see [18, II, § 2, proposition 2.2]). Now,

$$\prod_{\mu \in S(E/F)} W(\mu) = 1$$

is a consequence of the fact that $S(E/F)$ contains no character of order 2, when $\ell \neq 2$. ||

After proving (4.2b) for case 1(a), we proceed to case 1(b): $\ell = 2$. So the residue class field characteristic p cannot be 2. Again,

$$m(\varphi_{E/F}) = 2(\, m(\varphi) - 1\,) + 1$$

according to theorem A.2 part (a). This means the conductor of $\varphi_{E/F}$ is odd and greater than one. If we write $m(\varphi) = 2 \cdot d_{(\varphi)}$ and write $m(\varphi_{E/F}) = 1 + 2 \cdot d_{(\varphi_{E/F})}$, then

$$d_{(\varphi_{E/F})} = m(\varphi) - 1 = 2 \cdot d_{(\varphi)} - 1 \qquad (4.2n).$$

With the choice of parameter c as in case 1(a) before, theorem A.2 part (d) asserts that

$$\varphi_{E/F}(1 + x) = \psi_E(c\,x) \qquad \text{for } x \in P_E^{\,1 + d_{(\varphi_{E/F})}}.$$

Since E/F is totally ramified, we can select the parameter η in theorem A.3 from O_{F_o} such that

$$\psi_E(c\,\delta^2\,x)^{-1} = \exp\left(\frac{2\pi i}{p}\, Tr_{k_E/F_p}(\eta\,x)\right) \qquad \text{for all } x \in O_E$$

with

$$\delta = \frac{\pi_F^{d(\varphi)}}{\pi_E} .$$

This choice of δ is legitimate because of (4.2n).

In particular, when $x \in O_F$ and $\zeta = e^{\frac{2\pi i}{p}}$, we have

$$\psi_F(2\,c\,\delta^2\,x)^{-1} = \zeta^{\,Tr_{k_F/F_p}(\eta\,x)} .$$

To see that $\delta^2 \in F$, it is important to remember our uniformizing parameters satisfy

$$\pi_F = (-1)^{\ell+1}\,\pi_E^{\ell} .$$

The order of $c\delta^2$ in F is $d+1$. Therefore, given $\alpha \in U_F$ defined by

$$-\,2\,c\,\delta^2 = \frac{\alpha}{\pi_F^{d+1}}$$

it is possible to identify $\eta\,\alpha^{-1}$ with the parameter $t = Tr_{F/F_o}\big(p/\pi_F^{d+1}\big)$ in theorem 4.1.1 (see (4.1a)). Precisely,

$$\eta\,\alpha^{-1} \equiv t \quad mod\ P_F \qquad (4.2o).$$

On the other hand, it follows from part (a) of theorem A.3 that

$$W(\varphi_{E/F}) = \varphi_{E/F}^{-1}(c)\,\psi_E(c)\ \ \psi_E\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\,\eta}{P_E}\right)(-1)^{f-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{f}$$

(4.2p)

where f can be taken as the residue class field degree $[k_F : F_p]$ and $\gamma \in O_{F_o}$ (since $O_{E_o} = O_{F_o}$) is characterized by

$$\varphi_{E/F}^{-1}(1 + \delta x)\, \psi_E(c\, \delta\, x) \;=\; \psi_E\Big(c\, \delta^2 \Big(\frac{x^2}{2} + \gamma x \Big) \Big) \qquad \text{for all } x \in O_E\,.$$

We are going to show that γ, regarded as an element in k_F, must be zero.

First, notice that

$$N_{E/F}(1 + \delta x) \;=\; 1 \;+\; Tr_{E/F}(\delta x) \;+\; N_{E/F}(\delta x)$$

when $[E : F] = \ell = 2$. Then

$$\varphi_{E/F}^{-1}(1 + \delta x)\, \psi_E(c\, \delta\, x) \;=\; \varphi^{-1}(\, 1 + Tr_{E/F}(\delta x) + N_{E/F}(\delta x)\,)\, \psi_F(\, c\; Tr_{E/F}(\delta x)\,)$$

which is equal to

$$\varphi^{-1}(\, 1 \;+\; Tr_{E/F}(\delta x)\,)\, \varphi^{-1}(\, 1 \;+\; N_{E/F}(\delta x)\,)\, \psi_F(\, c\; Tr_{E/F}(\delta x)\,)$$

as $N_{E/F}(\delta x) \in P_F^{2 \cdot d_{(\varphi)} - 1}$ by (4.2n) and $Tr_{E/F}(\delta x) \in P_F^{d_{(\varphi)}}$ by lemma 4.2.4. Next, recall from theorem A.1 part (a)

$$\varphi^{-1}(\, 1 \;+\; Tr_{E/F}(\delta x)\,)\, \psi_F(\, c\; Tr_{E/F}(\delta x)\,) \;=\; 1\;.$$

Consequently,

$$\varphi_{E/F}^{-1}(1 + \delta x)\, \psi_E(c\,\delta\, x) \;=\; \varphi^{-1}(\,1 + N_{E/F}(\delta x)\,) \;=\; \varphi(\,1 \,-\, N_{E/F}(\delta x)\,)\ .$$

Meanwhile, $N_{E/F}(\delta) \;=\; -\,\delta^2$ with our choice of δ. In other words,

$$\begin{aligned} \varphi_{E/F}^{-1}(1 + \delta x)\, \psi_E(c\,\delta\, x) \;&=\; \varphi(\,1 + \delta^2\, N_{E/F}(x)\,) \\ &=\; \psi_F(\,c\,\delta^2\, N_{E/F}(x)\,) \\ &=\; \psi_E\Big(\frac{c\,\delta^2\, N_{E/F}(x)}{2}\Big)\ . \end{aligned}$$

Finally, $\sigma(x) \;\equiv\; x \;\; mod\ P_E$ for all $\sigma \in Gal(E/F)$. So we have

$$N_{E/F}(x) \;\equiv\; x^2 \;\; mod\ P_E\ .$$

In summary,

$$\varphi_{E/F}^{-1}(1 + \delta x)\, \psi_E(c\,\delta\, x) \;=\; \psi_E\Big(\,c\,\delta^2\,\frac{x^2}{2}\,\Big)$$

from which we conclude that it is possible to take $\gamma \;=\; 0$. Combine this with theorem A.1 part (a) and the fact that $k_E \;=\; k_F$. $(4.2p)$ becomes

$$W(\varphi_{E/F}) \;=\; W(\varphi)^2\, \left(\frac{-2\,\eta}{P_F}\right) (-1)^{\mathrm{f}-1} \left(\sqrt{(-1)^{\frac{p-1}{2}}}\,\right)^{\mathrm{f}}.$$

Just as in case 1(a) before, theorem A.1 part (c) asserts

$$W(\varphi\cdot\mu) \;=\; W(\varphi)\;\cdot\;\mu^{-1}(c)\ .$$

Hence

$$\prod_{\mu \in S(E/F)} W(\varphi \cdot \mu) \;=\; W(\varphi)^2 \prod_{\mu \in S(E/F)} \mu^{-1}(c)\ .$$

To establish (4.2*b*), it remains to show

$$\left(\frac{-2\,\eta}{P_F}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}} W(\mu_o) \;=\; \mu_o^{-1}(c)$$

where μ_o is the non-trivial character in $S(E/F)$. Because $N_{E/F}(\delta) = -\,\delta^2$, we will be content with

$$\left(\frac{-2\,\eta}{P_F}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}} W(\mu_o) \;=\; \mu_o^{-1}(-\,c\,\delta^2) \qquad (4.2q).$$

According to theorem 4.1.1

$$N(P_F)^{1/2}\;W(\mu_o) \;=\; -\,\mu_o(t\,\pi_F^{d+1})\,G_{\mathfrak{f}}\,(\mu_o^{-1})$$

with $t \;=\; Tr_{F/F_o}\!\left(p/\pi_F^{d+1}\right) \;\in\; U_{F_o}$. Thus we have

$$\left(\frac{-2\,\eta}{P_F}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}} W(\mu_o)$$

$$=\; \left(\frac{-2\,\eta}{P_F}\right)(-1)^{\mathrm{f}}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}} N(P_F)^{-1/2}\;\mu_o(t\,\pi_F^{d+1})\;G_{\mathfrak{f}}\,(\mu_o^{-1})\ .$$

Restricted to the unit group U_F, μ_o can be interpreted as the unique character of $k_F^\times$ with order 2. In fact, since $p \neq 2$, given a character χ of $k_F^\times$

with order $|k_F^\times|$,

$$\mu_o(x) \;=\; \chi^{|k_F^\times|/2}(x) \;=\; \left(\frac{x}{P_F}\right) \qquad \text{on } U_F/U_F^1 \simeq k_F^\times \qquad (4.2r).$$

One immediate consequence of the above observation is that

$$\left(\frac{-2\,\eta}{P_F}\right) \mu_o(t\,\pi_F^{d+1}) \;=\; \left(\frac{-2\,\eta}{P_F}\right) \left(\frac{t}{P_F}\right) \mu_o(\pi_F^{d+1}) \;.$$

By (4.2*o*) and the definition of α,

$$\left(\frac{-2\,\eta}{P_F}\right) \mu_o(t\,\pi_F^{d+1}) \;=\; \left(\frac{-2\,\alpha^{-1}}{P_F}\right) \mu_o(\pi_F^{d+1}) \;=\; \mu_o\!\left(\frac{1}{c\,\delta^2}\right) .$$

In the last equality, we make use of the identification in (4.2*r*) as well.

So

$$\left(\frac{-2\,\eta}{P_F}\right) (-1)^{\mathrm{f}-1} \left(\sqrt{(-1)^{\frac{p-1}{2}}}\,\right)^{\mathrm{f}} \; W(\mu_o)$$

$$= \; \mu_o^{-1}(c\,\delta^2) \; (-1)^{\mathrm{f}} \left(\sqrt{(-1)^{\frac{p-1}{2}}}\,\right)^{\mathrm{f}} \; N(P_F)^{-1/2} \; G_{\mathrm{f}}\,(\mu_o^{-1})$$

and (4.2*q*) follows once we verify that

$$(-1)^{\mathrm{f}} \left(\sqrt{(-1)^{\frac{p-1}{2}}}\,\right)^{\mathrm{f}} \; N(P_F)^{-1/2} \; G_{\mathrm{f}}\,(\mu_o^{-1}) \;=\; \mu_o^{-1}(-1) \;=\; \left(\frac{-1}{P_F}\right)$$

Let $q \;=\; |k_F| \;=\; p^{\mathrm{f}}$. It is another consequence of (4.2*r*) that

$$\mu_o(x) \;=\; \chi^{\frac{p-1}{2}}(\,x^{\frac{q-1}{p-1}}\,) \;=\; \chi^{\frac{p-1}{2}}(\,N_{k_F/F_p}(x)\,) \;=\; \underbrace{\left(\frac{N_{k_F/F_p}(x)}{p}\right)}_{\text{Legendre symbol}} \;.$$

Remember the Legendre symbol is the unique character of $F_p^{\times}$ with order two, when $p \neq 2$.

As a result, the Hasse-Davenport relation (see formula (6) in Evans [7]) yields

$$G_{\mathfrak{f}}\,(\mu_o^{-1}) \;=\; \left[\,-\sum_{x\,\in\,F_p^{\times}} \left(\frac{x}{p}\right)\zeta^{\,x}\,\right]^{\mathfrak{f}} .$$

In addition, the explicit value of the quadratic Gauss sum over F_p is known:

$$-\sum_{x\,\in\,F_p^{\times}} \left(\frac{x}{p}\right)\zeta^{\,x} \;=\; -\sqrt{(-1)^{\frac{p-1}{2}}\,p}\ .$$

See for example Ireland and Rosen [12, chapter 6, § 4, Theorem 1, p.75].

Now, because $N(P_F) \;=\; |k_F| \;=\; p^{\mathfrak{f}}$ and

$$\left(\frac{-1}{P_F}\right) \;=\; \left(\frac{-1}{p}\right)^{\mathfrak{f}} \;=\; (-1)^{\,(\frac{p-1}{2})\,\mathfrak{f}}$$

we have

$$\left(\frac{-1}{P_F}\right) \;=\; (-1)^{\mathfrak{f}}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\,\right)^{\mathfrak{f}}\; N(P_F)^{-1/2}\; G_{\mathfrak{f}}\,(\mu_o^{-1})\ .$$

As explained already, this implies $(4.2q)$ and ultimately $(4.2b)$. Hence case 1(b) is completed.

With case 1(a) and case 1(b), we have established $(4.2b)$ for all even

$m(\varphi)$ when E/F is tamely ramified. Case 2 below rounds off the proof of theorem 4.2.3 by aiming at the odd $m(\varphi)$ greater than one.

Case 2 : *Let* E/F *be totally and tamely ramified of prime degree* ℓ . *We assume* $m(\varphi)$ *is odd and greater than one. If* p *denotes the residue class field characteristic, then we divide the proof of* (4.2*b*) *for this case into*

(a) $p \neq 2$ *and* $\ell \neq 2$.

(b) $p \neq 2$ *and* $\ell = 2$.

(c) $p = 2$. *Since* E/F *is tamely ramified,* ℓ *must be odd.*

As a reminder, theorem A.2 as well as theorem A.1 part (*c*) are applicable here because $m(\varphi) > 1$ and E/F is tamely ramified. We are going to formulate two lemmas (4.2.5 and 4.2.6) to simplify the respective arguments in the above three subcases. In fact, it will be shown that lemma 4.2.5, combined with theorem A.2 and part (*a*) of theorem A.3, yields (4.2*b*) for case 2(a), while lemma 4.2.6 yields (4.2*b*) for case 2(b) via theorem A.1, theorem A.2, and theorem A.3 part (*a*) . Regarding case 2(c), we use lemma 4.2.5 again, in conjunction with theorem A.2 and theorem A.3.

Lemma 4.2.5. *Suppose E/F is a totally and tamely ramified Galois extension of prime degree $\ell \neq 2$ and the conductor $m(\varphi)$ of the quasi-character φ on $F^\times$ is greater than one. Then the 1st identity (4.2b) is reduced to*

$$W(\varphi_{E/F}) = W(\varphi)^{\ell} \qquad (4.2s).$$

Recall that the composition $\varphi \circ N_{E/F}$ is abbreviated to $\varphi_{E/F}$.

Proof. Due to claim V, which has been proved in case 1, (4.2b) is equivalent to

$$W(\varphi_{E/F}) = \prod_{\mu \in S(E/F)} W(\varphi \cdot \mu) .$$

Let $d_{(\varphi)}$ be the positive integer such that

$$m(\varphi) = \epsilon + 2 \cdot d_{(\varphi)}$$

where ϵ is either zero or one. By theorem A.1, $\exists\ c \in P_F^{-(d + m(\varphi))}$ satisfying

$$\varphi(1 + x) = \psi_F(c\,x) \qquad \text{for all } x \in P_F^{\epsilon + d_{(\varphi)}} .$$

By part (c) of theorem A.1, we have

$$W(\varphi \cdot \mu) = W(\varphi) \cdot \mu^{-1}(c) \qquad \text{for all } \mu \in S(E/F) .$$

If a non-trivial character μ_o is selected from $S(E/F)$, then

$$\prod_{\mu \in S(E/F)} W(\varphi \cdot \mu) = W(\varphi)^{\ell} \prod_{\mu \in S(E/F)} \mu^{-1}(c) = W(\varphi)^{\ell} \cdot \mu_o^{\frac{\ell(\ell-1)}{2}}(c^{-1})$$

which is equal to $W(\varphi)^{\ell}$ as μ_o has prime order $\ell \neq 2$. So (4.2b) becomes

$$W(\varphi_{E/F}) = W(\varphi)^{\ell} .$$

This is exactly (4.2s). ‖

Now we take into account that $m(\varphi)$ is odd. By part (a) of theorem A.2

$$m(\varphi_{E/F}) = \ell(\, m(\varphi) - 1\,) + 1$$

is odd when φ has odd conductor. Let $d_{(\varphi_{E/F})}$ be the positive integer satisfying $m(\varphi_{E/F}) = 1 + 2 \cdot d_{(\varphi_{E/F})}$. Then

$$d_{(\varphi_{E/F})} = \ell\, d_{(\varphi)} .$$

Remember $d_{(\varphi)}$ is defined by $m(\varphi) = 1 + 2 \cdot d_{(\varphi)}$.

Let us first assume $p \neq 2$ and set $\delta = \pi_F^{d_{(\varphi)}}$. We choose c , η , γ so that

(i) for all $x \in P_F^{1 + d_{(\varphi)}}$,

$$\varphi(1 + x) = \psi_F(c\, x) .$$

(ii) for all $x \in O_F$,

$$\psi_F(c\,\delta^2\,x)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\; Tr_{k_F/F_p}(\eta\,x)\right) .$$

(iii) for all $x \in O_F$,

$$\varphi^{-1}(1 \,+\, \delta x)\,\psi_F(c\,\delta\,x) \;=\; \psi_F\Big(c\,\delta^2\,\Big(\frac{x^2}{2} \,+\, \gamma x\Big)\Big) .$$

Now we are going to show that the same c , δ , η , γ satisfy

(iv) for all $x \in P_E^{1\,+\,d_{(\varphi_{E/F})}}$,

$$\varphi_{E/F}(1 \,+\, x) \;=\; \psi_E(c\,x) .$$

(v) for all $x \in O_E$,

$$\psi_E(c\,\delta^2\,x)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\; Tr_{k_E/F_p}(\ell\,\eta\,x)\right) .$$

To facilitate comparison, let us define $\eta_{(\varphi_{E/F})} \;=\; \ell\,\eta$.

(vi) for all $x \in O_E$,

$$\varphi_{E/F}^{-1}(1 \,+\, \delta x)\,\psi_E(c\,\delta\,x) \;=\; \psi_E\Big(c\,\delta^2\,\Big(\frac{x^2}{2} \,+\, \gamma x\Big)\Big) .$$

Recall that theorem A.2 gives (iv) . As for (v) ,

$$\psi_E(c\,\delta^2\,x)^{-1} \;=\; \psi_F(\,c\,\delta^2\,Tr_{E/F}(x)\,)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\;Tr_{k_F/F_p}(\,\eta\,Tr_{E/F}(x)\,)\right)$$

according to (ii) . However E/F is totally ramified. So

$$\sigma(x) \;\equiv\; x \quad mod\ P_E \qquad \text{for all } \sigma \in Gal(E/F)$$

which means

$$Tr_{E/F}(x) \;\equiv\; \ell\, x \quad mod\ P_E\ .$$

Therefore

$$Tr_{k_F/F_p}(\,\eta\,Tr_{E/F}(x)\,) \;=\; Tr_{k_E/F_p}(\,\eta\,Tr_{E/F}(x)\,) \;=\; Tr_{k_E/F_p}(\ell\,\eta\,x)$$

To prove (vi) , we recall that

$$N_{E/F}(1 + \delta x) \;\equiv\; 1 + Tr_{E/F}(\delta x) + Tr^{(2)}_{E/F}(\delta x) \quad mod\ P_F^{m(\varphi)}$$

for all $x \in O_E$. Hence $\varphi^{-1}_{E/F}(1 + \delta x)\,\psi_E(c\,\delta\,x)$ is equal to

$$\varphi^{-1}(\,1 + Tr_{E/F}(\delta x) + Tr^{(2)}_{E/F}(\delta x)\,)\;\psi_F(\,c\,Tr_{E/F}(\delta x)\,)$$

$$= \;\varphi^{-1}(\,1 + \delta\,Tr_{E/F}(x)\,)\;\varphi^{-1}(\,1 + \delta^2\,Tr^{(2)}_{E/F}(x)\,)\;\psi_F(\,c\,\delta\,Tr_{E/F}(x)\,)$$

$$= \;\psi_F\Big(\,c\,\delta^2\Big[\,\frac{Tr_{E/F}(x)^2}{2} + \gamma\,Tr_{E/F}(x)\Big]\Big)\;\varphi^{-1}(\,1 + \delta^2\,Tr^{(2)}_{E/F}(x)\,)\ .$$

The last equality is true because of (iii). On the other hand, observe

$$Tr_{E/F}(x)^2 \;=\; Tr_{E/F}(x^2) \,+\, 2\,Tr^{(2)}_{E/F}(x)\ .$$

Consequently $\varphi^{-1}_{E/F}(1 + \delta x)\,\psi_E(c\,\delta\,x)$ is equal to

$$\psi_E\Big(c\,\delta^2\,\big(\frac{x^2}{2} + \gamma x\big)\Big)\ \psi_F(\,c\,\delta^2\,Tr^{(2)}_{E/F}(x)\,)\ \varphi^{-1}(\,1 + \delta^2\,Tr^{(2)}_{E/F}(x)\,)\ .$$

(vi) is then obtained, as (i) implies

$$\psi_F(\,c\,\delta^2\,Tr^{(2)}_{E/F}(x)\,)\ \varphi^{-1}(\,1 + \delta^2\,Tr^{(2)}_{E/F}(x)\,) \;=\; 1\ .$$

.

With c, δ, η, γ as above, it follows from theorem A.3 part (a) that

$$W(\varphi_{E/F}) \;=\; \varphi^{-1}_{E/F}(c)\,\psi_E(c)\ \psi_E\Big(\,c\,\delta^2\,\frac{\gamma^2}{2}\,\Big)^{-1}\left(\frac{-2\ell\eta}{P_E}\right)\ (-1)^{\mathrm{f}-1}\,\Big(\sqrt{(-1)^{\frac{p-1}{2}}}\,\Big)^{\mathrm{f}} \qquad (4.2t).$$

Here $\mathrm{f} = [k_F : F_p] = [k_E : F_p]$ since E/F is totally ramified.

We are now in the position to prove $(4.2b)$ for case 2(a). Because of lemma 4.2.5, it is sufficient to establish $(4.2s)$. We apply theorem A.3 part

(a) to φ .

$$W(\varphi) \;=\; \varphi^{-1}(c)\,\psi_F(c)\;\;\psi_F\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\,\eta}{P_F}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}.$$

In the case 2(a), ℓ is assumed odd. Together with $k_F \;=\; k_E$, we conclude

$$\left(\frac{-2\,\eta}{P_E}\right) \;=\; \left(\frac{-2\,\eta}{P_F}\right) \;=\; \left(\frac{-2\,\eta}{P_F}\right)^{\ell}.$$

Thus $(4.2t)$ can be written

$$W(\varphi_{E/F}) \;=\; W(\varphi)^{\ell}\left(\frac{\ell}{P_E}\right)(-1)^{-(\mathrm{f}-1)(\ell-1)}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{-\mathrm{f}(\ell-1)}.$$

Meanwhile, because $\ell - 1$ is even,

$$\left(\frac{\ell}{P_E}\right)(-1)^{-(\mathrm{f}-1)(\ell-1)}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{-\mathrm{f}(\ell-1)} = \left(\frac{\ell}{p}\right)^{\mathrm{f}}\left((-1)^{\frac{p-1}{2}}\right)^{-\mathrm{f}(\frac{\ell-1}{2})}.$$

Here $\left(\frac{\ell}{p}\right)$ is the Legendre symbol. To obtain $(4.2s)$, we must show that the right hand side of the last equality is one. By the quadratic reciprocity law,

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) \;=\; (-1)^{(\frac{p-1}{2})(\frac{\ell-1}{2})}\ .$$

Therefore

$$\left(\frac{\ell}{p}\right)^{\mathrm{f}}\left((-1)^{\frac{p-1}{2}}\right)^{-\mathrm{f}(\frac{\ell-1}{2})} \;=\; \left(\frac{p}{\ell}\right)^{\mathrm{f}} \;=\; \left(\frac{p^{\mathrm{f}}}{\ell}\right).$$

Because E/F is a totally and tamely ramified Galois extension of degree ℓ, the local field F contains all the ℓ-th roots of unity (see [2, chapter 1, § 8, proposition 1, p.32]). So we have

$$p^{\mathfrak{f}} \equiv 1 \quad mod\ \ell \ .$$

See for example Cassels and Frohlich [2, chapter 3, § 1, lemma 4, p.87]. This proves (4.2s) and completes case 2(a).

Keeping c , δ , η , γ as in (i) through (vi) , we proceed to case 2(b), which depends on the following lemma.

Lemma 4.2.6. *Let E/F be a totally and tamely ramified quadratic extension. Then both* (4.2q) *and* (4.2r) *remain true for odd $m(\varphi)$ greater than one.*

Proof. Let μ_o be the non-trivial tame character in $S(E/F)$. By theorem 4.1.1,

$$N(P_F)^{1/2}\, W(\mu_o) \;=\; -\,\mu_o(t\,\pi_F^{d+1})\; G_{\mathfrak{f}}\,(\mu_o^{-1})$$

where $\mathfrak{f}$ is the residue class field degree $[k_F : F_p]$ and $t = Tr_{F/F_o}\big(p/\pi_F^{d+1}\big)$.

On the other hand, recall from theorem A.1 part (b) that $c \in P_F^{-(d+m(\varphi))}$.

If $\alpha \in U_F$ is defined by

$$-c\,\delta^2 = \frac{\alpha}{\pi_F^{d+1}},$$

it follows from (ii) that

$$\psi_F\left(\frac{\alpha\, x}{\pi_F^{d+1}}\right) = \exp\left(\frac{2\pi i}{p}\, Tr_{k_F/F_p}(\eta\, x)\right).$$

Together with $(4.1a)$, this implies

$$\eta\,\alpha^{-1} \equiv t \quad mod\ P_F .$$

Therefore

$$\mu_o(t\,\pi_F^{d+1}) = \mu_o(\eta\ \alpha^{-1}\,\pi_F^{d+1}) = \mu_o\left(\frac{-\eta}{c\,\delta^2}\right) = \mu_o(\eta)\ \mu_o^{-1}(-c\,\delta^2).$$

Meanwhile, restricted to the unit group, μ_o can be interpreted as the unique character of $k_F^{\times}$ with order 2, when the residue class field characteristic $p \neq 2$. So we identify

$$\mu_o(x) = \left(\frac{x}{P_F}\right) = \left(\frac{N_{k_F/F_p}(x)}{p}\right) \qquad \text{for all } x \in U_F .$$

This is $(4.2r)$. In summary,

$$N(P_F)^{1/2}\, W(\mu_o) = -\mu_o^{-1}(-c\,\delta^2)\left(\frac{\eta}{P_F}\right) G_{\mathfrak{f}}\,(\mu_o^{-1}) \qquad (4.2u).$$

With $\zeta = e^{\frac{2\pi i}{p}}$, the ordinary Gauss sum $G_{\mathrm{f}}(\mu_o^{-1})$ equals

$$-\sum_{x \in k_F^\times} \left(\frac{x}{P_F}\right) \zeta^{Tr_{k_F/F_p}(x)} = \left[-\sum_{x \in F_p^\times} \left(\frac{x}{p}\right) \zeta^{x} \right]^{\mathrm{f}} = \left[-\sqrt{(-1)^{\frac{p-1}{2}}\, p} \right]^{\mathrm{f}}$$

by the Hasse-Davenport relation and the explicit evaluation of the quadratic Gauss sum [12]. Since $N(P_F) = p^{\mathrm{f}}$, $(4.2u)$ becomes

$$W(\mu_o) = \mu_o^{-1}(-c\,\delta^2) \left(\frac{\eta}{P_F}\right) (-1)^{\mathrm{f}-1} \left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}$$

which is equivalent to $(4.2q)$ if we recall $\eta_{(\varphi_{E/F})} = 2\,\eta$ from (v), as well as the fact that

$$\left(\frac{-1}{P_F}\right) = \left(\frac{-1}{p}\right)^{\mathrm{f}} = \left[(-1)^{\frac{p-1}{2}}\right]^{\mathrm{f}} .$$

This concludes the proof of lemma 4.2.6. ||

From the above proof,

$$W(\mu_o) = \mu_o^{-1}(-c\,\delta^2) \left(\frac{\eta}{P_F}\right) (-1)^{\mathrm{f}-1} \left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}} .$$

Multiplying this to $(4.2t)$, we obtain

$$W(\varphi_{E/F})\, W(\mu_o) = \varphi_{E/F}^{-1}(c)\, \psi_E(c)\, \psi_E\!\left(c\,\delta^2\, \frac{\gamma^2}{2}\right)^{-1} \left(\frac{2\,\ell}{P_F}\right) \mu_o^{-1}(-c\,\delta^2) .$$

In case 2(b), the residue class field characteristic $p \neq 2$, but the degree $\ell = 2$. So

$$\left(\frac{2\,\ell}{P_F}\right) = \left(\frac{2^2}{P_F}\right) = 1 .$$

Moreover,

$$\mu_o^{-1}(\delta^2) = \mu_o^{-1}(\delta)^2 = 1$$

since $\delta \in F^\times$ and μ_o^{-1} has order $\ell = 2$. Consequently,

$$W(\varphi_{E/F})\; W(\mu_o) = \varphi_{E/F}^{-1}(c)\,\psi_E(c)\;\psi_E\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\;\mu_o^{-1}(-c)$$

$$= \left[\varphi^{-1}(c)\,\psi_F(c)\;\psi_F\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\right]^2\left(\frac{-1}{P_F}\right)\;\mu_o^{-1}(c) .$$

This last equality is true because of (4.2r) established in lemma 4.2.6.

By theorem A.3 part (a),

$$W(\varphi)^2 = \left[\varphi^{-1}(c)\,\psi_F(c)\;\psi_F\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\,\eta}{P_F}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}\right]^2$$

which simplifies to

$$\left[\varphi^{-1}(c)\,\psi_F(c)\;\psi_F\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\right]^2\left(\frac{-1}{P_F}\right) .$$

Therefore,

$$W(\varphi_{E/F})\; W(\mu_o) = W(\varphi)^2\;\mu_o^{-1}(c) .$$

Now, it follows from theorem A.1 part (c) that

$$W(\varphi_{E/F})\ W(\mu_o) \ = \ W(\varphi)^2\ \mu_o^{-1}(c) \ = \ \prod_{\mu \in S(E/F)} W(\varphi \cdot \mu)\ .$$

This is precisely $(4.2b)$, and case 2(b) is settled.

When E/F is a tamely ramified, case 2(a) and case 2(b) have completed the proof of the 1st identity for p odd.

Next, we are going to assume $p = 2$. Just like the case of odd residue class field characteristic, let $\delta = \pi_F^{d(\varphi)}$. Given c, η as in (i) and (ii), we claim (iv) and (v) still hold. Specifically, due to theorem A.2 part (d),

$$\varphi_{E/F}(1 + x) \ = \ \psi_E(c\,x) \qquad \text{for all } x \in P_E^{1 + d(\varphi_{E/F})}\ .$$

Besides, the argument we used to prove (v) remains valid for $p = 2$. So

$$\psi_E(c\,\delta^2\,x)^{-1} \ = \ (-1)^{\,Tr_{k_E/F_p}(\ell\,\eta\,x)} \tag{4.2v}$$

for all $x \in O_E$.

Now, suppose $\beta \in O_F$ satisfying $\beta^2 \equiv \eta^{-1} \mod P_F$. By theorem A.3 part (b), there exists $\gamma \in O_{F_o}$ such that

$$\varphi^{-1}(1 + \beta\,\delta\,x)\,\psi_F(c\,\beta\,\delta\,x) \ = \ \Delta_o'(x)\,(-1)^{Tr_{k_F/F_p}(\gamma\,x)} \qquad \text{for } x \in O_F$$

where

$$\Delta'_o = i^{\,Tr_{k_F/F_p}} \cdot (-1)^{Tr^{(2)}_{k_F/F_p}} .$$

Claim VI. *With the assumptions of case 2(c) and the above notations, if we define*

$$\gamma' = \gamma + \frac{\ell - 1}{2}$$

then for all $x \in O_E$,

$$\varphi^{-1}_{E/F}(1 + \beta\,\delta\,x)\,\psi_E(c\,\beta\,\delta\,x) = i^{\,Tr_{k_E/F_p}(x)}\ (-1)^{Tr^{(2)}_{k_E/F_p}(x)}\ (-1)^{Tr_{k_E/F_p}(\gamma' x)} .$$

Proof. Since $m(\varphi) = 1 + 2 \cdot d_{(\varphi)}$, we have

$$N_{E/F}(1 + \beta\,\delta\,x) \equiv (1 + \beta\,\delta\,Tr_{E/F}(x))\,(1 + \beta^2\,\delta^2\,Tr^{(2)}_{E/F}(x)) \quad mod\ P_F^{m(\varphi)}.$$

Hence $\varphi^{-1}_{E/F}(1 + \beta\,\delta\,x)\,\psi_E(c\,\beta\,\delta\,x)$ can be written

$$\varphi^{-1}(1 + \beta\,\delta\,Tr_{E/F}(x))\ \varphi^{-1}(1 + \beta^2\,\delta^2\,Tr^{(2)}_{E/F}(x))\ \psi_F(c\,\beta\,\delta\,Tr_{E/F}(x)) .$$

From the above definition of γ ,

$$\varphi^{-1}(1 + \beta\,\delta\,Tr_{E/F}(x))\ \psi_F(c\,\beta\,\delta\,Tr_{E/F}(x))$$

$$= \Delta_o'(\, Tr_{E/F}(x)\,)\ (-1)^{Tr_{k_F/F_p}(\,\gamma\, Tr_{E/F}(x)\,)}$$

while

$$\varphi^{-1}(\,1 + \beta^2\,\delta^2\, Tr^{(2)}_{E/F}(x)\,) \;=\; \psi_F(\,c\,\beta^2\,\delta^2\, Tr^{(2)}_{E/F}(x)\,)^{-1} \;=\; (-1)^{Tr_{k_F/F_p}(Tr^{(2)}_{E/F}(x))}$$

by (i) and (ii). In other words,

$$\varphi^{-1}_{E/F}(1 + \beta\,\delta\, x)\, \psi_E(c\,\beta\,\delta\, x) \;=\; \Delta_o'(\, Tr_{E/F}(x)\,)\,(-1)^{Tr_{k_F/F_p}(\gamma\, Tr_{E/F}(x) \,+\, Tr^{(2)}_{E/F}(x))} \qquad (4.2w).$$

Because the Galois extension E/F is totally ramified,

$$Tr_{E/F}(x) \;\equiv\; \ell\, x \quad mod\ P_E$$

and

$$Tr^{(2)}_{E/F}(x) \;\equiv\; \frac{\ell(\ell-1)}{2}\, x^2 \quad mod\ P_E\ .$$

Moreover, we have $k_E \;=\; k_F$. Consequently,

$$\Delta_o'(\, Tr_{E/F}(x)\,) \;=\; i^{\,Tr_{k_F/F_p}(\,Tr_{E/F}(x)\,)}\ (-1)^{Tr^{(2)}_{k_F/F_p}(\,Tr_{E/F}(x)\,)}$$

$$= \; i^{\,Tr_{k_E/F_p}(\ell\, x)}\ (-1)^{Tr^{(2)}_{k_E/F_p}(\ell\, x)}$$

and (4.2w) becomes

$$\varphi^{-1}_{E/F}(1 \,+\, \beta\,\delta\, x)\, \psi_E(c\,\beta\,\delta\, x)$$

$$= i^{\,Tr_{k_E/F_p}(\ell\, x)}\ (-1)^{Tr^{(2)}_{k_E/F_p}(\ell\, x)}\ (-1)^{Tr_{k_E/F_p}(\gamma\, \ell\, x\, +\, \frac{\ell(\ell-1)}{2}\, x^2)}$$

Now, observe that $\ell \neq 2$ means $\ell \equiv 1 \quad mod\ P_E$. So

$$\varphi^{-1}_{E/F}(1+\beta\,\delta\, x)\,\psi_E(c\,\beta\,\delta\, x) = i^{\,Tr_{k_E/F_p}(x)}\ (-1)^{Tr^{(2)}_{k_E/F_p}(x)}\ (-1)^{Tr_{k_E/F_p}(\gamma\, x\, +\, \frac{(\ell-1)}{2}\, x^2)}$$

This proves claim VI because

$$Tr_{k_E/F_p}(x) \;=\; Tr_{k_E/F_p}(x^2) \tag{4.2x}$$

when $p = 2$. ||

To prove (4.2b) for case 2(c), it is sufficient to obtain (4.2s) according to lemma 4.2.5. We apply theorem A.3 part (b) to $\varphi_{E/F}$. In view of the above claim, (4.2v) , theorem A.2 part (d) and

$$\beta^2 \;\equiv\; (\ell\,\eta)^{-1} \quad mod\ P_E \ ,$$

it follows that $W(\varphi_{E/F})$ is equal to

$$\varphi^{-1}_{E/F}(c)\ \psi_E(c)\ \ (-i)^{Tr_{k_E/F_p}(\gamma\, +\, \frac{\ell-1}{2})}\ (-1)^{Tr^{(2)}_{k_E/F_p}(\gamma\, +\, \frac{\ell-1}{2})}\ \Big(\frac{1\, +\, i}{\sqrt{2}}\Big)^{\mathrm{f}}\, (-1)^{\mathrm{f}-1}.$$

Here $\mathrm{f} = [k_F : F_p] = [k_E : F_p]$.

As $\gamma + \frac{\ell-1}{2} \in O_{F_o}$, we can make the identification below

$$(-i)^{Tr_{k_E/F_p}(\gamma\, +\, \frac{\ell-1}{2})}\ (-1)^{Tr^{(2)}_{k_E/F_p}(\gamma\, +\, \frac{\ell-1}{2})} \;=\; \Delta'_o\Big(\gamma\, +\, \frac{\ell-1}{2}\Big)^{-1} .$$

On the other hand, it is a property of the 2nd elementary symmetric function that

$$
\begin{aligned}
Tr^{(2)}_{k_F/F_p}\Big(\gamma + \frac{\ell-1}{2}\Big) \;=\;& Tr^{(2)}_{k_F/F_p}(\gamma) + Tr^{(2)}_{k_F/F_p}\Big(\frac{\ell-1}{2}\Big) \\
&+ Tr_{k_F/F_p}(\gamma)\; Tr_{k_F/F_p}\Big(\frac{\ell-1}{2}\Big) \\
&- Tr_{k_F/F_p}\Big(\frac{\gamma(\ell-1)}{2}\Big)
\end{aligned}
$$

which implies[1]

$$\Delta'_o\Big(\gamma + \frac{\ell-1}{2}\Big)^{-1} \;=\; \Delta'_o(\gamma)^{-1}\, \Delta'_o\Big(\frac{\ell-1}{2}\Big)^{-1} (-1)^{Tr_{k_F/F_p}\left(\frac{\gamma(\ell-1)}{2}\right)} .$$

Meanwhile, part (c) of theorem A.3 shows

$$\Delta'_o(\ell\,\gamma) \;=\; \Delta'_o(\gamma)^{\ell}\,(-1)^{Tr_{k_F/F_p}\left(\frac{\ell(\ell-1)}{2}\,\gamma^2\right)} .$$

However, prime ℓ is odd, and $\ell \equiv 1 \;\; mod \;\; P_F$. Together with $(4.2x)$, we have

$$\Delta'_o(\gamma) \;=\; \Delta'_o(\gamma)^{\ell}\,(-1)^{Tr_{k_F/F_p}\left(\frac{(\ell-1)}{2}\,\gamma\right)}$$

or equivalently

$$\Delta'_o(\gamma)^{-1}\,(-1)^{Tr_{k_F/F_p}\left(\frac{(\ell-1)}{2}\,\gamma\right)} \;=\; [\,\Delta'_o(\gamma)^{-1}\,]^{\ell} .$$

[1]See the footnote 1 in the appendix.

In summary,

$$W(\varphi_{E/F}) \;=\; \varphi_{E/F}^{-1}(c)\,\psi_E(c)\;[\,\Delta_o'(\gamma)^{-1}\,]^{\ell}\,\Delta_o'\Big(\frac{\ell-1}{2}\Big)^{-1}\Big(\frac{1+i}{\sqrt{2}}\Big)^{\mathrm{f}}(-1)^{\mathrm{f}-1}.$$

By theorem A.3 part (b),

$$W(\varphi)^{\ell} \;=\; \left(\varphi^{-1}(c)\,\psi_F(c)\;\Delta_o'(\gamma)^{-1}\,\Big(\frac{1+i}{\sqrt{2}}\Big)^{\mathrm{f}}(-1)^{\mathrm{f}\text{-}1}\right)^{\ell}$$

So, in order to obtain (4.2s), we must prove

$$\Delta_o'\Big(\frac{\ell-1}{2}\Big)^{-1}\Big(\frac{1+i}{\sqrt{2}}\Big)^{-\mathrm{f}\,(\ell-1)} \;=\; 1 \qquad (4.2y).$$

Recall

$$\Delta_o'\Big(\frac{\ell-1}{2}\Big) \;=\; i^{\,Tr_{k_F/F_p}(\frac{\ell-1}{2})}\;(-1)^{Tr^{(2)}_{k_F/F_p}(\frac{\ell-1}{2})}\,.$$

Claim VII. *For any odd prime ℓ, if we define a function Δ_o on the set of integers by*

$$\Delta_o(x) \;=\; \begin{cases} i & \text{when } x \text{ is odd} \\ 1 & \text{when } x \text{ is even} \end{cases}$$

then

$$\Delta_o'\Big(\frac{\ell-1}{2}\Big) \;=\; \Delta_o\Big(\frac{\ell-1}{2}\Big)^{\mathrm{f}}$$

where $\mathrm{f} = [k_F : F_p]$.

Proof. It can be shown that for all $n \geq 1$,

$$\Delta_o(nx) \;=\; \Delta_o(x)^n \;(-1)^{x^2 n(n-1)/2} \tag{4.2z}$$

by induction on n. In fact, we see from the definition of Δ_o that

$$\Delta_o((n+1)x) \;=\; \Delta_o(nx + x) \;=\; \Delta_o(nx)\; \Delta_o(x)\; (-1)^{nx^2}.$$

Hence the induction hypothesis yields

$$\Delta_o((n+1)x) \;=\; \Delta_o(x)^n \;(-1)^{x^2 n(n-1)/2}\; \Delta_o(x)\; (-1)^{nx^2}.$$

In other words

$$\Delta_o((n+1)x) \;=\; \Delta_o(x)^{n+1} \;(-1)^{x^2 n(n+1)/2}.$$

Now, because

$$Tr_{k_F/F_2}\Big(\frac{\ell-1}{2}\Big) \;\equiv\; \mathrm{f}\Big(\frac{\ell-1}{2}\Big) \quad mod\ 2$$

and

$$Tr^{(2)}_{k_F/F_2}\Big(\frac{\ell-1}{2}\Big) \;\equiv\; \frac{\mathrm{f}(\mathrm{f}-1)}{2}\;\Big(\frac{\ell-1}{2}\Big)^2 \quad mod\ 2$$

we conclude that

$$\Delta'_o\Big(\frac{\ell-1}{2}\Big) \;=\; \Delta_o\Big(Tr_{k_F/F_p}\Big(\frac{\ell-1}{2}\Big)\Big)\;\big(-1\big)^{Tr^{(2)}_{k_F/F_p}\left(\frac{\ell-1}{2}\right)}$$

$$= \Delta_o\Big(\mathrm{f}\,\big(\frac{\ell-1}{2}\big)\Big)\,\big(-1\big)^{\frac{\mathrm{f}(\mathrm{f}-1)}{2}\,\left(\frac{\ell-1}{2}\right)^2}$$

which is equal to $\Delta_o(\frac{\ell-1}{2})^{\mathrm{f}}$ by $(4.2z)$. ||

Due to claim VII,

$$\Delta_o'\Big(\frac{\ell-1}{2}\Big)^{-1}\Big(\frac{1+i}{\sqrt{2}}\Big)^{-\mathrm{f}\,(\ell-1)} = \Big[\Delta_o\Big(\frac{\ell-1}{2}\Big)\,i^{\frac{\ell-1}{2}}\Big]^{-\mathrm{f}}.$$

Observe that

$$\Delta_o\Big(\frac{\ell-1}{2}\Big)\,i^{\frac{\ell-1}{2}} = \begin{cases} 1 & \text{when } \ell \equiv \pm 1 \;\; mod\ 8 \\ -1 & \text{when } \ell \equiv \pm 3 \;\; mod\ 8 \end{cases}$$

which shares the same values with the Legendre symbol $(\frac{2}{\ell})$. As a result,

$$\Delta_o'\Big(\frac{\ell-1}{2}\Big)^{-1}\Big(\frac{1+i}{\sqrt{2}}\Big)^{-\mathrm{f}\,(\ell-1)} = \left(\frac{2}{\ell}\right)^{\mathrm{f}}$$

To obtain $(4.2y)$, we recall that F contains all the ℓ-th roots of unity since E/F is totally and tamely ramified Galois extension of degree ℓ. Therefore[2]

$$2^{\mathrm{f}} \equiv 1 \;\; mod\ \ell$$

and

$$\Delta_o'\Big(\frac{\ell-1}{2}\Big)^{-1}\Big(\frac{1+i}{\sqrt{2}}\Big)^{-\mathrm{f}\,(\ell-1)} = \left(\frac{2}{\ell}\right)^{\mathrm{f}} = \left(\frac{2^{\mathrm{f}}}{\ell}\right) = 1$$

[2]See [2, chapter 3, § 1, lemma 4, p.87].

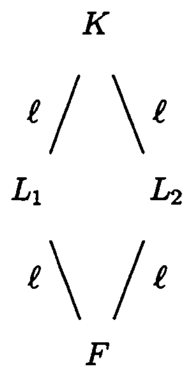
As noted before, this implies (4.2s). Via lemma 4.2.5, we can conclude that (4.2b) holds for case 2(c).

Case 1(a), (b) and case 2(a), (b), (c) have now been account for. We succeed in proving the 1st identity (4.2b) when the Galois extension E/F is totally and tamely ramified of prime degree. Therefore, the proof of theorem 4.2.3 is finally completed. ||

The argument presented in this section is due to Dwork. In his thesis [5], Dwork established the 1st identity not only for the tame case but also for the wild case. When E/F is no longer tame, the proof of (4.2b) is sensitive to the conductor of φ, the residue class field characteristic p, and the conductor of the abelian extension (relative to the size of $m(\varphi)$). See [5, chapter 3, p.75]). Lakkis [14] contains a sketch of the proof of the 1st identity, built upon earlier work by Hasse [10] and Lamprecht [15]. (see [14, Satz 1, pp.191 - 266]). However, to the best of my knowledge, not all the gaps in that proof are filled. Langlands intended to prove the 1st identity in chapter 10 of his Yale manuscript [16], which is missing in any existing version of the manuscript. Nonetheless, Langlands did set up carefully in chapter 8 and 9 of [16] the machinery necessary for the proof of this identity.

4.3 The second identity

Suppose $G = Gal(K/F)$ is the direct sum $Z_\ell \oplus Z_\ell$ of two cyclic groups of prime order ℓ. Let χ_K be a character of $K^\times$ such that $\chi_K \circ \sigma = \chi_K$ for any $\sigma \in G$ and $\chi_K \neq \chi_F \circ N_{K/F}$ for any character χ_F of $F^\times$. Given two distinct subfields L_1, L_2 of K/F, both of which have degree ℓ over F,



if χ_{L_1} and χ_{L_2} are characters of $L_1^\times$ and $L_2^\times$ respectively satisfying

$$\chi_{L_1} \circ N_{K/L_1} = \chi_K = \chi_{L_2} \circ N_{K/L_2}$$

then we prove in this section

$$W(\chi_{L_1}) \prod_{\mu \in S(L_1/F)} W(\mu) = W(\chi_{L_2}) \prod_{\mu' \in S(L_2/F)} W(\mu')$$

where $S(L_i/F)$ consists of characters of $F^\times$ annihilating $N_{L_i/F}(L_i^\times)$.

Additional notations: Just as in theorem 4.2.3, we will hereby use χ_{K/L_i} and $\chi_{L_i} \circ N_{K/L_i}$ interchangably. We continue to denote the conductor of a quasi-character χ by $m(\chi)$. In [16], $m(\chi_{L_i})$ is abbreviated to m_i, and we will do the same throughout this section. As for the ramification subgroups of G, we adhere to Serre's convention in [20].

Before the proof of the 2nd identity is discussed, let us make some general observations.

Lemma 4.3.0. *Let K/L be a Galois extension of prime degree ℓ, if χ_K is a quasi-character on K such that $\chi_K \circ \sigma = \chi_K$ for all $\sigma \in Gal(K/L)$, then there exists χ_L on $L^\times$ satisfying $\chi_K = \chi_L \circ N_{K/L}$. Furthermore, if χ_K is a character, so is χ_L.*

Proof. Because $\chi_K \circ \sigma = \chi_K$, it follows from Hilbert's theorem 90 that $\chi_K(a) = 1$ if $N_{K/L}(a) = 1$. So, it is possible to define χ_L on the norm group $N_{K/L}(K^\times)$ by

$$\chi_L(x) = \chi_K(y) \qquad \text{where } x = N_{K/L}(y).$$

Moreover, notice that $\chi_K = \chi_{K/L}$ holds automatically.

Since K/L is cyclic of prime degree, we have two possibilities (see [20, chapter V, §§ 2 – 3]):

(a) $U_L = N_{K/L}(U_K)$, and π_L modulo $N_{K/L}(K^\times)$ has order ℓ. i.e. K/L is unramified.

(b) $[U_L : N_{K/L}(U_K)] = \ell$, and $N_{K/L}(\pi_K)$ is a uniformizing parameter of L. i.e. K/L is totally ramified.

To define a quasi-character χ_L on all of $L^\times$, it is enough to specify $\chi_L|_{U_L}$ as well as $\chi_L(\pi_L)$ (see [22, Theorem 2.3.1]). In (a) , we can do so because $\chi_L({\pi_L}^\ell)$ has an ℓ-th root. If (b) is true, observe that $U_L^n \subseteq N_{K/L}(U_K)$ and $\chi_L(U_L^n) = 1$ for sufficiently large n. Consequently χ_L can be extended from $N_{K/L}(U_K)/U_L^n$ to U_L/U_L^n. The last assertion is immediate from the construction. ||

Lemma 4.3.1. *With the notations in the 2nd identity and the premises leading to it, let us define for each* $\sigma \in Gal(L_i/F)$ *the following characters of* $L_i^\times$ *.*

$$\chi_{L_i}^{\sigma} = \chi_{L_i} \circ \sigma$$

and

$$\chi_{L_i}^{\sigma - 1} = (\chi_{L_i}^{\sigma}) \cdot \chi_{L_i}^{-1} .$$

Then we have $\chi_{L_i}^{\sigma - 1} \in S(K/L_i)$ *. In fact, all the characters in* $S(K/L_i)$ *take the form* $\chi_{L_i}^{\sigma - 1}$*.*

Proof. Extend σ to an automorphism of K which is again denoted by σ. Because $Gal(K/F)$ is assumed abelian,

$$\chi_{L_i}^{\sigma} \circ N_{K/L_i} = (\chi_{L_i} \circ N_{K/L_i}) \circ \sigma = \chi_K \circ \sigma = \chi_K = \chi_{L_i} \circ N_{K/L_i} .$$

Hence $\chi_{L_i}^{\sigma - 1}$ is trivial on $N_{K/L_i}(K^\times)$.

Given $\sigma \neq 1$, it generates the cyclic group $Gal(L_i/F)$. Therefore $\chi_{L_i}^{\sigma - 1} \neq 1$; otherwise $\chi_{L_i}^{\sigma^k} = \chi_{L_i}$ for any integer k, and lemma 4.3.0 implies $\chi_{L_i} = \chi_F \circ N_{L_i/F}$ for some character χ_F of $F^\times$. This contradicts the premise $\chi_K \neq \chi_F \circ N_{K/F}$. Now, we observe that

$$\chi_{L_i}^{\sigma^k - 1} = \chi_{L_i}^{\sigma^m - 1} \quad \Longrightarrow \quad \chi_{L_i}^{\sigma^k} = \chi_{L_i}^{\sigma^m}$$

$$\Longrightarrow \quad \chi_{L_i}^{\sigma^{(k-m)}} = \chi_{L_i}$$

which means $\sigma^{(k-m)} = 1$. In other words, 1 , $\chi_{L_i}^{\sigma - 1}$, $\ldots$, $\chi_{L_i}^{\sigma^{(\ell-1)} - 1}$ are distinct characters. Lemma 4.3.1 is proved. ||

Because $\sigma(U_{L_i}^n) = U_{L_i}^n$ for $\sigma \in Gal(L_i/F)$, we see $m(\chi_{L_i}) = m(\chi_{L_i}^{\sigma})$. So it is a corollary of lemma 4.3.1 that

$$\nu \in S(K/L_i) \implies m_i \geq m(\nu) \qquad (4.3a).$$

Lemma 4.3.2. *The $Z_\ell \oplus Z_\ell$ extension allows three possible ramification group filtrations:*

(i) $G \neq G_0 = \ldots = G_u \neq G_{u+1} = \{1\}$

(ii) $G = G_0 = G_1 = \ldots = G_w \neq G_{w+1} = \ldots = G_u \neq G_{u+1} = \{1\}$

(iii) $G = G_0 = G_1 = \ldots = G_u \neq G_{u+1} = \{1\}$

Proof. Recall that G/G_0 is always cyclic, while G_0/G_1 is cyclic of degree prime to the residue class field characteristic p. Moreover, for $n \geq 1$, G_n is a p-group (see [20, chapter IV, § 2, p.67]). ||

Now, we assume that the $Z_\ell \oplus Z_\ell$ extension K/F is tamely ramified. In this case the ramification group filtration of $G = Gal(K/F)$ is known.

$$\begin{array}{rcl} G & = & Z_\ell \times Z_\ell \\ & & \cup \\ G_0 & = & Z_\ell \\ & & \cup \\ G_1 & = & \{1\} \end{array}$$

Compare this filtration with (i) in lemma 4.3.2. We see that the jump u equals zero.

Suppose E is the fixed field of the inertia group G_0. According to lemma 4.3.0 there exists character χ_E such that $\chi_E \circ N_{K/E} = \chi_K$. If we can show

$$W(\chi_E) \prod_{\mu \in S(E/F)} W(\mu) = W(\chi_{L_i}) \prod_{\mu' \in S(L_i/F)} W(\mu')$$

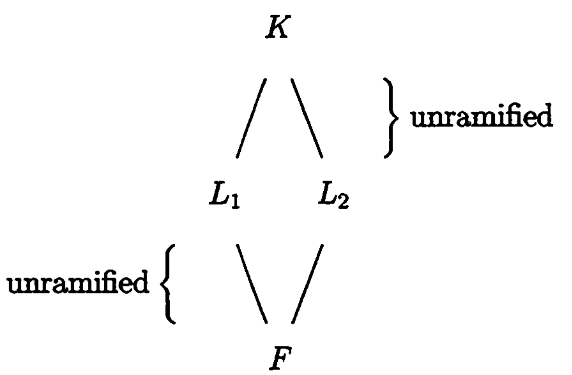
then the 2nd identity in the tame case follows. Thus, it remains to prove

Theorem 4.3.3. *In addition to the premises leading to the 2nd identity, suppose K/F is tamely ramified and the subfield L_1 coincides with the fixed field of the inertia group G_0, then*

$$W(\chi_{L_1}) \cdot \tau(\pi_F^d)^{\frac{\ell(\ell-1)}{2}} = W(\chi_{L_2}) \prod_{\mu \in S(L_2/F)} W(\mu) \qquad (4.3b)$$

where τ is any non-trivial character in $S(L_1/F)$.

Proof. First we collect some facts about the two conductors m_1 and m_2. As we assume L_1, L_2 are distinct, L_2/F must be totally ramified. This means K/L_2 is unramified.



(4.3c).

So $N_{K/L_2}(U_K^n) = U_{L_2}^n$ for all $n \geq 0$, and

$$m(\chi_K) = m(\chi_{L_2} \circ N_{K/L_2}) = m_2 \qquad (4.3d).$$

Since K/F is tame, so is the totally ramified extension K/L_1. Consequently, $N_{K/L_1}(U_K^1) = U_{L_1}^1$. The fact that K/L_1 is also cyclic of prime degree further asserts that

$$N_{K/L_1}(U_K^{\psi(n)}) = U_{L_1}^n \qquad \text{for all } n > 0.$$

and

$$N_{K/L_1}(U_K^{\psi(n)+1}) = U_{L_1}^{n+1} \qquad \text{for all } n \geq 0.$$

(see Serre [20] chapter V, § 3, corollary 3 p.85). Here the function ψ is given by

$$\psi(x) = \begin{cases} x & \text{for } -1 < x < 0. \\ \ell \cdot x & \text{for } x \geq 0. \end{cases}$$

For future reference, we will sometimes distinguish the above functon by writing ψ as Ψ_{K/L_1}. In contrast, Ψ_{K/L_2} is just the identity function.

Claim I. $m_1 > 1$ *implies* $m(\chi_K) = \psi(m_1 - 1) + 1$.

Proof. Because $m_1 - 1 > 0$,

$$\chi_{L_1}(N_{K/L_1}(U_K^{\psi(m_1-1)})) = \chi_{L_1}(U_{L_1}^{(m_1-1)}) \neq \{1\}.$$

On the other hand,

$$\chi_{L_1}(\, N_{K/L_1}(U_K^{\psi(m_1-1)\,+\,1})\,) \;=\; \chi_{L_1}(U_{L_1}^{(m_1-1)+1}) \;=\; \chi_{L_1}(U_{L_1}^{m_1}) \;=\; \{1\}\ .$$

Now recall that $\chi_K \;=\; \chi_{L_1} \circ N_{K/L_1}$. So $\psi(m_1-1)\,+\,1$ must be the conductor for χ_K . ||

With the notation Ψ_{K/L_i} introduced earlier, the above claim and $(4.3d)$ yield

Claim II. *If* $m_1 \;>\; 1$, *then*

$$m(\chi_K) \;=\; \Psi_{K/L_i}(m_i - 1) \,+\, 1 \qquad i \,=\, 1\,,\,2\ .$$

In other words, $m_2 \;=\; \ell\cdot(m_1-1)\,+\,1$, *which implies* $m_2 \,>\, m_1$.

Before we state the next claim, let us point out that $m_1 \;\geq\; 1$ when the Galois extension K/L_1 is totally and tamely ramified. In fact, because $[U_{L_1} : N_{K/L_1}(U_K)] \;=\; \ell$ and $N_{K/L_1}(\pi_K)$ is a uniformizing parameter of L_1 , the observation that $N_{K/L_1}(U_K^1) \;=\; U_{L_1}^1$ means all the non-trivial characters in $S(K/L_1)$ are tame. By $(4.3a)$, we have $m_1 \;\geq\; 1$.

Claim III. *For $\ell \neq 2$, we have $m_1 \equiv m_2 \mod 2$. i.e. m_1 and m_2 are either both odd or both even.*

Proof. Because of the formula $m_2 = \ell \cdot (m_1 - 1) + 1$ in Claim II, we obtain $m_1 \equiv m_2 \mod 2$ when ℓ is odd and $m_1 > 1$. In the case $m_1 = 1$, claim III follows from

Claim IV. *Regardless of the parity of ℓ, if $m_1 = 1$, then $m(\chi_K) = m_2 = 1$.*

Proof. As K/L_1 is tamely ramified, $N_{K/L_1}(U_K^1) = U_{L_1}^1$. So $m_1 = 1$ implies $m(\chi_K)$ is less than or equal to 1. However, $m(\chi_K) \neq 0$; otherwise there exists a character χ_F of $F^\times$ with $\chi_{L_2} = \chi_{L_2/F}$. This is a contradiction since $\chi_K \neq \chi_{K/F}$. In fact, if we define χ_F such that $\chi_F(N_{L_2/F}(\pi_{L_2})) = \chi_{L_2}(\pi_{L_2})$ and $\chi_F(u) = 1$ for all $u \in U_F$, then

$$\begin{aligned} m(\chi_K) = 0 \quad &\Longrightarrow \quad m_2 = 0 \\ &\Longrightarrow \quad \chi_{L_2/F} = \chi_{L_2} \\ &\Longrightarrow \quad \chi_{K/F} = \chi_K \end{aligned}$$

which cannot happen. ||

Now, for odd ℓ, $m_1 \equiv m_2 \mod 2$ is true for all possible values of m_1 as $m_1 \geq 1$ by (4.3a). We have completed the proof of claim III. $\|$

We are going to split the proof of theorem 4.3.3 into two parts. First, we verify (4.3b) by assuming $m_1 = 1$. Afterwards we handle the case $m_1 > 1$.

Theorem 4.3.4. *Suppose the Galois extension K/F is tamely ramified and subfield L_1 is unramified over F. If χ_{L_1} is tame i.e. $m_1 = 1$, then the 2nd identity* (4.3b) *holds.*

Proof. Consider the isomorphism

$$U_{L_2}/U_{L_2}^1 \simeq (U_{L_2} \cdot U_K^1)/U_K^1$$

induced by the inclusion map $U_{L_2} \hookrightarrow U_{L_2} \cdot U_K^1 \subseteq U_K$. Recall from claim IV that $m_1 = 1$ implies $m(\chi_K) = m_2 = 1$. Via the above isomorphism, it is possible to identify the restriction $\chi_{L_2}|_{U_{L_2}}$ as a character of $(U_{L_2} \cdot U_K^1)/U_K^1$, which can be extended to a character of U_K/U_K^1, again denoted by χ_{L_2}.

Similarly, we will abuse the notation χ_K, giving it dual meaning as a tame character of $K^\times$ and the corresponding character of U_K/U_K^1.

Let $q = p^{\mathrm{f}}$ be the cardinality of the residue class field k_F. Then $U_K/U_K^1 \simeq k_K^\times$ is cyclic of order $q^\ell - 1$. Given a character χ of U_K/U_K^1 with order $q^\ell - 1$, there is a unique nonnegative integer α less than $q^\ell - 1$ such that

$$\chi_{L_2}{}^{-1} = \chi^\alpha \qquad (4.3e).$$

Claim V. *The integer* α *defined by* (4.3e) *is relatively prime to* ℓ.

Proof. Suppose $\alpha = \ell s$ for some integer s. Let $proj : U_K \to U_K/U_K^1$ be the canonical projection. Because L_2/F is totally ramified, $N_{L_2/F}(\pi_{L_2})$ is a uniformizing parameter of F, and it is possible to define a character χ_F of $F^\times$ such that $\chi_F(N_{L_2/F}(\pi_{L_2})) = \chi_{L_2}(\pi_{L_2})$ and

$$\chi_F = \chi^s \circ proj \qquad \text{on } U_F.$$

With the observation

$$N_{L_2/F}(u) \equiv u^\ell \quad mod\ P_K \qquad \text{for } u \in U_{L_2},$$

it is immediate to check that $\chi_{L_2} = \chi_F \circ N_{L_2/F}$, which contradicts the assumption $\chi_K \neq \chi_{K/F}$. As a result, α cannot be divisible by the prime degree ℓ. This proves claim V. ||

Meanwhile, K/L_2 is unramified according to diagram (4.3c). Therefore

$$\chi_K^{-1} = \chi^{\alpha\,(1+q+\dots+q^{\ell-1})} \qquad \text{on } U_K/U_K^1 .$$

On the other hand, $U_{L_1}/U_{L_1}^1 \simeq U_K/U_K^1$. So the restriction $\chi_{L_1}|_{U_{L_1}}$ can be regarded as a character of U_K/U_K^1 via the isomorphism. Let χ_{L_1} stand for this character of U_K/U_K^1 as well. Then

$$\chi_{L_1}^{\ell} = \chi_K \qquad \text{on } U_K/U_K^1 .$$

Now, recall that F contains all the ℓ-th roots of unity because L_2/F is a totally and tamely ramified Galois extension of degree ℓ. This implies $\ell \mid (q-1)$ or equivalently

$$q \equiv 1 \;\; mod\,\ell \qquad (4.3f).$$

See [2, chapter3, § 1, lemma 4, p.87].

Hence, we have $1 + q + \dots + q^{\ell-1} \equiv 0 \;\; mod\,\ell$. Let

$$\beta = \frac{1 + q + \dots + q^{\ell-1}}{\ell} .$$

and notice

$$\chi_{L_1}^{-\ell} = \chi_K^{-1} = \chi^{\alpha\,\beta\,\ell} .$$

Evidently, the order of $\chi_{L_1} \cdot \chi^{\alpha\,\beta}$ divides ℓ. Since the order of $\chi^{(q-1)\,\beta}$ is exactly ℓ, we conclude

$$\chi_{L_1} \cdot \chi^{\alpha\,\beta} = (\,\chi^{(q-1)\,\beta}\,)^i \qquad \text{on } U_K/U_K^1 .$$

for some i. In other words,

$$\chi^{(\alpha\,-\,(q-1)\,i)\,\beta} = \chi_{L_1}^{-1} \tag{4.3g}$$

Observe that the integer $\alpha - (q-1)\,i$ in the exponent of χ must be relatively prime to ℓ. This is because

$$\alpha - (q-1)\,i \equiv \alpha \not\equiv 0 \;\; mod\,\ell$$

by $(4.3f)$ and claim V.

So, the following Gauss sum identity holds (see Evans [7, identity (3), p.198]).

$$1 = \frac{G_{\mathfrak{f}}\,(\,\chi^{\,\alpha\,-\,(q-1)\,i}\,)}{\chi^{\,\alpha\,-\,(q-1)\,i}\,(\ell)\,\cdot\,G_{\mathfrak{f}\ell}\;(\,\chi^{\,(\alpha\,-\,(q-1)\,i)\,\beta}\,)}\,\prod_{j=1}^{\ell-1} G_{\mathfrak{f}}\,(\,\chi^{\,j\,(q-1)\,/\,\ell}\,)\;.$$

Here $G_{\mathfrak{f}}(\chi^{\alpha - (q-1)i})$ is a sum over $k_F = k_{L_2}$ and $G_{\mathfrak{f}\ell}(\chi^{(\alpha - (q-1)i)\beta})$ is a sum over k_K. They are consistent with the ordinary Gauss sum notation in theorem 4.1.1.

Restricted to $k_{L_2}^{\times} \simeq (U_{L_2} \cdot U_K^1)/U_K^1$, the character χ has order $q-1$. Therefore,

$$G_{\mathfrak{f}}(\chi^{\alpha - (q-1)i}) = G_{\mathfrak{f}}(\chi^{\alpha}) .$$

Similarly,

$$\chi^{\alpha - (q-1)i}(\ell) = \chi^{\alpha}(\ell)$$

Thus we have

$$1 = \frac{G_{\mathfrak{f}}(\chi^{\alpha})}{\chi^{\alpha}(\ell) \cdot G_{\mathfrak{f}\ell}(\chi^{(\alpha - (q-1)i)\beta})} \prod_{j=1}^{\ell-1} G_{\mathfrak{f}}(\chi^{j(q-1)/\ell})$$

or equivalently

$$\chi^{\alpha}(\ell) \cdot G_{\mathfrak{f}\ell}(\chi^{(\alpha - (q-1)i)\beta}) = G_{\mathfrak{f}}(\chi^{\alpha}) \prod_{j=1}^{\ell-1} G_{\mathfrak{f}}(\chi^{j(q-1)/\ell}) .$$

Before converting this into a root number identity, we note that the restriction of every non-trivial $\mu \in S(L_2/F)$ to U_F corresponds to a character of the form $\chi^{j(q-1)/\ell}$ on $U_F/U_F^1 \simeq (U_{L_2} \cdot U_K^1)/U_K^1$, for some positive j less than or equal to $\ell - 1$.

Now, in view of (4.3e) and (4.3g), theorem 4.1.1 translates the above Gauss identity into

$$\chi_{L_2}^{-1}(\ell) \cdot \frac{N(P_{L_1})^{1/2}\; W(\chi_{L_1})}{-\;\chi_{L_1}(t_1\,\pi_F^{d+1})}$$
$$= \frac{N(P_{L_2})^{1/2}\; W(\chi_{L_2})}{-\;\chi_{L_2}\left(t_2\,\pi_{L_2}^{\ell d\,+\,(\ell-1)\,+\,1}\right)} \prod_{\substack{\mu\,\in\,S(L_2/F)\\ \mu\,\neq\,1}} \frac{N(P_F)^{1/2}\; W(\mu)}{-\;\mu(t\,\pi_F^{d+1})}$$

where

$$t = Tr_{F/F_o}\left(p/\pi_F^{d+1}\right)$$
$$t_1 = Tr_{L_1/(L_1)_o}\left(p/\pi_F^{d+1}\right)$$
$$t_2 = Tr_{L_2/(L_2)_o}\left(p/\pi_{L_2}^{\ell d\,+\,(\ell-1)\,+\,1}\right)$$

and $\ell d + (\ell - 1)$ is the order of the absolute different of L_2.

Since $N(P_{L_1})$ is the cardinality of the residue class field k_{L_1},

$$N(P_{L_1}) = p^{\mathrm{f}\,\ell} = p^{\mathrm{f}} \cdot (p^{\mathrm{f}})^{\ell-1} = N(P_{L_2}) \prod_{\substack{\mu\,\in\,S(L_2/F)\\ \mu\,\neq\,1}} N(P_F)\,.$$

Together with the fact that $W(1) = 1$, we have

$$\frac{\chi_{L_2}^{-1}(\ell) \cdot W(\chi_{L_1})}{-\;\chi_{L_1}(t_1\,\pi_F^{d+1})} = \frac{W(\chi_{L_2})}{-\;\chi_{L_2}\left(t_2\,\pi_{L_2}^{\ell d\,+\,(\ell-1)\,+\,1}\right)} \prod_{\mu\,\in\,S(L_2/F)} \frac{W(\mu)}{(-1)^{\ell-1}\,\mu(t\,\pi_F^{d+1})}$$

(4.3h).

We will obtain (4.3b) from (4.3h) first for odd ℓ and then for $\ell = 2$.

Case 1 : *ℓ is odd.*

Notice that a fixed non-trivial $\mu_o \in S(L_2/F)$ has order ℓ. Hence the product

$$\prod_{\mu \in S(L_2/F)} \mu(t\,\pi_F^{d+1})$$

is equal to

$$\prod_{j=0}^{\ell-1} \mu_o^j(t\,\pi_F^{d+1}) = \mu_o(t\,\pi_F^{d+1})^{\frac{\ell(\ell-1)}{2}} = (\,\mu_o(t\,\pi_F^{d+1})^{\ell}\,)^{\frac{\ell-1}{2}} = 1$$

and $(4.3h)$ is reduced to

$$\frac{\chi_{L_2}^{-1}(\ell)\cdot W(\chi_{L_1})}{-\,\chi_{L_1}(t_1\,\pi_F^{d+1})} = \frac{W(\chi_{L_2})}{-\,\chi_{L_2}(t_2\,\pi_{L_2}^{\ell d+(\ell-1)+1})} \prod_{\mu \in S(L_2/F)} W(\mu)\;.$$

In order to establish $(4.3b)$ from above, it is sufficient to prove

$$\frac{\chi_{L_2}^{-1}(\ell)\cdot \chi_{L_2}(t_2\,\pi_{L_2}^{\ell d+(\ell-1)+1})}{\chi_{L_1}(t_1\,\pi_F^{d+1})} = \frac{\chi_{L_2}^{-1}(\ell)\cdot \chi_{L_2}(t_2\,\pi_{L_2}^{\ell(d+1)})}{\chi_{L_1}(t_1\,\pi_F^{d+1})} = 1$$

because for odd ℓ

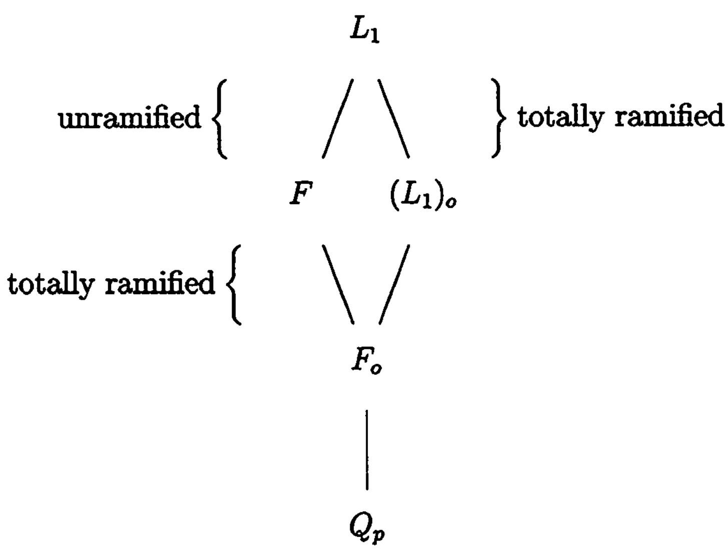
$$\tau(\pi_F^d)^{\frac{\ell(\ell-1)}{2}} = (\,\tau(\pi_F^d)^{\ell}\,)^{\frac{(\ell-1)}{2}} = (1)^{\frac{(\ell-1)}{2}} = 1\;.$$

(Recall τ is a non-trivial character in $S(L_1/F)$.)

Lemma. *If the prime degree ℓ is odd and the uniformizing parameters π_F and π_{L_2} are chosen such that $\pi_F = N_{L_2/F}(\pi_{L_2}) = (-1)^{\ell+1}\,\pi_{L_2}^{\ell}$, then*

$$\frac{\chi_{L_2}^{-1}(\ell)\cdot \chi_{L_2}(t_2\,\pi_{L_2}^{\ell(d+1)})}{\chi_{L_1}(t_1\,\pi_F^{d+1})} = 1\;.$$

Proof. Recall $t_1 = Tr_{L_1/(L_1)_o}\left(p/\pi_F^{d+1}\right)$. By definition, $(L_1)_o$ is the maximal subfield of L_1 that is unramified over Q_p. Therefore it must contain F_o.



(4.3i).

If f_{L_1/Q_p} is the residue class field degree $[k_{L_1} : F_p]$, then according to the above diagram

$$[F_o : Q_p]\,[L_1 : F] = \mathrm{f}_{L_1/Q_p} = [(L_1)_o : Q_p] = [F_o : Q_p]\,[(L_1)_o : F_o]\ .$$

So $[L_1 : F] = [(L_1)_o : F_o]$. It follows that $[F : F_o] = [L_1 : (L_1)_o]$.

Moreover,

$$F \cap (L_1)_o \; = \; F_o$$

and

$$F \cdot (L_1)_o \; = \; L_1 \; .$$

Consequently,

$$t_1 \; = \; Tr_{L_1/(L_1)_o}\left(\frac{p}{\pi_F^{d+1}}\right) \; = \; Tr_{F/F_o}\left(\frac{p}{\pi_F^{d+1}}\right) \; = \; t \; .$$

On the other hand, as indicated in diagram (4.3c), L_2/F is totally ramified and therefore so is L_2/F_o. In other words, $(L_2)_o \; = \; F_o$. With our choice of uniformizing parameters, this means

$$t_2 \; = \; Tr_{L_2/(L_2)_o}\left(\frac{p}{\pi_{L_2}^{\ell(d+1)}}\right) \; = \; Tr_{L_2/F_o}\left(\frac{p}{\pi_F^{d+1}}\right) \; = \; Tr_{F/F_o}\left(\frac{p\ell}{\pi_F^{d+1}}\right) \; = \; \ell\, t \; .$$

Now,

$$\frac{\chi_{L_2}^{-1}(\ell) \, \cdot \, \chi_{L_2}(t_2\, \pi_{L_2}^{\ell(d+1)})}{\chi_{L_1}(t_1\, \pi_F^{d+1})} \; = \; \frac{\chi_{L_2}^{-1}(\ell) \, \cdot \, \chi_{L_2}(\ell\, t\, \pi_F^{d+1})}{\chi_{L_1}(t\, \pi_F^{d+1})} \; = \; \frac{\chi_{L_2}(t\, \pi_F^{d+1})}{\chi_{L_1}(t\, \pi_F^{d+1})} \tag{4.3j}$$

As a result, Claim VI below completes the proof of our lemma.

Claim VI. *When ℓ is odd, we have* $\chi_{L_1} \; = \; \chi_{L_2}$ *on* $F^\times$.

Proof. Because $L_1 \neq L_2$, the norm groups $N_{L_1/F}(L_1^\times)$ and $N_{L_2/F}(L_2^\times)$ are distinct. So $\ell = [F^\times : N_{L_1/F}(L_1^\times)] = [F^\times : N_{L_2/F}(L_2^\times)]$ implies

$$F^\times = (N_{L_1/F}(L_1^\times))(N_{L_2/F}(L_2^\times)) .$$

Given $x \in F^\times$, there exist $\delta_1 \in L_1^\times$ and $\delta_2 \in L_2^\times$ such that $x = (N_{L_1/F}\,\delta_1)(N_{L_2/F}\,\delta_2)$. Observe

$$\chi_K(\delta_1) = \chi_{L_2}(N_{K/L_2}\,\delta_1) = \chi_{L_2}(N_{L_1/F}\,\delta_1)$$

At the same time

$$\chi_K(\delta_1) = \chi_{L_1}(N_{K/L_1}\,\delta_1) = \chi_{L_1}(\delta_1^\ell)$$

By lemma 4.3.1,

$$\chi_{L_1}(\delta_1^\ell) = \frac{\chi_{L_1}(N_{L_1/F}\,\delta_1)}{\prod_{\sigma \in Gal(L_1/F)} \chi_{L_1}^{\sigma - 1}(\delta_1)} = \frac{\chi_{L_1}(N_{L_1/F}\,\delta_1)}{\prod_{\nu \in S(K/L_1)} \nu(\delta_1)}$$

which is equal to $\chi_{L_1}(N_{L_1/F}\,\delta_1)$ because $\prod_{\nu \in S(K/L_1)} \nu(\delta_1) = 1$ when ℓ is odd.

In summary, we have $\chi_{L_2}(N_{L_1/F}\,\delta_1) = \chi_K(\delta_1) = \chi_{L_1}(N_{L_1/F}\,\delta_1)$.

Similarly, lemma 4.3.1 yields

$$\chi_{L_2}(\delta_2^\ell) = \chi_{L_2}(N_{L_2/F}\,\delta_2)$$

for odd ℓ. So

$$\begin{aligned} \chi_{L_1}(x) &= \chi_{L_1}(N_{L_1/F}\,\delta_1)\cdot\chi_{L_1}(N_{L_2/F}\,\delta_2) \\ &= \chi_{L_2}(N_{L_1/F}\,\delta_1)\cdot\chi_{L_1}(N_{K/L_1}\,\delta_2) \\ &= \chi_{L_2}(N_{L_1/F}\,\delta_1)\cdot\chi_{K}(\delta_2) \\ &= \chi_{L_2}(N_{L_1/F}\,\delta_1)\cdot\chi_{L_2}(N_{K/L_2}\,\delta_2) \\ &= \chi_{L_2}(N_{L_1/F}\,\delta_1)\cdot\chi_{L_2}(\delta_2^{\ell}) \\ &= \chi_{L_2}(N_{L_1/F}\,\delta_1)\cdot\chi_{L_2}(N_{L_2/F}\,\delta_2) \end{aligned}$$

and we have shown that $\chi_{L_1}(x) = \chi_{L_2}(x)$. Claim VI is proved. ||

Since $t = Tr_{F/F_o}\big(p/\pi_F^{d+1}\big)$ is a unit in O_{F_o} according to theorem 4.1.1, $t\,\pi_F^{d+1}$ indeed belongs to $F^{\times}$, and our lemma follows from (4.3j) together with claim VI. ||

This completes case 1, and we now proceed to deduce (4.3b) from (4.3h) for $\ell = 2$.

Case 2 : $\ell = 2$.

As K/F is tame, the residue class field characteristic $p \neq 2$. If μ is the non-trivial character in $S(L_2/F)$, then (4.3h) becomes

$$\frac{\chi_{L_2}^{-1}(2) \cdot W(\chi_{L_1})}{-\chi_{L_1}(t_1\,\pi_F^{d+1})} = \frac{W(\chi_{L_2}) \cdot W(\mu)}{\chi_{L_2}(t_2\,\pi_{L_2}^{2(d+1)}) \cdot \mu(t\,\pi_F^{d+1})} .$$

Combined with the following lemma, the above equality yields (4.3b).

Lemma. *Let the prime degree* $\ell = 2$. *If the uniformizing parameters* π_F *and* π_{L_2} *are chosen such that* $\pi_F = N_{L_2/F}(\pi_{L_2}) = (-1)^{2+1}\,\pi_{L_2}^2$ *, then*

$$\frac{\chi_{L_2}^{-1}(2) \cdot \chi_{L_2}(t_2\,\pi_{L_2}^{2(d+1)}) \cdot \mu(t\,\pi_F^{d+1})}{-\chi_{L_1}(t_1\,\pi_F^{d+1})} = \tau(\pi_F^d)$$

where τ *is the non-trivial character in* $S(L_1/F)$.

Proof. Just as in case 1, diagram (4.3i) shows that $[F : F_o] = [L_1 : (L_1)_o]$. Moreover, we have $F \cap (L_1)_o = F_o$ and $F \cdot (L_1)_o = L_1$. Therefore

$$t_1 = Tr_{L_1/(L_1)_o}\left(\frac{p}{\pi_F^{d+1}}\right) = Tr_{F/F_o}\left(\frac{p}{\pi_F^{d+1}}\right) = t .$$

On the other hand, because of our choice of uniformizing parameters, t_2 is equal to

$$Tr_{L_2/(L_2)_\circ}\left(\frac{p}{(-\,\pi_F)^{\,d+1}}\right) \;=\; Tr_{L_2/F_\circ}\left(\frac{p}{(-\,\pi_F)^{\,d+1}}\right) \;=\; Tr_{F/F_\circ}\left(\frac{2p}{(-\,\pi_F)^{\,d+1}}\right) .$$

In fact

$$t_2 \;=\; 2\,(-1)^{\,d+1}\,t \;.$$

Consequently

$$\frac{\chi_{L_2}^{-1}(2)\;\cdot\;\chi_{L_2}(t_2\,\pi_{L_2}^{\,2(d+1)})\;\cdot\;\mu(t\,\pi_F^{\,d+1})}{-\;\chi_{L_1}(t_1\,\pi_F^{\,d+1})}$$

can be written

$$\frac{\chi_{L_2}^{-1}(2)\;\cdot\;\chi_{L_2}(2\,(-1)^{\,d+1}\,t\,(-\,\pi_F)^{\,d+1})\;\cdot\;\mu(t\,\pi_F^{\,d+1})}{-\;\chi_{L_1}(t\,\pi_F^{\,d+1})} .$$

Hence,

$$\frac{\chi_{L_2}^{-1}(2)\;\cdot\;\chi_{L_2}(t_2\,\pi_{L_2}^{\,2(d+1)})\;\cdot\;\mu(t\,\pi_F^{\,d+1})}{-\;\chi_{L_1}(t_1\,\pi_F^{\,d+1})} \;=\; \frac{\chi_{L_2}(t\,\pi_F^{\,d+1})\;\cdot\;\mu(t\,\pi_F^{\,d+1})}{-\;\chi_{L_1}(t\,\pi_F^{\,d+1})}$$

(4.3k).

Claim VII. *For* $\ell \;=\; 2$, *we have*

$$\tau(x)\;\cdot\;\chi_{L_1}(x) \;=\; \mu(x)\;\cdot\;\chi_{L_2}(x) \qquad \textit{on } F^\times$$

where $\tau \in S(L_1/F)$ *and* $\mu \in S(L_2/F)$ *are both non-trivial.*

Proof. First, let us point out

$$\tau_{L_2/F} \;=\; \tau \circ N_{L_2/F} \quad \in \; S(K/L_2)$$

and

$$\mu_{L_1/F} \;=\; \mu \circ N_{L_1/F} \quad \in \; S(K/L_1)\ .$$

These are non-trivial characters because τ , μ are non-trivial on

$$F^\times \;=\; (\, N_{L_1/F}(L_1^\times)\,)(\, N_{L_2/F}(L_2^\times)\,)\ .$$

Given $x \in F^\times$, let $x = (N_{L_1/F}\,\delta_1)(N_{L_2/F}\,\delta_2)$. We observe

$$\chi_K(\delta_1) \;=\; \chi_{L_2}(N_{K/L_2}\,\delta_1) \;=\; \chi_{L_2}(N_{L_1/F}\,\delta_1)\ .$$

Also

$$\chi_K(\delta_1) \;=\; \chi_{L_1}(N_{K/L_1}\,\delta_1) \;=\; \chi_{L_1}(\delta_1{}^2) \;=\; \frac{\chi_{L_1}(N_{L_1/F}\,\delta_1)}{\chi_{L_1}^{\sigma\,-\,1}(N_{L_1/F}\,\delta_1)}$$

where σ is the non-trivial element in $Gal(L_1/F)$.

Thus

$$\chi_{L_2}(N_{L_1/F}\,\delta_1) \;=\; \frac{\chi_{L_1}(N_{L_1/F}\,\delta_1)}{\chi_{L_1}^{\sigma\,-\,1}(\delta_1)}\ .$$

By lemma 4.3.1

$$\chi_{L_1}(N_{L_1/F}\,\delta_1) \;=\; \mu_{L_1/F}(\delta_1)\cdot\chi_{L_2}(N_{L_1/F}\,\delta_1) \;=\; \mu(N_{L_1/F}\,\delta_1)\cdot\chi_{L_2}(N_{L_1/F}\,\delta_1)$$

(4.3*l*).

Meanwhile

$$\chi_K(\delta_2) = \chi_{L_2}(N_{K/L_2}\,\delta_2) = \chi_{L_2}(\delta_2^{\,2}) = \frac{\chi_{L_2}(N_{L_2/F}\,\delta_2)}{\chi_{L_2}^{\sigma' - 1}(\delta_2)}$$

if σ' is the non-trivial element in $Gal(L_2/F)$.

Again by lemma 4.3.1

$$\chi_{L_2}(N_{L_2/F}\,\delta_2) = \tau_{L_2/F}(\delta_2) \cdot \chi_K(\delta_2) = \tau(N_{L_2/F}\,\delta_2) \cdot \chi_K(\delta_2)$$

(4.3*m*).

Now

$$\tau(x) \cdot \chi_{L_1}(x) = \tau(N_{L_2/F}\,\delta_2) \cdot \chi_{L_1}(N_{L_1/F}\,\delta_1) \cdot \chi_{L_1}(N_{L_2/F}\,\delta_2) .$$

By (4.3*l*), we have

$$\tau(x) \cdot \chi_{L_1}(x) = \tau(N_{L_2/F}\,\delta_2) \cdot \mu(N_{L_1/F}\,\delta_1) \cdot \chi_{L_2}(N_{L_1/F}\,\delta_1) \cdot \chi_{L_1}(N_{L_2/F}\,\delta_2) .$$

Notice $N_{L_2/F}\,\delta_2 = N_{K/L_1}\,\delta_2$ and $\chi_{L_1} \circ N_{K/L_1} = \chi_K$. So

$$\tau(x) \cdot \chi_{L_1}(x) = \tau(N_{L_2/F}\,\delta_2) \cdot \mu(N_{L_1/F}\,\delta_1) \cdot \chi_{L_2}(N_{L_1/F}\,\delta_1) \cdot \chi_K(\delta_2) .$$

According to (4.3*m*),

$$\tau(x) \cdot \chi_{L_1}(x) = \mu(N_{L_1/F}\,\delta_1) \cdot \chi_{L_2}(N_{L_1/F}\,\delta_1) \cdot \chi_{L_2}(N_{L_2/F}\,\delta_2) .$$

This is equal to $\mu(x) \cdot \chi_{L_2}(x)$. Claim VII is established. ||

Apply claim VII to the right hand side of (4.3k).

$$\frac{\chi_{L_2}^{-1}(2) \cdot \chi_{L_2}(t_2\,\pi_{L_2}^{2(d+1)}) \cdot \mu(t\,\pi_F^{d+1})}{-\,\chi_{L_1}(t_1\,\pi_F^{d+1})} = -\,\tau(t\,\pi_F^{d+1})$$

Because τ is a non-trivial unramified character of order 2, the fact that $t \in U_{F_o}$ (see theorem 4.1.1) implies

$$\frac{\chi_{L_2}^{-1}(2) \cdot \chi_{L_2}(t_2\,\pi_{L_2}^{2(d+1)}) \cdot \mu(t\,\pi_F^{d+1})}{-\,\chi_{L_1}(t_1\,\pi_F^{d+1})} = \tau(\pi_F^{d})$$

This proves our lemma in case 2. ||

As remarked before, (4.3b) follows from (4.3h) together with this lemma. Finally we can conclude that whenever $m_1 = 1$, the 2nd identity (4.3b) holds for all primes ℓ. The proof of theorem 4.3.4 is now completed. ||

To conclude theorem 4.3.3, it is necessary to establish (4.3b) for $m_1 > 1$ as well. We will do so in the next theorem, but first let us quote a relevant lemma from Langlands [16].

Lemma 4.3.5 (Langlands). *Let* $Gal(K/F) = Z_\ell \oplus Z_\ell$ *be the direct* *sum of two cyclic groups of prime order* ℓ. *Let* L *be a proper subfield of* K/F. *In other words, both* $H = Gal(K/L)$ *and* $\overline{H} = Gal(L/F)$ *have order* ℓ.

(i) *In the case* L/F *is unramified, if* χ_L *is a character of* $L^\times$ *such that* $(\chi_L \circ \sigma)\cdot\chi_L^{-1} \in S(K/L)$ *for all* $\sigma \in \overline{H}$, *and* w *is the jump in the ramification group filtration*

$$H = H_0 = \ldots = H_w \neq H_{w+1} = \{1\}$$

then

$$\chi_L(x) = 1 \quad \text{for } x \in U_L^{w+1} \text{ with } N_{L/F}(x) = 1 .$$

(ii) *In the case* L/F *is ramified but* K/L *is not, if* χ_L *is a character of* $L^\times$ *such that* $(\chi_L \circ \sigma)\cdot\chi_L^{-1} \in S(K/L)$ *for all* $\sigma \in \overline{H}$, *and* u *is the jump in the ramification group filtration*

$$\overline{H} = (\overline{H})_0 = \ldots = (\overline{H})_u \neq (\overline{H})_{u+1} = \{1\}$$

then

$$\chi_L(x) = 1 \quad \text{for } x \in U_L^{u+1} \text{ with } N_{L/F}(x) = 1 .$$

(iii) With the notations in the 2nd identity and the premises leading to it, if L_1 is the fixed field of the inertia group for $Gal(K/F)$, then there exists a character χ'_F of $F^\times$ such that

$$m(\chi_{L_1}^{-1} \cdot \chi'_{L_1/F}) \;=\; u + 1$$

and

$$m(\chi_{L_2}^{-1} \cdot \chi'_{L_2/F}) \;=\; u + 1$$

Here $\chi'_{L_i/F}$ is the composition $\chi'_F \circ N_{L_i/F}$, while u is the jump in the ramification group filtration of $Gal(L_2/F)$. It can be shown that u also represents the jump in the ramification group filtration of $G_0 = Gal(K/L_1)$.

For notational simplicity, $(\chi_L \circ \sigma) \cdot \chi_L^{-1}$ which appears in part (i) and (ii) will be abbreviated to $\chi_L^{\sigma-1}$ just as in lemma 4.3.1.

Proof. We prove (i) first. Suppose σ generates $\overline{H}$. By Hilbert's theorem 90, there exists $y \in L^\times$ such that $x = \sigma(y)/y = y^{\sigma-1}$. As π_F is also a uniformizing parameter of L, the above y can actually be selected from U_L.

$$\frac{\sigma(y\,\pi_F^n)}{y\,\pi_F^n} \;=\; \frac{\sigma(y)}{y} \;=\; x \qquad \text{for any integer } n\,.$$

Moreover, we may assume that $y \notin U_F$ because only the case $x \neq 1$ requires an argument. Now

$$\sigma(y) = x\,y \equiv y \quad mod\ P_L^{w+1}.$$

So y is congruent to some $\zeta \in U_F$ modulo P_L. Again notice that $\sigma(y\,\zeta^{-1})/y\,\zeta^{-1} = y^{\,\sigma-1}$. In other words, y can be selected from U_L^1. Let $y = 1 + \varepsilon\,\pi_F^a$ where $\varepsilon \in U_L$. Then

$$y^{\,\sigma-1} \equiv 1 + (\sigma(\varepsilon) - \varepsilon)\,\pi_F^a \quad mod\ P_L^{a+1}.$$

The congruence $\sigma(\varepsilon) \equiv \varepsilon \quad mod\ P_L$ would imply $\varepsilon \equiv \zeta \quad mod\ P_L$ for some $\zeta \in U_F$. Hence, we could select a new y from U_L^{a+1}; otherwise

$$\sigma(\varepsilon) \not\equiv \varepsilon \quad mod\ P_L\ .$$

This latter scenario means $\sigma(\varepsilon) - \varepsilon$ is a unit, and $y^{\,\sigma-1} = x \in U_L^{w+1}$ indicates that $a \geq w + 1$. In the former scenario, our argument can be iterated until we have $a \geq w + 1$. Either way,

$$\chi_L(x) = \chi_L(y^{\,\sigma-1}) = \chi_L^{\sigma-1}(y) = 1$$

because characters in $S(K/L)$ have conductor at most $w + 1$. Hence we obtain (i).

Next we prove (ii). Again let $\langle\sigma\rangle = \overline{H}$. By Hilbert's theorem 90 there exists $y \in L^\times$ such that $x = y^{\sigma-1}$. Let $y = \varepsilon\,\pi_L^b$ where $\varepsilon \in U_L$ and b is an integer. Because

$$\frac{\sigma(\varepsilon\,\pi_L^b\,\pi_F^n)}{\varepsilon\,\pi_L^b\,\pi_F^n} = y^{\sigma-1} \qquad (*)$$

we may assume $b > 0$. Then

$$y^{\sigma-1} = (\varepsilon^{\sigma-1})\,(\pi_L^{\sigma-1})^b \equiv (\pi_L^{\sigma-1})^b \quad mod\ P_L^{u+1}$$

as $\sigma \in (\overline{H}\,)_u$. However, the fact that $\sigma \notin (\overline{H}\,)_{u+1}$ means

$$\pi_L^{\sigma-1} \not\equiv 1 \quad mod\ P_L^{u+1}.$$

On the other hand,

$$1 = N_{L/F}(\pi_L^{\sigma-1}) \equiv (\pi_L^{\sigma-1})^{\ell} \quad mod\ P_L^{u+1}$$

as $\pi_L^{\sigma-1}$ is a unit. Therefore $\pi_L^{\sigma-1}$ modulo P_L, being an element of the group $k_L^\times$, must have order ℓ. Now, recall that $y^{\sigma-1} = x \in U_L^{u+1}$. So

$$y^{\sigma-1} \equiv (\pi_L^{\sigma-1})^b \quad mod\ P_L^{u+1}$$

implies $(\pi_L^{\sigma-1})^b \equiv 1 \quad mod\ P_L^{u+1}$, and we have ℓ divides b.

By $(*)$, it is possible to select y from U_L. Finally,

$$\chi_L(x) = \chi_L(y^{\sigma-1}) = \chi_L^{\sigma-1}(y) = 1$$

because characters in $S(K/L)$ are unramified by assumption. Thus (ii) is proved.

To construct such a character χ'_F in (iii), we first define χ'_F on the unit group $U_F^{u+1} = N_{L_1/F}(U_{L_1}^{u+1})$ by

$$\chi'_F(z) = \chi_{L_1}(x) \qquad \text{where } x \in U_{L_1}^{u+1} \text{ and } z = N_{L_1/F}(x).$$

Part (i), which we have already established, asserts that the above definition is legitimate. Recall from (4.3a)

$$m_1 \geq u + 1 .$$

So χ'_F is in fact a character of $U_F^{u+1}/U_F^{m_1}$, which can be extended to a character of $U_F/U_F^{m_1}$ and ultimately to a character of $F^\times$, again denoted by χ'_F. Notice that from the definition we have

$$u + 1 \geq m(\chi_{L_1}^{-1} \cdot \chi'_{L_1/F}) .$$

Since the three characters $\chi_K^{-1}\cdot\chi'_{K/F}$, $\chi_{L_1}^{-1}\cdot\chi'_{L_1/F}$, $\chi_{L_2}^{-1}\cdot\chi'_{L_2/F}$ satisfy all the assumptions in the 2nd identity, we can apply (4.3a) again to conclude

$$m(\chi_{L_1}^{-1}\cdot\chi'_{L_1/F}) \;\geq\; u+1 \;.$$

In other words,

$$m(\chi_{L_1}^{-1}\cdot\chi'_{L_1/F}) \;=\; u+1 \qquad (**).$$

It remains to show that $m(\chi_{L_2}^{-1}\cdot\chi'_{L_2/F}) \;=\; u+1$ as well. Because $N_{K/L_1}(U_K^{u+1}) \;=\; U_{L_1}^{u+1}$, (**) implies

$$u+1 \;\geq\; m(\chi_K^{-1}\cdot\chi'_{K/F}) \;=\; m(\chi_{L_2}^{-1}\cdot\chi'_{L_2/F}) \;.$$

Assume $\chi_K^{-1}\cdot\chi'_{K/F}$ is trivial on U_K^u. Then $\chi_{L_1}^{-1}\cdot\chi'_{L_1/F}$ annihilates the norm group $N_{K/L_1}(U_K^u)$. Because $[\,U_{L_1}^u : N_{K/L_1}(U_K^u)\,] \;=\; \ell$, there exists a character $\nu \in S(K/L_1)$ such that $m(\nu\cdot\chi_{L_1}^{-1}\cdot\chi'_{L_1/F})$ is less than or equal to u. This is a contradiction to (4.3a). In summary, $\chi_K^{-1}\cdot\chi'_{K/F}$ cannot be trivial on $U_{L_2}^u$, and we obtain

$$u+1 \;=\; m(\chi_K^{-1}\cdot\chi'_{K/F}) \;=\; m(\chi_{L_2}^{-1}\cdot\chi'_{L_2/F}) \;.$$

This completes the proof of (iii), as well as lemma 4.3.5. ||

Remark: The above lemma and its proof hold even if K/F is wildly ramified. Nonetheless, we only make use of the tame case of lemma 4.3.5 to prove our next theorem and eventually theorem 4.3.3.

Theorem 4.3.6. *If the Galois extension K/F is tamely ramified and the subfield L_1 is unramified over F, then the 2nd identity (4.3b) holds for $m_1 > 1$.*

Proof. Recall from claim II that $m_2 > m_1 > 1$. Once again we are going to break up the argument into

Case 1 : *ℓ is odd.*

Case 2 : $\ell = 2$.

Let us consider **case 1** first. To obtain (4.3*b*) in this case, it is enough to show

$$W(\chi_{L_1}) = W(\chi_{L_2}) \tag{4.3n}$$

because $\tau(\pi_F^d)^{\frac{\ell(\ell-1)}{2}} = 1$ for odd ℓ and

Claim VIII. *If ℓ is odd,* $\prod_{\mu \in S(L_2/F)} W(\mu) = 1$.

Proof. As it is stated, the claim holds even if L_2/F is not tamely ramified. Nonetheless, we will address the immediate situation, assuming all non-trivial μ have conductor one. The argument for $m(\mu) > 1$ is very similar.

By definition, if $\mu \neq 1$,

$$W(\mu^{-1}) = N(P_F)^{-1/2} \sum_{x \in U_F/U_F^1} \mu\left(\frac{x}{\pi_F^{d+1}}\right) \psi_F\left(\frac{x}{\pi_F^{d+1}}\right) .$$

Its complex conjugate is given by

$$\begin{aligned}\overline{W(\mu^{-1})} &= N(P_F)^{-1/2} \sum_{x \in U_F/U_F^1} \mu^{-1}\left(\frac{x}{\pi_F^{d+1}}\right) \psi_F\left(\frac{-x}{\pi_F^{d+1}}\right) \\ &= N(P_F)^{-1/2} \mu(-1) \sum_{x \in U_F/U_F^1} \mu^{-1}\left(\frac{-x}{\pi_F^{d+1}}\right) \psi_F\left(\frac{-x}{\pi_F^{d+1}}\right) .\end{aligned}$$

Since multiplication by -1 yields a bijection from U_F/U_F^1 to itself,

$$\overline{W(\mu^{-1})} = \mu(-1)\ W(\mu) .$$

Observe that $\mu(-1)^2 = 1 = \mu(-1)^\ell$. So in the case ℓ is odd, $\mu(-1)$ must be 1, and

$$\overline{W(\mu^{-1})} = W(\mu) .$$

Meanwhile, $|W(\mu)| = 1$ (see Martinet [18] II § 2, proposition 2.2). As a result,

$$W(\mu^{-1}) = W(\mu)^{-1} .$$

Now, because ℓ is odd, $S(L_2/F)$ is a group with no character of order 2. Therefore we have claim VIII. ||

Recall that χ_{L_1} and the character χ'_F we constructed in part (*iii*) of lemma 4.3.5 share the same conductor $m_1 > 1$. Since K/F is tamely ramified, we have $m(\chi_{L_i}^{-1} \cdot \chi'_{L_i/F}) = 1$. Moreover, it follows from theorem A.2 part (*a*) that $m(\chi'_{L_i/F}) = \Psi_{L_i/F}(m_1 - 1) + 1$ which is greater than one. Let

$$m(\chi'_{L_i/F}) = \varepsilon_i + 2 \cdot d_{(\chi'_{L_i/F})}$$

where $d_{(\chi'_{L_i/F})}$ is a positive integer and ε_i is either one or zero. Then part (*c*) of theorem A.1 implies

$$W(\chi_{L_i}) = W(\chi_{L_i} \cdot (\chi'_{L_i/F})^{-1} \cdot \chi'_{L_i/F}) = W(\chi'_{L_i/F}) \cdot (\chi_{L_i}^{-1} \cdot \chi'_{L_i/F})(c_i) .$$

Here $c_i \in L_i^\times$ satisfies

$$\chi'_{L_i/F}(1 + x) = \psi_{L_i}(c_i x) \qquad \text{for } x \text{ of order} \geq \varepsilon_i + d_{(\chi'_{L_i/F})} .$$

In other words, $(4.3n)$ is equivalent to

$$W(\chi'_{L_1/F}) \cdot (\chi_{L_1}^{-1} \cdot \chi'_{L_1/F})(c_1) = W(\chi'_{L_2/F}) \cdot (\chi_{L_2}^{-1} \cdot \chi'_{L_2/F})(c_2)$$

which follows immediately from our next claim.

Claim IX. *For odd ℓ, we have*

(i) $W(\chi'_{L_i/F}) = W(\chi'_F)^{\ell}$.

(ii) $(\chi_{L_1}^{-1} \cdot \chi'_{L_1/F})(c_1) = (\chi_{L_2}^{-1} \cdot \chi'_{L_2/F})(c_2)$.

Proof. By the 1st identity which has already been proved in section 4.2,

$$W(\chi'_{L_i/F}) \prod_{\mu \in S(L_i/F)} W(\mu) = \prod_{\mu \in S(L_i/F)} W(\chi'_F \cdot \mu) .$$

Let τ be a non-trivial character in $S(L_1/F)$. Then $\prod_{\mu \in S(L_1/F)} W(\mu) = \tau(\pi_F^d)^{\frac{\ell(\ell-1)}{2}} = 1$ since ℓ is odd. As for $\prod_{\mu \in S(L_2/F)} W(\mu)$, we have seen in claim VIII that this product is also one. To summarize,

$$W(\chi'_{L_i/F}) = \prod_{\mu \in S(L_i/F)} W(\chi'_F \cdot \mu) .$$

Thus part (i) is completed once we show

$$\prod_{\mu \in S(L_i/F)} W(\chi'_F \cdot \mu) = W(\chi'_F)^{\ell} .$$

Recall $m(\chi'_F) = m_1 > 1$, while $m(\mu)$ is less than or equal to one. Suppose

$$m(\chi'_F) = m_1 = \varepsilon + 2 \cdot d_{(\chi'_F)}$$

with $d_{(\chi'_F)}$ a positive integer and $\varepsilon = 0$ or 1. Then part (c) of theorem A.1 yields

$$\begin{aligned} \prod_{\mu \in S(L_i/F)} W(\chi'_F \cdot \mu) &= \prod_{\mu \in S(L_i/F)} W(\chi'_F) \cdot \mu^{-1}(c) \\ &= W(\chi'_F)^{\ell} \prod_{\mu \in S(L_i/F)} \mu^{-1}(c) \end{aligned}$$

where c is the parameter in theorem A.1 for χ'_F, satisfying

$$\chi'_F(1+x) = \psi_F(c\,x) \qquad \text{for all } x \in P_F^{\varepsilon + d_{(\chi'_F)}}.$$

So it remains to prove

$$1 = \prod_{\mu \in S(L_i/F)} \mu^{-1}(c)$$

but this is evident once we fix a non-trivial character τ in $S(L_i/F)$. Specifically

$$\prod_{\mu \in S(L_i/F)} \mu^{-1}(c) = \prod_{m=0}^{\ell-1} \tau^{m}(c) = \tau(c)^{\frac{\ell(\ell-1)}{2}} = 1 .$$

We now proceed to verify

$$(\chi_{L_1}^{-1} \cdot \chi'_{L_1/F})(c_1) = (\chi_{L_2}^{-1} \cdot \chi'_{L_2/F})(c_2) .$$

Since K/F is tamely ramified and $m(\chi'_F) = m_1 > 1$, we may assume $c_1 = c_2 = c$ according to part (*b*) and part (*c*) of theorem A.2. Remember that $c \in F^\times$ is the parameter in theorem A.1 for χ'_F. So

$$\chi'_{L_1/F}(c) = \chi'_F(c)^\ell = \chi'_{L_2/F}(c)$$

and we can apply claim VI to complete part (ii). ||

As noted before, this claim establishes $(4.3n)$, and case 1 is concluded.

Let us turn to **case 2**. We must prove in this case

$$W(\chi_{L_1})\,\tau(\pi_F^d) = W(\chi_{L_2})\,W(\mu) \tag{4.3o}$$

where τ, μ are the non-trivial characters in $S(L_1/F)$ and $S(L_2/F)$ respectively.

Just like in case 1, the character χ'_F in part (*iii*) of lemma 4.3.5 has conductor $m_1 > 1$. So

$$m(\chi'_{L_i/F}) = \Psi_{L_i/F}(m_1 - 1) + 1$$

by theorem A.2 part (a). This implies $m(\chi'_{L_i/F}) > 1$. Meanwhile, the character $\chi_{L_i}^{-1} \cdot \chi'_{L_i/F}$ is tame. It follows from part (c) of theorem A.1 that

$$W(\chi_{L_i}) \;=\; W(\,\chi_{L_i} \cdot (\chi'_{L_i/F})^{-1} \cdot \chi'_{L_i/F}\,) \;=\; W(\chi'_{L_i/F}) \,\cdot\, (\chi_{L_i}^{-1} \cdot \chi'_{L_i/F})(c_i)$$

(4.3p)

Again parameter c_i for $\chi'_{L_i/F}$ is defined as in theorem A.1.

We now invoke the 1st identity:

$$W(\chi'_{L_2/F})\, W(\mu) \;=\; W(\chi'_F)\, W(\chi'_F \cdot \mu)$$

If $c \in P_F^{-(d + m(\chi'_F))}$ satisfies theorem A.1 for χ'_F, then theorem A.1 part (c) yields

$$W(\chi'_F \cdot \mu) \;=\; W(\chi'_F) \,\cdot\, \mu^{-1}(c)$$

as $m(\chi'_F) \;=\; m_1 \;>\; 1 \;=\; m(\mu)$. Consequently

$$W(\chi'_{L_2/F})\, W(\mu) \;=\; W(\chi'_F)^2 \,\cdot\, \mu^{-1}(c)$$

In similar fashion, it can be deduced from the 1st identity that

$$W(\chi'_{L_1/F})\, \tau(\pi_F^d) \;=\; W(\chi'_F)^2 \,\cdot\, \tau^{-1}(c)$$

As a result,

$$W(\chi'_{L_2/F})\, W(\mu) \,\cdot\, \mu(c) \;=\; W(\chi'_{L_1/F})\, \tau(\pi_F^d) \,\cdot\, \tau(c)$$

This equality together with (4.3p) will produce the 2nd identity (4.3o) if we show

$$\tau(c)^{-1} \cdot (\chi_{L_1}^{-1} \cdot \chi'_{L_1/F})(c_1) \;=\; \mu(c)^{-1} \cdot (\chi_{L_2}^{-1} \cdot \chi'_{L_2/F})(c_2) \qquad (4.3q)$$

First of all, we may take $c_1 = c$ and $c_2 = c$ due to part (b) and (d) of theorem A.2. Next, observe that

$$\chi'_{L_1/F}(c) \;=\; \chi'_F(c)^2 \;=\; \chi'_{L_2/F}(c)$$

Finally, claim VII implies

$$\tau(c)^{-1} \cdot \chi_{L_1}^{-1}(c) \;=\; \mu(c)^{-1} \cdot \chi_{L_2}^{-1}(c)$$

Therefore (4.3q) is true and we have completed case 2.

Now, (4.3b) is established for $m_1 > 1$ regardless of the parity of ℓ. In other words, theorem 4.3.6 is proved. ||

Put together theorem 4.3.4 and theorem 4.3.6. we are able to conclude the proof of theorem 4.3.3, from which the 2nd identity in the case K/F is tamely ramified follows. ||

We have followed Langlands [16] in the above proof of the 2nd identity when K/F is tamely ramified. His method in [16] actually applies to certain cases of the 2nd identity in which K/F is wildly ramified. However, as pointed out by Langlands, results analogous to lemma 4.3.5 account for many, but by no means all, cases in the proof of the 2nd identity. For odd residue class field characteristic p, Lakkis [14, Satz 2, p.226] contains the details of Dwork's proof of the 2nd identity when K/F is wildly ramified. Regarding $p = 2$, we are unable to locate the original proof in the literature. Casselman [1, Theorem 1.9, p.814] has shown that the 2nd identity is equivalent to an isomorphism between two irreducible components of the Weil representations (of $SL_2(F)$) associated to distinct quadratic extensions of F. So any independent proof of this isomorphism would complete the argument for the 2nd identity.

4.4 The third identity

We begin with some general facts required in the proof of the 3rd identity.

Theorem 4.4.1 (Langlands). *Suppose* $G = Gal(K/F)$ *is a semi-direct* *product HC where $C \triangleleft G$, $H \neq \{1\}$, and C is non-trivial abelian such that every non-trivial normal subgroup of G contains C . Hence $H \cap C = \{1\}$.*

(i) If K/F is tamely ramified, then C is equal to the inertia group G_o which must be cyclic of prime order in this case. Moreover the index $[G : G_o] = |H|$ divides $|C| - 1$.

(ii) If K/F is wildly ramified, then the higher ramification groups of G satisfy

$$C = G_1 = \ldots = G_u \neq G_{u+1} = \{1\}$$

and the index $[G_o : G_1]$ divides $|C| - 1$.

In this case, all the non-trivial elements in C have order p , the residue class field characteristic of F .

Proof. Notice the inertia group G_o cannot be trivial as G is non-abelian. Let us assume K/F to be tame first. Then it follows G_o is cyclic of prime order. Because G_o is a non-trivial normal subgroup, we have $C \subseteq G_o$. This means $C = G_o$ since the only non-trivial subgroup of a cyclic group of prime order is itself. To prove the other assertion in (i), we need to show that the centralizer of C

$$A = \{x \in G \mid xc = cx \quad \text{for all } c \in C\}$$

must be C itself. In fact, $A \cap H$ is normal in G, but it does not contain C. So

$$A \cap H = \{1\} .$$

Together with $A \supseteq C$, we conclude $A = C$ as every $x \in A$ can be written uniquely as a product hc with $h \in H$ and $c \in C$. An immediate consequence of $A = C$ is that the conjugacy class of every non-trivial $c \in C$ consists of $[G : C]$ number of elements. In other words, $[G : C]$ must divide $|C| - 1$, the number of non-trivial $c \in C$.

Now we proceed to the proof of (ii). Observe that the argument for $A = C$ remains valid when the extension K/F is wildly ramified. With $G_1 \neq \{1\}$, we have $C \subseteq G_1$ since the higher ramification groups are normal in G. On the other hand, notice that the centralizer B of G_1 is normal in G. Being a p-group, G_1 has a non-trivial center. Hence, B cannot be trivial, and it contains C as well. Meanwhile $B \subseteq A$, which implies $B = C$. Therefore C is equal to $B \cap G_1$, the center of G_1. As a result, $G_1 = C$; otherwise the non-trivial center of the nilpotent group G_1/C contains a cyclic group of prime order which is pullbacked to a normal abelian[3] subgroup of G_1 in which C has prime index, a contradiction to $A = C$.

Any other higher ramification group G_i that is non-trivial must coincide with C because $C = G_1 \supseteq G_i \supseteq C$. For future reference, let $u \geq 1$ be the integer such that $C = G_u \neq G_{u+1} = \{1\}$.

As for the divisibility claim in part (ii), we recall the homomorphism

$$\theta_i \ : \ G_i/G_{i+1} \longrightarrow U_K^i/U_K^{i+1} \qquad \text{for } i \geq 0$$

defined by

$$\theta_i(\sigma) = \frac{\sigma(\pi_K)}{\pi_K} \qquad \text{where } \pi_K \text{ has order one in } K\,.$$

According to Serre [20, chapter IV, § 2, proposition 9], given $s \in G_o$ and $\sigma \in G_u$, we have

$$\theta_u(s\sigma s^{-1}) = \theta_0(s)^u\, \theta_u(\sigma)$$

[3]If a group modulo its center is cyclic, then it must be abelian.

provided that both $\theta_u(s\sigma s^{-1})$ and $\theta_u(\sigma)$ are interpreted as elements of P_K^u/P_K^{u+1} via the isomorphism

$$U_K^u/U_K^{u+1} \simeq P_K^u/P_K^{u+1}.$$

It follows that s commutes with $\sigma \neq 1$ if and only if $\theta_0(s)^u \in U_K^1$. However, in view of the equality $\theta_u(s\sigma s^{-1}) = \theta_0(s)^u\,\theta_u(\sigma)$, we also have $\theta_0(s)^u \in U_K^1$ if and only if $s \in A$.

Since $A = C$, the G_o conjugacy class of each $\sigma \neq 1$ has exactly $[G_o : C]$ elements. In other words, $[G_o : C]$ divides $|G_u| - 1$.

Finally, the subgroup of C consisting of elements of order p or 1 is a non-trivial normal subgroup of G. So it must be C itself. This completes the proof of theorem 4.4.1. ||

In the above proof, we have established and used repeatedly the following result which we now highlight as a lemma.

Lemma 4.4.2. *If C is non-trivial, abelian and normal in a semi-direct product HC such that all non-trivial normal subgroups of HC contain C,* *then C is its own centralizer.*

Henceforth we keep the notations G , H , C and the assumptions in theorem 4.4.1. Recall the Galois group $G = Gal(K/F)$ acts on the character group of C, denoted by C^*. Particularly, if $g \in G$ and $\mu \in C^*$, then the G-action is given by

$$\mu^g(x) = \mu(g\,x\,g^{-1}) \qquad \text{for } x \in C\,.$$

Let $H = Gal(K/E)$, $C = Gal(K/L)$ and

$T =$ a complete set of representatives of the G-orbits

$G_\mu = stab_G(\mu)$, the isotropy group (stabilizer) of $\mu \in C^*$

$F_\mu =$ the fixed field of G_μ

$H_\mu = G_\mu \cap H$

It follows immediately that

Claim I. *(a) For all $g \in G$, we have $G_{(\mu^g)} = g^{-1}\,G_\mu\,g$.*

(b) $G_\mu = H_\mu C$.

In addition, part (b) of the above claim enables us to extend μ to a character of G_μ defined by

$$\mu'(hc) = \mu(c) \qquad \text{where } h \in H_\mu \text{ and } c \in C\,.$$

Via the reciprocity map, this μ' can be interpreted as a character of $F_\mu^\times$. The third identity then asserts that given any quasi-character χ_F on $F^\times$,

$$W(\chi_F \circ N_{E/F}) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu') = W(\chi_F) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\,\mu' \cdot (\chi_F \circ N_{F_\mu/F})\,) \tag{4.4a}$$

regardless of the choice of the representatives of the G-orbits.

Let us elaborate on this last remark before we continue. First of all, the G-orbits are in fact identical to the H-orbits. If $h \in H$, we observe

$$H_{(\mu^h)} = G_{(\mu^h)} \cap H = (h^{-1}\, G_\mu\, h) \cap H = h^{-1}\,(G_\mu \cap H)\, h$$

This means $G_{(\mu^h)} = (h^{-1}\, H_\mu\, h)C$ because of claim I. Suppose $\mathbf{C}^\times$ denotes the nonzero complex numbers. Then it follows that the diagram below is commutative.

$$\begin{array}{ccc} & G_\mu & \xrightarrow{\mu'} & \mathbf{C}^\times \\ hxh^{-1} & \uparrow & \nearrow_{(\mu^h)'} & \\ & G_{(\mu^h)} & & \end{array}$$

Equivalently, we can conclude that $(\mu')^h = (\mu^h)'$. Now, by lemma 1.2.10

$$W(\mu') = W((\mu')^h) = W((\mu^h)') \qquad (4.4b).$$

Similarly,

$$W((\mu^h)' \cdot (\chi_F \circ N_{h^{-1}(F_\mu)/F})) = W((\mu')^h \cdot (\chi_F \circ N_{F_\mu/F} \circ h)) .$$

When we interpret $(\mu')^h$ as a character of $h^{-1}(F_\mu^\times)$ and μ' as a character of $F_\mu^\times$, we have

$$(\mu')^h = \mu' \circ h \qquad \text{on } h^{-1}(F_\mu^\times)$$

according to the funtoriality properties of the reciprocity map (see Serre [20]). Furthermore, our next claim yields

$$W((\mu' \circ h) \cdot (\chi_F \circ N_{F_\mu/F} \circ h)) = W(\mu' \cdot (\chi_F \circ N_{F_\mu/F})) .$$

Claim II. *Suppose F is a local field with residue class field characteristic p and χ is a quasi-character on $F^\times$. If ϕ is a Q_p-isomorphism from F into* *an algebraic closure of* F *, then on* $\phi(F^\times)$ *we can define a quasi-character* $\chi \circ \phi^{-1}$ *by*

$$\chi \circ \phi^{-1}(y) = \chi(x) \qquad \text{where } \phi(x) = y\,.$$

Moreover,

$$W(\chi \circ \phi^{-1}) = W(\chi)\;.$$

Proof. $\chi \circ \phi^{-1}$ is a well defined homomorphism because ϕ is an isomorphism and x is uniquely determined by y. Let O_F , P_F , π_F , P_F^d , U_F be the ring of integers of F, the maximal ideal of O_F , a uniformizing parameter of F, the absolute different of F and the unit group of O_F respectively. Then $\phi(O_F)$, $\phi(P_F)$, $\phi(\pi_F)$, $\phi(P_F)^d$, $\phi(U_F)$ are the counterparts of the field $\phi(F)$ as any Q_p - isomorphism from a local field to its algebraic closure preserves the valuation. Hence F and $\phi(F)$ share the same absolute ramification index, residue class field and order of the absolute different. Also the conductor of $\chi \circ \phi^{-1}$ is equal to the conductor of χ. Let us denote this common conductor by m. Since

$$Tr_{\phi(F)/Q_p}\Big(\frac{y}{\phi(\pi_F)^{d+m}}\Big) = Tr_{F/Q_p}\Big(\frac{x}{\pi_F^{d+m}}\Big)$$

with $\phi(x) = y$, the canonical additive characters behaves similarly:

$$\psi_{\phi(F)}\Big(\frac{y}{\phi(\pi_F)^{d+m}} \Big) = \psi_F\Big(\frac{x}{\pi_F^{d+m}} \Big) .$$

Now

$$W(\chi \circ \phi^{-1}) = W(\chi)$$

is immediate from the definition of root number (for a quasi-character). ||

Claim II reveals

$$W(\, (\mu^h)' \cdot (\chi_F \circ N_{h^{-1}(F_\mu)/F})\,) = W(\, \mu' \cdot (\chi_F \circ N_{F_\mu/F})\,) .$$

Together with (4.4*b*), we have shown that (4.4*a*) is insensitive to the choice of representatives in T.

The rest of section 4.4 concentrates on the proof of (4.4*a*) in the case K/F is tamely ramified. All the assumptions and the notations introduced in this section up to (4.4*a*) will be kept in the subsequent discussion.

Lemma 4.4.3. *Suppose K/F is tamely ramified. Then C has prime order* *according to theorem 4.4.1. Let ℓ denote $|C|$. We have*

$$\begin{array}{ccccc} & & K & & \\ \text{unramified}\ \Big\{ & / & & \backslash^{\ell} & \Big\}\ \begin{array}{c}\text{totally}\\ \text{ramified}\end{array} \\ & E & & L & \\ \begin{array}{c}\text{totally}\\ \text{ramified}\end{array}\ \Big\{ & {}^{\ell}\backslash & & / & \Big\}\ \text{unramified} \\ & & F & & \end{array} \qquad (4.4c).$$

Moreover,

(1) $G_\mu = C$ *for all non-trivial* $\mu \in T$. *This implies* $F_\mu = L$.

(2) $|T| - 1 = (\ell - 1)/|H|$. *So* $\ell \neq 2$.

(3) with $q = |k_F|$, *the order of* q *modulo* ℓ *is* $[k_K : k_F]$, *the residue class field degree of* K/F.

(4) as characters of $L^\times$ *under the reciprocity map,* μ^h *and* μ *satisfy*

$$\mu^h = (\mu)^q \qquad \text{on } U_L$$

if h *is the Frobenius automorphism of* H.

(5) On E, *it is possible to identify the following i-th elementary symmetric functions.*

$$Tr^{(i)}_{E/F}(x) = Tr^{(i)}_{K/L}(x)$$

for $\ell \geq i \geq 1$.

Proof. Figure (4.4c) follows directly from theorem 4.4.1 part (i) . In particular, $G_o = C = Gal(K/L)$ reveals L/F must be unramified, whereas E/F is a ramified extension of degree ℓ because

$$[E:F] = \frac{|G|}{|H|} = |C| = \ell$$

and $H \cap G_o = H \cap C = \{1\}$ implies K/E is unramified.

Recall C is cyclic of prime order when K/F is tamely ramified. This means every non-trivial character of C has trivial kernel. So, any $x \in G_\mu$ must belong to the centralizer of C unless $\mu = 1$. By lemma 4.4.2, $G_\mu \subseteq C$. As C is abelian, $G_\mu \supseteq C$, and (1) is proved.

If $\mu \neq 1$, the G-orbit containing μ has exactly $[G:C]$ characters according to (1) . Since $H \cap C = \{1\}$, the index $[G:C] = |H|$. Therefore, the $\ell - 1$ non-trivial μ in C^* are divided into $(\ell-1)/|H|$ distinct G-orbits. Deleting the orbit for $\mu = 1$ from T , we obtain

$$|T| - 1 = \frac{\ell - 1}{|H|} .$$

Remember H is assumed to be non-trivial. So $\ell \neq 2$.

Now, let us proceed to (4) first, and then use it to establish (3). By means of the reciprocity map, we can interpret μ^h and μ as characters of $L^\times$. As we have seen before, it is a consequence of the functoriality properties of the reciprocity map that

$$\mu^h = \mu \circ h \qquad \text{on } L^\times$$

Meanwhile, because h is the Frobenius automorphism in $H = Gal(K/E)$,

$$h(x) \equiv x^q \quad mod\ P_K \qquad \text{for all } x \in O_K$$

with $q = |k_E|$. In fact, figure (4.4c) indicates q is equal to $|k_F|$. On the other hand, that K/F is tamely ramified implies the conductor of μ cannot exceed one. Hence we are able to conclude

$$\mu^h = \mu \circ h = \mu^q \qquad \text{on the unit group } U_L \subset O_K .$$

Generally, it is true that for $n \geq 1$,

$$\mu^{(h^n)} = (\mu)^{q^n} \qquad \text{on } U_L \qquad\qquad (4.4d).$$

The above equality is valid on $L^\times$ as well. Specifically, because K/L is totally ramified, $N_{K/L}(\pi_K)$ is a uniformizing parameter of L if π_K is a uniformizing parameter of K. Observe

$$\mu^{(h^n)}(\,N_{K/L}(\pi_K)\,) \;=\; 1 \;=\; (\mu)^{q^n}(\,N_{K/L}(\pi_K)\,)$$

holds automatically. Together with $(4.4d)$, we see that

$$\mu^{(h^n)} \;=\; (\mu)^{q^n} \qquad \text{on} \;\; L^\times .$$

Let us fix one $\mu \neq 1$. By (1), we have $H_\mu = G_\mu \cap H = \{1\}$. In other words, $\mu^{(h^n)} = \mu$ if and only if the order of h divides n. However, it is immediate from figure $(4.4c)$ that the Frobenius automorphism h has order $[k_K : k_F]$. Therefore, the residue class field degree $[k_K : k_F]$ is the smallest positive integer n such that $(\mu)^{q^n} = \mu$. As the order of μ is ℓ, it follows that $[k_K : k_F]$ coincides with the order of q modulo ℓ.

Since $H \cap C = \{1\}$, the composite of E and L coincides with K i.e.

$$EL = K \; .$$

So every F - isomorphism from E into K comes from a restriction (to E) of a unique automorphism in $Gal(K/L)$. This proves (5), and all of lemma 4.4.3 have now been established. ||

As before, we are going to abbreviate the composition $\chi_F \circ N_{E/F}$ to $\chi_{E/F}$ and the composition $\chi \circ N_{F_\mu/F}$ to $\chi_{F_\mu/F}$. In some occasions, we write $\chi_{K/F}$ to denote $\chi_F \circ N_{K/F}$ as well.

We have already seen in the previous lemma that $F_\mu = L$ unless $\mu = 1$. As a result, when K/F is tamely ramified, $(4.4a)$ becomes

$$W(\chi_{E/F}) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu) = W(\chi_F) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu \cdot \chi_{L/F}) \qquad (4.4e).$$

The proof of this identity depends on the conductor m of the quasi-character χ_F . We will first verify $(4.4e)$ for $m = 0$ or 1 . Then theorem 4.4.4 handles the case $m > 1$ and completes the proof of the 3rd identity when K/F is tamely ramified.

Suppose $m = 0$. The three quasi-characters $\chi_{E/F}$, χ_F , $\chi_{L/F}$ are all unramified. If d is the order of the absolute different of F , we have

$$W(\chi_{E/F}) = \chi_F(N_{E/F}(\pi_E)^{(\ell-1)+\ell d})$$

and

$$W(\chi_F) = \chi_F(\pi_F^d)$$

while

$$W(\mu \cdot \chi_{L/F}) \;=\; \chi_{L/F}(\pi_F^{d+1})\; W(\mu) \;=\; \chi_F(\pi_F^{d+1})^{|H|}\; W(\mu)$$

for all $\mu \neq 1$ because theorem 4.4.1 part (i) implies such μ are always tamely ramified.

Let us choose the uniformizing parameter π_F of F to be $N_{E/F}(\pi_E)$. Then (4.4e) for $m = 0$ follows once we show

$$\chi_F(\pi_F^{(\ell-1)+\ell d}) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu) \;=\; \chi_F(\pi_F^d) \prod_{\substack{\mu \in T \\ \mu \neq 1}} \chi_F(\pi_F^{d+1})^{|H|}\; W(\mu)\;.$$

Due to theorem 4.4.3 part (2), this is equivalent to

$$\chi_F(\pi_F^{(\ell-1)+\ell d}) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu) \;=\; \chi_F(\pi_F^d)\;\left[\chi_F(\pi_F^{d+1})^{|H|}\right]^{\frac{\ell-1}{|H|}} \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu)$$

which can be verified by inspection.

Next, we assume $m = 1$. Then $\chi_{L/F}$ has conductor one as well. Again, if π_E is a uniformizing parameter of E, we pick $\pi_F = N_{E/F}(\pi_E)$ to be our uniformizing parameter of F.

Claim III. *Under the assumptions of theorem 4.4.1, if K/F is tamely ramified, $m = 1$ implies $\chi_{E/F}$ is a tamely ramified quasi-character.*

Proof. As E/F has to be tamely ramified, $N_{E/F}(U_E^1) = U_F^1$. Hence

$$\chi_{E/F}(U_E^1) = \chi_F(U_F^1) = \{1\} .$$

Suppose $\chi_{E/F}$ is not tamely ramified. The above observation means $\chi_{E/F}$ is unramified. It follows from figure (4.4*c*) that $\chi_{K/F}$ is unramified as well. On the other hand, $\chi_{L/F}$ must be tame since L/F is unramified and $N_{L/F}(U_L) = U_F$. However $[U_L : N_{K/L}(U_K)] = \ell$. If $\chi_{L/F}$ annihilates $N_{K/L}(U_K)$, then it will have order ℓ on the unit group U_L. This means the order of χ_F on U_F ought to be ℓ, which is contradiction as ℓ cannot divide $|U_F/U_F^1| = q-1$ according to lemma 4.4.3 part (3). ||

Now, let us consider the following quotient

$$\frac{W(\chi_F) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu \cdot \chi_{L/F})}{W(\chi_{E/F}) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu)} \qquad (4.4f).$$

To proof (4.4*e*), it is equivalent to show that the above quotient equals one.

Because $\chi_{E/F}$ has conductor one by claim III, so does the quasi-character χ_F^ℓ. Moreover,

$$W(\chi_{E/F}) = \chi_F^\ell(\ell)\, W(\chi_F^\ell) .$$

This is a consequence of the fact that π_F^{d+1} as an element of E has order $(\ell - 1 + \ell d) + 1$ and that $U_F/U_F^1 = U_E/U_E^1$. Like $\chi_{L/F}$, every $\mu \neq 1$ is tamely ramified. Nonetheless, the quasi-character $(\mu \cdot \chi_{L/F})$ cannot be unramified; otherwise $\chi_{K/F}$ would be unramified, which implies $1 = \chi_{K/F}(U_K) = \chi_{E/F}(U_E)$, a contradiction to the claim III.

As a result, we can apply theorem 4.1.1 to rewrite the quotient $(4.4f)$ as

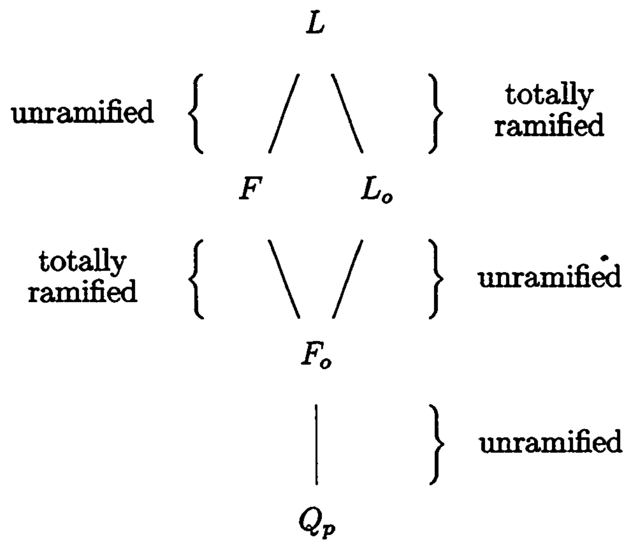
$$\frac{-\chi_F(t_F\,\pi_F^{d+1})\,G_{\mathrm{f}}\,(\chi_F^{-1})}{-\chi_F^{\ell}(t_F\,\pi_F^{d+1})\,\chi_F^{\ell}(\ell)\,G_{\mathrm{f}}\,(\chi_F^{-\ell})}\prod_{\substack{\mu\,\in\,T\\ \mu\,\neq\,1}}\frac{-(\mu\cdot\chi_{L/F})(t_L\,\pi_F^{d+1})\,G_{\mathrm{fn}}\,(\mu^{-1}\cdot\chi_{L/F}^{-1})}{-\mu(t_L\,\pi_F^{d+1})\,G_{\mathrm{fn}}\,(\mu^{-1})}\,.$$

Here d , f , n denote the order of the absolute different of F , the residue class field degree of F/Q_p and the residue class field degree $[k_K : k_F]$ respectively. Also, recall from theorem 4.4.1 that

$$\begin{aligned} t_F &= Tr_{F/F_o}\big(p/\pi_F^{d+1}\big) \\ t_L &= Tr_{L/L_o}\big(p/\pi_F^{d+1}\big)\,. \end{aligned}$$

Claim IV. *The two parameters* t_F *and* t_L *are equal.*

Proof. From the diagram



notice that L coincides with the composite FL_o and that $[F:F_o] = [L:L_o]$. Consequently every F_o - isomorphism from F into an algebraic closure of L is a restriction (to F) of some L_o - isomorphism from L into the same algebraic closure of L. It follows that

$$Tr_{F/F_o}(x) = Tr_{L/L_o}(x) \qquad \text{on } F .$$

This proves our claim. ||

Meanwhile, given $e = (\ell - 1)/\text{n}$ and $q = p^{\text{f}}$, it is a special case of the Gauss sum identity (2) in Evans [7] (with $r = 1$ and $\ell = w$, n is indeed the order of q modulo w by lemma 4.4.3) that

$$\frac{\chi_F^{-\ell}(\ell)\, G_{\mathfrak{f}}(\chi_F^{-1})}{G_{\mathfrak{f}}(\chi_F^{-\ell})} \prod_{j=1}^{e} \frac{G_{\mathfrak{f}n}(\mu^{i_j}\cdot \chi_F^{-\left(\frac{q^n-1}{q-1}\right)})}{G_{\mathfrak{f}n}(\mu^{i_j})} = 1$$

where $i_1 , \ldots , i_e$ are coset representatives for the quotient $F_\ell^\times / \langle q \rangle$.

In view of lemma 4.4.3, we can conclude that

$$\frac{\chi_F^{-\ell}(\ell)\, G_{\mathfrak{f}}(\chi_F^{-1})}{G_{\mathfrak{f}}(\chi_F^{-\ell})} \prod_{\substack{\mu \in T \\ \mu \neq 1}} \frac{G_{\mathfrak{f}n}(\mu^{-1}\cdot \chi_{L/F}^{-1})}{G_{\mathfrak{f}n}(\mu^{-1})} = 1 .$$

On the other hand, observe

$$\frac{-\chi_F(t_F\, \pi_F^{d+1})}{-\chi_F^{\ell}(t_F\, \pi_F^{d+1})} \prod_{\substack{\mu \in T \\ \mu \neq 1}} \frac{-(\mu\cdot \chi_{L/F})(t_L\, \pi_F^{d+1})}{-\mu(t_L\, \pi_F^{d+1})} = \frac{-\chi_F(t_F\, \pi_F^{d+1})}{-\chi_F^{\ell}(t_F\, \pi_F^{d+1})}\, \chi_{L/F}(t_L\, \pi_F^{d+1})^e .$$

By claim IV, this is equal to

$$\frac{-\chi_F(t_F\, \pi_F^{d+1})}{-\chi_F^{\ell}(t_F\, \pi_F^{d+1})}\, \chi_F(t_F\, \pi_F^{d+1})^{\ell-1} = 1 .$$

Therefore the quotient $(4.4f)$ must also be one, and we have established $(4.4e)$ in the case $m = 1$.

Theorem 4.4.4 (Langlands). *If K/F is tamely ramified and χ_F is a quasi-character of conductor $m > 1$, then the 3rd identity (4.4e) holds.*

Proof. We address the question of conductor first. Both $\chi_{L/F}$ and $(\mu\cdot\chi_{L/F})$ have the same conductor m. As for $\chi_{E/F}$, we have

Lemma 4.4.5. *With the assumptions in theorem 4.4.4, the conductor* m' *of* $\chi_{E/F}$ *is given by* $\ell(m-1) + 1$ *.*

Proof. Since K/E is unramified (see figure (4.4c) in lemma 4.4.3), $\chi_{K/F}$ and $\chi_{E/F}$ share the same conductor m'. By Serre [20] (chapter V, § 3, corollary 3, p.85)

$$N_{K/L}(U_K^{\ell(m-1)}) = U_L^{m-1}$$

and

$$N_{K/L}(U_K^{\ell(m-1)+1}) = U_L^{m} .$$

As L/F is unramified, this implies

$$N_{K/F}(U_K^{\ell(m-1)}) = U_F^{m-1}$$

and

$$N_{K/F}(U_K^{\ell(m-1)+1}) = U_F^{m} .$$

So $\chi_{K/F}$ annihilates $U_K^{\ell(m-1)+1}$, but

$$\chi_{K/F}(U_K^{\ell(m-1)}) = \chi_F(U_F^{m-1}) \neq \{1\} .$$

Therefore, the conductor of $\chi_{K/F}$ is equal to $\ell(m-1) + 1$. It follows $m' = \ell(m-1) + 1$. ||

Here is an immediate consequence of lemma 4.4.5.

Lemma 4.4.6. *Let* $m = \epsilon + 2\, d_{(\chi_F)}$ *and* $m' = \epsilon' + 2\, d_{(\chi_{E/F})}$ *where* $d_{(\chi_F)}$, $d_{(\chi_{E/F})}$ *are positive integers and* ϵ , ϵ' *are either zero or one.*

(i) When m *is odd,* m' *is also odd. i.e.* $\epsilon = \epsilon' = 1$. *Moreover,*

$$d_{(\chi_{E/F})} = \ell d_{(\chi_F)} .$$

(ii) When m *is even,* m' *is also even. i.e.* $\epsilon = \epsilon' = 0$. *We have*

$$d_{(\chi_{E/F})} = \ell d_{(\chi_F)} - \frac{\ell - 1}{2} .$$

The next lemma reduces the proof of (4.4*e*) to showing

$$W(\chi_{E/F}) = W(\chi_F) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu \cdot \chi_{L/F}) \qquad (4.4g).$$

Lemma. *The product* $\prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu)$ *is equal to one.*

Proof. Given a non-trivial $\mu \in T$, let $\nu \in T$ and $h \in H$ such that $\nu^h = \nu \circ h = \mu^{-1}$. Then (4.4*b*) together with part (1) of lemma 4.4.3

yield

$$W(\nu) \;=\; W(\mu^{-1}) \;=\; \mu(-1)\,\overline{W(\mu)}\ .$$

Because $\mu(-1) = \pm 1$ and the order ℓ of μ is odd by part (2) of lemma 4.4.3,

$$1 = \mu^{\ell}(-1) = \mu(-1)\ .$$

Consequently,

$$W(\mu)\,W(\nu) \;=\; 1$$

as root number of a character always have absolute value one (see for example Martinet [18] II, § 2, proposition 2.2). When $\mu \neq \nu$, the corresponding root numbers are multiplicative inverses of one another. In the case $\nu = \mu$, we have

$$W(\mu)^2 \;=\; 1\ .$$

Claim V. *If* $\mu^{-1} = \mu^{h}$ *for some* $h \in H$, *then* $W(\mu) = 1$.

Proof. By theorem 4.1.1,

$$N(P_L)^{1/2}\ W(\mu) \;=\; -\,\mu(t_L\,\pi_F^{d+1})\ G_{\mathrm{fn}}\,(\mu^{-1})$$

where d , f , n again denote the order of the absolute different of F , the residue class field degree of F/Q_p and the degree of the extension L/F . Recall that the parameter t_L defined by

$$t_L = Tr_{L/L_o}\left(\frac{p}{\pi_F^{d+1}}\right)$$

is in fact equal to

$$t_F = Tr_{F/F_o}\left(\frac{p}{\pi_F^{d+1}}\right) \in U_{F_o}$$

according to claim IV.

Let q be the cardinality of the residue class field k_F . Then

$$\sqrt{q^{\mathrm{n}}}\; W(\mu) = -\mu(t_L\, \pi_F^{d+1})\; G_{\mathrm{fn}}\,(\mu^{-1})\ .$$

Moreover,

$$\mu^{-1} = \mu^h = \mu^{q^r} \qquad \text{on } U_L$$

for some nonnegative integer $r < [k_K : k_F]$ in view of part (4) of lemma 4.4.3.

As a result,

$$\mu(t_L) = \mu(t_F) = \mu(t_F^{q^r}) = \mu^{-1}(t_F) = \mu^{-1}(t_L)$$

which means $\mu(t_L)^2 = 1$. Now because the order ℓ of μ is odd, the fact

$$\mu(t_L)^2 = 1 = \mu^{\ell}(t_L)$$

implies $\mu(t_L) = 1$.

Furthermore, part (5) of lemma 4.4.3 asserts $N_{K/L}(\pi_E) = N_{E/F}(\pi_E) = \pi_F$ (recall our choice of uniformizing parameter π_F). So μ must annihilate π_F . In summary,

$$\mu(t_L\, \pi_F^{d+1}) = 1 .$$

Therefore, we have

$$\sqrt{q^{\mathrm{n}}}\ W(\mu) = -G_{\mathrm{fn}}(\mu^{-1}) .$$

Choosing $\pi_F = N_{K/L}(\pi_E)$ also confirms that on $L^{\times}$,

$$\mu^{-1} = \mu^{h} = \mu^{q^r}$$

remains true. Consequently,

$$\mu = (\mu^{q^r})^{-1} = (\mu^{-1})^{q^r} = \mu^{q^{2r}} .$$

By (3) of lemma 4.4.3, $[k_K : k_F]$ divides $2r$. As $r < [k_K : k_F]$,

$$2r = [k_K : k_F] = \mathrm{n} .$$

It follows that

$$q^r \; W(\mu) \;\; = \;\; -\,G_{\text{fn}}\,(\mu^{-1}) \; .$$

Let ζ be a primitive p-th root of unity and ξ be a primitive ℓ-th root of unity. Then the Gauss sum $G_{\text{fn}}\,(\mu^{-1})$ is an algebraic integer in the number field $\mathbf{Q}(\zeta\,,\xi)$. Suppose $(1-\xi)$ is the ideal generated by $1-\xi$ within the ring of integer of $\mathbf{Q}(\zeta\,,\xi)$. Since

$$\mu^{-1}(x) \;\equiv\; 1 \quad mod\ (1-\xi)$$

we conclude

$$-\,G_{\text{fn}}\,(\mu^{-1}) \;\equiv\; -\,G_{\text{fn}}\,(1) \;\equiv\; -1 \quad mod\ (1-\xi) \; .$$

So

$$q^r \; W(\mu) \;\equiv\; -1 \quad mod\ (1-\xi) \; .$$

Recall that $W(\mu)^2 \; = \; 1$. In other words, $q^r \; W(\mu) \;\; = \;\; \pm\, q^r \;\; \in \;\; \mathbf{Z}$, the set of integers. Moreover, the above congruence holds even if $(1-\xi)$ is replaced by the prime ideal generated by $1-\xi$ in the ring of integer of $\mathbf{Q}(\xi)$. This means ℓ is the only prime number that divides $q^r \; W(\mu) \; + \; 1 \; \in \mathbf{Z}$. Equivalently,

$$q^r \; W(\mu) \;\equiv\; -1 \quad mod\ \ell \; .$$

Now, $W(\mu)$ cannot be -1 due to (3) of lemma 4.4.3, and we have finally proved claim V. ||

To summarize, it has been shown

$$W(\mu) = \begin{cases} 1 & \text{when } \mu^{-1} = \mu^h \text{ for some } h \in H. \\ W(\mu^{-1})^{-1} & \text{otherwise.} \end{cases}$$

Thus

$$\prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu) = 1$$

and the proof of our lemma is completed. ||

The above lemma reduces the proof of theorem 4.4.4 to verifying $(4.4g)$, which amounts to a comparision of the root numbers on the two sides in terms of various parameters that appear in the explicit evaluation of a root number given in theorem A.1, as well as in theorem A.3, of the appendix. First of all, let us express the conductor of χ_F and that of $\chi_{E/F}$ as we did in lemma 4.4.6.

$$m = \epsilon + 2\, d_{(\chi_F)}$$

and

$$m' = \epsilon' + 2\, d_{(\chi_{E/F})} .$$

By theorem A.1 (see appendix), there exists $c \in P_F^{-(d+m)}$ such that for all $x \in P_F^{\epsilon + d_{(\chi_F)}}$,

$$\chi_F(1 + x) = \psi_F(c\,x) \qquad (4.4h)$$

where ψ_F is again the canonical additive character of F. Then $c \in P_E^{-\ell(d+m)}$ or equivalently

$$c \in P_E^{-[(\ell-1+\ell d) + m']} .$$

Claim VI. *Given* c *as above, we have*

(i) $\chi_{E/F}(1 + x) = \psi_E(c\,x)$ *for all* $x \in P_E^{\epsilon' + d_{(\chi_{E/F})}}$.

(ii) $\chi_{L/F}(1 + x) = \psi_L(c\,x)$ *for all* $x \in P_L^{\epsilon + d_{(\chi_F)}}$.

Proof. Let us first suppose $x \in P_E^{\epsilon' + d_{(\chi_{E/F})}}$. Part (5) of lemma 4.4.3 implies $N_{E/F}(1+x) = N_{K/L}(1+x)$. According to Serre [20] (chapter V, § 3, lemma 5, p.83),

$$N_{K/L}(1+x) \equiv 1 + Tr_{K/L}(x) + N_{K/L}(x) \quad mod \;\; Tr_{K/L}\Big(P_K^{2[\epsilon' + d_{(\chi_{E/F})}]}\Big) .$$

Meanwhile, lemma 4.4.6 together with Serre [20] 's lemma 4 in chapter V,

§ 3 (p.83) reveal

$$Tr_{K/L}\left(P_K^{2[\epsilon' + d_{(\chi_{E/F})}]} \right) \subseteq P_L^m .$$

Therefore,

$$\begin{aligned} N_{E/F}(1 + x) &= N_{K/L}(1+x) \\ &\equiv 1 + Tr_{K/L}(x) + N_{K/L}(x) \quad mod\ P_L^m \\ &\equiv 1 + Tr_{E/F}(x) + N_{E/F}(x) \quad mod\ P_L^m \\ &\equiv 1 + Tr_{E/F}(x) + N_{E/F}(x) \quad mod\ P_F^m. \end{aligned}$$

The last congruence is true because L/F is unramified.

Notice that $N_{E/F}(x) \in P_F^{\epsilon' + d_{(\chi_{E/F})}}$. Using lemma 4.4.6 and the fact that $\ell \geq 3$, we can verify

$$\epsilon' + d_{(\chi_{E/F})} \geq m .$$

Hence

$$N_{E/F}(1 + x) \equiv 1 + Tr_{E/F}(x) \quad mod\ P_F^m .$$

In view of lemma 4.4.6 and Serre [20] 's lemma 4 in chapter V, § 3 (p.83),

$$Tr_{E/F}(x) = Tr_{K/L}(x) \in P_L^{\epsilon + d_{(\chi_F)}}.$$

As a result,

$$\chi_{E/F}(1 + x) = \chi_F(1 + Tr_{E/F}(x)) = \psi_F(c\,Tr_{E/F}(x)) = \psi_E(cx)$$

which is what we intended to establish in (i).

Next, we suppose $x \in P_L^{\epsilon + d(\chi_F)}$. Then for $i \geq 2$, the elementary symmetric function $Tr^{(i)}_{L/F}(x)$ belongs to P_L^m. So

$$\chi_{L/F}(1 + x) = \chi_F(1 + Tr_{L/F}(x)) = \psi_F(cTr_{L/F}(x)) = \psi_L(cx) .$$

This completes (ii) and claim VI. ||

Recall that χ_F and $\chi_{L/F}$ share the same conductor $m > 1$, while μ is tame. According to claim VI and part (c) of theorem A.1,

$$(\mu \cdot \chi_{L/F})(1 + x) = \psi_L(cx) \qquad \text{for } x \in P_L^{\epsilon + d(\chi_F)}$$

if c satisfies $(4.4h)$.

Now, notice $(\mu \cdot \chi_{L/F})$ also has conductor m. Due to lemma 4.4.6 and theorem A.1 part (a), our next lemma implies $(4.4g)$ when the conductor m is positive and even.

Lemma 4.4.7. *Suppose* c *satisfies* (4.4*h*) *. Then*

$$\chi_{E/F}^{-1}(c)\,\psi_E(c) \;=\; \chi_F^{-1}(c)\,\psi_F(c) \prod_{\substack{\mu \in T \\ \mu \neq 1}} (\mu \cdot \chi_{L/F})^{-1}(c)\;\psi_L(c)\;.$$

Proof. Since $c \in F^{\times}$, it follows from the diagram in lemma 4.4.3 that

$$\chi_{E/F}^{-1}(c)\,\psi_E(c) \;=\; \left[\chi_F^{-1}(c)\,\psi_F(c)\right]^{\ell}$$

and

$$\prod_{\substack{\mu \in T \\ \mu \neq 1}} (\mu \cdot \chi_{L/F})^{-1}(c)\;\psi_L(c) \;=\; [\,\chi_F^{-1}(c)\,\psi_F(c)\,]^{\ell-1} \prod_{\substack{\mu \in T \\ \mu \neq 1}} \mu^{-1}(c)\;.$$

So it remains to prove

$$\prod_{\substack{\mu \in T \\ \mu \neq 1}} \mu^{-1}(c) \;=\; 1\;.$$

Let us define $\alpha \in U_F$ by

$$c \;=\; \frac{\alpha}{\pi_F^{d+m}}\;.$$

Since ℓ is an odd prime,

$$1 = \prod_{\mu \in C^*} \mu^{-1}(\alpha)$$

which is equal to

$$\prod_{\substack{\mu \in T \\ \mu \neq 1}} \mu^{-1}(\alpha)^{|H|} \;=\; \Big[\prod_{\substack{\mu \in T \\ \mu \neq 1}} \mu^{-1}(\alpha)\Big]^{|H|}$$

because all $|H|$ characters in each H-orbit share the same value at $\alpha \in U_F$ by (4) of lemma 4.4.3.

In other words,

$$\Big[\prod_{\substack{\mu \in T \\ \mu \neq 1}} \mu^{-1}(\alpha) \Big]^{|H|} = 1 = \Big[\prod_{\substack{\mu \in T \\ \mu \neq 1}} \mu^{-1}(\alpha) \Big]^{\ell}$$

(the second equality follows from the fact $\mu^{\ell} = 1$). However, the exponents $|H|$ and ℓ are relatively prime (see (2) of lemma 4.4.3). Consequently, we see that

$$\prod_{\substack{\mu \in T \\ \mu \neq 1}} \mu^{-1}(\alpha) = 1 \ .$$

On the other hand, it has already been observed

$$\mu(\pi_F) = \mu(\, N_{E/F}(\pi_E)\,) = \mu(\, N_{K/L}(\pi_E)\,) = 1 \ .$$

Therefore we arrive at

$$\prod_{\substack{\mu \in T \\ \mu \neq 1}} \mu^{-1}(c) = \prod_{\substack{\mu \in T \\ \mu \neq 1}} \mu^{-1}\left(\frac{\alpha}{\pi_F^{d+m}} \right) = 1$$

and lemma 4.4.7 is proved. ||

Let us proceed to prove (4.4g) when m is odd and greater than one. Lemma 4.4.6 said $\chi_{E/F}$ has odd conductor, given m odd. The conductor of $(\mu \cdot \chi_{L/F})$ coincides with m. So it is odd. This means theorem A.1 part (b) applies to all the root numbers that appear in $(4.4g)$. With lemma 4.4.7 established, we can complete the proof of $(4.4g)$ and hence theorem 4.4.4 by

Theorem 4.4.8. *For m odd and greater than one, let $\delta = (\pi_F)^{d(\chi_F)}$. If c satisfies $(4.4h)$, then*

$$N(P_E)^{-1/2} \sum_{O_E/P_E} \chi_{E/F}^{-1}(1 + \delta x)\, \psi_E(c\,\delta\,x)$$

is equal to the product between

$$N(P_F)^{-1/2} \sum_{O_F/P_F} \chi_F^{-1}(1 + \delta x)\; \psi_F(c\,\delta\,x)$$

and

$$\prod_{\substack{\mu \in T \\ \mu \neq 1}} \left[N(P_L)^{-1/2} \sum_{O_L/P_L} (\mu \cdot \chi_{L/F})^{-1}(1 + \delta x)\; \psi_L(c\,\delta\,x) \right] .$$

Proof. Suppose $\eta \in O_F$ satisfies

$$\psi_F(c\,\delta^2\,x)^{-1} = \exp\left(\frac{2\pi i}{p}\, Tr_{k_F/F_p}(\eta\,x) \right) \qquad \text{for all } x \in O_F \qquad (4.4i).$$

First of all, we are going determine the counterpart of this η parameter for the additive characters ψ_E and ψ_L. Restricted to O_F, the function $\psi_E(c\,\delta^2\,x)^{-1}$ is equal to

$$\psi_F(c\,\delta^2\,\ell\,x)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\;Tr_{k_F/F_p}(\eta\,\ell\,x)\right)\,.$$

Since $\psi_E(c\,\delta^2\,x)$ can be interpreted as a function on O_E/P_E and the inclusion $O_F \hookrightarrow O_E$ induces an isomorphism from O_F/P_F onto O_E/P_E, we conclude

$$\psi_E(c\,\delta^2\,x)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\;Tr_{k_E/F_p}(\eta\,\ell\,x)\right) \qquad (4.4j)$$

holds for all $x \in O_E$.

On the other hand, given $x \in O_L$,

$$\psi_L(c\,\delta^2\,x)^{-1} \;=\; \psi_F(\,c\,\delta^2\,Tr_{L/F}(x)\,)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\;Tr_{k_F/F_p}(\,\eta\,Tr_{L/F}(x)\,)\right)\,.$$

As L/F is unramified, we obtain

$$\psi_L(c\,\delta^2\,x)^{-1} \;=\; \exp\left(\frac{2\pi i}{p}\;Tr_{k_L/F_p}(\eta\,x)\right) \qquad (4.4k).$$

Next, we compare γ parameters for χ_F , $\chi_{E/F}$ and $(\mu\cdot\chi_{L/F})$. According to theorem A.3, the argument will depend on the parity of the residue class field characteristic p.

Assume p is odd. Then there exists $\gamma \in O_{F_o}$ so that

$$\chi_F^{-1}(1 + \delta x)\,\psi_F(c\,\delta\,x) \;=\; \psi_F\Big(c\,\delta^2\Big(\frac{x^2}{2} + \gamma x\Big)\Big) \qquad \text{for all } x \in O_F \tag{4.4l}$$

by part (a) of theorem A.3.

Because of lemma 4.4.3 part (5), we have $N_{E/F}(1 + \delta x) = N_{K/L}(1 + \delta x)$ given $x \in O_E$, and

$$N_{K/L}(1 + \delta x) \;\equiv\; 1 + \delta\, Tr_{K/L}(x) + \delta^2\, Tr^{(2)}_{K/L}(x) \quad mod\, P_L^m$$

$$\equiv\; (1 + \delta Tr_{K/L}(x))(1 + \delta^2 Tr^{(2)}_{K/L}(x)) \quad mod\, P_L^m.$$

Recall L/F is unramified. It follows

$$N_{E/F}(1 + \delta x) \;\equiv\; (1 + \delta Tr_{E/F}(x))(1 + \delta^2 Tr^{(2)}_{E/F}(x)) \quad mod\, P_F^m.$$

Therefore, $\chi_{E/F}^{-1}(1 + \delta x)\,\psi_E(c\,\delta\,x)$ is equal to

$$\chi_F^{-1}(1 + \delta Tr_{E/F}(x))\;\chi_F^{-1}(1 + \delta^2 Tr^{(2)}_{E/F}(x))\;\psi_F(c\,\delta\, Tr_{E/F}(x))$$

on O_E. Now (4.4l) implies

$$\chi_{E/F}^{-1}(1 + \delta x)\,\psi_E(c\,\delta\,x)$$

$$= \psi_F\Big(c\,\delta^2 \Big(\frac{Tr_{E/F}(x)^2}{2} + \gamma\, Tr_{E/F}(x) \Big) \Big)\ \chi_F^{-1}(\,1 + \delta^2 Tr^{(2)}_{E/F}(x)\,)$$

$$= \psi_F\Big(c\,\delta^2 \Big(\frac{Tr_{E/F}(x)^2}{2} + \gamma\, Tr_{E/F}(x) \Big) \Big)\ \psi_F(\,c\,\delta^2\, Tr^{(2)}_{E/F}(x)\,)^{-1}$$

$$= \psi_F\Big(c\,\delta^2 \Big(\frac{Tr_{E/F}(x)^2 - 2\,Tr^{(2)}_{E/F}(x)}{2} + \gamma\, Tr_{E/F}(x) \Big) \Big)$$

$$= \psi_F\Big(c\,\delta^2 \Big(\frac{Tr_{E/F}(x^2)}{2} + \gamma\, Tr_{E/F}(x) \Big) \Big)\ .$$

Here we have used theorem A.1 part (b) as well as the fact

$$Tr_{E/F}(x)^2 = Tr_{E/F}(x^2) + 2\,Tr^{(2)}_{E/F}(x)\ .$$

In summary, for $x \in O_E$,

$$\chi^{-1}_{E/F}(1 + \delta x)\,\psi_E(c\,\delta\, x) = \psi_E\Big(c\,\delta^2 \Big(\frac{x^2}{2} + \gamma x \Big) \Big)\ .$$

Similarly, because

$$N_{L/F}(1 + \delta x) \equiv (\,1 + \delta Tr_{L/F}(x)\,)(\,1 + \delta^2 Tr^{(2)}_{L/F}(x)\,) \quad mod\ P_F^m$$

holds on O_L , it is possible to conclude

$$\chi^{-1}_{L/F}(1 + \delta x)\,\psi_L(c\,\delta\, x) = \psi_L\Big(c\,\delta^2 \Big(\frac{x^2}{2} + \gamma x \Big) \Big) \qquad \text{for } x \in O_L$$

by means of (4.4l) and theorem A.1 part (b) .

Since K/L is tamely ramified, all non-trivial μ have conductor one. This implies

$$(\mu\cdot\chi_{L/F})^{-1}(1+\delta x)\,\psi_L(c\,\delta\,x) \;=\; \psi_L\Big(c\,\delta^2\Big(\frac{x^2}{2}+\gamma x\Big)\Big) \qquad \text{for } x \in O_L\ .$$

Now we are in the position to complete the proof of theorem 4.4.8 when p is odd. The notations below are consistent with that of theorem A.3.

Lemma 4.4.9. *Given* p *odd, if* η , γ *are defined by* (4.4*i*) *and* (4.4*l*) *respectively, then*

$$\psi_E\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\ell\eta}{P_E}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}$$

is equal to the product between

$$\psi_F\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\eta}{P_F}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}$$

and

$$\prod_{\substack{\mu\,\in\,T\\ \mu\,\neq\,1}}\psi_L\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\eta}{P_L}\right)(-1)^{\mathrm{fn}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{fn}}$$

where f , n denote the residue class field degrees $[k_F : F_p]$ and $[k_K : k_F]$.

Proof. Because E/F is totally ramified, $k_E = k_F$. It follows

$$\frac{\psi_E\big(c\,\delta^2\,\frac{\gamma^2}{2}\big)^{-1}\left(\frac{-2\ell\eta}{P_E}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}}{\psi_F\big(c\,\delta^2\,\frac{\gamma^2}{2}\big)^{-1}\left(\frac{-2\eta}{P_F}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}} \;=\; \psi_F\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{1-\ell}\left(\frac{\ell}{P_F}\right)$$

Moreover, we observe

$$\left(\frac{\ell}{P_F}\right) = \left(\frac{\ell}{p}\right)^{\mathrm{f}} .$$

Hence

$$\frac{\psi_E(c\,\delta^2 \frac{\gamma^2}{2})^{-1}\left(\frac{-2\ell\eta}{P_E}\right)\,(-1)^{\mathrm{f}\text{-}1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}}{\psi_F(c\,\delta^2 \frac{\gamma^2}{2})^{-1}\left(\frac{-2\eta}{P_F}\right)\,(-1)^{\mathrm{f}\text{-}1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{f}}} = \psi_F\Big(c\,\delta^2 \frac{\gamma^2}{2}\Big)^{1-\ell}\left(\frac{\ell}{p}\right)^{\mathrm{f}} .$$

On the other hand, we have

$$\left(\frac{-2\,\eta}{P_L}\right) = \left(\frac{-2\,\eta}{P_F}\right)^{\mathrm{n}} .$$

By lemma 4.4.3 part (2)

$$\prod_{\substack{\mu\,\in\,T\\ \mu\,\neq\,1}} \psi_L\Big(c\,\delta^2 \frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\eta}{P_L}\right)\,(-1)^{\mathrm{fn}\text{-}1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{fn}}$$

$$= \left[\psi_L\Big(c\,\delta^2 \frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\eta}{P_F}\right)^{\mathrm{n}}(-1)^{\mathrm{fn}\text{-}1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\right)^{\mathrm{fn}}\right]^{(\ell-1)/\mathrm{n}}$$

$$= \psi_F\Big(c\,\delta^2 \frac{\gamma^2}{2}\Big)^{1-\ell}(-1)^{(\ell-1)/\mathrm{n}}\left[(-1)^{(\frac{p-1}{2})(\frac{\ell-1}{2})}\right]^{\mathrm{f}} .$$

From the quadratic reciprocity law,

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

Therefore, theorem 4.4.9 is proved once we show that

$$1 = (-1)^{(\ell-1)/\mathrm{n}}\left(\frac{p}{\ell}\right)^{\mathrm{f}}$$

or equivalently

$$(-1)^{(\ell-1)/\mathrm{n}} = \left(\frac{q}{\ell}\right)$$

where q is the cardinality of the residue class field k_F.

Recall the following property of the Legendre symbol

$$\left(\frac{q}{\ell}\right) \equiv q^{\frac{\ell-1}{2}} \quad mod\ \ell\ .$$

This means $\left(\frac{q}{\ell}\right) = 1$ if and only if the order of q modulo ℓ divides $(\ell-1)/2$. However, the order of q modulo ℓ is precisely $[k_K : k_F] = \mathrm{n}$ according to lemma 4.4.3 part (3), and n divides $(\ell-1)/2$ if and only if $(\ell-1)/\mathrm{n}$ is even. So indeed we have $(-1)^{(\ell-1)/\mathrm{n}} = \left(\frac{q}{\ell}\right)$. Lemma 4.4.9 is now established. ||

Comparing theorem A.1 part (*b*) with theorem A.3 part (*a*), we see that lemma 4.4.9 is in fact identical to theorem 4.4.8 when p is odd. So it remains to prove theorem 4.4.8 when $p = 2$.

Let us return to the γ parameters for χ_F , $\chi_{E/F}$ and $(\mu \cdot \chi_{L/F})$ in the case $p = 2$. By theorem A.3 part (b), there exists $\gamma \in O_{F_o}$ satisfying

$$\chi_F^{-1}(1 + \beta\delta x)\,\psi_F(c\,\beta\delta\,x) = i^{Tr_{k_F/F_p}(x)}\,(-1)^{Tr^{(2)}_{k_F/F_p}(x) + Tr_{k_F/F_p}(\gamma x)} \tag{4.4m}$$

on O_F. Remember $\beta \in O_F$ and $\beta^2 \equiv \eta^{-1} \;\; mod \; P_F$.

Claim VII. *As* ℓ *is not the residue class field characteristic* $p = 2$, *we have*

$$\beta^2 \equiv \eta^{-1} \equiv (\ell\eta)^{-1} \;\; mod \; P_F \,.$$

If γ *satisfies* (4.4m), *then*

(i) $\chi_{E/F}^{-1}(1 + \beta\delta x)\,\psi_E(c\,\beta\,\delta\,x)$

$$= i^{Tr_{k_E/F_p}(x)}\,(-1)^{Tr^{(2)}_{k_E/F_p}(x) + Tr_{k_E/F_p}[\,(\gamma + \frac{\ell-1}{2})\,x\,]} \qquad \text{for } x \in O_E \,.$$

(ii) $\chi_{L/F}^{-1}(1 + \beta\delta x)\,\psi_L(c\,\beta\delta\,x)$

$$= i^{Tr_{k_L/F_p}(x)}\,(-1)^{Tr^{(2)}_{k_L/F_p}(x) + Tr_{k_L/F_p}(\gamma x)} \qquad \text{for } x \in O_L \,.$$

Proof. The congruence

$$\beta^2 \equiv \eta^{-1} \equiv (\ell\eta)^{-1} \;\; mod \; P_F$$

is true because $\ell \equiv 1 \mod 2$ implies

$$\ell^{-1} \equiv 1 \mod P_F \qquad (4.4n).$$

The rest of the proof parallels our previous argument for the γ parameter of $\chi_{E/F}$ in the case p is odd. Since

$$N_{E/F}(1+\beta\delta x) = (1 + \beta\delta\, Tr_{E/F}(x))(1 + (\ell\eta)^{-1}\delta^2\, Tr^{(2)}_{E/F}(x)) \mod P_F^m$$

we can write $\chi^{-1}_{E/F}(1 + \beta\delta x)\,\psi_E(c\,\beta\delta x)$ as

$$\chi_F^{-1}(1 + \beta\delta\, Tr_{E/F}(x))\,\chi_F^{-1}(1 + (\ell\eta)^{-1}\delta^2\, Tr^{(2)}_{E/F}(x))\,\psi_F(c\,\beta\,\delta\, Tr_{E/F}(x))$$

which is equal to

$$\chi_F^{-1}(1 + \beta\delta\, Tr_{E/F}(x))\ \psi_F(c\,\beta\,\delta\, Tr_{E/F}(x))\ \psi_F(c\,(\ell\eta)^{-1}\delta^2\, Tr^{(2)}_{E/F}(x))^{-1}\ .$$

It follows from $(4.4j)$ and $(4.4m)$ that $\chi^{-1}_{E/F}(1 + \beta\delta x)\,\psi_E(c\,\beta\delta x) =$

$$i^{Tr_{k_F/F_p}(Tr_{E/F}(x))}\,(-1)^{Tr^{(2)}_{k_F/F_p}(Tr_{E/F}(x)) + Tr_{k_F/F_p}(\gamma\, Tr_{E/F}(x)) + Tr_{k_F/F_p}(Tr^{(2)}_{E/F}(x))}\ .$$

If $x \in O_F$, then $Tr_{E/F}(x) = \ell x$ and $Tr^{(2)}_{E/F}(x) = \frac{\ell(\ell-1)}{2}x^2$. Because of $(4.4n)$ as well as the fact that $Tr_{k_F/F_p}(x^2) = Tr_{k_F/F_p}(x)$,

$$\chi^{-1}_{E/F}(1 + \beta\delta x)\,\psi_E(c\,\beta\delta x)$$

$$= \; i^{Tr_{k_F/F_p}(x)} \, (-1)^{Tr^{(2)}_{k_F/F_p}(x) + Tr_{k_F/F_p}(\gamma\, x) + Tr_{k_F/F_p}(\frac{\ell-1}{2}\, x)} \; .$$

On the other hand, $\chi^{-1}_{E/F}(1 + \beta\,\delta\,x)\,\psi_E(c\,\beta\,\delta\,x)$ is a function on O_E/P_E by theorem A.1 part (b), and the inclusion $O_F \hookrightarrow O_E$ induces an isomorphism from O_F/P_F onto O_E/P_E. In particular $k_F = k_E$. Therefore,

$$\chi^{-1}_{E/F}(1 + \beta\,\delta\,x)\,\psi_E(c\,\beta\,\delta\,x) \;=\; i^{Tr_{k_E/F_p}(x)} \, (-1)^{Tr^{(2)}_{k_E/F_p}(x) + Tr_{k_E/F_p}\left[\,(\gamma + \frac{\ell-1}{2})\,x\,\right]}$$

and we arrive at part (i) of claim VII.

In contrast, the γ parameter for $\chi_{L/F}$ coincides with the γ parameter for χ_F even if $p = 2$. Specifically, given $x \in O_L$

$$\chi^{-1}_{L/F}(1 \,+\, \beta\,\delta\,x)\,\psi_L(c\,\beta\,\delta\,x)$$

$$= \; \chi^{-1}_F(\,1 \,+\, \beta\delta Tr_{L/F}(x)\,)\,\chi^{-1}_F(\,1 \,+\, \eta^{-1}\delta^2 Tr^{(2)}_{L/F}(x)\,)\,\psi_F(\,c\,\beta\,\delta\,Tr_{L/F}(x)\,)$$

$$= \; \chi^{-1}_F(\,1 \,+\, \beta\delta Tr_{L/F}(x)\,)\,\psi_F(\,c\,\beta\,\delta\,Tr_{L/F}(x)\,)\,\psi_F(\,c\,\eta^{-1}\,\delta^2\,Tr^{(2)}_{L/F}(x)\,)^{-1} \; .$$

By $(4.4k)$ and $(4.4m)$, this is equal to

$$i^{Tr_{k_F/F_p}(\,Tr_{L/F}(x)\,)} \, (-1)^{Tr^{(2)}_{k_F/F_p}(\,Tr_{L/F}(x)\,) + Tr_{k_F/F_p}(\,\gamma\, Tr_{L/F}(x)\,) + Tr_{k_F/F_p}(\,Tr^{(2)}_{L/F}(x)\,)} \; .$$

Recall from $(4.4c)$ that L/F is unramified. So we have

$$\chi^{-1}_{L/F}(1 \,+\, \beta\,\delta\,x)\,\psi_L(c\,\beta\,\delta\,x)$$

$$= i^{Tr_{k_L/F_p}(x)} (-1)^{Tr^{(2)}_{k_F/F_p}(Tr_{k_L/k_F}(x)) + Tr_{k_L/F_p}(\gamma x) + Tr_{k_F/F_p}(Tr^{(2)}_{k_L/k_F}(x))} .$$

As the 2nd elementary symmetric function satisfies the following transitivity property

$$Tr^{(2)}_{k_L/F_p}(x) = Tr^{(2)}_{k_F/F_p}(Tr_{k_L/k_F}(x)) + Tr_{k_F/F_p}(Tr^{(2)}_{k_L/k_F}(x)) \tag{4.4o}$$

we obtain

$$\chi^{-1}_{L/F}(1 + \beta\delta x)\, \psi_L(c\,\beta\,\delta\,x) = i^{Tr_{k_L/F_p}(x)} (-1)^{Tr^{(2)}_{k_L/F_p}(x) + Tr_{k_L/F_p}(\gamma x)} .$$

This concludes claim VII. ||

Since $\mu(U^1_L) = \{1\}$, part (ii) of the above claim yields

$$(\mu\cdot\chi_{L/F})^{-1}(1 + \beta\,\delta\,x)\, \psi_L(c\,\beta\,\delta\,x) = i^{Tr_{k_L/F_p}(x)} (-1)^{Tr^{(2)}_{k_L/F_p}(x) + Tr_{k_L/F_p}(\gamma x)} .$$

Now we proceed to complete the proof of theorem 4.4.8 in the case $p = 2$. By comparing theorem A.1 part (b) with theorem A.3 part(b), we conclude that it is sufficient to prove the following lemma.

Lemma 4.4.10. *Suppose* m *is odd and greater than one. Choose* γ *so that*

(4.4*m*) *holds. If* $p = 2$, *then*

$$\left[i^{Tr_{k_E/F_p}\left(\gamma + \frac{\ell-1}{2}\right)} (-1)^{Tr^{(2)}_{k_E/F_p}\left(\gamma + \frac{\ell-1}{2}\right)} \right]^{-1} \left(\frac{1+i}{\sqrt{2}}\right)^{\mathrm{f}} (-1)^{\mathrm{f}-1}$$

is equal to the product between

$$\left[i^{Tr_{k_F/F_p}(\gamma)} (-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)} \right]^{-1} \left(\frac{1+i}{\sqrt{2}}\right)^{\mathrm{f}} (-1)^{\mathrm{f}-1}$$

and

$$\prod_{\substack{\mu \in T \\ \mu \neq 1}} \left[i^{Tr_{k_L/F_p}(\gamma)} (-1)^{Tr^{(2)}_{k_L/F_p}(\gamma)} \right]^{-1} \left(\frac{1+i}{\sqrt{2}}\right)^{\mathrm{fn}} (-1)^{\mathrm{fn}-1} .$$

Again f , n *here denote* $[k_F : F_p]$ *and* $[k_K : k_F]$.

Proof. First of all, let us define a function Δ_o on the set of integers by

$$\Delta_o(x) = \begin{cases} 1 & \text{when } x \text{ is even} \\ i & \text{when } x \text{ is odd} \end{cases} \qquad (4.4p).$$

One immediate observation from this definition is that $\Delta_o(x)$ is not additive. In fact,

$$\Delta_o(x + y) = \Delta_o(x)\, \Delta_o(y)\, (-1)^{xy} \qquad (4.4q).$$

Also, notice Δ_o can be interpreted as a function on the finite field with two elements. Thus, we can identify $i^{Tr_{k_F/F_p}(x)}$ with $\Delta_o(Tr_{k_F/F_p}(x))$, and

(4.4q) implies

$$i^{Tr_{k_F/F_p}(x+y)} = i^{Tr_{k_F/F_p}(x)}\, i^{Tr_{k_F/F_p}(y)}\, (-1)^{Tr_{k_F/F_p}(x) Tr_{k_F/F_p}(y)} .$$

Next, we point out that it is possible to expand the 2nd elementary symmetric function of a sum.

$$\begin{aligned} Tr^{(2)}_{k_E/F_p}\Big(\gamma + \frac{\ell-1}{2}\Big) &= Tr^{(2)}_{k_E/F_p}(\gamma) + Tr^{(2)}_{k_E/F_p}\Big(\frac{\ell-1}{2}\Big) \\ &+ Tr_{k_E/F_p}(\gamma)\, Tr_{k_E/F_p}\Big(\frac{\ell-1}{2}\Big) \\ &- Tr_{k_E/F_p}\Big[\gamma\Big(\frac{\ell-1}{2}\Big)\Big] . \end{aligned}$$

Together with $k_E = k_F$, it follows that the quotient

$$\frac{\Big[i^{Tr_{k_E/F_p}\left(\gamma+\frac{\ell-1}{2}\right)}\,(-1)^{Tr^{(2)}_{k_E/F_p}\left(\gamma+\frac{\ell-1}{2}\right)}\Big]^{-1}\left(\frac{1+i}{\sqrt{2}}\right)^{\mathrm{f}}(-1)^{\mathrm{f}-1}}{\Big[i^{Tr_{k_F/F_p}(\gamma)}\,(-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)}\Big]^{-1}\left(\frac{1+i}{\sqrt{2}}\right)^{\mathrm{f}}(-1)^{\mathrm{f}-1}}$$

is equal to

$$\left\{ i^{Tr_{k_F/F_p}\left(\frac{\ell-1}{2}\right)}\,(-1)^{Tr^{(2)}_{k_F/F_p}\left(\frac{\ell-1}{2}\right)}\,(-1)^{Tr_{k_F/F_p}\left[\gamma\left(\frac{\ell-1}{2}\right)\right]} \right\}^{-1} .$$

On the other hand, because of (4.4o) and theorem A.3 part (c),

$$i^{Tr_{k_L/F_p}(\gamma)}\,(-1)^{Tr^{(2)}_{k_L/F_p}(\gamma)} = \Big[i^{Tr_{k_F/F_p}(\gamma)}\,(-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)}\Big]^{\mathrm{n}} .$$

As a result,

$$\prod_{\substack{\mu \in T \\ \mu \neq 1}} \left[i^{Tr_{k_L/F_p}(\gamma)} (-1)^{Tr^{(2)}_{k_L/F_p}(\gamma)} \right]^{-1} \left(\frac{1+i}{\sqrt{2}} \right)^{\text{fn}} (-1)^{\text{fn-1}}$$

$$= \left[i^{Tr_{k_F/F_p}(\gamma)} (-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)} \right]^{1-\ell} \left(\frac{1+i}{\sqrt{2}} \right)^{\text{f}(\ell\text{-1})} (-1)^{\frac{\ell\text{-1}}{\text{n}}}$$

by lemma 4.4.3 part (b).

Therefore, we must prove

$$\left\{ i^{Tr_{k_F/F_p}\left(\frac{\ell-1}{2}\right)} (-1)^{Tr^{(2)}_{k_F/F_p}\left(\frac{\ell-1}{2}\right)} (-1)^{Tr_{k_F/F_p}\left[\gamma\left(\frac{\ell-1}{2}\right)\right]} \right\}^{-1}$$

$$= \left[i^{Tr_{k_F/F_p}(\gamma)} (-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)} \right]^{1-\ell} \left(\frac{1+i}{\sqrt{2}} \right)^{\text{f}(\ell\text{-1})} (-1)^{\frac{\ell\text{-1}}{\text{n}}}$$

(4.4r).

With (4.4n), theorem A.3 part (c) asserts that

$$\left[i^{Tr_{k_F/F_p}(\gamma)} (-1)^{Tr^{(2)}_{k_F/F_p}(\gamma)} \right]^{1-\ell} = (-1)^{Tr_{k_F/F_p}\left[\left(\frac{(\ell-1)(\ell-2)}{2}\right)\gamma^2\right]}$$

$$= (-1)^{Tr_{k_F/F_p}\left[\left(\frac{\ell-1}{2}\right)\gamma^2\right]} .$$

The last equality is due to the congruence $\ell - 2 \equiv 1 \; mod \; P_F$.

Because the Frobenius automorphism in $Gal(k_F/F_p)$ sends γ to γ^2 , we see that (4.4r) is equivalent to

$$\left\{ i^{Tr_{k_F/F_p}\left(\frac{\ell-1}{2}\right)} (-1)^{Tr^{(2)}_{k_F/F_p}\left(\frac{\ell-1}{2}\right)} \right\}^{-1} = \left(\frac{1+i}{\sqrt{2}} \right)^{\text{f}(\ell\text{-1})} (-1)^{\frac{\ell\text{-1}}{\text{n}}}$$

(4.4s).

Claim VIII. *Suppose the function* Δ_o *is defined as in* (4.4p) . *Then*

$$i^{Tr_{k_F/F_p}\left(\frac{\ell-1}{2}\right)}\,(-1)^{Tr^{(2)}_{k_F/F_p}\left(\frac{\ell-1}{2}\right)} \;=\; \Delta_o\Big(\frac{\ell-1}{2}\Big)^{f}\,.$$

Proof. Let us prove a more general result below, from which our claim follows. Given any integer $z \geq 1$,

$$\Delta_o(zx)\;(-1)^{\left(\frac{z(z-1)}{2}\right)x^2} \;=\; \Delta_o(x)^z \qquad \text{for } x \in \mathbf{Z}$$

(4.4t).

When $z = 1$, the above equality is immediate. For $z > 1$, we use induction on z.

$$\Delta_o(x)^{z+1} \;=\; \Delta_o(x)\;(\Delta_o(x))^z \;=\; \Delta_o(x)\;\Delta_o(zx)\;(-1)^{\left(\frac{z(z-1)}{2}\right)x^2}$$

by the induction hypothesis. According to (4.4q) ,

$$\Delta_o(x+zx) \;=\; \Delta_o(x)\;\Delta_o(zx)\;(-1)^{(zx^2)}\,.$$

So

$$\Delta_o(x)^{z+1} \;=\; \Delta_o(x+zx)\;(-1)^{(zx^2)}\;(-1)^{\left(\frac{z(z-1)}{2}\right)x^2}$$

$$= \Delta_o(\,(z + 1)x\,)\ (-1)^{\left(\frac{z(z+1)}{2}\right)x^2}$$

completes the induction proof. Now, because

$$Tr_{k_F/F_p}\Big(\frac{\ell-1}{2}\Big) \equiv \mathrm{f}\Big(\frac{\ell-1}{2}\Big) \quad mod\ 2$$

and

$$Tr^{(2)}_{k_F/F_p}\Big(\frac{\ell-1}{2}\Big) \equiv \frac{\mathrm{f}\,(\mathrm{f}-1)}{2}\Big(\frac{\ell-1}{2}\Big)^2 \quad mod\ 2$$

our claim follows from (4.4t) with $z = \mathrm{f}$ and $x = (\ell-1)/2$. ||

By inspection, $\Delta_o\big(\frac{\ell-1}{2}\big)\,\big(\frac{1+i}{\sqrt{2}}\big)^{\ell-1}$ is equal to

$$\Delta_o\Big(\frac{\ell-1}{2}\Big)\ \big(i\big)^{\frac{\ell-1}{2}} = \begin{cases} 1 & \text{when } \ell \equiv \pm 1 \ mod\ 8 \\ -1 & \text{when } \ell \equiv \pm 3 \ mod\ 8 \end{cases}$$

which coincides with the Legendre symbol $\left(\frac{2}{\ell}\right)$.

This means

$$\Delta_o\Big(\frac{\ell-1}{2}\Big)^{\mathrm{f}}\ \Big(\frac{1+i}{\sqrt{2}}\Big)^{\mathrm{f}(\ell-1)} = \left(\frac{2}{\ell}\right)^{\mathrm{f}} = \left(\frac{q}{\ell}\right)$$

where q is the cardinality of the residue class field k_F.

Recall the Legendre symbol satisfies the congruence

$$\left(\frac{q}{\ell}\right) \equiv q^{\frac{\ell-1}{2}} \quad mod\ \ell\ .$$

In other words, $\left(\frac{q}{\ell}\right) = 1$ if and only if the order of q modulo ℓ divides $\frac{\ell-1}{2}$. However, according to lemma 4.4.3 part (c), the order of q modulo ℓ is exactly n, and n divides $\frac{\ell-1}{2}$ if and only if $\frac{\ell-1}{\mathrm{n}}$ is even due to lemma 4.4.3 part (b).

To summarize

$$\Delta_o\left(\frac{\ell-1}{2}\right)^{\mathrm{f}}\left(\frac{1+i}{2}\right)^{\mathrm{f}(\ell-1)} = (-1)^{\frac{\ell-1}{\mathrm{n}}}\ .$$

By claim VIII, this is identical to $(4.4s)$, which is equivalent to $(4.4r)$. Therefore lemma 4.4.10 is proved. ||

As we have already pointed out, because of theorem A.1 part (b) and theorem A.3, the above lemma together with lemma 4.4.9 complete the proof of theorem 4.4.8. ||

By combining lemma 4.4.7 and theorem 4.4.8, we have successfully verified $(4.4g)$. Hence $(4.4e)$ follows in the case χ_F has conductor $m > 1$, and theorem 4.4.4 is established. ||

Now, we see that (4.4e) holds not only for m zero and one but also for $m > 1$. This completes our discussion of the 3rd identity when K/F is tamely ramified.

Our proof of the 3rd identity for the tame case is a modification of chapter 13 in Langlands' manuscript [16]. When K/F is wildly ramified, Langlands' proof of this identity depends on the induction hypothesis of his theorem 2.1 in the manuscript (see chapter 14 in [16]). So the verification of the fundamental root number identities is in fact one part of the long induction that establishes the existence of local root number. According to chapter 14 in [16], four lemmas constitute the argument for the wild case. After proving the identity when the conductor m of χ_F is less than or equal to one, Langlands considers the quotient ρ between the two sides of the 3rd identity and shows that ρ is simultaneously an n-th root of unity and an ℓ-th root of unity where n and ℓ are relatively prime. His method is sensitive to the size of m as well as the parity of both m and u. (Recall from theorem 4.4.1 that u denotes the length of the ramification group filtration of $Gal(K/F)$.)

A Appendix: Dwork - Lamprecht Theory

This appendix serves as a reference to the Dwork - Lamprecht theory necessary to discuss the proof of the fundamental identities. All the results here can be developed without the previous chapters. As usual, if F is a finite extension of Q_p, then O_F , P_F , U_F , k_F , d , $N(P_F)$, π_F denote its ring of integer, the maximal ideal in its ring of integer, the unit group of its ring of integer, its residue class field, the order of its absolute different, the cardinality of its residue class field and a uniformizing parameter of F respectively. Moreover, $\psi_F = e^{2\pi i\,(\lambda \circ Tr_{F/Q_p})}$ is the canonical additive character of F. Here λ is defined on Q_p so that (i) $\lambda(x)$ is always a rational with a power of p as denominator and (ii) $x - \lambda(x)$ must be a p-adic integer.

By a quasi-character on $F^\times$ we mean a continuous homomorphism from the multiplicative group of F to the group of nonzero complex numbers.

Theorem A.1. *Let* χ_F *be a quasi-character on* $F^\times$ *with root number*[1]

[1]The definition of $W(\chi_F)$ for quasi-character χ_F coincides with the formula given in the introduction.

$W(\chi_F)$. *Suppose its conductor* $m = m(\chi_F)$ *is greater than one.*

(a) If m *is even, i.e.* $m = 2 \cdot d_{(\chi_F)}$ *for some integer* $d_{(\chi_F)} > 0$, *then there exists* $c \in P_F^{-(d+m)}$ *such that*

$$\psi_F(c\,x) = \chi_F(1 + x) \qquad \text{for } x \in P_F^{d_{(\chi_F)}} .$$

Moreover, for any such c, *we have*

$$W(\chi_F) = \chi_F^{-1}(c)\,\psi_F(c) .$$

(b) If m *is odd, i.e.* $m = 1 + 2 \cdot d_{(\chi_F)}$ *for some integer* $d_{(\chi_F)} > 0$, *then there exists* $c \in P_F^{-(d+m)}$ *such that*

$$\psi_F(c\,x) = \chi_F(1 + x) \qquad \text{for } x \in P_F^{1+d_{(\chi_F)}} .$$

For any such c *and any* $\delta \in P_F^{d_{(\chi_F)}}$,

$$W(\chi_F) = \chi_F^{-1}(c)\;\psi_F(c)\;\;N(P_F)^{-1/2} \sum_{O_F/P_F} \chi_F^{-1}(1 + \delta\,x)\,\psi_F(c\,\delta\,x) .$$

(c) If τ *is a quasi-character on* $F^\times$ *with conductor* $m(\tau)$ *less than or equal to* $d_{(\chi_F)}$ *then*

$$\chi_F\,(1 + x) = \tau \cdot \chi_F\,(1 + x) \qquad \text{for } x \in P_F^{d_{(\chi_F)}} .$$

According to part (a) and part (b), we have

$$\psi_F(c\,x) \;=\; \tau\cdot\chi_F\,(1 + x) \qquad \textit{for } x \in P_F^{\varepsilon + d(\chi_F)}$$

where ε is one for m odd and is zero for m even. Moreover,

$$W(\tau\cdot\chi_F) \;=\; W(\chi_F)\,\cdot\,\tau^{-1}(c)\ .$$

Proof. Let us point out that for any $c \in P_F^{-(m+d)}$

$$W(\chi_F) \;=\; N(P_F^m)^{-1/2} \sum_{U_F/U_F^m} \chi_F^{-1}\left(\frac{x}{\pi_F^{d+m}}\right)\psi_F\left(\frac{x}{\pi_F^{d+m}}\right)$$

$$=\; N(P_F^m)^{-1/2} \sum_{U_F/U_F^m} \chi_F^{-1}(c\,x)\,\psi_F(c\,x)\ .$$

Also, recall that χ_F being a quasi-character on $F^\times$ can be expressed as a product $\tilde{\chi}_F \cdot |\;|_F^s$ where $|\;|_F$ is the normalized absolute value of F, the exponent s is a complex number and $\tilde{\chi}_F$ is a character of $F^\times$ i.e. $\tilde{\chi}_F$ has finite order. (See Tate's thesis, theorem 2.3.1)

To prove our theorem, we apply proposition 1 and its corollary 2 in Tate [23, § 1] to the character $\tilde{\chi}_F$. ||

In the next theorem, we refer to Serre [20] for the theory of ramification groups.

Theorem A.2. *Suppose* K/F *is a Galois extension of prime degree* ℓ . *Let* G *be its Galois group and*

$$G = G_{-1} = \ldots = G_u \neq G_{u+1} = \{1\} .$$

be the ramification group filtration of G . *If* χ_F *is a quasi-character on* $F^\times$ *with conductor* $m(\chi_F) > max(1 , u+1)$, *then*

(a) the conductor of $\chi_{K/F} = \chi_F \circ N_{K/F}$ *is equal to*

$$\Psi_{K/F}(m(\chi_F) - 1) + 1 .$$

See Serre [20, chapter IV, § 3] for the definition of the real value function $\Psi_{K/F}$.

(b) in the case that K/F *is unramified, if* $c(\chi_F)$, $c(\chi_{K/F})$ *are c-parameters appearing in theorem A.1 for the respective quasi-characters, then it is possible to take* $c(\chi_{K/F}) = c(\chi_F)$. *With similar notation, we can also take*

$$c(\mu \cdot \chi_F) = c(\chi_F) \qquad \text{for any character } \mu \text{ of } F^\times / N_{K/F}(K^\times) .$$

(c) in the case that K/F *is ramified and* ℓ *is odd, part (b) still holds*

provided that $d_{(\chi_F)} \geq u + 1$ *where* $d_{(\chi_F)}$ *is the positive integer defined by* $m(\chi_F) = \varepsilon + 2 \cdot d_{(\chi_F)}$ *with* $\varepsilon = 0$ *or* 1 .

(d) in the case that K/F *is tamely ramified and* $\ell = 2$ *, we can still take*

$$c(\chi_{K/F}) = c(\mu \cdot \chi_F) = c(\chi_F) .$$

Again μ *is any character of* $F^\times / N_{K/F}(K^\times)$.

Proof. If K/F is unramified, then $\Psi_{K/F}$ is simply the identity function and part (a) follows immediately. Suppose K/F is totally ramified. Because $m(\chi_F) - 1 > u$, by Serre [20, chapter V, § 3, corollary 3, p.85]

$$\chi_F(N_{K/F}(U_K^{\Psi_{K/F}(\, m(\chi_F) - 1\,)})) = \chi_F(U_F^{(\, m(\chi_F) - 1\,)}) \neq \{1\} .$$

On the other hand,

$$\begin{aligned} \chi_F(N_{K/F}(U_K^{\Psi_{K/F}(\, m(\chi_F) - 1\,) + 1})) &= \chi_F(U_F^{(\, m(\chi_F) - 1\,) + 1}) \\ &= \chi_F(U_F^{m(\chi_F)}) \\ &= \{1\} . \end{aligned}$$

So $\Psi_{K/F}(\, m(\chi_F) - 1\,) + 1$ must be the conductor of $\chi_{K/F}$.

To prove part (b), recall that $m(\chi_{K/F}) = m(\chi_F) = \varepsilon + 2 \cdot d_{(\chi_F)}$ when K/F is unramified. Then we observe

$$N_{K/F}(1+x) \equiv 1 + Tr_{K/F}(x) \quad mod\ P_F^{m(\chi_F)}$$

for all $x \in P_K^{\varepsilon + d_{(\chi_F)}}$.

In other words

$$\chi_F(\,N_{K/F}(1+x)\,) = \chi_F(\,1 + Tr_{K/F}(x)\,)\ .$$

Since $T_{K/F}(x) \in P_F^{\varepsilon + d_{(\chi_F)}}$, theorem A.1 implies

$$\chi_F(\,N_{K/F}(1+x)\,) = \psi_F(\,c(\chi_F)\,Tr_{K/F}(x)\,)$$

which is equal to

$$\psi_F(\,Tr_{K/F}(\,c(\chi_F)\,x\,)\,) = \psi_K(\,c(\chi_F)\,x\,)\ .$$

Therefore we may take $c(\chi_{K/F}) = c(\chi_F)$.

The other assertion $c(\mu \cdot \chi_F) = c(\chi_F)$ is a consequence of part (c) of theorem A.1. Also, notice that part (b) is true regardless of the parity of ℓ.

As for part (c), we first apply part (a) to obtain

$$d_{(\chi_{K/F})} \geq m(\chi_F) \qquad (A.2.1).$$

Specifically,

$$m(\chi_{K/F}) \;=\; \Psi_{K/F}(\,m(\chi_F) - 1\,) \;+\; 1$$

$$= \begin{cases} 2\,\ell\, d_{(\chi_F)} \;-\; (\ell-1)(u+1) & \text{for } m(\chi_F) \text{ even} \\ 2\,\ell\, d_{(\chi_F)} \;-\; (\ell-1)u \;+\; 1 & \text{for } m(\chi_F) \text{ odd} \end{cases} \qquad (A.2.2).$$

Now, the assumptions ℓ is odd and $d_{(\chi_F)} \geq u+1$ yield $(A.2.1)$.

Because K/F is totally ramified, recall from Serre [20, chapter V § 3, lemma 5, p.83] that if $x \in P_K^{\varepsilon + d_{(\chi_{K/F})}}$

$$N_{K/F}(1+x) \;\equiv\; 1 + Tr_{K/F}(x) + N_{K/F}(x) \quad mod\ Tr_{K/F}(\,P_K^{2\cdot\varepsilon + 2\cdot d_{(\chi_{K/F})}}\,)\ .$$

By $(A.2.1)$, we already have $N_{K/F}(x) \in P_F^{m(\chi_F)}$. Therefore, once we show that

$$Tr_{K/F}(\,P_K^{2\cdot\varepsilon + 2\cdot d_{(\chi_{K/F})}}\,) \;\subseteq\; P_F^{m(\chi_F)}$$

the rest of the argument is reminiscent to that in part (b).

According to Serre [20, chapter V § 3, lemma 4, p.83],

$$Tr_{K/F}(\,P_K^{2\cdot\varepsilon + 2\cdot d_{(\chi_{K/F})}}\,) \;=\; P_F^{\,r}$$

where the exponent r is the largest integer less than or equal to

$$\frac{(u+1)(\ell-1) \; + \; 2\cdot\varepsilon \; + \; 2\cdot d_{(\chi_{K/F})}}{\ell} \; .$$

However, it follows from $(A.2.2)$ that the above fraction is at least as large as $m(\chi_F)$.

Let us prove part (d) now. We may assume K/F is totally ramified because of part (b) . Again

$$m(\chi_{K/F}) \;=\; \Psi_{K/F}(\, m(\chi_F) - 1\,) \;+\; 1 \;=\; 2\,(\, m(\chi_F) - 1\,) \;+\; 1$$

by part(a) . In other words

$$d_{(\chi_{K/F})} \;=\; m(\chi_F) \;-\; 1$$

Meanwhile, for all $x \in K$, we have

$$N_{K/F}(1+x) \;=\; 1 \;+\; Tr_{K/F}(x) \;+\; N_{K/F}(x) \; .$$

So, if $x \in P_K^{\,1\,+\,d_{(\chi_{K/F})}}$, then

$$N_{K/F}(1+x) \;\equiv\; 1 \;+\; Tr_{K/F}(x) \quad mod\ P_F^{m(\chi_F)}$$

and

$$\chi_F(\, N_{K/F}(1+x)\,) \;=\; \psi_F(\, c(\chi_F)\, Tr_{K/F}(x)\,) \;=\; \psi_K(\, c(\chi_F)\, x\,) \; .$$

As a result, we may take $c(\chi_{K/F}) \;=\; c(\chi_F)$.

The other assertion $c(\mu \cdot \chi_F) \;=\; c(\chi_F)$ is simply a consequence of part (c) in theorem A.1. ||

Theorem A.3 (Dwork). *Let F_p be the finite field with p elements and f be the residue class field degree $[\,k_F \,:\, F_p\,]$. Suppose χ_F is a quasi-character on $F^\times$ with conductor $m(\chi_F) \;=\; 1 + 2 \cdot d_{(\chi_F)}$ and c is the parameter in theorem A.1 for χ_F. Also, if F_o is the maximal unramified subfield of F/Q_p and $\delta \in F^\times$ has order $d_{(\chi_F)}$, then η denotes a unit in O_{F_o} satisfying*

$$\psi_F(c\,\delta^2\,x)^{-1} \;=\; \exp\!\left(\frac{2\pi i}{p}\; Tr_{k_F/F_p}(\eta\,x)\right)$$

for all $x \in O_F$.

(a) Given p odd, there exists $\gamma \in O_{F_o}$ such that

$$\chi_F^{-1}(1 \,+\, \delta x)\,\psi_F(c\,\delta\,x) \;=\; \psi_F\Big(\,c\,\delta^2\,\Big(\frac{x^2}{2} \,+\, \gamma x\Big)\Big)$$

for all $x \in O_F$.

In addition, if we let $\sqrt{1} = 1$ *and* $\sqrt{-1} = i$ *, then*

$$W(\chi_F) = \chi_F^{-1}(c)\,\psi_F(c)\;\psi_F\Big(c\,\delta^2\,\frac{\gamma^2}{2}\Big)^{-1}\left(\frac{-2\,\eta}{P_F}\right)(-1)^{\mathrm{f}-1}\left(\sqrt{(-1)^{\frac{p-1}{2}}}\,\right)^{\mathrm{f}}$$

where

$$\left(\frac{-2\,\eta}{P_F}\right) = \begin{cases} 1 & \textit{when } -2\,\eta \in k_F^2\,. \\ -1 & \textit{otherwise.} \end{cases}$$

(b) *Given* $p = 2$ *, let* $\beta^2 \equiv \eta^{-1}$ *mod* P_F *. Then there exists* $\gamma \in O_{F_o}$ *such that for all* $x \in O_F$

$$\chi_F^{-1}(1 + \beta\,\delta x)\,\psi_F(c\,\beta\,\delta\,x) = \Delta_o'(x)\;(-1)^{Tr_{k_F/F_p}(\gamma x)}$$

where $\Delta_o' = i^{\,Tr_{k_F/F_p}} \cdot (-1)^{Tr^{(2)}_{k_F/F_p}}$ *if we designate* $Tr^{(2)}_{k_F/F_p}$ *to be the 2nd elementary symmetric function.*

Moreover, we have

$$W(\chi_F) = \chi_F^{-1}(c)\,\psi_F(c)\;\Delta_o'(\gamma)^{-1}\left(\frac{1+i}{\sqrt{2}}\right)^{\mathrm{f}}(-1)^{\mathrm{f}-1}\,.$$

(c) *If* Δ_o' *is the function from* k_F *to the non-zero complex numbers defined in part* (b) *, then for any positive integer* n *,*

$$\Delta_o'(n\,x)\,(-1)^{Tr_{k_F/F_p}(\frac{n(n-1)}{2}\,x^2)} = \Delta_o'(x)^n\,.$$

Proof. The argument is due to Dwork, but first let me point out that if we abbreviate the conductor of χ_F to m, then

$$\chi_F^{-1}(\pi_F^{d+m})\, W(\chi_F) \;=\; \underbrace{N(P_F^m)^{-1/2} \sum_{U_F/U_F^m} \chi_F^{-1}(x)\, \psi_F\Big(\frac{x}{\pi_F^{d+m}}\Big)}_{(\,\chi_F^{-1}\,,\; (\psi_F)_{\pi_F^{-(d+m)}}\,) \text{ in Dwork's notation}} \tag{A.3.1}$$

Also, given parameter c in theorem A.1 for χ_F, let α be the unit determined by

$$c \;=\; \frac{\alpha}{\pi_F^{d+m}}$$

with the same choice of uniformizing parameter π_F as in $(A.3.1)$. Then

$$\chi_F^{-1}(1+x) \;=\; \psi_F\Big(\frac{\alpha\, x}{\pi_F^{d+m}}\Big)^{-1} \qquad \text{for all } x \in P_F^{1+d(\chi_F)}\,.$$

See theorem A.1.

Furthermore, given p odd, both η and γ depend on the choice of δ. In fact, η *mod* P_F is unique up to a multiple of a square in k_F, and the product $\delta\,\gamma$ is independent of the choice of δ. On the other hand, when $p = 2$, the product $\beta\,\delta$ is independent of the choice of δ. Consequently, γ *mod* P_F is uniquely determined.

Now, the last theorem in chapter II of Dwork's thesis [5] completes the proof of part(a) and part(b).

Part(c) can be obtained by induction. When $n = 1$, the equality in part(c) holds trivially. Assume that

$$\Delta_o'(n\,x)\,(-1)^{Tr_{k_F/F_p}(\frac{n(n-1)}{2}\,x^2)} = \Delta_o'(x)^n$$

is true for one particular n, and consider $\Delta_o'(\,(n+1)\,x\,)$. By definition,

$$\Delta_o'(\,(n+1)\,x\,) = \Delta_o'(n\,x + x) = i^{\,Tr_{k_F/F_p}(n\,x + x)} \cdot (-1)^{Tr^{(2)}_{k_F/F_p}(n\,x + x)} .$$

Now recall the following property of the second elementary symmetric function.

$$Tr^{(2)}_{k_F/F_p}(n\,x + x)$$
$$= Tr^{(2)}_{k_F/F_p}(n\,x) + Tr^{(2)}_{k_F/F_p}(x) + Tr_{k_F/F_p}(n\,x)\,Tr_{k_F/F_p}(x) - Tr_{k_F/F_p}(n\,x^2) .$$

As a result,

$$\Delta_o'(\,(n+1)\,x\,) = \Delta_o'(n\,x)\;\Delta_o'(x) \cdot (-1)^{Tr_{k_F/F_p}(n\,x^2)}$$

because[2]

$$i^{Tr_{k_F/F_p}(n\,x\,+\,x)} \cdot (-1)^{Tr_{k_F/F_p}(n\,x)\,Tr_{k_F/F_p}(x)} = i^{Tr_{k_F/F_p}(n\,x)} \cdot i^{Tr_{k_F/F_p}(x)} .$$

So the induction hypothesis implies

$$\Delta'_o(\,(n+1)\,x\,) = \Delta'_o(x)^n\,(-1)^{Tr_{k_F/F_p}(\frac{n(n-1)}{2}\,x^2)} \cdot \Delta'_o(x) \cdot (-1)^{Tr_{k_F/F_p}(n\,x^2)}$$

which means

$$\Delta'_o(\,(n+1)\,x\,) = \Delta'_o(x)^{n+1}\,(-1)^{Tr_{k_F/F_p}(\frac{n(n+1)}{2}\,x^2)}.$$

This completes our proof of part(c) and theorem A.3 as well. ||

---

[2] A caution to our exponential notation used in defining Δ'_o .

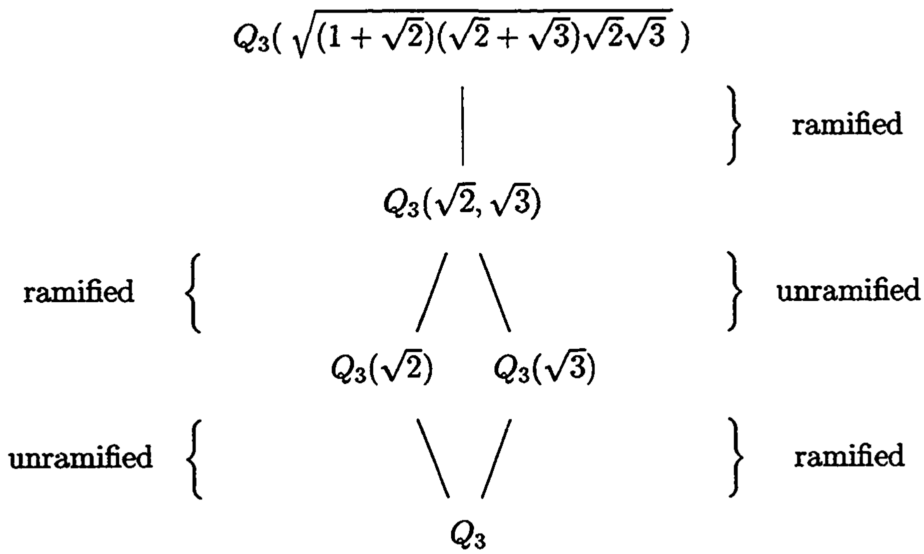
$$i^{Tr_{k_F/F_p}(a\,+\,b)} \neq i^{Tr_{k_F/F_p}(a)} \cdot i^{Tr_{k_F/F_p}(b)} \qquad \text{for some } a\,,\,b \in k_F$$

As an example, let $Tr_{k_F/F_p}(a) = 1 = Tr_{k_F/F_p}(b)$. Then, notice that $p = 2$ means $Tr_{k_F/F_p}(a+b) = 0 \in F_p$. Therefore

$$i^{Tr_{k_F/F_p}(a\,+\,b)} = 1 \neq -1 = i^{Tr_{k_F/F_p}(a)} \cdot i^{Tr_{k_F/F_p}(b)}$$

B Examples: The 2nd and 3rd Identities

(I) Consider the following extension of Q_3, the field of 3-adic numbers.



For the sake of notational simplicity, let us write

$$E = Q_3(\sqrt{(1+\sqrt{2})(\sqrt{2}+\sqrt{3})\sqrt{2}\sqrt{3}})$$

$$K = Q_3(\sqrt{2}, \sqrt{3})$$

$$L_1 = Q_3(\sqrt{2})$$

$$L_2 = Q_3(\sqrt{3})$$

$$u = (1+\sqrt{2})(\sqrt{2}+\sqrt{3})\sqrt{2}\sqrt{3}$$

We know that both E/K and L_2/Q_3 are totally ramified because $x^2 - u$ and $x^2 - 3$ are Eisenstein polynomials over K and Q_3 respectively. On the other hand, the quadratic polynomial $x^2 - 2$ does not split in the residue class field of Q_3. So L_1/Q_3 must be unramified. As a result, the ramification index and residue class field degree of K/Q_3 are both equal to 2, and therefore K/L_1 is totally ramified, while K/L_2 is not.

By localizing Dedekind's example of quaternion extension (See Dedekind [3] or Yui [27]) at $p = 3$, we conclude that E/Q_3 is in fact a Galois extension with

$$Gal(E/Q_3) = \underbrace{\{\pm 1, \pm i, \pm j, \pm k\}}_{\text{the quaternion group } H_8}$$

Notice that $G = Gal(E/Q_3)$ has 3 subgroups of index 2, all of which are cyclic of order 4. In other words,

$$Gal(E/L_i) \simeq L_i^\times / N_{E/L_i}(E^\times) \qquad \text{for } i = 1, 2$$

must be cyclic of order 4. Consequently, there are 2 characters of $L_i^\times$ that annihilate the norm group $N_{E/L_i}(E^\times)$ and have order 4. Later we will arbitrarily select one of the 2 characters for computation purpose. Meanwhile, let χ_{L_i} be such a character of $L_i^\times$. Then

1) $Gal(E/L_1)$ and $Gal(E/L_2)$ are subgroups of G with prime index 2.

2) $Gal(E/L_1) \cap Gal(E/L_2) = Gal(E/K)$ is the center of G.

3) if Z_2 denotes the cyclic group of order 2, we have an exact sequence

$$1 \longrightarrow Gal(E/K) \longrightarrow G \longrightarrow Z_2 \oplus Z_2 \longrightarrow 1$$

4) $\chi_{L_1} \circ N_{K/L_1} = \chi_{L_2} \circ N_{K/L_2}$.

5) $\chi_{L_1} \circ N_{K/L_1} \neq \chi \circ N_{K/Q_3}$ for any quasi-character χ on $Q_3^\times$.

These conditions[1] suggest that we can expect the 2nd identity to hold.

As $[L_i : Q_3] = 2$, let μ_i be the non-trivial character of $Q_3^\times / N_{L_i/Q_3}(L_i^\times)$. Observe that E/Q_3 is tamely ramified. Hence χ_{L_i}, μ_i have conductors less than or equal to one.

Lemma. *If we choose* $\pi_{L_1} = 3$ *and* $\pi_{L_2} = \sqrt{3}$ *to be our uniformizing parameters of* L_1 *and* L_2 *respectively, then*

[1]Here is the argument for 5). If $\chi_{L_1} \circ N_{K/L_1} = \chi \circ N_{K/Q_3}$ were to hold, such χ must annihilate the norm group $N_{E/Q_3}(E^\times)$. So the quasi-character can be interpreted as a character of H_8, but H_8 only yields 3 non-trivial characters of order 2, none of which satisfies

$$\chi_{L_1} \circ N_{K/L_1} = \chi \circ N_{K/Q_3}$$

(a) $\chi_{L_1}(3) = -1$, *and consequently* χ_{L_1} *must have order 4 on the unit group* U_{L_1}. *In particular,* $\chi_{L_1}(-1) = 1$.

(b) $\chi_{L_2}(\sqrt{3})$ *is a primitive 4th root of unity, while* $\chi_{L_2}(-1) = -1$.

Proof. Because $\chi_{L_1}^2$ has order 2, its kernel is the norm group $N_{K/L_1}(K^\times)$. So

$$1 = \chi_{L_1}^2(N_{K/L_1}(\sqrt{3})) = \chi_{L_1}^2(-3)$$

On the other hand, $\exists\, x \in U_{L_1}$ such that

$$x^2 \equiv -1 \mod P_{L_1}$$

as L_1 is the unique unramified quadratic extension over Q_3.

Then the fact that $\chi_{L_1}(U_{L_1}^1) = \{1\}$ implies

$$1 = \chi_{L_1}^2(-3) = \chi_{L_1}^2(x^2 3)$$

In other words, $\chi_{L_1}^2(3) = 1$ and therefore the restriction $\chi_{L_1}|_{U_{L_1}}$ is of order 4, since χ_{L_1} is assumed to have order 4. Precisely, if we choose the following coset representatives of $U_{L_1}/U_{L_1}^1$

$$\left\{ \pm 1 \;,\; \pm\sqrt{2} \;,\; \pm 1 \pm \sqrt{2} \right\}$$

then $\chi_{L_1}(\pm 1) = 1 , \chi_{L_1}(\pm\sqrt{2}) = -1 , \chi_{L_1}(\pm 1 \pm \sqrt{2}) = \pm i .$ $(B.I.1)$

To find the value of $\chi_{L_1}(3)$, we notice

$$N_{E/L_1}(\sqrt{u}) = N_{K/L_1}(-u) = 2\,(1+\sqrt{2})^2\,3$$

and $\chi_{L_1}(\,N_{E/L_1}(\sqrt{u})\,) = 1$. Thus

$$\chi_{L_1}(3) = \chi_{L_1}(\,2\,(1+\sqrt{2})^2\,)^{-1} = \chi_{L_1}(\,-\,(1+\sqrt{2})^2\,)^{-1} = (\pm i)^2 = -1$$

This completes part (a). Part (b) can be proved similarly. $|U_{L_2}/U^1_{L_2}| = 2$ means χ_{L_2} cannot have order 4 on the unit group U_{L_2}. As a result, $\chi_{L_2}(\sqrt{3}) = \pm i$. Meanwhile,

$$N_{E/L_2}(\sqrt{u}) = N_{K/L_2}(-u) = 6$$

So

$$1 = \chi_{L_2}(\,N_{E/L_2}(\sqrt{u})\,) = \chi_{L_2}(6) = \chi_{L_2}(-3)$$

Observe that $\chi_{L_2}(-1) = -1$; otherwise $\chi_{L_2}(\sqrt{3})$ would not be a primitive 4th root of unity. The proof of our lemma is now completed. ||

Now we are going to select one χ_{L_i} for each i in order to compute the root number and to verify the 2nd identity. As the proof of our previous lemma alludes, it is sufficient to specify the following character values.[2]

$$\chi_{L_1}(1+\sqrt{2}) = i \qquad \text{and} \qquad \chi_{L_2}(\sqrt{3}) = i$$

Moreover, it is a consequence of the lemma that the conductor of χ_{L_i} is exactly one.

By definition,

$$W(\chi_{L_1}) = N(P_{L_1})^{-1/2} \sum_{x \in U_{L_1}/U_{L_1}^1} \chi_{L_1}^{-1}\left(\frac{x}{3}\right) \psi_{L_1}\left(\frac{x}{3}\right)$$

where ψ_{L_i} is the canonical additive character of L_i. (See Tate [23].)

Let $\zeta = e^{\frac{2\pi i}{3}}$. By part (a) of the lemma and $(B.I.1)$ in its proof, we conclude

$$W(\chi_{L_1}) = \frac{1}{\sqrt{3^2}}\left(-\zeta^2 + (-\zeta^{-2}) + 1 + 1 + i\cdot\zeta^2 + (-i)\cdot\zeta^2 \right)$$

Therefore

$$W(\chi_{L_1}) = \frac{1}{3}(2 - \zeta - \zeta^2) = 1$$

Similarly, we compute

$$W(\chi_{L_2}) = N(P_{L_2})^{-1/2} \sum_{x \in U_{L_2}/U_{L_2}^1} \chi_{L_2}^{-1}\left(\frac{x}{\sqrt{3}^2}\right) \psi_{L_2}\left(\frac{x}{\sqrt{3}^2}\right)$$

[2]Our selection here is arbitrary. The two distinct characters of $L_1^\times/N_{E/L_1}(E^\times)$ (resp. $L_2^\times/N_{E/L_2}(E^\times)$) with order 4 are inverse of one another.

Part (b) of the lemma then yields

$$W(\chi_{L_2}) = \frac{1}{\sqrt{3}}(-\zeta^2 + \zeta^{-2}) = \frac{1}{\sqrt{3}}(-\zeta^2 + \zeta)$$

Next, we evaluate $W(\mu_i)$. Recall that μ_i is defined to be the non-trivial character of $Q_3^\times$ which annihilates the norm group $N_{L_i/Q_3}(L_i^\times)$. Because L_1/Q_3 is unramified,

$$W(\mu_1) = \mu_1(3)^0 = 1$$

In contrast, the conductor of μ_2 is one as L_2/Q_3 is totally and tamely ramified. Also, notice that $1 = \mu_2(N_{L_2/Q_3}(\sqrt{3})) = \mu_2(-3)$. Hence,

$$W(\mu_2) = \frac{1}{\sqrt{3}} \sum_{x \in U_{Q_3}/U_{Q_3}^1} \mu_2^{-1}\left(\frac{x}{3}\right) \psi_{Q_3}\left(\frac{x}{3}\right) = \frac{1}{\sqrt{3}}(-\zeta + \zeta^{-1})$$

Finally, we use these root numbers to verify that the 2nd identity indeed holds in this example.

$$\begin{aligned} W(\chi_{L_2})\, W(\mu_2) &= \frac{1}{\sqrt{3}}(-\zeta^2 + \zeta)\, \frac{1}{\sqrt{3}}(-\zeta + \zeta^{-1}) \\ &= \frac{1}{3}(1 - \zeta^2 - \zeta + 1) \\ &= \frac{1}{3}(2 - \zeta^2 - \zeta) \\ &= W(\chi_{L_1})\, W(\mu_1) \end{aligned}$$

If we localize Dedekind's example at $p = 2$, a totally and wildly ramified quaternion extension over Q_2 is obtained[3]. This means the conductors of χ_{L_i} and μ_i are both greater than one. While the calculation of the root number is more involved, it is expected that the 2nd identity remains true.

(II) Let $\zeta = e^{\frac{2\pi i}{5}}$. The polynomial is $x^5 - 2$ is Eisenstein over Q_2.

$$\begin{array}{ccccc} & & Q_2(\zeta, \sqrt[5]{2}) & & \\ \text{unramifed} & \left\{ \right. & {}^{4}/ \quad \backslash^{5} & \left. \right\} & \text{ramified} \\ & Q_2(\sqrt[5]{2}) & & Q_2(\zeta) & \\ \text{ramified} & \left\{ \right. & {}^{5}\backslash \quad /^{4} & \left. \right\} & \text{unramified} \\ & & Q_2 & & \end{array}$$

So the Galois group of $Q_2(\zeta, \sqrt[5]{2})/Q_2$ has order 20. Henceforth, we adopt the following notations:

$$K = Q_2(\zeta, \sqrt[5]{2})$$

$$L = Q_2(\zeta)$$

$$E = Q_2(\sqrt[5]{2})$$

[3]To see that $u = (1+\sqrt{2})(\sqrt{2}+\sqrt{3})\sqrt{2}\sqrt{3}$ is not a square in $K' = Q_2(\sqrt{2}, \sqrt{3})$, we observe $x^2 = u$ implies $N_{K'/Q_2(\sqrt{3})}(x)^2 = N_{K'/Q_2(\sqrt{3})}(u)$. However, $N_{K'/Q_2(\sqrt{3})}(u) = 6$ is not a square in $Q_2(\sqrt{3})$. In other words, the equation $x^2 = u$ cannot be solved in K'.

Observe that $Gal(K/L)$ is abelian and normal in $Gal(K/Q_2)$, while $Gal(K/E)$ is one of the five 2-sylow subgroups of $Gal(K/Q_2)$. Moreover, the center of $Gal(K/Q_2)$ is trivial. It follows that $Gal(K/L)$ is contained in all nontrivial normal subgroups of $Gal(K/Q_2)$.

Let us denote $Gal(K/Q_2)$ by G , $Gal(K/E)$ by H and $Gal(K/L)$ by C. Given a non-trivial character φ of H, we define $\chi \in G^*$ by[4]

$$\chi(h\,c) \;=\; \varphi(h) \qquad \text{for } h \in H \text{ and } c \in C$$

This is legitimate because $G = HC$ and $H \cap C = \{1\}$. Notice $C \lhd G$ implies that χ is indeed a homomorphism. From the definition, we have

$$\chi|_H = \varphi$$

.

Meanwhile, $\chi|_C$ is trivial.

Under the above circumstance, we can try verify the 3rd identity for χ interpreted as a character of $Q_2^\times / N_{K/Q_2}(K^\times)$.

$$W(\chi \circ N_{E/Q_2}) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\mu') \;=\; W(\chi) \prod_{\substack{\mu \in T \\ \mu \neq 1}} W(\,\mu' \cdot (\,\chi \circ N_{F_\mu/Q_2})\,)$$

[4]Recall G^* stands for the character group of G.

where T consists of the orbits of the G-action on C^* by conjugation, F_μ is the fixed field of the stabilizer of $\mu \in C^*$, and μ' is the character of $Gal(K/F_\mu)$ which coincides with μ on C but annihilates $H \cap Gal(K/F_\mu)$.

In our example, C is cyclic of prime order 5, which implies all $\mu \neq 1$ have trivial kernel. So, the isotropy group of μ is identical to the centralizer of C. However, the fact that G has trivial center means C is its own centralizer. Therefore, T contains exactly one orbit, and $F_\mu = L$ in this example. Hence, the 3rd identity follows from

$$W(\chi \circ N_{E/Q_2})\, W(\mu) \;=\; W(\chi)\, W(\, \mu \cdot (\, \chi \circ N_{L/Q_2})\,)$$

Now, recall that $\chi|_C$ is trivial. In other words, $\chi \circ N_{L/Q_2} = 1$, and it is sufficient to show

$$W(\chi \circ N_{E/Q_2}) \;=\; W(\chi)$$

Since L/Q_2 is unramified and $\chi \circ N_{L/Q_2} = 1$, χ must be an unramified character of order dividing 4. Consequently, $\chi \circ N_{E/Q_2}$ is also unramified with order dividing 4.

$$W(\chi \circ N_{E/Q_2}) \;=\; (\chi \circ N_{E/Q_2})(\sqrt[5]{2}\,)^4 \;=\; 1 \;=\; \chi(2)^0 \;=\; W(\chi)$$

As E/Q_2 is a totally and tamely ramified extension, the order of its different is one less than the ramification index.

Our selection of φ and the corresponding construction of χ have simplified tremendously the calculation. In fact, the above 3rd identity is supposed to hold even if we replace χ by any arbitrary quasi-character χ_{Q_2} on $Q_2^\times$. To illustrate this independence between the character and the Galois extension, let us choose χ_{Q_2} to be the wildly ramified character of $Q_2^\times$ which annihilates the norm group $N_{Q_2(\sqrt{2})/Q_2}(Q_2(\sqrt{2})^\times)$, and then verify

$$W(\chi_{Q_2} \circ N_{E/Q_2})\, W(\mu) \;=\; W(\chi_{Q_2})\, W(\,\mu \cdot (\,\chi_{Q_2} \circ N_{L/Q_2})\,)$$

where μ is a non-trivial character of $L^\times$ which annihilates $N_{K/L}(K^\times)$.

In this case[5] the conductor $m(\chi_{Q_2}) = 3$. If we pick the following representives for $U_{Q_2}/U_{Q_2}^3$

$$\{1\ ,\ 1+2\ ,\ 1+2+4\ ,\ 1+4\}$$

then $\chi_{Q_2}(1) = 1 = \chi_{Q_2}(1+2+4)$ and $\chi_{Q_2}(1+2) = -1 = \chi_{Q_2}(1+4)$

[5]The ramification groups for the wildly ramified extension $Q_2(\sqrt{2})/Q_2$ are known. See for example Serre [20] chapter 4, § 2, exercise 4, p.72.

because

$$N_{Q_2(\sqrt{2})/Q_2}(1+\sqrt{2}) \;=\; -1 \;\equiv\; 1 \,+\, 2 \,+\, 4 \quad mod\ 8$$

Moreover,

$$\chi_{Q_2}(2) \;=\; \chi_{Q_2}(\,-\,N_{Q_2(\sqrt{2})/Q_2}(\sqrt{2})\,) \;=\; \chi_{Q_2}(-1) \;=\; 1 \qquad (B.II.1)$$

Let $\eta \;=\; e^{\frac{2\pi i}{8}}$. By definition,

$$W(\chi_{Q_2}) \;=\; \frac{1}{\sqrt{2^3}} \sum_{x \,\in\, U_{Q_2}/U_{Q_2}^3} \chi_{Q_2}^{-1}\Big(\frac{x}{2^3}\Big)\ \eta^{\,x}$$

From above,

$$W(\chi_{Q_2}) \;=\; \frac{1}{\sqrt{2^3}}\left[\eta+(-\eta^{\,3})+\eta^{\,7}+(-\eta^{\,5})\right] \;=\; \frac{1}{\sqrt{2^3}}\left[2\eta+2\eta^{-1}\right] \;=\; 1$$

Besides the value of $W(\chi_{Q_2})$, we note that

$$\chi_{Q_2}(1\,+\,x) \;=\; \eta^{\,x}$$

if the order of x in Q_2 is greater than or equal to 2. Equivalently, with

$$c \;=\; \frac{1}{8} \qquad (B.II.2)$$

we have $\chi_{Q_2}(1+x) \;=\; \psi(c\,x)$ where ψ is the canonical additive character of Q_2 (See Tate [23]).

Next, we evaluate $W(\mu \cdot (\chi_{Q_2} \circ N_{L/Q_2}))$. Since K/L is tamely ramified, the conductor of μ must be one. By theorem A.1 part (c) and $(B.II.2)$,

$$W(\mu \cdot (\chi_{Q_2} \circ N_{L/Q_2})) = W(\chi_{Q_2} \circ N_{L/Q_2})\ \mu^{-1}\left(\frac{1}{8}\right)$$

which is equal to $W(\chi_{Q_2} \circ N_{L/Q_2})$ because $N_{K/L}(\sqrt[5]{2}) = 2$ implies $\mu(2) = 1$.

Now, theorem A.2 part (b) together with theorem A.1 part (b) show that

$$W(\chi_{Q_2} \circ N_{L/Q_2})$$
$$= (\chi_{Q_2} \circ N_{L/Q_2})^{-1}\left(\frac{1}{8}\right)\ \psi_L\left(\frac{1}{8}\right)\ \frac{1}{\sqrt{2^4}} \sum_{x \in O_L/P_L} (\chi_{Q_2} \circ N_{L/Q_2})^{-1}(1+2x)\ \psi_L\left(\frac{2x}{8}\right)$$

Again ψ_L denotes the canonical additive character of L. It follows that $W(\chi_{Q_2} \circ N_{L/Q_2})$ is equal to

$$\frac{-1}{\sqrt{2^4}} \sum_{x \in O_L/P_L} \chi_{Q_2}(1 + 2\,Tr_{L/Q_2}(x))\,\chi_{Q_2}(1 + 4\,Tr^{(2)}_{L/Q_2}(x))\ \psi_L\left(\frac{2x}{8}\right)$$

because $N_{L/Q_2}(1+2x) \equiv (1+2\,Tr_{L/Q_2}(x))(1+4\,Tr^{(2)}_{L/Q_2}(x))\ \mathit{mod}\ 8$.

To complete this calculation, let us fix a set of representatives of $U_L/U_L^1 = (O_L/P_L)^\times$.

$$\begin{array}{ccccc} 1, & 1+\zeta, & 1+\zeta^2, & \zeta^4, & \zeta^4(1+\zeta) \\ \zeta^4(1+\zeta^2), & \zeta^3, & \zeta^3(1+\zeta), & \zeta^3(1+\zeta^2), & \zeta^2 \\ \zeta^2(1+\zeta), & \zeta^2(1+\zeta^2), & \zeta, & \zeta(1+\zeta), & \zeta(1+\zeta^2) \end{array}$$

The respective values of the first and second symmetric functions are given in the table below. Here we have used the fact that

$$Tr_{L/Q_2}(x)^2 \;=\; Tr_{L/Q_2}(x^2) \;+\; 2\,Tr^{(2)}_{L/Q_2}(x)$$

$Tr_{L/Q_2}(x)$	$Tr_{L/Q_2}(x^2)$	$Tr^{(2)}_{L/Q_2}(x)$	x
-1	-1	1	$\zeta\ ,\ \zeta^2\ ,\ \zeta^3\ ,\ \zeta^4$
-2	-4	4	$\zeta(1+\zeta)\ ,\ \zeta(1+\zeta^2)$
-2	-4	4	$\zeta^2(1+\zeta^2)\ ,\ \zeta^3(1+\zeta)$
-2	6	-1	$\zeta^4(1+\zeta^2)\ ,\ \zeta^2(1+\zeta)$
3	1	4	$\zeta^4(1+\zeta)\ ,\ \zeta^3(1+\zeta^2)$
3	1	4	$1+\zeta\ ,\ 1+\zeta^2$
4	4	6	1

As a result, we can conclude

$$W(\chi_{Q_2} \circ N_{L/Q_2}) \;=\; \frac{-1}{\sqrt{2^4}}\left\{1 \;+\; 4i \;+\; 4 \;-\; 2 \;-\; 4i \;+\; 1\right\} \;=\; -1$$

and therefore

$$W(\,\mu \cdot (\chi_{Q_2} \circ N_{L/Q_2})\,) \;=\; -1$$

The above 15 representatives for U_L/U_L^1 may also be used in determining $W(\mu)$. Let us choose one non-trivial μ by assigning[6]

$$\mu(1 + \zeta) = \zeta$$

Meanwhile $\mu(2)$ is always 1 as $N_{K/L}(\sqrt[5]{2}) = 2$. By definition

$$W(\mu) = \frac{1}{\sqrt{2^4}} \sum_{x \in U_L/U_L^1} \mu^{-1}\left(\frac{x}{2}\right) \psi_L\left(\frac{x}{2}\right)$$

It follows from the above table and our choice of μ that $W(\mu)$ equals

$$\frac{1}{\sqrt{2^4}}\Big\{1 + (-\zeta) + (-\zeta^2) + (-\zeta^3) + (-\zeta^4) + 1 + (-\zeta)$$
$$+ \zeta^2 + (-\zeta^3) + (-\zeta^4) + 1 + \zeta + (-\zeta^2) + \zeta^3 + \zeta^4\Big\}$$

Hence

$$W(\mu) = 1$$

Finally, we compute $W(\chi_{Q_2} \circ N_{E/Q_2})$ and begin with

Claim. *The conductor of* $\chi_{Q_2} \circ N_{E/Q_2}$ *is 11.*

[6]It is sufficient to specify the value of $\mu(1+\zeta)$ because $1+\zeta$ is a generator for the cyclic group U_L/U_L^1.

Proof. As K/L is totally and tamely ramified Galois extension of prime degree 5, we have

$$N_{K/L}(U_K^{5n}) = U_L^n \qquad \text{for } n > 0$$

and

$$N_{K/L}(U_K^{5n+1}) = U_L^{n+1} \qquad \text{for } n \geq 0$$

See Serre [20] chapter V, § 3, corollary 3. On the other hand, $N_{L/Q_2}(U_L^n) = U_{Q_2}^n$ for all $n \geq 0$ because L/Q_2 is unramified. Consequently

$$N_{K/Q_2}(U_K^{5n}) = U_{Q_2}^n \qquad \text{for } n > 0$$

and

$$N_{K/Q_2}(U_K^{5n+1}) = U_{Q_2}^{n+1} \qquad \text{for } n \geq 0$$

In particular, $N_{K/Q_2}(U_K^{10}) = U_{Q_2}^2$ and $N_{K/Q_2}(U_K^{11}) = U_{Q_2}^3$

Now the fact that K/E is unramified means

$$N_{E/Q_2}(U_E^{10}) = U_{Q_2}^2$$

while

$$N_{E/Q_2}(U_E^{11}) = U_{Q_2}^3$$

Recall that χ_{Q_2} has conductor 3, and the claim is proved. ||

According to theorem A.2 part (b), if $x \in P_E^6$, then $\exists\, c$ such that

$$(\chi_{Q_2} \circ N_{E/Q_2})(1 + x) = \psi_E(c\,x)$$

Let us fix $\pi_E = \sqrt[5]{2}$ to be our uniformizing parameter of E. Observe that

$$U_E^6/U_E^{11} = \prod_{i=6}^{10} \langle\, 1 + \pi_E^i \,\rangle$$

where $\langle\, 1 + \pi_E^i \,\rangle$ is the cyclic group of order 2 generated by $1 + \pi_E^i \; mod \; U_E^{11}$.

Claim. *We can take* c *to be* $\frac{1}{8}$.

Proof. Since E/Q_2 is totally and tamely ramified of degree 5, the order of the absolute different of E is $5 - 1 = 4$. Together with the previous claim, we see $\frac{1}{8}$ as an element of E has the expected order of c. Due to the above decomposition of U_E^6/U_E^{11}, it is sufficient to prove that

$$(\chi_{Q_2} \circ N_{E/Q_2})(1 + \pi_E^i) = \psi_E\Big(\frac{\pi_E^i}{8}\Big) \qquad \text{for } 10 \geq i \geq 6$$

Notice that if $9 \geq i \geq 6$, then

$$N_{E/Q_2}(1 + \pi_E^i) = \prod_{j=0}^{4} (1 + \zeta^{ij}\,\pi_E^i) = 1 + 2^i \in U_{Q_2}^6$$

which is annihilated by χ_{Q_2} . Meanwhile

$$Tr_{E/Q_2}(\pi_E^i) = \sum_{j=0}^{4} \zeta^{ij}\, \pi_E^i = 0$$

implies $\psi_E\left(\frac{\pi_E^i}{8}\right) = 1$.

When $i = 10$, we have $N_{E/Q_2}(1 + \pi_E^{10}) = N_{E/Q_2}(1 + 4) = (1 + 4)^5$.

As a result,

$$(\chi_{Q_2} \circ N_{E/Q_2})(1 + \pi_E^{10}) = \chi_{Q_2}(1+4)^5 = -1 = \psi_E\left(\frac{4}{8}\right) = \psi_E\left(\frac{\pi_E^{10}}{8}\right)$$

This completes the proof of our claim. ||

By theorem A.1 part (b) , the root number $W(\chi_{Q_2} \circ N_{E/Q_2})$ is equal to

$$(\chi_{Q_2} \circ N_{E/Q_2})^{-1}\left(\frac{1}{8}\right) \psi_E\left(\frac{1}{8}\right) \frac{1}{\sqrt{2}} \sum_{x \in O_E/P_E} (\chi_{Q_2} \circ N_{E/Q_2})^{-1}(1 + 2x)\, \psi_E\left(\frac{2x}{8}\right)$$

If the primitive 8-th root of unity $e^{\frac{2\pi i}{8}}$ is denoted by η , then

$$\psi_E\left(\frac{1}{8}\right) = \eta^5 = \frac{-1 - i}{\sqrt{2}}$$

Combine with $(B.II.1)$ and the fact $|O_E/P_E| = 2$.

$$W(\chi_{Q_2} \circ N_{E/Q_2}) = \frac{-1 - i}{\sqrt{2}} \frac{1}{\sqrt{2}} \left(1 - i\right) = -1$$

Now, we are able to confirm the 3rd identity with character χ_{Q_2}.

$$\underbrace{W(\chi_{Q_2} \circ N_{E/Q_2})}_{-1} \ \underbrace{W(\mu)}_{1} = -1 = \underbrace{W(\chi_{Q_2})}_{1} \ \underbrace{W(\mu \cdot (\chi_{Q_2} \circ N_{L/Q_2}))}_{-1}$$

One example of the 3rd identity involving a wildly ramified Galois extension can be constructed if we replace the prime 2 in the above example by 5. The resulting Galois extension $Q_5(\sqrt[5]{5}, \zeta)$ over Q_5 is totally ramified which satisfies the conditions in the 3rd identity.

References

[1] W. CASSELMAN, On the representations of $SL_2(K)$ related to binary quadratic forms, *American Journal of Math, vol. 19 (1970), pp. 810-834.*

[2] J. W. S. CASSELS AND A. FROHLICH, Algebraic Number Theory, *Academic Press, New York, 1967.*

[3] R. DEDEKIND, Konstruktion von Quaternionkorpern, *Gesammelte mathematische Werke Bd. 2, Vieweg Braunschweig, 1931, pp.376-384.*

[4] P. DELIGNE, Les constants des equations fonctionnelles des fonctions L, *Lecture Notes in Math., vol. 349, Springer-Verlag, New York, 1973*, pp. 501-597.

[5] B. DWORK, On the Root Number in the Functional Equation of the Artin-Weil L-series, *Ph.D. Thesis, Columbia University, 1954*

[6] B. DWORK, On the Artin root number, *Amer. Jour. of Math., vol. 78(1956)*, pp. 444-472.

[7] R. J. EVANS, Identities for products of Gauss sums over finite fields, *Extrait de L'Enseignement mathematique, T. XXVII (1981), fasc. 3-4, pp.197-209.*

[8] A. FRÖHLICH AND M. TAYLOR, The Arithmetic Theory of Local Galois Gauss Sums for Tame Characters, *Phil. Trans. Roy. Soc. 298, 1980, pp.141-181.*

[9] L. GOLDSTEIN, Analytic Number Theory, *Prentice-Hall, New York, 1971*

[10] H.HASSE, Artinsche Führer, Artinsche L-Funcktionen und Gauss'schen summen über endlich algebraischen Zahlkörpern, *Arta salmenticensia, seccion de Mathematics, 1954.*

[11] E. HECKE, Über die L-functionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper, *Nachrichten Göttingen (1917)*, pp.299-318, Werke, no. 9.

[12] K. IRELAND AND M. ROSEN, A classical Introduction to Modern Number Theory, *2nd Edition, Springer-Verlag, New York, 1995, GTM 84.*

[13] H. JACQUET AND R. LANGLANDS, Automorphic Forms on GL(2), *Lecture Notes in Math., vol. 114. Springer-Verlag, New York, 1970.*

[14] K. LAKKIS, Die galoisschen Gauss'schen Summen von Hasse, *Thesis, Hamburg, 1964.*

[15] E. LAMPRECHT, Allgemeine Theorie der Gauss'schen Summen in endlichen kommutativen Ringen, *Math. Nachr. 9, 1953.*

[16] R. LANGLANDS, On the functional equation of the Artin L-functions, *Notes, Yale University, 1971.*

[17] R. LANGLANDS, On the functional equation of the Artin L-function, *www.sunsite,ubc.ca/DigitalMathArchive/Langlands/.*

[18] J. MARTINET, Character theory and Artin L-functions. *Proceeding Durham Symposium on Algebraic Number Fields, Academic Press, New York, 1977.*

[19] J. P. SERRE, Linear Representations of Finite Group, *Springer-Verlag, New York, 1996, GTM 42.*

[20] J. P. SERRE, Local Fields, *Springer-Verlag, New York, 1995, GTM 67.*

[21] J. TATE, Number theoretic background, *Proc. Symposia Pure Math., vol. 33, AMS (Providence, RI), 1979, Part 2, pp. 3-26.*

[22] J. TATE, Fourier analysis in number fields and Hecke's zeta function, *Algebraic Number Theory, eds. J.W.S. Cassels and A. Fröhlich, Thompson Book Co., Washington, D.C., 1967,* pp.305-347.

[23] J. TATE, Local constants, *Durham Symposium on Algebraic Number Fields, Ed. A. Fröhlich, Academic Press, New York,* 1977.

[24] A. WEIL, Uber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann., vol. 168 (1967),* pp. 149-156.

[25] A. WEIL, Dirichlet Series and Automorphic Forms, *Lecture Notes in Math., vol. 189, Springer-Verlag, New York, 1971.*

[26] A. WEIL, Exercices dyadiques, *Inv. Math. 27 (1974)* pp. 1-22.

[27] N. YUI AND C. JENSEN, Quaternion Extensions, *Algebraic Geometry and Commutative Algebra: In Honor of Masayoshi Nagata, Academic Press, New York, 1988, pp. 155-182.*